Руководство по настройке источников

Версия УМС2.0

Оглавление

Информация по релизам УМС 2.0 . . . 11
О релизе № 15 от 19.05.2026 . . . 11
О релизе № 14 от 05.05.2026 . . . 14
О релизе № 13 от 21.04.2026 . . . 18
О релизе № 12 от 08.04.2026 . . . 21
О релизе № 11 от 24.03.2026 . . . 24
О релизе № 10 от 11.03.2026 . . . 28
О релизе № 9 от 25.02.2026 . . . 32
О релизе № 8 от 10.02.2026 . . . 35
О релизе № 7 от 27.01.2026 . . . 39
О релизе № 6 от 23.12.2025 . . . 44
О релизе № 5 от 16.12.2025 . . . 46
О релизе № 4 от 02.12.2025 . . . 48
О релизе № 3 от 18.11.2025 . . . 51
О релизе № 2 от 05.11.2025 . . . 53
О релизе № 1 от 24.10.2025 . . . 55
Справочная информация по экспертизе . . . 62
Правила нормализации . . . 62
Поддерживаемые источники событий . . . 62
Правила корреляции . . . 70
Памятка по правилам корреляции . . . 70
Аналитические истории . . . 71
Антивирусное ПО . . . 72
Dr.Web Enterprise Security Suite . . . 72
Dr.Web Enterprise Security Suite: настройка источника . . . 72
Kaspersky Secure Mail Gateway . . . 74
Kaspersky Secure Mail Gateway: настройка источника . . . 75
Kaspersky Secure Mail Gateway: правила корреляции . . . 79
Kaspersky Security Center . . . 82
Kaspersky Security Center: настройка источника . . . 82
Kaspersky Security Center: сбор из СУБД MS SQL . . . 82
Kaspersky Security Center: сбор из СУБД MySQL (MariaDB) . . . 90
Kaspersky Security Center: сбор из СУБД PostgreSQL . . . 93
Positive Technologies Sandbox . . . 97
Positive Technologies Sandbox: настройка источника . . . 97
Бизнес-приложения . . . 100
Atlassian Confluence . . . 100
Atlassian Confluence: настройка источника . . . 100
Atlassian Confluence: правила корреляции . . . 105

Atlassian Jira . . . 109
Atlassian Jira: настройка источника . . . 109
Atlassian Jira: правила корреляции . . . 112
Jenkins . . . 119
Jenkins: настройка источника . . . 120
Nextcloud . . . 128
Nextcloud: настройка источника . . . 128
1С:Предприятие . . . 131
1С:Предприятие: настройка источника . . . 132
1С:Предприятие Журнал регистрации . . . 132
1С:Предприятие Технологический журнал . . . 140
Битрикс24 . . . 144
Битрикс24: сбор из СУБД MySQL (MariaDB) . . . 144
Пассворк . . . 148
Пассворк: настройка источника . . . 148
Пассворк: правила корреляции . . . 150
Веб-серверы . . . 157
Apache HTTP Server . . . 157
Apache HTTP Server: настройка источника . . . 157
Microsoft IIS . . . 160
Microsoft IIS: настройка источника . . . 160
Microsoft IIS: правила корреляции . . . 162
Nginx . . . 162
Nginx: настройка источника . . . 163
Межсетевые экраны . . . 165
Check Point Gaia . . . 165
Check Point Gaia: настройка источника . . . 165
Cisco ASA . . . 170
Cisco ASA: настройка источника . . . 170
Cisco ASA: правила корреляции . . . 172
Ideco NGFW . . . 174
Ideco NGFW: настройка источника . . . 174
ИнфоТеКС ViPNet Coordinator 4 . . . 176
ИнфоТеКС ViPNet Coordinator 4: настройка источника . . . 176
Код Безопасности Континент 3.9.3 . . . 180
Код Безопасности Континент 3.9.3: настройка источника . . . 180
Код Безопасности Континент 4 . . . 183
Код Безопасности Континент 4: настройка источника PostgreSQL . . . 183
Код Безопасности Континент 4: настройка источника Syslog . . . 189
Код Безопасности Континент 4: правила корреляции . . . 192
С-Терра Шлюз . . . 194
С-Терра Шлюз: настройка источника Syslog . . . 194

С-Терра Шлюз: правила корреляции 196
Операционные системы 199
Linux 199
Linux Auditd 199
Linux Auditd: настройка источника 199
Linux Auditd: правила корреляции 203
Linux R-Vision Endpoint 269
Linux R-Vision Endpoint: настройка источника 269
Microsoft Windows 272
Microsoft Active Directory Domain Services (ADDS) 273
Microsoft Active Directory Domain Services (ADDS): настройка источника 273
Microsoft Windows PowerShell 277
Microsoft Windows PowerShell: настройка источника 277
Microsoft Windows PowerShell: правила корреляции 279
Microsoft Windows Security 292
Microsoft Windows Security: настройка источника 292
Microsoft Windows Security: настройка расширенного аудита 297
Microsoft Windows Security: правила корреляции 315
Microsoft Windows Sysmon 359
Microsoft Windows Sysmon: настройка источника 359
Microsoft Windows Sysmon: правила корреляции 364
Microsoft Windows System 452
Microsoft Windows System: правила корреляции 452
Microsoft Windows Task Scheduler 524
Microsoft Windows Task Scheduler: настройка источника 525
Почтовые системы и серверы 527
Kaspersky Secure Mail Gateway 527
Kaspersky Secure Mail Gateway: правила корреляции 527
Microsoft Exchange Server 530
Microsoft Exchange Server: настройка источника 530
Microsoft Exchange Server: правила корреляции 537
Прокси-серверы 550
Kaspersky Web Traffic Security 550
Kaspersky Web Traffic Security: настройка источника 550
Solar webProxy 553
Solar webProxy: настройка источника 553
Solar webProxy: правила корреляции 557
Squid 559
Squid: настройка источника 559
Сетевые устройства 562
Cisco IOS 562
Cisco IOS: настройка источника 562

Cisco IOS XE 564
Cisco IOS XE: настройка источника 564
Cisco IOS XR 567
Cisco IOS XR: настройка источника 567
Cisco NetFlow 569
NetFlow Version 9: настройка источника 569
Cisco Nexus 571
Cisco Nexus: настройка источника 571
Eltex ESR 574
Eltex ESR: настройка источника 574
Fortinet FortiAnalyzer 577
Fortinet FortiAnalyzer: настройка источника 577
HP ProCurve 579
HP ProCurve: настройка источника 579
HPE ArubaOS-CX 582
HPE ArubaOS-CX: настройка источника 582
IPFIX 583
IPFIX: настройка источника 583
MikroTik RouterOS 585
MikroTik RouterOS: правила корреляции 585
Netgate pfSense 588
Netgate pfSense: настройка источника 588
Системы sandbox 592
Kaspersky Anti Targeted Attack Platform 592
Kaspersky Anti Targeted Attack Platform: настройка источника 592
Системы анализа сетевого трафика (NTA) 595
Positive Technologies ISIM 595
Positive Technologies ISIM: настройка источника 595
PT Network Attack Discovery 599
PT Network Attack Discovery: настройка источника 599
PT Network Attack Discovery: правила корреляции 602
Suricata 607
Suricata: настройка источника 607
Гарда NDR 609
Гарда NDR: настройка источника 609
Системы аутентификации, авторизации и учета 616
Efros DefOps NAC 616
Efros DefOps NAC: настройка источника 616
Системы виртуализации 619
Microsoft Hyper-V 619
Microsoft Hyper-V: настройка источника 619
Orion soft zVirt 621

Orion soft zVirt: настройка источника 621
VMware 624
VMware ESXi 624
VMware ESXi: настройка источника 625
VMware ESXi: правила корреляции 628
VMware vCenter Server 639
VMware vCenter Server: настройка источника 639
VMware vCenter Server: правила корреляции 641
VMware ESXi и VMware vCenter Server: правила корреляции 647
Системы динамической адресации 656
BIND DNS 656
BIND DNS: настройка источника 656
BIND DNS: правила корреляции 660
Microsoft DNS Server 665
Microsoft DNS Server: настройка источника 665
Microsoft DNS Server: правила корреляции 671
Microsoft DHCP Server 671
Microsoft DHCP Server: настройка источника 672
Системы защиты веб-приложений (WAF) 675
PT Application Firewall 3 675
PT Application Firewall 3: настройка источника 675
PT Application Firewall 4 679
PT Application Firewall 4: настройка источника 679
PT Application Firewall 4: правила корреляции 683
Гарда WAF 689
Гарда WAF: настройка источника 689
Гарда WAF: правила корреляции 694
Системы защиты конечных точек (Endpoint Protection) 699
Check Point Harmony Endpoint 699
Check Point Harmony Endpoint: настройка источника 699
BI.ZONE EDR 704
BI.ZONE EDR: настройка источника 704
Конфидент ЕЦУ Dallas Lock 706
Конфидент ЕЦУ Dallas Lock: настройка источника 706
ЕЦУ Dallas Lock: сбор событий в формате CEF 707
ЕЦУ Dallas Lock: сбор событий из СУБД PostgreSQL 709
Конфидент Dallas Lock 8.0 712
Конфидент Dallas Lock 8.0: настройка источника 712
Dallas Lock 8.0 Сервер Безопасности: сбор событий из СУБД MS SQL 713
Dallas Lock 8.0: сбор событий в формате CEF 730
Microsoft Endpoint Configuration Manager (MECM) 732
Microsoft Endpoint Configuration Manager: настройка источника 732

Код Безопасности Secret Net Studio . . . 737
Код Безопасности Secret Net Studio: настройка источника . . . 737
Код Безопасности Secret Net Studio: правила корреляции . . . 747
Системы защиты сети . . . 751
z_infotecs-vipnet-tias.adoc . . . 751
z_infotecs-vipnet-tias-guide.adoc . . . 751
Системы идентификации и управления доступом . . . 752
Microsoft Active Directory Federation Services (ADFS) . . . 752
Microsoft Active Directory Federation Services (ADFS): настройка источника . . . 752
Microsoft Active Directory Federation Services (ADFS): правила корреляции . . . 757
Multifactor Radius Adapter . . . 759
Multifactor Radius Adapter: настройка источника . . . 759
Системы киберразведки (TI) . . . 764
Kaspersky CyberTrace . . . 764
Kaspersky CyberTrace: настройка источника . . . 764
R-Vision TIP . . . 769
R-Vision TIP: настройка источника . . . 769
Системы мониторинга инфраструктуры . . . 773
Zabbix . . . 773
Zabbix: настройка источника . . . 773
Системы обнаружения и предотвращения вторжений (IDS/IPS) . . . 779
ИнфоТеКС ViPNet IDS NS . . . 779
ИнфоТеКС ViPNet IDS NS: настройка источника . . . 779
ИнфоТеКС ViPNet TIAS . . . 782
ИнфоТеКС ViPNet TIAS: настройка источника . . . 782
Системы организации терминального доступа . . . 786
Microsoft Windows Terminal Services . . . 786
Microsoft Windows Terminal Services: настройка источника . . . 786
Системы организации удаленного доступа . . . 789
OpenVPN . . . 789
OpenVPN: настройка источника . . . 789
OpenVPN и OpenVPN Access Server: правила корреляции . . . 792
VMware Horizon . . . 796
VMware Horizon: настройка источника . . . 796
Системы предотвращения утечек данных (DLP) . . . 800
InfoWatch Traffic Monitor . . . 800
InfoWatch Traffic Monitor: настройка источника . . . 800
InfoWatch Traffic Monitor: правила корреляции . . . 804
Solar Dozor . . . 807
Solar Dozor: настройка источника . . . 807
Гарда DLP . . . 810
Гарда DLP: настройка источника . . . 810

СёрчИнформ КИБ 817
СёрчИнформ КИБ: настройка источника 817
Системы резервного копирования и восстановления 821
Veeam Backup & Replication 821
Veeam Backup & Replication: настройка источника 821
Системы управления базами данных (СУБД) 823
Apache Cassandra 823
Apache Cassandra: настройка источника 823
ClickHouse 827
ClickHouse: настройка источника 827
ClickHouse: правила корреляции 831
MariaDB 836
MariaDB: настройка источника 836
Microsoft SQL Server 842
Microsoft SQL Server: настройка источника 842
Microsoft SQL Server: правила корреляции 853
MongoDB 865
MongoDB: настройка источника 865
Oracle Database 869
Oracle Database: настройка источника 869
Oracle Database (syslog): настройка источника 874
Oracle Database: правила корреляции 877
Oracle MySQL 883
Oracle MySQL: настройка источника 883
Oracle MySQL: правила корреляции 887
PostgreSQL 891
PostgreSQL: настройка источника 891
PostgreSQL: правила корреляции 894
РЕД База Данных 896
РЕД База Данных: настройка источника 896
СберТех Platform V Pangolin DB 899
СберТех Platform V Pangolin DB: настройка источника 899
Системы управления инцидентами ИБ 903
R-Vision SOAR 903
R-Vision SOAR: настройка источника 903
Системы управления ложными сетевыми объектами 906
R-Vision TDP 906
R-Vision TDP: настройка источника 906
Xello Deception 909
Xello Deception: настройка источника 909
Системы управления серверной инфраструктурой 912
Red Hat Ansible AWX 912

Ansible AWX: настройка источника . . . 912
Red Hat Ansible Tower . . . 914
Red Hat Ansible Automation Platform (Automation Controller): настройка источника . . . 914
Microsoft SCOM . . . 916
Microsoft System Center Operations Manager: настройка источника . . . 916
Службы каталогов (Directory Services) . . . 923
FreeIPA . . . 923
FreeIPA: настройка источника . . . 923
FreeIPA: правила корреляции . . . 926
РЕД АДМ . . . 944
РЕД АДМ: настройка источника . . . 944
Прочие системы и источники . . . 948
Sonatype Nexus Repository . . . 948
Sonatype Nexus Repository: настройка источника . . . 948
АйТи Бастион СКДПУ НТ . . . 950
АйТи Бастион СКДПУ НТ: настройка источника . . . 950
Универсальный коннектор CEF . . . 953
Универсальный коннектор CEF: настройка источника . . . 953

Настоящее руководство содержит рекомендации по подключению элементов IT-инфраструктуры организации к системе R-Vision Security Information and Event Management (далее — "R-Vision SIEM" или "система") для организации сбора событий с различных источников.

Документ включает инструкции по интеграции, настройке и проверке источников событий, а также описывает требования к их конфигурации. Руководство предназначено для специалистов, выполняющих внедрение и настройку R-Vision SIEM в организации.

Инструкции, которые содержатся в настоящем руководстве, относятся к универсальной модели события 2.0 (УМС 2.0). Универсальная модель позволяет приводить поступающие в систему базовые события к унифицированному формату с единым набором полей. УМС 2.0 представляет собой развитие предыдущей универсальной модели.

Информация по релизам УМС 2.0

Настройка источников событий в системе R-Vision SIEM обеспечивает сбор и обработку данных для мониторинга и анализа информационной безопасности.

Мы регулярно разрабатываем правила нормализации и корреляции для новых систем. Подробнее с ними можно ознакомиться в наших релизах.



Если у вас есть вопросы по поддерживаемым источникам или запрос на поддержку нового источника, вы можете обратиться в R-Vision SIEM Community.

2026

- О релизе № 15 от 19.05.2026
- О релизе № 14 от 05.05.2026
- О релизе № 13 от 21.04.2026
- О релизе № 12 от 08.04.2026
- О релизе № 11 от 24.03.2026
- О релизе № 10 от 11.03.2026
- О релизе № 9 от 25.02.2026
- О релизе № 8 от 10.02.2026
- О релизе № 7 от 27.01.2026

2025

- О релизе № 6 от 23.12.2025
- О релизе № 5 от 16.12.2025
- О релизе № 4 от 02.12.2025
- О релизе № 3 от 18.11.2025
- О релизе № 2 от 05.11.2025
- О релизе № 1 от 24.10.2025

О релизе № 15 от 19.05.2026

Для использования актуального пакета экспертизы необходимо обновить R-Vision SIEM до версии 2.5.0 и выше.

Кратко о релизе

- Добавлены новые индикаторы компрометации ФСТЭК России от 08.05.2026 по 14.05.2026.
- Внесены улучшения и исправления в правила нормализации для Check Point, Oracle, Microsoft, Solar и Kaspersky.

- Внесены улучшения и исправления в правила детектирования для Linux.
- Поддержаны новые источники: Fortinet FortiGate, Dallas Lock ВИ, Proxmox VE и Eltex MES.
- Добавлены новые правила детектирования для Cisco, Yandex Cloud, Microsoft Hyper-V, Microsoft Exchange, Xello, Solar Dozor и Microsoft Windows.

Правила нормализации

Новые правила

- **Fortinet**:
  - Добавлено правило нормализации для FortiGate.
- **Конфидент**:
  - Добавлено правило нормализации для Dallas Lock ВИ.
- **Proxmox**:
  - Добавлено правило нормализации для Proxmox VE.
- **Eltex**:
  - Добавлено правило нормализации для MES.

Улучшения и исправления

- **Check Point**:
  - NGFW: дополнен перечень обрабатываемых событий.
- **Oracle**:
  - MySQL: исправлено заполнение полей `device_domain`, `device_time`, `dst_user_name`, `dst_user_privileges`.
- **Microsoft**:
  - Active Directory Federation Services (AD FS): исправлена нормализация полей имя пользователя, SID пользователя и `InstanceID`.
  - Hyper-V: добавлены поля с информацией о виртуальных машинах.
  - Exchange: исправлены условия для событий аутентификации `IMAP`.
- **Solar**:
  - Web Proxy: исправлена обработка событий `instruction`.
- **Kaspersky**:
  - Anti Targeted Attack Platform (KATA): расширен фильтр правила для покрытия версий 6 и 7.

Правила детектирования

Новые правила

- **Cisco**:
  - Изменение AAA-серверов на Cisco ASA.

- Изменение настроек межсетевого экрана на Cisco ASA.
- Изменение состояния интерфейса на Cisco ASA.
- Изменение конфигурации VPN на Cisco ASA.
- Изменение привилегий локального пользователя на Cisco ASA.
- Изменение пароля локального пользователя на Cisco ASA.
- Массовые изменения конфигурации на Cisco ASA.
- Перезапуск устройства или модулей Cisco ASA.
- Изменение NTP или системного времени на Cisco ASA.
- Изменение крипто-карт на Cisco ASA.
- Изменение правил NAT на Cisco ASA.
- Отключение или ослабление логирования на Cisco ASA.
- Атака ARP spoofing на Cisco IOS.
- Конфигурация Cisco IOS с недоверенного IP-адреса.

- **Yandex Cloud**:
  - Пользователь не из списка администраторов создал кластер.
  - Пользователь изменил федерацию удостоверений.
  - Пользователь добавил сертификат в федерацию удостоверений.
  - Выданы административные права доступа к каталогу или облаку.
  - Включен небезопасный режим `IMDSv1` на ВМ.
  - Удален симметричный ключ в KMS.
  - Изменены права доступа к симметричному ключу.
  - Виртуальной машине назначен внешний IP-адрес.
  - Пользователю назначены привилегированные роли.
  - Метаданные ВМ содержат чувствительные данные.
  - Активность сервисной учетной записи из диапазона IP-адресов вне облака.
  - Виртуальной машине назначено несколько IP-адресов.
  - Создан публичный IP-адрес без защиты от DDoS-атак.
  - Виртуальной машине назначен сервисный аккаунт с доступом к секретам.
  - Предоставлен доступ к серийной консоли виртуальной машины.
- **Microsoft Hyper-V**:
  - Удалено несколько критичных/защитных ВМ.
  - Массовая приостановка виртуальных машин.
  - Отключена защитная виртуальная машина.
  - Клонирование критичной виртуальной машины.
  - Отключено несколько виртуальных средств защиты.

- **Microsoft Exchange**:
  - Атака Password Spraying по протоколам `IMAP` или `POP`.
  - Добавление и удаление прав к почтовому ящику Exchange за короткое время.
  - Подбор пароля к учетным записям Exchange по протоколам `IMAP` или `POP`.
  - Успешный подбор пароля к учетным записям Exchange по протоколам `IMAP` или `POP`.
- **Xello**:
  - Целенаправленное сканирование портов сервера-ловушки.
  - Попытка подключения к серверу-ловушке как к DB.
  - Вход пользователя в Web-консоль во внерабочее время.
  - Попытка авторизации на сервере-ловушке.
  - Отправка ICMP-пакетов на сервер-ловушку.
  - Попытка подключения к серверу-ловушке по неопределенной службе.
  - Попытка подключения к серверу-ловушке по `HTTP`/`HTTPS`.
  - Попытка подключения к серверу-ловушке по `LLMNR`.
  - Попытка подключения к серверу-ловушке по `RPC`.
  - Попытка подключения к серверу-ловушке по `RDP`.
  - Подключение к серверу-ловушке по протоколу `SSH`.
  - Подключение к серверу-ловушке по протоколу `SMB`.
  - Подключение к серверу-ловушке по протоколу `FTP`.
  - Сработка на сервере-ловушке Xello по web-протоколу.
- **Solar**:
  - В Solar Dozor зарегистрировано событие ИБ.
- **Microsoft Windows**:
  - Доступ к диспетчеру учетных данных.
  - Включение `LLMNR` через `DNSClient`.

Улучшения и исправления

- **Linux**:
  - Уничтожение информации на диске в Linux: корректировка фильтра для исключения ложных срабатываний.
- **Общее**:
  - Таблица IoC: добавлены новые индикаторы компрометации ФСТЭК России от 08.05.2026 по 14.05.2026.

О релизе № 14 от 05.05.2026

Для использования актуального пакета экспертизы необходимо обновить R-Vision SIEM до версии

2.5.0 и выше.

Кратко о релизе

- Добавлены новые индикаторы компрометации ФСТЭК России от 16.04.2026, 23.04.2026 и 29.04.2026.
- Внесены улучшения и исправления в правила нормализации для Ansible, Nexus, Microsoft, Nextcloud, Cisco, Eltex, Xello, Oracle, Solar, VMWare, Код Безопасности.
- Внесены улучшения и исправления в правила детектирования для Windows, Exchange.
- Поддержаны новые источники: Citrix VAD, XenApp, WinRM, WMI, Suricata, zVirt, DistKontrolUSB, Solar Inrights.
- Добавлены новые правила детектирования для VMware vCenter, Континент 4, Cisco ASA, Yandex Cloud, Windows, Solar Web Proxy, Linux, Microsoft SQL Server, Eltex vESR, Oracle Database.

Правила нормализации

Новые правила

- **Citrix**:
  - Добавлено правило нормализации для Citrix VAD.
  - Добавлено правило нормализации для XenApp.
- **Windows**:
  - Добавлено правило нормализации для WinRM.
- **Microsoft**:
  - Добавлено правило нормализации для WMI.
- **Suricata**:
  - Добавлено правило нормализации для Suricata.
- **zVirt**:
  - Добавлено правило нормализации для zVirt.
- **DistKontrolUSB**:
  - Добавлено правило нормализации для DistKontrolUSB.
- **Solar**:
  - Добавлено правило нормализации для Solar Inrights.

Улучшения и исправления

- **Ansible**:
  - AWX: исправлена категоризация, уточнены события входа, исправлено описание событий.
- **Nexus**:
  - Nexus Repository: исправление категоризации и поля `description`.
- **Microsoft**:

    - SQL Server: внесены правки в парсинг поля `is_dac`.
    - Exchange: исправлены условия для событий аутентификации для `POP3`.
    - Windows Security: добавлена нормализация события `4888`.
    - DNS Server: добавлена нормализация событий `eventid 525`, `eventid 569`.
- **Nextcloud**:
    - Nextcloud: исправление категоризации и полей `description`.
- **Cisco**:
    - IOS XE: правки категоризации.
    - NetFlow v9: удалено неиспользуемое условие, поправлено `description`.
    - ASA: нормализованы новые типы событий `411003`, `733100`.
- **Eltex**:
    - Eltex ESR: добавлены поля нормализации.
- **Xello**:
    - Deception: исправлены поля `device`.
- **Oracle**:
    - Database: небольшие правки в нормализации.
- **Solar**:
    - Dozor: добавлена обработка событий ИБ.
- **VMWare**:
    - Horizon: нормализованы новые типы событий.
    - vCenter: добавлена нормализация новых типов событий.
- **Код Безопасности**:
    - Континент 4: расширен частный маппинг.

Правила детектирования

Новые правила

- **VMware vCenter**:
    - Назначение административных или глобальных прав vCenter.
- **Континент 4**:
    - Изменение правил межсетевого экранирования Континент.
    - Добавление пользователя в критическую группу Континент TLS.
    - Изменение административной УЗ Континент TLS.
- **Cisco ASA**:
    - Потенциальная атака DoS на Cisco ASA.
    - Множественное выполнение команды `show`.

    - Изменение правил ACL на Cisco ASA.
- **Yandex Cloud**:
    - Создание, изменение и удаление групп безопасности.
- **Windows**:
    - Выполнение скриптов через проксирование `PubPrn`.
- **Solar Web Proxy**:
    - Изменены параметры внешних подключений на Solar Web Proxy.
    - Изменены критичные параметры системы Solar Web Proxy.
    - Изменение правил межсетевого экранирования и доступа в Solar Web Proxy.
- **Linux**:
    - Запуск процесса из нестандартной директории.
- **Microsoft SQL Server**:
    - Попытка подключения к СУБД через `DAC`.
- **Eltex vESR**:
    - Создание пользователя на Eltex vESR.
    - Изменение парольной политики на Eltex vESR.
    - Отключение межсетевого экрана на Eltex vESR.
    - Срабатывание функции защиты на Eltex vESR.
    - Журналирование отключено на Eltex vESR.
    - Успешный подбор пароля к маршрутизатору Eltex vESR.
    - Подбор пароля к маршрутизатору Eltex vESR.
    - Атака Password Spraying на Eltex vESR.
    - Вход привилегированного пользователя на Eltex vESR с неизвестного хоста.
- **Oracle Database**:
    - Экспорт базы данных Oracle.
    - Вход привилегированного пользователя в СУБД Oracle.
    - Манипуляция с учетными данными СУБД Oracle.
    - Подбор пароля к СУБД Oracle.
    - Поиск информации о структуре в OracleDB.
    - Успешный подбор пароля к СУБД Oracle.
    - Атака Password Spraying на OracleDB.
    - Поиск информации о конфигурации OracleDB.
    - Получение информации о пользователях СУБД Oracle.

Улучшения и исправления

- **Windows**:

    - Закрепление через изменения ключей автозапуска в реестре: добавлена проверка изменения переменной `path`.
    - Подгрузка подозрительного пакета процессом `lsass`: добавлено исключение для библиотеки `SFAPM.dll`.
    - Несистемный процесс повысил привилегии до системы: корректировка фильтра для исключения ложных срабатываний.
- **Exchange**:
    - Сбор адресов электронной почты: добавлены новые команды разведки.
- **Общее**:
    - Таблица IoC: добавлены новые индикаторы компрометации ФСТЭК России от 16.04.2026, 23.04.2026 и 29.04.2026.

О релизе № 13 от 21.04.2026

Для использования актуального пакета экспертизы необходимо обновить R-Vision SIEM до версии 2.5.0 и выше.

Кратко о релизе

- Добавлены новые индикаторы компрометации ФСТЭК России от 10.04.2026.
- Внесены улучшения и исправления в правила нормализации для Kaspersky Security Center, Kaspersky Anti Targeted Attack Platform, InfoWatch, Solar, Xello, Код Безопасности и универсальных функций системы.
- Внесены улучшения и исправления в правила детектирования для Microsoft Windows, Kaspersky, Linux и VMware.
- Выполнен перевод на Универсальную модель событий 2.0 (УМС 2.0) и поддержаны новые источники: Solar Web Proxy, UserGate NGFW, Microsoft Exchange, Cisco Nexus, MultiFactor RADIUS, Apache Cassandra, Citrix NetScaler, РЕД СОФТ РЕД АДМ, Eltex ESR и СберТех Pangolin SE.
- Добавлены новые правила детектирования для Код Безопасности Континент 4, Kaspersky, Microsoft Windows, Linux и InfoWatch Traffic Monitor.

Правила нормализации

Новые правила

- **Solar**:
    - Перевод правила нормализации для Web Proxy на модель 2.0.
- **UserGate**:
    - Перевод правила нормализации для NGFW на модель 2.0.
- **Microsoft**:
    - Добавлено правило нормализации Exchange для журналов IMAP и POP.
    - Перевод правила нормализации для Exchange Online на модель УМС 2.0.

- **Cisco**:
  - Перевод правила нормализации для Nexus на модель 2.0.
- **MultiFactor**:
  - Покрытие источника RADIUS в УМС 2.0.
- **Apache**:
  - Перевод правила нормализации для Cassandra в УМС 2.0.
- **Citrix**:
  - Перевод правила нормализации для NetScaler на модель 2.0.
- **РЕД СОФТ**:
  - Перевод правила нормализации для РЕД АДМ на модель 2.0.
- **Eltex**:
  - Добавлено правило нормализации для ESR.
- **СберТех**:
  - Перевод правила нормализации для Pangolin SE на модель 2.0.

Улучшения и исправления

- **Все источники**:
  - В правила нормализации добавлено приведение к строке значения, передаваемого в функцию `rv_contains_any()`.
- **Kaspersky**:
  - Kaspersky Anti Targeted Attack Platform (KATA): исправление поля `description`.
  - Kaspersky Security Center: донормализация события `klaud_ev_serverconnect`.
  - Kaspersky Security Center: оптимизация структуры правила, использование if-else в частном маппинге.
- **InfoWatch**:
  - Traffic Monitor: исправлена нормализация в событиях `update object`.
- **Solar**:
  - Dozor: поправлена категоризация событий.
- **Xello**:
  - Deception: обогащение нормализации частных событий.
- **Код Безопасности**:
  - Континент 4: модифицирована обработка событий ролей (БД).

Правила детектирования

Новые правила

- **Континент 4**:

    - Успешный подбор пароля к серверу Континент TLS.
    - Подбор пароля к серверу Континент TLS.
    - Вход привилегированного пользователя с неизвестного хоста.
    - Подбор пароля Континент методом Password Spraying.
- **Kaspersky**:
    - Множество хостов заражены одним типом ВПО.
    - Множественное срабатывание вердиктов средств АВЗ на одном хосте за сутки.
    - Программа безопасности не запущена.
    - Вирусная атака.
- **Microsoft Windows**:
    - Запуск неподписанного установочного файла TrueConf.
    - Массовые запросы сертификатов AD CS.
    - Включение флага SAN в AD CS.
    - Подмена установочных файлов TrueConf.
    - NTLM Relay на AD CS.
    - Аномальная аутентификация с использованием сертификата.
    - Злоупотребление выдачей сертификатов AD CS.
    - Уязвимая конфигурация шаблона AD CS.
    - Блокировка сервисного аккаунта.
    - Возможное сокрытие запланированной задачи.
- **Linux**:
    - Изменение меток времени через `touch`.
    - Отключение узла Linux.
    - Удаление пользователя или группы.
- **InfoWatch TM**:
    - Вход администратора на InfoWatch TM.
    - Массовое удаление пользователей.
    - Создание роли администратора в InfoWatch TM.
    - Создание администратора в InfoWatch TM.
    - Отключение политики защиты данных в InfoWatch TM.
    - Атака Brute Force к InfoWatch TM.
    - Успешная атака Brute Force к InfoWatch TM.
    - Password Spraying в InfoWatch TM.

Улучшения и исправления

- **Microsoft Windows**:

    - Запуск whoami с правами системы: добавлена проверка на легитимные ТУЗ.
    - Использование хакерской утилиты PowerSploit: исправления фильтра для исключения ложных срабатываний.
    - Вход на несколько узлов под одной учетной записью: внесены исправления в работу исключений.
    - Смена ассоциации запуска файла: добавлена поддержка событий Security 4657.
    - Внедрение стороннего ПО через отладчик IFEO: добавлена поддержка событий Security 4657.
    - Добавление в Appinit DLL полезной нагрузки: добавлена поддержка событий Security 4657.
    - Зафиксирована подмена файлов экрана заставки Windows: добавлена поддержка событий Security 4657.
    - Закрепление через изменения ключей автозапуска в реестре: добавлена поддержка событий Security 4657.
    - Кодирование файла в Base64 с помощью Certutil: добавлена поддержка флага `-decode`.
    - Изменение доверительных отношений между доменами: добавлена поддержка событий PowerShell.
- **Kaspersky**:
    - Множество хостов заражены одним типом ВПО: изменена нормализация в `on_correlate`.
- **Linux**:
    - Создание туннелей и перенаправление трафика: корректировка фильтра для исключения ложных срабатываний.
    - Изменение конфигурационных файлов службы firewalld: расширение корреляционного фильтра.
    - Изменение привилегий файлов Linux: расширение корреляционного фильтра.
    - Большое количество подозрительных команд: расширение корреляционного фильтра.
    - Разведка локальных УЗ в Linux: расширение корреляционного фильтра.
- **VMware**:
    - Отключено несколько критичных виртуальных машин: в описание добавлен период времени активности.
- **Общее**:
    - Таблица IoC: добавлены новые индикаторы компрометации ФСТЭК России от 10.04.2026.

О релизе № 12 от 08.04.2026

Для использования актуального пакета экспертизы необходимо обновить R-Vision SIEM до версии 2.5.0 и выше.

Кратко о релизе

- Добавлены новые индикаторы компрометации ФСТЭК России в период с 26.03.2026 по 03.04.2026.

- Внесены улучшения и исправления в правила нормализации для ClickHouse, Kaspersky, Linux, HPE ArubaOS и Microsoft Windows.
- Внесены улучшения и исправления в правила детектирования для Microsoft Windows.
- Поддержаны новые источники: pfSense, PT Application Firewall 4, Microsoft DNS Server, Microsoft ECM, Microsoft SCOM, Гарда NDR, Jenkins, HP ProCurve, Cisco IOS XR, Cisco IOS XE и S-Terra Gate.
- Добавлены новые правила детектирования для Solar Web Proxy, S-Terra Gate, Kaspersky, MikroTik, Cisco ASA, PT Application Firewall 4 и Microsoft SQL Server.

Правила нормализации

Новые правила

- **pfSense**:
  - Добавлено правило нормализации для pfSense.
- **PT Application Firewall 4**:
  - Добавлено правило нормализации для событий аудита PT Application Firewall 4.
- **Microsoft**:
  - Добавлено правило нормализации для DNS Server.
  - Добавлено правило нормализации для ECM.
  - Добавлено правило нормализации для SCOM.
- **Гарда**:
  - Добавлено правило нормализации для Гарда NDR.
- **Jenkins**:
  - Добавлено правило нормализации для Jenkins.
- **HP**:
  - Добавлено правило нормализации для ProCurve.
- **Cisco**:
  - Добавлено правило нормализации для IOS XR.
  - Добавлено правило нормализации для IOS XE.
- **S-Terra**:
  - Добавлено правило нормализации для Gate ST.

Улучшения и исправления

- **ClickHouse**:
  - ClickHouse: исправлена нормализация.
- **Kaspersky**:
  - Security Center: донормализация событий `000000d5`, `000000d3`.
- **Linux**:

- secure/auth: исправлена обработка ошибок.

- **HPE**:
  - ArubaOS: исправлена таблица обогащения.
- **Microsoft**:
  - Windows Security: добавлена нормализация событий `4608`, `4609`, `4611`, `4616`, `4634` и новых типов событий.

Правила детектирования

Новые правила

- **Solar**:
  - Изменение критичных ролей Solar Web Proxy.
  - Создание нового пользователя в Solar Web Proxy.
  - Вход привилегированной учетной записи с неизвестного IP в SWP.
- **S-Terra**:
  - Вход в привилегированный режим на S-Terra Gate.
  - Настроена отправка логов на неизвестный узел.
  - Удален файл на S-Terra Gate.
  - Выдача максимальных привилегий для пользователя.
  - Изменен пароль для привилегированного режима.
  - Создан пользователь на S-Terra Gate.
  - Очищен файл конфигурации на S-Terra Gate.
  - Отключена отправка событий на S-Terra Gate.
  - Подбор пароля для привилегированного режима.
- **Kaspersky**:
  - Самозащита антивируса ограничила доступ к защищаемому ресурсу.
  - Выключение механизма самозащиты KES.
- **MikroTik**:
  - Изменение конфигураций фильтра в MikroTik.
- **Cisco**:
  - Подбор пароля через SSH к Cisco ASA.
  - Успешный подбор пароля через SSH к Cisco ASA.
  - Доступ к привилегированному режиму после авторизации.
  - Успешный подбор пароля в привилегированный режим Cisco ASA.
- **PT Application Firewall 4**:
  - Попытка удаленного выполнения кода.

    - Атака на веб-ресурс.
    - Внедрение SQL-кода.
    - Атака типа SSRF.
    - Атака типа CSRF.
    - Атака типа XSS.
    - Попытка эксплуатации уязвимостей.
    - Атака на различные веб-ресурсы.
    - Атака с загрузкой файла.
    - Использование сканера уязвимостей.
    - Множество атак на веб-ресурс.
    - Подбор пароля к форме авторизации.
- **Microsoft SQL Server**:
    - Выгрузка ключа шифрования или сертификата MSSQL.
    - Поиск по регулярному выражению в объектах БД.

Улучшения и исправления

- **Microsoft Windows**:
    - Изменение атрибута для скрытия файла через PowerShell: исправление фильтра для исключения ложных срабатываний.
    - Добавление исполняемого файла к профилю PowerShell: исправление фильтра для исключения ложных срабатываний.
- **Общее**:
    - Таблица IoC: добавлены новые индикаторы компрометации ФСТЭК России от 26.03.2026 по 03.04.2026.

О релизе № 11 от 24.03.2026

Для использования актуального пакета экспертизы необходимо обновить R-Vision SIEM до версии 2.5.0 и выше.

Кратко о релизе

- Добавлены новые индикаторы компрометации ФСТЭК России от 12.03.2026 и 19.03.2026.
- Внесены улучшения и исправления в правила нормализации для OpenVPN, Гарда WAF и PT Network Attack Discovery.
- Внесены улучшения и исправления в правила детектирования для Microsoft Windows, PT Network Attack Discovery, Kaspersky и Microsoft SQL Server.
- Поддержаны новые источники: Ansible AWX, HPE ArubaOS, Squid, Гарда DLP и ИнфоТеКС ViPNet Coordinator 4.
- Добавлены новые правила детектирования для MySQL, Atlassian Confluence, ClickHouse, OpenVPN,

Microsoft SQL Server, Microsoft Windows, PostgreSQL и Гарда WAF.

Правила нормализации

Новые правила

- **Red Hat**:
  - Добавлено правило нормализации для Ansible AWX.
- **HPE**:
  - Добавлено правило нормализации для ArubaOS.
- **Squid**:
  - Добавлена поддержка источника.
- **ИнфоТеКС**:
  - Добавлено правило нормализации для ViPNet Coordinator 4.
- **Гарда**:
  - Добавлено правило нормализации для Гарда DLP.

Улучшения и исправления

- **Positive Technologies**:
  - PT Network Attack Discovery: добавлен парсинг cve из события атаки.
- **OpenVPN**:
  - OpenVPN: исправлена нормализация.
- **Гарда**:
  - Гарда WAF: исправлено приведение типов для пользовательских полей.
- **Все источники**:
  - Исправлено заполнение *_label для пользовательских полей, убран символ пустой строки для корректной работы RQL-запросов.

Правила детектирования

Новые правила

- **Microsoft Windows**:
  - Использование инструмента SharpHound.
- **MySQL**:
  - Чтение журналов MySQL.
  - Вход привилегированного пользователя в MySQL.
  - Успешный подбор пароля к СУБД MySQL.
  - Подбор пароля к СУБД MySQL.
  - Атака Password Spraying на СУБД MySQL.

- Назначение прав администратора MySQL.
- Остановка сессии пользователя в MySQL.
- Изменение пароля учетной записи MySQL.
- Массовое удаление таблиц MySQL.
- Изменение/удаление таблицы аудита MySQL.
- Создание резервной копии MySQL.
- Удаление базы данных в MySQL.
- Получение информации о версии MySQL.
- Получение списка подключений к MySQL.
- Просмотр пользовательских данных MySQL.

- **PostgreSQL**:
  - Изменение параметров аудита базы данных PostgreSQL.
  - Вход привилегированного пользователя с неизвестного хоста.
  - Взаимодействие с файловой системой из базы данных PostgreSQL.
  - Получение информации о существующих учетных записях в PostgreSQL.
  - Попытка удаления базы данных в PostgreSQL.
  - Изменен пароль от учетной записи с правами superuser в PostgreSQL.
  - Новая учетная запись с правами superuser в PostgreSQL.
  - Разведка структуры базы данных PostgreSQL.
  - Обнаружена попытка дампа базы данных или учетных данных PostgreSQL.
  - Успешный перебор пароля к СУБД PostgreSQL.
  - Атака типа Password Spraying к СУБД PostgreSQL.
  - Множественные неудачные попытки подключения к PostgreSQL.
- **ClickHouse**:
  - Изменение или удаление таблицы аудита ClickHouse.
  - Вход привилегированного пользователя в ClickHouse.
  - Попытка удаления базы данных в ClickHouse.
  - Создание привилегированного пользователя в ClickHouse.
  - Взаимодействие с файловой системой из БД ClickHouse.
  - Небезопасный способ аутентификации пользователя ClickHouse.
  - Использование LIKE для разведки в ClickHouse.
  - Попытка удаления нескольких таблиц в ClickHouse.
  - Получение информации о системе в ClickHouse.
  - Создание дампа таблиц в ClickHouse.
  - Атака Password Spraying на СУБД ClickHouse.

- Подбор пароля к СУБД ClickHouse.
- Успешный подбор пароля к СУБД ClickHouse.
- Получение информации о структуре ClickHouse.
- Изменение конфигурации базы данных ClickHouse.

- **OpenVPN**:
  - Успешный подбор пароля клиента OpenVPN.
- **Atlassian Confluence**:
  - Эксплуатация уязвимости в Confluence - CVE-2023-22515.
- **Microsoft SQL Server**:
  - Удаление нескольких таблиц в MS SQL Server.
  - Отправка результатов SQL-запроса почтой.
  - Попытка изменить состояние службы Windows.
  - Удаление базы данных в MS SQL Server.
  - Назначена роль администратора пользователю MS SQL Server.
  - Использование хранимых процедур sp_proxy и sp_grant_proxy.
  - Изменение аудита базы данных MS SQL Server.
  - Отключение политики входа пользователей MSSQL.
  - Попытка включить смешанную аутентификацию MSSQL.
  - Запись ключа реестра средствами MSSQL.
  - Включение небезопасных параметров в конфигурации MSSQL.
  - Установка небезопасного свойства MSSQL.
  - Использование процедур для локального выполнения кода.
  - Чтение ключа реестра средствами MSSQL.
  - Поиск резервных копий базы данных.
  - Получение информации о пользователях MSSQL.
  - Получение информации об аудите MS SQL Server.
  - Поиск пользователей с административными правами в MSSQL.
  - Получение информации об алгоритме шифрования БД.
  - Изменение пароля привилегированной УЗ MS SQL Server.
  - Вход привилегированного пользователя в MS SQL Server.
- **Гарда WAF**:
  - Множественные атаки на веб-приложение Гарда WAF.
  - Множественная атака на веб-приложение Гарда WAF.
  - Атака на веб-приложение Гарда WAF.

Улучшения и исправления

- **Windows**:
  - Аномальное поведение офисного ПО: добавлен тег.
  - Создание резервных копий MSSQL средствами PowerShell: добавлен блок response.
  - Использование WinApi через PowerShell: исправление фильтра для исключения ложных срабатываний.
- **PT Network Attack Discovery**:
  - Обнаружена попытка эксплуатации уязвимости: добавлено поле номера уязвимости.
- **Kaspersky**:
  - Обнаруженное вредоносное ПО не было удалено: исправлен фильтр второго алиаса.
- **Microsoft SQL Server**:
  - Доступ к локальной файловой системе MSSQL: расширение корреляционного фильтра.
  - Получение информации о версии MSSQL: расширение корреляционного фильтра.
- **Общее**:
  - Таблица IoC: добавлены новые индикаторы компрометации ФСТЭК России от 19.03.2026.
  - Таблица IoC: добавлены новые индикаторы компрометации ФСТЭК России от 12.03.2026.

О релизе № 10 от 11.03.2026

Для использования актуального пакета экспертизы необходимо обновить R-Vision SIEM до версии 2.5.0 и выше.

Кратко о релизе

- Добавлены новые индикаторы компрометации ФСТЭК России от 20.02.2026—26.02.2026.
- Внесены улучшения в правила нормализации для Kaspersky Anti Targeted Attack (KATA).
- Внесены улучшения и исправления в правила детектирования для Microsoft Windows и Linux.
- Поддержаны новые источники: Xello Deception, JetBrains TeamCity, Oracle Database, Dr.Web Enterprise Security Suite, Remote Desktop Services, Nextcloud, Cisco IPFIX, R-Vision Endpoint, Битрикс24, Гарда DBF, РЕД База Данных, СёрчИнформ КИБ.
- Добавлены новые правила детектирования для Microsoft Windows, Microsoft SQL Server, Microsoft Windows DNS Server, BIND DNS, PostgreSQL, Secret Net Studio, Atlassian Confluence, PT Network Attack Discovery, Гарда WAF.

Правила нормализации

Новые правила

- **Xello**:
  - Добавлено правило нормализации для Xello Deception.
- **JetBrains**:

    - Добавлено правило нормализации для TeamCity.
- **Oracle**:
    - Добавлено правило нормализации для Oracle Database.
- **Dr.Web**:
    - Добавлено правило нормализации для Dr.Web Enterprise Security Suite.
- **Microsoft Windows**:
    - Добавлено правило нормализации для Remote Desktop Services.
- **Nextcloud**:
    - Добавлено правило нормализации для Nextcloud.
- **Cisco**:
    - Добавлено правило нормализации для IPFIX.
- **R-Vision**:
    - Добавлено правило нормализации для R-Vision Endpoint.
- **1С-Битрикс**:
    - Добавлено правило нормализации для Битрикс24.
- **Гарда**:
    - Добавлено правило нормализации для Гарда DBF.
- **РЕД СОФТ**:
    - Добавлено правило нормализации для РЕД База Данных.
- **СёрчИнформ**:
    - Добавлено правило нормализации для СёрчИнформ КИБ.

Улучшения

- **Kaspersky**:
    - KATA: добавлена нормализация новых типов событий.

Правила детектирования

Новые правила

- **Microsoft Windows**:
    - Удаленное использование утилиты Atexec.
    - Атака Password Spraying на MS SQL Server.
    - Подбор пароля к MS SQL Server.
    - Изменение атрибутов учетной записи.
    - Создание резервной копии БД MS SQL Server.
- **Microsoft SQL Server**:

- Доступ к локальной файловой системе MSSQL.
- Получение информации о пользователях ОС.
- Получение информации о привилегиях пользователя MSSQL.
- Успешный подбор пароля MS SQL Server.
- Получение хэша пароля пользователей MSSQL.
- Попытка получить состояние службы Windows.
- Получение информации о версии MSSQL.
- Создание резервной копии БД MS SQL Server.

- **Microsoft Windows DNS Server**:
  - Несанкционированное изменение конфигурации DNS-сервера.
- **BIND DNS**:
  - Обнаружен DNS-запрос к Killswitch-домену WannaCry.
  - Обнаружен DNS-запрос к пулам Monero.
  - Использование DNS-туннеля.
  - Обнаружен DNS-запрос к подозрительным внешним службам.
  - Обнаружен DNS-запрос к ресурсам Telegram API.
  - Передача зоны DNS на недоверенный узел (AXFR).
  - Обнаружен DNS-запрос к домену localtonet.
  - Множественные DNS-запросы с одного устройства.
- **PostgreSQL**:
  - Изменение файла конфигурации базы данных PostgreSQL.
- **Secret Net Studio**:
  - Нарушение целостности объекта системы.
  - Изменение критически важной учетной записи.
  - Массовая блокировка узлов Secret Net Studio.
  - Многократная смена пароля учетной записи.
  - Изменение политики безопасности Secret Net Studio.
  - Массовая разблокировка узлов Secret Net Studio.
  - Вход пользователя из черного списка.
  - Отключение защитного механизма в Secret Net Studio.
  - Отключение механизма самозащиты в Secret Net Studio.
  - Изменение правил межсетевого экрана в Secret Net Studio.
  - Очищен журнал событий Secret Net Studio.
  - Подключено съемное устройство к компьютеру.
- **Atlassian Confluence**:

- Создание множества страниц Confluence.
- Эксплуатация уязвимости в Confluence — CVE-2023-22527.
- Выгрузка пространства Confluence.
- Выполнение OGNL-инъекции через Java-выражения в Confluence.
- Отключение аудита журналов приложения Confluence.
- Эксплуатация уязвимости в Confluence — CVE-2023-22518.
- Множественные попытки входа на веб-сервер Confluence.
- Выгрузка множества страниц Confluence.

- **PT Network Attack Discovery**:
  - Запрос на репликацию от недоверенного DNS-сервера.
  - Атака DCShadow PT NAD.
  - Попытки получения информации об учетных записях.
  - Атака DCSync PT NAD.
  - Обнаружен индикатор компрометации — IOC.
  - Обнаружены признаки использования вредоносной утилиты.
  - Обнаружена попытка эксплуатации уязвимости.
  - Подозрительная сетевая активность с нескольких узлов.
  - Подозрительная сетевая активность с одного узла.
  - Признаки использования утилиты для туннелирования трафика.
- **Гарда WAF**:
  - Отключение или изменение паттерна Garda WAF.
  - Массовое удаление УЗ Garda WAF.
  - Изменение настроек защиты подключенного сервера.
  - Добавление пользователю критичной роли Garda WAF.
  - Успешный подбор пароля к Garda WAF.
  - Подбор пароля пользователя к Garda WAF.
  - Атака Password Spraying к Garda WAF.

Улучшения и исправления

- **Windows**:
  - Закрепление через изменения ключей автозапуска в реестре: добавлено исключение для Microsoft Edge для уменьшения ложных срабатываний.
  - Выполнение команд в системе от редактора кода VSCode: корректировка фильтра для исключения ложных срабатываний.
  - Использование хакерской утилиты SharpHound: добавлен дополнительный командлет.
- **Linux**:

    - Изменение критичных файлов конфигурации интерактивной оболочки: исправлен фильтр.
    - Повышение привилегий до root: исправлен фильтр.
    - Повышение привилегий с помощью GTFOBins: добавлена проверка событий для уменьшения FP.
- **Общее**:
    - Таблица IoC: добавлены новые индикаторы компрометации ФСТЭК России от 20.02.2026—26.02.2026.

О релизе № 9 от 25.02.2026

Для использования актуального пакета экспертизы необходимо обновить R-Vision SIEM до версии 2.5.0 и выше.

Кратко о релизе

- Добавлены новые индикаторы компрометации ФСТЭК России от 06.02.2026—16.02.2026.
- Внесены улучшения в правила нормализации для MySQL.
- Внесены улучшения и исправления в правила детектирования для Microsoft Windows и Linux.
- Поддержаны новые источники: Fortinet FortiAnalyzer, Check Point GAiA, Nexus Repository, Windows Task Scheduler, AV Soft ATHENA, R-Vision TIP, ЕЦУ Dallas Lock, Сервер безопасности Dallas Lock.
- Добавлены новые правила детектирования для Microsoft Windows, MikroTik, Linux, OpenVPN, Atlassian Jira.

Правила нормализации

Новые правила

- **Fortinet**:
    - Добавлено правило нормализации для FortiAnalyzer.
- **Check Point**:
    - Добавлено правило нормализации для Check Point GAiA.
- **Nexus**:
    - Добавлено правило нормализации для Nexus Repository.
- **Microsoft**:
    - Добавлено правило нормализации для Windows Task Scheduler.
- **AV Soft**:
    - Добавлено правило нормализации для ATHENA.
- **R-Vision**:
    - Добавлено правило нормализации для R-Vision TIP.
- **Конфидент**:
    - Добавлено правило нормализации для ЕЦУ Dallas Lock.

- Добавлено правило нормализации для Сервера безопасности Dallas Lock.

Улучшения и исправления

- **Oracle**:
  - MySQL: добавлена нормализация новых типов событий.

Правила детектирования

Новые правила

- **Microsoft Windows**:
  - Использование средств виртуализации.
  - Потенциально вредоносное использование элементов панели управления.
  - Скачивание файлов через msedge_proxy.exe.
  - Изменение прав доступа к файлам.
  - Запуск процесса AddinUtil.exe из подозрительной директории.
  - Запуск произвольной DLL библиотеки средствами Msiexec.exe.
  - Создание нового процесса с помощью Taskmgr.exe.
  - Вызов функции DllUnregisterServer через Msiexec.exe.
  - Отключение логирования событий IIS.
  - Запуск замаскированного исполняемого файла через conhost.exe.
  - Запуск PowerShell окна в скрытом режиме.
  - Удалена глобальная группа с включенной безопасностью.
  - Генерация окна ввода пароля через Zenity.
  - Скачивание файлов с IP-адреса через CertOC.EXE.
  - Необычный аргумент или дочерний процесс Wlrmdr.exe.
  - Изменение пароля через утилиту mimikatz.
  - Кодирование в Base64 файла в подозрительном каталоге с помощью Certutil.
  - Скачивание файлов через Squirrel.exe.
  - Скачивание файлов через imewdbld.exe.
  - Изменение SID-History.
  - Отключение ETW провайдера Windows Defender.
  - Детектирование создания wmi подписки.
  - Подозрительный агент обновления Windows.
  - Скачивание файла средствами ProtocolHandler.
  - Запуск MSBuild для выполнения кода.
  - Компрометация через KrbRelayUp.

- Экспорт структуры AD через csvde.exe.
- Сброс пароля учетной записи через mimikatz.
- Необычное выполнение приложений через AtBroker.exe.
- Дамп памяти процесса средствами Dotnet-Dump.
- Выполнение разведки удаленных систем.
- Сбор структуры AD средствами Ldifde.
- Атака Pass the Ticket.
- Скачивание файлов через PresentationHost.exe.
- Запуск файла из Корзины.
- Использование устаревшей версии PowerShell v2.
- Добавление расширения в браузер средством CLI.
- Подозрительная DLL загружена средствами CertOC.exe.
- Установка root сертификата средствами CertMgr.exe.
- Закрепление в системе через Narrator.exe.
- Отключение или модификация Windows Defender.
- Изменение дескриптора безопасности в групповой политике.
- Импорт ключа реестра из ADS.
- Кодирование файла в Base64 с помощью Certutil.
- Изменение политик Windows Defender Firewall.
- SIP Hijacking Windows.
- Запуск подозрительного cab файла через msdt.exe.
- Скачивание файлов средствами MS-AppInstaller.
- Атака Code Signing Windows.
- Попытка дампа оперативной памяти с помощью RdrLeakDiag.exe.
- Атака CS Policy Modification.
- Отключение Privacy Settings Experience в реестре.
- Изменение доверительных отношений между доменами.
- Дамп памяти ядра через LiveKD.
- Обнаружение стеганографии в Windows.

- **MikroTik**:
  - Изменение групп в MikroTik.
- **Linux**:
  - Генерация окна ввода пароля через Zenity.
  - Атака regreSSHion.
  - Загрузка webshell оболочки Linux.

- Изменение библиотеки liblzma.
- Повышение привилегий при помощи pkexec.

- **OpenVPN**:
  - Множество неуспешных HTTP-запросов к OpenVPN AS.
  - Аномальный HTTP-запрос к webUI Access Server.
  - Подбор пароля в веб-консоль OpenVPN AS.
  - Подбор пароля клиента OpenVPN.
  - Подключение OpenVPN за пределами России.
- **Atlassian**:
  - Экспорт множества задач в Jira.

Улучшения и исправления

- **Windows**:
  - Использование хакерской утилиты OWA-Toolkit: скорректирован фильтр для исключения ложных срабатываний.
  - Использование вредоносных утилит: внесены корректировки в фильтр для снижения ложных срабатываний.
  - Эксплуатация Active Setup в реестре: изменен фильтр для снижения ложных срабатываний.
  - Ослабление защиты или мониторинга системы: исправлен фильтр событий eventid 4 для событий Sysmon.
- **Linux**:
  - Доступ к критичным файлам SSSD: добавлены исключения для системных процессов.
- **Общее**:
  - Таблица IoC: добавлены новые индикаторы компрометации ФСТЭК России от 06.02.2026—16.02.2026.

О релизе № 8 от 10.02.2026

Для использования актуального пакета экспертизы необходимо обновить R-Vision SIEM до версии 2.5.0 и выше.

Кратко о релизе

- Добавлены новые индикаторы компрометации ФСТЭК России от 30.01.2026.
- Внесены улучшения и исправления в правила нормализации для Atlassian Jira, Microsoft Exchange, Microsoft IIS, Microsoft Sysmon, Microsoft Windows Security.
- Внесены исправления в правила детектирования для Microsoft Windows и Linux.
- Поддержаны новые источники: Ideco NGFW, MongoDB Enterprise, Redis Enterprise Software, R-Vision SOAR, R-Vision TDP, MikroTik RouterOS, VMware Horizon, Oracle MySQL, Atlassian Confluence, Kaspersky Web Traffic Security (KWTS), PT Sandbox, 1С:Предприятие.

- Добавлены новые правила детектирования для Microsoft Windows, Microsoft Exchange, MikroTik, Linux, VMware ESXi, VMware vCenter Server.

Правила нормализации

Новые правила

- **Ideco**:
  - Добавлено правило нормализации для NGFW.
- **MongoDB**:
  - Добавлено правило нормализации для MongoDB Enterprise.
- **Redis**:
  - Добавлено правило нормализации для Redis Enterprise Software.
- **R-Vision**:
  - Добавлено правило нормализации для SOAR.
  - Добавлено правило нормализации для TDP.
- **MikroTik**:
  - Добавлено правило нормализации для RouterOS.
- **VMWare**:
  - Добавлено правило нормализации для VMWare Horizon.
- **Oracle**:
  - Добавлено правило нормализации для MySQL.
- **Atlassian**:
  - Добавлено правило нормализации для Confluence.
- **Kaspersky**:
  - Добавлено правило нормализации для KWTS.
- **Positive Technologies**:
  - Добавлено правило нормализации для Sandbox.
- **1C**:
  - Добавлено правило нормализации для 1С:Предприятие.

Улучшения и исправления

- **Atlassian**:
  - Jira: исправлено заполнение полей категоризации.
- **Microsoft**:
  - Exchange: исправлен маппинг `src_user_dn`.
  - IIS: добавлена обработка косой черты в имени пользователя для событий Exchange.
  - Sysmon: исправлен маппинг `array_field1`.

- Windows Security: добавлена нормализация новых полей в событии 4719, обновлена таблица обогащения.

Правила детектирования

Новые правила

- **Microsoft Windows**:
  - Вход с разных хостов на один хост под одной учетной записью.
  - Сокрытие данных в атрибутах файлов NTFS.
  - Вход на устройство под разными учетными записями.
  - Скрытие учетной записи через реестр Windows.
  - Вход на несколько узлов под одной учетной записью.
  - Обнаружена попытка дампа NTDS.dit.
  - Обнаружение атаки Password Spraying на Exchange.
  - Зафиксировано изучение общих сетевых ресурсов.
  - Подбор пароля к учетным записям Exchange.
  - Пользователь из черного списка вошел в Exchange.
  - Атака Password Spraying.
  - Перечисление ключей реестра для разведки.
  - Запуск множества подозрительных команд.
  - Вход под несуществующим пользователем.
  - Разведка процессов.
  - Запуск whoami с правами системы.
  - Изменение пароля пользователя или хоста с помощью Ksetup.exe.
  - Сбор информации о сетевых подключениях.
  - Запуск процесса от другого пользователя.
  - Добавление пользователя в критичные локальные группы.
  - Изменение атрибута для скрытия файла через PowerShell.
  - Несистемный процесс повысил привилегии до системного.
  - Атака Bad USB Windows.
  - Эксплуатация уязвимости ProxyNotShell (CVE-2022-41082).
  - Эксплуатация утилиты LaZagne.
  - Разведка учетных записей.
  - Запуск aspnet_compiler.exe для компиляции в нетипичной директории.
  - Потенциальное выполнение скрипта через WScript/CScript.
  - Эксфильтрация данных через finger.exe.

- Удаленный запуск процесса с помощью WMI.
- Выполнение Sysinternals PsSuspend.
- Попытка дампа LSASS с помощью утилиты HandleKatz.
- Создание Self Extracting Package в подозрительном месте.
- Извлечение cab-файлов через Wusa.EXE.
- Отключение ETW провайдера .NET.
- Запуск потенциально поддельного экземпляра hxtsr.exe.
- Использование инструмента SharpMove.
- Скачивание файла средствами MpCmpRun.EXE.
- Добавление источника загрузки в Winget.
- Разведка доменных трастов.
- Зафиксировано изучение системного времени.
- Подключение к SMB-папке по протоколу QUIC.
- Удаленная отладка браузера Windows.
- Использование утилиты Smbtakeover.
- Отключение или модификация Windows Audit Log Policy.
- Использование утилит для создания снимков экрана.
- Загрузка файлов с использованием LOLBins InstallUtil.exe.
- Эксплуатация уязвимости VSCode CVE-2023-46944.
- Получение учетных данных из реестра.
- Несистемный процесс повысил привилегии до системы.
- Вход под учетной записью администратора.
- Выполнение команд в системе от редактора кода VSCode.
- Запуск интерпретатора командной строки от WinRAR.
- Удаленное выполнение команд с помощью PsExec.
- Запуск ssh.exe с подозрительными параметрами.
- Атака Pass the Hash.
- Перехват RDP-соединения.
- Поиск процессов с уязвимыми модулями.
- Установка удаленной сессии при помощи WMI.
- Копирование веток реестра, содержащих хэши паролей.
- Атака Kerberoasting.
- Извлечение содержимого буфера в Windows.
- Скрытие файла через attrib.exe.
- Подозрительное выполнение Regasm/Regsvcs с нестандартным расширением.

    - Обнаружение компиляции исходного кода на Windows.
    - Создание обратного туннеля через ssh.exe.
- **Microsoft Exchange**:
    - Успешный подбор пароля к учетным записям Exchange.
    - Пользователь удалил доверие федерации из организации Exchange.
    - Пользователь изменил/удалил критическую группу рассылки.
    - Массовое удаление групп рассылок Exchange.
    - Пользователь создал/изменил политику назначения ролей управления.
    - Пользователь выполнил действие с ролью управления в Exchange.
- **MikroTik**:
    - Подключение к MikroTik с недоверенного IP.
    - Подбор пароля пользователя MikroTik.
    - Атака Password Spraying в MikroTik.
- **Linux**:
    - Злоупотребление расширенными атрибутами.
    - Изменение конфигурации OpenVPN Access Server.
    - Доступ к файлу с ключами и сертификатами OpenVPN.
    - Использование chisel для туннелирования трафика.
- **VMware ESXi**:
    - Изменение аудита виртуальной инфраструктуры.
- **VMware ESXi**, **VMware vCenter Server**:
    - Удалена критичная виртуальная машина.

Улучшения и исправления

- **Windows**:
    - Кража токена доступа из системного процесса: исправлен активный список на duplicate_token_legitimate_processes_cimv2.
    - Запуск файла без расширения: скорректировано исключение.
- **Linux**:
    - Добавлен фильтр в правила Linux для совместимости с Endpoint.
- **Общее**:
    - Таблица IoC: добавлены новые индикаторы компрометации ФСТЭК России от 30.01.2026.

О релизе № 7 от 27.01.2026

Для использования актуального пакета экспертизы необходимо обновить R-Vision SIEM до версии 2.3.0 и выше.

Кратко о релизе

- Добавлены новые индикаторы компрометации ФСТЭК России от 25.12.2025 и 15.01.2026.
- Внесены улучшения и исправления в правила нормализации для Microsoft, Kaspersky, Linux, VMware, Zabbix.
- Внесены исправления в правила детектирования для Microsoft Windows, Linux, Kaspersky.
- Поддержаны новые источники: Microsoft Active Directory, Positive Technologies Industrial Security Incident Manager (PT ISIM), Veeam Backup & Replication, Solar Dozor, Kaspersky Anti Targeted Attack Platform, Код Безопасности Континент 4.

Правила нормализации

Новые правила

- **Microsoft**:
  - Добавлено правило нормализации для Active Directory Domain Services.
  - Добавлено правило нормализации для Active Directory Web Services.
  - Добавлено правило нормализации для DNS Server.
- **Positive Technologies**:
  - Добавлено правило нормализации для ISIM.
- **Veeam**:
  - Добавлено правило нормализации для Veeam Backup & Replication.
- **Solar**:
  - Добавлено правило нормализации для Dozor.
- **Kaspersky**:
  - Добавлено правило нормализации для KATA.
- **Код Безопасности**:
  - Добавлено правило нормализации для Континент 4.

Улучшения и исправления

- **Microsoft**:
  - Exchange Agent: добавлен `device_fqdn`.
  - PowerShell/System: исправление обработки исключений.
  - Windows Security: дополнительно нормализованы события 4778, 4779.
  - IIS: добавлен маппинг параметров запроса.
- **Kaspersky**:
  - Security Center: добавлены два тестовых события, которых ранее не было.
- **Linux**:
  - Auditd: добавлен `dst_file_owner` к системным вызовам `openat`.

- **VMware**:
  - vCenter: поправлено поле `dst_hostname`.
- **Zabbix**:
  - Zabbix: внесены исправления в поле `description`.

Правила детектирования

Новые правила

- **Microsoft Windows**:
  - Атака DCShadow.
  - Удаленное подключение к узлу через туннелирование в Visual Studio Code.
  - Зафиксирована подгрузка подозрительного пакета процессом LSA.
  - Зафиксирована атака Golden Ticket.
  - Создание подозрительного процесса от `hh.exe`.
  - Скачивание удаленного файла средствами `hh.exe`.
  - Удаление временных RDP-файлов в Windows.
  - Новый сертификат `root` был установлен средствами `Certutil.exe`.
  - Ослабление защиты или мониторинга системы.
  - Удаление истории RDP-подключений через реестр.
  - Отключение ETW-провайдера PowerShell.
  - Успешная эксплуатация ProxyShell.
  - Удаленный контроль через Chrome Remote Desktop.
  - Эксплуатация утилиты GrimResource.
  - Удаленное выполнение команд с помощью SMBExec.
  - Загрузка dll-библиотеки средствами `mavinject`.
  - Инъекция AppDomain Manager.
  - Закрепление через Shim.
  - RDP-подключение с использованием туннеля.
  - Отключение службы Windows EventLog.
  - Закрепление через Outlook Home Page.
  - Туннелирование с использованием `ngrok`.
  - Использование утилиты `gs-netcat` из набора инструментов `gsocket`.
  - Манипуляции с теневыми копиями с помощью встроенных утилит.
  - Вход под учетной записью, созданной по умолчанию.
  - Обнаружен запуск XSL-скрипта.
  - Интерактивный вход под сервисной учетной записью.

- Изменение конфигурации загрузки безопасного режима.
- Выполнение манипуляций над учетной записью с помощью стороннего ПО.
- Журнал событий Windows был очищен.
- Запуск файла с двойным расширением.
- Изменение настроек Outlook.
- Добавление исполняемого файла к профилю PowerShell.
- Запуск файла без расширения.
- Включение или отключение учетной записи.
- Изменения в планировщике задач.
- Маскировка учетной записи под имя компьютера.
- Аномальное поведение офисного ПО.
- Множественные неудачные попытки аутентификации учетной записи.

- **Microsoft Exchange**:
  - Изменение политики Outlook on the Web (OWA) в системе Exchange.
  - Эксплуатация ProxyLogon в Microsoft Exchange (CVE-2021-27065).
  - Подозрение на эксплуатацию ProxyShell.
  - Пользователь выполнил действие с правилом транспорта в Exchange.
  - Удаление политики фильтров ВПО в системе Exchange.
  - Сбор адресов электронной почты из глобального списка адресов.
  - Добавление пользователя в группу рассылки в Microsoft Exchange.
  - Пользователь удалил почтовые ящики в Microsoft Exchange.
  - Удаление или размонтирование базы данных в Microsoft Exchange.
  - Сбор электронной почты в Microsoft Exchange.
  - Эксплуатация уязвимости CVE-2024-49040.
  - Изменение правила журнала в системе Exchange.
  - Утечка данных через массовую отправку писем.
  - Попытка выгрузить PST-файлы в Microsoft Exchange.
- **Microsoft AD FS**:
  - Множественные неудачные попытки аутентификации в AD FS.
  - Успешный подбор пароля в AD FS.
  - Кража/экспорт сертификатов AD FS.
  - Изменение Claims Provider Trust в AD FS.
- **Linux**:
  - Использование набора инструментов `gsocket`.
  - Эксплуатация уязвимости CVE-2023-46944 Visual Studio Code на Linux.

- **Atlassian**:
  - Эксплуатация уязвимости в Jira (CVE-2023-26256).
  - Создание множества задач пользователем в Jira.
  - Множество неудачных попыток входа в Jira.
  - Создание пользователя в Jira.
  - Изменение конфигурации журналов логирования в Jira.
  - Удаление множества задач пользователем в Jira.
  - Добавление пользователя в критичные группы.
  - Создание резервной копии Jira.
  - Дамп множества задач в Jira.
- **VMware**:
  - Удалено несколько критичных виртуальных машин.
  - Отключено несколько критичных виртуальных машин.
  - Отключена критичная виртуальная машина.
  - Создание множества виртуальных машин.
  - Остановка критичного сервиса ESXi.
  - Лишение пользователя доступа к ESXi.
- **Kaspersky**:
  - Обнаруженное вредоносное ПО не было удалено.
- **BIND**:
  - Подозрительные DNS-запросы к домену trycloudflare.com.

Улучшения и исправления

- **Общее**:
  - Таблица IoC: добавлены новые индикаторы компрометации ФСТЭК России от 25.12.2025 и 15.01.2026.
- **Microsoft Windows**:
  - Доступ к чувствительному сетевому диску Windows: исправление фильтра для исключения ложных сработок.
  - Закрепление через COM Hijacking: добавлены процессы Microsoft в фильтр исключений.
  - Кража токена доступа из системного процесса: замена таблицы обогащения на активный список.
- **Linux**:
  - Перехват SSH-сессии: упрощен фильтр.
  - Остановка критичных сервисов в Linux: добавлена техника.
- **Kaspersky**:
  - Получение массовой рассылки писем: обновлен фильтр.

- Вредоносная ссылка в письме: обновлен фильтр.
- Вредоносное вложение в письме: обновлен фильтр.
- Получение спам-письма: обновлен фильтр.
- Проверка подлинности отправителя сообщений: обновлен фильтр.
- Шифрованное вложение в письме: обновлен фильтр.

О релизе № 6 от 23.12.2025

Для использования актуального пакета экспертизы необходимо обновить R-Vision SIEM до версии 2.3.0 и выше.

Кратко о релизе

- Добавлены новые индикаторы компрометации ФСТЭК России от 15.12.2025.
- Внесены улучшения и исправления в правила нормализации для Microsoft Windows, Linux, Kaspersky.
- Внесены исправления в правила детектирования для VMware, Kaspersky.
- Поддержаны новые источники: Microsoft Exchange, ViPNet IDS NS/TIAS, Atlassian Jira, Zabbix, Kaspersky Secure Mail Gateway, Kaspersky CyberTrace, Cisco NetFlow, Cisco ASA, ClickHouse.

Правила нормализации

Новые правила

- **Microsoft**:
  - Добавлено правило нормализации для Microsoft Exchange.
- **ИнфоТеКС**:
  - Добавлено правило нормализации для ViPNet IDS NS/TIAS.
- **Atlassian**:
  - Добавлено правило нормализации для Jira.
- **Zabbix**:
  - Добавлено правило нормализации для Zabbix.
- **Kaspersky**:
  - Добавлено правило нормализации для Kaspersky Secure Mail Gateway.
  - Добавлено правило нормализации для Kaspersky CyberTrace.
- **Cisco**:
  - Добавлено правило нормализации для NetFlow.
  - Добавлено правило нормализации для ASA.
- **ClickHouse**:
  - Добавлено правило нормализации для ClickHouse.

Улучшения и исправления

- **Linux**:
  - Auditd: исправлено дублирование полей `dst_process_name` и `src_process_name`.
- **Microsoft**:
  - Sysmon: изменен формат поля `array_field` в событии 22.
  - Windows Security: добавлена нормализация событий 4886, 4887, 4898, 4899.
- **Kaspersky**:
  - Security Center: исправлено заполнение `dst_object_name` для случаев, когда `dst_file_path` является URL-адресом.

Правила детектирования

Новые правила

- **Microsoft Windows**:
  - Изменение политики выполнения PowerShell.
  - Обнаружение эксплуатации DDE через Office.
  - Изменение атрибутов групповой политики.
  - Создание новой доменной/локальной/компьютерной учетной записи.
  - Удаление доменной/локальной/компьютерной учетной записи.
  - Создание и удаление учетной записи за одну минуту.
  - Обнаружено использование службы BITS Jobs.
  - Создана пользовательская форма Outlook.
  - Добавление пользователя в критичные доменные группы.
  - Изменение SPN учетной записи.
  - Изучение конфигурации локальной системы.
  - Создание дампа NTDS.dit.
  - Построение образа в Windows.
  - Запуск скрипта из временной директории.
  - Уничтожение информации на диске в Windows.
  - Размещение архивов в сетевой папке Windows.
  - Изменена групповая политика домена по умолчанию.
  - Поиск данных в сетевых папках Windows.
  - Удален объект групповой политики.
- **Linux**:
  - Аномальное bind-монтирование.
  - Построение образа в Linux.

- Дамп памяти утилитой MimiPenguin на Linux.
- Изменение настроек пользователя.
- Вызов команды из модуля PAM.
- Перехват SSH-сессии.

- **Kaspersky**:
  - Зафиксированы устаревшие базы антивирусного ПО Kaspersky.

Улучшения и исправления

- **Общее**:
  - Таблица IoC: добавлены новые индикаторы компрометации ФСТЭК России от 15.12.2025.
- **VMware**:
  - Множественные неуспешные попытки аутентификации пользователя: исправлена ошибка в фильтре.
- **Kaspersky**:
  - Устройство давно не подключалось к серверу KSC: внесены исправления для корреляционного фильтра.

О релизе № 5 от 16.12.2025

Для использования актуального пакета экспертизы необходимо обновить R-Vision SIEM до версии 2.3.0 и выше.

Кратко о релизе

- Добавлены новые индикаторы компрометации ФСТЭК России от 05.12.2025.
- Внесены исправления в правила нормализации для Kaspersky Security Center, Check Point Harmony, Linux Auditd, Passwork, BI.ZONE EDR.
- Внесено улучшение в правило нормализации для Kaspersky Security Center.
- Внесены исправления в правила детектирования для VMware vCenter, Microsoft Windows, Linux.
- Поддержаны новые источники: Microsoft DHCP, Microsoft Active Directory Federation Services, Код Безопасности Континент 3, Efros DefOps NAC, PostgreSQL.

Правила нормализации

Новые правила

- **Microsoft**:
  - Добавлено правило нормализации для Microsoft DHCP.
  - Добавлено правило нормализации для Microsoft Active Directory Federation Services.
- **Код Безопасности**:
  - Континент 3: перевод правила в УМС 2.0.

- **Efros**:
  - Добавлено правило нормализации Efros DefOps NAC.
- **PostgreSQL**:
  - PostgreSQL: перевод правила в УМС 2.0.

Улучшения и исправления

- Kaspersky Security Center: добавлена нормализация новых типов событий, исправлено поле description.
- Check Point Harmony: исправлено поле description, добавлен способ подключения в наименовании правил.
- Linux Auditd: добавлено исправление маппинга полей array_field.
- Passwork: обновлена таблица обогащения, изменено поле description для событий с 2FA, поле device_event_category переведено в snakecase.
- BI.ZONE EDR: добавлен способ подключения в наименовании правил.

Правила детектирования

Новые правила

- **Microsoft Windows**:
  - Внедрение вредоносного агента Exchange.
  - Загрузка RstrtMgr.dll необычным процессом.
  - Загрузка DLL системным процессом из подозрительного места.
  - Загрузка процессом cmstp модулей для выполнения скриптов.
  - Произошло выполнение полезной нагрузки при наступлении WMI события.
  - Установка модуля IIS.
  - Выполнение прокси-файла через verclsid.
  - Создание правил почты через PowerShell.
  - Подозрительный доступ к облачным менеджерам секретов.
  - Использование подавления ошибок в PowerShell.
  - Исходящее подключение SYSTEM-процессов к нестандартным портам.
  - Установка пакетов msi из пользовательской директории.
  - Подозрительное чтение данных приложений.
  - Включено обратимое шифрование паролей.
  - Включение функции обратимого шифрования.
  - Подозрительные обращения к trycloudflare.com.
- **Linux**:
  - Добавление/удаление модулей ядра Linux.

- **Kaspersky**:
  - Зафиксирован переход по опасной ссылке.

Улучшения и исправления

- **Общее**:
  - Таблица IoC: добавлены новые индикаторы компрометации ФСТЭК России от 05.12.2025.
- **VMware vCenter**:
  - Создание снапшота критичной ВМ в vCenter: добавлен блок response.
  - Использование утилит ESXi через CLI: обновлен фильтр для детекта выполнения снапшотов через vim-cmd.
- **Microsoft Windows**:
  - Использование обфускации PowerShell: исправления фильтра для исключения FP.
  - Использование средств туннелирования трафика: добавлен тег T1599.
  - Использование WinApi через PowerShell: добавлен тег T1055.002.
  - Использование утилиты TikiTorch: добавлен тег T1055.002.
  - Использование вредоносных утилит: добавлен инструмент rclone.
  - Подозрительный доступ к памяти процесса LSASS: добавлены исключения для процессов Kaspersky.
  - Зафиксирована загрузка модуля WMI подозрительным процессом: внесены исправления для модуля исключений FP.
  - Смена ассоциации запуска файла: исправление фильтра для исключения ложных срабатываний.
- **Linux**:
  - Использование средств туннелирования трафика Linux: добавлен тег T1599.
  - Изменение конфигурационных файлов службы firewalld: добавлен тег T1599.
  - Создание туннелей и перенаправление трафика: добавлен тег T1599.
  - Использование хакерской утилиты в Linux: добавлен инструмент для эксфильтрации данных rclone.

О релизе № 4 от 02.12.2025

Для использования актуального пакета экспертизы необходимо обновить R-Vision SIEM до версии 2.3.0 и выше.

Кратко о релизе

- Выпущен пакет правил нормализации и детектирования, совместимый с Универсальной моделью события 2.0.
- Добавлена поддержка новых источников: Secret Net Studio, BindDNS, АйТи Бастион СКДПУ НТ, Check Point Harmony Endpoint, Microsoft Hyper-V.

- Выпущены новые правила детектирования для Linux, Microsoft Windows и FreeIPA.
- Добавлены новые индикаторы компрометации ФСТЭК России от 14.11.2025 и 27.11.2025.

Правила нормализации

Общее

- Обнаружен индикатор компрометации: добавлены новые индикаторы компрометации ФСТЭК России от 14.11.2025 и 27.11.2025.

Новые источники

- Secret Net Studio: добавлено правило нормализации.
- BindDNS: добавлено правило нормализации.
- АйТи Бастион СКДПУ НТ: добавлено правило нормализации.
- Check Point Harmony Endpoint: добавлено правило нормализации.
- Microsoft Hyper-V: добавлено правило нормализации.

Улучшения и исправления

- OpenVPN: скорректирована нормализация события `verify`.
- VMware ESXi/vCenter: доработана категоризация.
- FreeIPA: доработана нормализация полей `dst_object_type/value`.
- Microsoft Sysmon: исправлен маппинг полей для события `EventID 22`.
- Гарда WAF: скорректирована категоризация событий.

Правила детектирования

Новые правила

- **Linux**:
  - Создание интерактивной оболочки через GTFOBins.
  - Сетевое обращение от подозрительного скрипта в Linux.
  - Создан Reverse-shell сторонней утилитой в Linux.
  - Reverse-shell через Bash-сценарий.
  - Создание подозрительного Named Pipe с помощью Mkfifo.
  - Обнаружена команда Reverse/Bind Shell.
  - Создание файла через Python/Ruby сценарий.
  - Изменение `timers` на хосте Linux.
  - Использование утилиты `at`.
  - Повышение привилегий с помощью GTFOBins.
  - Повышение привилегий до root.

- Модификация разрешений системных файлов в Linux.
- Использование утилиты `fusermount`.
- Внедрение процесса в другой через `ptrace`.
- Создание/изменение правила `nf_tables`.

- **Microsoft Windows**:
  - Регистрация вредоносного Password Filter.
  - Удаленная эксплуатация DCOM-объекта ShellWindows.
  - Удаленная эксплуатация DCOM-объекта `Excel.Application`.
  - Чтение процесса `LSASS` от подозрительного процесса.
  - Добавление файла в директорию расширения браузера.
  - Очистка истории команд PowerShell в Windows.
  - Закрепление в директории автозагрузки.
  - Закрепление в Print Processors через подозрительную dll.
  - Изменение запланированной задачи в групповой политике.
  - Поиск учетных данных в групповых политиках.
  - Доступ к чувствительному сетевому диску Windows.
  - Закрепление через ключ `ReflectDebugger` утилиты WerFault.
  - Изменение критичных параметров сервиса.
  - Удаленный запуск процесса с помощью DCOM-объекта `MMC20.Application`.
  - Закрепление в системе через создание/изменение пакетов.
  - Эксплуатация Active Setup в реестре.
  - Эксплуатация сценариев входа в систему.
  - Изменение пути к исполняемому файлу в сервисе.
- **FreeIPA**:
  - Успешный подбор пароля пользователя по LDAP в FreeIPA.
  - Подбор пароля пользователя по LDAP в FreeIPA.
  - Обнаружение атаки Password Spraying на FreeIPA.
  - Успешный подбор пароля от FreeIPA Web UI.
  - Подбор пароля от FreeIPA Web UI.

Улучшения и исправления

- **Linux**:
  - Закрепление при помощи утилиты Trap: доработана обработка строк через регулярное выражение для снижения FP.
- **Microsoft Windows**:
  - Использование средств туннелирования трафика: исправлена ошибка в регулярном

выражении.

О релизе № 3 от 18.11.2025

Для использования актуального пакета экспертизы необходимо обновить R-Vision SIEM до версии 2.3.0 и выше.

Кратко о релизе

- Внесены исправления в правила нормализации для Linux Auditd.
- Внесены исправления в правила детектирования для Microsoft Windows.
- Поддержаны новые источники: Microsoft Windows Security, Microsoft SQL Server, Cisco IOS, InfoWatch Traffic Monitor, MariaDB, Universal CEF.

Правила нормализации

Новые правила

- Microsoft Windows Security: добавлено правило нормализации для источника.
- Microsoft SQL Server: добавлено правило нормализации для источника.
- Cisco IOS: добавлено правило нормализации для источника.
- InfoWatch Traffic Monitor: добавлено правило нормализации для источника.
- MariaDB: добавлено правило нормализации для источника.
- Universal CEF: добавлено правило нормализации для источника.

Улучшения и исправления

- Linux Auditd: скорректированы условия заполнения кастомных полей.

Правила детектирования

Новые правила

- **Kaspersky**:
  - Устройство давно не подключалось к серверу KSC.
  - Отключение продукта Kaspersky в результате выполнения задачи.
  - Отключение компонентов защиты продуктов Kaspersky.
  - Изменение политик администрирования на сервере KSC.
  - Создание и исполнение задачи на удаленную деинсталляцию программы средствами KSC.
  - Устройство давно не подключалось к серверу KSC.
  - Отключение продукта Kaspersky в результате выполнения задачи.
  - Отключение компонентов защиты продуктов Kaspersky.
  - Изменение политик администрирования на сервере KSC.

- Создание и исполнение задачи на удаленную деинсталляцию программы средствами KSC.

- **Linux**:
  - Использование утилиты kadmin.
  - Использование rsockstun клиента.
- **FreeIPA**:
  - Успешный подбор пароля пользователя FreeIPA.
  - Подбор пароля пользователя FreeIPA.
  - Добавление HBAC-правила через FreeIPA.
  - Изменение конфигурации sudo в FreeIPA.
  - Остановка/перезапуск сервисов FreeIPA.
  - Изменение оболочки входа средствами FreeIPA.
  - Разведка пользователей/ролей Free IPA.
  - Атака Golden Ticket FreeIPA.
  - Атака Silver Ticket FreeIPA
  - Выполнение бэкапа FreeIPA.
  - Чтение Ticket CCACHE файла.
  - Чтение LDAP секретов FreeIPA.
- **Passwork**:
  - Экспорт паролей/сейфа passwork.
  - Назначение роли администратора.
  - Создание пользователя.
  - Отключение 2FA.
  - Успешный брутфорс Passwork.
  - Брутфорс Passwork.
  - Изменение прав роли.
  - Массовое удаление сейфов, папок, паролей.
  - Добавление пользователя в критичный сейф.
  - Включение заблокированной УЗ.
  - Множественный просмотр паролей за короткий промежуток времени.
  - Массовое удаление учетных записей.
  - Вход под УЗ администратора.
- **Microsoft Windows**:
  - Отключение сбора событий EventLog через реестр.
  - Отключение или модификация Defender Firewall.
  - Защита от записи для хранилища отключена.

- Отключение снапшотов томов.

Улучшения и исправления

- **Microsoft Windows**:
  - Подозрительный доступ к памяти процесса LSASS: исправлена ошибка в фильтре.

О релизе № 2 от 05.11.2025

Для использования актуального пакета экспертизы необходимо обновить R-Vision SIEM до версии 2.3.0 и выше.

Кратко о релизе

- Внесены исправления в правила нормализации для BI.ZONE EDR, Microsoft PowerShell, Microsoft Windows System, Passwork.
- Поддержаны новые источники: Linux Auth, FreeIPA, Passwork, PT NAD, OpenVPN, PT AF 4, Microsoft IIS.

Правила нормализации

Новые правила

- Linux Auth: добавлено правило нормализации для источника.
- FreeIPA: добавлено правило нормализации для источника.
- Passwork: добавлено правило нормализации для источника.
- PT NAD: добавлено правило нормализации для источника.
- OpenVPN: добавлено правило нормализации для источника.
- PT AF 4: добавлено правило нормализации для источника.
- Microsoft IIS: добавлено правило нормализации для источника.

Улучшения и исправления

- BI.ZONE EDR: оптимизированы правила обработки событий от Windows и Linux.
- Microsoft PowerShell: добавлена корректная обработка событий со знаками экранирования.
- Microsoft Windows System: в правиле доработаны наименования кастомных полей.
- Passwork: доработан маппинг полей.

Правила детектирования

Новые правила

- **Microsoft Windows**:
  - Создан сервис с подозрительными параметрами.
  - Установлен сервис не из системного/стандартного пути.

- Создание или изменение сервиса с помощью командной строки.
- Зафиксированы подозрительные операции при помощи WMI.
- Разведка ключей реестра.
- Разведка системы при помощи WMI.
- URL-схема в командной строке процесса.
- Перечисление учетных записей в домене методом перебора.
- Подбор пароля учетной записи на хосте.

- **Linux**:
  - Изменение файлов в домашнем каталоге другим пользователем.
  - Чтение файлов с закрытыми ключами SSH.
  - Чтение памяти процессов на Linux.
- **Passwork**:
  - Успешный брутфорс Passwork.
  - Брутфорс Passwork.
  - Изменение прав роли.
  - Массовое удаление сейфов, папок, паролей.
  - Добавление пользователя в критичный сейф.
  - Включение заблокированной УЗ.
  - Множественный просмотр паролей за короткий промежуток времени.
  - Массовое удаление учетных записей.
- **VMware**:
  - Доступ к критичным файлам на сервере ESXi.
  - Эксплуатация уязвимости CVE-2021-22005 на сервере vCenter.
  - Эксплуатация уязвимости CVE-2021-21972 на сервере vCenter.
  - Доступ к критичным файлам на сервере vCenter.
  - Вызов и выполнение Guest API в гостевой ОС.
  - Использование find в ESXi.
  - Обнаружение уязвимой конфигурации ESXi.
  - Изменение конфигурации нескольких критичных виртуальных машин.
  - Удаление или отключение логирования команд.
  - Использование chmod в ESXi через CLI.
  - Изменение конфигурации критичной виртуальной машины.
  - Изменение меток времени через touch.
  - Маскировка через переименование/подмену index.html.

О релизе № 1 от 24.10.2025

Для использования актуального пакета экспертизы необходимо обновить R-Vision SIEM до версии 2.3.0 и выше.

Кратко о релизе

- Поддержаны новые источники: Apache HTTP-server (access.log / error.log), BI.ZONE EDR (Windows, Linux, Mac OS), Bind DNS, Гарда WAF, Kaspersky (CyberTrace, KATA, KSC, KSMG, KWTS), Linux Auditd, Microsoft Windows (System, Sysmon, PowerShell, Security), Nginx, PT WAF 3, VMware ESXi/vCenter.

Правила нормализации

Новые правила

- Apache HTTP-server (access.log / error.log): добавлено правило нормализации для источника.
- BI.ZONE EDR (Windows, Linux, Mac OS): добавлено правило нормализации для источника.
- Bind DNS: добавлено правило нормализации для источника.
- Гарда WAF: добавлено правило нормализации для источника.
- Kaspersky (CyberTrace, KATA, KSC, KSMG, KWTS): добавлено правило нормализации для источника.
- Linux Auditd: добавлено правило нормализации для источника.
- Microsoft Windows (System, Sysmon, PowerShell, Security): добавлено правило нормализации для источника.
- Nginx: добавлено правило нормализации для источника.
- PT WAF 3: добавлено правило нормализации для источника.
- VMware ESXi/vCenter: добавлено правило нормализации для источника.

Правила детектирования

Новые правила

- **VMware**:
  - Вход под привилегированной учетной записью vmware.
  - Использование утилит ESXi через CLI.
  - Создание ssh-туннелей на ESXi.
- **Kaspersky**:
  - Проверка подлинности отправителя сообщений.
  - Вредоносная ссылка в письме.
  - Шифрованное вложение в письме.
  - Получение спам-письма.
  - Вредоносное вложение в письме.

- Получение массовой рассылки писем.
- Повторное заражение хоста одним вирусом.
- Успешное исполнение задачи на удаленную установку программы средствами KSC.
- Удалено обнаруженное средствами АВЗ ВПО.
- Не было удалено обнаруженное средствами АВЗ ВПО.
- Множество хостов заражены одним типом ВПО.
- Множественное срабатывание вердиктов средств АВЗ на одном хосте.
- На сервере KSC созданы пакет установки и удаленная задача на установку пакета.
- Устройство перемещено в группу администрирования на сервере KSC.
- Изменена критичная политика продукта Kaspersky.
- Зафиксировано отключение задачи средств AV-защиты Kaspersky.
- Исполнение задачи на установку программы через установочные пакеты.

- **Linux**:
  - Разведка под сервисным пользователем.
  - Загрузка файла с помощью утилит GTFOBins.
  - Загрузка файла сервисной учетной записью.
  - Создание туннелей и перенаправление трафика.
  - Подозрительное изменение директории /etc.
  - Изменение системных библиотек Linux.
  - Модификация файлов MOTD в Linux.
  - Запуск процесса с помощью ld.so.
  - Модификация правил udev.
  - Кратковременное существование учетной записи.
  - Изменение критичных файлов Linux.
  - Закрепление в системе с использованием записей автозагрузки XDG.
  - Изменение бинарных файлов Linux.
  - Добавление расширения в браузер через CLI Linux.
  - Добавление файла в расширения браузера Linux.
  - Изменение задач cron.
  - Создание пользователя или группы.
  - Удаление файлов логирования в Linux.
  - Злоупотребление сырыми сокетами.
  - Загрузка файлов утилитой wget в директорию tmp.
  - Загрузка файлов с удаленных ресурсов стандартными утилитами.
  - Туннелирование с использованием ngrok в Linux.

- Использование утилиты SSHuttle для создания SSH-туннеля.
- Использование утилит для создания снимков экрана Linux.
- Размещение архивов в сетевой папке Linux.
- Чтение критичных файлов Linux.
- Извлечение содержимого буфера в Linux.
- Поиск данных в сетевых папках Linux.
- Чтение файлов с пользовательскими учетными данными.
- Успешный подбор пароля пользователя Linux.
- Доступ к критичным файлам SSSD.
- Успешный подбор пароля на хосте Linux.
- Подбор пароля пользователя Linux.
- Подбор пароля на хосте Linux.
- Чтение файлов с историей команд.
- Отключение или изменение службы SELinux.
- Изменение корневых сертификатов Linux.
- Изменение привилегий файлов Linux.
- Отключение службы firewalld.
- Изменение tmp файлов логирования Linux.
- Обнаружение стеганографии в Linux.
- Отключение или модификация Syslog Linux.
- Загрузка кода в процесс Linux.
- Изменение настроек для скрытия пользователей.
- Загрузка подозрительного ebpf модуля.
- Создание/изменение скрытых файлов Linux.
- Создание/изменение скрытых shared object файлов.
- Отключение мандатного контроля целостности.
- Изменение критичных файлов конфигурации интерактивной оболочки.
- Отключение службы Auditd.
- Изменение конфигурационных файлов службы firewalld.
- Изменение конфигурационных файлов служб журналирования.
- Компиляции исходного кода на Linux.
- Копирование стандартных исполняемых файлов.
- Поиск сетевых конфигураций.
- Использование утилит для сканирования сети.
- Поиск локализации системы Linux.

- Получение информации о текущем пользователе.
- Разведка локальных УЗ в Linux.
- Получена информация о системных службах на узле.
- Поиск файлов с suid/sgid битом.
- Поиск окружения контейнера через proc VFS.
- Обнаружение контейнеров через Inodes Listing.
- Разведка доменных УЗ в Linux.
- Разведка системной информации Linux.
- Разведка установленного ПО в Linux.
- Разведка Docker контейнеров через Dockerenv.
- Подозрительное чтение домашней директории пользователя.
- Разведка запущенных процессов в Linux.
- Большое количество подозрительных команд.
- Разведка парольной политики в Linux.
- Запуск утилиты msldapdump для разведки.
- Уничтожение информации на диске в Linux.
- Остановка критичных сервисов в Linux.

- **Microsoft Windows**:
  - Обогащение активного списка `legitimate_guids_svchost_processes_list`.
  - Использование PowerShell через сторонние инструменты.
  - Обход UAC через COM-объекты.
  - Использование библиотеки cygwin1.dll.
  - Зафиксирована загрузка модуля WMI подозрительным процессом.
  - Процесс загрузил модуль по UNC-пути.
  - Исходящее сетевое соединение PowerShell.
  - Эксплуатация уязвимости в WinRAR - CVE-2023-38831.
  - Маскировка запуска PowerShell.
  - Создание запланированной задачи через FileCreation.
  - Удаленная эксплуатация DCOM объекта IMsiServer.
  - Добавление в Netsh Helper DLL потенциальной полезной нагрузки.
  - Закрепление через Microsoft Office Add-ins.
  - Закрепление через COM Hijacking.
  - Закрепление в системе через ключ реестра MyComputer.
  - Изменение ключа реестра Debugger отладчика AeDebug.
  - Манипулирование запланированными задачами через реестр.

- Внедрение стороннего ПО через отладчик IFEO.
- Создание WMI подписки.
- Включение переменных среды COR Profiler.
- Закрепление через изменения ключей автозапуска в реестре.
- Смена ассоциации запуска файла.
- Закрепление через Office Template Macros.
- Добавление в AppCert DLL полезной нагрузки.
- Загрузка несуществующей dll для сервисов IKE, IKEEXT, SessionEnv.
- Добавление в Appinit DLL полезной нагрузки.
- Изменение настроек администратора Winget.
- Закрепление через Office Test.
- Зафиксирована подмена файлов экрана заставки Windows.
- Подмена системных файлов специальных возможностей.
- Запросы к API Telegram подозрительным процессом.
- Использование DNS туннеля.
- Подозрительные DNS-запросы к localtoNet домену.
- Подозрительный доступ к памяти процесса LSASS.
- Утечка NTLM через library-ms (CVE-2025-24071).
- Создание билета TGT при помощи хакерской утилиты.
- Использование утилиты RDPStrike.
- Дамп LSASS с помощью Диспетчера задач.
- Дамп LSASS с помощью Python-утилит.
- Порт RDP по умолчанию изменен на нестандартный.
- Загрузка модуля в процесс mmc из нестандартного пути.
- Выполнение скриптов через regsvr32.
- Эксплуатация Mark-of-the-Web bypass.
- Изменение чувствительных параметров RDP.
- Обнаружение HTML/SVG Smuggling в Windows.
- Загрузка процессом rundll32 модулей для выполнения скриптов.
- Изменение фона рабочего стола через реестр.
- Обход UAC с помощью ключа реестра DelegateExecute.
- Включение хранение хэша LM.
- Загрузка модуля в процесс odbcconf из нестандартного пути.
- Изменение чувствительных значений реестра.
- Установка нового значения DNS ServerLevelPluginDll.

- Загрузка модуля в процесс regsvr32 из нестандартного пути.
- Отключение Административных общих ресурсов при запуске.
- Включение в реестре DNS-over-HTTPS.
- Загрузка модуля в процесс rundll32 из нестандартного пути.
- Создание и удаление файла за короткий промежуток времени.
- Подозрительный путь DLL в IME реестре.
- Отключение контроля учетных записей пользователей.
- Скрытие запланированной задачи через реестр.
- Изменение ветки реестра Provisioning_Commands.
- Неподписанная DLL загружена утилитой Windows.
- Загрузка модуля в процесс cmstp из нестандартного пути.
- Отключение в реестре HECI.
- Изменена очередь загрузки драйвера Sysmon.
- Удаление метки MOTW Windows.
- Отключение CrashDump через изменение реестра.
- Изменение разрешения доступа к каналу Winevt через реестр.
- Сетевое подключение, инициированное процессом Winlogon.
- Создание подозрительного потока в mstsc.exe.
- Загрузка процессом mshta модулей для выполнения скриптов.
- Разрешение удаленного соединения между анонимными компьютерами.
- Модификация скрытых ключей Проводника.
- Сетевое подключение из подозрительной директории.
- Кража токена доступа из системного процесса.
- Подмена PID родительского процесса.
- Кража токена доступа при помощи именованных каналов.
- Использование ssh.exe для кражи NTLM-хэша.
- Создание удаленного потока с использованием функции LoadLibrary.
- Создание токена и имперсонация учетной записи.
- Использование утилиты TikiTorch.
- Создание удаленного потока подозрительным процессом.
- Загрузка amsi.dll необычным процессом.
- Отключение системы восстановления через реестр.
- Обогащение активного списка save_logons_cimv2.
- Использование Replace.exe.
- Загрузка файлов с веб-ресурсов стандартными утилитами.

- Сжатие дамп-файлов средствами 7Zip.
- Сжатие дамп-файлов средствами WinRAR.
- Попытка дампа процесса LSASS с помощью Procdump.
- Снэпшот базы данных AD средствами ADExplorer.
- Получение информации о службе RDP через sc.exe.
- Захват учетных данных с помощью Rpcping.exe.
- Остановка критичных сервисов.
- Использование хакерской утилиты DSInternals.
- Загрузка файлов с помощью PowerShell.
- Использование хакерской утилиты PSMapExec.
- Использование хакерской утилиты PowerShell-Suit.
- Использование обфускации PowerShell.
- Использование WinApi через PowerShell.
- Использование хакерской утилиты SharpHound.
- Использование хакерской утилиты PowerShellArsenal.
- Использование хакерской утилиты nishang.
- Использование хакерской утилиты OWA-Toolkit.
- Использование хакерской утилиты PowerSploit.
- Сжатие файлов средствами PowerShell.
- Прямой доступ к диску через PowerShell.
- Создание резервных копий MS SQL средствами PowerShell.
- Создание удаленного потока в процессе lsass.

Справочная информация по экспертизе

Данный раздел содержит справочные материалы для работы с экспертизой R-Vision SIEM. Они помогут вам быстро проверить совместимость с источниками событий и понять механизм работы правил корреляции.

- Правила нормализации
- Правила корреляции

Правила нормализации

- Поддерживаемые источники событий

Поддерживаемые источники событий

Данная таблица содержит список информационных систем, из которых в SIEM поступают события. Для указанных источников разработаны правила нормализации.

Вендор	Продукт	Версия	Тип подключения	ID правила нормализации
AhnLab	Absolute Data and Device Security (DDS)	-	Universal CEF	RV-N-243
AhnLab	AhnLab Malware Defense System (MDS)	-	Universal CEF	RV-N-243
Apache	Apache HTTP Server	2	Syslog (access) Syslog (error)	RV-N-231 RV-N-232
Apache	Apache Cassandra	4.1	Syslog	RV-N-343
Atlassian	Confluence	8, 9	Syslog	RV-N-237
Atlassian	Jira	-	Syslog	RV-N-238 RV-N-239
Avigilon	Avigilon Access Control Manager (ACM)	-	Universal CEF	RV-N-243
Ayehu	Ayehu eyeShare	-	Universal CEF	RV-N-243
Barracuda	Barracuda Networks NG Firewall	-	Universal CEF	RV-N-243
BeyondTrust	BeyondInsight	-	Universal CEF	RV-N-243
BeyondTrust	Privilege Management Console	-	Universal CEF	RV-N-243

Вендор	Продукт	Версия	Тип подключения	ID правила нормализации
BI.ZONE	BI.ZONE EDR	-	Kafka	RV-N-213 RV-N-214 RV-N-215 RV-N-216
BIND	BIND DNS	9.9	Syslog	RV-N-188
Bloombase	Bloombase StoreSafe	-	Universal CEF	RV-N-243
BMC	BMC CorreLog	-	Universal CEF	RV-N-243
Bricata	Bricata ProAccel	-	Universal CEF	RV-N-243
Brinqa Risk	Brinqa Risk Analytics	-	Universal CEF	RV-N-243
Broadcom	Symantec Advanced Threat Protection (ATP)	-	Universal CEF	RV-N-243
Broadcom	Symantec Endpoint Protection Mobile	-	Universal CEF	RV-N-243
Broadcom	Symantec Threat Hunting Center	-	Universal CEF	RV-N-243
Check Point	Check Point Endpoint Security	-	Syslog	RV-N-248
Check Point	Check Point Harmony Endpoint	-	Syslog	RV-N-248
Cisco	Cisco ASA	-	Syslog	RV-N-197
Cisco	Cisco IOS	12—15	Syslog	RV-N-244
Cisco	Cisco IOS XE	17.5—17.14	Socket	RV-N-330
Cisco	Cisco IOS XR	7.9.2	Socket	RV-N-333
Cisco	Cisco Secure Email Gateway (SEG)	-	Universal CEF	RV-N-243
Cisco	Cisco Secure Firewall Management Center	-	Universal CEF	RV-N-243
Cisco	NetFlow	9	Syslog	RV-N-197
Cisco	Nexus	10.1	Syslog	RV-N-339
Claroty	Claroty Continuous Threat Detection	-	Universal CEF	RV-N-243
ClickHouse	ClickHouse	-	DB	RV-N-193

Вендор	Продукт	Версия	Тип подключения	ID правила нормализации
CloudPassage	CloudPassage Halo	-	Universal CEF	RV-N-243
Corvil	Corvil Network Analytics	-	Universal CEF	RV-N-243
Cribl	Cribl Stream	-	Universal CEF	RV-N-243
CrowdStrike	Falcon Host	-	Universal CEF	RV-N-243
CyberArk	Privileged Threat Analytics (PTA)	-	Universal CEF	RV-N-243
DeepInstinct	DeepInstinct	-	Universal CEF	RV-N-243
Delinea	Delinea Secret Server	-	Universal CEF	RV-N-243
Digital Guardian	Digital Guardian Endpoint Threat Detection	-	Universal CEF	RV-N-243
Dr.Web	Dr.Web Enterprise Security Suite (ESS)	-	Universal CEF	RV-N-297
Dragos	Dragos Platform	-	Universal CEF	RV-N-243
EclecticIQ	EclecticIQ Intelligence Center	-	Universal CEF	RV-N-243
Edge Technologies	Edge Technologies AppBoard and enPortal	-	Universal CEF	RV-N-243
Efros	Efros DefOps NAC	-	Syslog	RV-N-261
Eltex	Eltex ESR	-	Socket	RV-N-345
ESET	ESET PROTECT	-	Universal CEF	RV-N-243
F5	BIG-IP Advanced Firewall Manager (AFM)	-	Universal CEF	RV-N-243
FFRI	FFR yarai	-	Universal CEF	RV-N-243
FireEye	FireEye CM Series	-	Universal CEF	RV-N-243
FireEye	FireEye Malware Protection System	-	Universal CEF	RV-N-243
Forcepoint	Forcepoint NGFW	-	Universal CEF	RV-N-243
Forcepoint	Forcepoint SMC	-	Universal CEF	RV-N-243
Fortinet	Fortinet FortiAnalyzer	-	Syslog	RV-N-285
Fortinet	FortiSOAR	-	Universal CEF	RV-N-243

Вендор	Продукт	Версия	Тип подключения	ID правила нормализации
FreeIPA	FreeIPA	3, 4	Syslog	RV-N-206 RV-N-207 RV-N-208 RV-N-209
Gigamon	Gigamon GigaVUE	-	Universal CEF	RV-N-243
Hewlett Packard Enterprise	Aruba ClearPass	-	Universal CEF	RV-N-243
Hewlett Packard Enterprise	ArubaOS-CX	10.05	Syslog	RV-N-313
HP	HP ProCurve	-	Syslog	RV-N-321
IBM	IBM InfoSphere Guardium	-	Universal CEF	RV-N-243
IETF	IPFIX	-	Netflow	RV-N-302
Illumio	Policy Compute Engine (PCE)	-	Universal CEF	RV-N-243
Imperva	Imperva Incapsula	-	Universal CEF	RV-N-243
Imperva	Imperva SecureSphere	-	Universal CEF	RV-N-243
InfoWatch	InfoWatch Traffic Monitor	3	DB	RV-N-198
Intralinks	Intralinks VIA	-	Universal CEF	RV-N-243
Jenkins	Jenkins	2.541.1	Syslog	RV-N-305
Kaspersky	Kaspersky Anti Targeted Attack Platform	-	Syslog	RV-N-181
Kaspersky	Kaspersky CyberTrace	-	Syslog	RV-N-182
Kaspersky	Kaspersky Secure Mail Gateway	-	Syslog	RV-N-184
Kaspersky	Kaspersky Security Center	14	DB MS SQL DB MySQL (MariaDB) DB PostgreSQL Syslog CEF	RV-N-183
Kaspersky	Kaspersky Web Traffic Security	6.1	Syslog	RV-N-185

Вендор	Продукт	Версия	Тип подключения	ID правила нормализации
Lieberman Software	Enterprise Random Password Manager (ERPM)	-	Universal CEF	RV-N-243
Lighttpd	Lighttpd	2.4	Syslog	RV-N-231 RV-N-232
Linux	Linux Auth	-	Syslog	RV-N-220
Linux	Linux Auditd	-	Syslog	RV-N-187
Linux	Linux R-Vision Endpoint	-	Syslog	RV-N-229
MariaDB	MariaDB	5—12	Syslog	RV-N-236
Microsoft	Active Directory Domain Services (ADDS)	2008—2022	R-Vision EVO Endpoint	RV-N-277
Microsoft	Active Directory Federation Services (ADFS)	2008—2022	R-Vision EVO Endpoint	RV-N-247
Microsoft	DHCP Server	2008—2022	R-Vision EVO Endpoint	RV-N-245
Microsoft	Exchange Server	2010—2019	R-Vision EVO Endpoint	RV-N-263 RV-N-264 RV-N-347
Microsoft	Hyper-V	-	R-Vision EVO Endpoint	RV-N-228
Microsoft	IIS	2008—2022	R-Vision EVO Endpoint	RV-N-230
Microsoft	Microsoft Windows Terminal Services	-	R-Vision EVO Endpoint	RV-N-310
Microsoft	Microsoft SQL Server	2008—2022	DB (журнал запросов) R-Vision EVO Endpoint (audit)	RV-N-192
Microsoft	Windows PowerShell	2008—2022	R-Vision EVO Endpoint	RV-N-218
Microsoft	Windows Security	2008—2022	R-Vision EVO Endpoint	RV-N-222
Microsoft	Windows Sysmon	2008—2022	R-Vision EVO Endpoint	RV-N-211

Вендор	Продукт	Версия	Тип подключения	ID правила нормализации
Microsoft	Windows System	2008—2022	R-Vision EVO Endpoint	RV-N-228
MongoDB	MongoDB	8	Syslog	RV-N-293
Multifactor	Multifactor Radius Adapter	-	Syslog	RV-N-340
Netgate	pfSense	2.7	Syslog	RV-N-336
NetIQ	NetIQ Identity Manager	-	Universal CEF	RV-N-243
NetScout	NetScout Systems nGenius Performance Manager	-	Universal CEF	RV-N-243
Netskope	Cloud Access Security Broker (CASB)	-	Universal CEF	RV-N-243
Netwrix	Netwrix Auditor	-	Universal CEF	RV-N-243
Nextcloud	Nextcloud	26—29	Syslog	RV-N-300
Nexthink	Nexthink Engine	-	Universal CEF	RV-N-243
Nginx	Nginx	-	Syslog	RV-N-234
NIKSUN	NIKSUN NetDetector	-	Universal CEF	RV-N-243
One Identity	One Identity Privileged Access Management (PAM)	-	Universal CEF	RV-N-243
OpenVPN	OpenVPN	2.4, 2.6	Syslog	RV-N-225 RV-N-226
OpenVPN	OpenVPN Access Server	-	Syslog	RV-N-227
Oracle	MySQL	8	Syslog/DB	RV-N-194 RV-N-195
Orion soft	zVirt	4	DB (PostgreSQL)	RV-N-341
PagerDuty	PagerDuty	-	Universal CEF	RV-N-243
Palo Alto	Cortex Data Lake	-	Universal CEF	RV-N-243
Palo Alto	PAN-OS	-	Universal CEF	RV-N-243
Penta Security	WAPPLES	-	Universal CEF	RV-N-243

Вендор	Продукт	Версия	Тип подключения	ID правила нормализации
Positive Technologies	PT Application Firewall	3	Syslog (audit) Syslog (atack)	RV-N-199 RV-N-200
Positive Technologies	PT Application Firewall	4	Syslog	RV-N-190 RV-N-338
Positive Technologies	PT Sandbox	-	Syslog	RV-N-288
Positive Technologies	PT Network Attack Discovery	-	Syslog	RV-N-203
PostgreSQL	PostgreSQL	14, 17	Syslog	RV-N-189
Progress	Kemp LoadMaster	-	Universal CEF	RV-N-243
Proofpoint	Proofpoint Insider Threat Management	-	Universal CEF	RV-N-243
Recorded Future	Intelligence Cloud Platform	-	Universal CEF	RV-N-243
Red Hat	Linux Auditd	-	Syslog	RV-N-187 RV-N-186 RV-A-2
ReversingLabs	ReversingLabs N1000 Appliance	-	Universal CEF	RV-N-243
R-Vision	R-Vision SOAR	-	Syslog	RV-N-292
R-Vision	R-Vision TDP	-	Socket	RV-N-287
R-Vision	R-Vision TIP	-	Socket	RV-N-298
R-Vision	Универсальный коннектор CEF	CEF v.26	Universal CEF	RV-N-243
SailPoint Technologies	SailPoint IdentityIQ	-	Universal CEF	RV-N-243
SentinelOne	SentinelOne	-	Universal CEF	RV-N-243
Sonatype	Sonatype Nexus Repository	3.89.0	Syslog	RV-N-304
Squid Software Foundation	Squid	4.5—7.4	Syslog	RV-N-309
Suricata	Suricata	-	Syslog	RV-N-314
Thales eSecurity	Vormetric Data Security Manager	-	Universal CEF	RV-N-243
ThreatConnect	Threat Intelligence Platform	-	Universal CEF	RV-N-243
ThreatQuotient	ThreatQuotient	-	Universal CEF	RV-N-243

Вендор	Продукт	Версия	Тип подключения	ID правила нормализации
TrapX Security	DeceptionGrid	-	Universal CEF	RV-N-243
Trend Micro	Trend Micro Control Manager	-	Universal CEF	RV-N-243
Trend Micro	Trend Micro Deep Security	-	Universal CEF	RV-N-243
Trend Micro	Trend Micro NGFW	-	Universal CEF	RV-N-243
Trustwave	Trustwave DbProtect	-	Universal CEF	RV-N-243
Varonis Systems	DatAdvantage	-	Universal CEF	RV-N-243
Veeam Software	Veeam Backup & Replication	11	R-Vision EVO Endpoint	RV-N-246
Veriato	Veriato 360	-	Universal CEF	RV-N-243
VMware	VMware Carbon Black EDR	-	Universal CEF	RV-N-243
VMware	VMware ESXi	6—8	Syslog	RV-N-179
VMware	VMware Horizon	8.10	Syslog	RV-N-295
VMware	VMware vCenter Server	6—8	Syslog	RV-N-180
Votiro	Votiro Disarmer for Windows	-	Universal CEF	RV-N-243
Webroot	Webroot BrightCloud	-	Universal CEF	RV-N-243
Zabbix	Zabbix	-	DB	RV-N-260
Zettaset	BDEncrypt	-	Universal CEF	RV-N-243
Zscaler	Zscaler Nanolog Streaming Service (NSS)	-	Universal CEF	RV-N-243
1С	1С:Предприятие	8.3	SMB	RV-N-258 RV-N-289
1С-Битрикс	Битрикс24	-	DB (MySQL)	RV-N-307
Айдеко	Ideco NGFW	-	Syslog	RV-N-296
АйТи Бастион	СКДПУ НТ	-	Universal CEF	RV-N-191 RV-N-243
Гарда Технологии	Гарда DLP	6.0	Syslog	RV-N-326
Гарда Технологии	Гарда NDR	4	DB Syslog	RV-N-335 RV-N-337
Гарда Технологии	Гарда WAF	2.4	DB (PostgreSQL)	RV-N-223

Вендор	Продукт	Версия	Тип подключения	ID правила нормализации
ИнфоТеКС	ViPNet IDS NS	3.10	Syslog CEF	RV-N-281
ИнфоТеКС	ViPNet Coordinator 4	4	Syslog CEF	RV-N-329
ИнфоТеКС	ViPNet TIAS	3.10	Syslog CEF	RV-N-283
Код Безопасности	Secret Net Studio	8	DB (audit) DB (sec events)	RV-N-109 RV-N-201 RV-N-202
Код Безопасности	Континент	3.9.3	Syslog	RV-N-266
Код Безопасности	Континент	4	Syslog, DB	RV-N-273 RV-N-274 RV-N-276
Пассворк	Пассворк	-	Syslog	RV-N-224
РЕД СОФТ	РЕД База Данных	5.1.4	Syslog	RV-N-318
С-Терра СиЭсПи	С-Терра Шлюз	4.3	Syslog	RV-N-311
СберТех	Platform V Pangolin DB	7	Syslog	RV-N-350
СёрчИнформ	СёрчИнформ КИБ	-	Socket	RV-N-312
Солар	Solar Dozor	7, 8	Syslog	RV-N-219
Солар	Solar webProxy	-	Syslog	RV-N-331

Правила корреляции

- Памятка по правилам корреляции
- Аналитические истории

Памятка по правилам корреляции

Правила корреляции в R-Vision SIEM — это не только набор выражений, которые определяют логику детектирования, но и полноценный экспертный контент. Он спроектирован так, чтобы аналитик мог быстрее погрузиться в контекст работы правила и оперативно перейти к локализации угрозы.

Глубокая экспертиза «из коробки»

- **Источник событий** (`data_source`) — перечень событий, необходимых для корректной работы правила. Это упрощает диагностику и позволяет определить, каких событий может не хватать в SIEM при отсутствии ожидаемых оповещений.
- **Экспертные ссылки** (`reference`) — перечень ссылок на внешние рекомендации и наши собственные аналитические разборы. Это позволяет даже начинающему специалисту мгновенно

погрузиться в контекст сложной атаки.

- **Связь с матрицей MITRE ATT&CK** (`tags`) — позволяет визуализировать общую защищенность инфраструктуры и понять «почерк» атакующего.
- **Корреляционное событие** (`on_correlate`) — правило интерпретирует технические данные и включает категоризацию и разъяснение на естественном языке (кто, что, где, когда и с каким результатом). Это позволяет аналитику получить полный контекст события, не просматривая сырые логи от источника.

Таксономия инцидента

Поле `incident_taxonomy` содержит информацию о категории, типе и уникальном ID инцидента. Это позволяет настроить бесшовную передачу подозрений на инцидент в SOAR-систему и запуск сценария реагирования.

Рекомендации по реагированию

В поле `response` заложен пошаговый план действий, который разделен на логические этапы:

- **Коммуникация** (`communication`): с кем нужно взаимодействовать и какие вопросы задать.
- **Анализ** (`analysis`): какие действия провести для подтверждения факта атаки и что именно проверить.
- **Локализация** (`containment`): как оперативно ограничить распространение угрозы.
- **Устранение** (`remediation`): как вернуть скомпрометированную систему в безопасное состояние.

Тестирование

Каждое разрабатываемое нами правило содержит Unit-тесты (`tests`) с примерами событий. Они гарантируют работоспособность логики. Вы можете использовать эти примеры как эталон, чтобы понять, как именно правило «видит» атаку.

Аналитические истории

Антивирусное ПО

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемого антивирусного программного обеспечения:

- Dr.Web Enterprise Security Suite
- Kaspersky Secure Mail Gateway
- Kaspersky Security Center
- Positive Technologies Sandbox

Dr.Web Enterprise Security Suite

- Dr.Web Enterprise Security Suite: настройка источника

Dr.Web Enterprise Security Suite: настройка источника

Данное руководство описывает процесс настройки сбора событий Dr.Web Enterprise Security Suite (ESS) в формате CEF и их отправки в R-Vision SIEM.

Предварительные требования

Перед настройкой пересылки событий в R-Vision SIEM убедитесь, что сетевая связность между сервером Dr.Web и SIEM обеспечена, а необходимые порты открыты.

Настройка Dr.Web ESS

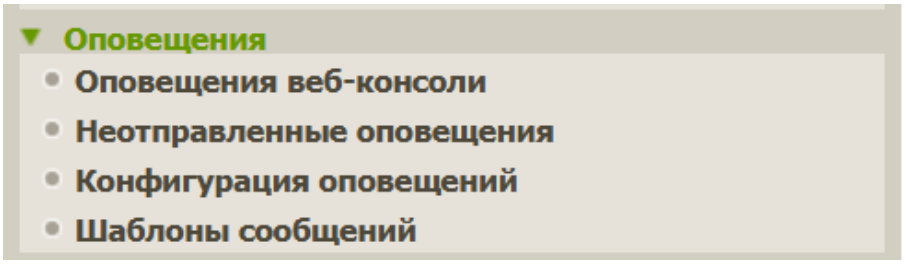
Настройка отправки событий в R-Vision SIEM

Чтобы настроить отправку событий Dr.Web ESS в R-Vision SIEM, выполните следующие шаги:

1. Войдите в веб-интерфейс Dr.Web под учетной записью с правами администратора.
2. Перейдите в раздел **Администрирование**.



3. В разделе **Оповещения** выберите вариант **Конфигурация оповещений**.



4. Выберите из выпадающего списка **Метод отправки оповещений** вариант **Syslog**.
5. В поле **Получатель** укажите адрес коллектора SIEM или промежуточный сервер Syslog в

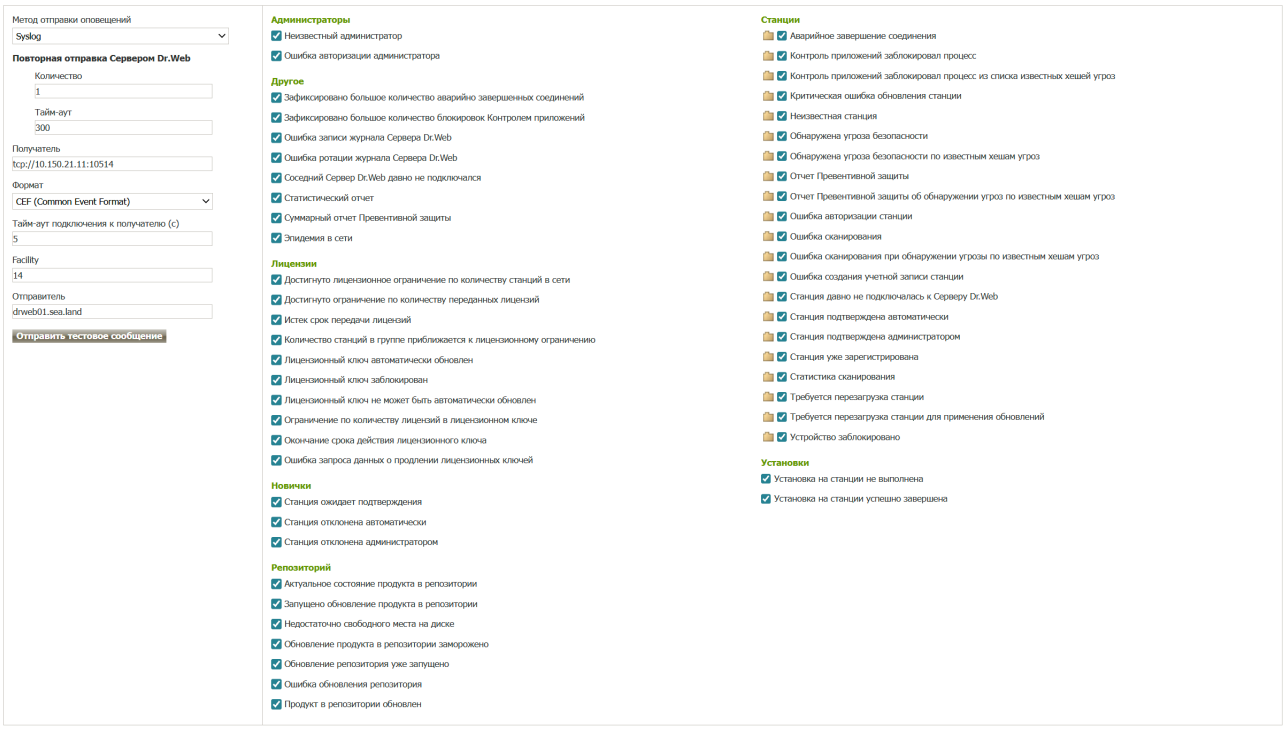
формате:

```
<protocol>://<ip>:<port>
```

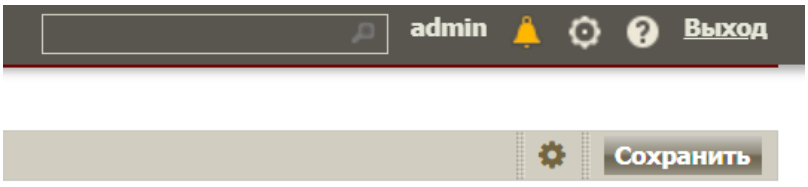
Здесь:

- `<protocol>` — сетевой протокол: `tcp` или `udp`.
- `<ip>` — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- `<port>` — порт точки входа Socket на конвейере SIEM.

6. Выберите из выпадающего списка формат событий **CEF (Common Event Format)**.
7. В поле **Отправитель** укажите FQDN сервера Dr.Web.
8. Убедитесь, что установлены все флажки.



9. Нажмите на кнопку **Сохранить** в правом верхнем углу.



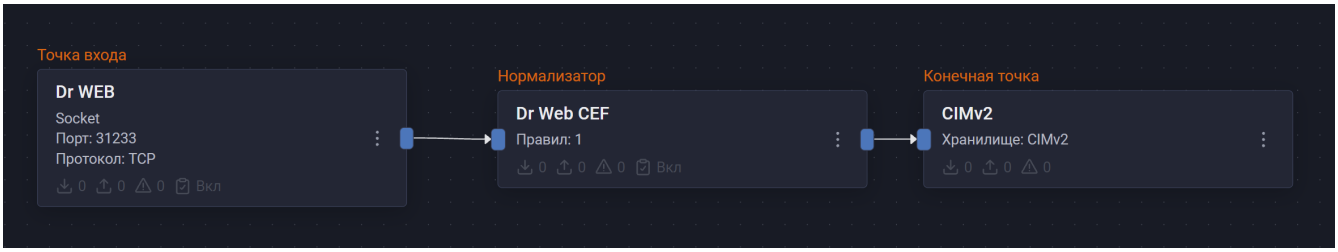
Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.

2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
    - Название: введите название точки входа.
    - Тип точки входа: выберите вариант **Socket**.
    - Порт точки входа: введите значение в соответствии с настройками на стороне Dr.Web ESS.
    - Протокол: выберите вариант в соответствии с настройками на стороне Dr.Web ESS.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Dr Wed ESS** (идентификатор правила: **RV-N-297**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

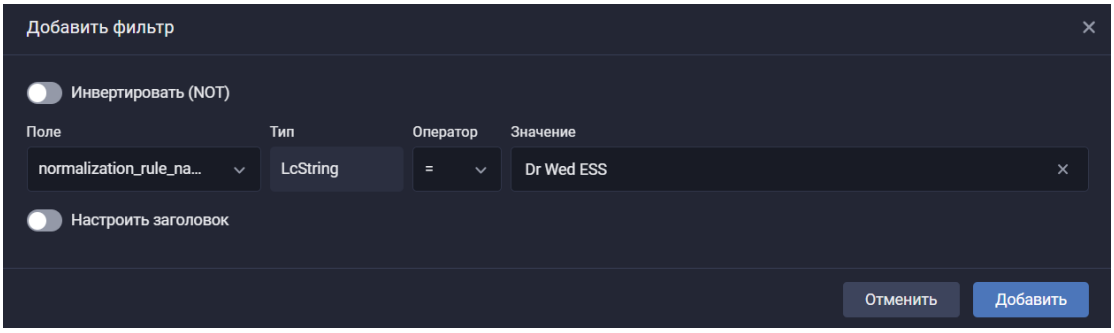
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Dr.Web ESS.

Найти события Dr.Web ESS в хранилище можно по следующему фильтру:

```
normalization_rule_name = "Dr Wed ESS"
```



Kaspersky Secure Mail Gateway

- Kaspersky Secure Mail Gateway: настройка источника
- Kaspersky Secure Mail Gateway: правила корреляции

Kaspersky Secure Mail Gateway: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Kaspersky Secure Mail Gateway в R-Vision SIEM.

Предварительные требования

Для включения экспорта событий в режиме Technical Support Mode требуется предварительно загрузить открытый ключ SSH в веб-интерфейсе приложения.

Настройка Kaspersky Secure Mail Gateway

Вы можете сохранять файлы с экспортированными событиями локально на сервере, а также настроить их публикацию во внешнюю SIEM-систему. Если вам не требуется сохранять файлы локально, пропустите шаги 4—7 из инструкции этого раздела.

Выполните инструкцию ниже на каждом узле кластера, события с которого вы хотите экспортировать в формате `CEF`.

Чтобы настроить экспорт событий в формате `CEF`, выполните следующие шаги:

1. Подключитесь к консоли управления виртуальной машиной Kaspersky Secure Mail Gateway под учетной записью `root`, используя закрытый ключ SSH. Вы войдете в режим Technical Support Mode.
2. Внесите следующие изменения в файл с параметрами экспорта событий `/opt/kaspersky/ksmg/share/templates/core_settings/event_logger.json.template`:
    - Укажите в блоке `siemSettings` одно из следующих значений параметра `facility`, если вы хотите выбрать категорию (facility) для `syslog`, в которую будут экспортироваться события:
        - `Auth`;
        - `Authpriv`;
        - `Cron`;
        - `Daemon`;
        - `Ftp`;
        - `Lpr`;
        - `Mail`;
        - `News`;
        - `Syslog`;
        - `User`;
        - `Uucp`;
        - `Local0`;
        - `Local1`;
        - `Local2`;
        - `Local3`;

- Local4;
- Local5;
- Local6;
- Local7.



Рекомендуется указать категорию (facility) для syslog, которая не используется другими программами на сервере. По умолчанию установлено значение local2.

- Установите значение параметра enabled равным true.
- Задайте уровень детализации экспорта, установив одно из следующих значений параметра logLevel:
  - Error — экспорт событий, связанных с возникновением ошибок;
  - Info — экспорт всех событий.

  Пример:

```
"siemSettings":
{
"enabled": true,
"facility": "Local2",
"logLevel": "Info"
}
```

3. В файле /etc/rsyslog.conf измените строку:

```
*.info;mail.none;authpriv.none;cron.none;local0.none;local1.none /var/log/messages
```

на:

```
*.info;mail.none;authpriv.none;cron.none;local0.none;local1.none;<категория
(facility), выбранная на шаге 2>.none /var/log/messages
```

4. Добавьте в файл /etc/rsyslog.conf следующую строку:

```
<категория (facility), выбранная на шаге 2>.* -/var/log/ksmg-cef-messages
```

5. Создайте файл /var/log/ksmg-cef-messages и настройте права доступа к нему, выполнив следующие команды:

```
touch /var/log/ksmg-cef-messages
chown root:klusers /var/log/ksmg-cef-messages
```

```
chmod 640 /var/log/ksmg-cef-messages
```

6. Настройте правила ротации файлов с экспортированными событиями, добавив в файл `/etc/logrotate.d/ksmg-syslog` следующие строки:

```
/var/log/ksmg-cef-messages
{
size 500M
rotate 10
notifempty
sharedscripts
postrotate
/usr/bin/systemctl kill -s HUP rsyslog.service >/dev/null 2>&1 || true
endscript
}
```

7. Перезапустите службу `rsyslog`, выполнив следующую команду:

```
service rsyslog restart
```

8. В веб-интерфейсе приложения перейдите в раздел **Параметры** → **Журналы и события** → **События**.
9. Внесите изменение в значение любого параметра.
10. Нажмите на кнопку **Сохранить**.



Это необходимо для синхронизации параметров между узлами кластера и применения изменений, внесенных в конфигурационный файл. После этого вы можете вернуть исходное значение измененного параметра.

Экспорт событий в формате CEF настроен.

Настройка отправки событий в SIEM-систему

Перед началом настройки убедитесь, что вы включили экспорт событий в формате CEF.

Выполните инструкцию ниже на каждом узле кластера, события с которого требуется публиковать в SIEM-систему.

Чтобы настроить публикацию событий приложения в SIEM-систему:

1. Подключитесь к консоли управления виртуальной машиной Kaspersky Secure Mail Gateway под учетной записью `root`, используя закрытый ключ SSH. Вы войдете в режим Technical Support Mode.
2. Укажите адрес и порт подключения к серверу с SIEM-системой, добавив в конец файла `/etc/rsyslog.conf` следующие строки:

```
$ActionQueueFileName ForwardToSIEM
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
$ActionResumeRetryCount -1
<категория (facility)>.* @@<IP-адрес SIEM-системы>:<порт, на котором SIEM-система
принимает сообщения от Syslog по протоколу TCP>
```



Перед внесением изменений в файл `/etc/rsyslog.conf` рекомендуется сделать его резервную копию. Ошибка при редактировании файла может привести к некорректной работе системы.

3. Перезапустите службу `rsyslog`, выполнив следующую команду:

```
service rsyslog restart
```

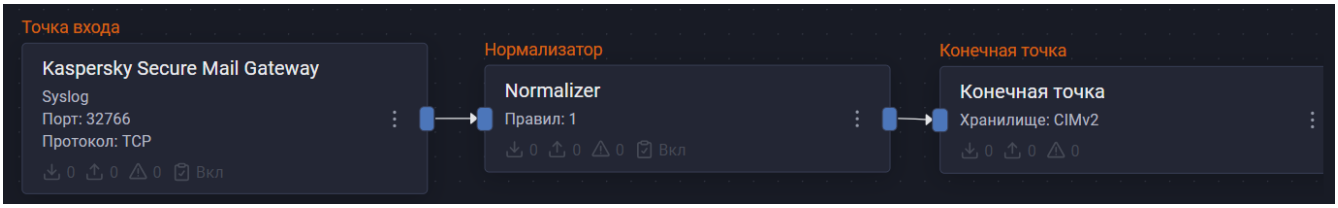
Публикация событий приложения в SIEM-систему настроена.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне Kaspersky Secure Mail Gateway.
   - Протокол: выберите вариант в соответствии с настройками на стороне Kaspersky Secure Mail Gateway.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Kaspersky Secure Mail Gateway** (идентификатор правила: **RV-N-184**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

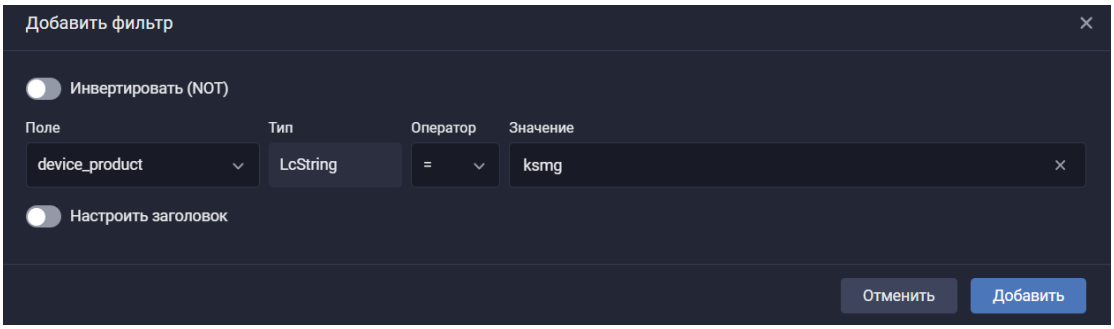
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Kaspersky Secure Mail Gateway.

Найти события Kaspersky Secure Mail Gateway в хранилище можно по следующему фильтру:

```
device_product = "ksmg"
```



Kaspersky Secure Mail Gateway: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-961	Шифрованное вложение в письме	Данное правило направлено на обнаружение шифрованного вложения в письме средствами KSMG. Данная атака может быть началом попыток получения доступа в ИС компании.	• Initial Access (TA0001) • Obfuscated Files or Information (T1027) • Internal Spearphishing (T1534) • Phishing (T1566) • Spearphishing Attachment (T1566.001) • Phishing for Information (T1598) • Spearphishing Attachment (T1598.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-962	Проверка подлинности отправителя сообщений	Данное правило направлено на детектирование инцидентов, связанных с проверкой подлинности отправителей сообщений в письме, с использованием средств KSMG. Проверка подлинности отправителей сообщений предназначена для дополнительной защиты почтовой инфраструктуры от атаки, при которой атакующий может заменить почту на доверенную.	• Initial Access (TA0001) • Internal Spearphishing (T1534) • Phishing (T1566) • Phishing for Information (T1598)
RV-D-963	Вредоносное вложение в письме	Данное правило направлено на обнаружение вредоносного вложения в письме средствами KSMG. Вредоносное вложение может содержаться как в тексте письма, так и в файле во вложении. Данная атака может быть началом попыток получения доступа в ИС компании.	• Initial Access (TA0001) • Internal Spearphishing (T1534) • Phishing (T1566) • Spearphishing Attachment (T1566.001) • Spearphishing Link (T1566.002) • Phishing for Information (T1598) • Spearphishing Attachment (T1598.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-964	Получение массовой рассылки писем	Данное правило направлено на детектирование инцидентов, связанных с массовой рассылкой писем, с использованием средств KSMG. Массовые рассылки могут быть использованы атакующими для распространения спама, фишинга или вредоносного ПО, а также для организации атак на почтовую инфраструктуру организации. Правило позволяет выявлять подозрительную активность, связанную с отправкой большого количества писем за короткий промежуток времени, что может указывать на попытку злоупотребления почтовой системой.	• Initial Access (TA0001) • Phishing (T1566) • Phishing for Information (T1598) • Email Bombing (T1667)
RV-D-965	Получение спам-письма	Данное правило направлено на обнаружение инцидентов, связанных с получением спам-писем, с использованием средств KSMG. Спам-письма могут содержать нежелательную рекламу, фишинговые ссылки или вредоносные вложения, что представляет угрозу для безопасности почтовой инфраструктуры и пользователей организации.	• Initial Access (TA0001) • Phishing (T1566) • Phishing for Information (T1598)

ID правила	Название правила	Описание	Тактики и техники
RV-D-966	Вредоносная ссылка в письме	Данное правило направлено на детектирование инцидентов, связанных с получением вредоносных ссылок в письме, на основе событий KSMG. Ссылки могут содержать вредоносные вложения, что представляет угрозу для безопасности почтовой инфраструктуры и пользователей организации.	• Initial Access (TA0001) • Drive-by Compromise (T1189) • User Execution (T1204) • Malicious Link (T1204.001) • Phishing (T1566) • Spearphishing Link (T1566.002) • Phishing for Information (T1598) • Spearphishing Link (T1598.003)

Kaspersky Security Center

- Kaspersky Security Center: настройка источника
- kaspersky-security-center-rules.pdf

Kaspersky Security Center: настройка источника

Данный раздел содержит инструкции по сбору событий из журналов Kaspersky Security Center различными методами:

- Kaspersky Security Center: сбор из СУБД MS SQL
- Kaspersky Security Center: сбор из СУБД MySQL (MariaDB)
- Kaspersky Security Center: сбор из СУБД PostgreSQL

Kaspersky Security Center: сбор из СУБД MS SQL

Предварительные требования

- Сетевая доступность сервера СУБД Kaspersky Security Center по целевому порту и протоколу для каждой ноды кластера SIEM.
- Учетная запись в СУБД с правами на чтение таблицы **kav.dbo.ev_event** (сбор событий из БД).

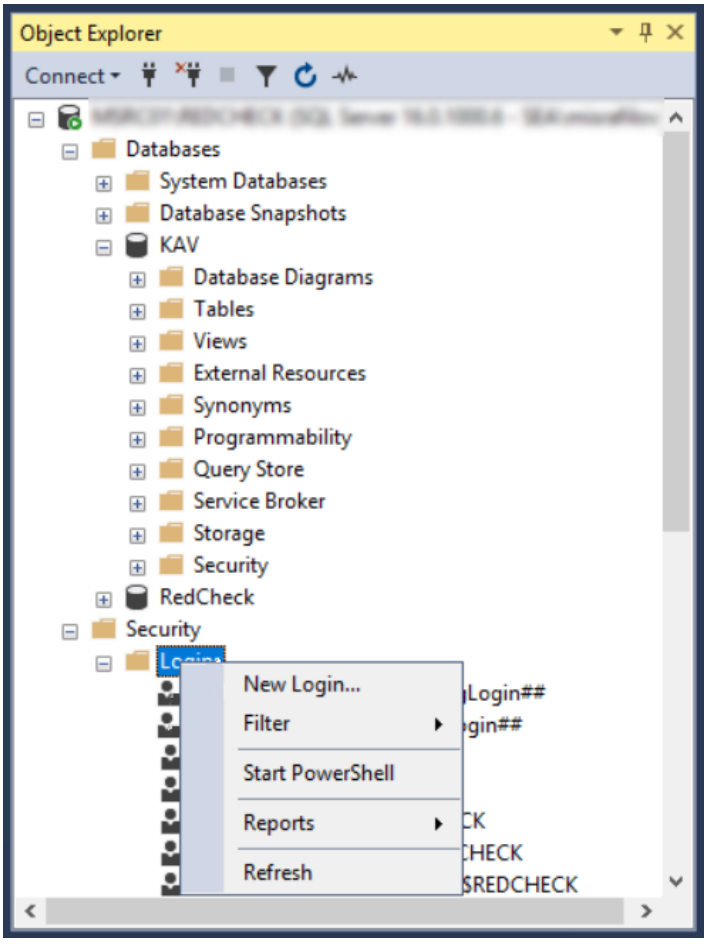
Настройка СУБД MS SQL

События Kaspersky Security Center записываются в таблицу `ev_event` базы данных KAV СУБД MS SQL. Для настройки сбора логов из базы данных необходимо к ней подключиться. Используйте для подключения специально созданную сервисную учетную запись (далее — УЗ).

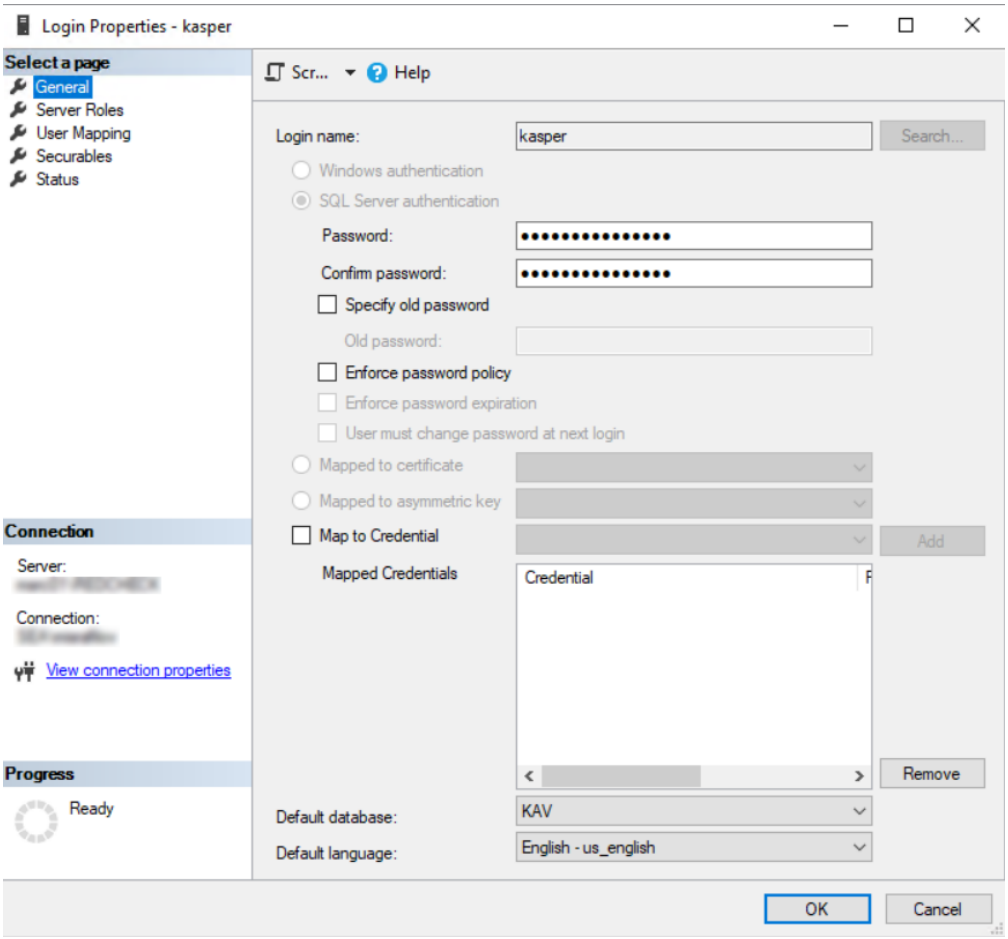
Создание учетной записи в СУБД MS SQL

Чтобы создать сервисную УЗ, подключитесь к СУБД с правами администратора. Для этого выполните следующие действия в SQL Server Management Studio:

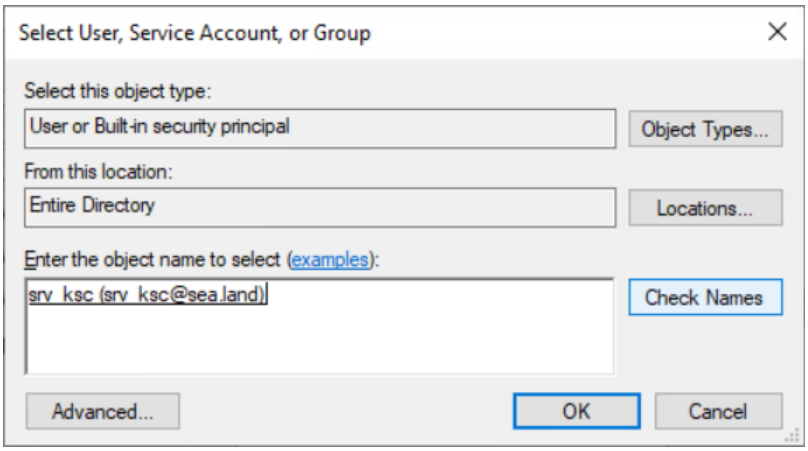
1. Выберите **New Login** в контекстном меню для **Security/Logins**.



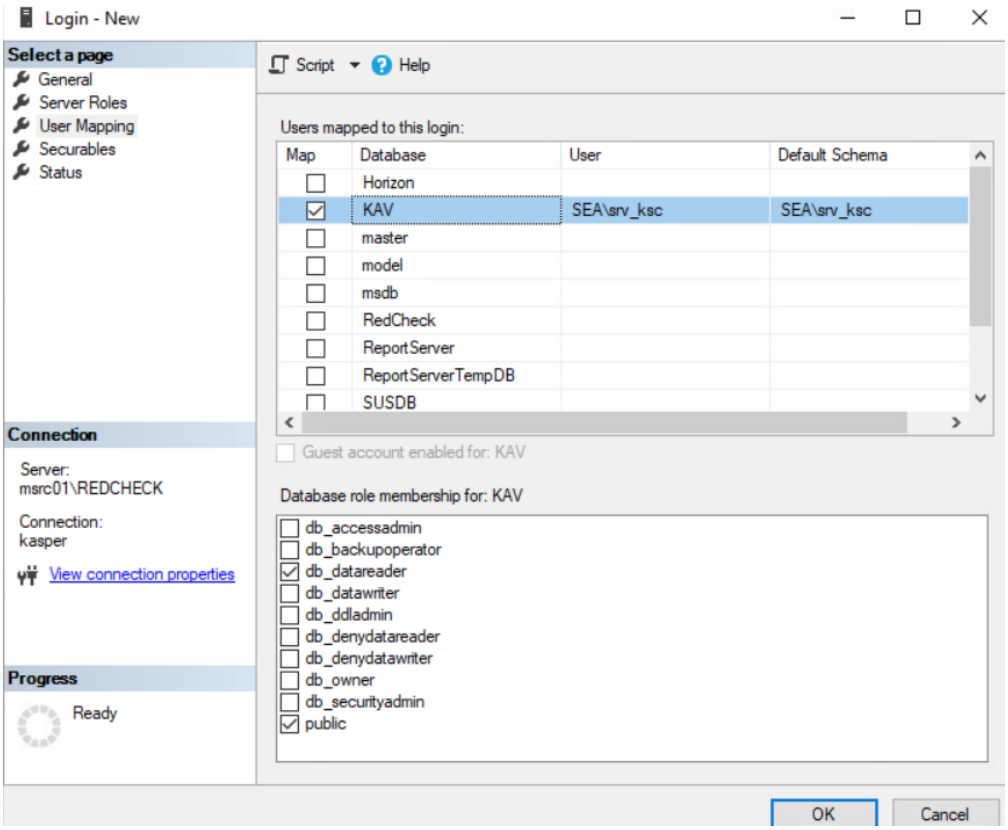
2. Создайте сервисную учетную запись.



Вместо локальной УЗ вы также можете использовать заранее созданную доменную.

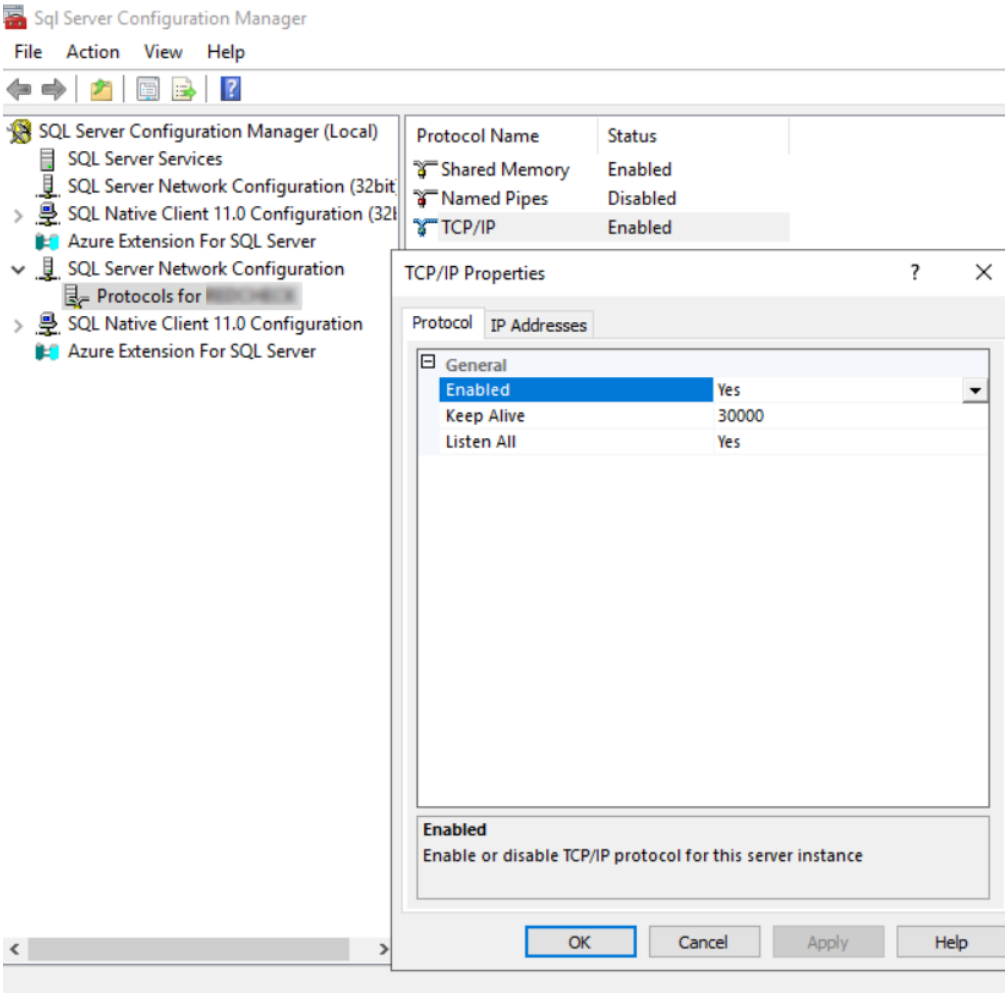


3. Предоставьте учетной записи права на чтение базы KAV.



Настройка сервера MS SQL

В настройках SQL Server Configuration Manager убедитесь, что TCP/IP включен в конфигурации сети SQL Server.



Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте секрет со строкой подключения. Для этого:
   a. Перейдите в **Ресурсы** → **Секреты** → **Создать**.
   b. В раскрывшемся окне создания секрета заполните поля:
      - Название: введите название секрета.
      - Описание (опционально): опишите, для чего будет использоваться секрет.
      - Тип секрета: выберите вариант **Строка подключения**.
      - Строка подключения — введите строку вида:

```
jdbc:sqlserver://DBSERVER:1433;encrypt=false;databaseName=KAV;user=kasper;password={passw0rd}
```

      Здесь:

      - `encrypt=false` — указывается так как SQL сервер по умолчанию не имеет подписанного сертификата центром сертификации.
      - `{passw0rd}` — пароль указывается в фигурных скобках для экранирования в случае

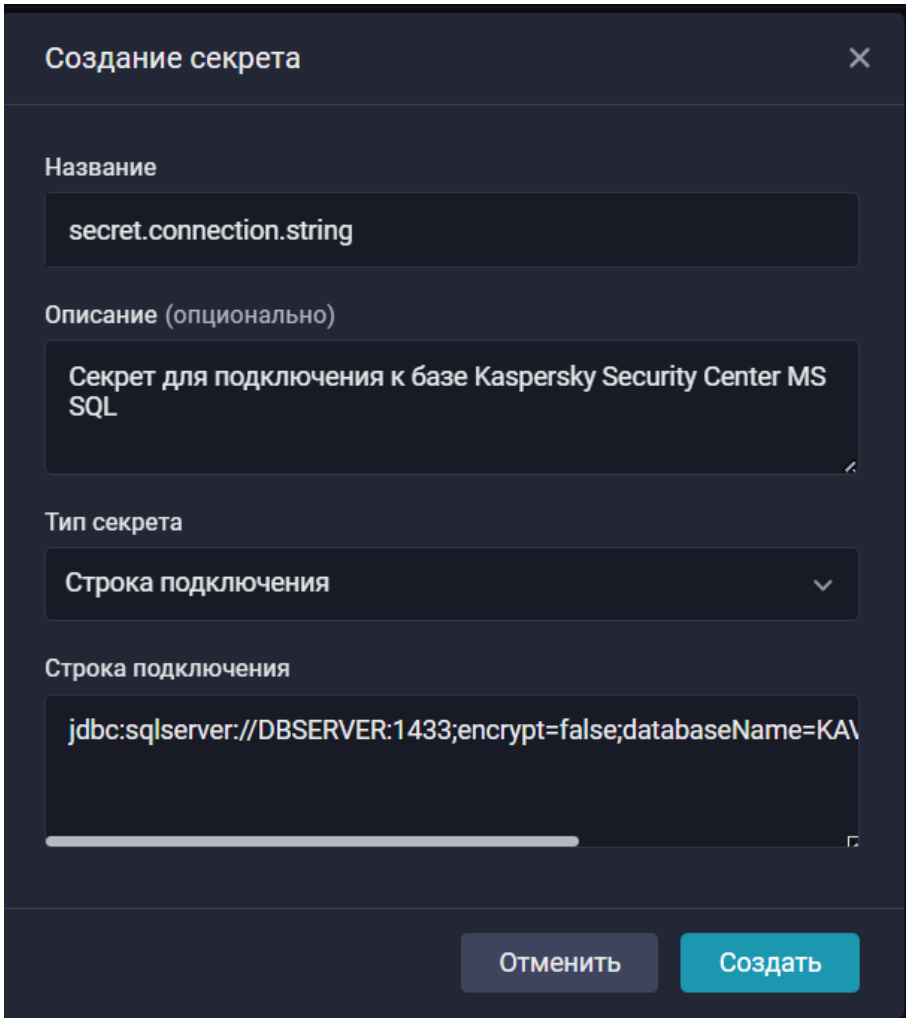
если пароль содержит спецсимволы.

Строка подключения в секрете в случае использования доменной учетной записи:

```
jdbc:sqlserver://DBSERVER:1433;encrypt=false;databaseName=KAV;authentication
Scheme=NTLM;integratedSecurity=true;user=srv_ksc;password={P@ssw0rd}
```

Здесь:

- `DBSERVER` — FQDN или IP-адрес сервера СУБД.
- `1433` — порт подключения.
- `authenticationScheme=NTLM` — параметр предназначен для использования наиболее безопасной версии протокола при согласовании с сервером. Данный параметр говорит драйверу не выполняет аутентификацию самостоятельно, а обращаться к SSPI Windows с запросом аутентификации на указанном сервере и SSPI сам определяет текущий домен, доступные учетные данные и доменные политики безопасности.



c. Нажмите на кнопку **Создать**.

2. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
3. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:

- Название: введите название точки входа.
- Тип точки входа: выберите вариант **Database**.
- Драйвер базы данных: выберите вариант MS SQL.
- Адрес подключения: выберите секрет, созданный ранее.
- SQL-запрос — введите запрос вида:

```
SELECT
    TOP 2000 'ksc' AS appname
    , ev.event_id AS event_id
    , ev.event_type_id AS deviceEventClassId
    , ev.severity AS severity
     , ev.task_display_name AS taskDisplayName
     , ev.product_name AS product_name
     , ev.product_displ_version AS product_version
     , ev.event_type AS externalId
     , ev.event_type_display_name AS event_subcode
     , ev.descr AS msg
     , CASE
         WHEN ev.rise_time is not NULL
            THEN DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),ev.rise_time
)
            ELSE ev.rise_time END AS endTime
    , CASE
        WHEN ev.registration_time is not NULL
            THEN
DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),ev.registration_time )
            ELSE ev.registration_time END AS kscRegistrationTime
     , cast(ev.par7 AS varchar(4000)) AS sourceUserName
     , hs.wstrWinName AS dHost
     , hs.wstrWinDomain AS strNtDom
     , serv.wstrWinName AS kscName
     , CAST(hs.nIp / 256 / 256 / 256 % 256 AS VARCHAR) + '.'
           + CAST(hs.nIp / 256 / 256 % 256 AS VARCHAR) + '.'
           + CAST(hs.nIp / 256 % 256 AS VARCHAR) + '.'
           + CAST(hs.nIp % 256 AS VARCHAR) AS sourceAddress
     , serv.wstrWinDomain AS kscNtDomain
     , CAST(serv.nIp / 256 / 256 / 256 % 256 AS VARCHAR) + '.'
       + CAST(serv.nIp / 256 / 256 % 256 AS VARCHAR) + '.'
       + CAST(serv.nIp / 256 % 256 AS VARCHAR) + '.'
       + CAST(serv.nIp % 256 AS VARCHAR) AS kscIP
     , CASE
         WHEN virus.tmVirusFoundTime IS NOT NULL
            THEN
DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),virus.tmVirusFoundTime )
            ELSE ev.registration_time END AS virusTime
     , virus.wstrObject AS filePath
     , virus.wstrVirusName AS virusName
     , virus.result_ev AS result
 FROM kav.dbo.ev_event AS ev
```

```
LEFT JOIN kav.dbo.v_akpub_host AS hs
   ON ev.nHostId = hs.nId
INNER JOIN kav.dbo.v_akpub_host AS serv
   ON serv.nId = 1
LEFT JOIN kav.dbo.rpt_viract_index AS Virus
   ON ev.event_type_id = virus.nEventVirus
WHERE event_id > ?
ORDER BY ev.event_id ASC
```

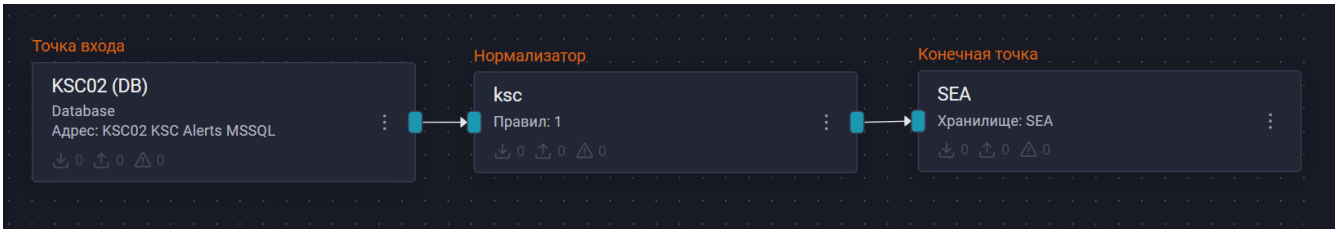


При большом количестве событий в СУБД рекомендуется добавлять `TOP 2000` в начало SQL-запроса.

- Поле идентификатора: введите ключ `event_id` со значением `1`.
- Интервал запроса, секунд: введите значение `15`.

4. Добавьте на конвейер элемент **Нормализатор** с правилом **Kaspersky Security Center - сбор из СУБД** (идентификатор правила: **RV-N-183**).
5. Соедините нормализатор с точкой входа.
6. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
7. Соедините конечную точку с нормализатором.
8. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

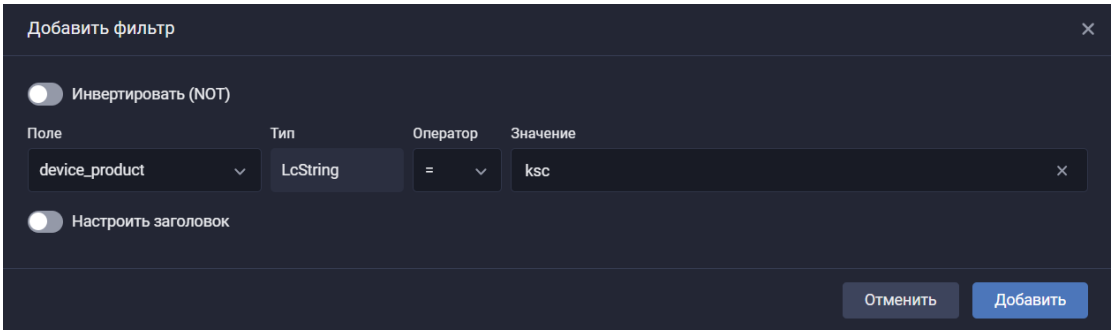


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события MS SQL.



Найти события Kaspersky Security Center в хранилище можно по следующему фильтру:

```
device_product = "ksc"
```



Kaspersky Security Center: сбор из СУБД MySQL (MariaDB)

Предварительные требования

- Сетевая доступность сервера СУБД Kaspersky Security Center по целевому порту и протоколу для каждой ноды кластера SIEM.
- Учетная запись в СУБД с правами на чтение таблицы **ev_event** (сбор событий из БД).

Настройка СУБД MySQL (MariaDB)

Создание учетной записи в СУБД MySQL (MariaDB)

Для создания сервисной УЗ подключитесь к СУБД с правами администратора. Для этого на сервере с установленной СУБД выполните следующие действия:

1. Выполните следующую команду от имени пользователя `root`:

   ```
   mysql -u root -p
   ```

2. Создайте сервисную учетную запись, выполнив следующую команду:

   ```
   CREATE USER 'kasper'@'localhost' IDENTIFIED BY 'passw0rd';
   ```

3. Предоставьте сервисной учетной записи права на подключение к базе и чтение таблицы:

   ```
   GRANT CONNECT ON DATABASE KAV to kasper;
   GRANT SELECT ON ev_event TO 'kasper'@'localhost';
   ```

Настройка в R-Vision SIEM

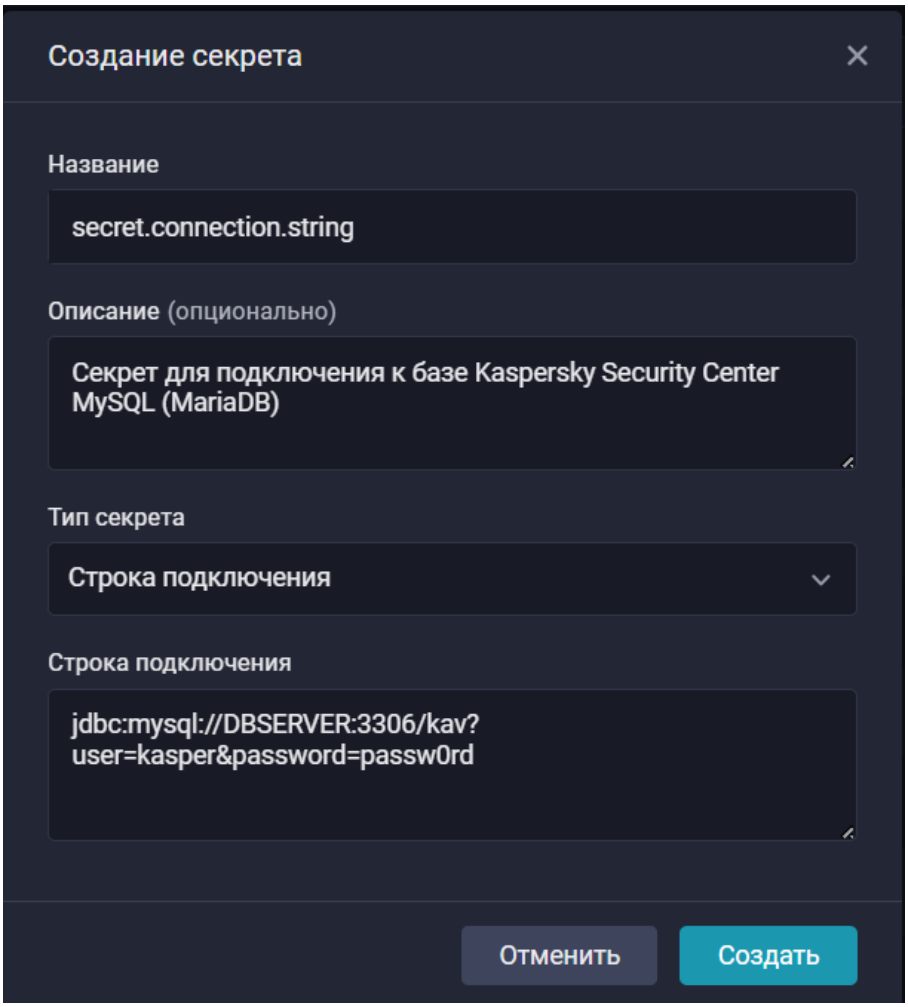
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте секрет со строкой подключения. Для этого:
   a. Перейдите в **Ресурсы** → **Секреты** → **Создать**.
   b. В раскрывшемся окне создания секрета заполните поля:
      - Название: введите название секрета.
      - Описание (опционально): опишите, для чего будет использоваться секрет.
      - Тип секрета: выберите вариант **Строка подключения**.
      - Строка подключения — введите строку вида:

        ```
        jdbc:mysql://DBSERVER:3306/kav?user=kasper&password=passw0rd
        ```

        Здесь:

- `DBSERVER` — FQDN или IP-адрес сервера СУБД.
- `3306` — порт подключения.



c. Нажмите на кнопку **Создать**.

2. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
3. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Database**.
   - Драйвер базы данных: выберите вариант MySQL.
   - Адрес подключения: выберите секрет, созданный ранее.
   - SQL-запрос — введите запрос вида:

```
SELECT 'ksc' AS appname,
    ev.event_id AS event_id,
    ev.event_type_id AS deviceEventClassId,
    ev.severity AS severity,
    ev.task_display_name AS taskDisplayName,
    ev.product_name AS product_name,
    ev.product_displ_version AS product_version,
    ev.event_type AS externalId,
    ev.event_type_display_name AS event_subcode,
```

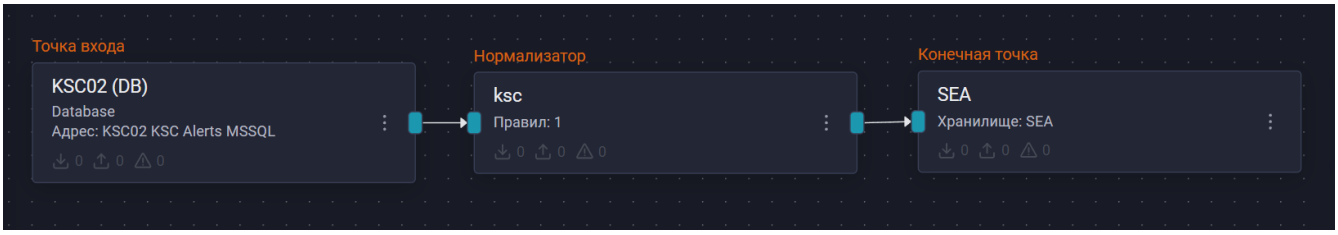
```
    ev.descr AS msg,
    CASE
        WHEN ev.rise_time IS NOT NULL THEN DATE_ADD(ev.rise_time, INTERVAL
TIMESTAMPDIFF(HOUR, UTC_TIMESTAMP(), NOW()) HOUR)
        ELSE ev.rise_time
    END AS endTime,
    CASE
        WHEN ev.registration_time IS NOT NULL THEN
DATE_ADD(ev.registration_time, INTERVAL TIMESTAMPDIFF(HOUR, UTC_TIMESTAMP(),
NOW()) HOUR)
        ELSE ev.registration_time
    END AS kscRegistrationTime,
    CAST(ev.par7 AS CHAR(4000)) AS sourceUserName,
    hs.wstrWinName AS dHost,
    hs.wstrWinDomain AS strNtDom,
    serv.wstrWinName AS kscName,
    CONCAT(
        FLOOR(hs.nIp / 256 / 256 / 256 % 256), '.',
        FLOOR(hs.nIp / 256 / 256 % 256), '.',
        FLOOR(hs.nIp / 256 % 256), '.',
        FLOOR(hs.nIp % 256)
    ) AS sourceAddress,
    serv.wstrWinDomain AS kscNtDomain,
    CONCAT(
        FLOOR(serv.nIp / 256 / 256 / 256 % 256), '.',
        FLOOR(serv.nIp / 256 / 256 % 256), '.',
        FLOOR(serv.nIp / 256 % 256), '.',
        FLOOR(serv.nIp % 256)
    ) AS kscIP,
    CASE
        WHEN virus.tmVirusFoundTime IS NOT NULL THEN
DATE_ADD(virus.tmVirusFoundTime, INTERVAL TIMESTAMPDIFF(HOUR, UTC_TIMESTAMP(),
NOW()) HOUR)
        ELSE ev.registration_time
    END AS virusTime,
    virus.wstrObject AS filePath,
    virus.wstrVirusName AS virusName,
    virus.result_ev AS result
FROM kav.ev_event AS ev
LEFT JOIN kav.v_akpub_host AS hs ON ev.nHostId = hs.nId
INNER JOIN kav.v_akpub_host AS serv ON serv.nId = 1
LEFT JOIN kav.rpt_viract_index AS virus ON ev.event_type_id = virus.nEventVirus
WHERE
 ev.event_id > ? ORDER BY ev.event_id ASC
```

- Поле идентификатора: введите ключ `event_id` со значением 1.
- Интервал запроса, секунд: введите значение 15.

4. Добавьте на конвейер элемент **Нормализатор** с правилом **Kaspersky Security Center - сбор из СУБД** (идентификатор правила: **RV-N-183**).

5. Соедините нормализатор с точкой входа.
6. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
7. Соедините конечную точку с нормализатором.
8. Сохраните и установите конфигурацию конвейера.

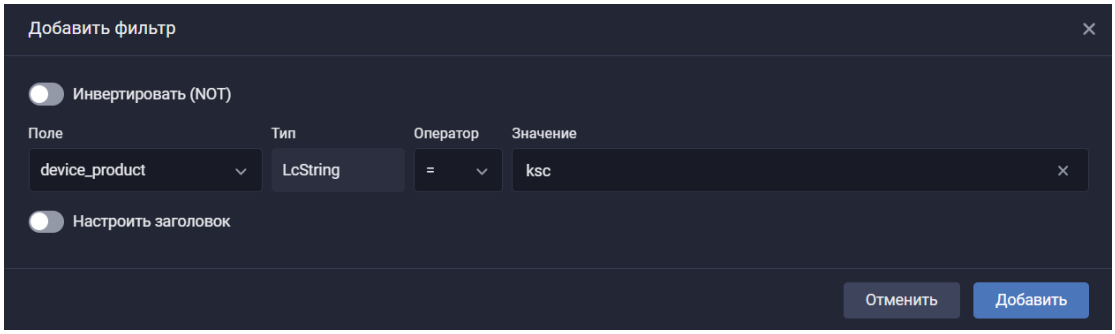
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события из MySQL.

Найти события Kaspersky Security Center в хранилище можно по следующему фильтру:

```
device_product = "ksc"
```



Kaspersky Security Center: сбор из СУБД PostgreSQL

Предварительные требования

- Сетевая доступность сервера СУБД Kaspersky Security Center по целевому порту и протоколу для каждой ноды кластера SIEM.
- Учетная запись в СУБД с правами на чтение таблицы **ev_event** (сбор событий из БД).

Настройка СУБД PostgreSQL

События Kaspersky Security Center записываются в таблицу `ev_event` базы данных KAV СУБД MS SQL. Для настройки сбора логов из базы данных необходимо к ней подключиться. Используйте для подключения специально созданную сервисную учетную запись (далее — УЗ).

Создание учетной записи в СУБД PostgreSQL

Чтобы создать сервисную УЗ, подключитесь к СУБД с правами администратора. Для этого выполните следующие действия на сервере с установленной СУБД:

1. Выполните следующую команду от имени пользователя postgres:

```
sudo -u postgres psql
```

2. Создайте сервисную учетную запись, выполнив следующие команды:

```
CREATE USER "kasper";
ALTER ROLE kasper WITH PASSWORD 'passw0rd';
```

3. Предоставьте сервисной учетной записи права на подключение к базе и чтение таблицы:

```
GRANT CONNECT ON DATABASE KAV to kasper;
GRANT SELECT ON ev_event TO kasper;
```

Настройка в R-Vision SIEM

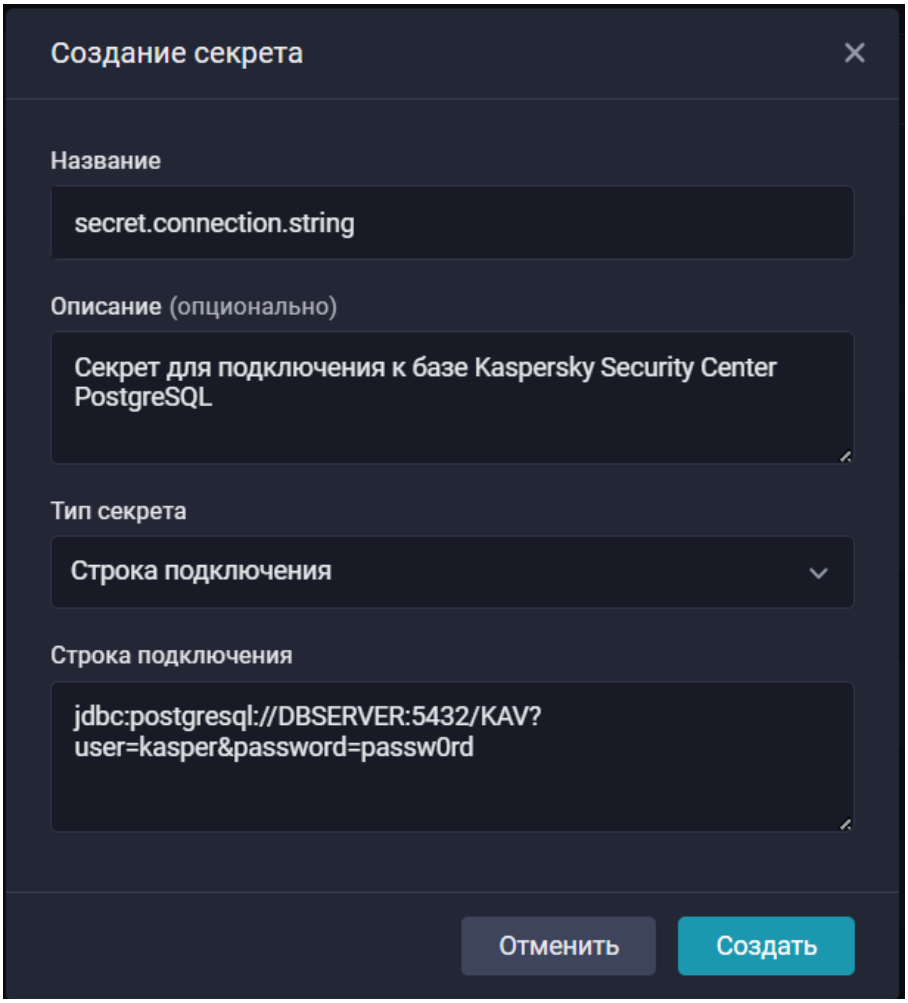
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте секрет со строкой подключения. Для этого:
   a. Перейдите в **Ресурсы** → **Секреты** → **Создать**.
   b. В раскрывшемся окне создания секрета заполните поля:
      - Название: введите название секрета.
      - Описание (опционально): опишите, для чего будет использоваться секрет.
      - Тип секрета: выберите вариант **Строка подключения**.
      - Строка подключения — введите строку вида:

        ```
        jdbc:postgresql://DBSERVER:5432/KAV?user=kasper&password=passw0rd
        ```

        Здесь:

        - `DBSERVER` — FQDN или IP-адрес сервера СУБД.
        - `5432` — порт подключения.



c. Нажмите на кнопку **Создать**.

2. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
3. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Database**.
   - Драйвер базы данных: выберите вариант MySQL.
   - Адрес подключения: выберите секрет, созданный ранее.
   - SQL-запрос — введите запрос вида:

```
SELECT 'ksc' AS appname,
    ev.event_id AS event_id,
    ev.event_type_id AS deviceEventClassId,
    ev.severity AS severity,
    ev.task_display_name AS taskDisplayName,
    ev.product_name AS product_name,
    ev.product_displ_version AS product_version,
    ev.event_type AS externalId,
    ev.event_type_display_name AS event_subcode,
    ev.descr AS msg,
    CASE
        WHEN ev.rise_time IS NOT NULL THEN ev.rise_time + INTERVAL '1 hour' *
```

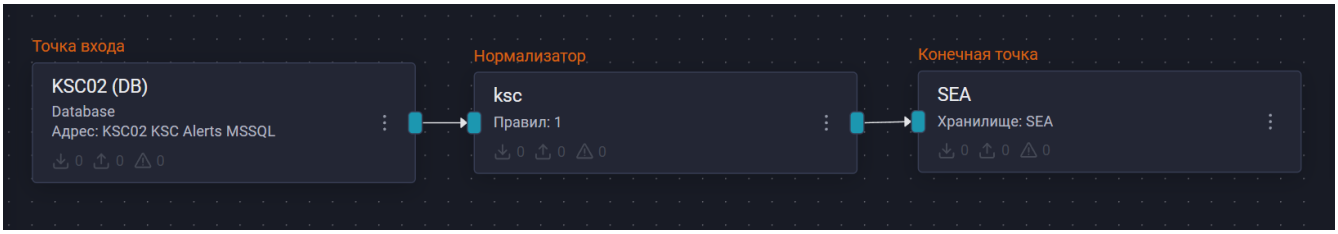
```
(EXTRACT(EPOCH FROM (NOW() AT TIME ZONE 'UTC' - NOW())) / 3600)
        ELSE ev.rise_time
    END AS endTime,
    CASE
        WHEN ev.registration_time IS NOT NULL THEN ev.registration_time +
INTERVAL '1 hour' * (EXTRACT(EPOCH FROM (NOW() AT TIME ZONE 'UTC' - NOW())) /
3600)
        ELSE ev.registration_time
    END AS kscRegistrationTime,
    CAST(ev.par7 AS VARCHAR(4000)) AS sourceUserName,
    hs."wstrWinName" AS dHost,
    hs."wstrWinDomain" AS strNtDom,
    serv."wstrWinName" AS kscName,
    CONCAT(
        (hs."nIp" >> 24) & 255, '.',
        (hs."nIp" >> 16) & 255, '.',
        (hs."nIp" >> 8) & 255, '.',
        hs."nIp" & 255
    ) AS sourceAddress,
    serv."wstrWinDomain" AS kscNtDomain,
    CONCAT(
        (serv."nIp" >> 24) & 255, '.',
        (serv."nIp" >> 16) & 255, '.',
        (serv."nIp" >> 8) & 255, '.',
        serv."nIp" & 255
    ) AS kscIP,
    CASE
        WHEN virus."tmVirusFoundTime" IS NOT NULL THEN virus."tmVirusFoundTime"
+ INTERVAL '1 hour' * (EXTRACT(EPOCH FROM (NOW() AT TIME ZONE 'UTC' - NOW())) /
3600)
        ELSE ev.registration_time
    END AS virusTime,
    virus."wstrObject" AS filePath,
    virus."wstrVirusName" AS virusName,
    virus.result_ev AS result
FROM ev_event AS ev
LEFT JOIN v_akpub_host AS hs ON ev."nHostId" = hs."nId"
INNER JOIN v_akpub_host AS serv ON serv."nId" = 1
LEFT JOIN rpt_viract_index AS virus ON ev.event_type_id = virus."nEventVirus"
WHERE ev.event_id > CAST(? AS BIGINT)
ORDER BY ev.event_id ASC LIMIT 10000;
```

- Поле идентификатора: введите ключ `event_id` со значением 1.
- Интервал запроса, секунд: введите значение 15.

4. Добавьте на конвейер элемент **Нормализатор** с правилом **Kaspersky Security Center - сбор из СУБД** (идентификатор правила: **RV-N-183**).
5. Соедините нормализатор с точкой входа.
6. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.

7. Соедините конечную точку с нормализатором.
8. Сохраните и установите конфигурацию конвейера.

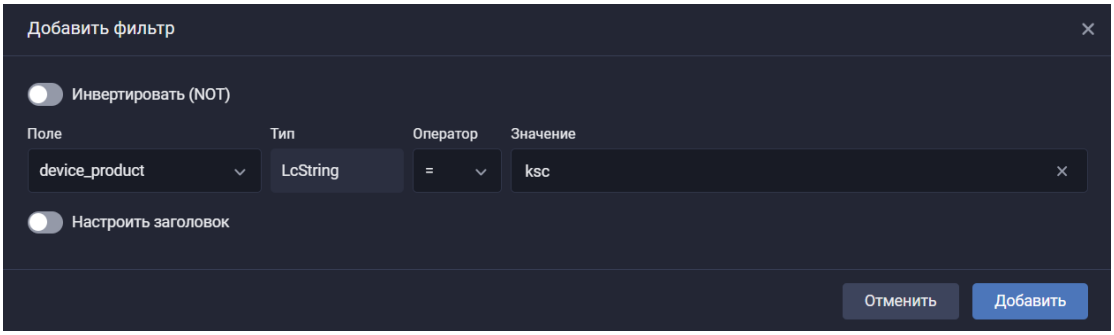
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события из PostgreSQL.

Найти события Kaspersky Security Center в хранилище можно по следующему фильтру:

```
device_product = "ksc"
```



Positive Technologies Sandbox

- Positive Technologies Sandbox: настройка источника

Positive Technologies Sandbox: настройка источника

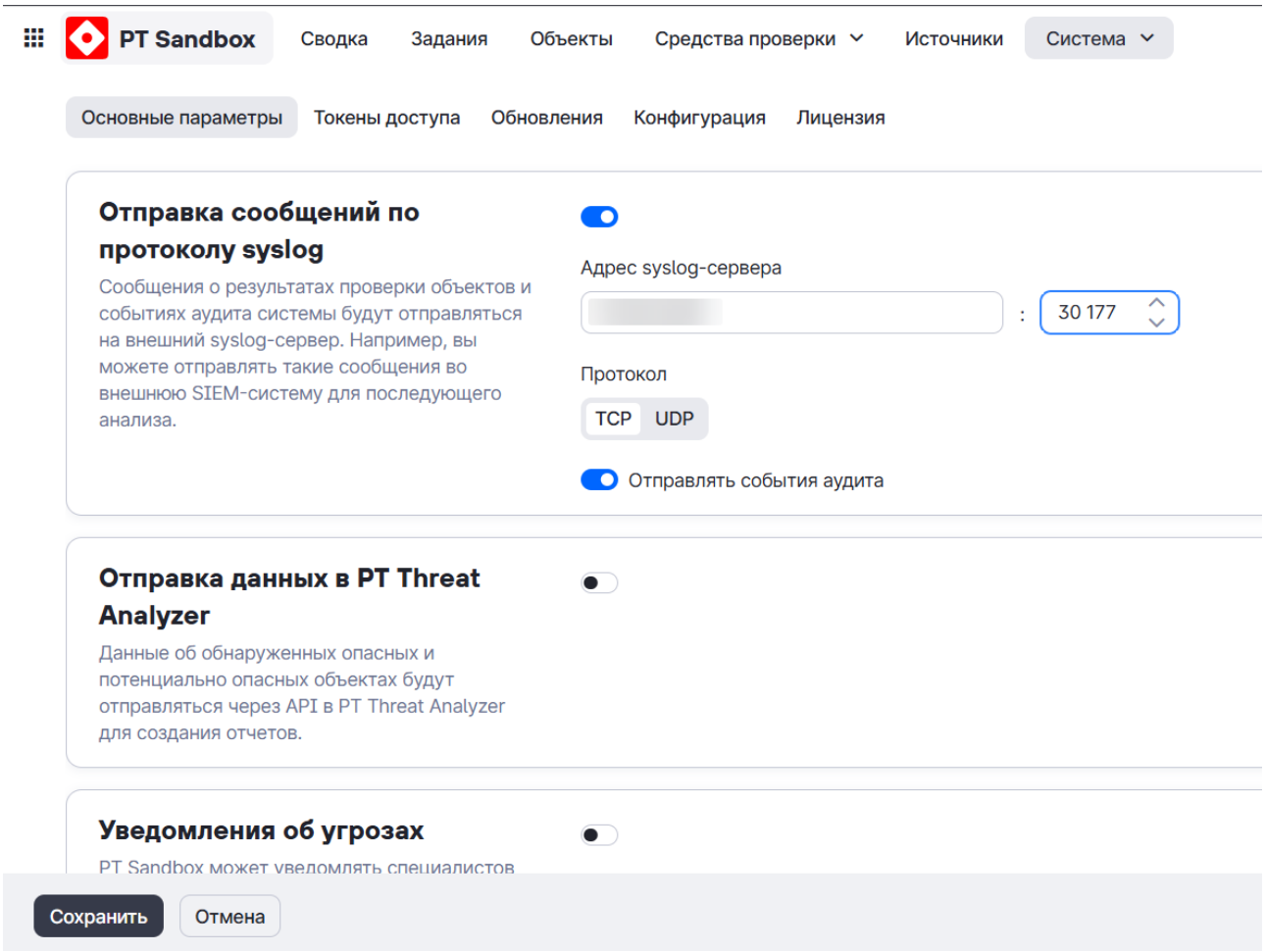
Данное руководство описывает процесс настройки сбора и отправки событий Positive Technologies Sandbox (PT Sandbox) в R-Vision SIEM.

Настройка Positive Technologies Sandbox

Для настройки отправки событий Positive Technologies Sandbox выполните следующие шаги:

1. В главном меню интерфейса Positive Technologies Sandbox перейдите в раздел **Система** → **Основные параметры**.
2. В группе параметров **Отправка сообщений по протоколу syslog** установите верхний переключатель в активное положение, чтобы включить отправку сообщений.
3. В поле **Адрес syslog-сервера** введите IP-адрес или полное доменное имя (FQDN) коллектора R-Vision SIEM.

4. Укажите значение порта в диапазоне 30000—32767 в соответствии с настройками на конвейере SIEM.
5. В поле **Протокол** выберите транспортный протокол **TCP**.
6. Установите переключатель **Отправлять события аудита** в активное положение.
7. Нажмите на кнопку **Сохранить**. Изменения будут применены в течение нескольких минут.



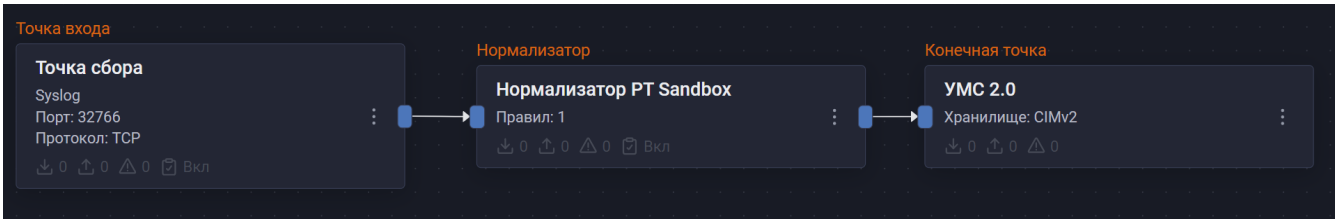
Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - **Название**: введите название точки входа.
   - **Тип точки входа**: выберите вариант **Syslog**.
   - **Порт точки входа**: введите значение в диапазоне 30000—32767.
   - **Протокол**: выберите вариант **TCP**.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Positive Technologies Sandbox** (идентификатор правила: **RV-N-288**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.

6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

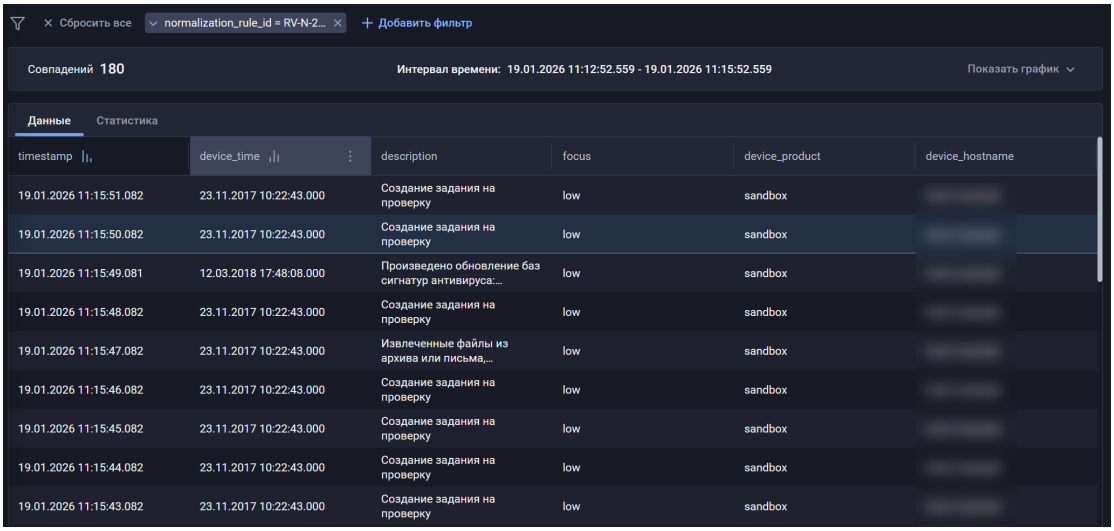


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события PT Sandbox.



Найти события Positive Technologies Sandbox в хранилище можно по следующему фильтру:

```
normalization_rule_id = "RV-N-288"
```



Бизнес-приложения

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых бизнес-приложений:

- Atlassian Confluence
- Atlassian Jira
- Jenkins
- Nextcloud
- 1С:Предприятие
- Битрикс24
- Пассворк

Atlassian Confluence

- Atlassian Confluence: настройка источника
- Atlassian Confluence: правила корреляции

Atlassian Confluence: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Atlassian Confluence в R-Vision SIEM.

Настройка Atlassian Confluence

Настройка логирования для Confluence 8

Для версии Confluence 8 необходимо дополнительно изменить режим логирования.

Убедитесь, что формат сообщения в журнале **atlassian-confluence.log** стандартный. Для этого:

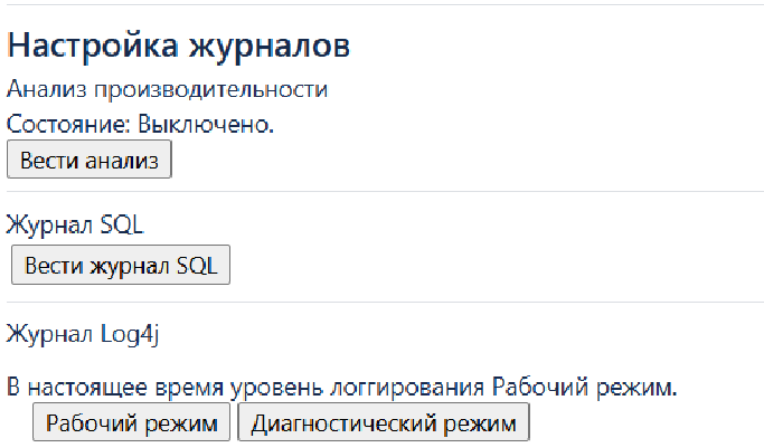
1. Откройте файл `/opt/atlassian/confluence/confluence/WEB-INF/classes/log4j.properties`.
2. Убедитесь, что в нем присутствует следующий параметр:

```
log4j.appender.confluencelog.layout.ConversionPattern=%d %p [%t] [%c{4}] %M
%enc{%m}{JSON}%n
```

Настройка сбора Audit для Confluence Data Center

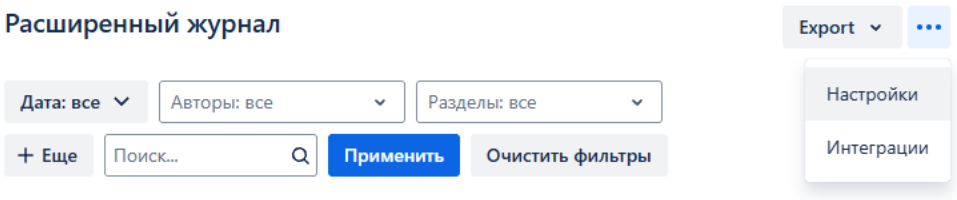
Для версии Confluence Data Center настройте сбор Audit. Для этого:

1. Войдите в веб-интерфейс от имени администратора системы.
2. Перейдите в меню **Основные настройки** → **Ведение журнала и профилирование**.
3. Выберите для журнала **Log4j** опцию **Рабочий режим**.

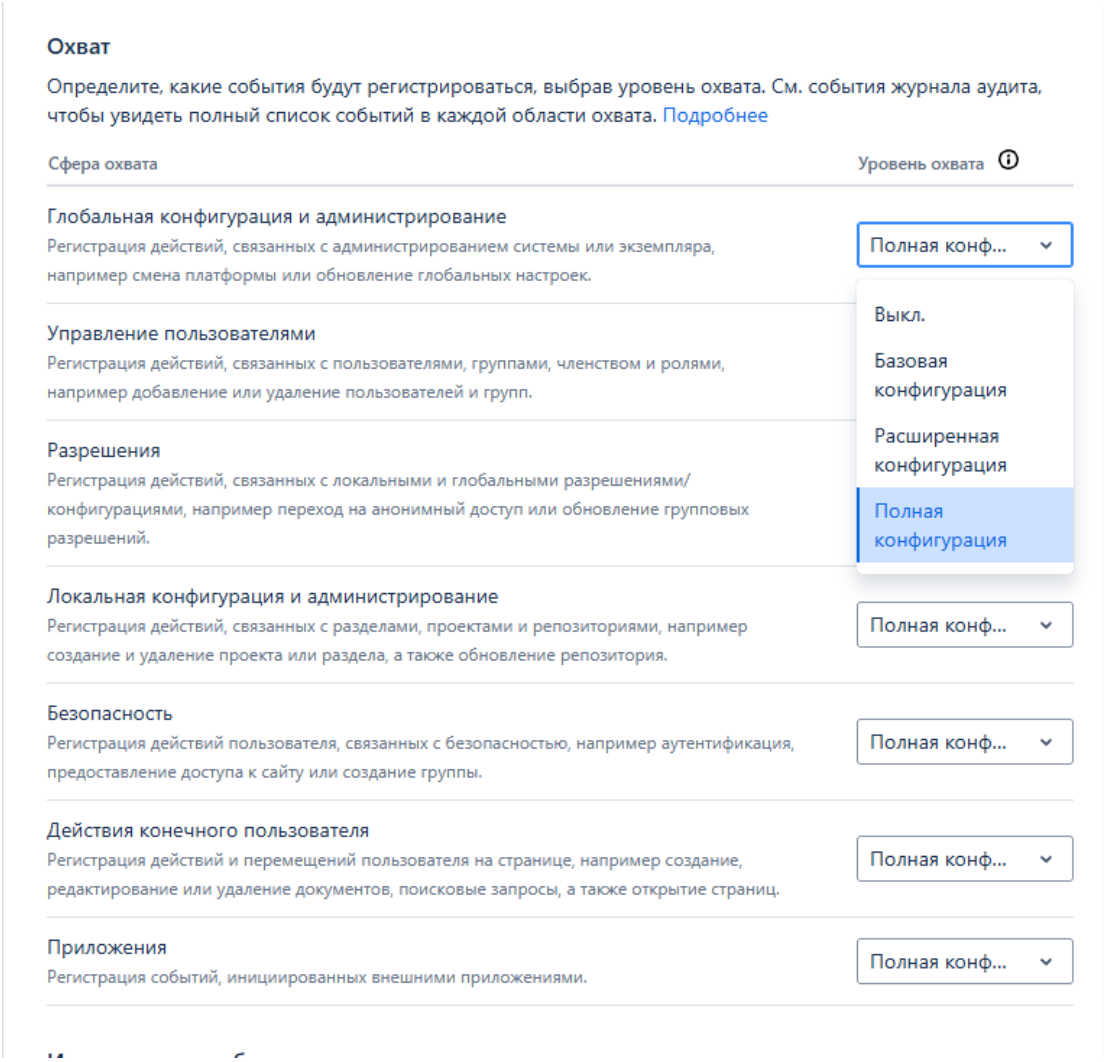


Включение рабочего режима начнет формировать лог-файлы по пути `/var/confluence/log/audit` в вашей ОС.

4. При необходимости измените уровни логирования для каждого типа событий.
5. Перейдите в раздел **Основные настройки** → **Расширенный журнал**.
6. Нажмите на кнопку ••• и выберите из выпадающего списка вариант **Настройки**.



7. Для необходимых параметров аудита установите уровень охвата **Полная конфигурация**.



8. Подключитесь к серверу Confluence по протоколу SSH от имени пользователя с правами root.
9. Откройте файл `server.xml` на редактирование. Путь к файлу по умолчанию: `/opt/confluence/conf/server.xml`.



Если Confluence установлен в нестандартную директорию, найти расположение файла можно с помощью команды:

```
find / -name "server.xml" 2>/dev/null | grep confluence
```

10. Отредактируйте файл конфигурации. Для этого:
    a. Откройте файл в текстовом редакторе.
    b. Найдите блок `AccessLogValve`. Конфигурация `AccessLogValue` по умолчанию представлена ниже:

```
<Valve className="org.apache.catalina.valves.AccessLogValve"
                       directory="logs"
                       maxDays="30"
                       pattern="%t %{X-AUSERNAME}o %I %h %r %s %Dms %b
%{Referer}i %{User-Agent}i"
                       prefix="conf_access_log"
```

```
                           requestAttributesEnabled="true"
                           rotatable="true"
                           suffix=".log"
               />
```

c. Замените значение параметра `pattern` на корректное значение: `%h %l %u %t "%r" %s %b "%{Referer}i" "%{User-Agent}i&quot`. Общий синтаксис должен принять следующий вид:

```
<Valve className="org.apache.catalina.valves.AccessLogValve"
                           directory="logs"
                           maxDays="30"
                           pattern='%h %l %u %t &amp;quot;%r&amp;quot; %s %b
&amp;quot;%{Referer}i&amp;quot; &amp;quot;%{User-Agent}i&amp;quot;'
                           prefix="conf_access_log"
                           requestAttributesEnabled="true"
                           rotatable="true"
                           suffix=".log"
                   />
```

d. Сохраните изменения и закройте редактор.

11. Примените изменения, перезапустив сервис. Способ может отличаться в зависимости от способа установки сервиса. Для установленного в систему сервиса используйте команду:

```
systemctl restart confluence
```

Настройка конфигурации rsyslog

1. Чтобы настроить передачу событий из файла, создайте файл `/etc/rsyslog.d/01-confluence.conf` со следующим содержимым:

```
module(load="imfile" mode="inotify")

input(
    type="imfile"
    File="/opt/confluence/logs/atlassian-confluence.log"
    Tag="Confluence_Log"
    Severity="info"
    Facility="local4"
)

input(
    type="imfile"
    File="/opt/confluence/logs/confluence_access.*.log"
    Tag="Confluence_Apache_Access"
    Severity="info"
    Facility="local4"
```

```
)
input(
    type="imfile"
    File="/var/confluence/log/audit_log.d/audit/*.log"
    Tag="confluence-audit"
    Ruleset = "confluence"
)

if $syslogtag == 'Confluence_Log' or $syslogtag == 'Confluence_Access' then {
        action(type="omfwd" Target="<target>" Port="<port>" Protocol="<protocol>")
        stop
}

ruleset(name="confluence") {
        action(type="omfwd" Target="<target>" Port="<port>" Protocol="<protocol>")
        stop
    )
```

Здесь:

- `<target>` — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- `<port>` — порт точки входа Syslog в конвейере SIEM.
- `<protocol>` — сетевой протокол: `tcp` или `udp`.

Использовались стандартные пути по умолчанию. Если путь был изменен, необходимо внести корректировки в конфигурационный файл



Конфигурационный файл `rsyslog` содержит стандартные системные пути. Однако администратор может переопределить их во время инсталляции ПО или при кастомизации конфигурации логгирования.

2. Перезапустите службу `rsyslog.service` с помощью команды:

```
systemctl restart rsyslog.service
```



Если используется Docker-версия Confluence, при запуске контейнера может потребоваться дополнительное монтирование раздела `/opt/atlassian/confluence` в файловую систему хоста.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.

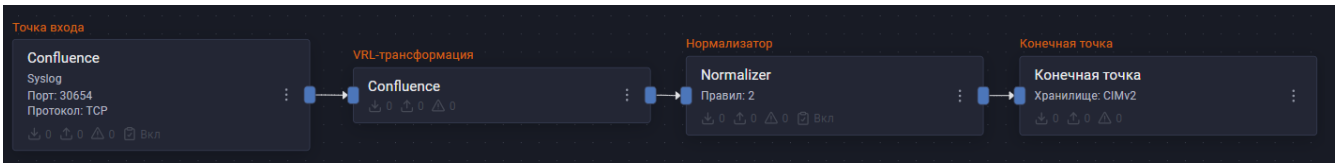
- Тип точки входа: выберите вариант **Syslog**.
- Порт точки входа: введите значение в соответствии с настройками на стороне Atlassian Confluence.
- Протокол: выберите вариант в соответствии с настройками на стороне Atlassian Confluence.

3. Добавьте VRL-трансформацию:

```
.device_event_id = "confluence"
```

4. Соедините добавленную точку входа и VRL-трансформацию.
5. Добавьте на конвейер элемент **Нормализатор** с правилами **Apache HTTP-server Access** (идентификатор правила: **RV-N-231**) и **Atlassian Confluence Audit** (идентификатор правила: **RV-N-237**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

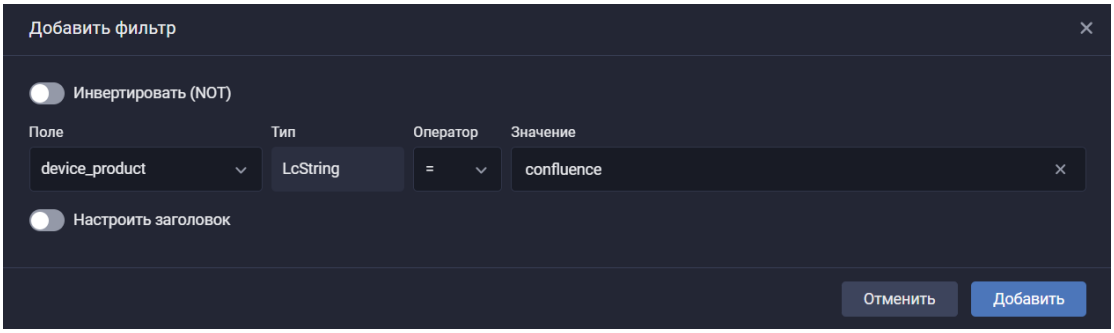
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Atlassian Confluence.

Найти события Atlassian Confluence в хранилище можно по следующему фильтру:

```
device_product = "confluence"
```



Atlassian Confluence: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1400	Выгрузка множества страниц Confluence	В Confluence существует функционал выгрузки отдельных страниц. Выгружать можно страницы в форматах PDF (конечная точка `pdfpageexport.action`) и Word (конечная точка `exportword`). В случае если осуществляется множественная выгрузка страниц, то данная активность может говорить об экспорте чувствительных данных с веб-сервера атакующими или нелегитимной работе внутренних сотрудников.	• Collection (TA0009) • Data from Information Repositories (T1213) • Confluence (T1213.001)
RV-D-1403	Выгрузка пространства Confluence	В Confluence существует функционал выгрузки целого пространства, которое может содержать множество страниц документов, фотографий и так далее. Выгружать пространства можно в форматах PDF (конечная точка `doflyingpdf.action`), HTML (конечная точка `doexportspace.action`) и XML (конечные точки `doexportspace.action` и `/rest/api/backup-restore/backup/space`). В случае если осуществляется выгрузка пространства, то данная активность может говорить об экспорте чувствительных данных с веб-сервера атакующими или нелегитимной работе внутренних сотрудников.	• Collection (TA0009) • Data from Information Repositories (T1213) • Confluence (T1213.001)
RV-D-1404	Множественные попытки входа на веб-сервер Confluence	Для входа в веб-сервер Confluence используются конечные точки `login.action` и `dologin.action`. Атакующие могут методом перебора постараться подобрать пароль к учетной записи.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1405	Эксплуатация уязвимости в Confluence - CVE-2023-22515	Уязвимость CVE-2023-22515 заключается в возможности перезапуска процесса настройки сервера, причем для этого даже не требуется аутентификация. Благодаря эксплуатации CVE-2023-22515 атакующий может получить возможность создания аккаунтов с правами администратора на уязвимом Confluence-сервере, а также иными привилегиями, доступными, если сервер находится в состоянии незавершенной установки.	• Execution (TA0002) • Exploitation for Privilege Escalation (T1068) • Exploit Public-Facing Application (T1190) • Exploitation for Client Execution (T1203)
RV-D-1406	Эксплуатация уязвимости в Confluence - CVE-2023-22527	Уязвимость Atlassian Confluence CVE-2023-22527 — это уязвимость инъекции OGNL (англ. Object-Graph Navigation Language), которая позволяет неавторизованным атакующим удаленно выполнять произвольные команды в уязвимом экземпляре Confluence. Эксплуатация уязвимости задействует файл шаблона Velocity с названием `text-inline.vm`.	• Execution (TA0002) • Exploitation for Privilege Escalation (T1068) • Exploit Public-Facing Application (T1190) • Exploitation for Client Execution (T1203)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1407	Выполнение OGNL инъекции через Java-выражения в Confluence	Данное правило детектирует потенциальное выполнение OGNL-инъекции через Java-выражения в Confluence. В случае наличия у определенной версии Confluence уязвимых компонентов, отвечающих за вычисления выражений OGNL из Java команд, возможно удаленное выполнение кода. Одним из примеров такой уязвимости является CVE-2022-26134. Уязвимость CVE-2022-26134 является OGNL-инъекцией, вследствие которой после подгрузки вредоносного Java-запроса в параметры HTTP-запроса (любого, в том числе несуществующего) производится неправильная обработка запроса OGNL и происходит удаленное выполнение кода.	• Execution (TA0002) • Exploitation for Client Execution (T1203)
RV-D-1408	Создание множества страниц Confluence	В Confluence существует функционал создания страниц. Атакующие, после аутентификации на веб-сервере Confluence могут использовать доступные им права для создания множества страниц. Это чревато такими последствиями, как перегрузка системы, заполнение хранилища, скрытие вредоносного контента и так далее.	• Impact (TA0040) • Defacement (T1491) • Internal Defacement (T1491.001) • External Defacement (T1491.002) • Data Manipulation (T1565) • Stored Data Manipulation (T1565.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1409	Отключение аудита журналов приложения Confluence	В Confluence существует функционал отключения модулей логирования непосредственно в веб-интерфейсе системы. При помощи данного функционала можно отключить основные логирующие компоненты `log4j`, отвечающие за логирование в Java-приложениях. Также в веб-интерфейсе можно отключить функционал ведения журнала SQL. Данная активность может затруднить расследование инцидента.	• Defense Evasion (TA0005) • Impair Defenses (T1562)
RV-D-1410	Эксплуатация уязвимости в Confluence - CVE-2023-22518	CVE-2023-22518 — это уязвимость неправильной авторизации в конечных точках setup-restore*.action для Atlassian Confluence Data Center и Server. Уязвимости подвержены все версии до 7.19.16, 8.3.4, 8.4.4, 8.5.3, 8.6.1. Атакующий может использовать эту уязвимость, отправляя запросы, содержащие необходимые параметры, к конечным точкам на экземпляре Confluence Data Center или Server. В результате атаки возможно полностью перезаписать содержимое атакуемого сервера Confluence на собственные данные, в том числе пересоздать учетную запись администратора, что может привести к потере контроля над сервером Confluence.	• Execution (TA0002) • Exploitation for Privilege Escalation (T1068) • Exploit Public-Facing Application (T1190) • Exploitation for Client Execution (T1203)

Atlassian Jira

- Atlassian Jira: настройка источника
- Atlassian Jira: правила корреляции

Atlassian Jira: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Atlassian Jira в R-Vision SIEM.

Настройка Atlassian Jira

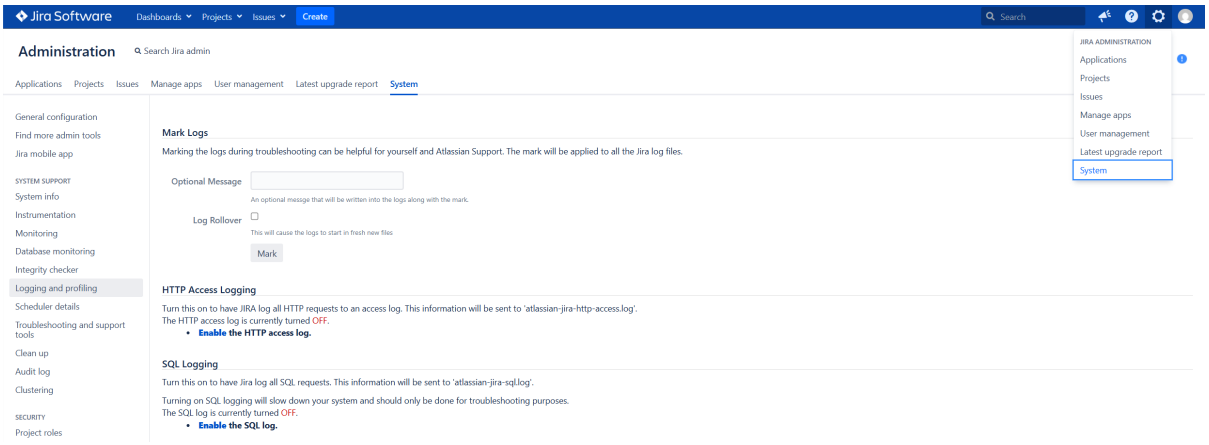
В инструкции рассматривается сбор событий из следующих журналов:

- **atlassian-jira-http-access.log** — журнал access web службы.
- **atlassian-jira.log** — общий лог, в который пишут логи отдельные службы.
- **audit/YYYYmmdd.00000.audit.log** — audit-журнал, доступный так же из сети по адресу `/plugins/servlet/audit`.

Настройка журналирования Atlassian Jira

Чтобы настроить журналирование Jira:

1. Включите логирование журнала access в настройках Jira:



2. Убедитесь, что формат сообщения в журнале **atlassian-jira.log** стандартный, для этого:
   a. Откройте файл `/opt/atlassian/jira/atlassian-jira/WEB-INF/classes/log4j2.xml`.
   b. Убедитесь, что в нем присутствует параметр:

```
log4j.appender.confluencelog.layout.ConversionPattern=%d %p [%t] [%c{4}] %M
%enc{%m}{JSON}%n
```

3. Настройте передачу событий из файла. Для этого создайте файл **/etc/rsyslog.d/02-jira.conf** со следующим содержимым:

```
module(load="imfile" mode="inotify")
input(
    type="imfile"
    File="/var/lib/docker/volumes/docker_jiraVar/_data/log/atlassian-jira.log"
    Tag="Jira_Log"
    Severity="info"
    Facility="local4"
)

input(
    type="imfile"
```

```
    File="/var/lib/docker/volumes/docker_jiraVar/_data/log/atlassian-jira-http-
access.log"
    Tag="Jira_Apache_Access"
    Severity="info"
    Facility="local4"
)


input(
    type="imfile"
    File="/var/lib/docker/volumes/docker_jiraVar/_data/log/audit/*.audit.log"
    Tag="Jira_Audit"
    Severity="info"
    Facility="local4"
)


if $syslogtag == 'Jira_Log' or $syslogtag == 'Jira_Apache_Access' or $syslogtag ==
'Jira_Audit' then {
  action(type="omfwd" Target="<target>" Port="<port>" Protocol="<protocol>")
  stop
}
```

Здесь:

- `<target>` — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- `<port>` — порт точки входа Syslog в конвейере SIEM.
- `<protocol>` — сетевой протокол: `tcp` или `udp`.

4. Перезапустите службу rsyslog.service с помощью команды:

```
systemctl restart rsyslog.service
```

5. Настройте нормализацию события журнала Apache Access, для этого:
   a. Откройте файл `/opt/atlassian/jira/conf/server.xml`.
   b. В файле **server.xml** найдите параметр className и измените его pattern на следующий:

```
%a %{jira.request.id}r %{jira.request.username}r %t &amp;quot;%m %U%q %H&amp;quot; %s %b
&amp;quot;%{Referer}i&amp;quot; &amp;quot;%{User-Agent}i&amp;quot;
```

Настройка в R-Vision SIEM

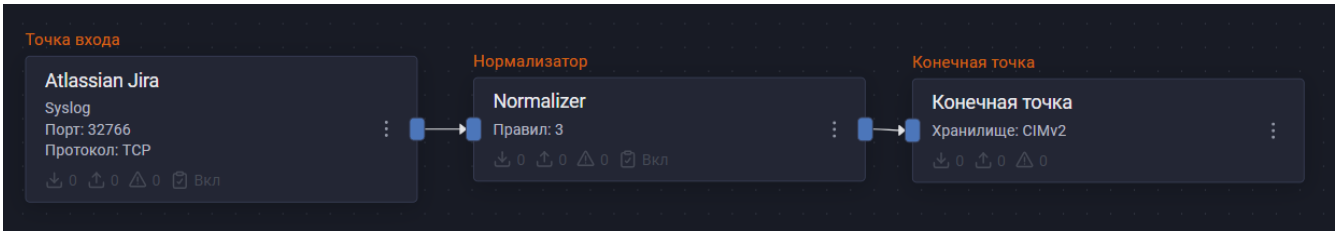
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. Перейдите в раздел **Ресурсы** → **Коллекторы** и создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:

- **Название**: введите произвольное, понятное название.
- **Тип точки входа**: выберите вариант **Syslog**.
- **Порт точки входа**: введите значение в соответствии с настройками на стороне Atlassian Jira.
- **Протокол**: выберите вариант в соответствии с настройками на стороне Atlassian Jira.

3. Добавьте на конвейер элемент **Нормализатор** с правилами **Atlassian Jira** (идентификаторы правил: **RV-N-238**, **RV-N-239**) и правилом **Apache HTTP-server Access** (идентификатор правила: **RV-N-231**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

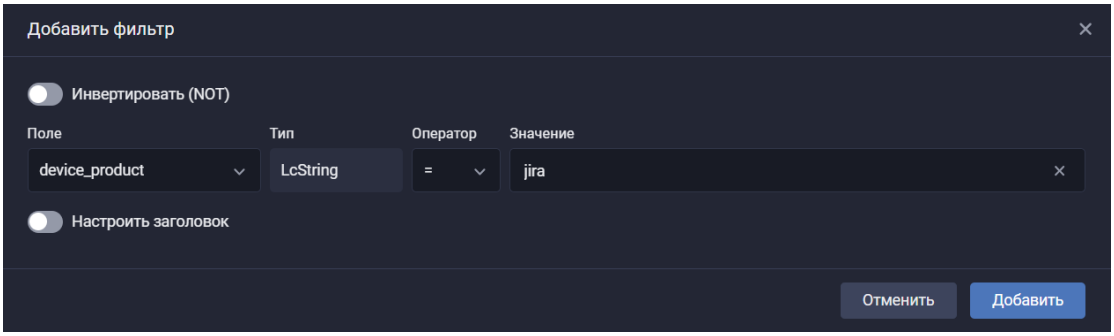
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Atlassian Jira.

Найти события Atlassian Jira в хранилище можно по следующему фильтру:

```
device_product = "jira"
```



Atlassian Jira: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1193	Создание множества задач пользователем в Jira	Массовое создание задач в Jira может указывать на попытку намеренно перегрузить систему (DoS) либо замаскировать иную подозрительную активность. Подобные действия способны негативно сказаться на рабочих процессах, привести к повышенной нагрузке на ресурсы и усложнить контроль за актуальными задачами. Следует учитывать, что автоматизированное или неконтролируемое добавление задач нередко применяется как способ отвлечения внимания, что затрудняет своевременное выявление действительно значимых инцидентов. Кроме того, такие действия могут использоваться для усложнения анализа происходящего и искусственного формирования ложных приоритетов в области информационной безопасности.	• Impact (TA0040) • Endpoint Denial of Service (T1499) • Application Exhaustion Flood (T1499.003) • Data Manipulation (T1565) • Stored Data Manipulation (T1565.001)
RV-D-1194	Удаление множества задач пользователем в Jira	Удаление множества задач в Jira за короткий промежуток времени может быть признаком потенциально вредоносной активности, связанной с попыткой атакующего скрыть следы предыдущей деятельности или манипулировать рабочими процессами. Такое поведение может привести к утрате важной информации и нарушению планов работы в управлении проектами. Это также может затруднить расследование инцидентов безопасности, так как удаленные задачи могут содержать критические данные о прогрессе проекта или уязвимостях. Массовое удаление задач может также сигнализировать о сбоях в интеграции или ошибочной автоматизации.	• Impact (TA0040) • Data Destruction (T1485) • Data Manipulation (T1565) • Stored Data Manipulation (T1565.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1195	Множество неудачных попыток входа в Jira	Множество неудачных попыток входа может указывать на попытку подбора пароля или осуществление bruteforce-атаки, направленной на кражу учетных записей. Такое поведение свидетельствует о возможном вмешательстве атакующего, который пытается получить несанкционированный доступ к системе Jira. В случае успешного доступа это может привести к утечке конфиденциальной информации, изменению настроек системы, удалению или изменению задач, а также к другим действиям, нарушающим работу системы. Постоянные неудачные попытки входа также могут перегрузить систему или привести к временной блокировке учетных записей.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)
RV-D-1196	Создание пользователя в Jira	Правило направлено на обнаружение активности, связанной с добавлением новых учетных записей в систему. Такое поведение может быть признаком попытки атакующего создать привилегированные учетные записи для дальнейшей работы под ними, чтобы не привлекать внимание. При успешном добавлении новых пользователей с повышенными привилегиями атакующий может получить доступ к конфиденциальной информации, изменять данные, выполнять команды или скрывать свои действия в системе. Это может привести к утечке данных и нарушению работоспособности сервисов.	• Persistence (TA0003) • Account Manipulation (T1098) • Create Account (T1136) • Local Account (T1136.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1197	Изменение конфигурации журналов логирования в Jira	Изменение конфигурации журналов логирования в Jira может быть признаком попытки атакующего скрыть следы своей деятельности или снизить видимость критических событий в системе. Изменение параметров логирования, особенно отключение журналов, приводит к потере возможности отслеживать важные действия, такие как попытки входа, изменения задач и конфигурации системы. Это затрудняет расследование инцидентов безопасности, так как отсутствие логов делает невозможным восстановление полной картины событий. Без надлежащего логирования можно пропустить аномалии и подозрительные действия, что повышает риск незамеченных атак.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)
RV-D-1224	Дамп множества задач в Jira	Дамп множества задач одним пользователем за короткий промежуток времени в Jira может быть признаком подозрительной активности, связанной с потенциальной утечкой данных. Экспорт информации сразу из нескольких проектов может использоваться атакующим для получения конфиденциальных данных о разработке, планировании, уязвимостях или внутренней структуре компании. Это может привести к утечке коммерческой тайны, раскрытию стратегий и нарушению безопасности проекта. Массовый дамп проектов может осуществляться сотрудником перед увольнением или для продажи данных конкурентам.	• Collection (TA0009) • Impact (TA0040) • Data from Information Repositories (T1213) • Confluence (T1213.001) • Data Manipulation (T1565) • Stored Data Manipulation (T1565.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1228	Эксплуатация уязвимости в Jira — CVE-2023-26256	Данное правило направлено на обнаружение эксплуатации уязвимости CVE-2023-26256 типа Directory Traversal и Local File Inclusion (LFI) в плагине Stagil Navigation для Atlassian Jira. Уязвимость позволяет атакующим считывать произвольные файлы на сервере через специально сформированные HTTP-запросы, что позволяет обойти ограничения доступа и получить доступ к важным файлам системы. Эксплуатация возможна в версиях плагина ниже 2.0.52. Правило срабатывает при обнаружении запросов, содержащих попытку доступа к файлам. Успешная эксплуатация может привести к утечке конфиденциальной информации или компрометации системы. В случае срабатывания правила необходимо получить разъяснения о причине данной активности от ответственного за учетную запись лица. В случае отсутствия обратной связи — заблокировать учетную запись сотрудника, заблокировать узел, с которого произошел запрос, и провести внутреннее расследование.	• Initial Access (TA0001) • Defense Evasion (TA0005) • Credential Access (TA0006) • Discovery (TA0007) • Collection (TA0009) • File and Directory Discovery (T1083) • Exploit Public-Facing Application (T1190) • Exploitation for Defense Evasion (T1211) • Exploitation for Credential Access (T1212) • Data from Information Repositories (T1213) • Confluence (T1213.001) • Unsecured Credentials (T1552) • Chat Messages (T1552.008)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1271	Добавление пользователя в критичные группы	Добавление учетной записи в группу с особыми привилегиями, доступ к которой ограничен, может представлять серьезную угрозу безопасности. Критичные группы обычно обладают расширенными правами на доступ к конфиденциальным данным, изменение конфигураций системы или управление ресурсами. Несанкционированное добавление в такую группу может свидетельствовать о компрометации учетной записи или внутренней угрозе. Атакующий может нарушить работу системы или изменить настройки безопасности.	• Persistence (TA0003) • Account Manipulation (T1098) • Additional Local or Domain Groups (T1098.007)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1310	Создание резервной копии Jira	Создание резервной копии Jira без предварительного согласования может быть опасным событием. Резервные копии содержат полный набор данных системы, включая конфиденциальную информацию: проекты, задачи, пользовательские данные, конфигурации и настройки безопасности. В случае несанкционированного создания резервной копии атакующий может получить доступ к данным, которые затем могут быть украдены, использованы для взлома системы или скомпрометированы. Кроме того, если резервная копия перемещена на внешнее устройство, это создает дополнительный риск утечки данных. Частое или несвоевременное создание резервных копий также может перегружать систему и создавать дополнительные риски для производительности, так как процесс резервного копирования использует ресурсы системы. Если резервные копии создаются без ведома администратора или в необычное время, это может свидетельствовать о потенциальной угрозе или нарушении безопасности. В случае срабатывания правила необходимо получить подтверждение легитимности активности от ответственного за учетную запись лица. В случае отсутствия подтверждения легитимности — заблокировать учетную запись сотрудника, провести внутреннее расследование.	• Collection (TA0009) • Impact (TA0040) • Data from Information Repositories (T1213) • Confluence (T1213.001) • Data Manipulation (T1565) • Stored Data Manipulation (T1565.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1327	Экспорт множества задач в Jira	Экспорт множества задач в Jira может быть признаком потенциальной утечки данных. Атакующий, имея доступ к системе, может экспортировать чувствительную информацию о задачах, проектных планах, уязвимостях, логах и других важных данных. Это может привести к утечке конфиденциальной информации, компрометации коммерческой тайны или раскрытию данных о внутренней инфраструктуре компании. Экспорт большого количества задач может также использоваться как подготовительный этап для последующих атак или злоупотребления данными. В случае срабатывания правила необходимо получить подтверждение легитимности активности от лица, ответственного за учетную запись. В случае отсутствия подтверждения легитимности — заблокировать учетную запись сотрудника, провести внутреннее расследование.	• Collection (TA0009) • Impact (TA0040) • Data from Information Repositories (T1213) • Confluence (T1213.001) • Data Manipulation (T1565) • Stored Data Manipulation (T1565.001)
RV-D-1537	Доступ к привилегированному режиму после авторизации	Правило обнаруживает вход в привилегированный режим на устройстве Cisco ASA после авторизации по SSH.	• Privilege Escalation (TA0004) • Valid Accounts (T1078) • Local Accounts (T1078.003)

Jenkins

- Jenkins: настройка источника

Jenkins: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Jenkins в R-Vision SIEM.

Предварительные требования

Перед настройкой пересылки событий в R-Vision SIEM убедитесь в выполнении следующих условий:

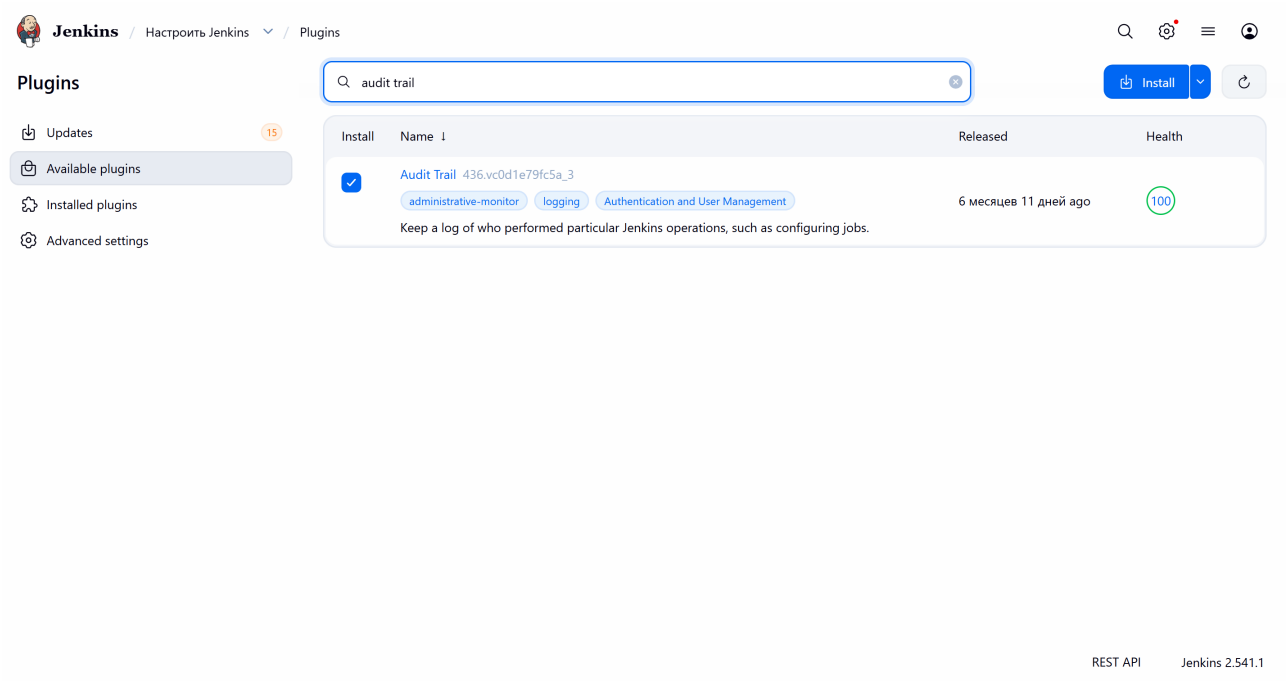
- Настройка производится УЗ с правами администратора.
- Сетевая связность между сервером Jenkins и SIEM (или промежуточным syslog-сервером) обеспечена, а необходимые порты открыты.

Настройка Jenkins

Настройка плагина аудита

Для установки плагина аудита Jenkins выполните следующее:

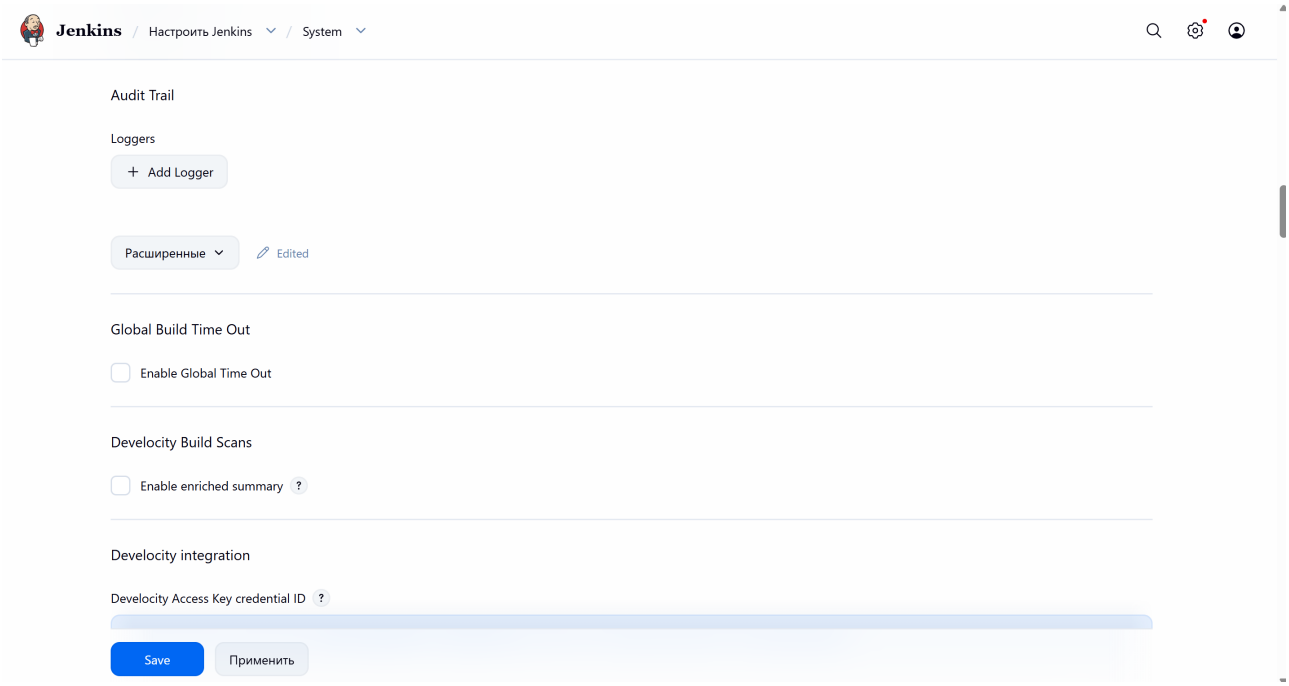
1. Войдите в веб-интерфейс **Jenkins**.
2. Перейдите в раздел **Настроить Jenkins**.
3. Выберите вариант **Plugins**.
4. Перейдите на вкладку **Available plugins**.
5. Найдите плагин **Audit Trail**.
6. Нажмите на кнопку **Install**.



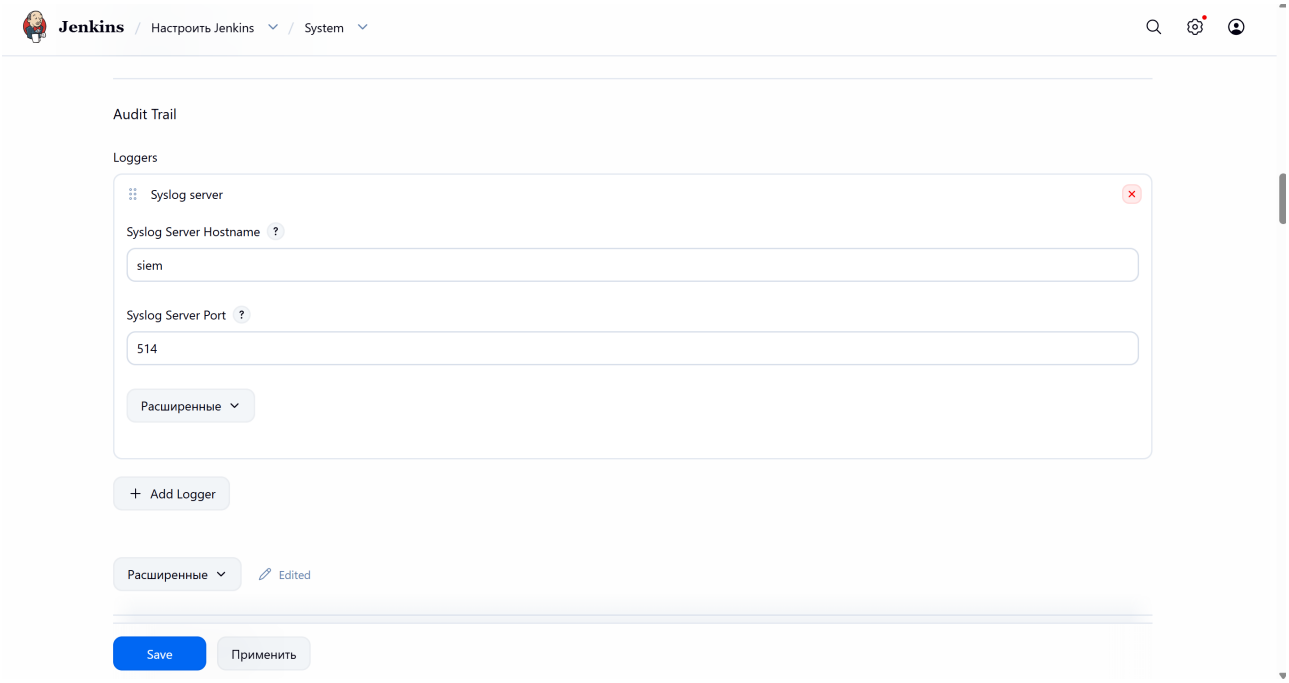
Для настройки плагина **Audit Trail** выполните следующее:

1. Перейдите в раздел **Настроить Jenkins**.
2. Выберите вариант **System**.

3. В подразделе **Audit Trail** нажмите на кнопку **Add Logger** (+) и добавьте logger типа `Syslog`.



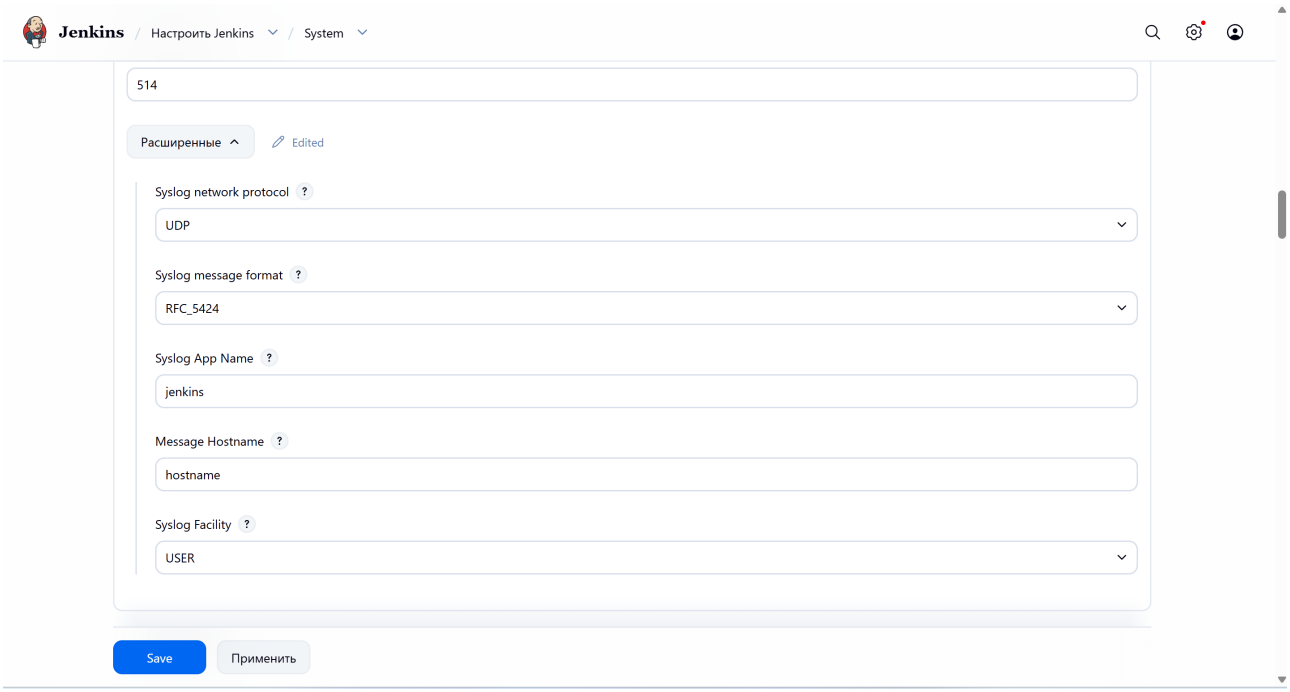
4. Заполните параметры в соответствии с изображением ниже:



Здесь:

- **Syslog Server Hostname** — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- **Syslog Server Port** — порт точки входа Syslog на конвейере SIEM.

5. В подразделе **Loggers** нажмите на кнопку **Расширенные** (⌄).
6. Заполните параметры в соответствии с изображением ниже:

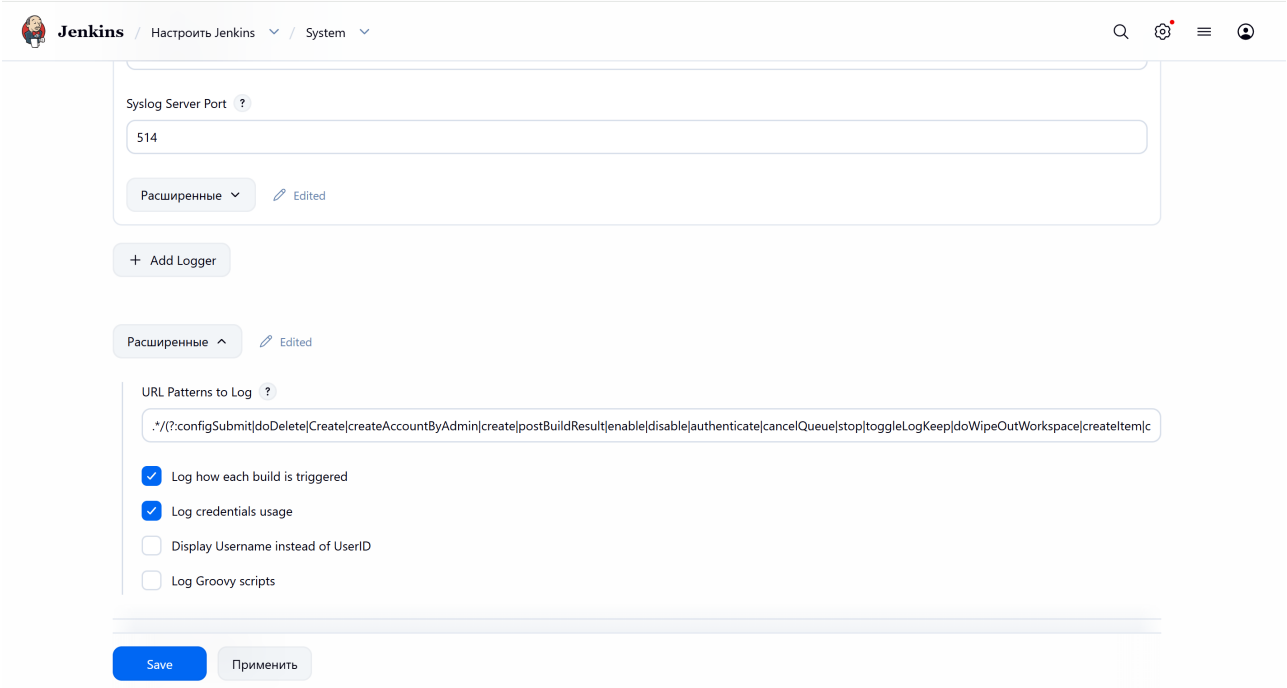


Здесь:

- **Syslog network protocol** — выберите сетевой протокол: `TCP` или `UDP`.
- **Syslog message format** — выберите вариант `RFC_5424`.
- **Syslog App Name** — введите значение `jenkins`.
- **Message Hostname** — укажите hostname узла, на котором развернут Jenkins.

7. В подразделе **Audit Trail** нажмите на кнопку **Расширенные** (⌄).
8. Измените значение параметра **URL Patterns to Log** на следующее:

```
.*/(?:configSubmit|doDelete|Create|createAccountByAdmin|create|postBuildResult|enable|disable|authenticate|cancelQueue|stop|toggleLogKeep|doWipeOutWorkspace|createItem|createView|toggleOffline|cancelQuietDown|quietDown|restart|exit|safeExit|login|logout)/?.*
```



9. Нажмите на кнопку **Save**.

Настройка логирования событий авторизации

Настройка логирования событий авторизации отличается в зависимости от способа запуска Jenkins.

Вариант 1. Jenkins развернут через Docker

Чтобы настроить логирование событий авторизации, выполните следующие шаги:

1. Чтобы логи безопасности с именами пользователей попадали в stdout (и далее в Docker logs), создайте Groovy-скрипт в папке `/var/jenkins_home/init.groovy.d/log-security.groovy`:

```
import java.util.logging.*
import groovy.json.JsonOutput

class FinalJsonFormatter extends Formatter {
    private static final String HOSTNAME =
java.net.InetAddress.getLocalHost().getHostName()

    @Override
    String format(LogRecord record) {
        try {
            def msg = formatMessage(record)
            def logEntry = [
                "timestamp": new java.text.SimpleDateFormat("yyyy-MM-
dd'T'HH:mm:ss.SSSZ").format(new Date(record.millis)),
                "hostname" : HOSTNAME.toString(),
                "level"    : record.level.toString(),
                "logger"   : record.loggerName.toString(),
                "message"  : msg ? msg.toString() : "empty",
                "user"     : (record.parameters?.find { it instanceof String } ?:
"system").toString()
```

```
            ]
            return JsonOutput.toJson(logEntry) + "\n"
        } catch (Exception e) {
            return "{\"error\": \"failed to format log\", \"reason\":
\"${e.message}\"}\n"
        }
    }
}

def handler = new ConsoleHandler()
handler.setFormatter(new FinalJsonFormatter())
handler.setLevel(Level.FINE)

// Настройка логгера только для событий входа и выхода.
[
    "jenkins.security.SecurityListener"
].each { name ->
    def l = Logger.getLogger(name)
    // Очистите старые хендлеры, чтобы избежать дублирования.
    l.getHandlers().each { l.removeHandler(it) }
    l.addHandler(handler)
    l.setLevel(Level.FINE)
    l.setUseParentHandlers(false)
}

println "--- Jenkins Auth Audit (JSON) Re-Applied ---"
```

2. Измените файл `docker-compose.yml` следующим образом:

```
services:
  jenkins: --- Добавлять в этот блок.
    ...
    hostname: "${HOSTNAME:-my-jenkins-server}"
    image: jenkins/jenkins:lts
    logging:
      driver: syslog
      options:
        syslog-address: "protocol://siem:port" ---- Поменять на свои значения.
        tag: "jenkins-master"
    ...
```

3. Перезапустите контейнер.

Вариант 2. Jenkins развернут локально

Чтобы настроить логирование событий авторизации, выполните следующие шаги:

1. В стандартной установке на Linux (Debian, Ubuntu, RHEL) домашняя директория Jenkins находится по адресу `/var/lib/jenkins`. Создайте папку по указанному адресу:

```
sudo mkdir -p /var/lib/jenkins/init.groovy.d
```

2. Создайте файл `/var/lib/jenkins/init.groovy.d/full-audit.groovy` и добавьте в него JSON-скрипт:

```
import java.util.logging.*
import groovy.json.JsonOutput

class FinalJsonFormatter extends Formatter {
    private static final String HOSTNAME =
java.net.InetAddress.getLocalHost().getHostName()

    @Override
    String format(LogRecord record) {
        try {
            def msg = formatMessage(record)
            def logEntry = [
                "timestamp": new java.text.SimpleDateFormat("yyyy-MM-
dd'T'HH:mm:ss.SSSZ").format(new Date(record.millis)),
                "hostname" : HOSTNAME.toString(),
                "level"    : record.level.toString(),
                "logger"   : record.loggerName.toString(),
                "message"  : msg ? msg.toString() : "empty",
                "user"     : (record.parameters?.find { it instanceof String } ?:
"system").toString()
            ]
            return JsonOutput.toJson(logEntry) + "\n"
        } catch (Exception e) {
            return "{\"error\": \"failed to format log\", \"reason\":
\"${e.message}\"}\n"
        }
    }
}

def handler = new ConsoleHandler()
handler.setFormatter(new FinalJsonFormatter())
handler.setLevel(Level.FINE)

// Настройка логгера только для событий входа и выхода.
[
    "jenkins.security.SecurityListener"
].each { name ->
    def l = Logger.getLogger(name)
    // Очистите старые хендлеры, чтобы избежать дублирования.
    l.getHandlers().each { l.removeHandler(it) }
    l.addHandler(handler)
    l.setLevel(Level.FINE)
    l.setUseParentHandlers(false)
}
```

```
println "--- Jenkins Auth Audit (JSON) Re-Applied ---"
```

3. Jenkins должен иметь возможность прочитать этот файл. Убедитесь, что владельцем является пользователь Jenkins:

```
sudo chown -R jenkins:jenkins /var/lib/jenkins/init.groovy.d/
sudo chmod 755 /var/lib/jenkins/init.groovy.d/
```

4. Чтобы rsyslog не отправлял в SIEM ненужные файлы, используйте фильтрацию по вашему формату. Для этого создайте файл `/etc/rsyslog.d/10-siem.conf`:

```
# Фильтрация логов: только от сервиса Jenkins и только указанный JSON.
if ($programname == 'jenkins') and ($msg contains '{"timestamp":') and ($msg
contains 'jenkins.security.SecurityListener') then {
    # Отправка в SIEM по TCP (замените IP и порт на свои).
    action(type="omfwd"
           target="<target>"
           port="<port>"
           protocol="<protocol>"
        )

    # Остановите дальнейшую обработку этой строки, чтобы она не дублировалась в
/var/log/syslog.
    stop
}
```

   Здесь:

   - `<target>` — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
   - `<port>` — порт точки входа Syslog на конвейере SIEM.
   - `<protocol>` — сетевой протокол: `tcp` или `udp`.

5. Перезапустите службу `rsyslog.service` с помощью команды:

```
systemctl restart rsyslog.service
```

Настройка в R-Vision SIEM

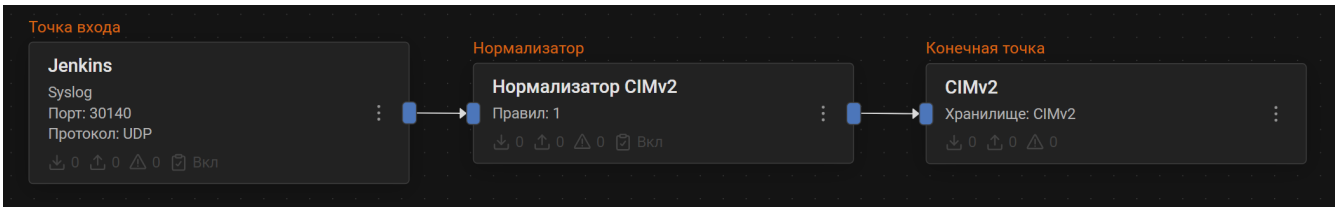
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.

- Тип точки входа: выберите вариант **Syslog**.
- Порт точки входа: введите значение в соответствии с настройками на стороне Jenkins.
- Протокол: выберите вариант в соответствии с настройками на стороне Jenkins.

3. Добавьте на конвейер элемент **Нормализатор** с правилом **Jenkins** (идентификатор правила: **RV-N-305**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

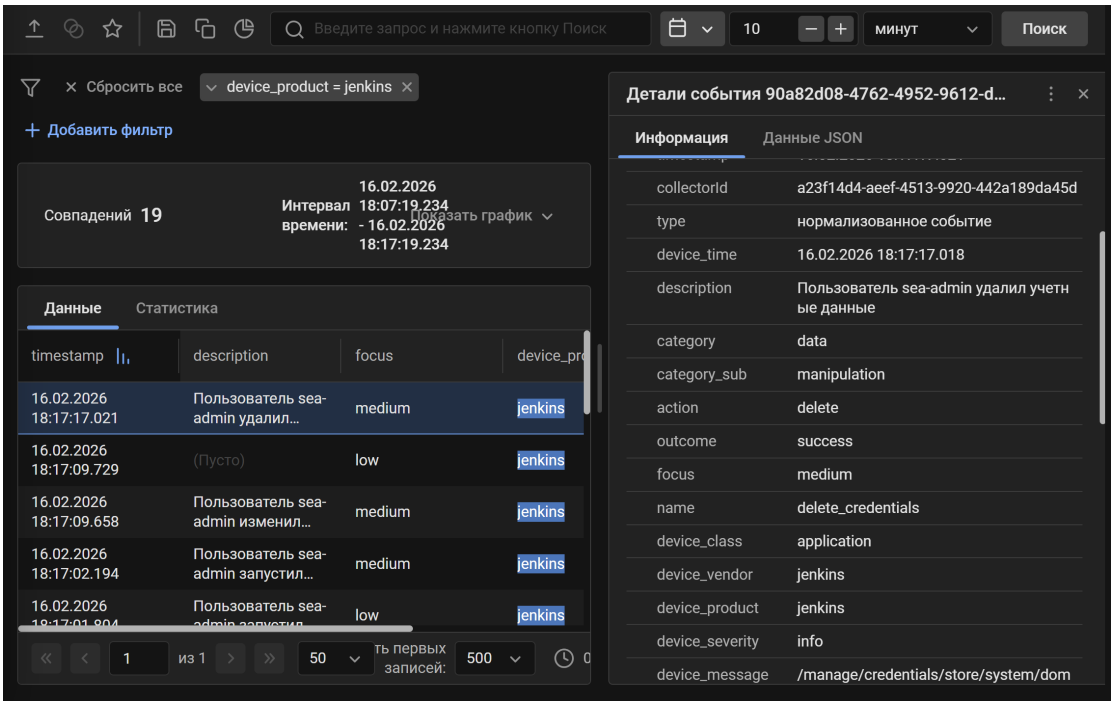
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Jenkins.

Найти события Jenkins в хранилище можно по следующему фильтру:

```
device_product = "jenkins"
```



Nextcloud

- Nextcloud: настройка источника

Nextcloud: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Nextcloud в R-Vision SIEM.

Предварительные требования

- Сетевая связность между сервером Nextcloud и SIEM (или промежуточным syslog-сервером) обеспечена, а необходимые порты открыты.
- Создана учетная запись с правами администратора для изменения конфигурации Nextcloud и rsyslog.

Настройка Nextcloud

Вариант 1. Nextcloud, развернутый через Docker

Для настройки аудита Nextcloud выполните следующие шаги:

1. Отредактируйте конфигурационный файл `var/www/config/config.php` внутри контейнера или на хосте (должен быть подключен volume):

```
'log_type' => 'file',
'logfile' => '/var/www/html/data/nextcloud.log',
'loglevel' => 1,
"log_type_audit" => "file",
"syslog_tag_audit" => "",
"logfile_audit" => "/var/www/html/data/nextcloud.log"
```

2. После изменений перезапустите контейнер:

```
sudo docker restart nextcloud
```

3. Пробросьте каталог `data` или файл `nextcloud.log` на хост:

```
volumes:
    - /opt/nextcloud/logs/nextcloud.log:/var/www/html/data/nextcloud.log
```

Вариант 2. Nextcloud, установленный через Snap

Для настройки аудита Nextcloud выполните следующие шаги:

1. Отредактируйте конфигурационный файл `var/snap/nextcloud/config/config.php`:

```
'log_type' => 'syslog',
'logfile' => '',
'loglevel' => 1,
'syslog_tag' => 'nextcloud',
"log_type_audit" => "syslog",
"syslog_tag_audit" => "nextcloud",
"logfile_audit" => ""
```

2. Перезапустите snap-сервис:

```
sudo snap restart nextcloud
```

Вариант 3. Обычная установка

Для настройки аудита Nextcloud выполните следующие шаги:

1. Отредактируйте конфигурационный файл `var/www/config/config.php`:

```
'log_type' => 'syslog',
'logfile' => '',
'loglevel' => 1,
'syslog_tag' => 'nextcloud',
"log_type_audit" => "syslog",
"syslog_tag_audit" => "nextcloud",
"logfile_audit" => ""
```

2. Перезапустите сервис, через который работает Nextcloud:

```
systemctl restart apache2
```

Настройка службы rsyslog

Чтобы настроить службу rsyslog, выполните следующие действия:

1. Создайте файл конфигурации rsyslog:

```
sudo nano /etc/rsyslog.d/10-siem.conf
```

2. Добавьте в созданный файл одно из следующих правил:

▼ *Конфигурация rsyslog. Обычная установка. Snap.*

```
if $programname == 'nextcloud' or $syslogtag == 'nextcloud' then {
    action(
        type="omfwd"
        target="siem"
```

```
        port="port"
        protocol="protocol"
    )
    stop
}
```

Здесь:

- `<target>` — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- `<port>` — порт точки входа Syslog на конвейере SIEM.
- `<protocol>` — сетевой протокол: `tcp` или `udp`.

▼ *Конфигурация rsyslog. Docker-установка.*

```
input(type="imfile"
      File="<path/to/logs>/nextcloud.log"
      Tag="nextcloud"
      PersistStateInterval="200")

if $programname == 'nextcloud' or $syslogtag == 'nextcloud' then {
    action(
        type="omfwd"
        target="siem"
        port="port"
        protocol="protocol"
    )
    stop
}
```

Здесь:

- `<target>` — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- `<port>` — порт точки входа Syslog на конвейере SIEM.
- `<protocol>` — сетевой протокол: `tcp` или `udp`.

3. Перезапустите rsyslog для применения изменений:

```
sudo systemctl restart rsyslog
```

Настройка в R-Vision SIEM

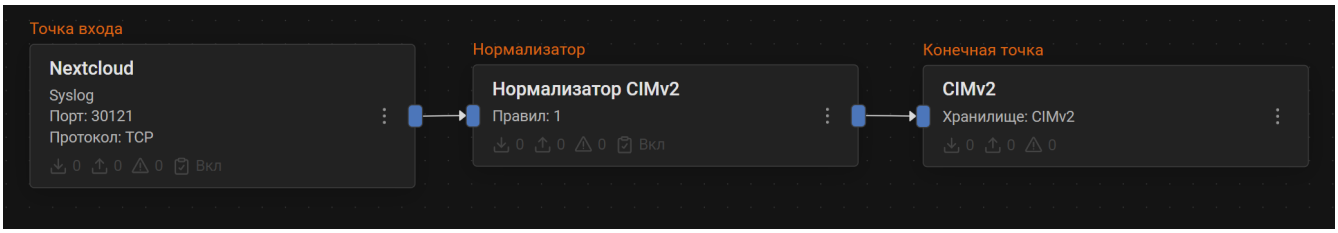
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.

- Тип точки входа: выберите вариант **Syslog**.
- Порт точки входа: введите значение в соответствии с настройками на стороне Nextcloud.
- Протокол: выберите вариант в соответствии с настройками на стороне Nextcloud.

3. Добавьте на конвейер элемент **Нормализатор** с правилом **Nextcloud** (идентификатор правила: **RV-N-300**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Установите конфигурацию конвейера.

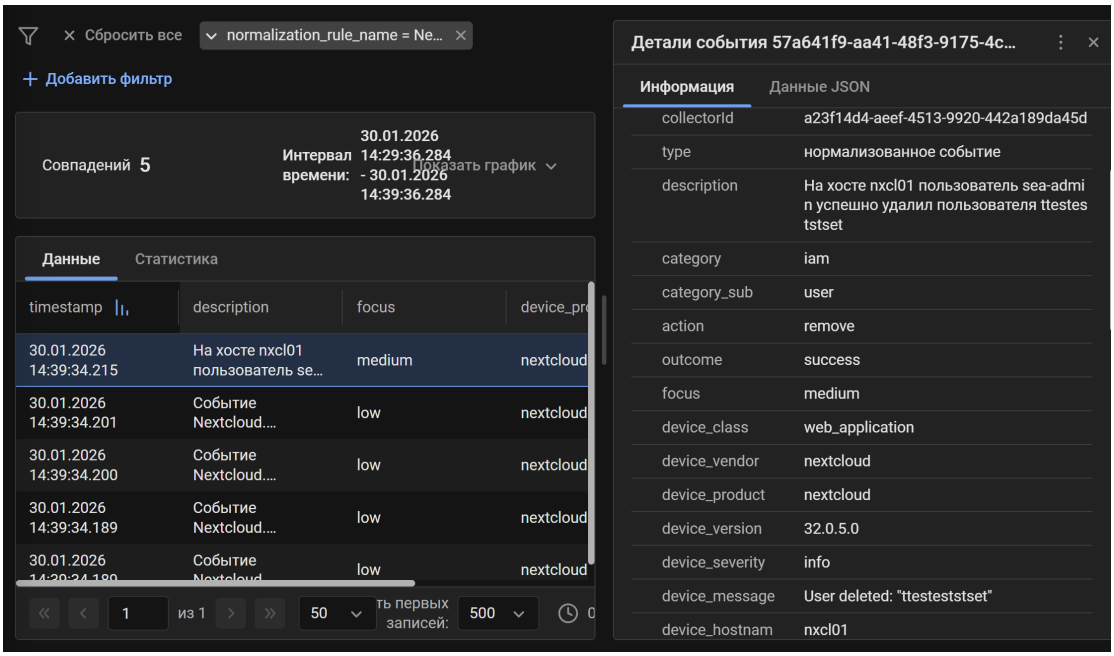
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Nextcloud.

Найти события Nextcloud в хранилище можно по следующему фильтру:

```
normalization_rule_name = "Nextcloud"
```



1С:Предприятие

- 1С:Предприятие: настройка источника

1С:Предприятие: настройка источника

- 1С:Предприятие Журнал регистрации
- 1С:Предприятие Технологический журнал

1С:Предприятие Журнал регистрации

Данное руководство описывает процесс настройки сбора событий журнала регистрации на сервере 1С:Предприятия и их последующей отправки в R-Vision SIEM.



Действия описаны на примере конфигурации **Зарплата и управление персоналом 3.1**. В других конфигурациях названия и расположение элементов интерфейса могут отличаться.

Предварительные требования

Перед настройкой пересылки событий в R-Vision SIEM убедитесь в выполнении следующих условий:

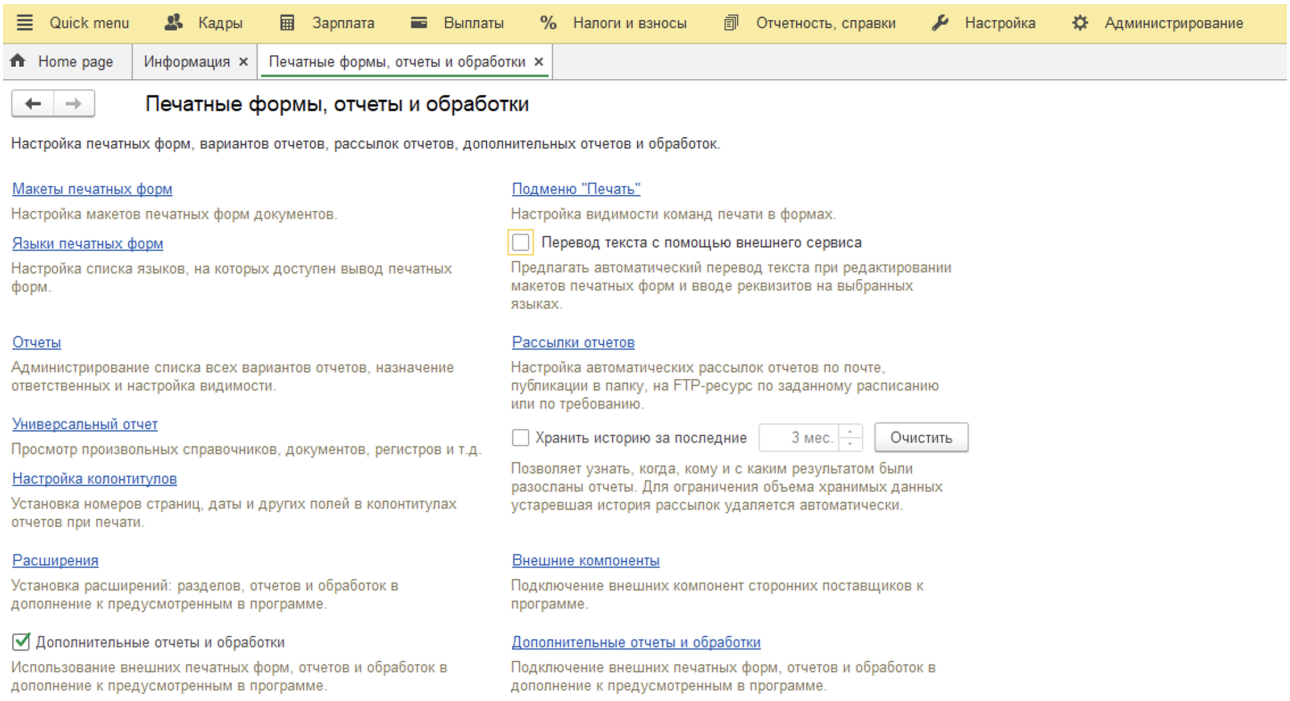
- Сетевая связность между сервером 1С:Предприятие и SIEM обеспечена, а необходимые порты открыты.

Настройка 1С:Предприятие

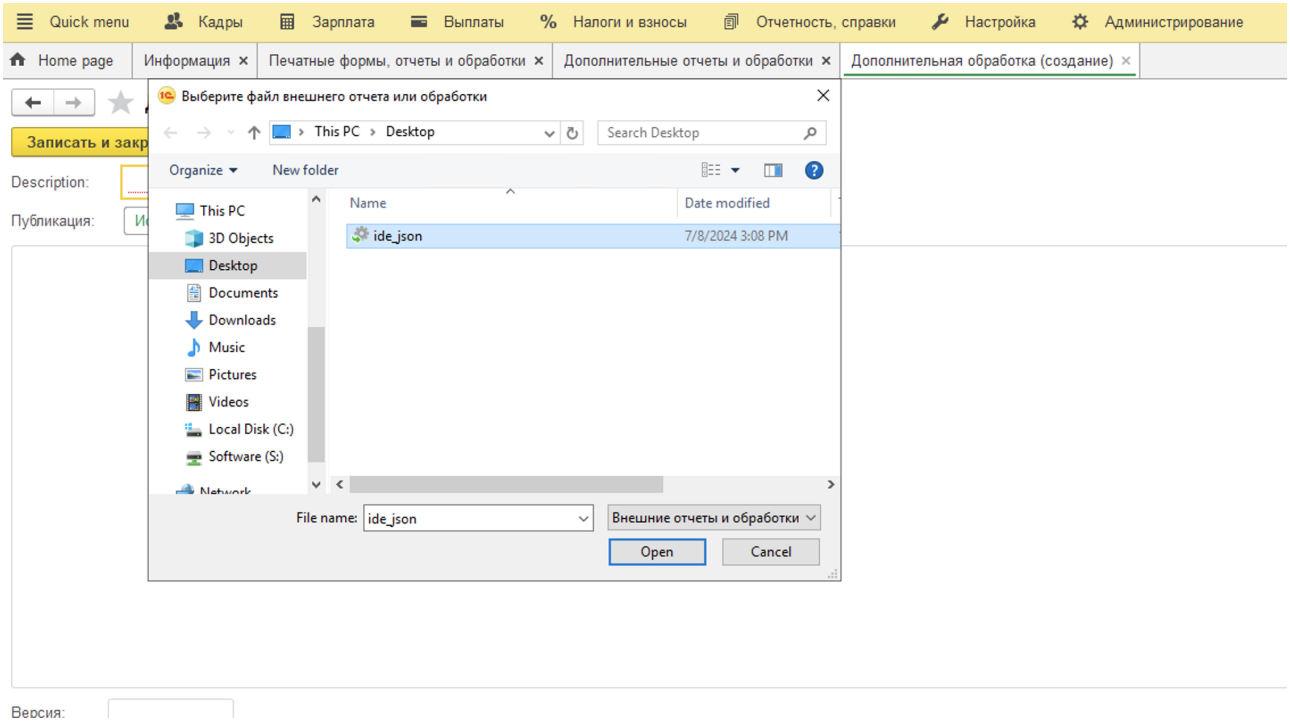
Настройка подсистемы журналирования

Чтобы настроить выгрузку регистрационного журнала в папку, выполните следующие действия:

1. Войдите в программу 1С:Предприятие. Для этого:
   a. Запустите 1С:Предприятие. Откроется окно **Запуск 1С:Предприятия**.
   b. Выберите в списке информационную базу и нажмите на кнопку **1С:Предприятие**.
   c. В открывшемся окне введите данные учетной записи администратора и нажмите на кнопку **Войти**. Откроется окно 1С:Предприятия.
2. Перейдите в раздел **Администрирование → Печатные формы, отчеты и обработки**.
3. Установите флажок **Дополнительные отчеты и обработки**.



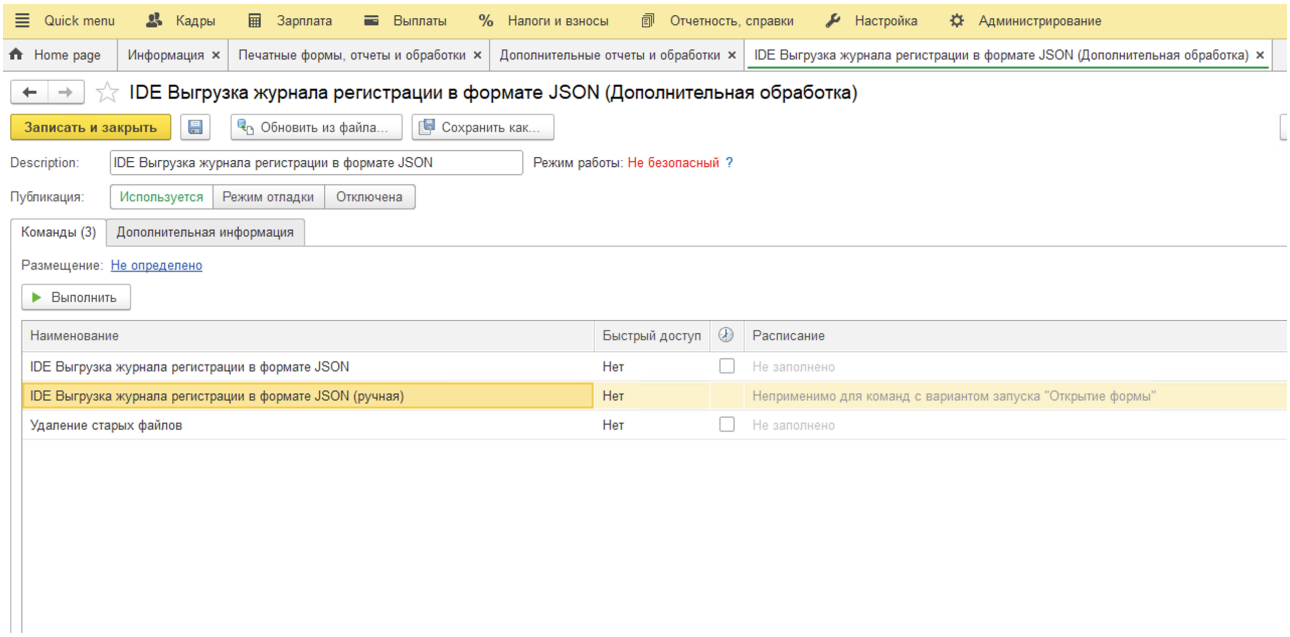
4. Перейдите в раздел **Дополнительные отчеты и обработки**.
5. На панели инструментов раздела нажмите на кнопку **Добавить из файла**. Откроется окно проводника.



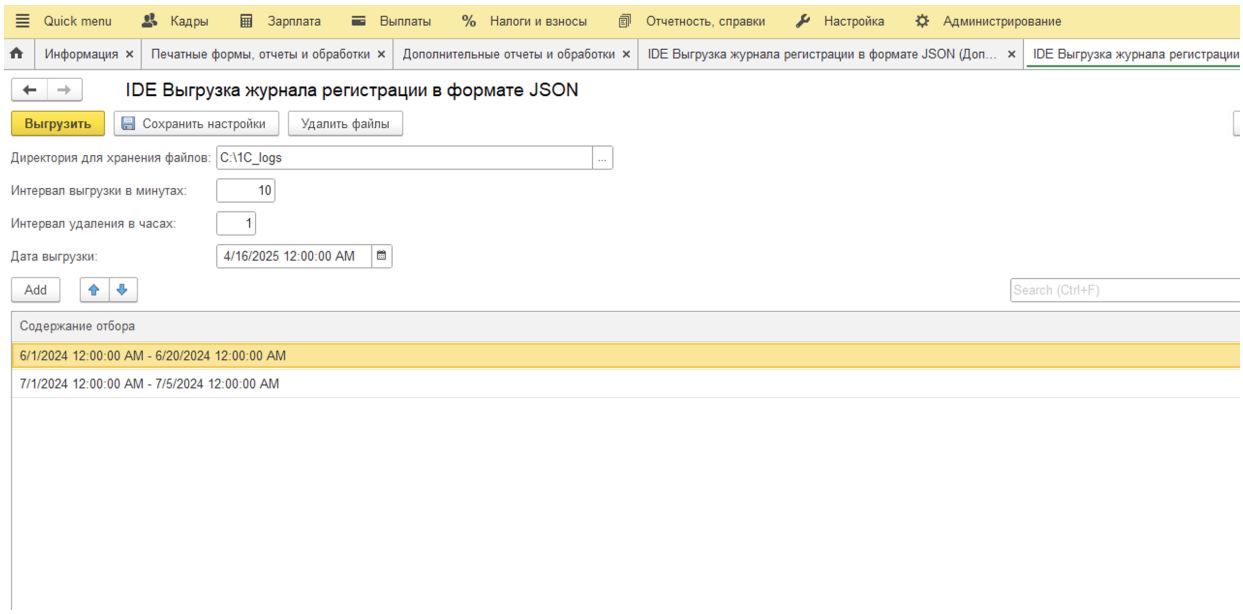
6. Выберите файл внешнего отчета или обработки и нажмите на кнопку **Open**. Откроется вкладка **IDE Выгрузка журнала регистрации в формате JSON (Дополнительная обработка)**.



Архив со сценарием обработки docs.rvision.ru/sources/ru/УМС 2.0/Applications/_attachments/ide_uploading_logbook_json.zip[представлен по ссылке].

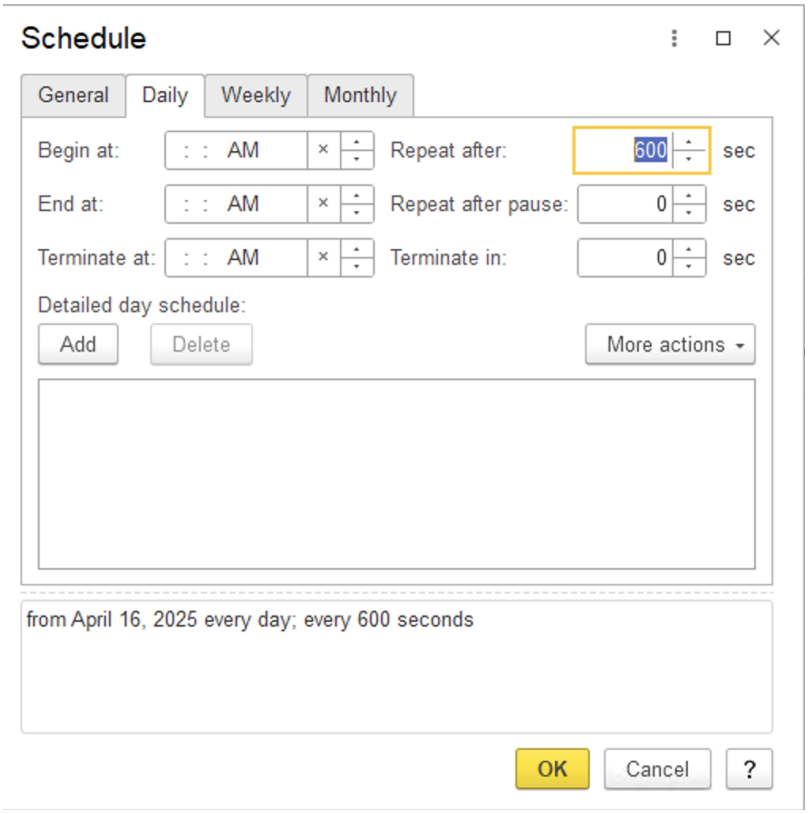


7. На панели инструментов вкладки нажмите на кнопку **Сохранить**.
8. На вкладке **Команды** выберите опцию **IDE Выгрузка журнала регистрации в формате JSON (ручная)** и нажмите на кнопку **Выполнить**. Откроется вкладка **IDE Выгрузка журнала регистрации в формате JSON**.
9. Укажите настройки выгрузки:
   - **Директория для хранения файлов**: введите путь для сохранения файлов журнала регистрации, например, `C:/1C_logs/`.
   - **Интервал выгрузки в минутах**: укажите временной промежуток в минутах, в течение которого события, зафиксированные в журнале регистрации, будут сохраняться в отдельном файле, например, `10`.
   - **Интервал удаления в часах**: укажите временной промежуток в часах, через который события, зафиксированные в журнале регистрации, будут автоматически удаляться, например, `1`.
   - **Дата выгрузки**: укажите дату, с которой начнется выгрузка журнала регистрации.

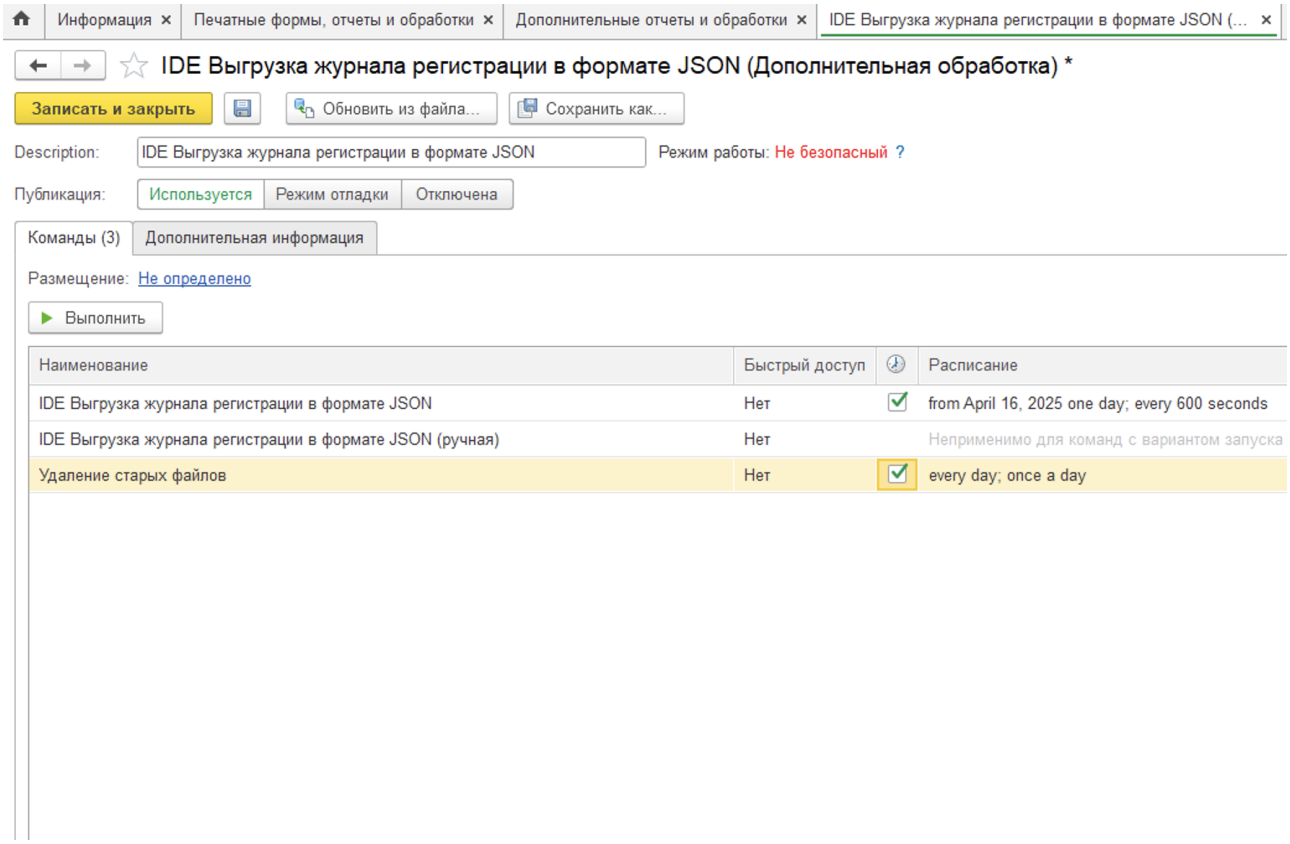


10. Нажмите на кнопку **Сохранить настройки** и подтвердите сохранение.

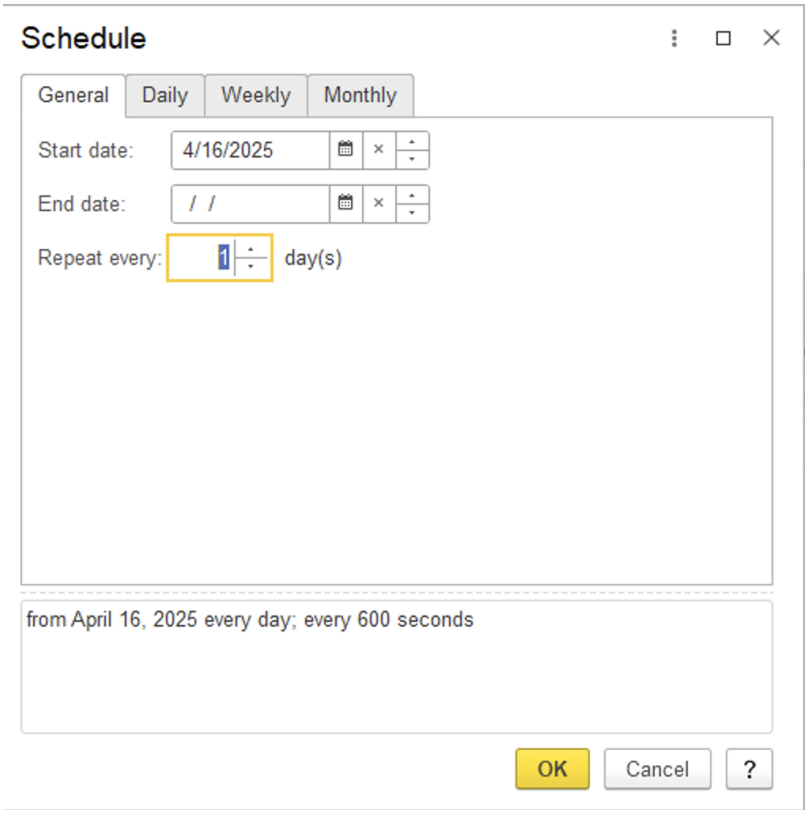
11. Закройте вкладку **IDE Выгрузка журнала регистрации в формате JSON**.
12. Перейдите на вкладку **IDE Выгрузка журнала регистрации в формате JSON (Дополнительная обработка)**.
13. На вкладке **Команды** установите флажок **IDE Выгрузка журнала регистрации в формате JSON**. Откроется окно **Schedule**.
14. Выберите вкладку **Daily** и в поле **Repeat after** введите значение `600`.
15. Нажмите на кнопку **OK**.



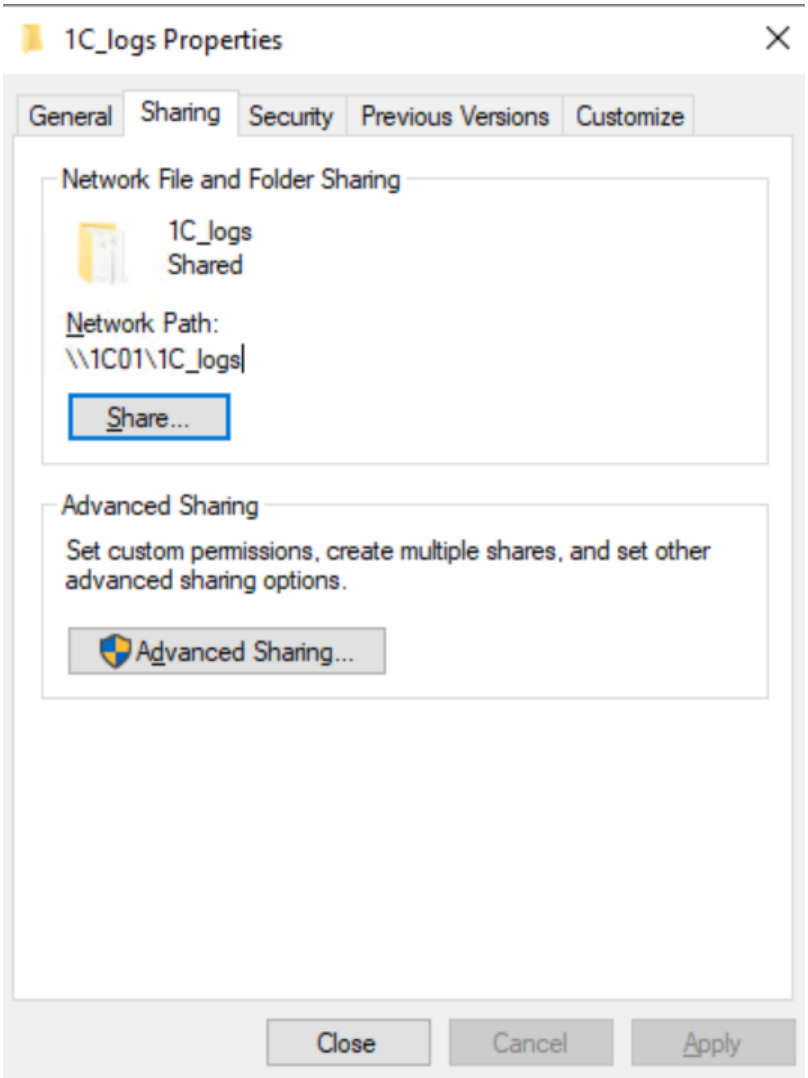
16. На вкладке **Команды** установите флажок **Удаление старых файлов**. Откроется окно **Schedule**.



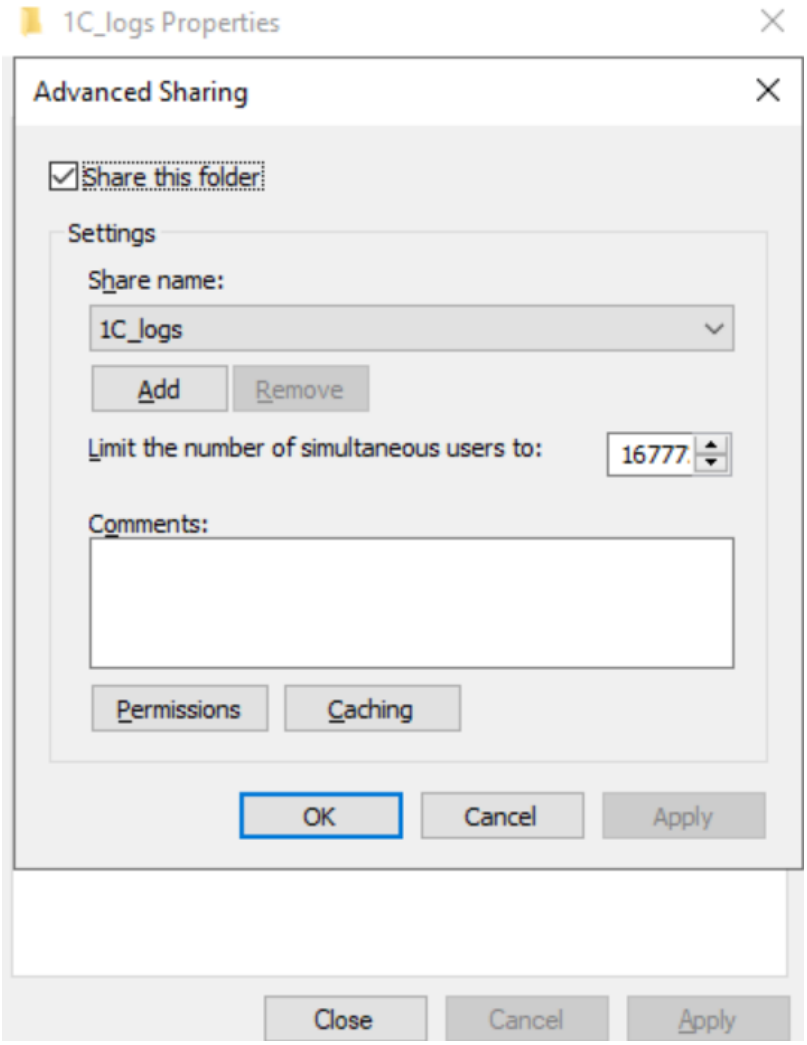
17. Выберите вкладку **General** и в поле **Repeat every** введите значение 1.
18. Нажмите на кнопку **OK**.



19. Нажмите на кнопку **Записать и закрыть**.
20. Откройте параметры папки, куда сохраняются события, перейдите во вкладку **Sharing**.



21. Нажмите **Advanced Sharing** и установите флажок **Share this folder**.



Настройка на стороне источника завершена.

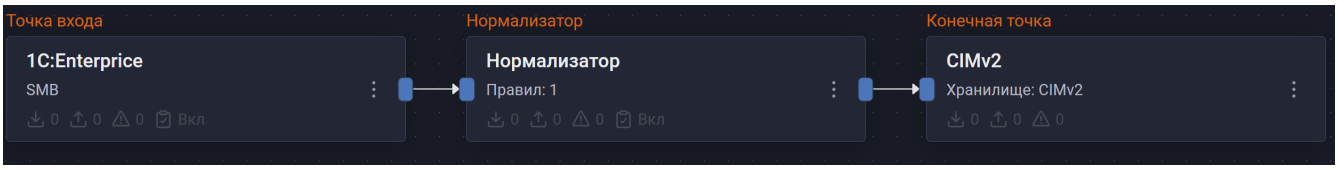
Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - **Название**: введите название точки входа.
   - **Тип точки входа**: выберите вариант **SMB**.
   - **Путь**: укажите сетевой путь к папке с событиями (значение из поля **Network Path**).
   - **Тип аутентификации**: выберите вариант **Auto**.
   - **Учетная запись**: выберите учетную запись, которая имеет доступ к серверу.
   - **Версия SMB**: выберите вариант **SMB3**.
   - **Маска файла**: введите `*.json`.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **1C-Soft 1C:Enterprise 8.3** (идентификатор правила: **RV-N-258**).
4. Соедините нормализатор с точкой входа.

5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

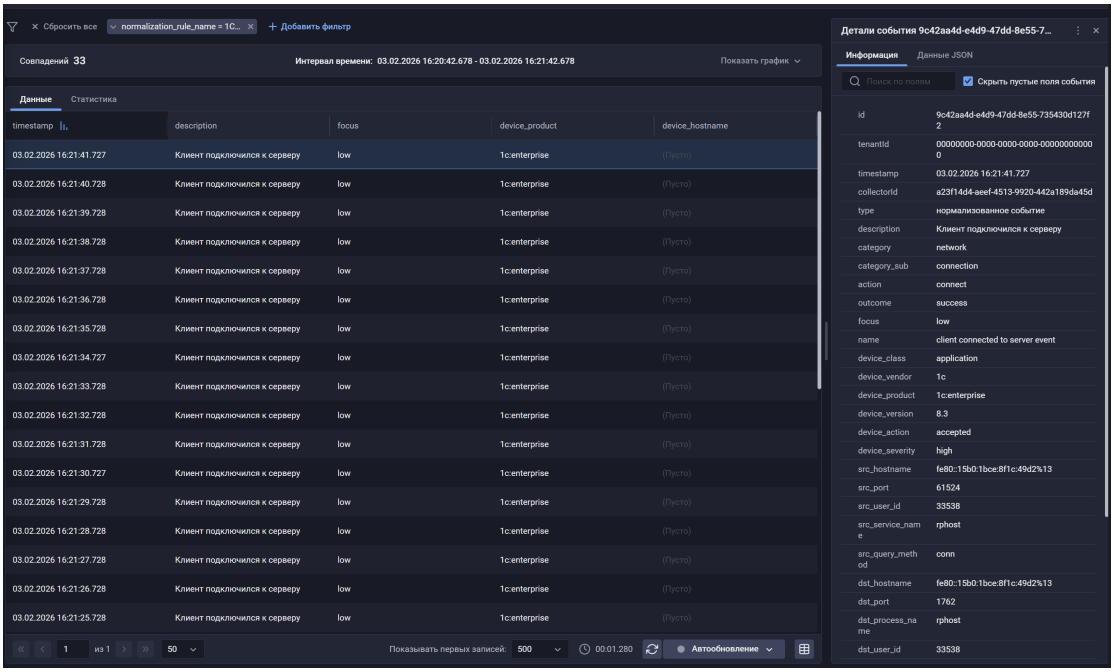
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события 1С:Предприятия.

Найти события 1С:Предприятия в хранилище можно по следующему фильтру:

```
normalization_rule_name = "1C:Enterprise registrationlog"
```



Типы обрабатываемых событий

- Успешная или неуспешная авторизация через толстый клиент, конфигуратор или COM-соединение.
- Успешная авторизация через толстый клиент.
- Ошибка авторизации через тонкий клиент.
- Ошибка авторизации через веб-клиент.
- Успешная авторизация через веб-клиент.
- Успешно установлено соединение с сервером 1С:Предприятия.
- Подключение к дизайнеру заблокировано другим пользователем.

- Просмотр списка пользователей, подключенных к серверу 1С:Предприятия.
- Просмотр пользователем параметров информационной базы.

1С:Предприятие Технологический журнал

Данное руководство описывает процесс настройки сбора событий технологического журнала на сервере 1С:Предприятия и их отправки в хранилище R-Vision SIEM.

Предварительные требования

Перед настройкой пересылки событий в R-Vision SIEM убедитесь в выполнении следующих условий:

- Сетевая связность между сервером 1С:Предприятие и SIEM обеспечена, а необходимые порты открыты.

Настройка 1С:Предприятие Технологический журнал

Настройка подсистемы журналирования

Чтобы настроить логирование событий технологического журнала на сервере 1С:Предприятия, выполните следующие шаги:

1. Создайте конфигурационный файл `logcfg.xml`. Расположение файла зависит от ОС и архитектуры сервера:
   - В Windows создайте файл в папке `\bin\conf` внутри папки, где установлено 1С:Предприятие.
   - В ОС семейства Unix с 32-битной архитектурой создайте файл в каталоге `/opt/1C/v8.3/i386/conf`.
   - В ОС семейства Unix с 64-битной архитектурой создайте файл в каталоге `/opt/1C/v8.3/x86_64/conf`.
2. Добавьте в файл следующие строки:

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <config xmlns="http://v8.1c.ru/v8/tech-log">

   </config>
   ```

3. Укажите внутри элемента `config` каталог для хранения файлов журнала и время хранения событий:

   ```
   <log location="<path>" history="<time>">

     <property name="all"/>
   </log>
   ```

   Здесь:

   - `<path>` — путь для хранения файлов журнала. Для Windows укажите общую папку, для ОС

семейства Unix — домашний каталог пользователя, от имени которого запускается сервер 1С:Предприятия.

- `<time>` — время хранения событий в часах. Например, для хранения событий за 7 суток укажите значение `168`.

4. Добавьте внутри элемента `log` фильтры событий:

```
<event>
  <eq property="name" value="CALL"/>
  <eq property="MName" value="authenticateServer"/>
</event>
<event>
  <eq property="name" value="SCALL"/>
  <eq property="MName" value="setSessionData"/>
  <eq property="t:applicationName" value="1CV8C"/>
</event>
<event>
  <eq property="name" value="EXCP"/>
  <eq property="t:applicationName" value="1CV8C"/>
  <like property="Descr" value="%VResourceInfoBaseServerImpl.cpp%"/>
</event>
<event>
  <eq property="name" value="EXP"/>
  <eq property="t:applicationName" value="WebServerExtension"/>
  <like property="Descr" value="%VResourceInfoBaseServerImpl.cpp%"/>
</event>
<event>
  <eq property="name" value="SCALL"/>
  <eq property="t:applicationName" value="WebServerExtension"/>
  <eq property="MName" value="setSessionData"/>
  <ne property="Usr" value="DefUser"/>
</event>
<event>
  <eq property="name" value="CONN"/>
  <like property="Txt" value="Accepted%"/>
</event>
<event>
  <eq property="name" value="CALL"/>
  <eq property="MName" value="lockConfig"/>
</event>
<event>
  <eq property="name" value="CALL"/>
  <eq property="MName" value="activeUsers"/>
</event>
<event>
  <eq property="name" value="CALL"/>
  <eq property="MName" value="readInfoBaseAdmParams"/>
  <ne property="Usr" value=""/>
</event>
```

5. Сохраните конфигурационный файл.

   Логирование событий технологического журнала настроено.

▼ *Пример конфигурационного файла для ОС Windows*

```
<?xml version="1.0" encoding="UTF-8"?>
<config xmlns="http://v8.1c.ru/v8/tech-log">
 <log location="C:\v8\logs" history="168">
  <event>
    <eq property="name" value="CALL"/>
    <eq property="MName" value="authenticateServer"/>
  </event>
  <event>
    <eq property="name" value="SCALL"/>
    <eq property="MName" value="setSessionData"/>
    <eq property="t:applicationName" value="1CV8C"/>
  </event>
  <event>
    <eq property="name" value="EXCP"/>
    <eq property="t:applicationName" value="1CV8C"/>
    <like property="Descr" value="%VResourceInfoBaseServerImpl.cpp%"/>
  </event>
  <event>
    <eq property="name" value="EXP"/>
    <eq property="t:applicationName" value="WebServerExtension"/>
    <like property="Descr" value="%VResourceInfoBaseServerImpl.cpp%"/>
  </event>
  <event>
    <eq property="name" value="SCALL"/>
    <eq property="t:applicationName" value="WebServerExtension"/>
    <eq property="MName" value="setSessionData"/>
    <ne property="Usr" value="DefUser"/>
  </event>
  <event>
    <eq property="name" value="CONN"/>
    <like property="Txt" value="Accepted%"/>
  </event>
  <event>
    <eq property="name" value="CALL"/>
    <eq property="MName" value="lockConfig"/>
  </event>
  <event>
    <eq property="name" value="CALL"/>
    <eq property="MName" value="activeUsers"/>
  </event>
  <event>
    <eq property="name" value="CALL"/>
    <eq property="MName" value="readInfoBaseAdmParams"/>
    <ne property="Usr" value=""/>
  </event>
```

```
  <property name="all"/>
  </log>
</config>
```

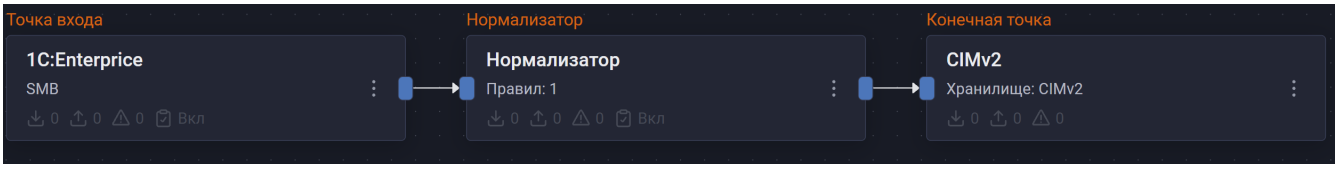
Этот файл создает технологический журнал в папке `C:\v8\logs` с хранением событий в течение 7 суток.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - **Название**: введите название точки входа.
   - **Тип точки входа**: выберите вариант **SMB**.
   - **Путь**: укажите путь к папке с событиями, он указан в конфигурационном файле logcfg.xml.
   - **Тип аутентификации**: выберите вариант **Auto**.
   - **Учетная запись**: выберите учетную запись, которая имеет доступ к серверу.
   - **Версия SMB**: выберите вариант **SMB3**.
   - **Маска файла**: введите `*.log`.
3. Добавьте на конвейер **Нормализатор** с правилом **1C-Soft 1C:Enterprise 8.3** (идентификатор правила: **RV-N-289**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

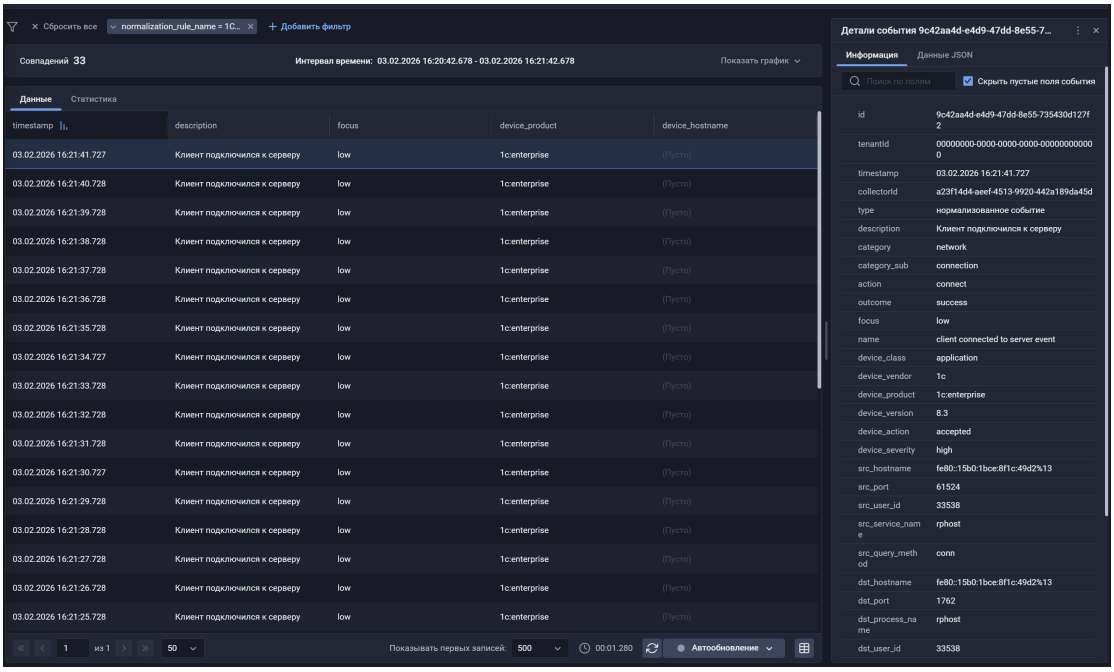


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события 1С:Предприятия.



Найти события 1С:Предприятия в хранилище можно по следующему фильтру:

```
normalization_rule_name = "1C:Enterprise techlog"
```



Битрикс24

- Битрикс24: сбор из СУБД MySQL (MariaDB)

Битрикс24: сбор из СУБД MySQL (MariaDB)

Данное руководство описывает процесс настройки сбора и отправки событий Битрикс24 в R-Vision SIEM.

Предварительные требования

- Сетевая доступность сервера СУБД Битрикс24 по целевому порту и протоколу для каждой ноды кластера SIEM.
- Учетная запись в СУБД с правами на чтение таблицы **b_event_log** (сбор событий из БД).

Настройка СУБД MySQL (MariaDB)

Создание учетной записи в СУБД MySQL (MariaDB)

Для создания сервисной УЗ подключитесь к СУБД с правами администратора. Для этого на сервере с установленной СУБД выполните следующие действия:

1. Выполните следующую команду от имени пользователя `root`:

```
mysql -u root -p
```

2. Создайте сервисную учетную запись, выполнив следующую команду:

```
CREATE USER 'reader'@'localhost' IDENTIFIED BY 'passw0rd';
```

3. Предоставьте сервисной учетной записи права на подключение к базе и чтение таблицы:

```
GRANT CONNECT ON DATABASE sitemanager to reader;
GRANT SELECT ON reader TO 'kasper'@'localhost';
```

Настройка в R-Vision SIEM

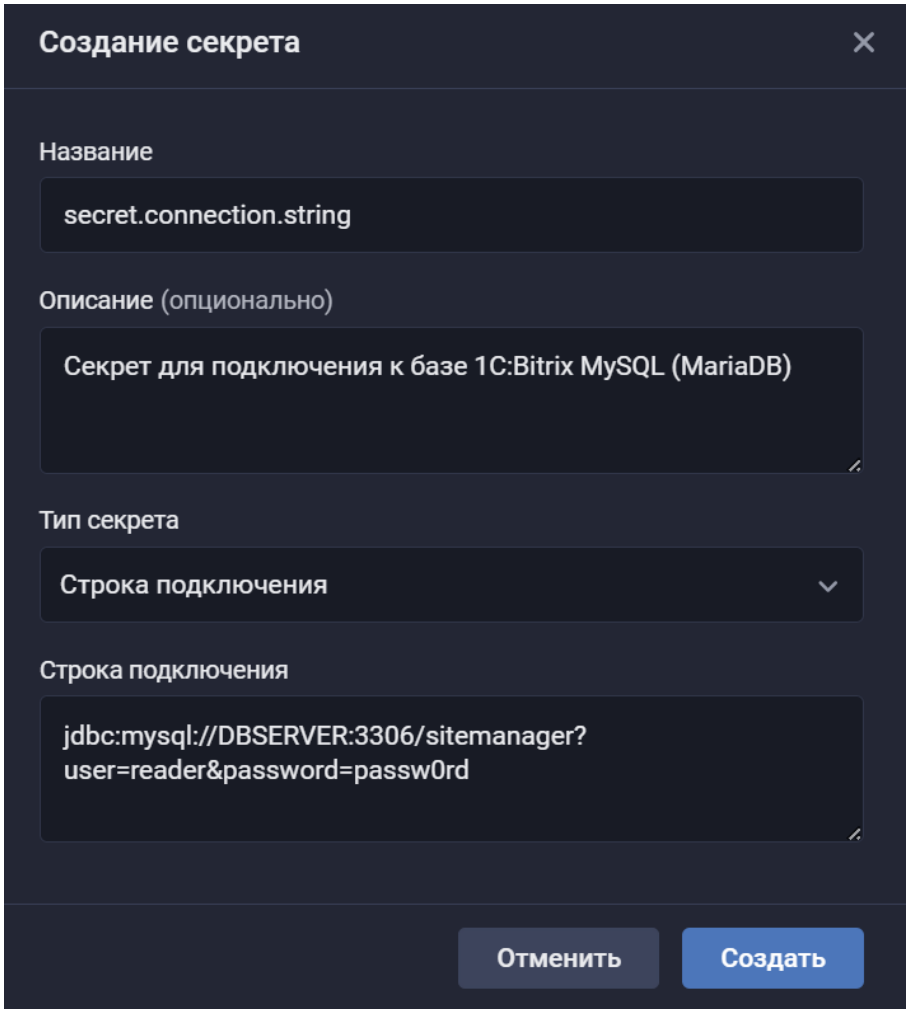
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте секрет со строкой подключения. Для этого:
   a. Перейдите в раздел **Ресурсы** → **Секреты**.
   b. Нажмите на кнопку **Создать** (+).
   c. В раскрывшемся окне создания секрета заполните поля:
      - Название: введите название секрета.
      - Описание (опционально): опишите, для чего будет использоваться секрет.
      - Тип секрета: выберите вариант **Строка подключения**.
      - Строка подключения — введите строку вида:

        ```
        jdbc:mysql://DBSERVER:3306/sitemanager?user=reader&password=passw0rd
        ```

        Здесь:

        - `DBSERVER` — FQDN или IP-адрес сервера СУБД.
        - `3306` — порт подключения.



d. Нажмите на кнопку **Создать**.

2. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
3. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Database**.
   - Драйвер базы данных: выберите вариант MySQL.
   - Адрес подключения: выберите секрет, созданный ранее.
   - SQL-запрос: введите запрос вида:

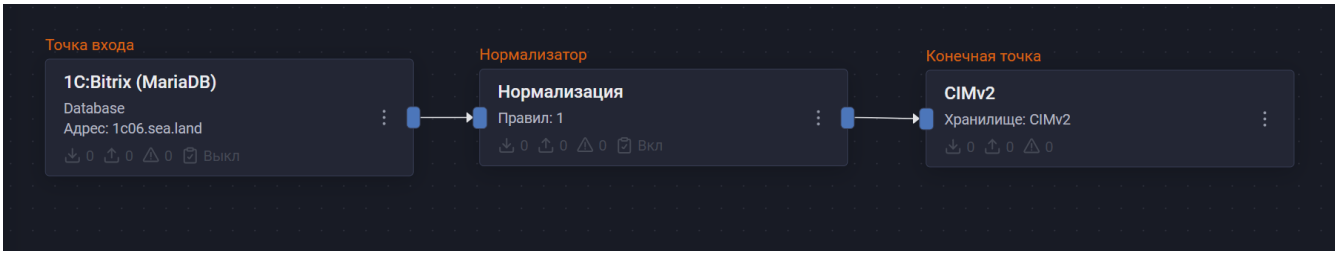
```
SELECT
    ID as ident
    ,TIMESTAMP_X
    ,SEVERITY
    ,AUDIT_TYPE_ID
    ,MODULE_ID
    ,ITEM_ID
    ,REMOTE_ADDR
    ,USER_AGENT
    ,REQUEST_URI
    ,USER_ID
    ,DESCRIPTION
```

```
    ,"Bitrix24" as appname
    ,@@hostname as hostname
FROM b_event_log WHERE ID > ?
ORDER BY ID ASC;
```

- Поле идентификатора: введите ключ `ident` со значением `1`.
- Интервал запроса, секунд: введите значение `15`.

4. Добавьте на конвейер элемент **Нормализатор** с правилом **1C:Bitrix24** (идентификатор правила: **RV-N-307**).
5. Соедините нормализатор с точкой входа.
6. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
7. Соедините конечную точку с нормализатором.
8. Сохраните и установите конфигурацию конвейера.

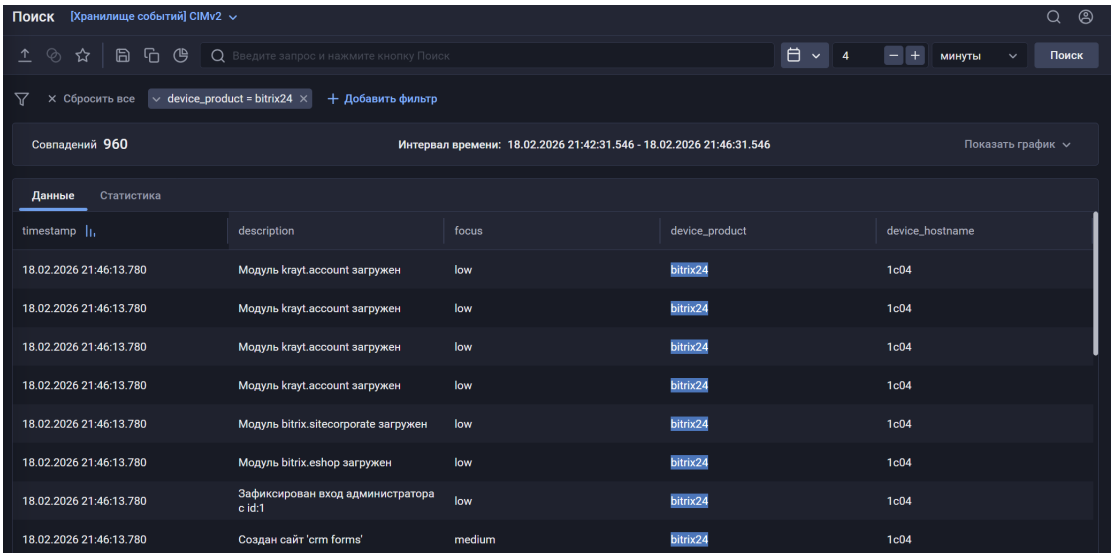
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события из MySQL.

Найти события Битрикс24 в хранилище можно по следующему фильтру:

```
device_product = "bitrix24"
```



Пассворк

- Пассворк: настройка источника
- Пассворк: правила корреляции

Пассворк: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Пассворк в R-Vision SIEM.

Предварительные требования

Перед настройкой пересылки событий в R-Vision SIEM убедитесь в выполнении следующих условий:

- Логирование событий настроено в соответствии с официальной документацией вендора.
- Сетевая связность между сервером Пассворк и SIEM (или промежуточным syslog-сервером) обеспечена, а необходимые порты открыты.

Настройка Пассворк

В настоящем руководстве рассматривается передача событий с помощью службы `rsyslog`. Предполагается, что `rsyslog` на станции с ОС Linux уже установлен.



Пассворк можно развернуть как в операционных системах Windows/Linux, так и в Docker-контейнере. Сбор событий описан в документации вендора, но, если вы выбираете Docker, нужно дополнительно пробрасывать файл журнала в корневую систему и настраивать считывание из файла.

Для настройки источника выполните следующие шаги:

1. Настройте передачу событий из файла, создав файл `/etc/rsyslog.d/02-passwork.conf` со следующим содержимым:

   ```
   if $msg contains "CEF:0|Passwork" then {
       action(type="omfwd"
              target="<target>"
              port="<port>"
              protocol="<protocol>"
       )
       stop
   }
   ```

   Здесь:

   - `<target>` — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
   - `<port>` — порт точки входа Syslog на конвейере SIEM.
   - `<protocol>` — сетевой протокол: `tcp` или `udp`.

2. Перезапустите службу `rsyslog.service` с помощью команды:

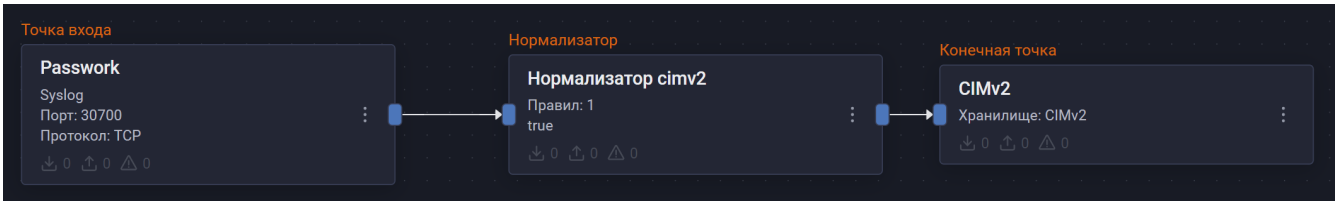
```
systemctl restart rsyslog.service
```

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - **Название**: введите произвольное, понятное название.
   - **Тип точки входа**: выберите вариант **Syslog**.
   - **Порт точки входа**: введите значение в соответствии с настройками на стороне Пассворк.
   - **Протокол**: выберите вариант в соответствии с настройками на стороне Пассворк.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Passwork** (идентификатор правила: **RV-N-224**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

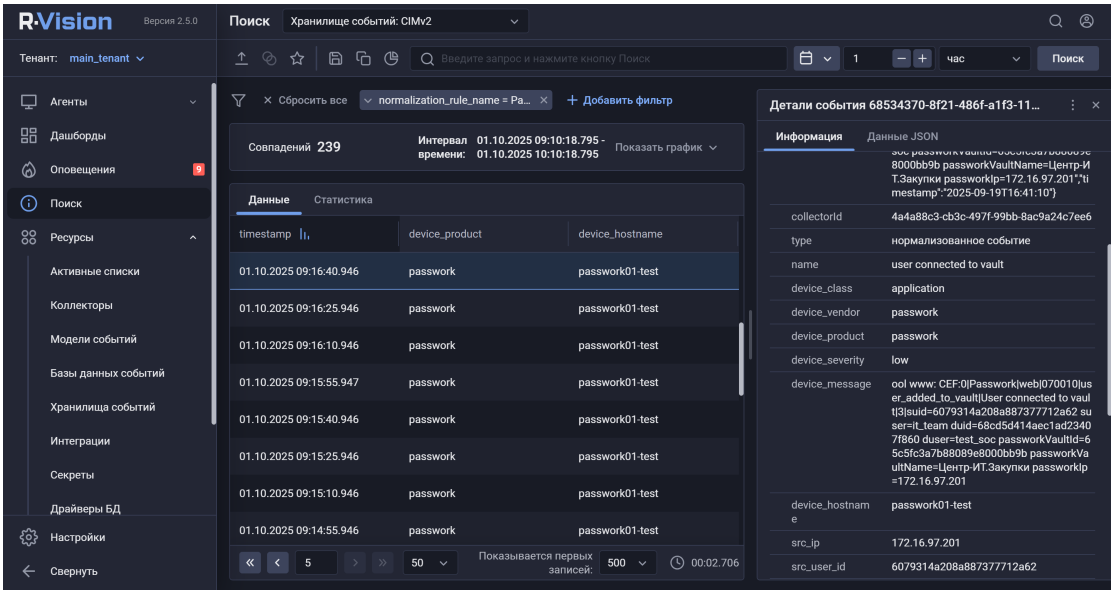
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Пассворк.

Найти события Пассворк в хранилище можно по следующему фильтру:

```
normalization_rule_name = "Passwork"
```



Пассворк: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1021	Массовое удаление учетных записей	Данное правило обнаруживает подозрительную активность по массовому удалению учетных записей в системе, когда в течение пяти минут происходит удаление пяти и более учетных записей. Подобные действия могут указывать на активность атакующего, пытающегося нанести ущерб работоспособности системы. При срабатывании правила необходимо опросить ответственного, от учетной записи которого были выполнены действия, для проверки их легитимности. В случае подтверждения инцидента требуется заблокировать учетную запись, восстановить удаленные учетные записи из резервной копии и инициировать расследование.	• Impact (TA0040) • Account Access Removal (T1531)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1027	Вход под УЗ администратора	Данное правило детектирует успешную аутентификацию под учетной записью администратора с IP-адреса, который не входит в список разрешенных для данных учетных записей. Данное событие указывает на потенциальную компрометацию УЗ администратора.	• Initial Access (TA0001) • Valid Accounts (T1078)
RV-D-1028	Множественный просмотр паролей за короткий промежуток времени	Данное правило обнаруживает подозрительную активность административной учетной записи в парольном менеджере, когда в течение трех минут происходит просмотр десяти и более паролей. Такие действия могут указывать на несанкционированный сбор учетных данных атакующим, получившим доступ к привилегированной учетной записи, с целью их последующего использования для горизонтального перемещения или повышения привилегий в сети. При срабатывании правила необходимо выяснить легитимность действий у владельца учетной записи и при необходимости заблокировать ее. В случае подтверждения инцидента требуется инициировать процесс расследования.	• Credential Access (TA0006) • Credentials from Password Stores (T1555)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1034	Брутфорс Passwork	Данное правило обнаруживает множественные неудачные попытки входа в систему парольного менеджера Passwork, включая ошибки аутентификации и неверные коды двухфакторной аутентификации (2FA). Подобная активность указывает на вероятную попытку подбора учетных данных (логина и пароля) или кода верификации для получения несанкционированного доступа к хранилищу паролей. При срабатывании правила рекомендуется идентифицировать учетную запись, на которую направлена атака, и уведомить ее владельца, а также связаться с лицом, ответственным за парольный менеджер, и предупредить о данной активности. Проанализировать источник атаки. В случае подтверждения инцидента необходимо заблокировать IP-адрес источника атаки и сменить пароль целевой учетной записи, инициировать процесс расследования.	• Credential Access (TA0006) • Brute Force (T1110)
RV-D-1038	Массовое удаление сейфов, папок, паролей	Данное правило обнаруживает подозрительную активность по удалению множества паролей, папок и сейфов за короткий промежуток времени. Подобные действия могут указывать на попытку атакующего удалить данные, чтобы саботировать работу компании. При срабатывании правила необходимо идентифицировать и опросить ответственного за учетную запись, выполнившего изменение, для проверки легитимности действий. В случае подтверждения инцидента необходимо инициировать процесс расследования.	• Impact (TA0040) • Data Destruction (T1485)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1039	Включение заблокированной УЗ	Данное правило обнаруживает подозрительную активность по разблокировке учетных записей. Подобные действия могут указывать на попытку атакующего активировать УЗ, которая является недействительной, и действовать он ее имени. При срабатывании правила необходимо идентифицировать и опросить ответственного за учетную запись, выполнившего изменение, для проверки легитимности действий. В случае подтверждения инцидента необходимо инициировать процесс расследования.	• Persistence (TA0003) • Account Manipulation (T1098)
RV-D-1040	Изменение прав роли	Данное правило обнаруживает подозрительные изменения привилегий, назначенных роли в системе. Подобные действия могут указывать на попытку атакующего повысить уровень доступа своей или другой роли для обхода механизмов безопасности и получения несанкционированных прав в системе. При срабатывании правила необходимо немедленно идентифицировать и опросить ответственного за учетную запись, выполнившего изменение, для проверки легитимности действий. В случае подтверждения инцидента необходимо инициировать процесс расследования.	• Persistence (TA0003) • Account Manipulation (T1098)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1044	Добавление пользователя в критичный сейф	Данное правило обнаруживает подозрительную активность по добавлению пользователей в критичный сейф паролей. Подобные действия могут указывать на попытку атакующего предоставить права на чтение критичных паролей для учетной записи, которая используется в атаке. При срабатывании правила необходимо идентифицировать и опросить ответственного за учетную запись, выполнившего изменение, для проверки легитимности действий. В случае подтверждения инцидента необходимо инициировать процесс расследования.	• Persistence (TA0003) • Account Manipulation (T1098)
RV-D-1045	Успешный брутфорс Passwork	Данное правило обнаруживает успешный вход в систему парольного менеджера Passwork после множества неудачных попыток аутентификации, что указывает на высокую вероятность компрометации учетных данных в результате атаки подбора. В случае срабатывания правила необходимо опросить владельца учетной записи для проверки легитимности данной активности. Если активность не является легитимной, требуется заблокировать скомпрометированную учетную запись, инициировать смену ее пароля, а также заблокировать IP-адрес источника атаки. Инициировать процесс расследования.	• Credential Access (TA0006) • Brute Force (T1110)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1046	Назначение роли администратора	Данное правило детектирует подозрительную активность по предоставлению прав администратора. Подобные действия могут указывать на попытку атакующего повысить уровень доступа своей или другой учетной записи для обхода механизмов безопасности и получения несанкционированных прав в системе. При срабатывании правила необходимо немедленно идентифицировать и опросить ответственного за учетную запись, выполнившего изменение, для проверки легитимности действий. В случае подтверждения инцидента необходимо инициировать процесс расследования.	• Persistence (TA0003) • Account Manipulation (T1098)
RV-D-1047	Экспорт паролей/сейфа Passwork	Данное правило детектирует события, связанные с экспортом данных (паролей, сейфов) из парольного менеджера Passwork. Подобные действия могут указывать на попытку несанкционированного копирования учетных данных атакующим. При срабатывании правила необходимо немедленно идентифицировать и опросить владельца учетной записи, от имени которой было выполнено действие, для проверки его легитимности. В случае подтверждения инцидента требуется заблокировать учетную запись, изменить все пароли, которые могли быть скомпрометированы, и провести расследование.	• Credential Access (TA0006) • Credentials from Password Stores (T1555) • Password Managers (T1555.005)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1059	Отключение 2FA	Данное правило обнаруживает подозрительную активность по отключению 2FA. Подобные действия могут указывать на попытку атакующего отключить систему защиты 2FA для получения доступа к учетной записи.	• Defense Evasion (TA0005) • Impair Defenses (T1562)
RV-D-1060	Создание пользователя	Данное правило обнаруживает подозрительную активность, связанную с созданием новых пользователей. Подобные действия могут указывать на попытку атакующего создать себе учетные записи для работы под ними, чтобы не вызывать подозрений или иметь возможность дольше оставаться в системе.	• Persistence (TA0003) • Create Account (T1136)

Веб-серверы

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых веб-серверов:

- Apache HTTP Server
- Microsoft IIS
- Nginx

Apache HTTP Server

- Apache HTTP Server: настройка источника

Apache HTTP Server: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Apache HTTP Server в R-Vision SIEM.

Настройка Apache HTTP Server

Описание подсистемы журналирования Apache HTTP Server

Журналирование событий службы Apache HTTP Server по умолчанию ведется в одной из следующих директорий:

- `/var/log/apache`;
- `/var/log/httpd`.

Запись событий осуществляется следующим образом:

1. В файл `error.log` собираются обращения хостов сети к ресурсам.
2. В файл `access.log` записываются события с ошибками в работе службы веб-сервера.

Настройка журналирования Apache HTTP Server

Для корректного отображения в R-Vision SIEM событий журнала access настройте на сервере Apache формат сообщений согласно следующим рекомендациям:

1. В файле `apache.conf` или `httpd.conf` найдите строку, задающую формат логов, и замените ее на следующий вариант:

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"
```



Для сервиса Apache Tomcat необходимо изменить формат лога в файле `server.xml`:

```
%a %{jira.request.id}r %{jira.request.username}r %t &amp;quot;%m %U%q
```

```
%H&amp;quot; %s %b &amp;quot;%{Referer}i&amp;quot; &amp;quot;%{User-Agent}i&amp;quot;
```

2. Перезапустите службу Apache HTTP Server с помощью команды:

```
systemctl restart httpd
```

Отправка событий Apache HTTP Server

Настройка отправки событий на сервер syslog

События службы Apache HTTP Server отправляются на централизованный сервер syslog. Затем происходит отправка событий в SIEM.

Чтобы настроить отправку событий службы Apache HTTP Server, выполните следующие шаги:

1. Откройте конфигурационный файл rsyslog: `/etc/rsyslog.conf` или `/etc/rsyslog.d/`.
2. Добавьте в файл следующие правила:

```
module(load="imfile")

input(
    type="imfile"
    File="/var/log/httpd/access_log"
    Tag="Apache_Access"
    Severity="info"
    Facility="local4"
)

input(
    type="imfile"
    File="/var/log/httpd/error_log"
    Tag="Apache_Error"
    Severity="info"
    Facility="local4"
)

if $syslogtag == 'Apache_Access' or $syslogtag == 'Apache_Error' then {
    action(
        type="omfwd"
        Target="<target>"
        Port="<port>"
        Protocol="udp"
    )
    stop
}
```

Здесь:

- `<target>` — IP-адрес или полное доменное имя (FQDN) сервера syslog.
- `<port>` — порт `514` или любой другой порт, настроенный для приема.

3. Чтобы изменения вступили в силу, перезапустите rsyslog с помощью команды:

```
sudo systemctl restart rsyslog
```

Настройка отправки событий в SIEM

Настройте отправку логов с сервера syslog в SIEM:

1. Откройте конфигурационный файл rsyslog: `/etc/rsyslog.conf` или `/etc/rsyslog.d/`.
2. Добавьте в файл следующее правило:

```
if $syslogtag == 'Apache' then {
  action(type="omfwd" target="target" port="port" protocol="tcp")
  stop
}
```

Здесь:

- `<target>` — IP-адрес или полное доменное имя (FQDN) узла кластера Kubernetes, на котором запущен коллектор SIEM.
- `<port>` — порт точки входа Syslog: значение в диапазоне 30000—32767.

3. Чтобы изменения вступили в силу, перезапустите rsyslog с помощью команды:

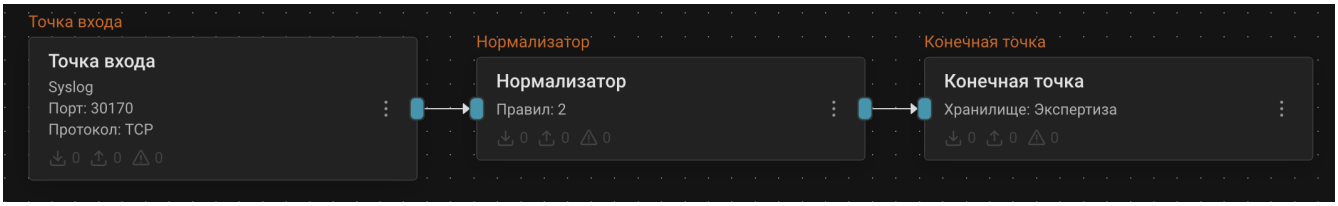
```
sudo systemctl restart rsyslog
```

Настройка в R-Vision SIEM

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне Apache HTTP Server.
   - Протокол: выберите вариант в соответствии с настройками на стороне Apache HTTP Server.
3. Добавьте на конвейер элемент **Нормализатор** с правилами **Apache HTTP-server Access** (идентификатор правила: **RV-N-231**) и **Apache HTTP-server Error** (идентификатор правила: **RV-N-232**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.

6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

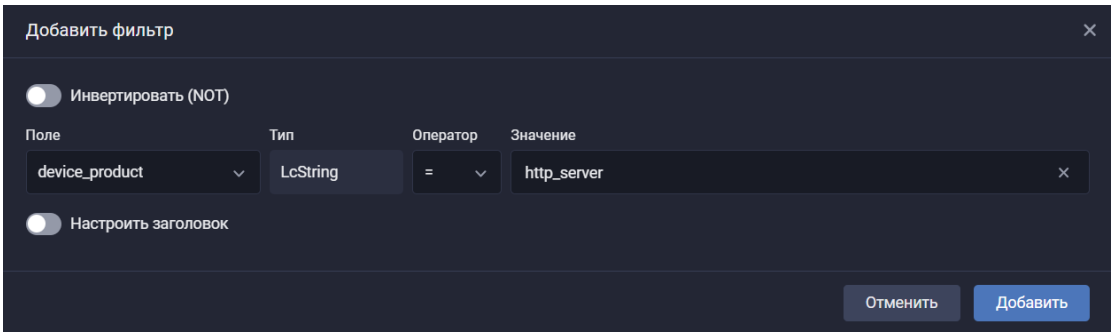
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Apache HTTP Server.

Найти события Apache HTTP Server в хранилище можно по следующему фильтру:

```
device_product = "http_server"
```



Microsoft IIS

- Microsoft IIS: настройка источника
- Microsoft IIS: правила корреляции

Microsoft IIS: настройка источника

Данное руководство описывает процесс настройки сбора событий Microsoft IIS (Internet Information Services) и их отправки в R-Vision SIEM.

Настройка Microsoft IIS

Настройка журналирования Microsoft IIS

В настоящем руководстве рассматривается передача событий с помощью агента платформы R-Vision EVO.

Включите логирование событий Microsoft через Event Viewer:

1. В дереве навигации перейдите по пути **Microsoft** → **Windows** → **IIS Logging** → **Logs**.

2. Чтобы настроить журналирование, выполните команду **Enable Log** в контекстном меню.
3. Установите на узле агент R-Vision EVO.

Настройка в R-Vision SIEM

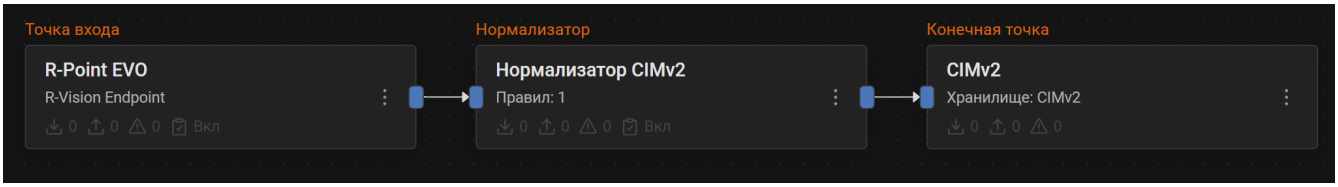
Настройка отправки событий в R-Vision SIEM

1. В веб-интерфейсе R-Vision SIEM перейдите в раздел **Агенты** → **Группы агентов**.
2. Создайте группу и добавьте в нее узел, на котором установлен агент.
3. В созданной группе узлов в секции **Чтение файлов** нажмите на кнопку **Добавить настройку** (+).
4. В выпадающем списке **Тип журнала** выберите вариант **eventchannel**.
5. В поле **Имя журнала** введите значение `Microsoft-Windows-IIS-Logging/Logs`.
6. Если необходимо выбирать события по определенным критериям, введите в поле **Фильтр (формат XPATH)** выражение XPath. Если фильтр не нужен, введите символ *.
7. Нажмите на кнопку **Сохранить и применить**.
8. Дождитесь применения политики группы на узле. Сбор событий настроен.

Настройка обработки событий в R-Vision SIEM

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **R-Vision Endpoint**.
   - Домен: введите значение в формате `gw-<your_gateway_id>`, где `<your_gateway_id>` — ID шлюза.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Microsoft IIS Access** (идентификатор правила: **RV-N-230**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

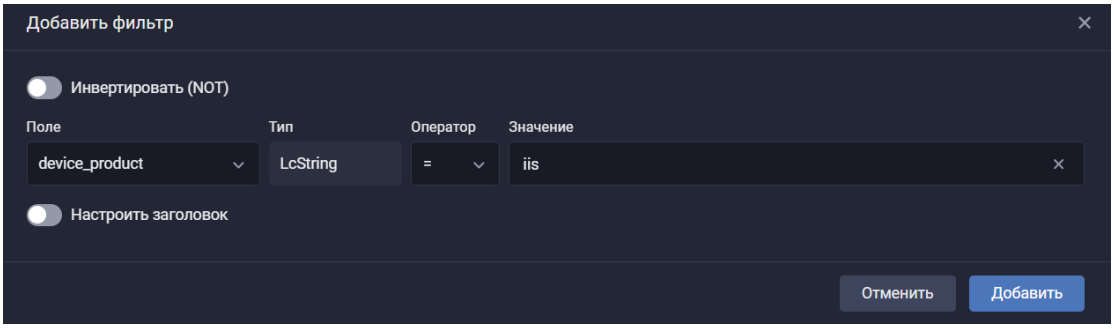
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Microsoft IIS.

Найти события Microsoft IIS в хранилище можно по следующему фильтру:

```
device_product = "iis"
```



Microsoft IIS: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1131	Установка модуля IIS	Appcmd.exe — легитимная утилита управления Microsoft IIS, входящая в состав Internet Information Services и предназначенная для настройки веб-сервера через командную строку. Данный инструмент позволяет добавлять и регистрировать собственные ISAPI-фильтры, Native-модули и управляемые модули, что может быть использовано атакующим для внедрения вредоносных компонентов в конвейер обработки запросов IIS. Это позволяет реализовать механизм закрепления и выполнения кода в контексте рабочего процесса веб-сервера, маскируя активность под легитимные операции обслуживания инфраструктуры.	• Execution (TA0002) • Persistence (TA0003) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Windows Command Shell (T1059.003) • Server Software Component (T1505) • IIS Components (T1505.004)

Nginx

- Nginx: настройка источника

Nginx: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Nginx в R-Vision SIEM.

Настройка Nginx

В настоящем руководстве рассматривается передача событий с помощью службы rsyslog. Предполагается, что rsyslog на станции с ОС Linux уже установлен.



Журналирование событий службы Nginx по умолчанию ведется в директории `/var/log/nginx`. Дополнительных действий по настройке журналирования не требуется.

Для настройки источника выполните следующие действия:

1. Настройте передачу событий из файла. Для этого создайте файл `/etc/rsyslog.d/03-Nginx.conf` со следующим содержимым:

```
$ModLoad imfile

$InputFileName /var/log/nginx/access.log
$InputFileTag nginx-access
$InputFileSeverity info
$InputFileFacility local4
$InputRunFileMonitor
$InputRunFileMonitor

$InputFileName /var/log/nginx/error.log
$InputFileTag nginx-error
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor
$InputRunFileMonitor

if $syslogtag contains 'nginx' then {
  action(type="omfwd" target="<target>" port="<port>" protocol="<protocol>")
  stop
}
```

   Здесь:

   - `<target>` — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
   - `<port>` — порт точки входа Syslog на конвейере SIEM.
   - `<protocol>` — сетевой протокол: `tcp` или `udp`.

2. Перезапустите службу rsyslog.service с помощью команды:

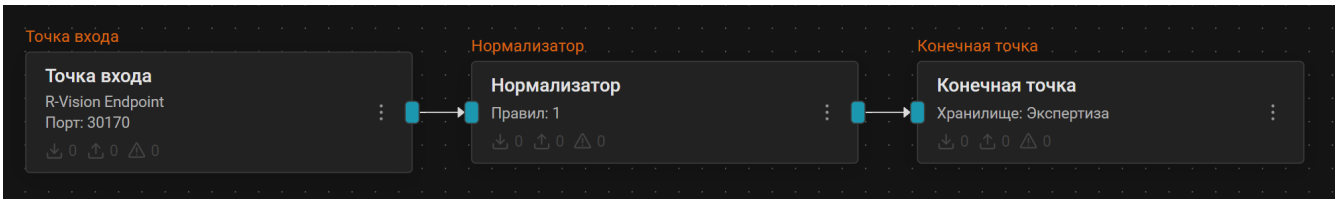
```
systemctl restart rsyslog.service
```

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне Nginx.
   - Протокол: выберите вариант в соответствии с настройками на стороне Nginx.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Nginx** (идентификатор правила: **RV-N-234**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

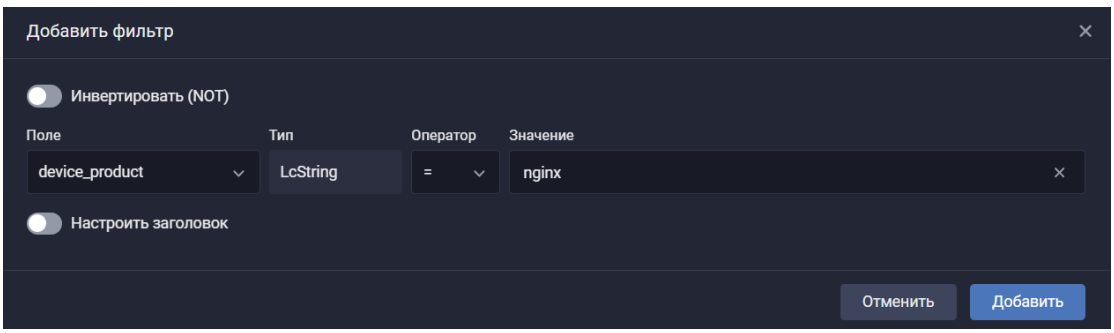
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Nginx.

Найти события Nginx в хранилище можно по следующему фильтру:

```
device_product = "nginx"
```



Межсетевые экраны

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых межсетевых экранов:

- Check Point Gaia
- Cisco ASA
- Ideco NGFW
- ИнфоТеКС ViPNet Coordinator 4
- Код Безопасности Континент 3.9.3
- Код Безопасности Континент 4
- С-Терра Шлюз

Check Point Gaia

- Check Point Gaia: настройка источника

Check Point Gaia: настройка источника

Данная инструкция описывает настройку экспорта событий безопасности из управления Check Point Gaia в систему R-Vision SIEM с использованием компонента Log Exporter. Поддерживаются версии 81 и 82.

Предварительные требования

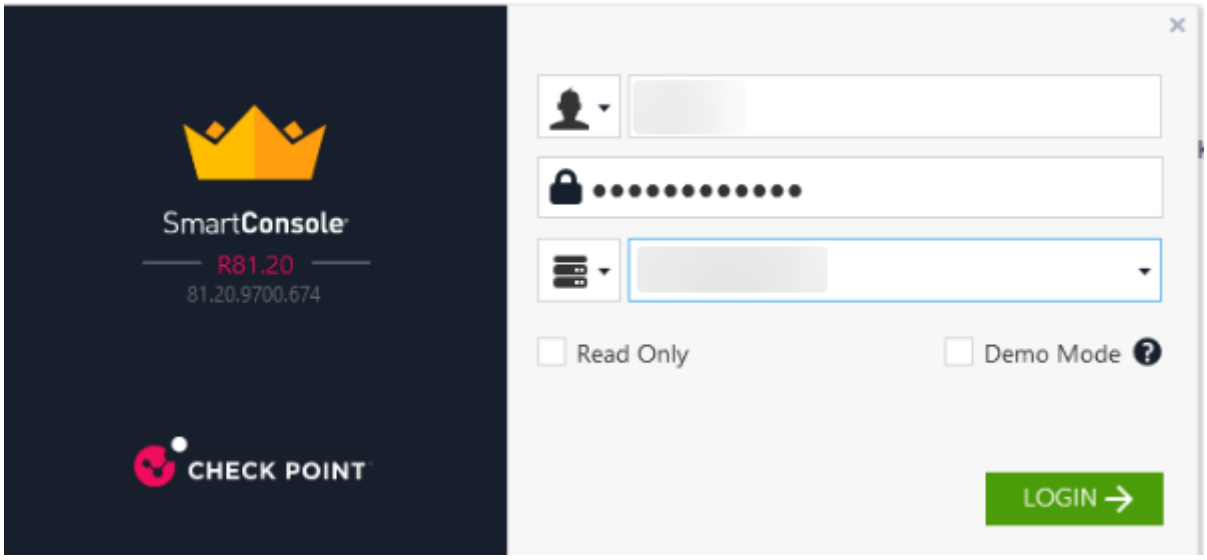
- Проведена предварительная настройка Check Point Gaia.
- Настроено сетевое подключение к серверу с помощью **SmartConsole**.
- Обеспечена возможность сетевого подключения с сервера Check Point Gaia к нодам R-Vision SIEM.
- Для настройки требуются права администратора домена безопасности (Domain Administrator или эквивалентные).

Настройка экспорта логов из Check Point Gaia в SIEM

1. **Подключение к среде управления**

   Войдите в **SmartConsole**, указав параметры подключения к серверу управления (**Security Management Server**):

   - **Server**: IP-адрес или FQDN Security Management Server.
   - **User**: имя администратора (например, `admin`).
   - **Password**: пароль администратора.

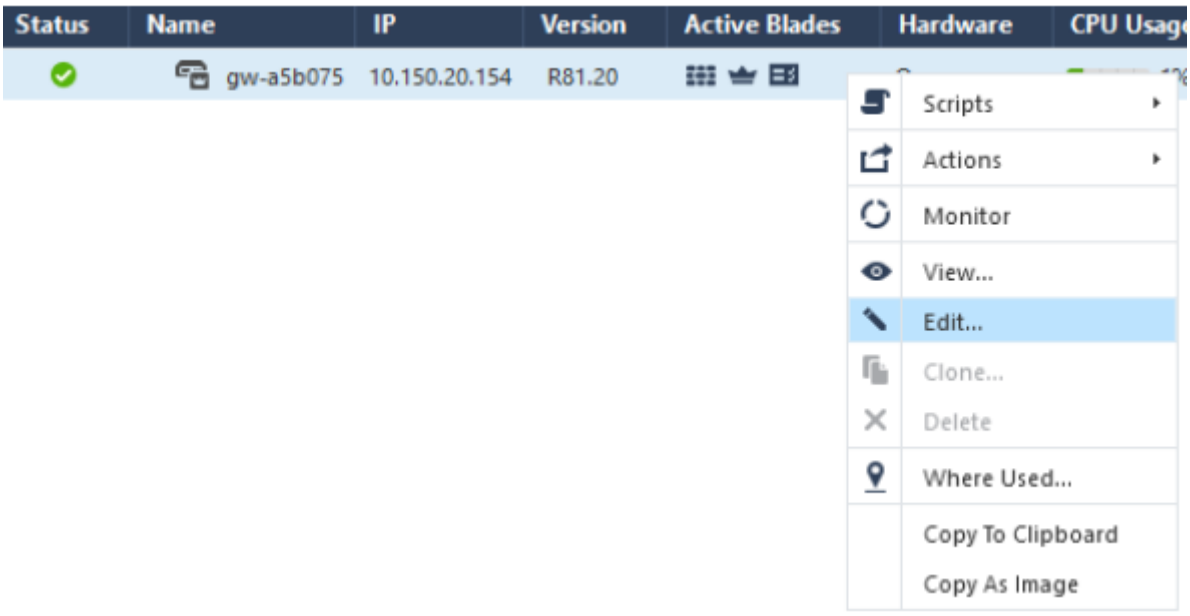


2. **Выбор домена безопасности**

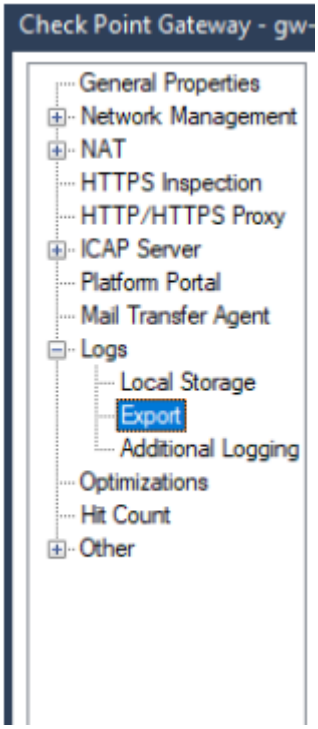
   После успешной аутентификации выберите домен или сервер управления, с которого требуется экспортировать логи.

3. **Открытие настроек экспорта логов**

   В дереве объектов выберите сервер управления, щелкните правой кнопкой мыши и выберите **Edit**.



   Перейдите в раздел: **Logs & Reports** → **Log Exporters**.



4. **Создание нового экспортера**

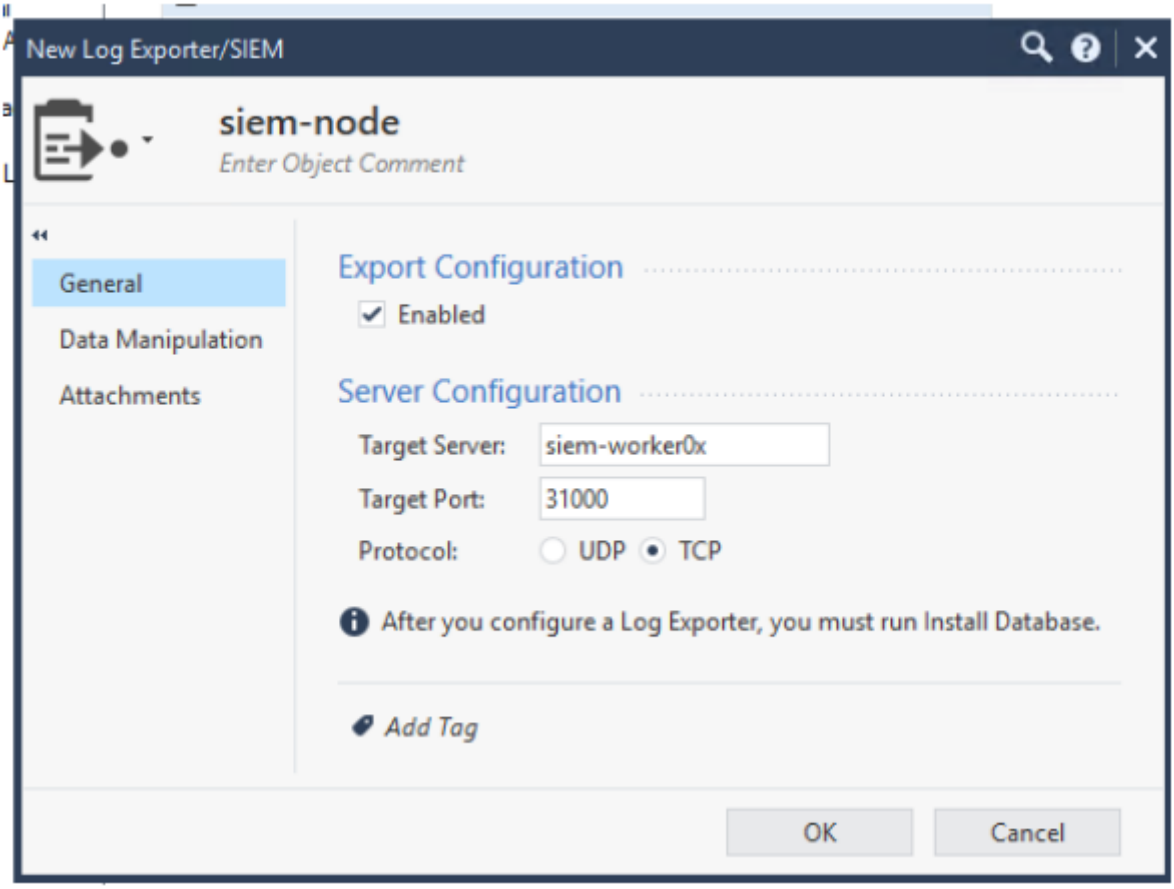
   Нажмите кнопку **Add New** (+), затем выберите восьмиконечную звезду ✳ → **New Log Exporter / SIEM**.



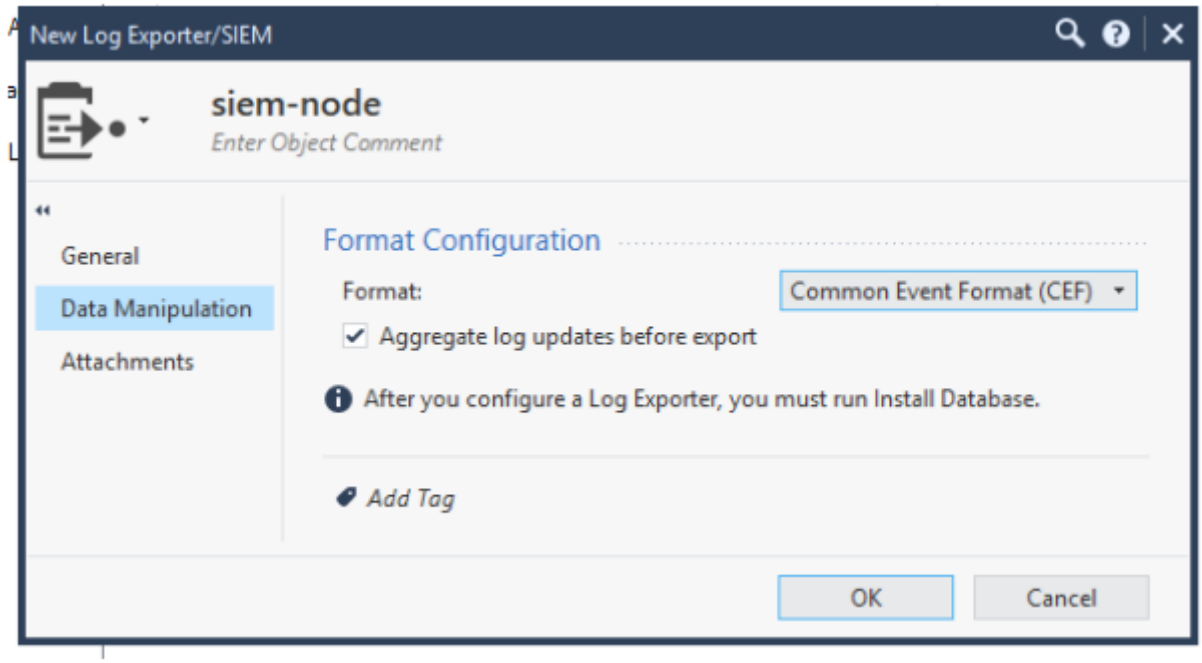
5. **Конфигурация подключения к SIEM**

   Заполните параметры экспорта:

   - **Name**: введите произвольное имя экспортера (например, `R-Vision-SIEM`).
   - **Target**: укажите IP-адрес и порт принимающего коллектора R-Vision SIEM.
   - **Protocol**: выберите `TCP` или `UDP` (в зависимости от настроек точки входа в SIEM).



- **Data Manipulation** → **Format**: выберите `CEF` (Common Event Format).



6. **Завершение настройки**

Нажмите **OK** для сохранения конфигурации. Для применения изменений выполните установку политик (**Install Policy**) на шлюзах безопасности.



После установки политик экспорт событий начнётся автоматически. Первые события появятся в SIEM в течение нескольких минут. Рекомендуется проверить

доставку логов с помощью встроенного мониторинга или инструментов отладки на стороне шлюза (например, `fw log`).

Настройка в R-Vision SIEM

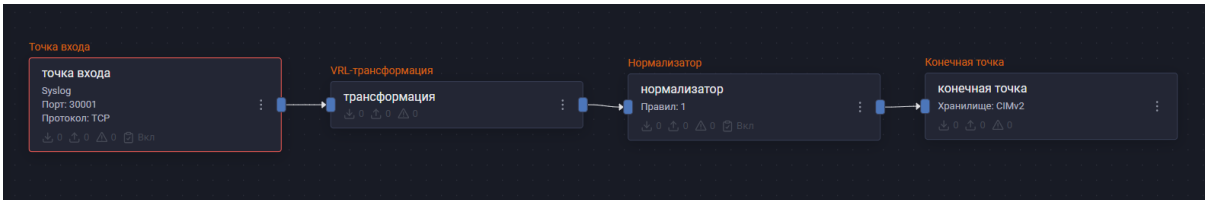
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - **Название**: введите название точки входа.
   - **Тип точки входа**: выберите вариант **Syslog**.
   - **Порт точки входа**: введите значение в соответствии с настройками на стороне Check Point Gaia.
   - **Протокол**: выберите вариант в соответствии с настройками на стороне Check Point Gaia.
3. Добавьте на конвейер элемент **VRL-трансформация** со следующим кодом:

```
.hostname = "<your_device_hostname>"
```

4. Соедините добавленную точку входа и VRL-трансформацию.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **Check Point Gaia** (идентификатор правила: **RV-N-301**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

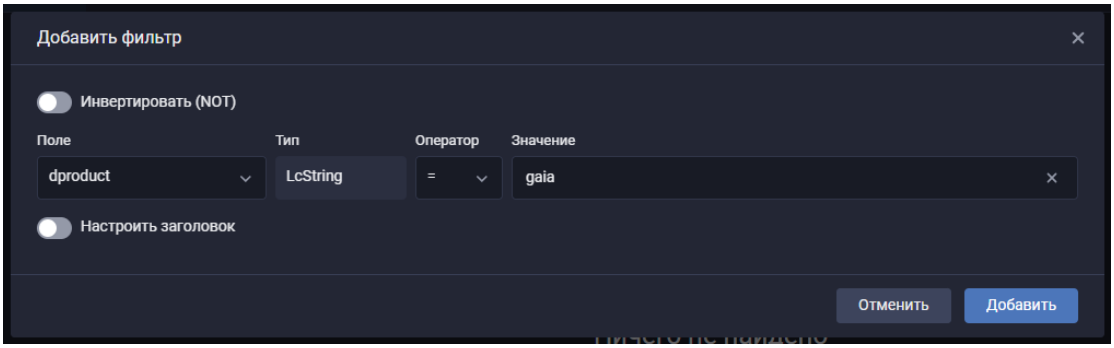


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Check Point Gaia.



Найти события в хранилище можно по следующему фильтру:

```
device_product = "gaia"
```



Cisco ASA

- Cisco ASA: настройка источника
- Cisco ASA: правила корреляции

Cisco ASA: настройка источника

Данное руководство описывает процесс настройки отправки событий межсетевого экрана Cisco ASA в R-Vision SIEM.

Настройка Cisco ASA

Настройте передачу событий по **syslog**. Для этого в режиме конфигурации терминала выполните следующие действия:

1. Включите логирование командой:

   ```
   ciscoasa(config)# logging enable
   ```

2. Настройте добавление hostname в сообщение syslog командой:

   ```
   ciscoasa(config)# logging device-id hostname
   ```

3. Укажите интерфейс, адрес коллектора SIEM, протокол и порт:

   ```
   ciscoasa(config)# logging host <iface> <target> <protocol>/<port>
   ```

   Здесь:

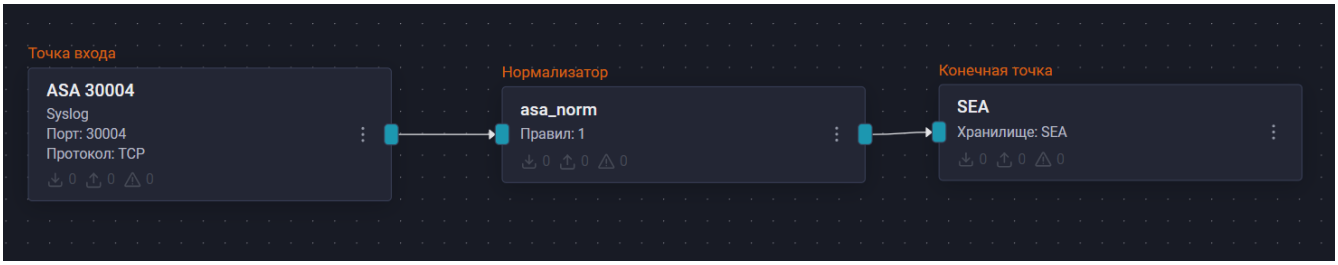
   - `<iface>` — интерфейс, через который будут отправляться события.
   - `<target>` — IP-адрес коллектора SIEM.
   - `<port>` — порт точки входа Syslog в конвейере SIEM.
   - `<protocol>` — сетевой протокол: `tcp` или `udp`.

Настройка в R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие действия:

1. В интерфейсе R-Vision SIEM перейдите в раздел **Ресурсы** → **Коллекторы** и откройте карточку коллектора.
2. На вкладке **Обогащение** добавьте таблицу обогащения **cisco_asa_categorization** (идентификатор таблицы: **RV-ET-29**).
3. В том же коллекторе создайте новый конвейер.
4. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Тип точки входа: Syslog;
   - Порт точки входа и протокол: в соответствии с настройками на стороне Cisco ASA.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **Cisco ASA** (идентификатор правила: **RV-N-197**).
6. Соедините нормализатор с точкой входа.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

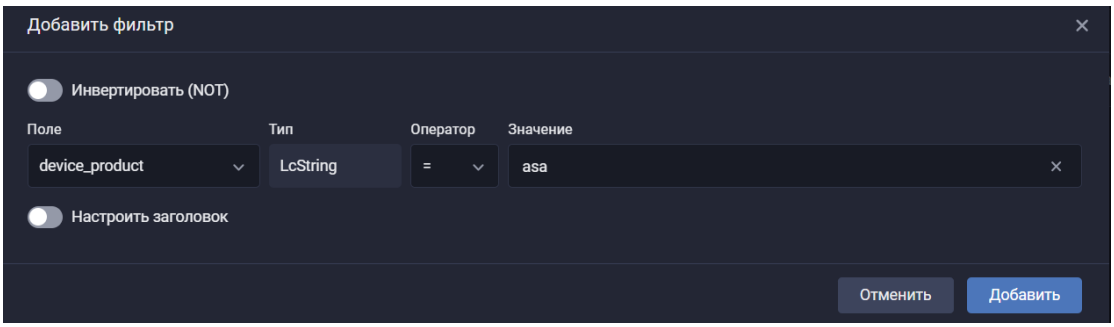
Пример конфигурации конвейера:



Если настройка выполнена корректно, после настройки передачи событий в хранилище начнут поступать события Cisco ASA.

Найти события Cisco ASA в хранилище можно по следующему фильтру:

```
device_product = "asa"
```



Cisco ASA: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1531	Успешный подбор пароля через SSH к Cisco ASA	Правило обнаруживает успешную попытку входа по SSH после нескольких неудачных попыток подключения.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)
RV-D-1532	Успешный подбор пароля в привилегированный режим Cisco ASA	Правило обнаруживает успешную попытку входа в административный режим после нескольких неудачных попыток подключения.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)
RV-D-1533	Подбор пароля через SSH к Cisco ASA	Правило обнаруживает потенциальный перебор учетных записей на устройстве по SSH.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001) • Password Spraying (T1110.003)
RV-D-1531	Успешный подбор пароля через SSH к Cisco ASA	Правило обнаруживает успешную попытку входа по SSH после нескольких неудачных попыток подключения.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1532	Успешный подбор пароля в привилегированный режим Cisco ASA	Правило обнаруживает успешную попытку входа в административный режим после нескольких неудачных попыток подключения.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)
RV-D-1533	Подбор пароля через SSH к Cisco ASA	Правило обнаруживает потенциальный перебор учетных записей на устройстве по SSH.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001) • Password Spraying (T1110.003)
RV-D-1607	Множественное выполнение команды show	Правило направлено на обнаружение потенциальной разведки локальных конфигураций и подключений Cisco ASA при помощи выполнения множества команд "show" от имени одного пользователя за короткий период времени.	• Discovery (TA0007) • System Network Configuration Discovery (T1016)
RV-D-1609	Изменение правил ACL на Cisco ASA	Правило обнаруживает выполнение команд на Cisco ASA, направленных на изменение конфигурации или установленных правил Access List и их применение в Access Groups.	• Lateral Movement (TA0008) • Command and Control (TA0011) • Command and Scripting Interpreter (T1059) • Network Device CLI (T1059.008)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1611	Потенциальная атака DoS на Cisco ASA	Правило предназначено для выявления более чем 2000 попыток подключения в течение минуты к одному внутреннему узлу. Подобная активность может свидетельствовать о проведении DDoS-атаки. При обнаружении инцидента необходимо оперативно связаться с сетевыми администраторами для блокировки адреса инициатора соединений.	• Impact (TA0040) • Network Denial of Service (T1498)

Ideco NGFW

- Ideco NGFW: настройка источника

Ideco NGFW: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Ideco NGFW в R-Vision SIEM.

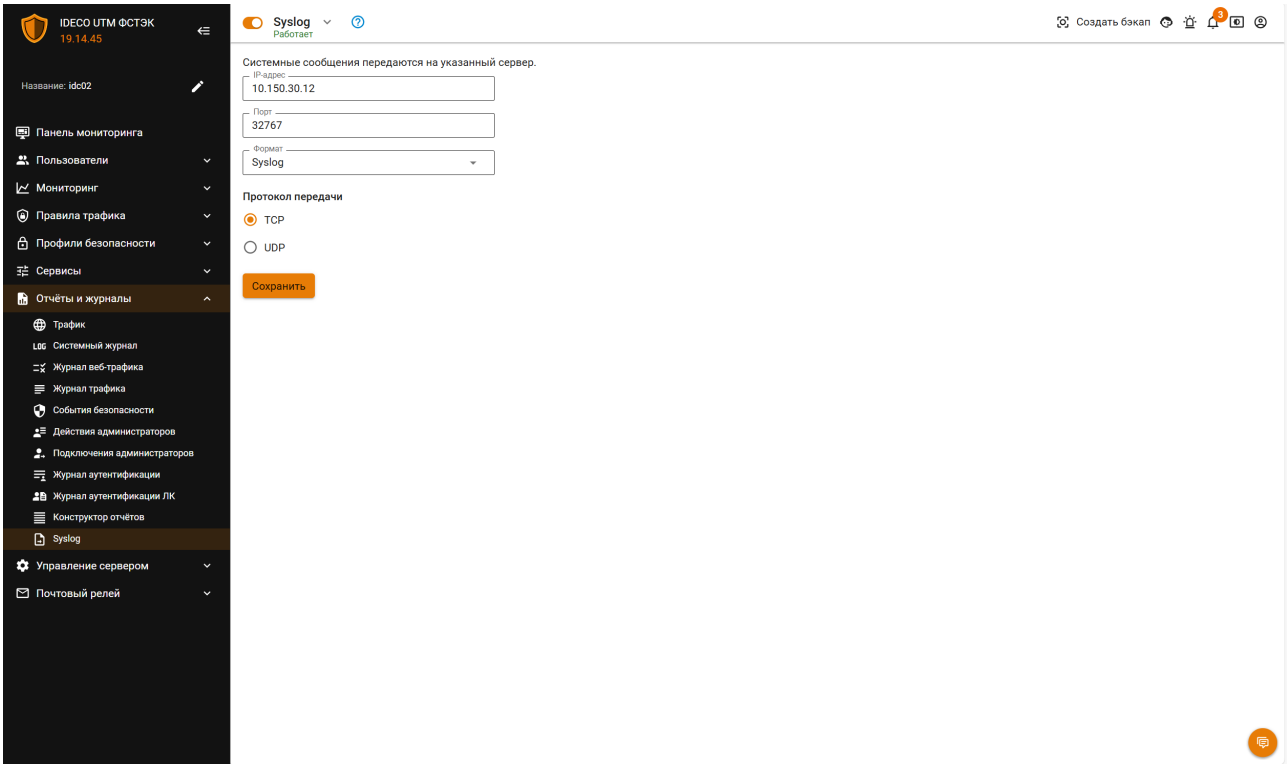
Предварительные требования

Необходима сетевая доступность между Ideco NGFW и коллектором R-Vision SIEM.

Настройка Ideco NGFW

Для пересылки событий, зарегистрированных Ideco NGFW, в R-Vision SIEM по протоколу Syslog:

1. Авторизуйтесь в веб-интерфейсе панели администрирования Ideco NGFW.
2. Перейдите в раздел **Отчёты и журналы** → **Syslog**
3. В открывшемся разделе введите данные коллектора R-Vision SIEM:
   - **IP-адрес**: введите IP-адрес коллектора.
   - **Порт**: введите порт коллектора, на который планируется отправлять события.
   - **Формат**: выберите из выпадающего списка значение **Syslog**.
   - **Протокол передачи**: выберите вариант **TCP** или **UDP**.
4. В верхнем левом углу переведите переключатель **Syslog** в активное положение.



5. Нажмите на кнопку **Сохранить**.

Настройка Ideco NGFW завершена.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

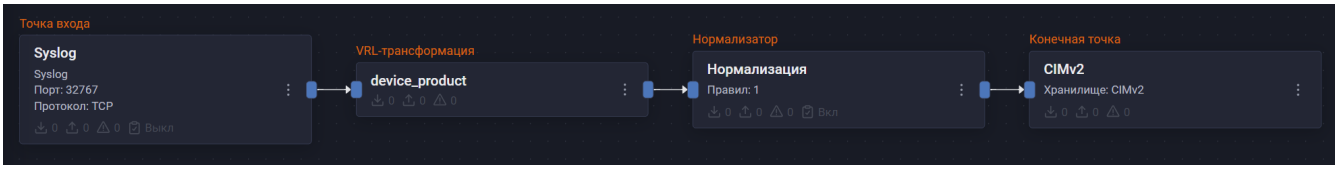
1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в диапазоне 30000—32767.
   - Протокол: выберите вариант в соответствии с настройками на стороне промежуточного syslog-сервера.
3. Добавьте на конвейер элемент **VRL-трансформация** со следующим содержимым:

```
.device_vendor = "ideco"
.device_product = "ngfw"
```

4. Соедините VRL-трансформацию с точкой входа.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **Ideco NGFW** (идентификатор правила: **RV-N-296**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.

8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

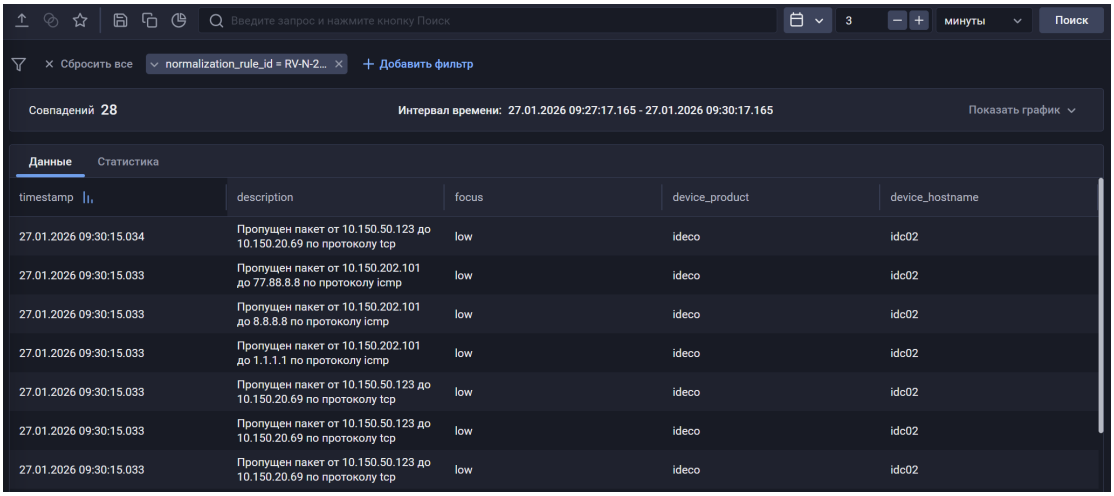


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Ideco NGFW.



Найти события Ideco NGFW в хранилище можно по следующему фильтру:

```
normalization_rule_id = "RV-N-296"
```



ИнфоТеКС ViPNet Coordinator 4

- ИнфоТеКС ViPNet Coordinator 4: настройка источника

ИнфоТеКС ViPNet Coordinator 4: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий ViPNet Coordinator 4 в R-Vision SIEM.

Предварительные требования

Необходим промежуточный syslog-сервер, выделенный под передачу событий из ViPNet Coordinator 4, который будет перенаправлять события в R-Vision SIEM. Данная необходимость обусловлена ограничением со стороны ViPNet Coordinator 4 по портам доставки Syslog (514) для системных событий аудита.

Настройка ViPNet Coordinator 4

Для настройки отправки событий ViPNet Coordinator 4 в SIEM-систему в формате syslog выполните следующие действия:

1. Войдите в интерфейс командной строки ViPNet Coordinator.
2. Перейдите в режим администратора:

   ```
   enable
   ```

3. Укажите целевой IP-адрес для отправки событий с помощью команды:

   ```
   machine set loghost <IP-адрес syslog-сервера>
   ```

   где `<IP-адрес syslog-сервера>` — адрес промежуточного syslog-сервера, в рамках которого планируется осуществлять сбор событий ViPNet Coordinator 4.

4. Остановите работу службы iplir:

   ```
   iplir stop
   ```

5. Откройте файл конфигурации службы iplir:

   ```
   iplir config
   ```

6. В секции `misc` введите следующие значения:

   ```
   cef_ip = <IP-адрес>
   cef_port = 514
   cef_format= xf
   cef_enabled = yes
   ```

   где `<IP-адрес>` — адрес промежуточного syslog-сервера, с помощью которого планируется осуществлять сбор событий ViPNet Coordinator 4.

7. Сохраните изменения.
8. Закройте файл.
9. Откройте конфигурацию интерфейса, с которого необходимо получать события о трафике:

   ```
   iplir config eth<номер интерфейса>
   ```

10. В конфигурации интерфейса укажите следующие значения:

```
[db]
maxsize= 50 MBytes
timedif= 60
registerall= on  # Значение по умолчанию - off.
registerbroadcast= off
omittcpclientport= off
registerevents= on

[cef]
# Для регистрации всех событий - значение all.
# Для регистрации заблокированных пакетов - значение blocked.
event= all
```

11. Сохраните изменения с помощью сочетания клавиш CTRL+O.
12. Закройте файл.
13. Включите службу iplir:

```
iplir start
```

14. Добавьте правило фильтрации:

```
firewall local add 3 rule "Allow Syslog" src @local dst <IP-адрес коллектора> udp
dport <Порт коллектора> pass
```

Настройка отправки событий ViPNet Coordinator 4 завершена.

Настройка промежуточного syslog-сервера на примере rsyslog



ViPNet Coordinator 4 отправляет системные события на порт со значением 514 по протоколу udp.

Алгоритм настройки syslog-сервера следующий следующий:

1. Создайте и откройте файл конфигурации rsyslog в директории `/etc/rsyslog.d/`:

```
sudo nano /etc/rsyslog.d/40-vipnet-hw.conf
```

2. Скопируйте в файл конфигурации следующие строки:

```
module(load="imtcp")
input(type="imtcp" port="514")
module(load="imudp")
input(type="imudp" port="514")

if $fromhost-ip == '<ip ViPNet Coordinator 4>' then {
```

```
  action(
    type="omfwd"
    target="<ip R-Vision SIEM>"
    port="<port>"
    protocol="<proto>"
  )
  stop
}
```

Здесь:

- `<ip ViPNet Coordinator 4>` — адрес интерфейса ViPNet Coordinator 4, с которого будут отправляться события.
- `<ip R-Vision SIEM>` — адрес коллектора R-Vision SIEM.
- `<port>` — порт приема событий, указанный в R-Vision SIEM.
- `<proto>` — протокол передачи.

3. Сохраните конфигурацию.
4. Перезагрузите службу rsyslog:

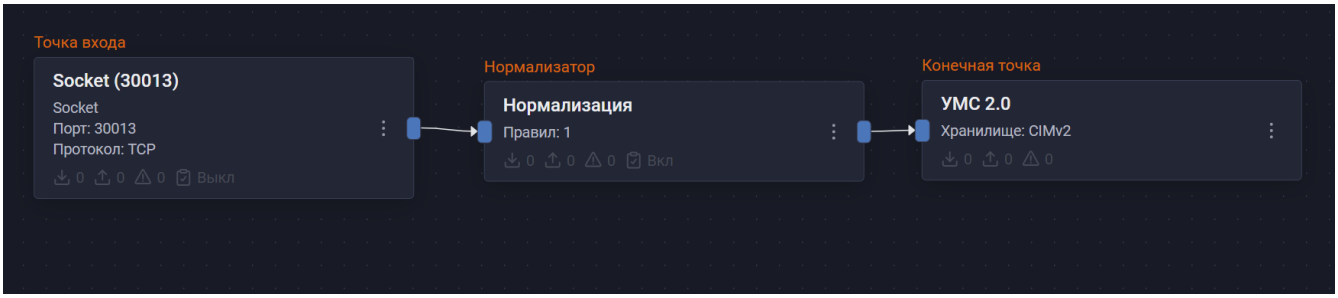
```
sudo systemctl restart rsyslog
```

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM перейдите в раздел **Ресурсы** → **Коллекторы** и откройте карточку коллектора.
2. На вкладке **Обогащение** добавьте таблицу обогащения коллектора **hw_fw_events**.
3. В том же коллекторе создайте новый конвейер.
4. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в диапазоне 30000—32767.
   - Протокол: выберите вариант в соответствии с настройками на стороне промежуточного syslog-сервера.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **ViPNet Coordinator 4** (идентификатор правила: **RV-N-329**).
6. Соедините нормализатор с точкой входа.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

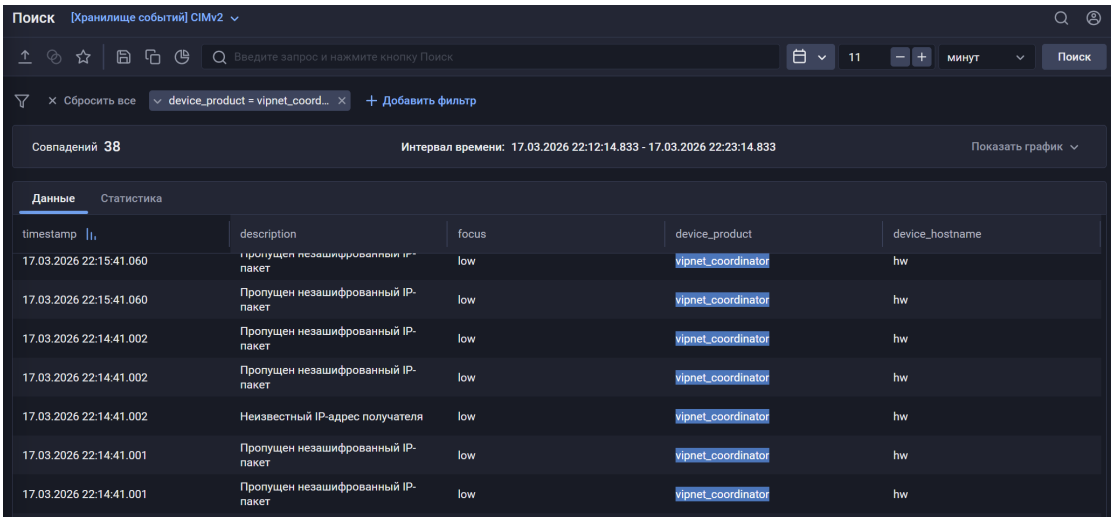
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события ViPNet Coordinator 4.

Найти события ViPNet Coordinator 4 в хранилище можно по следующему фильтру:

```
device_product = "vipnet_coordinator"
```



Код Безопасности Континент 3.9.3

- Код Безопасности Континент 3.9.3: настройка источника

Код Безопасности Континент 3.9.3: настройка источника

Данное руководство описывает процесс настройки передачи событий аппаратно-программного комплекса шифрования (АПКШ) Континент 3 в R-Vision SIEM посредством syslog.

Функционал передачи событий во внешние системы через Syslog имеется в версии Континент 3.9.3

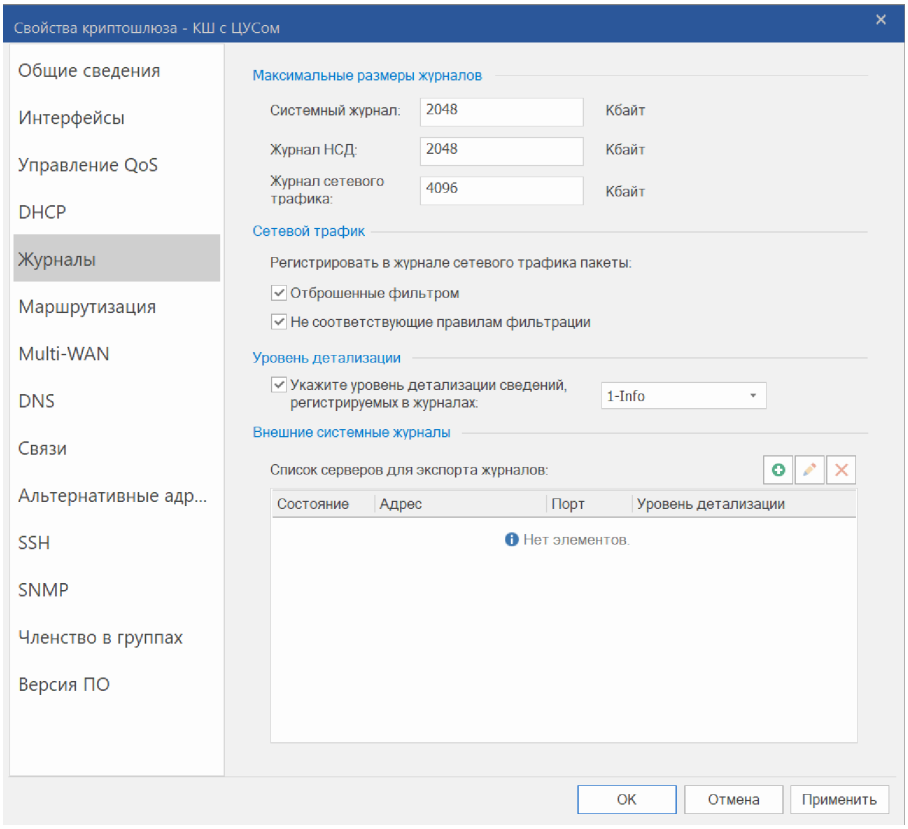
Настройка Континент 3.9.3

Для настройки syslog на АПКШ Континент 3.9.3 выполните следующие шаги:

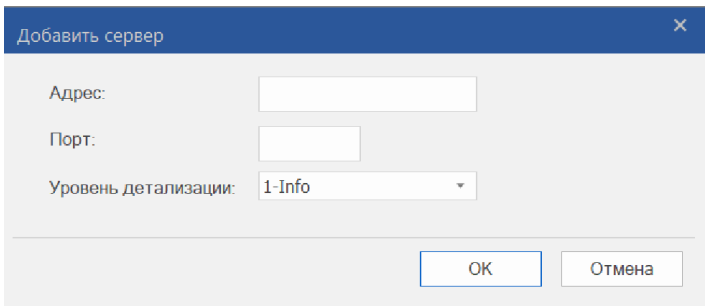
1. Подключитесь к центру управления сетью с помощью ПО "Программа Управления ЦУС"

(сокращенно ПУ ЦУС).

2. Откройте вкладку **Криптошлюзы**.
3. Выберите криптошлюз (далее — КШ), с которого необходимо отправлять события в SIEM.
4. Вызовите контекстное меню для КШ и выберите пункт **Свойства**. Откроется меню настроек КШ.
5. Откройте вкладку **Журналы**.
6. В разделе **Внешние системные журналы** нажмите на кнопку .



7. В открывшемся окне заполните поля:
   - Адрес: укажите адрес коллектора R-Vision SIEM.
   - Порт: укажите порт точки входа на конвейере.
   - Уровень детализации: выберите вариант `1 Info`.



8. Нажмите на кнопку **ОК**.
9. Нажмите на кнопку **Применить**.

Настройка Континент 3.9.3 завершена.

Настройка в R-Vision SIEM

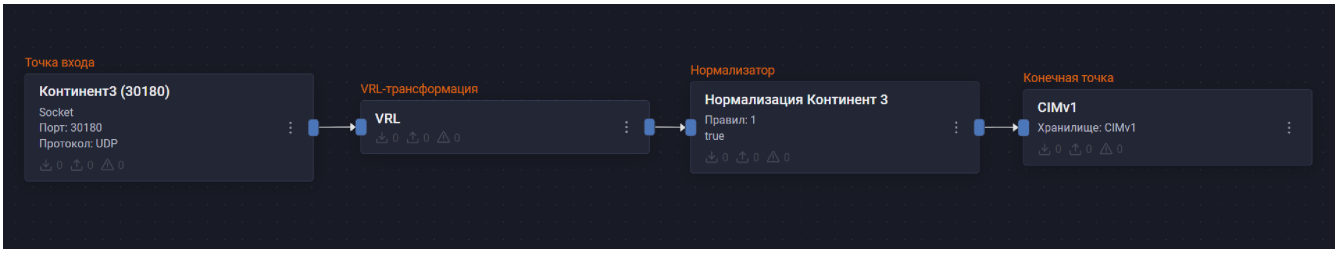
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Socket**.
   - Порт точки входа: введите значение в диапазоне 30000—32767.
   - Протокол: выберите вариант в соответствии с настройками на стороне Континент 3.9.3.
3. Добавьте VRL-трансформацию со следующим содержимым:

```
.device_product = "kontinent"
```

4. Соедините добавленную точку входа и VRL-трансформацию.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **Код Безопасности Континент 3.9.3** (идентификатор правила: **RV-N-266**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

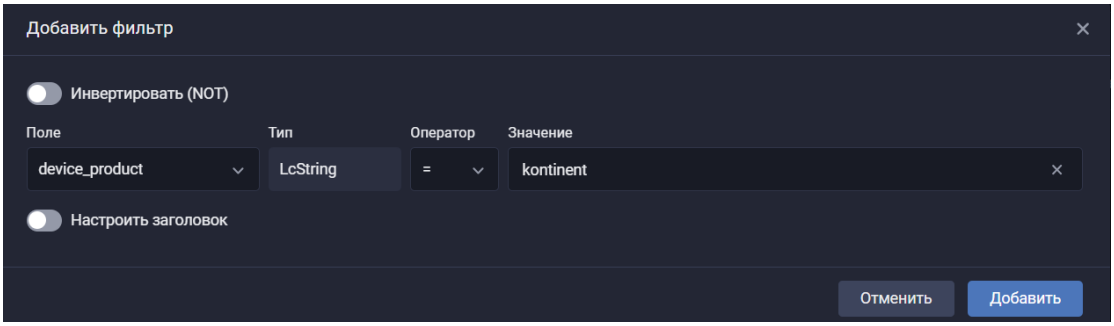
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события из Континент 3.9.3.

Найти события Континент 3.9.3 в хранилище можно по следующему фильтру:

```
device_product = "kontinent"
```



Код Безопасности Континент 4

- Код Безопасности Континент 4: настройка источника PostgreSQL
- Код Безопасности Континент 4: настройка источника Syslog
- Код Безопасности Континент 4: правила корреляции

Код Безопасности Континент 4: настройка источника PostgreSQL

Данное руководство описывает процесс настройки сбора и отправки событий аппаратно-программного комплекса шифрования (АПКШ) Континент 4 в R-Vision SIEM посредством PostgreSQL.

Предварительные требования

Необходима внешняя БД PostgreSQL для хранения событий Континент 4 и их последующей передачи в R-Vision SIEM.

Настройка СУБД PostgreSQL

Для создания БД в PostgreSQL подключитесь к СУБД от имени пользователя, имеющего права администратора СУБД. Дальнейший алгоритм настройки:

1. Создайте Администратора будущей БД. Данная запись потребуется для записи событий в БД:

   ```
   CREATE USER root WITH PASSWORD 'password';
   ```

2. Создайте БД `kontinent`, администратором которой будет созданный на предыдущем шаге пользователь:

   ```
   CREATE DATABASE kontinent OWNER root;
   ```

3. Создайте пользователя для чтения таблиц БД `kontinent`:

   ```
   CREATE USER reader WITH PASSWORD 'password';
   ```

4. Подключитесь к БД `kontinent`:

```
\c kontinent
```



Данная команда работает, если настройка производится через клиент psql. Если вы проводите настройку с помощью другого внешнего клиента, то создайте новое подключение к СУБД с указанием БД `kontinent`.

5. Предоставьте права на подключение к БД пользователю `reader`:

```
GRANT CONNECT ON DATABASE kontinent TO reader;
```

6. Установите права пользователя `reader` по умолчанию для таблиц, которые будут создаваться пользователем `root`:

```
ALTER DEFAULT PRIVILEGES FOR USER root IN SCHEMA public
GRANT SELECT ON TABLES TO reader;
```

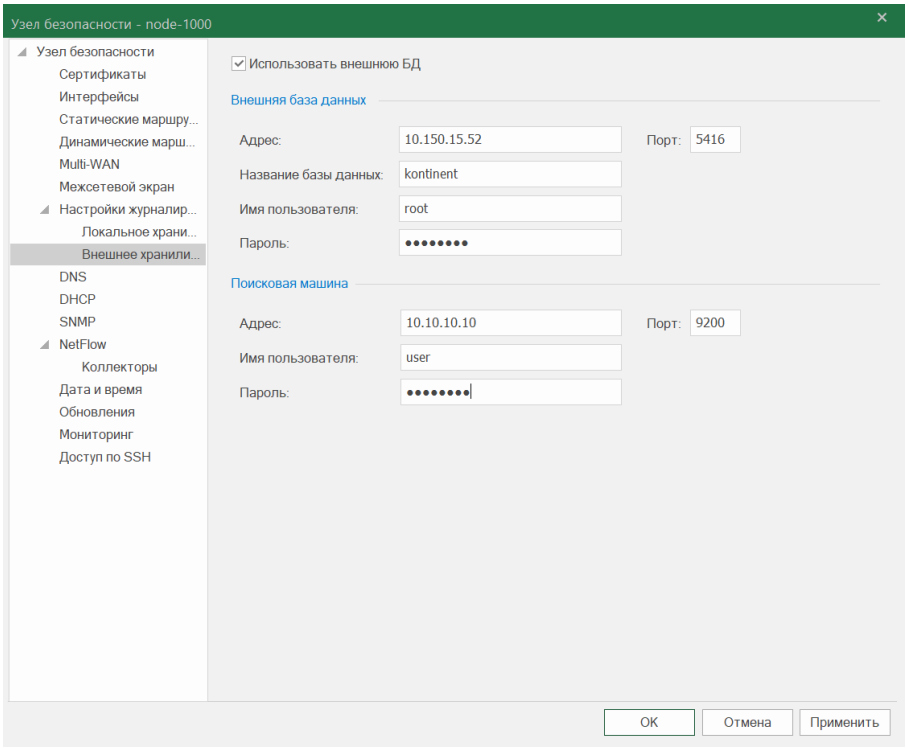
Настройка PostgeSQL завершена.

Настройка Континент 4

Для настройки отправки событий во внешнюю СУБД PostgreSQL на АПКШ Континент 4 выполните следующие шаги:

1. Подключитесь к центру управления сетью (далее — ЦУС) с помощью ПО "Континент. Менеджер конфигурации".
2. Откройте вкладку **Структура**.
3. Выберите узел безопасности (далее — УБ), с которого необходимо отправлять события в SIEM.
4. Вызовите контекстное меню для УБ и выберите пункт **Свойства**. Откроется меню настроек УБ.
5. Откройте вкладку **Настройки журналирования** → **Внешнее хранилище**.
6. Для параметра **Детализация** задайте значение **Высокий**.
7. Нажмите на кнопку добавления внешнего системного журнала.
8. Заполните параметры для блока **Внешняя база данных**:
   - Адрес: введите IP-адрес СУБД.
   - Порт: введите значение порта, прослушиваемого сервером СУБД.
   - Название базы данных: введите имя БД, подготовленной для записи событий Континент 4.
   - Имя пользователя: введите имя пользователя с правами на запись в БД.
   - Пароль: введите пароль пользователя.
9. Блок **Поисковая машина** заполните любыми данными.

   Настройки журналирования должны выглядеть следующим образом:



10. Нажмите на кнопку **Применить**.
11. Нажмите на кнопку **ОК**.
12. Отправьте конфигурацию на УБ. Для этого:
    a. В главном меню нажмите на кнопку .
    b. Отметьте УБ, для которого настраивалось внешнее журналирование.
    c. Нажмите на кнопку **ОК**.

Настройка на стороне АПКШ Континент 4 завершена.

Настройка в R-Vision SIEM

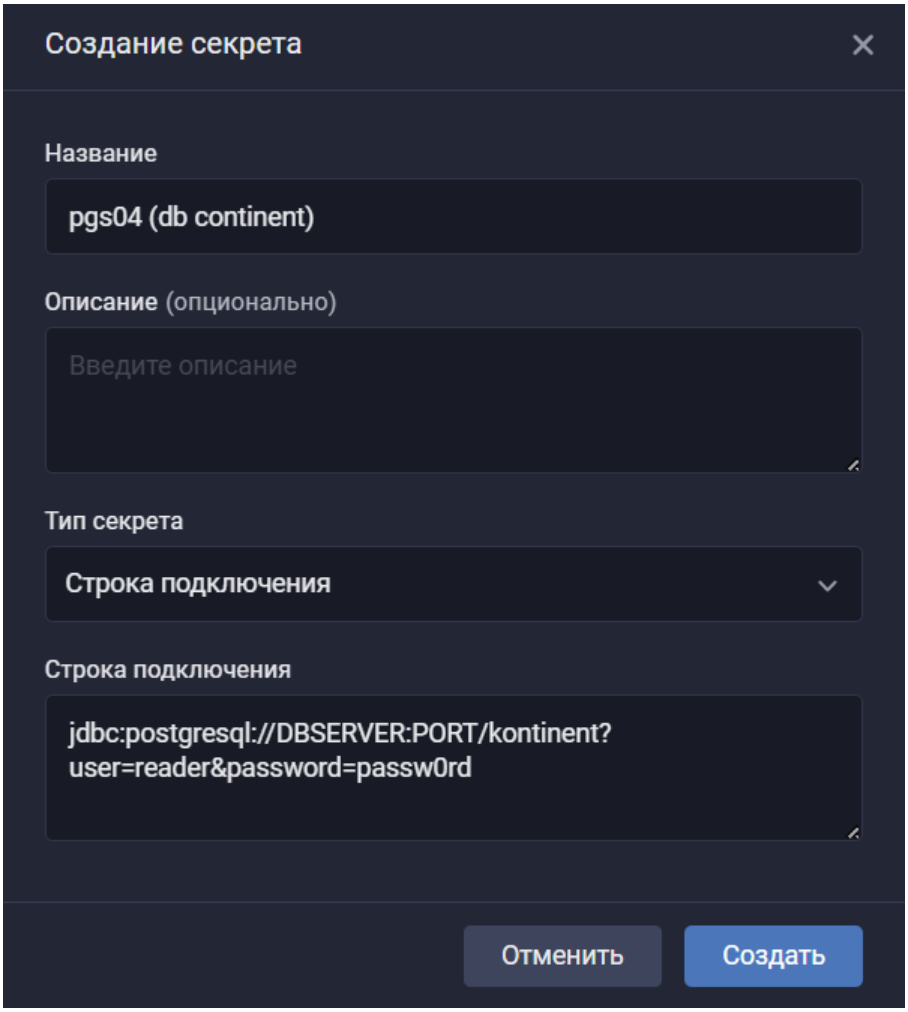
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте секрет со строкой подключения. Для этого:
    a. Перейдите в раздел **Ресурсы** → **Секреты**.
    b. Нажмите на кнопку **Создать** (+).
    c. В раскрывшемся окне создания секрета заполните поля:
        - Название: введите название секрета.
        - Описание (опционально): опишите, для чего будет использоваться секрет.
        - Тип секрета: выберите вариант **Строка подключения**.
        - Строка подключения: введите строку вида:

```
jdbc:postgresql://DBSERVER:PORT/kontinent?user=reader&password=passw0rd
```

Здесь:

- DBSERVER — FQDN или IP-адрес сервера с СУБД.
- PORT — порт, прослушиваемый СУБД.



d. Нажмите на кнопку **Создать**.

2. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
3. Далее необходимо добавить три элемента типа **Точка входа**:
   a. Точка входа для сбора событий аудита:
      - Название: введите название точки входа.
      - Тип точки входа: выберите вариант **Database**.
      - Драйвер базы данных: выберите вариант PostgreSQL.
      - Адрес подключения: выберите секрет, созданный ранее.
      - SQL-запрос: введите запрос вида:

```
SELECT
    id
    ,timestamp
    ,timestamp_str
    ,hostname
```

```
    ,syslogfacility
    ,syslogseverity
    ,sourcename
    ,message
    ,msgrepeatcount
    ,hwserial
    ,additional
    ,'Journal_1' AS sourceservicename
    ,'Kontinent 4' as appname
FROM public.log
WHERE id > CAST(? AS BIGINT)
ORDER BY id ASC LIMIT 10000;
```

- Поле идентификатора: введите ключ `id` со значением `1`.
- Интервал запроса, секунд: введите значение `15`.

b. Точка входа для сбора событий фильтрации:

- Название: введите название точки входа.
- Тип точки входа: выберите вариант **Database**.
- Драйвер базы данных: выберите вариант PostgreSQL.
- Адрес подключения: выберите секрет, созданный ранее.
- SQL-запрос: введите запрос вида:

```
SELECT
    id
    ,timestamp
    ,timestamp_str
    ,sensor_id
    ,event_type, src_ip
    ,src_port, dest_ip
    ,dest_port
    ,proto
    ,in_iface
    ,action
    ,signature_id
    ,signature
    ,category
    ,severity
    ,payload
    ,packet
    ,msgrepeatcount
    ,dest_domain
    ,revision
    ,signature_body
    ,sourcename
    ,hostname
    ,dest_country
    ,src_country
```

```
    ,username
    ,vrf
    ,'Journal_2' AS sourceservicename
    ,'Kontinent 4' as appname
FROM public.ids_log
WHERE id > CAST(? AS BIGINT)
ORDER BY id ASC LIMIT 10000;
```

- Поле идентификатора: введите ключ `id` со значением `1`.
- Интервал запроса, секунд: введите значение `15`.

c. Точка входа для сбора событий управления конфигурацией:

- Название: введите название точки входа.
- Тип точки входа: выберите вариант **Database**.
- Драйвер базы данных: выберите вариант PostgreSQL.
- Адрес подключения: выберите секрет, созданный ранее.
- SQL-запрос: введите запрос вида:

```
SELECT
    id
    ,timestamp
    ,timestamp_str
    ,hostname
    ,syslogseverity
    ,category
    ,subject
    ,action
    ,hwserial
    ,sourcename
    ,'Journal_3' AS sourceservicename
    ,'Kontinent 4' as appname
FROM public.management_log
WHERE id > CAST(? AS BIGINT)
ORDER BY id ASC LIMIT 10000;
```



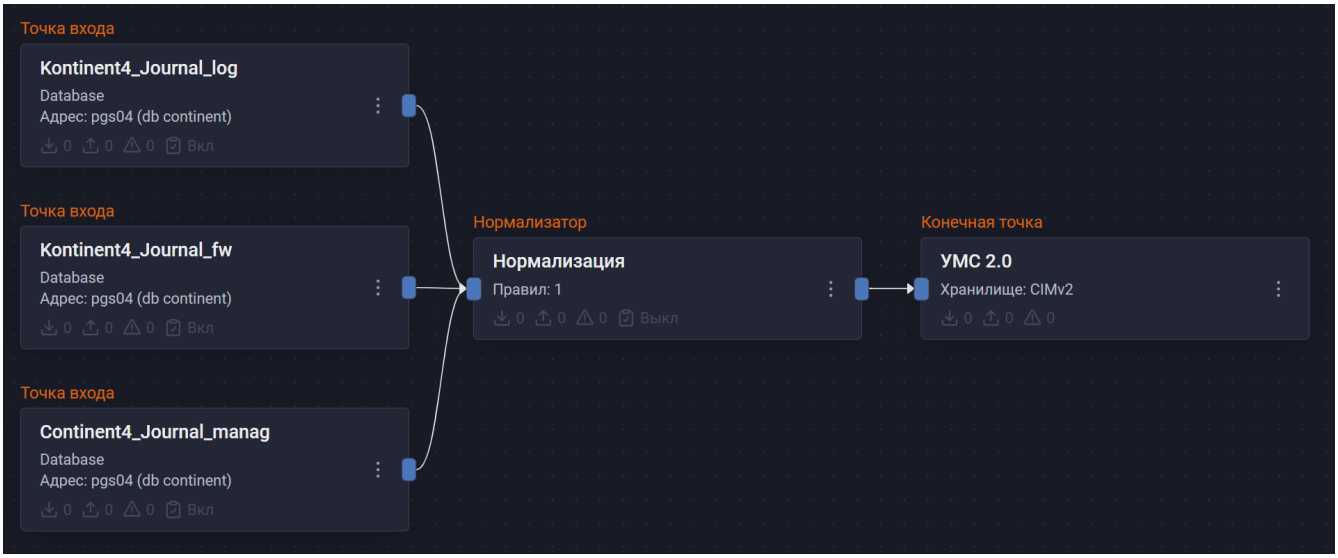
При большом количестве событий в СУБД рекомендуется добавлять `LIMIT 10000` в конец SQL-запроса.

- Поле идентификатора: введите ключ `id` со значением `1`.
- Интервал запроса, секунд: введите значение `15`.

4. Добавьте на конвейер элемент **Нормализатор** с правилом **Код Безопасности Континент 4 БД** (идентификатор правила: **RV-N-276**).
5. Соедините нормализатор с точками входа.
6. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.

7. Соедините конечную точку с нормализатором.
8. Сохраните и установите конфигурацию конвейера.

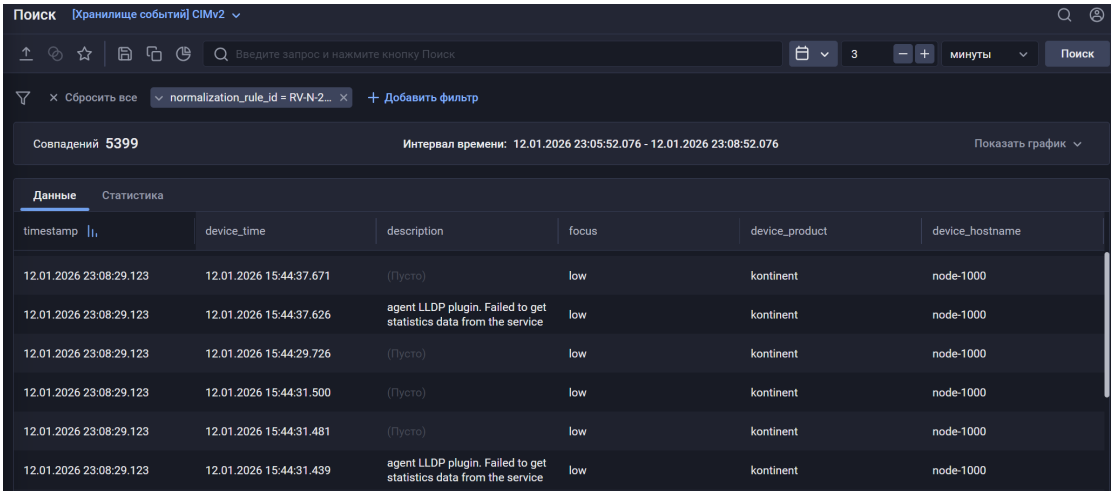
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Континент 4.

Найти события Континент 4 в хранилище можно по следующему фильтру:

```
normalization_rule_id = "RV-N-276"
```



Код Безопасности Континент 4: настройка источника Syslog

Данное руководство описывает процесс настройки сбора и отправки событий аппаратно-программного комплекса шифрования (АПКШ) Континент 4 в R-Vision SIEM посредством Syslog.

Настройка Континент 4

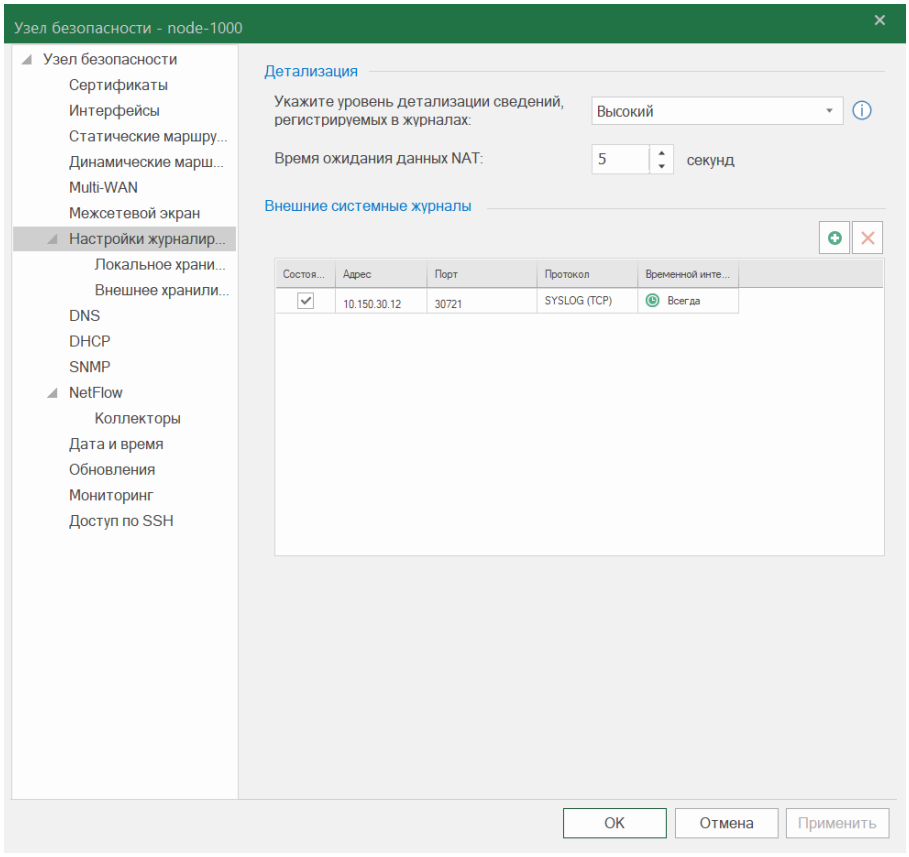
Система позволяет отправлять события аудита во внешние системы посредством Syslog. Для передачи функциональных событий АПКШ Континент 4 во внешние

системы можно воспользоваться вынесенной СУБД Postgres.

Для настройки Syslog на АПКШ Континент 4 выполните следующие шаги:

1. Подключитесь к центру управления сетью (далее — ЦУС) с помощью ПО "Континент. Менеджер конфигурации".
2. Откройте вкладку **Структура**.
3. Выберите узел безопасности (далее — УБ), с которого необходимо отправлять события в SIEM.
4. Вызовите контекстное меню для УБ и выберите пункт **Свойства**. Откроется меню настроек УБ.
5. Откройте вкладку **Настройки журналирования**.
6. Для параметра **Детализация** задайте значение **Высокий**.
7. Нажмите на кнопку добавления внешнего системного журнала.
8. Заполните следующие параметры:
   - Адрес: введите IP-адрес коллектора SIEM или syslog-сервера, через который будут передаваться данные в SIEM.
   - Порт: введите значение порта, который планируется прослушивать.
   - Протокол: введите требуемый протокол.
   - Временной интервал: выберите вариант **Всегда**.

   Настройки журналирования должны выглядеть следующим образом:



9. Нажмите на кнопку **Применить**.
10. Нажмите на кнопку **ОК**.

11. Отправьте конфигурацию на УБ. Для этого:
    a. В главном меню нажмите на кнопку .
    b. Отметьте УБ, для которого настраивалось внешнее журналирование.
    c. Нажмите на кнопку **ОК**.

Настройка на стороне АПКШ Континент 4 завершена.

Настройка в R-Vision SIEM

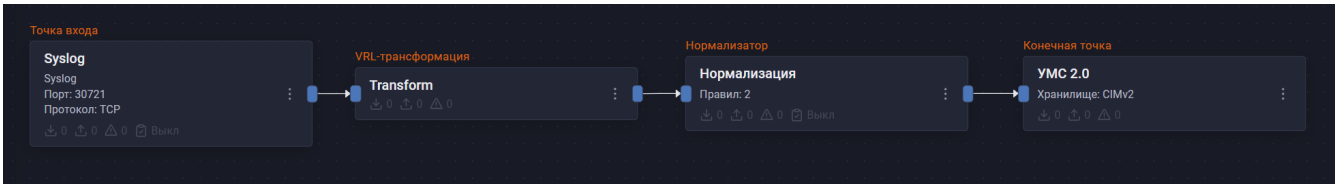
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
    - Название: введите название точки входа.
    - Тип точки входа: выберите вариант **Syslog**.
    - Порт точки входа: введите значение в диапазоне 30000—32767.
    - Протокол: выберите вариант в соответствии с настройками на стороне Континент 4.
3. Добавьте на конвейер элемент **VRL-трансформация** со следующим кодом:

```
.device_product = "kontinent"
.device_version = "4"
```

4. Соедините трансформацию с точкой входа.
5. Добавьте на конвейер элемент **Нормализатор** с правилами **Код Безопасности Континент 4 NXLOG** (идентификатор правила: **RV-N-273**) и **Код Безопасности Континент 4** (идентификатор правила: **RV-N-274**).
6. Соедините нормализатор с трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

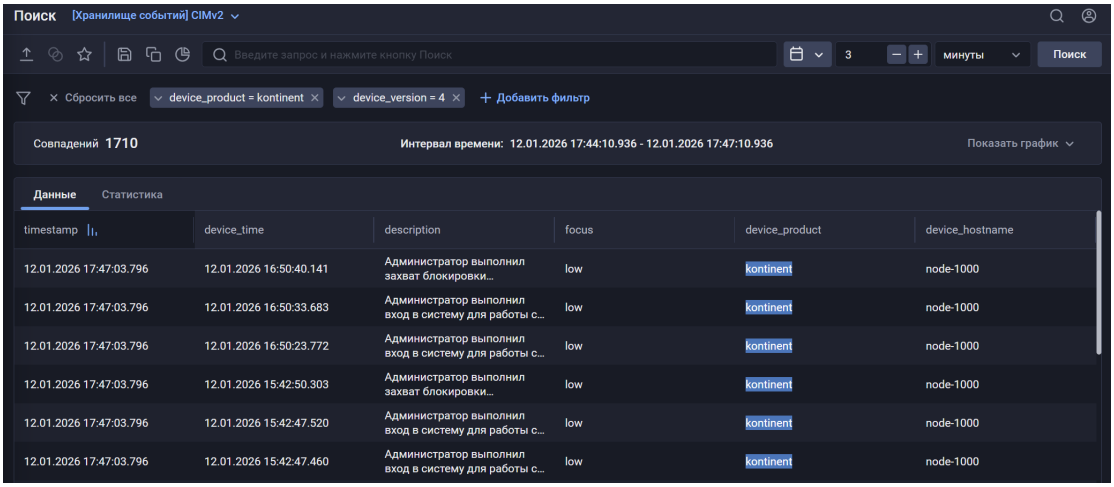


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Континент 4.



Найти события Континент 4 в хранилище можно по следующему фильтру:

```
device_product = "kontinent" and device_version = "4"
```



Код Безопасности Континент 4: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1534	Подбор пароля к серверу Континент TLS	Правило детектирует потенциальный перебор учетных записей на устройстве Континент при входе по SSH через меню локального управления или веб-консоль. В случае возникновения активности необходимо опросить владельца учетной записи инициатора активности о попытках входа с неверными учетными данными. В случае если легитимность подтвердить не удалось, заблокировать учетную запись до выяснений обстоятельств инцидента.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)
RV-D-1541	Успешный подбор пароля к серверу Континент TLS	Правило детектирует потенциальный перебор учетных записей на устройстве с последующим успешным входом по SSH или через меню локального управления.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1545	Вход привилегированного пользователя с неизвестного хоста	Правило детектирует вход на устройство Континент TLS привилегированного пользователя с неизвестного хоста.	• Initial Access (TA0001) • Valid Accounts (T1078) • Local Accounts (T1078.003)
RV-D-1546	Подбор пароля Континент методом Password Spraying	Правило обнаруживает неверные попытки аутентификации с разными учетными записями на одном устройстве в течение пяти минут. В случае возникновения активности необходимо опросить ответственного за хост, инициирующий запросы, о выявленной активности. В случае если легитимность подтвердить не удалось, изолировать хост-источник активности на время выяснения обстоятельств инцидента.	• Credential Access (TA0006) • Brute Force (T1110) • Password Spraying (T1110.003)
RV-D-1601	Добавление пользователя в критическую группу Континент TLS	Правило детектирует событие добавления пользователя в критическую группу на сервере Континент TLS.	• Persistence (TA0003) • Account Manipulation (T1098) • Additional Local or Domain Groups (T1098.007)
RV-D-1602	Изменение административной УЗ Континент TLS	Правило детектирует событие изменения административной учетной записи на сервере Континент TLS.	• Persistence (TA0003) • Account Manipulation (T1098)
RV-D-1604	Изменение правил межсетевого экранирования Континент	Правило детектирует событие изменения правил межсетевого экранирования на сервере Континент.	• Defense Evasion (TA0005)

С-Терра Шлюз

- С-Терра Шлюз: настройка источника Syslog
- С-Терра Шлюз: правила корреляции

С-Терра Шлюз: настройка источника Syslog

Данное руководство описывает процесс настройки сбора и отправки событий программно-аппаратного комплекса С-Терра Шлюз в R-Vision SIEM посредством Syslog.

Настройка С-Терра Шлюз

Для настройки Syslog на С-Терра Шлюз выполните следующие шаги:

1. Откройте Cisco-like консоль источника.
2. Перейдите в режим администрирования.

   ```
   enable
   ```

3. Перейдите в режим конфигурации.

   ```
   configure terminal
   ```

4. Включите логирования и установите необходимый уровень.

   ```
   logging on
   logging trap debugging
   ```

5. Чтобы настроить службу отправки, выполните следующие шаги:
   a. Откройте интерфейс командной строки источника.
   b. Введите следующие команды:

      ```
      log_mgr set-syslog -y enable -a <ip-коллектора SIEM> -f local7
      log_mgr set -l debug
      ```

6. Установите предподготовленные, то есть уже имеющиеся в источнике, конфигурационные файлы логирования:

   ```
   log_mgr set -e /opt/VPNagent/etc/msg_grpCERTS.ini -f
   log_mgr set -e /opt/VPNagent/etc/msg_grpKERNEL.ini -f
   log_mgr set -e /opt/VPNagent/etc/msg_grpLDAP.ini -f
   log_mgr set -e /opt/VPNagent/etc/msg_grpPOLICY.ini -f
   log_mgr set -e /opt/VPNagent/etc/msg_grpSYSTEM.ini -f
   ```

7. Откройте указанный файл:

```
nano /etc/rsyslog.conf
```

8. Добавьте в файл следующую строку:

```
local7.* @<ip-адрес коллектора SIEM>:<Порт>
```

9. Сохраните файл.
10. Перезагрузите службу rsyslog:

```
systemctl restart rsyslog.service
```

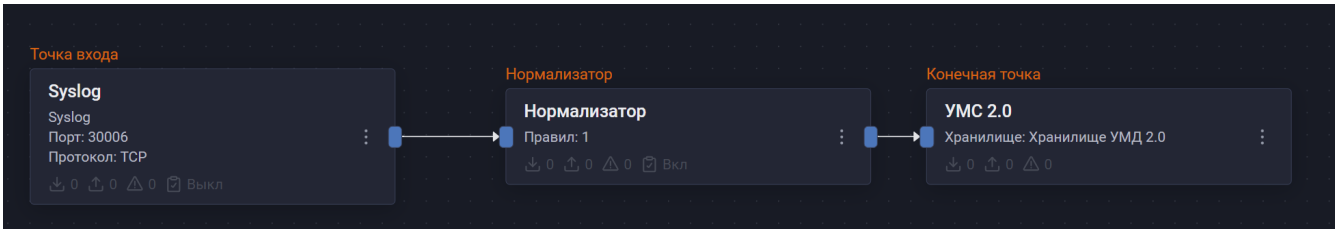
Настройка источника завершена.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в диапазоне 30000—32767.
   - Протокол: выберите вариант в соответствии с настройками на стороне С-Терра Шлюз.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **S-Terra Gate ST** (идентификатор правила: **RV-N-311**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

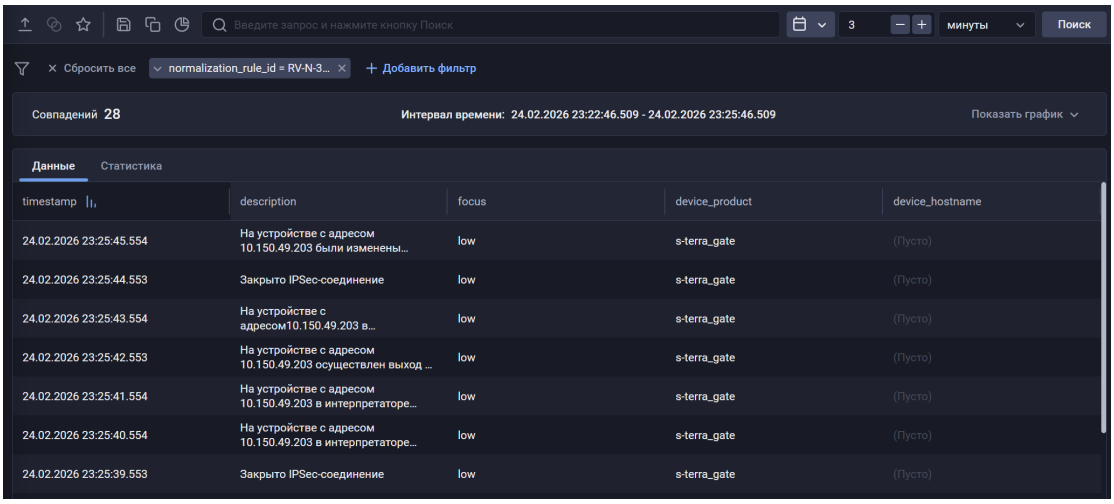


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут

поступать события С-Терра Шлюз.

Найти события С-Терра Шлюз в хранилище можно по следующему фильтру:

```
normalization_rule_id = "RV-N-311"
```



С-Терра Шлюз: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1526	Создан пользователь на S-Terra Gate	Атакующие после получения доступа к системе S-Terra могут создать нового пользователя, таким образом можно временно закрепиться в системе и вносить свои изменения в конфигурацию.	• Persistence (TA0003) • Account Manipulation (T1098) • Create Account (T1136) • Local Account (T1136.001)
RV-D-1527	Отключена отправка событий на S-Terra Gate	После получения доступа к системе S-Terra атакующие могут отключить отправку системных событий на удаленный узел, чтобы скрыть свои дальнейшие вредоносные действия.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1528	Изменен пароль для привилегированного режима	Атакующие после получения доступа к системе S-Terra и внесения изменений могут изменить пароль или секрет для входа в привилегированный режим, таким образом, можно временно закрепиться в системе и вносить свои изменения в конфигурацию, это также не позволит администратору быстро изменить настройки системы.	• Persistence (TA0003) • Account Manipulation (T1098)
RV-D-1529	Очищен файл конфигурации на S-Terra Gate	Атакующие, после получения доступа к системе S-Terra для изменения конфигурации системы, могут очистить текущий файл конфигурации для сброса настроек и установки своей конфигурации.	• Defense Evasion (TA0005) • Indicator Removal (T1070) • Clear Network Connection History and Configurations (T1070.007)
RV-D-1530	Вход в привилегированный режим на S-Terra Gate	Атакующие для получения доступа к системе S-Terra и изменения параметров должны сначала войти в привилегированный режим системы. Таким образом можно закрепиться в системе или вносить свои изменения в конфигурацию.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Valid Accounts (T1078) • Local Accounts (T1078.003)
RV-D-1536	Удален файл на S-Terra Gate	Атакующие, после получения доступа к системе S-Terra, могут удалить критичные файлы или папки из системы, например, файлы логов, пользователей или конфигурации системы.	• Impact (TA0040) • Data Destruction (T1485) • Lifecycle-Triggered Deletion (T1485.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1538	Подбор пароля для привилегированного режима	Атакующие для получения доступа к привилегированному режиму S-Terra Gate могут попробовать подобрать пароль. Данное правило обнаруживает множественные неудачные попытки входа в привилегированный режим.	• Brute Force (T1110)
RV-D-1539	Выдача максимальных привилегий для пользователя	Атакующие после получения доступа к системе S-Terra могут попробовать выдать максимальные привилегии в системе для пользователя, что позволит закрепиться на устройстве.	• Privilege Escalation (TA0004) • Valid Accounts (T1078) • Local Accounts (T1078.003) • Account Manipulation (T1098) • Abuse Elevation Control Mechanism (T1548)
RV-D-1540	Настроена отправка логов на неизвестный узел	Атакующие после получения доступа к системе S-Terra могут изменить конфигурацию и установить отправку логов системы на другой неизвестный узел, тем самым отключить мониторинг устройства.	• Execution (TA0002) • Command and Scripting Interpreter (T1059) • Network Device CLI (T1059.008)

Операционные системы

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых операционных систем:

- Linux
- Microsoft Windows
- Microsoft Windows Task Scheduler

Linux

Данный раздел содержит инструкции по сбору событий из журналов Linux различными методами:

- Linux Auditd
- Linux R-Vision Endpoint

Linux Auditd

- Linux Auditd: настройка источника
- Linux Auditd: правила корреляции

Linux Auditd: настройка источника

Данное руководство описывает процесс отправки событий службы Linux Auditd в R-Vision SIEM.

Настройка Auditd



В настоящем руководстве рассматривается передача событий с помощью службы rsyslog. Предполагается, что rsyslog на станции с ОС Linux уже установлен.

Настройка журналирования Auditd

Журналирование событий службы Auditd определяет, какие события будут регистрироваться в системе. Журналирование событий настраивается с помощью правил. Если у вас уже настроена служба Auditd, пропустите этот пункт и перейдите к настройке передачи событий.

Для настройки журналирования Auditd выполните следующие действия:

1. Проверьте, установлена ли служба Auditd, с помощью команды:

```
auditctl -v
```

   - Если служба установлена, на экране отобразится версия установленной службы, например, `auditctl version 3.0.7`.



Если версия установленной службы ниже 2.6, обновите службу согласно рекомендациям производителя ОС.

- Если служба не установлена, на экране отобразится сообщение об ошибке. В этом случае необходимо установить службу с помощью одной из следующих команд:
  - На ОС ALT Linux:

    ```
    apt-get install -y audit audispd-plugins
    ```

  - На ОС Astra Linux, Debian или Ubuntu:

    ```
    apt-get install -y auditd audispd-plugins
    ```

  - На ОС CentOS, Oracle Linux, Red Hat Enterprise Linux или РЕД ОС:

    ```
    yum install -y audit audispd-plugins
    ```

  - На ОС SUSE Linux Enterprise Server:

    ```
    zypper install audit audispd-plugins
    ```

  - На VMware Photon OS:

    ```
    sudo dnf install -y yum
    sudo yum install audit audispd-plugins
    ```

  - На ОС Platform V SberLinux OS Server:

    ```
    rpm install <path_to_audit-*.x86_64.rpm>
    ```

    Здесь `<path_to_audit-*.x86_64.rpm>` — путь к файлу `audit-*.x86_64.rpm`.

    Файл `audit-*.x86_64.rpm` нужно скопировать из пакета `./sberlinux-9-for-x86_64-baseos-rpms/Packages/a/audit-*.x86_64.rpm`, который находится в архиве с установщиком Platform V SberLinux OS Server.

2. Запустите и добавьте службу Auditd в автозагрузку с помощью команды:

   ```
   systemctl enable --now auditd.service
   ```

3. Включите в файле `/etc/audit/auditd.conf` обогащенный режим логирования:

   ```
   log_format = ENRICHED
   disp_qos = lossless
   ```



Обогащенный режим доступен для Auditd версии 2.6 и выше.

4. Настройте службу Auditd, применив рекомендованные компанией R-Vision правила Auditd. Для этого:
   a. Скачайте правила по ссылке.
   b. Скопируйте файл `audit.rules` в директорию `/etc/audit/rules.d`.



Для РЕД ОС 8 используйте файл с правилами `redos8-audit.rules`.

   c. Перезапустите службу Auditd с помощью команды:

```
systemctl restart auditd.service
```

5. После перезапуска убедитесь, что служба запустилась корректно:

```
systemctl status auditd.service
```

6. Убедитесь в наличии событий в файле `/var/log/audit/audit.log`:

```
tail -f /var/log/audit/audit.log
```

Отправка событий Auditd

Для пересылки логов Auditd по syslog выполните следующие шаги:

1. Убедитесь, что установлен плагин audispd. Установка плагина осуществляется в пункте Настройка журналирования Auditd.



Если установка плагина невозможна или нежелательна, можно использовать модуль `imfile rsyslog` для чтения событий из файла `audit.log`. В таком случае нужно вручную указать для параметра `syslogtag` значение `audisp-syslog`.

2. Включите передачу audit по syslog, установив в параметре `active` значение `yes`:
   - для Auditd версий 3.0 или выше — в файле `/etc/audit/plugins.d/syslog.conf`;
   - для Auditd версий ниже 3.0 — в файле `/etc/audisp/plugins.d/syslog.conf`.
3. Перезапустите службу Auditd с помощью команды:

```
systemctl restart auditd.service
```

4. Создайте правило `/etc/rsyslog.d/40-auditd.conf` со следующим содержимым:

```
if $programname contains 'audisp' or $syslogtag contains 'audisp' then {
 action(type="omfwd" Target="<target>" Port="<port>" Protocol="<protocol>")
```

```
  stop
 }
```

Здесь:

- `<target>` — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- `<port>` — порт точки входа Syslog на конвейере SIEM.
- `<protocol>` — сетевой протокол: `tcp` или `udp`.



При использовании плагина audispd для отправки событий используется модуль `imjournal rsyslog`. Количество отправленных событий может превышать ограничения, установленные для модуля `imjournal`. Чтобы предотвратить возможную потерю событий, отключите или увеличьте стандартные ограничения. Для этого добавьте параметры `Ratelimit.Interval` и `Ratelimit.Burst` в строку подключения модуля `imjournal` в файле `/etc/rsyslog.conf`:

```
module(load="imjournal"
    UsePid="system"
    StateFile="imjournal.state"
    Ratelimit.Interval="0"
    Ratelimit.Burst="0")
```

5. Перезапустите службу rsyslog с помощью команды:

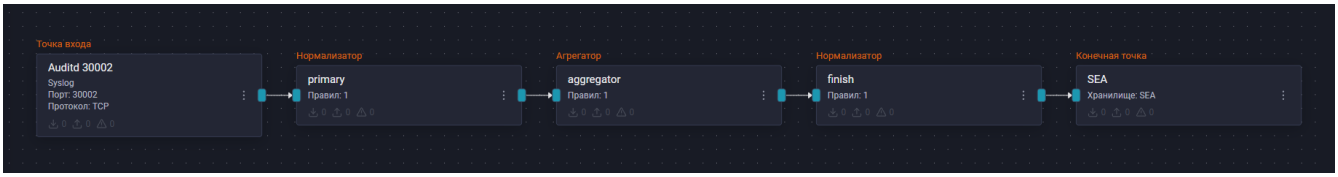
```
systemctl restart rsyslog.service
```

Настройка в R-Vision SIEM

1. В интерфейсе R-Vision SIEM в карточке коллектора перейдите на вкладку **Обогащение**.
2. Добавьте таблицы обогащения **auditd_events**, **auditd_error_codes** и **auditd_syscalls**.
3. Создайте новый конвейер в данном коллекторе.
4. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне Auditd.
   - Протокол: выберите вариант **TCP**.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **Linux Auditd - первичная нормализация (шаг 1)** (идентификатор правила: **RV-N-187**).
6. Соедините нормализатор с точкой входа.
7. Добавьте на конвейер элемент **Агрегатор** с правилом **Linux Auditd - правило агрегации (шаг 2)** (идентификатор правила: **RV-A-2**).

8. Соедините агрегатор с нормализатором.
9. Добавьте на конвейер элемент **Нормализатор** с правилом **Linux Auditd - правило интерпретации (шаг 3)** (идентификатор правила: **RV-N-186**).
10. Соедините второй нормализатор с агрегатором.
11. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
12. Соедините конечную точку со вторым нормализатором.
13. Сохраните и установите конфигурацию конвейера.

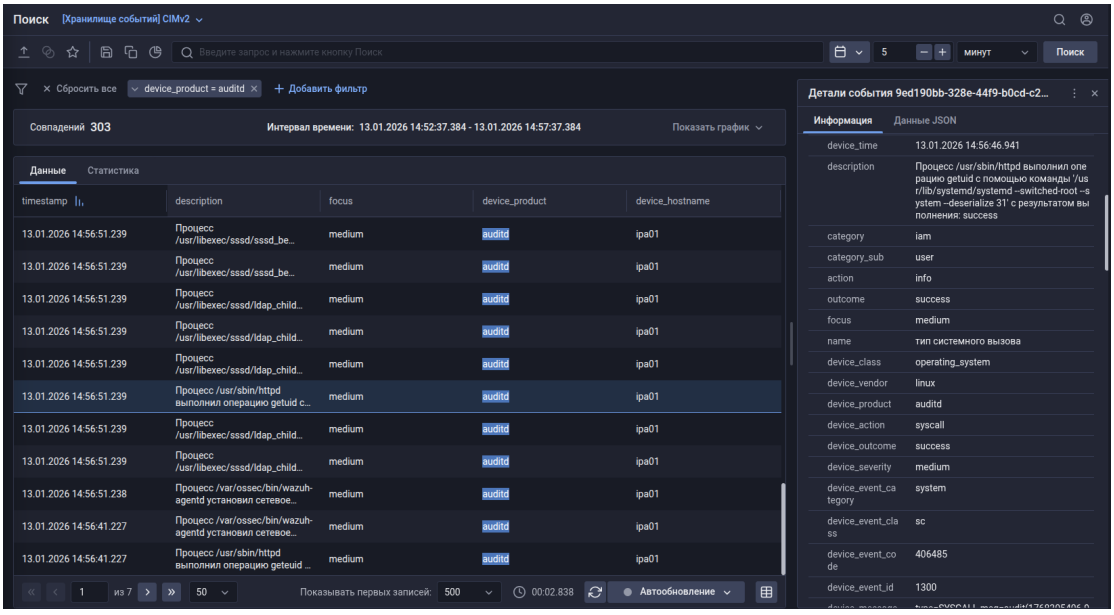
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Auditd.

Найти события источника в хранилище можно по следующему фильтру:

```
device_product = "auditd"
```



Linux Auditd: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-786	Большое количество подозрительных команд	Правило предназначено для выявления выполнения большого числа команд за короткий промежуток времени, что характерно для действий атакующего на этапе разведки. При первом подключении к хосту атакующий стремится получить максимум информации о системе, используя стандартные утилиты Linux. При срабатывании данного правила следует опросить пользователя, инициирующего активность, на предмет легитимности действий. Если инцидент подтверждается, необходимо заблокировать скомпрометированную учетную запись, провести анализ событий на целевом хосте на предмет возможных действий по закреплению в инфраструктуре, выяснить точку входа атакующего и устранить уязвимости. По возможности проанализировать сетевое окружение в поисках точек закрепления или оставленных утилит.	• Discovery (TA0007) • System Network Configuration Discovery (T1016) • Process Discovery (T1057) • System Information Discovery (T1082) • Software Discovery (T1518)

ID правила	Название правила	Описание	Тактики и техники
RV-D-787	Получение информации о текущем пользователе	Информация о текущем пользователе является важной частью разведки и подготовки для атакующих. Обычно атакующий может пытаться получить данную информацию после получения доступа в результате эксплуатации уязвимости или повышения привилегий. В случае подтверждения нелегитимной активности необходимо незамедлительно изолировать хост и отключить скомпрометированную учетную запись. Далее проверить возможные пути распространения атаки и осуществить поиск изначальной причины компрометации узла и учетной записи.	• Discovery (TA0007) • Account Discovery (T1087) • Local Account (T1087.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-788	Разведка доменных УЗ в Linux	Атакующие могут пытаться получить список учетных записей домена в среде Linux, используя утилиты, такие как ldapsearch или ldapdomaindump. Эта информация позволяет им определить существующие учетные записи, выявить привилегированные учетные записи и подготовиться к дальнейшим атакам, таким как подбор паролей или расширение прав доступа. Правило нацелено на выявление попыток получения списка учетных записей домена в Linux с использованием команд, характерных для разведки учетных записей. Если правило срабатывает, необходимо проверить, кто инициировал выполнение команды, и оценить легитимность активности. Если действие не санкционировано, рекомендуется провести расследование, определить потенциальные цели атакующих и принять меры по защите учетных записей, включая ограничение доступа, изменение учетных данных или мониторинг последующей активности.	• Discovery (TA0007) • Account Discovery (T1087) • Domain Account (T1087.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-789	Разведка локальных УЗ в Linux	Важно отслеживать попытки получения списка учетных записей локальной системы, так как атакующие могут использовать эту информацию для определения привилегированных пользователей, а также для последующего перебора паролей или повышения привилегий. Данное правило детектирует выполнение команд, позволяющих просмотреть локальные учетные записи, такие как просмотр файла `/etc/passwd`, проверка sudoers или анализ активных пользователей. При срабатывании правила рекомендуется проверить, выполнялись ли данные команды уполномоченным пользователем. Если действия выглядят подозрительными, следует провести расследование, проверить логи на предмет других аномалий и при необходимости ограничить доступ подозрительной учетной записи.	• Discovery (TA0007) • Account Discovery (T1087) • Local Account (T1087.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-790	Разведка установленного ПО в Linux	Атакующие могут попытаться получить список установленного или используемого программного обеспечения (ПО). Эта информация может помочь атакующим сформировать последующее поведение для развития атаки. Правило детектирует использование легитимного ПО для получения списка программ, исполняемых файлов и средств защиты. При срабатывании правила рекомендуется уточнить легитимность активности пользователя, от имени которого выполнялись операции. Если активность не подтверждается, рекомендуется сразу заблокировать учетную запись и начать расследование инцидента.	• Reconnaissance (TA0043) • Discovery (TA0007) • Software Discovery (T1518) • Security Software Discovery (T1518.001) • Gather Victim Host Information (T1592) • Software (T1592.002)
RV-D-791	Поиск локализации системы Linux	Обнаружение использования команд настроек локализации Linux. Атакующие могут использовать полученную информацию для понимания специфики образа Linux и дальнейшего продвижения в инфраструктуре. В случае подтверждения нелегитимной активности необходимо незамедлительно изолировать хост и отключить скомпрометированную учетную запись (УЗ). Далее проверить возможные пути распространения атаки и осуществить поиск изначальной причины компрометации узла/учетной записи.	• Discovery (TA0007) • System Location Discovery (T1614) • System Language Discovery (T1614.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-792	Поиск сетевых конфигураций	Обнаружение использования команд для поиска сетевых конфигураций на узле Linux. Атакующий, попав на хост или повысив привилегии, может попытаться разведать сетевые настройки и окружения захваченного узла. В случае подтверждения нелегитимной активности необходимо незамедлительно изолировать хост и отключить скомпрометированную учетную запись. Далее проверить возможные пути распространения атаки и осуществить поиск изначальной причины компрометации узла/учетной записи.	• Reconnaissance (TA0043) • Discovery (TA0007) • System Network Configuration Discovery (T1016) • Internet Connection Discovery (T1016.001) • Gather Victim Network Information (T1590)
RV-D-793	Разведка запущенных процессов в Linux	Обнаружение использования команд для поиска процессов на узле Linux. Атакующий, попав на хост или повысив привилегии, может попытаться разведать текущие процессы узла. В случае подтверждения нелегитимной активности необходимо незамедлительно изолировать хост и отключить скомпрометированную учетную запись. Далее проверить возможные пути распространения атаки и осуществить поиск изначальной причины компрометации узла/учетной записи.	• Discovery (TA0007) • Process Discovery (T1057)

ID правила	Название правила	Описание	Тактики и техники
RV-D-794	Поиск окружения контейнера через proc VFS	Обнаруживает потенциальный поиск окружения контейнера с помощью списка определенных функций ядра в виртуальной файловой системе `/proc`. При срабатывании правила рекомендуется уточнить легитимность активности пользователя, от имени которого выполнялись операции. Если активность не подтверждается, рекомендуется сразу заблокировать учетную запись и начать расследование инцидента.	• Discovery (TA0007) • System Information Discovery (T1082)
RV-D-795	Обнаружение контейнеров через Inodes Listing	Правило предназначено для обнаружения попыток определения, выполняется ли процесс внутри контейнера. Детектируется запуск команды, которая выводит номер inode (индекса) корневого каталога `/` с помощью утилиты `ls`. При срабатывании правила рекомендуется уточнить легитимность активности пользователя, от имени которого выполнялись операции. Если активность не подтверждается, рекомендуется сразу заблокировать учетную запись и начать расследование инцидента.	• Discovery (TA0007) • System Information Discovery (T1082)

ID правила	Название правила	Описание	Тактики и техники
RV-D-796	Использование утилит для сканирования сети	Обнаруживает использование инструментов для сетевого сканирования. Эти инструменты можно использовать, например, для поиска открытых локальных или удаленных портов. При срабатывании правила рекомендуется уточнить легитимность активности пользователя, от имени которого выполнялись операции. Если активность не подтверждается, рекомендуется сразу заблокировать учетную запись и начать расследование инцидента.	• Reconnaissance (TA0043) • Discovery (TA0007) • Network Service Discovery (T1046) • Active Scanning (T1595) • Scanning IP Blocks (T1595.001)
RV-D-797	Разведка Docker контейнеров через Dockerenv	Обнаруживает чтение файла `.dockerenv`, что может быть признаком потенциального обнаружения контейнера. При срабатывании правила рекомендуется уточнить легитимность активности пользователя, от имени которого выполнялись операции. Если активность не подтверждается, рекомендуется сразу заблокировать учетную запись и начать расследование инцидента.	• Discovery (TA0007) • System Information Discovery (T1082) • Container and Resource Discovery (T1613)

ID правила	Название правила	Описание	Тактики и техники
RV-D-798	Поиск файлов с suid/sgid битом	Биты suid/sgid выставляются на файлах в Linux. Если файл содержит данный бит, то независимо от того, кто его запускает, он будет запускаться от имени пользователя, который владеет данным файлом. Атакующие зачастую проверяют подобные файлы, так как с помощью них можно повысить привилегии. Правило обнаруживает поиск файлов с suid/sgid битом. При срабатывании правила рекомендуется уточнить легитимность активности пользователя, от имени которого выполнялись операции. Если активность не подтверждается, рекомендуется сразу заблокировать учетную запись и начать расследование инцидента.	• Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Abuse Elevation Control Mechanism (T1548) • Setuid and Setgid (T1548.001)
RV-D-799	Подозрительное чтение домашней директории пользователя	Обнаружение чтения домашней директории другим пользователем. Атакующий, попав на хост под учетной записью пользователя, может попытаться читать директории других пользователей для поиска критичных файлов. В случае подтверждения нелегитимной активности необходимо незамедлительно изолировать хост и отключить скомпрометированную учетную запись. Далее проверить возможные пути распространения атаки и осуществить поиск изначальной причины компрометации узла/учетной записи.	• Discovery (TA0007) • File and Directory Discovery (T1083)

ID правила	Название правила	Описание	Тактики и техники
RV-D-800	Злоупотребление сырыми сокетами	Сырые сокеты позволяют реализовать в пользовательском пространстве новые протоколы стека Ipv4. Сокеты raw принимают и передают необработанные дейтаграммы без добавления в них каких-либо заголовков. Сырые сокеты позволяют атакующим проводить атаки типа DoS или незаметно управлять руткитами. Правило обнаруживает использование сырых сокетов типа SOCK_RAW, что может быть признаком активности, связанной с перехватом или манипуляцией трафиком. Если активность была инициирована неизвестным процессом и/или в поле cmd содержится подозрительная команда, то следует начать расследование.	• Command and Control (TA0011) • Non-Application Layer Protocol (T1095)

ID правила	Название правила	Описание	Тактики и техники
RV-D-801	Запуск утилиты msldapdump для разведки	Утилита msldapdump предназначена для сбора информации из службы LDAP. Она часто используется для аудита Active Directory (AD), так как LDAP является одним из ключевых протоколов, который AD использует для организации и хранения данных. Атакующие могут использовать утилиту msldapdump для разведки и сбора информации о структуре и объектах Active Directory (AD) с целью подготовки атак на сеть или системы организации. При срабатывании данного правила рекомендуется немедленно проверить учетную запись и действия пользователя, запустившего команду. При подтверждении нелегитимной активности заблокировать УЗ инициатора и провести расследование на предмет возможной компрометации системы.	• Discovery (TA0007) • Remote System Discovery (T1018) • Network Service Discovery (T1046) • Permission Groups Discovery (T1069) • Domain Groups (T1069.002) • Account Discovery (T1087) • Domain Account (T1087.002) • Password Policy Discovery (T1201) • Group Policy Discovery (T1615)

ID правила	Название правила	Описание	Тактики и техники
RV-D-802	Разведка парольной политики в Linux	Атакующие на этапе разведки могут получить доступ к сведениям о политике паролей, используемой локально или в корпоративной сети. Политики паролей — это способ принудительного использования сложных паролей, которые трудно угадать или взломать с помощью атаки Brute Force. Полученная информация может помочь атакующему создать список распространенных паролей и запустить атаки Brute Force, которые соответствуют установленной политике. При регистрации события требуется изучить активность учетной записи. В случае выявления признаков компрометации произвести ее блокировку и изоляцию хоста.	• Discovery (TA0007) • Password Policy Discovery (T1201)
RV-D-803	Разведка системной информации Linux	Когда атакующие получают доступ к инфраструктуре, они начинают собирать информацию о системе. Это включает в себя получение сведений о конфигурации системы. В случае с Linux-устройствами атакующие могут получить такую информацию, как версии операционной системы, установленные пакеты, аппаратное обеспечение и другие параметры конфигурации. Эти сведения могут помочь им в дальнейших действиях, например, при попытке проникновения или проведении атаки.	• Discovery (TA0007) • System Information Discovery (T1082) • Gather Victim Host Information (T1592) • Client Configurations (T1592.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-804	Получена информация о системных службах на узле	Правило обнаруживает получение информации о системных службах на узле с помощью утилит systemctl, services и использования характерных ключей или с помощью чтения директорий, содержащих список сервисов. Эта информация необходима для формирования последующих действий атакующими. В случае обнаружения нелегитимной активности рекомендуется изолировать хост от локальной сети, проверить, откуда было произведено подключение, убедиться, что не были скомпрометированы другие узлы в сети. После этого сбросить пароли учетных записей, обновить сертификаты, провести внутреннее расследование с целью установления возможных методов закрепления в системе и причин возникновения инцидента.	• Discovery (TA0007) • System Service Discovery (T1007)

ID правила	Название правила	Описание	Тактики и техники
RV-D-805	Извлечение содержимого буфера в Linux	Атакующие могут использовать утилиты copyq, xclip, xsel и wl-paste для кражи данных из буфера обмена в системах Linux. Это правило отслеживает попытки запуска данных утилит с параметрами, указывающими на обращение к буферу обмена, что может свидетельствовать о попытках эксфильтрации данных. При срабатывании правила рекомендуется проверить легитимность действий пользователя, инициировавшего команду, и при выявлении подозрительной активности — принять меры для предотвращения дальнейшего сбора и передачи данных, а также провести расследование для выявления возможной компрометации системы.	• Collection (TA0009) • Clipboard Data (T1115)
RV-D-806	Чтение критичных файлов Linux	Правило обнаруживает чтение критичных файлов на узле Linux, в которых хранятся учетные данные и данные конфигурации системы. Атакующий, попав на хост, может попытаться прочитать данные файлы для дальнейшей эскалации атаки. В случае подтверждения нелегитимной активности рекомендуется изолировать хост, заблокировать пользователя, проверить, откуда было произведено подключение, убедиться, что не были скомпрометированы другие узлы и пользователи. После этого сбросить пароли учетных записей, обновить сертификаты, провести внутреннее расследование с целью установления возможных методов закрепления в системе и причин возникновения инцидента.	• Collection (TA0009) • Data from Local System (T1005) • Unsecured Credentials (T1552) • Credentials In Files (T1552.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-807	Загрузка файлов с удаленных ресурсов стандартными утилитами	Для развития атаки атакующие могут доставлять файлы с удаленных ресурсов. В целях маскировки и обхода политики безопасности для загрузки используются легитимные утилиты, которые предустановлены в системе по умолчанию или могут быть доставлены иным способом. В случае возникновения активности необходимо определить, к какому ресурсу осуществляется обращение. Если ресурс имеет признаки нелегитимности, необходимо опросить пользователя, ответственного за учетную запись (УЗ) инициатора активности, на предмет легитимности данной загрузки. Если легитимность загрузки подтвердить не удалось, необходимо заблокировать УЗ инициатора активности на время проведения расследования.	• Command and Control (TA0011) • Ingress Tool Transfer (T1105)

ID правила	Название правила	Описание	Тактики и техники
RV-D-808	Использование утилиты SSHuttle для создания SSH-туннеля	Атакующие могут использовать туннелирование для сетевого взаимодействия с целевыми системами, чтобы избежать обнаружения или сетевой фильтрации и (или) получить доступ к недоступным другими способами системам. Правило детектирует попытки использования на устройстве SSHuttle, написанной на Python. SSHuttle - это утилита для создания прокси и пересылки пакетов через ssh. При обнаружении активности рекомендуется определить легитимность использования инструмента. Если легитимность подтвердить не удалось, необходимо изолировать хост и заблокировать учетную запись, активность которой выявлена.	• Command and Control (TA0011) • Protocol Tunneling (T1572)
RV-D-809	Загрузка файлов утилитой wget в директорию tmp	Правило направлено на обнаружение использования wget для загрузки файлов во временные директории, такие как `/tmp` или `/var/tmp`. При обнаружении активности рекомендуется определить легитимность загрузки файлов и их источника. Если легитимность подтвердить не удалось, необходимо изолировать хост и заблокировать учетную запись, активность которой выявлена.	• Command and Control (TA0011) • Ingress Tool Transfer (T1105)

ID правила	Название правила	Описание	Тактики и техники
RV-D-810	Отключение или модификация Syslog Linux	Служба Syslog является одним из основных инструментов для отслеживания событий безопасности. Атакующие, получившие доступ к системе, могут попытаться отключить службу Syslog или изменить ее конфигурацию с целью скрыть свою активность. При срабатывании данного правила необходимо связаться с владельцем учетной записи (УЗ), от имени которой произошло событие, для уточнения легитимности действий. Если действия не подтверждены владельцем, необходимо заблокировать скомпрометированную УЗ и закрыть все ее активные сессии, а также восстановить работу службы Syslog.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Indicator Blocking (T1562.006)
RV-D-811	Отключение службы firewalld	Отключение брандмауэра может позволить атакующим получить доступ к системе через открытые порты, что может привести к компрометации данных или установке вредоносного ПО. При срабатывании данного правила необходимо связаться с владельцем учетной записи, от имени которой произошло событие, для уточнения легитимности действий. Если действия не подтверждены владельцем, необходимо заблокировать скомпрометированную УЗ и восстановить работу firewalld.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify System Firewall (T1562.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-868	Отключение службы Auditd	Атакующие могут отключить систему аудита Linux, чтобы скрыть вредоносную активность и избежать обнаружения. Система аудита Linux работает на уровне ядра и ведет журналы событий для приложений и системной активности, такой как события процессов, сети, файлов и входа в систему, на основе предварительно настроенных правил. При срабатывании данного правила необходимо связаться с владельцем учетной записи, от имени которой произошло событие, для уточнения легитимности действий. Если действия не подтверждены владельцем, необходимо заблокировать скомпрометированную УЗ и восстановить работу службы Auditd.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Linux Audit System (T1562.012)

ID правила	Название правила	Описание	Тактики и техники
RV-D-869	Добавление файла в расширения браузера Linux	Данное правило направлено на обнаружение подозрительных действий, связанных с добавлением файлов в директорию расширений браузера в операционной системе Linux. Такие действия могут быть использованы атакующим для установки вредоносных или нежелательных расширений, которые могут изменять поведение браузера, собирать конфиденциальные данные пользователя или выполнять другие вредоносные операции. В случае срабатывания правила необходимо запросить информацию о причинах активности у ответственного за учетную запись. Если подтверждения легитимности не последовало, рекомендуется временно заблокировать учетную запись, ограничить доступ к узлу, с которого произошли подозрительные действия, и инициировать внутреннее расследование.	• Persistence (TA0003) • Software Extensions (T1176) • Browser Extensions (T1176.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-870	Добавление расширения в браузер через CLI Linux	Данное правило направлено на обнаружение подозрительных действий, связанных с добавлением расширений в браузер с использованием командной строки (CLI) в операционной системе Linux. Такие действия могут быть использованы атакующим для автоматизированной установки вредоносных или нежелательных расширений, которые могут изменять поведение браузера, собирать конфиденциальные данные пользователя или выполнять другие вредоносные операции. В случае срабатывания правила необходимо запросить информацию у ответственного за учетную запись о причинах активности. Если подтверждения легитимности не последовало, рекомендуется временно заблокировать учетную запись, ограничить доступ к узлу, с которого произошли подозрительные действия, и инициировать внутреннее расследование.	• Persistence (TA0003) • Software Extensions (T1176) • Browser Extensions (T1176.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-871	Запуск процесса с помощью ld.so	Запуск процесса с помощью ld.so — это метод, который может быть использован для обхода стандартных механизмов загрузки программ и выполнения произвольного кода. Например, атакующие могут использовать подмену переменных окружения или указание нестандартных библиотек, чтобы внедрить вредоносный код или изменить поведение приложения. При срабатывании данного правила рекомендуется немедленно проанализировать процесс, вызвавший выполнение команды, проверить системные журналы и выявить возможные векторы атаки. Если обнаружены признаки компрометации, следует изолировать затронутую систему, связаться с ответственным лицом и инициировать процесс расследования.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Hijack Execution Flow (T1574) • Dynamic Linker Hijacking (T1574.006)

ID правила	Название правила	Описание	Тактики и техники
RV-D-872	Изменение бинарных файлов Linux	Изменение бинарных файлов — это процесс, который может быть использован для компрометации системы или выполнения несанкционированных действий. Атакующие могут модифицировать или заменять исполняемые файлы, чтобы внедрить вредоносный код, получить несанкционированный доступ или скрыть свою активность. При срабатывании данного правила рекомендуется немедленно проверить учетную запись и действия пользователя, запустившего команду. При подтверждении нелегитимной активности требуется заблокировать УЗ инициатора и провести расследование на предмет возможной компрометации системы.	• Persistence (TA0003) • Compromise Host Software Binary (T1554)

ID правила	Название правила	Описание	Тактики и техники
RV-D-873	Изменение системных библиотек Linux	Изменение системных библиотек Linux — это процесс, который может быть использован для компрометации системы или выполнения несанкционированных действий. Атакующие могут заменить или модифицировать системные библиотеки, чтобы внедрить вредоносный код или скрыть свою активность. Например, в CVE-2024-3094 атакующие получали бэкдор в SSH благодаря изменению библиотеки liblzma. При срабатывании данного правила рекомендуется немедленно проверить учетную запись и действия пользователя, запустившего команду. При подтверждении нелегитимной активности требуется заблокировать УЗ инициатора и провести расследование на предмет возможной компрометации системы.	• Persistence (TA0003) • Compromise Host Software Binary (T1554)

ID правила	Название правила	Описание	Тактики и техники
RV-D-874	Модификация файлов MOTD в Linux	В операционных системах Linux файл MOTD (Message of the Day) отображает сообщение, которое пользователи видят при входе в систему через консоль или по SSH. Файл находится в директории `/etc/update-motd.d/` и может содержать важную информацию для пользователей. Атакующие могут использовать модификацию файлов MOTD для внедрения вредоносного кода или скриптов, которые будут выполняться при входе пользователя в систему. Эта техника позволяет атакующему закрепиться в системе и потенциально повысить свои привилегии. При обнаружении такого события рекомендуется проверить внесенные изменения и удостовериться в легитимности действий пользователя, инициировавшего изменения. При наличии признаков злоупотребления требуется ограничить доступ пользователя, проанализировать журналы и инициировать расследование на предмет возможной компрометации системы, удалить добавленные или измененные файлы.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Event Triggered Execution (T1546) • Unix Shell Configuration Modification (T1546.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-875	Поиск данных в сетевых папках Linux	Атакующие после компрометации системы могут использовать сетевые ресурсы, чтобы обнаружить интересующие их файлы. Они ищут определенные типы файлов, такие как документы, электронные таблицы, технические спецификации, базы данных или архивы, которые могут содержать пароли, личные данные клиентов, финансовую информацию и другие ценные сведения. При срабатывании данного правила корреляции необходимо просмотреть время срабатывания, пользователя и критичность сетевого диска. При аномальной активности или нетипичном имени файлов рекомендуется запросить у инициатора подтверждение легитимности его действий. Если действия не подтверждаются, следует заблокировать учетную запись пользователя, сбросить активные сессии нарушителя и провести расследование на возможность компрометации других хостов в сети, по возможности проверить содержимое файлов.	• Discovery (TA0007) • Collection (TA0009) • Data from Network Shared Drive (T1039) • File and Directory Discovery (T1083)

ID правила	Название правила	Описание	Тактики и техники
RV-D-876	Использование утилит для создания снимков экрана Linux	Атакующие могут использовать различные утилиты для создания снимков экрана в Linux. Снимки экрана могут содержать конфиденциальные документы, данные аутентификации, информацию для проведения платежных операций и иную конфиденциальную информацию. Информация со снимков может помочь атакующему сформировать вектор для дальнейшего распространения. При срабатывании правила корреляции требуется изучить активность учетной записи. В случае выявления признаков компрометации необходимо произвести ее блокировку и изоляцию хоста.	• Collection (TA0009) • Screen Capture (T1113)

ID правила	Название правила	Описание	Тактики и техники
RV-D-877	Туннелирование с использованием ngrok в Linux	Утилита ngrok позволяет организовать подключение к удаленному хосту из сети Интернет без статического белого IP-адреса, что активно используется атакующими для создания каналов утечки данных, получения доступа к внутренним сервисам (RDP, SSH) для атаки извне, а также организации каналов командования и управления (C2). Правило детектирует параметры, с которыми создается процесс ngrok, события создания и изменения файла конфигурации. При обнаружении активности рекомендуется определить легитимность использования инструмента. Если легитимность подтвердить не удалось, необходимо изолировать хост и заблокировать учетную запись, от имени которой выявлена активность.	• Command and Control (TA0011) • Proxy (T1090) • External Proxy (T1090.002) • Web Service (T1102) • Protocol Tunneling (T1572)

ID правила	Название правила	Описание	Тактики и техники
RV-D-879	Удаление файлов логирования в Linux	После выполнения ряда действий в системе атакующие могут попытаться удалить следы своего присутствия. Одним из наиболее распространенных методов является удаление файлов логирования. Данное правило отслеживает попытки удаления файлов, содержащих важную информацию о действиях атакующего, что помогает обнаружить попытки сокрытия следов. При попытке удаления лог-файлов необходимо оперативно провести анализ журналов событий для выявления действий атакующего. Важно попытаться восстановить удаленные файлы с помощью резервных копий или инструментов восстановления, усилить защиту логирования, используя неизменяемые журналы или специализированные решения. В случае инцидента необходимо заблокировать учетную запись, от имени которой производились действия, провести расследование для определения масштаба ущерба и установления дальнейших шагов по устранению последствий.	• Defense Evasion (TA0005) • Indicator Removal (T1070) • Clear Linux or Mac System Logs (T1070.002) • Clear Command History (T1070.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-880	Загрузка подозрительного ebpf модуля	Правило обнаруживает использование системного вызова bpf. Данный вызов может использоваться атакующими для внедрения вредоносных ebpf модулей, что приведет к закреплению в системе. Модуль ebpf сложно обнаружить, так как он работает непосредственно в самом ядре. Такие модули могут использоваться не только для закрепления, но и для обхода средств защиты (скрытие процессов, сетевых подключений, перехват системных вызовов). При обнаружении активности рекомендуется определить легитимность действий. Если легитимность подтвердить не удалось, необходимо изолировать хост и заблокировать учетную запись, от имени которой выявлена активность.	• Defense Evasion (TA0005) • Rootkit (T1014)

ID правила	Название правила	Описание	Тактики и техники
RV-D-881	Изменение критичных файлов конфигурации интерактивной оболочки	Изменение параметров ведения журнала и очистка истории команд в Linux могут быть использованы атакующими для сокрытия своей деятельности и затруднения обнаружения. Атакующий может изменить настройки оболочки или переменные окружения, связанные с ведением истории команд, чтобы предотвратить запись своих дальнейших действий. Это позволяет скрыть выполненные команды и затруднить расследование инцидентов безопасности. При обнаружении изменения параметров журнала и очистки истории команд Linux на хосте необходимо заблокировать учетную запись, от имени которой произошел инцидент, закрыть ее активные сессии в корпоративной сети, по возможности изолировать пораженный хост и восстановить первичные настройки логирования команд.	• Defense Evasion (TA0005) • Indicator Removal (T1070) • Clear Command History (T1070.003) • Event Triggered Execution (T1546) • Unix Shell Configuration Modification (T1546.004) • Impair Defenses (T1562) • Impair Command History Logging (T1562.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-882	Изменение конфигурационных файлов служб журналирования	Конфигурационные файлы служб журналирования содержат настройки, которые определяют, как собираются и обрабатываются журналы событий. Несанкционированное изменение этих файлов может привести к тому, что критическая информация о событиях системы не будет правильно собрана или отправлена для анализа, что, в свою очередь, может скрыть следы злонамеренных действий. При срабатывании данного правила необходимо провести проверку легитимности действий, запросив подтверждение от пользователя, от имени которого произошло событие. Если активность не санкционирована, необходимо заблокировать учетную запись и закрыть все текущие сессии с ней, а также восстановить конфигурационные файлы из резервной копии.	• Defense Evasion (TA0005) • Indicator Removal (T1070) • Clear Linux or Mac System Logs (T1070.002) • Clear Network Connection History and Configurations (T1070.007) • Impair Defenses (T1562) • Indicator Blocking (T1562.006) • Disable or Modify Linux Audit System (T1562.012)

ID правила	Название правила	Описание	Тактики и техники
RV-D-883	Компиляции исходного кода на Linux	Атакующие могут использовать доставку вредоносных файлов в виде исходного кода для обхода защитных механизмов, предназначенных для блокировки исполняемых файлов. Такие файлы требуют компиляции перед запуском, что обычно выполняется с помощью утилит gcc, g++, cargo, rustc, go. Данное правило позволяет выявлять подозрительные случаи компиляции исходного кода на целевой системе, которые могут свидетельствовать о попытках обхода защитных мер. При срабатывании правила рекомендуется проанализировать контекст выполнения команды, связаться с пользователем, инициировавшим активность, чтобы уточнить легитимность действий и назначение скомпилированного файла.	• Defense Evasion (TA0005) • Obfuscated Files or Information (T1027) • Compile After Delivery (T1027.004)
RV-D-884	Копирование стандартных исполняемых файлов	Данное правило отслеживает открытие бинарных файлов для чтения. Данные файлы являются стандартными утилитами в системах семейства Unix. Атакующий может копировать эти файлы в файлы с другой директорией и именем для избегания обнаружения. При срабатывании правила рекомендуется проанализировать контекст выполнения команды, связаться с пользователем, инициировавшим активность, чтобы уточнить легитимность действий и причины копирования утилит.	• Defense Evasion (TA0005) • Masquerading (T1036) • Rename Legitimate Utilities (T1036.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-886	Отключение мандатного контроля целостности	Данное правило направлено на детектирование подозрительных действий, связанных с отключением Механизмов Контроля Целостности (МКЦ) в Astra Linux. Отключение происходит за счет изменения файла `fs-ilev.conf` или через GUI и CLI. Данная активность является аномальной для стандартных административных задач и может указывать на попытку атакующего отключить защитные механизмы системы или скрыть следы своей активности. Обнаружение основывается на событиях изменения содержимого файла или выполнения команды. Несанкционированное изменение конфигурации МКЦ может привести к нарушению целостности системы, открывая возможности для дальнейших атак и компрометации критически важных данных. В случае срабатывания правила необходимо запросить информацию о причинах активности у ответственного за узел. Если подтверждения легитимности не последовало, рекомендуется ограничить доступ к узлу, с которого произошли подозрительные действия, и инициировать внутреннее расследование.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-890	Создание пользователя или группы	Правило выявляет создание новой локальной учетной записи или группы на хосте. Такие действия могут выполняться как легитимными администраторами, так и атакующими для закрепления в системе. Создание учетных записей или групп может быть использовано атакующими для получения долгосрочного доступа, обхода механизмов аутентификации или эскалации привилегий. Правило анализирует события из auth.log и auditd, отслеживая операции ADD_USER и ADD_GROUP.	• Persistence (TA0003) • Account Manipulation (T1098) • Create Account (T1136) • Local Account (T1136.001)
RV-D-892	Модификация правил udev	udev - это утилита в системах Linux, предназначенная для управления устройствами ввода/вывода и их событиями. Управление происходит путем создания правил в директориях `/etc/udev/rules.d/` и `/usr/lib/udev/rules.d/`. Атакующие могут использовать эти правила для запуска процессов или выполнения определенных файлов. Поэтому необходимо отслеживать создание/изменение правил в данных директориях.	• Persistence (TA0003) • Event Triggered Execution (T1546) • Udev Rules (T1546.017)

ID правила	Название правила	Описание	Тактики и техники
RV-D-893	Закрепление в системе с использованием записей автозагрузки XDG	Атакующие могут добавлять или изменять XDG Autostart Entries (записи автозагрузки XDG) для выполнения вредоносных программ или команд при входе пользователя в систему. XDG Autostart Entries используют файлы `.desktop` для настройки окружающей среды пользователя и определяют, какие приложения должны запускаться при входе пользователя. Правило детектирует создание и изменение файлов в директориях, где по умолчанию содержатся записи автозагрузки.	• Persistence (TA0003) • Boot or Logon Autostart Execution (T1547) • XDG Autostart Entries (T1547.013)
RV-D-894	Подозрительное изменение директории `/etc`	Правило обнаруживает изменения файлов в каталоге `/etc` на узле Linux, в котором хранится множество конфигураций системы. Атакующий, попав на хост, может попытаться изменить данные файлы конфигурации для атаки с помощью утилит для редактирования файлов.	• Execution (TA0002) • Persistence (TA0003) • Scheduled Task/Job (T1053) • Cron (T1053.003) • Event Triggered Execution (T1546) • Unix Shell Configuration Modification (T1546.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-896	Размещение архивов в сетевой папке Linux	Атакующие могут размещать данные, собранные из нескольких систем, в централизованном месте или каталоге на одной системе перед эксфильтрацией. Данные могут храниться в отдельных файлах или объединяться в один файл с помощью таких методов, как архивирование собранных данных. При срабатывании данного правила корреляции необходимо просмотреть время срабатывания, пользователя и критичность сетевого диска. При аномальной активности или подозрительном имени архива и его расположения рекомендуется запросить у инициатора подтверждение легитимности его действий. Если действия не подтверждаются, следует заблокировать учетную запись пользователя, сбросить активные сессии нарушителя и провести расследование на возможность компрометации других хостов в сети, по возможности проверить содержимое архива в изолированной среде.	• Collection (TA0009) • Data Staged (T1074) • Remote Data Staging (T1074.002) • Archive Collected Data (T1560)

ID правила	Название правила	Описание	Тактики и техники
RV-D-901	Остановка критичных сервисов в Linux	Данное правило направлено на мониторинг и предотвращение атак, направленных на остановку системных сервисов, что может нарушить работоспособность системы или привести к утрате данных. Атакующие могут остановить критически важные сервисы в системе. Также остановка сервиса может затормозить расследование инцидента. Правило детектирует системный вызов "SERVICE_STOP" для важных сервисов в системе. При срабатывании правила следует уточнить легитимность действий пользователя, который выполнил остановку, или определить причину остановки сервиса. Если легитимность не подтверждена, следует начать расследование и по возможности изолировать хост.	• Impact (TA0040) • Service Stop (T1489) • Endpoint Denial of Service (T1499) • Service Exhaustion Flood (T1499.002) • Application or System Exploitation (T1499.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-902	Уничтожение информации на диске в Linux	Атакующие могут использовать методы удаления или порчи данных, чтобы нанести существенный ущерб компании. Это правило направлено на детектирование активности, которая приводит к безвозвратному удалению или искажению данных, делающему их восстановление невозможным. Рассмотрены стандартные инструменты Linux, которые могут быть использованы для подобных действий. В рамках реагирования на инцидент необходимо связаться с ответственным за узел или учетную запись и выяснить причину активности. При отсутствии подтверждения легитимности действий следует временно изолировать узел, отключить учетную запись и инициировать процесс расследования.	• Impact (TA0040) • Disk Wipe (T1561) • Disk Content Wipe (T1561.001) • Disk Structure Wipe (T1561.002)
RV-D-906	Создание туннелей и перенаправление трафика	Правило отслеживает команды и процессы, которые могут использоваться для создания сетевых туннелей или перенаправления трафика. Атакующие часто применяют утилиты, такие как ssh, iptables, nc (netcat), redir, rinetd и sodevice_event_category, для обхода сетевых ограничений и скрытого взаимодействия с удаленными системами.	• Defense Evasion (TA0005) • Lateral Movement (TA0008) • Command and Control (TA0011) • Remote Services (T1021) • SSH (T1021.004) • Protocol Tunneling (T1572) • Network Boundary Bridging (T1599)

ID правила	Название правила	Описание	Тактики и техники
RV-D-907	Разведка под сервисным пользователем	Обнаружение использования утилит для разведки на узле Linux от имени сервисной учетной записи. Атакующий, попав на хост под сервисной УЗ, может попытаться получить дополнительные данные о хосте и окружении для дальнейшей атаки.	• Discovery (TA0007) • Lateral Movement (TA0008) • System Network Configuration Discovery (T1016) • Network Service Discovery (T1046) • System Information Discovery (T1082) • Account Discovery (T1087) • Lateral Tool Transfer (T1570)
RV-D-908	Загрузка файла сервисной учетной записью	Обнаружение использования утилит для загрузки файлов на узле Linux от сервисной учетной записи. Атакующий, попав на хост под сервисной учетной записью, может попытаться загрузить дополнительные файлы для атаки.	• Lateral Movement (TA0008) • Lateral Tool Transfer (T1570)
RV-D-909	Загрузка файла с помощью утилит GTFOBins	Обнаружение использования утилит GTFOBins для загрузки файлов на узле Linux. GTFOBins - список бинарных файлов Unix, которые могут быть использованы для обхода локальных ограничений безопасности. Атакующий, попав на хост, может попытаться загрузить дополнительные файлы для развития атаки.	• Lateral Movement (TA0008) • Lateral Tool Transfer (T1570)

ID правила	Название правила	Описание	Тактики и техники
RV-D-914	Доступ к критичным файлам SSSD	System Security Services Daemon (SSSD) – это пакет приложений для управления аутентификацией и авторизацией в операционных системах на базе Linux. SSSD является альтернативой Samba и позволяет подключить Linux-машину к уже имеющемуся домену Active Directory или FreeIPA. Поскольку служба SSSD отвечает за аутентификацию, файлы SSSD содержат критичные данные, к которым может быть получен доступ. Файлы SSSD могут хранить информацию о хэшах паролей пользователей. Атакующий может использовать его для подбора пароля учетных записей с помощью хэша.	• Initial Access (TA0001) • Credential Access (TA0006) • OS Credential Dumping (T1003) • Cached Domain Credentials (T1003.005) • Valid Accounts (T1078) • Domain Accounts (T1078.002) • Steal or Forge Kerberos Tickets (T1558)
RV-D-915	Подбор пароля пользователя Linux	Правило детектирует перебор паролей для одного пользователя. Для получения доступа к учетной записи или хосту атакующий может попробовать подобрать пароль с помощью перебора. При срабатывании правила рекомендуется выяснить необходимую информацию у владельца учетной записи.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)
RV-D-916	Успешный подбор пароля пользователя Linux	Правило детектирует перебор паролей для одного пользователя с последующим успешным входом. Для получения доступа к учетной записи или хосту атакующий может попробовать подобрать пароль с помощью перебора.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-919	Изменение конфигурационных файлов службы firewalld	Изменение конфигурационных файлов брандмауэра может позволить атакующим получить доступ к системе через открытые порты, что может привести к компрометации данных или установке вредоносного ПО. При срабатывании данного правила необходимо связаться с владельцем учетной записи, от имени которой произошло событие, для уточнения легитимности действий. Если действия не подтверждены владельцем, необходимо заблокировать скомпрометированную учетную запись и восстановить работу firewalld.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify System Firewall (T1562.004) • Network Boundary Bridging (T1599)
RV-D-920	Отключение или изменение службы SELinux	SELinux (Security-Enhanced Linux) — это механизм мандатного контроля доступа в операционных системах Linux, обеспечивающий дополнительный уровень безопасности посредством принудительного применения политик доступа. Правило детектирует попытки отключения или изменения режима работы SELinux, что может свидетельствовать о попытках атакующего обойти защитные механизмы системы. При срабатывании данного правила рекомендуется немедленно проверить учетную запись и действия пользователя, инициировавшего изменение. При подтверждении нелегитимной активности - восстановить исходные настройки SELinux и провести расследование на предмет возможной компрометации системы.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-921	Изменение привилегий файлов Linux	Правило обнаруживает использование системных вызовов chmod/chown. В Linux DAC (Discretionary access control) является основным средством контроля доступа к файлам. У каждого файла имеются владелец и права, которые задают действия, которые может выполнять владелец. Данный вызов может использоваться атакующими для изменения прав на файл или директорию, что может приводить к обходу защиты или закреплению в системе. В случае срабатывания данного правила необходимо связаться с владельцем учетной записи, от имени которой произошло событие, чтобы уточнить легитимность действий. Если владелец не подтверждает легитимность, нужно заблокировать учетную запись, разорвать все активные сессии и провести расследование с целью выявления возможной компрометации других хостов в сети.	• Defense Evasion (TA0005) • File and Directory Permissions Modification (T1222) • Linux and Mac File and Directory Permissions Modification (T1222.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-922	Изменение настроек для скрытия пользователей	Данное правило отслеживает выполнение команд, которые используются для изменения настроек, направленных на сокрытие учетных записей пользователей в системе Linux. Такие действия могут быть частью процесса подготовки скрытых учетных записей для последующего использования атакующими. Например, команды `gsettings` и `crudini` могут быть использованы для изменения видимости пользователей на экране входа или в системных службах. При обнаружении подобных команд рекомендуется немедленно проверить контекст выполнения, учетную запись инициатора, а также состояние системы на предмет компрометации.	• Defense Evasion (TA0005) • Hide Artifacts (T1564) • Hidden Users (T1564.002)
RV-D-923	Создание/изменение скрытых файлов Linux	Скрытые файлы в Linux обозначаются с помощью точки (.) в начале названия файла. Атакующие могут использовать данные файлы для сокрытия вредоносных файлов. Часто такие файлы создаются в доступных для непривилегированного пользователя директориях: `/tmp`, `/var/tmp`, `/dev/shm`, `/home`. В случае срабатывания правила и подтверждения нелегитимной активности необходимо незамедлительно изолировать хост и отключить скомпрометированную учетную запись. Далее проверить возможные пути распространения атаки и осуществить поиск изначальной причины компрометации узла/учетной записи.	• Defense Evasion (TA0005) • Hide Artifacts (T1564) • Hidden Files and Directories (T1564.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-924	Создание/изменение скрытых shared object файлов	Правило обнаруживает создание/изменение shared object скрытых файлов в определенных директориях. Названия скрытых файлов начинаются с символа `.`. Файлы с расширением `.so` содержат динамически загружаемую разделяемую библиотеку. Атакующие используют комбинацию скрытых файлов (для маскировки) и формата `.so` (для выполнения кода) для внедрения в системные процессы. Это позволяет им оставаться в системе после перезагрузки, повышать привилегии и скрывать свое присутствие. Данная техника также используется различным вредоносным ПО, включая руткиты и майнеры. В случае возникновения инцидента требуется опросить ответственного за учетную запись инициатора активности. Если легитимность подтвердить не удалось, удалить добавленный/измененный скрытый shared object файл и заблокировать УЗ инициатора на время выяснения обстоятельств инцидента ИБ.	• Defense Evasion (TA0005) • Hide Artifacts (T1564) • Hidden Files and Directories (T1564.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-925	Загрузка кода в процесс Linux	Правило обнаруживает использование системного вызова memfd_create в отношении популярных у атакующих процессов. Данный вызов может использоваться атакующими для внедрения вредоносного кода в память процесса, что позволяет обходить применяемые средства защиты и обеспечивает закрепление в системе. При срабатывании правила необходимо проанализировать процесс, инициировавший вызов, включая его аргументы и окружение, проверить целостность связанных исполняемых файлов, а также исследовать поведение целевого процесса на предмет аномалий. В случае подтверждения компрометации рекомендуется изолировать скомпрометированный хост до завершения мероприятий по реагированию.	• Defense Evasion (TA0005) • Reflective Code Loading (T1620)

ID правила	Название правила	Описание	Тактики и техники
RV-D-926	Изменение корневых сертификатов Linux	Корневые сертификаты (root certificates) являются основой инфраструктуры публичных ключей (PKI) и используются для обеспечения безопасности и доверия. Атакующие могут установить корневой сертификат на скомпрометированной системе, чтобы избежать предупреждений при подключении к контролируемым ими веб-серверам. При обнаружении подобных команд рекомендуется немедленно проверить контекст выполнения, учетную запись инициатора, а также состояние системы на предмет компрометации.	• Defense Evasion (TA0005) • Subvert Trust Controls (T1553) • Install Root Certificate (T1553.004)
RV-D-927	Обнаружение стеганографии в Linux	Данное правило предназначено для обнаружения запуска утилит steghide, stegpy и stegolsb, которые могут использоваться для сокрытия или извлечения скриптов bash в изображениях или аудиофайлах. Такие методы позволяют атакующим скрывать вредоносный код, значительно усложняя его выявление стандартными средствами мониторинга. При срабатывании правила рекомендуется уточнить легитимность действий у пользователя, инициировавшего изменения, а также проверить ключи, с которыми были запущены утилиты, чтобы понять характер и цель их использования.	• Defense Evasion (TA0005) • Obfuscated Files or Information (T1027) • Steganography (T1027.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-928	Изменение tmp файлов логирования Linux	Правило обнаруживает потенциально вредоносную активность, связанную с модификацией временных лог-файлов в директориях `/tmp`. Атакующий может изменять или очищать временные логи, чтобы удалить записи о выполненных им командах, попытках доступа или других следах своей деятельности.	• Defense Evasion (TA0005) • Indicator Removal (T1070) • Clear Linux or Mac System Logs (T1070.002)
RV-D-929	Чтение файлов с историей команд	В Unix-системах команды, введенные пользователем в командной оболочке (shell), обычно сохраняются в специальных файлах истории. Атакующий может получить доступ к этим файлам и извлечь из них информацию о действиях пользователей, которая может содержать сведения об используемых учетных записях и другую конфиденциальную информацию.	• Credential Access (TA0006) • Unsecured Credentials (T1552) • Shell History (T1552.003)
RV-D-930	Чтение файлов с пользовательскими учетными данными	Правило обнаруживает попытки прочитать файлы с данными учетных записей пользователей, а также использование инструментов, позволяющих осуществлять дамп учетных данных из этих файлов, например, утилиты hashdump.	• Credential Access (TA0006) • OS Credential Dumping (T1003) • /etc/passwd and /etc/shadow (T1003.008) • Unsecured Credentials (T1552) • Credentials In Files (T1552.001)
RV-D-931	Подбор пароля на хосте Linux	Правило детектирует перебор пароля для разных пользователей на одном хосте. Для получения доступа к учетной записи или хосту атакующий может попробовать подобрать пароль с помощью перебора.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-932	Успешный подбор пароля на хосте Linux	Правило детектирует перебор учетных записей на одном хосте с последующим успешным входом. Для получения доступа к учетной записи или хосту атакующий может попробовать подобрать пароль с помощью перебора.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001) • Password Spraying (T1110.003)
RV-D-944	Изменение задач cron	Cron – это планировщик задач Linux, который позволяет автоматизированно выполнять запланированные задачи на устройстве по заранее заданному триггеру. Атакующий может создать задачу или модифицировать существующую так, чтобы выполнялся его вредоносный код, таким образом происходит закрепление в системе. Данная техника привлекает атакующих тем, что запланированные задачи являются легитимными, что позволяет замаскировать вредоносные действия, а сам функционал планировщика задач не будет отключен администраторами, так как на нем строится работа системы. Правило детектирует изменения в диспетчере запланированных задач cron.	• Persistence (TA0003) • Scheduled Task/Job (T1053) • Cron (T1053.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-945	Изменение критичных файлов Linux	В Linux все конфигурации и настройки представлены файлами. Атакующий может изменять файлы различных конфигураций для закрепления, сокрытия своих действий, повышения привилегий. Так, например, изменение конфигурации сервисов атакующим может привести к выполнению вредоносного кода. Изменение файлов конфигурации auditd может привести к отключению подсистемы мониторинга событий, таким образом действия атакующего будут не обнаружены. Изменение ssh config может привести к закреплению в системе. Изменение библиотеки ld_preload может привести к сокрытию или закреплению атакующего путем скрытого выполнения вредоносного кода. Изменение файлов загрузки также приводит к закреплению через внедрение кода при загрузке системы. Изменение файлов конфигурации модулей может позволить атакующему внедрить свой модуль в ядро. Изменение сетевых файлов может позволить распространиться по сети или наоборот отключить хост от мониторинга. В файле конфигурации сервиса BIND настраиваются зоны DNS, которые определяют, как разрешать имена в сети. Это предоставляет атакующим возможность манипулировать настройками DNS-сервера для подмены DNS-записей. Также через конфигурационный файл можно отключать DNSSEC или изменять настройки ACL. Правило обнаруживает любые	• Persistence (TA0003) • Defense Evasion (TA0005) • Credential Access (TA0006) • Masquerading (T1036) • Masquerade Task or Service (T1036.004) • Boot or Logon Initialization Scripts (T1037) • RC Scripts (T1037.004) • Indicator Removal (T1070) • Clear Linux or Mac System Logs (T1070.002) • Account Manipulation (T1098) • SSH Authorized Keys (T1098.004) • Create or Modify System Process (T1543) • Systemd Service (T1543.002) • Event Triggered Execution (T1546) • Unix Shell Configuration Modification (T1546.004) • Modify Authentication Process (T1556) • Pluggable Authentication Modules (T1556.003) • Impair Defenses (T1562)

ID правила	Название правила	Описание	Тактики и техники
RV-D-946	Кратковременное существование учетной записи	Данное правило выявляет случаи создания и последующего удаления учетной записи или группы в короткий промежуток времени. Такой сценарий может указывать на попытки атакующего скрыть следы своей активности. Правило анализирует события ADD_USER, DEL_USER, ADD_GROUP и DEL_GROUP из auth.log и auditd, сопоставляя создание и удаление одного и того же объекта в течение 120 секунд. Легитимные срабатывания могут быть связаны с административными ошибками или тестированием.	• Persistence (TA0003) • Account Manipulation (T1098) • Create Account (T1136) • Local Account (T1136.001)
RV-D-947	Изменение настроек пользователя	Правило обнаруживает изменения настроек пользователя, включая изменения профилей и привилегий. Обычно данные изменения доступны только привилегированному пользователю и используются атакующим для закрепления в системе. Однако при некорректной настройке доступов они могут использоваться и для повышения привилегий. Атакующий может как вносить изменения в файлы вручную, так и воспользоваться специальными утилитами, такими как usermod или groupmod.	• Persistence (TA0003) • Account Manipulation (T1098) • Additional Local or Domain Groups (T1098.007) • Abuse Elevation Control Mechanism (T1548) • Sudo and Sudo Caching (T1548.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-967	Изменение файлов в домашнем каталоге другим пользователем	Правило обнаруживает изменения файлов в домашнем каталоге другим пользователем на узле Linux. Атакующий, попав на хост, может попытаться изменить файлы в директории другого пользователя для закрепления под данным пользователем или получения контроля над его данными. В случае обнаружения активности требуется уточнить причины выполненных действий у владельца учетной записи или ответственного за хост. В случае подтверждения нелегитимной активности рекомендуется изолировать хост, заблокировать пользователя, проверить, откуда было произведено подключение, убедиться, что не были скомпрометированы другие узлы и пользователи. После этого необходимо сбросить пароли учетных записей, обновить сертификаты, провести внутреннее расследование с целью установления возможных методов закрепления в системе и причин возникновения инцидента.	• Persistence (TA0003) • Data Manipulation (T1565) • Stored Data Manipulation (T1565.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-970	Закрепление при помощи утилиты Trap	Атакующие могут использовать обработчик ошибок Trap для закрепления в системе. Обработчик Trap может обрабатывать сигналы, например SIGINT (прерывание, вызванное нажатием CTRL+C). При помещении полезной нагрузки в сигнал и нажатии CTRL+C вместо завершения программы сигнал SIGINT активируется и выполнит полезную нагрузку. Правило нацелено на мониторинг размещения полезной нагрузки в Trap при помощи событий process-creation. При срабатывании правила рекомендуется проверить команду, добавленную в обработчик сигнала, и установить источник выполнения. Если команда выглядит подозрительно, следует проанализировать активность пользователя и рассмотреть возможность изоляции узла для дальнейшего расследования.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Event Triggered Execution (T1546) • Trap (T1546.005)
RV-D-973	Добавление/удаление модулей ядра Linux	Модули ядра – это фрагменты кода, которые могут быть загружены и выгружены в ядро по требованию. Они расширяют функциональность ядра без необходимости перезагрузки системы. Атакующий может пытаться внедрить свой модуль для закрепления в системе или удалить уже существующие для обхода защиты. Правило обнаруживает добавление или удаление модулей ядра Linux с помощью соответствующих системных вызовов.	• Persistence (TA0003) • Defense Evasion (TA0005) • Rootkit (T1014) • Boot or Logon Autostart Execution (T1547) • Kernel Modules and Extensions (T1547.006)

ID правила	Название правила	Описание	Тактики и техники
RV-D-974	Чтение файлов с закрытыми ключами SSH	В Unix-системах закрытые ключи представляют собой конфиденциальные криптографические данные, обычно используемые для аутентификации пользователя в системах, где реализован протокол SSH (Secure Shell). Закрытый ключ и соответствующий ему открытый ключ являются частью пары ключей. Закрытый ключ должен храниться в тайне и защищаться от несанкционированного доступа, в то время как открытый ключ может быть свободно распространяем. Если атакующий получит доступ к закрытому ключу пользователя, он сможет аутентифицироваться на всех серверах, где этот ключ является доверенным. Это может привести к полной компрометации учетной записи и системных ресурсов.	• Credential Access (TA0006) • Unsecured Credentials (T1552) • Private Keys (T1552.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-975	Чтение памяти процессов на Linux	Данное правило обнаруживает попытки прочитать файлы `/proc/[pid]/maps` и `/proc/[pid]/mem`. Файл `/proc/[pid]/maps` содержит информацию о карте памяти процесса: какие области памяти и с какими правами доступа он использует. Файл `/proc/[pid]/mem` позволяет читать и изменять содержимое памяти процесса. Чтение или изменение этих файлов является признаком попытки получить доступ к памяти другого процесса. Такая активность часто используется вредоносными программами или инструментами для кражи паролей, например MimiPenguin, а также для внедрения кода в процессы через файловую систему `/proc`.	• Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Credential Access (TA0006) • OS Credential Dumping (T1003) • Proc Filesystem (T1003.007) • Process Injection (T1055) • Proc Memory (T1055.009)
RV-D-978	Создание/изменение правила nf_tables	nf_tables - это подсистема ядра Linux, обеспечивающая фильтрацию и классификацию сетевых пакетов/дейтаграмм/фреймов. Из-за архитектурных особенностей выполнения данного модуля в последнее время обнаруживается множество уязвимостей с использованием nftables, например, CVE-2023-4015, CVE-2023-35001, CVE-2024-1086 и другие. Для взаимодействия с данным модулем в Linux существует специальный тип сокета - NETLINK_NETFILTER, вызов которого и отслеживается в данном правиле.	• Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Exploitation for Privilege Escalation (T1068) • Impair Defenses (T1562) • Disable or Modify System Firewall (T1562.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-979	Внедрение процесса в другой через ptrace	Внедрение системных вызовов ptrace - это метод выполнения произвольного кода в адресном пространстве отдельного активного процесса. Атакующие могут внедрять вредоносный код в процессы с помощью системных вызовов ptrace, чтобы обойти защиту на основе процессов, получить доступ к конфиденциальным данным, таким как пароли ssh, а также повысить привилегии, например, DirtyCow. По умолчанию в системах Linux вызов ptrace не используется программами в фоновом режиме, однако может использоваться сторонним ПО.	• Privilege Escalation (TA0004) • Process Injection (T1055) • Ptrace System Calls (T1055.008)
RV-D-1010	Использование средств туннелирования трафика Linux	Средства туннелирования трафика, такие как ngrok, rsockstun, localtonet и другие, активно используются атакующими для организации обратных туннелей и проксирования трафика, позволяя обходить сетевые ограничения и устанавливать устойчивую связь с инфраструктурой управления (C2). Данное правило отслеживает запуск утилит с параметрами, характерными для организации обратных туннелей (revsocks, rsockstun, chisel).	• Defense Evasion (TA0005) • Command and Control (TA0011) • Proxy (T1090) • Protocol Tunneling (T1572) • Encrypted Channel (T1573) • Network Boundary Bridging (T1599)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1015	Использование хакерской утилиты в Linux	Правило обнаруживает запуск утилит, идентифицируемых по имени целевого процесса, которые могут применяться для проведения атак.	• Execution (TA0002) • Defense Evasion (TA0005) • Command and Control (TA0011) • Exfiltration (TA0010) • Direct Volume Access (T1006) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Windows Command Shell (T1059.003) • Proxy (T1090) • Exfiltration Over Web Service (T1567) • Exfiltration to Cloud Storage (T1567.002) • Protocol Tunneling (T1572) • Encrypted Channel (T1573) • Develop Capabilities (T1587)
RV-D-1099	Reverse shell через Bash-сценарий	Reverse shell (Обратное подключение) — метод, используемый атакующими для получения контроля над системой через установленное сетевое соединение с хоста жертвы на хост атакующего. Правило отслеживает создание сетевого соединения командной оболочкой Bash.	• Execution (TA0002) • Command and Control (TA0011) • Command and Scripting Interpreter (T1059) • Unix Shell (T1059.004) • Non-Standard Port (T1571)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1100	Создан Reverse shell сторонней утилитой в Linux	Reverse shell (Обратное подключение) — метод, используемый атакующими для получения контроля над системой через установленное сетевое соединение с хоста жертвы на хост атакующего. Правило детектирует сетевые соединения и последующий запуск командной оболочки.	• Execution (TA0002) • Command and Scripting Interpreter (T1059) • Unix Shell (T1059.004) • Python (T1059.006)
RV-D-1101	Создание подозрительного Named Pipe с помощью mkfifo	Обнаруживает создание нового именованного pipe с помощью утилиты mkfifo в потенциально подозрительной директории.	• Execution (TA0002) • Lateral Movement (TA0008) • Inter-Process Communication (T1559) • Lateral Tool Transfer (T1570)
RV-D-1104	Сетевое обращение от подозрительного скрипта в Linux	Запуск скриптов с расширениями `.py`, `.js`, `.rb`, `.php`, `.sh`, `.pl`, `.groovy`, `.ts`, `.kts` может свидетельствовать о потенциально вредоносной активности. Если такие скрипты устанавливают исходящие сетевые соединения, это может указывать на попытку передачи конфиденциальных данных или получение удаленного доступа к системе.	• Execution (TA0002) • Command and Control (TA0011) • Command and Scripting Interpreter (T1059) • Unix Shell (T1059.004) • User Execution (T1204) • Malicious File (T1204.002) • Non-Standard Port (T1571)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1105	Эксплуатация уязвимости CVE-2023-46944 VSCode на Linux	Правило срабатывает при открытии Git-репозитория в VSCode, как в доверенной, так и в недоверенной среде, где файле `.git/config` в функции fsmonitor указана вредоносная команда. Данная активность относится к уязвимой версии расширения GitLens до 13.6.0 включительно, ей присвоен номер CVE-2023-46944. Также данная активность может возникнуть при открытии вредоносного Git-репозитория в доверенной среде, но с исправленной версией GitLens или вообще без установленного расширения в версиях редактора выше 1.63.1.	• Execution (TA0002) • Exploitation for Client Execution (T1203)
RV-D-1106	Создание интерактивной оболочки через GTFOBins	GTFOBins — это открытый проект, представляющий собой каталог бинарных файлов UNIX/Linux, которые могут быть использованы атакующими для обхода ограничений безопасности в системе. Эти утилиты обычно предустановлены на большинстве Linux-систем и обладают возможностями, которые могут быть использованы для выполнения различных действий.	• Execution (TA0002) • Command and Scripting Interpreter (T1059) • Unix Shell (T1059.004) • Lua (T1059.011) • System Binary Proxy Execution (T1218)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1108	Повышение привилегий до root	Правило обнаруживает смену непривилегированного пользователя на пользователя root, что может свидетельствовать о повышении привилегий. Атакующие зачастую пытаются поднять привилегии до root и дальше работать уже от имени привилегированного аккаунта.	• Initial Access (TA0001) • Persistence (TA0003) • Privilege Escalation (TA0004) • Exploitation for Privilege Escalation (T1068) • Valid Accounts (T1078) • Local Accounts (T1078.003) • Account Manipulation (T1098)
RV-D-1109	Повышение привилегий с помощью GTFOBins	GTFOBins — это открытый проект, представляющий собой каталог бинарных файлов UNIX/Linux, которые могут быть использованы атакующими для обхода ограничений безопасности в системе. Также, в случае неправильных настроек безопасности, с помощью данных утилит можно повысить привилегии в системе, на что и направлено данное правило. Утилиты обычно предустановлены на большинстве Linux-систем и обладают функциональностью, которая может быть использована для выполнения различных действий.	• Execution (TA0002) • Privilege Escalation (TA0004) • Command and Scripting Interpreter (T1059) • Unix Shell (T1059.004) • Lua (T1059.011) • Abuse Elevation Control Mechanism (T1548) • Setuid and Setgid (T1548.001) • Sudo and Sudo Caching (T1548.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1110	Использование утилиты fusermount	fusermount — это утилита, используемая для монтирования и размонтирования файловых систем, работающих через FUSE (Filesystem in Userspace). Утилита fusermount может быть использована для эксплуатации уязвимостей, связанных с файловыми системами, такими как OverlayFS. Уязвимость OverlayFS (CVE-2023-0386) позволяет непривилегированному пользователю создавать исполняемые файлы с SUID-битом и с их помощью получать привилегии root. При срабатывании данного правила рекомендуется немедленно проверить учетную запись и действия пользователя, запустившего команду. При подтверждении нелегитимной активности — заблокировать УЗ инициатора и провести расследование на предмет возможной компрометации системы.	• Privilege Escalation (TA0004) • Exploitation for Privilege Escalation (T1068)
RV-D-1111	Использование утилиты at	Утилита at используется для выполнения задач в определенное время. Атакующие могут использовать ее для выполнения вредоносного кода и закрепления в системе.	• Persistence (TA0003) • Scheduled Task/Job (T1053) • At (T1053.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1112	Изменение timers на хосте Linux	Timers в Linux — это механизм, позволяющий выполнять определенные действия по расписанию или через заданные интервалы времени. Таймеры используются для выполнения задач, которые должны запускаться в будущем или периодически. Атакующие могут использовать данный функционал для выполнения вредоносного кода и закрепления в системе.	• Execution (TA0002) • Scheduled Task/Job (T1053) • Systemd Timers (T1053.006)
RV-D-1114	Модификация разрешений системных файлов в Linux	Изменение прав доступа к файлам может свидетельствовать о подозрительной активности, связанной с попытками атакующих получить несанкционированный доступ к системным ресурсам. Такие операции могут использоваться для повышения привилегий процесса или обхода механизма контроля доступа, закрепления в системе. Если данная активность инициализируется вне контекста обычных операций системы, это может свидетельствовать о компрометации системы. При обнаружении такого события рекомендуется тщательно проверить источники и цели изменений, удостовериться в легитимности действий пользователя, инициировавшего изменения. При наличии признаков злоупотребления — ограничить доступ пользователя, проанализировать журналы и провести полное расследование на предмет возможной компрометации системы.	• Persistence (TA0003) • File and Directory Permissions Modification (T1222) • Linux and Mac File and Directory Permissions Modification (T1222.002) • Abuse Elevation Control Mechanism (T1548) • Setuid and Setgid (T1548.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1115	Создание файла через Python/Ruby-сценарий	Правило предназначено для обнаружения случаев создания новых файлов при помощи сценариев на Python или Ruby. Эта техника может быть использована атакующими для сохранения полезной нагрузки или выполнения действий в рамках подготовки к атаке. Данное правило нацелено на идентификацию подозрительных операций, связанных с созданием файлов с использованием скриптов.	• Execution (TA0002) • Command and Scripting Interpreter (T1059) • Python (T1059.006)
RV-D-1116	Обнаружена команда Reverse/Bind shell	Правило обнаруживает выполнение команд, создающих Reverse или Bind shell, что может указывать на компрометацию системы. Атакующие могут использовать данный метод для получения контроля над системой через сетевое соединение с хостом атакующего.	• Execution (TA0002) • Command and Control (TA0011) • Command and Scripting Interpreter (T1059) • Unix Shell (T1059.004) • Python (T1059.006) • Non-Standard Port (T1571)
RV-D-1122	Вызов команды из модуля PAM	Обнаружение использования команд, выполненных из модуля PAM Linux. Атакующий может внедрить в PAM вредоносный код для получения учетных данных пользователей или закрепления в системе.	• Persistence (TA0003) • Credential Access (TA0006) • Modify Authentication Process (T1556) • Pluggable Authentication Modules (T1556.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1132	Дамп памяти утилитой MimiPenguin на Linux	Правило детектирует попытки использования утилиты MimiPenguin для извлечения паролей из памяти процессов. Данное правило позволяет детектировать использование команд для дампа памяти, что является одним из признаков работы утилиты.	• Credential Access (TA0006) • OS Credential Dumping (T1003) • Proc Filesystem (T1003.007) • /etc/passwd and /etc/shadow (T1003.008)
RV-D-1137	Построение образа в Linux	Правило обнаруживает команды для создания образа контейнера, используемые, чтобы обойти защиту от получения вредоносных образов из общедоступных реестров.	• Defense Evasion (TA0005) • Build Image on Host (T1612)
RV-D-1138	Перехват SSH-сессии	Атакующие могут осуществлять перехват активных SSH-сессий для получения несанкционированного доступа к конфиденциальной информации или продвижения по инфраструктуре. Правило обнаруживает попытки чтения файла `/proc/<pid>/environ` SSH-процесса, принадлежащего другому пользователю, что позволяет извлечь критичные переменные окружения, включая SSH_AUTH_SOCK. Обладая данными переменными, атакующий может использовать SSH-агент жертвы для аутентификации на удаленных системах без необходимости знания паролей или доступа к файлам ключей, что приводит к эскалации привилегий и неконтролируемому перемещению по сети.	• Lateral Movement (TA0008) • Remote Service Session Hijacking (T1563) • SSH Hijacking (T1563.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1156	Аномальное Bind-монтирование	Bind Mounts (связанные монтирования) – это техника сокрытия артефактов, которая позволяет атакующим скрывать свою активность от системных утилит, создавая ложное представление о выполняющихся процессах. Bind Mounts сопоставляет каталог или файл из одного места файловой системы в другое, аналогично ярлыкам в Windows.	• Defense Evasion (TA0005) • Hide Artifacts (T1564) • Bind Mounts (T1564.013)
RV-D-1334	Атака regreSSHion	При попытке аутентификации в сервисе SSH у пользователя есть лимит времени, чтобы завершить процесс (по умолчанию 120 секунд). Если аутентификация не произошла, sshd-сервер асинхронно вызывает сигнальную функцию sigalarm, которая в свою очередь вызывает системные функции управления памятью, причем небезопасным для асинхронного выполнения образом. При выполнении атакующим ряда условий, с некоторой (достаточно небольшой) вероятностью это вызывает состояние гонки (race condition), приводящее к нарушению границ памяти и выполнению произвольного кода на сервере.	• Initial Access (TA0001) • Exploit Public-Facing Application (T1190)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1552	Отключение узла Linux	Правило детектирует события инициирования выключения или перезагрузки Linux-узла на основе выполнения команд systemctl, reboot, poweroff, shutdown, а также вызовов init с уровнями 0 и 6. Подобные действия могут быть как частью штатного администрирования (плановые работы, обновления, управление сервисами), так и признаком вредоносной активности. Атакующие нередко используют перезагрузку или выключение системы для нарушения доступности сервисов (DoS) либо сокрытия следов компрометации, включая очистку volatile-артефактов, прерывание процессов мониторинга и усложнение расследования.	• Impact (TA0040) • System Shutdown/Reboot (T1529)
RV-D-1558	Удаление пользователя или группы	Правило выявляет удаление локальной учетной записи или группы в операционной системе Linux. Данная активность может свидетельствовать о попытках атакующего скрыть следы компрометации (Anti-forensics), нарушить работу системных сервисов или дестабилизировать управление доступом на хосте. Правило анализирует события выполнения системных утилит userdel и groupdel для обнаружения фактов модификации локальной базы пользователей и групп.	• Persistence (TA0003) • Account Manipulation (T1098) • Create Account (T1136) • Local Account (T1136.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1566	Изменение меток времени через touch Linux	Атакующие могут изменять атрибуты времени файлов, чтобы скрыть новые файлы или изменения в существующих. Timestomping — это относительно простая, но эффективная техника сокрытия следов, активно применяемая в атакующих цепочках. Она может быть реализована с использованием встроенной утилиты touch, которая может изменять значения atime и mtime, что и используется атакующими для сокрытия следов путем установки произвольных дат доступа и модификации файлов.	• Defense Evasion (TA0005) • Indicator Removal (T1070) • Timestomp (T1070.006)
RV-D-1603	Запуск процесса из нестандартной директории	Обнаружение запуска процессов из нестандартных директорий в Linux, не относящихся к типовым системным путям (/bin, /usr/bin, /usr/sbin и др.). Подобное поведение может указывать на выполнение пользовательских или вредоносных бинарных файлов, размещенных в нестандартных локациях (например, /tmp, /var/tmp, домашние директории пользователей).	• Execution (TA0002) • Defense Evasion (TA0005) • Masquerading (T1036) • Match Legitimate Resource Name or Location (T1036.005)

Linux R-Vision Endpoint

- Linux R-Vision Endpoint: настройка источника

Linux R-Vision Endpoint: настройка источника

Данное руководство описывает процесс сбора и отправки событий операционных систем на основе ядра Linux в R-Vision SIEM с помощью агента платформы R-Vision.

Предварительные требования

Перед началом настройки убедитесь, что выполнены следующие условия:

- Версия ядра Linux на машинах, с которых планируется сбор событий, не ниже 5.10
- Ядро Linux должно поддерживать BPF

Настройка ОС Linux

Настройка сбора событий ОС Linux с помощью агента платформы R-Vision включает установку агента R-Vision на конечное устройство и конфигурирование группы агентов.

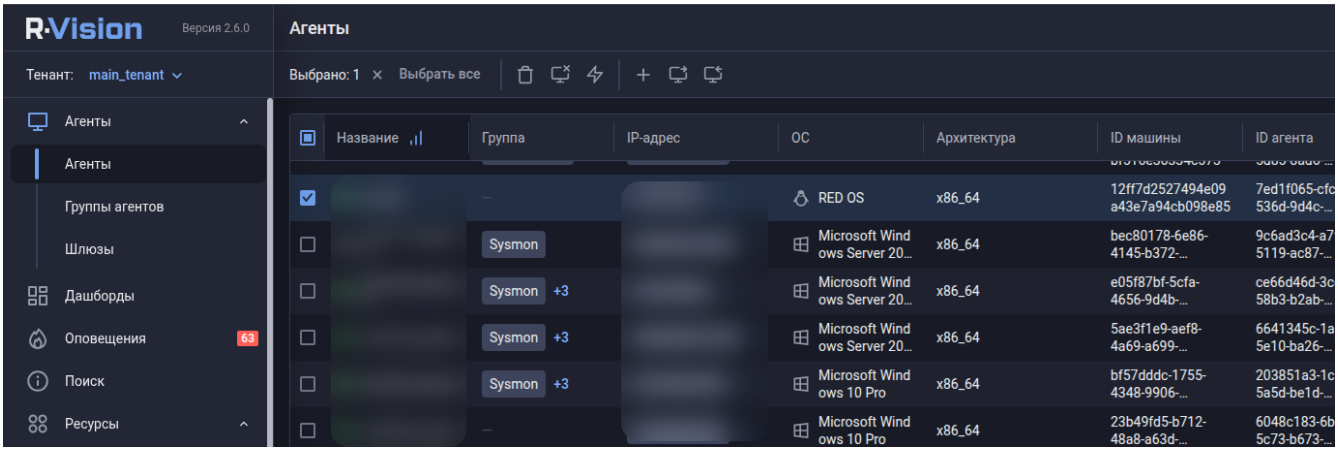
Установка агента

Установите агент R-Vision Endpoint на станцию и настройте его связь с кластером R-Vision SIEM. После этого в веб-интерфейсе R-Vision SIEM в разделе **Агенты** появится информация о подключенном хосте.

Для установки агента обратитесь к документации продукта R-Vision SIEM.

Для настройки подключения агента R-Vision Endpoint к кластеру R-Vision SIEM обратитесь к документации продукта R-Vision SIEM.

После настройки связи агента с кластером R-Vision SIEM, убедитесь, что рабочая станция появилась в списке агентов:



Настройка в R-Vision SIEM

Настройка отправки событий в R-Vision SIEM

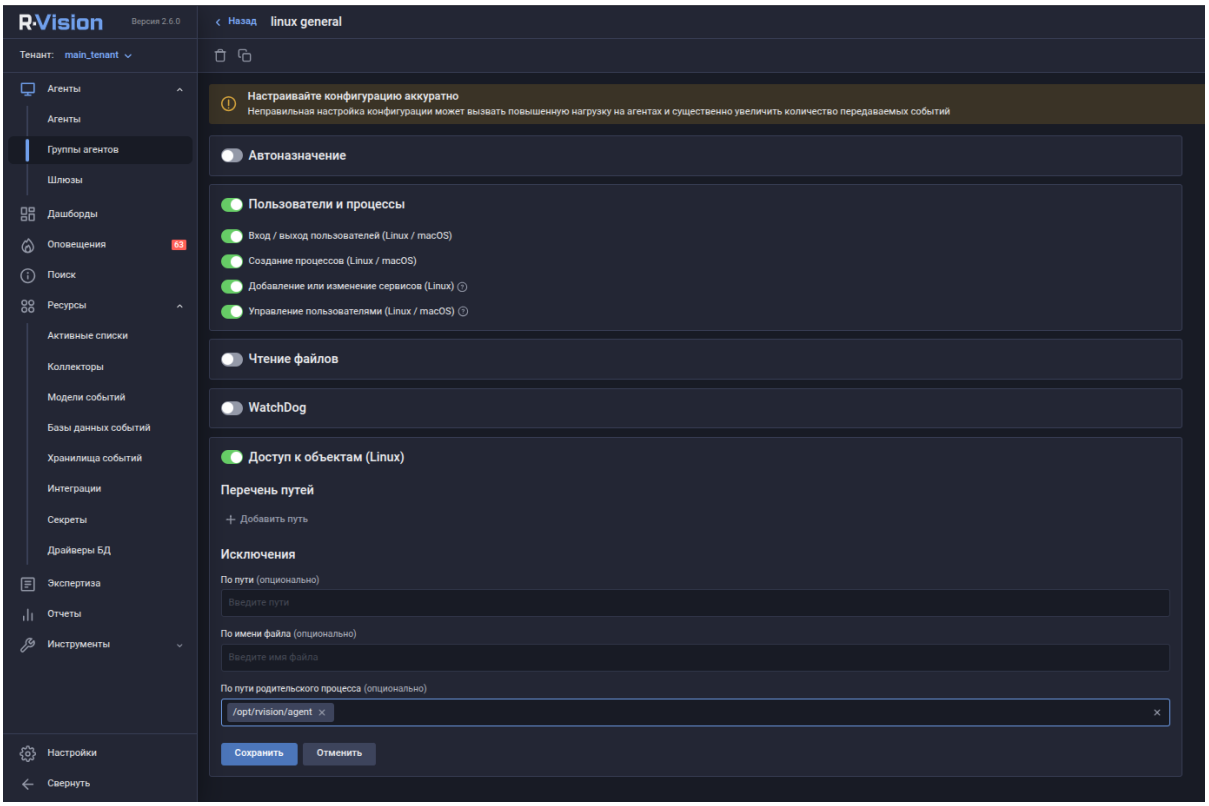
1. В веб-интерфейсе R-Vision SIEM перейдите в раздел **Агенты** → **Группы агентов**.
2. Создайте группу и добавьте в нее узел, на котором установлен агент.
3. В созданной группе узлов в секции **Пользователи и процессы** переведите следующие переключатели в активное положение:
   - **Вход/выход пользователей (Linux / macOS)**;
   - **Создание процессов (Linux / macOS)**;
   - **Добавление или изменение сервисов (Linux)**;
   - **Управление пользователями (Linux / macOS)**.
4. В созданной группе узлов в секции **Доступ к объектам (Linux)** добавьте **Исключения**:

Добавление исключения нужно для того, чтобы агент не "спамил" событиями о своей активности. Аналогично можно добавить исключения для других

легитимных системных служб.

- **По пути родительского процесса**:
  - `/opt/rvision/agent`

5. Нажмите на кнопку **Сохранить**.



Добавление узла в группу

Для добавления узла под управлением ОС Linux в созданную группу:

1. В веб-интерфейсе R-Vision SIEM перейдите в раздел **Агенты**.
2. Выберите нужный узел и нажмите на кнопку на панели инструментов.
3. Выберите ранее созданную группу и нажмите на кнопку **Добавить**.
4. Дождитесь применения политики группы на агенте.

Настройка обработки событий в R-Vision SIEM

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** с типом **R-Vision Endpoint**.

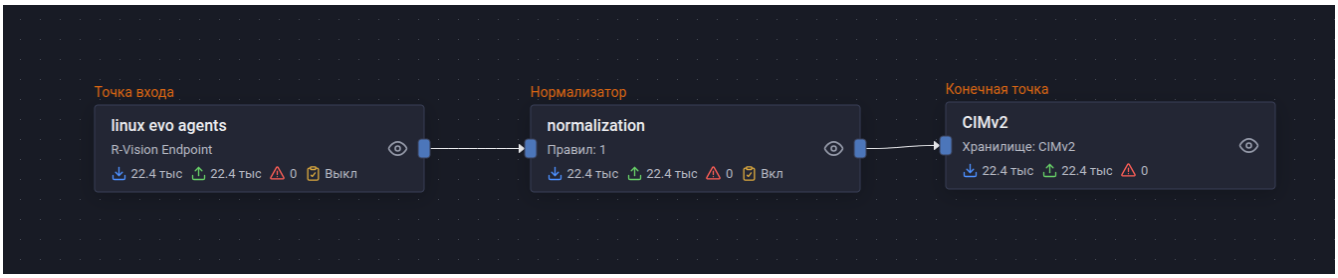


Для настройки точки входа типа R-Vision Endpoint обратитесь к документации продукта R-Vision SIEM.

3. Добавьте на конвейер элемент **Нормализатор** с правилом **R-Vision Endpoint for Linux** (идентификатор правила: **RV-N-299**).
4. Соедините нормализатор с точкой входа.

5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

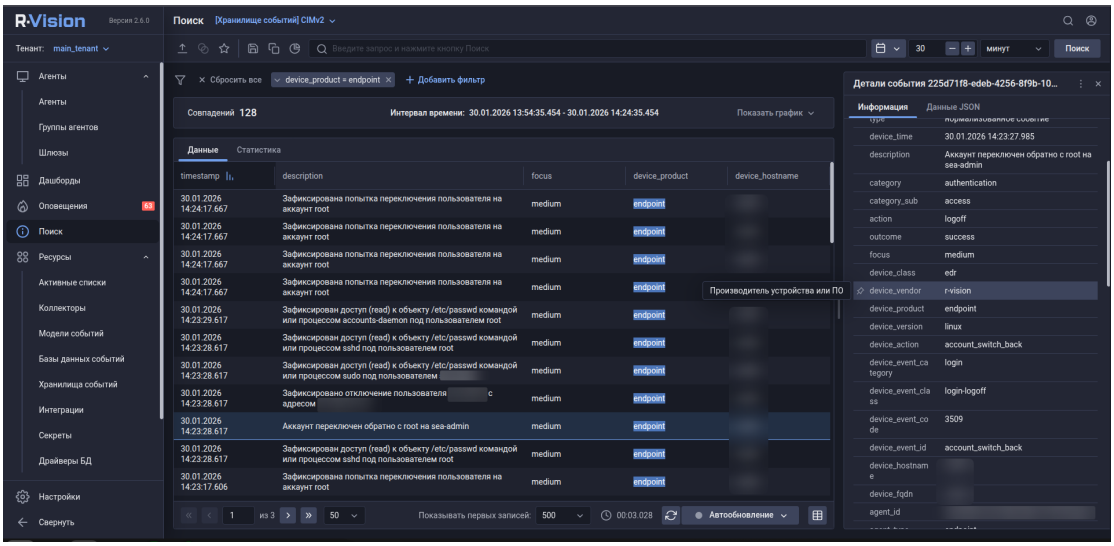
Пример конфигурации конвейера:



После настройки группы агентов и передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события хоста под управлением ОС Linux.

Найти события хоста под управлением ОС Linux в хранилище можно по следующему фильтру:

```
device_product = "endpoint"
```



Microsoft Windows

Раздел содержит инструкции по сбору событий из журналов операционных систем семейства Windows, а также инструкции по настройке параметров аудита.

- Microsoft Active Directory Domain Services (ADDS)
- Microsoft Windows PowerShell
- Microsoft Windows Security
- Microsoft Windows Sysmon
- Microsoft Windows System

- Microsoft Windows Task Scheduler

Microsoft Active Directory Domain Services (ADDS)

- Microsoft Active Directory Domain Services (ADDS): настройка источника

Microsoft Active Directory Domain Services (ADDS): настройка источника

Данное руководство описывает процесс отправки событий из журнала Windows Domain Services в R-Vision SIEM с помощью продукта R-Vision Endpoint в составе платформы EVO.

Настройка Windows для сбора событий ADDS

В этом разделе описана настройка сбора событий журнала Domain Services с помощью R-Vision EVO Agent.

Процесс состоит из трех шагов:

1. Настройка сбора событий журнала Domain Services
2. Установка и подключение агента R-Vision EVO
3. Настройка политики сбора событий в SIEM

Настройка сбора событий журнала Domain Services

Чтобы события появлялись в журнале Domain Services, необходимо включить аудит в настройках Windows. Политику можно применить следующими способами:

- через GPO (рекомендуется для домена);
- локально — для отдельных хостов (не рекомендуется для масштабного использования).

▼ *Настройка через доменные политики*

Предварительные требования

- Ваша Windows-машина должна быть включена в домен.
- Ваша учетная запись должна обладать правами администратора домена (`Domain Admin`).
- Для сбора событий должны быть настроены параметры аудита.

Настройка сбора событий Windows

Чтобы настроить сбор событий Windows, выполните следующие действия:

1. Откройте **Group Policy Management**.
2. Создайте новую GPO или отредактируйте существующую.
3. Перейдите в раздел **Computer Configuration** → **Policies** → **Windows Settings** → **Domain Services Settings** → **Advanced Audit Policy Configuration**.
4. Включите необходимые параметры аудита.
5. Привяжите политику к нужному OU.
6. Дождитесь применения политики на хостах или выполните `gpupdate /force`.

▼ *Настройка через локальные политики*

Предварительные требования

- Ваша учетная запись должна обладать правами локального администратора.
- Для сбора событий должны быть настроены параметры аудита.

Настройка сбора событий Windows

Чтобы настроить сбор событий Windows, выполните следующие действия:

1. Откройте **Local Domain Services Policy** (`secpol.msc`).
2. Перейдите в раздел **Local Policies** → **Audit Policy** или **Advanced Audit Policy Configuration**.
3. Включите необходимые параметры аудита (`Успех` / `Отказ`).
4. Примените изменения.
5. Обновите политики командой `gpupdate /force` или перезагрузите хост.

Настройка параметров аудита

В групповой политике устройства включите следующие параметры:

Расширенный аудит событий:

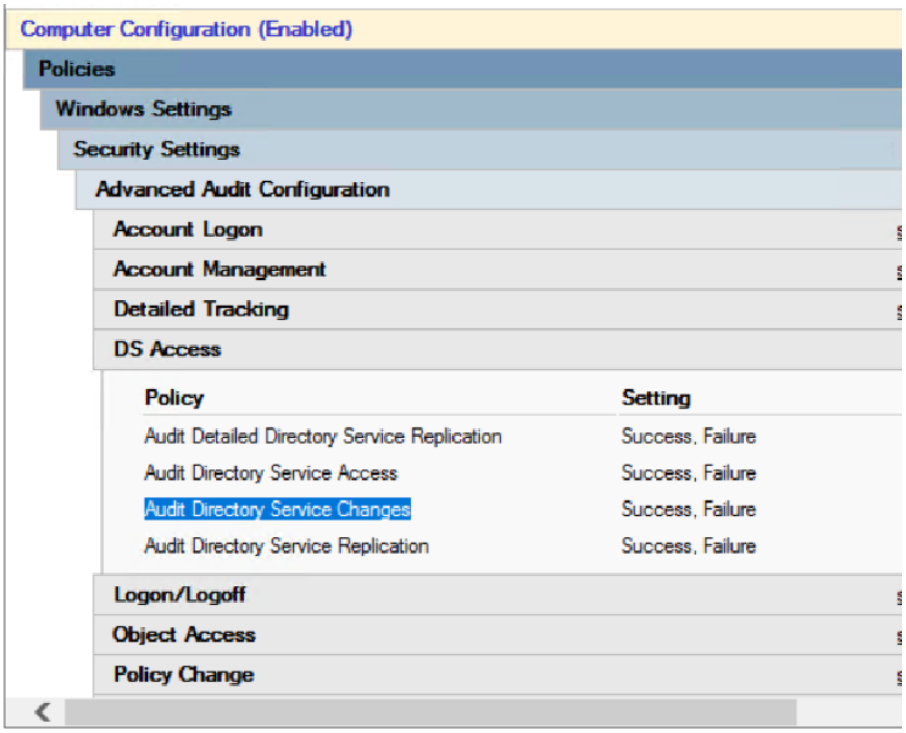
- **Аудит изменений службы каталогов**:
  - `Успех`;
  - `Отказ`.
- **Аудит управления учетными записями пользователей**:
  - `Успех`;
  - `Отказ`.
- **Аудит управления группами безопасности**:
  - `Успех`;
  - `Отказ`.
- **Аудит управления группами рассылки**:
  - `Успех`;
  - `Отказ`.
- **Аудит управления учетными записями компьютера**:
  - `Успех`;
  - `Отказ`.
- **Проверка учетных данных аудита**:
  - `Успех`;
  - `Отказ`.
- **Аудит доступа к службе каталогов**:

- `Успех`;
- `Отказ`.



Для корректного сбора событий **Аудит доступа к службе каталогов** требуется дополнительная настройка прав доступа к объектам Active Directory. Настройте права согласно официальной инструкции Microsoft.

Пример включения одного из параметров аудита:



Установка и подключение агента R-Vision EVO

Установите R-Vision EVO Agent на целевой хост, следуя официальной инструкции.

После установки настройте подключение агента к менеджеру агентов SIEM в соответствии с инструкцией.

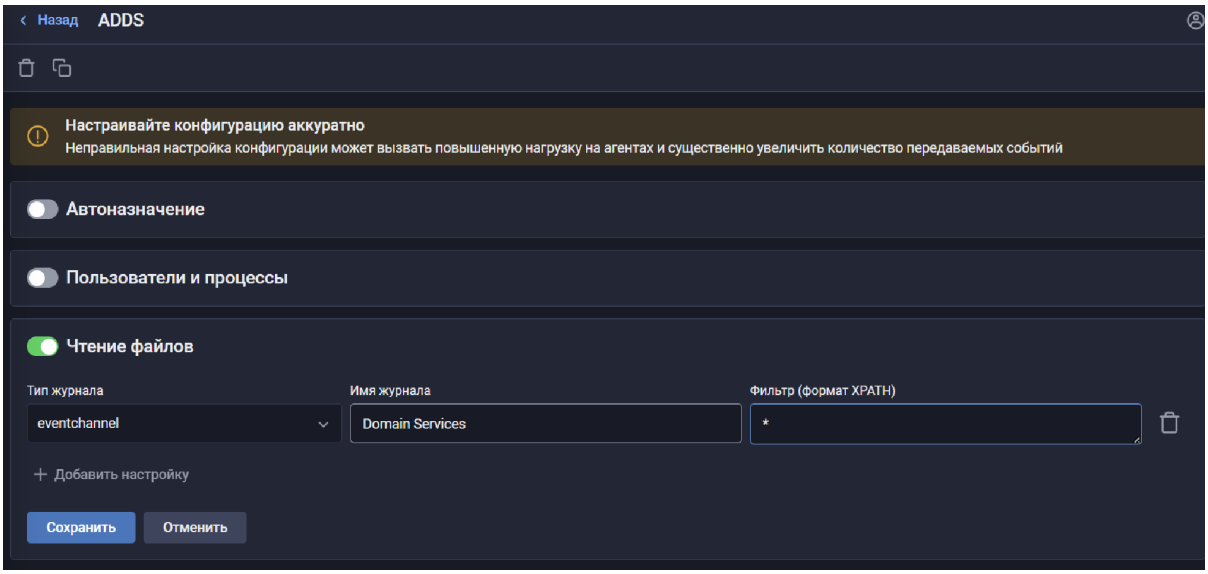
Настройка политики сбора событий в SIEM

Для сбора событий журнала Windows Domain Services создайте политику сбора и добавьте в нее требуемый узел. Информацию о работе с группами агентов можно найти в инструкции по настройке групп.

1. Перейдите к настройке нужной группы агентов.
2. Убедитесь, что переключатель **Чтение файлов** переведен в активное положение.
3. Добавьте новый элемент:
   - **Тип журнала**: `eventchannel`.
   - **Имя журнала**: `Domain Services`.
   - **Фильтр (формат XPath)**:
     - для сбора всех событий укажите *;

- для сбора конкретных событий задайте XPath-фильтр.

Пример конфигурации:



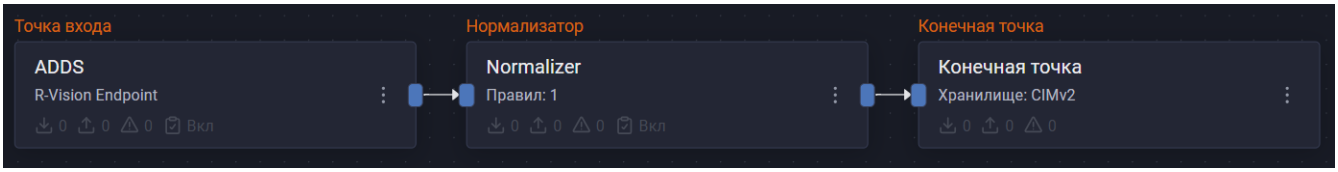
Информацию о формировании корректных XPath-фильтров можно найти в документации по синтаксису XPath.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **R-Vision Endpoint**.
   - Домен: введите значение `gw-<your_gateway_id>`, где `<your_gateway_id>` — ID вашего шлюза.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Microsoft Active Directory Domain Services** (идентификатор правила: **RV-N-277**).
4. Соедините точку входа с нормализатором.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

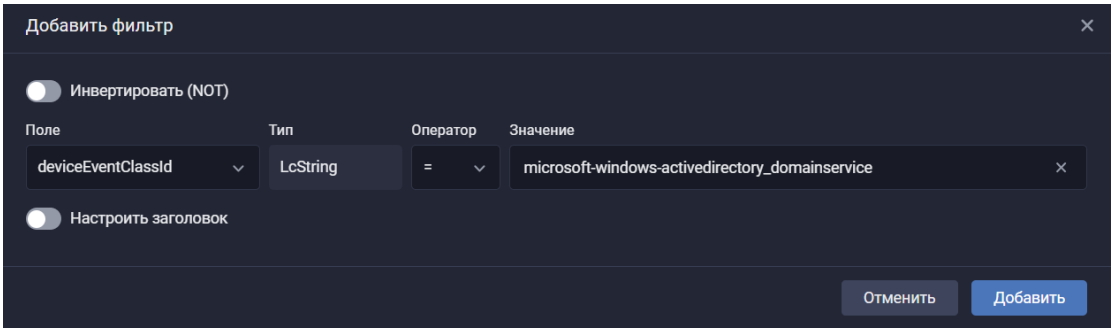


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут

поступать события Microsoft Active Directory Domain Services.

Найти события Microsoft Active Directory Domain Services в хранилище можно по следующему фильтру:

```
deviceEventClassId = "microsoft-windows-activedirectory_domainservice"
```



Microsoft Windows PowerShell

- Microsoft Windows PowerShell: настройка источника
- Microsoft Windows PowerShell: правила корреляции

Microsoft Windows PowerShell: настройка источника

Данное руководство описывает процесс настройки сбора событий Microsoft Windows PowerShell и их отправки в R-Vision SIEM.

Предварительные требования

Перед началом настройки убедитесь, что выполнены следующие условия:

- На машине, с которой планируется сбор событий, установлен агент R-Vision EVO Endpoint.
- Агент находится в активном состоянии и успешно подключен к R-Vision SIEM.
- Пользователь, выполняющий настройку, имеет права администратора локальной машины.
- Система работает под управлением Microsoft Windows с установленным Microsoft Windows PowerShell.

Настройка Microsoft Windows PowerShell

Настройка журналирования Microsoft Windows PowerShell

В настоящем руководстве рассматривается передача событий с помощью продукта R-Vision Endpoint.

Настройте групповую политику (GPO):

- Нажмите Win + R.
- Введите команду:

```
gpedit.msc
```

1. Нажмите на кнопку **OK**.
2. Перейдите в раздел **Конфигурация компьютера** → **Административные шаблоны** → **Компоненты Windows** → **Windows PowerShell**.
3. Найдите параметр **Включить ведение журнала модулей**.
4. Откройте его и выберите **Включено**.
5. В разделе **Имена модулей** нажмите на кнопку **Показать** и добавьте *, чтобы логировать все модули PowerShell.
6. Нажмите на кнопку **OK**.
7. Найдите параметр **Включить регистрацию блоков сценариев PowerShell**.
8. Установите значение **Включено**.
9. Нажмите на кнопку **OK**.
10. После внесения изменений выполните команду:

    ```
    gpudate /force
    ```

Настройка отправки событий в R-Vision Endpoint

1. В веб-интерфейсе **R-Vision SIEM** перейдите в раздел **Агенты** → **Группы агентов**.
2. Создайте группу **Windows PowerShell** или добавьте следующую конфигурацию в существующую группу:
   - Тип журнала: `eventfile`.
   - Путь: `C:\Windows\System32\winevt\Logs\Microsoft-Windows-PowerShell%4Operational.evtx`.
   - Фильтр (формат XPATH): *.
3. Нажмите на кнопку **Сохранить**.
4. Перейдите на вкладку **Агенты**.
5. Нажмите на узел, на котором установлен агент.
6. В открывшемся окне нажмите на кнопку ⋮ и выберите пункт **Добавить в группу**.
7. В появившемся окне найдите настроенную группу и нажмите на кнопку **Добавить**.
8. Дождитесь применения политики группы на узле.

Сбор событий настроен.

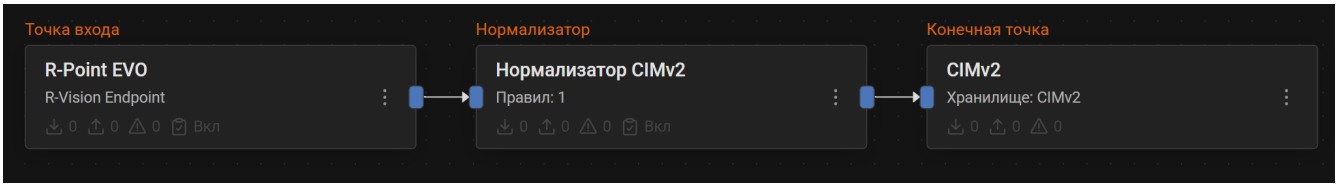
Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.

2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
    - Название: введите название точки входа.
    - Тип точки входа: выберите вариант **R-Vision Endpoint**.
    - Порт точки входа: введите значение в соответствии с настройками на стороне сервера.
    - Протокол: выберите вариант в соответствии с настройками на стороне сервера.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Microsoft Windows PowerShell** (идентификатор правила: **RV-N-218**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

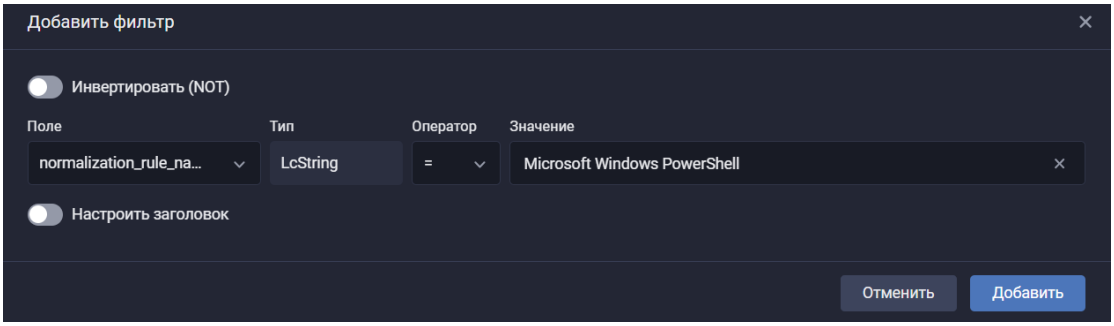
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Microsoft Windows PowerShell.

Найти события Microsoft Windows PowerShell в хранилище можно по следующему фильтру:

```
normalization_rule_name = "Microsoft Windows PowerShell"
```



Microsoft Windows PowerShell: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-770	Использование хакерской утилиты DSInternals	PowerShell — это мощный интерактивный интерфейс командной строки и среда написания сценариев в Windows. Атакующие могут использовать PowerShell для выполнения ряда действий, включая обнаружение информации и выполнение кода. На PowerShell написано множество хакерских утилит, в том числе DSInternals. DSInternals — это инструмент для администраторов и аудиторов Active Directory, который позволяет получить доступ к скрытым функциям и данным. Атакующие могут использовать его при атаках на AD и получении информации из него. Данное правило нацелено на обнаружение событий выполнения модулей или запуска командлетов, связанных с хакерской утилитой DSInternals в оболочке PowerShell. В случае детектирования данной активности необходимо связаться с ответственным лицом и получить подтверждение легитимности действий. Если подтверждение не будет получено — заблокировать учетную запись и узел, инициировать процесс расследования.	• Execution (TA0002) • Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Credential Access (TA0006) • Discovery (TA0007) • OS Credential Dumping (T1003) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Password Policy Discovery (T1201) • Domain or Tenant Policy Modification (T1484) • Steal or Forge Kerberos Tickets (T1558)

ID правила	Название правила	Описание	Тактики и техники
RV-D-771	Использование хакерской утилиты nishang	PowerShell — это мощный интерактивный интерфейс командной строки и среда написания сценариев в Windows. Атакующие могут использовать PowerShell для выполнения ряда действий, включая обнаружение информации и выполнение кода. На PowerShell написано множество хакерских утилит, в том числе nishang.Nishang — это фреймворк, состоящий из набора скриптов, который позволяет использовать PowerShell для обеспечения тестирования на проникновение. Но атакующие также могут использовать его для достижения своих целей. Данное правило нацелено на обнаружение событий выполнения модулей или запуска командлетов, связанных с данной утилитой. В случае детектирования данной активности необходимо связаться с ответственным лицом и получить подтверждение легитимности действий. Если подтверждение не будет получено — заблокировать учетную запись и узел, инициировать процесс расследования.	• Initial Access (TA0001) • Execution (TA0002) • Persistence (TA0003) • Defense Evasion (TA0005) • Credential Access (TA0006) • Discovery (TA0007) • Collection (TA0009) • Command and Control (TA0011) • Exfiltration (TA0010) • OS Credential Dumping (T1003) • LSASS Memory (T1003.001) • Security Account Manager (T1003.002) • Data from Local System (T1005) • Obfuscated Files or Information (T1027) • Command Obfuscation (T1027.010) Exfiltration Over C2

ID правила	Название правила	Описание	Тактики и техники
RV-D-772	Использование хакерской утилиты OWA-Toolkit	PowerShell — это мощный интерактивный интерфейс командной строки и среда написания сценариев в Windows. Злоумышленники могут использовать PowerShell для выполнения ряда действий, включая обнаружение информации и выполнение кода. На PowerShell написано множество хакерских утилит, в том числе OWA-Toolkit. OWA-Toolkit — это инструмент, который помогает в атаках на Exchange/Outlook Web Access (OWA). OWA — это веб-интерфейс для доступа к почтовым ящикам и календарям, хранящимся на серверах Exchange. OWA-Toolkit может использоваться для разных целей, таких как подбор паролей к учетным записям OWA, сбор и анализ данных из OWA, копирование глобального адресного списка (GAL) из OWA, выполнение команд на целевых системах через OWA. OWA-Toolkit может использоваться злоумышленниками для получения доступа к конфиденциальной информации, компрометации учетных записей, выполнения дальнейших атак на внутреннюю сеть или обхода защитных механизмов. Правило нацелено на обнаружение модулей и запуск командлетов, связанных с утилитой OWA-Toolkit в оболочке PowerShell.	• Initial Access (TA0001) • Execution (TA0002) • Persistence (TA0003) • Collection (TA0009) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Email Collection (T1114) • External Remote Services (T1133) • Archive Collected Data (T1560)

ID правила	Название правила	Описание	Тактики и техники
RV-D-773	Использование хакерской утилиты PowerShell-Suit	PowerShell — это мощный интерактивный интерфейс командной строки и среда написания сценариев в Windows. Злоумышленники могут использовать PowerShell для выполнения ряда действий, включая обнаружение информации и выполнение кода. На PowerShell написано множество хакерских утилит, в том числе PowerShell-Suit. PowerShell-Suite –- это набор инструментов и скриптов, предназначенных для автоматизации и управления системами. Атакующие могут его использовать, так как он имеет множество модулей и затрагивает большое количество техник и тактик, таких как Discovery, Credential Access, Execution, Scripting, Lateral Movement. Правило нацелено на обнаружение событий выполнения модулей или запуска командлетов, связанных с хакерской утилитой PowerShell-Suit в оболочке PowerShell. В случае детектирования данной активности необходимо связаться с ответственным лицом и получить подтверждение легитимности действий. Если подтверждение не будет получено — заблокировать учетную запись и узел, инициировать процесс расследования.	• Execution (TA0002) • Credential Access (TA0006) • Discovery (TA0007) • Lateral Movement (TA0008) • OS Credential Dumping (T1003) • LSASS Memory (T1003.001) • Remote Services (T1021) • Windows Remote Management (T1021.006) • Process Discovery (T1057) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-774	Использование хакерской утилиты PowerShellArsenal	PowerShell - это мощный интерактивный интерфейс командной строки и среда написания сценариев в Windows. Злоумышленники могут использовать PowerShell для выполнения ряда действий, включая обнаружение информации и выполнение кода. На PowerShell написано множество хакерских утилит, в том числе PowerShellArsenal. PowerShellArsenal — это модуль PowerShell, который может использоваться для дизассемблирования кода, извлечения данных из памяти, анализа кода .NET, разбора форматов файлов и структур памяти, получения внутренней информации о системе и т.д. Атакующие могут использовать его для достижения своих целей. Данное правило нацелено на обнаружение событий выполнения модулей или запуска командлетов, связанных с хакерской утилитой PowerShellArsenal в оболочке PowerShell. В случае детектирования данной активности необходимо связаться с ответственным лицом и получить подтверждение легитимности действий. Если подтверждение не будет получено — заблокировать учетную запись и узел, инициировать процесс расследования.	• Execution (TA0002) • Credential Access (TA0006) • Discovery (TA0007) • Lateral Movement (TA0008) • OS Credential Dumping (T1003) • LSASS Memory (T1003.001) • Remote Services (T1021) • Windows Remote Management (T1021.006) • Process Discovery (T1057) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-775	Загрузка файлов с помощью PowerShell	Данное правило направленно на детектирование событий по загрузке файлов с помощью PowerShell. Атакующие могут отправлять жертвам фишинговые письма с PowerShell-скриптом, который скачивает файлы для атаки, не привлекая внимания антивируса. Чтобы предотвратить это, нужно обнаруживать и блокировать модули и командлеты, которые связаны с загрузкой файлов в PowerShell. В случае детектирования данной активности необходимо связаться с ответственным лицом и получить подтверждение легитимности действий. Если подтверждение не будет получено — заблокировать учетную запись и узел, инициировать процесс расследования.	• Initial Access (TA0001) • Execution (TA0002) • Lateral Movement (TA0008) • Command and Control (TA0011) • Remote Services (T1021) • SSH (T1021.004) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Ingress Tool Transfer (T1105) • Phishing (T1566) • Spearphishing Link (T1566.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-776	Использование обфускации PowerShell	PowerShell — это мощный интерактивный интерфейс командной строки и среда написания сценариев в Windows. Атакующие могут использовать PowerShell для выполнения ряда действий, включая обнаружение информации и выполнение кода. Для того чтобы обойти обнаружение, атакующие используют обфускацию кода. Обфускация кода — это метод, позволяющий затруднить анализ строк и шаблонов в командах и скриптах. Этот тип запутывания может быть включен в команды, выполняемые доставляемыми полезными нагрузками, в том числе в PowerShell. Правило нацелено на обнаружение модулей и запуск командлетов, связанных с обфускацией кода в оболочке PowerShell.	• Execution (TA0002) • Defense Evasion (TA0005) • Obfuscated Files or Information (T1027) • Command Obfuscation (T1027.010) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-777	Использование WinApi через PowerShell	Windows API — это набор функций, которые предоставляются системными DLL-файлами, такими как kernel32.dll, user32.dll и другими. Эти функции позволяют работать с операционной системой на низком уровне. PowerShell WinAPI используется для того, чтобы задействовать возможности Windows API в сценариях PowerShell, которые не могут быть реализованы с помощью стандартных командлетов или .NET-классов. Например, с помощью PowerShell WinAPI можно вызывать функции для работы с файлами, реестром, процессами, окнами, сетью и другими аспектами системы. PowerShell WinAPI может использоваться атакующими для выполнения различных атак на компьютеры и сети. Например, с его помощью можно скрывать активность от антивирусов и других средств обнаружения (используя функции для инъекции кода, изменения прав доступа, создания скрытых окон), получать доступ к защищенным данным (используя функции для чтения и записи памяти, дампа паролей, перехвата клавиатурного ввода), а также управлять удаленными системами (используя функции для создания и удаления процессов, открытия и закрытия сессий, отправки и получения сообщений). Правило нацелено на детектирование использования функций WinAPI в оболочке PowerShell или PowerShell-скриптах.	• Execution (TA0002) • Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Obfuscated Files or Information (T1027) • Process Injection (T1055) • Process Injection (T1055) • Portable Executable Injection (T1055.002) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Native API (T1106)

ID правила	Название правила	Описание	Тактики и техники
RV-D-778	Использование хакерской утилиты PowerSploit	PowerShell — это мощный интерактивный интерфейс командной строки и среда написания сценариев в Windows. Атакующие могут использовать PowerShell для выполнения ряда действий, включая обнаружение информации и выполнение кода. На PowerShell написано множество хакерских утилит, в том числе PowerSploit.PowerSploit — это набор модулей Microsoft PowerShell, которые могут быть использованы для тестирования на проникновение. Атакующие активно применяют его для проведения кибератак, используя его расширенный функционал. Данное правило нацелено на обнаружение событий по запуску модулей или командлетов, связанных с хакерской утилитой PowerSploit в оболочке PowerShell. В случае детектирования данного инцидента необходимо связаться с ответственным лицом и получить подтверждение легитимности действий. Если подтверждение не будет получено, необходимо заблокировать учетную запись и узел, инициировать процесс расследования.	• Execution (TA0002) • Persistence (TA0003) • Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Credential Access (TA0006) • Discovery (TA0007) • Collection (TA0009) • OS Credential Dumping (T1003) • Data from Local System (T1005) • Direct Volume Access (T1006) • Query Registry (T1012) • Obfuscated Files or Information (T1027) • Indicator Removal from Tools (T1027.005) • Command Obfuscation (T1027.010) • Windows Management Instrumentati

ID правила	Название правила	Описание	Тактики и техники
RV-D-779	Использование хакерской утилиты PSMapExec	PowerShell — это мощный интерактивный интерфейс командной строки и среда написания сценариев в Windows. Атакующие могут использовать PowerShell для выполнения ряда действий, включая обнаружение информации и выполнение кода. На PowerShell написано множество хакерских утилит, в том числе PsMapExec.PsMapExec — это фреймворк для пост-эксплуатации и оценки компрометации среды Active Directory на базе PowerShell. PsMapExec позволяет выполнять различные действия на удаленных компьютерах, используя разные протоколы и методы аутентификации. Данное правило нацелено на обнаружение модулей и запуск командлетов, связанных с хакерской утилитой PsMapExec. В случае обнаружения корреляционного события необходимо связаться с ответственным лицом, получить подтверждение легитимности действий. Если подтверждение не будет получено, необходимо заблокировать учетную запись и узел, инициировать процесс расследования.	• Initial Access (TA0001) • Execution (TA0002) • Credential Access (TA0006) • Lateral Movement (TA0008) • Remote Services (T1021) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Valid Accounts (T1078) • Steal or Forge Kerberos Tickets (T1558) • Golden Ticket (T1558.001) • System Services (T1569)

ID правила	Название правила	Описание	Тактики и техники
RV-D-780	Использование хакерской утилиты SharpHound	PowerShell — это мощный интерактивный интерфейс командной строки и среда написания сценариев в Windows. Атакующие могут использовать PowerShell для выполнения ряда действий, включая обнаружение информации и выполнение кода. На PowerShell написано множество хакерских утилит, одна из которых — SharpHound. SharpHound — это инструмент, который собирает данные из Active Directory в формате JSON для дальнейшего анализа при помощи утилиты BloodHound. BloodHound — это инструмент для разведки Active Directory (AD), который может раскрывать скрытые связи и определять пути атаки в среде AD. Благодаря ему атакующий может построить подробную карту домена со всеми доверительными отношениями, УЗ и объектами. SharpHound, в свою очередь, позволяет собрать необходимую для этого информацию, обладая минимальными правами пользователя. BloodHound позволяет построить маршрут атаки, по которому атакующие смогут быстрее всего добраться до интересующей их цели в домене. В случае обнаружения корреляционного события необходимо связаться с ответственным лицом, получить подтверждение легитимности действий. Если подтверждение не будет получено, необходимо заблокировать учетную запись и узел, инициировать процесс расследования.	• Execution (TA0002) • Discovery (TA0007) • Remote System Discovery (T1018) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Account Discovery (T1087) • Local Account (T1087.001) • Domain Trust Discovery (T1482)

ID правила	Название правила	Описание	Тактики и техники
RV-D-782	Прямой доступ к диску через PowerShell	Правило отслеживает прямой доступ к логическим томам диска через PowerShell с использованием пути `\\.{volume_name}` и класса `IO.FileStream`. Атакующий может использовать эту технику для обхода стандартных механизмов контроля доступа файловой системы, что позволяет получить низкоуровневый доступ к данным на диске. Это может быть использовано для скрытных операций с данными, таких как чтение, запись или модификация важных файлов. Для выполнения атаки атакующий может воспользоваться правами, которые позволяют ему выполнять команды PowerShell. В случае невозможности подтверждения легитимности события следует обратить внимание на учетную запись, с которой был выполнен доступ, и провести дополнительные проверки на наличие признаков атаки.	• Defense Evasion (TA0005) • Direct Volume Access (T1006)
RV-D-783	Сжатие файлов средствами PowerShell	Данное правило обнаруживает использование командлета Compress-Archive в PowerShell для сжатия файлов и папок. Такое поведение может указывать на подготовку к эксфильтрации данных, поскольку атакующие нередко архивируют файлы перед их передачей. При срабатывании правила необходимо определить, какие файлы были сжаты и кто инициировал выполнение командлета. Если активность выглядит подозрительно или сжаты были критичные файлы, следует начать расследование и при необходимости изолировать хост, чтобы предотвратить возможную утечку данных.	• Collection (TA0009) • Archive Collected Data (T1560) • Archive via Utility (T1560.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1133	Использование подавления ошибок в PowerShell	Правило нацелено на обнаружение использования параметров подавления ошибок (-ErrorAction SilentlyContinue и аналогичных) при выполнении командлетов PowerShell. Атакующие применяют эти параметры, чтобы скрыть ошибки, предотвратить прерывание выполнения и усложнить анализ активности. Подобное поведение может указывать на попытку маскировки операций, особенно если команда выполняется нетипичным пользователем или в подозрительном контексте.	• Defense Evasion (TA0005) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Hide Artifacts (T1564) • Ignore Process Interrupts (T1564.011)
RV-D-1135	Внедрение вредоносного агента Exchange	Данное правило направлено на обнаружение создания или модификации транспортных агентов Microsoft Exchange с использованием командлетов PowerShell (Install-TransportAgent или Set-TransportAgent).	• Persistence (TA0003) • Server Software Component (T1505) • Transport Agent (T1505.002)

Microsoft Windows Security

- Microsoft Windows Security: настройка источника
- Microsoft Windows Security: настройка расширенного аудита
- Microsoft Windows Security: правила корреляции

Microsoft Windows Security: настройка источника

Данное руководство описывает процесс отправки событий из журнала Windows Security в R-Vision SIEM с помощью продукта R-Vision EVO.

Настройка Microsoft Windows Security

В данном разделе описана настройка сбора событий журнала Windows Security с помощью агента R-Vision EVO. Процесс включает следующие этапы:

1. Настройка сбора событий Microsoft Windows Security
2. Установка и подключение агента R-Vision EVO

3. Настройка политики сбора событий в R-Vision SIEM

Настройка сбора событий Microsoft Windows Security

Чтобы события появлялись в журнале Security, необходимо включить аудит в настройках Windows. Политику можно применить:

- через GPO (рекомендуется для домена);
- локально для отдельных хостов (не рекомендуется для масштабного использования).

▼ *Настройка через доменные политики*

Предварительные требования

- Ваша Windows-машина должна быть включена в домен.
- Ваша учетная запись должна обладать правами администратора домена (`Domain Admin`).
- Должны быть включены параметры аудита.

Настройка сбора событий Microsoft Windows

Чтобы настроить сбор событий Microsoft Windows, выполните следующие шаги:

1. Откройте консоль **Group Policy Management**.
2. Создайте новую GPO или отредактируйте существующую.
3. Перейдите в раздел **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Advanced Audit Policy Configuration**.
4. Включите необходимые параметры аудита.
5. Привяжите политику к нужному OU (Organizational Unit).
6. Дождитесь применения политики на хостах или выполните команду `gpupdate /force`.

▼ *Настройка через локальные политики*

Предварительные требования

- Ваша учетная запись должна обладать правами локального администратора.
- Должны быть включены параметры аудита, необходимые для сбора событий.

Настройка сбора событий Microsoft Windows

Чтобы настроить сбор событий Microsoft Windows, выполните следующие шаги:

1. Откройте консоль **Local Security Policy**, используя команду `secpol.msc`.
2. Перейдите в раздел **Local Policies** → **Audit Policy** или **Advanced Audit Policy Configuration**.
3. Включите необходимые параметры аудита (`успех` / `отказ`).
4. Примените изменения.
5. Обновите политики командой `gpupdate /force` или перезагрузите хост.

Настройка параметров аудита

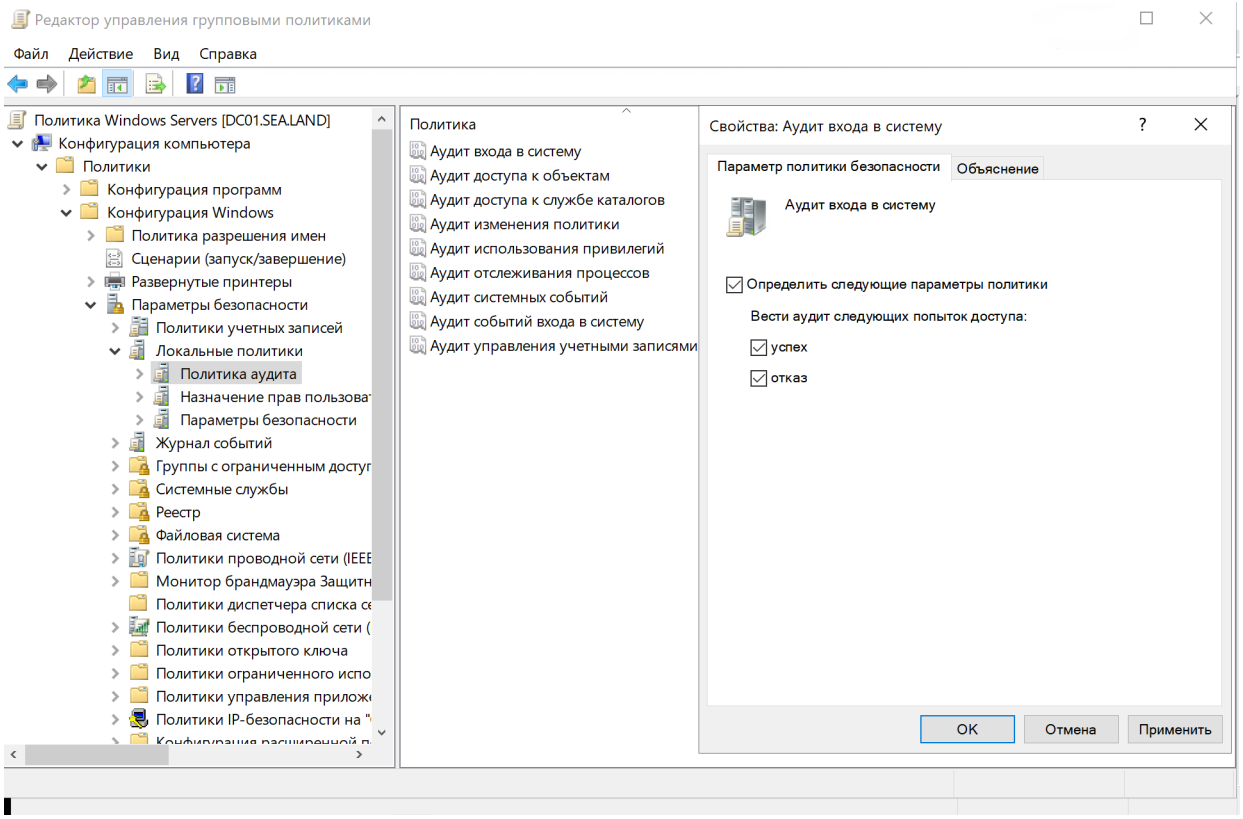
В групповой политике устройства включите следующие параметры.

1. Аудит событий:
    - **Аудит входа в систему**: успех, отказ.
    - **Аудит доступа к объектам**: успех.
    - **Аудит доступа к службам каталогов**: успех.
    - **Аудит изменения политики**: успех.
    - **Аудит использования привилегий**: успех.
    - **Аудит отслеживания процессов**: успех.
    - **Аудит системных событий**: успех.
    - **Аудит событий входа в систему**: успех, отказ.
    - **Аудит управления учетными записями**: успех, отказ.
2. Расширенный аудит событий:
    - **Проверка учетных данных аудита**: успех, отказ.
    - **Аудит управления учетными записями компьютера**: успех, отказ.
    - **Аудит управления группами безопасности**: успех, отказ.
    - **Аудит управления учетными записями пользователей**: успех, отказ.
    - **Аудит изменений службы каталогов**: успех, отказ.
    - **Расширение системы безопасности аудита**: успех, отказ.
    - **Аудит доступа к службе каталогов**: успех, отказ.



Для корректного сбора событий **Аудит доступа к службе каталогов** требуется дополнительная настройка прав доступа к объектам Active Directory. Настройте права согласно официальной инструкции Microsoft.

Пример включения одного из параметров аудита:



Установка и подключение агента R-Vision EVO

Установите агент R-Vision EVO на целевой хост, следуя официальной инструкции.

После установки настройте подключение агента к менеджеру агентов R-Vision SIEM в соответствии с инструкцией.

Настройка политики сбора событий в R-Vision SIEM

Для сбора событий журнала Microsoft Windows Security создайте политику сбора и добавьте в нее требуемый узел. Информацию о работе с группами агентов можно найти в инструкции по настройке групп.

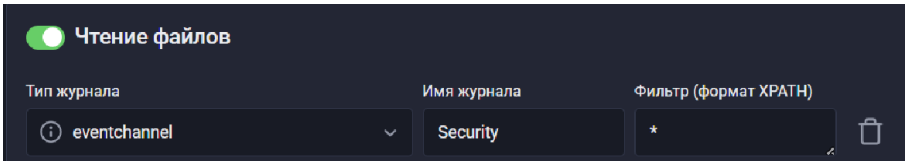
Чтобы настроить сбор событий из журнала **Security**, выполните следующие шаги:

1. Перейдите к настройке нужной группы агентов.
2. Убедитесь, что переключатель **Чтение файлов** установлен в активное положение.
3. Добавьте новый элемент:
   - **Тип журнала**: `eventchannel`.
   - **Имя журнала**: `Security`.
   - **Фильтр (формат XPath)**:
     - для сбора всех событий укажите символ *;
     - для сбора конкретных событий задайте XPath-фильтр.



Информацию о формировании корректных XPath-фильтров можно найти в документации по синтаксису XPath.

Пример конфигурации:

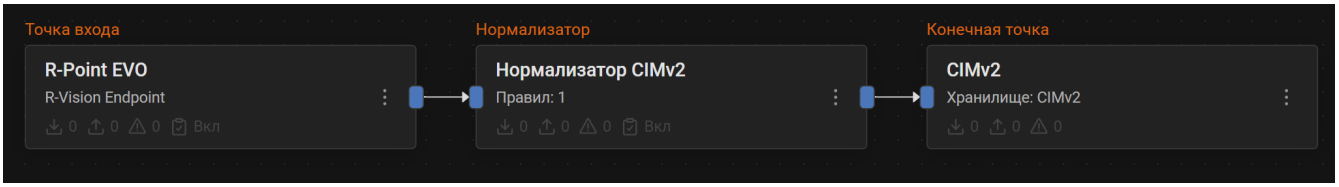


Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **R-Vision Endpoint**.
   - Домен: введите значение `gw-<your_gateway_id>`, где `<your_gateway_id>` — ID вашего шлюза.
3. Добавьте на конвейер элемент **Нормализатор** с правилом для нормализации событий журнала **Microsoft Windows Security** (идентификатор правила: **RV-N-222**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

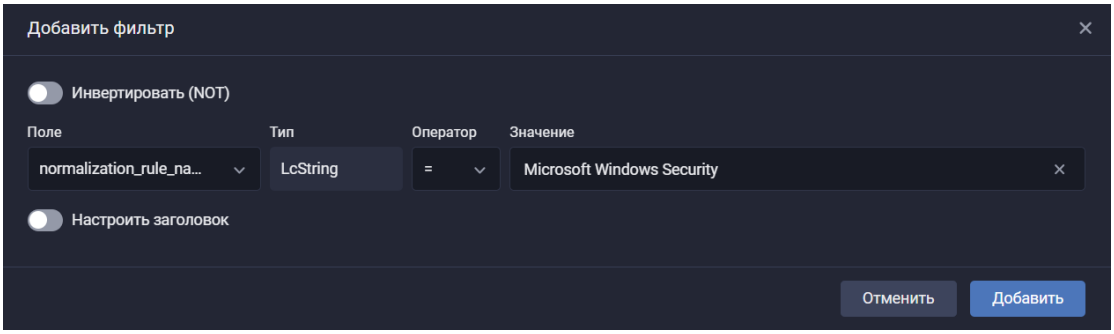


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Microsoft Windows Security.



Найти события Microsoft Windows Security в хранилище можно по следующему фильтру:

```
normalization_rule_name = "Microsoft Windows Security"
```



Microsoft Windows Security: настройка расширенного аудита

Общие сведения

Настройка расширенной политики аудита присутствует в ОС Windows Vista/Server 2008 и выше. Политики расширенного аудита поддерживают все серверные версии Windows (Standard и Datacenter) и корпоративные клиентские машины редакции «Профессиональная» (Pro) и «Корпоративная» (Enterprise).

На текущий момент в последних версиях ОС Windows, таких как Windows 10/11, Windows Server 2016, Windows Server 2019 и Windows Server 2022 существует 10 категорий и 61 подкатегория политик аудита.

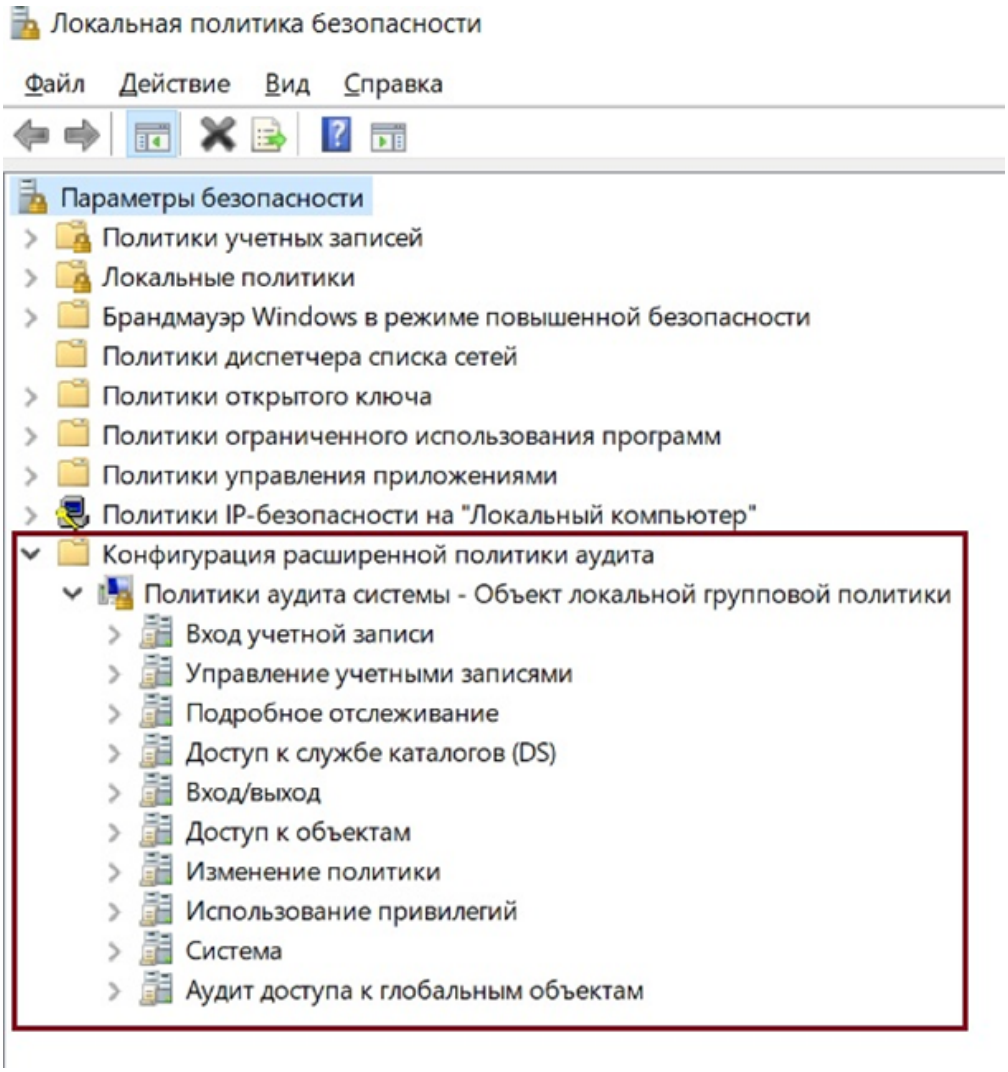
В более низких версиях операционных систем от Microsoft часть политик может отсутствовать.

Настройка расширенной политики аудита

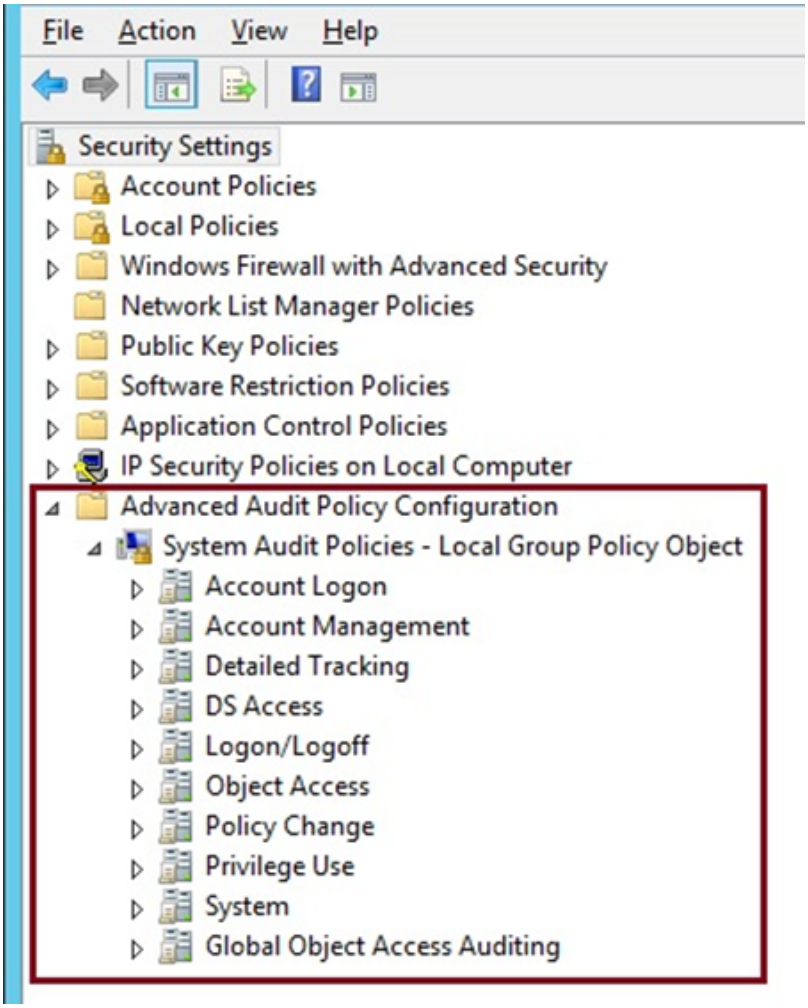
Настройка осуществляется через локальную политику безопасности (gpedit.msc) или групповые политики (gpmc.msc).

Путь к настройкам расширенного аудита:

- в ОС на русском языке: **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Конфигурация расширенной политики аудита**;



- в ОС на английском языке: **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Advanced Audit Policy Configuration**.



Рекомендованные параметры политики расширенного аудита для рабочих станций и серверов

Категория (Category)	**Подкатегория (Subcategory)**	**Параметры аудита (Audit settings)**
Вход учетной записи (Account Logon)	Аудит проверки учетных данных (Audit Credential Validation)	Успех и Отказ (Success and Failure)
Управление учетными записями (Account Management)	Аудит других событий управления учетными записями (Audit Other Account Management Events)	Успех (Success)
	Аудит управления группами безопасности (Audit Security Group Management)	Успех (Success)
	Аудит управления учетными записями пользователей (Audit User Account Management)	Успех и Отказ (Success and Failure)

Категория (Category)	Подкатегория (Subcategory)	Параметры аудита (Audit settings)
Подробное отслеживание (Detailed Tracking)	Аудит активности DPAPI (Audit DPAPI Activity)	Успех и Отказ (Success and Failure)
	PNP-действие аудита (Audit PNP Activity)	Успех (Success)
	Аудит создания процессов (Audit Process Creation)	Успех (Success)  Для данных политик аудита необходимо дополнительно включить политику **Включать командную строку в события создания процессов** (**Include command line in process creation events**).
	Аудит завершения процессов (Audit Process Termination)	Успех (Success)
Вход/выход (Logon/Logoff)	Аудит блокировки учетных записей (Audit Account Lockout)	Отказ (Failure)
	Аудит выхода из системы (Audit Logoff)	Успех (Success)
	Аудит входа в систему (Audit Logon)	Успех и Отказ (Success and Failure)
	Аудит других событий входа и выхода (Audit Other Logon/Logoff Events)	Успех и Отказ (Success and Failure)
	Аудит специального входа (Audit Special Logon)	Успех (Success)

Категория (Category)	Подкатегория (Subcategory)	Параметры аудита (Audit settings)
Доступ к объектам (Object Access)	Аудит сведений об общем файловом ресурсе (Audit Detailed File Share)	Успех и Отказ (Success and Failure)
	Аудит общего файлового ресурса (Audit File Share)	Успех (Success)
	Аудит файловой системы (Audit File System)	Успех (Success)
	Аудит работы с дескрипторами (Audit Handle Manipulation)	Успех (Success)
	Аудит объектов ядра (Audit Kernel Object) [Объект-задание]	Успех и Отказ (Success and Failure)
	Аудит других событий доступа к объектам (Audit Other Object Access Events)	Успех (Success)
	Аудит реестра (Audit Registry)	Успех (Success)
	Аудит съемного носителя (Audit Removable Storage)	Успех (Success)
Изменение политики (Policy Change)	Аудит изменения политики аудита (Audit Policy Change)	Успех (Success)
	Аудит изменения политики проверки подлинности (Audit Authentication Policy Change)	Успех (Success)
	Аудит изменения политики на уровне правил MPSSVC (Audit MPSSVC Rule-Level Policy Change)	Успех и Отказ (Success and Failure)
Система (System)	Аудит изменения состояния безопасности (Audit Security State Change)	Успех (Success)
	Аудит расширения системы безопасности (Audit Security System Extension)	Успех (Success)

Политика расширенного аудита для контроллеров домена (DC)

Категория (Category)	**Подкатегория (Subcategory)**	**Параметры аудита (Audit settings)**
Вход учетной записи (Account Logon)	Аудит проверки учетных данных (Audit Credential Validation)	Успех и Отказ (Success and Failure)
	Аудит службы проверки подлинности Kerberos (Audit Kerberos Authentication Service)	Успех и Отказ (Success and Failure)
	Аудит операций с билетами службы Kerberos (Audit Kerberos Service Ticket Operations)	Успех и Отказ (Success and Failure)
Управление учетными записями (Account Management)	Аудит управления группами приложений (Audit Application Group Management)	Успех и Отказ (Success and Failure)
	Аудит управления учетными записями компьютеров (Audit Computer Account Management)	Успех (Success)
	Аудит управления группами распространения (Audit Distribution Group Management)	Успех (Success)
	Аудит других событий управления учетными записями (Audit Other Account Management Events)	Успех (Success)
	Аудит управления группами безопасности (Audit Security Group Management)	Успех (Success)
	Аудит управления учетными записями пользователей (Audit User Account Management)	Успех и Отказ (Success and Failure)

Категория (Category)	Подкатегория (Subcategory)	Параметры аудита (Audit settings)
Подробное отслеживание (Detailed Tracking)		

Категория (Category)	Подкатегория (Subcategory)	Параметры аудита (Audit settings)

Категория (Category)	Подкатегория (Subcategory)	Параметры аудита (Audit settings)
	Аудит завершения процессов (Audit Process Termination)	Успех (Success)
Доступ к службе каталогов DS (DS Access)	Аудит подробной репликации службы каталогов (Audit Detailed Directory Service Replication)	Успех и Отказ (Success and Failure)
	Аудит доступа к службе каталогов (Audit Directory Service Access)	Успех и Отказ (Success and Failure)
	Аудит изменения службы каталогов (Audit Directory Services Changes)	Успех (Success)
	Аудит репликации службы каталогов (Audit Directory Service Replication)	Успех и Отказ (Success and Failure)
Вход/выход (Logon/Logoff)	Аудит блокировки учетных записей (Audit Account Lockout)	Отказ (Failure)
	Аудит выхода из системы (Audit Logoff)	Успех (Success)
	Аудит входа в систему (Audit Logon)	Успех и Отказ (Success and Failure)
	Аудит других событий входа и выхода (Audit Other Logon/Logoff Events)	Успех и Отказ (Success and Failure)
	Аудит специального входа (Audit Special Logon)	Успех (Success)
Доступ к объектам (Object Access)	Аудит сведений об общем файловом ресурсе (Audit Detailed File Share)	Успех и Отказ (Success and Failure)
	Аудит общего файлового ресурса (Audit File Share)	Успех (Success)
	Аудит файловой системы (Audit File System)	Успех (Success)
	Аудит работы с дескрипторами (Audit Handle Manipulation)	Успех (Success)
	Аудит объектов ядра (Audit Kernel Object) [Объект-задание]	Успех и Отказ (Success and Failure)
	Аудит других событий доступа к объектам (Audit Other Object Access Events)	Успех (Success)
	Аудит реестра (Audit Registry)	Успех (Success)
	Аудит съемного носителя (Audit Removable Storage)	Успех (Success)

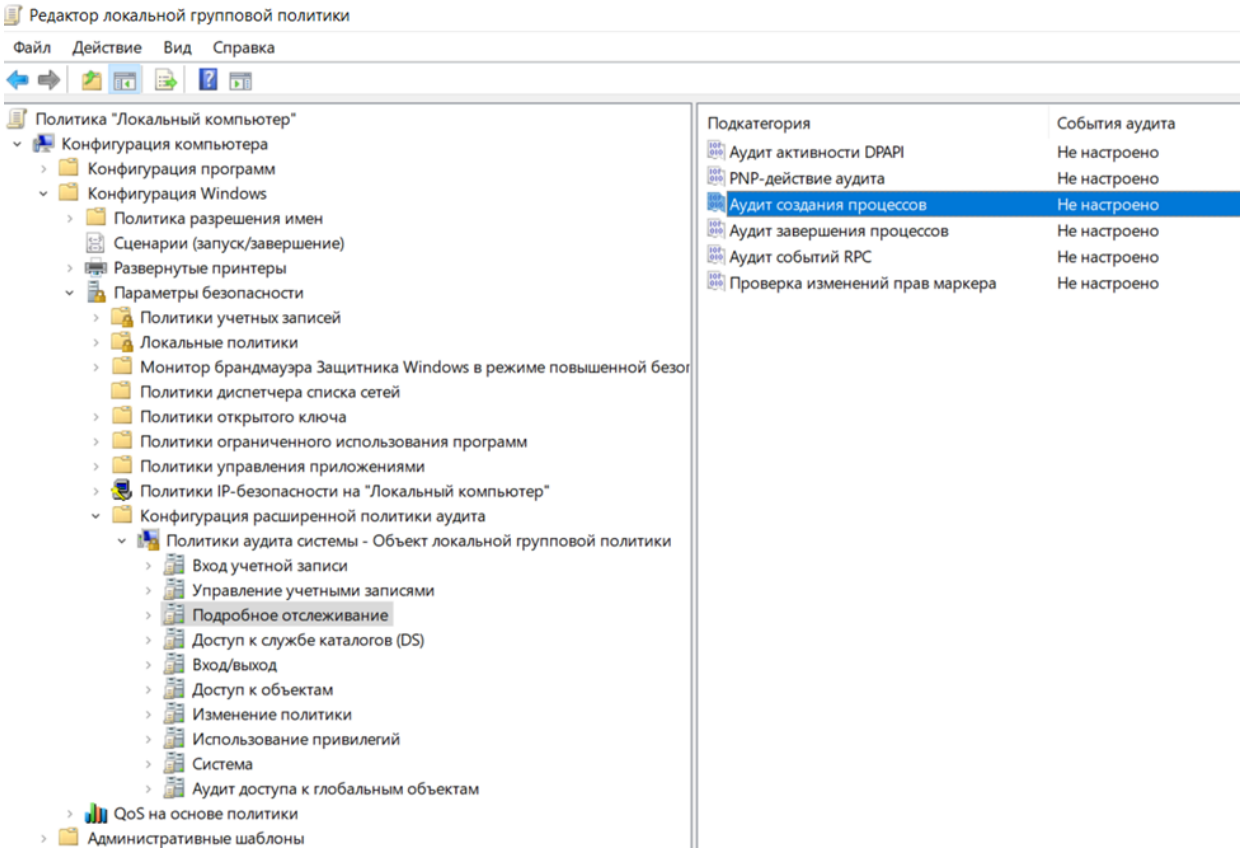
Категория (Category)	Подкатегория (Subcategory)	Параметры аудита (Audit settings)
Изменение политики (Policy Change)	Аудит изменения политики аудита (Audit Policy Change)	Успех (Success)
	Аудит изменения политики проверки подлинности (Audit Authentication Policy Change)	Успех (Success)
	Аудит изменения политики на уровне правил MPSSVC (Audit MPSSVC Rule-Level Policy Change)	Успех и Отказ (Success and Failure)
Система (System)	Аудит изменения состояния безопасности (Audit Security State Change)	Успех (Success)
	Аудит расширения системы безопасности (Audit Security System Extension)	Успех (Success)

Аудит командной строки

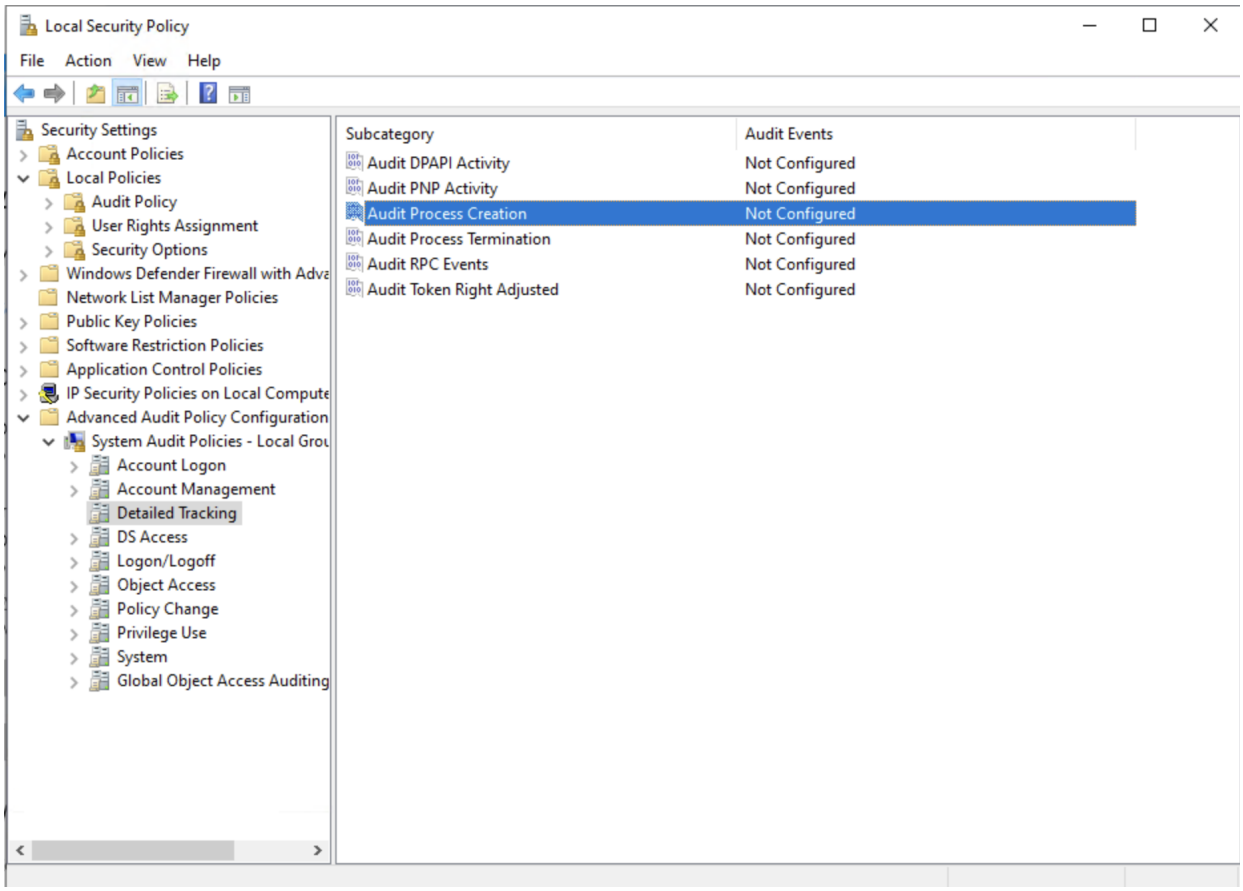
Включение аудита создания процессов

Политика **Аудит создания процессов** (**Audit Process Creation**) включается через консоль gpedit.msc (локальные политики) или gpmc.msc (групповые политики). Для этого выполните следующие шаги:

1. Перейдите к настройкам политики по пути:
    - в ОС на русском языке: **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Конфигурация расширенной политики аудита** → **Подробное отслеживание**;



- в ОС на английском языке: **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Advanced Audit Policy Configuration** → **Detailed Tracking**.

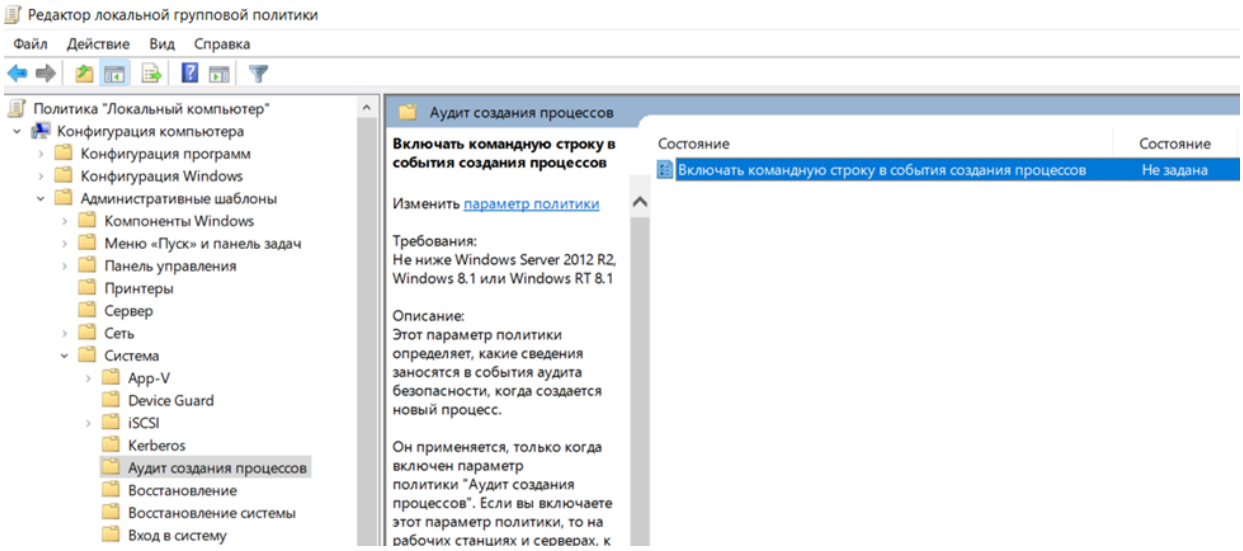


2. Установите флажки напротив следующих параметров:
   - **Настроить следующие события аудита** (**Configure the following audit events**);
   - **Успех** (**Success**).
3. Нажмите на кнопку **Применить** (**Apply**).

Включение командной строки в события создания процессов

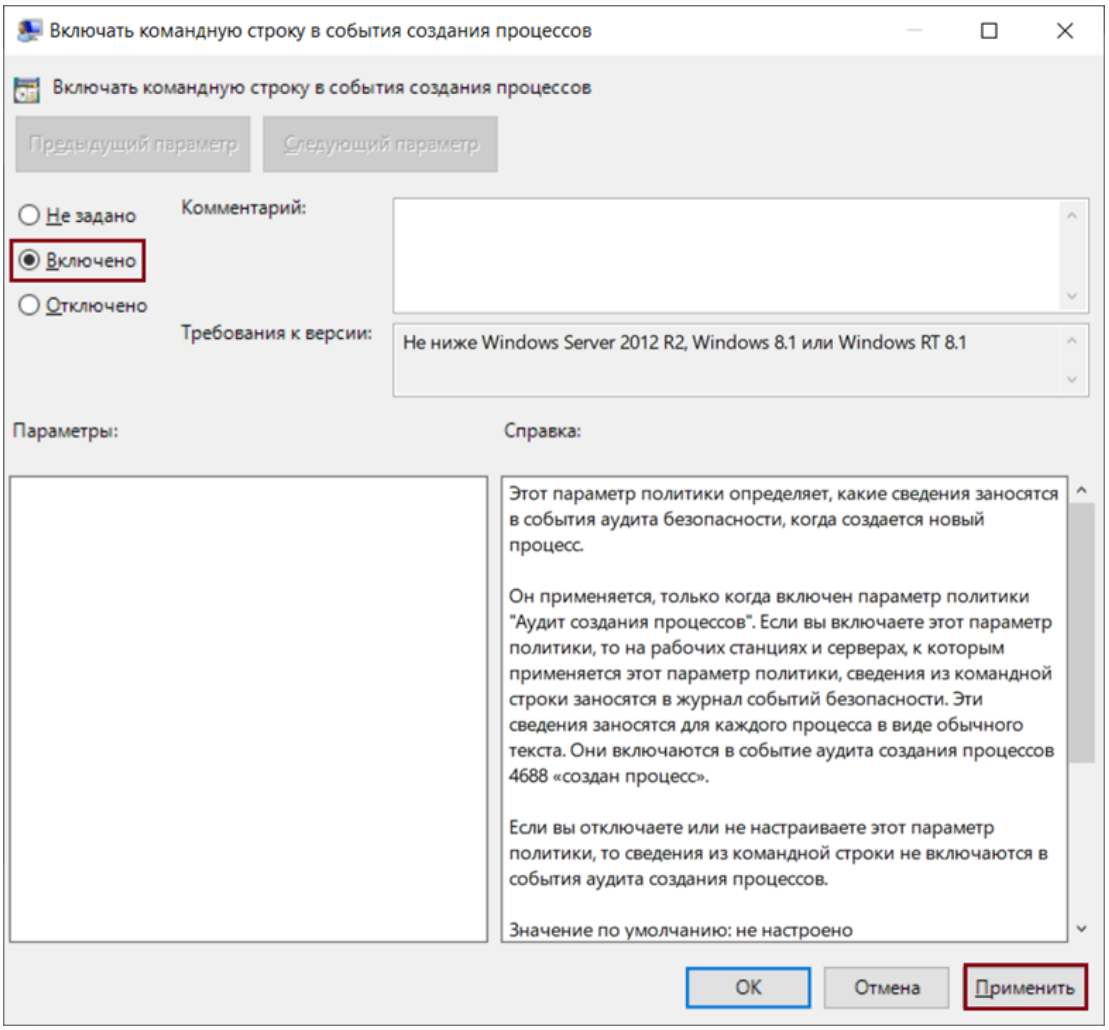
Политика **Включать командную строку в события создания процессов** (**Include command line in process creation events**) включается через консоль gpedit.msc (локальные политики) или gpmc.msc (групповые политики). Для этого выполните следующие шаги:

1. Перейдите к настройкам политики по пути:
   - в ОС на русском языке: **Конфигурация компьютера** → **Политики** → **Административные шаблоны** → **Система** → **Аудит создания процессов**;



- в ОС на английском языке: **Computer Configuration** → **Policies** → **Administrative Templates** → **System** → **Audit Process Creation**.

2. Выберите вариант **Включено** (**Enabled**).



3. Нажмите на кнопку **Применить** (**Apply**).



Если на хосте уже включена политика **Аудит создания процессов** (**Audit Process Creation**), вам необходимо только включить политику **Включать командную строку в события создания процессов** (**Include command line in process creation events**).

> Дополнительная перезагрузка хоста не требуется.

Дополнительные настройки

Журналирование PowerShell

Перед настройкой журналирования PowerShell убедитесь, что у вас установлена версия PowerShell 5.0 или выше (предустановлена в Windows 10/11, Windows Server 2016, Windows Server 2019 и Windows Server 2022).

Для полного логирования событий PowerShell необходимо включить следующие политики ведения журналов:

- **Включить регистрацию блоков сценариев PowerShell** (**Turn on PowerShell Script Block Logging**);
- **Включить ведение журнала модулей** (**Turn on Module Logging**).

Настройка политик осуществляется через оснастку gpedit.msc (локальные политики) или gpmc.msc (групповые политики). Для этого необходимо перейти к настройкам политик по пути:

- в ОС на русском языке: **Конфигурация компьютера** → **Политики** → **Административные шаблоны** → **Компоненты Windows** → **Windows PowerShell**;
- в ОС на английском языке: **Computer Configuration** → **Policies** → **Administrative Templates** → **Windows Components** → **Windows PowerShell**.

При необходимости вы можете отключить PowerShell 2.0, так как данная версия не имеет встроенных механизмов логирования и защиты, используемых в последних версиях.

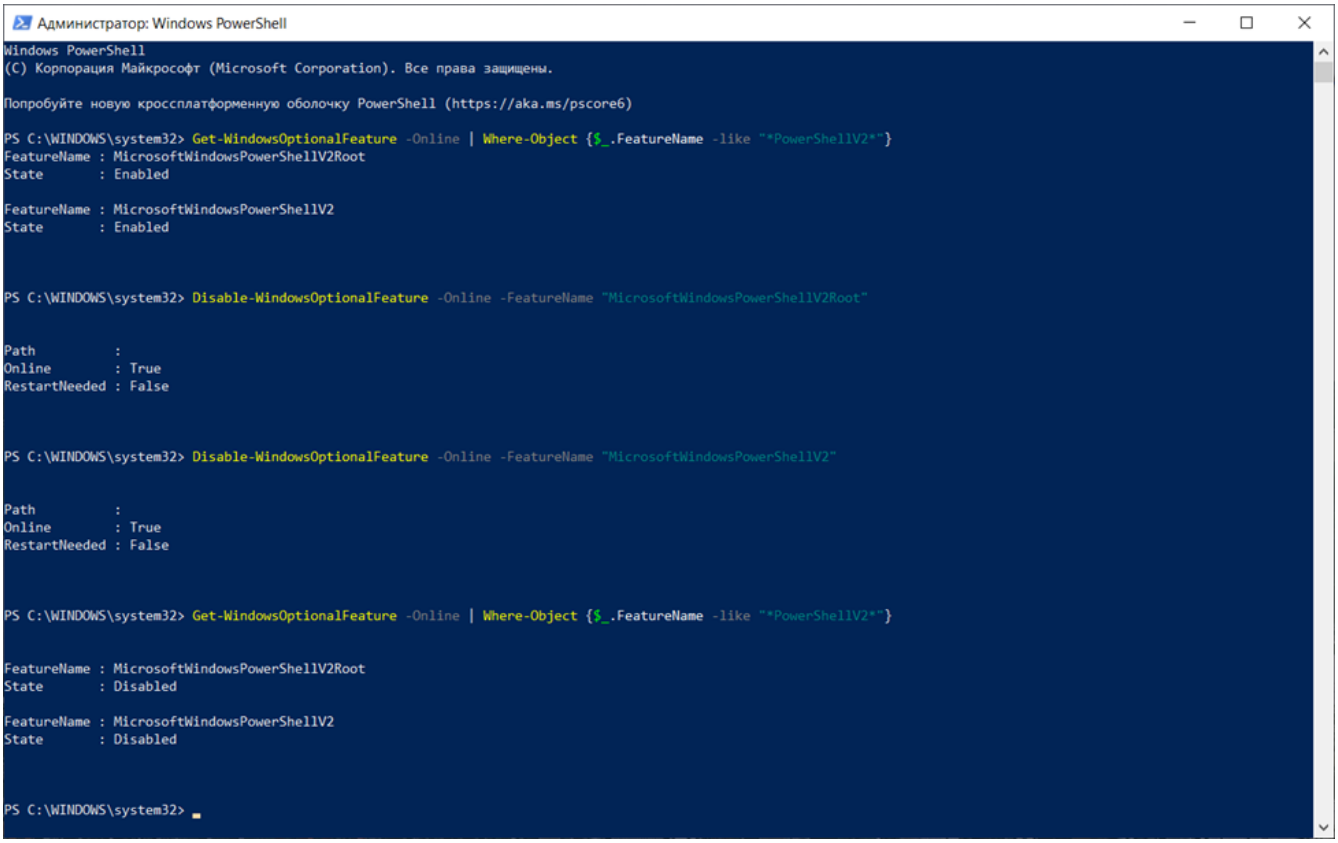
Чтобы посмотреть текущий статус Windows PowerShell 2.0, выполните следующую команду:

```
_Get-WindowsOptionalFeature -Online | Where-Object {$_.FeatureName -like
"*PowerShellV2*"}
```

Чтобы отключить Windows PowerShell 2.0, выполните следующую команду:

```
_Disable-WindowsOptionalFeature -Online -FeatureName
"MicrosoftWindowsPowerShellV2Root"_

_Disable-WindowsOptionalFeature -Online -FeatureName "MicrosoftWindowsPowerShellV2"_
```

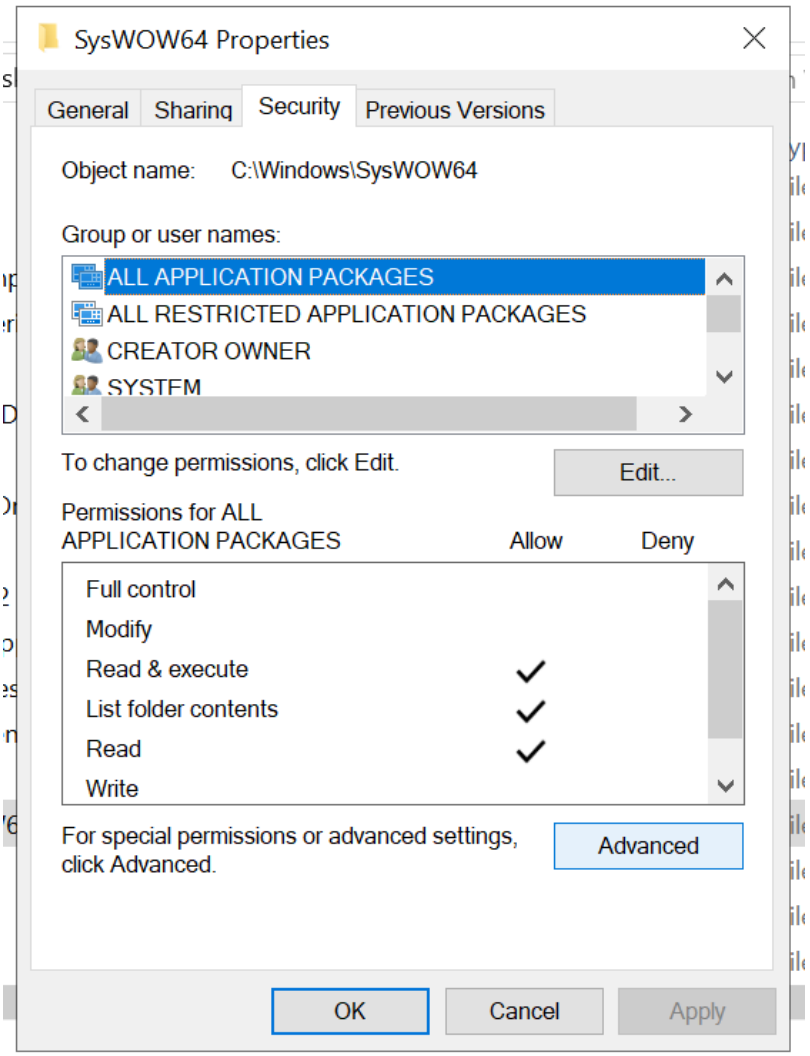


Настройка аудита доступа к файлам

Аудит доступа к файлам настраивается для каждого каталога отдельно.

Для включения аудита выполните следующие шаги:

1. Перейдите в групповой или локальной политике в раздел **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Advanced Audit Policy Configuration** → **Object Access**.
2. Для каждого файла или каталога аудит настраивается отдельно. Чтобы настроить аудит требуемой директории, включая все вложенные файлы и папки, выполните следующие шаги:
   a. Откройте свойства директории.
   b. На вкладке **Security** нажмите на кнопку **Advanced**.

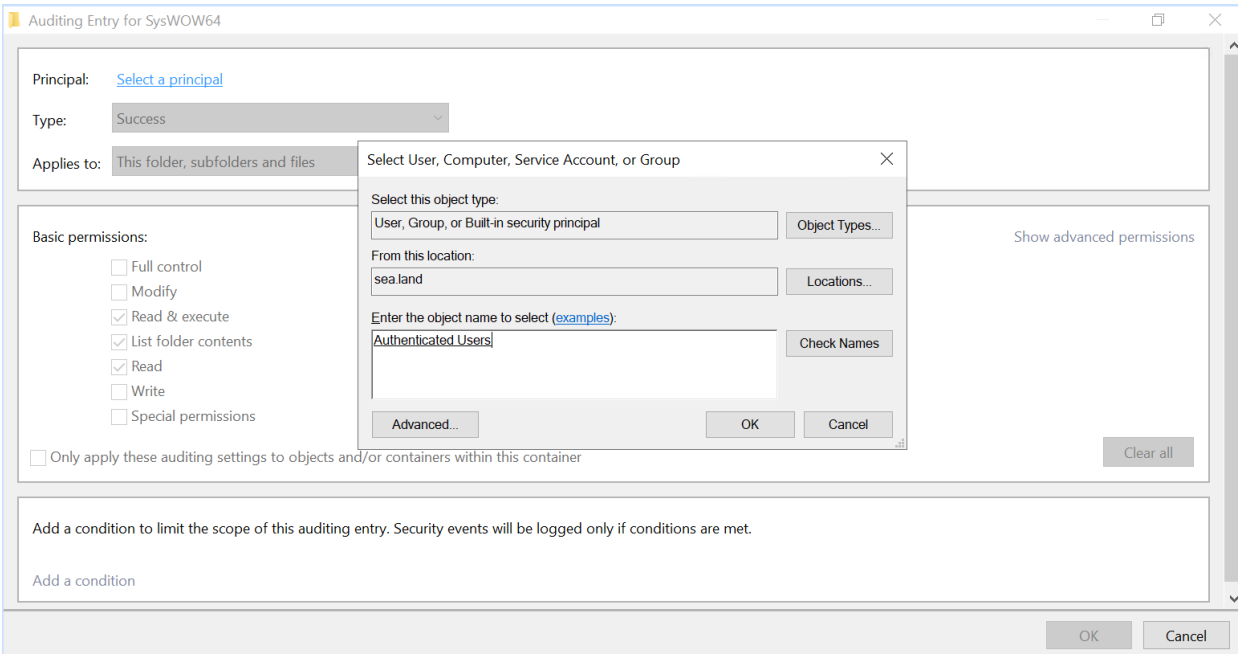


c. В появившемся окне перейдите на вкладку **Auditioning**.

d. Нажмите на кнопку **Add**, чтобы добавить новую запись.

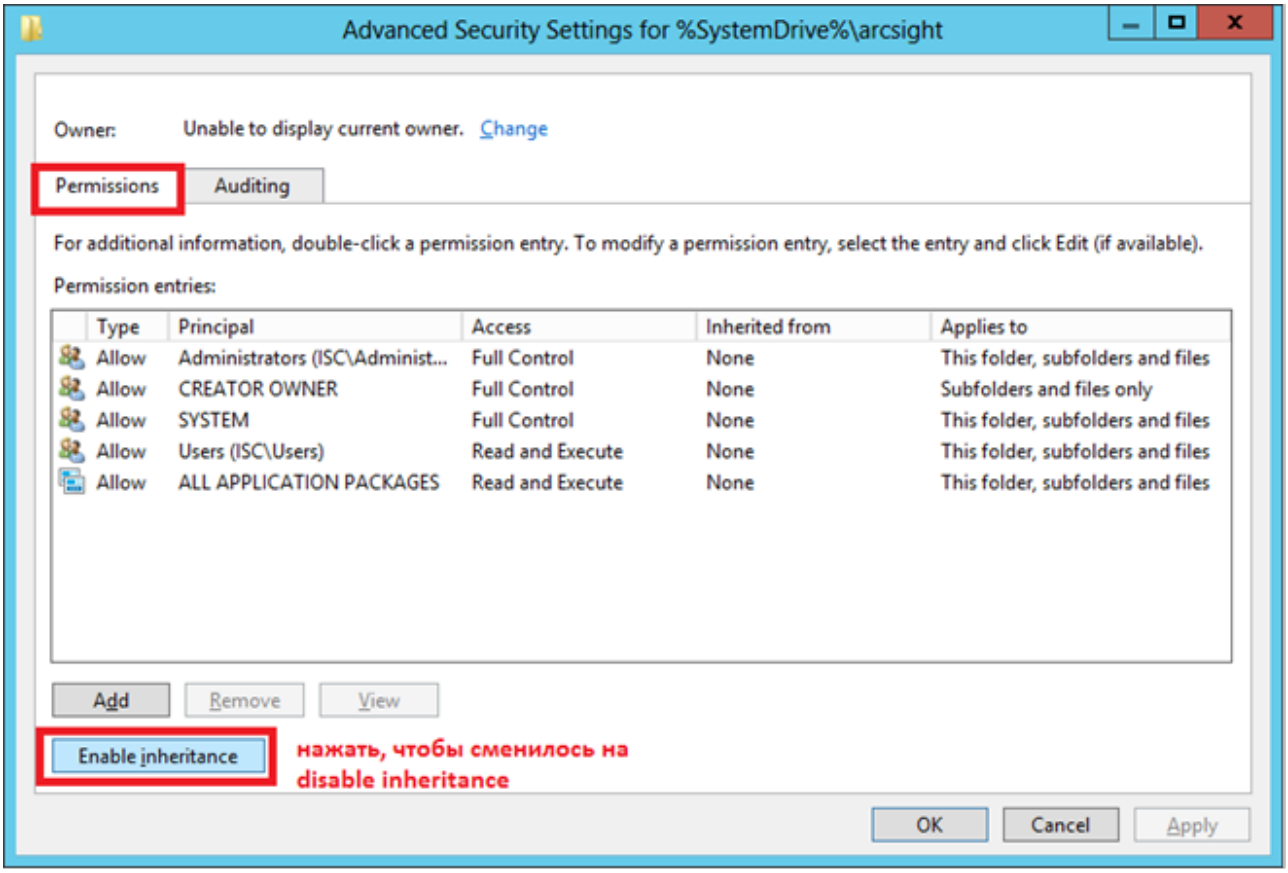
e. В появившемся окне нажмите на кнопку **Select a principal**.

f. Выберите учетные записи, которые необходимо логировать.

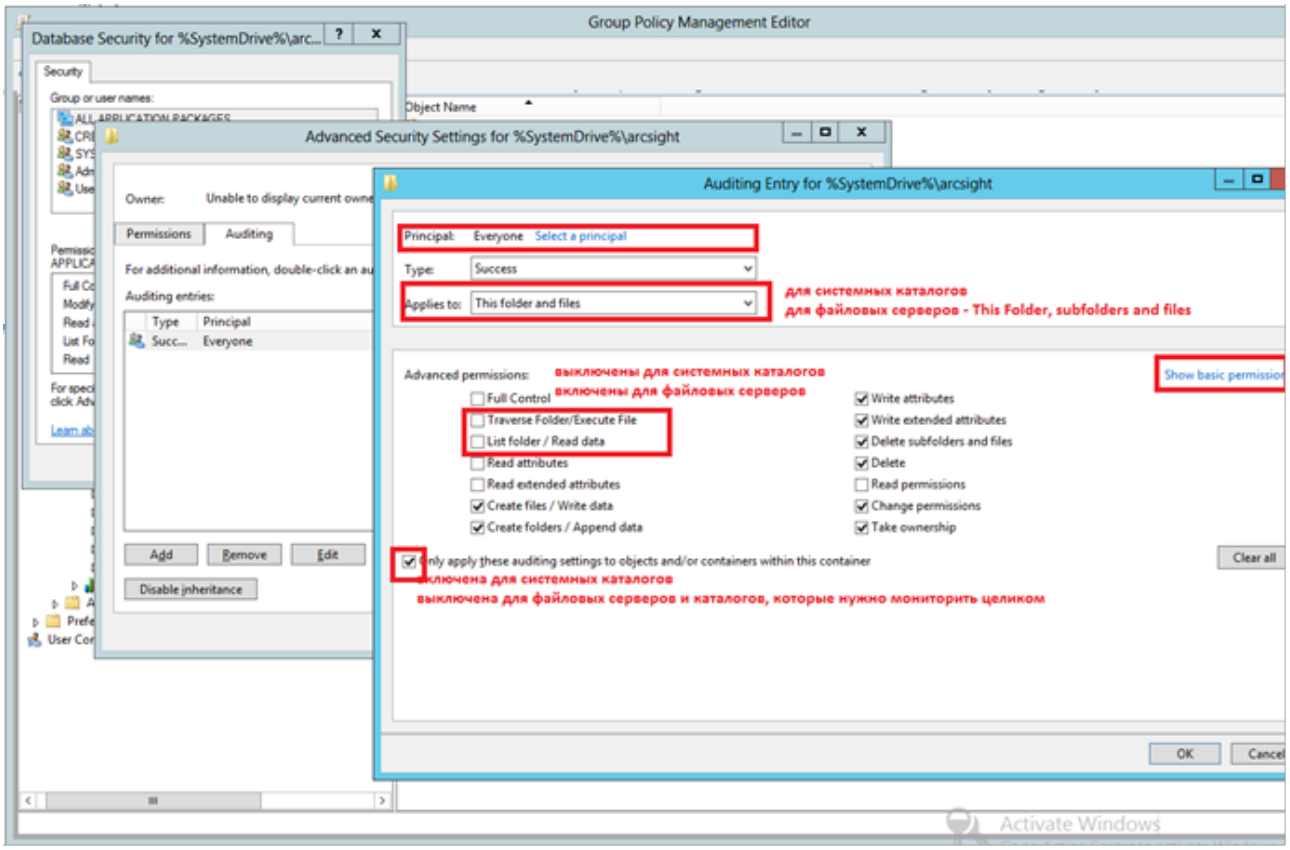


Пример включения аудита через групповую политику:

1. Чтобы параметры прав доступа к папке не перезаписались, необходимо выключить наследование. Для этого на вкладке **Permissions** нажмите на кнопку **Enable inheritance**. Название кнопки будет изменено на **Disable inheritance**.



2. На вкладке **Auditing** настройте требуемые параметры аудита.



3. При необходимости воспользуйтесь рекомендациями по настройке аудита файлов на разных типах хостов:

> Указанные ниже записи являются рекомендованными и могут отличаться в зависимости от архитектурных параметров информационной системы. Нижеперечисленные пункты в сумме могут оказывать сильную нагрузку на операционные системы и быстро заполнять хранилища событий.

Для системных файлов с опцией **Только для этой папки и файлов** (**This folder and files**) необходимо выполнить следующие действия:

1. Отключить наследование во вложенных каталогах.
2. Аудит в этих каталогах включать только на изменения.

Список каталогов для включения аудита:

- `c:\windows`;
- `c:\windows\system32`;
- `c:\windows\tasks`;
- `c:\yindows\SysWOW64`;
- `c:\windows\system32\drivers\etc\hosts`;
- `c:\windows\system32\Wbem`;
- `c:\windows\system`.

Данные каталоги являются критическими для мониторинга вредоносной активности. Изменение данных в этих директориях может указывать на попытки:

- установки вредоносного ПО и потенциального закрепления в системе;
- снижения уровня безопасности системы: изменения конфигурационных файлов, например, `hosts`, для обхода фильтрации, перехвата трафика или отключения защитных механизмов;
- повышения привилегий: модификации системных служб, задач планировщика или объектов WMI для выполнения кода с высокими привилегиями;
- нарушения работоспособности системы: непреднамеренного или злонамеренного удаления или изменения критических файлов, ведущего к отказу в обслуживании или нестабильной работе;
- сокрытия следов: очистки или изменения журналов событий и следов деятельности.

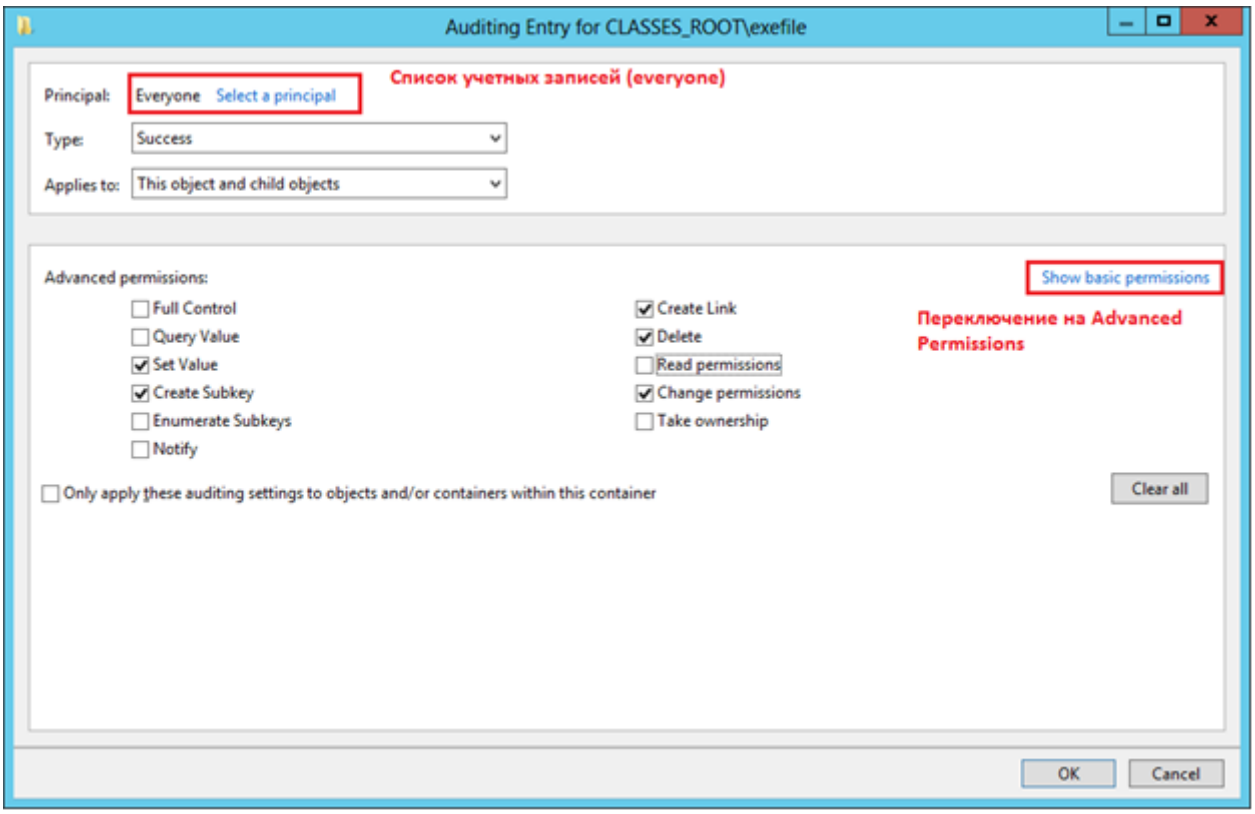
Вследствие расширенного аудита могут возникать проблемы с производительностью или целостностью мониторинга:

- замедление отклика системы из-за обработки большого количества данных;
- повышенная нагрузка на диск из-за его постоянной активности;
- повышенная нагрузка на ЦП из-за траты вычислительной мощи на обработку событий аудита;
- отключение аудита из-за переполнения дисков.

Настройка аудита реестра

Настройка аудита реестра групповых политик выполняется в разделе **Policies** → **Windows Settings** → **Security Settings** → **Registry** → **Add Key**.

Выберите путь к веткам реестра и выполните настройку аудита реестра аналогично настройке аудита доступа к файлам.



Ключи реестра для настройки SACL при применении доменных политик

В случае отсутствия указанных веток реестра их настройка не выполняется.

Ключи реестра для локальной настройки SACL (regedit)

Microsoft Windows Security: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-980	Установлено ПО для удаленного доступа	Атакующие могут использовать легитимное программное обеспечение, маскирующееся под легитимное, для осуществления удаленного управления, получения чувствительной информации или других вредоносных действий. Данное правило обнаруживает установку сервиса, который необходим для фоновой работы ПО для удаленного доступа и возможности подключения к устройству.	• Persistence (TA0003) • Lateral Movement (TA0008) • Command and Control (TA0011) • Remote Services (T1021) • VNC (T1021.005) • External Remote Services (T1133) • Remote Access Tools (T1219) • Remote Desktop Software (T1219.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-986	Зафиксирована атака типа AS-REP Roasting	В Active Directory-домене практически всегда используется Kerberos как средство аутентификации. Протокол Kerberos выдает ключи доступа или билеты, которые содержат фрагмент данных, зашифрованный с помощью исходного ключа пользователя, полученного из его пароля. Если получить такой ключ, то можно перебрать множество паролей оффлайн, основываясь на этих данных, и таким образом угадать пароль пользователя. На этом принципе основаны атаки Kerberoast и AS-REP Roasting. Принципиальное отличие AS-REP Roasting — это получение этого ключа без аутентификации в Active Directory, для атаки нужно лишь имя уязвимого пользователя и возможность подключения к контроллеру домена. Такая ситуация происходит, потому что параметр userAccountControl пользователя AD может содержать флаг `DONT_REQ_PREAUTH`, который позволяет запросить билет с ключом пользователя без предварительной аутентификации. Этот режим необходим для устаревших устройств, которые не поддерживают аутентификацию через Kerberos, но при этом нуждаются в доступе к ключам.	• Initial Access (TA0001) • Persistence (TA0003) • Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Credential Access (TA0006) • Valid Accounts (T1078) • Domain Accounts (T1078.002) • Brute Force (T1110) • Password Cracking (T1110.002) • Steal or Forge Kerberos Tickets (T1558) • AS-REP Roasting (T1558.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-988	Атака DCSync	Правило направлено на детектирование выполнения атаки DCSync. DCSync -– атака, позволяющая атакующему выдавать себя за контроллер домена (DC, domain controller) с целью получения учетных данных пользователей для последующего горизонтального перемещения в сети и/или доступа к конфиденциальной информации. В основе атаки лежит механизм, предусмотренный для выполнения репликации данных между контроллерами домена (DC). Правило направлено на детектирование выполнения репликации домена (атаки DCSync) именно от пользовательских учетных записей. Если будет выполняться репликация от машинной учетной записи, то правило это не обнаружит.	• Credential Access (TA0006) • OS Credential Dumping (T1003) • DCSync (T1003.006)
RV-D-993	Попытка дампа процесса LSASS с помощью comsvcs.dll	Атакующий может попытаться получить данные учетных записей, сделав дамп процесса LSASS (Local Security Authority Subsystem Service), в памяти которого хранятся учетные данные пользователей. Для этого может использоваться встроенная библиотека comsvcs.dll и ее функция MiniDump, предназначенная для создания дампов процессов. Правило фиксирует попытку получения дампа, но не свидетельствует о его успешном выполнении.	• Credential Access (TA0006) • OS Credential Dumping (T1003) • LSASS Memory (T1003.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-996	Возможно успешный подбор пароля пользователя	Множественные попытки входа на хост с одного удаленного узла с указанием неверного пароля и удачный вход после этого могут указывать на успешный подбор пароля. Для получения доступа к учетной записи или хосту атакующий может попробовать подобрать пароль с помощью перебора. Правило выявляет успешную аутентификацию, следующую после множественных неудачных попыток входа по протоколам NTLM и Kerberos на доменных и локальных хостах.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)
RV-D-999	Подозрительный доступ к файлу NTDS.dit	Атакующие для получения данных всех учетных записей в домене могут попробовать получить дамп файла `NTDS.dit`. Данный файл содержит информацию о всех пользователях в домене, включая хэши их паролей. Данное правило позволяет обнаружить подозрительные доступы к файлу `NTDS.dit`, что может свидетельствовать о попытке получения дампа или копирования файла.	• Credential Access (TA0006) • OS Credential Dumping (T1003) • NTDS (T1003.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1006	Использование средств туннелирования трафика	Средства туннелирования трафика, такие как ngrok, rsockstun, localtonet и другие, активно используются атакующими для организации обратных туннелей и проксирования трафика, позволяя обходить сетевые ограничения и устанавливать устойчивую связь с инфраструктурой управления (C2). Данное правило отслеживает запуск утилит с характерными для запуска обратных туннелей параметрами, например, `-R`.	• Defense Evasion (TA0005) • Command and Control (TA0011) • Proxy (T1090) • Protocol Tunneling (T1572) • Encrypted Channel (T1573) • Network Boundary Bridging (T1599)
RV-D-1008	Подбор пароля учетной записи на хосте	Множественные попытки входа на хост с одного удаленного узла с указанием неверного пароля могут указывать на подбор пароля. Атакующий для получения доступа к учетной записи или хосту может попробовать подобрать пароль методом перебора. Правило обнаруживает на доменном или локальном хосте подбор пароля для учетной записи по протоколам NTLM и Kerberos.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)
RV-D-1009	Множественные неудачные попытки аутентификации учетной записи	Для получения доступа к домену атакующий может попробовать подобрать пароль для учетной записи в домене с помощью перебора паролей. Правило обнаруживает множественные попытки проверки учетных данных на доменном контроллере с неверным паролем по протоколам NTLM или Kerberos.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1011	Перечисление учетных записей в домене методом перебора	Для получения информации о существующих учетных записях в домене атакующий может использовать перебор по списку возможных пользователей для последующего перебора паролей. Данное правило обнаруживает перебор учетных записей в домене по протоколам NTLM и Kerberos. В событиях NTLM аутентификации 4776 может не всегда отображаться имя хоста. В этом случае можно посмотреть события 4625 с аналогичной учетной записью в дельту времени или события 4771 с Kerberos-аутентификацией.	• Credential Access (TA0006) • Discovery (TA0007) • Account Discovery (T1087) • Domain Account (T1087.002) • Brute Force (T1110) • Password Guessing (T1110.001)
RV-D-1012	Разведка системы при помощи WMI	Данное правило срабатывает в случае возможной разведки системы при помощи WMI. WMI — это функция администрирования, которая позволяет получать доступ к компонентам системы Windows. WMI может быть использован атакующими для выполнения вредоносных команд и полезной нагрузки, а также для сбора информации о системе и перемещения по сети. Разведка системы при помощи WMI может свидетельствовать о действиях атакующего по определению дальнейших векторов атак. Также данная активность может быть ложно-положительной и свидетельствовать о работе легитимного ПО. В случае срабатывания правила необходимо опросить пользователя, ответственного за учетную запись инициатора активности, на предмет выполняемых действий. В случае нелегитимности — заблокировать УЗ инициатора активности.	• Discovery (TA0007) • Windows Management Instrumentation (T1047) • Gather Victim Host Information (T1592) • Client Configurations (T1592.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1014	URL-схема в командной строке процесса	Чтобы избежать обнаружения, атакующий может выполнять команды и запускать исполняемые файлы через "посредника" в виде системных программ. Системные исполняемые файлы зачастую подписаны и могут быть занесены в списки исключений СЗИ (средств защиты информации). Некоторые из них в качестве аргумента могут принимать URL файла, что позволяет атакующему выполнить вредоносный код или команды без их предварительной загрузки на хост. Детектирование опирается на то, что в легитимных целях система не передает URL-адреса указанным программам.	• Execution (TA0002) • Defense Evasion (TA0005) • Command and Scripting Interpreter (T1059) • Shared Modules (T1129) • User Execution (T1204) • Malicious File (T1204.002)
RV-D-1016	Разведка ключей реестра	Правило обнаруживает перечисление ключей реестра, которые могут быть интересны при разведке информации об узле. Данная техника часто используется атакующими на начальном этапе атаки для сбора критически важной информации о системе установленного ПО, параметров безопасности, данных автозагрузки и истории действий пользователя. Полученные сведения позволяют атакующему оценить вектор для дальнейшей эксплуатации. В случае срабатывания правила необходимо опросить пользователя, ответственного за учетную запись инициатора активности, на предмет выполняемых действий. В случае нелегитимности — заблокировать УЗ инициатора активности.	• Discovery (TA0007) • Query Registry (T1012) • System Information Discovery (T1082)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1017	Зафиксированы подозрительные операции при помощи WMI	Данное правило детектирует проведение подозрительных операций при помощи WMI. Под подозрительными операциями подразумевается активность, не характерная при обычной работе пользователя. К ним относятся методы PutInstance (метод, который позволяет создавать или обновлять экземпляр существующего класса в репозитории WMI) и ExecMethod (позволяет выполнять метод, экспортированный объектом CIM). При возникновении активности рекомендуется проанализировать смежные события по созданию процессов на предмет подозрительной активности. Данная активность является аномальной и может говорить о попытках атакующего закрепиться на хосте или исполнить вредоносный код. В случае срабатывания данного правила требуется опросить пользователя, ответственного за УЗ инициатора активности, на предмет указанных в событии действий. Если активность не является легитимной, требуется заблокировать УЗ инициатора активности на время инцидента.	• Execution (TA0002) • Persistence (TA0003) • Windows Management Instrumentation (T1047)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1018	Создание или изменение сервиса с помощью командной строки	Для закрепления или повышения привилегий в системе атакующий может использовать сервисы. Правило позволяет обнаружить попытку создания сервиса или изменения конфигурации сервиса с помощью системных утилит `sc.exe/wmic.exe/reg.exe`. Использование данных утилит с командами создания или изменения сервисов не является типичным для систем Windows, что может указывать на нелегитимную активность. Данное правило детектирует использование системных утилит с конкретными параметрами, характерными для изменения пути к исполняемым файлам существующих сервисов или создания атакующим нового сервиса в системе. Просмотреть сервисы на хосте можно в оснастке services.msc.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Service Stop (T1489) • Hijack Execution Flow (T1574) • Services Registry Permissions Weakness (T1574.011)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1019	Создан сервис с подозрительными параметрами	Данное правило срабатывает при создании сервиса с нестандартным исполняемым файлом или путем к нему (например, при наличии в пути папки temp, tmp или использовании переменных окружения %temp%), который выполнит сервис при запуске. Исполнение таких параметров в созданных сервисах используется в хакерских инструментах Meterpreter и Cobalt Strike для повышения привилегий. В данном случае функция GetSystem создает сервис с правами System, в который передаются команды посредством named pipe. Named pipe — это канал для обмена данными между инициатором — "сервером" и клиентом. Также данное правило срабатывает при использовании таких утилит, как `smbexec`, `psexec`, так как они используют сервисы для выполнения команд, и при любом использовании командной строки в созданном сервисе.	• Execution (TA0002) • System Services (T1569) • Service Execution (T1569.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1020	Установлен сервис не из системного/стандартного пути	Для закрепления или повышения привилегий в системе атакующий может использовать сервисы. Правило обнаруживает создание сервиса, у которого исполняемый файл находится не в системном или стандартном пути. Так как у атакующего может не хватать прав на запись исполняемого файла (вредоносного программного обеспечения) в системную директорию, он может использовать любое другое местоположение в файловой системе, а для гарантированного его запуска — применять сервисы. Легитимные сервисы, как правило, располагают исполняемые файлы в системных путях. Просмотреть установленные сервисы и связанные с ними исполняемые файлы можно в оснастке services.msc. Исключения для легитимных путей к файлам указаны в поле `on_event`.	• Execution (TA0002) • System Services (T1569) • Service Execution (T1569.002)
RV-D-1051	Размещение архивов в сетевой папке Windows	Атакующие могут размещать данные, собранные из нескольких систем, в централизованном месте или в каталоге на одной системе перед эксфильтрацией. Данные могут храниться в отдельных файлах или объединяться в один файл с помощью таких методов, как архивирование собранных данных.	• Collection (TA0009) • Data Staged (T1074) • Remote Data Staging (T1074.002) • Archive Collected Data (T1560)
RV-D-1052	Поиск данных в сетевых папках Windows	Атакующие могут использовать сетевые ресурсы на скомпрометированных компьютерах, чтобы найти интересующие их файлы для последующего развития атаки.	• Collection (TA0009) • Data from Network Shared Drive (T1039)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1053	Удален объект групповой политики	Групповая политика — это набор параметров для централизованного управления пользователями и компьютерами в домене. Компонентами групповой политики являются контейнер групповой политики и объекты, которые находятся в нем. Атакующий может воспользоваться правами на удаление GPO для обхода политик и выполнения деструктивных действий. Данное правило отслеживает использование прав на удаление объектов или контейнеров групповой политики.	• Privilege Escalation (TA0004) • Domain or Tenant Policy Modification (T1484) • Group Policy Modification (T1484.001)
RV-D-1054	Изменена групповая политика домена по умолчанию	В доменной инфраструктуре Active Directory существуют Default Domain Policy (политика домена по умолчанию) и Default Domain Controllers Policy (политика для доменных контроллеров), у которых по умолчанию есть свой уникальный ID групповой политики. Default Domain Policy содержит в себе базовые политики для домена и имеет уникальный глобальный идентификатор GUID 31b2f340-016d-11d2-945f-00c04fb984f9, по которому можно определить, что это за объект групповой политики. Default Domain Controllers Policy содержит в себе базовые политики для контроллеров домена, GUID — 6AC1786C-016F-11D2-945F-00C04FB984F9. Данное правило обнаруживает попытки редактирования файлов групповой политики. Такие изменения атакующий может использовать для повышения привилегий или закрепления в системе.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Domain or Tenant Policy Modification (T1484) • Group Policy Modification (T1484.001) • Modify Authentication Process (T1556) • Reversible Encryption (T1556.005)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1078	Доступ к чувствительному сетевому диску Windows	Атакующие могут использовать сетевые ресурсы на скомпрометированных компьютерах, чтобы найти интересующие их файлы. При срабатывании данного правила корреляции необходимо посмотреть время срабатывания, пользователя и критичность сетевого диска.	• Collection (TA0009) • Data from Network Shared Drive (T1039)
RV-D-1079	Изменение запланированной задачи в групповой политике	Для повышения привилегий и закрепления в системе атакующий может использовать объекты групповых политик. Объекты групповых политик — это контейнеры с параметрами групповой политики, состоящие из файлов, которые хранятся по сетевому пути `\\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\` или локально на доменном контроллере по пути `C:\Windows\SYSVOL\domain\Policies`. Для этого атакующий может изменить или создать файл групповой политики, чтобы исполнить вредоносную команду/код. В данном правиле отслеживаются изменение или создание запланированной задачи в групповой политике по сетевому пути.	• Privilege Escalation (TA0004) • Domain or Tenant Policy Modification (T1484) • Group Policy Modification (T1484.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1080	Поиск учетных данных в групповых политиках	Данное правило направлено на детектирование атаки, связанной с поиском файлов групповых политик, содержащих конфиденциальную информацию. Атакующий может использовать команды, такие как `findstr` или `Get-GPPPassword`, для поиска XML-файлов в папке SYSVOL, где могут храниться настройки групповых политик, включая зашифрованные пароли. Успешная эксплуатация позволяет извлечь данные, которые могут быть использованы для дальнейшего распространения по сети, повышения привилегий или доступа к другим системам. В случае срабатывания правила необходимо получить разъяснения о причине данной активности от лица, ответственного за учетную запись. В случае отсутствия обратной связи — заблокировать учетную запись сотрудника, заблокировать узел, с которого произошел запрос, и провести внутреннее расследование.	• Credential Access (TA0006) • Unsecured Credentials (T1552) • Group Policy Preferences (T1552.006)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1091	Чтение процесса LSASS от подозрительного процесса	Атакующий может попытаться получить данные других учетных записей с помощью дампа системного процесса LSASS (Local Security Authority Subsystem Service), который хранит в своей памяти учетные данные авторизованных пользователей на узле. Данное правило обнаруживает предоставление доступа на чтение процесса LSASS подозрительным процессам. Существует системное/легитимное ПО, которое обращается к процессу LSASS с правами на чтение. Данные процессы внесены в исключения в поле `on_event`. В исключения входят `taskmgr.exe` (диспетчер задач), который при запуске запрашивает доступ на чтение lsass, утилиты из набора Microsoft Sysinternals, например, Process Explorer, Process Monitor, Autoruns. Правило не свидетельствует о фактическом удачном дампе процесса, а указывает на получение доступа от подозрительного или нестандартного для Windows процесса.	• Credential Access (TA0006) • OS Credential Dumping (T1003) • LSASS Memory (T1003.001)
RV-D-1092	Закрепление в директорию автозагрузки	Атакующий, с целью закрепления, может добавить ВПО в директории автозапуска. Указанная активность позволит потенциальному ВПО запускаться каждый раз при включении системы. Данная активность является аномальной и может свидетельствовать об активности ВПО.	• Persistence (TA0003) • Boot or Logon Autostart Execution (T1547) • Registry Run Keys / Startup Folder (T1547.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1093	Закрепление в Print Processors через подозрительную DLL	Служба очереди печати (`spoolsv.exe`) работает за счет DLL-библиотек, которые загружаются во время загрузки ПК, и атакующие злоупотребляют ими, выполняя свои DLL во время загрузки. Одним из способов добавления DLL является добавление нужной DLL по определенному пути файловой системы.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Boot or Logon Autostart Execution (T1547) • Print Processors (T1547.012)
RV-D-1094	Очистка истории команд PowerShell в Windows	Данное правило направлено на детектирование подозрительных действий, связанных с использованием техники очистки истории команд PowerShell, которая позволяет атакующему скрывать следы своей активности, удаляя или предотвращая сохранение выполненных команд. Такое поведение является аномальным для стандартной работы пользователей и может указывать на попытку атакующего замаскировать свои действия в системе. Обнаружение осуществляется на основании использования ключевых команд PowerShell, таких как Clear-History, Remove-Item, с обращением к файлу истории или изменения параметров Set-PSReadlineOption.	• Defense Evasion (TA0005) • Indicator Removal (T1070) • Clear Command History (T1070.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1095	Добавление файла в директорию расширения браузера	Данное правило направлено на обнаружение подозрительных действий, связанных с добавлением файлов в директорию расширений браузера. Такие действия могут быть использованы атакующими для установки вредоносных или нежелательных расширений, которые могут изменять поведение браузера, собирать конфиденциальные данные пользователя или выполнять другие вредоносные операции.	• Persistence (TA0003) • Software Extensions (T1176) • Browser Extensions (T1176.001) • Browser Information Discovery (T1217)
RV-D-1096	Удаленная эксплуатация DCOM-объекта Excel.Application	Правило детектирует удаленный запуск процессов с помощью DCOM. После получения первоначального доступа атакующий может начать горизонтальное перемещение по инфраструктуре. С помощью объектов Excel.Application атакующий может скрытно выполнять вредоносный код через автоматические макросы Excel.	• Lateral Movement (TA0008) • Remote Services (T1021) • Distributed Component Object Model (T1021.003)
RV-D-1107	Регистрация вредоносного Password Filter	Пакеты уведомлений LSA (Notification Packages) являются критически важным компонентом подсистемы аутентификации Windows, отвечающим за проверку и обработку паролей в доменной среде. Эти пакеты, представляющие собой динамические библиотеки (DLL), загружаются процессом Local Security Authority (LSA) при запуске системы и получают доступ к учетным данным пользователей в момент их изменения. Легитимно используются для реализации расширенных политик сложности паролей.	• Persistence (TA0003) • Modify Authentication Process (T1556) • Password Filter DLL (T1556.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1119	Включение функции обратимого шифрования	Обратимое шифрование паролей является альтернативным методом хранения учетных данных в Active Directory, при котором пароли сохраняются с использованием двустороннего алгоритма шифрования вместо криптостойких хэшей. В отличие от стандартного хэширования NTLM, данный метод позволяет восстановить исходные пароли в открытом виде при наличии соответствующих ключей дешифрования.	• Persistence (TA0003) • Credential Access (TA0006) • Credentials from Password Stores (T1555) • Modify Authentication Process (T1556) • Reversible Encryption (T1556.005) • Impair Defenses (T1562)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1125	Включено обратимое шифрование паролей	В Active Directory по умолчанию пароли хранятся в виде необратимых хэшей (NTLM), что обеспечивает базовую защиту даже при компрометации базы данных. В системе существует механизм обратимого шифрования паролей (Reversible Encryption), предназначенный для обратной совместимости с устаревшими приложениями, которые требуют доступа к паролю в открытом виде. Это позволяет атакующему, получившему доступ к данным домена, легко расшифровать пароли пользователей.	• Persistence (TA0003) • Defense Evasion (TA0005) • Credential Access (TA0006) • Valid Accounts (T1078) • Account Manipulation (T1098) • Domain or Tenant Policy Modification (T1484) • Use Alternate Authentication Material (T1550) • Unsecured Credentials (T1552) • Modify Authentication Process (T1556) • Reversible Encryption (T1556.005) • Steal or Forge Kerberos Tickets (T1558)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1127	Выполнение прокси-файла через verclsid	Verclsid.exe — легитимная утилита проверки COM-объектов, предназначенная для регистрации и верификации CLSID через COM-инфраструктуру. Эта утилита может выполнять произвольный код из DLL-файлов, указанных в качестве COM-серверов, что позволяет атакующему обойти механизмы контроля приложений, маскируя выполнение вредоносной нагрузки под подписанный системный процесс.	• Execution (TA0002) • Defense Evasion (TA0005) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Windows Command Shell (T1059.003) • System Binary Proxy Execution (T1218) • Verclsid (T1218.012)
RV-D-1128	Подозрительное чтение данных приложений	Большинство браузеров и некоторые приложения для обмена сообщениями хранят учетные данные, cookie-файлы, историю просмотров и конфигурации в локальных директориях профиля пользователя (например, AppData в Windows). Эти директории часто становятся первой целью атакующих для разведки (T1217 Browser Information Discovery). Данное правило отслеживает обращение к файлам, где хранятся учетные данные или другие чувствительные данные в хранилищах браузеров и приложений, с целью выявления подозрительных операций чтения.	• Discovery (TA0007) • Browser Information Discovery (T1217)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1129	Установка пакетов msi из пользовательской директории	Атакующие могут встроить вредоносный код (скрипты или бинарные файлы) в установочные пакеты программ, и при установке легитимного приложения этот код запускается автоматически, нередко с повышенными правами. В операционных системах семейства Windows в качестве установочных пакетов чаще всего используются файлы формата `.msi`. Правило позволяет обнаруживать установку MSI-пакетов из пользовательских или временных директорий.	• Privilege Escalation (TA0004) • Defense Evasion (TA0005) • System Binary Proxy Execution (T1218) • Msiexec (T1218.007) • Event Triggered Execution (T1546) • Installer Packages (T1546.016)
RV-D-1134	Создание правил почты через PowerShell	Данное правило направлено на обнаружение создания или модификации правил почтовых ящиков (InboxRule) или транспортных правил (TransportRule) с использованием командлетов PowerShell. Эти правила являются штатными функциями Microsoft Exchange, предназначенными для автоматической обработки и маршрутизации сообщений. Атакующий изменяет или добавляет их с целью скрытой пересылки конфиденциальных данных, автоматического удаления предупреждений систем безопасности или сокрытия следов своей деятельности.	• Execution (TA0002) • Defense Evasion (TA0005) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Hide Artifacts (T1564) • Email Hiding Rules (T1564.008)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1136	Построение образа в Windows	Правило обнаруживает команды для построения образа контейнера, используемые, чтобы обойти защиту от получения вредоносных образов из общедоступных реестров.	• Defense Evasion (TA0005) • Build Image on Host (T1612)
RV-D-1146	Изменение атрибутов групповой политики	Правило отслеживает изменение атрибутов элементов групповой политики (GPO). При модификации GPO могут изменяется атрибуты gPCMachineExtensionNames (определяет действия GPO в контексте компьютера), gPCUserExtensionNames (определяет действия GPO в контексте пользователя), gPCFileSysPath (указывает на папку, связанную с объектом групповой политики). Значение данных атрибутов обновляется при изменении объектов групповой политики. Атакующий может изменять объекты GPO для закрепления или повышения привилегий, изменяя задачи планировщика, ключи реестра, элементы автозагрузки и другие параметры. Для проведения атаки требуется учетная запись, которая имеет необходимые привилегии для изменения GPO.	• Privilege Escalation (TA0004) • Domain or Tenant Policy Modification (T1484) • Group Policy Modification (T1484.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1148	Удаление доменной\локальной\компьютерной учетной записи	После попадания в корпоративную сеть атакующий может попробовать закрепиться в системе через создание новой учетной записи. Данные действия избавляют от необходимости использовать уже скомпрометированные учетные записи или поддержание шелла для вторичного доступа в систему. После выполнения злонамеренных действий атакующий может попытаться удалить учетную запись, чтобы скрыть свои следы. Таким образом, данным правилом определяется удаление доменной\локальной\компьютерной учетной записи от подозрительной учетной записи.	• Persistence (TA0003) • Account Manipulation (T1098) • Create Account (T1136) • Local Account (T1136.001) • Domain Account (T1136.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1149	Добавление пользователя в критичные доменные группы	После попадания в корпоративную сеть атакующий может попробовать закрепиться в системе через создание новой учетной записи. Данные действия избавляют от необходимости использовать уже скомпрометированные учетные записи или поддержание шелла для вторичного доступа в систему. Чтобы можно было выполнять какие-либо действия под новой учетной записью, в том числе подключаться удаленно, нужно предоставить права для этих действий этой учетной записи. Для этого атакующий может попробовать добавить учетную запись в доменные группы, которые предоставляют необходимый доступ. Кроме того, наличие уязвимости в продукте VMware ESXi позволяет автоматически получать административный доступ к ESXi-гипервизорам, подключенным к Active Directory. Для этого атакующему достаточно добавить любого доменного пользователя в доменную группу ESX Admins, что делает важным отслеживание любых добавлений пользователей в данную группу.	• Persistence (TA0003) • Account Manipulation (T1098) • Additional Local or Domain Groups (T1098.007)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1150	Создание новой доменной\локальной\компьютерной учетной записи	После попадания в корпоративную сеть атакующий может попробовать закрепиться в системе через создание новой учетной записи. Данные действия избавляют от необходимости использовать уже скомпрометированные учетные записи или поддержание шелла для вторичного доступа в систему. Таким образом, данным правилом определяется создание новой доменной\локальной\компьютерной учетной записи от подозрительной учетной записи.	• Persistence (TA0003) • Account Manipulation (T1098) • Create Account (T1136) • Local Account (T1136.001) • Domain Account (T1136.002)
RV-D-1151	Изменение SPN учетной записи	Service Principal Name (SPN) — это уникальный идентификатор, который используется Kerberos для идентификации сервиса. Атакующий может попытаться изменить SPN для обхода различных механизмов аутентификации. Изменение данного атрибута может помочь атакующему провести репликацию данных между контроллерами домена (атаки DCSync и DCShadow) или получить доступ к билету Kerberos целевой учетной записи (атака Kerberoasting). Для проведения атаки атакующему требуются права, эквивалентные правам администратора домена. Правило детектирует наличие в измененном SPN объекта Global Catalog (GC), не являющегося DC, а также изменение SPN-аккаунта пользователя.	• Privilege Escalation (TA0004) • Account Manipulation (T1098)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1153	Создание и удаление учетной записи за одну минуту	После попадания в корпоративную сеть атакующий может попробовать закрепиться в системе через создание новой учетной записи. Данные действия избавляют от необходимости использования скомпрометированных учетных записей и шелла для повторного доступа. Атакующий или вредоносное программное обеспечение для большей конспирации может создать учетную запись, выполнить вредоносное действие под ней и сразу же ее удалить. Таким образом, данным правилом определяется создание новой доменной\локальной учетной записи и последующее ее удаление в течение минуты.	• Persistence (TA0003) • Account Manipulation (T1098) • Create Account (T1136) • Local Account (T1136.001) • Domain Account (T1136.002)
RV-D-1160	Создана пользовательская форма Outlook	Формы Outlook -– это возможность создания и использования пользовательских форм в Microsoft Outlook для управления информацией и данными. Атакующий может создать пользовательские формы Outlook, которые будут выполнять код при отправке специально созданного сообщения электронной почты, использующего ту же пользовательскую форму Outlook.	• Persistence (TA0003) • Office Application Startup (T1137) • Outlook Forms (T1137.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1161	Изменение настроек Outlook	Атакующие могут изменять критические настройки Microsoft Outlook через утилиту reg.exe или прямые записи в реестр Windows, чтобы обойти встроенные механизмы защиты почтового клиента. Используя изменение таких параметров, как включение «небезопасных» правил обработки почты, установка произвольных URL-адресов домашней страницы, автозапуск макросов и понижение уровня безопасности.	• Persistence (TA0003) • Defense Evasion (TA0005) • Modify Registry (T1112) • Office Application Startup (T1137) • Office Template Macros (T1137.001) • Outlook Home Page (T1137.004) • Outlook Rules (T1137.005)
RV-D-1162	Маскировка учетной записи под имя компьютера	После получения доступа к корпоративной сети атакующий может закрепиться в системе, создав новую учетную запись. Это позволяет отказаться от использования скомпрометированных учетных записей и поддержания постоянного шелла для повторного доступа. Для маскировки может быть создана учетная запись (далее — УЗ), внешне похожая на компьютерную, отличительным признаком которой является символ $ в конце имени. Данное правило выявляет создание или изменение доменной или локальной учетной записи, замаскированной под компьютерную учетную запись.	• Persistence (TA0003) • Defense Evasion (TA0005) • Masquerading (T1036) • Masquerade Account Name (T1036.010) • Create Account (T1136) • Local Account (T1136.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1165	Включение или отключение учетной записи	После попадания в корпоративную сеть атакующий может попробовать закрепиться в системе. Для этого ему требуется доступ к учетной записи. Чтобы не создавать новую учетную запись, атакующий может включить уже существующую учетную запись и после совершения атаки отключить ее. Данные действия избавляют от необходимости использовать уже скомпрометированные учетные записи, что маскирует выполняемые действия. Таким образом, данным правилом определяется включение и отключение доменной\локальной учетной записи.	• Persistence (TA0003) • Account Manipulation (T1098)
RV-D-1168	Изменения в планировщике задач	Task Scheduler или Планировщик задач — служба в Windows, которая позволяет автоматизированно выполнять запланированные задачи на устройстве по заранее заданному триггеру: время, наступление определенного события и другие. Данная служба удобна для атакующего тем, что запланированные задачи являются легитимными в операционной системе Windows. Это позволяет замаскировать вредоносные действия, а сам функционал планировщика задач не будет отключен администраторами, так как на нем строится работа всей системы. Данное правило направлено на детектирование внесения изменений в службу Task Scheduler с помощью инструментов, основанных на специальном API для работы с задачами.	• Execution (TA0002) • Persistence (TA0003) • Scheduled Task/Job (T1053) • At (T1053.002) • Scheduled Task (T1053.005)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1175	Аномальное поведение офисного ПО	Данное правило направлено на детектирование подозрительных действий, связанных с использованием офисных приложений (например, Microsoft Word, Excel или PowerPoint), которые являются аномальными для их стандартного поведения. Такое поведение может указывать на попытку атакующего эксплуатировать макросы, вставлять вредоносный код или инициировать запуск внешних исполняемых файлов. Детект выполняется при создании потока в процессах офисных приложений или запуска от их имени файлов, расширение которых не является для них нормой, например, `.exe`, `.bat` и другие. Успешная эксплуатация позволяет атакующему получить доступ к критически важным данным, что может быть использовано для дальнейшего продвижения по сети, повышения привилегий или компрометации систем.	• Privilege Escalation (TA0004) • Process Injection (T1055) • Thread Execution Hijacking (T1055.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1181	Интерактивный вход под сервисной учетной записью	Сервисная учетная запись, предназначенная для автоматизации задач, часто имеет доступ к важным данным и потенциально может иметь особые привилегии (права администратора). Поэтому важно отслеживать активность данных учетных записей. Интерактивный вход под такой учетной записью является необычной активностью. Они не персонализированы, и обычные пользователи не работают из-под них. Интерактивный вход может указывать на взлом учетной записи. Обнаружение активности требует внесения полного перечня сервисных учетных записей в активный список `service_account_list_cimv2`.	• Initial Access (TA0001) • Valid Accounts (T1078)
RV-D-1184	Вход под учетной записью, созданной по умолчанию	Правило предназначено для выявления входов в систему с использованием локальных учетных записей, создаваемых по умолчанию. В перечень таких учетных записей входят: Administrator, Guest, Local Service, DefaultAccount, WDAGUtilityAccount и Network Service. Активность, выполняемая под данными учетными записями, требует контроля, поскольку в штатной конфигурации они, как правило, отключены, а вход под ними не считается нормальной практикой.	• Initial Access (TA0001) • Valid Accounts (T1078) • Default Accounts (T1078.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1185	Манипуляции с теневыми копиями с помощью встроенных утилит	Для затруднения автоматического восстановления данных в системе атакующий может удалить или изменить теневые копии на Windows Server, что сделает их недоступными. Правило позволяет обнаружить удаление, изменение, отключение теневых копий с использованием встроенных утилит и команд `wmic`, `vssadmin`, `wbadmin`, `diskshadow` или отключение режима авто-восстановления при загрузке системы с помощью встроенной утилиты `bcdedit.exe`, что часто используют атакующие одновременно с удалением резервных копий. Данное правило направлено на обнаружение в командной строке запуска упомянутых утилит с параметрами, позволяющими манипулировать теневыми копиями.	• Impact (TA0040) • Inhibit System Recovery (T1490)
RV-D-1205	Новый сертификат root был установлен средствами Certutil.exe	Обнаружено выполнение утилиты `Certutil.exe` с флагом `addstor` для установки нового сертификата системы. Атакующие могут установить корневой сертификат на взломанную систему, чтобы избежать предупреждений при подключении к контролируемым веб-серверам. Корневые сертификаты являются частью инфраструктуры открытых ключей (PKI) и используются для проверки подлинности сертификатов удостоверяющих центров (ЦС). Если атакующий установит свой собственный корневой сертификат на целевой системе, то затем сможет подделывать сертификаты для любых веб-сайтов или служб без предупреждения или обнаружения со стороны браузера или клиента.	• Defense Evasion (TA0005) • Subvert Trust Controls (T1553) • Install Root Certificate (T1553.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1207	Удаленное выполнение команд с помощью SMBExec	Правило обнаруживает последовательность событий, которая указывает на использование утилиты для горизонтального перемещения и удаленного выполнения команд SMBExec из набора Impacket. Impacket — это набор утилит на Python, которые используют различные сетевые протоколы Windows для выполнения команд на удаленных системах. При использовании Smbexec для исполнения команд на удаленной системе происходит подключение к общей доступной папке с помощью протокола Smb (Server Message Block). Далее создается новый сервис, после чего исполняются заданные команды с правами созданного сервиса.	• Execution (TA0002) • Persistence (TA0003) • Lateral Movement (TA0008) • Remote Services (T1021) • SMB/Windows Admin Shares (T1021.002) • Create or Modify System Process (T1543) • Windows Service (T1543.003) • System Services (T1569) • Service Execution (T1569.002) • Lateral Tool Transfer (T1570)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1216	Подгрузка подозрительного пакета процессом LSA	Правило выявляет загрузку процессом LSA пакетов аутентификации, не относящихся к стандартному набору, используемому в штатной работе операционной системы, например, пакетов, загружаемых из нестандартного пути. Такая активность может указывать на попытку внедрения стороннего кода в процесс LSA с целью получения доступа к учетным данным для повышения привилегий.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Boot or Logon Autostart Execution (T1547) • Security Support Provider (T1547.005)
RV-D-1220	Атака DCShadow	DCShadow — это метод манипулирования объектами AD путем регистрации поддельного DC и моделирования необходимого поведения. При регистрации DC для узла добавляется атрибут SPN с неизменяемым GUID E3514235-4B06-11D1-AB04-00C04FC2DCD2. Атрибут определяет хост, с которым DC может проводить репликацию. После регистрации атакующий может внедрять и реплицировать изменения в инфраструктуру AD для любого объекта домена. Для проведения атаки требуются привилегии администратора домена. Правило отслеживает добавление узлу атрибута SPN, соответствующего GUID, и событие репликации DC с данным узлом.	• Defense Evasion (TA0005) • Rogue Domain Controller (T1207)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1234	Извлечение cab-файлов через Wusa.EXE	Атакующие используют `wusa.exe` с параметром `/extract` как LOLBin для распаковки CAB-архивов из пользовательских или временных директорий без применения сторонних утилит, что помогает обходить контроль запуска ПО и снижать заметность активности. Риск заключается в скрытой доставке и извлечении вредоносных компонентов (DLL, EXE, скриптов) в доверенном контексте системной утилиты с последующим выполнением, что затрудняет обнаружение и может привести к компрометации хоста. Данное правило обнаруживает запуск утилиты `wusa.exe` с аргументом `/extract` из подозрительных путей.	• Execution (TA0002) • System Binary Proxy Execution (T1218)
RV-D-1247	Атака Pass the Hash	Данное правило направлено на обнаружение подозрительных действий, связанных с использованием техники Pass-the-Hash (PtH), которая позволяет атакующему аутентифицироваться в системе, применяя NTLM-хэш пароля вместо его ввода. Такое поведение является аномальным для стандартных сценариев аутентификации и может указывать на попытку атакующего получить доступ к системам без знания пароля учетной записи. Обнаружение выполняется при анализе событий входа или при выполнении PowerShell-скриптов. Успешная эксплуатация PtH может привести к несанкционированному доступу к критически важным данным, использованию привилегированных учетных записей и дальнейшему продвижению атакующего в инфраструктуре.	• Defense Evasion (TA0005) • Use Alternate Authentication Material (T1550) • Pass the Hash (T1550.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1257	Атака Kerberoasting	Kerberoasting нацелен на получение билетов TGS, ассоциированных с пользовательскими учетными записями в Active Directory (AD). Для шифрования этих билетов используются сервисные ключи, полученные из паролей сервисных пользователей. Таким образом, методом подбора можно взломать пароль сервисной учетной записи в автономном режиме.	• Credential Access (TA0006) • Steal or Forge Kerberos Tickets (T1558) • Kerberoasting (T1558.003)
RV-D-1262	Копирование веток реестра, содержащих хэши паролей	Данное правило направлено на обнаружение подозрительных действий, связанных с использованием техники OS Credential Dumping, которая позволяет атакующим извлекать учетные данные (логины и пароли) из операционных систем. Правило детектирует два случая копирования веток реестра — это эксплуатация уязвимостей в Security Account Manager (SAM) и Local Security Authority (LSA) Secrets. SAM хранит хэши паролей пользователей, что делает его целью для атакующих. Из LSA атакующий может получить пароль учетной записи, от имени которой запускается какой-либо сервис, и учетные данные компьютерной учетной записи. Захват хэшей паролей позволяет атакующему впоследствии производить атаки на подбор паролей в оффлайн-режиме, расшифровать хэши и получить доступ к учетным записям пользователей.	• Credential Access (TA0006) • OS Credential Dumping (T1003) • Security Account Manager (T1003.002) • LSA Secrets (T1003.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1265	Удаленный запуск процесса с помощью WMI	Правило обнаруживает удаленный запуск процессов с помощью WMI (wmiexec + wmic). После получения первоначального доступа атакующий начинает горизонтальное перемещение по корпоративной сети жертвы. Одной из популярных утилит для этих целей является WMIExec из пакета Impacket или встроенная в Windows утилита wmic, которая предназначена для удаленного администрирования и позволяет запускать процессы, используя систему удаленного управления сервисами и передачи файлов.	• Lateral Movement (TA0008) • Remote Services (T1021)
RV-D-1274	Вход с разных хостов на один хост под одной учетной записью	Правило обнаруживает авторизацию пользователя на одном узле с разных хостов за короткий промежуток времени. Данное поведение является аномальным, атакующий может попытаться зайти на узел с разных хостов для горизонтального перемещения в информационной системе.	• Initial Access (TA0001) • Valid Accounts (T1078)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1277	Добавление пользователя в критичные локальные группы	После попадания в корпоративную сеть атакующий может попробовать закрепиться в системе через создание новой учетной записи. Данные действия избавляют от необходимости использовать уже скомпрометированные учетные записи или поддержания подключения для вторичного доступа в систему. Чтобы можно было выполнять какие-либо действия под новой учетной записью, в том числе подключаться удаленно, нужно назначить права на выполнение этих действий для этой учетной записи. Для этого атакующий может попробовать добавить учетную запись в локальные группы, которые предоставляют необходимый доступ.	• Persistence (TA0003) • Account Manipulation (T1098) • Additional Local or Domain Groups (T1098.007)
RV-D-1278	Вход под несуществующим пользователем	Правило предназначено для детектирования попыток входа под логином несуществующей учетной записи при доменной авторизации. Оно позволяет зафиксировать подозрительную активность или попытку несанкционированного доступа в информационную систему.	• Initial Access (TA0001) • Valid Accounts (T1078)
RV-D-1281	Вход на устройство под разными учетными записями	Правило детектирует множество подключений под разными учетными записями (УЗ) к одному узлу за 120 секунд. Атакующий может получить доступ к нескольким УЗ с разными привилегиями и подключаться под ними к одному известному ему устройству.	• Initial Access (TA0001) • Valid Accounts (T1078)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1284	Атака Password Spraying	Для получения доступа к домену атакующий может попробовать подобрать пароль для учетной записи в домене с помощью перебора одного или нескольких паролей одновременно для нескольких пользователей. Данный метод является менее заметным, так как происходит несколько попыток входа на одну учетную запись, что предотвращает ее блокировку. Правило обнаруживает распыление паролей для подбора учетных данных по NTLM и Kerberos с ошибкой `неверный пароль` для разных УЗ с одного хоста. В событиях NTLM аутентификации 4776 может не всегда отображаться имя хоста, в этом случае можно посмотреть события 4625 с аналогичной учетной записью в дельту времени или события 4771 с Kerberos аутентификацией.	• Credential Access (TA0006) • Brute Force (T1110) • Password Spraying (T1110.003) • Credential Stuffing (T1110.004)
RV-D-1285	Вход под учетной записью администратора	Правило предназначено для обнаружения входов в систему с использованием учетных записей администраторов. Учетные записи с повышенными привилегиями, подлежащие усиленному мониторингу, перечислены в списке `privileged_users_and_hosts`.	• Initial Access (TA0001) • Valid Accounts (T1078)
RV-D-1286	Вход на несколько узлов под одной учетной записью	Правило предназначено для обнаружения входов одного пользователя на различные узлы в ограниченный промежуток времени. Такая активность может быть характерна для атакующего, который получил доступ к учетной записи пользователя и использует ее для горизонтального перемещения.	• Initial Access (TA0001) • Valid Accounts (T1078) • Domain Accounts (T1078.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1287	Несистемный процесс повысил привилегии до системы	Правило обнаруживает создание процесса с SYSTEM-правами от пользовательского процесса. Это возможно при эксплуатации уязвимостей, связанных с получением системного токена, например, уязвимостей типа Potato. Полученный токен далее используется для создания процесса от пользователя SYSTEM через API-вызовы CreateProcessAsUser, CreateProcessWithToken. Детектирование построено на том, что процесс атакующего, изначально не имеющий системных прав, порождает процесс от пользователя SYSTEM.	• Privilege Escalation (TA0004) • Access Token Manipulation (T1134)
RV-D-1323	Потенциально вредоносное использование элементов панели управления	Данное правило выявляет нетипичное использование элементов панели управления Windows (файлов с расширением .cpl), которое может указывать на попытки выполнения кода или обхода защитных механизмов.	• Execution (TA0002) • Persistence (TA0003) • Defense Evasion (TA0005) • System Binary Proxy Execution (T1218) • Control Panel (T1218.002) • Event Triggered Execution (T1546)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1335	Изменение доверительных отношений между доменами	Атакующие могут создавать новые доверительные отношения между доменами, изменять параметры существующих или модифицировать конфигурацию доверительных отношений между доменами и тенантами, чтобы обойти защитные механизмы или повысить привилегии. Неавторизованные изменения могут привести к серьезным инцидентам безопасности.	• Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Domain or Tenant Policy Modification (T1484) • Trust Modification (T1484.002)
RV-D-1354	Изменение дескриптора безопасности в групповой политике	Дескриптор безопасности - это таблица с правами доступа для объектов в домене, группы или пользователя. Каждый объект групповой политики имеет свой уникальный глобальный идентификатор - GUID, по которому можно определить, что это за объект групповой политики. Атакующий, например, заполучив доступ к учетной записи, которая имеет права на изменение дескриптора безопасности для объекта групповой политики, может добавить права на изменение политики для другого объекта, с помощью которого он сможет в дальнейшем изменить групповую политику в домене.	• Domain or Tenant Policy Modification (T1484) • Group Policy Modification (T1484.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1361	Изменение пароля через утилиту mimikatz	После попадания в корпоративную сеть атакующий может скомпрометировать существующие учетные записи. Как правило, при компрометации атакующий знает только хэш пароля учетной записи. Есть сервисы, такие как Outlook Web Access, которые требуют явного указания пароля, а не его хэша. Поэтому атакующий для дальнейшего использования этой учетной записи может попробовать изменить пароль. Для этого во фреймворке mimikatz есть специальный модуль ChangeNTLM для смены пароля. Данная функция формирует нетипичные логи для смены пароля, поэтому данное правило направлено на детект смены пароля именно через mimikatz.	• Persistence (TA0003) • Account Manipulation (T1098)
RV-D-1362	Детектирование создания WMI-подписки	Подписка на события Windows Management Instrumentation (WMI Event Subscription) представляет собой механизм в Windows для отслеживания событий, происходящих в системе, с использованием WMI. Когда происходит событие, система может реагировать, выполняя предопределенные действия. Использование WMI Event Subscription может иметь потенциальные риски безопасности, так как атакующие могут использовать этот механизм для создания скрытых механизмов слежения или выполнения вредоносных действий в системе.	• Execution (TA0002) • Persistence (TA0003) • Windows Management Instrumentation (T1047) • Event Triggered Execution (T1546) • Windows Management Instrumentation Event Subscription (T1546.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1363	Удалена глобальная группа с включенной безопасностью	Обнаружение активности при удалении глобальной группы с поддержкой безопасности представляет собой серьезную угрозу для информационной безопасности. Этот вид атаки может привести к нарушению привилегированного доступа к данным и ресурсам, управляемым этой группой. Последствия удаления глобальной группы могут включать в себя утечку конфиденциальной информации и нарушение принципов безопасности системы.	• Persistence (TA0003) • Account Manipulation (T1098)
RV-D-1364	Изменение SID-History	SID History - это свойство объекта пользователя или группы, которое позволяет объекту сохранять идентификатор безопасности при переносе из одного домена в другой в рамках консолидации или реструктуризации домена. При переносе объекта в новый домен ему назначается новый идентификатор безопасности в целевом домене. Журнал SID позволяет объекту сохранить исходный идентификатор безопасности, чтобы не потерять доступ к ресурсам в исходном домене. Этим механизмом также можно злоупотреблять в качестве закрепления: добавление идентификатора безопасности привилегированной учетной записи или группы к атрибуту SID-History контролируемой учетной записи предоставляет права, связанные с учетной записью или группой, для которой добавляется идентификатор безопасности.	• Privilege Escalation (TA0004) • Access Token Manipulation (T1134) • SID-History Injection (T1134.005)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1370	Сброс пароля учетной записи через mimikatz	После проникновения в корпоративную сеть атакующий может получить список учетных записей и захватить контроль над той, которая имеет права на сброс паролей. Это позволяет ему изменять пароли других пользователей в домене, устанавливая свои. Достигнув цели, атакующий может, например, с помощью DCSync извлечь хэши старых паролей и затем восстановить предыдущий пароль, чтобы скрыть факт несанкционированного изменения. Во фреймворке mimikatz для этого предусмотрен модуль SetNTLM. Поскольку этот метод создает нетипичные логи сброса пароля, правило направлено на выявление подобных действий.	• Persistence (TA0003) • Account Manipulation (T1098)
RV-D-1379	Изменение прав доступа к файлам	Данное правило направлено на детектирование подозрительных действий, связанных с изменением прав доступа к файлам и папкам, что может свидетельствовать о попытке атакующего эскалировать привилегии или скрыть следы своей активности. Техника T1222.001 позволяет атакующему изменять владельца или модифицировать ACL (список управления доступом) файловых объектов путем получения несанкционированного доступа к данным или возможности их удаления. Успешная эксплуатация данной техники может привести к компрометации конфиденциальной информации, дальнейшему продвижению атакующего по сети и затруднению расследования инцидентов.	• Defense Evasion (TA0005) • File and Directory Permissions Modification (T1222) • Windows File and Directory Permissions Modification (T1222.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1382	Изменение атрибутов учетной записи	Правило отслеживает изменение атрибутов учетных записей. При изменении атрибута можно закрепиться в системе или повысить свои привилегии. Для проведения атаки атакующему требуется учетная запись, которая имеет необходимые привилегии для изменения атрибута.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Account Manipulation (T1098) • Boot or Logon Autostart Execution (T1547)
RV-D-1563	Блокировка сервисного аккаунта	Блокировка или неудачные попытки входа в критически важные сервисные учетные записи являются индикатором серьезного технического сбоя или целенаправленной атаки на отказ в обслуживании (DoS). Сервисные учетные записи используются для работы ключевых бизнес-приложений, баз данных и системных служб. В отличие от обычных пользователей, их блокировка часто приводит к немедленной остановке автоматизированных процессов. Данное правило отслеживает события аутентификации NTLM (Event ID 4776) на контроллерах домена и детектирует ошибки, связанные с неверным паролем (0xc000006a) или уже заблокированным состоянием учетной записи (0xc0000234), если имя пользователя входит в список `service_accounts_cimv2`.	• Credential Access (TA0006) • Impact (TA0040) • Brute Force (T1110) • Password Guessing (T1110.001) • Service Stop (T1489)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1610	Выполнение скриптов через проксирование PubPrn	Атакующий может использовать штатный скрипт Windows `pubprn.vbs` совместно с `cscript.exe` или `wscript.exe` для проксированного выполнения удаленного scriptlet-объекта через схему `script:`. Такой запуск позволяет замаскировать выполнение полезной нагрузки под легитимные компоненты Windows Script Host и обойти часть механизмов контроля приложений.	• Execution (TA0002) • Defense Evasion (TA0005) • System Script Proxy Execution (T1216) • PubPrn (T1216.001)

Microsoft Windows Sysmon

- Microsoft Windows Sysmon: настройка источника
- Microsoft Windows Sysmon: правила корреляции

Microsoft Windows Sysmon: настройка источника

Данное руководство описывает процесс отправки событий из журнала Windows Sysmon в R-Vision SIEM с помощью агента платформы R-Vision EVO.

Настройка ОС Windows

Настройка сбора событий журнала Windows Sysmon с помощью агента R-Vision EVO включает в себя:

- установку службы Sysmon;
- установку агента R-Vision EVO на конечную точку.

Установка службы Sysmon

Для мониторинга событий с помощью сервиса Sysmon вам необходимо распространить сервис Sysmon на все машины, с которых вы планируете собирать данные. Для этого:

1. Загрузите архив с сервисом Sysmon. Последняя версия сервиса доступна на официальном сайте Microsoft.
2. Загрузите политику мониторинга. Политику мониторинга можно найти по ссылке.
3. Сконфигурируйте пути Sysmon в вашей операционной системе. Планируемая к использованию учетная запись должна иметь доступ к исполняемому файлу `Sysmon.exe` и к политике мониторинга.
4. Разместите файлы на вашем файловом сервере по планируемому пути.
5. Измените пути в следующем Powershell-скрипте. Назовите его sysmon.ps1.

```
$sysmon = C:\Windows\Sysmon64.exe -s | select-string "System Monitor v"
```

```
# Путь к ранее скачанному и распакованному приложению Sysmon, расположенному на
файловом сервере:
$sysmonsource = '\\<FS-name>\Sysmon\Sysmon64.exe'

# Путь к вашему файлу с политикой мониторинга, расположенному на файловом сервере:
$sysmonconfig = '\\<FS-name>\Sysmon\monitoring.xml'

# Строка, указывающая версию вашего ПО (опционально):
$sysmonstring = 'System Monitor <Версия Sysmon> - System activity monitor'

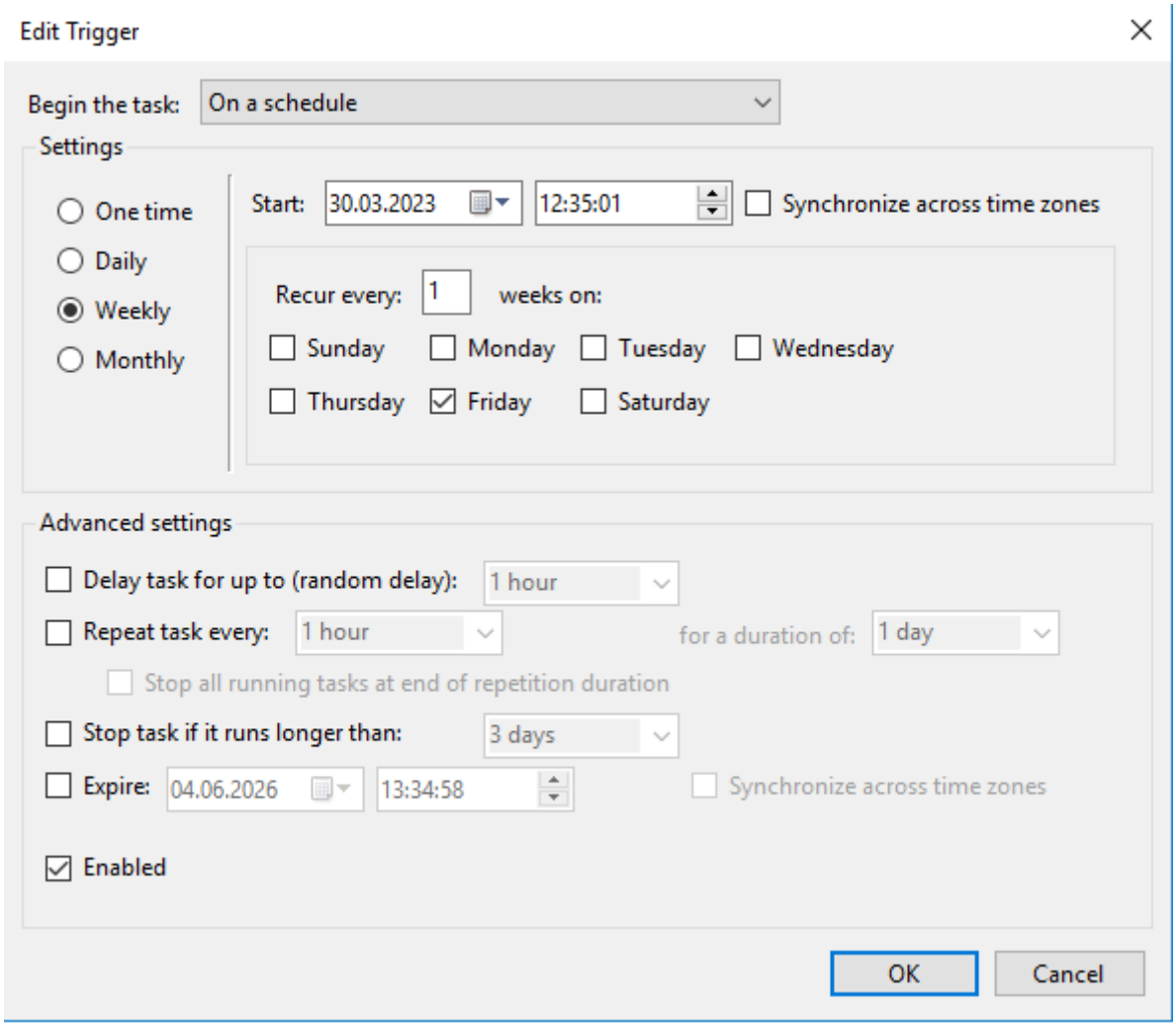
# Путь на вашей машине, по которому вы планируете устанавливать сервис Sysmon:
$filePath = 'C:\Sysmon\Sysmon64.exe'

IF (Test-Path $filePath) {
    IF ($sysmon.ToString() -eq $sysmonstring) {
        & $sysmonsource -c $sysmonconfig
    } ELSE {
        # Uninstall sysmon and re-install new version
        & $filePath -u
    Remove-Item –path $filePath
        & $sysmonsource -i $sysmonconfig -acceptEula
    }
} ELSE {
    & $sysmonsource -i $sysmonconfig -acceptEula
}
```

Здесь `<FS-name>` — DNS или IP-адрес вашего файлового сервера.

6. В зависимости от используемого типа авторизации и размещения машины в вашей сети, создайте дополнительную групповую или локальную политику. Создайте задачу по расписанию. Для этого:
   a. Настройте триггер:
      i. Выберите из выпадающего списка **Begin the task** опцию **On a schedule**.
      ii. Задайте расписание для выполнения задачи.

      Пример расписания:



iii. Нажмите на кнопку **OK**.

b. Настройте действие:

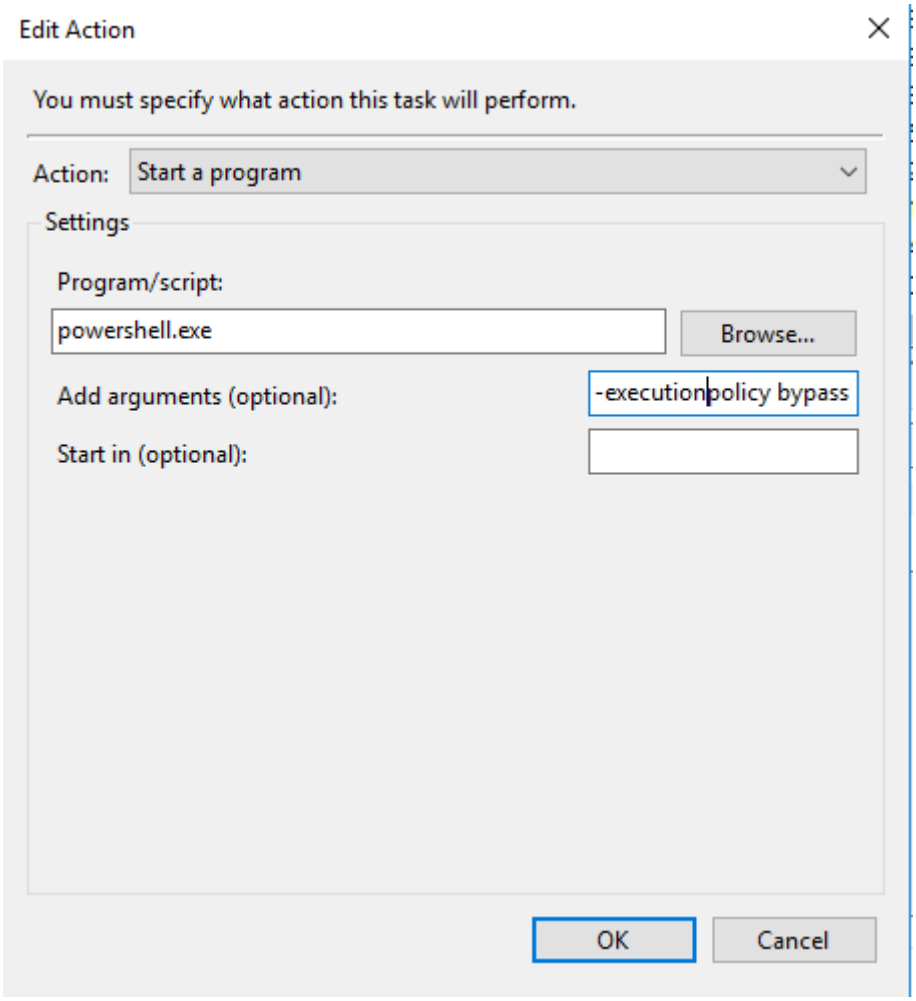
i. Выберите из выпадающего списка **Action** опцию **Start a program**.

ii. В поле **Program/script** введите команду для запуска `powershell.exe`.

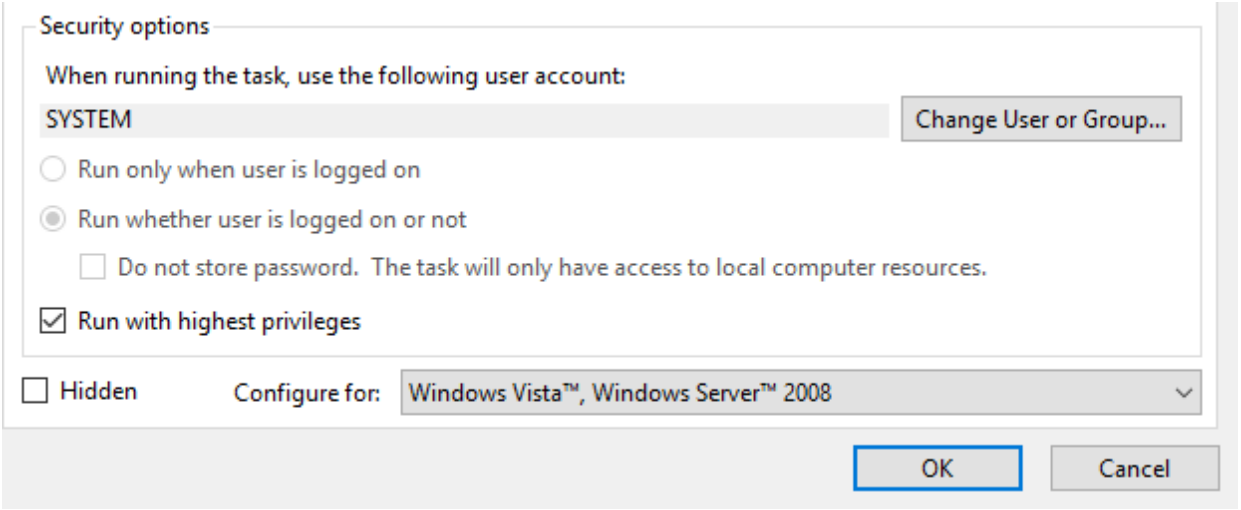
iii. В поле **Add arguments (optional)** введите значение `-executionpolicy bypass -file \\<FS-name>\Sysmon\sysmon.ps1`.

Здесь `<FS-name>` — DNS или IP-адрес вашего файлового сервера.

iv. Нажмите на кнопку **OK**.



c. В форме **Security options** установите флажок **Run with highest privileges**.



7. Сохраните изменения.

Для первичной синхронизации политик используйте принудительную синхронизацию с помощью команды `gpupdate /force`.

Установка агента

Для установки агента обратитесь к документации продукта R-Vision SIEM.

Установите агент R-Vision EVO на станцию и настройте его связь с R-Vision SIEM. После этого в веб-интерфейсе R-Vision SIEM в разделе **Агенты** появится информация о подключенном хосте.

Настройка в R-Vision SIEM

Настройка отправки событий в R-Vision SIEM

1. В веб-интерфейсе R-Vision SIEM перейдите в раздел **Агенты** → **Группы агентов**.
2. Создайте группу и добавьте в нее узел, на котором установлен агент.
3. В созданной группе узлов в секции **Чтение файлов** нажмите на кнопку **Добавить настройку** (＋).
4. В выпадающем списке **Тип журнала** выберите вариант **eventchannel**.
5. В поле **Имя журнала** введите значение `Microsoft-Windows-Sysmon/Operational`.
6. Если необходимо выбирать события по определенным критериям, введите в поле **Фильтр (формат XPATH)** выражение XPath. Если фильтр не нужен, введите символ `*`.
7. Нажмите на кнопку **Сохранить**.
8. Дождитесь применения политики группы на узле. Сбор событий настроен.

Добавление узла в группу

Для добавления узла в созданную группу:

1. В веб-интерфейсе R-Vision SIEM перейдите в раздел **Агенты**.
2. Выберите нужный узел и нажмите на кнопку на панели инструментов.
3. Выберите ранее созданную группу и нажмите на кнопку **Добавить**.
4. Дождитесь применения политики на агенте.

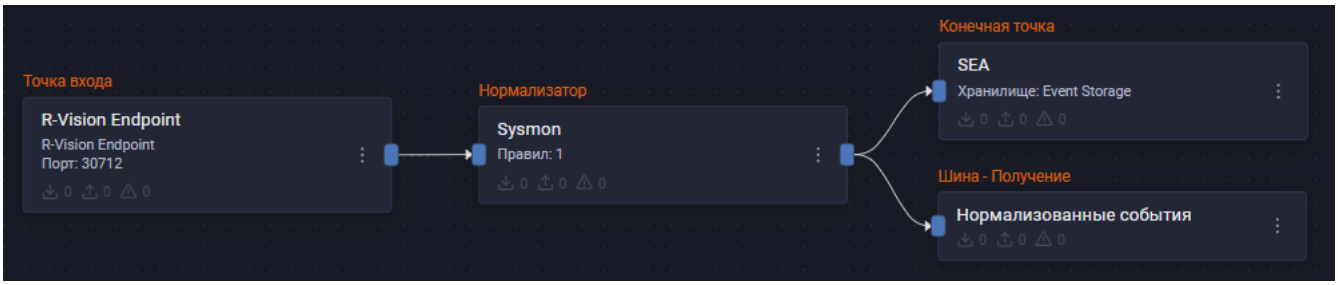
Настройка обработки событий в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **R-Vision Endpoint**.
   - Домен: введите значение в формате `gw-<your_gateway_id>`, где `<your_gateway_id>` — ID шлюза.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Microsoft Windows Sysmon** (идентификатор правила: **RV-N-211**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Добавьте на конвейер элемент **Шина**, настроенный на получение. Он передает нормализованные события для дальнейшей работы с ними.
7. Соедините конечную точку и шину с нормализатором.

8. Сохраните и установите конфигурацию конвейера.

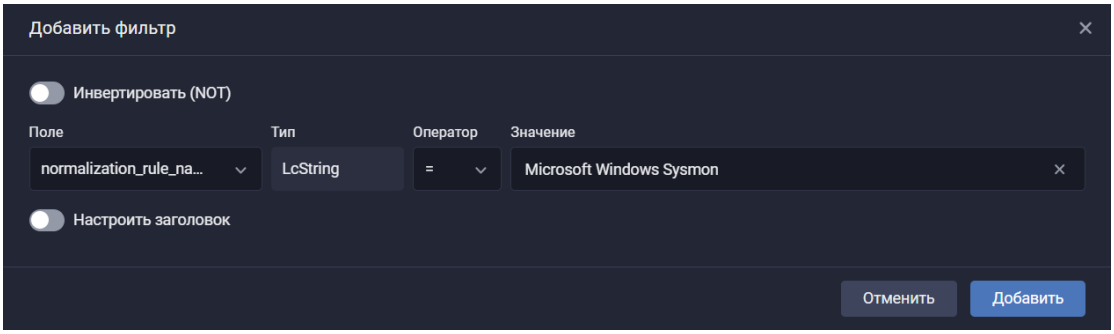
Пример конфигурации конвейера:



После настройки политики сбора и передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события хоста из журнала Windows Sysmon.

Найти события Windows Sysmon в хранилище можно по следующему фильтру:

```
normalization_rule_name = "Microsoft Windows Sysmon"
```



Microsoft Windows Sysmon: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-AL-4	Обогащение активного списка "legitimate_guids_svchost_processes_cimv2"	Правило собирает данные о легитимных процессах svchost, связанных со службой Schedule, и наполняет этими значениями активный список `legitimate_guids_svchost_processes_cimv2`.	-

ID правила	Название правила	Описание	Тактики и техники
RV-D-812	Процесс загрузил модуль по UNC-пути	Атакующие могут загружать вредоносные библиотеки напрямую с удаленных ресурсов, используя легитимные системные утилиты, такие как rundll32.exe или regsvr32.exe. Это позволяет обойти загрузку вредоносного содержимого на диск и использовать доверенные исполняемые файлы Windows как прокси для выполнения кода. Такой подход позволяет избежать срабатывания многих защитных механизмов, основанных на анализе дисковой активности или проверке цифровой подписи исполняемых файлов. При загрузке библиотеки по UNC-пути (`\\server\share\malicious.dll`) процесс обращения к удаленному ресурсу может быть зафиксирован с помощью событий загрузки модулей. При срабатывании следует проверить загруженную библиотеку и инициирующий процесс. При наличии признаков компрометации — изолировать хост и начать расследование.	• Execution (TA0002) • Shared Modules (T1129)
RV-D-813	Исходящее сетевое соединение PowerShell	Обнаружение сетевого соединения, инициированного процессом PowerShell. Часто вредоносные сценарии PowerShell загружают дополнительную полезную нагрузку или связываются с каналами управления через необычные порты или IP-адреса.	• Execution (TA0002) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-814	Использование PowerShell через сторонние инструменты	Для выполнения команд PowerShell можно использовать только библиотеки, отвечающие за его функционал, при этом не будет запущен основной процесс powershell.exe. Данный метод позволит атакующим обойти ограничения на запуск процесса PowerShell, а также скрыть события выполнения команд. Также возможен запуск команд PowerShell через стороннюю библиотеку, в таком случае ее нужно сначала запустить, например с помощью библиотеки rundll32.dll или других утилит, таких как InstallUtil.exe, regsvcs.exe, regasm.exe, regsvr32. Если в срабатывании участвует один из данных инструментов, следует проверить, какие были выполнены команды в системе с участием конкретной утилиты в дельту времени срабатывания. Для детектирования используются события загрузки библиотек, относящихся к использованию командного интерпретатора. При срабатывании правила следует определить, что за процесс использует библиотеку PowerShell. Если он не является легитимным, необходимо временно изолировать хост и провести внутреннее расследование.	• Execution (TA0002) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-815	Использование библиотеки cygwin1.dll	Использование библиотеки cygwin1.dll, которая обеспечивает UNIX-подобную среду и оболочку командной строки в Windows, может быть как легитимным, так и свидетельствовать о попытках атакующих использовать UNIX-инструменты для обхода защитных механизмов и выполнения команд. Данное правило выявляет запуск процессов с загрузкой библиотеки cygwin1.dll. При срабатывании рекомендуется проверить контекст запуска процесса, определить легитимность приложения и происхождение библиотеки, проанализировать цепочку запуска и права пользователя. При подтверждении подозрительной активности необходимо начать расследование инцидента, при необходимости временно изолировать пострадавший хост и заблокировать учетную запись, под которой выявлена активность.	• Execution (TA0002) • Command and Scripting Interpreter (T1059) • Unix Shell (T1059.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-816	Зафиксирована загрузка модуля WMI подозрительным процессом	Это правило обнаруживает, когда подозрительный процесс загружает модуль WMI (Windows Management Instrumentation). WMI — это функция администрирования, которая позволяет получать доступ к компонентам системы Windows. WMI может быть использован атакующими для выполнения вредоносных команд и полезной нагрузки, а также для сбора информации о системе и перемещения по сети. Загрузка модуля WMI подозрительным процессом позволит ему выполнять функции WMI от своего имени. Если WMI-библиотека загружается процессом, не относящимся к системному ПО или известным агентам администрирования, это может указывать на попытку скрытного использования WMI. При срабатывании правила следует определить, что за процесс загрузил модуль, проверить, выполнялись ли через него команды, и опросить пользователя-инициатора. При отсутствии подтверждения — временно заблокировать учетную запись и инициировать расследование.	• Execution (TA0002) • Windows Management Instrumentation (T1047)

ID правила	Название правила	Описание	Тактики и техники
RV-D-817	Манипулирование запланированными задачами через реестр	Планировщик задач (Task Scheduler) — это служба в Windows, которая позволяет автоматизированно выполнять запланированные задачи на устройстве по заранее заданному триггеру (время, наступление определенного события и другие). Данная служба привлекает внимание атакующих, так как планировщик задач не будет отключен администраторами в связи с тем, что на нем строится работа всей системы. Данное правило направлено на детектирование подозрительных действий с запланированными задачами непосредственно через реестр. Оно может детектировать, например, манипуляции через службу Remote Registry. Реализовано данное правило за счет исключения легитимной работы планировщика задач (служба Schedule). Также логикой правила затрагивается сокрытие запланированной задачи из планировщика задач (ключи SD и Index в интересующих ветках). В случае срабатывания правила требуется изучить содержимое задачи, а также определить инициатора добавления задачи. Необходимо опросить инициатора активности на предмет легитимности действий. Если легитимность подтвердить не удалось, следует заблокировать учетную запись инициатора активности и удалить задачу из планировщика задач.	• Execution (TA0002) • Persistence (TA0003) • Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Scheduled Task/Job (T1053) • Scheduled Task (T1053.005) • Modify Registry (T1112)

ID правила	Название правила	Описание	Тактики и техники
RV-D-818	Загрузка несуществующей dll для сервисов IKE, IKEEXT, SessionEnv	Данное правило обнаруживает попытки загрузки устаревших или несуществующих DLL-библиотек (wlbsctrl.dll, tsmsisrv.dll, tsvipsrv.dll) системным процессом svchost.exe. Эти библиотеки ранее использовались службами IKE, IKEEXT и SessionEnv, которые отсутствуют в современных версиях Windows. Подобная активность может свидетельствовать о попытке выполнения произвольного кода атакующих через механизм подмены DLL (DLL Side-Loading). Использование данной техники часто связано с целями обхода механизмов защиты, сохранения доступа в системе или повышения привилегий. В случае срабатывания рекомендуется проверить источник и целевую DLL, а также выявить возможные следы вмешательства или сохраненного доступа. Если активность не является легитимной, рекомендуется при необходимости изолировать хост для предотвращения дальнейшего развития атаки.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Hijack Execution Flow (T1574) • DLL (T1574.001) • DLL Side-Loading (T1574.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-819	Загрузка модуля в процесс cmstp из нестандартного пути	Атакующие могут использовать системную утилиту cmstp.exe (Connection Manager Profile Installer) для загрузки и выполнения вредоносных библиотек DLL, маскируясь под легитимную активность системы. Утилита предназначена для установки профилей подключения и использует inf-файлы, которые могут содержать секции RegisterOCXSection и UnRegisterOCXSection — именно через них атакующие могут указать путь к вредоносной DLL. При нормальной работе системы cmstp.exe загружает модули из стандартных системных директорий (System32, Program Files и другие). Это правило выявляет попытки загрузки модулей в процессе cmstp.exe из подозрительных пользовательских путей. При срабатывании необходимо запросить объяснение у пользователя или администратора, проверить путь к DLL, а также инициирующий inf-файл. В случае подтверждения инцидента необходимо изолировать хост, сменить пароль от учетной записи пользователя, от имени которой выполнялись действия, начать расследование.	• Execution (TA0002) • Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Shared Modules (T1129) • System Binary Proxy Execution (T1218) • CMSTP (T1218.003) • Hijack Execution Flow (T1574) • DLL (T1574.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-820	Неподписанная DLL загружена утилитой Windows	Атакующие часто используют доверенные утилиты Windows для выполнения произвольного кода, поскольку такие процессы могут быть исключены из контроля средствами защиты информации. Данное правило отслеживает случаи загрузки неподписанных или неподтвержденных DLL-библиотек такими системными утилитами, как rundll32.exe, regsvr32.exe, installutil.exe, regasm.exe и другими. Такая активность может свидетельствовать о попытке обхода механизмов защиты и выполнения вредоносного кода в доверенном контексте. При срабатывании правила рекомендуется проверить источник DLL, наличие цифровой подписи, определить, был ли запуск инициирован пользователем или сторонним ПО. При отсутствии подтверждения — изолировать хост, сменить пароль пользователя и инициировать расследование.	• Defense Evasion (TA0005) • System Binary Proxy Execution (T1218) • Regsvcs/Regasm (T1218.009) • Regsvr32 (T1218.010) • Rundll32 (T1218.011)

ID правила	Название правила	Описание	Тактики и техники
RV-D-821	Изменение ветки реестра Provisioning_Commands	Внесение изменений в ветку реестра \SOFTWARE\Microsoft\Provisioning\Commands\ может использоваться атакующими для маскировки запуска вредоносного программного обеспечения. Изменения в данной ветке позволяют конфигурировать запуск исполняемых файлов через легитимный системный инструмент provlaunch.exe, предназначенный для выполнения вспомогательных действий при установке, обновлении или настройке ОС. Подобный подход позволяет обойти защитные механизмы и затруднить обнаружение. При выявлении подобной активности следует проверить, кто инициировал изменение, проанализировать путь и содержимое исполняемого файла, а при наличии признаков компрометации — изолировать хост и провести дальнейшее расследование.	• Defense Evasion (TA0005) • Modify Registry (T1112) • System Binary Proxy Execution (T1218)

ID правила	Название правила	Описание	Тактики и техники
RV-D-822	Загрузка модуля в процесс mmc из нестандартного пути	В попытке избежать обнаружения атакующий может выполнять команды/запускать исполняемые файлы через "посредника" в виде системных программ. Системные исполняемые файлы зачастую подписаны, могут быть занесены в списки исключений средств защиты информации. Одной из таких программ является mmc.exe, позволяющая загрузить оснастку на локальную или удаленную машину. Атакующий может создать свою оснастку в которой будет ссылаться на какой-либо COM-объект (через CLSID), и при загрузке этой оснастки будет выполнен его "код" (например, загружена dll из значения реестра `InProcServer32` для этого CLSID). Правило выявляет случаи, когда mmc.exe загружает модули из нестандартных директорий, не характерных для легитимного использования. При срабатывании правила рекомендуется уточнить характер активности, проверить легитимность загружаемого модуля, инициировавшего процесс, а также провести дополнительный анализ поведения узла.	• Execution (TA0002) • Defense Evasion (TA0005) • Shared Modules (T1129) • System Binary Proxy Execution (T1218) • MMC (T1218.014)

ID правила	Название правила	Описание	Тактики и техники
RV-D-823	Загрузка процессом mshta модулей для выполнения скриптов	Данное правило предназначено для выявления случаев загрузки в процесс mshta.exe библиотек, связанных с выполнением скриптов (vbscript.dll, jscript.dll, jscript9.dll). Такой сценарий может свидетельствовать об использовании утилиты mshta в качестве "посредника" для выполнения вредоносных HTA-файлов, содержащих встроенные скрипты. Подобная техника применяется атакующими с целью обхода защитных механизмов, так как mshta является легитимным и подписанным системным исполняемым файлом. Рекомендуется проверить командную строку процесса mshta.exe, а также сетевую активность и родительские процессы. При подтверждении подозрительной активности следует выгрузить и проанализировать HTA-файл (если доступен), исследовать процесс mshta.exe, провести проверку на наличие аналогичных артефактов в системе и инфраструктуре.	• Execution (TA0002) • Defense Evasion (TA0005) • Shared Modules (T1129) • System Binary Proxy Execution (T1218) • Mshta (T1218.005)

ID правила	Название правила	Описание	Тактики и техники
RV-D-824	Сетевое подключение из подозрительной директории	Данное правило направлено на обнаружение сетевого подключения из подозрительных мест в файловой системе. Активность может быть вызвана вредоносным программным обеспечением, которое устанавливает связь с удаленным сервером для передачи или получения вредоносных данных. Обнаружение такой сетевой активности из подозрительных директорий может быть признаком компрометации системы. Рекомендуется проверить путь запуска процесса, инициировавшего подключение, и убедиться в легитимности исполняемого файла, уточнить действия у пользователя. При наличии признаков вредоносной активности следует изолировать хост и начать расследование.	• Command and Control (TA0011) • Ingress Tool Transfer (T1105)

ID правила	Название правила	Описание	Тактики и техники
RV-D-825	Сетевое подключение, инициированное процессом Winlogon	Процесс winlogon.exe отвечает за аутентификацию пользователей и управление сеансами входа в систему, обеспечивая инициализацию пользовательского окружения и запуск необходимых системных процессов после успешного входа. Обычно winlogon.exe не устанавливает сетевые соединения с внешними IP-адресами, так как его основная функция — управление локальным входом в систему. Такое поведение может свидетельствовать об аномальной активности. Рекомендуется уточнить цель установления соединения, определить легитимность назначения, проверить наличие подозрительных модулей, загруженных в память процесса, и при необходимости инициировать процедуру изоляции хоста и расследования.	• Defense Evasion (TA0005) • System Binary Proxy Execution (T1218) • Rundll32 (T1218.011)

ID правила	Название правила	Описание	Тактики и техники
RV-D-826	Загрузка модуля в процесс odbcconf из нестандартного пути	В попытке избежать обнаружения атакующий может выполнять команды/запускать исполняемые файлы через "посредника" в виде системных программ. Системные исполняемые файлы зачастую подписаны, могут быть занесены в списки исключений средств защиты информации. Одной из таких программ является odbcconf, предназначенная для настройки ODBC-драйверов. При регистрации dll драйвера odbcconf выполнит ее функцию `DllRegisterServer`. Детектирование опирается на предположение, что в системах, где не развернуто ПО для работы с базами данных, odbcconf не используется, а в системах, где оно развернуто, используется редко. Ввиду этого правило обнаруживает загрузку в память процесса библиотек не из системных директорий. При срабатывании правила рекомендуется проверить целевую DLL, инициирующий процесс и причины запуска утилиты. Необходимо подтвердить легитимность действия и, при наличии признаков компрометации, провести расследование и применить меры по изоляции узла.	• Execution (TA0002) • Defense Evasion (TA0005) • Shared Modules (T1129) • System Binary Proxy Execution (T1218) • Odbcconf (T1218.008)

ID правила	Название правила	Описание	Тактики и техники
RV-D-827	Загрузка модуля в процесс regsvr32 из нестандартного пути	В попытке избежать обнаружения атакующий может выполнять команды/запускать исполняемые файлы через "посредника" в виде системных программ. Использование системной утилиты regsvr32, подписанной и часто исключаемой из контроля средств защиты, может применяться для обхода защитных механизмов. При регистрации DLL через regsvr32 возможно выполнение кода из функции DllMain загружаемой библиотеки, что представляет риск исполнения вредоносного кода. Рекомендуется обратить внимание на процессы regsvr32.exe с модулем, загруженным из путей, отличных от стандартных системных директорий. При подтверждении подозрительной активности следует изолировать хост для предотвращения дальнейшего распространения, провести детальный анализ загруженного модуля и процесса, а также проверить наличие похожих инцидентов в системе и инфраструктуре.	• Execution (TA0002) • Defense Evasion (TA0005) • Shared Modules (T1129) • System Binary Proxy Execution (T1218) • Regsvr32 (T1218.010)

ID правила	Название правила	Описание	Тактики и техники
RV-D-828	Выполнение скриптов через regsvr32	В попытке избежать обнаружения команды могут выполняться через "посредника" — системные программы, подписанные Microsoft и нередко включенные в исключения средств защиты. Во время регистрации DLL и элементов OLE в реестре Windows через regsvr32 может выполняться код из регистрируемого объекта. Детектирование основано на факте загрузки специфических библиотек в процесс regsvr32, не характерных для его обычной работы. При срабатывании правила рекомендуется проверять все случаи загрузки таких библиотек, особенно вне сценариев обновления или установки легитимного ПО. При подтверждении нежелательной активности следует изолировать хост от сети, проанализировать задействованные библиотеки и цепочки процессов, а также проверить инфраструктуру на аналогичные случаи.	• Execution (TA0002) • Defense Evasion (TA0005) • Shared Modules (T1129) • System Binary Proxy Execution (T1218) • Regsvr32 (T1218.010)

ID правила	Название правила	Описание	Тактики и техники
RV-D-829	Загрузка модуля в процесс rundll32 из нестандартного пути	Атакующие часто используют легитимные системные исполняемые файлы (Living off the Land Binaries, LOLBins) для обхода защитных решений. Один из таких файлов — rundll32.exe, который позволяет загружать и выполнять DLL-библиотеки. В рамках легитимного поведения rundll32.exe загружает модули из системных директорий Windows. Однако загрузка библиотек из нестандартных путей (например, временных директорий, пользовательских папок или сторонних каталогов) может свидетельствовать о попытке обхода механизмов защиты, включая обход контроля приложений, антивирусов или EDR. При срабатывании правила рекомендуется проверить путь загружаемой DLL, проанализировать ее цифровую подпись и происхождение, исследовать цепочку запуска rundll32.exe и родительские процессы, а также проверить права учетной записи, инициировавшей запуск. При подтверждении подозрительной активности следует начать расследование и временно изолировать хост.	• Execution (TA0002) • Defense Evasion (TA0005) • Shared Modules (T1129) • System Binary Proxy Execution (T1218) • Rundll32 (T1218.011)

ID правила	Название правила	Описание	Тактики и техники
RV-D-830	Загрузка процессом rundll32 модулей для выполнения скриптов	В попытке избежать обнаружения атакующий может выполнять команды или запускать исполняемые файлы через "посредника" — легитимные системные программы, которые часто подписаны и считаются доверенными. Одной из таких программ является rundll32.exe. В ней есть возможность использовать для выполнения команд языки JavaScript или VBScript через указание в аргументе rundll32 схем `javascript:` или `vbscript:` соответственно. После схемы атакующим указывается метод `RunHTMLApplication` из файла `mshtml.dll` и далее соответствующий код. Данное правило выявляет случаи загрузки этих скриптовых движков процессом rundll32.exe. При срабатывании рекомендуется проверить контекст запуска процесса, убедиться в легитимности используемых скриптов и происхождения командной строки. При подтверждении подозрительной активности необходимо начать расследование инцидента и при необходимости временно изолировать пострадавший хост.	• Execution (TA0002) • Defense Evasion (TA0005) • Shared Modules (T1129) • System Binary Proxy Execution (T1218) • Rundll32 (T1218.011)

ID правила	Название правила	Описание	Тактики и техники
RV-D-831	Запросы к API Telegram подозрительным процессом	В рамках своей работы ВПО может взаимодействовать с ботами Telegram, которые могут использоваться в качестве сервера управления (далее C2). К примеру, бэкдор RingSpy отправляет файлы на управляющий сервер с использованием сетевого ресурса токен бота/sendDocument, а текст — токен бота/sendMessage. Таким образом, выявление подобных обращений может свидетельствовать о возможном взаимодействии с C2 через Telegram. В случае возникновения активности рекомендуется опросить пользователя, ответственного за учетную запись, которая инициировала активность. Если легитимность запроса подтвердить не удалось, то следует заблокировать учетную запись.	• Command and Control (TA0011) • Exfiltration (TA0010) • Web Service (T1102) • Bidirectional Communication (T1102.002) • Exfiltration Over Web Service (T1567)

ID правила	Название правила	Описание	Тактики и техники
RV-D-832	Подозрительные DNS-запросы к localtoNet домену	Данное правило обнаруживает подозрительные DNS-запросы к доменам, связанным с туннелированием трафика через утилиту `localtoNet`. Применение этой утилиты может свидетельствовать о попытках атакующих закрепиться в инфраструктуре или скрыть свою активность через использование промежуточного узла для ретрансляции трафика. Это может быть частью более широких атак, направленных на скрытое перемещение внутри сети и обход ограничений безопасности. В случае срабатывания правила рекомендуется уточнить у пользователя причину использования утилиты. Если активность не является легитимной, следует начать расследование и изолировать хост.	• Command and Control (TA0011) • Protocol Tunneling (T1572)

ID правила	Название правила	Описание	Тактики и техники
RV-D-833	Загрузка amsi.dll необычным процессом	Детектирование загрузки amsi.dll необычным процессом. AMSI.dll — это библиотека динамической загрузки (DLL), связанная с Antimalware Scan Interface (AMSI). AMSI предоставляет интерфейс для интеграции антивирусных продуктов и других средств обнаружения вредоносного программного обеспечения с приложениями и скриптами, выполняемыми на компьютере. Атакующие, стремясь обойти встроенные средства защиты, могут загружать amsi.dll нестандартными или специально подготовленными процессами. Это позволяет им вмешиваться в работу AMSI или полностью обходить его, тем самым скрывая выполнение вредоносного кода от антивирусных решений. В рамках детектирования отслеживается загрузка библиотеки amsi.dll процессами, не связанными с системой или известным легитимным ПО. При срабатывании правила необходимо определить, какой процесс загрузил библиотеку, и проверить, не использовались ли при этом техники обхода AMSI. В случае подозрительной активности рекомендуется временно заблокировать УЗ или хост и провести расследование на предмет попыток обхода защитных механизмов.	• Defense Evasion (TA0005) • Impact (TA0040) • Inhibit System Recovery (T1490)

ID правила	Название правила	Описание	Тактики и техники
RV-D-834	Маскировка запуска PowerShell	PowerShell — это мощный интерактивный интерфейс командной строки и среда написания сценариев в Windows. Атакующие могут использовать PowerShell для выполнения ряда действий, включая сбор информации, загрузку вредоносного кода и выполнение команд. В рамках техники маскировки (masquerading) PowerShell может быть переименован, перемещен в другую директорию или запускаться через сторонние оболочки, чтобы скрыть свое истинное происхождение. Такое поведение часто используется для обхода защитных решений, которые ориентируются на известные пути запуска. Обнаружение запуска PowerShell вне стандартного каталога `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe` может свидетельствовать о попытке маскировки. Рекомендуется проверить путь к исполняемому файлу, инициирующий процесс, аргументы запуска, а также загрузку подозрительных модулей или сетевую активность. При наличии признаков компрометации — изолировать хост и начать расследование.	• Execution (TA0002) • Defense Evasion (TA0005) • Masquerading (T1036) • Match Legitimate Resource Name or Location (T1036.005) • Space after Filename (T1036.006) • Double File Extension (T1036.007) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-835	Создание запланированной задачи через FileCreation	Запланированные задачи — это один из встроенных механизмов Windows, позволяющий выполнять действия по расписанию или при наступлении определенных условий. Атакующие могут использовать планировщик задач для закрепления в системе (persistence) или выполнения вредоносного кода с повышенными привилегиями. В нормальных условиях задачи создаются с использованием интерфейсов ОС, таких, как `schtasks.exe` или COM API, и сохраняются в стандартной директории `C:\Windows\System32\Tasks`. Однако при прямом создании или модификации этих файлов вручную, без использования штатных инструментов, может фиксироваться событие `FileCreate`. Такое поведение может свидетельствовать о попытке обхода защитных механизмов или использования нестандартного способа создания задачи. Рекомендуется проверить, какой процесс инициировал создание файла, а также проанализировать его содержимое и запуск. Убедитесь, что действия не связаны с легитимным ПО или системной активностью. При наличии признаков вредоносного поведения изолируйте хост и начните расследование.	• Execution (TA0002) • Persistence (TA0003) • Privilege Escalation (TA0004) • Scheduled Task/Job (T1053) • Scheduled Task (T1053.005)

ID правила	Название правила	Описание	Тактики и техники
RV-D-836	Эксплуатация уязвимости в WinRAR - CVE-2023-38831	CVE-2023-38831 — это критическая уязвимость в программе сжатия WinRAR, которая позволяет атакующим выполнить произвольный код на компьютере пользователя. Уязвимость заключается в запуске файла с произвольными командами при открытии легитимного файла из архива, в результате чего может быть произведено выполнение полезной нагрузки. Данное правило детектирует подобную эксплуатацию. При срабатывании правила следует проанализировать события на целевом хосте. Если выявленная активность окажется подозрительной, необходимо инициировать внутреннее расследование и временно заблокировать учетную запись инициатора до завершения проверки.	• Execution (TA0002) • Exploitation for Client Execution (T1203)

ID правила	Название правила	Описание	Тактики и техники
RV-D-837	Изменение ключа реестра Debugger отладчика AeDebug	Правило нацелено на обнаружение изменения значения ключа реестра Debugger в ветке AeDebug, которое может быть использовано атакующими для закрепления в системе. Данный ключ позволяет определить, какое приложение будет запускаться при сбое процесса. Заменив путь к легитимному отладчику на вредоносное приложение или DLL, атакующий может добиться выполнения своего кода с повышенными правами при сбое системных процессов. Изменение данного параметра нередко используется в рамках обеспечения механизмов постоянства, особенно после первоначального проникновения. При срабатывании правила необходимо определить, какой процесс произвел изменение, от имени какого пользователя, а также оценить легитимность действия. В случае подозрительной активности следует провести дальнейшее расследование и, при необходимости, восстановить оригинальные значения ключа.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Boot or Logon Autostart Execution (T1547)

ID правила	Название правила	Описание	Тактики и техники
RV-D-838	Смена ассоциации запуска файла	Атакующие могут закрепиться в системе, запустив вредоносное содержимое, инициируемое ассоциацией типов файлов. При открытии файла проверяется программа по умолчанию, используемая для открытия файла, также называемая ассоциацией файлов. Выбранные ассоциации файлов хранятся в реестре Windows и могут редактироваться пользователями, администраторами с помощью встроенной утилиты assoc или программами, имеющими доступ к реестру. Правило нацелено на мониторинг смены ассоциации через реестр. При этом исключается вариант смены при помощи утилиты OpenWith. При срабатывании правила необходимо установить, какой процесс внес изменения, от имени какого пользователя, и была ли операция ожидаемой. Если обнаружена подозрительная активность, рекомендуется восстановить исходные ассоциации и провести дополнительный анализ системы на предмет других признаков компрометации.	• Persistence (TA0003) • Event Triggered Execution (T1546) • Change Default File Association (T1546.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-839	Добавление в AppCert DLL полезной нагрузки	Атакующие могут закрепиться в системе и/или повысить привилегии, запустив вредоносный контент, запускаемый библиотеками DLL AppCedevice_time, загруженными в процессы. Библиотеки динамических ссылок (DLL), указанные в разделе AppCertDLLs в разделе `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\` загружаются в каждый процесс, который вызывает используемые функции интерфейса прикладного программирования (API) CreateProcess, CreateProcessAsUser, CreateProcessWithLoginW, CreateProcessWithTokenW или WinExec. Атакующие могут воспользоваться этим, чтобы заставить систему загружать и выполнять вредоносную DLL в контексте доверенных процессов. Правило направлено на выявление добавления DLL-файлов в реестр через AppCertDLLs. При срабатывании необходимо установить, какая DLL была добавлена, какой процесс выступил инициатором, а также проанализировать сопутствующие действия (изменения файлов, сетевую активность, задания планировщика). При подтвержденных признаках компрометации следует изолировать хост и провести расследование.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Event Triggered Execution (T1546) • AppCert DLLs (T1546.009)

ID правила	Название правила	Описание	Тактики и техники
RV-D-840	Добавление в Appinit DLL полезной нагрузки	Атакующие могут закрепиться в системе и/или повысить привилегии, выполняя вредоносный код, запускаемый библиотеками DLL AppInit, загруженными в процессы. Dynamic Link Libraries (DLLs), указанные в значении AppInit_DLLs в разделах реестра `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows` или `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows`, загружаются в каждый процесс, использующий user32.dll. Почти все пользовательские процессы в Windows обращаются к user32.dll, поэтому загрузка AppInit_DLLs происходит часто. Правило нацелено на выявление добавления полезной нагрузки в виде dll-файла через реестр в Appinit DLL. При срабатывании правила рекомендуется определить, какой процесс инициировал изменение, проверить наличие других признаков вредоносной активности (загрузка исполняемых файлов, сетевые подключения) и при необходимости изолировать хост для дальнейшего анализа.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Event Triggered Execution (T1546) • AppInit DLLs (T1546.010)

ID правила	Название правила	Описание	Тактики и техники
RV-D-841	Подмена системных файлов специальных возможностей	Атакующие могут закрепиться в системе и/или повышать привилегии, выполняя вредоносный код, запускаемый с помощью функций специальных возможностей Windows. Например, заменяя исполняемые файлы, отвечающие за "залипание клавиш" (sethc.exe) или "центр управления" (utilman.exe), на командную строку (cmd.exe) или другую программу, обеспечивающую работоспособность на экране авторизации и не требующую авторизации. Правило нацелено на выявление попыток подмены исполняемых файлов или связанных с ними ключей реестра. При срабатывании правила рекомендуется проверить содержимое затронутых файлов и ключей реестра, определить, кто инициировал изменение, и выявить сопутствующую подозрительную активность — создание или перемещение исполняемых файлов, сетевые подключения, новые задачи в планировщике и другие признаки дальнейшей вредоносной активности. При наличии признаков компрометации стоит изолировать хост и начать расследование.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Event Triggered Execution (T1546) • Accessibility Features (T1546.008) • Hijack Execution Flow (T1574) • Executable Installer File Permissions Weakness (T1574.005)

ID правила	Название правила	Описание	Тактики и техники
RV-D-842	Обход UAC с помощью ключа реестра DelegateExecute	С помощью изменения ключей реестра `HKCU:\open\command`, `\environment\windi` и `\environment\systemroot` можно обойти подтверждение прав администратора для запуска вредоносного программного обеспечения. Данное правило выявляет попытку обхода контроля учетных записей пользователей (UAC) через модификацию реестра, а именно — ключа `HKCU:\Software\Classes\Folder\shell\open\command`. При создании параметра DelegateExecute со значением (Empty) в этой ветке реестра возможно выполнение вредоносного кода с повышенными привилегиями без запроса UAC. Это происходит потому, что Windows использует механизм автоматического делегирования выполнения при наличии DelegateExecute, не требуя подтверждения прав администратора. Этот метод активно используется вредоносными программами для эскалации привилегий без взаимодействия с пользователем. При срабатывании правила рекомендуется проверять процессы, инициировавшие изменение ключа, особенно если это нестандартные или неизвестные исполняемые файлы. Следует обратить внимание на активность пользователя и наличие признаков автоматического запуска вредоносного кода. При наличии признаков компрометации рекомендуется временно изолировать систему, провести антивирусное	• Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Abuse Elevation Control Mechanism (T1548) • Bypass User Account Control (T1548.002) • Hijack Execution Flow (T1574) • Executable Installer File Permissions Weakness (T1574.005)

ID правила	Название правила	Описание	Тактики и техники
RV-D-843	Отключение CrashDump через изменение реестра	Данное правило выявляет изменения в параметре реестра, отвечающем за включение создания CrashDump — дампа памяти при аварийном завершении процесса. Отключение этой функции через запись в ветке реестра `SYSTEM\CurrentControlSet\Control\CrashControl` позволяет атакующим скрывать следы сбоев и аварийных остановок программ, что усложняет последующий анализ инцидентов и расследование атак. Такое поведение часто используется в целях обхода средств обнаружения и предотвращения реагирования на инциденты. При срабатывании правила необходимо проверить инициатора изменения, изучить контекст активности и определить, было ли отключение сделано легитимно. В случае подозрений рекомендуется провести расследование, восстановить параметры системы.	• Defense Evasion (TA0005) • Modify Registry (T1112)

ID правила	Название правила	Описание	Тактики и техники
RV-D-844	Создание подозрительного потока в mstsc.exe	Процесс mstsc.exe предназначен для подключения к удаленным рабочим столам с использованием протокола RDP (Remote Desktop Protocol). Данное правило обнаруживает удаленное создание потока в процессе mstsc.exe процессом, расположенным в потенциально подозрительном месте. Этот прием часто используется атакующими для перехвата некоторых API, используемых DLL, загружаемыми mstsc.exe во время аутентификации по RDP, с целью кражи учетных данных. При обнаружении необходимо изучить происхождение процесса-инициатора, проверить целостность и легитимность задействованных файлов и провести расследование на предмет возможного вмешательства или компрометации системы. Если изменения не подтверждены как легитимные, следует предпринять меры по ограничению доступа и начать расследование.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-845	Создание и удаление файла за короткий промежуток времени	Атакующие могут использовать командную строку (cmd.exe) для выполнения автоматизированных сценариев, при которых файл создается и вскоре удаляется. Это позволяет минимизировать следы в системе и затруднить анализ инцидента. Подобный подход реализован, например, в RingSpy. Данный прием может использоваться для временного сохранения полезной нагрузки, скриптов или других вспомогательных компонентов, необходимых на этапе инициализации атаки. В данном правиле рассматриваются исключительно случаи, когда действия выполняются с помощью интерпретатора командной строки, поскольку такая активность от другого легитимного ПО может быть частью штатной работы. При срабатывании следует проверить, какой файл был создан и удален, и каким образом он использовался между этими действиями. В случае подозрительной активности — инициировать изоляцию хоста и провести расследование.	• Defense Evasion (TA0005) • Indicator Removal (T1070) • File Deletion (T1070.004) • Relocate Malware (T1070.010)

ID правила	Название правила	Описание	Тактики и техники
RV-D-846	Изменение чувствительных параметров RDP	Атакующие могут изменять чувствительные параметры службы удаленного рабочего стола (RDP) через реестр для обхода настроек безопасности, скрытого подключения к сессиям пользователей (shadowing), запуска программ при установлении RDP-сессии или замены служебной библиотеки TermService, что позволяет закрепиться в системе или выполнить произвольный код. Эти действия могут быть частью сценариев persistence и defense evasion. Детектирование основано на фиксации изменений в ключевых ветках реестра, связанных с RDP. При срабатывании правила необходимо установить пользователя, от имени которого были внесены изменения в реестр, и оценить легитимность этой активности. Если действия не связаны с административными задачами или групповыми политиками, следует изолировать хост от сети, сменить пароль учетной записи, от имени которой производились изменения, и провести анализ на наличие следов компрометации.	• Persistence (TA0003) • Defense Evasion (TA0005) • Modify Registry (T1112) • Server Software Component (T1505) • Terminal Services DLL (T1505.005)

ID правила	Название правила	Описание	Тактики и техники
RV-D-847	Порт RDP по умолчанию изменен на нестандартный	Удаленный рабочий стол (RDP) — это распространенная функция в операционных системах. Она позволяет пользователю входить в удаленную систему, используя интерактивный сеанс с графическим интерфейсом пользователя. Microsoft называет свою реализацию протокола удаленного рабочего стола (RDP) службами удаленного рабочего стола (RDS). Когда атакующий изменяет порт RDP на нестандартный, это может помочь ему обойти стандартные механизмы защиты и проникнуть в систему без обнаружения. Обнаружение таких изменений важно для обеспечения безопасности, так как это может указывать на потенциальные попытки атакующих получить несанкционированный доступ к системе.	• Defense Evasion (TA0005) • Boot or Logon Autostart Execution (T1547) • Port Monitors (T1547.010)

ID правила	Название правила	Описание	Тактики и техники
RV-D-848	Изменена очередь загрузки драйвера Sysmon	Обнаружены изменения в очереди загрузки драйвера Sysmon. Если драйвер Sysmon настроен на загрузку после другого зарегистрированного сервиса, он не сможет загрузиться вместе с ним. Это может указывать на попытку атакующих изменить приоритет загрузки драйвера Sysmon, что может привести к его неправильной работе или отключению. Подобная атака может использоваться для обхода мониторинга безопасности, который осуществляется драйвером Sysmon, и скрыть свои действия на зараженной системе. При срабатывании правила рекомендуется проверить, кем и при каких условиях было изменено значение Altitude в соответствующем ключе реестра, сопоставить его с эталонной конфигурацией, восстановить корректное значение и перезапустить службу Sysmon, а также проанализировать журналы на предмет других признаков компрометации.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-849	Изменение разрешения доступа к каналу Winevt через реестр	Изменение разрешений доступа к каналу Winevt через реестр представляет собой потенциальную тактику атакующих для изменения настроек безопасности и получения несанкционированного доступа к системным событиям Windows. Атакующие могут попытаться вмешаться в ключ реестра ChannelAccess, чтобы изменить настройки доступа к каналу событий Windows, например, добавить себя в список разрешенных пользователей или групп. Обнаружение подобных вмешательств в реестр и изменений доступа к каналу событий Windows критически важно для обнаружения и предотвращения потенциальных атак, поскольку это может сигнализировать о попытке получить привилегированный доступ к системным данным и манипулировать ими. При обнаружении подобных действий следует немедленно реагировать, анализировать источник вмешательства и принимать меры по восстановлению целостности системы и усилению ее защиты.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable Windows Event Logging (T1562.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-850	Изменение фона рабочего стола через реестр	Обнаружение изменения фонового изображения рабочего стола через модификацию ключей реестра. Такая техника часто применяется вредоносными программами для демонстрации записки с требованием выкупа или другого навязчивого изображения на фоне рабочего стола пользователя. При срабатывании правила рекомендуется определить, какой процесс инициировал изменение, проверить наличие других признаков вредоносной активности (загрузка исполняемых файлов, сетевые подключения), и при необходимости — изолировать хост для дальнейшего анализа.	• Defense Evasion (TA0005) • Impact (TA0040) • Modify Registry (T1112) • Defacement (T1491) • Internal Defacement (T1491.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-851	Отключение в реестре HECI	Обнаруживает изменения ключа реестра HypervisorEnforcedCodeIntegrity (HECI) и установку значения `Enabled` в `0`, чтобы отключить функцию Hypervisor Enforced Code Integrity. Это позволяет атакующему загружать неподписанный и недоверенный код для выполнения в ядре. При срабатывании правила рекомендуется проверить, каким процессом и пользователем было изменено значение параметра, определить, было ли это связано с администрированием или потенциальной вредоносной активностью, восстановить корректное значение и перезагрузить систему для применения настроек, а также провести анализ журналов событий и активности на хосте, чтобы выявить другие признаки компрометации и исключить возможность повторного изменения параметра.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-852	Отключение Административных общих ресурсов при запуске	Правило детектирует отключение Административных общих ресурсов через реестр. Административные общие ресурсы — это скрытые сетевые ресурсы, созданные операционными системами Microsoft Windows NT, которые предоставляют системным администраторам удаленный доступ к каждому дисковому тому в системе, подключенному к сети. При срабатывании правила рекомендуется проверить, каким пользователем и процессом было изменено значение параметра, определить, является ли это частью штатных административных действий или результатом потенциальной вредоносной активности, восстановить исходное значение параметра для обеспечения доступа администратора и проанализировать журналы событий на наличие других признаков попыток скрыть активность или ограничить удаленное администрирование.	• Defense Evasion (TA0005) • Indicator Removal (T1070) • Network Share Connection Removal (T1070.005)

ID правила	Название правила	Описание	Тактики и техники
RV-D-853	Отключение контроля учетных записей пользователей	Данное правило обнаруживает изменение системных настроек, влияющих на работу контроля привилегий через реестр. Подобные модификации могут быть использованы для обхода встроенных средств защиты и выполнения несанкционированных действий с повышенными правами. При выявлении события рекомендуется проверить инициатора изменения, связанные процессы и общий контекст активности, чтобы определить, является ли действие легитимным. Если установлено, что изменение выполнено несанкционированно, следует начать расследование и сбросить пароль учетной записи, инициировавшей активность.	• Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Abuse Elevation Control Mechanism (T1548) • Bypass User Account Control (T1548.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-854	Включение в реестре DNS-over-HTTPS	Правило детектирует изменения в ветках реестра, отвечающих за функции включения DNS-over-HTTPS. Атакующие могут использовать DNS-over-HTTPS для маскировки интернет-активности или процесса утечки данных. При включении этой функции теряется возможность видеть такие данные, как тип запроса, ответ и IP-адрес источника, которые часто используются для выявления подозрительной активности. При срабатывании рекомендуется проверить, кто и каким процессом внес изменения, проанализировать сопутствующую сетевую активность на предмет необычных DNS-запросов, оценить необходимость использования DNS-over-HTTPS в текущей среде, а при выявлении подозрительных действий — рассмотреть возможность отключения данной функции и начать расследование на предмет выявления других индикаторов компрометации или подозрительных действий.	• Defense Evasion (TA0005) • Impact (TA0040) • Modify Registry (T1112) • Inhibit System Recovery (T1490)

ID правила	Название правила	Описание	Тактики и техники
RV-D-855	Установка нового значения DNS ServerLevelPluginDll	Данное правило выявляет изменение параметра реестра ServerLevelPluginDll, который определяет путь к DLL-библиотеке, загружаемой в контексте службы DNS-сервера Windows. Подобная модификация позволяет подключать пользовательские или вредоносные плагины, что дает возможность атакующим выполнить произвольный код с правами службы DNS — часто это привилегии уровня SYSTEM и потенциально полный контроль над контроллером домена. При выявлении изменений рекомендуется проверить инициатора и контекст активности, чтобы оценить легитимность действия. В случае подозрений следует предпринять меры по восстановлению исходных настроек, ограничению доступа к управлению DNS и провести расследование инцидента с целью выявления возможной компрометации.	• Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Modify Registry (T1112) • Hijack Execution Flow (T1574) • DLL Side-Loading (T1574.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-856	Разрешение удаленного соединения между анонимными компьютерами	В Windows существуют параметры реестра, изменение которых может ослабить встроенные механизмы безопасности и открыть возможности для удаленного взаимодействия с системой. Включение значений `AllowAnonymousCallback`, `AllowDCOMReflection` и `OnlyUseLatestCLR` может указывать на попытку обойти стандартные ограничения доступа или подготовку к удаленному выполнению кода через механизмы WMI, DCOM или .NET. Значение `AllowAnonymousCallback` позволяет устанавливать удаленные подключения к WMI между компьютерами без доверительных отношений. `AllowDCOMReflection` разрешает анонимный доступ к DCOM-интерфейсу, а `OnlyUseLatestCLR` может повлиять на поведение .NET-приложений, запуская их всегда на последней установленной версии CLR, что может быть использовано для обхода настроек совместимости или защиты. Данное правило отслеживает случаи включения этих параметров реестра, что может быть признаком активности атакующего, использующего fileless-техники или настраивающего систему под дальнейшую атаку. При срабатывании правила рекомендуется проверить, кем было выполнено изменение (пользователь и процесс), а также установить, связано ли оно с легитимной административной задачей. Если источник изменений неизвестен или вызывает подозрения, необходимо	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-857	Модификация скрытых ключей Проводника	Данное правило выявляет попытки изменения параметров отображения скрытых и системных файлов в проводнике Windows через модификацию соответствующих ключей реестра. Этот прием нередко используется вредоносными программами для сокрытия своей активности от пользователя. Атакующий может изменить значения ключей Hidden и ShowSuperHidden, чтобы скрыть вредоносные файлы и затруднить их обнаружение. Такие изменения могут указывать на попытку уклонения от обнаружения и свидетельствовать о компрометации системы. При срабатывании правила необходимо проанализировать процесс, инициировавший изменение реестра, и установить, соответствует ли оно легитимной пользовательской или административной активности. В случае отсутствия объяснимых причин следует инициировать дополнительное расследование на наличие вредоносного ПО, включая проверку автозагрузки, задач планировщика и сетевой активности. Также рекомендуется временно изолировать систему от сети до завершения анализа.	• Defense Evasion (TA0005) • Hide Artifacts (T1564) • Hidden Files and Directories (T1564.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-858	Скрытие запланированной задачи через реестр	Атакующие могут скрывать запланированные задачи в системе, изменяя значение параметра `Index` в ветке реестра TaskCache. Установка значения `DWORD(0x00000000)` делает задачу невидимой для стандартных административных инструментов, таких как `schtasks /query`, что позволяет скрыть следы присутствия и сохранить присутствие в системе. Такая техника может применяться после создания задачи вручную или с помощью вредоносного кода. При срабатывании следует проверить путь в реестре, имя задачи и инициирующий процесс. При наличии подозрительной активности — изолировать хост и провести расследование.	• Defense Evasion (TA0005) • Hide Artifacts (T1564) • Hidden Files and Directories (T1564.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-859	Подозрительный путь DLL в IME реестре	Атакующие могут использовать механизм Windows Input Method Editor (IME) для незаметной загрузки вредоносных библиотек. Для этого они регистрируют путь к DLL в значении Ime File под ключами `HKLM\SYSTEM\CurrentControlSet\Control\Keyboard Layouts\*`, а затем инициируют загрузку через сообщение `WM_INPUTLANGCHANGEREQUEST`. Такой подход позволяет внедрить произвольный код в доверенные процессы без явного запуска исполняемого файла и может не сопровождаться подозрительной сетевой или файловой активностью. Подобные пути к DLL в нестандартных и временных директориях (Temp, AppData, Public) являются индикатором возможной компрометации. При срабатывании проверьте целостность указанной библиотеки, инициировавший процесс и историю изменений системного реестра. При подтверждении вредоносного характера изолируйте узел и начните расследование.	• Persistence (TA0003) • Defense Evasion (TA0005) • Modify Registry (T1112) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-860	Включение хранение хеша LM	Изменение значения реестра NoLMHash в Windows разрешает системе хранить устаревшие LM-хеши паролей, которые обладают низкой стойкостью к взлому и могут быть использованы атакующими для компрометации учетных данных. Обычно данный параметр установлен в положение, запрещающее хранение LM-хешей. Обнаружение такого изменения указывает на снижение уровня безопасности системы и возможную подготовку к атакам на учетные записи. Рекомендуется проверить причину изменения, убедиться в легитимности операции и при подозрении на компрометацию инициировать расследование.	• Defense Evasion (TA0005) • Modify Registry (T1112)

ID правила	Название правила	Описание	Тактики и техники
RV-D-861	Создание билета TGT при помощи хакерской утилиты	Атакующие, обладающие хешем пароля учетной записи KRBTGT, могут подделывать билеты Kerberos, осуществляя атаку, известную как "золотой билет" (Golden Ticket). Золотые билеты позволяют генерировать билеты TGT для любой учетной записи в Active Directory и использовать их для запроса билетов службы (TGS), которые предоставляют доступ к различным ресурсам. Для получения TGS атакующие вынуждены взаимодействовать с Центром распространения ключей (KDC), который работает на всех контроллерах домена, входящих в состав Active Directory. Учетная запись KRBTGT используется службой KDC и отвечает за шифрование и подписание всех Kerberos-билетов. Для ликвидации последствий атаки Golden Ticket необходимо дважды сменить пароль учетной записи KRBTGT. Если билет не выгружается в виде файла, а загружается напрямую в память, и события в журнале Windows отсутствуют, правило не сможет обнаружить активность.	• Privilege Escalation (TA0004) • Credential Access (TA0006) • Steal or Forge Kerberos Tickets (T1558) • Golden Ticket (T1558.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-862	Дамп LSASS с помощью Python-утилит	Атакующий может попытаться получить данные других учетных записей с помощью дампа системного процесса LSASS (Local Security Authority Subsystem Service), который хранит в своей памяти учетные данные авторизованных пользователей на узле. Данное правило обнаруживает попытку дампа процесса с помощью мониторинга обращения к процессу lsass с маской доступа 0x1fffff и с использованием библиотек python. При срабатывании правила и отсутствии подтвержденной легитимной активности необходимо завершить активные сеансы на пораженном узле, сбросить пароли всех пользователей, активных в момент события, а также провести проверку на наличие инструментов удаленного доступа или подключения к внешним управляющим серверам. При обнаружении признаков внешнего взаимодействия следует заблокировать соответствующий IP-адрес и изолировать хост от сети до завершения расследования.	• Credential Access (TA0006) • OS Credential Dumping (T1003) • LSASS Memory (T1003.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-863	Подозрительный доступ к памяти процесса LSASS	Атакующий может попытаться получить данные учетных записей с помощью дампа системного процесса LSASS (Local Security Authority Subsystem Service), который хранит в своей памяти учетные данные авторизованных пользователей на узле. Данное правило обнаруживает предоставление доступа на чтение виртуальной памяти LSASS подозрительным процессам. Существует системное/легитимное ПО, которое обращается к процессу LSASS с правами на чтение виртуальной памяти; данные процессы внесены в исключения в поле `aliases:filter` (массив `exceptions_list`). В случае срабатывания правила рекомендуется проверить, что за процесс инициирует доступ к LSASS, возможно, были выполнены команды или запущено нелегитимное программное обеспечение. Если это легитимное ПО в инфраструктуре, то его можно внести в исключения аналогично другим процессам. Если в исключениях есть ПО, которое не используется в инфраструктуре и его активность нужно отслеживать, можно удалить значение или закомментировать существующую строку.	• Credential Access (TA0006) • OS Credential Dumping (T1003) • LSASS Memory (T1003.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-864	Дамп LSASS с помощью Диспетчера задач	Правило обнаруживает создание файла `lsass.dmp` от процесса taskmgr.exe. Это означает, что был создан дамп процесса LSASS (Local Security Authority Subsystem Service), который хранит в своей памяти учетные данные авторизованных пользователей на узле, с помощью процесса Windows Task Manager (Диспетчер задач). Такая активность может свидетельствовать о попытке извлечения учетных данных и часто связана с действиями атакующих. При срабатывании правила необходимо определить, какой именно файл был создан, а также уточнить легитимность активности. Если легитимность не установлена, следует классифицировать событие как инцидент безопасности и инициировать дальнейшее расследование.	• Credential Access (TA0006) • OS Credential Dumping (T1003) • LSASS Memory (T1003.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-865	Использование утилиты RDPStrike	Утилита RDPStrike предназначена для извлечения паролей в открытом виде из процесса mstsc.exe. После внедрения вредоносного кода в указанный процесс она устанавливает аппаратные точки останова (hardware breakpoints) на три API-функции: SspiPrepareForCredRead, CryptProtectMemory и CredIsMarshaledCredentialW, что позволяет перехватывать учетные данные и сохранять их в файл во временной директории. Утилита отслеживает создание новых процессов и при обнаружении запуска mstsc.exe автоматически внедряет код с целью кражи данных. При срабатывании правила корреляции и отсутствии подтвержденной легитимной активности рекомендуется завершить активные сессии с зараженного хоста, сбросить пароль учетной записи, активной на данном устройстве, а также проверить наличие подключений к серверам управления. Если сервер управления расположен внутри инфраструктуры, следует изолировать хост, при нахождении во внешней сети — заблокировать соответствующий адрес.	• Credential Access (TA0006) • Collection (TA0009) • Process Injection (T1055) • Dynamic-link Library Injection (T1055.001) • Input Capture (T1056) • Credential API Hooking (T1056.004) • Exploitation for Credential Access (T1212)

ID правила	Название правила	Описание	Тактики и техники
RV-D-866	Отключение системы восстановления через реестр	Правило нацелено на обнаружение модификации веток реестра, которые отвечают за функцию восстановления системы. Мониторинг веток реестра имеет критическое значение для обеспечения безопасности и целостности компьютерных систем. Подобный мониторинг позволяет оперативно выявлять любые изменения, направленные на отключение или модификацию функции восстановления системы, и и реагировать на них. Данные изменения могут привести к серьезным последствиям, таким как потеря данных, угрозы безопасности и нарушение нормального функционирования системы. При срабатывании правила необходимо проверить легитимность изменения, установить, каким пользователем и каким процессом оно было выполнено, проанализировать систему на наличие признаков вредоносной активности и, при необходимости, восстановить настройки восстановления и инициировать дальнейшее расследование.	• Impact (TA0040) • Inhibit System Recovery (T1490)

ID правила	Название правила	Описание	Тактики и техники
RV-D-867	Создание WMI-подписки	Подписка на события Windows Management Instrumentation (WMI Event Subscription) представляет собой механизм в Windows для отслеживания событий, происходящих в системе, с использованием WMI. Когда происходит событие, система может реагировать, выполняя предопределенные действия. Использование WMI Event Subscription может иметь потенциальные риски безопасности, так как атакующие могут использовать этот механизм для создания скрытых механизмов слежения или выполнения вредоносных действий в системе. В рамках реагирования на данный инцидент необходимо связаться с лицом, ответственным за узел/учетную запись, и выяснить, чем вызвана данная активность. В случае отсутствия подтверждения легитимности необходимо заблокировать узел/учетную запись до выяснения обстоятельств.	• Execution (TA0002) • Persistence (TA0003) • Privilege Escalation (TA0004) • Windows Management Instrumentation (T1047) • Event Triggered Execution (T1546) • Windows Management Instrumentation Event Subscription (T1546.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-878	Закрепление через изменения ключей автозапуска в реестре	Атакующий, с целью обеспечения своего закрепления, может изменить ключи запуска в реестре. Указанная активность позволит потенциальному ВПО запускаться каждый раз при включении системы. Данная активность является аномальной и может говорить об активности ВПО. В случае возникновения активности требуется опросить УЗ инициатора активности. В случае если легитимность подтвердить не удалось — убрать добавленный ключ реестра и заблокировать УЗ инициатора активности на время выяснения обстоятельств инцидента ИБ.	• Persistence (TA0003) • Boot or Logon Autostart Execution (T1547) • Registry Run Keys / Startup Folder (T1547.001)
RV-D-885	Удаление метки MOTW Windows	Атакующий может удалить метку безопасности Mark-of-the-Web, которая указывает, что файл был загружен из Интернета, с целью избежать предупреждений или блокировок в Windows. При срабатывании данного правила корреляции необходимо проверить, какие процессы запускались на хосте ранее, от какой учетной записи и в каком контексте. Следует запросить подтверждение легитимности действий у владельца УЗ и при неподтверждении — заблокировать данную УЗ, по возможности изучить источник происхождения файла, у которого удаляют метку MOTW, проверить события на предмет компрометации сети.	• Defense Evasion (TA0005) • Subvert Trust Controls (T1553) • Mark-of-the-Web Bypass (T1553.005) • Hide Artifacts (T1564) • NTFS File Attributes (T1564.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-887	Создание удаленного потока в процессе lsass	Данное правило направлено на детектирование выполнения кода в процессе lsass.exe с помощью создания удаленного потока. Такое поведение позволяет атакующему извлекать учетные данные из памяти процесса или выполнять произвольный код с привилегиями системного процесса. Успешная эксплуатация может привести к компрометации учетных данных, повышению привилегий или дальнейшему распространению в сети. В случае срабатывания правила необходимо запросить разъяснения о причине данной активности у ответственного за учетную запись. При отсутствии объяснений — заблокировать учетную запись, изолировать узел и провести внутреннее расследование.	• Privilege Escalation (TA0004) • Process Injection (T1055) • Thread Execution Hijacking (T1055.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-888	Закрепление через Microsoft Office Add-ins	Атакующие могут использовать надстройки Microsoft Office, чтобы закрепиться в скомпрометированной системе. Надстройки Microsoft Office (Office Add-ins) представляют собой дополнительные модули, которые расширяют функциональность приложений Office, таких, как Word, Excel, PowerPoint и Outlook. Они используются для автоматизации задач, интеграции с внешними сервисами или добавления пользовательских функций. При срабатывании правила следует запросить у пользователя цели добавления файла надстройки. При подтверждении инцидента следует заблокировать УЗ инициатора и удалить добавленные файлы надстроек, по возможности изучить их в изолированной среде.	• Persistence (TA0003) • Office Application Startup (T1137) • Add-ins (T1137.006)

ID правила	Название правила	Описание	Тактики и техники
RV-D-889	Закрепление в системе через ключ реестра MyComputer	Это правило обнаруживает изменение значения (Default) в ключе реестра MyComputer и его подразделах, указывающее на назначение исполняемого файла, который будет запускаться при соответствующем действии, например, при очистке диска или других системных операциях. Такая модификация часто используется атакующими для закрепления вредоносного кода в системе (Persistence), позволяя автоматически запускать вредоносные программы при взаимодействии с функциями Windows Explorer. При срабатывании необходимо проверить инициирующий процесс и пользователя, а также провести расследование на предмет возможной активности атакующих.	• Persistence (TA0003) • Boot or Logon Autostart Execution (T1547)

ID правила	Название правила	Описание	Тактики и техники
RV-D-891	Закрепление через Office Test	Атакующие могут использовать ключ реестра Office Test для Microsoft Office, чтобы закрепиться в скомпрометированной системе. В реестре существует ключ Office Test, где пользователь может указать произвольную DLL-библиотеку, которая будет выполняться при каждом запуске приложения Office. Считается, что этот ключ реестра используется Microsoft для загрузки DLL-библиотек в целях тестирования и отладки при разработке приложений Office. Этот ключ реестра не создается по умолчанию при установке Office. При срабатывании правила следует запросить у пользователя объяснение своих действий о вмешательстве в данную ветку реестра. При подтверждении инцидента следует вернуть настройки системы в исходное состояние, заблокировать УЗ инициатора и изолировать добавленные файлы, по возможности изучить их в изолированной среде.	• Persistence (TA0003) • Defense Evasion (TA0005) • Modify Registry (T1112) • Office Application Startup (T1137) • Office Template Macros (T1137.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-895	Создание токена и имперсонация учетной записи	Атакующие могут создавать новые токены и выдавать себя за существующих пользователей, чтобы повысить привилегии и обойти контроль доступа. Правило предназначено для выявления случаев запуска cmd.exe, где в качестве пользователя указана системная учетная запись, а инициатором запуска выступает пользовательская учетная запись. Такое поведение может указывать на попытку атакующего выполнить команды с повышенными привилегиями через манипуляцию токеном. В случае срабатывания правила, рекомендуется уточнить активность с пользователем, инициировавший ее. Если активность подозрительная, то рекомендуется изолировать хост и проанализировать цепочку событий, приведших к запуску команды.	• Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Access Token Manipulation (T1134) • Create Process with Token (T1134.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-897	Эксплуатация Mark-of-the-Web bypass	Уязвимость в 7-Zip позволяет обойти механизм безопасности Windows Mark-of-the-Web (MOTW), предназначенный для защиты пользователей от потенциально опасных файлов, загруженных из интернета. Проблема возникает из-за того, что при извлечении файлов из специально подготовленного архива с меткой MOTW программа не сохраняет метку для извлеченных файлов. Это создает возможность для атакующих выполнять произвольный код от имени текущего пользователя без активации защитных механизмов. При срабатывании правила следует уточнить у пользователя, который открыл архив, происхождение архива и способ его получения. Проверить, были ли внесены в систему изменения, при наличии подозрительной активности и сомнениях в источнике, откуда был получен архив, рекомендуется изолировать хост.	• Defense Evasion (TA0005) • Subvert Trust Controls (T1553) • Mark-of-the-Web Bypass (T1553.005)

ID правила	Название правила	Описание	Тактики и техники
RV-D-898	Использование ssh.exe для кражи NTLM-хеша	Данное правило направлено на детектирование атаки, связанной с использованием ssh.exe для кражи NTLM-хеша через принудительную аутентификацию. Атакующий может запустить ssh.exe с параметром `-i`, указывая путь к закрытому ключу через UNC, что позволяет инициировать аутентификацию и перехват NTLM-хеша. Успешная эксплуатация данной техники может привести к компрометации учетных данных и дальнейшему распространению атаки в сети. В случае срабатывания правила необходимо уточнить легитимность использования ssh.exe у владельца учетной записи. При отсутствии обоснованного объяснения рекомендуется заблокировать учетную запись, ограничить доступ к узлу, с которого зафиксирована активность, и провести расследование возможной компрометации инфраструктуры.	• Credential Access (TA0006) • Forced Authentication (T1187)

ID правила	Название правила	Описание	Тактики и техники
RV-D-899	Обход UAC через COM-объекты	Атакующие могут использовать COM-модель Windows для обхода контроля учетных записей (UAC) и выполнения кода с повышенными привилегиями. COM (Component Object Model) обеспечивает межпроцессное взаимодействие, позволяя объектам в разных процессах обмениваться данными и вызывать методы друг друга. Этот механизм активно используется в Windows и им можно злоупотребить для эскалации привилегий. Данное правило корреляции нацелено на выявление попыток эксплуатации COM-объектов для повышения прав без взаимодействия с пользователем (UAC bypass). При срабатывании правила рекомендуется в процессе расследования обратить внимание на наличие события Sysmon 7, в котором неизвестный процесс загрузил системную библиотеку cmlua.dll (часто используется в UAC bypass). Если процесс действительно неизвестен, рекомендуется изолировать хост.	• Execution (TA0002) • Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Abuse Elevation Control Mechanism (T1548) • Bypass User Account Control (T1548.002) • Inter-Process Communication (T1559) • Component Object Model (T1559.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-900	Использование DNS туннеля	DNS Tunneling — это метод кодирования передаваемой информации в DNS запросах. Данный метод может использоваться атакующими для обхода правил межсетевого экранирования и эксфильтрации данных. Правило отслеживает уникальные запросы для одного домена (значения после первой точки). При достижении заданного порога генерируются корреляционные события. В случае возникновения активности рекомендуется изучить процесс, выполняющий DNS-запросы, а также проверить легитимность домена. В случае если легитимность подтвердить не удалось — заблокировать домен и изолировать хост. При легитимности домена требуется добавить его в список исключений excludeDomain.	• Command and Control (TA0011) • Exfiltration Over Alternative Protocol (T1048) • Exfiltration Over Unencrypted Non-C2 Protocol (T1048.003) • Application Layer Protocol (T1071) • DNS (T1071.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-904	Удаленная эксплуатация DCOM объекта IMsiServer	Правило обнаруживает удаленный запуск процессов с помощью DCOM IMsiServer. После получения первоначального доступа атакующий начинает горизонтальное перемещение по корпоративной сети жертвы, используя DCOM IMsiServer, который позволяет удаленно транспортировать полезную нагрузку на удаленный хост и выполнить ее. При срабатывании данного правила необходимо проанализировать, какой объект был передан, под какой учетной записью и в какое время. Опросить ответственного за учетную запись пользователя и при неподтверждении активности — заблокировать учетную запись, по возможности изолировать атакованный хост от сетевого окружения и проанализировать переданную нагрузку в изолированной среде. Проверить активность на атакованном хосте после передачи полезной нагрузки.	• Defense Evasion (TA0005) • Lateral Movement (TA0008) • Remote Services (T1021) • Distributed Component Object Model (T1021.003) • System Binary Proxy Execution (T1218) • Msiexec (T1218.007)

ID правила	Название правила	Описание	Тактики и техники
RV-D-905	Утечка NTLM через library-ms (CVE-2025-24071)	Уязвимость CVE-2025-24071 связана с механизмом обработки файлов в Windows Explorer и системой индексирования. Эти компоненты автоматически анализируют файлы с расширением .library-ms, которые могут быть извлечены при распаковке вредоносных архивов. При этом файл может содержать ссылку на SMB-ресурс, что приводит к автоматической NTLM-аутентификации на атакующем SMB-сервере без взаимодействия с пользователем. Это вызывает утечку хеша NTLMv2 учетной записи жертвы, что может быть использовано для дальнейших атак. Данное правило отслеживает создание файлов с данным расширением и подключение по SMB к неизвестному ресурсу, что может быть признаком эксплуатации этой уязвимости. При срабатывании правила необходимо уточнить, кто инициировал создание файла .library-ms и подключение к SMB-ресурсу, а также проверить, соответствует ли подключение назначению хоста. Если активность выглядит подозрительной, следует изолировать хост, расследовать происхождение файла и проанализировать связанные события для подтверждения или опровержения возможного инцидента.	• Credential Access (TA0006) • Forced Authentication (T1187) • Adversary-in-the-Middle (T1557) • LLMNR/NBT-NS Poisoning and SMB Relay (T1557.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-910	Изменение чувствительных значений реестра	Правило обнаруживает изменение чувствительных значений реестра, которые могут использоваться для ухода от обнаружения или ослабления защиты при компрометации узла.	• Persistence (TA0003) • Defense Evasion (TA0005) • Modify Registry (T1112)
RV-D-911	Добавление в Netsh Helper DLL потенциальной полезной нагрузки	Атакующие могут использовать вспомогательные DLL-файлы netsh.exe для запуска произвольного кода при закреплении. Этот запуск будет происходить каждый раз, когда выполняется netsh.exe, что может происходить автоматически, с другой техникой закрепления доступа или если в системе присутствует программное обеспечение (например, VPN), которое использует netsh.exe в рамках своей нормальной функциональности. Netsh.exe — это утилита командной строки, используемая для взаимодействия с настройками сети системы. Она содержит функционал для добавления вспомогательных DLL-файлов, расширяющих возможности утилиты. Пути к зарегистрированным вспомогательным DLL-файлам netsh.exe находятся в реестре Windows по адресу `HKLM\SOFTWARE\Microsoft\Netsh`. Правило нацелено на выявление добавления файла с расширением `.dll` по пути `software\microsoft\netsh`.	• Persistence (TA0003) • Event Triggered Execution (T1546) • Netsh Helper DLL (T1546.007)

ID правила	Название правила	Описание	Тактики и техники
RV-D-912	Кража токена доступа из системного процесса	Кража токена доступа SYSTEM полезна в случаях, когда определенные привилегии были отозваны у учетной записи локального администратора через групповую политику. Например, привилегия SeDebugPrivilege может быть удалена из группы локальных администраторов, чтобы затруднить атакующему сброс учетных данных или взаимодействие с памятью других процессов. Однако привилегии не могут быть отозваны у учетной записи SYSTEM, поскольку они необходимы для работы операционной системы. Это делает токены доступа SYSTEM чрезвычайно ценными для атакующих в условиях усиленной безопасности. Некоторые системные процессы, обладают такими токенами и атакующие могут получить этот токен, создав поток к системному процессу, при помощи функции DuplicateTokenEx() могут дублировать токен и использовать его в своих процессах с правами SYSTEM. При возникновении данной активности необходимо опросить владельца учетной записи (УЗ) инициатора активности на предмет совершаемых действий. В случае если подтвердить легитимность не удалось, следует заблокировать УЗ инициатора активности.	• Privilege Escalation (TA0004) • Access Token Manipulation (T1134) • Token Impersonation/Theft (T1134.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-913	Обнаружение HTML/SVG Smuggling в Windows	Правило предназначено для выявления техники HTML/SVG Smuggling, при которой вредоносные файлы в формате `.html`, `.htm` или `.svg` создаются в критичных директориях пользователя и запускаются в браузере. Техника используется атакующими для обхода фильтров веб-контента и доставки вредоносных файлов через HTML-документы, часто прикрепленные к фишинговым письмам. При возникновении корреляционного события необходимо проверить происхождение обнаруженных файлов и уточнить у пользователя активность.	• Defense Evasion (TA0005) • Obfuscated Files or Information (T1027) • HTML Smuggling (T1027.006) • SVG Smuggling (T1027.017)
RV-D-933	Создание удаленного потока с использованием функции LoadLibrary	Обнаружение потенциального использования API CreateRemoteThread и функции LoadLibrary для внедрения DLL в процесс.	• Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Process Injection (T1055) • Dynamic-link Library Injection (T1055.001)
RV-D-934	Создание удаленного потока подозрительным процессом	Правило направлено на обнаружение нестандартных процессов, создающих удаленные потоки.	• Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Process Injection (T1055)

ID правила	Название правила	Описание	Тактики и техники
RV-D-935	Кража токена доступа при помощи именованных каналов	Именованные каналы — это форма межпроцессного взаимодействия (IPC), которая позволяет взаимодействовать процессам, изначально не предназначенным для взаимодействия друг с другом. Кража токена доступа при помощи именованных каналов — техника, позволяющая повысить привилегии до локальной системы. Техника реализована за счет функции API ImpersonateNamedPipeClient, которая позволяет серверу именованного канала (тому, кто инициировал взаимодействие) олицетворить токен клиента (тот, к кому было осуществлено подключение через именованные каналы). Стоит отметить, что для кражи токена доступа клиента процесс сервера должен обладать привилегией SeImpersonatePrivilege. Техника Named Pipe Token Impersonation используется различными фреймворками и утилитами, такими как Cobalt Strike, Metasploit (getsystem command), PoshC2. При возникновении данной активности необходимо опросить владельца учетной записи (УЗ) инициатора активности на предмет совершаемых действий. В случае если подтвердить легитимность не удалось, следует заблокировать УЗ инициатора активности.	• Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Access Token Manipulation (T1134) • Token Impersonation/Theft (T1134.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-936	Использование утилиты TikiTorch	Данное правило направлено на детектирование использования утилиты TikiTorch, применяемой для выполнения инъекций в процессы с помощью такого метода, как создание удаленного потока. Утилита позволяет атакующему внедрять произвольный код в адресное пространство доверенных процессов, что может использоваться для обхода механизмов защиты, маскировки вредоносной активности и выполнения команд с привилегиями целевого процесса. Успешная эксплуатация может привести к повышению привилегий, выполнению вредоносного кода в контексте целевого процесса или последующему распространению в сети. В случае срабатывания правила необходимо получить разъяснения о причине данной активности от ответственного за учетную запись. В случае отсутствия обратной связи — провести внутреннее расследование, заблокировать учетную запись сотрудника, временно изолировать узел, на котором произошел инцидент.	• Privilege Escalation (TA0004) • Process Injection (T1055) • Process Injection (T1055) • Portable Executable Injection (T1055.002) • Thread Execution Hijacking (T1055.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-937	Подмена PID родительского процесса	Атакующие могут использовать технику подмены идентификатора родительского процесса (Parent Process ID Spoofing), чтобы скрыть истинное происхождение вредоносного процесса и обойти механизмы обнаружения, основанные на анализе цепочек родитель-потомок. Правило предназначено для выявления попыток подмены PID родительского процесса через анализ событий Sysmon, связанных с созданием процессов (Event ID 1) и загрузкой библиотек (Event ID 7). При обнаружении процесса с неподписанными библиотеками или подозрительными цепочками запуска рекомендуется провести анализ активности, связанной с данным процессом. Проверить параметры запуска подозрительного процесса и его родителя. Уточнить активность с пользователем, указанным в инициирующем процессе (если применимо). Если активность подозрительная, изолировать хост и провести углубленный анализ.	• Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Access Token Manipulation (T1134) • Parent PID Spoofing (T1134.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-938	Внедрение стороннего ПО через отладчик IFEO	Атакующие могут закрепиться в системе и/или повысить привилегии, запустив вредоносный код, запускаемый отладчиками Image File Execution Options (IFEO). IFEO позволяют разработчику подключать отладчик к приложению. При создании процесса к его имени добавляется отладчик, присутствующий в IFEO приложениях, что позволяет запускать новый процесс под управлением отладчика. Правило нацелено на добавление исполняемого файла в виде "хелпера" к другому файлу через реестр.	• Persistence (TA0003) • Event Triggered Execution (T1546) • Image File Execution Options Injection (T1546.012)

ID правила	Название правила	Описание	Тактики и техники
RV-D-939	Закрепление через Office Template Macros	Атакующие могут использовать шаблоны Microsoft Office, чтобы закрепиться в скомпрометированной системе. Microsoft Office содержит шаблоны, которые входят в состав распространенных приложений Office и используются для настройки стилей. Базовые шаблоны приложения используются при каждом его запуске. Данное правило фиксирует три способа эксплуатации макросов в шаблонах. При частых срабатываний правила обращайте внимание на сообщение, которое выводит оповещение. При срабатывании правила следует запросить у пользователя объяснение своих действий с шаблоном Word или Excel, а также, если был изменен ключ реестра. При подтверждении инцидента следует вернуть настройки системы в исходное состояние, заблокировать УЗ инициатора и изолировать добавленные файлы, по возможности изучить их в изолированной среде.	• Persistence (TA0003) • Defense Evasion (TA0005) • Modify Registry (T1112) • Office Application Startup (T1137) • Office Template Macros (T1137.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-940	Закрепление через COM Hijacking	COM (Component Object Model) — это стандарт, позволяющий разработчикам повторно использовать в своем коде независимые компоненты ПО. При этом им не нужно знать внутреннее устройство данных компонентов, заниматься их совместимостью на разных языках программирования и повторной компиляцией. Атакующие могут закрепиться в системе, выполняя полезную нагрузку, вызванную перехваченными ссылками на объекты Component Object Model (COM). Ссылки на различные объекты COM хранятся в реестре. Для захвата COM-объекта требуется внести изменения в реестр, чтобы заменить ссылку на легитимный системный компонент, что может привести к тому, что этот компонент не будет работать при выполнении. Когда этот системный компонент будет вызван в ходе обычной работы системы, вместо него будет выполнена полезная нагрузка. В случае возникновения активности требуется опросить ответственного за учетную запись инициатора активности. В случае если легитимность подтвердить не удалось, убрать добавленный/измененный ключ реестра и заблокировать УЗ инициатора активности на время выяснения обстоятельств инцидента ИБ.	• Execution (TA0002) • Persistence (TA0003) • Privilege Escalation (TA0004) • Event Triggered Execution (T1546) • Component Object Model Hijacking (T1546.015) • Inter-Process Communication (T1559) • Component Object Model (T1559.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-941	Включение переменных среды COR Profiler	Это правило обнаруживает изменение в реестре, связанное с установкой переменных среды для .NET Framework и .NET Core CLR, таких, как COR_ENABLE_PROFILING и COR_PROFILER. Эти переменные могут использоваться атакующими для внедрения вредоносных CLR-профайлеров с целью закрепления, повышения привилегий и обхода защитных механизмов. Настройка подобных переменных указывает на потенциально нежелательную или вредоносную активность. При срабатывании необходимо проверить легитимность изменений, определить инициирующий процесс и пользователя, а также провести анализ системы на предмет угроз. Без подтверждения легитимности рекомендуется ограничить права пользователя и начать расследование инцидента.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Hijack Execution Flow (T1574) • COR_PROFILER (T1574.012)

ID правила	Название правила	Описание	Тактики и техники
RV-D-942	Изменение настроек администратора Winget	Обнаружение изменений в настройках администратора приложения AppInstaller (winget). Winget — это инструмент командной строки для управления пакетами в операционной системе Windows. Он предоставляет удобный способ установки, удаления и обновления приложений через командную строку. Атакующий может изменить конфигурацию и параметры инструмента управления пакетами на операционной системе Windows, чтобы осуществить внедрение вредоносного программного обеспечения, модифицировать источники пакетов для загрузки поддельных приложений или изменить поведение winget с целью нарушения безопасности системы. При срабатывании правила корреляции следует проверить активность с пользователем, который указан как инициатор (src_user_name). В случае подтверждения несанкционированных изменений рекомендуется восстановить исходные настройки Winget и провести проверку системы на наличие вредоносного ПО, начать расследование.	• Command and Control (TA0011) • Ingress Tool Transfer (T1105)

ID правила	Название правила	Описание	Тактики и техники
RV-D-943	Зафиксирована подмена файлов экрана заставки Windows	Атакующие могут закрепиться в системе и\или повышать привилегии выполняя вредоносный код, запускаемый с помощью различных функций Windows. Например, заменяя файлы, отвечающие за заставку Windows (screensaver), на "командную строку" (cmd.exe), полезную нагрузку или ВПО. Можно вызвать их исполнение при включении экрана заставки в Windows.	• Persistence (TA0003) • Event Triggered Execution (T1546) • Screensaver (T1546.002)
RV-D-957	Использование rsockstun клиента	Rsockstun — это инструмент для создания обратного SOCKS5-туннеля с поддержкой SSL и прокси, позволяющий устройствам за NAT или брандмауэрам безопасно подключаться к удаленному серверу и перенаправлять трафик. Данная утилита используется атакующими для обхода сетевых ограничений и создания защищенных каналов связи. Ранее в отчете от Лаборатории Касперского отмечалось применение rsockstun группировкой Head Mare в атаках на государственные структуры России и Беларуси. При срабатывании правила необходимо проверить и уточнить у пользователя, для чего запускалась данная утилита. Если активность подтвердить не удалось, следует заблокировать IP-адрес, указанный в src_ip, сменить пароль пользователя и начать расследование.	• Command and Control (TA0011) • Proxy (T1090) • Protocol Tunneling (T1572) • Encrypted Channel (T1573)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1120	Подозрительные обращения к trycloudflare.com	Данное правило выявляет обращения к доменам в зоне trycloudflare.com на основе событий DNS-запросов (Sysmon EventID 22). Такие домены используются при создании временных туннелей через Cloudflare Tunnel, что позволяет атакующим обходить сетевые ограничения и скрывать C2-каналы или доставку полезной нагрузки. Обнаружение DNS-запроса к подобному ресурсу может свидетельствовать о подозрительной активности.	• Command and Control (TA0011) • Proxy (T1090) • Protocol Tunneling (T1572)
RV-D-1123	Исходящее подключение SYSTEM-процессов к нестандартным портам	Атакующие могут использовать подключения с нестандартными сочетаниями протоколов и портов. Например, протокол HTTPS через порт 8088 или порт 587 вместо традиционного порта 443. Чаще всего к данной технике прибегают для обхода фильтрации или чтобы усложнить анализ сетевого трафика. В качестве реального примера применения подобной техники можно привести группировку OceanLotus. В своих атаках они доставляют бэкдор через документы-ловушки, затем загружают полезную нагрузку, используют side-loading библиотек и запускают бэкдор с привилегиями SYSTEM. Далее связь с C2-сервером устанавливается через TCP на нестандартный порт (14146), что не выглядит как легитимный системный трафик.	• Command and Control (TA0011) • Non-Standard Port (T1571)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1140	Произошло выполнение полезной нагрузки при наступлении WMI события	Данное правило детектирует выполнение полезной нагрузки при срабатывании WMI Event Subscription. WMI Event Subscription (подписка на события в Windows Management Instrumentation) представляет собой механизм в операционной системе Windows, который позволяет отслеживать различные события, происходящие в системе, и реагировать на них. Атакующие могут использовать WMI Event Subscription для выполнения вредоносных действий при наступлении определенного системного события, что обеспечивает закрепление в системе. Для получения дополнительной информации о том, какой процесс был запущен, можно использовать события Sysmon с Event ID 1 и 10. В рамках реагирования на данный инцидент необходимо связаться с ответственным за узел/учетную запись и выяснить, чем вызвана данная активность. В случае отсутствия подтверждения легитимности необходимо заблокировать узел/учетную запись до выяснения обстоятельств.	• Execution (TA0002) • Persistence (TA0003) • Privilege Escalation (TA0004) • Windows Management Instrumentation (T1047) • Event Triggered Execution (T1546) • Windows Management Instrumentation Event Subscription (T1546.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1141	Загрузка процессом cmstp модулей для выполнения скриптов	В попытке избежать обнаружения атакующий может выполнять команды или запускать исполняемые файлы через «посредника» — системные утилиты. Такие исполняемые файлы, как правило, подписаны и могут быть внесены в списки исключений средств защиты информации (далее — СЗИ). Одним из таких инструментов является cmstp.exe, предназначенный для добавления и удаления профилей службы диспетчера подключений. Для добавления профилей используется INF-файл, в котором можно указать в секции [UnRegisterOCXSection] путь к COM-объекту в виде .sct-файла. При обработке такого файла cmstp.exe загружает модули jscript.dll или vbscript.dll в зависимости от используемого языка сценария. Такая активность может указывать на попытку обхода механизмов защиты и выполнения произвольного кода с использованием доверенного процесса. При срабатывании правила рекомендуется проверить источник и содержимое используемого INF-файла, установить, запускался ли он пользователем или сторонним ПО, и уточнить действия у пользователя. При отсутствии подтверждений — изолировать хост, сменить пароль пользователя и инициировать расследование.	• Execution (TA0002) • Defense Evasion (TA0005) • Shared Modules (T1129) • System Binary Proxy Execution (T1218) • CMSTP (T1218.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1142	Загрузка DLL системным процессом из подозрительного места	Данное правило отслеживает событие загрузки dll системным процессом (например, расположенным в System32 или SysWOW64) из подозрительного местоположения или из папки с особыми разрешениями, такой как `C:\Users\Public`. Такая активность может указывать на попытки атакующего внедрить вредоносный код в системные процессы, обойти механизмы безопасности и скрыть следы своей деятельности. Загрузка DLL из нестандартных или незащищенных директорий повышает риск эксплуатации уязвимостей и реализации техник обхода защиты. При срабатывании правила рекомендуется проверить процессы, загрузившие DLL из подозрительных директорий, на предмет легитимности, а также уточнить действия у пользователя. Если подтверждения нет, следует сменить пароль пользователя, изолировать хост и начать расследование.	• Defense Evasion (TA0005) • Indicator Removal (T1070)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1143	Загрузка RstrtMgr.dll необычным процессом	Правило обнаруживает загрузку библиотеки RstrtMgr.dll процессами, не относящимися к стандартным системным. RstrtMgr.dll — динамическая библиотека, которую атакующие используют в программах-вымогателях для завершения процессов, мешающих шифрованию файлов (например, Conti ransomware, Cactus ransomware). Библиотека используется вредоносным ПО BiBi wiper для Windows. Кроме того, RstrtMgr.dll может применяться для обхода средств анализа, блокируя определенные процессы. При обнаружении события необходимо проверить его легитимность и исследовать хост на наличие аномалий.	• Defense Evasion (TA0005) • Impact (TA0040) • Data Encrypted for Impact (T1486) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)
RV-D-1147	Создание дампа NTDS.dit	Правило предназначено для выявления попыток создания дампа базы данных NTDS.dit с использованием утилиты ntdsutil, применяемой для управления доменными службами Active Directory. В правиле фиксируются события, связанные с созданием файла `ntds.dit`. Эксплуатация NTDS.dit позволяет извлечь хеши паролей (включая административные), что упрощает проведение атак типа Pass-the-Hash или Golden Ticket.	• Credential Access (TA0006) • OS Credential Dumping (T1003) • NTDS (T1003.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1163	Изменение политики выполнения PowerShell	PowerShell — командная оболочка Windows, активно используемая как администраторами, так и атакующими. По умолчанию политика выполнения PowerShell ограничивает запуск неподписанных скриптов. Однако атакующие могут изменить эту политику на менее строгую (например, `Bypass` или `Unrestricted`), чтобы обойти механизмы безопасности и выполнить вредоносные сценарии. Такое поведение часто связано с попытками уклонения от обнаружения. Правило детектирует изменение политики выполнения PowerShell через создание или изменение соответствующих записей реестра. Рекомендуется проверить легитимность процесса, инициировавшего изменение, и установить, было ли это связано с подозрительной активностью или нарушением политики безопасности.	• Execution (TA0002) • Defense Evasion (TA0005) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Modify Registry (T1112)
RV-D-1186	Инъекция AppDomain Manager	AppDomain Manager Injection — техника подмены логики загрузки сборок в .NET Framework. Атакующий размещает рядом с исполняемым файлом конфигурацию *.exe.config с параметрами `appDomainManagerAssembly` и `appDomainManagerType`, из-за чего при запуске приложения загружается вредоносная DLL и выполняется код в InitializeNewDomain до основной логики процесса.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Hijack Execution Flow (T1574) • AppDomain Manager (T1574.014)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1208	Удаленный контроль через Chrome Remote Desktop	Chrome Remote Desktop (CRD) — официальное программное обеспечение от Google для удаленного управления компьютером. Замечено, что атакующие устанавливают CRD для скрытого удаленного контроля через инфраструктуру Google, таким образом минуя ограничения NAT и сетевые фильтры. Данное правило выявляет обращения к доменам в зоне googleapis.com на основе событий DNS-запросов (Sysmon EventID 22) и запуск процесса с хешем, принадлежащий бинарному файлу `remoting_host.exe`, который запускается для установления удаленной сессии.	• Command and Control (TA0011) • Remote Access Tools (T1219) • Remote Desktop Software (T1219.002)
RV-D-1252	Попытка дампа LSASS с помощью утилиты HandleKatz	Атакующий может попытаться получить данные других учетных записей с помощью дампа системного процесса LSASS (Local Security Authority Subsystem Service), который хранит в своей памяти учетные данные авторизованных пользователей на узле. Данное правило обнаруживает попытку дампа процесса с помощью мониторинга обращения к процессу LSASS с маской доступа 0x1440.	• Execution (TA0002) • Credential Access (TA0006) • OS Credential Dumping (T1003) • LSASS Memory (T1003.001) • Native API (T1106)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1356	Закрепление в системе через Narrator.exe	Атакующие могут злоупотреблять встроенными средствами специальных возможностей Windows (Accessibility Features), такими как `Narrator.exe`, для закрепления, эскалации привилегий или скрытого выполнения кода.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Event Triggered Execution (T1546) • Accessibility Features (T1546.008) • Hijack Execution Flow (T1574) • DLL (T1574.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1572	Запуск неподписанного установочного файла TrueConf	TrueConf Server — программная платформа для видеоконференцсвязи (ВКС). Используется для организации корпоративных коммуникаций, вебинаров и удаленного взаимодействия. В рамках атак, подобных CVE-2026-3502 (операция TrueChaos), атакующие могут использовать механизм обновления для доставки модифицированных или неподписанных установочных файлов клиентской части. Данное правило детектирует запуск установочного файла TrueConf с отсутствующей или недействительной цифровой подписью, что может указывать на попытку эксплуатации скомпрометированного канала обновлений или подмену дистрибутива.	• Execution (TA0002) • User Execution (T1204)

Microsoft Windows System

- Microsoft Windows System: правила корреляции

Microsoft Windows System: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-785	Остановка критичных сервисов	Данное правило направлено на детектирование подозрительных действий, связанных с остановкой критически важных сервисов, обеспечивающих стабильное функционирование системы или приложений. Такое поведение является аномальным для стандартных административных задач и может указывать на попытку атакующего нарушить работу системы, отключить защитные механизмы или подготовить инфраструктуру для дальнейших атак. Обнаружение основывается на событиях остановки служб, таких как Service Control Manager (Event ID 7036) в Windows. Остановка ключевых служб может привести к отказу в обслуживании, снижению уровня безопасности системы или потере данных, что делает своевременное обнаружение и реагирование критически важными для защиты инфраструктуры. В случае срабатывания правила необходимо запросить информацию у ответственного за узел о причинах активности. Если подтверждения легитимности не последовало, рекомендуется ограничить доступ к узлу, с которого произошли подозрительные действия, и инициировать внутреннее расследование.	• Impact (TA0040) • Service Stop (T1489)

ID правила	Название правила	Описание	Тактики и техники
RV-D-917	Сжатие дамп-файлов средствами 7-Zip	Атакующие могут пользоваться различными утилитами для сжатия или шифрования данных перед их эксфильтрацией. Некоторые сторонние утилиты могут быть предустановлены в ОС, например `tar` в Linux и macOS или `zip` в Windows. Также могут использоваться сторонние утилиты, такие как 7-Zip, WinRAR и WinZip, для выполнения аналогичных действий. Данное правило обнаруживает использование 7-Zip для сжатия файла с расширениями ".dmp" и ".dump", что может быть одним из этапов процесса эксфильтрации дампов. В случае срабатывания рекомендуется уточнить у пользователя, который инициировал активность, является ли она легитимной. Если подтверждения нет, рекомендуется начать расследование, проверив активность связанных процессов, сетевых подключений и другие возможные признаки утечки данных.	• Collection (TA0009) • Archive Collected Data (T1560) • Archive via Utility (T1560.001)
RV-D-918	Сжатие дамп-файлов средствами WinRAR	Обнаруживает использование WinRAR для сжатия файлов с расширением ".dmp" или ".dump", что может быть одним из этапов процесса эксфильтрации дампов.	• Collection (TA0009) • Archive Collected Data (T1560) • Archive via Utility (T1560.001)
RV-D-948	Загрузка файлов с веб-ресурсов стандартными утилитами	В качестве развития своего присутствия в системе, атакующие могут доставлять файлы с удаленных веб-ресурсов. Как правило, источником выступают C2-сервера, которые по веб-протоколам передачи данных направляют полезную нагрузку на хосты жертвы. Чтобы избежать обнаружения, атакующие, как правило, используют LOLBINS для загрузки файлов с удаленных веб-ресурсов.	• Command and Control (TA0011) • Ingress Tool Transfer (T1105)

ID правила	Название правила	Описание	Тактики и техники
RV-D-953	Использование Replace.exe	Правило обнаруживает использование файла Replace.exe, который может быть использован для замены файла другим файлом. Replace.exe — это утилита командной строки Windows, которая используется для замены одних файлов другими. Флаг -a, как правило, означает автоматическую замену файлов без запроса подтверждения пользователя. Опасности использования replace.exe с флагом -a могут быть связаны с потенциальной потерей данных или перезаписью важных файлов системы. При возникновении данной активности необходимо опросить владельца учетной записи (УЗ) инициатора на предмет совершаемых действий. В случае если подтвердить легитимность не удалось, то следует заблокировать УЗ инициатора активности.	• Command and Control (TA0011) • Ingress Tool Transfer (T1105)
RV-D-955	Попытка дампа процесса LSASS с помощью Procdump	Атакующий может попытаться получить данные других учетных записей с помощью дампа системного процесса LSASS (Local Security Authority Subsystem Service), который хранит в своей памяти учетные данные авторизованных пользователей на узле. Одним из способов дампа учетных записей является использование утилиты Procdump, входящей в набор Microsoft Sysinternals. Данная утилита позволяет делать дампы процессов. Правило обнаруживает попытку дампа процесса LSASS с помощью мониторинга событий запуска команд, относящихся к синтаксису утилиты Procdump. Правило не свидетельствует о фактическом удачном дампе, оно только указывает на попытку его получения.	• Credential Access (TA0006) • OS Credential Dumping (T1003) • LSASS Memory (T1003.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-956	Получение информации о службе RDP через sc.exe	Обнаруживает перечисление и запрос чувствительных служб в системе с использованием sc.exe. Атакующие часто пытаются перечислить службы, запущенные в системе, для выявления потенциальных векторов атак. При возникновении данной активности необходимо опросить владельца учетной записи (УЗ) инициатора на предмет совершаемых действий. В случае если подтвердить легитимность не удалось, то следует заблокировать УЗ инициатора активности.	• Credential Access (TA0006) • OS Credential Dumping (T1003)
RV-D-958	Захват учетных данных с помощью Rpcping.exe	Атакующие используют инструмент Rpcping.exe для отправки тестового RPC-соединения на целевой сервер (-s) и принудительной отправки NTLM-хэша в процессе. Этот метод позволяет им захватывать учетные данные, такие как NTLM-хэши, которые затем могут быть использованы для атаки методом "Pass the Hash" или другими способами, использующими скомпрометированные учетные данные. Обнаружение подобного использования Rpcping.exe является важным аспектом обеспечения безопасности системы и помогает предотвратить возможные атаки на учетные данные.	• Credential Access (TA0006) • OS Credential Dumping (T1003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-960	Снэпшот базы данных AD средствами ADExplorer	Обнаруживает выполнение программы Sysinternals ADExplorer с флагом "-snapshot" для сохранения локальной копии базы данных активного каталога в подозрительный каталог. Атакующие используют ADExplorer для снятия "снимка" AD с целью последующего анализа в оффлайн-режиме. Это позволяет им провести разведку структуры домена, учетных записей, групп и отношений доверия без непрерывного взаимодействия с контроллером домена, что снижает шансы на обнаружение. При возникновении данной активности необходимо опросить владельца учетной записи (УЗ) инициатора на предмет совершаемых действий. В случае если подтвердить легитимность не удалось, то следует заблокировать УЗ инициатора активности.	• Credential Access (TA0006) • Unsecured Credentials (T1552) • Credentials In Files (T1552.001) • Bash History (T1552.003)
RV-D-1022	Отключение или модификация Defender Firewall	Атакующие могут отключать или модифицировать системный firewall, чтобы обойти средства контроля, ограничивающие использование сети. Изменения могут включать отключение всего механизма или же добавление, удаление, изменение отдельных правил. Правило обнаруживает изменение значений ключей реестра, которые указывают на отключение Windows Defender Firewall.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify System Firewall (T1562.004)
RV-D-1023	Отключение сбора событий EventLog через реестр	Правило обнаруживает изменение значений или ключей реестра, которые указывают на отключение сбора событий EventLog, изменение места сохранения логов системы или изменение параметров автозапуска EventLog.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable Windows Event Logging (T1562.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1024	Отключение снапшотов томов	Данное правило направлено на детектирование команд по отключению снапшотов томов. Это позволит отключить диагностику службы теневого копирования томов. Данная активность может быть началом атаки по шифрованию данных, отсутствие резервных копий не даст откатиться к предыдущим версиям томов.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)
RV-D-1025	Защита от записи для хранилища отключена	Данное правило детектирует изменения реестра, при которых отключается защита от записи для устройств хранения данных. Данный метод часто используется программами-вымогателями, что может быть началом более масштабной атаки.	• Defense Evasion (TA0005) • Impair Defenses (T1562)
RV-D-1076	Закрепление через ключ ReflectDebugger утилиты WerFault	Правило обнаруживает изменение значения реестра ReflectDebugger утилиты WerFault. Атакующий может использовать эту технику для закрепления в системе. В значение ключа ReflectDebugger записывается путь к исполняемому файлу, который будет запускаться при вызове `werfault.exe -pr <любое_значение>`. Такая техника позволяет обойти традиционные механизмы автозапуска, так как задействует малоизвестную функциональность системы. Это правило выявляет попытки установки подобного механизма закрепления, отслеживая изменения ключа реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Hangs\ReflectDebugger` либо наличие значений с именем ReflectDebugger в указанном пути.	• Persistence (TA0003) • Defense Evasion (TA0005) • Masquerading (T1036) • Rename Legitimate Utilities (T1036.003) • Modify Registry (T1112) • Event Triggered Execution (T1546)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1077	Изменение критичных параметров сервиса	Для закрепления или повышения привилегий в системе атакующий может использовать сервисы. Все сервисы хранятся в реестре по пути `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`. При внесении каких-либо изменений в сервис как стандартным путем через services.msc, sc.exe и другие, так и нестандартным путем, например, редактированием реестра через утилиту reg, это будет отражаться в изменениях в соответствующих ключах в реестре. У сервисов существует два критичных параметра с названиями ключей ServiceDll, FailureCommand, которые могут использовать атакующие. Значение ServiceDll используется для изменения пути к исполняемому библиотеке сервиса. Значение FailureCommand предназначено для исполнения файла или команды при ошибке в работе сервиса, в том числе, преднамеренной. Данный метод является более скрытным, чем изменение исполняемого файла сервиса. В данном правиле отслеживаются любые изменения данных параметров.	• Execution (TA0002) • Persistence (TA0003) • Privilege Escalation (TA0004) • Defense Evasion (TA0005) • System Services (T1569) • Service Execution (T1569.002) • Hijack Execution Flow (T1574) • Services Registry Permissions Weakness (T1574.011)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1081	Изменение пути к исполняемому файлу в сервисе	Для закрепления или повышения привилегий в системе атакующий может использовать сервисы. Все сервисы хранятся в реестре по пути `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`. При внесении каких-либо изменений в сервис как стандартным путем через services.msc, sc.exe и другие, так и нестандартным путем, например, при редактировании реестра через утилиты reg, regedit.exe, powershell и другие, это будет отражаться в изменениях в соответствующих ключах в реестре. У сервисов существует критичный параметр с названием ключа ImagePath. Данный ключ предполагает указание команды или пути к исполняемому файлу сервиса. Редактирование напрямую этого ключа позволяет атакующему изменить путь к исполняемому файлу сервиса, тем самым при старте сервиса запустится указанный файл или исполнится указанная команда. Правило не отслеживает изменение пути сервиса от утилит, использующих API сервисов. В данном случае все изменения происходят от процесса services.exe. Так как большинство легитимных изменений происходят от имени процесса services.exe, то их отслеживание будет создавать много ложных срабатываний. Также правило содержит исключение для процесса TiWorker.exe. Windows Update TrustedInstaller Worker Process — системный процесс, отвечающий за установку обновлений операционной системы. В исключение добавлены процессы с именами procexp/procexp64.exe и procmon/procmon64.exe. Это утилиты из набора Sysinternals, при их запуске с правами администратора они создают сервис и прописывают в нем путь к своему исполняемому драйверу.	• Execution (TA0002) • Persistence (TA0003) • Privilege Escalation (TA0004) • Defense Evasion (TA0005) • System Services (T1569) • Service Execution (T1569.002) • Hijack Execution Flow (T1574) • Executable Installer File Permissions Weakness (T1574.005) • Services File Permissions Weakness (T1574.010) • Services Registry Permissions Weakness (T1574.011)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1082	Эксплуатация сценариев входа в систему	Атакующие могут использовать сценарии входа в систему Windows, автоматически выполняемые при инициализации входа в систему, для закрепления. Windows позволяет запускать сценарии входа в систему каждый раз, когда определенный пользователь или группа пользователей входят в систему. Это делается путем добавления пути к ветке реестра `HKCU\Environment` параметра UserInitMprLogonScript со значением файла сценария (.bat).	• Persistence (TA0003) • Privilege Escalation (TA0004) • Boot or Logon Initialization Scripts (T1037) • Logon Script (Windows) (T1037.001)
RV-D-1083	Эксплуатация Active Setup в реестре	Active Setup — это механизм Windows, который используется для запуска программ при входе пользователя в систему. Атакующие часто используют Active Setup в Windows для закрепления в системе, добавляя ключ реестра, который запускает программу при входе пользователя в систему. Active Setup можно использовать, создав ключ в разделе `HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\` и установив вредоносный путь StubPath. Этот путь указывает на программу, которая будет запускаться при входе пользователя в компьютер. Выполненная от имени пользователя, она будет иметь уровень разрешений, связанный с этой учетной записью.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Boot or Logon Autostart Execution (T1547) • Active Setup (T1547.014)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1084	Закрепление в системе через изменение пакетов проверки подлинности	Пакеты аутентификации в Windows имеют решающее значение для управления операционной системой, процессами входа в систему и протоколами безопасности. Эти пакеты, обычно в виде динамических библиотек (DLL), загружаются процессом Local Security Authority (LSA) при запуске системы. Их основная роль заключается в облегчении различных процессов входа в систему и реализации протоколов безопасности, что делает их неотъемлемым компонентом системы аутентификации в Windows. Указанная активность может свидетельствовать о попытках ВПО закрепиться в системе.	• Persistence (TA0003) • Boot or Logon Autostart Execution (T1547) • Authentication Package (T1547.002) • Modify Authentication Process (T1556) • Password Filter DLL (T1556.002)
RV-D-1085	Эксплуатация драйверов LSASS в реестре	Драйверы LSASS в Windows — это легитимные драйверы, загружаемые подсистемой Local Security Authority для управления различными политиками безопасности. Атакующие могут получить постоянный доступ к скомпрометированным системам, изменив или добавив драйверы, связанные с LSASS. Данную технику использует бэкдор Wingbird, который позволяет подгружать вредоносную .dll процессом LSASS.	• Persistence (TA0003) • Boot or Logon Autostart Execution (T1547) • LSASS Driver (T1547.008)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1086	Эксплуатация Port Monitors в реестре	Атакующие могут использовать мониторы портов для запуска вредоносной DLL во время загрузки системы для закрепления или повышения привилегий. Монитор портов можно установить с помощью API-вызова AddMonitor, чтобы задать DLL для загрузки при старте. Данная DLL может быть расположена в `C:\Windows\System32` и будет загружена службой печати, `spoolsv.exe`, при загрузке, что позволяет запускаться потенциальному ВПО с разрешениями уровня SYSTEM. Также можно загрузить произвольную DLL, прописав полный путь для этой DLL в `HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors`, создав собственный ключ.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Boot or Logon Autostart Execution (T1547) • Port Monitors (T1547.010)
RV-D-1087	Закрепление в системе через эксплуатацию Print Processors	Служба очереди печати (spoolsv.exe) работает за счет dll-библиотек, которые загружаются во время загрузки ПК, и атакующие ими злоупотребляют, выполняя свои dll во время загрузки. Одним из способов добавления dll является изменение определенных веток реестра с указанием нужной dll. Схожая техника реализована в PrintNightmare, где при помощи реестра происходит создание принтера, который указывает на вредоносную dll.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Boot or Logon Autostart Execution (T1547) • Print Processors (T1547.012)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1088	Закрепление в системе посредством эксплуатации SSP	Security Support Providers (SSPs) — это динамические библиотеки, которые предоставляют сервисы аутентификации и безопасности, обычно загружаемые процессом LSA. Атакующие могут злоупотреблять поставщиками поддержки безопасности (SSP) для выполнения DLL-файлов при загрузке системы. DLL-файлы Windows SSP загружаются в процесс Локального центра безопасности (LSA) при запуске системы. После загрузки в LSA DLL-файлы SSP имеют доступ к зашифрованным и открытым паролям, которые хранятся в Windows, например, к паролю домена.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Boot or Logon Autostart Execution (T1547) • Security Support Provider (T1547.005)
RV-D-1089	Создания/изменения ключей поставщиков времени в реестре	Атакующие могут злоупотреблять поставщиками времени для запуска вредоносных библиотек DLL при загрузке системы. Служба времени Windows (W32Time) обеспечивает синхронизацию времени между доменами и внутри них. Поставщики времени W32Time отвечают за получение временных меток из аппаратных / сетевых ресурсов и вывод этих значений другим сетевым клиентам. Атакующие также могут злоупотреблять этой архитектурой для закрепления в системе, в частности, путем регистрации и включения вредоносной библиотеки DLL в качестве поставщика времени.	• Persistence (TA0003) • Boot or Logon Autostart Execution (T1547) • Time Providers (T1547.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1090	Закрепление через изменение параметров Winlogon	Атакующие могут использовать функции Winlogon для выполнения библиотек DLL и/или исполняемых файлов при входе пользователя в систему для закрепления в инфраструктуре. Модификации этих разделов реестра могут привести к тому, что Winlogon загрузит и выполнит вредоносные библиотеки DLL и/или исполняемые файлы. Указанная активность может свидетельствовать о попытках ВПО закрепиться в системе.	• Persistence (TA0003) • Boot or Logon Autostart Execution (T1547) • Winlogon Helper DLL (T1547.004)
RV-D-1113	Удаленный запуск процесса с помощью DCOM объекта MMC20.Application	Детектируется удаленный запуск процессов с помощью DCOM (dcomexec из Impacket). После получения первоначального доступа атакующий начинает горизонтальное перемещение по корпоративной сети жертвы. Одной из популярных утилит для этих целей является DCOMExec из пакета Impacket с помощью объекта MMC20.Application. MMC20.Application — это COM-объект, позволяющий создавать сценарии для компонентов оснастки MMC. DCOMExec использует метод с именем ExecuteShellCommand в Document.ActiveView для удаленного выполнения команд.	• Lateral Movement (TA0008) • Remote Services (T1021) • Distributed Component Object Model (T1021.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1117	Удаленная эксплуатация DCOM объекта ShellWindows	Данное правило обнаруживает удаленный запуск процессов с помощью DCOM (dcomexec из Impacket). После получения первоначального доступа атакующий начинает горизонтальное перемещение по корпоративной сети жертвы. Одной из популярных утилит для этих целей является DCOMExec из пакета Impacket с помощью объектов ShellWindows или ShellBrowserWindow. Этот вид DCOM объектов может эксплуатироваться только на ОС до Windows Server 2012, на более поздних версиях ОС Windows вендор закрыл возможность эксплуатации данного DCOM объекта. Данные COM-объекты имеют возможность запуска произвольного исполняемого файла из-под родительского процесса explorer.exe.	• Lateral Movement (TA0008) • Remote Services (T1021) • Distributed Component Object Model (T1021.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1124	Использование вредоносных утилит	Для выполнения вредоносных действий атакующий может использовать утилиты и инструменты, загруженные на хост. Правило обнаруживает использование таких инструментов по их имени, оригинальному имени файла или метаданным.	• Execution (TA0002) • Defense Evasion (TA0005) • Exfiltration (TA0010) • Direct Volume Access (T1006) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Windows Command Shell (T1059.003) • Exfiltration Over Web Service (T1567) • Exfiltration to Cloud Storage (T1567.002)
RV-D-1126	Подозрительный доступ к облачным менеджерам секретов	Атакующие могут получить учетные данные из облачных хранилищ секретов, таких как AWS Secrets Manager, GCP Secret Manager, Azure Key Vault и Terraform Vault. Менеджеры секретов поддерживают безопасное централизованное управление паролями, ключами API и другими учетными данными. При использовании менеджеров секретов облачные сервисы могут динамически получать учетные данные через API-запросы, а не обращаться к секретам, незащищенно хранящимся в текстовых файлах или переменных окружения. Атакующие могут использовать полученные учетные данные для перемещения внутри периметра сети и доступа к конфиденциальной информации.	• Credential Access (TA0006) • Credentials from Password Stores (T1555) • Cloud Secrets Management Stores (T1555.006)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1139	Изучение конфигурации локальной системы	После получения первоначального доступа к цели атакующие в рамках своей активности по изучению локального окружения могут производить разведку установленной операционной системы, программного и аппаратного обеспечения и т.д. Получение данной информации позволяет атакующему подготовить ресурсы для эксплуатации уязвимых систем. Например, к системным утилитам, которые позволяют производить изучение системы, могут относиться `systeminfo` или `driverquery`. При срабатывании данного правила требуется узнать у пользователя, ответственного за УЗ, о выполнении данных команд, поскольку активность может быть легитимной, вызванной работами администратора. Если активность подтвердить не удается, следует проанализировать дельту активности на предмет подозрительных действий и заблокировать УЗ инициатора активности.	• Discovery (TA0007) • Application Window Discovery (T1010) • Windows Management Instrumentation (T1047) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Windows Command Shell (T1059.003) • System Information Discovery (T1082) • Peripheral Device Discovery (T1120) • Gather Victim Host Information (T1592) • Client Configurations (T1592.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1144	Уничтожение информации на диске в Windows	Атакующие могут использовать методы удаления или порчи данных, чтобы нанести существенный ущерб компании. Это правило направлено на детектирование активности, которая приводит к безвозвратному удалению или искажению данных до состояния, при котором их восстановление становится крайне сложным или невозможным. Рассмотрены стандартные инструменты Windows, которые могут быть использованы для подобных действий.	• Impact (TA0040) • Disk Wipe (T1561) • Disk Content Wipe (T1561.001) • Disk Structure Wipe (T1561.002)
RV-D-1145	Запуск скрипта из временной директории	Атакующий может использовать временные папки и директории для скрытой загрузки и исполнения вредоносных скриптов. Данное правило обнаруживает запуск скриптов из временной директории.	• Execution (TA0002) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Windows Command Shell (T1059.003) • Visual Basic (T1059.005) • Python (T1059.006) • JavaScript (T1059.007)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1157	Обнаружено использование службы BITS Jobs	Атакующие для скрытой загрузки файлов или выполнения кода могут использовать службу BITS Jobs (Windows Background Intelligent Transfer). BITS Jobs — это служба с асинхронной передачей файлов с низкой пропускной способностью, которая обычно используется системой или программами для фоновой загрузки файлов, используя доступную полосу пропускания и не прерывая работу других сетевых приложений, для обновлений и других необходимых для системы файлов. Данное правило обнаруживает использование службы BITS Jobs с характерными ключами и командами в интерактивной оболочке cmd и PowerShell.	• Persistence (TA0003) • Defense Evasion (TA0005) • BITS Jobs (T1197)
RV-D-1159	Обнаружение эксплуатации DDE через Office	Атакующие могут воспользоваться динамическим обменом данными (DDE) в Windows для выполнения произвольных команд. DDE — это клиент-серверный протокол, обеспечивающий одноразовое или непрерывное межпроцессное взаимодействие между приложениями. Атакующие могут внедрять команды DDE в документы Microsoft Office как напрямую, так и через встроенные файлы, чтобы затем использовать их для выполнения кода при открытии пользователем вложений в фишинговых письмах или при обращении к веб-контенту, тем самым обходя использование макросов Visual Basic for Applications (VBA). Данное правило отслеживает ситуации, когда офисный процесс (Word или Excel) инициирует запуск процесса командной строки (cmd) или PowerShell.exe, что может быть подозрительным.	• Execution (TA0002) • Inter-Process Communication (T1559) • Dynamic Data Exchange (T1559.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1164	Запуск файла без расширения	Атакующий может скрыть отображаемый тип файла с помощью удаления его расширения. В таком случае файл можно визуально замаскировать под папку, что может привести к случайному запуску вредоносного кода пользователем или обходу средств защиты, которые основываются на проверке файлов по их расширению.	• Execution (TA0002) • Defense Evasion (TA0005) • Obfuscated Files or Information (T1027) • Masquerading (T1036) • Masquerade File Type (T1036.008) • Command and Scripting Interpreter (T1059) • Hide Artifacts (T1564) • Hidden Files and Directories (T1564.001)
RV-D-1169	Журнал событий Windows был очищен	В целях сокрытия следов присутствия в инфраструктуре и затруднения последующего расследования атакующий может очистить журналы событий. Например, для этого могут использоваться встроенные утилиты или стороннее ПО. Обнаружить очистку журнала Security можно по событиям с ID 1102, очистку журналов System и Application — с помощью событий с ID 104. Событие сгенерируется как при удалении журналов через командную строку, так и через графический интерфейс.	• Defense Evasion (TA0005) • Indicator Removal (T1070) • Clear Windows Event Logs (T1070.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1170	Добавление исполняемого файла к профилю PowerShell	Атакующие могут использовать профили PowerShell для выполнения вредоносного содержимого при запуске PowerShell. Профиль PowerShell — это скрипт, который запускается при старте PowerShell. PowerShell поддерживает несколько профилей в зависимости от пользователя или хост-программы. Атакующие могут изменять эти профили, чтобы включать произвольные исполняемые файлы и обеспечить тем самым закрепление. Каждый раз, когда пользователь открывает сеанс PowerShell, файл будет выполняться, если не будет использован флаг -NoProfile при его запуске.	• Persistence (TA0003) • Event Triggered Execution (T1546) • PowerShell Profile (T1546.013)
RV-D-1174	Запуск файла с двойным расширением	Атакующий может использовать возможности Windows для сокрытия истинного расширения файла. По умолчанию в системе отображается только первое расширение, указанное после первой точки в имени файла. Если в имени имеется две точки и более, то расширение файла, которое будет восприниматься системой как актуальное, будет находиться после последней точки. Техника заключается в том, чтобы заставить пользователя запустить безопасный, по его мнению, файл, за которым может скрываться вредоносное ПО.	• Execution (TA0002) • Defense Evasion (TA0005) • Masquerading (T1036) • Double File Extension (T1036.007) • User Execution (T1204) • Malicious File (T1204.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1176	Изменение конфигурации загрузки безопасного режима	Атакующие могут добавить вредоносные приложения в минимальный набор служб, запускаемых в безопасном режиме, изменяя определенные значения реестра. Этот метод обеспечивает скрытное выполнение вредоносного кода при минимальных возможностях обнаружения, так как в безопасном режиме отключены большинство защитных механизмов, включая антивирусные программы и системы мониторинга. Правило отслеживает несанкционированные изменения в реестре, касающиеся конфигураций безопасного режима и автозагрузки на системах Windows.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Safe Mode Boot (T1562.009)
RV-D-1177	Выполнение манипуляций над учетной записью с помощью стороннего ПО	После попадания в корпоративную сеть атакующий может попробовать закрепиться в системе через создание новой учетной записи. Данные действия избавляют от необходимости использовать уже скомпрометированные учетные записи или поддержание шелла для вторичного доступа в систему. Создание\изменение\удаление учетных записей является стандартной процедурой при работе администратора, однако для этих действий он должен использовать строго регламентированное ПО. Использование ПО, не соответствующее этому регламенту, выглядит аномальным. Данное правило выявляет использование сторонних утилит для выполнения каких-либо действий над учетными записями.	• Persistence (TA0003) • Account Manipulation (T1098) • Create Account (T1136) • Local Account (T1136.001) • Domain Account (T1136.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1187	Обнаружен запуск XSL скрипта	XSL — это файлы расширяемого языка таблиц стилей, которые обычно используются для описания обработки и рендеринга данных в файлах XML. Для поддержки сложных операций стандарт XSL включает поддержку встроенных сценариев на различных языках. Атакующие могут встраивать вредоносные скрипты в XSL файлы и запускать их с помощью встроенной утилиты wmic.exe или msxsl.exe, обычно загружаемой отдельно, что позволяет обходить ограничение запуска определенного ПО в системе.	• Defense Evasion (TA0005) • XSL Script Processing (T1220)
RV-D-1190	Закрепление через Shim	Атакующие используют специальные файлы, называемые базами данных совместимости (SDB), для запуска вредоносного кода при выполнении определенных приложений. SDB — это файлы, которые позволяют исправлять проблемы совместимости приложений с новыми версиями Windows без изменения исходного кода. Атакующие могут создавать свои собственные SDB, содержащие исправления, которые могут повышать привилегии, обходить контроль учетных записей пользователей, внедрять DLL в процессы. Затем атакующие могут устанавливать свои SDB с помощью утилиты sdbinst.exe или вручную через реестр. При запуске приложения, для которого установлена SDB, Windows будет автоматически применять исправления из SDB, тем самым запуская вредоносный код. Правило нацелено на выявление добавления полезной нагрузки через реестр или при помощи sdbinst в реестр базы данных совместимости (SDB).	• Persistence (TA0003) • Event Triggered Execution (T1546) • Application Shimming (T1546.011)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1192	Отключение службы Windows EventLog	Правило обнаруживает команды, которые могут указывать на отключение сбора событий или отключение службы Windows EventLog.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable Windows Event Logging (T1562.002)
RV-D-1198	Использование утилиты gs-netcat из набора инструментов gsocket	Утилита gs-netcat позволяет устанавливать безопасное TCP-соединение между двумя и более хостами, используя глобальную сеть ретрансляции сокетов (GSRN). Инструмент используется, когда у хостов нет сетевой связности, и активно используется атакующими. В возможности инструмента входит трансляция сетевых подключений, передача данных, доступ к интерактивному шеллу. Правило детектирует создание процесса `gs-netdevice_event_category`, а также подключение к серверу управления.	• Command and Control (TA0011) • Proxy (T1090) • External Proxy (T1090.002) • Protocol Tunneling (T1572)
RV-D-1199	Туннелирование с использованием ngrok	ngrok позволяет организовать подключение к удаленному хосту из сети Интернет без статического белого IP-адреса. Правило детектирует параметры, с которыми создается процесс ngrok, события создания и изменения файла конфигурации, а также сетевые подключения.	• Command and Control (TA0011) • Proxy (T1090) • External Proxy (T1090.002) • Web Service (T1102) • Protocol Tunneling (T1572)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1200	RDP подключение с использованием туннеля	Атакующие часто используют RDP для управления скомпрометированным хостом. При отсутствии у них прямого сетевого доступа они могут организовать туннелируемое соединение, например, с использованием ngrok или gs-netcat. Данное правило отслеживает подключение по RDP к хосту при помощи создания туннеля.	• Command and Control (TA0011) • Protocol Tunneling (T1572)
RV-D-1203	Загрузка dll-библиотеки средствами mavinject	Данное правило направлено на обнаружение подозрительных действий, связанных с использованием системного компонента mavinject.exe (Microsoft Application Virtualization Injector) для внедрения вредоносного кода в доверенные процессы с использованием параметров /INJECTRUNNING или /HMODULE. Эти параметры позволяют загружать вредоносные DLL в адресное пространство процессов или модифицировать их таблицы импорта. Такое поведение является аномальным для стандартных сценариев использования mavinject.exe и может указывать на попытку атакующего использовать легитимный инструмент для обхода защитных механизмов и выполнения вредоносных операций. Эксплуатация этой техники может привести к выполнению произвольного кода атакующим.	• Defense Evasion (TA0005) • System Binary Proxy Execution (T1218) • Mavinject (T1218.013)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1204	Эксплуатация утилиты GrimResource	GrimResource позволяет атакующему выполнять произвольный код в консоли управления Microsoft (mmc.exe) с минимальными предупреждениями системы безопасности, что подходит для получения начального доступа и обхода средств защиты. Добавляя ссылку на уязвимый ресурс APDS в соответствующий раздел StringTable созданного MSC-файла, атакующие могут выполнять произвольный javascript в контексте mmc.exe.	• Defense Evasion (TA0005) • System Binary Proxy Execution (T1218) • MMC (T1218.014)
RV-D-1210	Отключение ETW провайдера PowerShell	Правило обнаруживает изменение значений ключей реестра, которые указывают на отключение ETW провайдера PowerShell от сессии или использование команд системной утилиты logman. Эти действий позволяют отключить генерацию событий PowerShell_Operational.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Indicator Blocking (T1562.006)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1212	Скачивание удаленного файла средствами hh.exe	Данное правило направлено на обнаружение подозрительных действий, связанных с использованием системного компонента hh.exe (Microsoft HTML Help Executable) для запуска удаленных файлов. Такое поведение является аномальным для стандартных сценариев использования hh.exe и может указывать на попытку атакующего использовать легитимный процесс для загрузки и выполнения кода с удаленного ресурса. Обнаружение выполняется при анализе командной строки процесса hh.exe, где в параметрах указывается URL или IP-адрес. Атака, основанная на запуске удаленных файлов через hh.exe, может быть частью более сложных сценариев компрометации, включая доставку вредоносного ПО, удаленное выполнение кода и эксфильтрацию данных. Использование доверенного системного процесса затрудняет обнаружение таких атак средствами традиционного мониторинга и защиты.	• Defense Evasion (TA0005) • Ingress Tool Transfer (T1105) • System Binary Proxy Execution (T1218) • Compiled HTML File (T1218.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1213	Создание подозрительного процесса от hh.exe	Данное правило направлено на обнаружение подозрительных действий, связанных с использованием системного компонента hh.exe (Microsoft HTML Help Executable) для выполнения вредоносного кода. Такое поведение является аномальным для стандартных сценариев использования hh.exe и может указывать на попытку атакующего использовать легитимный процесс для обхода защитных механизмов и выполнения вредоносных операций. Обнаружение выполняется при анализе событий создания процессов, где hh.exe выступает в роли родительского процесса. Чаще всего такие события связаны с запуском специально подготовленных CHM-файлов (Compiled HTML Files), содержащих вредоносные команды или скрипты. Успешная эксплуатация этой техники может привести к загрузке и выполнению вредоносного ПО, сбору данных, эскалации привилегий или дальнейшему продвижению атакующего в инфраструктуре.	• Defense Evasion (TA0005) • System Binary Proxy Execution (T1218) • Compiled HTML File (T1218.001)
RV-D-1214	Ослабление защиты или мониторинга системы	Правило обнаруживает команды или изменения в реестре, которые могут указывать на ослабление защиты или мониторинга системы.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1215	Зафиксирована атака Golden Ticket	Атакующие, у которых есть хэш пароля учетной записи KRBTGT, могут подделывать билеты Kerberos, производя атаку, также известную как золотой билет. Золотые билеты позволяют атакующим генерировать билеты для любой учетной записи в Active Directory. Используя золотой билет, атакующие затем могут запрашивать билеты службы предоставления билетов (TGS), которые предоставляют доступ к определенным ресурсам. Золотые билеты требуют, чтобы атакующие взаимодействовали с Центром распространения ключей (KDC) для получения TGS. Служба KDC работает на всех контроллерах домена, которые являются частью домена Active Directory. KRBTGT является учетной записью сервиса Kerberos Key Distribution Center (KDC) и отвечает за шифрование и подпись всех заявок Kerberos. Правило направлено на использование в явном виде утилит mimikatz и Rubeus с параметрами, указывающими на атаку Golden Ticket.	• Credential Access (TA0006) • Steal or Forge Kerberos Tickets (T1558) • Golden Ticket (T1558.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1217	Удаление истории RDP подключений через реестр	В ветках реестра `HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default` и `HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers` содержится информация, полезная для восстановления хронологии RDP-подключений и анализа активности. Servers хранит список серверов (имена или IP) с настройками для каждого подключения. Default содержит общие настройки и данные последних сеансов. Эти ветки помогают изучить историю сеансов и выявить подозрительную активность. Поэтому атакующие могут стремиться удалить эти данные, чтобы скрыть свои следы. Данное правило нацелено на выявление попыток удалить историю RDP подключений, которая содержатся в реестре.	• Defense Evasion (TA0005) • Indicator Removal (T1070) • Clear Network Connection History and Configurations (T1070.007)
RV-D-1218	Удаленное подключение к узлу через туннелирование в VSCode	Правило срабатывает при установлении соединения с сервером для удаленного управления узлом с помощью функции редактора кода VSCode для использования туннелей — ключа "tunnel" в командной строке. Правило также обнаруживает запросы доменов Microsoft, такие, как tunnels.api.visualstudio.com и devtunnels.ms, которые нужны для первичной конфигурации сервера и запроса доступных кластеров, что указывает на создание туннеля.	• Execution (TA0002) • Command and Scripting Interpreter (T1059) • Software Extensions (T1176) • IDE Extensions (T1176.002) • User Execution (T1204) • Malicious Link (T1204.001) • Remote Access Tools (T1219) • IDE Tunneling (T1219.001) • Protocol Tunneling (T1572)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1223	Удаление временных RDP файлов в Windows	Удаление сетевых файлов, таких как RDP-кэш или файл Default.rdp, является одной из техник сокрытия активности атакующего в системе. Эти файлы могут содержать полезную информацию для расследования инцидентов, включая историю подключений, адреса хостов и другие данные, которые могут указать на компрометацию. Данное правило отслеживает попытки удалить временные файлы RDP через PowerShell или cmd и попытки стереть историю RDP подключений через реестр.	• Defense Evasion (TA0005) • Indicator Removal (T1070) • Clear Network Connection History and Configurations (T1070.007)
RV-D-1229	Добавление источника загрузки в Winget	Данное правило обнаруживает попытки добавления новых, потенциально небезопасных или непроверенных репозиториев в менеджер пакетов Windows (Winget) с помощью команды `winget source add`. По умолчанию Winget использует доверенный источник Microsoft Store, и добавление сторонних источников значительно повышает риски безопасности. Это может быть индикатором попытки атакующего установить вредоносное ПО, обойти политики контроля приложений или внедрить скомпрометированный пакет в систему.	• Command and Control (TA0011) • Ingress Tool Transfer (T1105)
RV-D-1231	Создание Self Extracting Package в подозрительном месте	Правило обнаруживает использование iexpress.exe для создания Self Extracting Package по файлам Self Extraction Directive (SED), расположенным в потенциально подозрительных каталогах (Temp, ProgramData, Tasks и др.). Атакующие могут использовать IExpress как LOLBin для упаковки и развертывания вредоносных исполняемых файлов в нестандартные пути, минуя базовые политики.	• Execution (TA0002) • System Binary Proxy Execution (T1218)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1232	Потенциальное выполнение скрипта через WScript/CScript	Правило детектирует запуск скриптов JS, VBS и WSF через интерпретаторы wscript.exe или cscript.exe из временных и пользовательских директорий, таких как Temp и AppData. Подобная активность характерна для работы дропперов и загрузчиков, которые используют запись в незащищенные каталоги для обхода базовых политик ограничения ПО. Мониторинг данных путей позволяет выявить выполнение вредоносного кода на этапе закрепления в системе.	• Execution (TA0002) • Command and Scripting Interpreter (T1059) • Visual Basic (T1059.005) • JavaScript (T1059.007)
RV-D-1233	Подозрительное выполнение Regasm/Regsvcs с нестандартным расширением	Regsvcs.exe и Regasm.exe — это легитимные утилиты Microsoft .NET Framework, используемые для регистрации .NET-сборок. Однако атакующие могут использовать эти утилиты (LOLBINs) для выполнения вредоносного кода, маскируя его под безобидные файлы с нестандартными расширениями — например, .jpg, .txt или .gif. Это правило выявляет попытки запуска Regsvcs или Regasm с параметрами, содержащими файлы с подозрительными расширениями, что может указывать на технику маскировки вредоносной нагрузки или попытку обхода защиты на этапе исполнения.	• Defense Evasion (TA0005) • System Binary Proxy Execution (T1218) • Regsvcs/Regasm (T1218.009)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1235	Разведка доменных трастов	Детектирует выполнение команд для выявления доверительных отношений (трастов) между доменами. Атакующие могут собирать информацию о доверительных отношениях, которая может быть использована для поиска путей бокового перемещения в многодоменных инфраструктурах или лесах Active Directory. Доверительные отношения позволяют пользователям доверенного домена получать доступ к ресурсам доверяющего домена. Полученная информация может помочь атакующему в проведении атак SID History Injection, Pass the Ticket и Kerberoasting.	• Reconnaissance (TA0043) • Execution (TA0002) • Discovery (TA0007) • Command and Scripting Interpreter (T1059) • Domain Trust Discovery (T1482) • Gather Victim Network Information (T1590) • Network Trust Dependencies (T1590.003)
RV-D-1236	Эксфильтрация данных через finger.exe	Атакующий может использовать встроенную утилиту finger.exe для эксфильтрации данных или установки связи с C2-серверами, обходя традиционные средства контроля и фильтрации. Утилита взаимодействует с удаленным сервером через протокол Finger (TCP/79), который редко применяется в легитимной деятельности. Правило выявляет запуск finger.exe с подозрительными аргументами, содержащими символ "@", в сочетании с сетевым подключением к порту 79.	• Command and Control (TA0011) • Exfiltration (TA0010) • Exfiltration Over Alternative Protocol (T1048) • Exfiltration Over Unencrypted Non-C2 Protocol (T1048.003) • Ingress Tool Transfer (T1105)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1238	Скачивание файла средствами MpCmpRun.EXE	Правило направлено на обнаружение использования Windows Defender MpCmdRun для скачивания файлов. MpCmdRun.exe — легитимная консольная утилита Microsoft Defender, предназначенная для управления антивирусом, обновления сигнатур и выполнения сервисных операций. Атакующие могут применять MpCmdRun.exe для доставки полезной нагрузки, обхода ограничений на загрузку файлов, маскировки сетевой активности под легитимную работу защитного ПО и снижения вероятности детектирования.	• Defense Evasion (TA0005) • Command and Control (TA0011) • Ingress Tool Transfer (T1105) • System Binary Proxy Execution (T1218)
RV-D-1240	Изменение атрибута для скрытия файла через PowerShell	Атакующие нередко используют сокрытие файлов и каталогов для обхода систем обнаружения. Большинство операционных систем поддерживают концепцию "скрытых" файлов, чтобы избежать их случайного изменения пользователями. Сокрытие файлов может быть частью более сложных атак, таких как внедрение вредоносного ПО, кража данных или обеспечение присутствия атакующих в системе. Данное правило отслеживает действия по сокрытию файлов путем изменения атрибута, отвечающего за их видимость, с использованием PowerShell.	• Defense Evasion (TA0005) • Hide Artifacts (T1564) • Hidden Files and Directories (T1564.001)
RV-D-1241	Запуск потенциально поддельного экземпляра hxtsr.exe	HxTsr.exe — это исполняемый файл Microsoft под названием Microsoft Outlook Communications. Он является частью приложений Outlook и обычно находится в подпапке WindowsApps каталога `C:\Program Files`. Любые экземпляры hxtsr.exe, расположенные вне этой папки, могут быть вредоносным ПО, маскирующимся под легитимный процесс.	• Defense Evasion (TA0005) • Masquerading (T1036)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1243	Запуск aspnet_compiler.exe для компиляции в нетипичной директории	Данное правило фиксирует использование утилиты aspnet_compiler.exe для компиляции кода, расположенного в нетипичных или временных директориях. Использование доверенного бинарного файла Microsoft для сборки и выполнения кода позволяет атакующим обходить политики ограничения запуска приложений и скрывать вредоносную активность под видом легитимных процессов .NET. Такая активность может свидетельствовать о попытках выполнения произвольного кода через технику side-loading или использование подписанных приложений в качестве проводников атаки.	• Defense Evasion (TA0005) • Trusted Developer Utilities Proxy Execution (T1127)
RV-D-1244	Атака Bad USB Windows	BadUSB — это тип атак, основанных на использовании скомпрометированных или специально модифицированных USB-устройств. Такие устройства внешне выглядят как обычные флеш-накопители или периферийные устройства, но содержат в себе микроконтроллеры, позволяющие имитировать действия клавиатуры или других HID-устройств (Human Interface Device). Это дает возможность атакующему выполнять произвольные команды на целевой системе без ведома пользователя. Уникальность BadUSB заключается в том, что они эксплуатируют доверие операционной системы к периферийным устройствам. Когда такое устройство подключается, система автоматически распознает его как легитимное HID-устройство и позволяет ему вводить команды, как если бы это делал пользователь с помощью клавиатуры.	• Initial Access (TA0001) • Execution (TA0002) • Replication Through Removable Media (T1091) • Communication Through Removable Media (T1092) • Hardware Additions (T1200) • Input Injection (T1674)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1245	Обнаружение компиляции исходного кода на Windows	Атакующие могут использовать доставку вредоносных файлов в виде исходного кода для обхода защитных механизмов, предназначенных для блокировки исполняемых файлов. Такие файлы требуют компиляции перед запуском, что обычно выполняется с помощью csc.exe, msbuild.exe, dotnet.exe, vbc.exe или gcc.exe. Данное правило позволяет выявлять подозрительные случаи компиляции исходного кода на целевой системе, которые могут свидетельствовать о попытках обхода защитных мер.	• Defense Evasion (TA0005) • Obfuscated Files or Information (T1027) • Compile After Delivery (T1027.004)
RV-D-1246	Создание обратного туннеля через ssh.exe	Правило предназначено для обнаружения использования ssh.exe с подозрительными параметрами, позволяющими создавать обратные SSH-туннели с помощью флага -R. Оно отслеживает попытки скрытого удаленного доступа, связывая выполнение команды с IP-адресом для обратного подключения. Правило помогает выявить атаки, использующие SSH для обхода средств защиты и продвижения по сети.	• Command and Control (TA0011) • Protocol Tunneling (T1572)
RV-D-1248	Удаленная отладка браузера Windows	Атакующие могут использовать легитимный функционал отладки браузера для перехвата сеанса пользователя. Данные действия позволяют получить доступ к ресурсам и информации в браузере от имени жертвы.	• Collection (TA0009) • Browser Session Hijacking (T1185) • Steal Web Session Cookie (T1539)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1249	Подключение к SMB папке по протоколу QUIC	Правило обнаруживает подключение к общей SMB-папке через протокол QUIC. Такой тип активности может быть легитимным, например, при использовании скриптов или инструментов администрирования, однако также может указывать на подозрительную активность — исследование сетевых ресурсов, несанкционированный доступ или обход стандартных политик безопасности.	• Lateral Movement (TA0008) • Lateral Tool Transfer (T1570)
RV-D-1250	Выполнение Sysinternals PsSuspend	Sysinternals PsSuspend — это утилита для управления состоянием процессов, позволяющая приостанавливать и возобновлять их выполнение на уровне ядра. Правило предназначено для выявления использования данной утилиты, которую атакующие могут применять для временного отключения системных или защитных компонентов в рамках техник закрепления или уклонения от обнаружения. Хотя PsSuspend является легитимным инструментом администрирования, его применение на пользовательских или критически важных системах без соответствующего контекста может свидетельствовать о подозрительной активности.	• Persistence (TA0003) • Discovery (TA0007) • Create or Modify System Process (T1543) • Windows Service (T1543.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1251	Сокрытие данных в атрибутах файлов NTFS	Атакующие могут скрывать вредоносные данные или бинарные файлы в метаданных атрибутов файлов, а не в самих файлах. Один из таких атрибутов — это ADS (Alternate Data Streams), который предназначен для хранения метаданных объекта в NTFS. Скрытие вредоносных данных в этом атрибуте позволяет обходить защитные механизмы, такие как инструменты для сканирования статических индикаторов и антивирусные программы. Данное правило направлено на выявление попыток извлечения данных из ADS с использованием команд PowerShell, а также на анализ событий Sysmon для обнаружения подозрительных операций с созданием ADS-потоков.	• Defense Evasion (TA0005) • Hide Artifacts (T1564) • NTFS File Attributes (T1564.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1253	Эксплуатация утилиты LaZagne	LaZagne — это инструмент с открытым исходным кодом, предназначенный для извлечения паролей и учетных данных, сохраненных на локальных компьютерах. Он способен находить пароли в популярном программном обеспечении, используя различные методы хранения (открытый текст, API, собственные алгоритмы, базы данных и т. д.). При срабатывании данного правила необходимо запросить у пользователя подтверждение легитимности его действий. Если действия не подтверждаются, следует изолировать хост, заблокировать учетную запись пользователя, провести очистку от вредоносного программного обеспечения и проверить сетевое окружение на предмет компрометации других систем.	• Credential Access (TA0006) • OS Credential Dumping (T1003) • LSASS Memory (T1003.001) • LSA Secrets (T1003.004) • Cached Domain Credentials (T1003.005) • Unsecured Credentials (T1552) • Credentials In Files (T1552.001) • Credentials from Password Stores (T1555) • Keychain (T1555.001) • Credentials from Web Browsers (T1555.003) • Windows Credential Manager (T1555.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1254	Использование утилиты Smbtakeover	Smbtakeover — это утилита для реализации техники по отвязке 445-го порта устройств Windows без загрузки драйверов, перезагрузки целевого устройства и без загрузки модулей в LSASS. Скрипт позволяет удаленно, используя WMI, "освободить" 445-й порт от прослушивания, что в дальнейшем может использоваться для relay-атак либо перенаправления трафика на Responder для получения NTLM-хешей.	• Execution (TA0002) • Credential Access (TA0006) • Lateral Movement (TA0008) • Remote Services (T1021) • SMB/Windows Admin Shares (T1021.002) • Windows Management Instrumentation (T1047) • Adversary-in-the-Middle (T1557) • LLMNR/NBT-NS Poisoning and SMB Relay (T1557.001)
RV-D-1255	Скрытие файла через attrib.exe	Атакующие часто прибегают к сокрытию файлов и каталогов для обхода средств обнаружения. В большинстве операционных систем предусмотрен механизм "скрытых" файлов, предназначенный для их защиты от случайного изменения пользователями. Однако скрытие файлов может использоваться и в рамках более сложных сценариев, включая распространение вредоносного программного обеспечения, несанкционированный доступ к данным или закрепление присутствия в системе. Данное правило фиксирует попытки изменения видимости файлов за счет установки соответствующего атрибута с использованием утилиты attrib.exe.	• Defense Evasion (TA0005) • Hide Artifacts (T1564) • Hidden Files and Directories (T1564.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1256	Использование инструмента SharpMove	Правило фиксирует запуск хакерской утилиты SharpMove, которая позволяет на удаленном компьютере создавать запланированные задачи, выполнять "SCM"-запросы, запускать VBScript с использованием WMI и выполнять другие различные действия.	• Lateral Movement (TA0008) • Remote Services (T1021) • SMB/Windows Admin Shares (T1021.002)
RV-D-1258	Перехват RDP соединения	Данное правило направлено на детектирование атаки RDP Hijacking, при которой атакующий может получить несанкционированный доступ к активным сеансам удаленного рабочего стола (RDP) без ведома пользователя. Атака осуществляется путем подключения к сеансу с использованием команд mstsc или tscon, что позволяет атакующему перехватить управление и выполнять действия от имени легитимного пользователя. Детектирование срабатывает при обнаружении попыток использования shadow-соединений или переключений сеансов, что позволяет своевременно выявить возможное злоупотребление административными привилегиями. Успешная эксплуатация может привести к компрометации учетных данных, нарушению конфиденциальности данных и несанкционированному выполнению действий от имени пользователя.	• Lateral Movement (TA0008) • Remote Service Session Hijacking (T1563) • RDP Hijacking (T1563.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1259	Установка удаленной сессии при помощи WMI	Данное правило детектирует установку удаленной сессии при помощи WMI. Существует два протокола удаленного подключения через WMI — DCOM и WinRM. Данное правило обнаруживает оба вида указанных ранее удаленных подключений. Основное отличие заключается в том, что для протокола DCOM пространством имен, к которому выполняется подключение, является стандартное пространство cimv2, а в случае использования WinRM — пространство interop. Отследить, откуда было совершено подключение, можно по смежному событию 4624 по LogonID инициатора активности. Оба вида данной активности являются аномальными и могут свидетельствовать о попытках атакующего удаленно подключиться к хосту при помощи WMI.	• Lateral Movement (TA0008) • Windows Management Instrumentation (T1047)
RV-D-1260	Использование утилит для создания снимков экрана	Атакующие могут делать снимки экрана для сохранения информации во время проведения атаки. Снимки экрана могут содержать конфиденциальные документы, данные аутентификации, информацию для проведения платежных операций и иную конфиденциальную информацию. Информация со снимков может помочь атакующему сформировать вектор для дальнейшего распространения.	• Collection (TA0009) • Screen Capture (T1113)
RV-D-1261	Извлечение содержимого буфера в Windows	Атакующие могут использовать командлет PowerShell Get-Clipboard и утилиты nirsrc_process_cmdline, copyq для кражи данных из буфера обмена в системах Windows. Данное правило отслеживает попытки запуска этих инструментов с параметрами, указывающими на обращение к буферу обмена, что может свидетельствовать о попытках эксфильтрации данных.	• Collection (TA0009) • Clipboard Data (T1115)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1263	Отключение или модификация Windows Audit Log Policy	Для сокрытия своих действий в системе атакующий может отключить или изменить политику аудита. Правило обнаруживает команды и события, которые указывают на изменение или сброс политик локального аудита для логирования событий.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable Windows Event Logging (T1562.002)
RV-D-1264	Отключение ETW провайдера .NET	Правило обнаруживает изменение значений ключей реестра, которые указывают на отключение ETW-провайдера .NET от сессии или использование команды изменения окружения. Эти действия позволяют отключить генерацию событий, связанных с .NET.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Indicator Blocking (T1562.006)
RV-D-1266	Эксплуатация уязвимости VSCode CVE-2023-46944	Правило выявляет подозрительную цепочку выполнения процессов, при которой процесс Git запускает скрипт или команду, а его родительским процессом является Visual Studio Code. Активность может указывать на эксплуатацию уязвимости CVE-2023-46944, связанной с некорректной обработкой параметра fsmonitor в конфигурации Git-репозитория. В уязвимых версиях Visual Studio Code и некоторых расширениях (включая GitLens) открытие специально подготовленного репозитория может приводить к неявному выполнению произвольной команды, указанной в конфигурационном файле репозитория, без явного согласия пользователя. Эксплуатация возможна при открытии вредоносного репозитория в доверенном контексте (Workspace Trust) либо при использовании уязвимых версий компонентов и может привести к выполнению кода с правами пользователя, открывшего репозиторий.	• Execution (TA0002) • Exploitation for Client Execution (T1203)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1267	Поиск процессов с уязвимыми модулями	Правило фиксирует попытки получения списка определенных DLL- или EXE-файлов с использованием утилиты tasklist.exe. Подобная активность может указывать на действия, направленные на выявление идентификатора процесса (PID), в котором используется указанная библиотека. В дальнейшем это может быть использовано для выполнения нежелательных операций, включая создание дампа памяти процесса или иные потенциально опасные действия.	• Credential Access (TA0006) • Discovery (TA0007) • OS Credential Dumping (T1003) • Process Discovery (T1057)
RV-D-1268	Запуск ssh.exe с подозрительными параметрами	Правило предназначено для обнаружения использования ssh.exe с параметрами, позволяющими выполнять команды в обход защитных механизмов. Атакующий может задействовать PermitLocalCommand, LocalCommand или ProxyCommand для выполнения команд без явного подключения к удаленному серверу, что может указывать на попытку скрытого выполнения действий, обхода системных политик или маскировки вредоносной активности.	• Defense Evasion (TA0005) • Indirect Command Execution (T1202) • System Binary Proxy Execution (T1218)
RV-D-1269	Разведка учетных записей	Правило нацелено на обнаружение массовой выгрузки списка аккаунтов и групп, как локальных, так и доменных. Атакующие могут попытаться получить список действительных учетных записей, имен пользователей или электронных адресов в системе или в скомпрометированной среде. Эта информация может помочь атакующим определить существующие учетные записи, что облегчает проведение дополнительных атак, таких как перебор паролей (brute-force), целевой фишинг (spear-phishing) или захват учетных записей (например, [Valid Accounts](T1078)).	• Discovery (TA0007) • Command and Scripting Interpreter (T1059) • Account Discovery (T1087) • Local Account (T1087.001) • Domain Account (T1087.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1272	Удаленное выполнение команд с помощью PsExec	Данное правило направлено на обнаружение подозрительных действий, связанных с использованием утилиты PsExec для удаленного выполнения команд через временные службы. Для детектирования используются события 4697 и 5145. Эксплуатация этой техники позволяет атакующему выполнять команды с повышенными привилегиями и может быть частью сложной атаки.	• Execution (TA0002) • Persistence (TA0003) • Lateral Movement (TA0008) • Remote Services (T1021) • SMB/Windows Admin Shares (T1021.002) • Create or Modify System Process (T1543) • Windows Service (T1543.003) • System Services (T1569) • Service Execution (T1569.002) • Lateral Tool Transfer (T1570)
RV-D-1273	Обнаружена попытка дампа NTDS.dit	Атакующие для получения данных всех учетных записей в домене могут попытаться получить дамп файла NTDS.dit. Данный файл содержит информацию обо всех пользователях в домене, включая хеши их паролей. Данное правило позволяет обнаружить использование команд, характерных для получения дампа NTDS.dit или создания теневой копии диска для последующего извлечения файла из нее.	• Defense Evasion (TA0005) • Credential Access (TA0006) • OS Credential Dumping (T1003) • NTDS (T1003.003) • Direct Volume Access (T1006)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1275	Получение учетных данных из реестра	Данное правило направлено на детектирование атак, связанных с извлечением конфиденциальной информации из реестра Windows. Атакующий может использовать стандартные утилиты, такие как reg.exe, wmic.exe или PowerShell, для поиска и извлечения ключей и значений, содержащих чувствительные данные, например, пароли (DefaultPassword, AutoAdminLogon) или параметры учетных записей. Успешная эксплуатация позволяет получить доступ к критически важным данным для дальнейшего продвижения по сети, повышения привилегий или компрометации систем.	• Credential Access (TA0006) • Unsecured Credentials (T1552) • Credentials in Registry (T1552.002)
RV-D-1276	Запуск интерпретатора командной строки от WinRAR	Правило выявляет запуск интерпретатора командной строки (cmd.exe), инициированный процессом архиватора WinRAR (WinRAR.exe). Подобная активность не является типичной для штатного использования архиватора и может указывать на доставку и запуск вредоносной полезной нагрузки через специально сформированный архив. Правило позволяет обнаружить возможную эксплуатацию уязвимости CVE-2023-38831, при которой в одном архиве содержатся несколько файлов с совпадающими именами, что может привести к их последовательному запуску.	• Execution (TA0002) • Defense Evasion (TA0005) • Obfuscated Files or Information (T1027) • Compression (T1027.015) • Exploitation for Client Execution (T1203)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1279	Выполнение команд в системе от редактора кода VSCode	Правило выявляет запуск командной оболочки cmd.exe или PowerShell из процесса редактора кода Visual Studio Code. Такое поведение может указывать на попытку эксплуатации уязвимости CVE-2023-36867 в расширении GitHub Pull Requests and Issues, связанной с некорректной обработкой файлов формата Markdown и потенциально приводящей к удаленному выполнению команд.	• Execution (TA0002) • Command and Scripting Interpreter (T1059) • Software Extensions (T1176) • IDE Extensions (T1176.002) • User Execution (T1204) • Malicious Link (T1204.001)
RV-D-1280	Зафиксировано изучение системного времени	После получения первоначального доступа к цели атакующие в рамках своей активности по изучению локального и удаленного окружения могут производить разведку системного времени. Эта информация может быть полезна для выполнения других техник, например, для запуска файла с помощью запланированной задачи или для обнаружения информации о местоположении на основе часового пояса. Атакующие также могут использовать знание системного времени в качестве отсрочки выполнения до определенной даты или времени. Примерами утилит для разведки времени являются w32tm или tzutil. Также стоит отметить, что данная активность часто встречается при работе ВПО, например Ursnif использует утилиту time для разведки системного времени.	• Discovery (TA0007) • Windows Management Instrumentation (T1047) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Windows Command Shell (T1059.003) • System Time Discovery (T1124)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1282	Несистемный процесс повысил привилегии до системного	Правило выявляет случаи создания процесса с правами SYSTEM из пользовательского процесса. Такая ситуация возможна при эксплуатации уязвимостей, связанных с получением системного токена, например, уязвимостей семейства Potato. Захваченный токен затем используется для запуска процесса от имени SYSTEM с помощью API-вызовов CreateProcessAsUser или CreateProcessWithToken. Детектирование основано на факте, что процесс, изначально не обладающий системными привилегиями, инициирует создание процесса от имени SYSTEM.	• Privilege Escalation (TA0004) • Access Token Manipulation (T1134)
RV-D-1288	Загрузка файлов с использованием LOLBins InstallUtil.exe	Атакующие могут попытаться обойти систему защиты, используя для запуска программного обеспечения стандартную утилиту Windows InstallUtil.exe. Данный инструмент позволяет выполнять код в обход политик ограничения запуска приложений.	• Defense Evasion (TA0005) • System Binary Proxy Execution (T1218) • InstallUtil (T1218.004)
RV-D-1289	Запуск процесса от другого пользователя	Атакующие могут создать новый процесс с существующим маркером для повышения привилегий и обхода механизмов контроля доступа. Процессы могут быть созданы с маркером и результирующим контекстом безопасности другого пользователя с помощью таких механизмов, как CreateProcessWithTokenW, runas. Правило предназначено для выявления создания процессов с маркером, не связанным с текущим пользователем.	• Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Access Token Manipulation (T1134) • Create Process with Token (T1134.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1292	Изучение общих сетевых ресурсов	Атакующему может потребоваться информация о сетевых ресурсах в инфраструктуре для дальнейшего продвижения внутри сети (Lateral Movement). Полученные данные позволяют атакующему выявить новые цели и расширить область атаки.	• Execution (TA0002) • Discovery (TA0007) • Windows Management Instrumentation (T1047) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Windows Command Shell (T1059.003) • Network Share Discovery (T1135)
RV-D-1294	Перечисление ключей реестра для разведки	Правило обнаруживает перечисление ключей реестра, которые могут быть интересны при разведке информации об узле, путем выявления команд, используемых для получения информации о ключах реестра.	• Discovery (TA0007) • Query Registry (T1012)
RV-D-1298	Запуск whoami с правами системы	Атакующий после получения доступа к системе или после повышения привилегий может проверить уровень своих полномочий. Одним из способов это сделать является команда whoami: она показывает, от имени какого пользователя сейчас активна сессия. Правило обнаруживает использование данной команды с привилегиями системы.	• Discovery (TA0007) • System Owner/User Discovery (T1033)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1300	Сбор информации о сетевых подключениях	После успешной компрометации среды атакующие могут попытаться получить информацию о существующих сетевых подключениях, чтобы спланировать свои дальнейшие действия. Это можно сделать, например, при использовании утилит netstat или net. Полученная информация может быть использована для дальнейшего продвижения по хостам инфраструктуры.	• Discovery (TA0007) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Windows Command Shell (T1059.003)
RV-D-1302	Разведка процессов	Правило детектирует выполнение команд для исследования запущенных в системе процессов. Атакующие могут предпринимать попытки получения информации о выполняемых процессах для формирования представления о программном обеспечении и приложениях, работающих на узлах сети. Полученные данные могут использоваться в ходе автоматизированной разведки для определения последующих шагов, включая полное заражение цели или выполнение специфических вредоносных действий.	• Execution (TA0002) • Discovery (TA0007) • Windows Management Instrumentation (T1047) • Process Discovery (T1057) • Command and Scripting Interpreter (T1059) • Gather Victim Host Information (T1592) • Software (T1592.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1303	Изменение пароля пользователя или хоста с помощью Ksetup.exe	Изменение пароля текущего пользователя или хоста с использованием утилиты ksetup.exe может создавать существенную угрозу информационной безопасности. Данный инструмент может быть задействован для несанкционированного изменения учетных данных пользователя, например, при компрометации системы или получении доступа к учетной записи без соответствующих прав. В результате изменения паролей возможно расширение уровня доступа к системе, включая получение контроля над конфиденциальной информацией и учетными записями с повышенными привилегиями.	• Impact (TA0040) • Account Access Removal (T1531)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1305	Запуск множества подозрительных команд	Данное правило направлено на обнаружение подозрительных действий, связанных с выполнением большого количества легитимных команд за короткий промежуток времени. Такое поведение не характерно для стандартных сценариев административной активности и может указывать на попытку атакующего скрыть вредоносную деятельность или затруднить анализ событий. Обнаружение выполняется при анализе последовательности команд, выполняемых через системные утилиты, такие как cmd.exe, PowerShell или другие доверенные инструменты Windows. Подобная активность может быть связана с разведкой, модификацией системных параметров, отключением защитных механизмов или подготовкой системы к дальнейшим этапам атаки.	• Discovery (TA0007) • Remote System Discovery (T1018) • Network Service Discovery (T1046) • Windows Management Instrumentation (T1047) • System Network Connections Discovery (T1049) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Windows Command Shell (T1059.003) • System Information Discovery (T1082) • Account Discovery (T1087) • Local Account (T1087.001) • Domain Account (T1087.002) • System Time Discovery (T1124) • Domain Trust Discovery

ID правила	Название правила	Описание	Тактики и техники
RV-D-1306	Скрытие учетной записи через реестр Windows	Атакующий с целью сокрытия своего присутствия в системе может скрыть скомпрометированную или недавно созданную учетную запись в окне входа Windows (окно ввода логина и пароля для аутентификации на хосте). Данная активность является специфичной и может свидетельствовать о действиях атакующего или работе вредоносного ПО. Часто такие манипуляции связаны с активностью майнеров.	• Defense Evasion (TA0005) • Hide Artifacts (T1564) • Hidden Users (T1564.002)
RV-D-1311	Дамп памяти ядра через LiveKD	Дамп памяти ядра через LiveKD может использоваться для несанкционированного сбора конфиденциальной информации о системе и пользователях. Обнаружение выполнения LiveKD с флагом "-m" для потенциального дампа памяти ядра может указывать на злонамеренные действия, направленные на получение конфиденциальных данных или эксплуатацию уязвимостей операционной системы. Такая активность может привести к серьезным последствиям, включая утечку информации и нарушение безопасности системы. Обнаружение использования LiveKD с флагом "-m" требует немедленного реагирования и принятия дополнительных мер по обеспечению безопасности.	• Credential Access (TA0006) • OS Credential Dumping (T1003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1312	Закрепление через Outlook Home Page	Атакующие могут использовать домашнюю страницу Microsoft Outlook, чтобы закрепиться в скомпрометированной системе. Домашняя страница Outlook — это устаревшая функция, применявшаяся для настройки отображения папок Outlook. Эта функция позволяет загружать внутренний или внешний URL-адрес и отображать его содержимое при каждом открытии папки. Атакующие могут создать вредоносную HTML-страницу, которая будет выполнять определенный код при загрузке домашней страницы Outlook.	• Persistence (TA0003) • Office Application Startup (T1137) • Outlook Home Page (T1137.004)
RV-D-1314	Попытка дампа оперативной памяти с помощью RdrLeakDiag.exe	Обнаружение использования утилиты rdrleakdiag.exe LOLBIN для дампа памяти процесса указывает на потенциально нежелательную или вредоносную активность. RdrLeakDiag.exe является инструментом, используемым для анализа и создания дампов памяти процессов в Windows, и его использование может быть связано с попытками атакующих изучить или эксплуатировать уязвимости в системе.	• Defense Evasion (TA0005) • Masquerading (T1036) • Invalid Code Signature (T1036.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1315	Скачивание файлов средствами MS-AppInstaller	Обнаружение использования "ms-appinstaller" для потенциальной загрузки вредоносных файлов через AppInstaller.exe. AppInstaller.exe — это ПО, связанное с механизмом установки приложений. MS-AppInstaller является утилитой, которая позволяет устанавливать и обновлять приложения из магазина Microsoft Store и других источников. AppInstaller.exe и MS-AppInstaller тесно связаны и работают вместе для обеспечения процесса установки приложений. Атакующие могут использовать это приложение для установки вредоносного ПО. Такие загрузки могут осуществляться через скомпрометированные источники или в результате фишинговых атак.	• Command and Control (TA0011) • Ingress Tool Transfer (T1105) • User Execution (T1204) • Malicious File (T1204.002)
RV-D-1318	Скачивание файлов через imewdbld.exe	Обнаружение использования "imewdbld" для загрузки файлов. Файл imewdbld.exe является исполняемым файлом, связанным с Microsoft IME (Input Method Editor). Он используется для работы с расширенными словарями ввода текста.	• Defense Evasion (TA0005) • System Binary Proxy Execution (T1218)
RV-D-1319	Скачивание файлов через Squirrel.exe	Squirrel.exe — это компонент, используемый во многих приложениях на базе Electron (например, Slack, Teams, Discord и других) для управления обновлениями. Атакующие могут злоупотреблять этим бинарным файлом, чтобы загружать вредоносные файлы на систему, минуя некоторые меры защиты, так как Squirrel.exe считается доверенным исполняемым файлом (LOLBIN). Данное правило предназначено для выявления подозрительной активности, связанной с запуском Squirrel.exe или update.exe с ключами --download, --update или --updaterollback=, а также с указанием URL, что может указывать на попытку загрузки внешнего ресурса.	• Command and Control (TA0011) • Ingress Tool Transfer (T1105)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1326	Отключение Privacy Settings Experience в реестре	Обнаружение модификаций реестра, которые отключают функцию Privacy Settings Experience. Privacy Settings Experience (Опыт настройки конфиденциальности) в Windows представляет собой экран, который появляется при входе в новую учетную запись пользователя впервые или после обновления (например, новой сборки или версии Windows 10). На этом экране пользователю предлагается просмотреть или выбрать параметры конфиденциальности для своей учетной записи.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)
RV-D-1328	Атака CS Policy Modification	Атакующие могут намеренно отключить проверку подписи, используя стандартные возможности Windows или модифицируя ее настройки. Происходит модификация реестра, в частности ключа BehaviorOnFailedVerify, который отвечает за действия в Windows при обнаружении неподписанного драйвера. Также при помощи утилиты bcdedit.exe атакующие могут управлять параметрами загрузчика Windows (Boot Configuration Data, BCD). Она часто используется атакующими для включения тестового режима или отключения проверки целостности системы.	• Defense Evasion (TA0005) • Subvert Trust Controls (T1553) • Code Signing (T1553.002) • Code Signing Policy Modification (T1553.006)
RV-D-1329	Кодирование файла в Base64 с помощью Certutil	Правило обнаруживает кодирование файлов в Base64 с помощью утилиты Certutil.	• Defense Evasion (TA0005) • Obfuscated Files or Information (T1027)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1330	Использование средств виртуализации	Атакующие могут использовать технологии виртуализации, чтобы избежать обнаружения. Запуская вредоносный код внутри виртуального экземпляра, атакующие могут скрыть артефакты, связанные с их поведением, от средств безопасности, которые не могут отслеживать активность внутри виртуального экземпляра.	• Defense Evasion (TA0005) • Hide Artifacts (T1564) • Run Virtual Instance (T1564.006)
RV-D-1331	SIP Hijacking Windows	Атакующий может подменить или скомпрометировать библиотеку или компонент операционной системы, который управляет списком доверенных корневых сертификатов. Например, они могут подделать или заменить сертификат с целью обмануть систему в принятии неподписанных или поддельных программ.	• Defense Evasion (TA0005) • Subvert Trust Controls (T1553) • SIP and Trust Provider Hijacking (T1553.003)
RV-D-1332	Изменение политик Windows Defender Firewall	Правило обнаруживает использование системной утилиты netsh, которая отвечает за конфигурацию Defender Firewall и командлетов PowerShell, которые используются для изменения политик фильтрации трафика.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify System Firewall (T1562.004)
RV-D-1335	Изменение доверительных отношений между доменами	Атакующие могут создавать новые доверительные отношения между доменами, изменять параметры существующих или модифицировать конфигурацию доверительных отношений между доменами и тенантами, чтобы обойти защитные механизмы или повысить привилегии. Неавторизованные изменения могут привести к серьезным инцидентам безопасности.	• Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Domain or Tenant Policy Modification (T1484) • Trust Modification (T1484.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1336	Кодирование в Base64 файла в подозрительном каталоге с помощью Certutil	Атакующие могут попытаться затруднить обнаружение или анализ файла путем кодирования его содержимого в системе или при передаче. Правило обнаруживает кодирование файлов в Base64 в подозрительном каталоге с помощью утилиты Certutil.	• Defense Evasion (TA0005) • Obfuscated Files or Information (T1027)
RV-D-1338	Атака Code Signing Windows	Атакующие могут подписывать вредоносные программы легитимными цифровыми сертификатами или подделывать подписи для обхода проверок доверия. Это позволяет вредоносному ПО выглядеть безопасным, увеличивая вероятность его запуска.	• Defense Evasion (TA0005) • Subvert Trust Controls (T1553) • Code Signing (T1553.002)
RV-D-1339	Обнаружение стеганографии в Windows	Данное правило выявляет попытки извлечения закодированных команд PowerShell, встроенных в изображения формата PNG с использованием методов стеганографии, созданных утилитами Invoke-PSImage, steghide, stegpy, stegolsb. Подобные действия могут указывать на подготовку к выполнению скрытых вредоносных операций или передачу конфиденциальных данных.	• Defense Evasion (TA0005) • Command and Control (TA0011) • Data Obfuscation (T1001) • Steganography (T1001.002) • Obfuscated Files or Information (T1027) • Steganography (T1027.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1340	Запуск подозрительного cab-файла через msdt.exe	Обнаружено выполнение msdt.exe с использованием флага "cab", который может указывать на подозрительные файлы diagcab со встроенными файлами ответов, использующими CVE-2022-30190. Атакующие могут использовать этот метод для запуска подозрительных файлов в формате .cab, скрывая свои действия за активностью диагностического инструмента Windows. Запуск подобных файлов через msdt.exe может предоставить возможность выполнения вредоносного кода или проведения атаки на систему.	• Defense Evasion (TA0005) • Indirect Command Execution (T1202)
RV-D-1341	Дамп памяти процесса средствами Dotnet-Dump	Обнаруживает выполнение команды "dotnet-dump" с флагом "collect". Выполнение может указывать на потенциальный дамп критических процессов, таких как LSASS.	• Defense Evasion (TA0005) • System Binary Proxy Execution (T1218)
RV-D-1342	Отключение или модификация Windows Defender	Правило обнаруживает модификацию параметров или отключение Windows Defender (Защитник Windows) с помощью выполнения команд в командном интерпретаторе CMD или PowerShell, изменения ключей в реестре или удаления запланированных задач.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)
RV-D-1343	Скачивание файлов с IP-адреса через CertOC.EXE	Правило выявляет запуск штатной утилиты Windows CertOC.exe с параметрами загрузки сертификатных данных по прямому IP-адресу, что может свидетельствовать о злоупотреблении легитимным системным бинарным файлом (LOLBAS) для скрытной загрузки полезной нагрузки, установления связи с C2 или обхода механизмов фильтрации и контроля приложений.	• Defense Evasion (TA0005) • Command and Control (TA0011) • Ingress Tool Transfer (T1105) • System Binary Proxy Execution (T1218)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1344	Выполнение разведки удаленных систем	После успешной компрометации среды атакующие могут попытаться получить информацию об окружении, чтобы спланировать свои дальнейшие действия. Это можно сделать, выполнив команды для перечисления сетевых ресурсов, пользователей, подключений, файлов и установленного программного обеспечения безопасности. В данном правиле будут рассматриваться попытки перечисления окружающих сетевых ресурсов, например при помощи команды net, использования механизма ADSISearcher (данный механизм используется в некоторых скриптах утилиты Powersploit).	• Discovery (TA0007) • Remote System Discovery (T1018) • Windows Management Instrumentation (T1047) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Windows Command Shell (T1059.003)
RV-D-1345	Необычный аргумент или дочерний процесс Wlrmdr.exe	Обнаруживает выполнение "Wlrmdr.exe" с флагом командной строки "-u", который позволяет всему, что ему передано, быть аргументом API ShellExecute, что позволит атакующему выполнить полезную нагрузку с бинарными файлами. Детект также нацелен на любые необычные дочерние процессы, порожденные от "Wlrmdr.exe", в качестве дополнения к тем, которые имеют телеметрию "ParentImage".	• Defense Evasion (TA0005) • System Binary Proxy Execution (T1218)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1346	Необычное выполнение приложений через AtBroker.exe	Обнаруживает запуск сторонних приложений при помощи вспомогательных технологий (Assistive Technology Applications) через "Atbroker.EXE". AtBroker.exe — это программное обеспечение для управления виртуальным рабочим столом или виртуальными окнами. Такие приложения могут предоставлять дополнительные возможности доступности, такие как управление окнами с помощью голоса, альтернативные методы ввода или персонализированные настройки интерфейса.	• Defense Evasion (TA0005) • System Binary Proxy Execution (T1218)
RV-D-1347	Добавление расширения в браузер средством CLI	Данное правило направлено на обнаружение подозрительных действий, связанных с добавлением расширений в браузер с использованием командной строки (CLI). Такие действия могут быть использованы атакующим для автоматизированной установки вредоносных или нежелательных расширений, которые могут изменять поведение браузера, собирать конфиденциальные данные пользователя или выполнять другие вредоносные операции.	• Persistence (TA0003) • Software Extensions (T1176) • Browser Extensions (T1176.001)
RV-D-1348	Сбор структуры AD средствами Ldifde	Обнаружено выполнение утилиты Ldifde.exe для экспорта структуры Active Directory. LDIFDE (LDAP Data Interchange Format Data Exchange) — это утилита, которая позволяет выполнять импорт и экспорт данных в каталог Active Directory. Атакующие могут использовать Ldifde.exe для сбора информации о структуре каталогов, пользователях, группах и других объектах в сети, что является предварительным этапом для дальнейших действий, таких как эксфильтрация данных.	• Execution (TA0002) • Collection (TA0009) • Data from Local System (T1005)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1349	Экспорт структуры AD через csvde.exe	Обнаружено выполнение утилиты csvde.exe для экспорта структуры Active Directory. CSVDE (Comma Separated Values Data Exchange) — это утилита, предназначенная для импорта и экспорта данных в каталог Active Directory в формате CSV (Comma Separated Values).	• Discovery (TA0007) • Account Discovery (T1087) • Domain Account (T1087.002)
RV-D-1350	Использование устаревшей версии PowerShell v2	Атакующие для скрытия своей активности могут использовать старую версию движка PowerShell, так как в таком случае выполненные команды не будут отображены в событиях 400, 800, 4103 и версия PowerShell v2 не поддерживает защиту AMSI.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Downgrade Attack (T1562.010)
RV-D-1351	Скачивание файлов через PresentationHost.exe	Правило предназначено для выявления подозрительного использования утилиты PresentationHost.exe, которая запускает XAML Browser Applications (файлы с расширением .xbap). Несмотря на свою легитимную функцию в рамках .NET Framework, данный исполняемый файл может быть использован атакующими для загрузки файлов из внешних источников с целью обхода традиционных механизмов контроля и доставки вредоносного кода. Поскольку PresentationHost.exe является доверенным компонентом Windows, его использование в подобных сценариях затрудняет обнаружение атаки и может быть частью техники Living off the Land.	• Defense Evasion (TA0005) • Command and Control (TA0011) • Ingress Tool Transfer (T1105) • Trusted Developer Utilities Proxy Execution (T1127) • ClickOnce (T1127.002)
RV-D-1352	Запуск файла из Корзины	Правило обнаруживает запуск процесса из Корзины (Recycle Bin) или из папки, маскирующейся под Корзину.	• Defense Evasion (TA0005) • Hide Artifacts (T1564) • Hidden Files and Directories (T1564.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1353	Подозрительная DLL загружена средствами CertOC.exe	Обнаруживает, когда пользователь устанавливает сертификаты с помощью CertOC.exe для загрузки целевого DLL-файла. CertOC.exe — это файл, используемый для установки и управления сертификатами в операционной системе Windows. Флаг "loadDLL" указывает на то, что CertOC.exe загружает динамическую библиотеку (DLL).	• Defense Evasion (TA0005) • System Binary Proxy Execution (T1218)
RV-D-1355	Импорт ключа реестра из ADS	Импорт ключа реестра из ADS (Alternate Data Stream) представляет собой процесс загрузки данных реестра из альтернативного потока данных, который может содержаться в файле на диске. Это означает, что помимо основного содержимого файла, в нем могут содержаться и другие скрытые данные, которые не видны обычным образом. Обнаружение импорта ключа реестра из ADS важно, так как это может быть использовано зловредным программным обеспечением для скрытого хранения конфигурационной информации или других данных. В связи с этим обнаружение такого импорта становится важным для обнаружения потенциальных угроз и неправомерной деятельности. Это связано с обнаружением импорта альтернативного потока данных в реестр с помощью regedit.exe, так как оба процесса направлены на выявление скрытых данных или действий в реестре, которые могут быть пропущены стандартными методами анализа.	• Defense Evasion (TA0005) • Modify Registry (T1112)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1357	Установка root сертификата средствами CertMgr.exe	Обнаружено выполнение утилиты CertMgr.exe с флагом 'add' для установки нового сертификата системы. Атакующие могут установить корневой сертификат на взломанную систему, чтобы избежать предупреждений при подключении к контролируемым веб-серверам. Корневые сертификаты являются частью инфраструктуры открытых ключей (PKI) и используются для проверки подлинности сертификатов удостоверяющих центров. Если атакующий установит свой собственный корневой сертификат на целевой системе, то затем сможет подделывать сертификаты для любых веб-сайтов или служб без предупреждения или обнаружения со стороны браузера или клиента.	• Defense Evasion (TA0005) • Subvert Trust Controls (T1553) • Install Root Certificate (T1553.004)
RV-D-1358	Генерация окна ввода пароля через Zenity	Zenity — утилита, которая позволяет генерировать графические диалоговые окна, сгенерированные через командную строку или через выполнение shell-скриптов (на Windows это `cmd`, на Linux это `bash`). Атакующие могут подделывать окна ввода пароля для получения и сбора учетных данных пользователей.	• Credential Access (TA0006) • Collection (TA0009) • Input Capture (T1056) • GUI Input Capture (T1056.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1359	Запуск PowerShell-окна в скрытом режиме	Атакующие могут использовать PowerShell в скрытом режиме для выполнения вредоносных действий, избегая их обнаружения пользователями. Запуск PowerShell с параметром -WindowStyle Hidden позволяет скрыть окно выполнения, что затрудняет визуальное обнаружение активности. Это может использоваться в атаках для обхода защиты, выполнения вредоносных скриптов, автоматизации процессов без уведомления пользователя. Данное правило отслеживает попытки запуска PowerShell с параметром -WindowStyle Hidden через события Windows Security, Sysmon и PowerShell Operational.	• Defense Evasion (TA0005) • Hide Artifacts (T1564) • Hidden Window (T1564.003)
RV-D-1360	Отключение ETW провайдера Windows Defender	Правило обнаруживает изменение значений ключей реестра или команды, которые указывают на отключение ETW провайдера Windows Defender для отключения сбора событий журнала Windows Defender/Operational. Подобная активность нехарактерна для стандартных административных сценариев и может указывать на попытку атакующего скрыть свое присутствие и затруднить сбор телеметрии защитными средствами Windows.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Indicator Blocking (T1562.006)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1366	Запуск MSBuild для выполнения кода	Данное правило направлено на детектирование подозрительных действий, связанных с использованием системного компонента MSBuild.exe для выполнения произвольного кода. Такое поведение не характерно для стандартных сценариев использования MSBuild.exe и может указывать на попытку атакующего использовать легитимный инструмент для обхода защитных механизмов и запуска вредоносных операций. Детект выполняется при анализе событий создания процессов, где MSBuild.exe запускается с аргументами, содержащими пути к файлам с расширениями .csproj, .xml, .proj и другими. Злоупотребление MSBuild.exe позволяет скрывать вредоносную активность, так как процесс подписан Microsoft и входит в стандартный набор инструментов Windows. Успешная эксплуатация этой техники может привести к выполнению вредоносного кода, сбору данных, эскалации привилегий или дальнейшему продвижению атакующего в инфраструктуре.	• Defense Evasion (TA0005) • Trusted Developer Utilities Proxy Execution (T1127) • MSBuild (T1127.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1367	Атака Pass the Ticket	Данное правило направлено на детектирование подозрительных действий, связанных с использованием техники Pass-the-Ticket (PtT), которая позволяет атакующему аутентифицироваться в системе, применяя полученные билеты Kerberos вместо ввода учетных данных. Такое поведение отклоняется от стандартных сценариев аутентификации и может свидетельствовать о попытке атакующего получить доступ к системам с использованием поддельных или скомпрометированных билетов. Детект выполняется при использовании утилит Mimikatz и Rubeus и их подозрительных команд. Успешная эксплуатация PtT может привести к несанкционированному доступу к критическим ресурсам, использованию привилегированных учетных записей и продвижению атакующего по сети.	• Defense Evasion (TA0005) • Use Alternate Authentication Material (T1550) • Pass the Ticket (T1550.003)
RV-D-1368	Скачивание файла средствами ProtocolHandler	Правило предназначено для выявления использования компонента ProtocolHandler.exe для загрузки файлов по сетевым протоколам, таким как HTTP, HTTPS или FTP, что может указывать на попытку скрытной доставки вредоносных загрузок без использования очевидных инструментов. Атакующие могут применять ProtocolHandler в рамках техник обхода средств защиты и установления каналов управления и контроля, поскольку эта легитимная утилита Windows может быть использована в обход систем мониторинга. Загруженные файлы, как правило, сохраняются во временных каталогах кэша, что затрудняет их обнаружение.	• Defense Evasion (TA0005) • Command and Control (TA0011) • Ingress Tool Transfer (T1105) • System Binary Proxy Execution (T1218)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1369	Подозрительный агент обновления Windows	Правило предназначено для выявления подозрительного использования агента обновления Windows (wuauclt.exe) без указания флагов командной строки, что может свидетельствовать о попытках обхода защитных механизмов и маскировки запуска вредоносных процессов. Атакующие могут использовать wuauclt.exe для запуска других программ в обход контроля со стороны систем защиты, так как данный агент является доверенным компонентом Windows и может применяться в рамках техники маскировки под легитимные процессы.	• Defense Evasion (TA0005) • Masquerading (T1036)
RV-D-1371	Запуск замаскированного исполняемого файла через conhost.exe	Правило предназначено для выявления запуска исполняемых файлов через процесс conhost.exe, замаскированных под документы или изображения (например, с расширениями .pdf, .png, .jpg и другие), размещенных во временных каталогах пользователя или системы. Подобное поведение нехарактерно для штатной работы Windows и может свидетельствовать о попытке скрытого запуска вредоносной нагрузки с использованием маскировки под легитимные файлы.	• Execution (TA0002) • Defense Evasion (TA0005) • Obfuscated Files or Information (T1027) • Compression (T1027.015) • Masquerading (T1036) • Masquerade File Type (T1036.008) • System Binary Proxy Execution (T1218)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1372	Отключение логирования событий IIS	Правило обнаруживает команды, которые могут использоваться атакующими для отключения логирования событий сервера IIS.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable Windows Event Logging (T1562.002)
RV-D-1373	Вызов функции DllUnregisterServer через Msiexec.exe	Обнаружение MsiExec, загружающего DLL и вызывающего ее функцию DllUnregisterServer, является типичным признаком процесса деинсталляции программного обеспечения. MsiExec — это исполняемый файл Windows Installer, используемый для управления установкой и удалением программ. При деинсталляции программы MsiExec может загружать DLL, отвечающие за удаление программных компонентов, и вызывать их функции, такие как DllUnregisterServer, для корректного удаления следов установки. Мониторинг и обнаружение этих действий могут быть полезны для контроля установленного программного обеспечения и обеспечения целостности системы.	• Defense Evasion (TA0005) • System Binary Proxy Execution (T1218) • Msiexec (T1218.007)
RV-D-1374	Создание нового процесса с помощью Taskmgr.exe	Обнаруживает создание процесса через диспетчер задач Windows. Это может быть попытка обойти User Account Control (UAC) — механизм безопасности Windows.	• Defense Evasion (TA0005) • Masquerading (T1036)
RV-D-1376	Запуск произвольной DLL библиотеки средствами Msiexec.exe	Атакующие могут использовать msiexec.exe для проксирования выполнения вредоносной полезной нагрузки. Msiexec.exe — это утилита командной строки для установщика Windows, поэтому обычно ассоциируется с выполнением инсталляционных пакетов (.msi).	• Defense Evasion (TA0005) • System Binary Proxy Execution (T1218) • Msiexec (T1218.007)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1378	Запуск процесса AddInUtil.exe из подозрительной директории	Правило предназначено для обнаружения запуска легитимной утилиты AddInUtil.exe из нестандартных директорий Windows. По умолчанию этот бинарный файл располагается в каталогах .NET Framework (например, `C:\Windows\Microsoft.NET\Framework\`), поэтому его выполнение из пользовательских или временных папок считается аномалией. Такое поведение может указывать на попытку использования системного инструмента для проксирования выполнения стороннего кода (техника Living off the Land).	• Defense Evasion (TA0005) • System Binary Proxy Execution (T1218)
RV-D-1380	Скачивание файлов через msedge_proxy.exe	Обнаружение использования msedge_proxy.exe для загрузки файлов. Файл msedge_proxy.exe связан с браузером Microsoft Edge и отвечает за обработку сетевого трафика и связь между браузером и Интернетом.	• Defense Evasion (TA0005) • Command and Control (TA0011) • Ingress Tool Transfer (T1105)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1445	Удаленное использование утилиты Atexec	Атакующий может выполнять команды на целевой системе, используя инструмент atexec, который применяется для создания и немедленного запуска запланированного задания на удаленном хосте через SMB. Удаленное создание/исполнение/удаление задачи возможно с помощью RPC-процедур, таких как SchRpcRegisterTask, SchRpcRun и SchRpcDelete. Команда, переданная в atexec, устанавливается как действие запланированной задачи. Результат выполненной команды помещается во временный файл и далее считывается при помощи сетевого ресурса ADMIN$. Вывод команды извлекается путем перенаправления вывода во временный файл, который затем считывается через сетевой ресурс ADMIN$. Запланированные задачи могут создаваться и легитимно, но правило рассчитано на быструю последовательность операций и различия родителя задачи и выполнившего.	• Execution (TA0002) • Lateral Movement (TA0008) • Remote Services (T1021) • SMB/Windows Admin Shares (T1021.002) • Scheduled Task/Job (T1053) • At (T1053.002)
RV-D-1446	Компрометация через KrbRelayUp	Данное правило предназначено для выявления атак Kerberos Relay, при которых атакующие используют уязвимости в протоколах аутентификации для перехвата и перенаправления запросов, что позволяет им получить доступ к защищенным ресурсам. Такие атаки могут применяться для эскалации привилегий или несанкционированного доступа к критически важным данным.	• Privilege Escalation (TA0004) • Exploitation for Privilege Escalation (T1068)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1499	Использование инструмента SharpHound	Утилита SharpHound (коллектор данных для инструмента BloodHound) используется атакующими для разведки в среде Active Directory (AD). Инструмент собирает информацию о пользователях, группах, компьютерах, активных сессиях и доверительных отношениях. В дальнейшем эти данные применяются в BloodHound для выявления скрытых связей и автоматизированного построения кратчайших маршрутов атаки (Attack Paths) к критичным активам и привилегированным учетным записям. Обнаружение несанкционированной активности SharpHound с высокой долей вероятности свидетельствует о присутствии атакующего в инфраструктуре, этапе сбора данных и подготовке к продвижению по сети (Lateral Movement).	• Execution (TA0002) • Discovery (TA0007) • Remote System Discovery (T1018) • System Owner/User Discovery (T1033) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Permission Groups Discovery (T1069) • Local Groups (T1069.001) • Domain Groups (T1069.002) • Account Discovery (T1087) • Local Account (T1087.001) • Domain Account (T1087.002) • Domain Trust Discovery (T1482)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1570	Возможное сокрытие запланированной задачи	Task Scheduler или Планировщик задач — служба в Windows, которая позволяет автоматизированно выполнять запланированные задачи на устройстве по заранее заданному триггеру: время, наступление определенного события и другие. Данная служба удобна для атакующего тем, что запланированные задачи являются легитимными в операционной системе Windows. Это позволяет замаскировать вредоносные действия, а сам функционал планировщика задач не будет отключен администраторами, так как на нем строится работа всей системы. Данное правило направлено на детектирование удаления файлов запланированных задач из файловой системы и манипуляций с дескрипторами безопасности задачи.	• Execution (TA0002) • Persistence (TA0003) • Scheduled Task/Job (T1053) • At (T1053.002) • Scheduled Task (T1053.005)
RV-D-1571	Подмена установочных файлов TrueConf	TrueConf Server - программная платформа для видеоконференцсвязи (ВКС). Она помогает сотрудникам общаться и эффективно работать на расстоянии, а также легко проводить вебинары и удаленное обучение. На данный момент известен случай эксплуатации уязвимости CVE-2026-3502 китайской APT-группировкой в рамках операции TrueChaos, направленной на государственные организации стран Юго-Восточной Азии. В рамках атаки атакующие злоупотребляли доверенным механизмом обновления, используя его для доставки вредоносного ПО из-за отсутствия корректной проверки подлинности обновлений. Данное правило детектирует подмену файлов клиента на сервере TrueConf как признак компрометации сервера и начала атаки.	• Initial Access (TA0001) • Supply Chain Compromise (T1195) • Compromise Software Supply Chain (T1195.002)

Microsoft Windows Task Scheduler

Данный раздел содержит инструкции по сбору событий из журналов Microsoft Windows Task

Scheduler различными методами:

- Microsoft Windows Task Scheduler: настройка источника

Microsoft Windows Task Scheduler: настройка источника

Данное руководство описывает процесс настройки сбора событий Microsoft Windows Task Scheduler и их отправки в R-Vision SIEM.

Настройка Microsoft Windows Task Scheduler

Настройка журналирования Microsoft Windows Task Scheduler



В настоящем руководстве рассматривается передача событий с помощью агента платформы R-Vision EVO.

Включите логирование событий Microsoft через Event Viewer:

1. В дереве навигации перейдите по пути **Microsoft** → **Windows** → **TaskScheduler** → **Operational**.
2. Чтобы настроить журналирование, выполните команду **Enable Log** в контекстном меню.
3. Проверьте, что сервис **Task Scheduler** запущен.
4. Установите на узле агент R-Vision EVO.

Настройка в R-Vision SIEM

Настройка отправки событий в R-Vision SIEM

1. В веб-интерфейсе R-Vision SIEM перейдите в раздел **Агенты** → **Группы агентов**.
2. Создайте группу и добавьте в нее узел, на котором установлен агент.
3. В созданной группе узлов в секции **Чтение файлов** нажмите на кнопку **Добавить настройку** (+).
4. В выпадающем списке **Тип журнала** выберите вариант **eventchannel**.
5. В поле **Имя журнала** введите значение `Microsoft-Windows-Task-Scheduler/Operational`.
6. Если необходимо выбирать события по определенным критериям, введите в поле **Фильтр (формат XPATH)** выражение XPath. Если фильтр не нужен, введите символ *.
7. Нажмите на кнопку **Сохранить и применить**.
8. Дождитесь применения политики группы на узле. Сбор событий настроен.

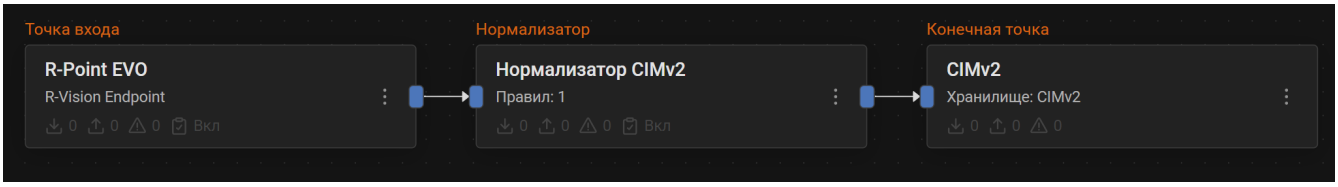
Настройка обработки событий в R-Vision SIEM

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **R-Vision EVO Endpoint**.
   - Домен: введите значение в формате `gw-<your_gateway_id>`, где `<your_gateway_id>` — ID шлюза.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Microsoft Windows Task Scheduler**

(идентификатор правила: **RV-N-303**).

4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

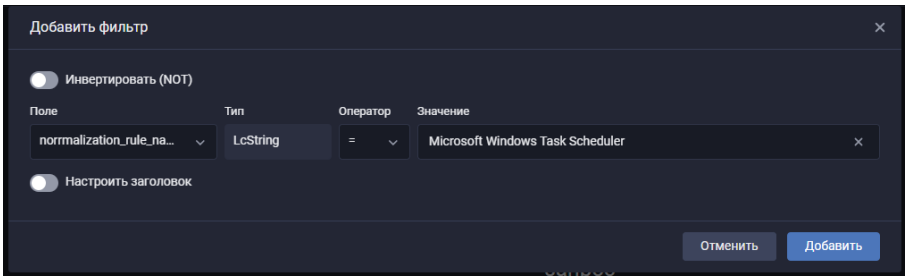
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Microsoft Windows Task Scheduler.

Найти события Microsoft Windows Task Scheduler в хранилище можно по следующему фильтру:

```
normalization_rule_name = "Microsoft Windows Task Scheduler"
```



Почтовые системы и серверы

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых почтовых систем и серверов:

- Kaspersky Secure Mail Gateway
- Microsoft Exchange Server

Kaspersky Secure Mail Gateway

- Kaspersky Secure Mail Gateway: правила корреляции

Kaspersky Secure Mail Gateway: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-961	Шифрованное вложение в письме	Данное правило направлено на обнаружение шифрованного вложения в письме средствами KSMG. Данная атака может быть началом попыток получения доступа к ИС компании.	• Initial Access (TA0001) • Obfuscated Files or Information (T1027) • Internal Spearphishing (T1534) • Phishing (T1566) • Spearphishing Attachment (T1566.001) • Phishing for Information (T1598) • Spearphishing Attachment (T1598.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-962	Проверка подлинности отправителя сообщений	Данное правило направлено на детектирование инцидентов, связанных с проверкой подлинности отправителей сообщений в письме, с использованием средств KSMG. Проверка подлинности отправителей сообщений предназначена для дополнительной защиты почтовой инфраструктуры от атаки, при которой атакующий может заменить почту на доверенную.	• Initial Access (TA0001) • Internal Spearphishing (T1534) • Phishing (T1566) • Phishing for Information (T1598)
RV-D-963	Вредоносное вложение в письме	Данное правило направлено на обнаружение вредоносного вложения в письме средствами KSMG. Вредоносное вложение может содержаться как в теле письма, так и в файле во вложении. Данная атака может быть началом попыток получения доступа к ИС компании.	• Initial Access (TA0001) • Internal Spearphishing (T1534) • Phishing (T1566) • Spearphishing Attachment (T1566.001) • Spearphishing Link (T1566.002) • Phishing for Information (T1598) • Spearphishing Attachment (T1598.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-964	Получение массовой рассылки писем	Данное правило направлено на детектирование инцидентов, связанных с массовой рассылкой писем, с использованием средств KSMG. Массовые рассылки могут быть использованы атакующими для распространения спама, фишинга или вредоносного ПО, а также для организации атак на почтовую инфраструктуру организации. Правило позволяет выявлять подозрительную активность, связанную с отправкой большого количества писем за короткий промежуток времени, что может указывать на попытку злоупотребления почтовой системой.	• Initial Access (TA0001) • Phishing (T1566) • Phishing for Information (T1598) • Email Bombing (T1667)
RV-D-965	Получение спам-письма	Данное правило направлено на обнаружение инцидентов, связанных с получением спам-писем, с использованием средств KSMG. Спам-письма могут содержать нежелательную рекламу, фишинговые ссылки или вредоносные вложения, что представляет угрозу для безопасности почтовой инфраструктуры и пользователей организации.	• Initial Access (TA0001) • Phishing (T1566) • Phishing for Information (T1598)

ID правила	Название правила	Описание	Тактики и техники
RV-D-966	Вредоносная ссылка в письме	Данное правило направлено на детектирование инцидентов, связанных с получением вредоносных ссылок в письме, на основе событий KSMG. Ссылки могут содержать вредоносные вложения, что представляет угрозу для безопасности почтовой инфраструктуры и пользователей организации.	• Initial Access (TA0001) • Drive-by Compromise (T1189) • User Execution (T1204) • Malicious Link (T1204.001) • Phishing (T1566) • Spearphishing Link (T1566.002) • Phishing for Information (T1598) • Spearphishing Link (T1598.003)

Microsoft Exchange Server

- Microsoft Exchange Server: настройка источника
- Microsoft Exchange Server: правила корреляции

Microsoft Exchange Server: настройка источника

Данное руководство описывает процесс настройки сбора событий Microsoft Exchange Server и их отправки в R-Vision SIEM.

Настройка Microsoft Exchange Server

Настройка журналирования



В настоящем руководстве рассматривается передача событий с помощью агента платформы R-Vision EVO. Для пересылки событий в R-Vision SIEM установите на узле агент R-Vision EVO.

В рамках событий будет осуществлена настройка для следующих журналов:

- Журнал **MSExchange Management**;

- Журнал **Message Tracking**;
- Журнал **IMAP4**;
- Журнал **POP3**.

Журнал MSExchange Management

Для настройки записи событий в журнал **MSExchange Management** выполните следующие шаги:

1. Откройте **Exchange Management Shell**.
2. Введите команду:

```
Get-AdminAuditLogConfig | Format-List AdminAuditLogEnabled
```

3. Если будет выведено значение `False`, введите команду:

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $true
```

После этого команды, вводимые в **Exchange Management Shell**, будут записываться в событиях журнала **MSExchange Management**.

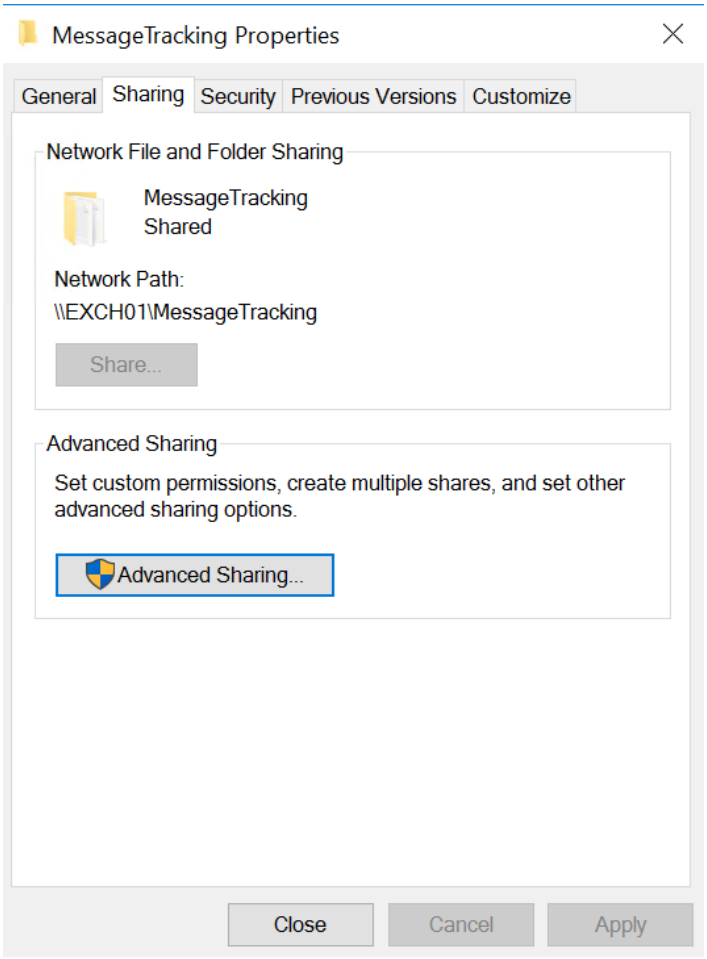
Журнал Message Tracking

Журнал **Message Tracking** включен по умолчанию. Дополнительная настройка не требуется.

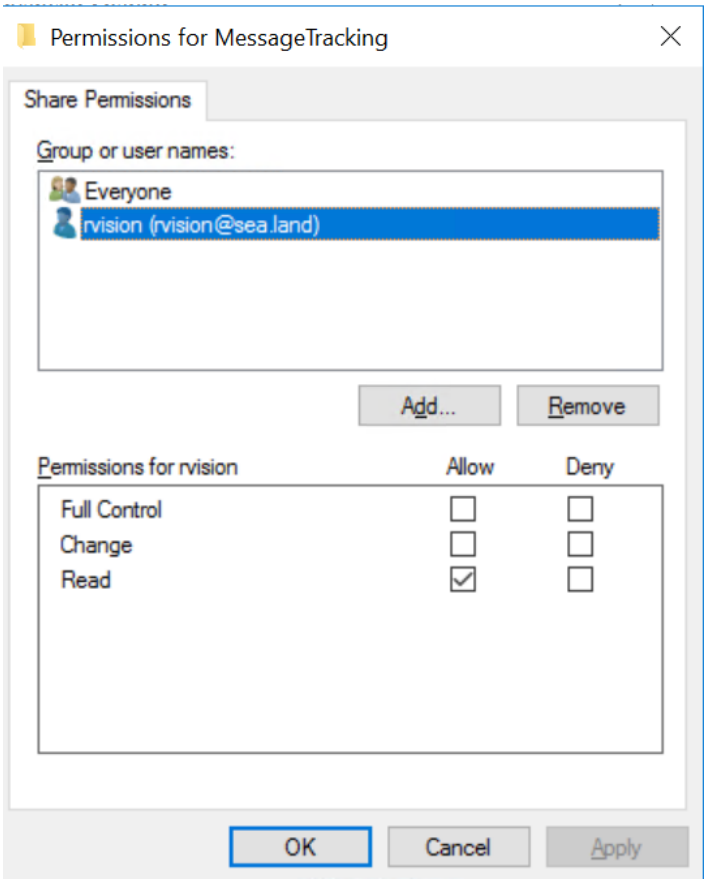
Данный журнал регистрирует события обработки писем на стороне сервера.

Сбор событий данного журнала будет производиться посредством обращения к файлам событий по протоколу SMB. Для этого необходимо настроить доступ для папки хранения логов:

1. Перейдите в каталог хранения журналов Exchange: `C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs`.
2. В контекстном меню каталога **MessageTracking** выберите вариант **Properties**.
3. Откройте вкладку **Sharing** и нажмите на кнопку **Advanced Sharing...**.



4. В открывшемся окне установите флажок **Share this folder** и нажмите на кнопку **Permissions**.
5. В окне настройки прав добавьте УЗ, от имени которой планируется читать файлы событий через SMB, и добавьте права на чтение.
6. Нажмите на кнопку **OK**.



7. Нажмите на кнопку **Done**.

Настройка для журнала **Message Tracking** завершена.

Журналы IMAP4 и POP3

Данные журналы хранят события взаимодействия с почтовыми клиентами сервера Exchange. Для настройки записи событий в данные журналы выполните следующие шаги:

1. Откройте **Exchange Management Shell**.
2. Включите аудит IMAP4 командой:

```
Set-ImapSettings -ProtocolLogEnabled $true
```

3. Включите аудит POP3 командой:

```
Set-PopSettings -ProtocolLogEnabled $true
```

4. Настройте права доступа для каталогов хранения логов по аналогии с настройкой для журнала **Message Tracking**. Данные каталоги расположены по следующим путям:
   - IMAP4: `C:\Program Files\Microsoft\Exchange Server\V15\Logging\Imap4`.
   - POP3: `C:\Program Files\Microsoft\Exchange Server\V15\Logging\Pop3`.

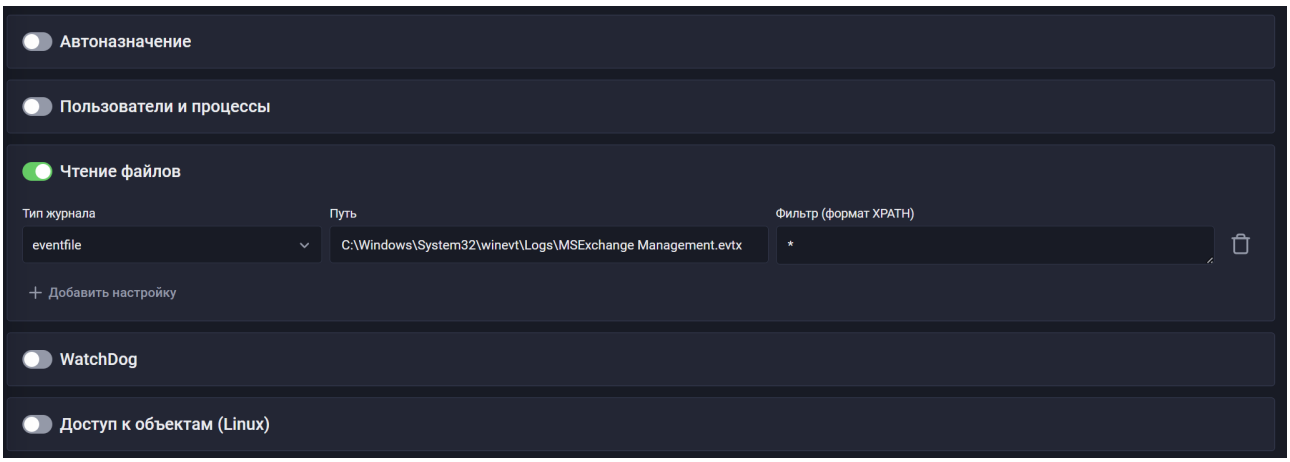
Настройка для журналов **IMAP4** и **POP3** завершена.

Настройка в R-Vision SIEM

Настройка отправки событий в R-Vision SIEM

Для отправки событий источника в R-Vision SIEM выполните следующие шаги:

1. В веб-интерфейсе R-Vision SIEM перейдите в раздел **Агенты** → **Группы агентов**.
2. Создайте группу и добавьте в нее узел, на котором установлен агент.
3. В созданной группе узлов в секции **Чтение файлов** нажмите на кнопку **Добавить настройку** (+).
4. В выпадающем списке **Тип журнала** выберите вариант **eventfile**.
5. В поле **Путь** введите значение `C:\Windows\System32\winevt\Logs\MSExchange Management.evtx`.
6. Если необходимо выбирать события по определенным критериям, введите в поле **Фильтр (формат XPATH)** выражение XPath. Если фильтр не нужен, введите символ *.



7. Нажмите на кнопку **Сохранить и применить**.
8. Дождитесь применения политики группы на узле. Сбор событий настроен.

Настройка обработки событий в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **R-Vision Endpoint**.
   - Домен: введите значение в формате `gw-<your_gateway_id>`, где `<your_gateway_id>` — ID шлюза.
3. Добавьте на конвейер элемент **Точка входа** для сбора событий журнала **Tracking Message** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **SMB**.
   - Путь к ресурсу: введите значение в формате `\\<server_name>\MessageTracking`, где `<server_name>` — FQDN сервера Exchange.

- Тип аутентификации (опционально): выберите тип, настроенный в вашем домене
- Учетные данные: выберите секрет с учетной записью, которая имеет права на чтение каталога через SMB.
- Версия SMB: выберите вариант **SMB3**.
- Маска файла: введите значение `*.LOG`.
- Интервал запроса, секунд: введите значение `15`.
- Таймаут запроса, секунд: введите значение `5`.

4. Добавьте на конвейер элемент **VRL-трансформация** со следующим кодом:

```
.device_product = "exchange"
.device_event_category = "email_transport"
```

5. Соедините VRL-трансформацию с точкой входа, настроенной для журнала **Tracking Message**.
6. Добавьте на конвейер элемент **Точка входа** для сбора событий журнала **IMAP4** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **SMB**.
   - Путь к ресурсу: введите значение в формате `\\<server_name>\Imap4`, где `<server_name>` — FQDN сервера Exchange.
   - Тип аутентификации: выберите тип, настроенный в вашем домене.
   - Учетные данные: выберите секрет с учетной записью, которая имеет права на чтение каталога через SMB.
   - Версия SMB: выберите вариант **SMB3**.
   - Маска файла: введите значение `*.LOG`.
   - Интервал запроса, секунд: введите значение `15`.
   - Таймаут запроса, секунд: введите значение `5`.
7. Добавьте на конвейер элемент **VRL-трансформация** со следующим кодом:

```
.device_product = "exchange"
.device_event_category = "imap"
```

8. Соедините VRL-трансформацию с точкой входа, настроенной для журнала **IMAP4**.
9. Добавьте на конвейер элемент **Точка входа** для сбора событий журнала **POP3** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **SMB**.
   - Путь к ресурсу: введите значение в формате `\\<server_name>\Pop3`, где `<server_name>` — FQDN сервера Exchange.
   - Тип аутентификации: выберите тип, настроенный в вашем домене.

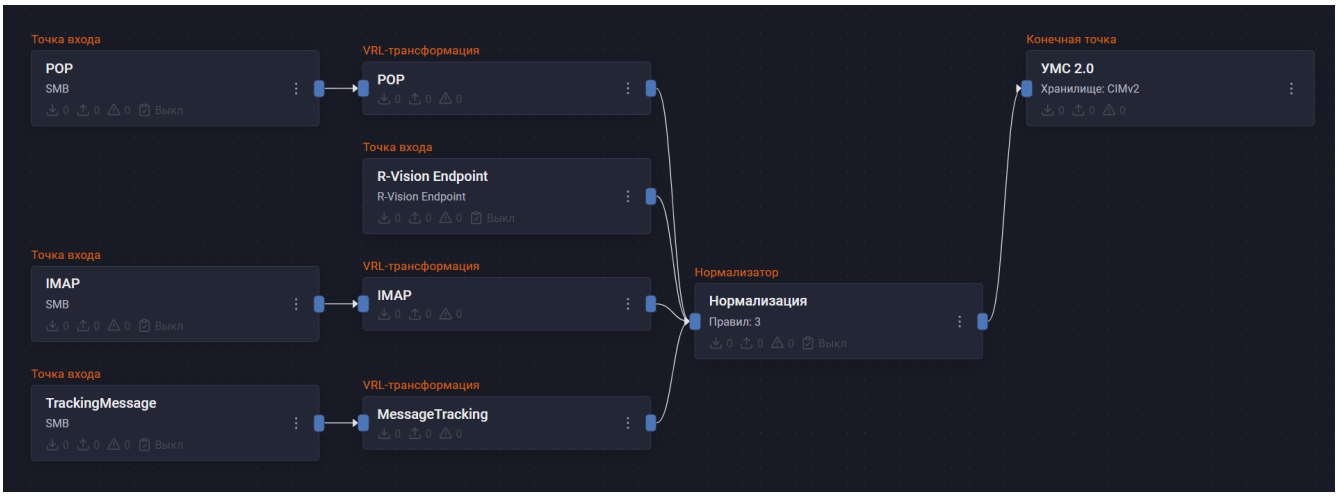
- Учетные данные: выберите секрет с учетной записью, которая имеет права на чтение каталога через SMB.
- Версия SMB: выберите вариант **SMB3**.
- Маска файла: введите значение `*.LOG`.
- Интервал запроса, секунд: введите значение `15`.
- Таймаут запроса, секунд: введите значение `5`.

10. Добавьте на конвейер элемент **VRL-трансформация** со следующим кодом:

```
.device_product = "exchange"
.device_event_category = "pop"
```

11. Соедините VRL-трансформацию с точкой входа, настроенной для журнала **POP3**.
12. Добавьте на конвейер элемент **Нормализатор** с правилами:
    - **Microsoft Exchange Management** (идентификатор правила: **RV-N-263**);
    - **Microsoft Exchange Server** (идентификатор правила: **RV-N-264**);
    - **Microsoft Exchange Server IMAP/POP** (идентификатор правила: **RV-N-347**).
13. Соедините нормализатор с точкой входа типа **R-Vision Endpoint** и созданными VRL-трансформациями.
14. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
15. Соедините конечную точку с нормализатором.
16. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

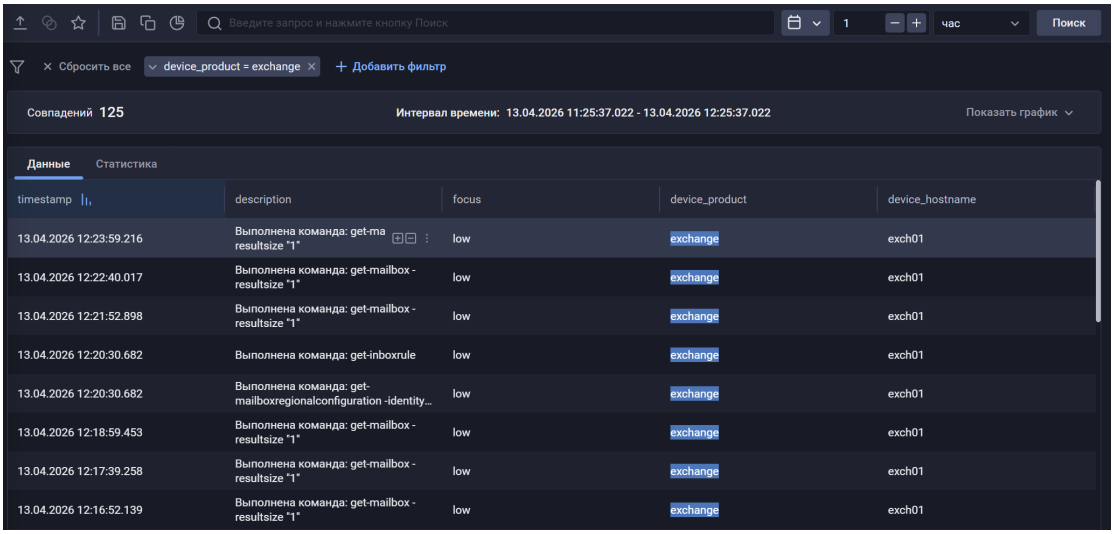


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Microsoft Exchange Server.



Найти события Microsoft Exchange Server в хранилище можно по следующему фильтру:

```
device_product = "exchange"
```



Microsoft Exchange Server: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1166	Утечка данных через массовую отправку писем	Правило предназначено для выявления аномальных сценариев массовой отправки писем с внутренних учетных записей на один внешний адрес. Такая активность может указывать на компрометацию почтовых ящиков или попытку передачи конфиденциальной информации через почтовые каналы.	• Collection (TA0009) • Exfiltration (TA0010) • Exfiltration Over Alternative Protocol (T1048) • Email Collection (T1114)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1167	Эксплуатация уязвимости CVE-2024-49040	Правило предназначено для выявления писем, доставленных через Microsoft Exchange, в которых наблюдается расхождение между реальным SMTP-отправителем (envelope sender, P2 FROM) и адресом, указанным в заголовке From. Атакующие могут намеренно подменять значение заголовка From для маскировки источника письма, имитации доверенных внешних или внутренних отправителей и повышения вероятности успешной фишинговой атаки. В рамках правила анализируются события Message Tracking Logs типа RECEIVE. Детект срабатывает в случаях, когда отображаемый отправитель письма не совпадает с адресом отправителя, использованным на уровне SMTP.	• Initial Access (TA0001) • Defense Evasion (TA0005) • Phishing (T1566) • Spearphishing Link (T1566.002) • Email Spoofing (T1672)
RV-D-1171	Попытка выгрузить PST-файлы в MS Exchange	Атакующие могут использовать штатные административные возможности Microsoft Exchange для скрытой эксфильтрации почтовых данных. В частности, командлеты PowerShell `New-MailboxExportRequest` и `Remove-MailboxExportRequest` позволяют экспортировать содержимое почтовых ящиков в PST-файлы и одновременно удалять следы этой операции. Такой сценарий не требует уязвимостей и маскируется под легитимную административную деятельность, что делает его особенно опасным.	• Defense Evasion (TA0005) • Indicator Removal (T1070) • Clear Mailbox Data (T1070.008)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1172	Изменение правила журнала в системе Exchange	Атакующие, получившие доступ к привилегированной учетной записи Exchange, могут создавать, изменять или удалять Journal Rules для реализации скрытого сбора переписки (эксфильтрации) или для обхода требований комплаенса и сокрытия активности (например, отключив правило или сменив адрес журналирования). Правило предназначено для выявления изменений конфигурации Exchange Journal Rules (журналирование почты), выполняемых через Exchange PowerShell.	• Defense Evasion (TA0005) • Collection (TA0009) • Email Collection (T1114) • Email Forwarding Rule (T1114.003) • Impair Defenses (T1562)
RV-D-1173	Изменение политики Microsoft Office OWA в системе Exchange	Атакующие, получившие доступ к привилегированной учетной записи Exchange, могут создавать, изменять или удалять политики OWA с целью ослабления защитных ограничений, повышения удобства эксплуатации скомпрометированных почтовых ящиков или обхода организационных мер безопасности. Например, отключение ограничений на вложения или изменение политики для конкретных пользователей может упростить доставку вредоносных файлов, фишинговых вложений или дальнейшее развитие атаки.	• Persistence (TA0003) • Defense Evasion (TA0005) • Account Manipulation (T1098) • Impair Defenses (T1562)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1178	Сбор электронной почты в MS Exchange	Атакующие, получившие доступ к учетной записи с достаточными привилегиями, могут злоупотреблять встроенными средствами Exchange для скрытого сбора конфиденциальной информации из почтовых ящиков. В частности, с использованием PowerShell-командлетов возможно выборочно извлекать письма по ключевым словам, временным диапазонам или другим критериям и копировать их в подконтрольный почтовый ящик или экспортировать для последующей эксфильтрации.	• Collection (TA0009) • Email Collection (T1114) • Remote Email Collection (T1114.002)
RV-D-1179	Удаление или размонтирование базы данных в MS Exchange	Атакующие с привилегированной учетной записью Exchange могут удалять или размонтировать базы данных почтовых ящиков, что приводит к потере данных, нарушению работы сервисов и потенциальной утечке информации. Подобные действия могут выполняться через PowerShell-командлеты `Remove-MailboxDatabase` и `Dismount-Database` в Exchange Management Shell или удаленно через административные интерфейсы.	• Impact (TA0040) • Data Destruction (T1485) • Lifecycle-Triggered Deletion (T1485.001) • Data Manipulation (T1565) • Stored Data Manipulation (T1565.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1180	Пользователь удалил почтовые ящики в MS Exchange	Атакующие, получившие доступ к привилегированной учетной записи Exchange (или скомпрометировав учетные данные администратора), могут удалять или отключать почтовые ящики пользователей через Exchange PowerShell для сокрытия следов и нарушения доступности корпоративной переписки. Команды `Remove-Mailbox` и `Disable-Mailbox` приводят к потере доступа к содержимому ящика и могут использоваться как точечно (для конкретных сотрудников), так и массово (для дестабилизации работы организации). Правило предназначено для выявления операций удаления/отключения почтовых ящиков, выполняемых через Exchange Management Shell и фиксируемых в журналах выполнения cmdlet (CmdletLogs).	• Persistence (TA0003) • Impact (TA0040) • Account Manipulation (T1098) • Data Destruction (T1485) • Lifecycle-Triggered Deletion (T1485.001)
RV-D-1182	Пользователь выполнил действие с правилом транспорта в Exchange	Атакующие, получившие доступ к учетной записи с административными или делегированными правами в Microsoft Exchange, могут злоупотреблять правилами транспорта (Transport Rules) для скрытого сбора, перенаправления или модификации электронной почты. Подобные действия могут выполняться через PowerShell-командлеты `New-TransportRule`, `Set-TransportRule` и `Remove-TransportRule` в Exchange Management Shell.	• Defense Evasion (TA0005) • Collection (TA0009) • Email Collection (T1114) • Email Forwarding Rule (T1114.003) • Hide Artifacts (T1564) • Email Hiding Rules (T1564.008)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1183	Добавление пользователя в группу рассылки в MS Exchange	Атакующие, получившие доступ к администраторской учетной записи Exchange, могут добавлять пользователей или внешние адреса в группы рассылки, чтобы получить доступ к конфиденциальной переписке или обеспечить скрытую рассылку сообщений. Наиболее часто это выполняется через Exchange Management Shell и фиксируется в журналах выполнения cmdlet (CmdletLogs). Правило выявляет попытки добавления участников в группы рассылки, включая команды `Add-DistributionGroupMember`, `Update-DistributionGroupMember` и `Set-DistributionGroup` с параметрами, связанными с членством.	• Persistence (TA0003) • Account Manipulation (T1098)
RV-D-1188	Сбор адресов электронной почты из глобального списка	Атакующий, получивший доступ к учетной записи с правами управления Microsoft Exchange (включая делегированные или административные права), может использовать встроенный PowerShell-командлет `Get-GlobalAddressList` для получения дампа списков адресов Exchange, например глобальных списков адресов (GAL).	• Discovery (TA0007) • Account Discovery (T1087) • Email Account (T1087.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1189	Удаление политики фильтров ВПО в системе Exchange	Атакующий, получивший доступ к учетной записи с административными правами в Microsoft Exchange, может целенаправленно ослаблять защитные механизмы почтовой инфраструктуры. Одним из таких действий является удаление политики фильтрации вредоносного ПО, что приводит к отключению встроенной фильтрации защиты Exchange. После отключения данной защиты атакующий получает возможность доставлять вредоносные вложения и ссылки без срабатывания стандартных средств фильтрации, а также подготавливать почтовую среду для последующих атак (например, phishing).	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)
RV-D-1191	Подозрение на эксплуатацию ProxyShell	ProxyShell — общее название для трех уязвимостей в Microsoft Exchange, совокупная эксплуатация которых позволяет удаленному неавторизованному атакующему выполнить произвольный код на уязвимом сервере. Как сообщают исследователи, в настоящее время атакующие пытаются удаленно проэксплуатировать ProxyShell через Client Access Service (CAS), запущенный на порту 443 в Internet Information Services (IIS). Правило выявляет HTTP-запросы, характерные для попыток эксплуатации ProxyShell, на основе анализа URL-шаблонов и кодов ответа сервера.	• Initial Access (TA0001) • Exploit Public-Facing Application (T1190)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1211	Успешная эксплуатация ProxyShell	ProxyShell — общее название для трех уязвимостей в Microsoft Exchange, совокупная эксплуатация которых позволяет удаленному неавторизованному атакующему выполнить произвольный код на уязвимом сервере. Как сообщают исследователи, в настоящее время атакующие пытаются удаленно проэксплуатировать ProxyShell через Client Access Service (CAS), запущенный на порту 443 в Internet Information Services (IIS). Правило выявляет HTTP-запросы, характерные для успешной эксплуатации ProxyShell, на основе анализа URL-шаблонов и кодов ответа сервера.	• Initial Access (TA0001) • Exploit Public-Facing Application (T1190)
RV-D-1221	Эксплуатация ProxyLogon в Microsoft Exchange (CVE-2021-27065)	ProxyLogon — это цепочка критических уязвимостей в Microsoft Exchange Server, позволяющая удаленному неаутентифицированному лицу получить административный доступ к серверу и выполнить произвольный код. Эксплуатация уязвимостей осуществляется через компонент Client Access Service (CAS), доступный по HTTPS (порт 443), что делает атаку возможной напрямую из интернета. Данное правило отслеживает именно уязвимость CVE-2021-27065 из цепочки ProxyLogon — наиболее распространенный сценарий атаки, когда атакующий изменяет конфигурацию виртуального каталога OAB для внедрения вредоносного кода или установки веб-шелла на сервере Exchange.	• Initial Access (TA0001) • Exploit Public-Facing Application (T1190)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1227	Эксплуатация уязвимости ProxyNotShell (CVE-2022-41082)	ProxyNotShell — это цепочка уязвимостей в Microsoft Exchange Server, позволяющая удаленному атакующему выполнить произвольный код на сервере после успешной аутентификации. В отличие от ProxyLogon и ProxyShell, эксплуатация ProxyNotShell требует наличия действительных учетных данных, что делает атаку менее «шумной» и усложняет ее обнаружение на ранних этапах. Данное правило выявляет характерную последовательность действий, включающую успешную сетевую аутентификацию по протоколу NTLM к службе IIS (`w3wp.exe`) и последующий запуск интерпретаторов команд `cmd.exe` или `powershell.exe`, инициированный процессом `w3wp.exe` от имени учетной записи SYSTEM. Такая цепочка событий может указывать на выполнение произвольных команд в контексте сервиса Exchange.	• Initial Access (TA0001) • Exploit Public-Facing Application (T1190)
RV-D-1283	Обнаружение атаки Password Spraying на Exchange	Атакующие могут использовать механизмы аутентификации Microsoft Exchange для подбора учетных данных пользователей с целью получения несанкционированного доступа к почтовым ящикам и связанным сервисам. Данное правило выявляет признаки подбора пароля на основе анализа журналов IIS и фиксирует серию неудачных попыток входа в OWA, превышающую установленный порог в 5 неуспешных аутентификаций для нескольких учетных записей с одного IP-адреса в течение 5 минут.	• Credential Access (TA0006) • Brute Force (T1110) • Password Spraying (T1110.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1290	Пользователь из черного списка вошел в Exchange	Успешная аутентификация в Exchange с использованием учетной записи из черного списка указывает либо на ошибку в управлении доступом, либо на активное использование скомпрометированных учетных данных. Доступ к Exchange предоставляет атакующему возможность читать и отправлять почту, получать чувствительную информацию и развивать атаку внутри домена.	• Initial Access (TA0001) • Valid Accounts (T1078) • Domain Accounts (T1078.002)
RV-D-1291	Пользователь удалил доверие федерации из организации Exchange	Атакующий, получивший доступ к учетной записи с административными правами в Microsoft Exchange, может целенаправленно изменять доверительные отношения почтовой инфраструктуры с внешними организациями. Одним из таких действий является удаление федеративного доверия (Federation Trust), которое используется для федеративной аутентификации и взаимодействия в гибридных и межорганизационных сценариях.	• Defense Evasion (TA0005) • Domain or Tenant Policy Modification (T1484) • Trust Modification (T1484.002)
RV-D-1293	Пользователь создал/изменил политику назначения ролей управления	Атакующий, получивший доступ к учетной записи с административными правами в Microsoft Exchange, может изменить модель распределения привилегий внутри почтовой инфраструктуры. Одним из таких действий является создание, изменение или расширение политик назначения ролей управления (Role Assignment Policy).	• Privilege Escalation (TA0004) • Account Manipulation (T1098)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1295	Пользователь выполнил действие с ролью управления в Exchange	Атакующий, получивший доступ к учетной записи с административными правами в Microsoft Exchange, может изменять роли управления и состав административных групп (RBAC). Подобные действия позволяют повысить привилегии, закрепиться в системе, получить доступ к чувствительным операциям Exchange или ограничить доступ другим администраторам.	• Privilege Escalation (TA0004) • Account Manipulation (T1098)
RV-D-1296	Пользователь изменил/удалил критическую группу рассылки	Distribution Groups (группы рассылки) в Microsoft Exchange — это группы Active Directory с поддержкой почты, предназначенные исключительно для доставки электронных сообщений группе получателей (например, почтовые адреса сотрудников или сервисных аккаунтов). Изменение состава, параметров или структуры группы рассылки может привести к несанкционированному доступу к данным, распространяемым по почте. При добавлении своей учетной записи атакующий получает легитимный доступ к сообщениям, адресованным группе получателей. Это позволяет обходить механизмы прямого доступа к почтовым ящикам и получать чувствительную информацию через стандартную рассылку.	• Privilege Escalation (TA0004) • Impact (TA0040) • Account Manipulation (T1098) • Account Access Removal (T1531)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1297	Массовое удаление групп рассылок Exchange	В Microsoft Exchange группы рассылки (distribution groups) и динамические группы рассылки (dynamic distribution groups) используются для доставки почтовых сообщений группам пользователей и сервисных учетных записей. Такие группы часто задействованы в операционных процессах, служебных уведомлениях, автоматизированных рассылках и взаимодействии между подразделениями. Массовое удаление групп рассылки приводит к немедленному нарушению доставки почты, потере доступа пользователей к служебной информации и сбою бизнес-процессов, зависящих от электронной переписки.	• Impact (TA0040) • Account Access Removal (T1531)
RV-D-1307	Подбор пароля к учетным записям Exchange	Атакующие могут использовать механизмы аутентификации Microsoft Exchange для подбора учетных данных пользователей с целью получения несанкционированного доступа к почтовым ящикам и связанным сервисам. Данное правило выявляет признаки подбора пароля на основе анализа журналов IIS и фиксирует серию неудачных попыток входа в OWA, превышающую установленный порог в 10 неуспешных аутентификаций для одной учетной записи с одного IP-адреса в течение 5 минут.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1308	Успешный подбор пароля к учетным записям Exchange	Атакующие могут использовать механизмы аутентификации Microsoft Exchange для подбора учетных данных пользователей с целью получения несанкционированного доступа к почтовым ящикам и связанным сервисам. Данное правило выявляет признаки успешного подбора пароля, фиксируя не менее 10 неуспешных попыток входа для одной учетной записи с одного IP-адреса в течение 5 минут, после которых регистрируется успешная попытка. Такая последовательность событий с высокой вероятностью указывает на компрометацию учетной записи.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)

Прокси-серверы

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых прокси-серверов:

- Kaspersky Web Traffic Security
- Solar webProxy
- Squid

Kaspersky Web Traffic Security

- Kaspersky Web Traffic Security: настройка источника

Kaspersky Web Traffic Security: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Kaspersky Web Traffic Security в R-Vision SIEM.

Предварительные требования

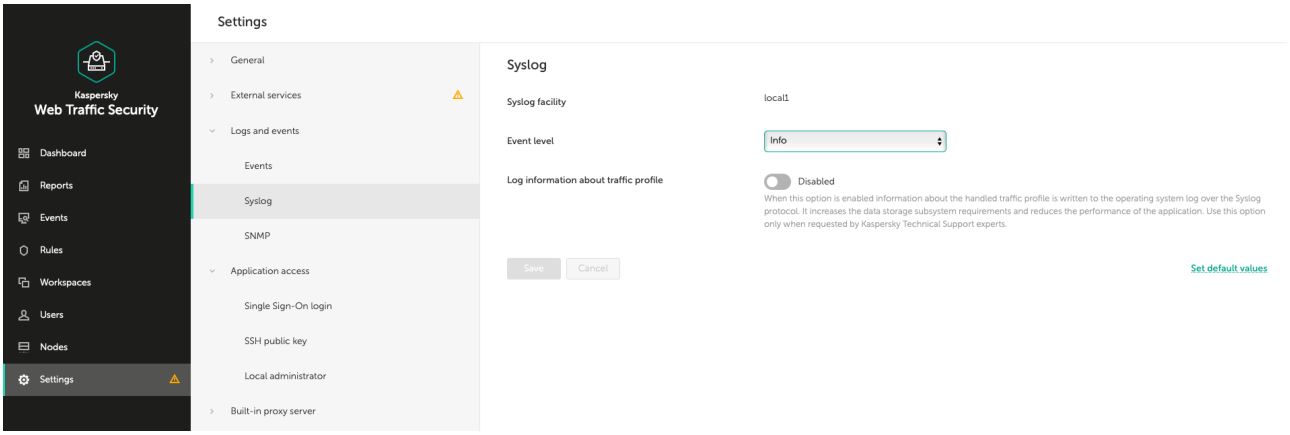
- Настройка отправки событий осуществляется с помощью Technical Support Mode, доступ к которому можно получить только через SSH-интерфейс. Для первичного входа в SSH-интерфейс необходимо загрузить свой персональный ключ доступа SSH через интерфейс администратора.
- Перед настройкой пересылки событий в R-Vision SIEM убедитесь, что обеспечена сетевая доступность нод кластера SIEM по целевому порту и протоколу для источника.

Настройка Kaspersky Web Traffic Security

Настройка журналирования Kaspersky Web Traffic Security

Для настройки rsyslog выполните следующие действия:

1. Подключитесь к консоли управления Kaspersky Web Traffic Security.
    - Если Kaspersky Web Traffic Security был установлен из ISO-файла, подключитесь к консоли управления Kaspersky Web Traffic Security с помощью учетной записи root по протоколу SSH.
    - Если Kaspersky Web Traffic Security был установлен из RPM- или DEB-пакета, запустите командную оболочку операционной системы для выполнения команд с полномочиями суперпользователя (администратора системы).
2. Из веб-меню администратора перейдите в меню настройки syslog. Запомните или запишите значение Syslog facility, используемого основной системой. Данное значение может меняться в зависимости от инсталляции.



3. События передаются во внешнюю SIEM-систему с помощью системной службы ведения журналов rsyslog. Убедитесь, что служба установлена и запущена, с помощью команды:

```
systemctl status rsyslog
```

   - Если служба установлена и запущена, ее статус будет `running`.
   - Если служба rsyslog не запущена или отсутствует, установите и активируйте службу rsyslog согласно документации вашей операционной системы.

4. Укажите адрес и порт подключения к серверу с SIEM-системой. Для этого создайте файл `/etc/rsyslog.d/kwts-cef-messages.conf` и добавьте в него следующие строки:

```
$ActionQueueFileName ForwardToSIEM5
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
$ActionResumeRetryCount -1
<facility>.* @@<IP-адрес любого доступного рабочего узла SIEM>:<Номер выбранного
порта вашей точки входа>
<facility>.* stop
```

   Здесь:

   - `<facility>` — значение Syslog facility, которое вы посмотрели на шаге 2. По умолчанию значение Syslog facility — `local5`.

5. Перезапустите службу rsyslog с помощью команды:

```
systemctl restart rsyslog
```

Отправка событий Kaspersky Web Traffic Security

Перед включением экспорта событий в формате CEF требуется установить пакет обновления `siem_logging_fixes.zip` на каждом узле кластера Kaspersky Web Traffic Security. Пакет обновления предоставляется по запросу в службу технической поддержки.

Выполните следующие шаги на каждом узле кластера, события с которого требуется

экспортировать в формате CEF.

1. Подключитесь к консоли управления Kaspersky Web Traffic Security.
   - Если Kaspersky Web Traffic Security был установлен из ISO-файла, подключитесь к консоли управления виртуальной машиной Kaspersky Web Traffic Security под учетной записью root, используя закрытый ключ SSH. Будет осуществлен вход в Technical Support Mode.
   - Если Kaspersky Web Traffic Security был установлен из RPM- или DEB-пакета, запустите командную оболочку операционной системы для выполнения команд с полномочиями суперпользователя (администратора системы).
2. Перейдите в каталог `/opt/kaspersky/kwts/share/templates/core_settings` и создайте резервную копию файла `event_logger.json.template` с помощью команды:

   ```
   cp -p event_logger.json.template event_logger.json.template.backup
   ```

3. Откройте файл `event_logger.json.template` в режиме редактирования и, соблюдая синтаксис и структуру JSON-файла, в секции `siemSettings` укажите следующие значения параметров:
   - `enabled: true`;
   - `facility: Local5` — указанный ранее на шаге настройки rsyslog;
   - `logLevel: Info`.
4. В веб-интерфейсе приложения в разделе **Параметры** → **Журналы и события** внесите изменения в значение любого параметра и нажмите на кнопку **Сохранить**. Это необходимо для синхронизации параметров между узлами кластера и применения изменений, внесенных в конфигурационный файл. После этого можно вернуть исходное значение измененного параметра.
5. Убедитесь, что изменения применены, с помощью команды:

   ```
   /opt/kaspersky/kwts/bin/kwts-control --get-settings 20 --format json | grep -A 4
   siemSettings
   ```

   Результат выполнения команды должен содержать параметры со значениями, указанными на шаге 3.

Экспорт событий в формате CEF настроен.

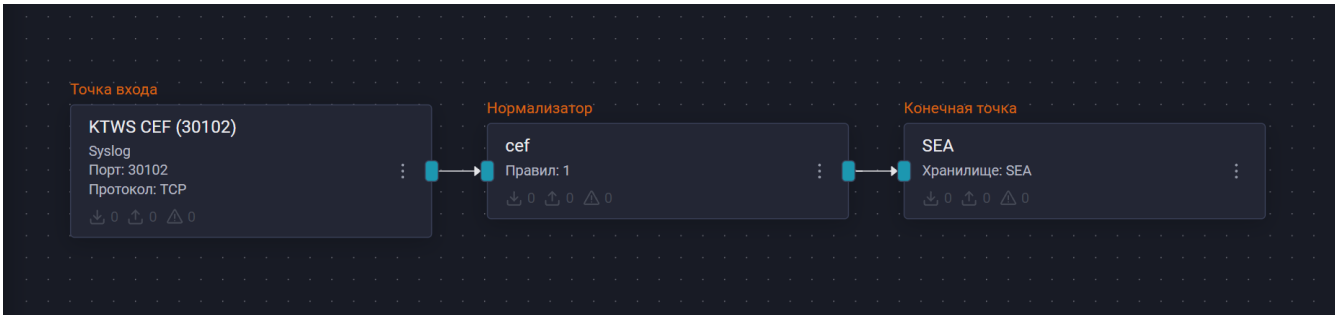
Настройка в R-Vision SIEM

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в диапазоне 30 000—32 000, указанное ранее в разделе отправки событий Kaspersky Web Traffic Security.
   - Протокол: выберите вариант в соответствии с настройками на стороне Kaspersky Web Traffic

Security.

3. Добавьте на конвейер элемент **Нормализатор** с правилом **Kaspersky Web Traffic Security** (идентификатор правила: **RV-N-185**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

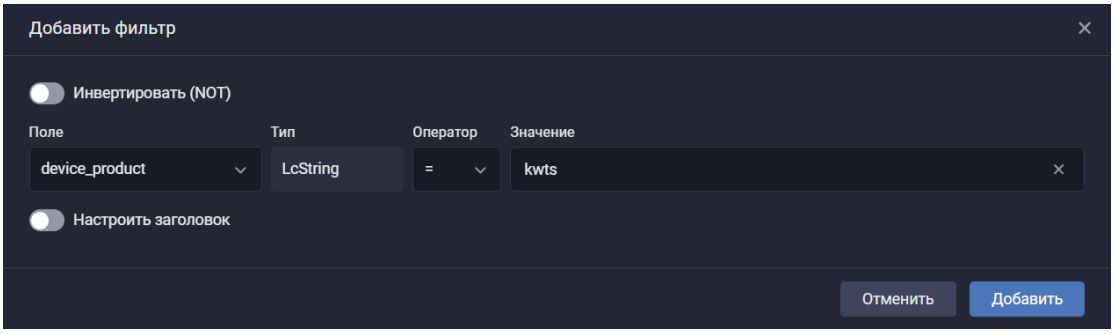
Пример конфигурации конвейера:



Если настройка выполнена корректно, после настройки передачи событий в хранилище начнут поступать события Kaspersky Web Traffic Security.

Найти события Kaspersky Web Traffic Security в хранилище можно по следующему фильтру:

```
device_product = "kwts"
```



Solar webProxy

- Solar webProxy: настройка источника
- Solar webProxy: правила корреляции

Solar webProxy: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Solar webProxy в R-Vision SIEM.

Предварительные требования

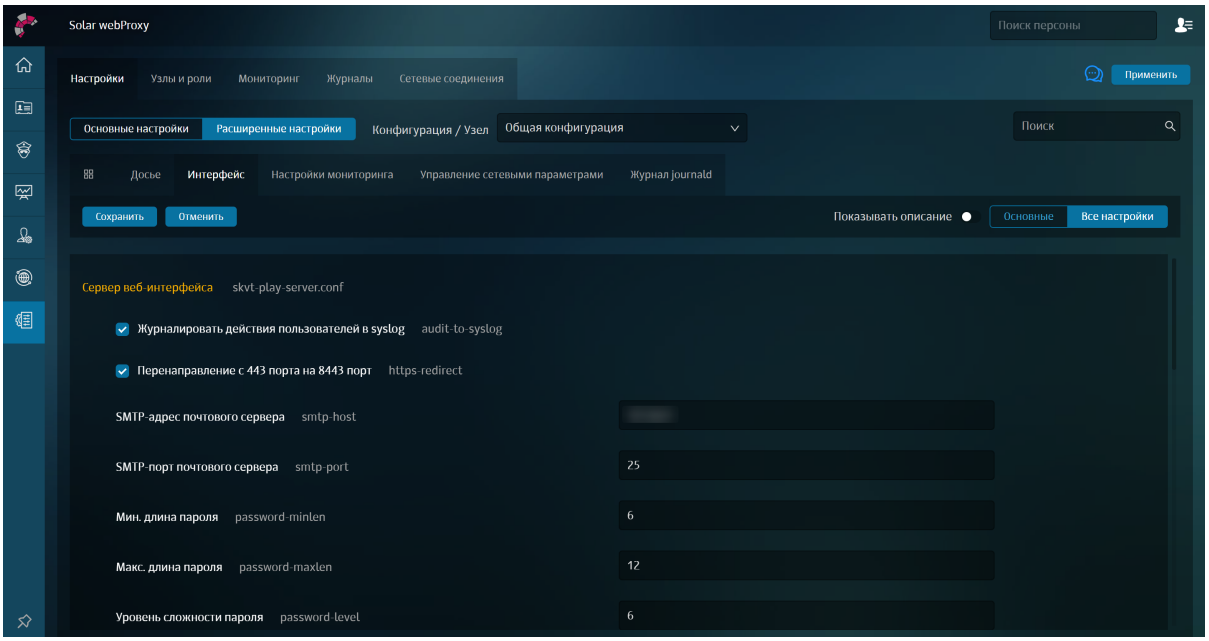
Перед настройкой сбора событий в R-Vision SIEM убедитесь в выполнении следующих условий:

- Сетевая связность между сервером Solar webProxy и R-Vision SIEM (или промежуточным узлом) обеспечена, а необходимые порты открыты.
- Учетная запись имеет права администратора для настройки журналирования.

Настройка Solar webProxy

Для настройки аудита пользователей Solar webProxy выполните следующие действия:

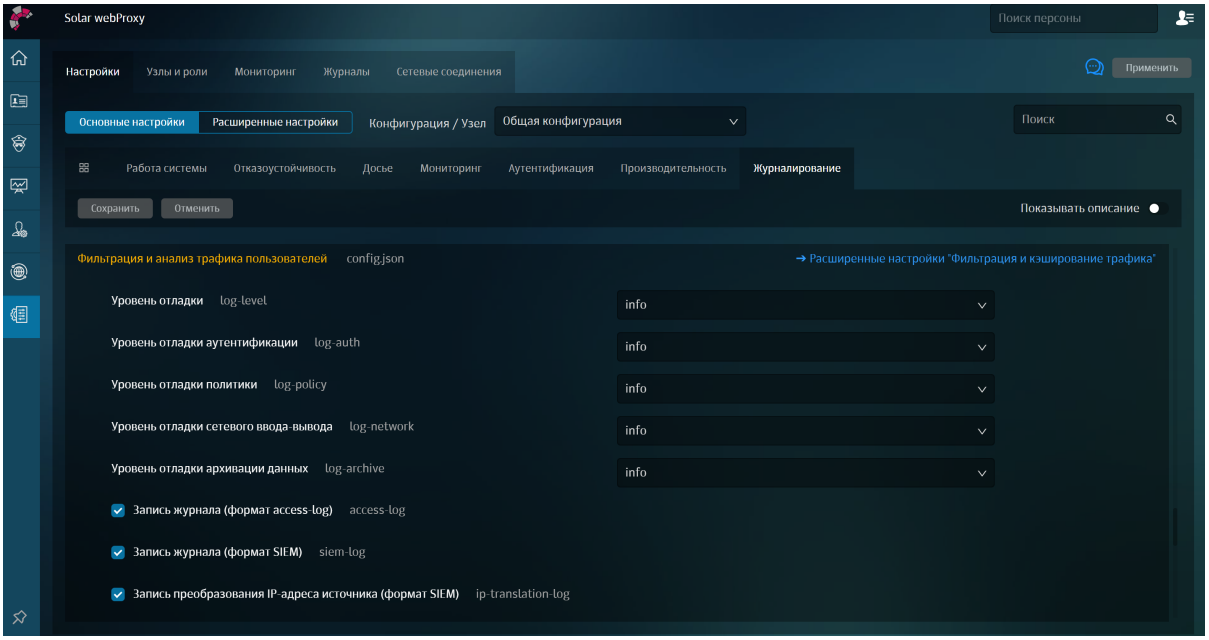
1. В разделе **Система** → **Основные настройки** → **Журналирование** → **Сервер веб-интерфейса** установите флажок **Журналировать действия пользователей в syslog**.



2. Нажмите **Сохранить** и **Применить**.

Для настройки журналирования `access.log` выполните следующие действия:

1. В разделе **Система** → **Основные настройки** → **Журналирование** → **Фильтрация и анализ трафика пользователей** установите флажки **Запись журнала (формат access-log)**, **Запись журнала (формат SIEM)**, **Запись преобразования IP-адреса источника (формат SIEM)**.



2. Нажмите **Сохранить** и **Применить**.

Настройка отправки событий в R-Vision SIEM

Чтобы настроить отправку событий Solar webProxy, выполните следующие шаги:

1. Откройте конфигурационный файл `syslog-ng` по пути `/etc/syslog-ng/conf.d/10-skvtlog.conf`.
2. Добавьте в файл следующие правила:

```
source skvt {
        file("/opt/dozor/var/log/skvt-play-server/current" flags(no-parse));
};

destination d_siem {
    <protocol>("<target>" port(<port>));
};

rewrite r_add_tag {
    set("webproxy", value("PROGRAM"));
};

log {
    source(skvt);
    rewrite(r_add_tag);
    destination(d_siem);
    flags(final);
};

filter access {
    message("acc-ip:") and program("java");
};

rewrite r_tag {
```

```
    set("webproxy-access", value("PROGRAM"));
};

log {
    source(s_src);
    filter(access);
    rewrite(r_tag);
    destination(d_siem);
};
```

Здесь:

- `<target>`: IP-адрес или полное доменное имя (FQDN) коллектора R-Vision SIEM.
- `<port>`: порт точки входа `Syslog` на конвейере R-Vision SIEM.
- `<protocol>`: сетевой протокол (`tcp` или `udp`).

3. Перезапустите службу `syslog-ng` с помощью команды:

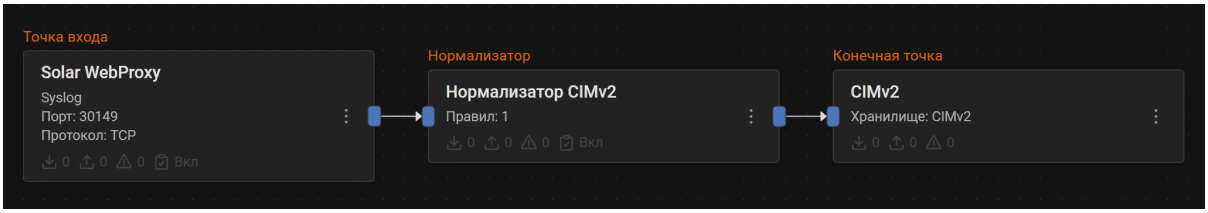
```
systemctl restart syslog-ng
```

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне Solar webProxy.
   - Протокол: выберите вариант в соответствии с настройками на стороне Solar webProxy.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Solar webProxy** (идентификаторы правил: *RV-N-331, RV-N-351).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

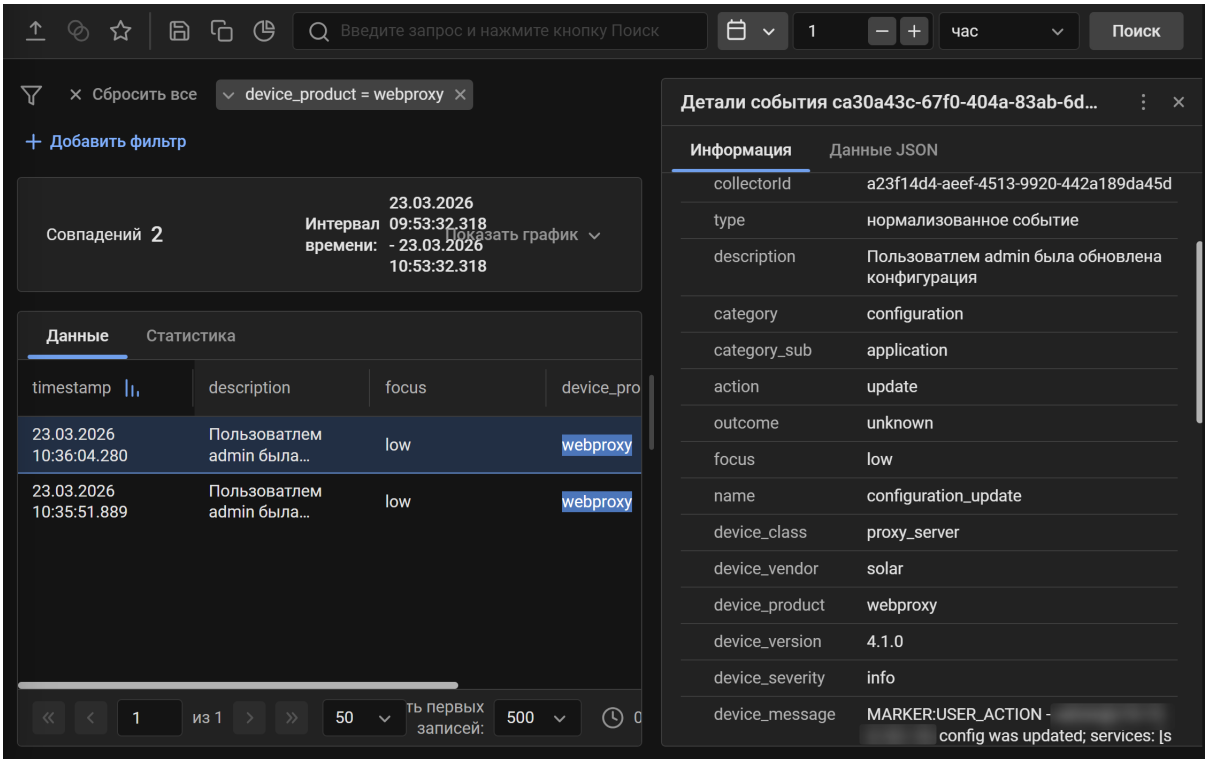
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Solar webProxy.[TIP]

Найти события Solar webProxy в хранилище можно по следующему фильтру:

```
device_product = "webproxy"
```



Solar webProxy: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1542	Создание нового пользователя в Solar Web Proxy	Атакующие после получения доступа к Solar Web Proxy могут попробовать закрепиться в системе с помощью создания нового пользователя.	• Persistence (TA0003) • Create Account (T1136) • Local Account (T1136.001) • Domain Account (T1136.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1543	Вход привилегированной учетной записи с неизвестного IP в SWP	После получения доступа к привилегированной учетной записи атакующие, используя эту запись, могут зайти на сервер с повышенными правами для проведения дальнейших деструктивных действий. Данное правило позволяет фиксировать подключения под привилегированными учетными записями с неизвестных источников.	• Initial Access (TA0001) • Valid Accounts (T1078) • Domain Accounts (T1078.002) • Local Accounts (T1078.003)
RV-D-1544	Изменены параметры внешних подключений на Solar Web Proxy	После получения доступа к системе Solar Web Proxy, атакующие могут изменить параметры внешних подключений для изменения или удаления `proxy` или `ICAP` серверов для проведения дальнейших деструктивных действий.	• Defense Evasion (TA0005) • Impair Defenses (T1562)
RV-D-1547	Изменение критичных ролей Solar Web Proxy	После получения доступа к системе Solar Web Proxy атакующие могут создать новую роль с привилегированными правами на редактирование параметров системы или добавить критичные права для существующей группы для дальнейшего развития атаки.	• Persistence (TA0003) • Account Manipulation (T1098)
RV-D-1573	Изменение правил межсетевого экранирования и доступа в Solar Web Proxy	После получения доступа к системе Solar Web Proxy атакующие могут изменить, добавить или удалить правила для политик SWP, тем самым изменить правила доступа, фильтрации трафика, маршрутизации соединений и другие, что может позволить продолжить перемещение по сети.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001) • Disable or Modify System Firewall (T1562.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1578	Изменены критичные параметры системы Solar Web Proxy	Правило выявляет факты модификации критических параметров конфигурации на сервере Solar Web Proxy. После успешной компрометации административного доступа атакующие могут целенаправленно изменять системные настройки для снижения уровня защищенности инфраструктуры и сокрытия дальнейших вредоносных действий. Подобные изменения конфигурации направлены на создание слепых зон для средств детектирования, что позволяет атакующим организовать скрытые каналы связи с внешними управляющими серверами, беспрепятственно осуществлять эксфильтрацию данных и обходить корпоративные политики веб-фильтрации.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)

Squid

- Squid: настройка источника

Squid: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Squid в R-Vision SIEM.

Настройка Squid

В настоящем руководстве рассматривается передача событий с помощью службы rsyslog. Предполагается, что rsyslog на станции с ОС Linux уже установлен.



Журналирование событий службы Squid по умолчанию ведется в директории `/var/log/squid`.

Для корректного отображения в R-Vision SIEM событий журнала access настройте на сервере Squid формат сообщений согласно следующим рекомендациям:

1. В файле `/etc/squid/squid.conf` найдите строку, задающую формат логов, и замените ее на следующий вариант:

```
logformat custom %>a - %un [%tl] "%rm %ru %Sh/%<A %mt %Ss" %03>Hs %<st
```

```
access_log daemon:/var/log/squid/access.log custom
```

2. Настройте передачу событий из файла. Для этого создайте файл `/etc/rsyslog.d/10-Squid.conf` со следующим содержимым:

```
module(load="imfile")

input(
    type="imfile"
    File="/var/log/squid/access.log"
    Tag="Squid"
    Severity="info"
    Facility="local4"
)

if $syslogtag == 'Squid' then {
  action(type="omfwd" target="<target>" port="<port>" protocol="<protocol>")
  stop
}
```

   Здесь:

   - `<target>` — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
   - `<port>` — порт точки входа Syslog на конвейере SIEM.
   - `<protocol>` — сетевой протокол: `tcp` или `udp`.

3. Перезапустите службу rsyslog с помощью команды:

```
systemctl restart rsyslog
```

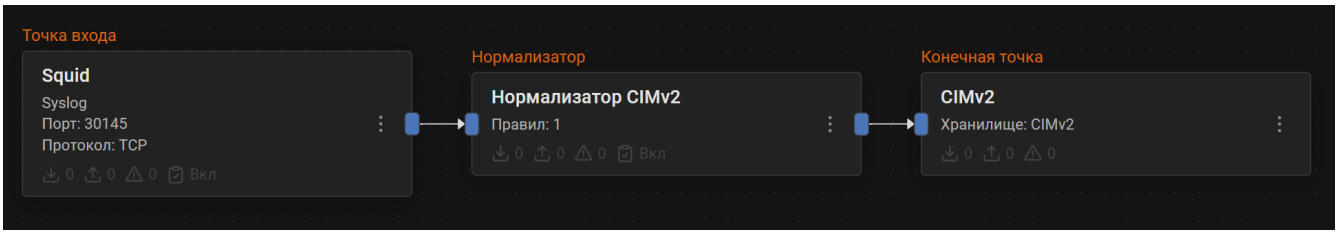
Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне Squid.
   - Протокол: выберите вариант в соответствии с настройками на стороне Squid.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Squid** (идентификатор правила: **RV-N-309**).
4. Соедините нормализатор с точкой входа.

5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

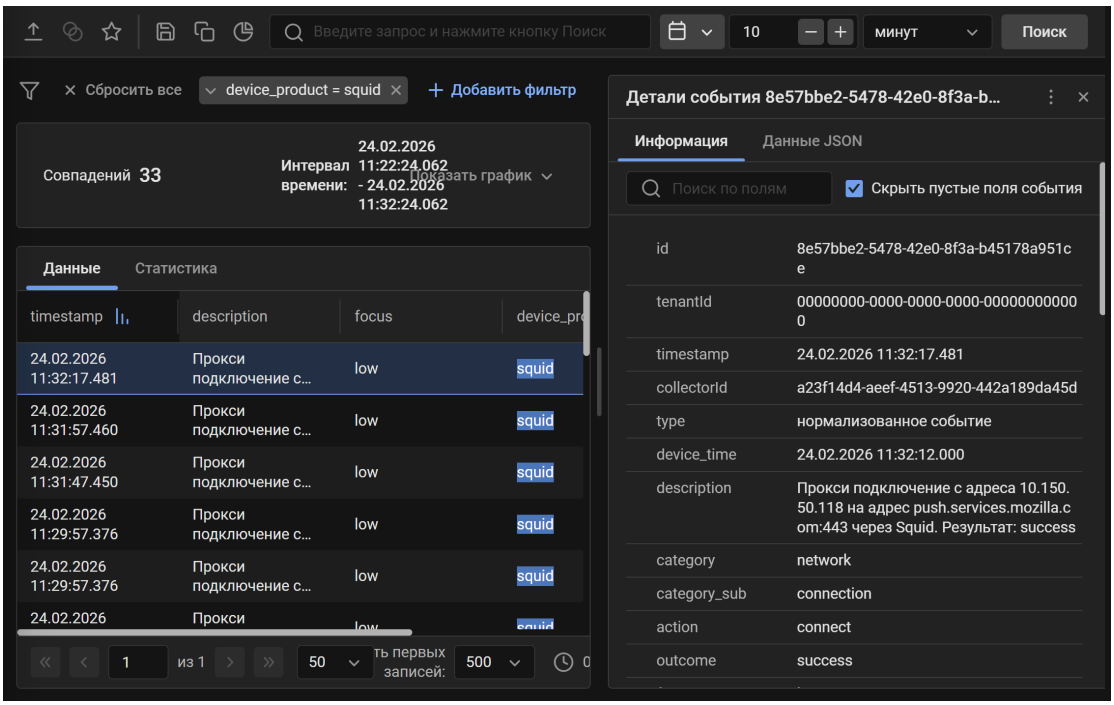
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Squid.

Найти события Squid в хранилище можно по следующему фильтру:

```
device_product = "squid"
```



Сетевые устройства

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых сетевых устройств:

- Cisco IOS
- Cisco IOS XE
- Cisco IOS XR
- Cisco NetFlow
- Cisco Nexus
- eltex-vesr.pdf
- Fortinet FortiAnalyzer
- HP ProCurve
- HPE ArubaOS-CX
- IPFIX
- MikroTik RouterOS
- Netgate pfSense

Cisco IOS

- Cisco IOS: настройка источника

Cisco IOS: настройка источника

Данное руководство описывает процесс настройки сбора событий Cisco IOS и их отправки в R-Vision SIEM.

Предварительные требования

Перед настройкой пересылки событий в R-Vision SIEM убедитесь, что сетевая связность между устройствами Cisco IOS и R-Vision SIEM (или промежуточным узлом) обеспечена, а необходимые порты открыты.

Настройка Cisco IOS

Настройка отправки событий в R-Vision SIEM

Отправка сообщений осуществляется посредством протокола syslog. Для настройки передачи событий выполните следующие команды в режиме глобальной конфигурации (`configure terminal`):

```
logging on
logging trap informational
logging facility local7
logging host <target> transport <protocol> port <port>
```

```
logging source-interface <interface>
```

Здесь:

- `logging on` — включение логирования.
- `logging trap informational` — установка уровня логирования (`informational`).
- `logging facility local7` — указание категории источника сообщений (`facility`).
- `<target>` — IP-адрес узла кластера K8s, на котором запущен коллектор.
- `<protocol>` — протокол передачи (в примере конфигурации используется `tcp`).
- `<port>` — порт точки входа Syslog на конвейере SIEM.
- `<interface>` — интерфейс Cisco IOS, с которого будут отправляться события (`g1/0/1`).



При создании точки входа указывайте любой свободный порт больше 30000. Точка входа в конвейере должна быть создана заранее.

Настройка в R-Vision SIEM

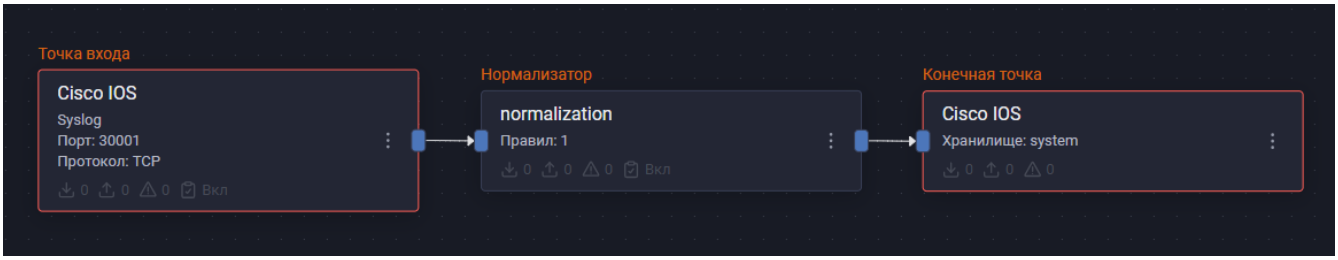
Для настройки сбора и нормализации событий Cisco IOS в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите произвольное, понятное название.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне источника (любой свободный порт больше 30000).
   - Протокол: выберите вариант в соответствии с настройками на стороне источника.
3. Добавьте элемент **VRL-трансформация** со следующим кодом:

   ```
   .device_product = "ios"
   ```

4. Соедините добавленный блок VRL-трансформации с точкой входа.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **Cisco IOS** (идентификатор правила: **RV-N-244**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

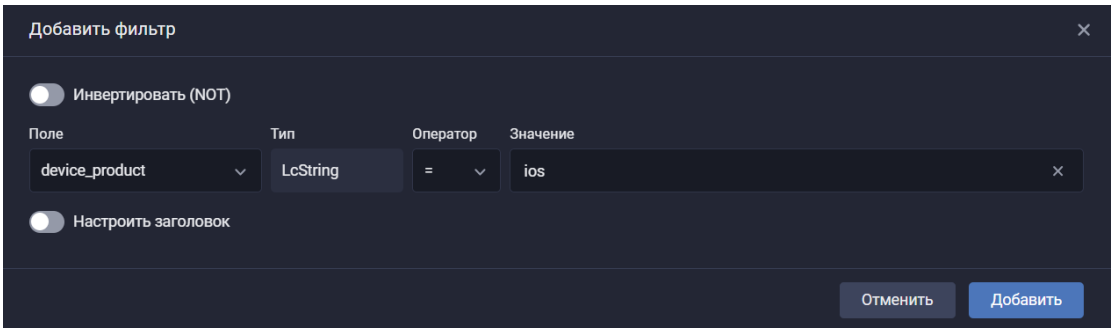
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Cisco IOS.

Найти события Cisco IOS в хранилище можно по следующему фильтру:

```
device_product = "ios"
```



Cisco IOS XE

- Cisco IOS XE: настройка источника

Cisco IOS XE: настройка источника

Данное руководство описывает процесс настройки сбора событий Cisco IOS XE и их отправки в R-Vision SIEM.

Предварительные требования

Перед настройкой пересылки событий в R-Vision SIEM убедитесь, что сетевая связность между устройствами Cisco IOS XE и R-Vision SIEM (или промежуточным узлом) обеспечена, а необходимые порты открыты.

Настройка Cisco IOS XE

Настройка отправки событий в R-Vision SIEM

Отправка сообщений осуществляется посредством протокола `syslog`. Для настройки передачи событий выполните следующие команды в режиме глобальной конфигурации (`configure terminal`):

```
# Укажите IP-адрес вашего сервера мониторинга
logging host <target> transport <protocol> port <port>
```

```
# Уровень важности логов для отправки (7 - всё, 6 - информационные, 4 -
предупреждения)
logging trap informational

# Укажите категорию источника сообщений (`facility`)
logging facility local7

# Укажите интерфейс, с которого будут уходить логи (важно для VPN/VRF)
logging source-interface <interface>

# Укажите использовать имя хоста в заголовке логов
hostname <router-hostname>
logging origin-id hostname

# Настройте метки времени в логах
service timestamps log datetime msec localtime show-timezone year
no service sequence-numbers

# Настраиваем аудит
archive
 log config
  logging enable
  notify syslog
  hidekeys  # Скрывать пароли в логах
 exit
exit

# В режиме (config)
login on-failure log   # Логировать неудачные попытки входа
login on-success log   # Логировать успешные входы
exit

# Сохраняем настройки
write mem
```

Здесь:

- `<router-hostname>`: имя хоста Cisco IOS XE.
- `<target>`: IP-адрес узла кластера K8s, на котором запущен коллектор.
- `<protocol>`: транспортный протокол (`tcp` или `udp`).
- `<port>`: порт точки входа на конвейере R-Vision SIEM.
- `<interface>`: интерфейс Cisco IOS XE, с которого будут отправляться события (`g1/0/1`).



При создании точки входа указывайте любой свободный порт больше 30000. Точка входа в конвейере должна быть создана заранее.

Настройка в R-Vision SIEM

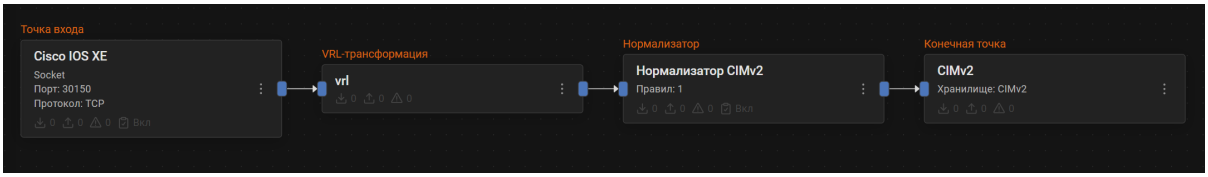
Для настройки сбора и нормализации событий Cisco IOS XE в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM перейдите в раздел **Ресурсы** → **Коллекторы** и откройте карточку коллектора.
2. На вкладке **Обогащение** добавьте таблицы обогащения **cisco_ios_xe_categorization** (идентификаторы таблиц: **RV-ET-42**, **RV-ET-43**).
3. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
4. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - **Название**: введите название точки входа.
   - **Тип точки входа**: выберите вариант **Socket**.
   - **Порт точки входа**: введите значение в соответствии с настройками на стороне источника (любой свободный порт больше 30000).
   - **Протокол**: выберите вариант в соответствии с настройками на стороне источника.
5. Добавьте элемент **VRL-трансформация** со следующим кодом:

```
.device_product = "ios_xe"
```

6. Соедините добавленную точку входа и VRL-трансформацию.
7. Добавьте на конвейер элемент **Нормализатор** с правилом **Cisco IOS XE** (идентификатор правила: **RV-N-330**).
8. Соедините нормализатор с VRL-трансформацией.
9. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
10. Соедините конечную точку с нормализатором.
11. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

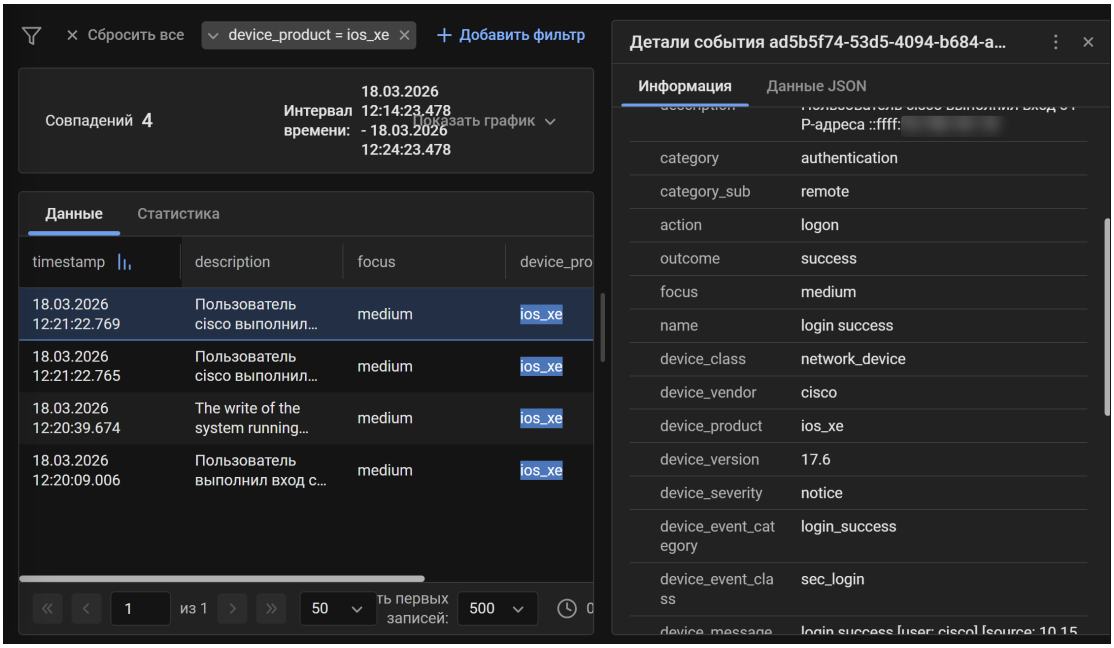


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Cisco IOS XE.



Найти события Cisco IOS XE в хранилище можно по следующему фильтру:

```
device_product = "ios_xe"
```



Cisco IOS XR

- Cisco IOS XR: настройка источника

Cisco IOS XR: настройка источника

Данное руководство описывает процесс настройки сбора событий Cisco IOS XR и их отправки в R-Vision SIEM.

Предварительные требования

Перед настройкой пересылки событий в R-Vision SIEM убедитесь, что сетевая связность между устройствами Cisco IOS XR и R-Vision SIEM (или промежуточным узлом) обеспечена, а необходимые порты открыты.

Настройка Cisco IOS XR

Настройка отправки событий в R-Vision SIEM

Отправка сообщений осуществляется посредством протокола `syslog`. Для настройки передачи событий выполните следующие команды в режиме глобальной конфигурации (`configure terminal`):

```
conf t
# 1. Основные параметры системы
hostname <router-hostname>
service timestamps log datetime msec show-timezone year

# 2. Настройка удаленного Syslog-сервера
# Указываем IP, VRF (обычно default) и кастомный порт (если нужно)
logging <target> vrf default port <port>

# Указываем интерфейс-источник (чтобы пакеты не отбивались фаерволом сервера)
```

```
logging source-interface <interface> vrf default

# Уровень детализации: informational (5)
logging trap informational

# 3. Логирование действий (кто и что настраивал)
logging events display-location

# Сохраняем настройки
commit
```

Здесь:

- `<router-hostname>`: имя хоста Cisco IOS XR.
- `<target>`: IP-адрес узла кластера K8s, на котором запущен коллектор.
- `<port>`: порт точки входа `Socket` на конвейере R-Vision SIEM.
- `<interface>`: интерфейс Cisco IOS XR, с которого будут отправляться события (`g1/0/1`).



При создании точки входа указывайте любой свободный порт больше 30000. Точка входа в конвейере должна быть создана заранее.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий Cisco IOS XR в R-Vision SIEM выполните следующие шаги:

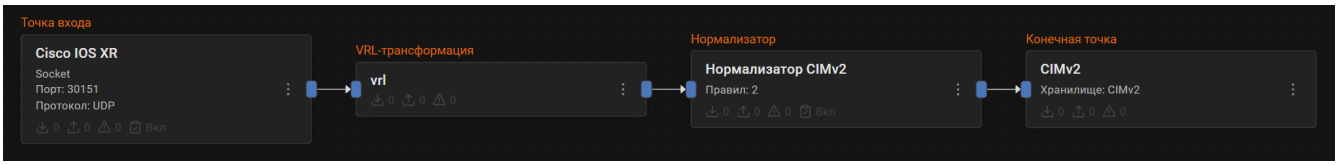
1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - **Название**: введите название точки входа.
   - **Тип точки входа**: выберите вариант **Socket**.
   - **Порт точки входа**: введите значение в соответствии с настройками на стороне источника (любой свободный порт больше 30000).
   - Протокол: выберите вариант в соответствии с настройками на стороне источника.
3. Добавьте элемент **VRL-трансформация** со следующим кодом:

   ```
   .device_product = "ios_xr"
   ```

4. Соедините добавленный блок VRL-трансформации с точкой входа.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **Cisco IOS XR** (идентификатор правила: **RV-N-333**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.

9. Сохраните и установите конфигурацию конвейера.

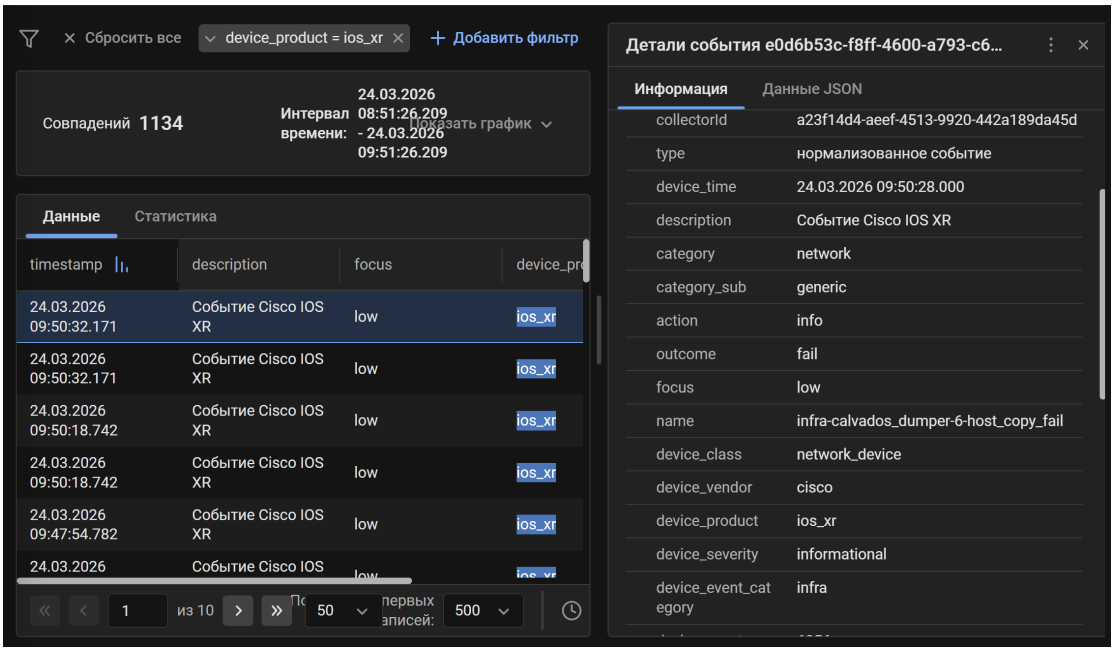
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Cisco IOS XR.

Найти события Cisco IOS XR в хранилище можно по следующему фильтру:

```
device_product = "ios_xr"
```



Cisco NetFlow

Данный раздел содержит список инструкций по настройке источника NetFlow:

- NetFlow Version 9: настройка источника

NetFlow Version 9: настройка источника

Данное руководство описывает процесс настройки сбора событий NetFlow Version 9 и их отправки в R-Vision SIEM.

Предварительные требования

Перед настройкой сбора событий в R-Vision SIEM убедитесь в выполнении следующих условий:

- У получаемого R-Vision SIEM потока NetFlow данные должны быть структурированы в

соответствии со стандартом Cisco.

Настройка NetFlow Version 9

Настройка NetFlow Version 9 различается в зависимости от операционной системы сетевого оборудования (IOS-XE, IOS-XR, NX-OS и т.д.). Поэтому рекомендуется производить настройку в соответствии с эксплуатационной документацией производителя вашего оборудования.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM в карточке коллектора перейдите на вкладку **Обогащение**.
2. Добавьте таблицу обогащения `netflow_tcp_flags`.
3. Создайте новый конвейер в данном коллекторе.
4. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - **Название**: введите произвольное, понятное название.
   - **Тип точки входа**: выберите вариант **NetFlow**.
   - **Порт точки входа**: введите значение в диапазоне `30000–32767`.
   - **Протокол**: выберите вариант **UDP**.
5. Добавьте на конвейер элемент **VRL-трансформация** со следующим содержимым:

```
main = .raw.netflow_packets[0].V9.flowsets[0].data.data_fields
if is_null(main) {
    . = .raw.netflow_packets[0].V9.flowsets[1].data.data_fields
} else {
    . = main
}
```

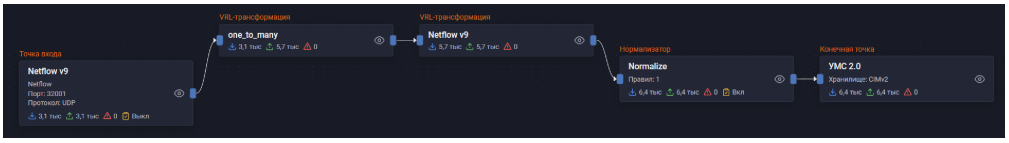
6. Соедините добавленный блок VRL-трансформации с точкой входа.
7. Добавьте на конвейер еще один элемент **VRL-трансформация** со следующим содержимым:

```
.raw = .
.id = uuid_v4()
.timestamp= %vector.ingest_timestamp
.tenantId = "${TENANT_ID}"
.collectorId = "${COLLECTOR_ID}"
.type = 0
.device_product = "netflow_v9"
```

8. Соедините второй блок VRL-трансформации с первым.
9. Добавьте на конвейер элемент **Нормализатор** с правилом **NetFlow v9** (идентификатор правила: **RV-N-272**).

10. Соедините нормализатор со вторым блоком VRL-трансформации.
11. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
12. Соедините конечную точку с нормализатором.
13. Сохраните и установите конфигурацию конвейера.

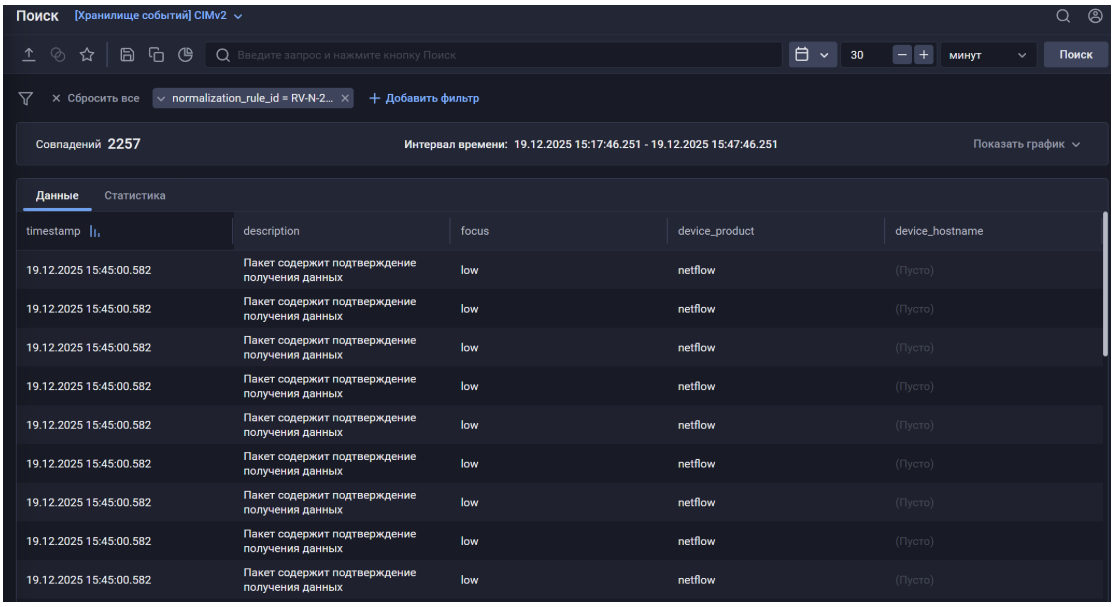
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события из NetFlow v9.

Найти события NetFlow Version 9 в хранилище можно по следующему фильтру:

```
normalization_rule_id = "RV-N-272"
```



Cisco Nexus

- Cisco Nexus: настройка источника

Cisco Nexus: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Cisco Nexus в R-Vision SIEM.

Предварительные требования

Перед настройкой пересылки событий в R-Vision SIEM убедитесь, что сетевая связность между устройствами Cisco Nexus и R-Vision SIEM (или промежуточным узлом) обеспечена, а необходимые

порты открыты.

Настройка Cisco Nexus

Настройка отправки событий в R-Vision SIEM

Отправка сообщений осуществляется посредством протокола `syslog`.

Для настройки передачи событий выполните следующие команды в режиме глобальной конфигурации (`configure terminal`):

```
# Укажите IP-адрес вашего сервера и уровень детализации (6 — Informational).
logging server <target> 6 port <port>

# Укажите интерфейс, с которого будут уходить логи.
logging source-interface <interface>

# Настройте метки времени в логах.
logging timestamp milliseconds

# Укажите требование использовать имя хоста в заголовке логов.
logging origin-id <router-hostname>

# Укажите формат логов.
logging rfc-strict 5424

# Сохраните настройки.
copy running-config startup-config
```

Здесь:

- `<router-hostname>` — имя хоста Cisco Nexus;
- `<target>` — IP-адрес узла кластера K8s, на котором запущен коллектор;
- `<port>` — порт точки входа **Socket** на конвейере R-Vision SIEM;
- `<interface>` — интерфейс Cisco Nexus, с которого будут отправляться события, например, `ethernet 1/1`.



При создании точки входа указывайте любой свободный порт больше 30 000. Точка входа в конвейере должна быть создана заранее.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
    - Название: введите название точки входа.

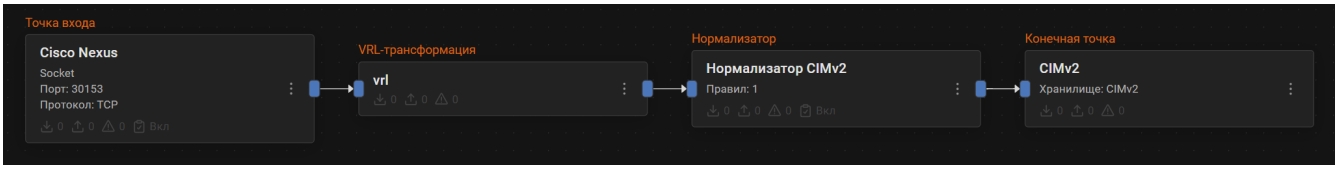
- Тип точки входа: выберите вариант **Socket**.
- Порт точки входа: введите значение в соответствии с настройками на стороне Cisco Nexus.
- Протокол: выберите вариант в соответствии с настройками на стороне Cisco Nexus.

3. Добавьте на конвейер элемент **VRL-трансформация** со следующим кодом:

```
.device_product = "nexus"
```

4. Соедините точку входа с VRL-трансформацией.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **Cisco Nexus** (идентификатор правила: **RV-N-339**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

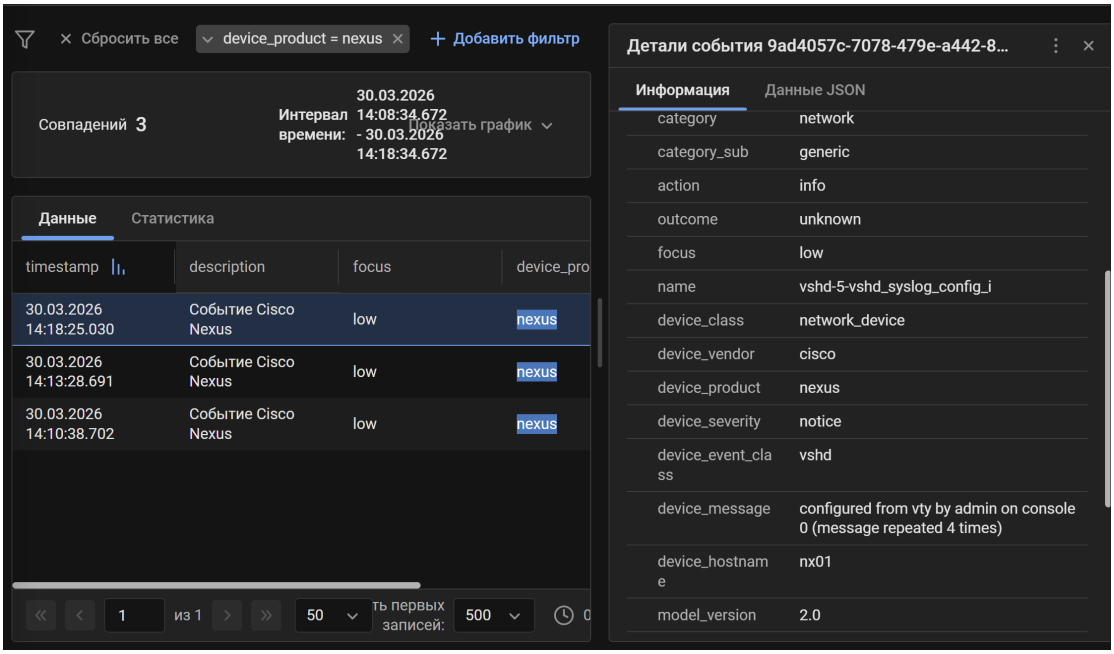
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Cisco Nexus.

Найти события Cisco Nexus в хранилище можно по следующему фильтру:

```
device_product = "nexus"
```



Eltex ESR

- Eltex ESR: настройка источника

Eltex ESR: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий физических и виртуальных маршрутизаторов семейства Eltex ESR в R-Vision SIEM.

Предварительные требования

Перед настройкой пересылки событий в R-Vision SIEM убедитесь, что сетевая связность между устройством Eltex ESR и R-Vision SIEM, или промежуточным узлом, обеспечена, а необходимые порты открыты.

Настройка Eltex ESR

Конфигурация логирования

1. Перейдите в меню конфигурации с помощью команды:

   ```
   configure
   ```

2. Настройте сбор логов из необходимых журналов, выполнив для каждого из них команду:

   ```
   logging <journal-name>
   ```

   Здесь:

   - `<journal-name>` — имя журнала.



Список поддерживаемых журналов для других моделей и версий описан в документации производителя.

Поддерживаются следующие журналы:

- `aaa` — журнал авторизации и аутентификации.
- `acl` — журнал работы со списками контроля доступа.
- `firewall` — журнал параметров файрвола.
- `ips` — журнал IP-адресов.
- `login` — журнал параметров логина.
- `nat` — журнал NAT.
- `service` — журнал сервисных параметров.
- `syslog` — журнал параметров syslog.
- `userinfo` — журнал изменений в профиле пользователя.

3. Настройте отправку логов в syslog-коллектор с помощью команды:

```
syslog host <hostname>
```

Здесь:

- `<hostname>` — имя вашего хоста в системе Eltex.

4. Перейдите в меню настройки вашего хоста. Для отправки логов укажите следующие параметры конфигурации:
   - `remote-address` — адрес syslog-коллектора, поддерживаются IPv4- и IPv6-адреса;
   - `port` — порт прослушивания syslog-коллектора;
   - `severity` — уровень логирования, начиная с которого события будут передаваться в SIEM. Доступные уровни логирования:
     - `emerg` — критическая ситуация.
     - `alert` — небезопасные действия.
     - `crit` — проверка состояния.
     - `error` — ошибка.
     - `warning` — вывод предупреждений.
     - `notice` — события в рамках ожидаемого поведения.
     - `info` — статистика.
     - `debug` — отладка поступающих сообщений.
     - `none` — отсутствие передачи событий.
   - `transport` — протокол передачи данных: `udp` или `tcp`.

Пример общей настройки параметров:

```
remote-address <address>
port 30104
severity info
transport udp
```

5. Выйдите в основное меню настройки с помощью команды:

```
exit
```



Команду необходимо ввести два раза.

6. Примените изменения и запишите их в память устройства с помощью команд:

```
commit
confirm
```

7. Сохраните конфигурацию с помощью команды:

```
save
```

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

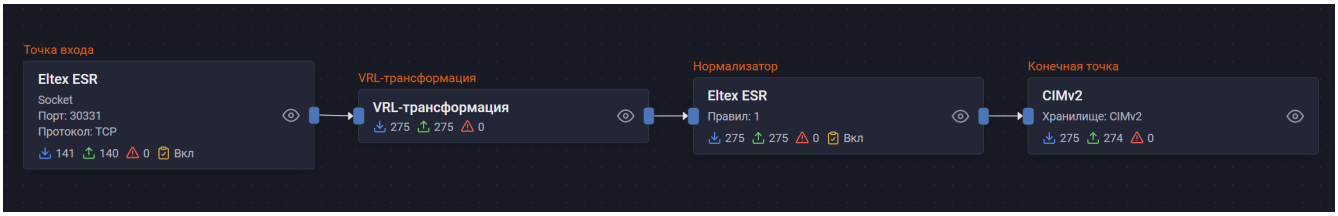
1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Socket**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне Eltex ESR.
   - Протокол: выберите вариант в соответствии с настройками на стороне Eltex ESR.
3. Добавьте на конвейер элемент **VRL-трансформация** со следующим кодом:

```
.device_product = "esr"
```

4. Соедините точку входа с VRL-трансформацией.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **Eltex ESR** (идентификатор правила: **RV-N-345**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.

8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

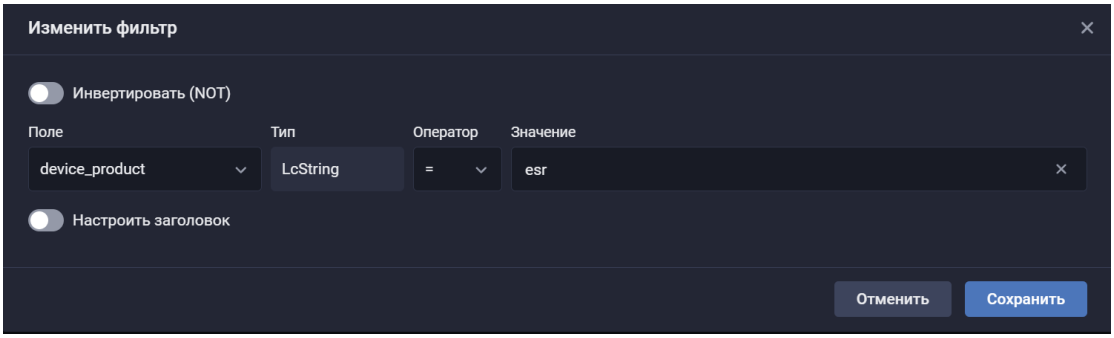
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Eltex ESR.

Найти события Eltex ESR в хранилище можно по следующему фильтру:

```
device_product = "esr"
```



Fortinet FortiAnalyzer

- Fortinet FortiAnalyzer: настройка источника

Fortinet FortiAnalyzer: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Fortinet FortiAnalyzer в R-Vision SIEM.

Предварительные требования

- Сетевая доступность устройства FortiAnalyzer по целевому порту и протоколу для каждой ноды кластера R-Vision SIEM.

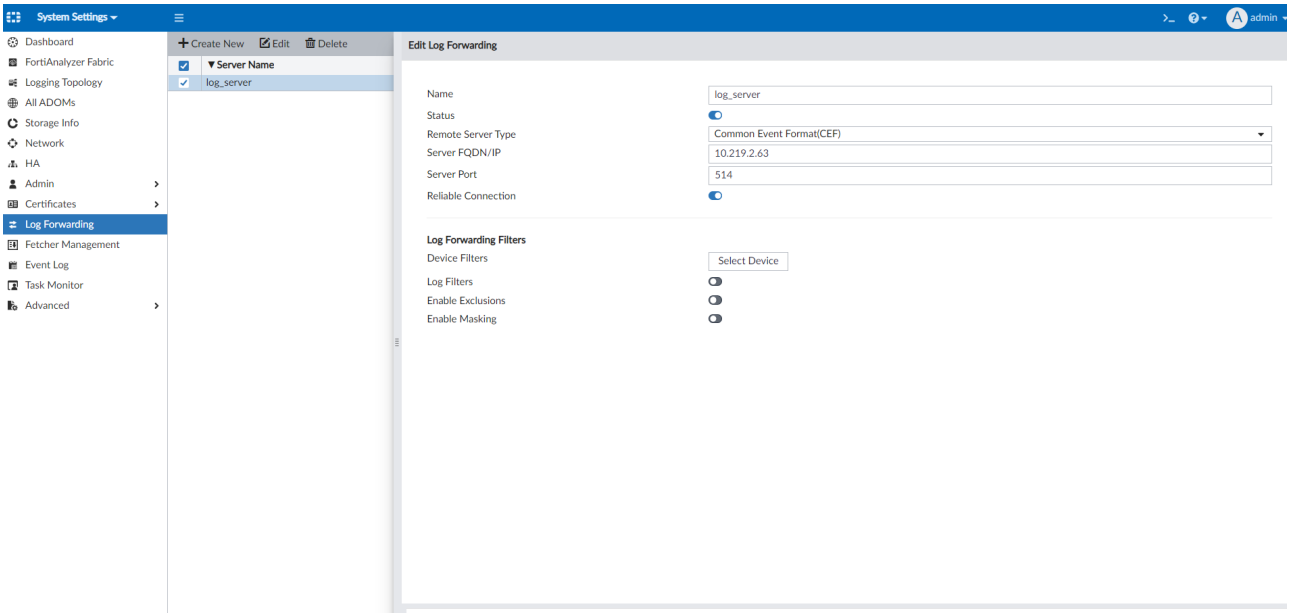
Настройка Fortinet FortiAnalyzer

Для сбора событий Fortinet FortiAnalyzer необходимо настроить подключение R-Vision SIEM посредством протокола `syslog`.

Настройка журналирования

Для настройки пересылки событий выполните следующие шаги:

1. Откройте панель администратора Fortinet FortiAnalyzer.
2. Перейдите в раздел **Log Forwarding**.
3. Создайте новый сервер трансляции:
   - **Name**: введите произвольное имя.
   - **Status**: выберите значение `enabled`.
   - **Remote Server Type**: выберите значение `Common Event Format(CEF)`.
   - **Server FQDN/IP**: укажите IP-адрес любой ноды R-Vision SIEM.
   - **Server Port**: укажите порт точки входа R-Vision SIEM, настроенный в соответствии с настройкой в R-Vision SIEM.
   - **Reliable Connection**: выберите значение `enabled`.
4. Сохраните конфигурацию.



Настройка на стороне Fortinet FortiAnalyzer завершена.

Настройка в R-Vision SIEM

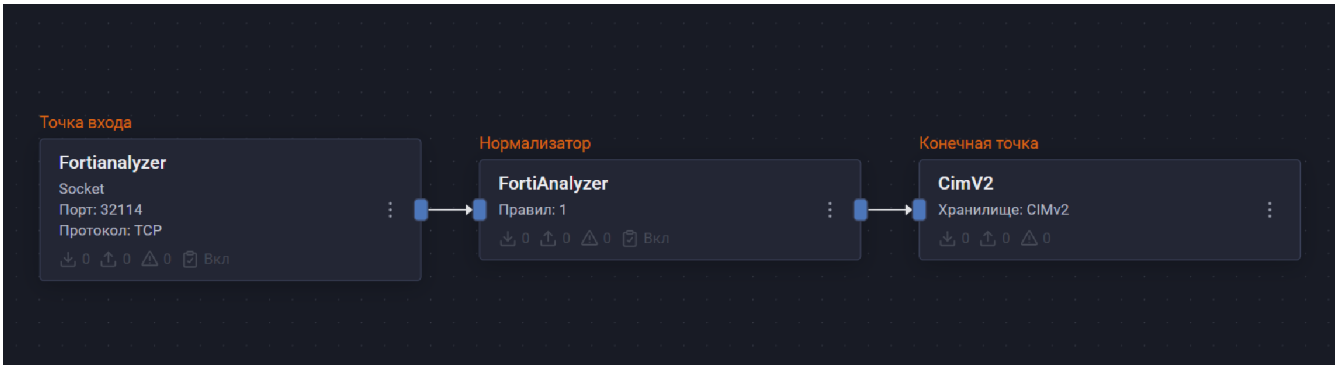
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Socket**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне Fortinet FortiAnalyzer.

- Протокол: выберите вариант **TCP**.

3. Добавьте на конвейер элемент **Нормализатор** с правилом **Fortinet FortiAnalyzer** (идентификатор правила: **RV-N-285**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

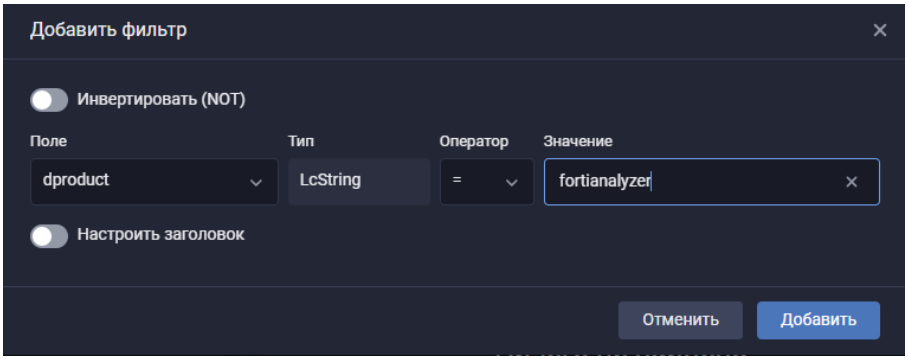
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Fortinet FortiAnalyzer.

Найти события Fortinet FortiAnalyzer в хранилище можно по следующему фильтру:

```
device_product = "fortianalyzer"
```



HP ProCurve

- HP ProCurve: настройка источника

HP ProCurve: настройка источника

Данное руководство описывает процесс настройки сбора событий HP ProCurve и их отправки в R-Vision SIEM.

Предварительные требования

Перед настройкой пересылки событий в R-Vision SIEM убедитесь, что сетевая связность между устройствами HP ProCurve и промежуточным узлом обеспечена, а необходимые порты открыты.

Настройка HP ProCurve

Настройка отправки событий на промежуточный rsyslog-сервер

HP ProCurve поддерживает отправку только на порт `514` по протоколу `UDP`. Поэтому необходимо использовать промежуточный сервер `rsyslog` для приема и пересылки событий. Отправка сообщений осуществляется посредством протокола `syslog`.

Для настройки передачи событий выполните следующие команды в режиме глобальной конфигурации (`configure terminal`):

```
enable
configure
logging <target>
logging facility user
write memory
```

Здесь:

- `<target>`: IP-адрес промежуточного сервера `rsyslog`.

Настройка на промежуточном rsyslog-сервере

Настройка отправки событий в R-Vision SIEM

На сервере `rsyslog` создайте конфигурационный файл `ProCurve.conf`:

```
if $fromhost-ip == '<host>' then {
  action(type="omfwd" Target="<target>" Port="<port>" Protocol="<protocol>")
  stop
}
```

Здесь:

- `<host>`: IP-адрес HP ProCurve.
- `<target>`: IP-адрес коллектора R-Vision SIEM.
- `<port>`: порт точки входа `Syslog` на конвейере R-Vision SIEM.
- `<protocol>`: транспортный протокол (`tcp` или `udp`).

Настройка в R-Vision SIEM

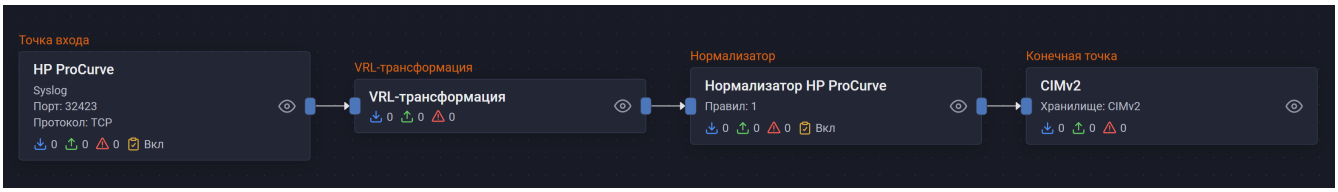
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - **Название**: введите название точки входа.
   - **Тип точки входа**: выберите вариант **Syslog**.
   - **Порт точки входа**: введите значение в соответствии с настройками на стороне промежуточного сервера.
   - **Протокол**: выберите вариант в соответствии с настройками на стороне промежуточного сервера.
3. Добавьте элемент **VRL-трансформация** со следующим кодом:

```
.device_product = "procurve"
```

4. Соедините добавленную точку входа и VRL-трансформацию.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **Hewlett Packard Enterprise ProCurve** (идентификатор правила: **RV-N-321**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

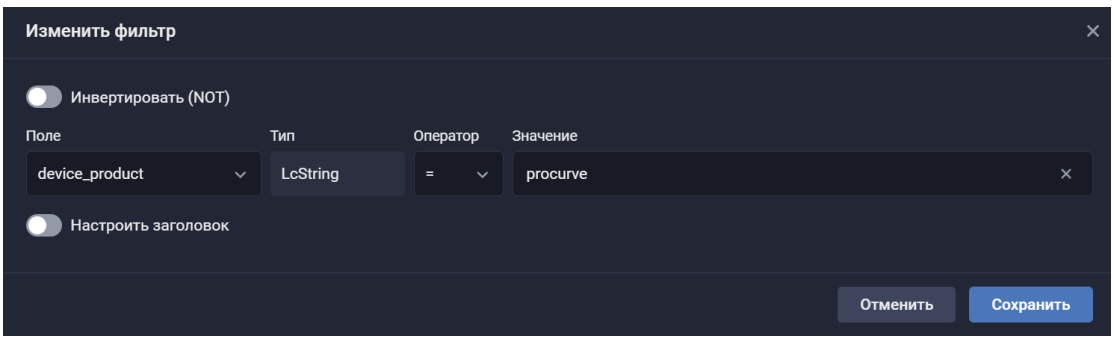
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события HP ProCurve.

Найти события HP ProCurve в хранилище можно по следующему фильтру:

```
device_product = "procurve"
```



HPE ArubaOS-CX

- HPE ArubaOS-CX: настройка источника

HPE ArubaOS-CX: настройка источника

Данное руководство описывает процесс отправки событий сетевого коммутатора ArubaOS-CX в R-Vision SIEM.

Предварительные требования

Перед настройкой пересылки событий в R-Vision SIEM убедитесь в выполнении следующих условий:

- Сетевая доступность сервера СУБД источника по целевому порту и протоколу для каждой ноды кластера R-Vision SIEM.

Настройка ArubaOS-CX

Настройте отправку событий на сетевом коммутаторе, последовательно выполнив команды:

```
# conf
# logging <target> <protocol> <port>
# write memory
```

Здесь:

- `<target>`: IP-адрес коллектора R-Vision SIEM.
- `<port>`: порт точки входа `Syslog` в конвейере R-Vision SIEM.
- `<protocol>`: сетевой протокол (`tcp` или `udp`).

Настройка в R-Vision SIEM

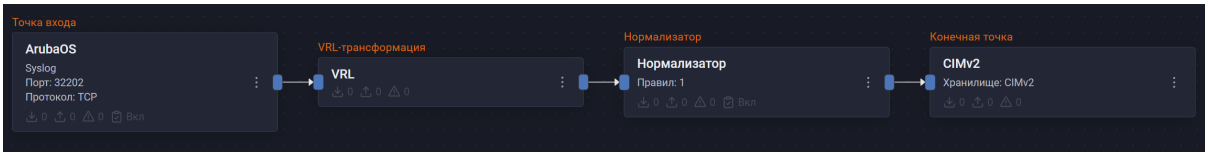
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне источника (любой свободный порт больше 30000).
   - Протокол: выберите вариант в соответствии с настройками на стороне источника.
3. Добавьте элемент **VRL-трансформация** со следующим кодом:

```
.device_product = "arubaos-cx"
```

4. Соедините добавленную точку входа и VRL-трансформацию.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **HPE ArubaOS-CX 10.04+** (идентификатор правила: **RV-N-313**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

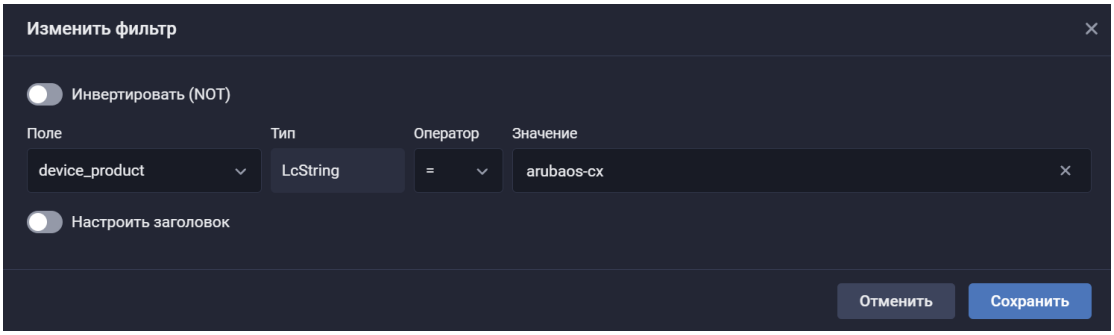
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события ArubaOS-CX.

Найти события ArubaOS-CX в хранилище можно по следующему фильтру:

```
device_product = "arubaos-cx"
```



IPFIX

- IPFIX: настройка источника

IPFIX: настройка источника

Данное руководство описывает процесс настройки сбора событий IPFIX и их отправки в R-Vision SIEM.

Предварительные требования

Перед настройкой сбора событий в R-Vision SIEM убедитесь в выполнении следующих условий:

- У получаемого R-Vision SIEM потока NetFlow данные должны быть структурированы в соответствии со стандартом Cisco.
-

Сетевая связность между устройством, передающим NetFlow и SIEM (или промежуточным syslog-сервером) обеспечена, а необходимые порты открыты.

Настройка IPFIX

Настройка IPFIX различается в зависимости от операционной системы сетевого оборудования: Cisco IOS XE, Cisco IOS XR, Cisco NX-OS и другие. Поэтому рекомендуется производить настройку в соответствии с эксплуатационной документацией производителя вашего оборудования.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM в карточке коллектора перейдите на вкладку **Обогащение**.
2. Добавьте таблицу обогащения **netflow_tcp_flags**.
3. Создайте новый конвейер в данном коллекторе.
4. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Netflow**.
   - Порт точки входа: введите значение в диапазоне `30000–32767`.
   - Протокол: выберите вариант **UDP**.
5. Добавьте на конвейер элемент **VRL-трансформация** со следующим содержимым:

```
main = .raw.netflow_packets[0].IPFix.sets[0].data.data_fields
if is_null(main) {
    . = .raw.netflow_packets[0].IPFix.sets[1].data.data_fields
} else {
    . = main
}
```

6. Соедините добавленный блок VRL-трансформации с точкой входа.
7. Добавьте на конвейер еще один элемент **VRL-трансформация** со следующим содержимым:

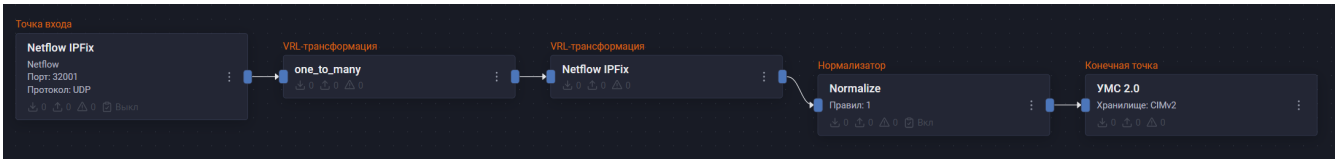
```
.raw = .
.id = uuid_v4()
.timestamp= %vector.ingest_timestamp
.tenantId = "${TENANT_ID}"
.collectorId = "${COLLECTOR_ID}"
.type = 0
.device_product = "ipfix"
```

8. Соедините второй блок VRL-трансформации с первым.
9. Добавьте на конвейер элемент **Нормализатор** с правилом **NetFlow IPFix (10)** (идентификатор

правила: **RV-N-302**).

10. Соедините нормализатор со вторым блоком VRL-трансформации.
11. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
12. Соедините конечную точку с нормализатором.
13. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

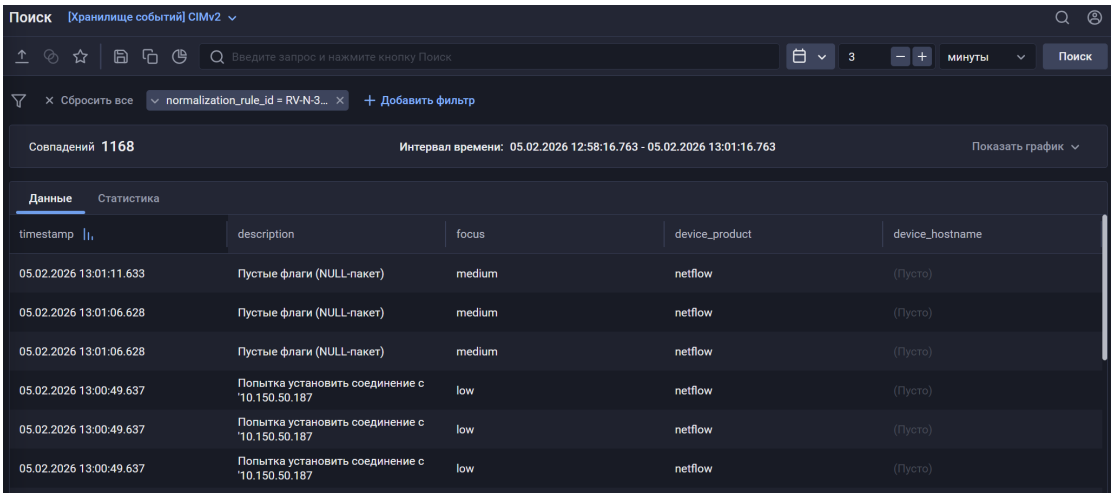


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события IPFIX.



Найти события IPFIX в хранилище можно по следующему фильтру:

```
normalization_rule_id = "RV-N-302"
```



MikroTik RouterOS

- MikroTik RouterOS: правила корреляции

MikroTik RouterOS: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1299	Атака Password Spraying в MikroTik	Данное правило направлено на обнаружение атак типа Password Spraying на интерфейсы управления MikroTik (Winbox, SSH), которые могут свидетельствовать о попытке атакующего получить доступ с использованием распространенных паролей для различных учетных записей. В отличие от классического брутфорса, такие атаки характеризуются небольшим количеством попыток входа на каждую учетную запись, но охватывают множество пользователей, что затрудняет их обнаружение стандартными средствами защиты. Успешная реализация этой техники позволяет атакующему получить контроль над маршрутизатором с минимальным риском блокировки учетной записи.	• Credential Access (TA0006) • Brute Force (T1110) • Password Spraying (T1110.003)
RV-D-1301	Подбор пароля пользователя MikroTik	Данное правило направлено на выявление атак методом перебора пароля к интерфейсам управления MikroTik (Winbox, SSH), которые могут свидетельствовать о попытке атакующего подобрать учетные данные для несанкционированного доступа. Такие атаки характеризуются множественными неудачными попытками авторизации и являются аномальными для штатных операций администрирования. Эксплуатация этой атаки позволяет получить контроль над маршрутизатором, что открывает возможности для изменения сетевых настроек или перехвата трафика.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1304	Подключение к MikroTik с недоверенного IP	Правило предназначено для обнаружения потенциально несанкционированного доступа к устройствам MikroTik с использованием привилегированной учетной записи. Оно срабатывает при установлении соединения с IP-адреса, не входящего в список доверенных хостов, что может указывать на компрометацию учетных данных или попытку обхода политики безопасности.	• Initial Access (TA0001) • Valid Accounts (T1078) • Default Accounts (T1078.001)
RV-D-1375	Изменение групп в MikroTik	Данное правило направлено на обнаружение несанкционированных изменений в составе критичных групп пользователей MikroTik, которые могут свидетельствовать о попытке атакующего повысить привилегии или ограничить доступ администраторов. Такие изменения являются аномальными для штатных операций администрирования и могут указывать на компрометацию учетных записей или злоупотребление легитимными правами. Эксплуатация этой техники позволяет атакующему получить полный контроль над сетевым оборудованием или заблокировать доступ легитимных администраторов.	• Privilege Escalation (TA0004) • Abuse Elevation Control Mechanism (T1548)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1377	Изменение конфигураций фильтра в Mikrotik	Данное правило направлено на выявление несанкционированных изменений конфигураций фильтров MikroTik, которые могут свидетельствовать о попытке атакующего перехватить или заблокировать сетевой трафик. Подобные модификации правил фаервола или NAT являются аномальными для стандартных операций администрирования и могут указывать на компрометацию учетных записей либо эксплуатацию уязвимостей. Использование этой техники позволяет атакующему перенаправлять данные через подконтрольные серверы, нарушать доступ к ресурсам или скрытно внедряться в сетевую инфраструктуру.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify System Firewall (T1562.004)

Netgate pfSense

- Netgate pfSense: настройка источника

Netgate pfSense: настройка источника

Данное руководство описывает процесс настройки сбора событий pfSense и их отправки в R-Vision SIEM.

Предварительные требования

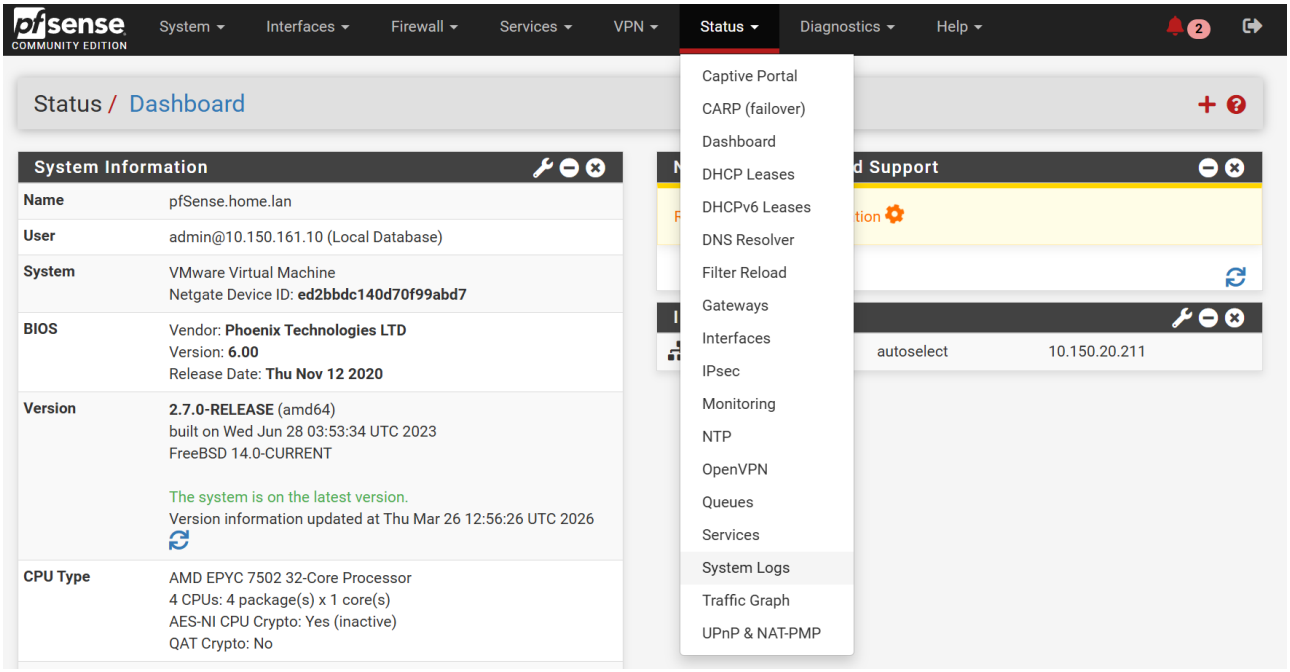
Перед настройкой пересылки событий в R-Vision SIEM убедитесь, что сетевая связность между устройствами pfSense и R-Vision SIEM (или промежуточным узлом) обеспечена, а необходимые порты открыты.

Настройка pfSense

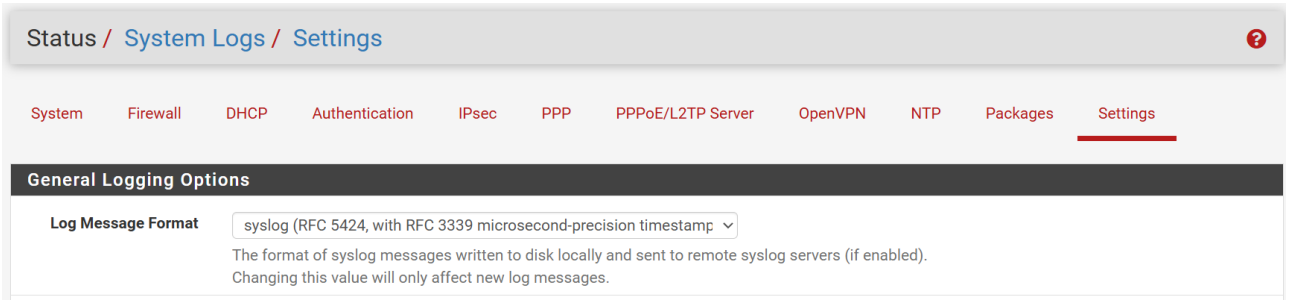
Настройка отправки событий в R-Vision SIEM

Отправка сообщений осуществляется посредством протокола syslog. Для настройки передачи событий выполните следующие шаги:

1. Войдите в веб-интерфес **pfSense**.
2. Перейдите в раздел **Status** → **System Logs**:



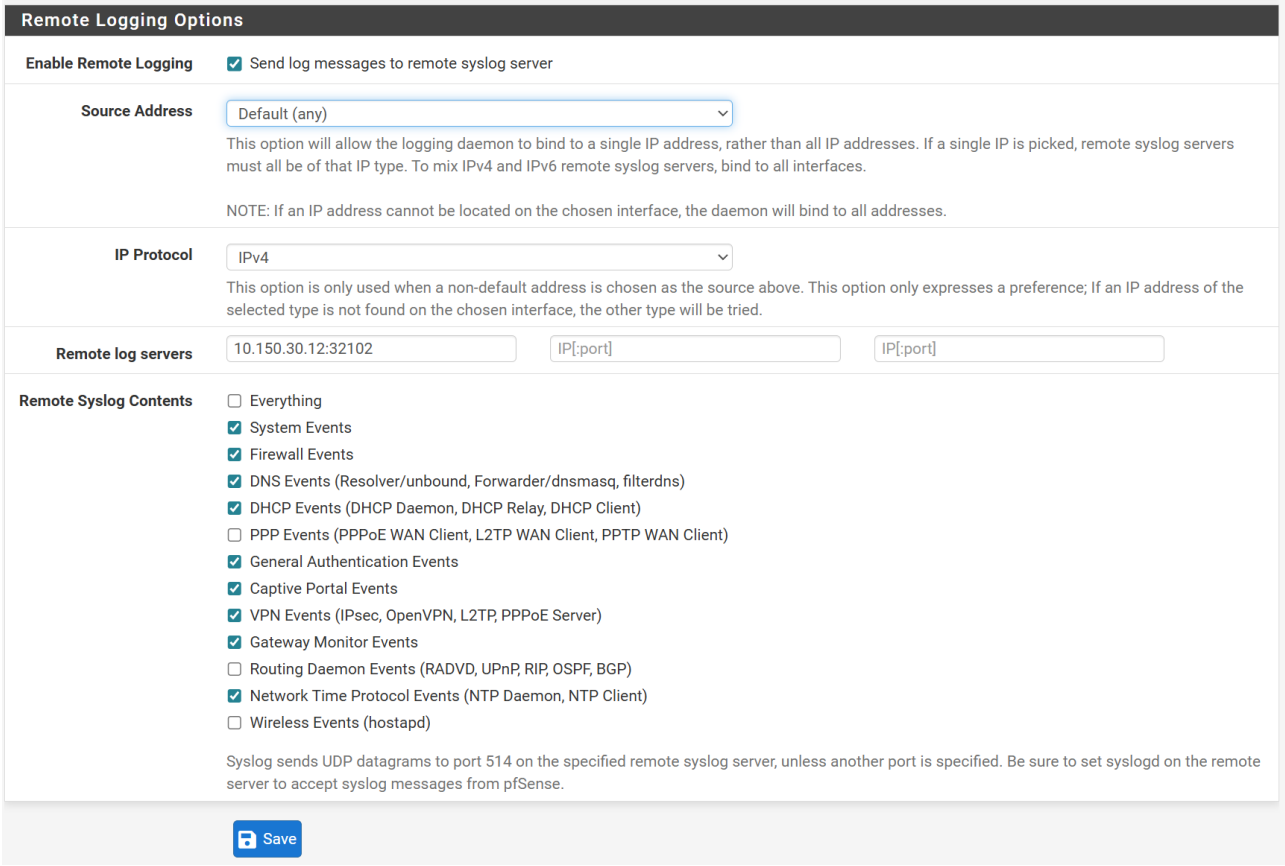
3. Откройте вкладку **Settings**.
4. В пункте **Log Message Format** выберите из выпадающего списка вариант **syslog**.



5. Внизу страницы установите флажок в поле **Enable Remote Logging**.
6. В поле **IP Protocol** выберите из выпадающего списка вариант **IPv4**.
7. Введите IP-адрес коллектора SIEM и порт в формате: `<target>:<port>`.

   Здесь:

   - `<target>` — IP-адрес узла кластера K8s, на котором запущен коллектор.
   - `<port>` — порт точки входа Syslog на конвейере SIEM.
8. Выберите события, которые необходимо отправлять в SIEM.
9. Нажмите на кноку **Save**.



Netgate pfSense отправляет события только по протоколу UDP. При создании точки входа указывайте протокол UDP и любой свободный порт со значением больше 30000. Точка входа в конвейере должна быть создана заранее.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий Netgate pfSense в R-Vision SIEM выполните следующие шаги:

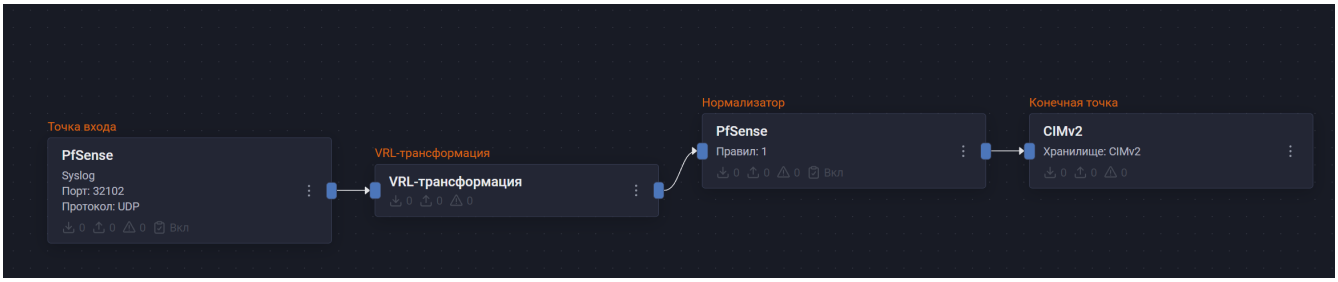
1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите произвольное, понятное название.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне источника (любой свободный порт со значением больше 30000).
   - Протокол: выберите вариант **UDP**.
3. Добавьте VRL-трансформацию со следующим кодом:

```
.device_product = "pfsense"
```

4. Соедините точку входа с VRL-трансформацией.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **Netgate pfSense** (идентификатор правила: **RV-N-336**).

6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

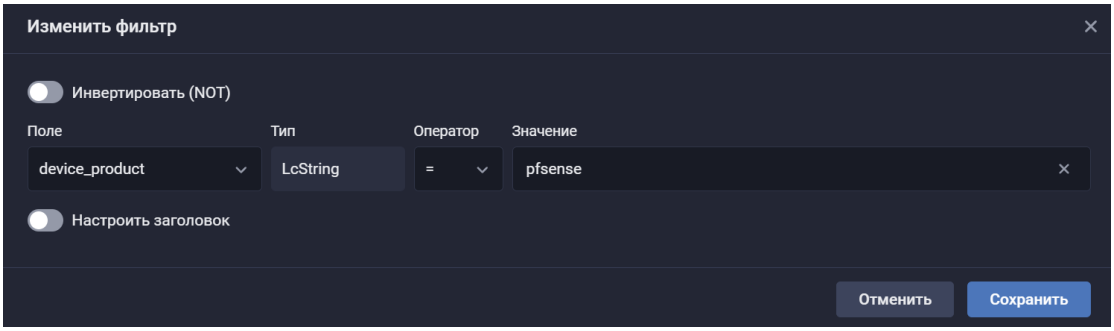
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события pfSense.

Найти события pfSense в хранилище можно по следующему фильтру:

```
device_product = "pfsense"
```



Системы sandbox

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых систем класса sandbox (сетевая песочница):

- Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform

- Kaspersky Anti Targeted Attack Platform: настройка источника

Kaspersky Anti Targeted Attack Platform: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Kaspersky Anti Targeted Attack Platform в R-Vision SIEM.

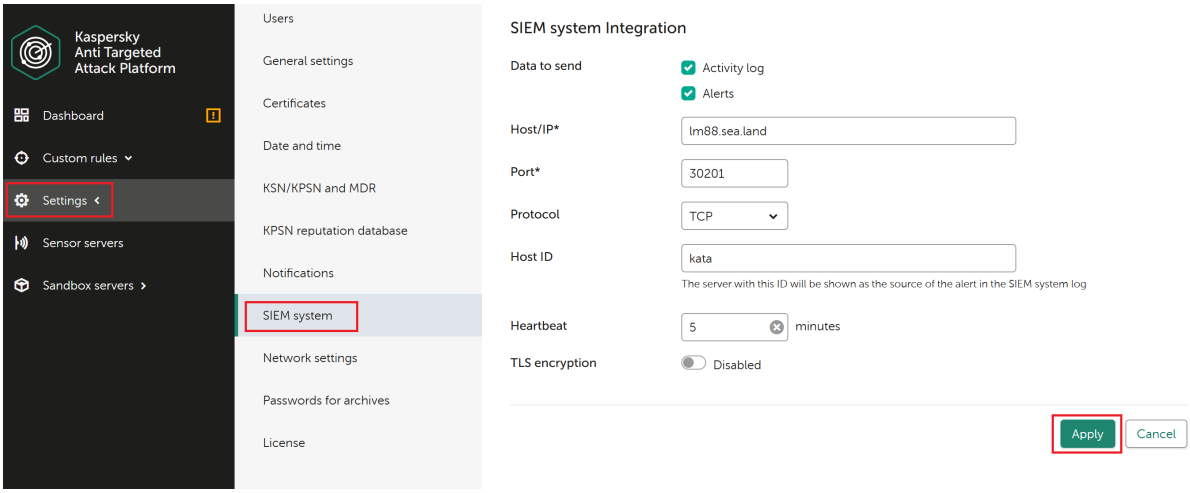
Предварительные требования

Перед настройкой пересылки событий в R-Vision SIEM убедитесь, что обеспечена сетевая доступность между сервером Kaspersky Anti Targeted Attack Platform и коллектором R-Vision SIEM.

Настройка Kaspersky Anti Targeted Attack Platform

Для настройки пересылки событий из Kaspersky Anti Targeted Attack Platform в R-Vision SIEM выполните следующие шаги:

1. Откройте веб-консоль центрального узла Kaspersky Anti Targeted Attack Platform.
2. Установите флажок **Локальный администратор**.
3. Введите данные учетной записи администратора.
4. Перейдите в раздел **Параметры** → **SIEM-система**.
5. Заполните необходимые поля:
   - **Данные для отправки**: установите флажки **Журнал активности** и **Обнаружения**.
   - **Хост/IP**: введите IP-адрес или FQDN-адрес коллектора R-Vision SIEM.
   - **Порт**: введите порт коллектора R-Vision SIEM.
   - **Протокол**: выберите протокол `TCP` или `UDP`.
   - **ID хоста**: введите идентификатор хоста сервера, который будет указан в журнале R-Vision SIEM как источник обнаружения.
   - **Периодичность сигнала**: введите количество минут в диапазоне 1—59.
   - **TLS-шифрование**: при необходимости включите данную опцию (по умолчанию отключена).
6. Нажмите на кнопку **Применить**.

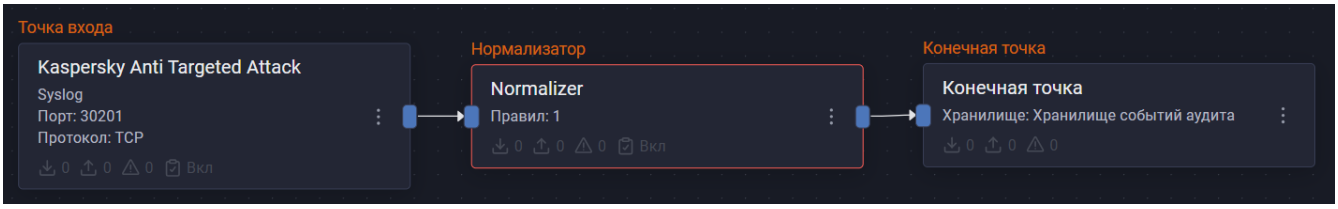


Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне Kaspersky Anti Targeted Attack Platform.
   - Протокол: выберите вариант в соответствии с настройками на стороне Kaspersky Anti Targeted Attack Platform.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Kaspersky Anti Targeted Attack Platform** (идентификатор правила: **RV-N-181**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

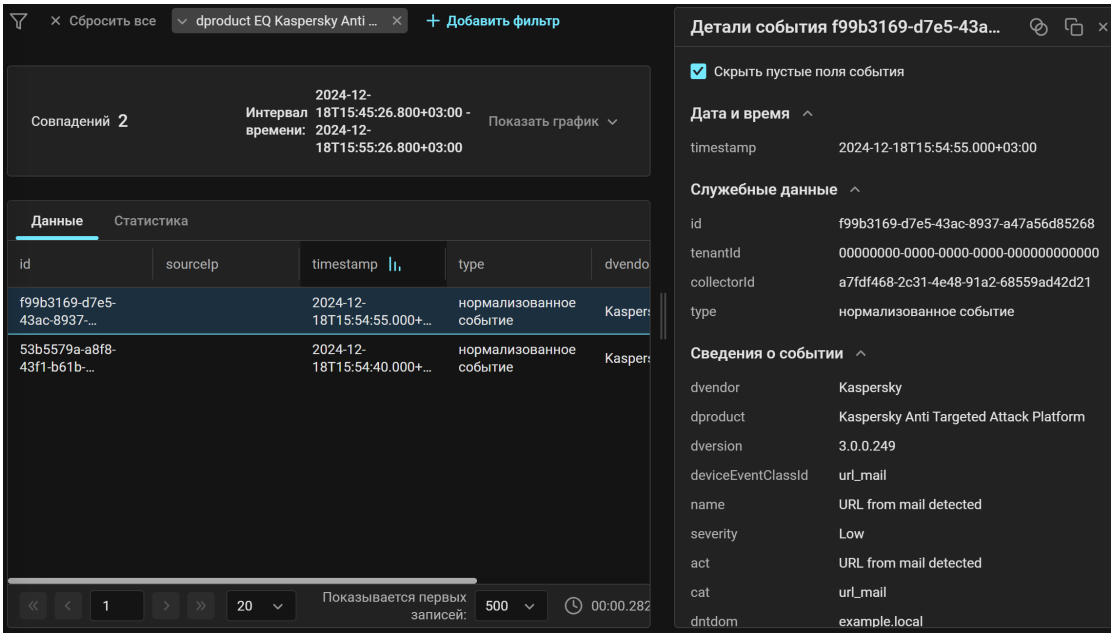
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Kaspersky Anti Targeted Attack Platform.

Найти события Kaspersky Anti Targeted Attack Platform в хранилище можно по следующему фильтру:

```
dproduct = "Kaspersky Anti Targeted Attack Platform"
```



Перечень событий

С перечнем событий можно ознакомиться в официальной документации Kaspersky.

Системы анализа сетевого трафика (NTA)

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых систем анализа сетевого трафика:

- Positive Technologies ISIM
- PT Network Attack Discovery
- Suricata
- Гарда NDR

Positive Technologies ISIM

- Positive Technologies ISIM: настройка источника

Positive Technologies ISIM: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Positive Technologies ISIM в R-Vision SIEM.

Предварительные требования

- Сетевая доступность сервера Positive Technologies ISIM по целевому порту и протоколу для каждой ноды кластера SIEM.

Настройка Positive Technologies ISIM

Для пересылки событий, зарегистрированных Positive Technologies ISIM, в R-Vision SIEM по протоколу Syslog:

1. Перейдите в директорию `/opt/ptisim/lib/ptisim-httpapi/templates/alerts/notify`

   ```
   cd /opt/ptisim/lib/ptisim-httpapi/templates/alerts/notify
   ```

2. В данной директории имеется 3 раздела отвечающих за формат присылаемого сообщения, это:
   - `alert_create_message`
   - `alert_status_message`
   - `alert_progress_message`

   В каждом из этих разделов нужно произвести настройку шаблона сообщения. Рассмотрим на примере `alert_create_message`:

   a. Перейдите в директорию `alert_create_message/syslog`

   b. Скопируйте файлы `ru.html` и `eng.html`:

   ```
   cp ru.html ru.html.old
   ```

```
cp eng.html eng.html.old
```

c. В файлах `ru.html` и `eng.html` необходимо заменить содержание на следующее:

```
{% include "alerts/notify/_syslog_base.html" %}Created:
incident_id:`{{incident.id}}`, incident_name:`{{ incident.name.eng }}`,
incident_at_step:{{ incident.progress }}/{{ incident.capacity }},
incident_url:`{{ incident_url }}, incident_status:`{{incident.status}}`,
incident_start_time:`{{incident.start.strftime("%Y-%m-%dT%H:%M:%SZ")}}`,
incident_src_ip:`{{incident.src_ip}}`,
incident_src_mac:`{{incident.src_mac}}`,
incident_dst_ip:`{{incident.dst_ip}}`,
incident_dst_mac:`{{incident.dst_mac}}`,
incident_group:`{{incident.group}}`, incident_shost:`{{station_name}}`,
incident_end_time:`{{incident.end.strftime("%Y-%m-%dT%H:%M:%SZ")}}`,
incident_type:`{{incident.type}}`, incident_dvc:`{{ip}}`
{# all available fields /opt/ptisim/etc/fullview/httpapi.conf.d/incidents-
notify-fields.yaml #}
```

3. В директориях `alert_status_message` и `alert_progress_message` необходимо проделать те же действия, используя следующие шаблоны:

- для `alert_status_message`:

```
{% include "alerts/notify/_syslog_base.html" %}Incident change status:
incident_id:`{{incident.id}}`, incident_name:`{{ incident.name.eng }}`,
incident_at_step:{{ incident.progress }}/{{ incident.capacity }},
incident_url:`{{ incident_url }}`, incident_status:`{{incident.status}}`,
incident_start_time:`{{incident.start.strftime("%Y-%m-%dT%H:%M:%SZ")}}`,
incident_src_ip:`{{incident.src_ip}}`, incident_src_mac:`{{incident.src_mac}}`,
incident_dst_ip:`{{incident.dst_ip}}`, incident_dst_mac:`{{incident.dst_mac}}`,
incident_group:`{{incident.group}}`, incident_shost:`{{station_name}}`,
incident_end_time:`{{incident.end.strftime("%Y-%m-%dT%H:%M:%SZ")}}`,
incident_type:`{{incident.type}}`, incident_dvc:`{{ip}}`
{# all available fields /opt/ptisim/etc/fullview/httpapi.conf.d/incidents-
notify-fields.yaml #}
```

- для `alert_progress_message`:

```
{% include "alerts/notify/_syslog_base.html" %}Incident change progress:
incident_id:`{{incident.id}}`, incident_name:`{{ incident.name.eng }}`,
incident_at_step:{{ incident.progress }}/{{ incident.capacity }},
incident_old_step:`{{ old_progress }}/{{ incident.capacity }}`, incident_url:`{{
incident_url }}`, incident_status:`{{incident.status}}`,
incident_start_time:`{{incident.start.strftime("%Y-%m-%dT%H:%M:%SZ")}}`,
incident_src_ip:`{{incident.src_ip}}`, incident_src_mac:`{{incident.src_mac}}`,
incident_dst_ip:`{{incident.dst_ip}},` incident_dst_mac:`{{incident.dst_mac}}`,
incident_group:`{{incident.group}}`, incident_shost:`{{station_name}}`,
```

```
incident_end_time:`{{incident.end.strftime("%Y-%m-%dT%H:%M:%SZ")}}`,
incident_type:`{{incident.type}}`, incident_dvc:`{{ip}}`
{# all available fields /opt/ptisim/etc/fullview/httpapi.conf.d/incidents-
notify-fields.yaml #}
```

4. Далее необходимо перезагрузить службу `ptisim-httpapi.service`:

```
sudo systemctl restart ptisim-httpapi.service
```

5. Необходимо создать правило МЭ, которое позволит передавать события на коллектор, для этого внесите в конец файла `/opt/ptisim/default.rules` следующие строки:

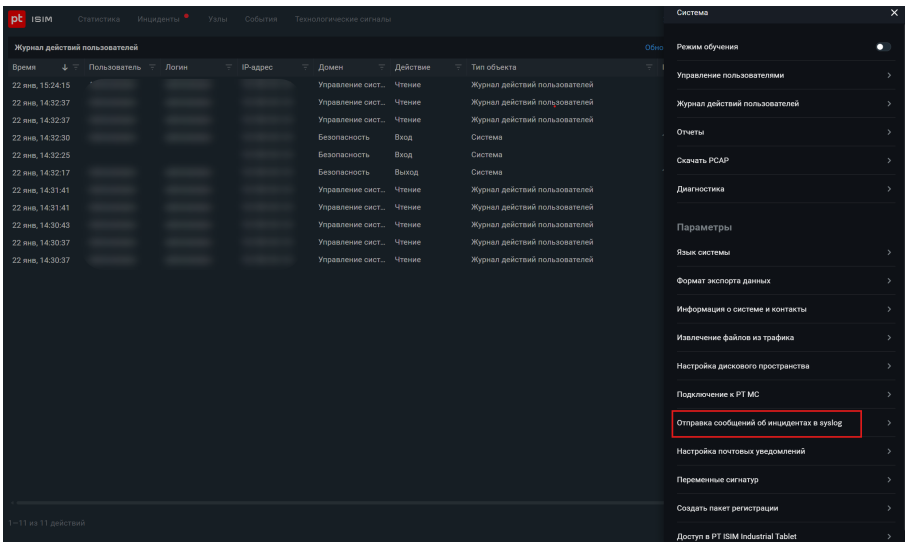
```
# Если для передачи предполагается использовать tcp
-A OUTPUT -p tcp --dport <порт коллектора SIEM в диапазоне 30000--32767> -j ACCEPT
-A INPUT -p tcp --sport <порт коллектора SIEM в диапазоне 30000--32767> -j ACCEPT

# Если для передачи предполагается использовать udp
-A OUTPUT -p udp --dport <порт коллектора SIEM в диапазоне 30000--32767> -j ACCEPT
```

6. Сохраните файл и перезапустите службу `ptisim-firewall`:

```
sudo systemctl restart ptisim-firewall.service
```

7. Теперь необходимо настроить отправку инцидентов через syslog в веб-интерфейсе. Войдите веб-интерфейс.
8. Перейдите в раздел **Система** → **Отправка сообщений об инцидентах в syslog**



9. В данном разделе отметьте **Отправлять** и в соответствующих полях введите информацию о SIEM:
   - IP-адрес: укажите IP-адрес коллектора R-Vision SIEM.
   - Транспортный протокол: выберите вариант **TCP** или **UDP**.

- Порт: укажите открытый порт коллектора (введите значение в диапазоне **30000—32767**).

10. Нажмите **Сохранить**.

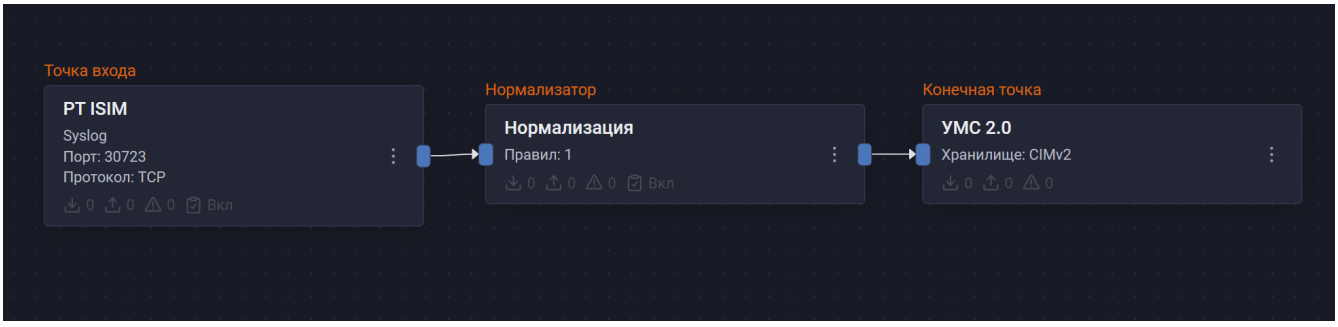
Настройка передачи инцидентов завершена.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне Positive Technologies ISIM.
   - Протокол: выберите вариант в соответствии с настройками на стороне Positive Technologies ISIM.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Positive Technologies ISIM** (идентификатор правила: **RV-N-286**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

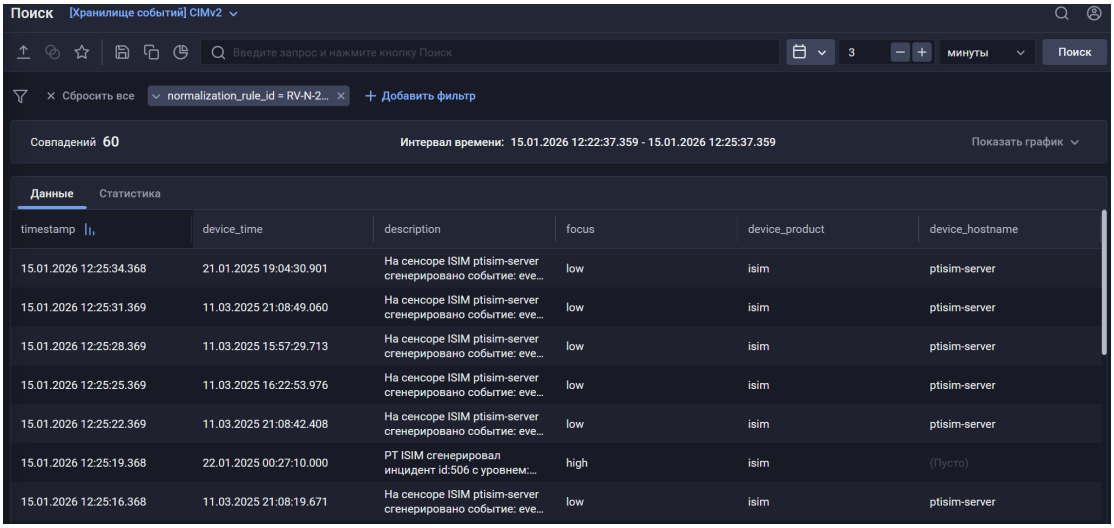


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Positive Technologies ISIM.



Найти события Positive Technologies ISIM в хранилище можно по следующему фильтру:

```
normalization_rule_id = "RV-N-286"
```



PT Network Attack Discovery

- PT Network Attack Discovery: настройка источника
- PT Network Attack Discovery: правила корреляции

PT Network Attack Discovery: настройка источника

Данное руководство описывает процесс настройки подсистемы журналирования и отправки событий из PT Network Attack Discovery (PT NAD) в R-Vision SIEM.

Настройка PT NAD

Описание подсистемы журналирования PT NAD

Согласно п. 10.11 руководства администратора PT Network Attack Discovery, продукт может записывать в системный журнал syslog следующие сведения:

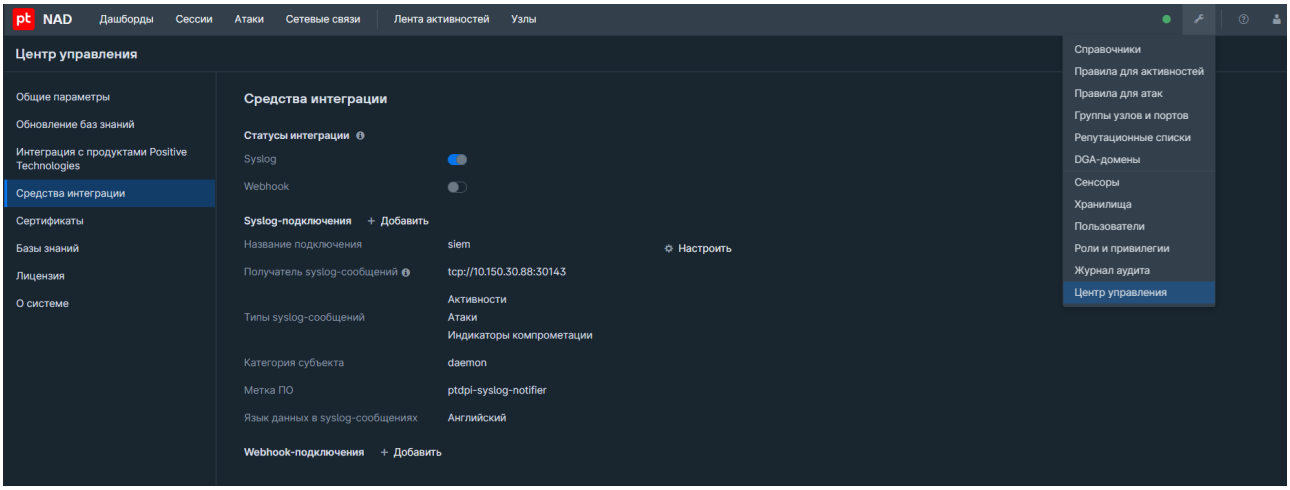
- информация об активностях;
- информация о выявленных атаках;
- информация об обнаруженных индикаторах компрометации;
- результаты ретроспективного анализа;
- уведомления о заполнении журнала аудита.

Настройка отправки событий делится на два этапа:

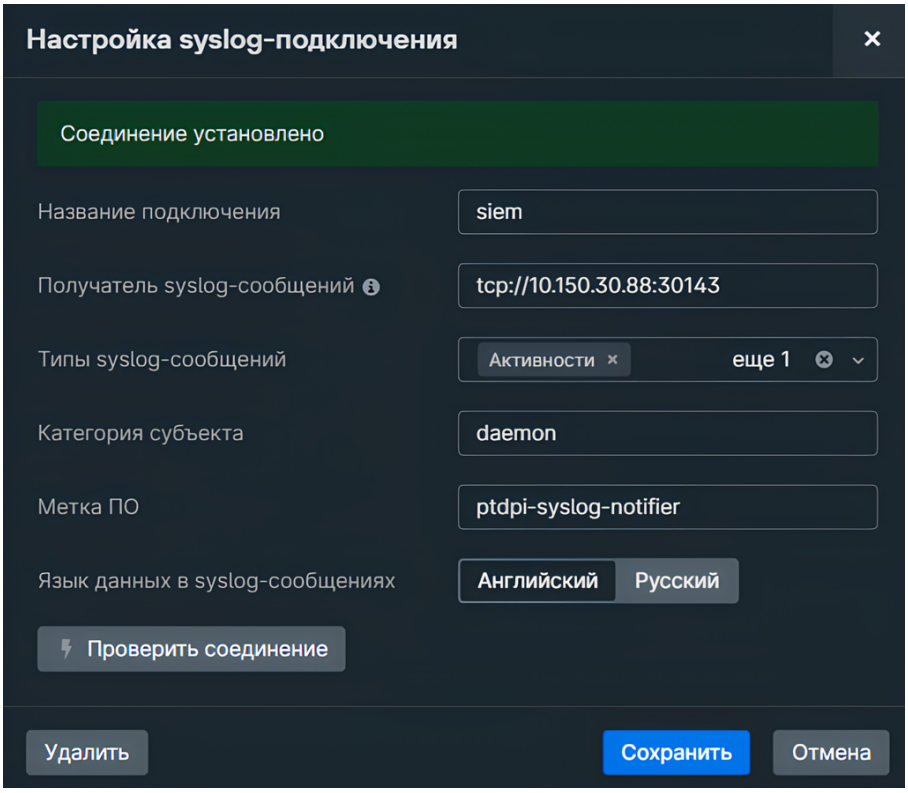
1. Настройка syslog-сообщений об активностях, атаках и индикаторах компрометации (п. 10.11.1 руководства администратора PT NAD).
2. Настройка syslog-сообщений о результатах ретроспективного анализа и уведомлениях о заполнении журнала аудита (п. 10.11.2 руководства администратора PT NAD).

Настройка syslog-сообщений об активностях, атаках и индикаторах компрометации

1. В веб-интерфейсе PT NAD перейдите в раздел **Центр управления** → **Средства интеграции**.



2. Переведите переключатель **Syslog** в активное положение и нажмите на кнопку **Добавить** в настройках Syslog-подключения. Откроется окно настройки подключения.



3. В поле **Получатель syslog-сообщений** укажите протокол, адрес и порт syslog-сервера в формате `<протокол>://<адрес>:<порт>`.
4. Проверьте корректность настроек с помощью кнопки **Проверить соединение**.
5. Нажмите на кнопку **Сохранить**, чтобы применить изменения.

Настройка syslog-сообщений о результатах ретроспективного анализа и уведомлениях

1. Откройте файл `/etc/rsyslog.d/45-ptdpi.conf`.
2. Раскомментируйте строку и задайте значения параметров `target`, `port` и `protocol`. Например:

```
action(type="omfwd" target="10.150.30.88" port="30143" protocol="tcp")
```

3. После раскомментирования строки и указания параметров файл конфигурации должен выглядеть следующим образом:

```
#
# output ptdpi alerts and nad-events to log file and SIEM

if (($programname == "ptdpi" and $msg startswith " [") or $programname == "nad-event") then {
    action(type="omfwd" target="10.150.30.88" port="30143" protocol="tcp")
    stop
}

# template with more info then default
#template(name="ptdpiFmt" type="string"
#         string="%TIMESTAMP% %HOSTNAME% [f:%syslogfacility%'%syslogfacility-text%',"\
#                "l:%syslogseverity%'%syslogseverity-text%'] %syslogtag%%msg:::sp-if-no-1st-sp%%msg:::drop-last-lf%\n"
#        )
# using template:
#action(type="omfile" file="/opt/ptsecurity/log/<name>.log" template="<template name>")
#:programname, isequal, "<prog name>"    /opt/ptsecurity/log/<name>.log;<';' + template name>

##########################################
# output ptdpi service log to log file
```

4. Сохраните изменения в файле `/etc/rsyslog.d/45-ptdpi.conf`.
5. Перезапустите службу rsyslog с помощью команды:

```
sudo systemctl restart rsyslog.service
```

6. Чтобы включить запись syslog-сообщений о ретроспективном анализе и заполнении журнала аудита, выполните следующие шаги:
   a. Откройте файл `/opt/ptsecurity/etc/nad.settings.yaml`.
   b. Раскомментируйте параметры `retrospective_notify_syslog` и `journal_notify_syslog`.
   c. Установите для данных параметров значение `true`.
   d. Перезапустите службы с помощью команд:

```
sudo systemctl restart nad-task-server.service
sudo systemctl restart nad-web-server.service
```

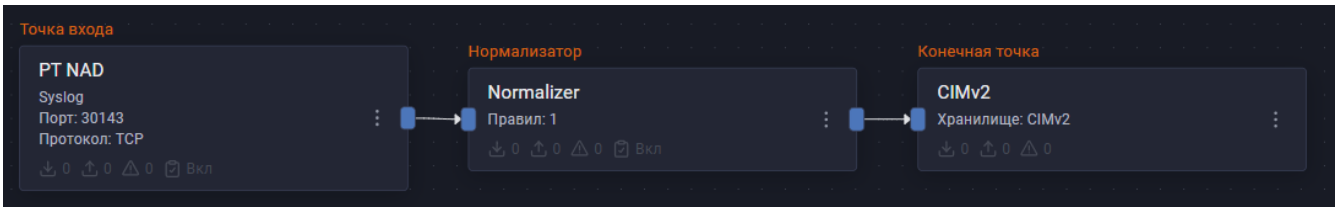
Настройка в R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне PT NAD.
   - Протокол: выберите вариант в соответствии с настройками на стороне PT NAD.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Positive Technologies Network Attack Discovery** (идентификатор правила: **RV-N-203**).
4. Соедините нормализатор с точкой входа.

5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

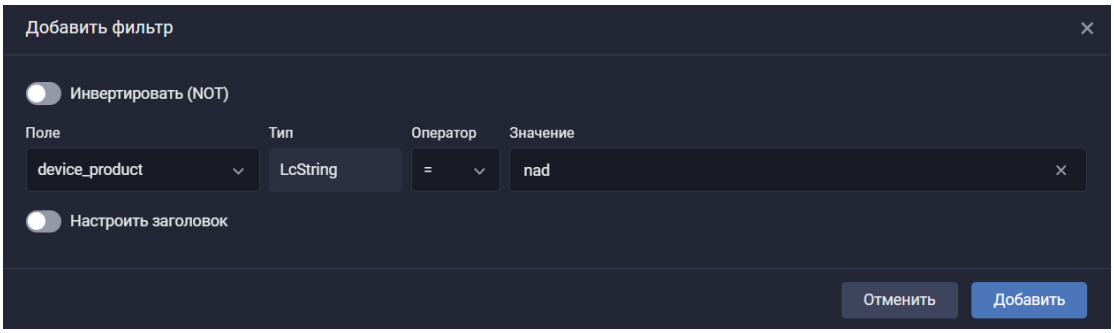
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события PT NAD.

Найти события PT NAD в хранилище можно по следующему фильтру:

```
device_product = "nad"
```



PT Network Attack Discovery: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1381	Признаки использования утилиты для туннелирования трафика	Система PT NAD позволяет обнаруживать использование различных средств для туннелирования трафика. Туннелирование трафика может быть использовано для обхода межсетевых экранов, IDS/IPS и других механизмов безопасности. Атакующий может использовать это для эксфильтрации данных, скрытного управления вредоносными программами или для скрытой коммуникации с командно-контрольными серверами (C2).	• Command and Control (TA0011) • Protocol Tunneling (T1572)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1383	Обнаружены признаки использования вредоносной утилиты	Система PT NAD позволяет обнаруживать признаки использования вредоносных утилит. Атака с использованием вредоносной утилиты предполагает, что атакующий применяет специальные программы для получения несанкционированного доступа, сбора данных или повреждения системы. Обнаруженные утилиты могут включать Metasploit, Cobalt Strike, Powershell Empire и другие.	• Command and Control (TA0011) • Fallback Channels (T1008) • Remote Services (T1021) • Remote Desktop Protocol (T1021.001) • Scheduled Transfer (T1029) • Application Layer Protocol (T1071) • Web Protocols (T1071.001) • File Transfer Protocols (T1071.002) • Proxy (T1090) • Internal Proxy (T1090.001) • Multi-hop Proxy (T1090.003) • Web Service (T1102) • One-Way Communication (T1102.003) • Multi-Stage Channels (T1104) • Data Encoding (T1132)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1384	Обнаружен индикатор компрометации - IOC	Система PT NAD позволяет обнаруживать в сетевом трафике индикаторы компрометации. В случае срабатывания правила рекомендуется проверить актуальность данного IOC, хост инициатора активности, по возможности опросить ответственного за узел, если активность не является легитимной, то провести внутреннее расследование.	• Command and Control (TA0011) • Application Layer Protocol (T1071)
RV-D-1389	Атака DCSync PT NAD	Система PT NAD позволяет обнаруживать попытки атаки DCSync. Атака позволяет атакующему выдавать себя за контроллер домена (DC, domain controller) с целью получения учетных данных пользователей для последующего горизонтального перемещения в сети и/или доступа к конфиденциальной информации. В основе атаки лежит механизм, предусмотренный для выполнения репликации данных между контроллерами домена (DC).	• Credential Access (TA0006) • OS Credential Dumping (T1003) • DCSync (T1003.006)
RV-D-1390	Атака DCShadow PT NAD	Система PT NAD позволяет обнаруживать попытки атаки DCShadow. При помощи DCShadow атакующий может скрытно изменить данные в Active Directory (AD), маскируясь под легитимный контроллер домена (DC). Атакующий создает фиктивный контроллер домена, регистрируя его в AD, и использует его для внесения изменений, таких как добавление учетных записей или изменение прав доступа. Эти изменения выглядят как легитимные, что затрудняет их обнаружение с помощью стандартных механизмов мониторинга и журналирования.	• Defense Evasion (TA0005) • Rogue Domain Controller (T1207)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1391	Попытки получения информации об учетных записях	Система PT NAD позволяет обнаруживать запросы для получения информации об учетных записях. Данная активность может выполняться администраторами, разрешенными инструментами или атакующими, осуществляющими несанкционированный сбор информации.	• Discovery (TA0007) • Account Discovery (T1087) • Domain Account (T1087.002)
RV-D-1396	Обнаружена попытка эксплуатации уязвимости	Система PT NAD позволяет обнаруживать попытки эксплуатации уязвимостей.	• Initial Access (TA0001) • Exploit Public-Facing Application (T1190) • Exploitation for Client Execution (T1203)
RV-D-1397	Запрос на репликацию от недоверенного DNS-сервера	Система PT NAD позволяет обнаружить атаку с недоверенной репликацией DNS-зоны. Репликация DNS-зоны через запрос AXFR — это процесс, при котором все содержимое DNS-зоны передается от одного DNS-сервера другому, обычно для синхронизации данных между основным и резервными серверами. Запрос AXFR (Asynchronous Full Transfer Zone) предназначен для легальной передачи полной копии зоны, однако его использование может быть опасным, если такой запрос разрешен от недоверенных источников.	• Reconnaissance (TA0043) • Application Layer Protocol (T1071) • DNS (T1071.004) • Gather Victim Network Information (T1590) • DNS (T1590.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1398	Подозрительная сетевая активность с одного узла	Система PT NAD обнаруживает атаки на основе сигнатурного анализа. Данное правило выявляет множественные срабатывания сигнатур за короткий промежуток времени с одного источника, направленные на различные узлы сети.	• Execution (TA0002) • Exploitation for Client Execution (T1203)
RV-D-1399	Подозрительная сетевая активность с нескольких узлов	Система PT NAD обнаруживает атаки на основе сигнатур. Данное правило выявляет множественные срабатывания сигнатур за короткий промежуток времени с разных узлов, направленные на один хост.	• Execution (TA0002) • Exploitation for Client Execution (T1203)

Suricata

- Suricata: настройка источника

Suricata: настройка источника

Данное руководство описывает процесс настройки журнала `eve-log` и отправки событий Suricata в R-Vision SIEM.

Предварительные требования

- Сетевая доступность нод кластера SIEM по целевому порту и протоколу для Suricata.

Настройка Suricata

1. В файле `/etc/suricata/suricata.yaml` включите в параметрах логирования `eve-log` для `syslog`:

```
# Extensible Event Format (nicknamed EVE) event log in JSON format
 - eve-log:
     enabled: yes
     filetype: syslog #regular|syslog|unix_dgram|unix_stream|redis
     #filename: eve.json
     # Enable for multi-threaded eve.json output; output files are amended with
     # with an identifier, e.g., eve.9.json
     #threaded: false
     #prefix: "@cee: " # prefix to prepend to each log entry
     # the following are valid when type: syslog above
     identity: "suricata"
     facility: local5
     level: Warning ## possible levels: Emergency, Alert, Critical,
```

```
                    ## Error, Warning, Notice, Info, Debug
      #ethernet: no  # log ethernet header in events when available
```

2. Перезапустите службу `suricata.service` с помощью команды:

```
systemctl restart suricata.service
```

3. Настройте передачу событий по `syslog`. Для этого создайте файл `/etc/rsyslog.d/50-suricata-eve.conf` со следующим содержимым:

```
if $syslogtag == 'suricata' or $programname == 'suricata' then {
  action(type="omfwd" Target="<target>" Port="<port>" Protocol="<protocol>")
  stop
}
```

   - `<target>`: IP-адрес или полное доменное имя (FQDN) коллектора R-Vision SIEM.
   - `<port>`: порт точки входа `Syslog` в конвейере R-Vision SIEM.
   - `<protocol>`: сетевой протокол (`tcp` или `udp`).

4. Перезапустите службу `rsyslog.service` с помощью команды:

```
systemctl restart rsyslog.service
```

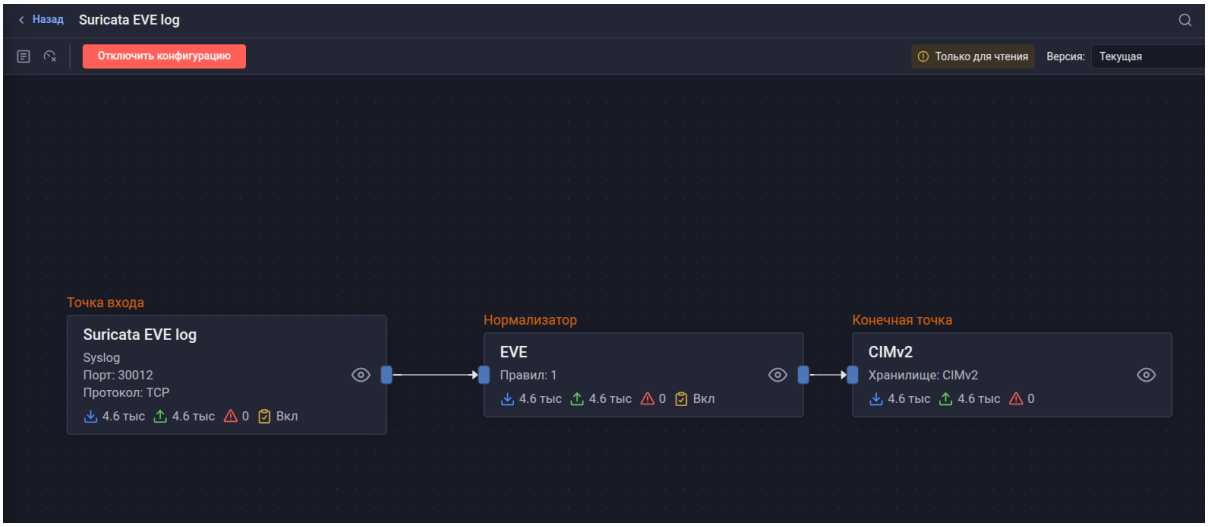
Настройка передачи событий журнала `eve-log` завершена.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий Suricata в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - **Название**: введите название точки входа.
   - **Тип точки входа**: выберите вариант **Syslog**.
   - **Порт точки входа**: введите значение в соответствии с настройками на стороне Suricata.
   - **Протокол**: выберите вариант в соответствии с настройками на стороне Suricata.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Suricata EVE** (идентификатор правила: **RV-N-314**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

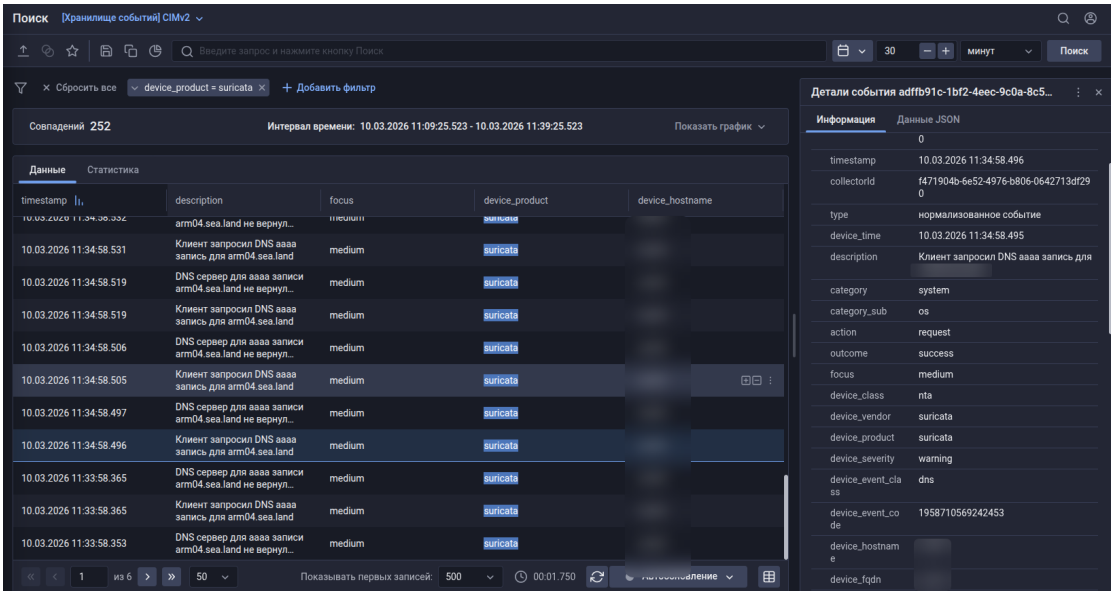
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Suricata.

Найти события Suricata в хранилище можно по следующему фильтру:

```
device_product = "suricata"
```



Гарда NDR

- Гарда NDR: настройка источника

Гарда NDR: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий средства сетевого обнаружения и реагирования Гарда NDR в R-Vision SIEM.

Предварительные требования

- Сетевая доступность сервера управления Гарда NDR по целевому порту и протоколу для коллектора SIEM.
- Сетевая доступность сервера ClickHouse Гарда NDR по целевому порту и протоколу для коллектора SIEM.
- Учетная запись в СУБД ClickHouse с правами на чтение (сбор событий из БД).

Настройка Гарда NDR

Описание подсистемы журналирования

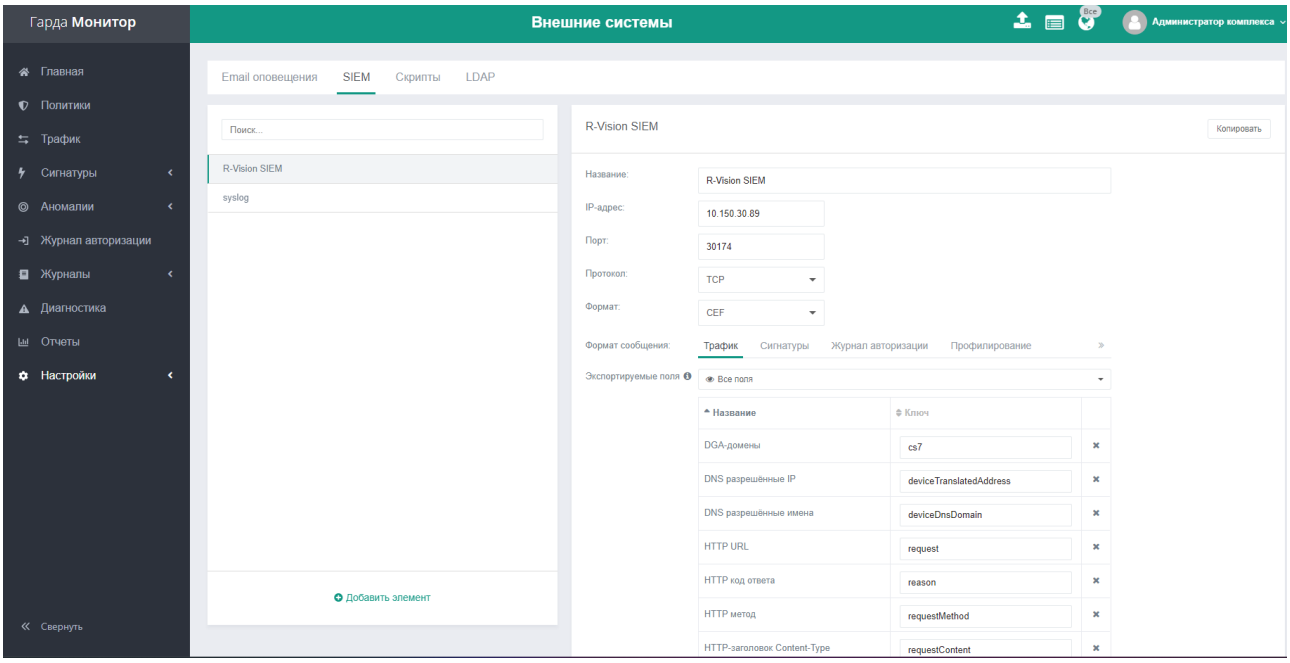
Гарда NDR позволяет передавать события, регистрируемые в рамках политик, по Syslog в формате CEF. Данные журналов действий пользователей и системных событий пишутся в СУБД ClickHouse.

Отправка событий Гарда NDR

Настройка логирования для политики сбора трафика

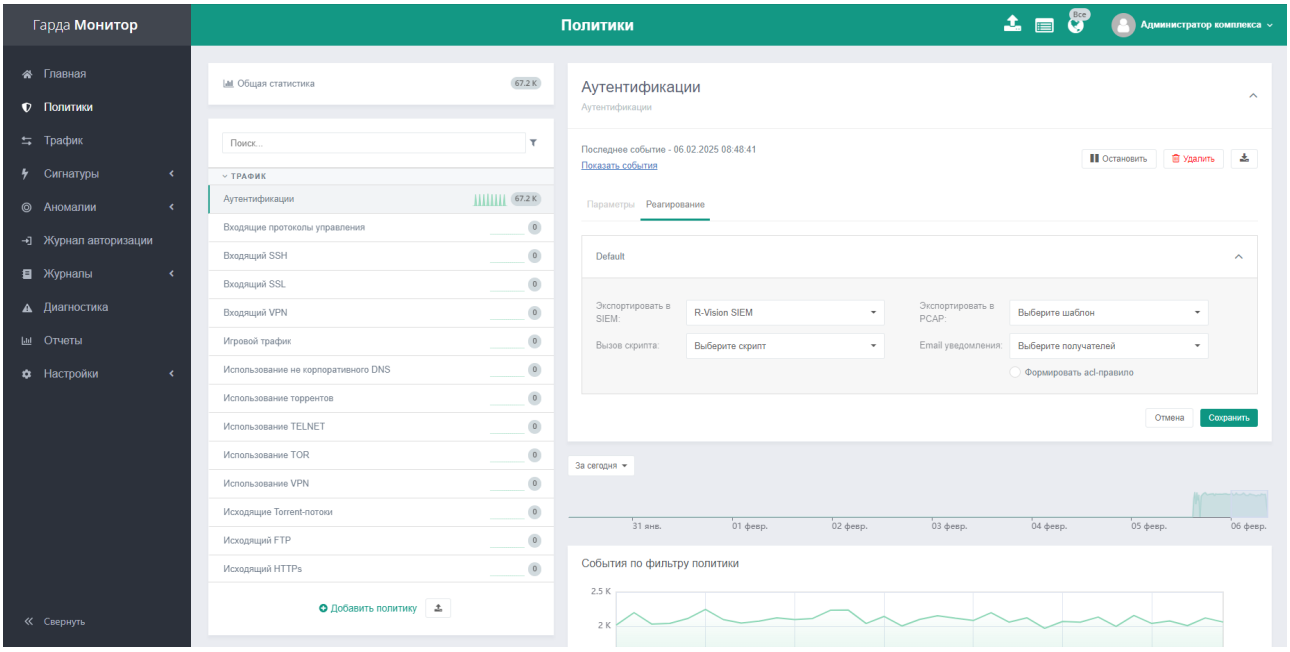
Чтобы настроить экспорт событий Гарда NDR, выполните следующие шаги:

1. На панели администрирования **Гарда Монитор** перейдите в раздел **Настройки** → **Внешние системы** → **SIEM**.
2. Нажмите на кнопку **Добавить элемент** (＋).
3. Заполните поля **Название**, **IP-адрес**, **Порт** и **Протокол**, указав в них данные точки входа из конвейера SIEM.
4. Сохраните изменения.



5. Перейдите в раздел **Политики**.
6. Выберите политику, события которой нужно пересылать в R-Vision SIEM.
7. Перейдите на вкладку **Реагирование** и раскройте настройки.

8. В поле **Экспортировать в SIEM** выберите из выпадающего списка созданный ранее профиль.



Настройка экспорта событий политики в R-Vision SIEM завершена.

9. Повторите шаги 6—8 для каждой политики.

Настройка ClickHouse для сбора событий журналов действий пользователей и системных событий

Чтобы настроить ClickHouse для передачи событий журналов, выполните следующие шаги:

1. На сервере ClickHouse откройте файл `/etc/clickhouse-server/users.xml`.
2. Задайте пароль пользователю `readonly` в теге `<password>`.
3. В теге `<ip>` укажите адреса коллекторов R-Vision SIEM или целую подсеть, откуда пользователю будет разрешено подключаться к СУБД.

   Пример конфигурации:

```
<readonly>
    <password>readonly</password>
    <networks incl="networks" replace="replace">
        <ip>::1</ip>
        <ip>127.0.0.1</ip>
        <ip>10.150.0.0/16</ip>
    </networks>
    <profile>readonly</profile>
    <quota>default</quota>
</readonly>
```

4. В конфигурационном файле `/etc/clickhouse-server/config.xml` раскомментируйте блок:

```
<http_port>8123</http_port>
```

5. Перезапустите сервер ClickHouse:

```
systemctl restart clickhouse-server
```

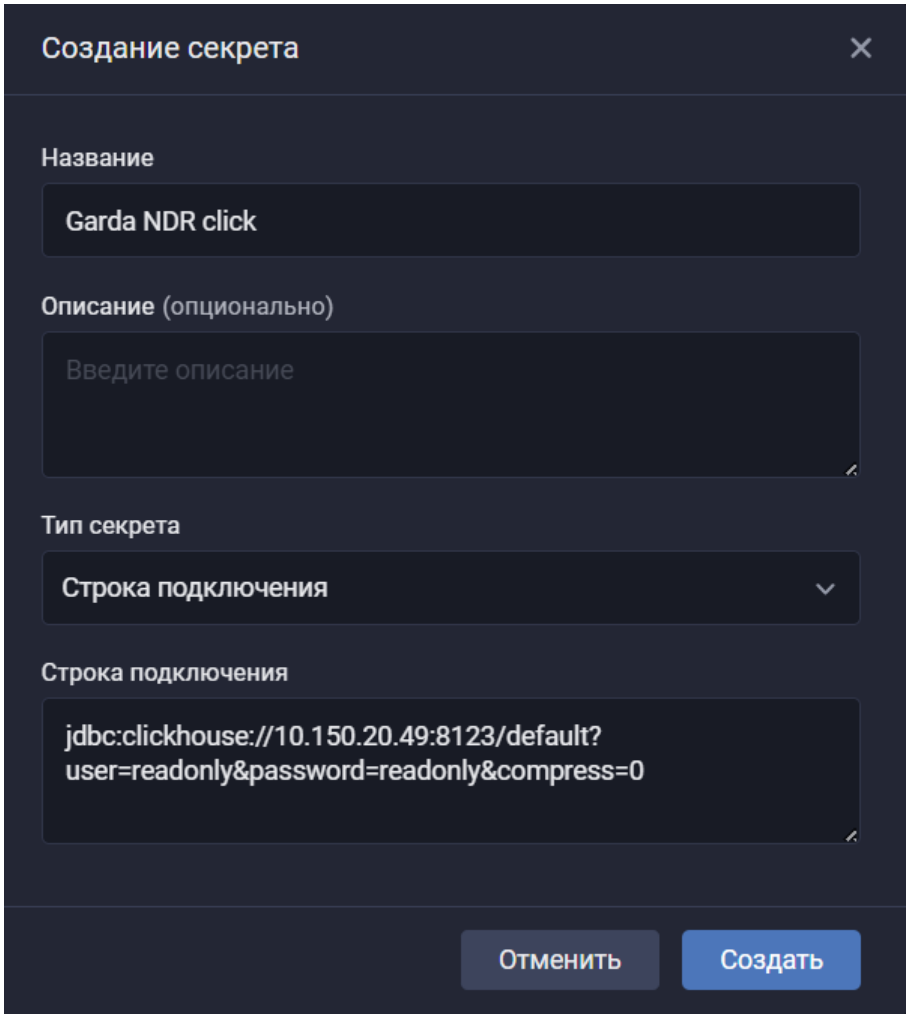
Подготовка ClickHouse для передачи событий журналов в R-Vision SIEM завершена.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте секрет со строкой подключения. Для этого:
   a. Перейдите в раздел **Ресурсы** → **Секреты**.
   b. Нажмите на кнопку **Создать** (＋).
   c. В раскрывшемся окне создания секрета заполните поля:
      - Название: введите название секрета.
      - Описание (опционально): опишите, для чего будет использоваться секрет.
      - Тип секрета: выберите вариант **Строка подключения**.
      - Строка подключения: введите строку вида:

```
jdbc:clickhouse://10.150.20.49:8123/default?user=readonly&password=readonly&
compress=0
```



d. Нажмите на кнопку **Создать**.

2. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
3. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название **Garda NDR Traffic**.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне Гарда NDR.
   - Протокол: выберите вариант в соответствии с настройками на стороне Гарда NDR.
4. Добавьте VRL-трансформацию:

```
.device_product = "Garda NDR"
.device_event_category = "traffic event"
```

5. Соедините добавленную точку входа и VRL-трансформацию.
6. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название **Garda NDR User Actions**.
   - Тип точки входа: выберите вариант **Database**.
   - Драйвер базы данных: выберите вариант **ClickHouse**.
   - Адрес подключения: выберите секрет, созданный ранее.

- SQL-запрос: введите запрос вида:

```
SELECT *,
hostName() AS device_hostname,
toUnixTimestamp(TimeReal) AS rt
FROM monitor.logging_user_actions WHERE rt > ? ORDER BY rt ASC;
```

- Поле идентификатора: введите ключ `rt` со значением 1.
- Интервал запроса, секунд: введите значение 15.

7. Добавьте VRL-трансформацию:

```
.device_product = "Garda NDR"
.device_event_category= "user action"
```

8. Соедините добавленную точку входа и VRL-трансформацию.
9. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название **Garda NDR System Messages**.
   - Тип точки входа: выберите вариант **Database**.
   - Драйвер базы данных: выберите вариант **ClickHouse**.
   - Адрес подключения: выберите секрет, созданный ранее.
   - SQL-запрос: введите запрос вида:

```
SELECT *,
hostName() AS device_hostname,
toUnixTimestamp(TimeReal) AS rt
FROM monitor.logging_system_messages WHERE rt > ? ORDER BY rt ASC;
```

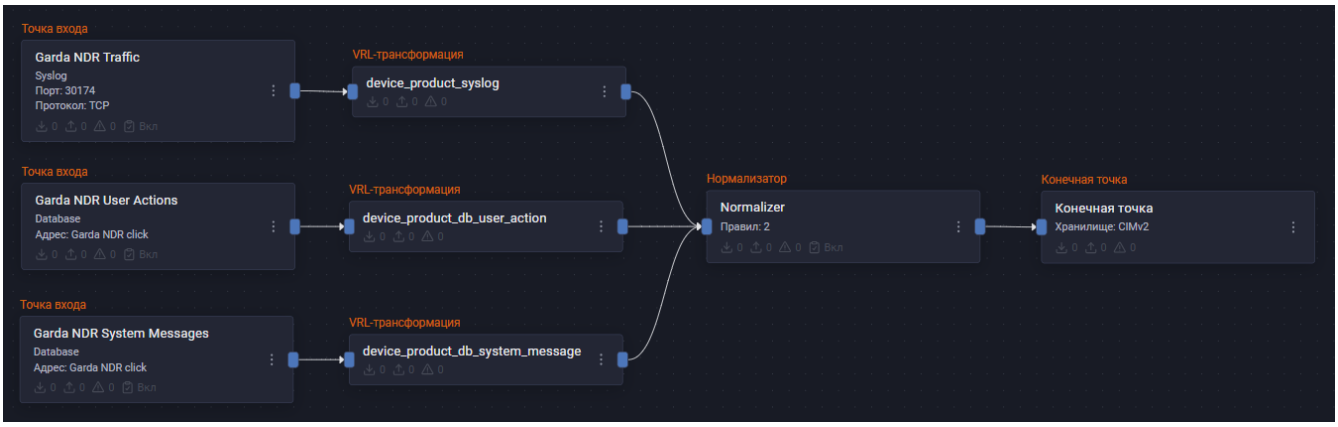
   - Поле идентификатора: введите ключ `rt` со значением 1.
   - Интервал запроса, секунд: введите значение 15.
10. Добавьте VRL-трансформацию:

```
.device_product = "Garda NDR"
.device_event_category = "system message"
```

11. Соедините добавленную точку входа и VRL-трансформацию.
12. Добавьте на конвейер элемент **Нормализатор** с правилами **Garda NDR DB** (идентификатор правила: **RV-N-335**) и **Garda NDR Syslog** (идентификатор правила: **RV-N-337**).
13. Соедините нормализатор с тремя добавленными VRL-трансформациями.
14. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
15. Соедините конечную точку с нормализатором.

16. Сохраните и установите конфигурацию конвейера.

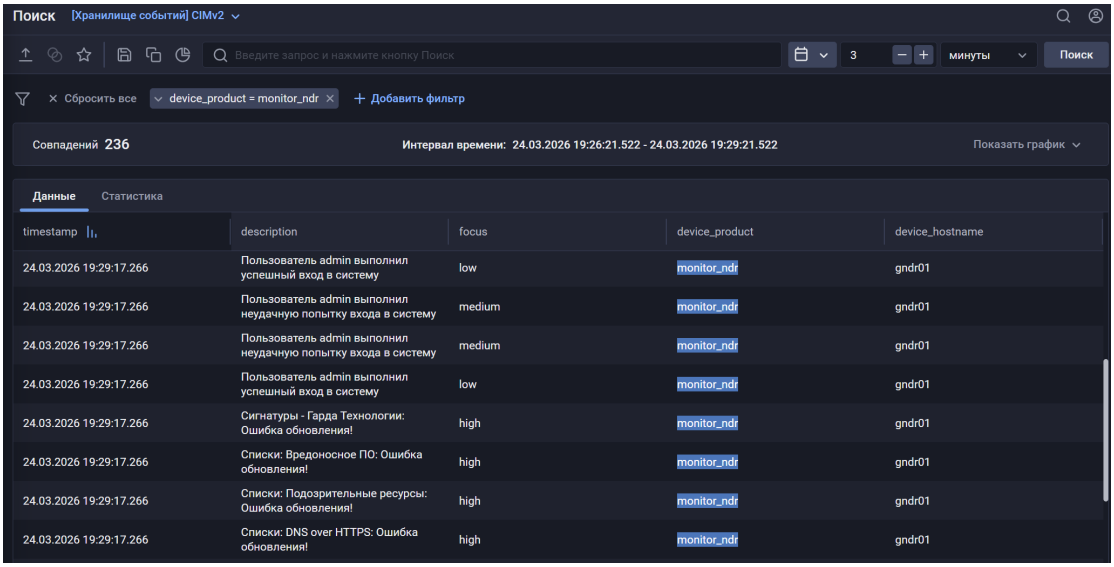
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Гарда NDR.

Найти события Гарда NDR в хранилище можно по следующему фильтру:

```
device_product = "monitor_ndr"
```



Системы аутентификации, авторизации и учета

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых систем аутентификации, авторизации и учета:

- Efros DefOps NAC

Efros DefOps NAC

- Efros DefOps NAC: настройка источника

Efros DefOps NAC: настройка источника

Данная инструкция описывает настройку сбора событий Efros DefOps NAC и их последующей отправки в R-Vision SIEM.

Предварительные требования

Сетевая доступность нод кластера SIEM по целевому порту и протоколу для источника.

Настройка Efros DefOps NAC

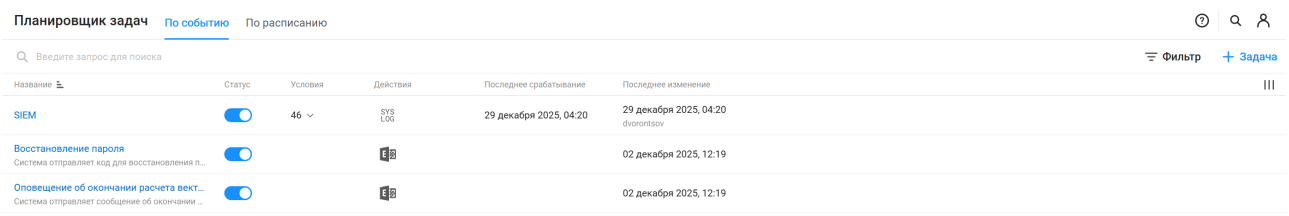
Настройка журналирования

Создание планировщика и отправка событий

Для осуществления сбора логов в SIEM необходимо в веб-интерфейсе Efros DefOps NAC создать планировщик задач и настроить отправку Syslog-сообщений.

Для создания планировщика задач выполните следующие действия:

1. Войдите в веб-интерфейс с правами администратора.
2. Перейдите в раздел **Администрирование** → **Планировщик**.
3. Убедитесь что открыта вкладка **По событию** и нажмите на кнопку **Задача** (+).



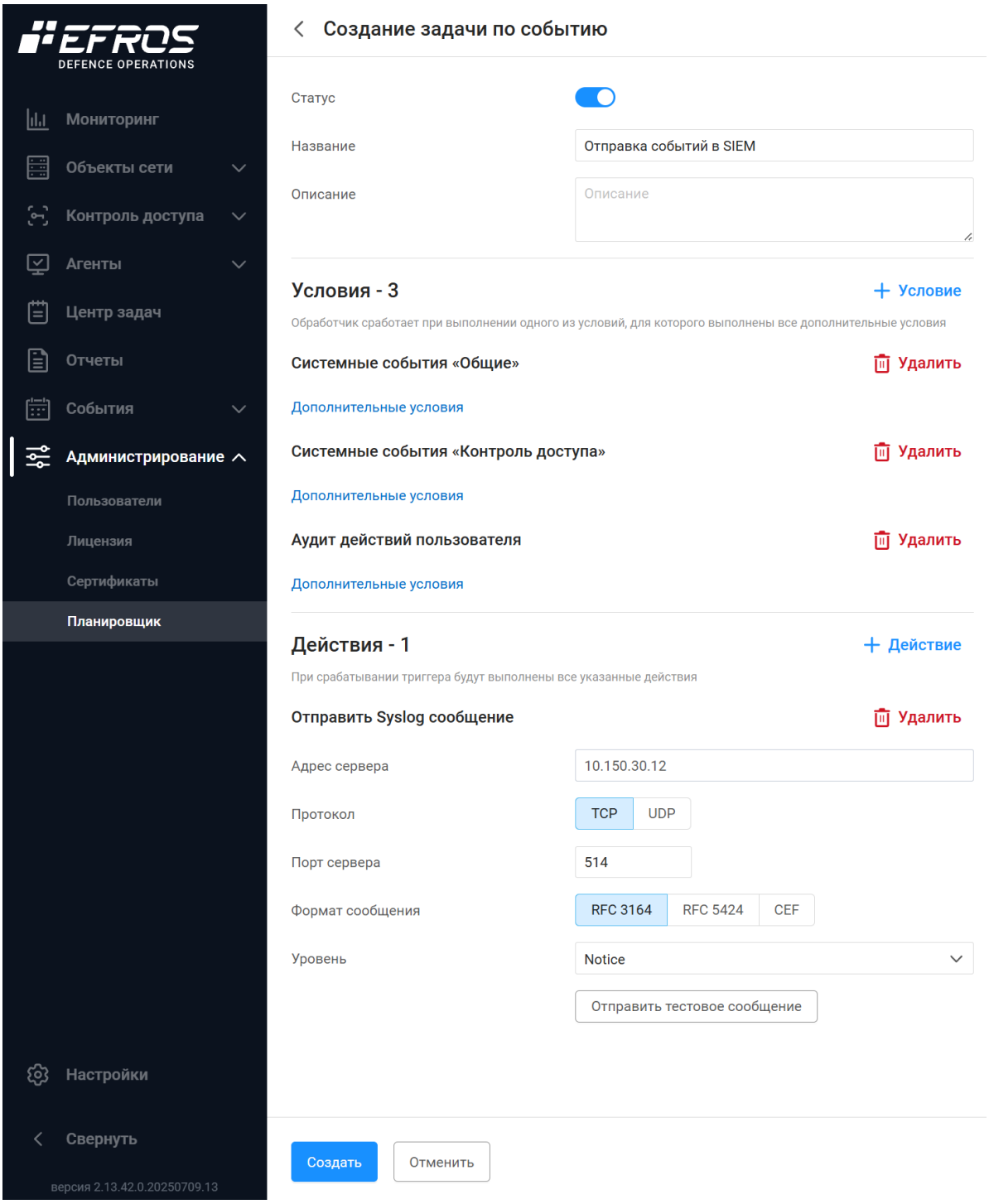
4. В открывшемся окне настройте параметры задачи:
   a. Переведите переключатель **Статус** в активное положение.
   b. Введите название планировщика.
   c. Добавьте необходимые условия.
   d. Добавьте действие **Отправить Syslog сообщение** со следующими настройками:

i. **Адрес сервера**: укажите IP-адрес коллектора SIEM.

ii. **Протокол**: выберите протокол отправки событий **TCP**.

iii. **Порт сервера**: укажите порт точки входа на конвейере SIEM.

iv. **Формат сообщения**: выберите вариант **RFC 3164**.



5. Нажмите на кнопку **Создать**.

При срабатывании выбранных в планировщике условий события будут отправляться в R-Vision SIEM.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие

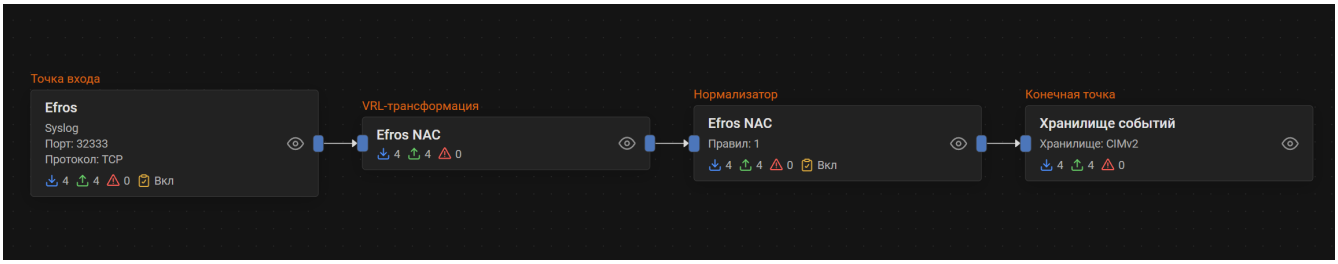
шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне Efros DefOps NAC.
   - Протокол: выберите из выпадающего списка вариант **TCP**.
3. Добавьте VRL-трансформацию со следующим кодом:

```
.device_vendor = "efros"
```

4. Соедините VRL-трансформацию с точкой входа.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **Efros NAC** (идентификатор правила: **RV-N-261**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

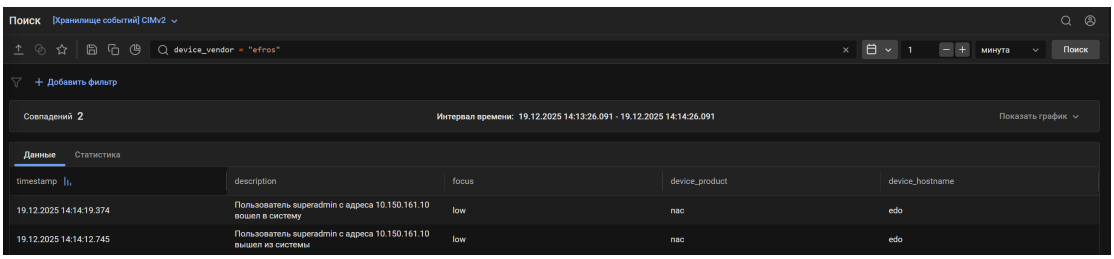
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Efros DefOps NAC.

Найти события Efros DefOps NAC в хранилище можно по следующему фильтру:

```
device_vendor = "efros"
```



Системы виртуализации

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых систем виртуализации:

- Microsoft Hyper-V
- Orion soft zVirt
- VMware ESXi
- VMware vCenter Server

Microsoft Hyper-V

- Microsoft Hyper-V: настройка источника

Microsoft Hyper-V: настройка источника

Данное руководство описывает процесс отправки событий из журналов Hyper-V в R-Vision SIEM с помощью продукта R-Vision EVO Endpoint.

Предварительные требования

- На машине, с которой планируется сбор событий, установлен агент R-Vision EVO Endpoint.
- Агент находится в активном состоянии и успешно подключён к R-Vision SIEM.
- Пользователь, выполняющий настройку, имеет права администратора локальной машины.
- Система работает под управлением Microsoft Windows с установленным Microsoft Windows Hyper-V.

Настройка сбора событий Microsoft Hyper-V

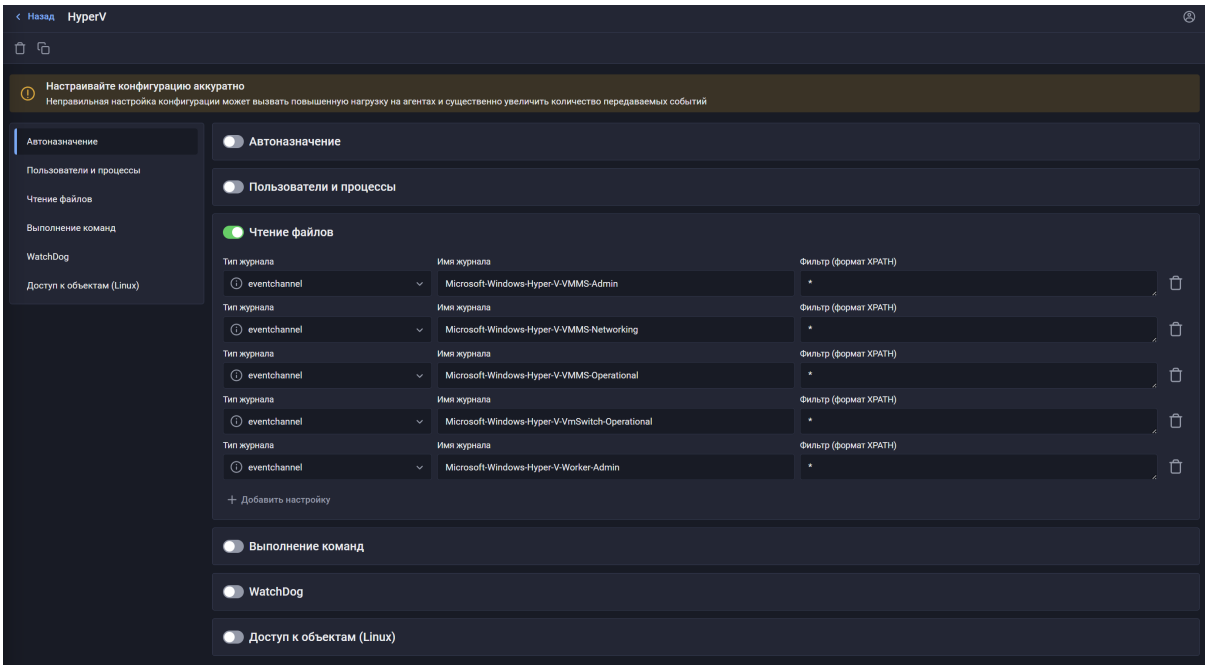
Настройка политики сбора событий

Для настройки сбора событий журналов Hyper-V выполните следующие действия:

1. В главном меню интерфейса R-Vision SIEM перейдите в раздел **Агенты** → **Группы агентов**.
2. Нажмите на кнопку **Создать** (+).
3. В раскрывшемся окне введите название группы.
4. В настройках группы переведите переключатель **Чтение файлов** в активное положение.
5. В разделе **Чтение файлов** нажмите на кнопку **Добавить** (+) и добавьте следующие журналы (тип **eventchannel**):
   - `Microsoft-Windows-Hyper-V-VMMS-Admin`
   - `Microsoft-Windows-Hyper-V-VMMS-Networking`
   - `Microsoft-Windows-Hyper-V-VMMS-Operational`
   - `Microsoft-Windows-Hyper-V-VmSwitch-Operational`

- Microsoft-Windows-Hyper-V-Worker-Admin

6. Нажмите на кнопку **Сохранить**.



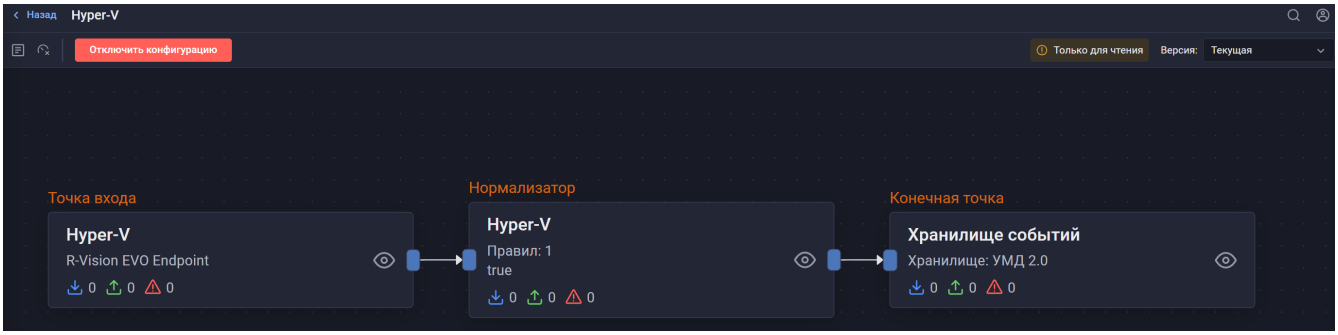
7. Добавьте нужные узлы в созданную группу:
   a. Перейдите в список агентов.
   b. Выберите нужный узел и нажмите на кнопку ⋮ .
   c. Выберите созданную группу и нажмите **Добавить**.
8. Дождитесь применения политики на агенте.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **R-Vision EVO Endpoint**.
   - Домен: введите значение в соответствии с настройками на стороне шлюза.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Microsoft Windows Hyper-V** (идентификатор правила: **RV-N-228**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

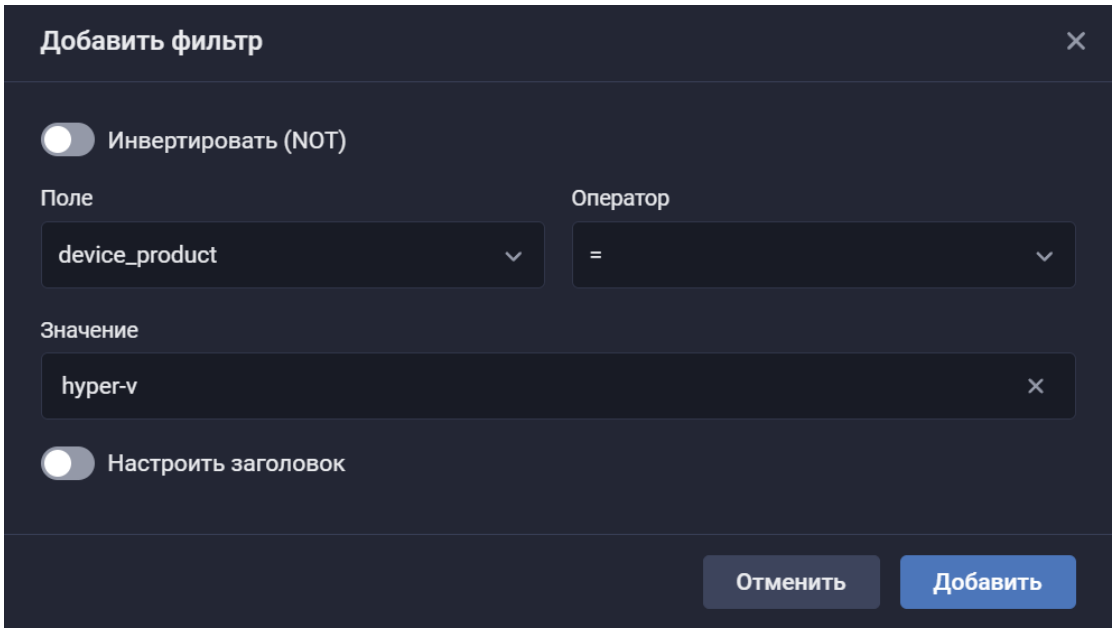
Пример конфигурации конвейера:



После настройки политики сбора и передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события хоста из журналов Windows Hyper-V.

Найти события Windows Hyper-V в хранилище можно по следующему фильтру:

```
device_product = "hyper-v"
```



Orion soft zVirt

- Orion soft zVirt: настройка источника

Orion soft zVirt: настройка источника

Данное руководство описывает процесс отправки событий аудита ИБ сервиса Hosted Engine платформы виртуализации zVirt.

Предварительные требования

Перед настройкой пересылки событий в R-Vision SIEM убедитесь, что сетевая связность между сервером СУБД, используемым средством виртуализации zVirt, и SIEM обеспечена, а необходимые порты открыты.

Настройка zVirt

Для настройки источника выполните следующие шаги:

1. Разрешите подключаться к СУБД извне по паролю. Для этого добавьте в файл `pg_hba.conf` следующую строку:

   ```
   host    all             all             0.0.0.0/0           md5
   ```

2. Перезапустите сервис:

   ```
   systemctl restart postgresql.service
   ```

3. Создайте учетную запись, от имени которой будет производиться подключение к СУБД. Для этого подключитесь к СУБД локально от имени учетной записи `postgres`:

   ```
   sudo -u postgres psql
   ```

4. Создайте пользователя, который впоследствии будет читать записи из таблицы аудита, наделив его правами на подключение к базе `engine`:

   ```
   create user zvirt_logger;
   alter role zvirt_logger with password 'password';
   grant connect on engine to zvirt_logger;
   ```

Настройка в R-Vision SIEM

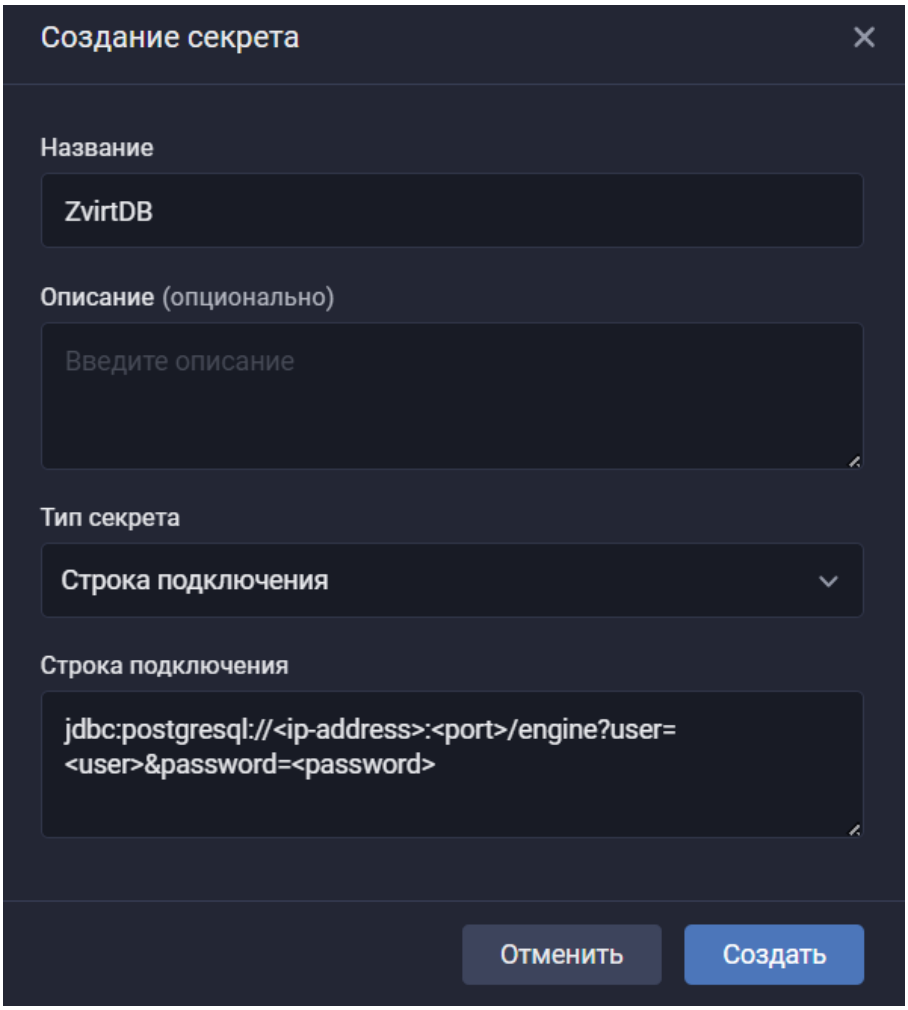
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте секрет со строкой подключения. Для этого:
   a. Перейдите в раздел **Ресурсы** → **Секреты**.
   b. Нажмите на кнопку **Создать** (＋).
   c. В раскрывшемся окне создания секрета заполните поля:
      - **Название**: введите название секрета.
      - **Описание (опционально)**: опишите, для чего будет использоваться секрет.
      - **Тип секрета**: выберите вариант **Строка подключения**.
      - **Строка подключения**: введите строку вида:

        ```
        jdbc:postgresql://<ip-address>:<port>/engine?user=<user>&password=<password>
        ```

        где:

- `<ip-address>` — адрес вашего сервера Hosted Engine.
- `<port>` — порт подключения к СУБД Hosted Engine. По умолчанию используется порт `5432`.
- `<user>` — имя пользователя для подключения к Hosted Engine.
- `<password>` — пароль пользователя для СУБД Hosted Engine.



d. Нажмите на кнопку **Создать**.

2. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
3. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - **Название**: введите название точки входа.
   - **Тип точки входа**: выберите вариант **Database**.
   - **Драйвер базы данных**: выберите вариант **PostgreSQL**.
   - **Адрес подключения**: выберите секрет, созданный ранее.
   - **SQL-запрос**: для сбора логов из таблицы `audit_log` добавьте следующую команду:

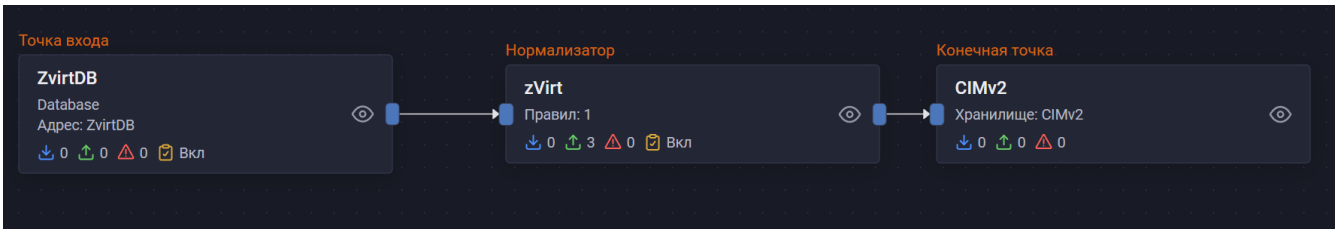
```
SELECT
    *,
    'zVirt' AS appname,
    (SELECT inet_server_addr()) AS server_ip
FROM audit_log
```

```
WHERE audit_log_id > ?::integer;
```

- **Поле идентификатора**: введите ключ `audit_log_id` со значением `1`.

4. Добавьте на конвейер элемент **Нормализатор** с правилом **Orion Soft zVirt** (идентификатор правила: **RV-N-341**).
5. Соедините нормализатор с точкой входа.
6. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
7. Соедините конечную точку с нормализатором.
8. Сохраните и установите конфигурацию конвейера.

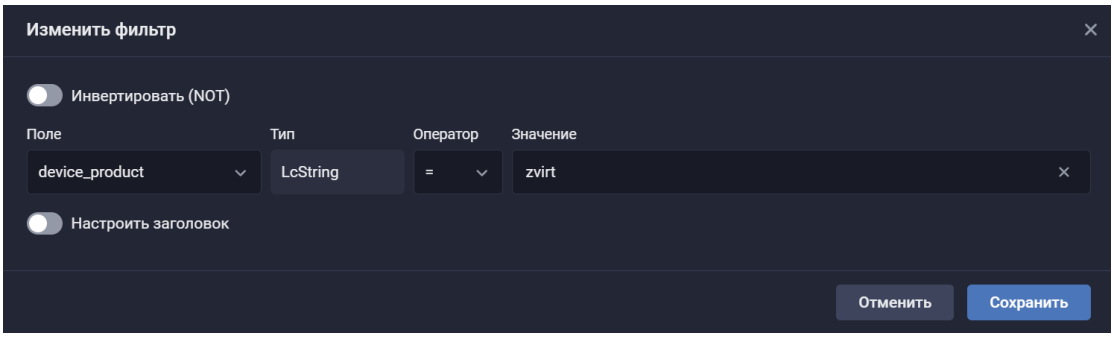
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события zVirt.

Найти события zVirt в хранилище можно по следующему фильтру:

```
device_product = "zvirt"
```



VMware

- VMware ESXi
- VMware vCenter Server
- VMware ESXi и VMware vCenter Server: правила корреляции

VMware ESXi

- VMware ESXi: настройка источника
- VMware ESXi: правила корреляции

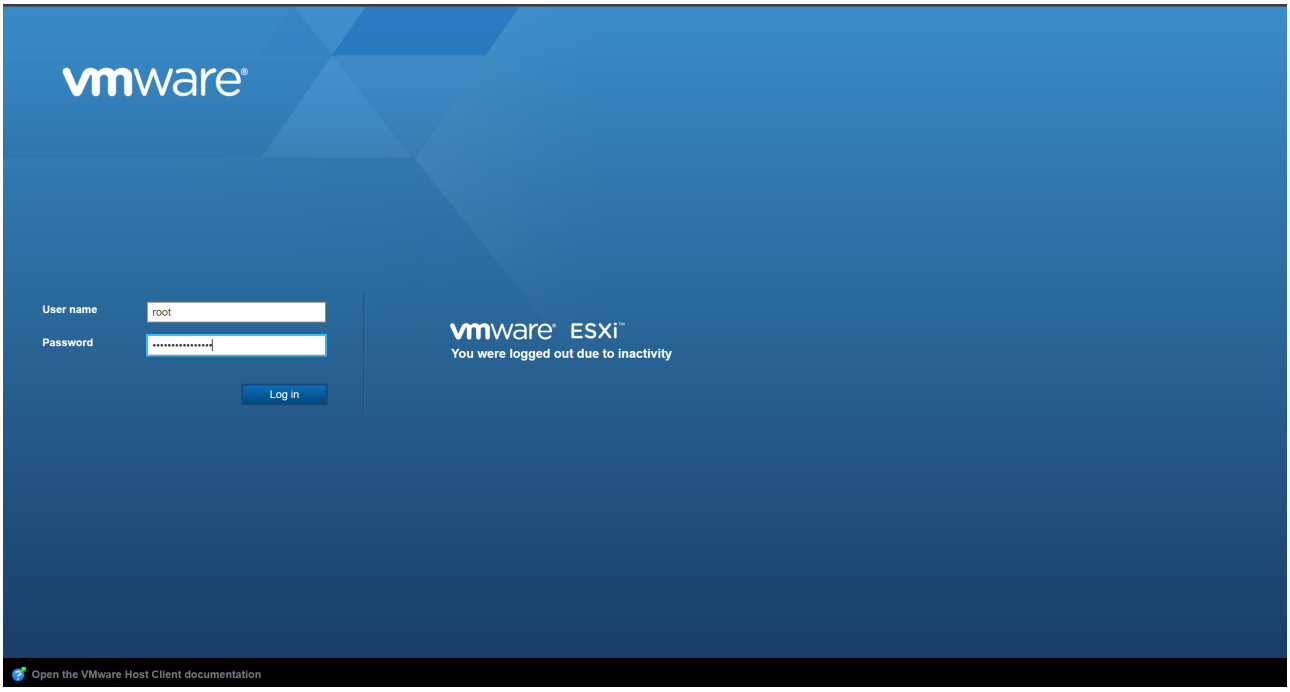
VMware ESXi: настройка источника

Данное руководство описывает процесс отправки событий источника VMware ESXi в R-Vision SIEM.

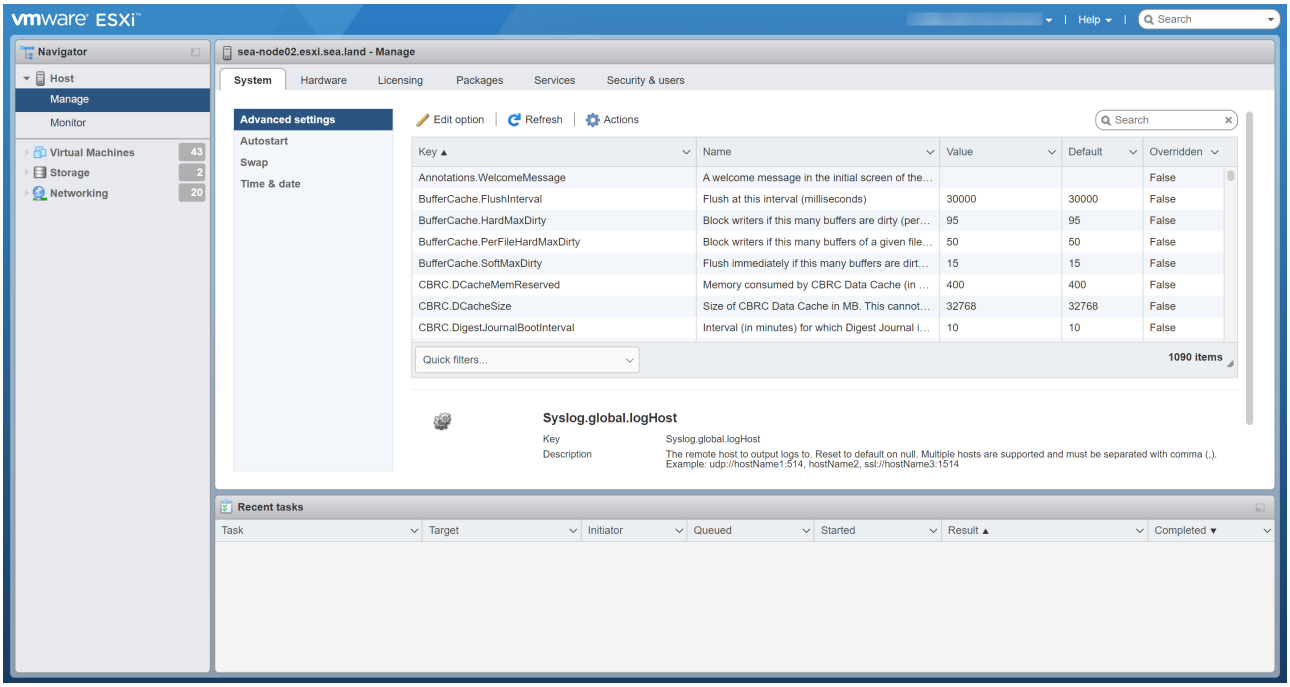
Настройка VMware ESXi

Для настройки источника выполните следующие шаги:

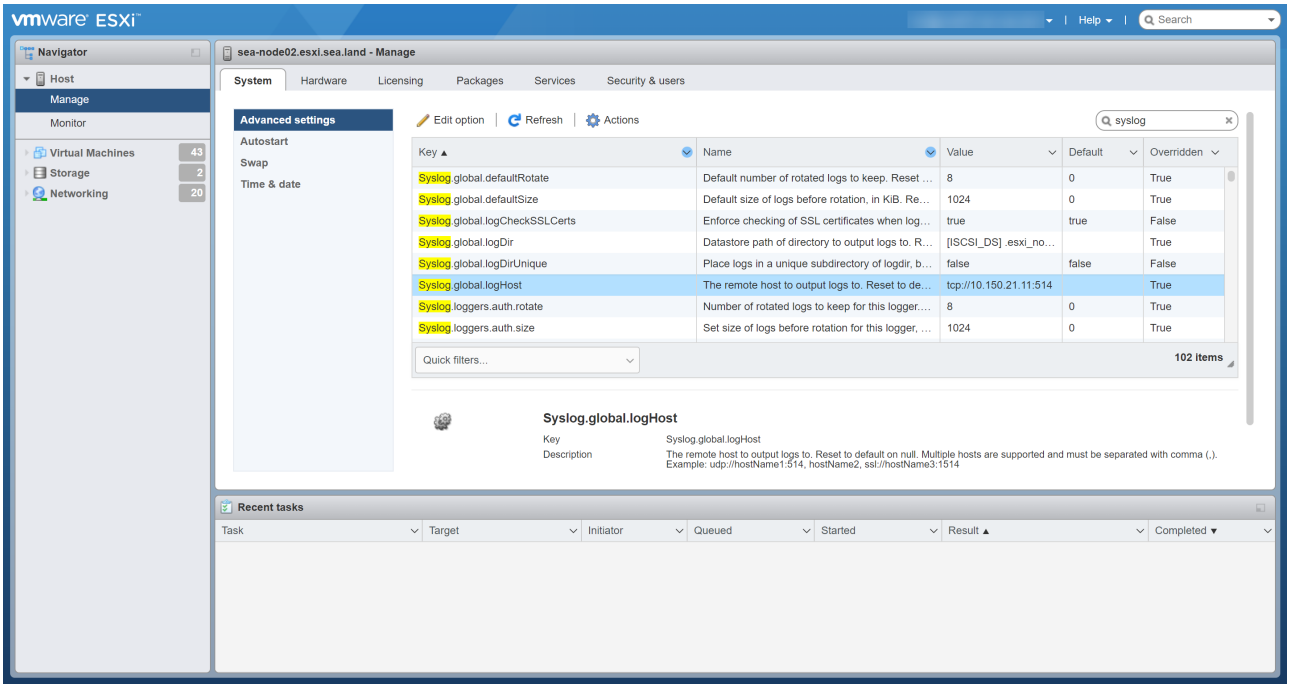
1. Войдите в веб-интерфейс VMware ESXi.



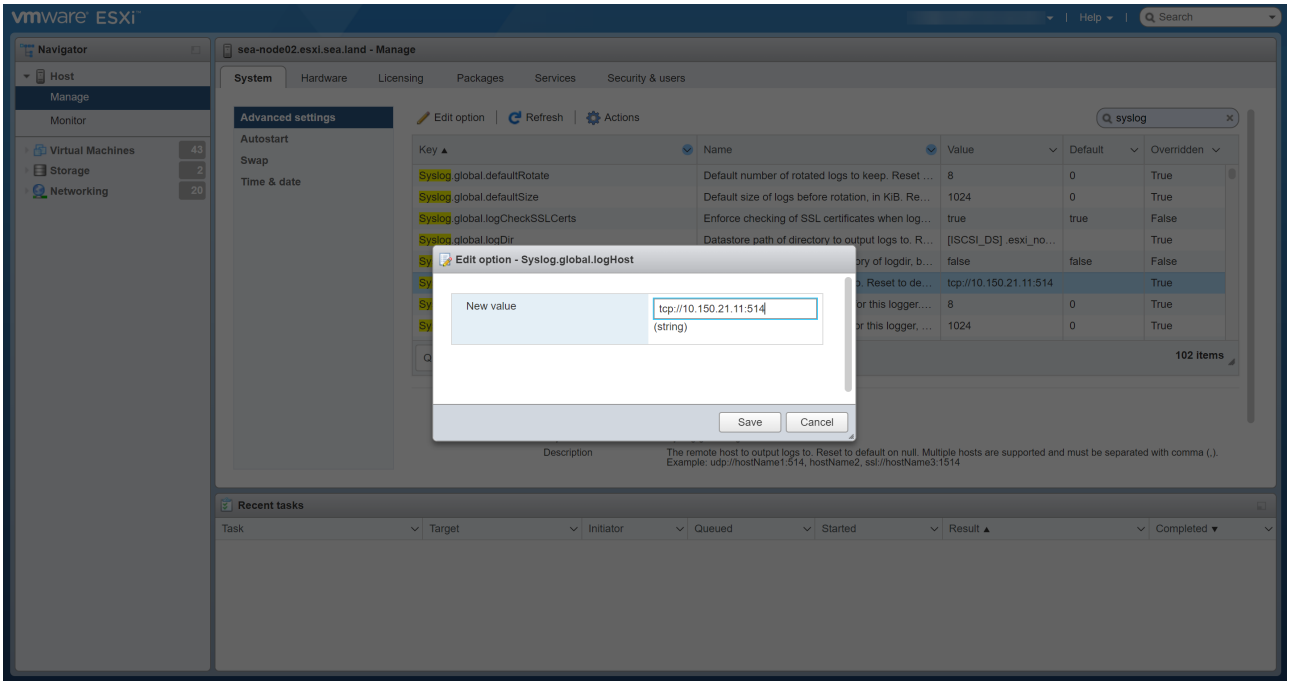
2. Перейдите в раздел **Manage**.



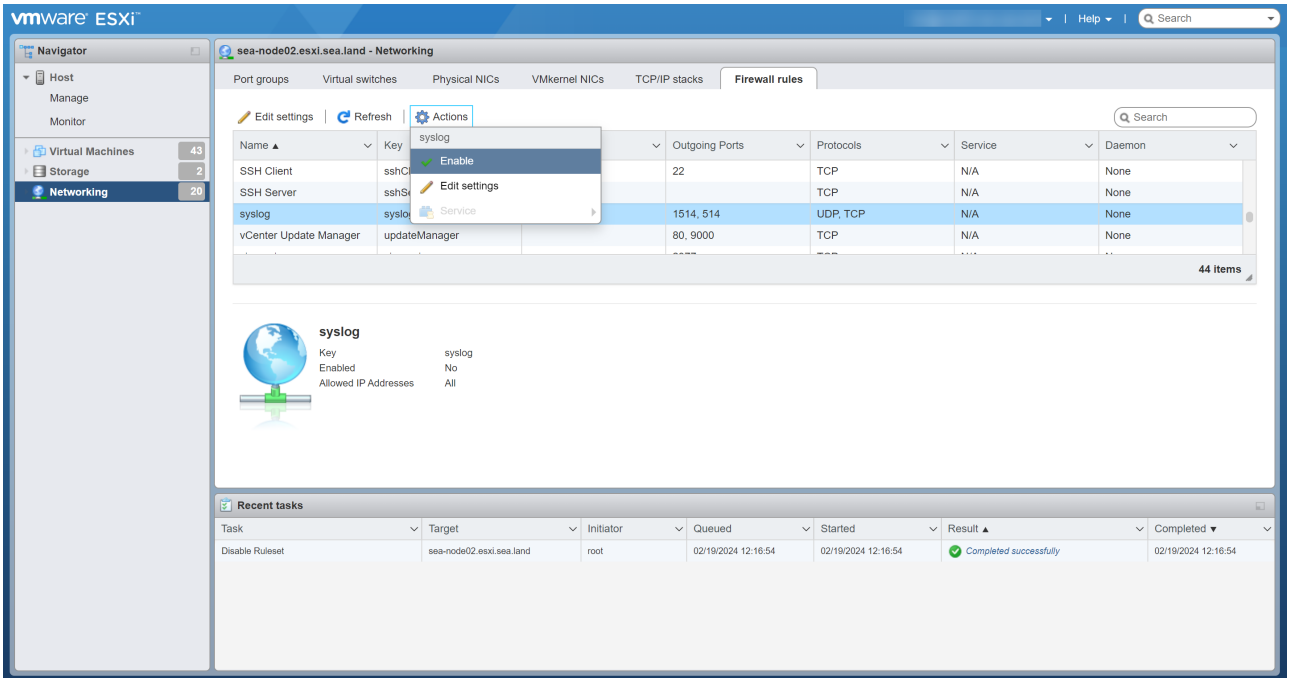
3. На вкладке **System** в разделе **Advanced settings** выберите параметр **Syslog.global.logHost**.



4. Нажмите на кнопку **Edit option**. Откроется окно настроек параметра.
5. Укажите адрес коллектора SIEM, порт точки входа и протокол.



6. Нажмите на кнопку **Save**.
7. Перейдите в раздел **Networking**.
8. На вкладке **Firewall rules** выберите из выпадающего списка **Actions** опцию **Enable**, чтобы включить сервис **syslog**.



Настройка на стороне источника завершена.

Настройка в R-Vision SIEM

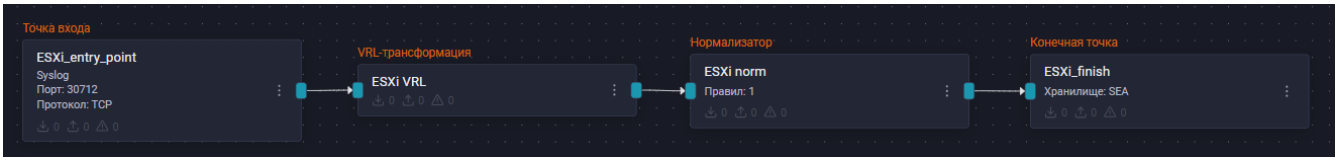
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне ESXi.
   - Протокол: выберите вариант в соответствии с настройками на стороне ESXi.
3. Добавьте VRL-трансформацию:

```
.device_product = "esxi"
```

4. Соедините добавленную точку входа и VRL-трансформацию.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **VMware ESXi** (идентификатор правила: **RV-N-179**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

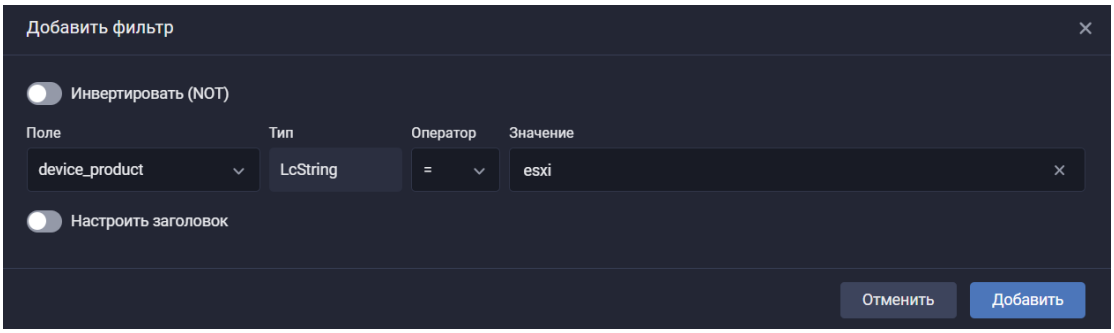
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события ESXi.

Найти события ESXi в хранилище можно по следующему фильтру:

```
device_product = "esxi"
```



VMware ESXi: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-981	Создание ssh-туннелей на ESXi	При наличии прав на выполнение команд на хосте атакующий может использовать SSH для организации обратного доступа или скрытого взаимодействия с внешними и внутренними ресурсами через SSH-туннели. Данное правило направлено на выявление создания SSH-туннелей на ESXi-серверах. Оно срабатывает при обнаружении выполнения SSH-команд с аргументами, указывающими на проброс портов `-L`, `-R` или `-D`. Такой подход позволяет зафиксировать попытки организации обхода сетевых политик, удаленного доступа или скрытого трафика в обход мониторинга. При срабатывании правила следует проверить, кто последний осуществлял подключение к серверу и уточнить у ответственных лиц легитимность активности. Также можно использовать команду `ps -c | grep ssh` для анализа активных процессов на сервере ESXi. Если в выводе содержится процесс SSH с подозрительной командой, рекомендуется немедленно завершить этот процесс и начать полноценное расследование в случае отсутствия обоснования для использования туннелей.	• Execution (TA0002) • Command and Control (TA0011) • Command and Scripting Interpreter (T1059) • Unix Shell (T1059.004) • Proxy (T1090) • Protocol Tunneling (T1572)

ID правила	Название правила	Описание	Тактики и техники
RV-D-984	Использование утилит ESXi через CLI	Данное правило направлено на выявление использования административных утилит на серверах VMware ESXi. Эти утилиты включают команды, такие как `vim-cmd`, `esxcli`, `esxcfg-advcfg` и `vmkfstools`, которые могут использоваться для управления виртуализацией, пользователями и разрешениями, создания и удаления виртуальных машин, изменения настроек сети и других критичных операций на сервере ESXi. Использование этих утилит без соответствующего контекста может указывать на попытки злоупотреблений или несанкционированного доступа, особенно если действия выполняются через командную строку, а не через веб-панель управления. Правило срабатывает при обнаружении запуска указанных утилит с ключевыми параметрами `get`, `set`, `kill`, `list`, что позволяет зафиксировать попытки просмотра или изменения конфигурации, завершения процессов и других операций, влияющих на работу инфраструктуры виртуализации. При срабатывании правила необходимо проверить, кто последний выполнял команды на сервере, и уточнить у владельца УЗ легитимность действий. В случае подтверждения нелегитимной активности следует немедленно сменить пароль от УЗ администратора сервера.	• Execution (TA0002) • Persistence (TA0003) • Defense Evasion (TA0005) • Discovery (TA0007) • Lateral Movement (TA0008) • Impact (TA0040) • System Network Configuration Discovery (T1016) • Remote System Discovery (T1018) • Remote Services (T1021) • SSH (T1021.004) • System Network Connections Discovery (T1049) • Process Discovery (T1057) • Command and Scripting Interpreter (T1059) • Unix Shell (T1059.004) Hypervisor

ID правила	Название правила	Описание	Тактики и техники
RV-D-1007	Использование chmod в ESXi через CLI	Использование команды chmod через оболочку ESXi может указывать на попытку изменить права доступа к критически важным файлам или сделать доставленные скрипты исполняемыми, как это наблюдалось в атаках группировки Nevada, направленных на шифрование виртуальных машин. Правило также отслеживает запуск chmod с ключом `+w`, который позволяет редактировать файлы, изначально недоступные для изменения, например crontab, что может привести к добавлению заданий, выполняющихся от имени root. При срабатывании правила необходимо определить инициатора команды, проверить ее легитимность и, при отсутствии разрешения, провести расследование, сменить пароль соответствующей учетной записи и отключить SSH-доступ, если он не используется для администрирования.	• Execution (TA0002) • Defense Evasion (TA0005) • Command and Scripting Interpreter (T1059) • Unix Shell (T1059.004) • File and Directory Permissions Modification (T1222) • Linux and Mac File and Directory Permissions Modification (T1222.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1030	Удаление или отключение логирования команд	Удаление или отключение логирования команд является распространенной техникой сокрытия активности, особенно на платформах без полноценного агентского мониторинга, таких как VMware ESXi. Установив переменную окружения `HISTFILE` в значение `0`, `/dev/null` или удалив файл истории (например, `/.ash_history`), атакующий может предотвратить запись вводимых команд в рамках интерактивной сессии shell. Такое поведение часто наблюдается во вредоносных инструментах, включая бэкдоры, использующие эту технику для минимизации следов присутствия. Данное правило отслеживает команды, отключающие ведение истории команд. При срабатывании правила рекомендуется незамедлительно проверить активные shell-сессии на хосте, приостановить подозрительную активность, инициировать изоляцию системы (если это возможно), заблокировать или временно ограничить доступ для затронутой учетной записи. Если активность не подтверждена как легитимная, стоит сменить пароль от УЗ, которые имеют привилегии администратора.	• Defense Evasion (TA0005) • Indicator Removal (T1070) • Clear Command History (T1070.003) • Impair Defenses (T1562) • Impair Command History Logging (T1562.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1031	Изменение меток времени через touch	Атакующие могут изменять атрибуты времени файлов, чтобы скрыть новые файлы или изменения в существующих. Timestomping — это относительно простая, но эффективная техника сокрытия следов, активно применяемая в атакующих цепочках. На платформе ESXi она может быть реализована с использованием встроенной утилиты touch, которая может изменять значения atime и mtime, что и используется атакующими для сокрытия следов, для установки произвольных дат доступа и модификации файлов. При срабатывании правила рекомендуется незамедлительно проверить активные shell-сессии на хосте, приостановить подозрительную активность, инициировать изоляцию системы (если это возможно), заблокировать или временно ограничить доступ для затронутой учетной записи. Если активность не подтверждена как легитимная, стоит сменить пароль от УЗ, которые имеют привилегии администратора.	• Defense Evasion (TA0005) • Indicator Removal (T1070) • Timestomp (T1070.006)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1032	Маскировка через переименование/подмену index.html	Хосты VMware ESXi используют файл `index.html` в своем веб-интерфейсе для задач управления. Атакующие могут переименовывать этот файл, чтобы избежать обнаружения или заменить его вредоносной версией, что упрощает несанкционированный доступ или утечку данных. Данное правило на основе событий auditd отслеживает выполнение команд, которые могут привести к модификации или замене файла `index.html`. При срабатывании правила определите, какой пользователь или процесс выполнил действие, и проанализируйте журнал входов для выявления возможного несанкционированного доступа. При необходимости изолируйте хост и проверьте файлы на наличие признаков вредоносной активности.	• Defense Evasion (TA0005) • Masquerading (T1036) • Match Legitimate Resource Name or Location (T1036.005)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1033	Доступ к критичным файлам на сервере ESXi	Правило детектирует доступ к критичным файлам на сервере ESXi. К критичным файлам относятся `/var/spool/cron/crontabs/root` и `/etc/rc.local.d/local.sh`. Внося изменения в первый, атакующий может установить скрытые задачи, которые будут выполняться с повышенными правами, что позволяет обеспечить постоянный доступ или выполнение вредоносного кода. Второй файл используют для того, чтобы внедрить команды, автоматически исполняющиеся при загрузке системы, что также способствует сохранению контроля над системой. Данные действия могут указывать на активность шифровальщиков, которые ранее были замечены в атаках на ESXi. Подробнее в разделе reference. При срабатывании правила необходимо проверить, является ли доступ легитимным, если нет, то провести внутреннее расследование и временно ограничить доступ к серверам ESXi. Если возможно, отключите на сервере доступ по ssh и смените пароли от административных учетных записей.	• Execution (TA0002) • Persistence (TA0003) • Boot or Logon Initialization Scripts (T1037) • RC Scripts (T1037.004) • Scheduled Task/Job (T1053) • Cron (T1053.003) • Command and Scripting Interpreter (T1059) • Unix Shell (T1059.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1042	Использование find в ESXi	Использование команды `find` с ключом `-exec` позволяет выполнять команды для каждого найденного файла, что может быть использовано для запуска несанкционированных команд, таких как удаление файлов с расширением `.log` или поиск файлов, характерных для систем VMware ESXi, например, `/etc/vmware/*`, `/usr/lib/vmware/*`, `/vmfs/*`. Данное правило направлено на выявление использования команды `find` с параметром `-exec` или просто на поиск критичных для ESXi-файлов, что может быть признаком проведения разведки или подготовки к шифрованию виртуальной инфраструктуры и других вредоносных действий. При срабатывании этого правила рекомендуется проверить, что именно выполнялось через `find -exec`, либо для чего был осуществлен поиск файлов. Также установить, кто является инициатором действий. Если активность не является легитимной, следует сменить пароль администратора, отключить SSH на сервере и начать расследование.	• Execution (TA0002) • Defense Evasion (TA0005) • Discovery (TA0007) • Collection (TA0009) • Data from Local System (T1005) • Command and Scripting Interpreter (T1059) • Unix Shell (T1059.004) • Indicator Removal (T1070) • File Deletion (T1070.004) • File and Directory Discovery (T1083)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1043	Обнаружение уязвимой конфигурации ESXi	Правило предназначено для выявления потенциально уязвимой конфигурации на серверах VMware ESXi. Оно срабатывает в случаях, когда на узле запускается сервис slpd либо отключается встроенный межсетевой экран, что может свидетельствовать об изменении настроек безопасности. Особенно критичен запуск службы slpd, так как она ранее использовалась в атаках, связанных с уязвимостью CVE-2021-21974, которая позволяет выполнить удаленный код через компонент OpenSLP. Для успешной эксплуатации этой уязвимости необходимо, чтобы служба slpd была активна, а входящий трафик по порту 427 разрешен. Именно поэтому отключение межсетевого экрана также представляет опасность. Это может привести к открытию необходимого для атаки сетевого порта. При срабатывании правила необходимо определить, какое именно действие было выполнено — запуск slpd или отключение межсетевого экрана. Проверьте журнал событий ESXi и определите последнего пользователя, заходившего в систему. Уточните у него легитимность действий. Если активность оказалась нелегитимной, рекомендуется сменить пароль от учетной записи, с которой, вероятно, были внесены изменения, а также от всех учетных записей с привилегиями администратора или входящих в соответствующие группы.	• Initial Access (TA0001) • Execution (TA0002) • Defense Evasion (TA0005) • Lateral Movement (TA0008) • Command and Scripting Interpreter (T1059) • Unix Shell (T1059.004) • Exploit Public-Facing Application (T1190) • Exploitation of Remote Services (T1210) • Impair Defenses (T1562) • Disable or Modify System Firewall (T1562.004) • System Services (T1569)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1202	Лишение пользователя доступа к ESXi	Данное правило предназначено для выявления случаев удаления локальной учетной записи или ее прав доступа на гипервизорах VMware ESXi через веб-интерфейс (GUI). Такая активность может свидетельствовать о попытке атакующего закрепиться в инфраструктуре и устранить доступ легитимных администраторов, чтобы предотвратить вмешательство в дальнейшие вредоносные действия, например, шифрование виртуальных машин.	• Impact (TA0040) • Account Access Removal (T1531)
RV-D-1206	Остановка критичного сервиса ESXi	При наличии прав на выполнение команд на сервере ESXi атакующий может использовать бинарный файл для остановки критичной службы vpxa, что блокирует возможность управления сервером ESXi через сервер vCenter. Этот шаг может являться подготовительным этапом перед шифрованием ВМ, направленным на предотвращение вмешательства со стороны администраторов или специалистов по безопасности, обеспечивая атакующему возможность продолжить шифрование виртуальных машин без помех, как это делала вредоносная утилита MrAgent в атаках на ESXi. Данное правило направлено на выявление остановки службы vpxa путем отслеживания запуска команды через оболочку.	• Impact (TA0040) • Service Stop (T1489)
RV-D-1222	Изменение аудита виртуальной инфраструктуры	После получения доступа к виртуальной инфраструктуре атакующие могут изменить конфигурацию аудита, чтобы нарушить отправку событий или полностью отключить логирование системы.	• Impact (TA0040) • Data Destruction (T1485) • Impair Defenses (T1562)

VMware vCenter Server

- VMware vCenter Server: настройка источника
- VMware vCenter Server: правила корреляции

VMware vCenter Server: настройка источника

Данное руководство описывает процесс отправки событий источника VMware vCenter Server в R-Vision SIEM.

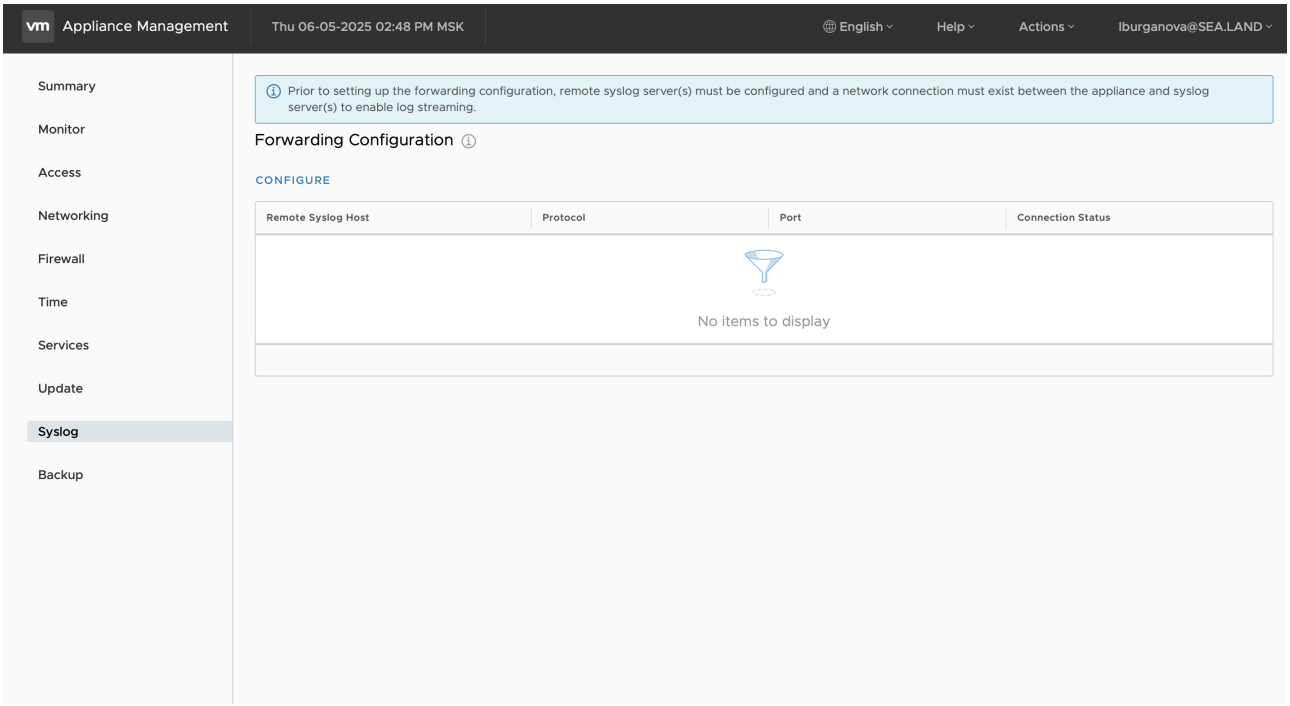
Настройка VMware vCenter Server

Для настройки источника выполните следующие шаги:

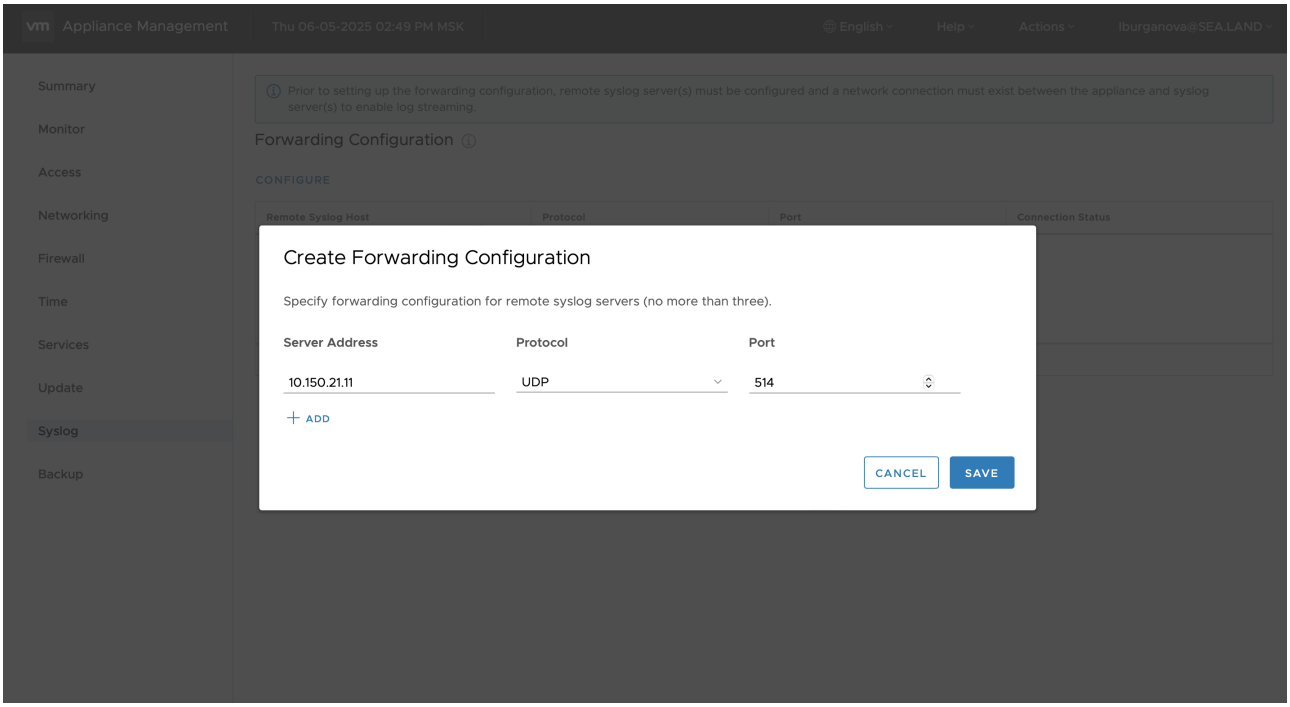
1. Войдите в интерфейс управления VMware vCenter Server Appliance (VCSA) Management:
   a. Откройте веб-браузер.
   b. Перейдите по адресу:

   ```
   https://<IP-адрес-или-FQDN>:5480
   ```

   где `<IP-адрес-или-FQDN>` — актуальные данные вашей системы.
2. Перейдите в раздел **Syslog**.
3. Нажмите на кнопку **CONFIGURE**. Откроется окно создания конфигурации переадресации.



4. Укажите адрес удаленного syslog-сервера или конвейера в SIEM, а также протокол и порт.



5. Нажмите на кнопку **SAVE**.

Настройка на стороне источника завершена.

Настройка в R-Vision SIEM

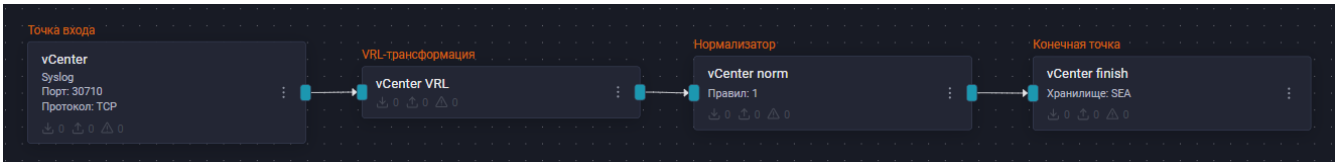
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне vCenter.
   - Протокол: выберите вариант в соответствии с настройками на стороне vCenter.
3. Добавьте VRL-трансформацию:

```
.device_product = "vcenter"
```

4. Соедините добавленную точку входа и VRL-трансформацию.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **VMware vCenter** (идентификатор правила: **RV-N-180**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

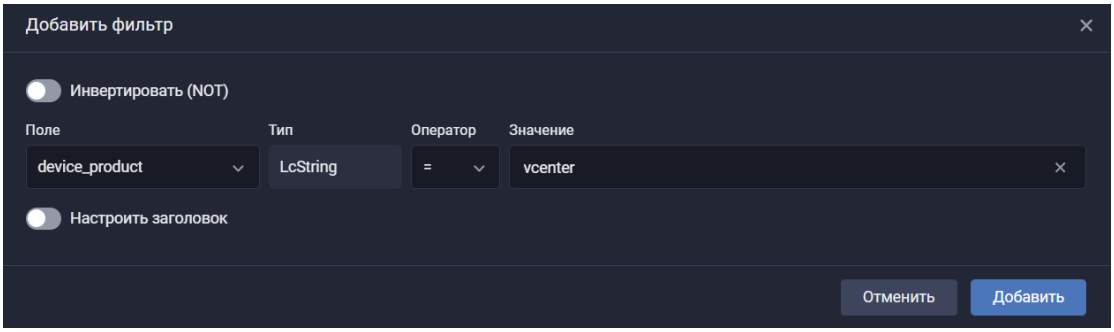
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события vCenter.

Найти события vCenter в хранилище можно по следующему фильтру:

```
device_product = "vcenter"
```



VMware vCenter Server: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1000	Клонирование критичной виртуальной машины	После получения доступа к виртуальной инфраструктуре атакующие могут клонировать одну или несколько виртуальных машин, чтобы получить доступ к конфиденциальным данным, учетным записям пользователей, использовать их для дальнейшего перемещения по сети или закрепления в системе. При срабатывании данного правила необходимо проверить законность действий пользователя — уточнить, были ли они санкционированы. Если легитимность не подтверждается, следует временно заблокировать учетную запись и инициировать внутреннее расследование.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Credential Access (TA0006) • OS Credential Dumping (T1003)
RV-D-1001	Клонирование критичных виртуальных машин	Получив доступ к виртуальной инфраструктуре, атакующие могут клонировать одну или несколько виртуальных машин с целью извлечения конфиденциальной информации, получения учетных данных для последующего горизонтального перемещения по сети или для устойчивого закрепления в инфраструктуре. При срабатывании правила следует установить легитимность выполняемых действий, связаться с ответственным за соответствующую учетную запись, при необходимости временно приостановить ее работу и инициировать внутреннее расследование.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Credential Access (TA0006) • OS Credential Dumping (T1003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1035	Эксплуатация уязвимости CVE-2021-22005 на сервере vCenter	Правило детектирует эксплуатацию уязвимости CVE-2021-22005 на сервере vCenter, уязвимые версии указаны в reference. Уязвимость позволяет неавторизованным пользователям загружать произвольные данные на сервер через обращения по адресам, относящимся к сбору аналитики и телеметрии. Эксплуатацию можно провести с выключенным CEIP (Customer Experience Improvement Program). В случае подтверждения инцидента рекомендуется проверить места возможного размещения web-shell, нелегитимные запланированные задачи cron или другие методы закрепления в системе, обновить уязвимую версию vCenter или принять меры по закрытию доступа к уязвимым адресам.	• Initial Access (TA0001) • Execution (TA0002) • Lateral Movement (TA0008) • Exploit Public-Facing Application (T1190) • Exploitation for Client Execution (T1203) • Exploitation of Remote Services (T1210)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1036	Эксплуатация уязвимости CVE-2021-21972 на сервере vCenter	Правило детектирует эксплуатацию уязвимости CVE-2021-21972 на сервере vCenter, уязвимые версии указаны в reference. Данная уязвимость позволяет загружать неавторизованному пользователю произвольные данные на сервер через POST-запрос на адрес `/ui/vropspluginui/rest/services/uploadova`. Файл будет загружен от пользователя vsphere-ui. Таким образом, можно, например, загрузить свой ключ SSH на сервер vCenter для данного пользователя и подключиться к серверу по ключу. В случае подтверждения инцидента рекомендуется проверить места возможного размещения web-shell, нелегитимные запланированные задачи cron или другие методы закрепления в системе, обновить уязвимую версию vCenter или принять меры по закрытию доступа к уязвимым адресам.	• Initial Access (TA0001) • Execution (TA0002) • Lateral Movement (TA0008) • Command and Control (TA0011) • Application Layer Protocol (T1071) • Web Protocols (T1071.001) • Exploit Public-Facing Application (T1190) • Exploitation for Client Execution (T1203) • Exploitation of Remote Services (T1210)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1037	Доступ к критичным файлам на сервере vCenter	Правило детектирует доступ к критичным файлам на сервере vCenter. Данные действия могут указывать на попытку эксплуатацию уязвимости CVE-2022-22948, уязвимые версии указаны в reference. Уязвимость позволяет получить учетные данные для подключения к хостам ESXi с привилегиями пользователя vpxuser. Также отслеживаются изменения файлов `/var/spool/cron/crontabs/root` и `/etc/rc.local.d/local.sh`, которые были замечены в атаках на ESXi. Внося изменения в первый файл, атакующий может установить скрытые задачи, которые будут выполняться с повышенными правами, что позволяет обеспечить постоянный доступ или выполнение вредоносного кода. Второй файл используют для того, чтобы внедрить команды, автоматически исполняющиеся при загрузке системы, что также способствует сохранению контроля над системой. В случае срабатывания правила рекомендуется проверить, является ли доступ к файлу, содержащему ключ (symkey.dat) для пароля vpxuser или пароль (vcdb.properties) для подключения к базе данных PostgreSQL, легитимным, если нет, то провести внутреннее расследование и временно ограничить доступ к серверам ESXi и vCenter.	• Initial Access (TA0001) • Execution (TA0002) • Persistence (TA0003) • Credential Access (TA0006) • Lateral Movement (TA0008) • Boot or Logon Initialization Scripts (T1037) • RC Scripts (T1037.004) • Scheduled Task/Job (T1053) • Cron (T1053.003) • Valid Accounts (T1078) • Default Accounts (T1078.001) • Brute Force (T1110) • Password Cracking (T1110.002) • Exploit Public-Facing Application (T1190) • Exploitation for Client Execution (T1203)
			Exploitation of

ID правила	Название правила	Описание	Тактики и техники
RV-D-1130	Создание снапшота ВМ в vCenter	Атакующий может создать снапшот или резервную копию данных в облачной учетной записи, чтобы обойти защиту. Снапшот — это копия компонента облачной среды, такого как виртуальная машина (ВМ), виртуальный жесткий диск или том, по состоянию на определенный момент времени. Атакующий может воспользоваться полученными разрешениями, чтобы создать снапшот и обойти ограничения на доступ к существующей вычислительной инфраструктуре. Далее создать облачный экземпляр, смонтировать в нем один или несколько заготовленных снапшотов, а затем применить политику, которая предоставит доступ к экземпляру, например, политику межсетевого экрана, разрешающую входящий и исходящий доступ по SSH.	• Defense Evasion (TA0005) • Modify Cloud Compute Infrastructure (T1578) • Create Snapshot (T1578.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1554	Назначение административных или глобальных прав vCenter	Правило отслеживает события в VMware vCenter, связанные с созданием ролей и назначением прав доступа, включая административные или глобальные привилегии. Атакующий, получив доступ к учетной записи с достаточными правами, может создать новую роль с расширенными привилегиями или назначить себе (или другой учетной записи) высокоуровневые права (например, на уровне `vCenter` или `Datacenter`). Это позволяет закрепиться в инфраструктуре, расширить зону контроля и получить полный доступ к управлению виртуальной инфраструктурой (виртуальные машины, сети, хранилища). Подобные действия являются критичными с точки зрения безопасности и должны подлежать контролю.	• Persistence (TA0003) • Account Manipulation (T1098)

VMware ESXi и VMware vCenter Server: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-985	Вход под привилегированной учетной записью VMware	После получения доступа к привилегированной учетной записи атакующие, используя эту запись, могут зайти на сервер с повышенными правами для проведения дальнейших деструктивных действий. В случае срабатывания правила рекомендуется проверить, является ли хост инициатора входа легитимным (если да, то его можно внести в исключения через активный список privileged_users_and_hosts), в ином случае, в зависимости от возможностей, следует временно ограничить использование учетной записи, сменить пароль, заблокировать доступ с хоста инициатора к серверу.	• Initial Access (TA0001) • Valid Accounts (T1078) • Local Accounts (T1078.003)
RV-D-992	Множественные неуспешные попытки аутентификации пользователя	Для получения доступа к виртуальной инфраструктуре атакующие могут попытаться подобрать пароль к учетной записи. Данное правило фиксирует множественные неудачные попытки входа от имени одного пользователя. Рекомендуется проверить, является ли такая активность легитимной. В случае подтверждения инцидента следует заблокировать адрес, с которого выполнялись попытки аутентификации, и сменить пароль для соответствующей учетной записи. Также рекомендуется ограничить доступ из внешней сети к серверу vCenter. Если попытки входа зафиксированы из внутренней сети организации, необходимо провести внутреннее расследование.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1002	Выгрузка файла с критичной виртуальной машины	После получения доступа к виртуальной инфраструктуре атакующие могут выгрузить данные, хранящиеся в хранилище гипервизора. Это могут быть как отдельные файлы, так и файлы, относящиеся к конкретной виртуальной машине, например, ее память или весь актуальный образ. После этого атакующие получают доступ к данным на машине, в том числе, к учетным данным.	• Credential Access (TA0006) • Collection (TA0009) • OS Credential Dumping (T1003) • Automated Collection (T1119)
RV-D-1003	Выгрузка нескольких файлов с критичной виртуальной машины	После получения доступа к виртуальной инфраструктуре атакующие могут выгрузить данные, хранящиеся в хранилище гипервизора. Это могут быть как отдельные файлы, так и файлы, относящиеся к конкретной виртуальной машине, например, ее память или весь актуальный образ. После этого атакующие получают доступ к данным на машине, в том числе, к учетным данным.	• Credential Access (TA0006) • Collection (TA0009) • OS Credential Dumping (T1003) • Automated Collection (T1119)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1004	Обнаружение атаки Password Spraying	Для получения доступа к виртуальной инфраструктуре атакующие могут попробовать подбирать пароли для разных учетных записей. Данное правило обнаруживает множественные неудачные попытки входа из-под разных пользователей с одного хоста. Рекомендуется проверить, является ли данная активность легитимной или нет. В случае подтверждения инцидента рекомендуется заблокировать адрес, с которого происходят попытки аутентификации и сменить пароль для учетной записи. Также заблокировать доступ из внешней сети к серверу vCenter, если попытки были из внутренней сети организации, то провести внутреннее расследование.	• Credential Access (TA0006) • Brute Force (T1110) • Password Spraying (T1110.003) • Credential Stuffing (T1110.004)
RV-D-1005	Возможно успешный подбор пароля пользователя на VMware	Для получения доступа к виртуальной инфраструктуре атакующие могут попытаться подобрать пароль к учетной записи. Данное правило фиксирует множественные неудачные попытки входа под одним пользователем, за которыми следует успешная аутентификация. Рекомендуется проверить, является ли такая активность легитимной. В случае подтверждения инцидента следует заблокировать адрес, с которого выполнялись попытки аутентификации, и сменить пароль для соответствующей учетной записи. Также рекомендуется ограничить доступ из внешней сети к серверу vCenter. Если попытки входа зафиксированы из внутренней сети организации, необходимо провести внутреннее расследование.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1026	Изменение конфигурации критичной виртуальной машины	После получения доступа к виртуальной инфраструктуре нарушитель может изменить конфигурацию виртуальной машины (параметры памяти, хранилища или сети), чтобы нарушить работоспособность программного обеспечения, или использовать ее вычислительные мощности в своих целях. Правило предназначено для обнаружения изменений конфигурации виртуальной машины из списка critical_vm_cimv2. Для анализа подобного события требуется проверить в интерфейсе vCenter/ESXi измененные параметры, после чего запросить у ответственного за учетную запись пользователя пояснения о причинах внесенных изменений. Если легитимность действий не подтверждается, необходимо инициировать расследование инцидента.	• Command and Control (TA0011) • Impact (TA0040) • Non-Application Layer Protocol (T1095) • Data Destruction (T1485) • Impair Defenses (T1562) • Data Manipulation (T1565) • Runtime Data Manipulation (T1565.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1029	Изменение конфигурации нескольких критичных виртуальных машин	После получения доступа к виртуальной инфраструктуре пользователь может изменить параметры виртуальных машин, например, настройки памяти, хранилища или сети, что может привести к сбоям в работе программного обеспечения или к использованию ресурсов системы в нештатных целях. Правило предназначено для обнаружения событий изменений конфигурации нескольких виртуальных машин из списка critical_vm_cimv2. При выявлении подобного события необходимо через интерфейс vCenter/ESXi проверить, какие параметры были изменены, и запросить у владельца учетной записи объяснение причин внесенных изменений. Если действия не подтверждаются как легитимные, следует инициировать расследование инцидента.	• Command and Control (TA0011) • Impact (TA0040) • Non-Application Layer Protocol (T1095) • Data Destruction (T1485) • Impair Defenses (T1562) • Data Manipulation (T1565) • Runtime Data Manipulation (T1565.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1041	Вызов и выполнение Guest API в гостевой ОС	Правило детектирует использование легитимного VMware Guest Operations API для выполнения операций внутри гостевой ОС. Атакующие могут вызывать такие методы, как запуск программ, передача файлов или получение списка процессов, при наличии доступа к ESXi/vCenter и установленным VMware Tools в виртуальной машине. Подобная активность может указывать на горизонтальное перемещение или скрытное взаимодействие с гостевой системой. При срабатывании правила рекомендуется проверить легитимность действий пользователя, вызвавшего API, а также проанализировать выполняемые команды, передаваемые файлы и связанные с ними процессы внутри гостевой ОС. Если легитимность активности подтвердить не удалось, следует сменить пароль пользователя, временно изолировать виртуальную машину и начать расследование.	• Execution (TA0002) • ESXi Administration Command (T1675)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1209	Создание множества виртуальных машин	После получения доступа к виртуальной инфраструктуре атакующие могут инициировать создание нескольких виртуальных машин. Такие действия позволяют массово разворачивать виртуальные экземпляры для дальнейшего перемещения внутри сети, интенсивного потребления серверных ресурсов, а также запускать виртуальные машины на основе шаблонов или образов с целью получения информации или доступа к учетным данным.	• Defense Evasion (TA0005) • Impact (TA0040) • Data Destruction (T1485) • Endpoint Denial of Service (T1499) • OS Exhaustion Flood (T1499.001) • Impair Defenses (T1562) • Hide Artifacts (T1564) • Run Virtual Instance (T1564.006)
RV-D-1219	Отключено несколько критичных виртуальных машин	Получив доступ к виртуальной инфраструктуре, нарушители могут вывести из строя одну или несколько виртуальных машин, на которых размещены средства защиты, с целью обхода механизмов обнаружения, а также системы, обрабатывающие критически важную для организации информацию, что приводит к нарушению стабильной работы инфраструктуры.	• Impact (TA0040) • Data Destruction (T1485) • System Shutdown/Reboot (T1529) • Impair Defenses (T1562)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1225	Удалена критичная виртуальная машина	Получив доступ к виртуальной инфраструктуре, атакующие могут удалить одну или несколько виртуальных машин, например, с целью отключения защитного программного обеспечения или нарушения стабильной работы инфраструктуры.	• Impact (TA0040) • Data Destruction (T1485)
RV-D-1226	Удалено несколько критичных виртуальных машин	В случае компрометации виртуальной инфраструктуры атакующие могут удалить одну или несколько виртуальных машин, что может быть использовано для отключения средств защиты или нарушения функционирования инфраструктуры.	• Impact (TA0040) • Data Destruction (T1485)
RV-D-1270	Отключена критичная виртуальная машина	После получения доступа к виртуальной инфраструктуре атакующие могут отключить одну или несколько виртуальных машин, на которых установлено защитное ПО, для дальнейшего обхода обнаружения, или машины, на которых обрабатывается критичная для организации информация, для нарушения работоспособности инфраструктуры.	• Impact (TA0040) • Data Destruction (T1485) • System Shutdown/Reboot (T1529) • Impair Defenses (T1562)

Системы динамической адресации

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых систем динамической адресации:

- BIND DNS
- Microsoft DNS Server
- Microsoft DHCP Server

BIND DNS

- BIND DNS: настройка источника

BIND DNS: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий BIND DNS в R-Vision SIEM.

Предварительные требования

Перед настройкой пересылки событий в R-Vision SIEM убедитесь в выполнении следующих условий:

- Сетевая связность между сервером BIND DNS и SIEM (или промежуточным узлом) обеспечена, а необходимые порты открыты.

Настройка BIND DNS

Настройка журналирования BIND DNS

Для настройки журналирования BIND DNS выполните следующие действия:

1. Добавьте в файл `named.conf` следующую конфигурацию логирования:



Файл конфигурации `named.conf` в разных ОС может находиться либо в `/etc/`, либо в `/etc/bind/`.

```
logging {
        channel anomalies_log {
                file "/var/log/named/anomalies.log" versions 5 size 50m;
                severity info;
                print-category yes;
                print-severity yes;
                print-time yes;
        };
        channel security_log {
                file "/var/log/named/security.log" versions 3 size 5m;
                severity info;
                print-category yes;
                print-severity yes;
```

```
                print-time yes;
        };
        channel query_log {
                file "/var/log/named/query.log" versions 600 size 20m;
                print-time yes;
                print-category yes;
                print-severity yes;
                severity info;
        };

        // categories binginds
        category queries { query_log; };

        category resolver { anomalies_log; };
        category dnssec { anomalies_log; };
        category lame-servers { anomalies_log; };
        category network { anomalies_log; };
        category rate-limit { anomalies_log; };

        category xfer-in { security_log; };
        category xfer-out { security_log; };
        category security { security_log; };
        category client  { security_log; };
        category update-security  { security_log; };

};
```

2. Перезапустите сервис named с помощью команды:

```
sudo systemctl restart named.service
```

Журналирование BIND DNS настроено.

Настройка отправки событий в R-Vision SIEM

В настоящем руководстве рассматривается передача событий с помощью службы syslog.

rsyslog

Предполагается, что `rsyslog` на станции с ОС Linux уже установлен и модуль `imfile` подгружен в `/etc/rsyslog.conf`. Для настройки передачи событий из файлов BIND DNS выполните следующие действия:

1. Создайте файл `/etc/rsyslog.d/99-binddns-siem.conf` со следующим содержимым:

```
input(type="imfile"
      File="/var/log/named/security.log"
      Tag="bind-security"
      Severity="info"
```

```
      Facility="local7"
)

input(type="imfile"
      File="/var/log/named/anomalies.log"
      Tag="bind-anomalies"
      Severity="info"
      Facility="local7"
)

input(type="imfile"
      File="/var/log/named/query.log"
      Tag="bind-queries"
      Severity="info"
      Facility="local7"
)

if $syslogtag contains 'bind' then {
  action(type="omfwd" Target="<target>" Port="<port>" Protocol="udp")
}
```

Здесь:

- `<target>` — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- `<port>` — порт точки входа Syslog на конвейере SIEM.

2. Перезапустите сервис `rsyslog` с помощью команды:

```
sudo systemctl restart rsyslog
```

Отправка событий BIND DNS настроена.

syslog-ng

Предполагается, что `syslog-ng` на станции с ОС Linux уже установлен. Для настройки передачи событий из файлов BIND DNS выполните следующие действия:

1. Создайте файл `/etc/syslog-ng/conf.d/binddns-siem.conf` со следующим содержимым:

```
source binddns {
        file("/var/log/named/anomalies.log" flags(no-parse)
log_prefix("bind-anomalies: "));
        file("/var/log/named/security.log" flags(no-parse) log_prefix("bind-
security: "));
        file("/var/log/named/query.log" flags(no-parse) log_prefix("bind-
queries: "));
};

destination siem {
        udp("<target>" port(<port>)); # указать IP и порт точки входа SIEM
```

```
};

log {
        source(binddns); destination(siem);
};
```

Здесь:

- `<target>` — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- `<port>` — порт точки входа Syslog на конвейере SIEM.

2. Перезапустите сервис `syslog-ng` с помощью команды:

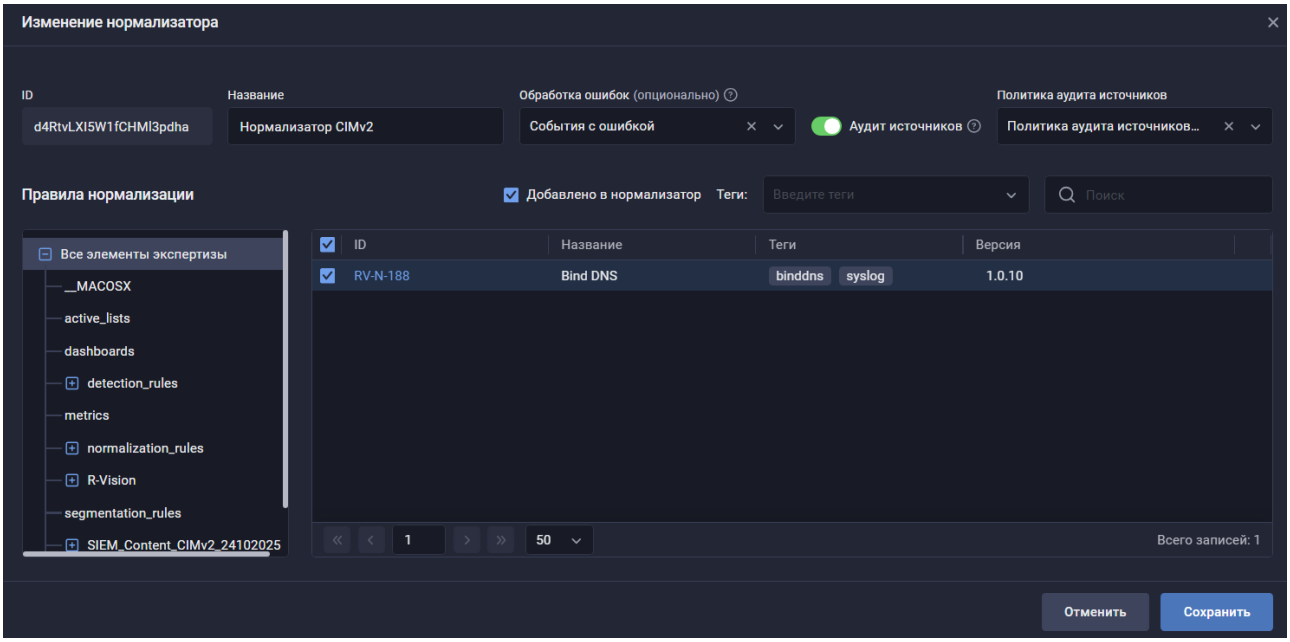
```
sudo systemctl restart syslog-ng
```

Отправка событий BIND DNS настроена.

Настройка в R-Vision SIEM

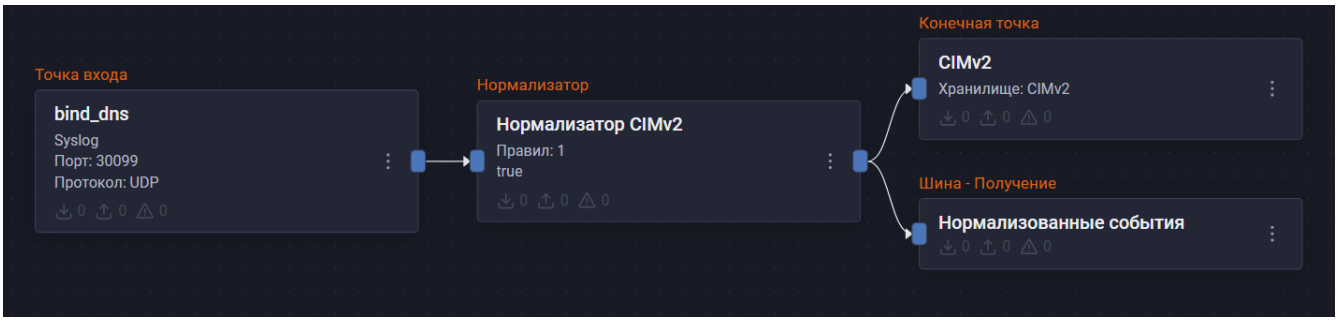
Для настройки сбора и нормализации событий BIND DNS в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне источника.
   - Протокол: выберите вариант в соответствии с настройками на стороне источника.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **BIND DNS** (идентификатор правила: **RV-N-188**).



4. Соедините точку входа с нормализатором.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. При необходимости добавьте на конвейер элемент **Шина**, настроенный на получение. Он используется для проброса событий между конвейерами.
7. Соедините конечную точку и шину с нормализатором.
8. Сохраните и установите конфигурацию конвейера.

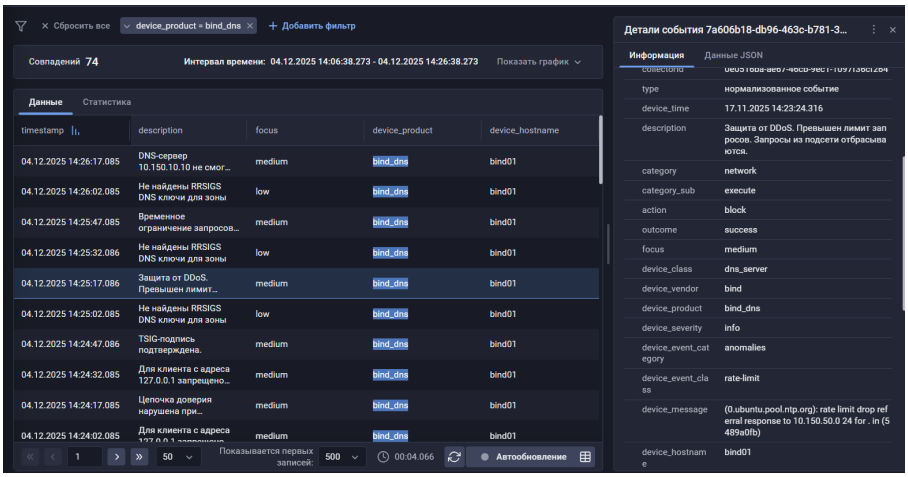
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события BIND DNS.

Найти события BIND DNS в хранилище можно по следующему фильтру:

```
device_product = "bind_dns"
```



BIND DNS: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1309	Подозрительные DNS-запросы к домену trycloudflare.com	Cloudflare Tunnel — это решение, изначально предназначенное для безопасной публикации внутренних ресурсов через инфраструктуру Cloudflare. Однако из-за своей гибкости и простоты запуска он стал популярным и среди атакующих. Особый интерес вызывает возможность создания туннеля без регистрации с использованием временного домена trycloudflare.com. Данное правило выявляет подозрительные DNS-запросы к этому домену. Такие действия могут быть связаны с атакующими, стремящимися установить скрытый доступ к сети или маскировать свою активность через прокси-серверы.	• Resource Development (TA0042) • Command and Control (TA0011) • Proxy (T1090) • Protocol Tunneling (T1572) • Acquire Infrastructure (T1583) • Web Services (T1583.006)
RV-D-1385	DNS-запрос к домену localtonet	Данное правило выявляет подозрительные DNS-запросы к домену localtonet, которые могут указывать на использование утилиты для туннелирования трафика или другие попытки обхода защитных механизмов. Такие действия могут быть связаны с атакующими, стремящимися установить скрытый доступ к сети или маскировать свою активность через прокси-серверы.	• Command and Control (TA0011) • Protocol Tunneling (T1572)
RV-D-1386	Передача зоны DNS на недоверенный узел (AXFR)	AXFR Zone Transfer — это метод передачи всей зоны DNS (репликация зоны) между серверами, который может быть использован атакующими для получения полного содержимого зоны на этапе разведки и сбора информации. Данное правило отслеживает запросы типа AXFR к зонам и определяет их отправку на недоверенные хосты.	• Reconnaissance (TA0043) • Gather Victim Network Information (T1590) • DNS (T1590.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1387	DNS-запрос к подозрительным внешним службам	Данное правило выявляет подозрительные DNS-запросы к доменам внешних служб, которые часто используются популярными сканерами уязвимостей и платформами для тестирования безопасности веб-приложений. Такие инструменты могут применяться атакующими на начальной стадии атаки для сбора разведывательной информации.	• Reconnaissance (TA0043) • Initial Access (TA0001) • Exploit Public-Facing Application (T1190) • Active Scanning (T1595) • Vulnerability Scanning (T1595.002)
RV-D-1388	Обнаружен DNS-запрос к пулам Monero	Это правило обнаруживает подозрительные DNS-запросы к доменам, связанным с известными пулами майнинга Monero, что может указывать на вредоносную деятельность, такую как майнинг криптовалюты с использованием скомпрометированных хостов. После срабатывания правила важно определить, какой клиент инициировал DNS-запрос. Если активность подозрительна, необходимо заблокировать доступ к этим доменам и провести тщательный анализ хоста на предмет потенциальных компрометаций или программного обеспечения для майнинга.	• Impact (TA0040) • Resource Hijacking (T1496) • Compute Hijacking (T1496.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1392	Использование DNS-туннеля	DNS Tunneling — это метод кодирования передаваемой информации в DNS запросах. Данный метод может использоваться атакующими для обхода правил межсетевого экранирования и эксфильтрации данных. Правило отслеживает уникальные запросы для одного домена (значения после первой точки). При достижении заданного порога генерируются корреляционные события. Данное правило направлено на выявление DNS-запросов, содержащих base64-закодированные строки.	• Command and Control (TA0011) • Exfiltration (TA0010) • Exfiltration Over Alternative Protocol (T1048) • Exfiltration Over Unencrypted Non-C2 Protocol (T1048.003) • Application Layer Protocol (T1071) • DNS (T1071.004) • Data Encoding (T1132) • Standard Encoding (T1132.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1393	DNS-запрос к ресурсам Telegram API	Данное правило выявляет подозрительные DNS-запросы к домену api.telegram.org, которые могут использоваться ботами Telegram для передачи данных или выполнения управляющих команд. Такие действия потенциально могут быть связаны с обходом защитных механизмов и скрытой вредоносной активностью.	• Command and Control (TA0011) • Exfiltration (TA0010) • Exfiltration Over Alternative Protocol (T1048) • Exfiltration Over Unencrypted Non-C2 Protocol (T1048.003) • Application Layer Protocol (T1071) • DNS (T1071.004) • Web Service (T1102) • Bidirectional Communication (T1102.002)
RV-D-1394	Обнаружен DNS-запрос к Killswitch-домену WannaCry	KillSwitch — это механизм экстренной остановки ВПО, встроенный разработчиками, который позволяет отключить или прекратить распространение вредоносной программы. В случае WannaCry, KillSwitch был реализован через проверку доступности определённого домена. Данное правило предназначено для выявления DNS-запросов к KillSwitch-доменам, связанным с WannaCry. Данное поведение может указывать на компрометацию хоста и заражение вредоносным ПО.	• Execution (TA0002) • User Execution (T1204) • Malicious File (T1204.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1395	Множественные DNS-запросы с одного устройства	Множественные запросы к одному ресурсу с одного/различных хостов могут указывать на активность вредоносного ПО, устанавливающего связь с C2-серверами атакующего. Так атакующие могут взаимодействовать, используя протокол уровня приложений системы доменных имен (DNS), чтобы избежать обнаружения/сетевой фильтрации, смешиваясь с существующим трафиком.	• Command and Control (TA0011) • Exfiltration (TA0010) • Exfiltration Over Alternative Protocol (T1048) • Exfiltration Over Unencrypted Non-C2 Protocol (T1048.003) • Application Layer Protocol (T1071) • DNS (T1071.004)

Microsoft DNS Server

- Microsoft DNS Server: настройка источника
- Microsoft DNS Server: правила корреляции

Microsoft DNS Server: настройка источника

Данное руководство описывает процесс настройки сбора событий Microsoft DNS Server и их отправки в R-Vision SIEM.

Настройка Microsoft DNS Server

Настройка журналирования



В настоящем руководстве рассматривается передача событий с помощью агента платформы R-Vision EVO. Для пересылки событий в R-Vision SIEM установите на узле агент R-Vision EVO.

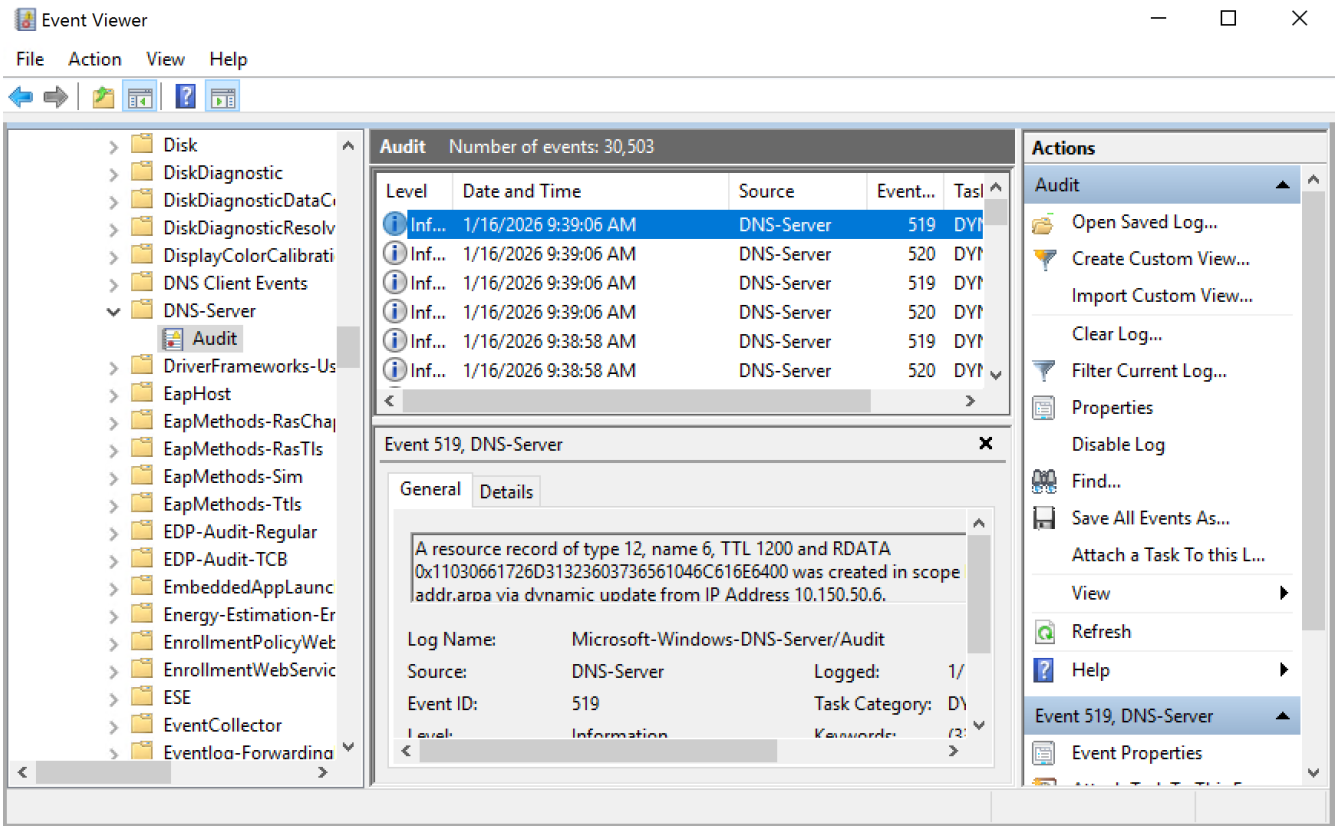
Журнал Audit

Журнал **Microsoft-Windows-DNSServer/Audit** включен по умолчанию. Дополнительная настройка не требуется.

Выполните следующие шаги, чтобы проверить наличие событий:

1. Перейдите в раздел **Event Viewer**.
2. Нажмите сочетание клавиш WIN+R.
3. Введите значение `eventvwr.msc`.
4. Нажмите ENTER.
5. Перейдите в раздел **Приложения и службы → Журналы → Microsoft → Windows → DNS-Server**.

В разделе **DNS-Server** находится несколько журналов, включая **Audit** и **Analytical**. События в журнале **Audit** регистрируют изменения конфигурации сервера, зон или записей ресурсов. По ним можно определить, кем и когда были внесены изменения.

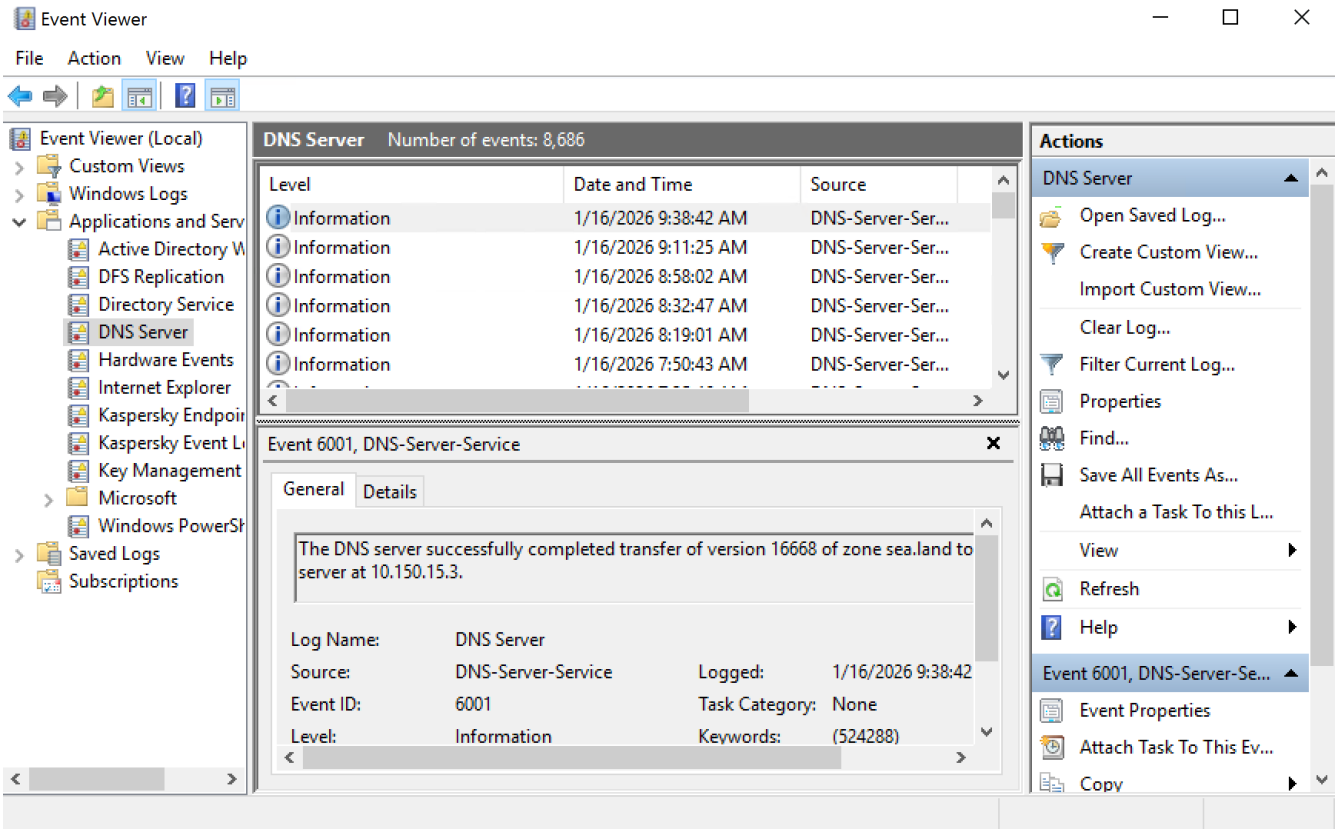


Журнал DNS Server

Журнал **DNS Server** включен по умолчанию. Дополнительная настройка не требуется.

Данный журнал регистрирует события общей работоспособности и основных операций службы DNS:

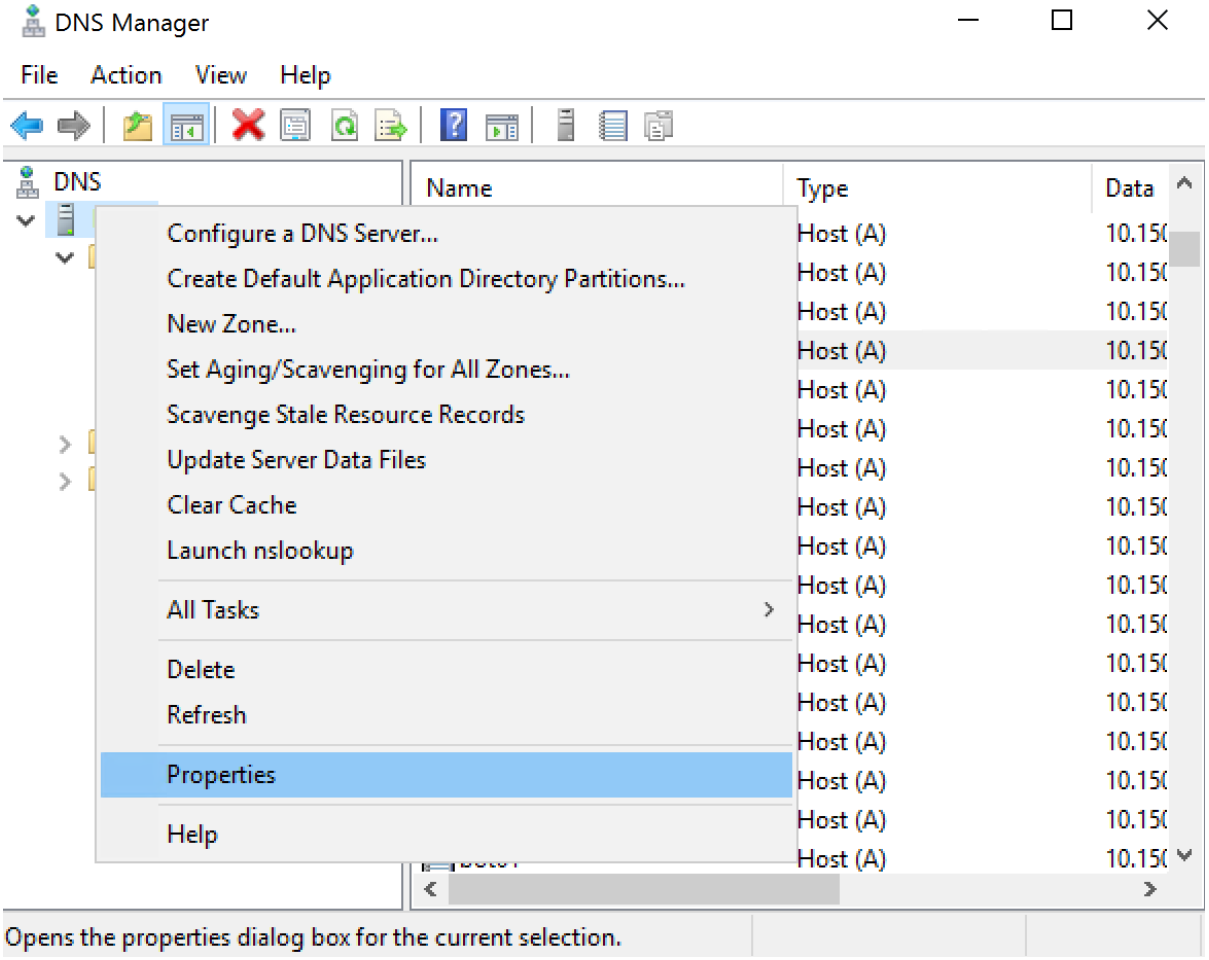
1. **Запуск и остановка службы** — сообщения о том, когда служба DNS-сервера была запущена или остановлена.
2. **Ошибки и предупреждения** — критические системные события, такие как невозможность открытия сокета на определенном IP-адресе (Event ID 408), проблемы с загрузкой зон, ошибки репликации Active Directory (если DNS интегрирован с AD).
3. **Основные операции** — уведомления об успешных динамических обновлениях записей (dynamic updates), изменениях зоны или операциях DNSSEC.



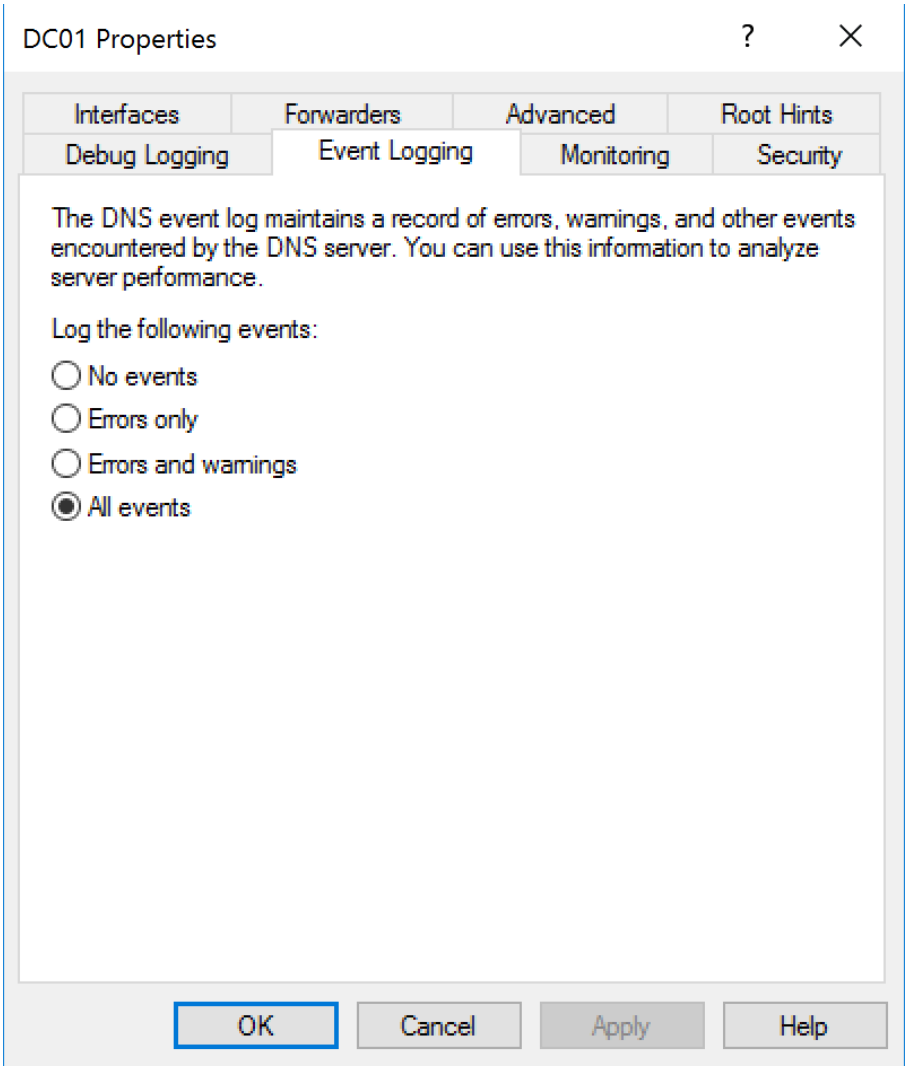
Настройка уровня логирования

Вы можете указать необходимый уровень логирования DNS-сервера, для этого:

1. Откройте оснастку **DNS Manager**.
2. В контекстном меню требуемого DNS-сервера выберите пункт **Properties**.



3. В появившемся окне перейдите на вкладку **Event Logging** и выберите необходимый уровень логирования.



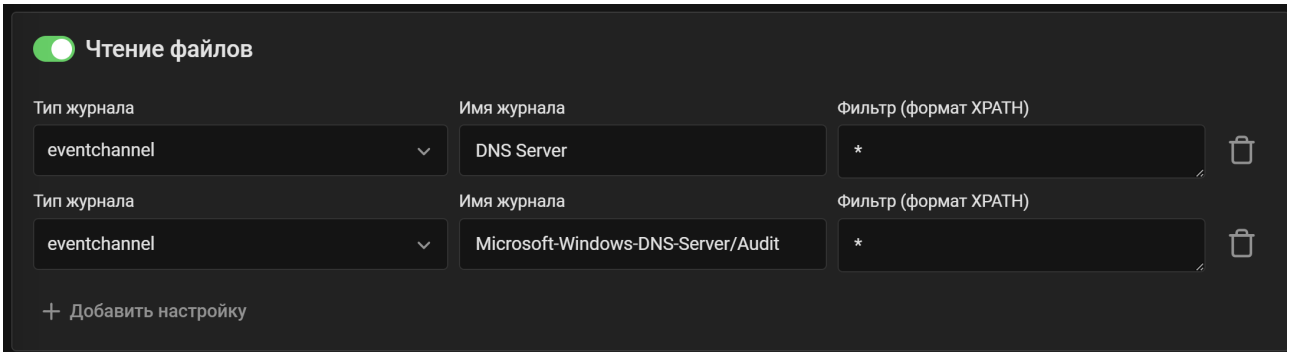
4. Нажмите на кнопку **OK**.

Настройка в R-Vision SIEM

Настройка отправки событий в R-Vision SIEM

Для отправки событий источника в R-Vision SIEM выполните следующие шаги:

1. В веб-интерфейсе R-Vision SIEM перейдите в раздел **Агенты** → **Группы агентов**.
2. Создайте группу и добавьте в нее узел, на котором установлен агент.
3. В созданной группе узлов в секции **Чтение файлов** нажмите на кнопку **Добавить настройку** (＋).
4. В выпадающем списке **Тип журнала** выберите вариант **eventchannel**.
5. В поле **Имя журнала** введите значение `DNS Server`.
6. Если необходимо выбирать события по определенным критериям, введите в поле **Фильтр (формат XPATH)** выражение XPath. Если фильтр не нужен, введите символ `*`.
7. Добавьте второй журнал с названием `Microsoft-Windows-DNS-Server/Audit` и аналогичными настройками.



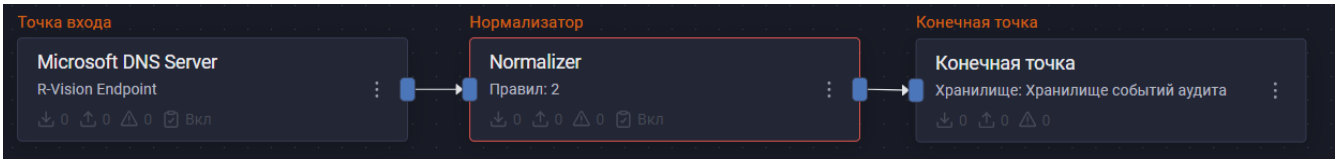
8. Нажмите на кнопку **Сохранить и применить**.
9. Дождитесь применения политики группы на узле. Сбор событий настроен.

Настройка обработки событий в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **R-Vision Endpoint**.
   - Домен: введите значение в формате `gw-<your_gateway_id>`, где `<your_gateway_id>` — ID шлюза.
3. Добавьте на конвейер элемент **Нормализатор** с правилами **Microsoft DNS Audit** (идентификатор правила: **RV-N-249**) и **Microsoft DNS Server Service** (идентификатор правила: **RV-N-251**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

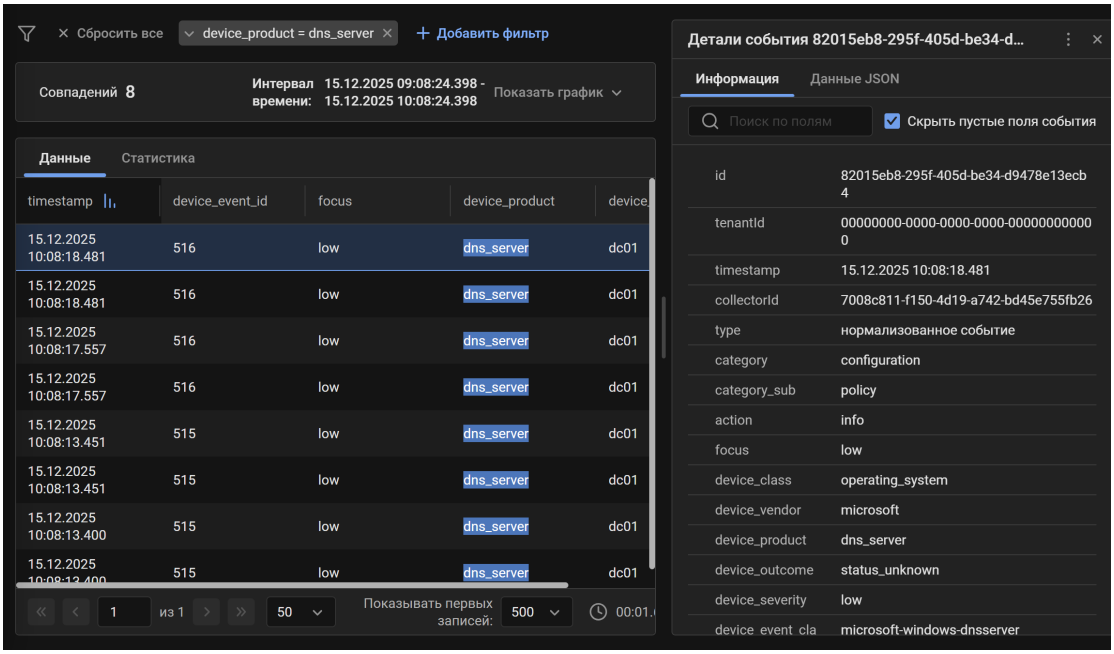


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Microsoft DNS Server.



Найти события Microsoft DNS Server в хранилище можно по следующему фильтру:

```
device_product = "dns_server"
```



Microsoft DNS Server: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1413	Несанкционированное изменение конфигурации DNS-сервера	Правило позволяет обнаружить несанкционированные изменения конфигурации Windows DNS Server, которые могут привести к деградации или недоступности сервиса. Отслеживаются действия с зонами DNS (удаление, изменение параметров), DNS-переадресаторами (серверами пересылки запросов), root hints и DNSSEC-ключами/подписями. Фиксируются соответствующие события аудита в журнале Microsoft-Windows-DNSServer/Audit (EventID 513, 514, 537, 540, 525, 569 и др.), что позволяет своевременно выявлять попытки вмешательства в работу службы DNS.	• Impact (TA0040) • Data Manipulation (T1565) • Stored Data Manipulation (T1565.001) • Compromise Infrastructure (T1584) • DNS Server (T1584.002)

Microsoft DHCP Server

- Microsoft DHCP Server: настройка источника

Microsoft DHCP Server: настройка источника

Данное руководство описывает процесс настройки сбора событий Microsoft DHCP Server и их отправки в R-Vision SIEM.

Настройка Microsoft DHCP Server

Настройка журналирования



В настоящем руководстве рассматривается передача событий с помощью агента платформы R-Vision EVO. Для пересылки событий в R-Vision SIEM установите на узле агент R-Vision EVO.

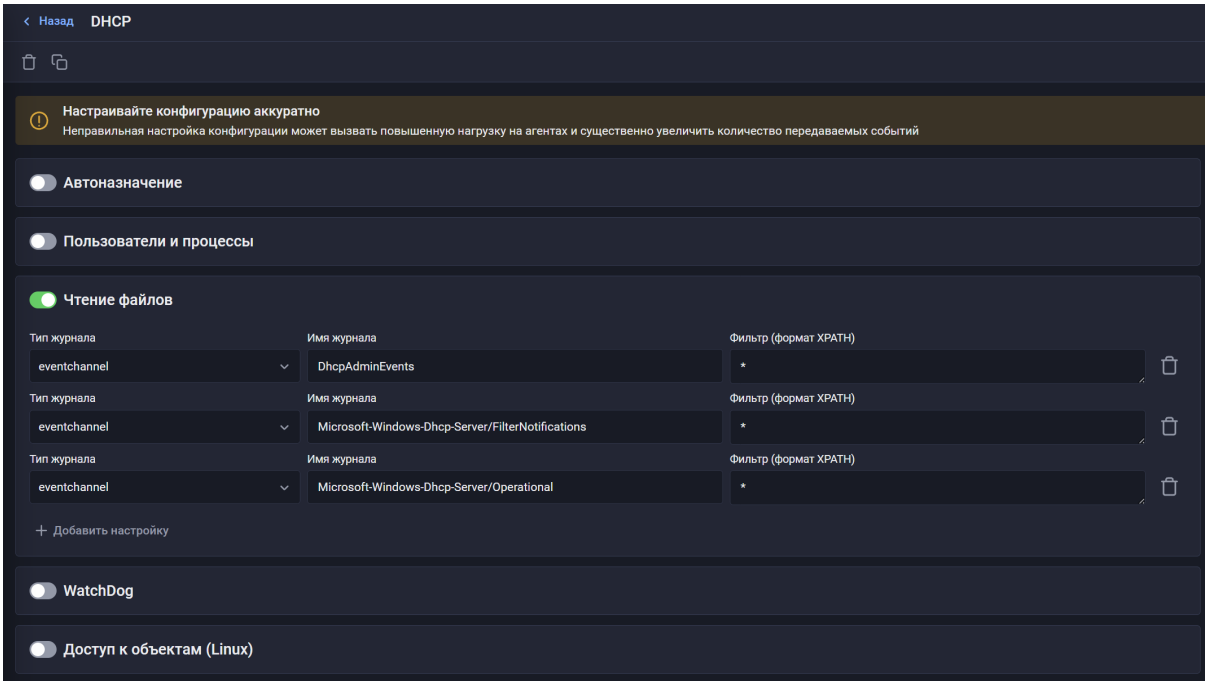
События источника сохраняются в журналах `DhcpAdminEvents`, `Microsoft-Windows-Dhcp-Server/Operational`, `Microsoft-Windows-Dhcp-Server/FilterNotifications`.

Настройка в R-Vision SIEM

Настройка отправки событий в R-Vision SIEM

Для отправки событий источника в R-Vision SIEM выполните следующие шаги:

1. В веб-интерфейсе R-Vision SIEM перейдите в раздел **Агенты** → **Группы агентов**.
2. Создайте группу и добавьте в нее узел, на котором установлен агент.
3. В созданной группе узлов в секции **Чтение файлов** нажмите на кнопку **Добавить настройку** (+).
4. В выпадающем списке **Тип журнала** выберите вариант **eventchannel**.
5. В поле **Имя журнала** введите значение `DhcpAdminEvents`.
6. Если необходимо выбирать события по определенным критериям, введите в поле **Фильтр (формат XPATH)** выражение XPath. Если фильтр не нужен, введите символ `*`.
7. Аналогичным образом добавьте журналы `Microsoft-Windows-Dhcp-Server/Operational` и `Microsoft-Windows-Dhcp-Server/FilterNotifications`.



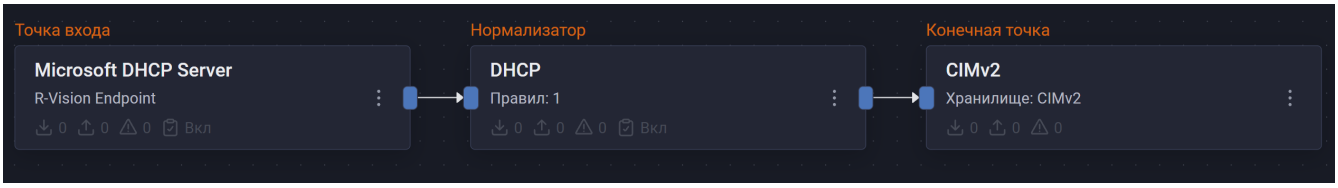
8. Нажмите на кнопку **Сохранить и применить**.
9. Дождитесь применения политики группы на узле. Сбор событий настроен.

Настройка обработки событий в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **R-Vision Endpoint**.
   - Домен: введите значение в формате `gw-<your_gateway_id>`, где `<your_gateway_id>` — ID шлюза.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Microsoft DHCP-Server** (идентификатор правила: **RV-N-245**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

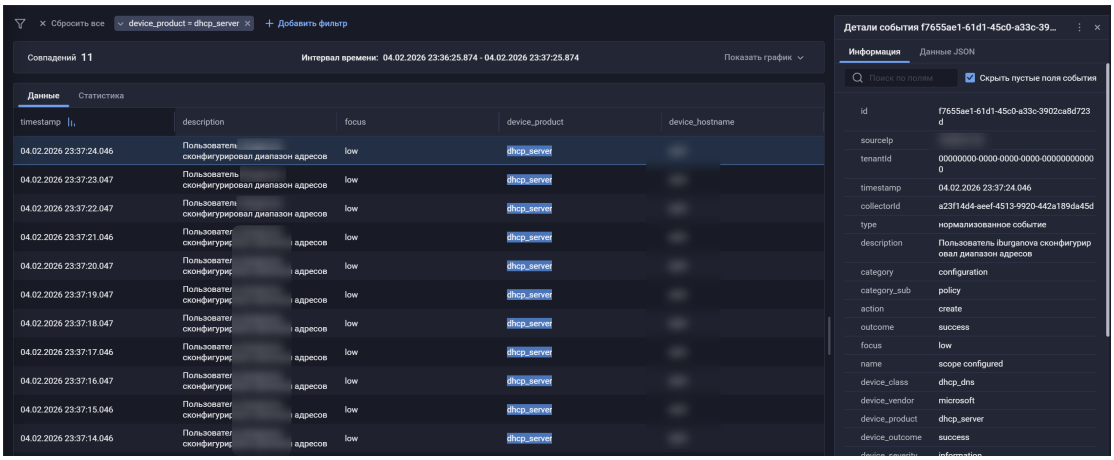


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут

поступать события Microsoft DHCP Server.

Найти события Microsoft DHCP Server в хранилище можно по следующему фильтру:

```
device_product = "dhcp_server"
```



Системы защиты веб-приложений (WAF)

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых систем защиты веб-приложений:

- PT Application Firewall 3
- PT Application Firewall 4
- Гарда WAF

PT Application Firewall 3

- PT Application Firewall 3: настройка источника

PT Application Firewall 3: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Positive Technologies Application Firewall 3 (PT AF 3) в R-Vision SIEM.

Настройка PT AF 3



Для источника PT AF 3 на конвейере коллектора R-SIEM **необходимо** создать отдельную точку входа с выделенным портом, в которую будут поступать только события от PT AF 3. При попадании в эту же точку входа событий от других источников работа правил нормализации будет некорректной, а ожидаемый результат на выходе непредсказуемым.

Настройка отправки событий делится на два этапа:

1. Настройка системных сообщений.
2. Настройка прикладных событий веб-приложений.

Включение логирования системных и прикладных событий WAF

Для включения логирования системных и прикладных событий в консоли WSC выполните команды:

```
syslog set uri @@<target>:<port>
syslog set criticality error
syslog set send enabled
config commit
```

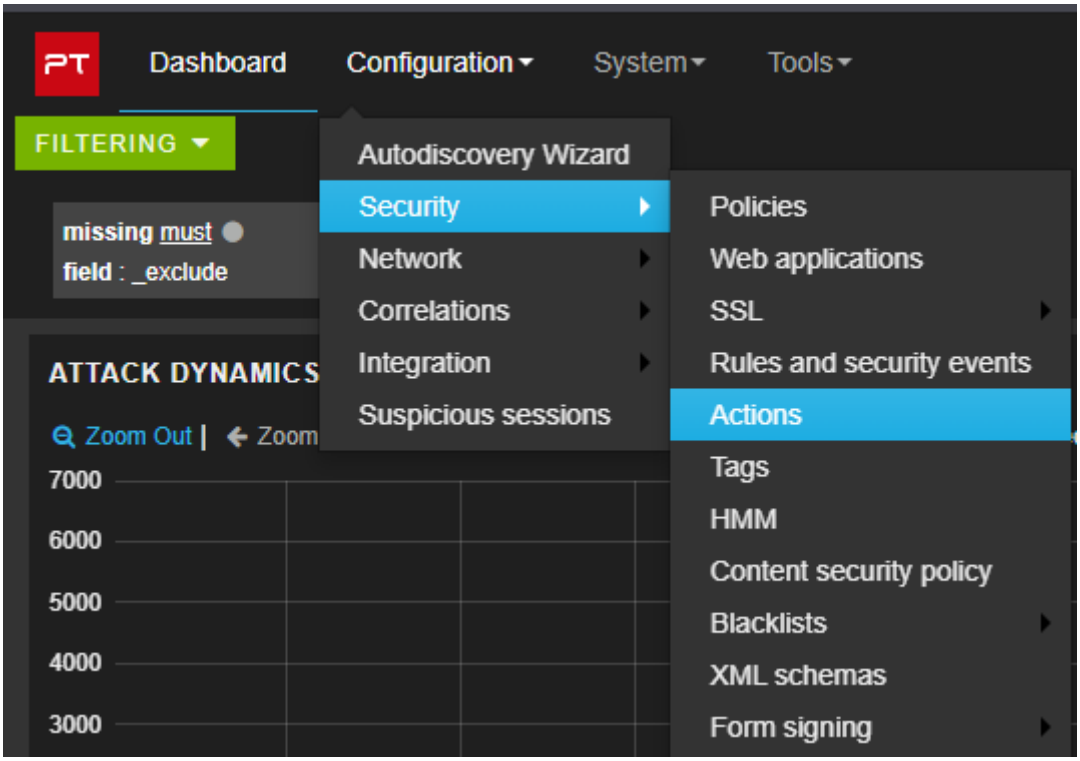
Здесь:

- `@@` — указатель на протокол TCP.
- `<target>` — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- `<port>` — порт точки входа Syslog на конвейере SIEM.

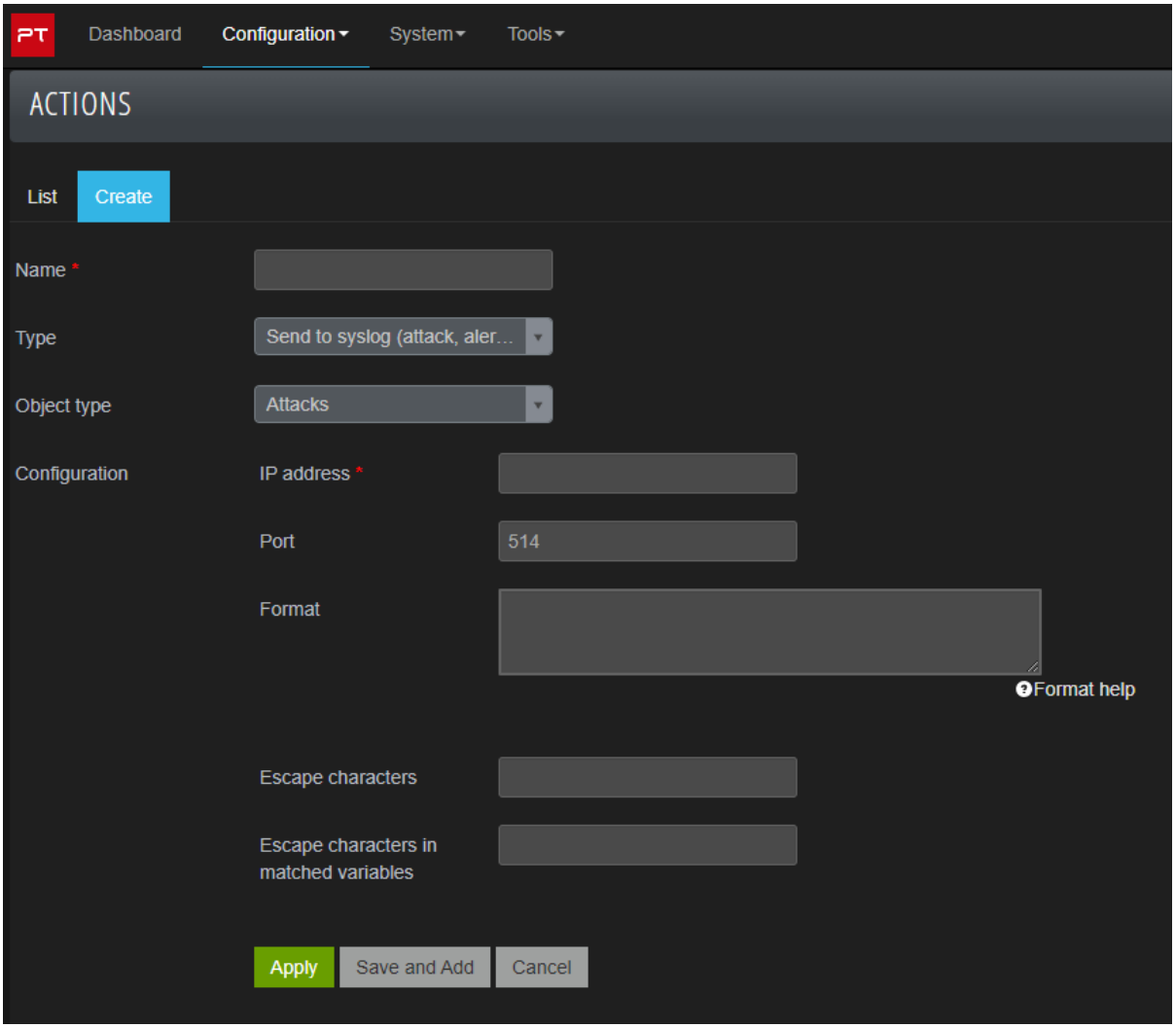
Включение логирования событий веб-приложений

На панели управления сервера PT AF 3 выполните следующие действия:

1. Перейдите в раздел **Configuration** → **Security** → **Actions**:



2. В разделе **Actions** нажмите на кнопку **Create**:



3. Создайте 3 действия:

   a. Действие **Attacks** со следующими параметрами:

      - Name: введите значение `Send attack to syslog`.
      - Type: выберите вариант **Send to syslog (attack, alert, vulnerability)**.
      - Object type: выберите вариант **Attacks**.
      - IP address: введите IP-адрес syslog-сервера.
      - Port: укажите порт syslog-сервера.
      - Format — введите строку:

```
-- Attack -- %EVENT_ID -- %EVENT_SEVERITY -- %EVENT_DESCRIPTION --
%POLICY_NAME -- %REQUEST_HOST -- %REQUEST_PATH -- %MATCHED.VALIDATOR --
%MATCHED.VARIABLE -- %MATCHED.VALUE -- %REQUEST_QUERY
```

   Остальные параметры оставьте без изменений и нажмите на кнопку **Apply**.

   b. Действие **Alerts** со следующими параметрами:

      - Name: введите значение `Send alert to syslog`.

- Type: выберите вариант **Send to syslog (attack, alert, vulnerability)**.
- Object type: выберите вариант **Alerts**.
- IP address: введите IP-адрес syslog-сервера.
- Port: укажите порт syslog-сервера.
- Format — введите строку:

```
-- Alert -- %ALERT_SEVERITY -- %ALERT_NAME -- %ALERT_DESCRIPTION
```

Остальные параметры оставьте без изменений и нажмите на кнопку **Apply**.

c. Действие **Vulnerability** со следующими параметрами:

- Name: введите значение `Send vulnerability to syslog`.
- Type: выберите вариант **Send to syslog (attack, alert, vulnerability)**.
- Object type: выберите вариант **Vulnerabilities**.
- IP address: введите IP-адрес syslog-сервера.
- Port: укажите порт syslog-сервера.
- Format — введите строку:

```
-- Vulnerability -- %EVENT_ID -- %EVENT_SEVERITY -- %EVENT_DESCRIPTION --
%POLICY_NAME -- %REQUEST_HOST -- %REQUEST_PATH -- %MATCHED.VALIDATOR --
%MATCHED.VARIABLE -- %MATCHED.VALUE
```

Остальные параметры оставьте без изменений и нажмите на кнопку **Apply**.

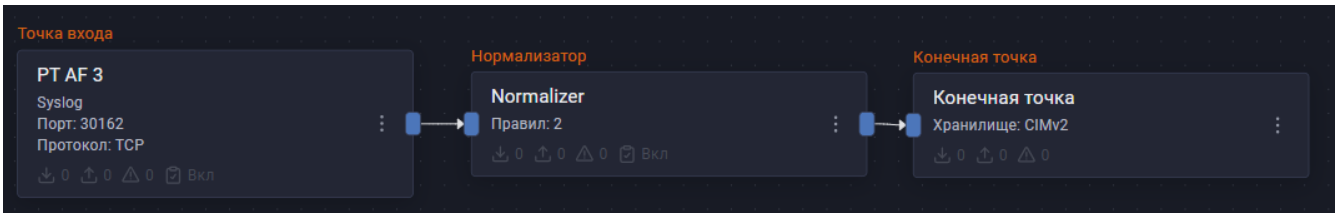
Настройка в R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие действия:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне PT AF 3.
   - Протокол: выберите вариант в соответствии с настройками на стороне PT AF 3.
3. Добавьте на конвейер элемент **Нормализатор** со следующими правилами:
   - **Positive Technologies Application Firewall 3** (идентификатор правила: **RV-N-199**);
   - **Positive Technologies Application Firewall 3** (идентификатор правила: **RV-N-200**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.

7. Сохраните и установите конфигурацию конвейера.

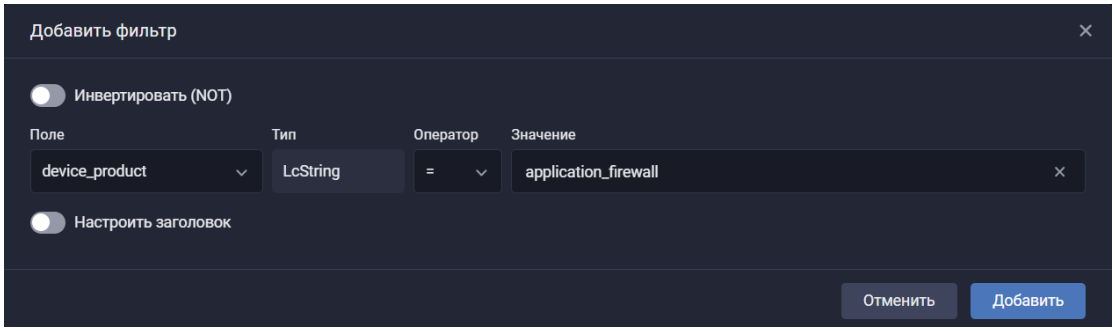
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события PT AF 3.

Найти события PT AF 3 в хранилище можно по следующему фильтру:

```
device_product = "application_firewall"
```



PT Application Firewall 4

- PT Application Firewall 4: настройка источника
- PT Application Firewall 4: правила корреляции

PT Application Firewall 4: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Positive Technologies Application Firewall 4 (PT AF 4) в R-Vision SIEM.

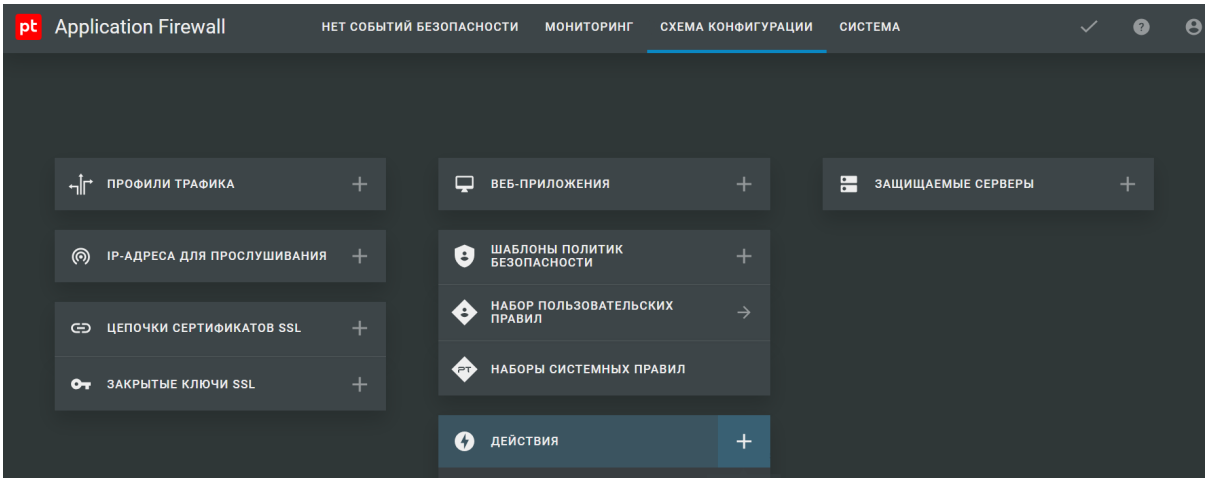
Предварительные требования

- Сетевая доступность сервера PT AF 4 по целевому порту и протоколу до коллектора, который будет принимать события.

Настройка PT Application Firewall 4

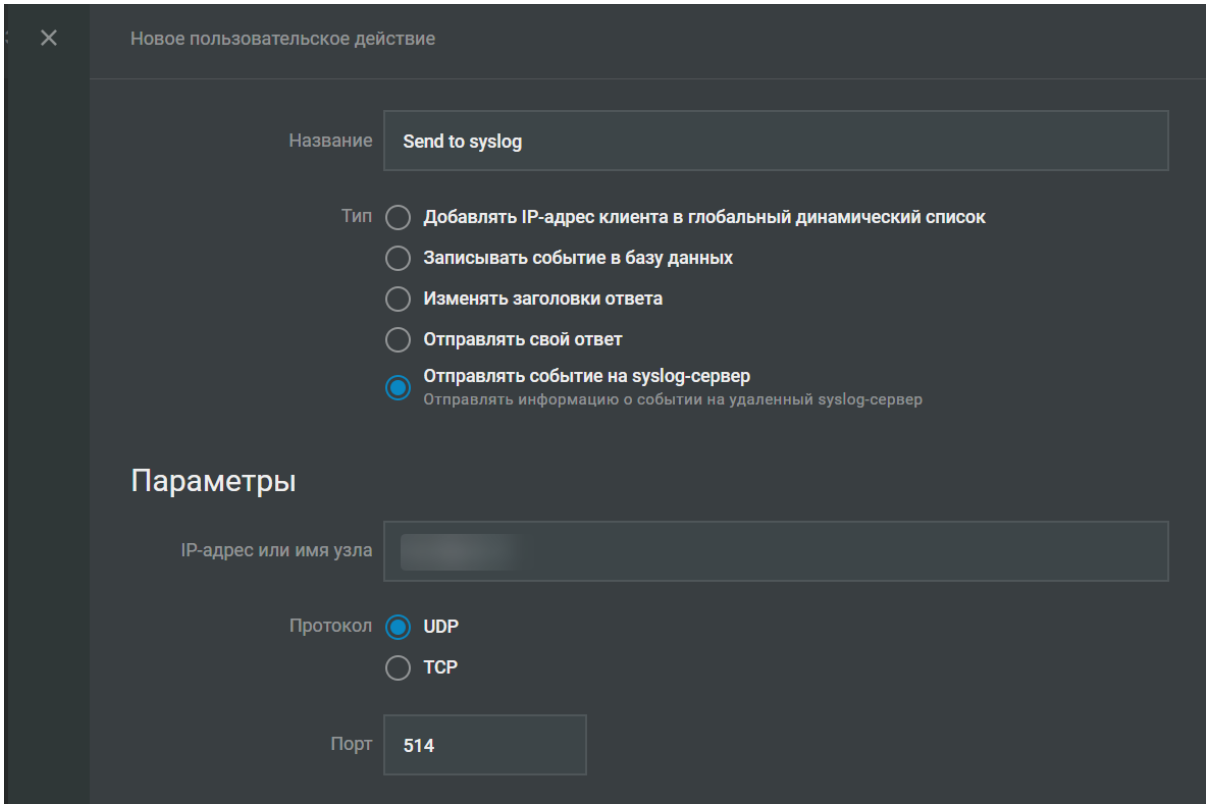
Для настройки отправки событий на панели управления сервера PT AF 4 выполните следующие шаги:

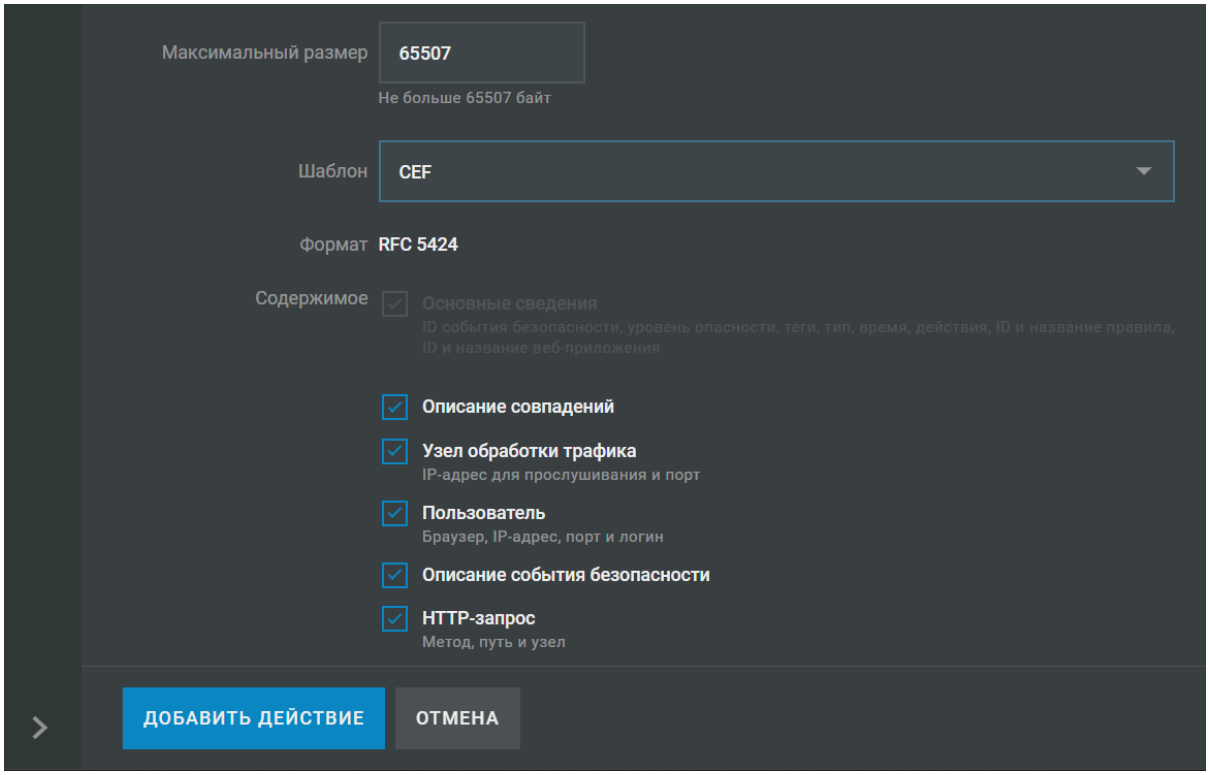
1. В главном меню перейдите на вкладку **Схема конфигурации**.
2. В разделе **Действия** нажмите на кнопку ＋.



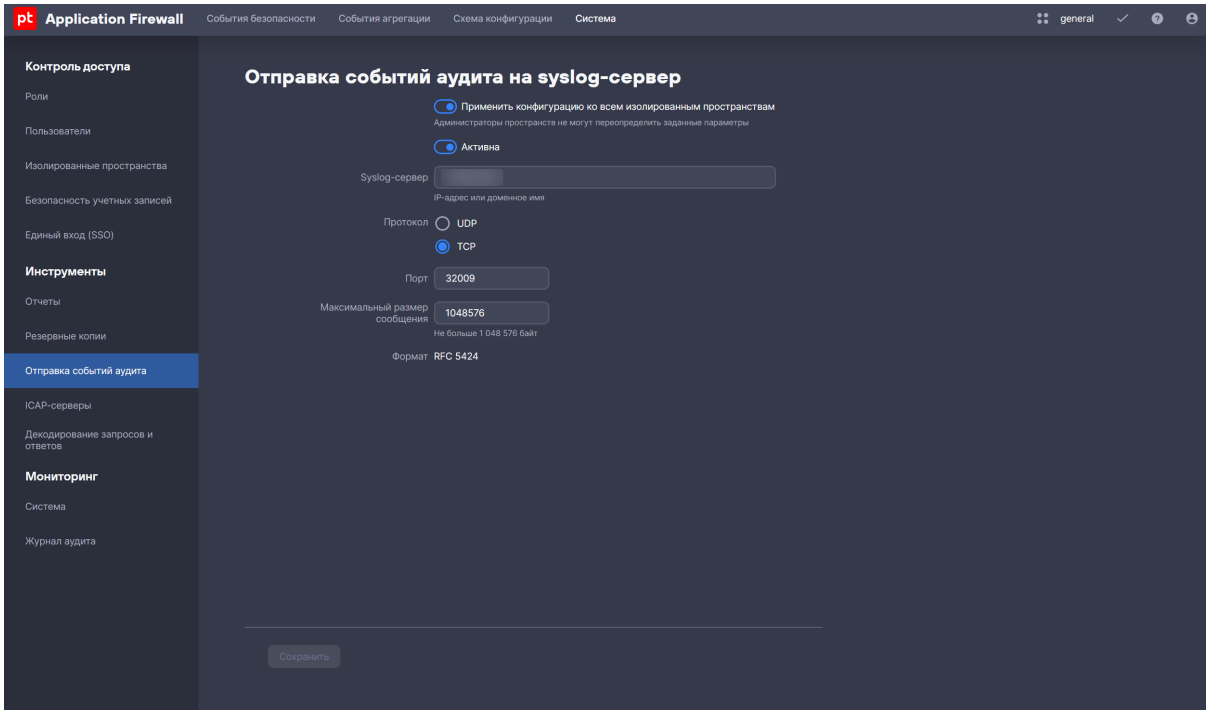
3. Создайте новое действие со следующими параметрами:
   - Название: введите значение `Send to syslog`.
   - Тип: выберите вариант **Отправлять событие на syslog-сервер**.
   - IP-адрес или имя узла: введите IP-адрес сервера `syslog`.
   - Протокол: выберите вариант `TCP` или `UDP`.
   - Порт: введите порт в диапазоне от `30000` до `32767`.
   - Максимальный размер: введите значение `65507`.
   - Шаблон: выберите вариант `CEF`.

   Остальные параметры оставьте без изменений.





4. Нажмите на кнопку **Добавить действие**.
5. После добавления действия перейдите в раздел **Система** → **Отправка событий аудита**.
6. Настройте параметры в соответствии с настройками точки входа конвейера R-Vision SIEM:
   - Применить конфигурацию ко всем изолированным пространствам: включите.
   - Активна: включите.
   - Syslog-сервер: введите IP-адрес коллектора R-Vision SIEM.
   - Протокол: выберите вариант `TCP` или `UDP`.
   - Порт: введите порт в диапазоне от `30000` до `32767`.
   - Максимальный размер сообщения: оставьте значение по умолчанию.



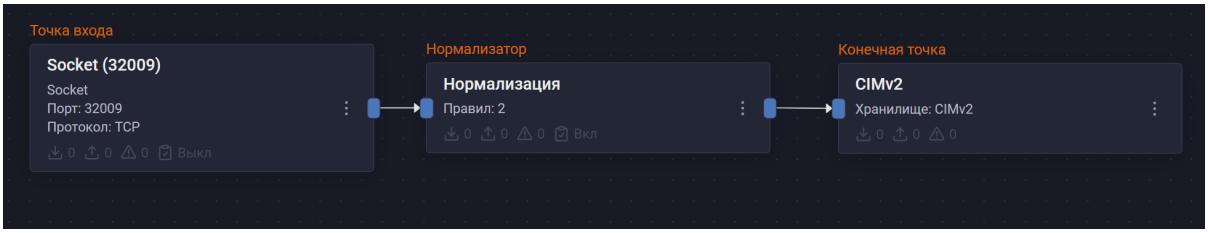
Настройка PT AF 4 завершена.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - **Название**: введите название точки входа.
   - **Тип точки входа**: выберите вариант **Socket**.
   - **Порт точки входа**: введите значение в соответствии с настройками на стороне источника.
   - **Протокол**: выберите вариант в соответствии с настройками на стороне источника.
3. Добавьте на конвейер элемент **Нормализатор** с правилами **Positive Technologies Application Firewall 4** (идентификатор правила: **RV-N-190**) и **Positive Technologies Application Firewall 4 Audit** (идентификатор правила: **RV-N-338**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

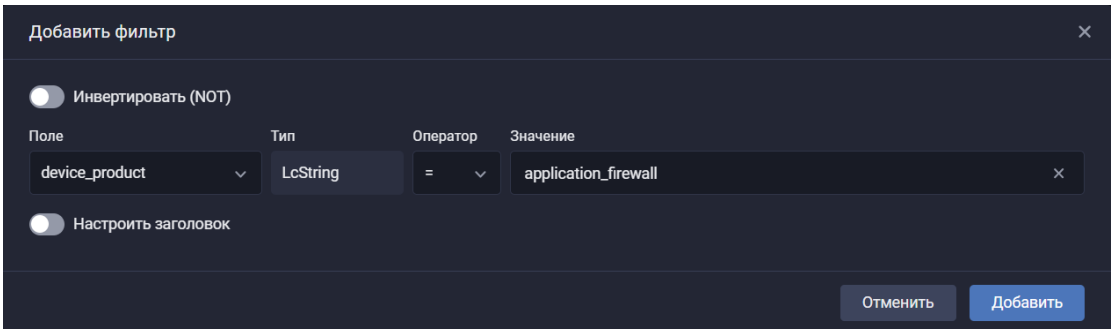
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события PT AF 4.

Найти события PT AF 4 в хранилище можно по следующему фильтру:

```
device_product = "application_firewall"
```



PT Application Firewall 4: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1505	Подбор пароля к форме авторизации	Правило осуществляет регистрацию оповещений на основании событий от Application Firewall компании Positive Technologies (PT AF), сообщающих о неудачных попытках аутентификации в веб-приложении.	• Credential Access (TA0006) • Account Discovery (T1087) • Local Account (T1087.001) • Brute Force (T1110) • Password Guessing (T1110.001) • Password Spraying (T1110.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1511	Множество атак на веб-ресурс	Правило осуществляет регистрацию оповещений на основании нескольких событий от Application Firewall компании Positive Technologies (PT AF), сообщающих о возможных атаках на веб-приложение.	• Initial Access (TA0001) • Execution (TA0002) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Windows Command Shell (T1059.003) • Unix Shell (T1059.004) • Python (T1059.006) • Exploit Public-Facing Application (T1190) • Server Software Component (T1505) • Web Shell (T1505.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1512	Атака на различные веб-ресурсы	Правило детектирует события Application Firewall Positive Technologies (PT AF), указывающие на атаки, направленные на несколько веб-приложений, что может свидетельствовать о массовой эксплуатации или поиске уязвимостей.	• Initial Access (TA0001) • Execution (TA0002) • Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Windows Command Shell (T1059.003) • Unix Shell (T1059.004) • Python (T1059.006) • Exploit Public-Facing Application (T1190) • Server Software Component (T1505) • Web Shell (T1505.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1514	Атака с загрузкой файла	Правило осуществляет регистрацию оповещений на основании событий от Application Firewall компании Positive Technologies (PT AF), сообщающих о возможной атаке File Upload при помощи защищаемого веб-приложения. Данный тип атаки направлен на последующее выполнение загруженного файла на сервере (например, через доступ к web-root) или использование его в качестве точки закрепления. Вредоносный файл в данном случае фактически передается на сервер и может быть сохранен в файловой системе.	• Initial Access (TA0001) • Persistence (TA0003) • Command and Control (TA0011) • Ingress Tool Transfer (T1105) • Drive-by Compromise (T1189) • Exploit Public-Facing Application (T1190) • Server Software Component (T1505) • Web Shell (T1505.003) • Phishing for Information (T1598) • Spearphishing Link (T1598.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1515	Использование сканера уязвимостей	Правило детектирует события Application Firewall Positive Technologies (PT AF), указывающие на использование инструментов автоматизированного тестирования на проникновение, что может свидетельствовать о ранней стадии атаки.	• Reconnaissance (TA0043) • Initial Access (TA0001) • Exploit Public-Facing Application (T1190) • Active Scanning (T1595) • Vulnerability Scanning (T1595.002)
RV-D-1518	Атака типа XSS	Обнаружение попыток эксплуатации уязвимости типа Cross-Site Scripting (XSS) на веб-приложении на основе событий от Application Firewall компании Positive Technologies (PT AF). Данный тип атак направлен на внедрение вредоносного клиентского кода (чаще всего JavaScript) в веб-страницу, который выполняется в браузере жертвы.	• Initial Access (TA0001) • Command and Scripting Interpreter (T1059) • JavaScript (T1059.007) • Exploit Public-Facing Application (T1190)
RV-D-1520	Попытка эксплуатации уязвимостей	Правило осуществляет регистрацию оповещений на основе получения событий от Application Firewall компании Positive Technologies (PT AF), сообщающих о возможной эксплуатации уязвимостей веб-приложения.	• Initial Access (TA0001) • Exploit Public-Facing Application (T1190)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1521	Атака типа SSRF	Обнаружение попыток эксплуатации уязвимости типа Server-Side Request Forgery (SSRF) на основании событий от Application Firewall компании Positive Technologies (PT AF). Данный тип атак позволяет атакующему инициировать сетевые запросы от имени уязвимого веб-приложения к внутренним или внешним ресурсам.	• Reconnaissance (TA0043) • Initial Access (TA0001) • Exploit Public-Facing Application (T1190) • Active Scanning (T1595)
RV-D-1522	Атака типа CSRF	Обнаружение попыток эксплуатации уязвимости типа Cross-Site Request Forgery (CSRF) на основе событий от Application Firewall компании Positive Technologies (PT AF). Данный тип атак позволяет атакующему инициировать нежелательные действия в веб-приложении от имени аутентифицированного пользователя без его ведома.	• Initial Access (TA0001) • Exploit Public-Facing Application (T1190)
RV-D-1524	Внедрение SQL-кода	Обнаружение попыток внедрения SQL-кода (SQL Injection) на основе событий от Application Firewall компании Positive Technologies (PT AF). Данный тип атак направлен на внедрение вредоносных SQL-запросов в параметры веб-приложения с целью несанкционированного доступа к базе данных.	• Initial Access (TA0001) • Exploit Public-Facing Application (T1190)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1525	Попытка удаленного выполнения кода	Обнаружение попыток удаленного выполнения кода (Remote Code Execution, RCE) на основании событий от Application Firewall компании Positive Technologies (PT AF). Данный тип атак направлен на выполнение произвольных команд или кода на сервере, на котором размещено веб-приложение.	• Initial Access (TA0001) • Execution (TA0002) • Command and Scripting Interpreter (T1059) • Exploit Public-Facing Application (T1190)
RV-D-1535	Атака на веб-ресурс	Обнаружение попыток атак на веб-приложение на основе событий от Application Firewall компании Positive Technologies (PT AF). Правило фиксирует различные типы вредоносной активности, направленной на веб-ресурс, включая эксплуатацию уязвимостей, сканирование, внедрение вредоносных данных и другие аномальные действия.	• Reconnaissance (TA0043) • Initial Access (TA0001) • Exploit Public-Facing Application (T1190) • Active Scanning (T1595)

Гарда WAF

- Гарда WAF: настройка источника
- Гарда WAF: правила корреляции

Гарда WAF: настройка источника

Гарда WAF — это комплексное решение класса WAAP (Web Application and API Protection), которое включает расширенные инструменты для защиты веб-приложений и API от атак и уязвимостей, выявляет аномалии и угрозы нулевого дня.

Данное руководство описывает процесс настройки сбора и отправки событий программного комплекса Гарда WAF в R-Vision SIEM.

Предварительные требования

- Сетевой доступ к БД Гарда WAF.
- Учетная запись в СУБД с правами на чтение БД Гарда WAF (Сбор событий из БД).

Настройка Гарда WAF

Настройки СУБД PostgreSQL

События Гарда WAF записываются в базу данных `waf` СУБД PostgreSQL. Чтобы подключиться к базе данных (далее — БД) для сбора логов, используйте специально созданную сервисную учетную запись (далее — УЗ).

Создание учетной записи в СУБД PostgreSQL

Чтобы создать сервисную УЗ, подключитесь к СУБД с правами администратора. Для этого выполните следующие действия на сервере с установленной СУБД:

1. Выполните следующую команду от имени пользователя `postgres`:

   ```
   sudo -u postgres psql
   ```

2. Создайте сервисную учетную запись, выполнив следующие команды:

   ```
   CREATE USER "gwaf_reader";
   ALTER ROLE gwaf_reader WITH PASSWORD 'passw0rd';
   ```

3. Выдайте права на чтение БД:

   ```
   GRANT SELECT ON ALL TABLES IN SCHEMA public TO gwaf_reader;
   ```

Настройка в R-Vision SIEM

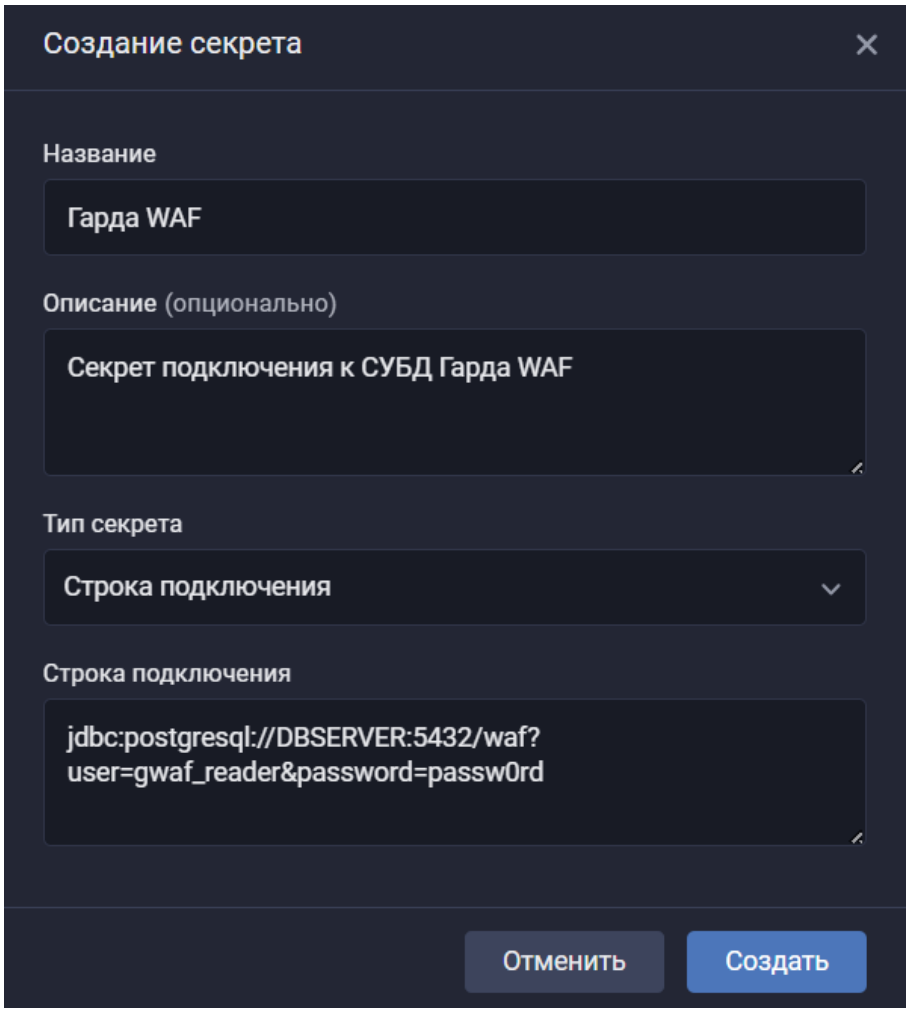
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте секрет со строкой подключения. Для этого:
   a. Перейдите в раздел **Ресурсы** → **Секреты**.
   b. Нажмите на кнопку **Создать** (＋).
   c. В раскрывшемся окне создания секрета заполните поля:
      - Название: введите название секрета.
      - Описание (опционально): опишите, для чего будет использоваться секрет.
      - Тип секрета: выберите вариант **Строка подключения**.
      - Строка подключения: введите строку вида:

        ```
        jdbc:postgresql://DBSERVER:5432/waf?user=gwaf_reader&password=passw0rd
        ```

        Здесь:

- DBSERVER — FQDN или IP-адрес сервера СУБД.
- 5432 — порт подключения.



d. Нажмите на кнопку **Создать**.

2. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
3. Добавьте на конвейер элемент **Точка входа** для событий аудита со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Database**.
   - Драйвер базы данных: выберите вариант **PostgreSQL**.
   - Адрес подключения: выберите секрет, созданный ранее.
   - SQL-запрос: введите запрос вида:

```
SELECT
    ilr.id AS ilr_id,
    ilr.chain_id,
    ilr.accuracy,
    ilr.intervention_hostname,
    ilr.matched_data,
    ilr.maturity,
    ilr.message,
    ilr.passive,
```

```
    ilr.ref,
    ilr.rev,
    ilr.rule_id,
    ilr.severity,
    ilr.uri AS ilr_uri,
    ilr.ver,
    ilt.tags,
    icr.cluster_id,
    icr.cluster_name,
    icr.instance_id,
    icr.timestamp as timestamp,
    icr.worker_process_id,
    icr.worker_thread_id,
    icr.client_address,
    icr.hostname AS icr_hostname,
    icr.request_id,
    icr.request_id_hash,
    icr.server_id,
    icr.is_blocked,
    icr.status_code,
    icr.max_severity,
    icr.min_severity,
    icr.user_agent,
    icr.is_passive,
    rlr.uri AS request_uri,
    rlr.method as method,
    inet_server_addr() AS dvc,
    'Garda WAF' as product
FROM public.intervention_log_record ilr
LEFT JOIN
    (
        SELECT
        log_id,
        string_agg(name, ', ') AS tags
        FROM
        public.intervention_log_record_tag
        GROUP BY
        log_id
    ) ilt ON ilr.id = ilt.log_id
JOIN
    public.interventions_chain_record icr ON ilr.chain_id = icr.id
LEFT JOIN
    public.request_log_record rlr ON icr.request_id = rlr.request_id
WHERE icr.timestamp > CAST(? AS BIGINT)
ORDER BY
icr.timestamp;
```

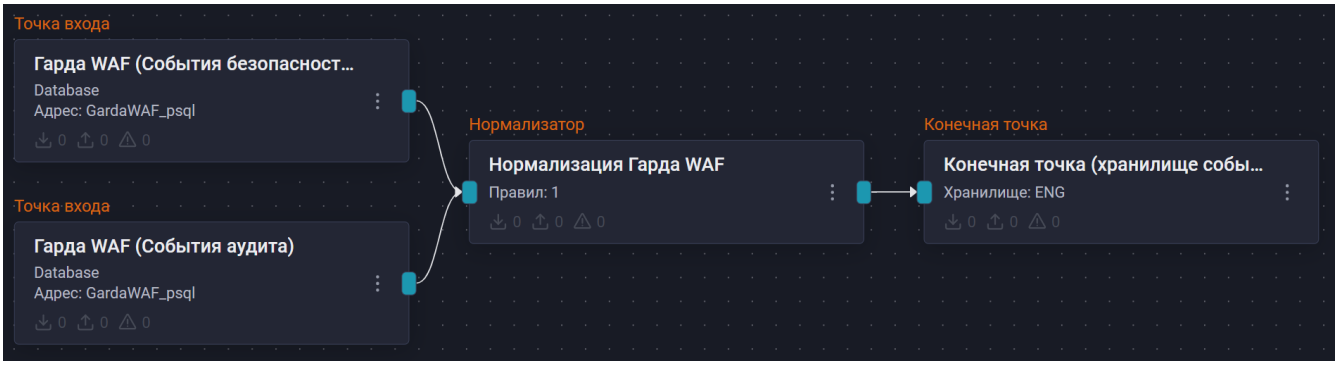
- Поле идентификатора: введите ключ `timestamp` со значением `1742380463`.
- Интервал запроса, секунд: введите значение `20`.

4. Добавьте на конвейер вторую точку входа для событий безопасности со следующими параметрами:
    - Название: введите название точки входа.
    - Тип точки входа: выберите вариант **Database**.
    - Драйвер базы данных: выберите вариант **PostgreSQL**.
    - Адрес подключения: выберите секрет, созданный ранее.
    - SQL-запрос: введите запрос вида:

```
SELECT
    ae.event_id as event_id,
    ae.cluster_id,
    ae.server_index,
    ae.timestamp,
    ae.username,
    ae.event_type,
    ae.entity_type,
    ae.event,
    ae.service_name,
    ae.cluster_name,
    ae.ip_address,
    scah.allowed_hostnames as server_name,
    inet_server_addr() AS dvc,
    'Garda WAF' as product,
    'Audit' as type_event
FROM public.audit_event ae
LEFT JOIN public.server_configuration_allowed_hostnames scah
    ON ae.server_index = scah.server_configuration_id
WHERE ae.event_id > CAST(? AS BIGINT)
ORDER BY ae.event_id ASC LIMIT 10000;
```

    - Поле идентификатора: введите ключ `event_id` со значением `1`.
    - Интервал запроса, секунд: введите значение `60`.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **Garda WAF** (идентификатор правила: **RV-N-223**).
6. Соедините нормализатор с точками входа.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Установите конфигурацию конвейера.

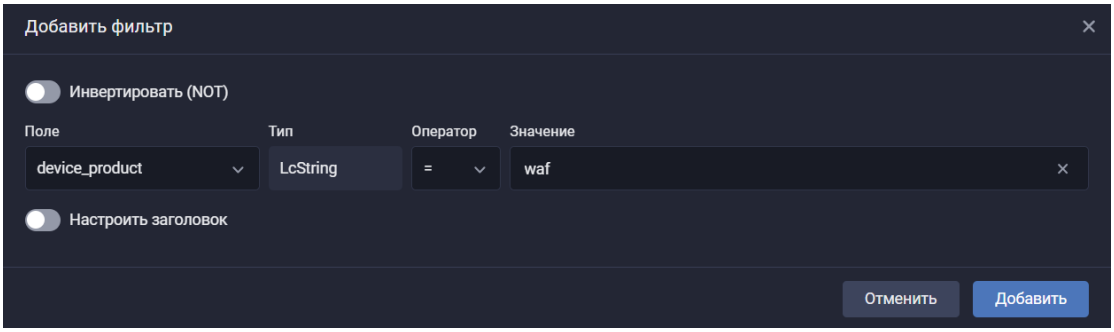
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Гарда WAF из PostgreSQL.

Найти события Гарда WAF в хранилище можно по следующему фильтру:

```
device_product = "waf"
```



Гарда WAF: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1441	Подбор пароля пользователя к Garda WAF	Правило детектирует перебор паролей для одного пользователя. Для получения доступа к учетной записи или хосту атакующий может попробовать подобрать пароль с помощью перебора.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001) • Password Spraying (T1110.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1442	Успешный подбор пароля к Garda WAF	Правило детектирует успешную аутентификацию после серии попыток подбора пароля. Для получения доступа к учетной записи или хосту атакующий может попробовать подобрать пароль с помощью перебора.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001) • Password Spraying (T1110.003)
RV-D-1443	Атака Password Spraying на Garda WAF	Атакующие могут использовать один или небольшой список часто используемых паролей для многих различных учетных записей, чтобы попытаться получить действительные учетные данные.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001) • Password Spraying (T1110.003)
RV-D-1444	Добавление пользователю критичной роли в Garda WAF	Атакующий в рамках закрепления может создать новую роль с критичными правами или назначить расширенные права доступа существующей роли. Данное правило также детектирует создание пользователя. В случае детектирования данного инцидента необходимо получить подтверждение активности от ответственного лица за учетную запись.	• Persistence (TA0003) • Account Manipulation (T1098) • Additional Local or Domain Groups (T1098.007)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1448	Массовое удаление УЗ Garda WAF	Атакующий, получив доступ к административной панели Garda WAF, может удалить учетные записи пользователей, чтобы затруднить их повторный вход и скрыть следы своей активности. Массовое удаление учетных записей может указывать на попытку нарушения работы системы безопасности. Правило обнаруживает множественные удаления учетных записей в Garda WAF инициированное одной учетной записью.	• Impact (TA0040) • Account Access Removal (T1531)
RV-D-1451	Отключение или изменение паттерна Garda WAF	Атакующий в рамках защиты от обнаружения может отключить или удалить паттерны валидации, которые отвечают за валидацию обращений к защищаемому ресурсу, а также отключить и удалить паттерны, отвечающие за парольную политику.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)
RV-D-1452	Изменение настроек защиты подключенного сервера	Правило отслеживает изменение настроек защиты на подключенных серверах, использующих ModSecurity. Основной фокус – детектирование перехода в пассивные режимы, когда защита перестает активно блокировать атаки.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1454	Атака на веб-приложение Garda WAF	Garda WAF — это сетевой экран уровня приложений, который защищает и обнаруживает веб-атаки на сайты и приложения. В результате мы можем получать оповещения средства защиты информации (далее — СЗИ) о произошедших событиях веб-атаки.	• Initial Access (TA0001) • Execution (TA0002) • Exploit Public-Facing Application (T1190) • Server Software Component (T1505) • Web Shell (T1505.003)
RV-D-1458	Множественные атаки на веб-приложение Garda WAF	Garda WAF — это сетевой экран уровня приложений, который защищает и обнаруживает веб-атаки на сайты и приложения. В результате мы можем получать оповещения средства защиты информации (далее — СЗИ) о произошедших событиях веб-атаки. Данное правило детектирует множественные веб-атаки различных типов, направленные на один хост.	• Initial Access (TA0001) • Execution (TA0002) • Exploit Public-Facing Application (T1190) • Server Software Component (T1505) • Web Shell (T1505.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1460	Множественная атака на веб-приложение Garda WAF	Garda WAF — это сетевой экран уровня приложений, который защищает и обнаруживает веб-атаки на сайты и приложения. В результате мы можем получать оповещения от средства защиты информации (далее — СЗИ) о произошедших событиях веб-атаки. Данное правило обнаруживает на веб-сервере множественные атаки одного типа.	• Initial Access (TA0001) • Execution (TA0002) • Persistence (TA0003) • Exploit Public-Facing Application (T1190) • Server Software Component (T1505) • Web Shell (T1505.003)

Системы защиты конечных точек (Endpoint Protection)

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых систем защиты конечных точек:

- BI.ZONE EDR
- Check Point Harmony Endpoint
- Microsoft Endpoint Configuration Manager (MECM)
- Код Безопасности Secret Net Studio

Check Point Harmony Endpoint

- Check Point Harmony Endpoint: настройка источника

Check Point Harmony Endpoint: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Check Point Harmony Endpoint в R-Vision SIEM.

Предварительные требования

Необходим промежуточный syslog-сервер, выделенный под передачу событий из Check Point Harmony Endpoint, который будет перенаправлять события в R-Vision SIEM. Данная необходимость обусловлена ограничением со стороны Check Point Harmony Endpoint по портам доставки Syslog (6514, 514).

Настройка Check Point Harmony Endpoint

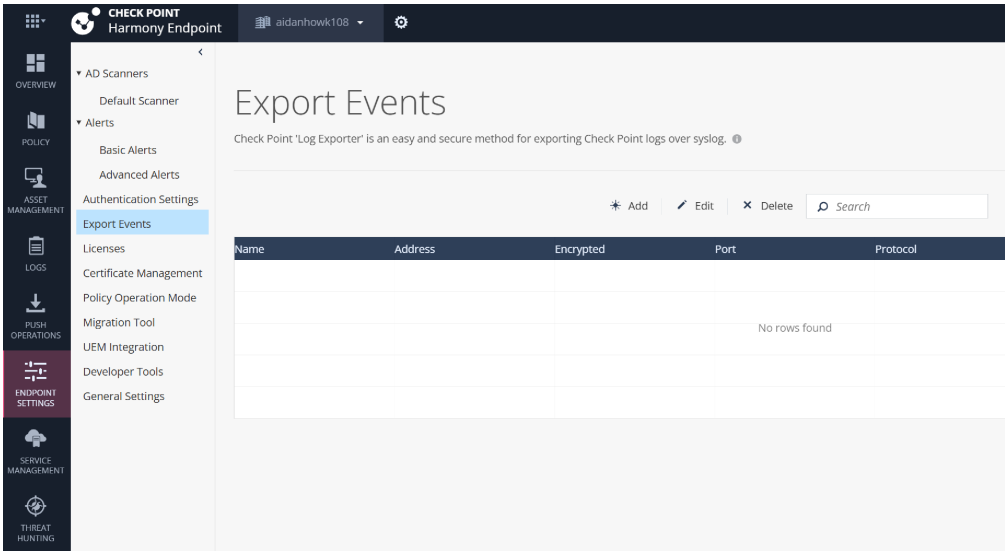
Для пересылки событий, зарегистрированных Check Point Harmony Endpoint, в R-Vision SIEM по протоколу Syslog:

1. Авторизуйтесь на портале управления Check Point.

   Портал управления Check Point расположен по адресу: `Check Point Portal`.

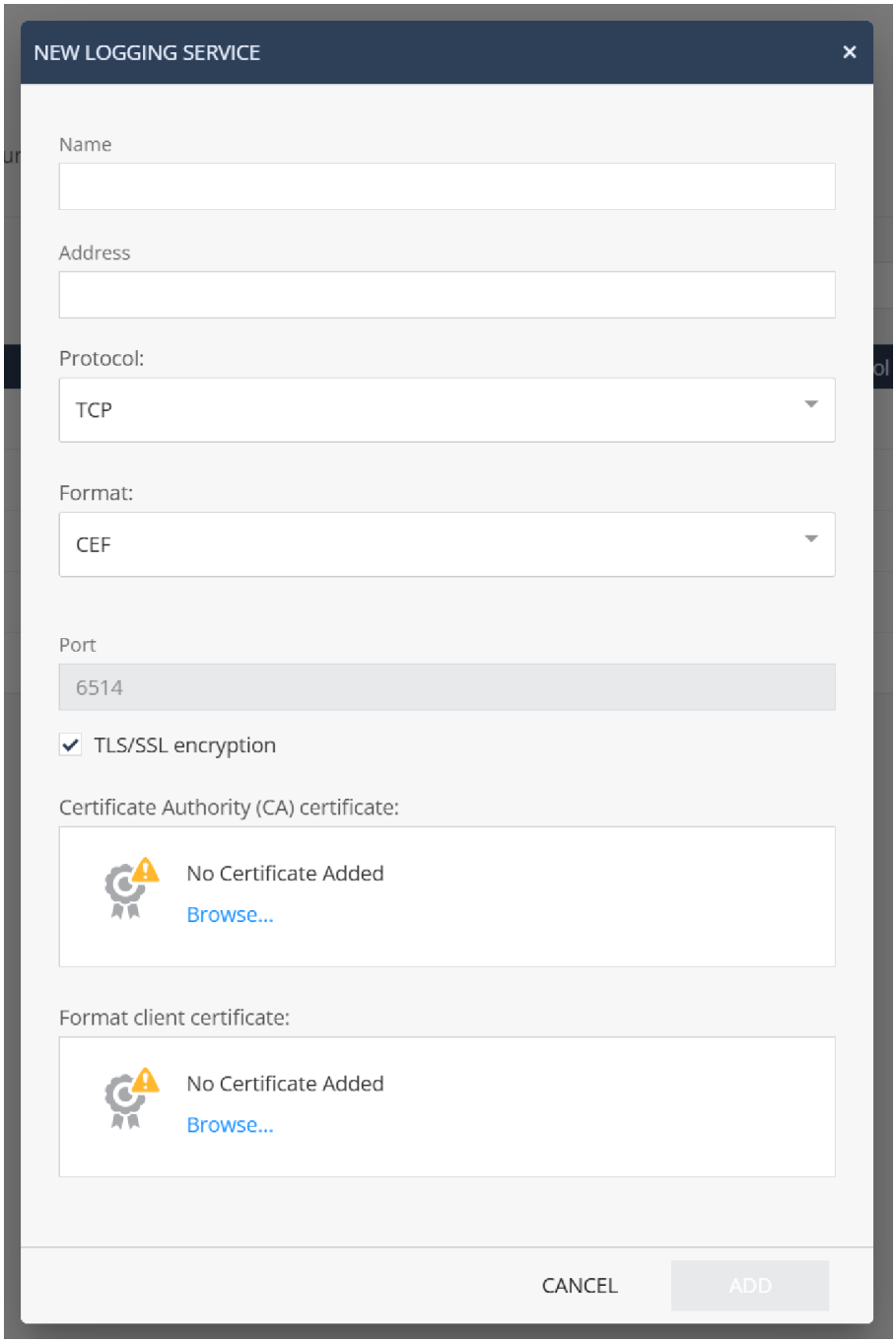
2. В меню слева перейдите в раздел **ENDPOINT SETTINGS** → **Export Events**.
3. Нажмите на кнопку **Add**.



4. В появившемся окне введите данные коллектора R-Vision SIEM:
   - **Name**: введите произвольное название коллектора.
   - **Address**: введите адрес коллектора R-Vision SIEM или промежуточного syslog-сервера.
   - **Protocol**: выберите из выпадающего списка вариант `TCP` или `UDP`.
   - **Format**: выберите из выпадающего списка вариант `CEF`.
   - **Port**: при использовании TLS/SSL будет статически задан порт со значением `6514`, в ином случае — `514`.
   - **Certificate Authority (CA) certificate**: при использовании TLS/SSL загрузите сертификат CA.
   - **Format client certificate**: при использовании TLS/SSL загрузите сертификат клиента.



Сертификат клиента должен быть выпущен центром сертификации, сертификат которого загружается в поле **Certificate Authority (CA) certificate**.



5. Нажмите на кнопку **ADD**.

Настройка Check Point Harmony Endpoint завершена.

Настройка промежуточного syslog-сервера на примере rsyslog

Если передача событий будет осуществляться без использования TLS/SSL, алгоритм настройки следующий:

1. Создайте и откройте файл конфигурации rsyslog в директории `/etc/rsyslog.d/`:

```
sudo nano /etc/rsyslog.d/40-harmony.conf
```

2. Скопируйте в файл конфигурации следующие строки:

```
# Настройка для передачи по протоколу tcp.
module(load="imtcp")
input(type="imtcp" port="514")

# Настройка для передачи по протоколу udp.
module(load="imudp")
input(type="imudp" port="6514")

action(
    type="omfwd"
    target="<ip R-Vision SIEM>"
    port="<port>"
    protocol="<proto>"
)
```

Здесь:

- `<ip R-Vision SIEM>` — адрес коллектора R-Vision SIEM.
- `<port>` — порт приема событий, указанный в R-Vision SIEM.
- `<proto>` — протокол передачи.

3. Сохраните конфигурацию.
4. Перезагрузите службу rsyslog:

```
sudo systemctl restart rsyslog
```

Если передача событий будет осуществляться с использованием TLS/SSL, необходимо использовать алгоритм, описанный выше. Однако будут отличия в конфигурации:

```
module(load="imtcp")
module(load="lmnsd_gtls")

global(
    DefaultNetstreamDriver="gtls"
    DefaultNetstreamDriverCAFile="/etc/rsyslog-keys/ca/ca.crt"
    DefaultNetstreamDriverCertFile="/etc/rsyslog-keys/server/server.crt"
    DefaultNetstreamDriverKeyFile="/etc/rsyslog-keys/server/server.key"
)

input(
    type="imtcp"
    port="6514"
    StreamDriver.Name="gtls"
    StreamDriver.Mode="1"
    StreamDriver.AuthMode="x509/name" # Если не нужно подтверждение от клиента,
используйте значение anon.
)
```

```
action(
    type="omfwd"
    target="<ip R-Vision SIEM>"
    port="<port>"
    protocol="<proto>"
)
stop
```

Здесь:

- `ca.crt` — корневой сертификат центра сертификации. Данный сертификат также загружается при настройке Check Point Harmony.
- `server.crt` — сертификат syslog-сервера.
- `server.key` — закрытый ключ syslog-сервера.

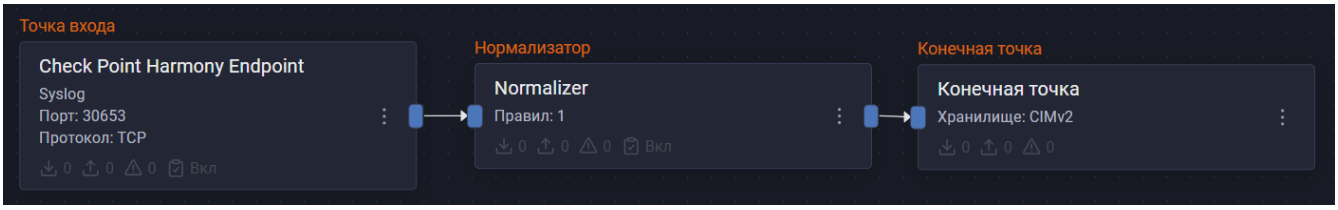
Данные сертификаты необходимо получить в центре сертификации и разместить на syslog-сервере.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
    - Название: введите название точки входа.
    - Тип точки входа: выберите вариант **Syslog**.
    - Порт точки входа: введите значение в диапазоне 30000—32767.
    - Протокол: выберите вариант в соответствии с настройками на стороне промежуточного syslog-сервера.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Checkpoint Endpoint** (идентификатор правила: **RV-N-248**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

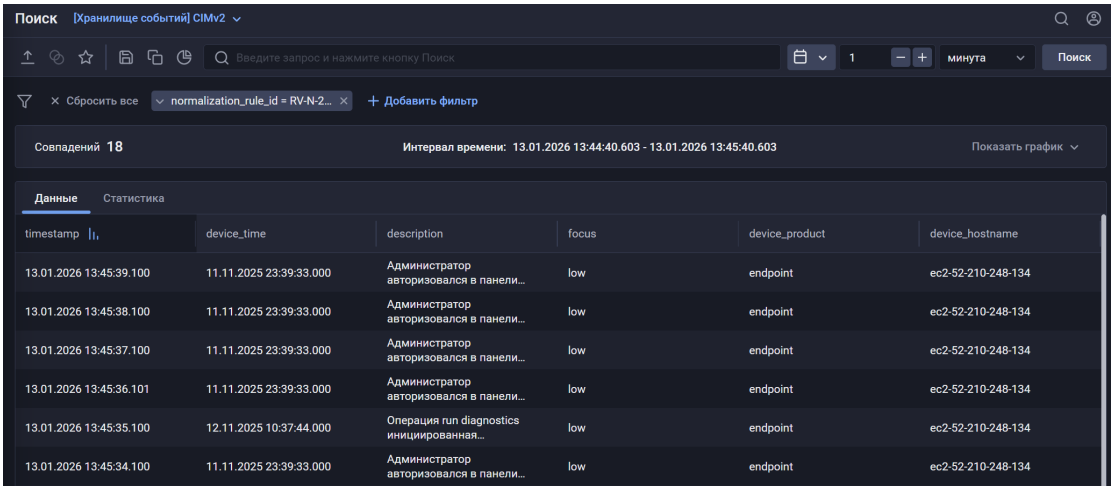


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут

поступать события Check Point Harmony Endpoint.

Найти события Check Point Harmony Endpoint в хранилище можно по следующему фильтру:

```
normalization_rule_id = "RV-N-248"
```



BI.ZONE EDR

- BI.ZONE EDR: настройка источника

BI.ZONE EDR: настройка источника

Данное руководство описывает процесс настройки сбора событий BI.ZONE EDR и их отправки в R-Vision SIEM.

Предварительные требования

Перед настройкой пересылки событий в R-Vision SIEM убедитесь в выполнении следующих условий:

- Настроен сбор событий с конечных точек с помощью агента BI.ZONE EDR.
- Сетевая связность между брокерами Kafka и SIEM обеспечена, а необходимые порты открыты.
- Подготовлены следующие параметры для подключения:
  - Адрес(а) брокеров Kafka.
  - Порт подключения.
  - Наименование топика (topic).
  - Тип аутентификации (без аутентификации или SASL/SSL).
  - Логин и пароль (если требуется).

Настройка BI.ZONE EDR

Настройка отправки событий в R-Vision SIEM

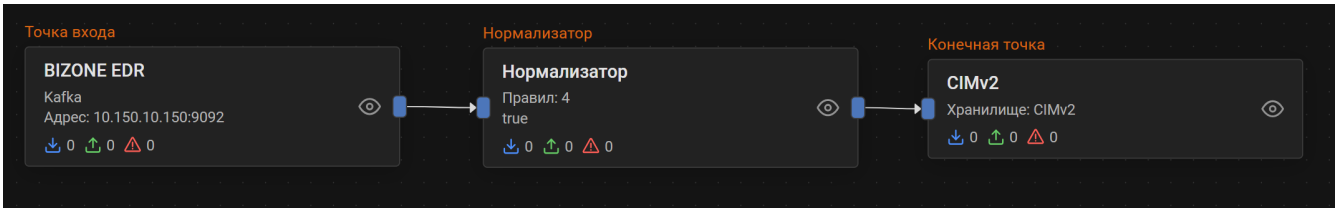
Настройка экспорта событий в Kafka на стороне BI.ZONE EDR выполняется исключительно средствами вендора. Для выполнения данной настройки обратитесь к официальной документации BI.ZONE EDR.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий BI.ZONE EDR в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите произвольное, понятное название.
   - Тип точки входа: выберите вариант **Kafka**.
   - Адреса подключения: введите список адресов серверов в кластере Kafka (формат: IP-адрес:порт, например, 10.14.22.123:9092, 10.14.23.332:9092).
   - Название группы потребителей: укажите название Consumer group (например, event-consumer-group).
   - Названия топиков: укажите названия топиков Kafka, из которых будут читаться события.
   - Включить TLS (опционально): активируйте для использования шифрования. При включении:
     - Выберите секрет типа **Контейнер PKCS** или **Контейнер PKCS#12**, хранящий данные сертификата TLS.
3. Добавьте на конвейер элемент **Нормализатор** с правилами **BI.ZONE EDR** (идентификаторы правил: **RV-N-213**, **RV-N-214**, **RV-N-215**, **RV-N-216**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

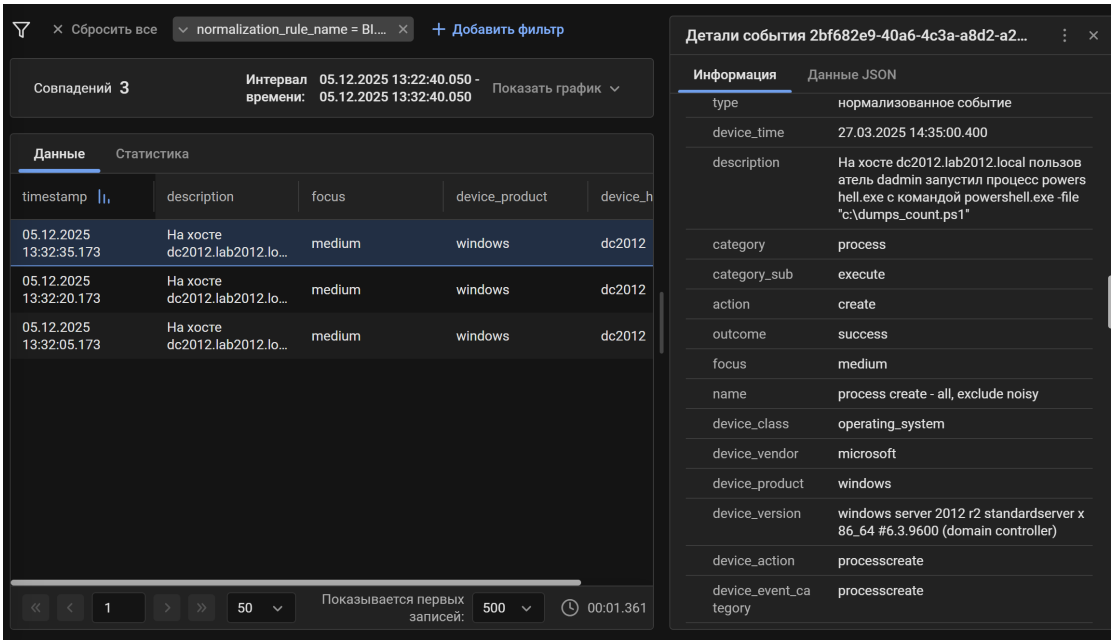
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события BI.ZONE EDR.

Найти события BI.ZONE EDR в хранилище можно по следующему фильтру:

```
normalization_rule_name = "BI.ZONE EDR"
```



Конфидент ЕЦУ Dallas Lock

- Конфидент ЕЦУ Dallas Lock: настройка источника

Конфидент ЕЦУ Dallas Lock: настройка источника

Описание источника

Единый центр управления Dallas Lock — кроссплатформенное изделие в продуктовой линейке Dallas Lock, предназначенное для решения следующих задач:

- Создание единого отказоустойчивого домена безопасности (далее — ДБ) и организация централизованного управления средствами защиты информации линейки Dallas Lock:
  - СЗИ НСД Dallas Lock 8.0 редакций «K» и «C» (далее — DL 8.0);
  - СЗИ НСД Dallas Lock Linux;
  - СЗИ ВИ Dallas Lock;
  - СДЗ Dallas Lock;
  - СДЗ УБ Dallas Lock;
  - WAF Dallas Lock.
- Удаленное управление рабочими станциями и серверами.
- Удаленная настройка, а также сбор журналов и отчетов с рабочих станций и серверов при помощи Агента ЕЦУ.
- Контроль целостности настроек сетевого оборудования по SNMP/SSH и сбор событий по Syslog.

Система имеет два способа сбора событий:

1. ЕЦУ Dallas Lock: сбор событий из СУБД PostgreSQL
2. ЕЦУ Dallas Lock: сбор событий в формате CEF

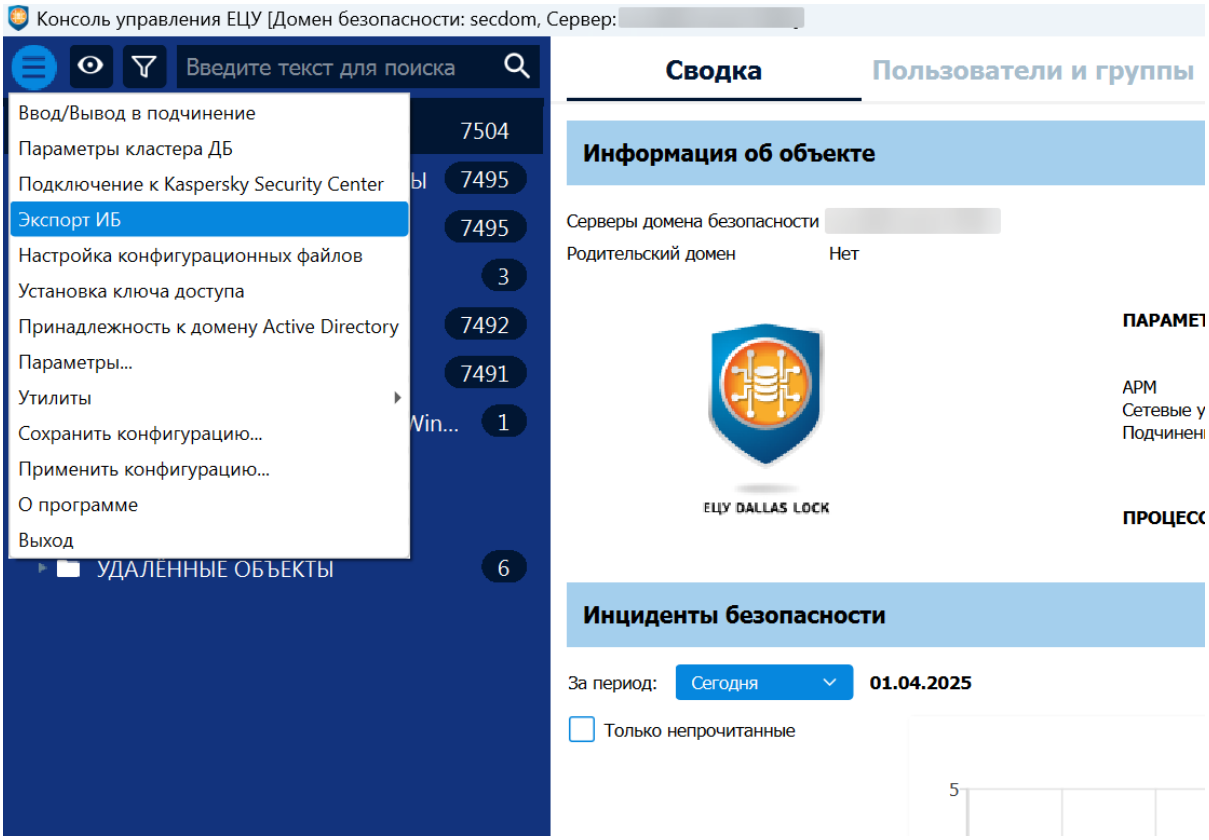
ЕЦУ Dallas Lock: сбор событий в формате CEF

Данное руководство описывает процесс настройки сбора и отправки событий ЕЦУ Dallas Lock в R-Vision SIEM.

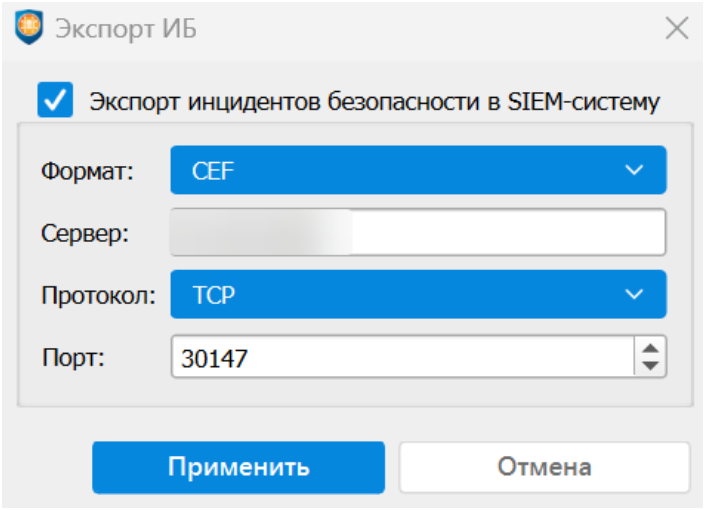
Настройка ЕЦУ Dallas Lock

Для пересылки событий, зарегистрированных ЕЦУ Dallas Lock, в R-Vision SIEM в формате CEF выполните следующие действия:

1. Откройте **Консоль управления ЕЦУ**.
2. Нажмите на кнопку меню в левом верхнем углу и выберите из выпадающего списка пункт **Экспорт ИБ**. Откроется окно настройки экспорта.



3. В открывшемся окне установите флажок **Экспорт инцидентов безопасности в SIEM-систему**.
4. Выберите из выпадающего списка **Формат** вариант CEF.
5. В поле **Сервер** введите IP-адрес коллектора.
6. Выберите из выпадающего списка **Протокол** транспортный протокол, настроенный на коллекторе.
7. В поле **Порт** введите значение порта точки входа.



8. Нажмите на кнопку **Применить**.

Настройка на стороне ЕЦУ Dallas Lock завершена.

Настройка в R-Vision SIEM

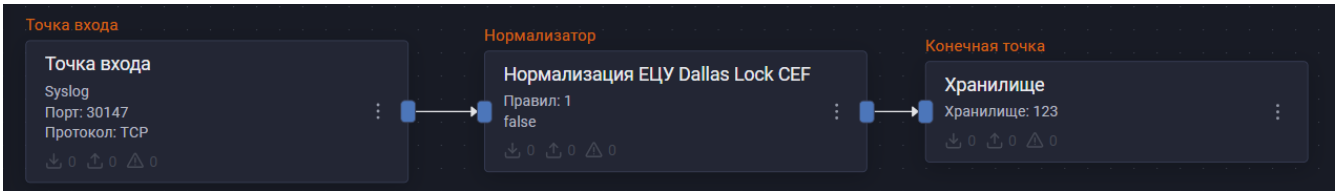
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне ЕЦУ Dallas Lock.
   - Протокол: выберите вариант в соответствии с настройками на стороне ЕЦУ Dallas Lock.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Confident Dallas Lock syslog** (идентификатор правила: **RV-N-291**).

   Правило **RV-N-291** также нормализует события, получаемые из Dallas Lock 8.0.

4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

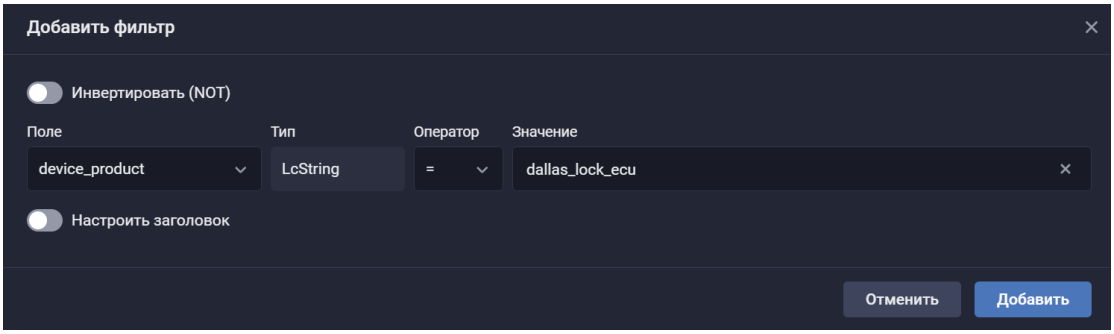
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события ЕЦУ Dallas Lock.

Найти события ЕЦУ Dallas Lock в хранилище можно по следующему фильтру:

```
device_product = "dallas_lock_ecu"
```



ЕЦУ Dallas Lock: сбор событий из СУБД PostgreSQL

Данное руководство описывает процесс настройки сбора и отправки событий ЕЦУ Dallas Lock в R-Vision SIEM из СУБД PostgreSQL.

Предварительные требования

- Сетевая доступность сервера СУБД источника по целевому порту и протоколу для каждой ноды кластера R-Vision SIEM.
- Учетная запись в СУБД с правами на чтение таблиц БД.

Настройка СУБД PostgreSQL

Для настройки сбора логов из базы данных необходимо подключиться к ней с использованием специальной сервисной учетной записи (далее — УЗ).

Создание учетной записи в СУБД PostgreSQL

Чтобы создать сервисную УЗ, подключитесь к СУБД с правами администратора. Для этого выполните следующие действия на сервере с установленной СУБД:

1. Выполните следующую команду от имени пользователя `postgres`:

   ```
   sudo -u postgres psql
   ```

2. Создайте сервисную учетную запись, выполнив следующие команды:

   ```
   CREATE USER "dl_reader";
   ALTER ROLE dl_reader WITH PASSWORD 'passw0rd';
   ```

3. Предоставьте права на подключение к базе данных и чтение таблицы:

```
GRANT CONNECT ON DATABASE dallaslock to dl_reader;
GRANT SELECT ON ALL TABLES IN SCHEMA public TO dl_reader;
```

Настройка в R-Vision SIEM

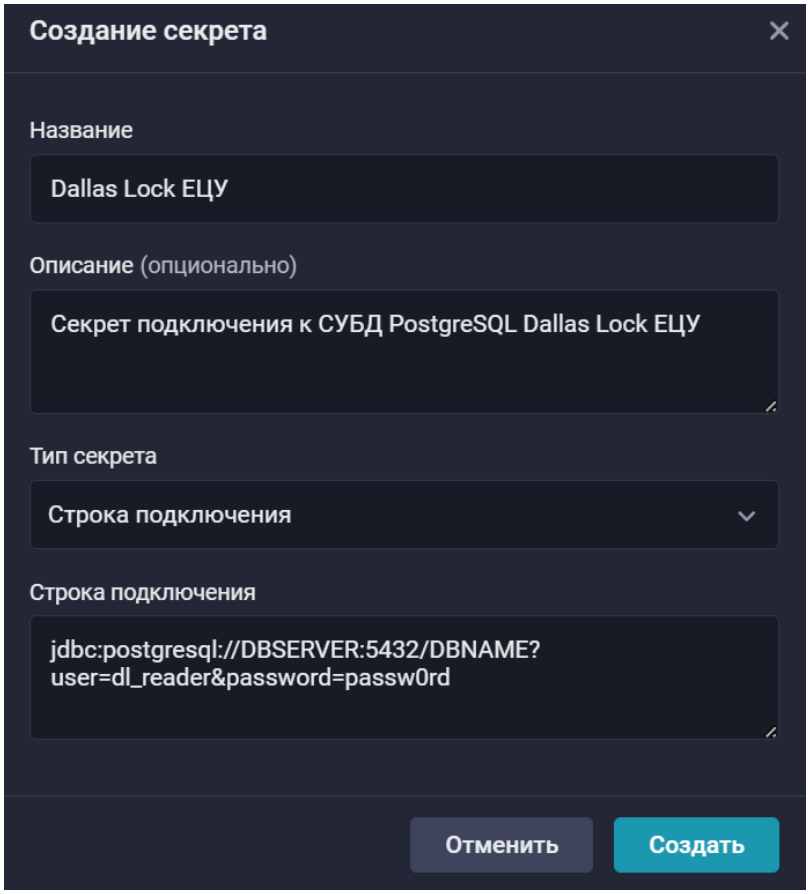
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте секрет со строкой подключения. Для этого:
   a. Перейдите в раздел **Ресурсы** → **Секреты**.
   b. Нажмите на кнопку **Создать** (+).
   c. В раскрывшемся окне создания секрета заполните поля:
      - Название: введите название секрета.
      - Описание (опционально): опишите, для чего будет использоваться секрет.
      - Тип секрета: выберите вариант **Строка подключения**.
      - Строка подключения: введите строку вида:

        ```
        jdbc:postgresql://DBSERVER:5432/DBNAME?user=dl_reader&password=passw0rd
        ```

        Здесь:

        - `DBSERVER` — FQDN или IP-адрес сервера СУБД.
        - `5432` — порт подключения.



d. Нажмите на кнопку **Создать**.

2. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
3. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Database**.
   - Драйвер базы данных: выберите вариант **PostgreSQL**.
   - Адрес подключения: выберите секрет, созданный ранее.
   - SQL-запрос: введите запрос вида:

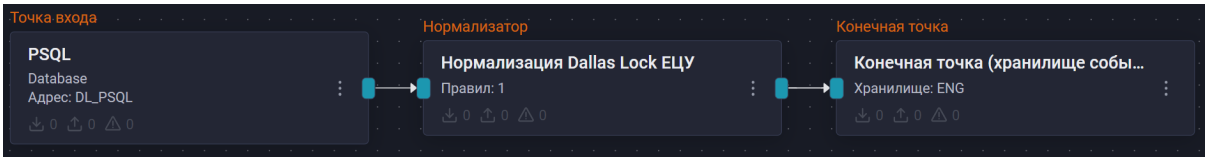
```
SELECT record_id as record_id
    ,timestamp as timestamp
    ,timestamp_timezone as timezone
    ,user as user
    ,event_id as event_id
    ,obj_name as obj
    ,status as status
    ,comment as comment
    ,guid as guid
    ,(SELECT vers_t.value FROM public.ucc_metainfo vers_t WHERE vers_t.key =
'version') as version
    ,'DL_PSQL' as filter
    ,inet_server_addr() AS dvc
FROM public.jrn_uccmainjournal
WHERE record_id > CAST(? AS BIGINT)
```

```
ORDER BY record_id ASC;
```

- Поле идентификатора: введите ключ `record_id` со значением `1`.
- Интервал запроса, секунд: введите значение `300`.

4. Добавьте на конвейер элемент **Нормализатор** с правилом **Confident Dallas Lock ECU PSQL** (идентификатор правила: **RV-N-289**).
5. Соедините нормализатор с точкой входа.
6. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
7. Соедините конечную точку с нормализатором.
8. Сохраните и установите конфигурацию конвейера.

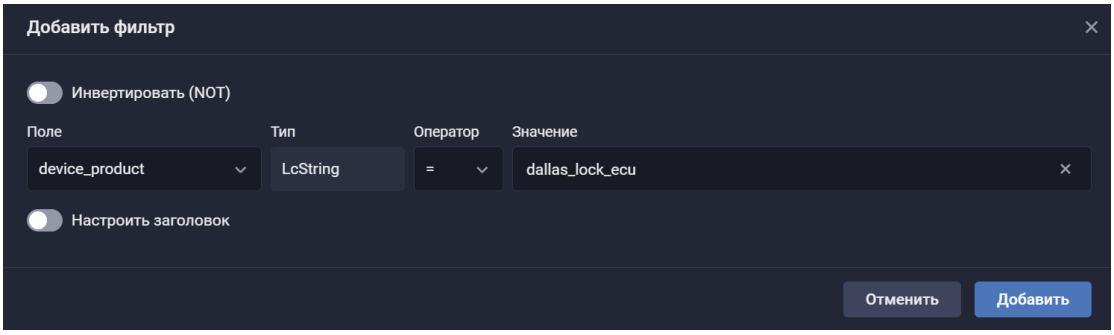
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события ЕЦУ Dallas Lock.

Найти события ЕЦУ Dallas Lock в хранилище можно по следующему фильтру:

```
device_product = "dallas_lock_ecu"
```



Конфидент Dallas Lock 8.0

- Конфидент Dallas Lock 8.0: настройка источника

Конфидент Dallas Lock 8.0: настройка источника

Описание источника

Система защиты информации Dallas Lock 8.0 предназначена для:

- предотвращения получения защищаемой информации заинтересованными лицами с нарушением установленных норм и правил и обладателями информации с нарушением

установленных правил разграничения доступа к защищаемой информации;

- осуществления контроля за потоками информации, поступающими в автоматизированную систему (далее — АС) и выходящими за ее пределы;
- обеспечения защиты информации в АС посредством ее фильтрации.

Dallas Lock 8.0 имеет возможность централизованного управления посредством Dallas Lock 8.0 Сервер Безопасности.

Данный раздел содержит список инструкций по настройке источника Dallas Lock 8.0:

- Dallas Lock 8.0 Сервер Безопасности: сбор событий из СУБД MS SQL
- Dallas Lock 8.0: сбор событий в формате CEF

Dallas Lock 8.0 Сервер Безопасности: сбор событий из СУБД MS SQL

Данное руководство описывает процесс настройки сбора и отправки событий Dallas Lock 8.0 Сервер Безопасности в R-Vision SIEM.

Предварительные требования

- Сетевая доступность сервера СУБД источника по целевому порту и протоколу для каждой ноды кластера R-Vision SIEM.
- Учетная запись в СУБД с правами на чтение таблиц, используемых Dallas Lock 8.0 Сервер Безопасности.

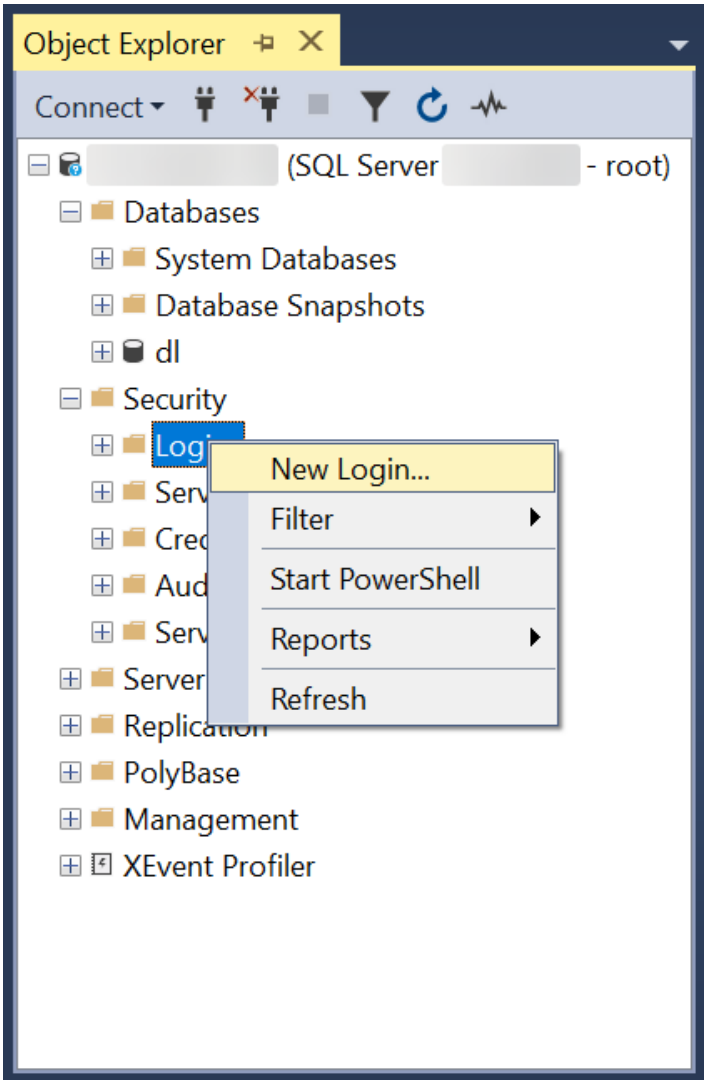
Настройка Dallas Lock 8.0 Сервер Безопасности

Для сбора событий Dallas Lock 8.0 Сервер Безопасности из базы данных MS SQL необходимо настроить подключение R-Vision SIEM под служебной УЗ с соответствующими правами.

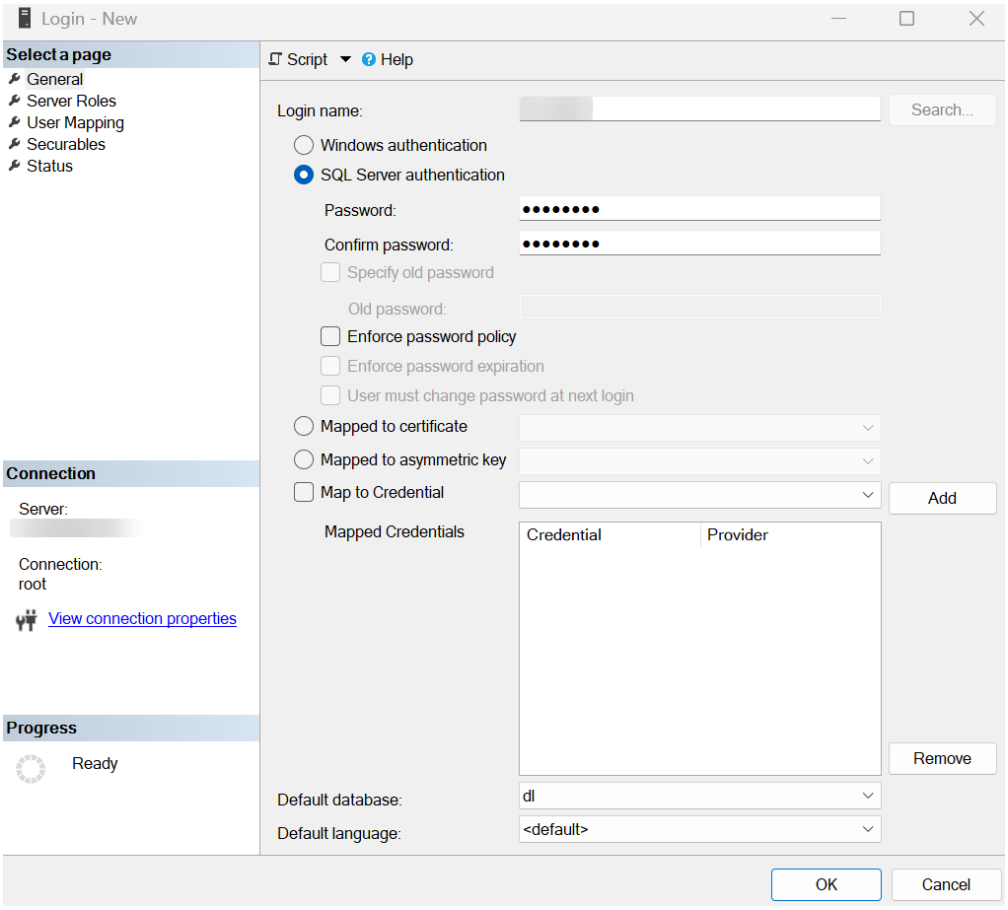
Создание учетной записи в СУБД MS SQL

Чтобы создать сервисную УЗ, подключитесь к СУБД с правами администратора. Для этого выполните следующие действия:

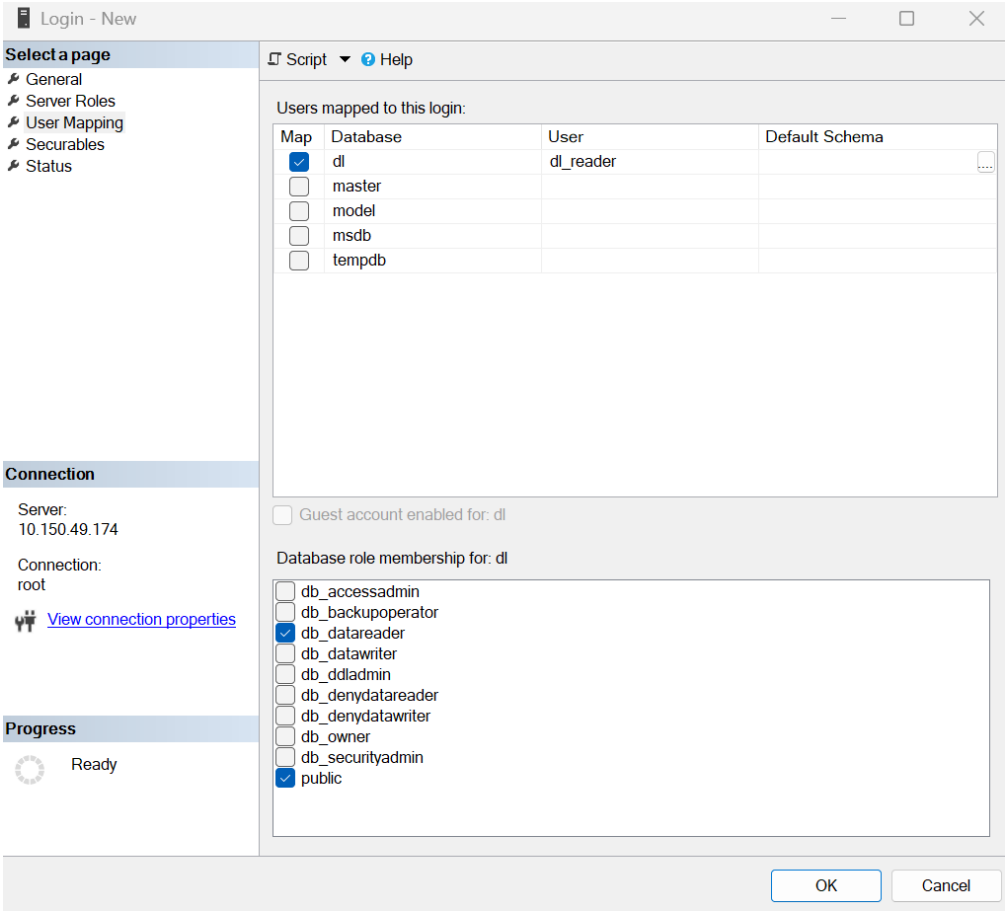
1. Войдите в веб-интерфейс **SQL Server Management Studio**.
2. Откройте контекстное меню **Logins**.
3. Выберите в контекстном меню вариант **New Login**.



4. В появившемся окне создайте сервисную учетную запись.



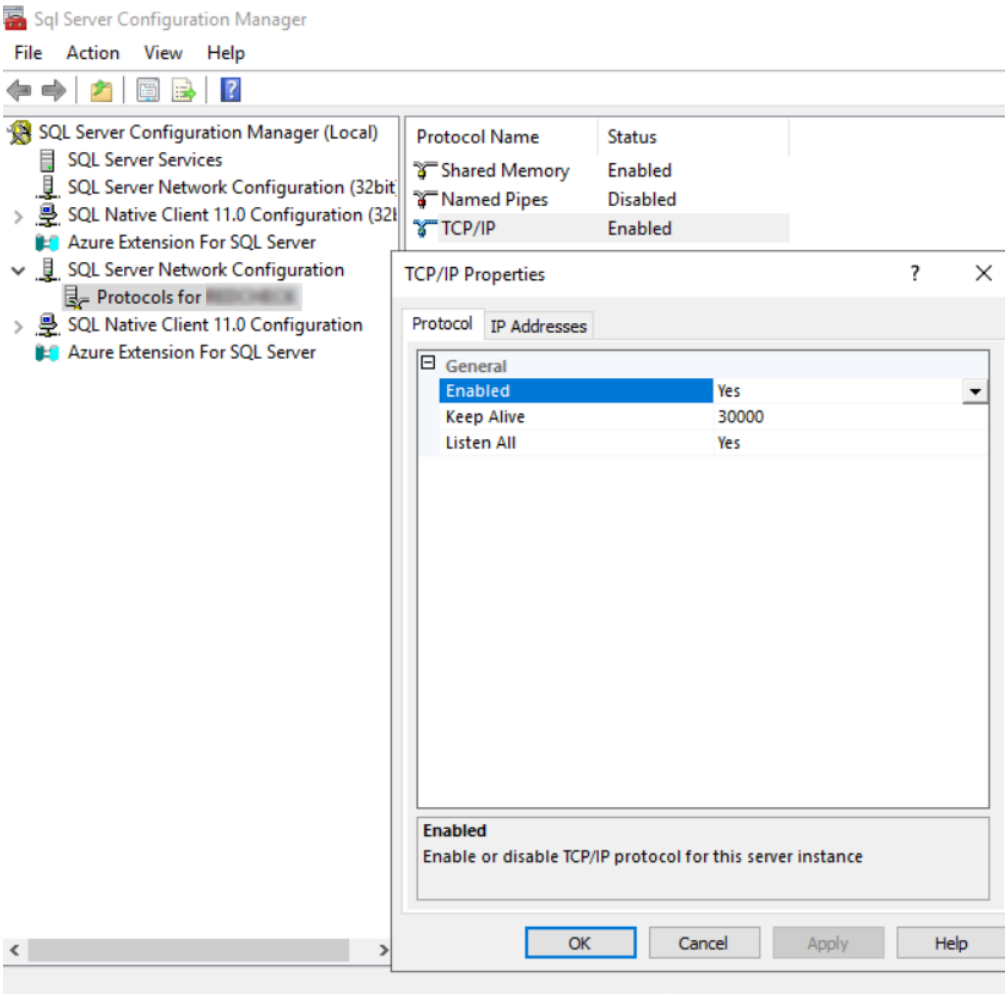
5. Предоставьте учетной записи права на чтение базы данных Dallas Lock.



6. Нажмите на кнопку **OK**.

Настройка сервера MS SQL

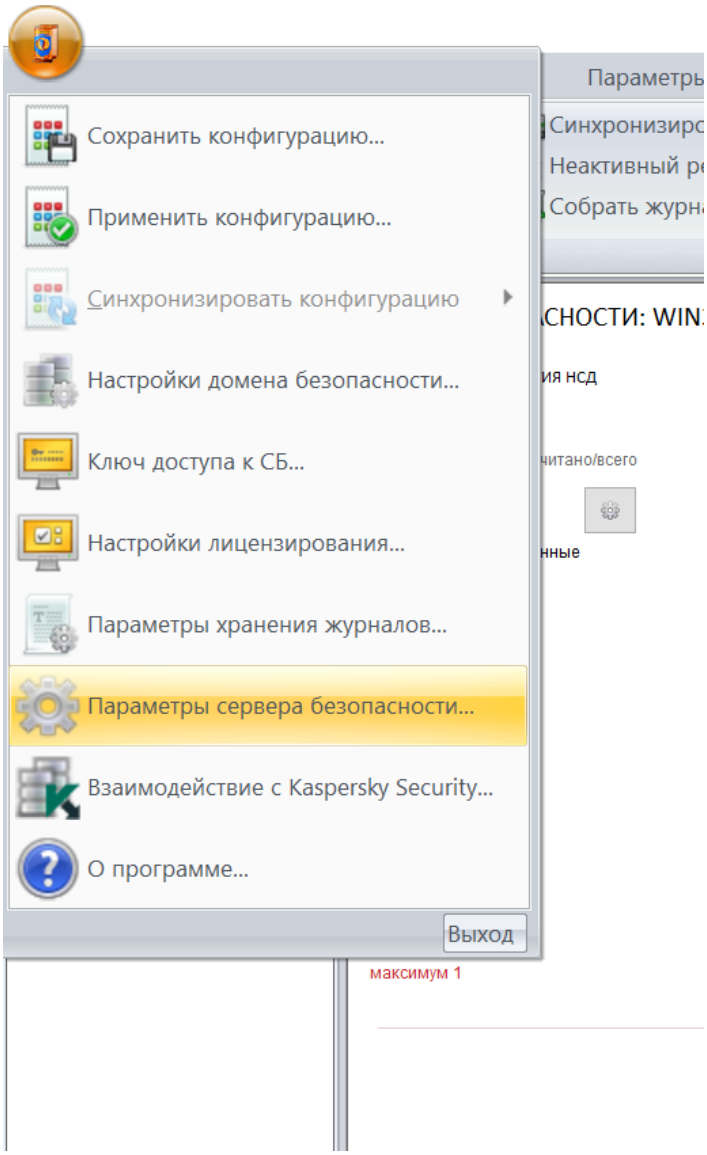
В настройках **SQL Server Configuration Manager** убедитесь, что протокол `TCP/IP` включен в конфигурации сети SQL Server.



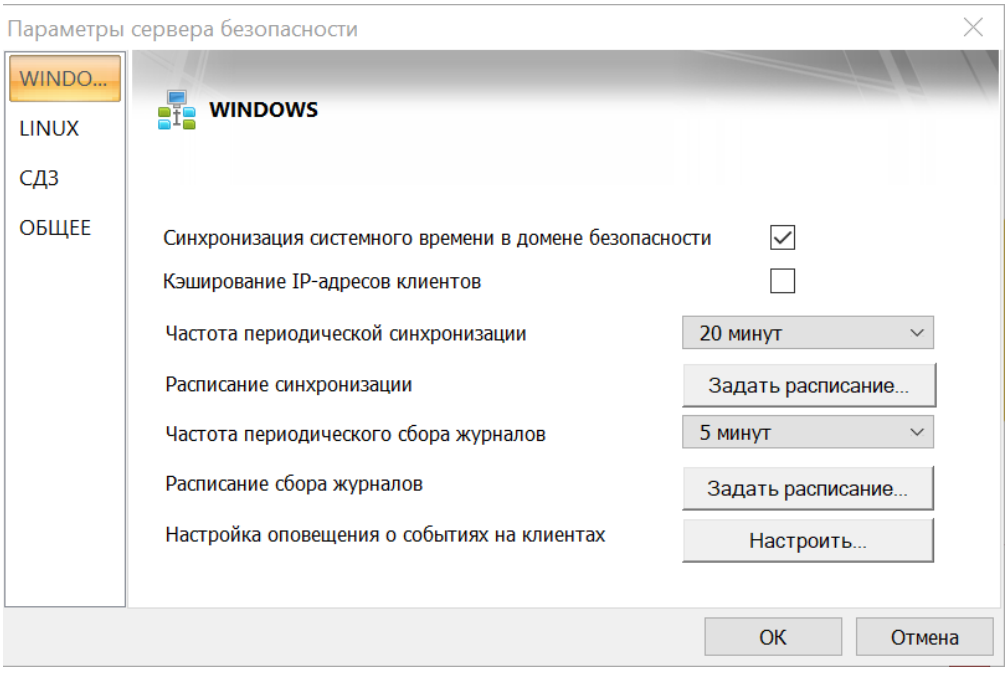
Настройка журналирования Dallas Lock 8.0 Сервер Безопасности

Необходимо настроить периодичность сбора событий с конечных АРМ на Сервер Безопасности. Для этого выполните следующие шаги:

1. Откройте панель администратора Сервера Безопасности.
2. Нажмите на кнопку  и в выпадающем меню выберите вариант **Параметры сервера безопасности**. Откроется окно настройки сервера безопасности.



3. В появившемся окне на вкладках **WINDOWS** и **LINUX** установите для параметра **Частота периодического сбора журналов** минимально возможное значение 5 минут.



4. Нажмите на кнопку **ОК**.

Настройка на стороне Dallas Lock 8.0 Сервер Безопасности завершена.

Настройка в R-Vision SIEM

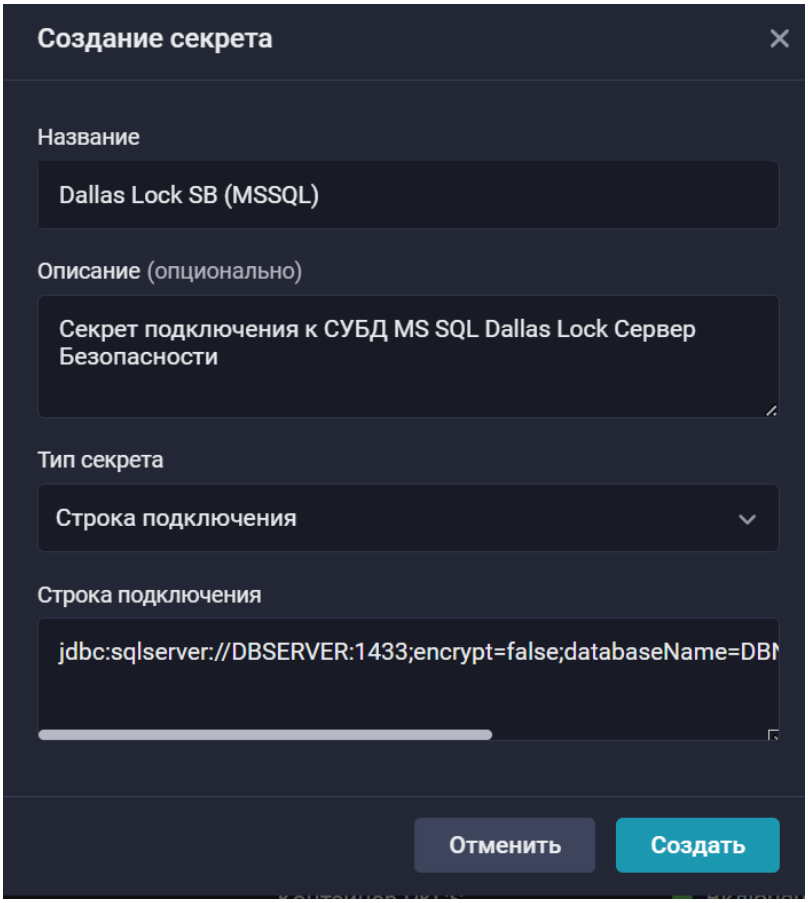
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте секрет со строкой подключения. Для этого:
   a. Перейдите в раздел **Ресурсы** → **Секреты**.
   b. Нажмите на кнопку **Создать** (+).
   c. В раскрывшемся окне создания секрета заполните поля:
      - **Название**: введите название секрета.
      - **Описание** (опционально): опишите, для чего будет использоваться секрет.
      - **Тип секрета**: выберите вариант **Строка подключения**.
      - **Строка подключения** — введите строку вида:

        ```
        jdbc:sqlserver://DBSERVER:1433;encrypt=false;databaseName=DBNAME;user=dl_rea
        der;password=passw0rd
        ```

        Здесь:

        - `DBSERVER` — FQDN или IP-адрес сервера СУБД.
        - `DBNAME` — название экземпляра БД.
        - `1433` — порт подключения.



d. Нажмите на кнопку **Создать**.

2. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
3. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - **Название**: введите название точки входа.
   - **Тип точки входа**: выберите вариант **Database**.
   - **Драйвер базы данных**: выберите вариант **MS SQL**.
   - **Адрес подключения**: выберите секрет, созданный ранее.
   - **SQL-запрос** — введите запрос вида:

     ▼ *SQL-запрос*

```
SELECT TOP 10000 'CONNECT' AS journal_name
    ,recID AS connect_rec_id
    ,dateAndTime AS event_date
    ,clientName AS client_name
    ,mandatLevel AS mandat_level
    ,userName AS user_name
    ,result AS result
    ,processName AS process_name
    ,processID as process_id
    ,permit AS permit
    ,EventOnConnect AS event_on_connect
    ,DnsName AS dns_name
    ,protocol AS protocol
```

```
    ,localAddress AS local_address
    ,(LocalPort & 255) * 256 | cast((LocalPort/256) & 255 as bigint) AS
local_port
    ,RemoteAddress AS remote_address
    ,(RemotePort & 255) * 256 | cast((RemotePort/256) & 255 as bigint) AS
remote_port
    ,inDataLen AS in_bytes
    ,outDataLen AS out_bytes
    ,ruleId AS rule_id
    ,NULL AS alarm_level
    ,NULL AS rule_action
    ,AddressType AS address_type
    ,NULL AS src_address
    ,NULL AS dst_address
    ,NULL AS signature_number
    ,NULL AS signature_info
    ,NULL AS computer_name
    ,NULL AS comment
    ,NULL as parameter
    ,NULL as action
    ,NULL as type_of_attack
    ,NULL as target_user_name
    ,NULL AS latest_protocol_id
    ,NULL AS direction
    ,NULL AS bytes
    ,NULL AS resource
    ,NULL AS printer_name
    ,NULL AS document
    ,NULL AS printer_port
    ,NULL AS pages_printed
    ,NULL AS copies_printed
    ,NULL AS shadow_copy
    ,NULL AS wrong_user_pw
    ,NULL AS logon_mode
FROM [dbo].[Connect] where dateAndTime >= DATEADD(MINUTE, -5, GetDate())
UNION ALL

SELECT TOP 10000 'PACKETS' AS journal_name
    ,recID AS packets_rec_id
    ,dateAndTime AS event_date
    ,clientName AS client_name
    ,mandatLevel AS mandat_level
    ,userName AS user_name
    ,result AS result
    ,processName AS process_name
    ,processID as process_id
    ,permit AS permit
    ,NULL AS event_on_connect
    ,DnsName AS dns_name
    ,NULL AS protocol
    ,localAddress AS local_address
```

```
    ,(LocalPort & 255) * 256 | cast((LocalPort/256) & 255 as bigint) AS
local_port
    ,RemoteAddress AS remote_address
    ,(RemotePort & 255) * 256 | cast((RemotePort/256) & 255 as bigint) AS
remote_port
    ,NULL AS in_bytes
    ,NULL AS out_bytes
    ,ruleId AS rule_id
    ,NULL AS alarm_level
    ,NULL AS rule_action
    ,AddressType AS address_type
    ,NULL AS src_address
    ,NULL AS dst_address
    ,NULL AS signature_number
    ,NULL AS signature_info
    ,NULL as computer_name
    ,NULL AS comment
    ,NULL as parameter
    ,NULL as action
    ,NULL as type_of_attack
    ,NULL as target_user_name
    ,LatestProtocolID AS latest_protocol_id
    ,direction AS direction
    ,length AS bytes
    ,NULL AS resource
    ,NULL AS printer_name
    ,NULL AS document
    ,NULL AS printer_port
    ,NULL AS pages_printed
    ,NULL AS copies_printed
    ,NULL AS shadow_copy
    ,NULL AS wrong_user_pw
    ,NULL AS logon_mode
FROM [dbo].[Packets] where dateAndTime >= DATEADD(MINUTE, -5, GetDate())
UNION ALL

SELECT TOP 10000 'IPS_TRAFFIC' AS journal_name
    ,recID AS traffic_rec_id
    ,dateAndTime AS event_date
    ,clientName AS client_name
    ,mandatLevel AS mandat_level
    ,userName AS user_name
    ,result AS result
    ,processName AS process_name
    ,processID AS process_id
    ,NULL AS permit
    ,NULL AS event_on_connect
    ,NULL AS dns_name
    ,protocol AS protocol
    ,NULL AS local_address
    ,NULL AS local_port
```

```
    ,NULL AS remote_address
    ,NULL AS remote_port
    ,NULL AS in_bytes
    ,NULL AS out_bytes
    ,NULL AS rule_id
    ,AlarmLevel AS alarm_level
    ,ruleAction AS rule_action
    ,AddressType AS address_type
    ,SourceAddress AS src_address
    ,DestAddress AS dst_address
    ,SignatureNumber AS signature_number
    ,Info AS signature_info
    ,NULL AS computer_name
    ,comment AS comment
    ,NULL AS parameter
    ,NULL AS action
    ,NULL AS type_of_attack
    ,NULL as target_user_name
    ,NULL AS latest_protocol_id
    ,NULL AS direction
    ,NULL AS bytes
    ,NULL AS resource
    ,NULL AS printer_name
    ,NULL AS document
    ,NULL AS printer_port
    ,NULL AS pages_printed
    ,NULL AS copies_printed
    ,NULL AS shadow_copy
    ,NULL AS wrong_user_pw
    ,NULL AS logon_mode
FROM [dbo].[IPS_Traffic] where dateAndTime >= DATEADD(MINUTE, -5, GetDate())
UNION ALL

SELECT TOP 10000 'PROCESS' AS journal_name
    ,recID AS processes_rec_id
    ,dateAndTime AS event_date
    ,clientName AS client_name
    ,mandatLevel AS mandat_level
    ,userName AS user_name
    ,result AS result
    ,processName AS process_name
    ,processID AS process_id
    ,NULL AS permit
    ,NULL AS event_on_connect
    ,NULL AS dns_name
    ,NULL AS protocol
    ,NULL AS local_address
    ,NULL AS local_port
    ,NULL AS remote_address
    ,NULL AS remote_port
    ,NULL AS in_bytes
```

```
    ,NULL AS out_bytes
    ,NULL AS rule_id
    ,NULL AS alarm_level
    ,NULL AS rule_action
    ,NULL AS address_type
    ,NULL AS src_address
    ,NULL AS dst_address
    ,NULL AS signature_number
    ,NULL AS signature_info
    ,NULL AS computer_name
    ,NULL AS comment
    ,NULL AS parameter
    ,action AS action
    ,NULL AS type_of_attack
    ,NULL as target_user_name
    ,NULL AS latest_protocol_id
    ,NULL AS direction
    ,NULL AS bytes
    ,NULL AS resource
    ,NULL AS printer_name
    ,NULL AS document
    ,NULL AS printer_port
    ,NULL AS pages_printed
    ,NULL AS copies_printed
    ,NULL AS shadow_copy
    ,NULL AS wrong_user_pw
    ,NULL AS logon_mode
FROM [dbo].[Process] where dateAndTime >= DATEADD(MINUTE, -5, GetDate())
UNION ALL

SELECT TOP 10000 'IPS_APP_CTRL' AS journal_name
    ,recID AS app_ctrl_rec_id
    ,dateAndTime AS event_date
    ,clientName AS client_name
    ,mandatLevel AS mandat_level
    ,userName AS user_name
    ,result AS result
    ,processName AS process_name
    ,processID AS process_id
    ,permit AS permit
    ,NULL AS event_on_connect
    ,NULL AS dns_name
    ,NULL AS protocol
    ,NULL AS local_address
    ,NULL AS local_port
    ,NULL AS remote_address
    ,NULL AS remote_port
    ,NULL AS in_bytes
    ,NULL AS out_bytes
    ,NULL AS rule_id
    ,NULL AS alarm_level
```

```
    ,NULL AS rule_action
    ,NULL AS address_type
    ,NULL AS src_address
    ,NULL AS dst_address
    ,NULL AS signature_number
    ,NULL AS signature_info
    ,NULL AS computer_name
    ,comment AS comment
    ,NULL AS parameter
    ,NULL AS action
    ,TypeOfAttack AS type_of_attack
    ,NULL as target_user_name
    ,NULL AS latest_protocol_id
    ,NULL AS direction
    ,NULL AS bytes
    ,NULL AS resource
    ,NULL AS printer_name
    ,NULL AS document
    ,NULL AS printer_port
    ,NULL AS pages_printed
    ,NULL AS copies_printed
    ,NULL AS shadow_copy
    ,NULL AS wrong_user_pw
    ,NULL AS logon_mode
FROM [dbo].[IPS_App_Ctrl] where dateAndTime >= DATEADD(MINUTE, -5, GetDate())
UNION ALL

SELECT TOP 10000 'ACCOUNT' AS journal_id
    ,recID AS accounts_rec_id
    ,dateAndTime AS event_date
    ,clientName AS client_name
    ,mandatLevel AS mandat_level
    ,userName AS user_name
    ,result AS result
    ,NULL AS process_name
    ,NULL AS process_id
    ,NULL AS permit
    ,NULL AS event_on_connect
    ,NULL AS dns_name
    ,NULL AS protocol
    ,NULL AS local_address
    ,NULL AS local_port
    ,NULL AS remote_address
    ,NULL AS remote_port
    ,NULL AS in_bytes
    ,NULL AS out_bytes
    ,NULL AS rule_id
    ,NULL AS alarm_level
    ,NULL AS rule_action
    ,NULL AS address_type
    ,NULL AS src_address
```

```
    ,NULL AS dst_address
    ,NULL AS signature_number
    ,NULL AS signature_info
    ,computerName AS computer_name
    ,comment AS comment
    ,NULL AS parameter
    ,action AS action
    ,NULL AS type_of_attack
    ,targetUserName as target_user_name
    ,NULL AS latest_protocol_id
    ,NULL AS direction
    ,NULL AS bytes
    ,NULL AS resource
    ,NULL AS printer_name
    ,NULL AS document
    ,NULL AS printer_port
    ,NULL AS pages_printed
    ,NULL AS copies_printed
    ,NULL AS shadow_copy
    ,NULL AS wrong_user_pw
    ,NULL AS logon_mode
FROM [dbo].[Account] where dateAndTime >= DATEADD(MINUTE, -5, GetDate())
UNION ALL

SELECT TOP 10000 'POLICY' AS journal_name
    ,recID AS policies_rec_id
    ,dateAndTime AS event_date
    ,clientName AS client_name
    ,mandatLevel AS mandat_level
    ,userName AS user_name
    ,result AS result
    ,NULL AS process_name
    ,NULL AS process_id
    ,NULL AS permit
    ,NULL AS event_on_connect
    ,NULL AS dns_name
    ,NULL AS protocol
    ,NULL AS local_address
    ,NULL AS local_port
    ,NULL AS remote_address
    ,NULL AS remote_port
    ,NULL AS in_bytes
    ,NULL AS out_bytes
    ,NULL AS rule_id
    ,NULL AS alarm_level
    ,NULL AS rule_action
    ,NULL AS address_type
    ,NULL AS src_address
    ,NULL AS dst_address
    ,NULL AS signature_number
    ,NULL AS signature_info
```

```
    ,computerName AS computer_name
    ,comment AS comment
    ,parameter AS parameter
    ,action AS action
    ,NULL AS type_of_attack
    ,NULL as target_user_name
    ,NULL AS latest_protocol_id
    ,NULL AS direction
    ,NULL AS bytes
    ,NULL AS resource
    ,NULL AS printer_name
    ,NULL AS document
    ,NULL AS printer_port
    ,NULL AS pages_printed
    ,NULL AS copies_printed
    ,NULL AS shadow_copy
    ,NULL AS wrong_user_pw
    ,NULL AS logon_mode
FROM [dbo].[Policy] where dateAndTime >= DATEADD(MINUTE, -5, GetDate())
UNION ALL

SELECT TOP 10000 'ACCESS' AS journal_name
    ,recID AS access_rec_id
    ,dateAndTime AS event_date
    ,clientName AS client_name
    ,mandatLevel AS mandat_level
    ,userName AS user_name
    ,result AS result
    ,processName AS process_name
    ,NULL AS process_id
    ,NULL AS permit
    ,NULL AS event_on_connect
    ,NULL AS dns_name
    ,NULL AS protocol
    ,NULL AS local_address
    ,NULL AS local_port
    ,NULL AS remote_address
    ,NULL AS remote_port
    ,NULL AS in_bytes
    ,NULL AS out_bytes
    ,NULL AS rule_id
    ,NULL AS alarm_level
    ,NULL AS rule_action
    ,NULL AS address_type
    ,NULL AS src_address
    ,NULL AS dst_address
    ,NULL AS signature_number
    ,NULL AS signature_info
    ,computerName AS computer_name
    ,NULL AS comment
    ,NULL AS parameter
```

```
    ,action AS action
    ,NULL AS type_of_attack
    ,NULL as target_user_name
    ,NULL AS latest_protocol_id
    ,NULL AS direction
    ,NULL AS bytes
    ,resource AS resource
    ,NULL AS printer_name
    ,NULL AS document
    ,NULL AS printer_port
    ,NULL AS pages_printed
    ,NULL AS copies_printed
    ,shadowCopy AS shadow_copy
    ,NULL AS wrong_user_pw
    ,NULL AS logon_mode
FROM [dbo].[Access] where dateAndTime >= DATEADD(MINUTE, -5, GetDate())
UNION ALL

SELECT TOP 10000 'PRINT' AS journal_name
    ,recID AS print_rec_id
    ,dateAndTime AS event_date
    ,clientName AS client_name
    ,mandatLevel AS mandat_level
    ,userName AS user_name
    ,result AS result
    ,processName AS process_name
    ,NULL AS process_id
    ,NULL AS permit
    ,NULL AS event_on_connect
    ,NULL AS dns_name
    ,NULL AS protocol
    ,NULL AS local_address
    ,NULL AS local_port
    ,NULL AS remote_address
    ,NULL AS remote_port
    ,NULL AS in_bytes
    ,NULL AS out_bytes
    ,NULL AS rule_id
    ,NULL AS alarm_level
    ,NULL AS rule_action
    ,NULL AS address_type
    ,NULL AS src_address
    ,NULL AS dst_address
    ,NULL AS signature_number
    ,NULL AS signature_info
    ,computerName AS computer_name
    ,NULL AS comment
    ,NULL AS parameter
    ,NULL AS action
    ,NULL AS type_of_attack
    ,NULL as target_user_name
```

```
    ,NULL AS latest_protocol_id
    ,NULL AS direction
    ,NULL AS bytes
    ,NULL AS resource
    ,printerName AS printer_name
    ,document AS document
    ,port AS printer_port
    ,pagesPrinted AS pages_printed
    ,copies AS copies_printed
    ,shadowCopy AS shadow_copy
    ,NULL AS wrong_user_pw
    ,NULL AS logon_mode
FROM [dbo].[Printer] where dateAndTime >= DATEADD(MINUTE, -5, GetDate())
UNION ALL

SELECT TOP 10000 'LOGON' AS journal_name
    ,recID AS logon_rec_id
    ,dateAndTime AS event_date
    ,clientName AS client_name
    ,mandatLevel AS mandat_level
    ,userName AS user_name
    ,result AS result
    ,NULL AS process_name
    ,NULL AS process_id
    ,NULL AS permit
    ,NULL AS event_on_connect
    ,NULL AS dns_name
    ,NULL AS protocol
    ,NULL AS local_address
    ,NULL AS local_port
    ,NULL AS remote_address
    ,NULL AS remote_port
    ,NULL AS in_bytes
    ,NULL AS out_bytes
    ,NULL AS rule_id
    ,NULL AS alarm_level
    ,NULL AS rule_action
    ,NULL AS address_type
    ,NULL AS src_address
    ,NULL AS dst_address
    ,NULL AS signature_number
    ,NULL AS signature_info
    ,computerName AS computer_name
    ,NULL AS comment
    ,NULL AS parameter
    ,NULL AS action
    ,NULL AS type_of_attack
    ,NULL as target_user_name
    ,NULL AS latest_protocol_id
    ,NULL AS direction
    ,NULL AS bytes
```

```
    ,NULL AS resource
    ,NULL AS printer_name
    ,NULL AS document
    ,NULL AS printer_port
    ,NULL AS pages_printed
    ,NULL AS copies_printed
    ,NULL AS shadow_copy
    ,wrongUserPW AS wrong_user_pw
    ,logonMode AS logon_mode
FROM [dbo].[Logon] where dateAndTime >= DATEADD(MINUTE, -5, GetDate())
```

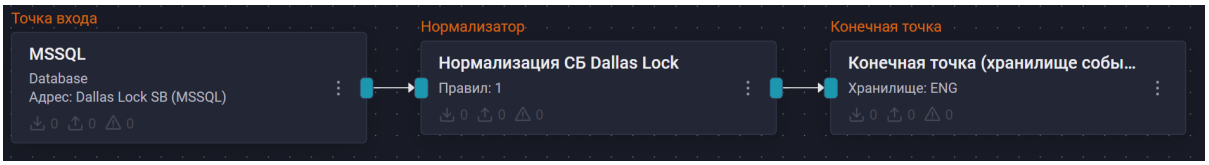


В представленном запросе из каждой таблицы собирается по 10000 событий. Если возникает проблема с выгрузкой событий, рекомендуется понизить количество событий, собираемых одним запросом.

- Поле идентификатора: заполнять не нужно.
- Интервал запроса, секунд: введите значение `120`.

4. Добавьте на конвейер элемент **Нормализатор** с правилом **Confident Dallas Lock SB** (идентификатор правила: **RV-N-290**).
5. Соедините нормализатор с точкой входа.
6. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
7. Соедините конечную точку с нормализатором.
8. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

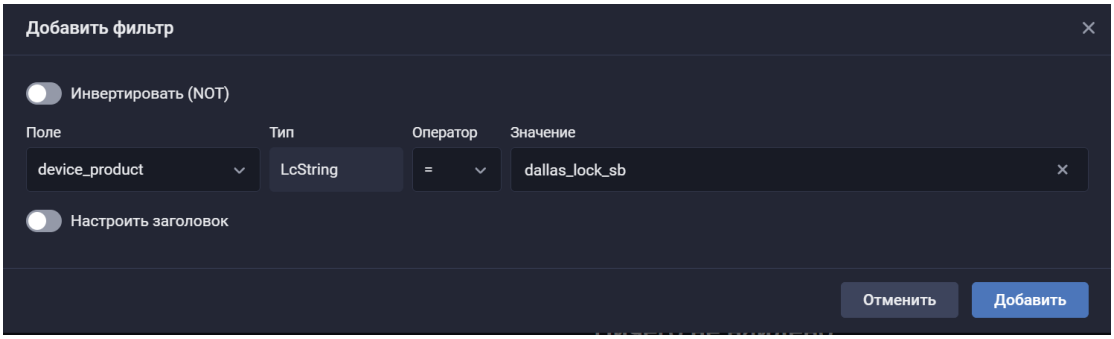


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Dallas Lock 8.0 Сервер Безопасности.



Найти события Dallas Lock 8.0 Сервер Безопасности в хранилище можно по следующему фильтру:

```
device_product = "dallas_lock_sb"
```



Dallas Lock 8.0: сбор событий в формате CEF

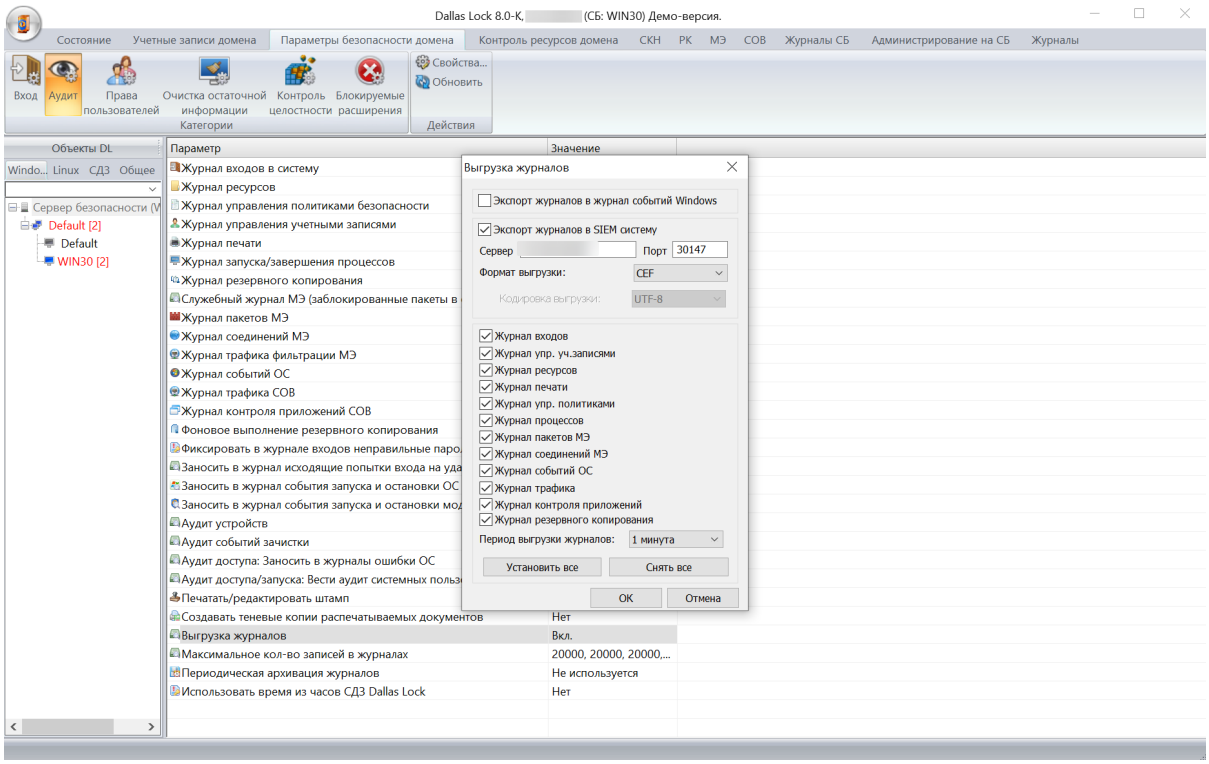
Данное руководство описывает процесс настройки сбора и отправки событий Dallas Lock 8.0 в R-Vision SIEM.

Настройка Dallas Lock 8.0

Настройка сбора событий Dallas Lock 8.0 Сервер Безопасности производится аналогично.

Для пересылки событий, зарегистрированных Dallas Lock 8.0, в R-Vision SIEM в формате CEF выполните следующие действия:

1. Войдите в веб-интерфейс **Dallas Lock 8.0**.
2. Откройте вкладку **Параметры безопасности домена**.
3. Нажмите на кнопку **Аудит**.
4. В открывшемся списке параметров выберите пункт **Выгрузка журналов**.
5. В появившемся окне настройте параметры выгрузки журналов:
   - Установите флажок **Экспорт журналов в SIEM систему**.
   - В поле **Сервер** укажите IP-адрес коллектора.
   - В поле **Порт** введите значение порта коллектора.
   - Выберите из выпающего списка **Формат выгрузки** вариант CEF.
   - Установите флажки напротив всех журналов.
   - Установите период выгрузки.



6. Нажмите на кнопку **OK**.

Настройка на стороне источника завершена.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

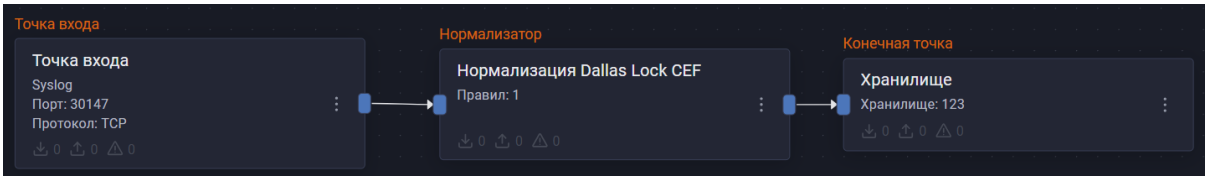
1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне Dallas Lock 8.0.
   - Протокол: выберите вариант в соответствии с настройками на стороне Dallas Lock 8.0.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Confident Dallas Lock syslog** (идентификатор правила: **RV-N-291**).



Правило **RV-N-291** также нормализует события, получаемые из ЕЦУ Dallas Lock в формате CEF.

4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

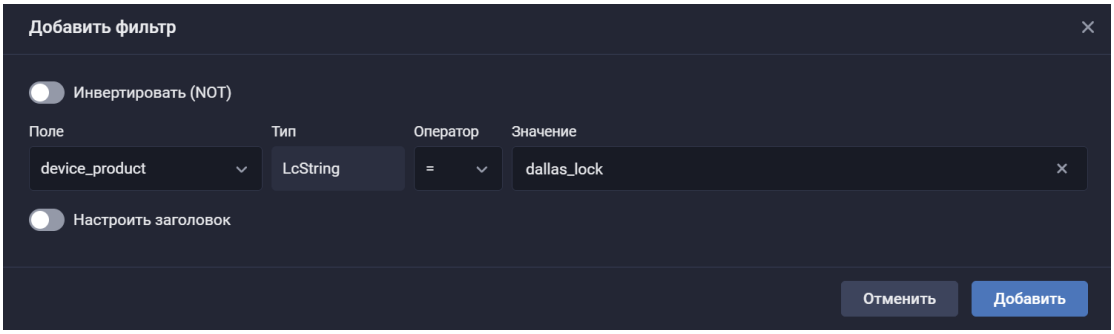
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Dallas Lock 8.0.

Найти события Dallas Lock 8.0 в хранилище можно по следующему фильтру:

```
dproduct = "Dallas Lock"
```



Microsoft Endpoint Configuration Manager (MECM)

- Microsoft Endpoint Configuration Manager: настройка источника

Microsoft Endpoint Configuration Manager: настройка источника

Данное руководство описывает процесс настройки сбора событий Microsoft ECM и их отправки в R-Vision SIEM.

Предварительные требования

Перед настройкой пересылки событий в R-Vision SIEM убедитесь в выполнении следующих условий:

- Сетевая доступность сервера СУБД источника по целевому порту и протоколу для каждой ноды кластера R-Vision SIEM.
- Учетная запись в СУБД с правами на чтение таблицы `dbo.Alert`.

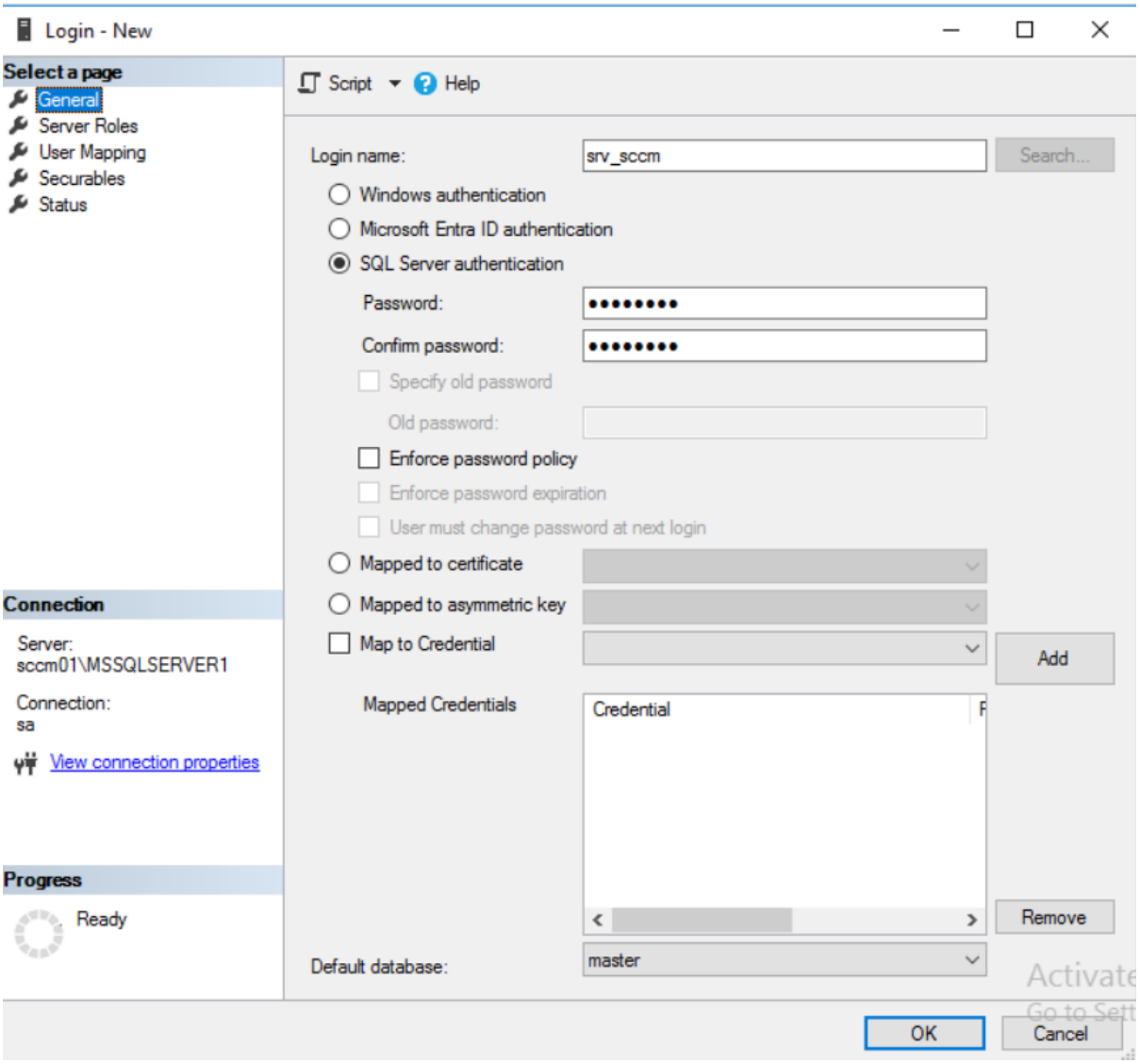
Настройка СУБД MS SQL

События Microsoft ECM записываются в таблицу `dbo.Alert` базы данных `CCM` СУБД MS SQL. Для настройки сбора логов из базы данных необходимо подключиться к ней с использованием сервисной учетной записи (далее — УЗ).

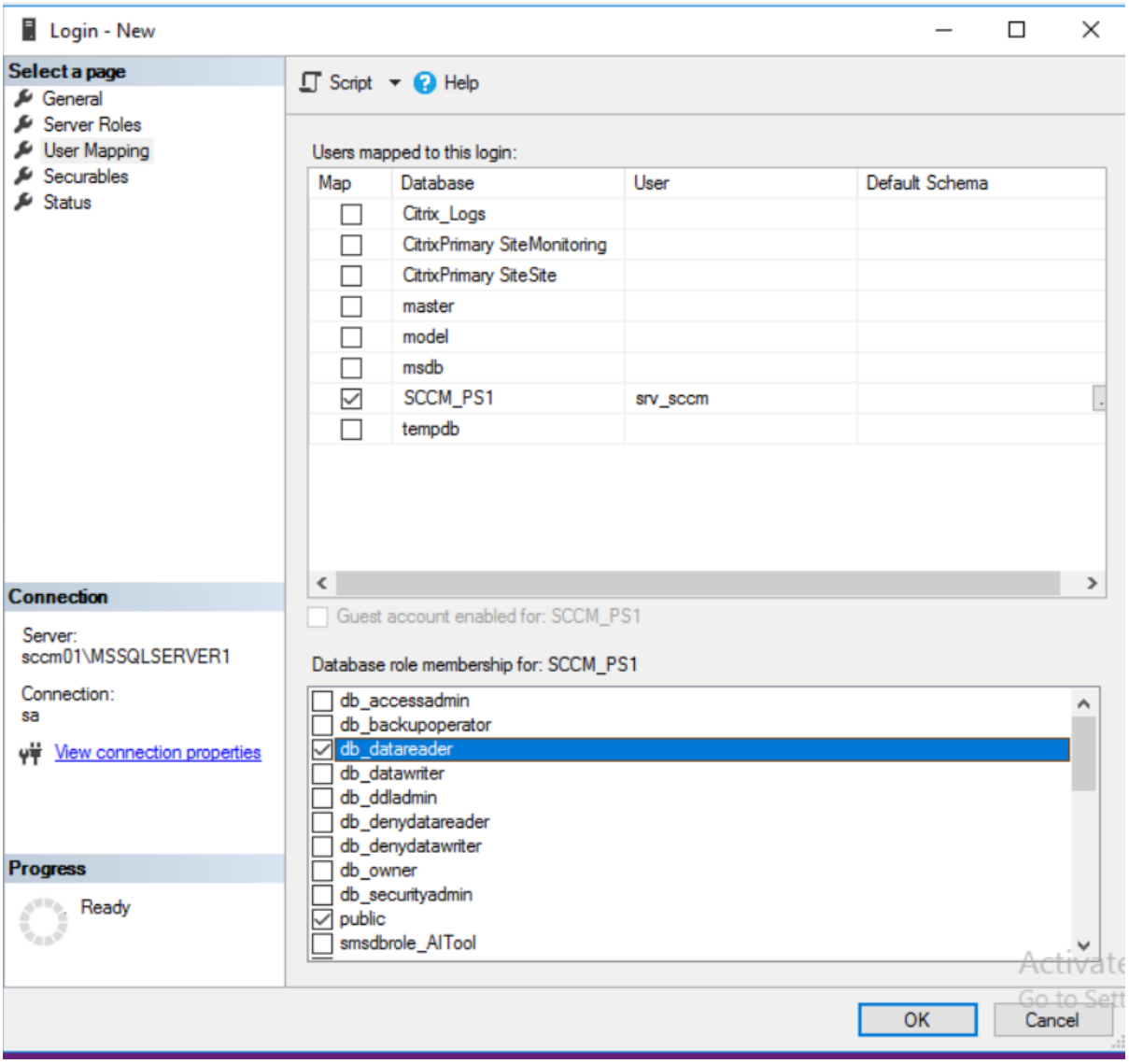
Создание учетной записи в СУБД MS SQL

Чтобы создать сервисную УЗ, подключитесь к СУБД с правами администратора. Для этого выполните следующие действия в SQL Server Management Studio:

1. Выберите **New Login** в контекстном меню для **Security/Logins**.
2. Создайте сервисную учетную запись.

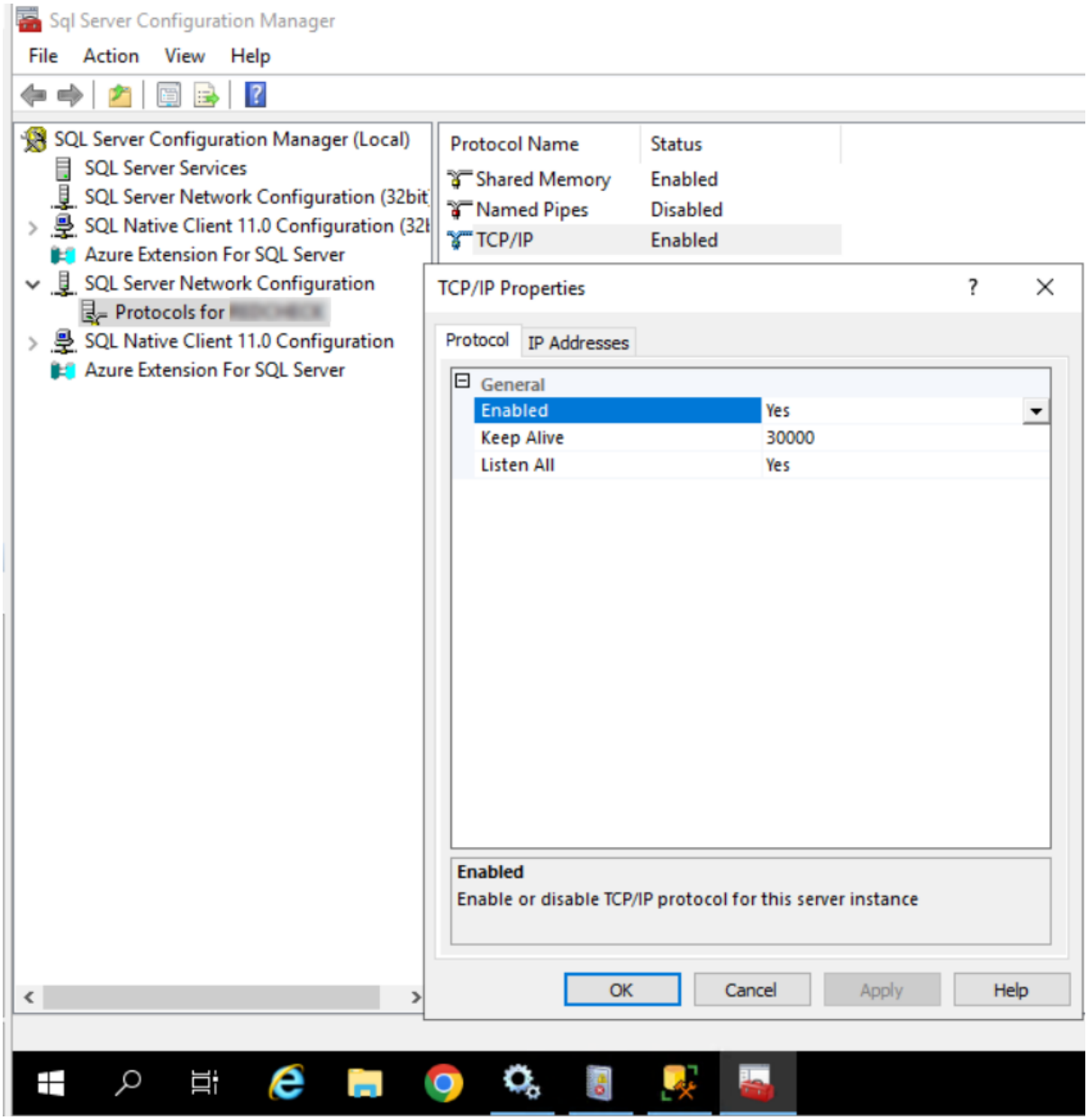


3. Предоставьте учетной записи права на чтение базы `CCM`.



Настройка сервера MS SQL

В настройках **SQL Server Configuration Manager** убедитесь, что `TCP/IP` включен в конфигурации сети SQL Server.



Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте секрет со строкой подключения. Для этого:
   a. Перейдите в раздел **Ресурсы** → **Секреты** → **Создать**.
   b. В раскрывшемся окне создания секрета заполните поля:
      - **Название**: введите название секрета.
      - **Описание** (опционально): опишите, для чего будет использоваться секрет.
      - **Тип секрета**: выберите вариант **Строка подключения**.
      - **Строка подключения**: введите строку вида:

```
jdbc:sqlserver://<DB_SERVER>\<DB_INSTANCE>:<DB_PORT>;encrypt=false;databaseName=<DB_NAME>;user=<DB_USER>;password=<DB_PASSWORD>
```

Здесь:

- `<DB_SERVER>`: IP адрес инстанса СУБД.
- `<DB_INSTANCE>`: название инстанса СУБД.
- `<DB_PORT>`: порт инстанса СУБД (для MS SQL стандартный порт `1433`).
- `<DB_INSTANCE>`: название инстанса СУБД.
- `<DB_NAME>`: имя базы, используемой продуктом ECM.
- `<DB_USER>`: системный аккаунт с правами на чтение.
- `<DB_PASSWORD>`: пароль системного аккаунта.

c. Нажмите на кнопку **Создать**.

2. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
3. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Database**.
   - Драйвер базы данных: выберите вариант **MS SQL**.
   - Адрес подключения: выберите секрет, созданный ранее.
   - SQL-запрос: введите запрос вида:

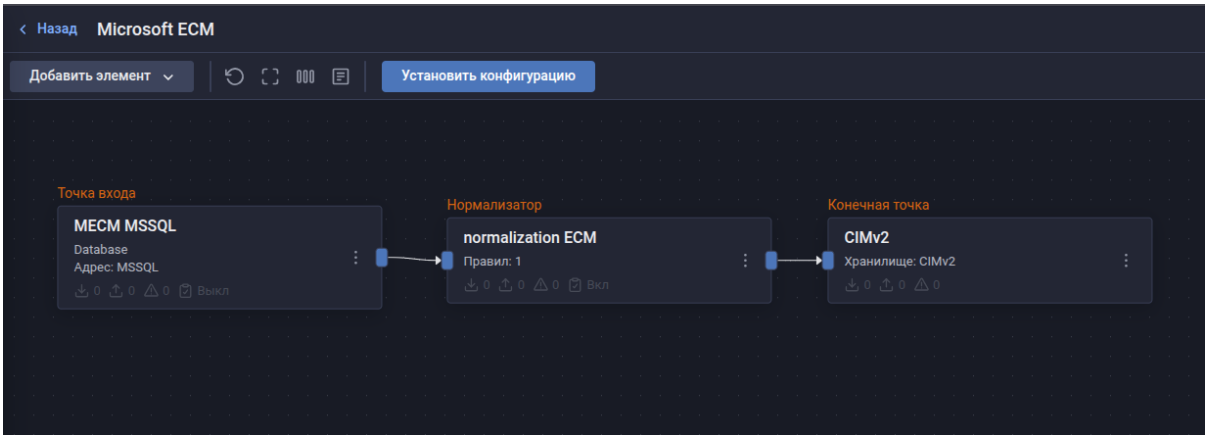
```
SELECT @@SERVERNAME AS hostname, 'ecm' AS appname, ac.Name AS className,
al.AlertID AS alertId, al.TypeID, al.Name AS alertName, al.Severity,
al.CreatedBy, al.CreationTime, al.ModifiedBy, al.ClosedBy FROM dbo.Alert al JOIN
dbo.AlertClass ac ON ac.TypeID = al.TypeID WHERE alertId > ? ORDER BY al.AlertID
ASC;
```



При большом количестве событий в СУБД рекомендуется добавлять `TOP 10000` в начало SQL-запроса.

   - Поле идентификатора: введите ключ `alertId` со значением `1`.
   - Интервал запроса, секунд: введите значение `15`.
4. Добавьте на конвейер элемент **Нормализатор** с правилом **Microsoft ECM** (идентификатор правила: **RV-N-325**).
5. Соедините нормализатор с точкой входа.
6. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
7. Соедините конечную точку с нормализатором.
8. Сохраните и установите конфигурацию конвейера.

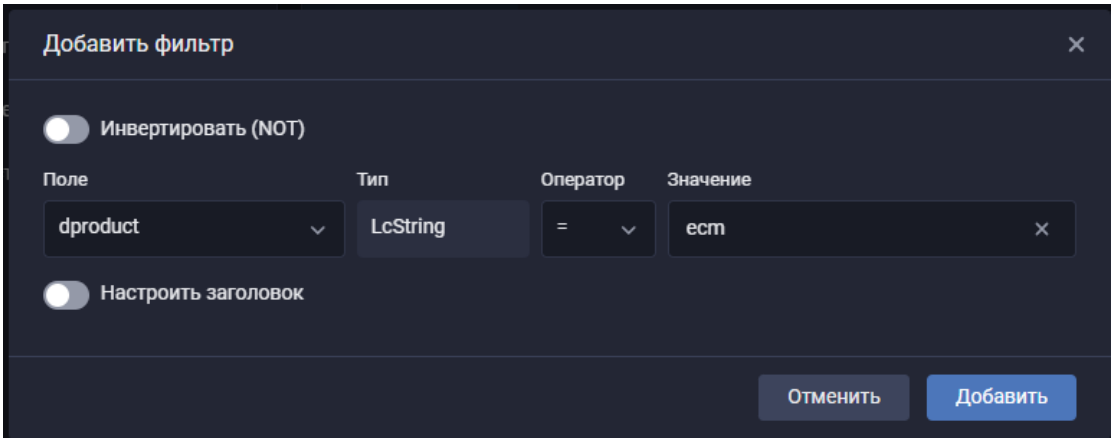
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать уведомления консоли ECM.

Найти события Microsoft ECM в хранилище можно по следующему фильтру:

```
device_product = "ecm"
```



Код Безопасности Secret Net Studio

- Код Безопасности Secret Net Studio: настройка источника
- Код Безопасности Secret Net Studio: правила корреляции

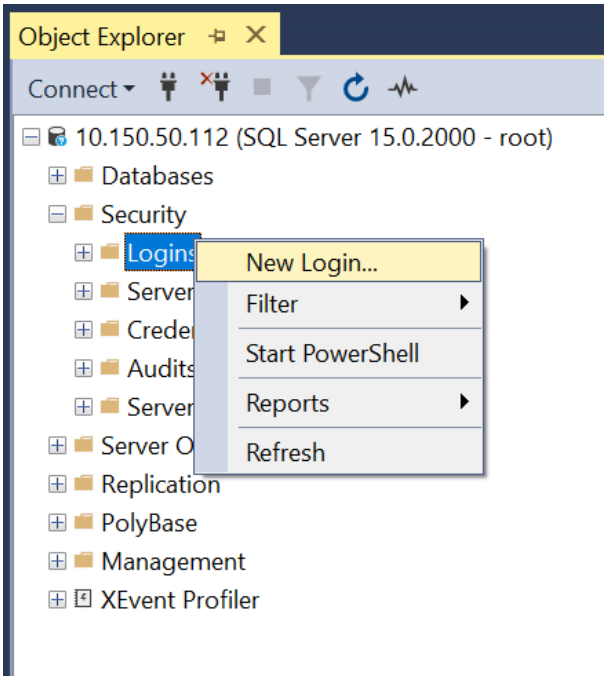
Код Безопасности Secret Net Studio: настройка источника

Secret Net Studio — это средство защиты информации от несанкционированного доступа, выполняющее функции контроля конфиденциальности, целостности и доступа к информации на рабочих станциях.

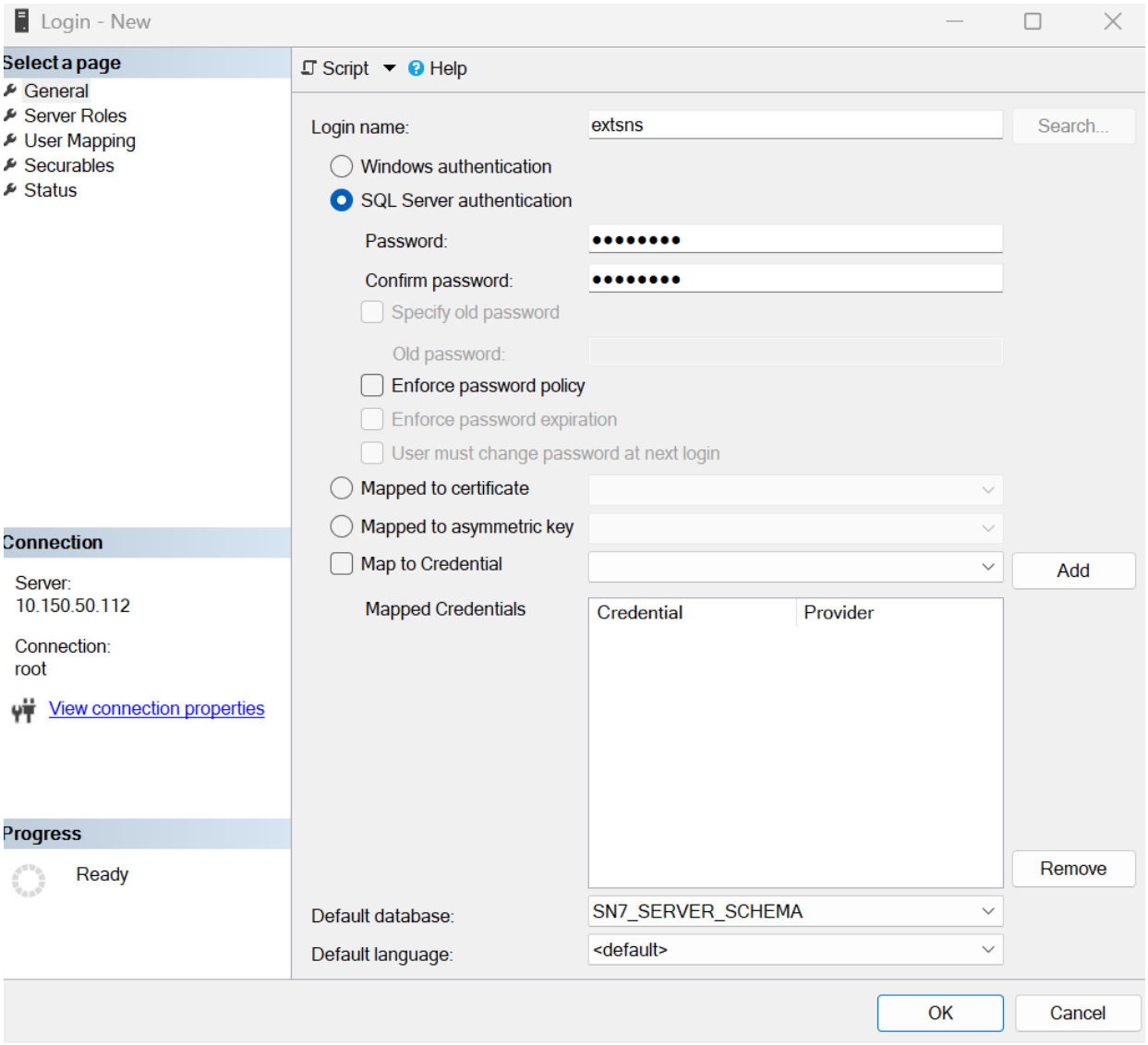
Настройка СУБД MS SQL

Для создания сервисной УЗ необходимо подключиться к СУБД посредством SQL Server Management Studio под административной УЗ.

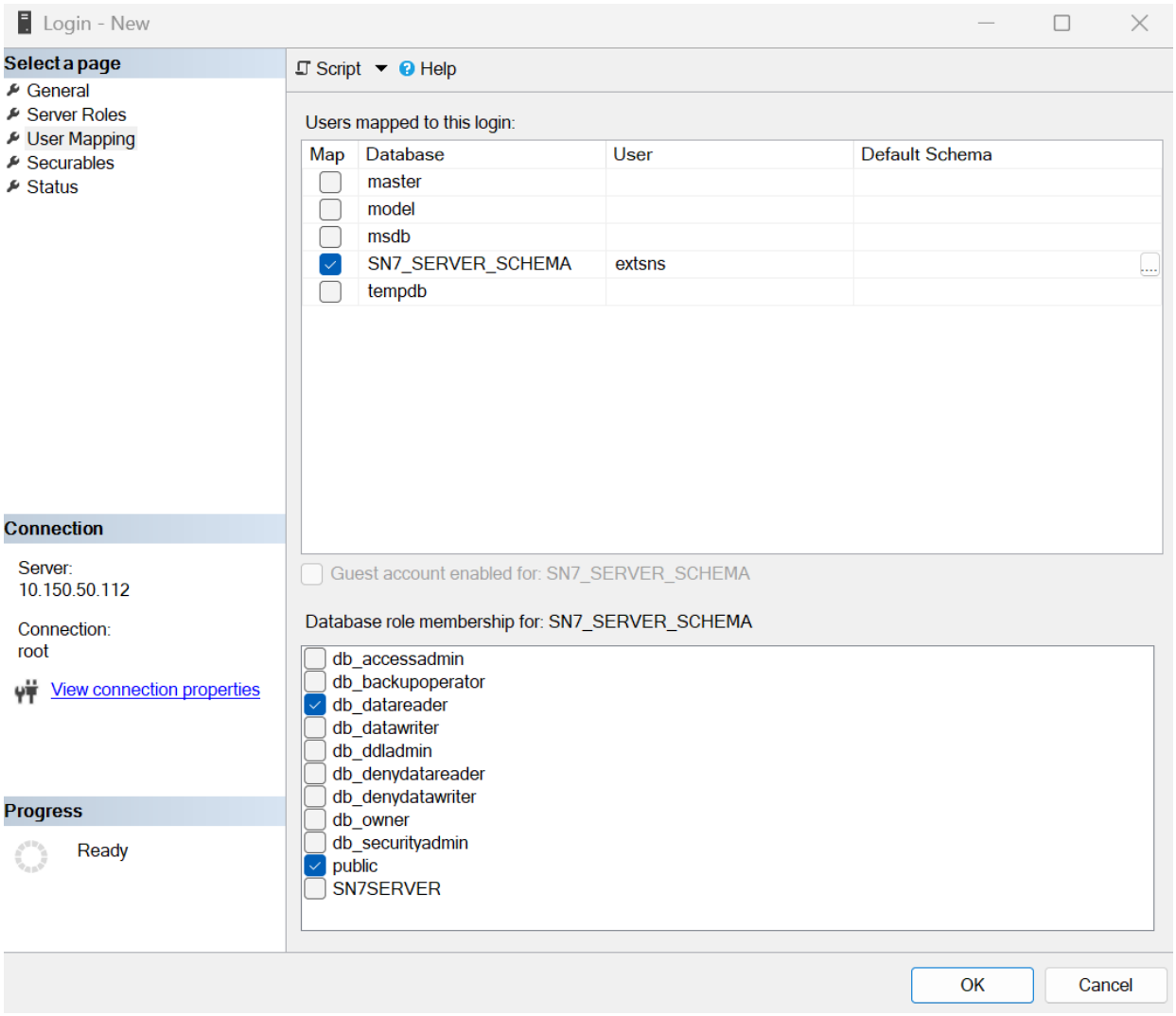
1. Откройте контекстное меню для **Security** → **Logins** и выберите опцию **New Login**.



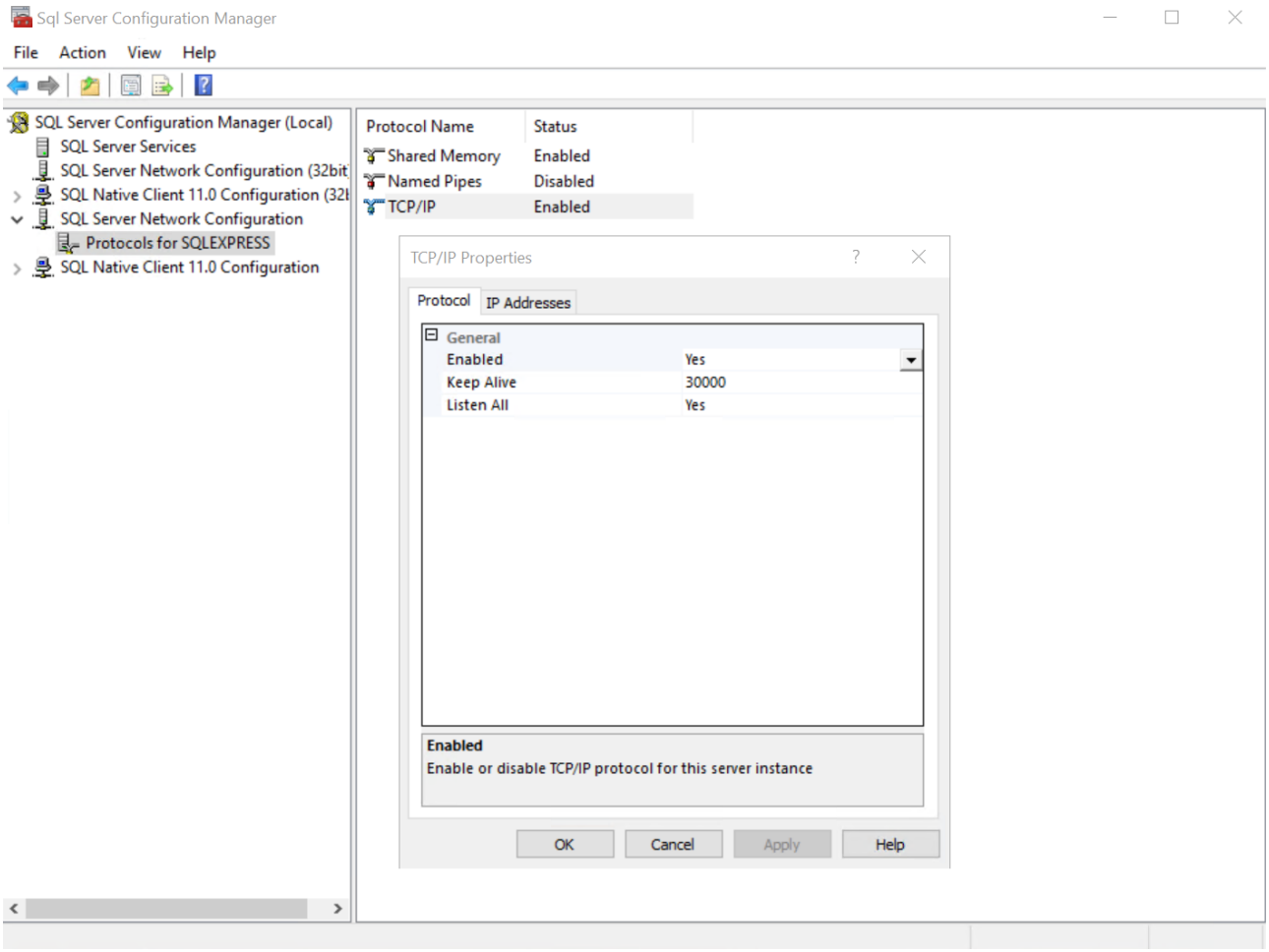
2. В разделе **General** создайте сервисную УЗ со следующими параметрами:
   - В поле **Login name** введите название учетной записи.
   - Выберите вариант **SQL Server authentication**.
   - В поле **Default database** выберите из выпадающего списка базу данных Secret Net Studio.



3. Перейдите в раздел **User Mapping**.
   - Установите флажок напротив базы данных Secret Net Studio.
   - Выберите для пользователя роли **db_datareader** и **public**.



4. В настройках **SQL Server Configuration Manager** убедитесь, что протокол **TCP/IP** включен в конфигурации сети SQL Server.

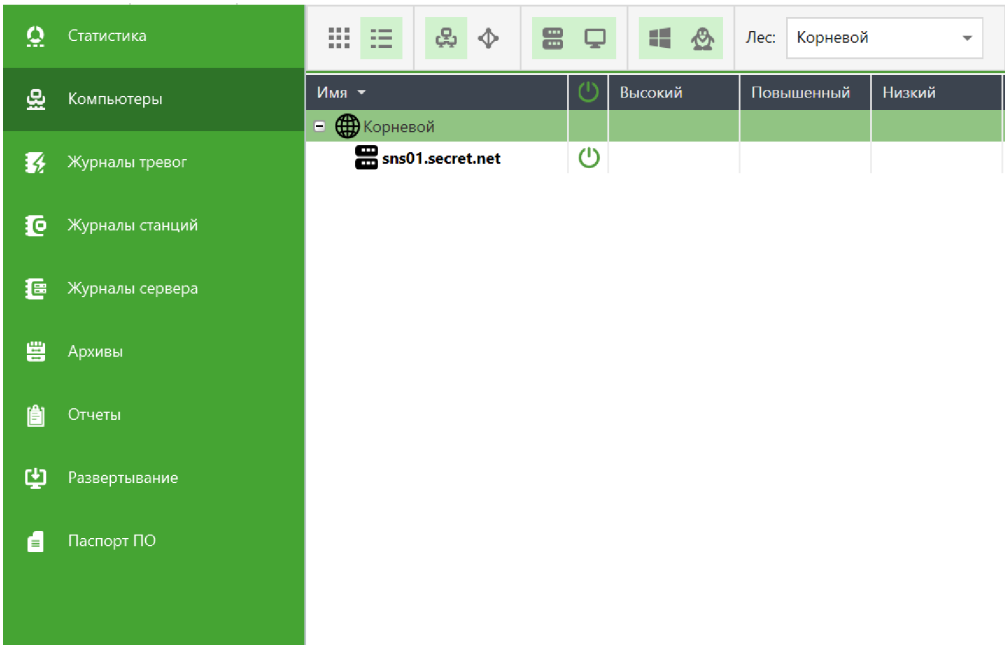


Настройка СУБД MS SQL завершена.

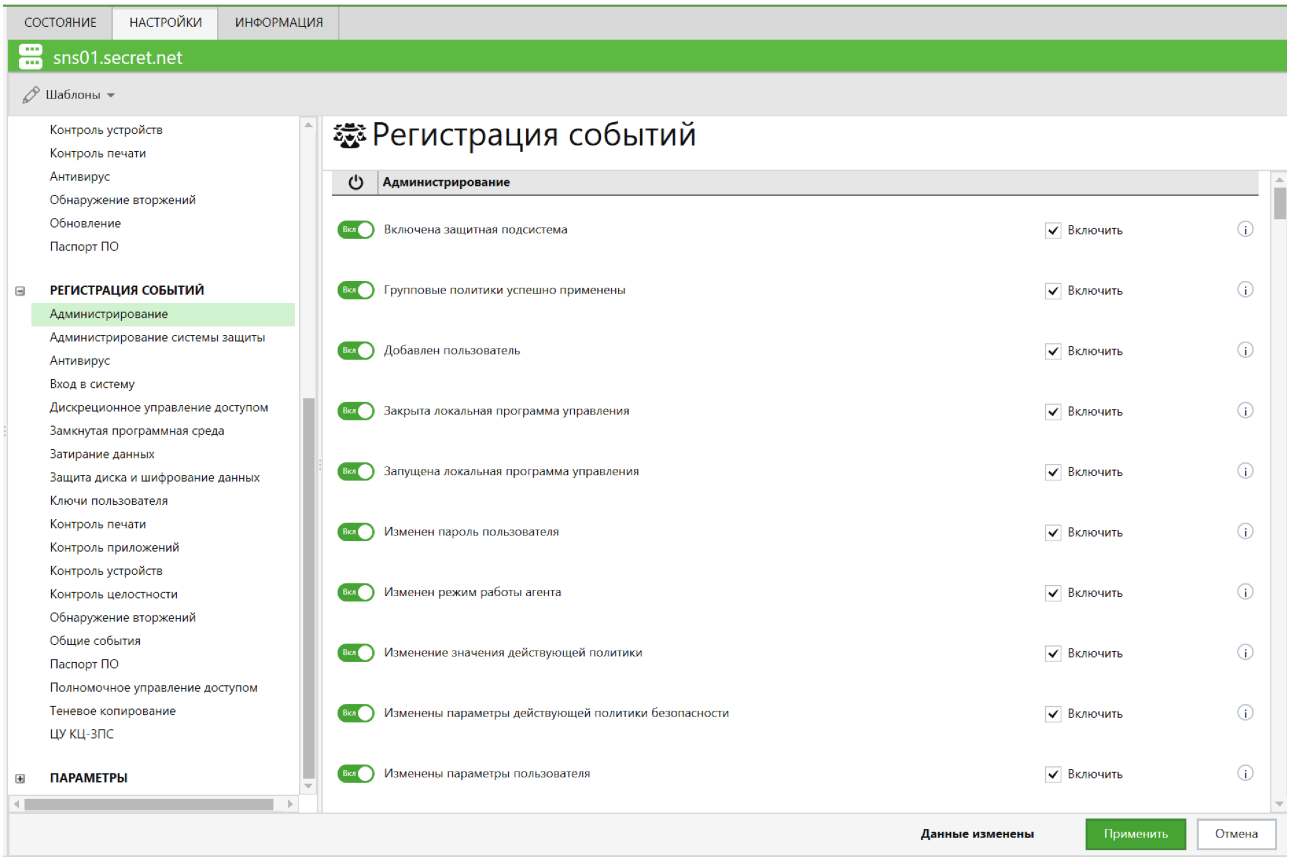
Настройка Secret Net Studio

Для настройки источника выполните следующие шаги:

1. Запустите **Центр управления Secret Net Studio**.
2. В главном меню выберите вкладку **Компьютеры**.



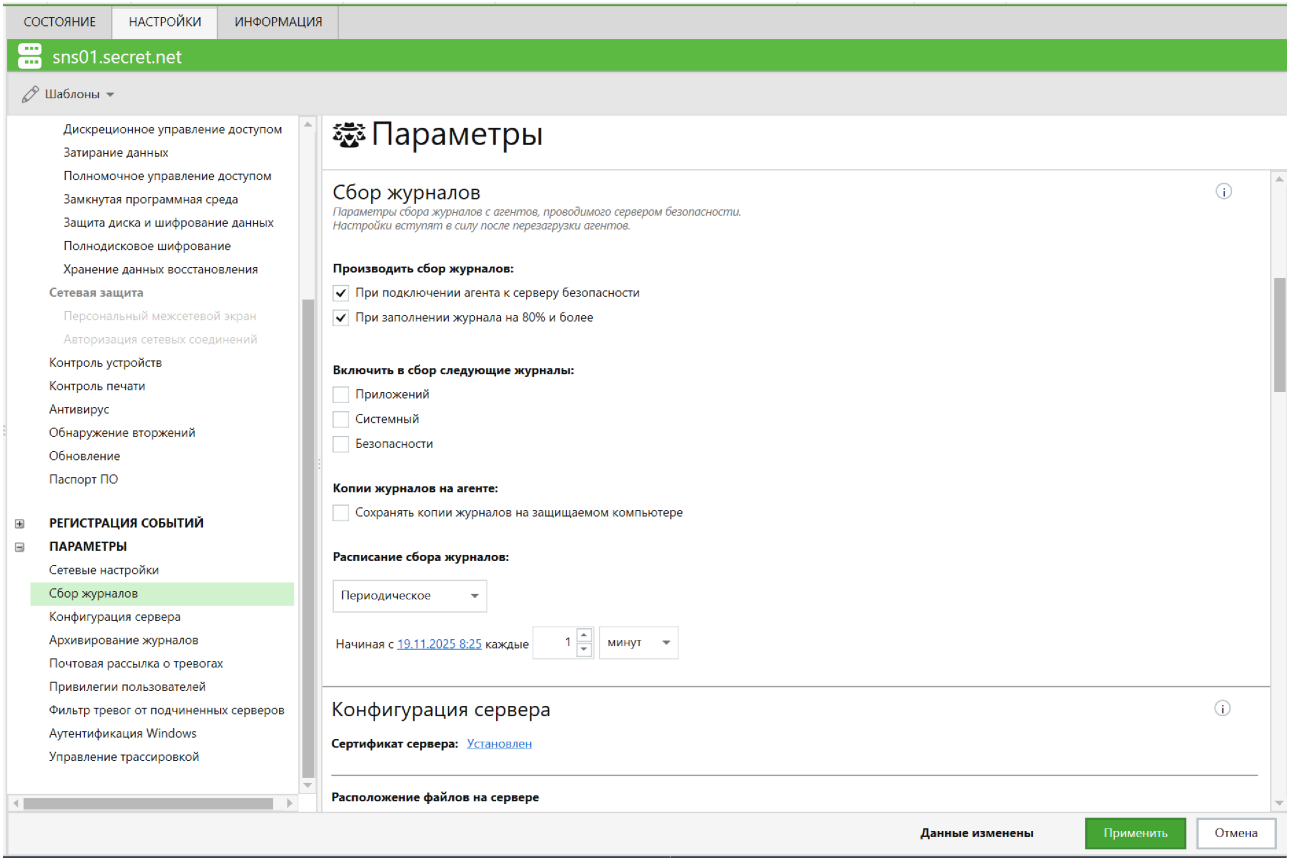
3. В открывшемся окне выберите узел или группу узлов для настройки.
4. Откройте вкладку **Настройки**.
5. Выберите из списка раздел **Регистрация событий**.



6. Включите типы событий, необходимые для журналирования.

> Рекомендуется включить журналирование для всех типов событий, кроме **Запуск процесса** и **Завершение процесса** в категории **Контроль приложений**.

7. Перейдите в раздел **Параметры** → **Сбор журналов**.
8. В параметре **Производить сбор журналов** установите флажки напротив следующих пунктов:
   - **При подключении агента к серверу безопасности**;
   - **При заполнении журнала на 80% и более**.
9. В параметре **Включить в сбор следующие журналы** снимите флажки напротив следующих пунктов:
   - **Приложений**;
   - **Системный**;
   - **Безопасности**.
10. Выберите из выпадающего списка **Расписание сбора журналов** вариант **Периодическое**.
11. Укажите интервал в одну минуту.



12. Нажмите на кнопку **Применить**.

Настройка в R-Vision SIEM

Для настройки сбора событий безопасности для защищаемых АРМ и сбора событий аудита сервера безопасности Secret Net Studio в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте секрет со строкой подключения. Для этого:
   a. Перейдите в раздел **Ресурсы** → **Секреты**.
   b. Нажмите на кнопку **Создать** (+).
   c. В раскрывшемся окне создания секрета заполните поля:
      - Название: введите название секрета.
      - Описание (опционально): опишите, для чего будет использоваться секрет.
      - Тип секрета: выберите вариант **Строка подключения**.
      - Строка подключения: введите строку вида:

```
jdbc:sqlserver://DBSERVER:1433;encrypt=false;databaseName=SN7_SERVER_SCHEMA;
user=reader;password=passw0rd
```

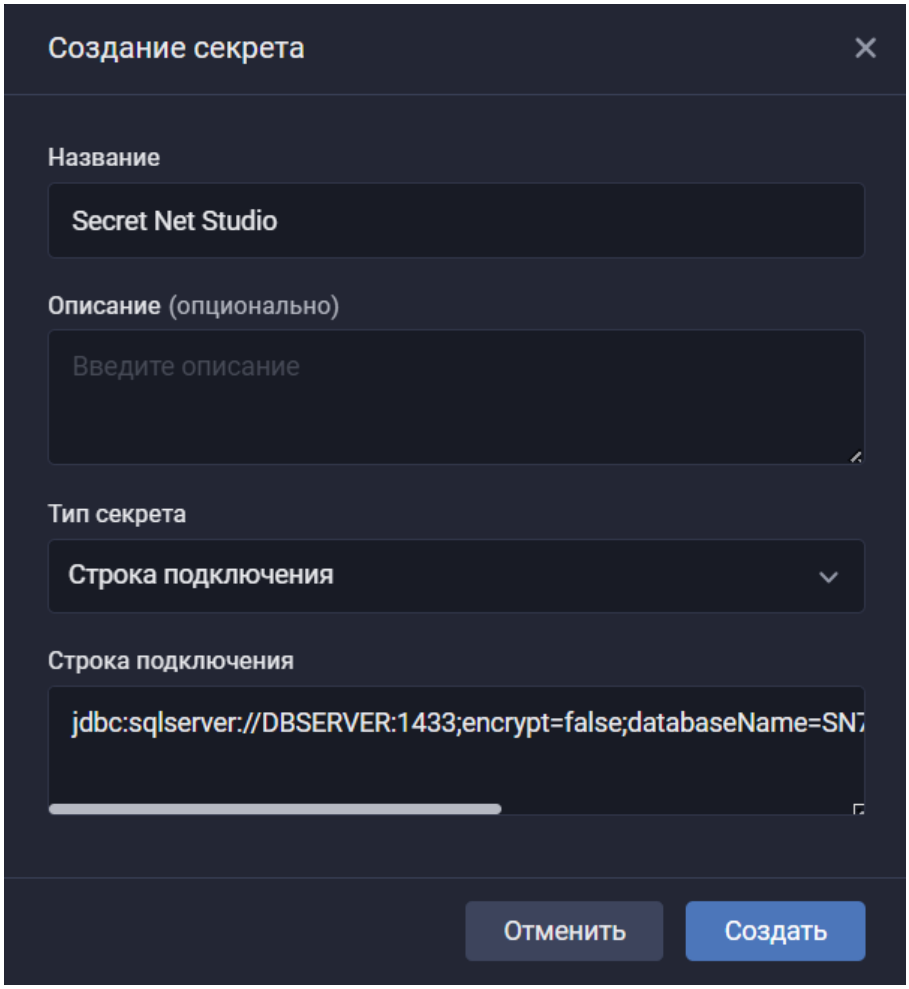
Строка подключения в секрете в случае использования доменной учетной записи:

```
jdbc:sqlserver://DBSERVER:1433;encrypt=false;databaseName=SN7_SERVER_SCHEMA;
authenticationScheme=NTLM;integratedSecurity=true;user=srv_sns;password=pass
```

```
w0rd
```

Здесь:

- DBSERVER — FQDN или IP-адрес сервера СУБД.
- 1433 — порт подключения.



d. Нажмите на кнопку **Создать**.

2. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
3. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Database**.
   - Драйвер базы данных: выберите вариант **MS SQL**.
   - Адрес подключения: выберите секрет, созданный ранее.
   - SQL-запрос: введите запрос вида:

```
SELECT
    EventLogRecID as event_id,
    DATEADD (
        hour,
        DATEDIFF (hour, GETUTCDATE (), GETDATE ()),
```

```
        TimeWritten
    ) as rt,
    Version as dversion,
    EventCategory as deviceEventClassId,
    CategoryMessage as cat,
    EventMessage as msg,
    TypeDescription as facillity,
    SourceName as destinationServiceName,
    Computername as shost,
    Msid as machineid,
    UserSid as suid,
    UserName as suser,
    UserDomainName as sntdom,
    ThreatLevel as severity,
    LogName as dproduct,
    replace(@@SERVERNAME,@@SERVICENAME, '') + DEFAULT_DOMAIN() as dvchost
,
    CONNECTIONPROPERTY ('local_net_address') AS dvc,
    'SNS security events' as EventFilter
FROM
    SN7_SERVER_SCHEMA.dbo.EventLogRec as ev
    LEFT JOIN dbo.EventLog as evlog ON ev.EventLogType = evlog.LogType
    LEFT JOIN dbo.Client as clients ON ev.ClientId = clients.ClientID
WHERE
    EVENTLOGTYPE = 4
    AND EVENTLOGRECID > ?
```

- Поле идентификатора: введите ключ `event_id` со значением `1`.
- Интервал запроса, секунд: введите значение `60`.

4. Добавьте на конвейер второй элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Database**.
   - Драйвер базы данных: выберите вариант **MS SQL**.
   - Адрес подключения: выберите секрет, созданный ранее.
   - SQL-запрос: введите запрос вида:

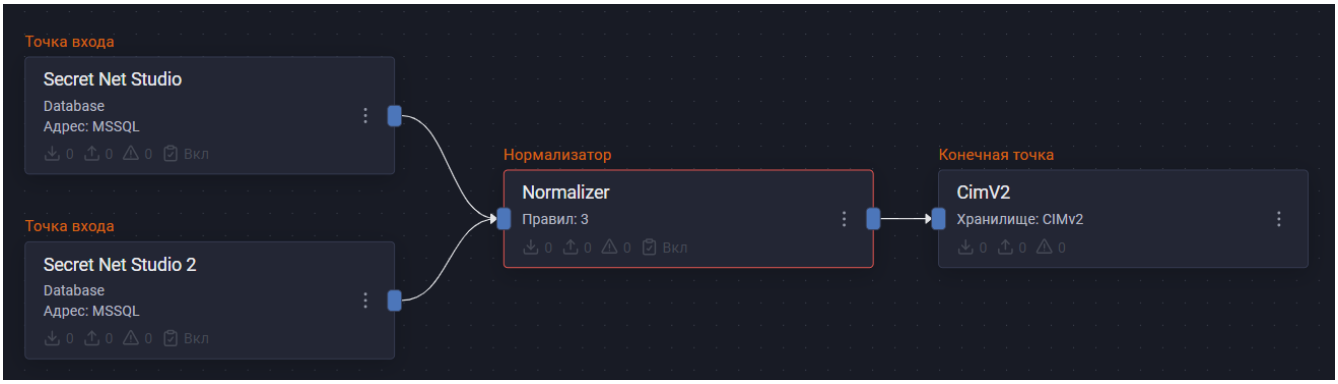
```
SELECT
    ClientClass,
    ClientType,
    MName,
    MSid,
    UName,
    USid,
    DATEADD (
        hour,
        DATEDIFF (hour, GETUTCDATE (), GETDATE ()),
        DateStart
```

```
    ) as DateStart,
    DATEADD (
        hour,
        DATEDIFF (hour, GETUTCDATE (), GETDATE ()),
        DateEnd
    ) as DateEnd,
    ExitCode,
    SessionGUID,
    ActionCode,
    TemplateCode,
    DATEADD (
        hour,
        DATEDIFF (hour, GETUTCDATE (), GETDATE ()),
        ActionTime
    ) as ActionTime,
    ActionParameters as msg,
    ResultCode,
    ClientSessionID,
    SessionActionID,
    GETDATE () as rt,
    replace(@@SERVERNAME,@@SERVICENAME, '') + DEFAULT_DOMAIN() as dvchost
,
    CONNECTIONPROPERTY ('local_net_address') AS dvc,
    'SNS audit events' as EventFilter
FROM
    SN7_SERVER_SCHEMA.dbo.ServerLog
where
    (
        DATEADD (
            hour,
            DATEDIFF (hour, GETUTCDATE (), GETDATE ()),
            ActionTime
        ) >= DATEADD (SECOND, -15, GetDate ())
    )
```

- Поле идентификатора: заполнять не нужно.
- Интервал запроса, секунд: введите значение 15.

5. Добавьте на конвейер элемент **Нормализатор** со следующими правилами:
   - **Код безопасности Secret Net Studio события аудита с сервера безопасности** (идентификаторы правил: **RV-N-109**, **RV-N-201**);
   - **Код безопасности Secret Net Studio события безопасности с защищенных АРМ** (идентификатор правила: **RV-N-202**).
6. Соедините нормализатор с точками входа.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

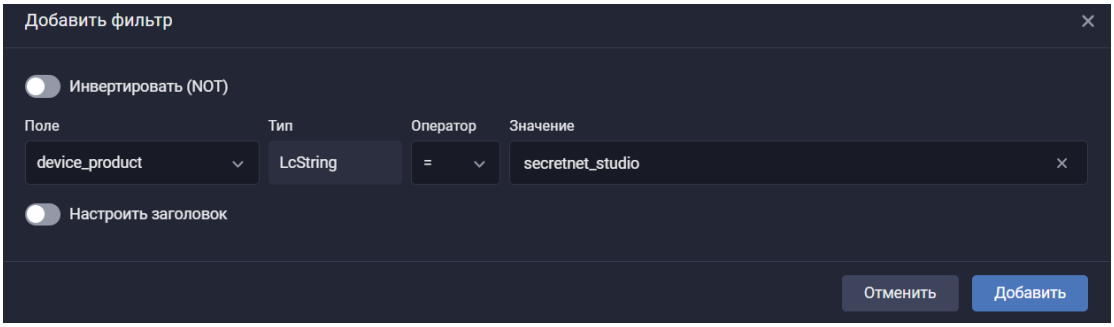
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Secret Net Studio.

Найти события Secret Net Studio в хранилище можно по следующему фильтру:

```
device_product = "secretnet_studio"
```



Код Безопасности Secret Net Studio: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-847d6ab7be99	Нарушение целостности объекта системы	Механизм контроля целостности осуществляет слежение за неизменностью контролируемых объектов (файлов, каталогов, элементов системного реестра). Правило регистрирует корреляционное событие при внесении изменений в контролируемый объект или его удалении.	• Impact (TA0040) • Data Manipulation (T1565) • Stored Data Manipulation (T1565.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1415	Подключено съемное устройство к компьютеру	Одной из функций механизма контроля подключения и изменения устройств в Secret Net Studio является поддержание в актуальном состоянии списка устройств компьютера. Правило обнаруживает подключение нового устройства и регистрирует корреляционное событие.	• Collection (TA0009) • Data from Removable Media (T1025)
RV-D-1416	Изменение политики безопасности Secret Net Studio	Изменение действующей политики осуществляется администратором локально или централизованно через центр управления. Правило обнаруживает изменения в действующей политике безопасности Secret Net Studio и регистрирует корреляционное событие.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)
RV-D-1417	Очищен журнал событий Secret Net Studio	Атакующий, с целью сокрытия следов присутствия в инфраструктуре и затруднения последующего расследования, может очистить журналы событий. Правило обнаруживает факт очистки журнала пользователем.	• Defense Evasion (TA0005) • Indicator Removal (T1070) • Clear Persistence (T1070.009)
RV-D-1422	Отключение механизма самозащиты в Secret Net Studio	Отключение механизма самозащиты может позволить атакующему произвести несанкционированную остановку или модификацию критических служб, процессов и механизмов защиты.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1423	Отключение защитного механизма в Secret Net Studio	Механизмы защиты осуществляют различные функции по защите от несанкционированного доступа к ресурсам хоста, на котором установлен Secret Net Studio. При их отключении может значительно снизиться уровень защищенности узла. Правило обнаруживает факт отключения защитного механизма.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)
RV-D-1424	Изменение правил межсетевого экрана в Secret Net Studio	Изменение или удаление правил межсетевого экранирования может расширить поверхность атаки для атакующего, а также ограничить легитимный доступ для администраторов к консоли управления. Правило обнаруживает добавление, удаление или изменение правил межсетевого экрана.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify System Firewall (T1562.004)
RV-D-1426	Многократная смена пароля учетной записи	Многократная смена пароля учетной записи в течение короткого промежутка времени является признаком аномального поведения пользователя. Правило обнаруживает аномальное поведение на основе событий изменения пароля и создает корреляционное событие после нескольких таких попыток.	• Persistence (TA0003) • Impact (TA0040) • Account Manipulation (T1098) • Account Access Removal (T1531)
RV-D-1431	Массовая блокировка узлов Secret Net Studio	Блокировка узлов Secret Net Studio может осуществляться вручную администратором или на основании нарушений, выявленных механизмом контроля целостности. Правило обнаруживает множественную блокировку узлов в сети и регистрирует корреляционное событие.	• Impact (TA0040) • Endpoint Denial of Service (T1499)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1432	Массовая разблокировка узлов Secret Net Studio	Разблокировка узлов Secret Net Studio может осуществляться администратором локально или через центр управления. После разблокирования узла снимаются ограничения на вход. Правило обнаруживает множественное разблокирование узлов в сети и регистрирует корреляционное событие.	• Defense Evasion (TA0005) • Exploitation for Defense Evasion (T1211)
RV-D-1434	Вход пользователя из черного списка	Правило обнаруживает вход в систему пользователя из черного списка (активного списка secretnet_significant_users), содержащего учетные записи, под которыми запрещен вход на устройство с установленным средством защиты информации Secret Net Studio.	• Initial Access (TA0001) • Defense Evasion (TA0005) • Valid Accounts (T1078)
RV-D-1435	Изменение критически важной учетной записи	При изменении параметров пользователя можно расширить или ограничить доступ к конфиденциальным ресурсам. Правило обнаруживает изменение параметров критически важных пользователей, включенных в активный список `privileged_users_and_hosts`.	• Impact (TA0040) • Account Manipulation (T1098) • Account Access Removal (T1531)

Системы защиты сети

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых систем защиты сети:

- z_infotecs-vipnet-tias.pdf

z_infotecs-vipnet-tias.adoc

z_infotecs-vipnet-tias-guide.adoc

Системы идентификации и управления доступом

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых систем идентификации и управления доступом:

- Microsoft Active Directory Federation Services (ADFS)
- Multifactor Radius Adapter

Microsoft Active Directory Federation Services (ADFS)

- Microsoft Active Directory Federation Services (ADFS): настройка источника
- Microsoft Active Directory Federation Services (ADFS): правила корреляции

Microsoft Active Directory Federation Services (ADFS): настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Microsoft Active Directory Federation Services (AD FS) в R-Vision SIEM с помощью агента R-Vision Endpoint.

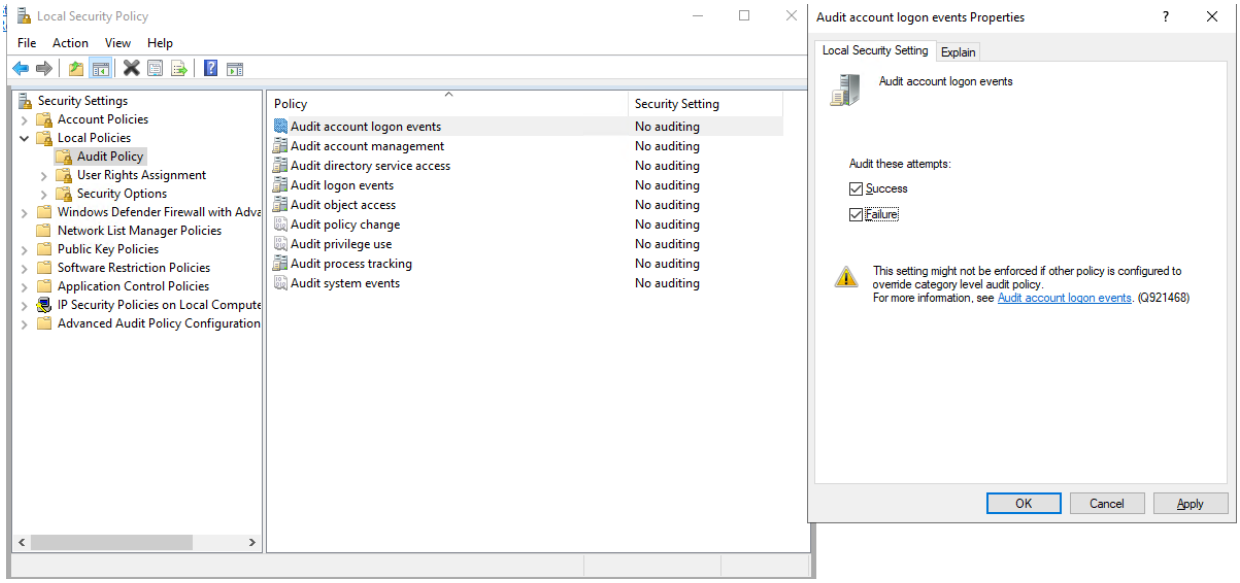
Настройка AD FS

Настройка сбора событий журнала AD FS с помощью агента R-Vision Endpoint включает в себя:

- настройку журналирования AD FS;
- установку агента R-Vision Endpoint на конечную точку.

Настройка журналирования AD FS

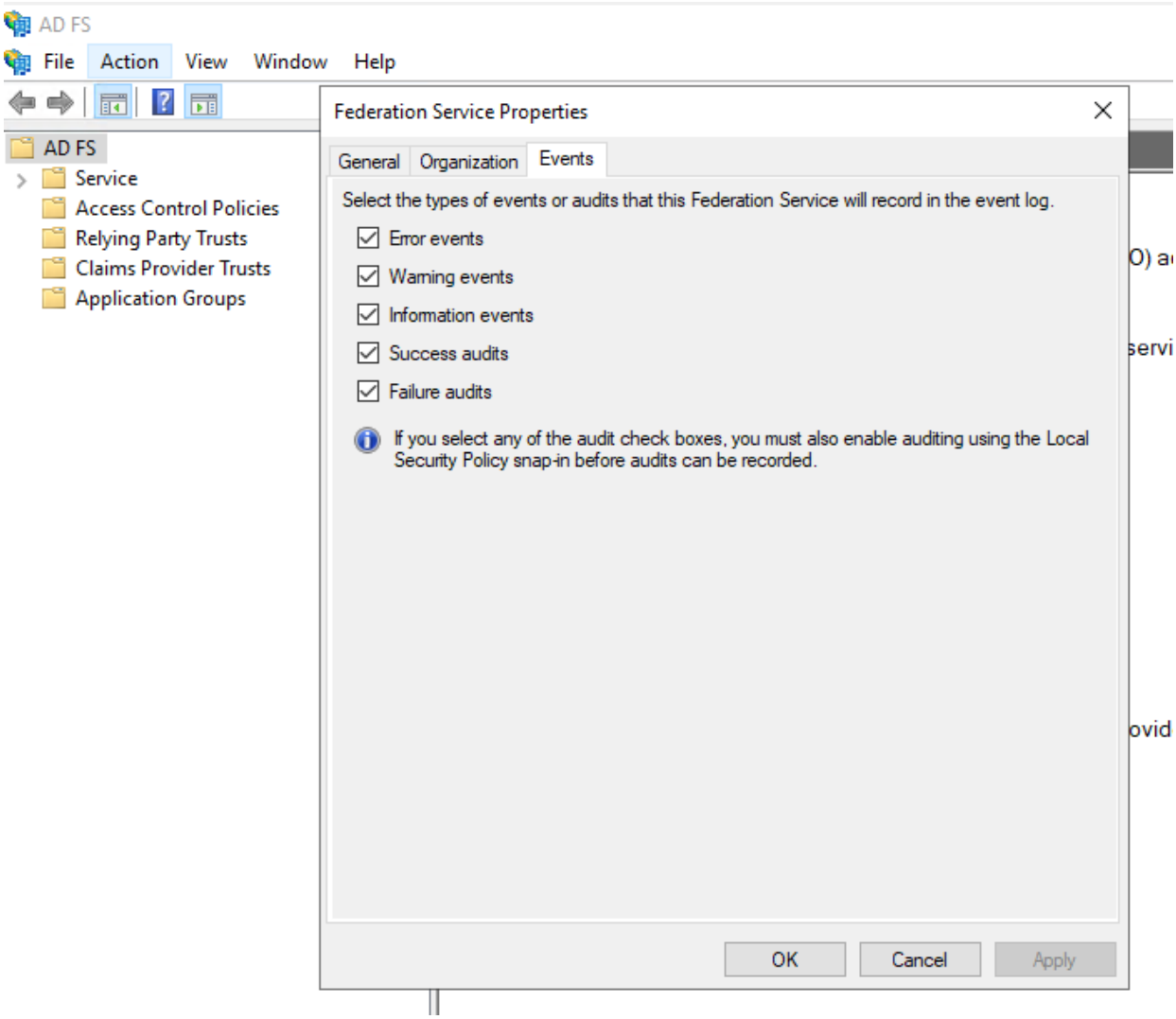
1. На хосте AD FS включите аудит безопасности в локальной политике. Для этого:
    a. Нажмите сочетание клавиш WIN+R. Откроется окно **Run**.
    b. В открывшемся окне введите команду `secpol.msc`.
    c. Нажмите на кнопку **OK**.
    d. В оснастке **Local Security Policy** перейдите в раздел **Security Settings** → **Local Policies** → **Audit Policy**.
    e. Включите логирование **Success** и **Failure** для политик **Audit account logon events** и **Audit logon events**.



2. Разрешите аудит в конфигурации AD FS и включите аудит входа, выполнив в PowerShell от имени администратора последовательно команды:

```
Set-AdfsProperties -AuditLevel Verbose
auditpol /set /subcategory:"Application Generated" /success:enable /failure:enable
```

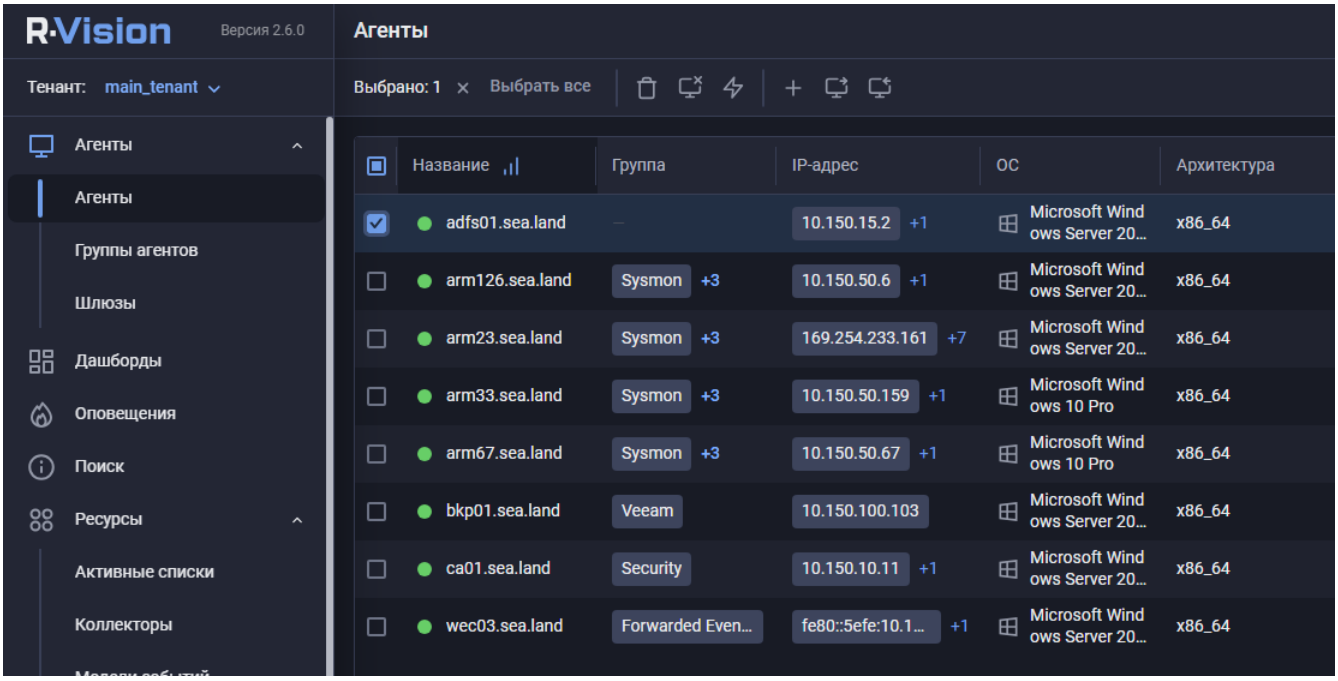
3. Убедитесь, что служба AD FS настроена на аудит. Для этого:
   a. Откройте оснастку **AD FS**.
   b. Перейдите в раздел **Action**.
   c. Откройте настройки **AD FS**.
   d. В появившемся окне перейдите на вкладку **Events**.
   e. Убедитесь, что все флажки установлены.



Установка агента R-Vision Endpoint

Для установки агента обратитесь к документации продукта R-Vision SIEM.

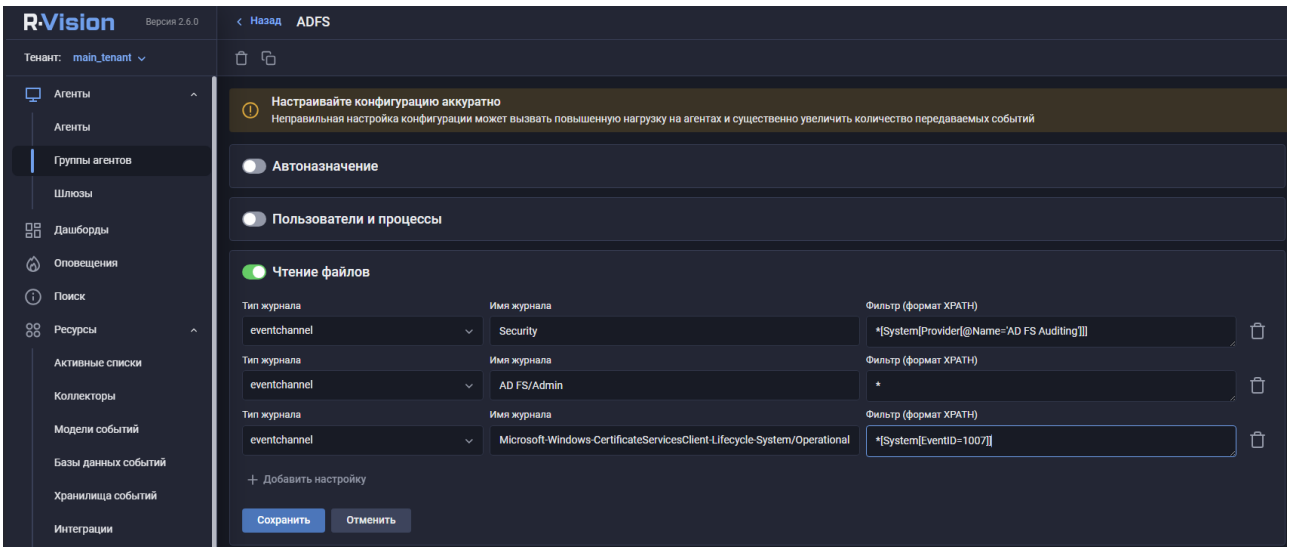
Установите агент R-Vision Endpoint на станцию и настройте его связь с R-Vision SIEM. После этого в веб-интерфейсе R-Vision SIEM в разделе **Агенты** появится информация о подключенном хосте.



Настройка в R-Vision SIEM

Настройка отправки событий в R-Vision SIEM

1. В веб-интерфейсе R-Vision SIEM перейдите в раздел **Агенты** → **Группы агентов**.
2. Создайте группу и добавьте в нее узел, на котором установлен агент.
3. В созданной группе узлов в секции **Чтение файлов** нажмите на кнопку **Добавить настройку** (+).
4. Настройте сбор событий из трех журналов типа **eventchannel**:
   a. Для первого журнала: **Имя журнала** — `Security`, **Фильтр** — `*[System[Provider[@Name='AD FS Auditing']]]`.
   b. Для второго журнала: **Имя журнала** — `AD FS/Admin`, **Фильтр** — `*`.
   c. Для третьего журнала: **Имя журнала** — `Microsoft-Windows-CertificateServicesClient-Lifecycle-System/Operational`, **Фильтр** — `*[System[EventID=1007]]`.
5. Нажмите на кнопку **Сохранить**.



6. Дождитесь применения политики группы на узле. Сбор событий настроен.

Добавление узла в группу

Для добавления узла в созданную группу:

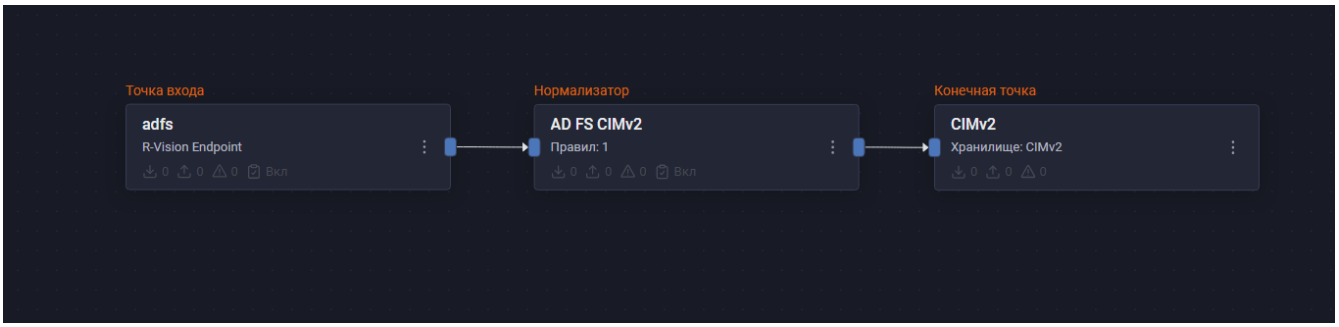
1. В веб-интерфейсе R-Vision SIEM перейдите в раздел **Агенты**.
2. Выберите нужный узел и нажмите на кнопку на панели инструментов.
3. Выберите ранее созданную группу и нажмите на кнопку **Добавить**.
4. Дождитесь применения политики на агенте.

Настройка обработки событий в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **R-Vision Endpoint**.
   - Домен: введите значение в формате `gw-<your_gateway_id>`, где `<your_gateway_id>` — ID шлюза.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Microsoft ADFS** (идентификатор правила: **RV-N-247**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

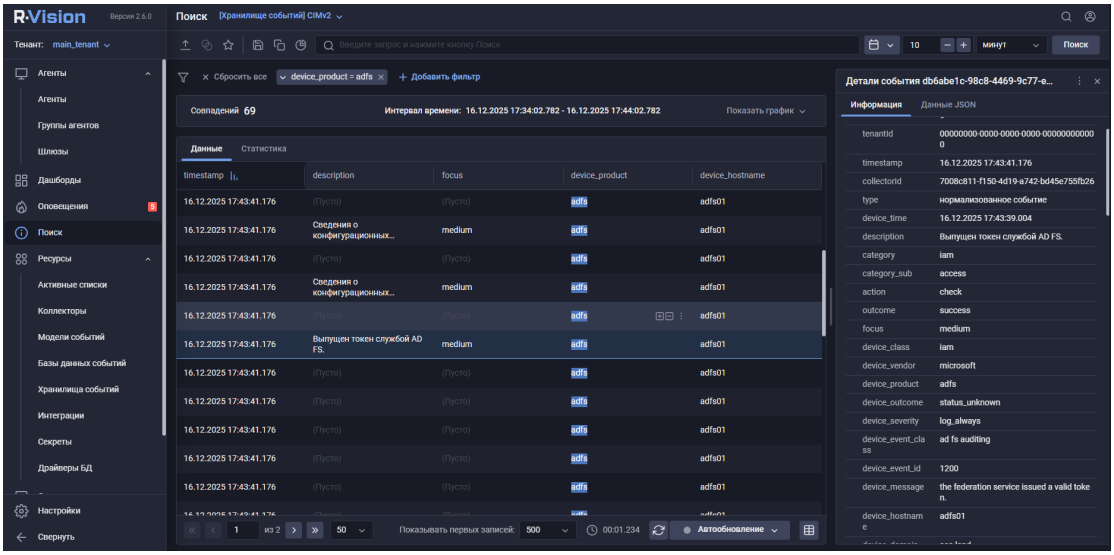
Пример конфигурации конвейера:



После настройки политики сбора и передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события AD FS.

Найти события AD FS в хранилище можно по следующему фильтру:

```
device_product = "adfs"
```



Microsoft Active Directory Federation Services (ADFS): правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1152	Кража/экспорт сертификатов ADFS	Правило обнаруживает экспорт криптографических сертификатов на сервере ADFS, что может свидетельствовать о подготовке атаки Golden SAML. Экспорт сертификатов используется атакующими для последующей подделки SAML-токенов и обхода механизмов аутентификации в домене.	• Persistence (TA0003) • Defense Evasion (TA0005) • Credential Access (TA0006) • Unsecured Credentials (T1552) • Private Keys (T1552.004) • Forge Web Credentials (T1606) • SAML Tokens (T1606.002) • Steal or Forge Authentication Certificates (T1649)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1154	Множественные неудачные попытки аутентификации в ADFS	Для получения доступа к учетным записям и сервисам, защищенным федеративной аутентификацией, атакующий может выполнять перебор паролей через веб-интерфейс ADFS. Правило обнаруживает множественные неудачные попытки проверки учетных данных в ADFS (Token validation failed с причиной `The user name or password is incorrect`) за ограниченный промежуток времени, что может указывать на атаку brute force.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)
RV-D-1155	Успешный подбор пароля в ADFS	Для получения несанкционированного доступа к учетной записи атакующий может выполнить перебор паролей через службу ADFS. Правило обнаруживает успешную аутентификацию в ADFS после серии неуспешных попыток входа с причиной `The user name or password is incorrect`, что с высокой вероятностью указывает на успешный подбор пароля и компрометацию учетной записи.	• Credential Access (TA0006) • Valid Accounts (T1078) • Domain Accounts (T1078.002) • Brute Force (T1110) • Password Guessing (T1110.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1158	Изменение Claims Provider Trust в ADFS	Для управления источниками удостоверений в ADFS используются объекты Claims Provider Trust. Изменение или добавление таких доверий может повлиять на процесс аутентификации и авторизации пользователей. Правило обнаруживает изменения и административные операции с Claims Provider Trust в ADFS, зафиксированные в журналах службы и PowerShell, что может указывать на попытку вмешательства в конфигурацию федеративной аутентификации.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Account Manipulation (T1098) • Modify Authentication Process (T1556)

Multifactor Radius Adapter

- Multifactor Radius Adapter: настройка источника

Multifactor Radius Adapter: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Multifactor Radius Adapter в R-Vision SIEM.

Предварительные требования

Перед настройкой пересылки событий в R-Vision SIEM убедитесь в выполнении следующих условий:

- Сетевая связность между RADIUS-сервером Multifactor Radius Adapter и R-Vision SIEM (или промежуточным узлом) обеспечена, а необходимые порты открыты.

Настройка Multifactor Radius Adapter

Настройка журналирования Multifactor Radius Adapter

Для настройки журналирования Multifactor Radius Adapter выполните следующие действия:

linux

1. В файле `/opt/multifactor/radius/multifactor-radius-adapter.dll.config` установите следующие значения параметрам:

```
<add key="logging-level" value="Debug"/>
<add key="logging-format" value="json"/>
```

2. Перезапустите сервис `multifactor-radius` с помощью команды:

```
sudo systemctl restart multifactor-radius.service
```

Журналирование и отправка событий Multifactor Radius Adapter для Linux настроены.

windows

1. В файле `C:\Program Files\MFA Radius\MultiFactor.Radius.Adapter.exe.config` установите следующие значения параметрам:

```
<add key="logging-level" value="Debug"/>
<add key="logging-format" value="json"/>
<add key="syslog-app-name" value="mfa-radius"/>
<add key="syslog-server" value="udp://<target>:<udp_port>"/>
<add key="syslog-format" value="RFC5424"/>
<add key="syslog-facility" value="Auth"/>
<add key="syslog-use-tls" value="false" />
```

Здесь:

- `<target>`: IP-адрес или полное доменное имя (FQDN) коллектора R-Vision SIEM.
- `<udp_port>`: UDP-порт точки входа `Syslog` на конвейере R-Vision SIEM.

2. Перезапустите сервис `Multifactor Radius` в оснастке `services.msc`.

Журналирование Multifactor Radius Adapter для Windows настроено.

Настройка отправки событий в R-Vision SIEM (Только для Linux)

В настоящем руководстве рассматривается передача событий с помощью службы `syslog`.

rsyslog

Предполагается, что `rsyslog` на станции с ОС Linux уже установлен и модуль `imfile` подгружен в `/etc/rsyslog.conf`. Для настройки передачи событий из файлов Multifactor Radius Adapter выполните следующие действия:

1. Создайте файл `/etc/rsyslog.d/99-mfa-siem.conf` со следующим содержимым:

```
input(
    type="imfile"
    File="/opt/multifactor/radius/logs/log*"
    Tag="mfa-radius"
    Severity="info"
    Facility="local6"
)

# Пересылка на удалённые rsyslog
```

```
if $syslogtag == 'mfa-radius' then {
  action(type="omfwd" target="<target>" port="<port>" protocol="udp")
  stop
}
```

Здесь:

- `<target>`: IP-адрес или полное доменное имя (FQDN) коллектора R-Vision SIEM.
- `<port>`: порт точки входа `Syslog` на конвейере R-Vision SIEM.

2. Перезапустите сервис `rsyslog` с помощью команды:

```
sudo systemctl restart rsyslog
```

Отправка событий Multifactor Radius Adapter настроена.

syslog-ng

Предполагается, что `syslog-ng` на станции с ОС Linux уже установлен. Для настройки передачи событий из файлов Multifactor Radius Adapter выполните следующие действия:

1. Создайте файл `/etc/syslog-ng/conf.d/mfa-siem.conf` со следующим содержимым:

```
source mfa {
        file("/opt/multifactor/radius/logs/*.txt" flags(no-parse)
log_prefix("mfa-radius: "));
};

destination siem {
        udp("<target>" port(<port>)); # указать IP и порт точки входа SIEM
};

log {
        source(mfa); destination(siem);
};
```

Здесь:

- `<target>`: IP-адрес или полное доменное имя (FQDN) коллектора R-Vision SIEM.
- `<port>`: порт точки входа `Syslog` на конвейере R-Vision SIEM.

2. Перезапустите сервис `syslog-ng` с помощью команды:

```
sudo systemctl restart syslog-ng
```

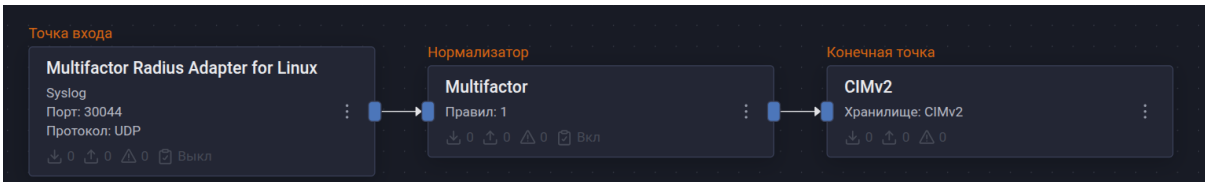
Отправка событий Multifactor Radius Adapter настроена.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий Multifactor Radius Adapter в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне источника.
   - Протокол: выберите вариант в соответствии с настройками на стороне источника.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Multifactor Radius Adapter** (идентификатор правила: **RV-N-340**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

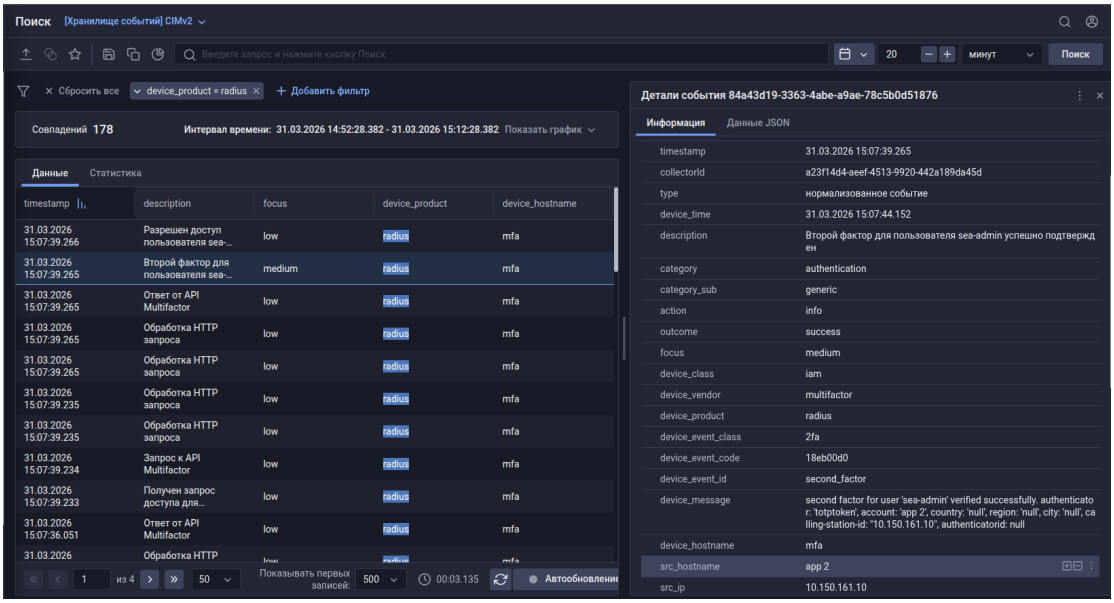
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Multifactor Radius Adapter.

Найти события Multifactor Radius Adapter в хранилище можно по следующему фильтру:

```
device_product = "radius"
```


Поиск
[Хранилище событий] CIMv2
Введите запрос и нажмите кнопку Поиск
20
минут
Поиск
Сбросить все
device_product = radius
Добавить фильтр
Совпадений 178
Интервал времени: 31.03.2026 14:52:28.382 - 31.03.2026 15:12:28.382
Показать график
Данные
Статистика
timestamp
description
focus
device_product
device_hostname
31.03.2026 15:07:39.266
Разрешен доступ пользователя sea-...
low
radius
mfa
31.03.2026 15:07:39.265
Второй фактор для пользователя sea-...
medium
radius
mfa
31.03.2026 15:07:39.265
Ответ от API Multifactor
low
radius
mfa
31.03.2026 15:07:39.265
Обработка HTTP запроса
low
radius
mfa
31.03.2026 15:07:39.265
Обработка HTTP запроса
low
radius
mfa
31.03.2026 15:07:39.235
Обработка HTTP запроса
low
radius
mfa
31.03.2026 15:07:39.235
Обработка HTTP запроса
low
radius
mfa
31.03.2026 15:07:39.234
Запрос к API Multifactor
low
radius
mfa
31.03.2026 15:07:39.233
Получен запрос доступа для...
low
radius
mfa
31.03.2026 15:07:36.051
Ответ от API Multifactor
low
radius
mfa
31.03.2026
Обработка HTTP
1
из 4
50
Показывать первых записей:
500
00:03.135
Автообновлени
Детали события 84a43d19-3363-4abe-a9ae-78c5b0d51876
Информация
Данные JSON
timestamp
31.03.2026 15:07:39.265
collectorId
a23f14d4-aeef-4513-9920-442a189da45d
type
нормализованное событие
device_time
31.03.2026 15:07:44.152
description
Второй фактор для пользователя sea-admin успешно подтвержден
category
authentication
category_sub
generic
action
info
outcome
success
focus
medium
device_class
iam
device_vendor
multifactor
device_product
radius
device_event_class
2fa
device_event_code
18eb00d0
device_event_id
second_factor
device_message
second factor for user 'sea-admin' verified successfully. authenticator: 'totptoken', account: 'app 2', country: 'null', region: 'null', city: 'null', calling-station-id: "10.150.161.10", authenticatorid: null
device_hostname
mfa
src_hostname
app 2
src_ip
10.150.161.10

Системы киберразведки (TI)

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых систем киберразведки:

- Kaspersky CyberTrace
- R-Vision TIP

Kaspersky CyberTrace

- Kaspersky CyberTrace: настройка источника

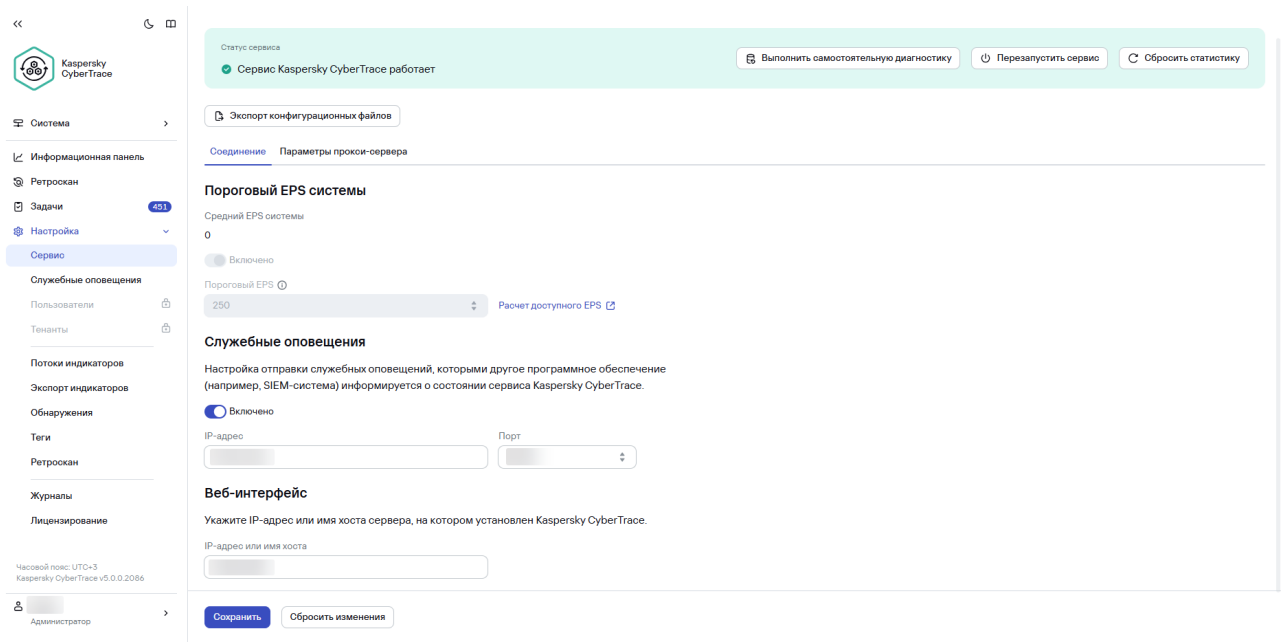
Kaspersky CyberTrace: настройка источника

Данное руководство описывает процесс настройки формата событий источника Kaspersky CyberTrace для работы нормализации событий в R-Vision SIEM.

Настройка Kaspersky CyberTrace

Чтобы настроить Kaspersky CyberTrace:

1. В веб-интерфейсе Kaspersky CyberTrace откройте **Управление** → **Система**.
2. Перейдите в меню **Настройка** → **Сервис**.
3. Включите передачу событий в SIEM.
4. Укажите **Адрес сервера** и **Порт** точки входа конвейера SIEM.
5. Укажите адрес интерфейса CyberTrace.
6. Нажмите на кнопку **Сохранить**.



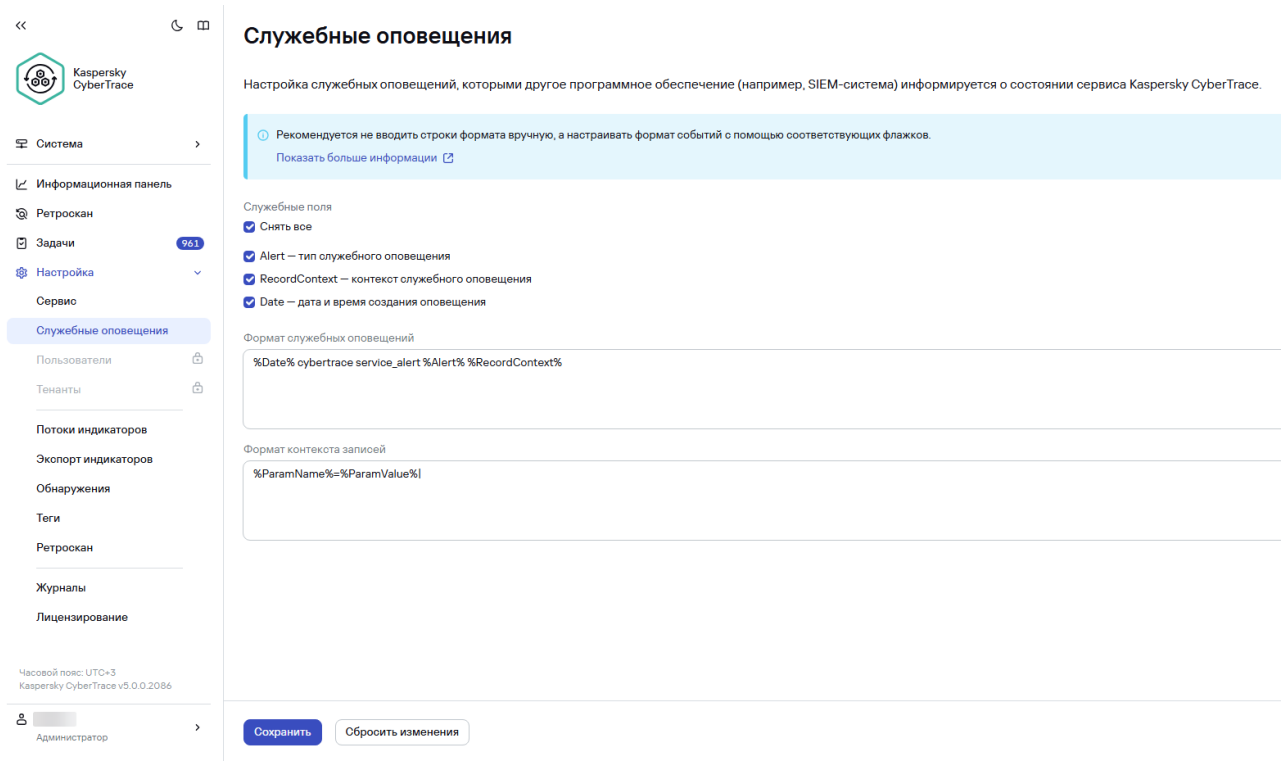
7. Перейдите в меню **Настройка** → **Служебные оповещения**.
8. Установите формат служебных оповещений по следующему шаблону:

```
%Date% <cybertrace> service_alert %Alert% %RecordContext%
```

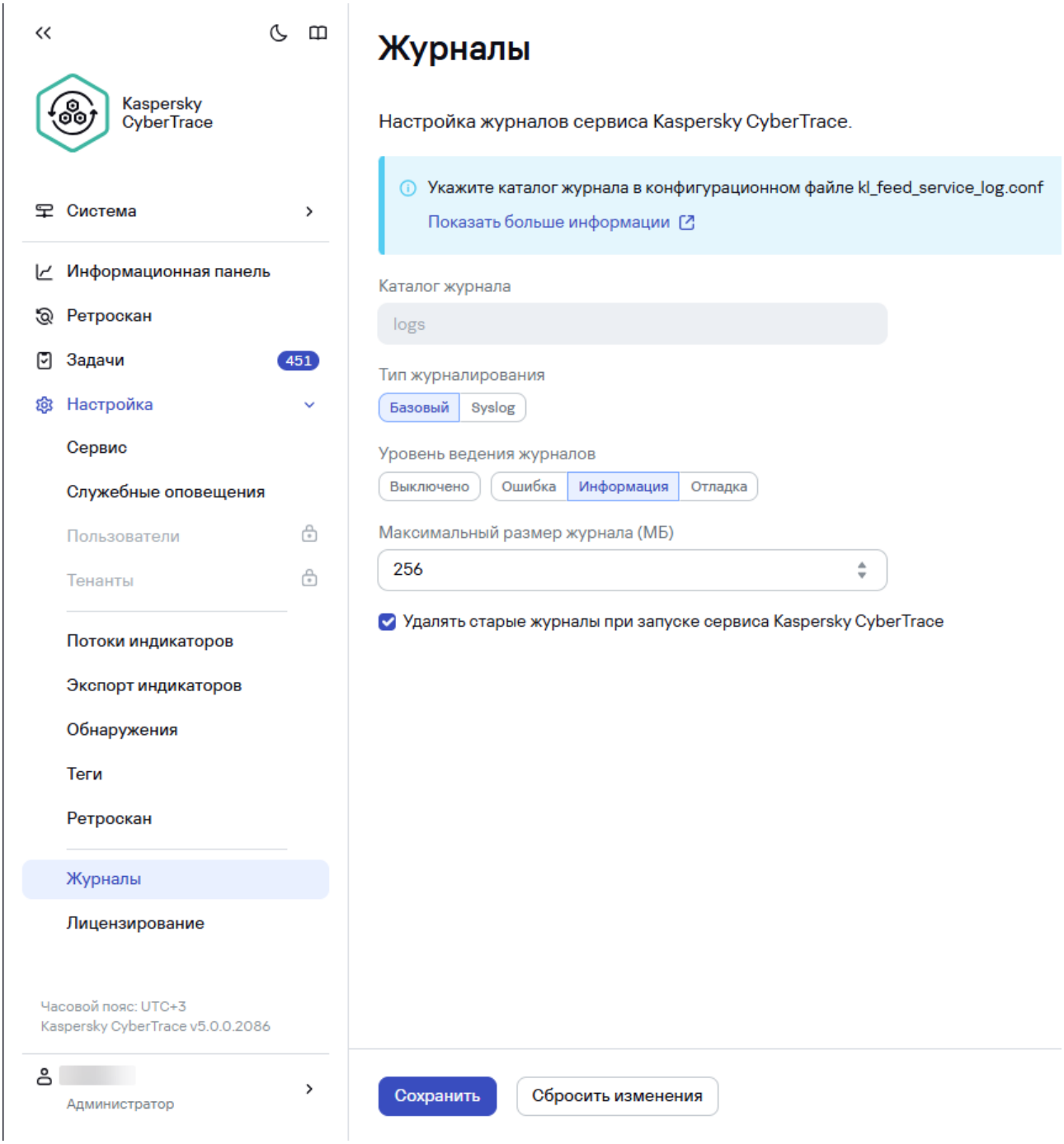
Где <cybertrace> — имя хоста CyberTrace.

9. Установите формат контекста записей по следующему шаблону:

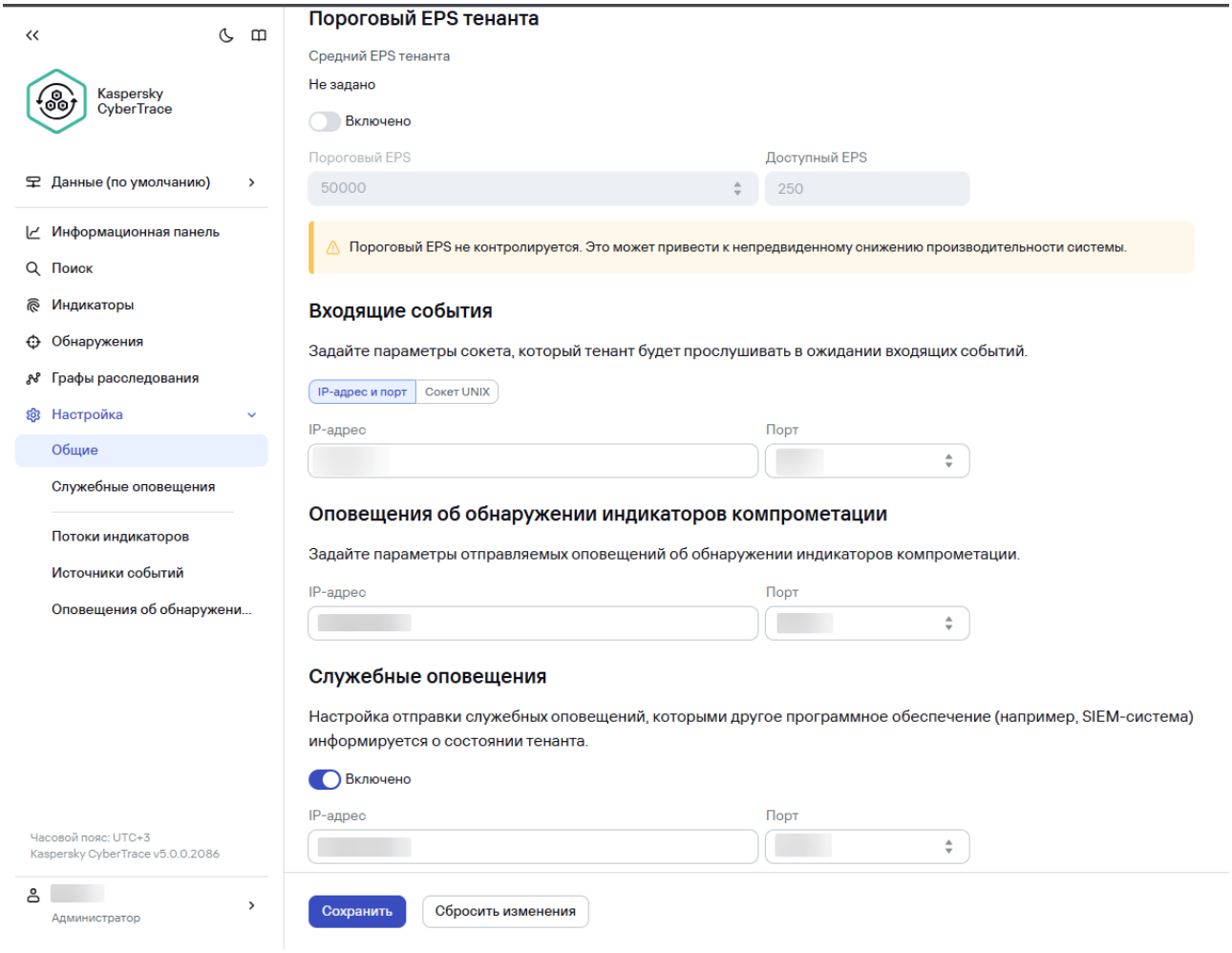
```
%ParamName%=%ParamValue%|
```



10. Перейдите в меню **Настройка** → **Журналы**.
11. Включите тип журналирования **Базовый**.
12. Выберите подходящий уровень ведения журналов и максимальный размер файла логов.



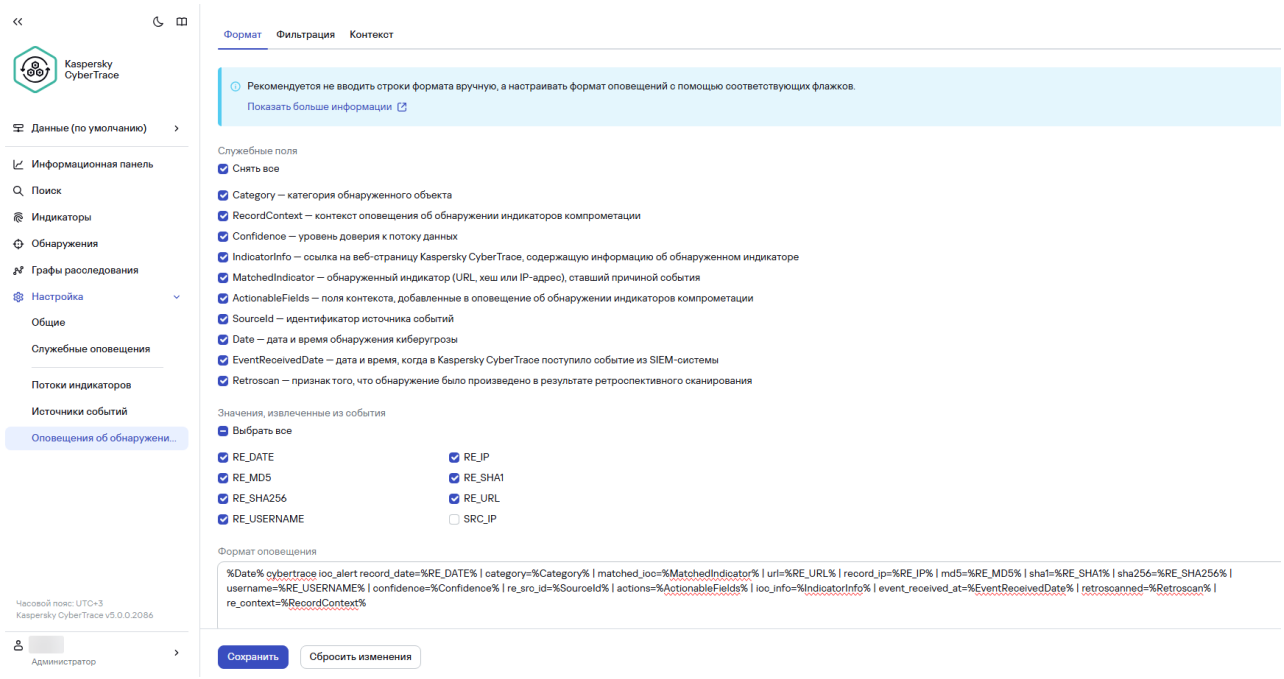
13. В веб-интерфейсе Kaspersky CyberTrace откройте **Управление** → **Данные (по умолчанию)**.
14. Перейдите в меню **Настройка** → **Общие**.
15. Укажите **Адрес сервера** и **Порт** хоста, на котором развернут `Kaspersky CyberTrace` для получения событий от других источников.
16. Укажите **Адрес сервера** и **Порт** точки входа конвейера `SIEM`, куда будут отправляться события обнаружения индикаторов компрометации.
17. Укажите **Адрес сервера** и **Порт** конвейера `SIEM` для отправки служебных оповещений.
18. Нажмите на кнопку **Сохранить**.



19. Перейдите в меню **Настройка** → **Оповещения об обнаружении индикаторов**.
20. Установите формат оповещений по следующему шаблону:

```
%Date% <cybertrace> ioc_alert record_date=%RE_DATE% | category=%Category% |
matched_ioc=%MatchedIndicator% | url=%RE_URL% | record_ip=%RE_IP% | md5=%RE_MD5% |
sha1=%RE_SHA1% | sha256=%RE_SHA256% | username=%RE_USERNAME% |
confidence=%Confidence% | re_src_id=%SourceId% | actions=%ActionableFields% |
ioc_info=%IndicatorInfo% | event_received_at=%EventReceivedDate% |
retroscanned=%Retroscan% | re_context=%RecordContext%
```

Где `<cybertrace>` — имя хоста CyberTrace.



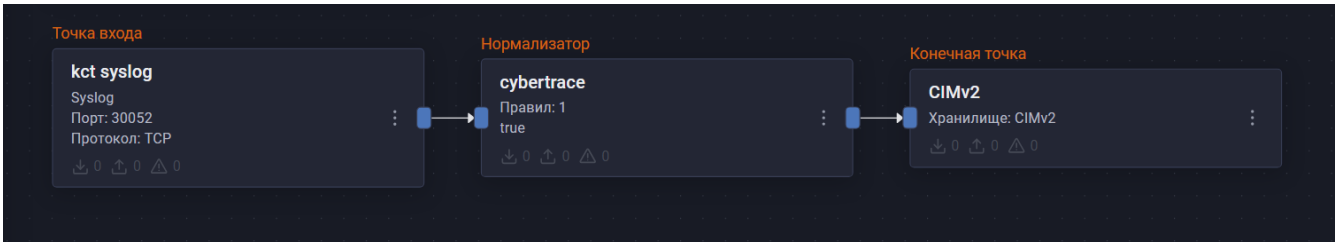
Настройка источника завершена.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В веб-интерфейсе R-Vision SIEM перейдите в раздел **Ресурсы** → **Коллекторы** и создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите произвольное, понятное название.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне Kaspersky CyberTrace.
   - Протокол: выберите вариант в соответствии с настройками на стороне Kaspersky CyberTrace.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Kaspersky CyberTrace** (идентификатор правила: **RV-N-182**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

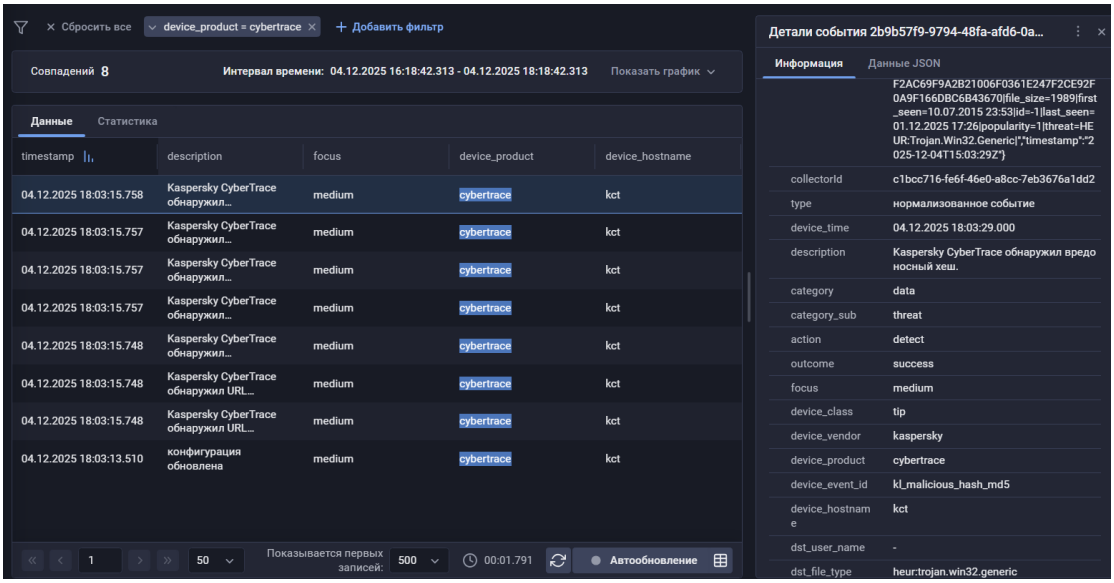
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события CyberTrace.

Найти события CyberTrace в хранилище можно по следующему фильтру:

```
device_product = "cybertrace"
```



R-Vision TIP

- R-Vision TIP: настройка источника

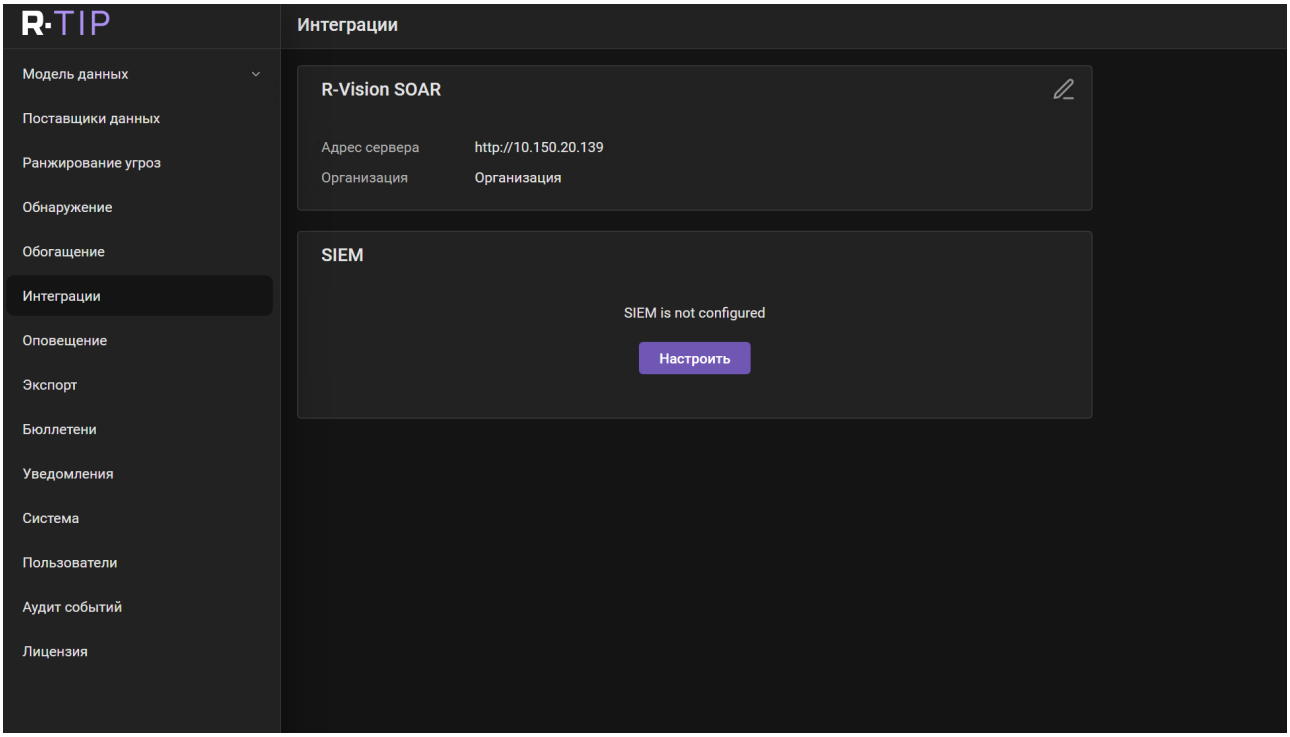
R-Vision TIP: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий источника R-Vision TIP (Threat Intelligence Platform) в R-Vision SIEM.

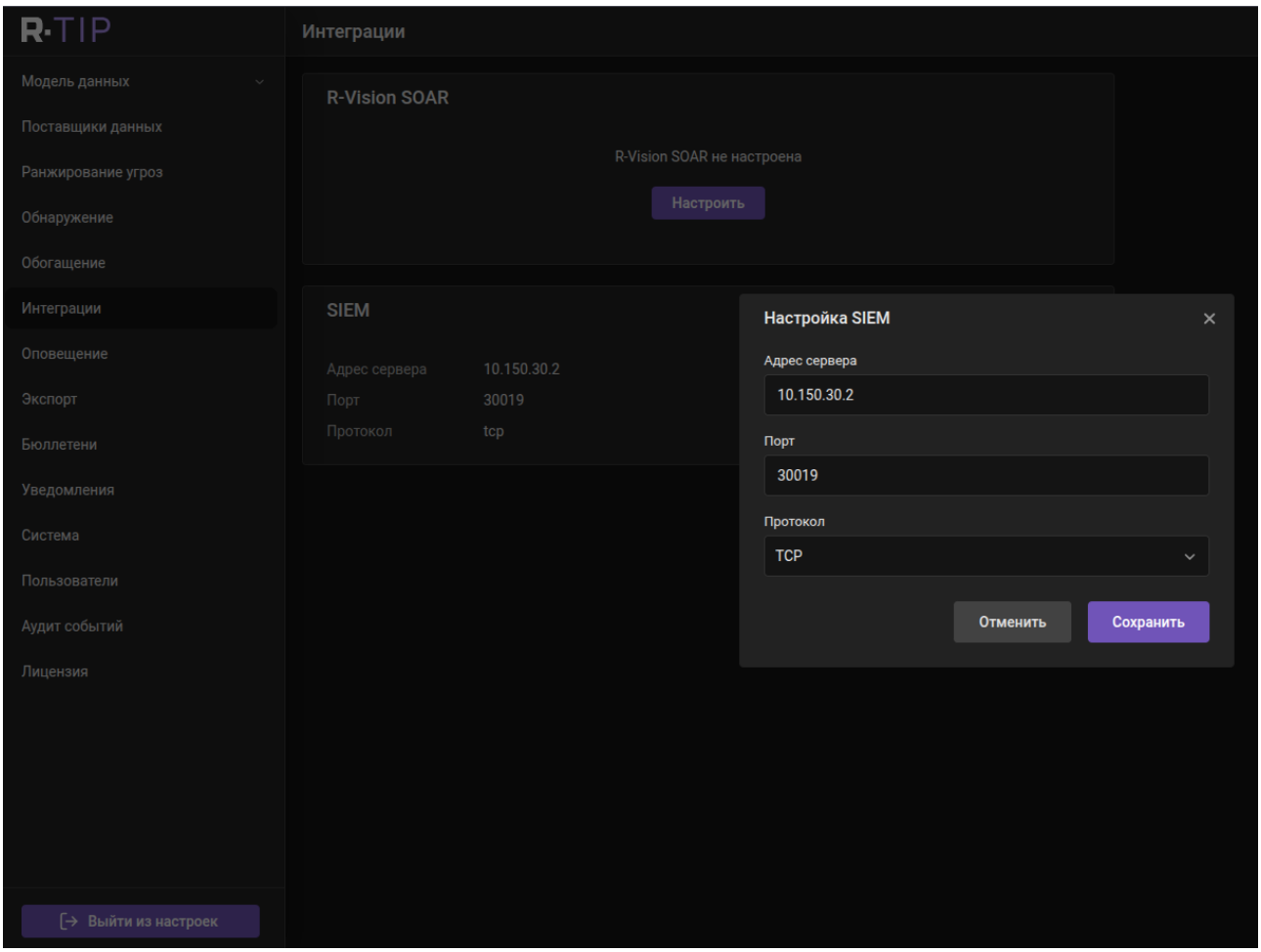
Настройка R-Vision TIP

Чтобы настроить R-Vision TIP:

1. В веб-интерфейсе R-Vision TIP нажмите на кнопку **Настройки** (⚙).
2. Перейдите в раздел **Интеграции**.
3. Добавьте интеграцию **SIEM**, для этого нажмите на кнопку **Настроить**.



4. В появившемся окне заполните поля **Адрес сервера**, **Порт** и **Протокол**.
5. Нажмите на кнопку **Сохранить**.



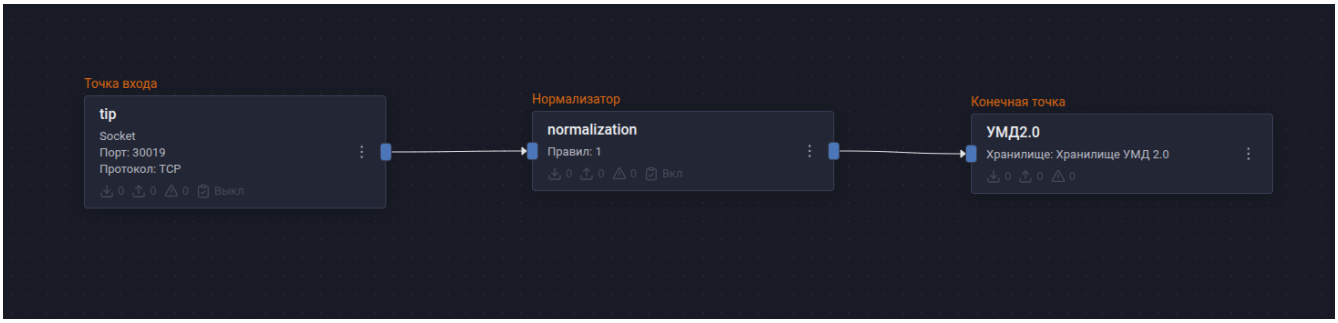
Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие

шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Socket**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне R-Vision TIP.
   - Протокол: выберите вариант в соответствии с настройками на стороне R-Vision TIP.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **R-Vision TIP** (идентификатор правила: **RV-N-298**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

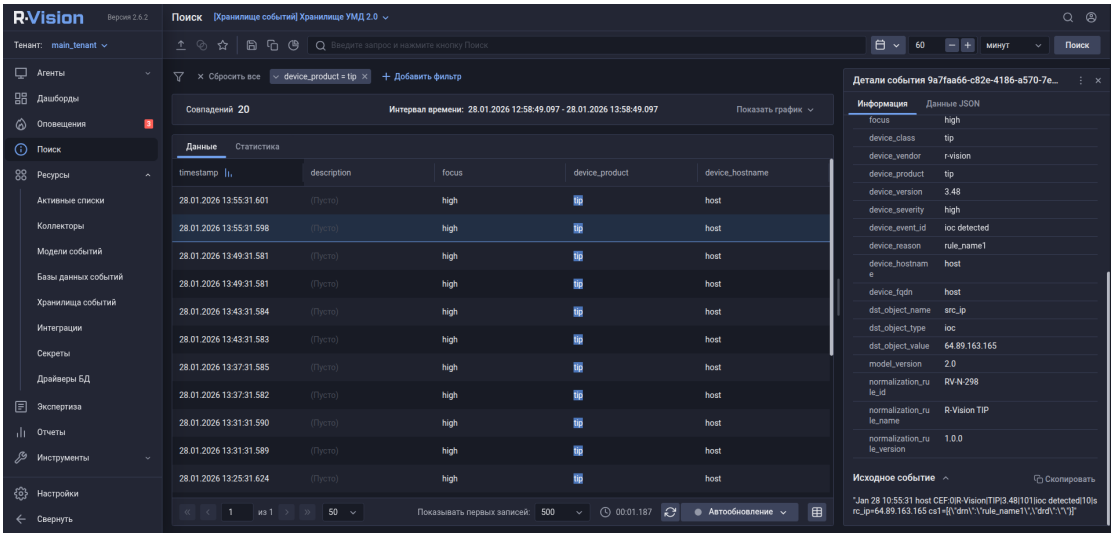
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события TIP.

Найти события TIP в хранилище можно по следующему фильтру:

```
device_product = "tip"
```


R-Vision
Версия 2.6.2
Тенант: main_tenant
Агенты
Дашборды
Оповещения
Поиск
Ресурсы
Активные списки
Коллекторы
Модели событий
Базы данных событий
Хранилища событий
Интеграции
Секреты
Драйверы БД
Экспертиза
Отчеты
Инструменты
Настройки
Свернуть
Поиск
[Хранилище событий] Хранилище УМД 2.0
Введите запрос и нажмите кнопку Поиск
60
минут
Поиск
Сбросить все
device_product = tip
Добавить фильтр
Совпадений 20
Интервал времени: 28.01.2026 12:58:49.097 - 28.01.2026 13:58:49.097
Показать график
Данные
Статистика
timestamp
description
focus
device_product
device_hostname
28.01.2026 13:55:31.601 (Пусто) high tip host
28.01.2026 13:55:31.598 (Пусто) high tip host
28.01.2026 13:49:31.581 (Пусто) high tip host
28.01.2026 13:49:31.581 (Пусто) high tip host
28.01.2026 13:43:31.584 (Пусто) high tip host
28.01.2026 13:43:31.583 (Пусто) high tip host
28.01.2026 13:37:31.585 (Пусто) high tip host
28.01.2026 13:37:31.582 (Пусто) high tip host
28.01.2026 13:31:31.590 (Пусто) high tip host
28.01.2026 13:31:31.589 (Пусто) high tip host
28.01.2026 13:25:31.624 (Пусто) high tip host
1 из 1
50
Показывать первых записей: 500
00:01.187
Автообновление
Детали события 9a7faa66-c82e-4186-a570-7e...
Информация
Данные JSON
focus high
device_class tip
device_vendor r-vision
device_product tip
device_version 3.48
device_severity high
device_event_id ioc detected
device_reason rule_name1
device_hostname host
device_fqdn host
dst_object_name src_ip
dst_object_type ioc
dst_object_value 64.89.163.165
model_version 2.0
normalization_rule_id RV-N-298
normalization_rule_name R-Vision TIP
normalization_rule_version 1.0.0
Исходное событие
Скопировать
"Jan 28 10:55:31 host CEF:0|R-Vision|TIP|3.48|101|ioc detected|10|src_ip=64.89.163.165 cs1={\"dm\":\"rule_name1\",\"drd\":\"\"}"

Системы мониторинга инфраструктуры

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых систем мониторинга инфраструктуры:

- Zabbix

Zabbix

- Zabbix: настройка источника

Zabbix: настройка источника

Данная инструкция описывает настройку сбора событий на сервере Zabbix и их последующей отправки в R-Vision SIEM.

Предварительные требования

Перед настройкой Zabbix убедитесь, что у вас имеется:

- Сетевой доступ к БД;
- Учетная запись в СУБД с правами администратора на доступ к БД Zabbix в вашей системе управления базами данных (далее — СУБД).

Настройка Zabbix

Описание подсистемы журналирования

Zabbix записывает свои события в базу данных Zabbix вашей СУБД.



База данных Zabbix создается автоматически при установке сервера Zabbix версии 6.0 и выше. Если вы используете более старую версию, обратитесь к документации Zabbix для первичной настройки.



Названия таблиц в вашей СУБД могут отличаться от названий таблиц, приведенных в данной инструкции. Если вы не можете найти необходимые таблицы в вашей СУБД или получаете ошибки существования таблиц, обратитесь к разделу документации, соответствующему вашей версии сервиса, для поиска соответствий.

Настройка журналирования

Создание сервисной учетной записи

Для осуществления сбора логов из базы данных требуется подключиться к ней с использованием специализированной учетной записи (далее — УЗ). Данная УЗ предназначена для обеспечения доступа к базе данных автоматическим сервисом.

Чтобы создать сервисную УЗ, подключитесь к СУБД с правами администратора. Для этого выполните следующие действия на сервере с установленной СУБД:



В качестве примера используется СУБД PostgreSQL.

1. Выполните следующую команду от имени пользователя с правами администратора:

   ```
   sudo -u <admin> psql
   ```

   где `<admin>` — название учетной записи с правами администратора.

2. Создайте сервисную учетную запись, выполнив следующие команды:

   ```
   CREATE USER "<new_user>";
   ALTER ROLE <new_user> WITH PASSWORD '<passw0rd>';
   ```

   где:

   - `<new_user>` — имя созданной УЗ.
   - `<passw0rd>` — пароль для созданной УЗ.

3. Предоставьте права на подключение к базе данных и чтение таблицы. К правам пользователя предъявляются следующие требования:

   - возможность подключения к базе данных Zabbix;
   - возможность выполнения SELECT-запросов к таблицам audit и alerts базы данных Zabbix.

   Пример 1. Пример запроса для создания пользователя в PostgreSQL 14.0

   ```
   GRANT CONNECT ON DATABASE Zabbix TO <new_user>;
   GRANT USAGE ON SCHEMA public TO <new_user>;
   GRANT SELECT ON ALL TABLES IN SCHEMA public TO <new_user>;
   ```

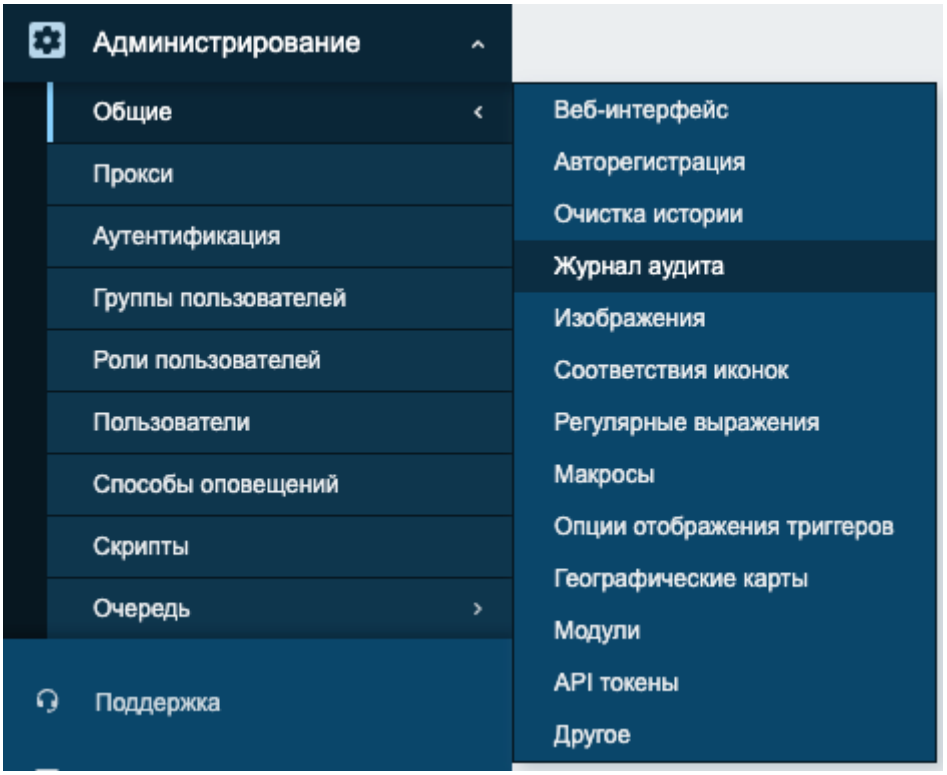


Вы также можете ограничить доступ УЗ к таблицам, предоставив SELECT-привилегии только для таблиц audit и alerts.

Включение сбора событий аудита

Для настройки логирования событий аудита в Zabbix выполните следующие действия:

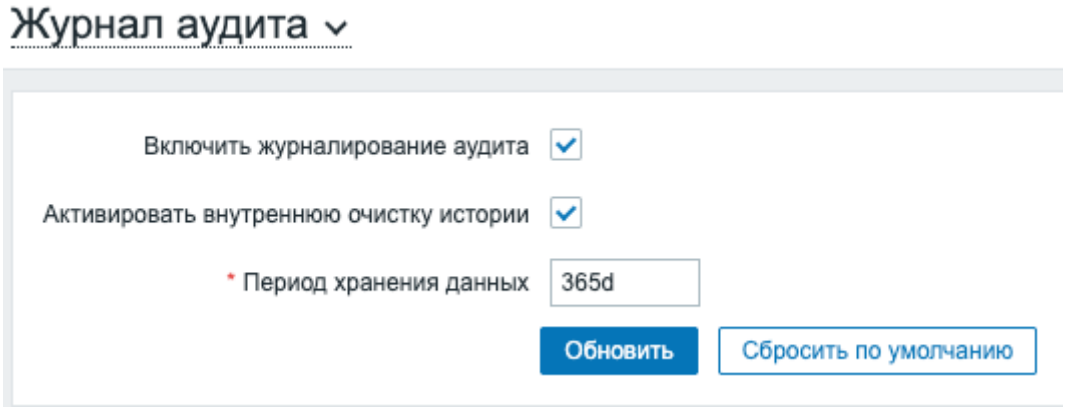
1. Подключитесь к веб-интерфейсу Zabbix.
2. Войдите в веб-интерфейс с помощью УЗ, имеющей права администратора Zabbix.
3. Перейдите в раздел **Администрирование** → **Общие** → **Журнал аудита**.



Если вы используете английскую версию Zabbix, перейдите в раздел **Administration** → **General** → **Audit Log**.

4. Установите флажок напротив параметра **Включить журналирование аудита**.

В английской версии Zabbix установите флажок напротив параметра **Enable Audit Log**.



5. После настройки журналирования события аудита начнут записываться в вашу СУБД.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте секрет со строкой подключения. Для этого:
   a. Перейдите в раздел **Ресурсы** → **Секреты**.
   b. Нажмите на кнопку **Создать**.

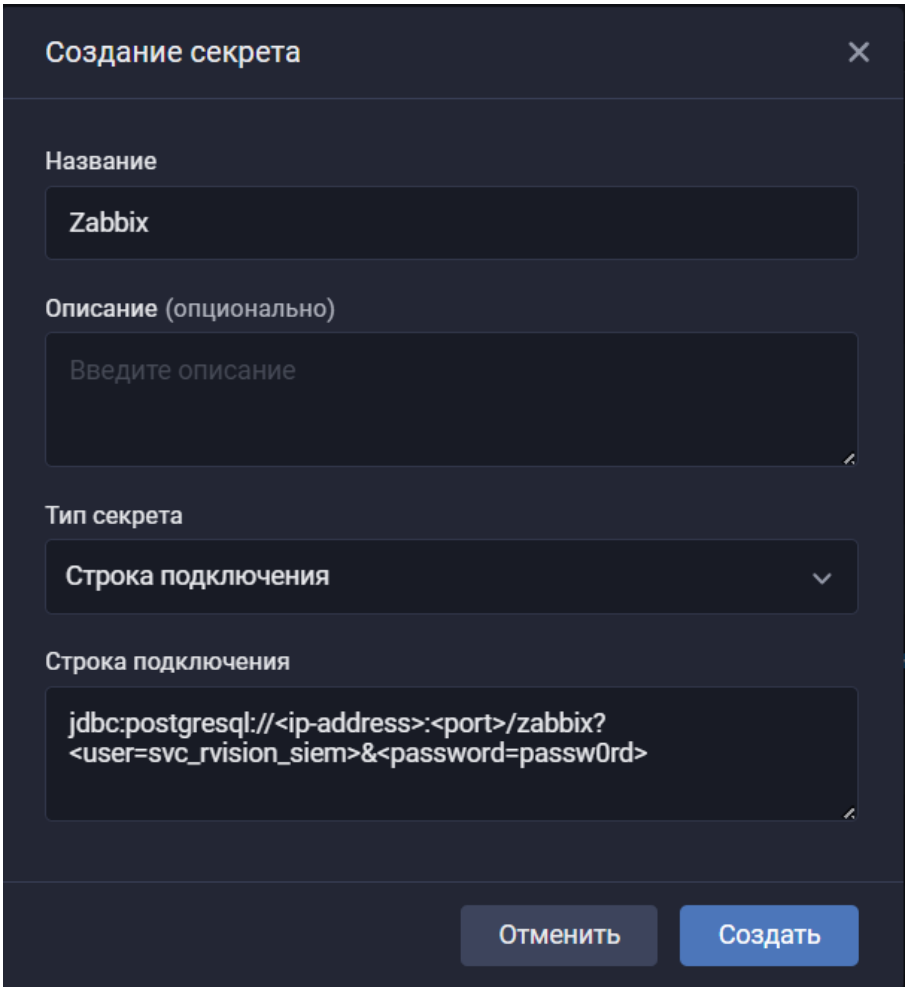
c. В раскрывшемся окне создания секрета заполните поля:

- **Название**: введите название секрета.
- **Описание** (опционально): опишите, для чего будет использоваться секрет.
- **Тип секрета**: выберите вариант **Строка подключения**.
- **Строка подключения**: введите строку вида:

```
jdbc:postgresql://<ip-
address>:<port>/zabbix?user=<svc_rvision_siem>&password=<passw0rd>
```

где:

- `<ip-address>` — данные вашего сервера СУБД Zabbix.
- `<port>` — порт подключения к вашей СУБД. По умолчанию используется порт 5432.
- `<svc_rvision_siem>` — пример имени пользователя для подключения к СУБД Zabbix.
- `<passw0rd>` — пример пароля пользователя СУБД Zabbix.



d. Нажмите на кнопку **Создать**.

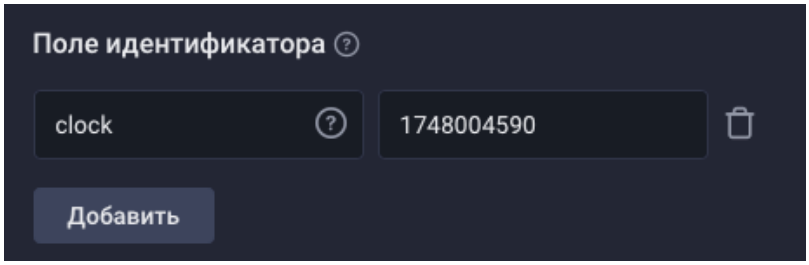
2. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
3. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - **Название**: введите название точки входа.

- **Тип точки входа**: выберите вариант **Database**.
- **Драйвер базы данных**: выберите вариант **PostgreSQL**.
- **Адрес подключения**: выберите секрет, созданный ранее.
- **SQL-запрос**: для сбора логов из таблицы auditlog добавьте следующую команду:

```
SELECT 'Zabbix_Audit' AS appname,
auditid,
username,
clock,
ip,
action,
resourcename,
resourcetype,
details FROM auditlog WHERE clock > ?::integer ORDER BY clock ASC;
```

- **Поле идентификатора**: введите ключ `clock` со значением текущего времени в формате Unix time.

  Пример указания параметра **Поле идентификатора**:



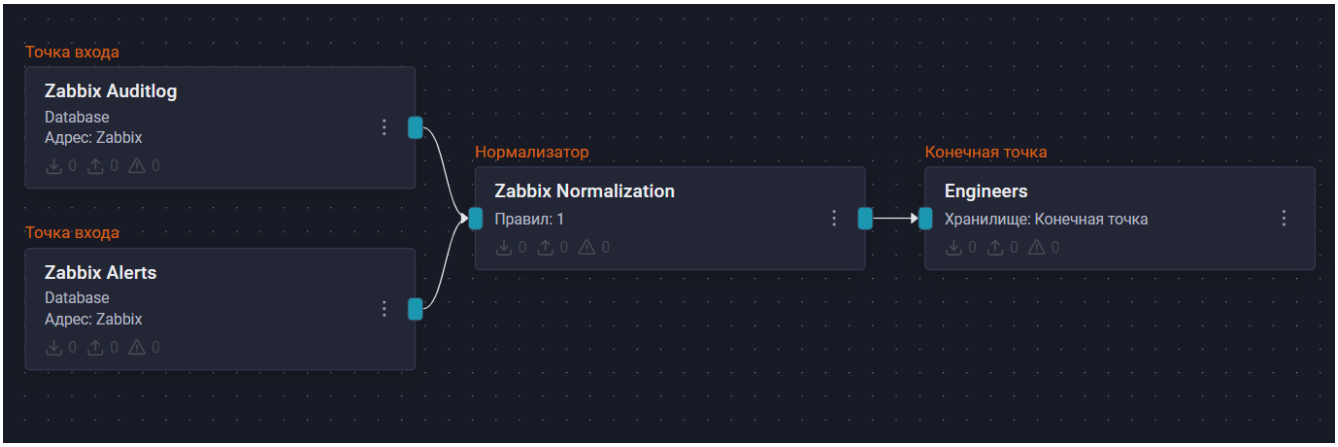
4. Добавьте на конвейер еще один элемент **Точка входа** со следующими параметрами:
   - **Название**: введите название точки входа.
   - **Тип точки входа**: выберите вариант **Database**.
   - **Драйвер базы данных**: выберите вариант **PostgreSQL**.
   - **Адрес подключения**: выберите секрет, созданный ранее.
   - **SQL-запрос**: для сбора логов из таблицы alerts добавьте следующую команду:

```
SELECT 'Zabbix_Alerts' AS appname,
alertid,
actionid,
eventid,
userid,
clock,
subject,
status,
message,
retries FROM alerts WHERE clock > ?::integer ORDER BY clock ASC;
```

- **Поле идентификатора**: введите ключ `clock` со значением текущего времени в формате Unix time.

5. Добавьте на конвейер элемент **Нормализатор** с правилом **Zabbix** (идентификатор правила: **RV-N-260**).
6. Соедините нормализатор с точками входа.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

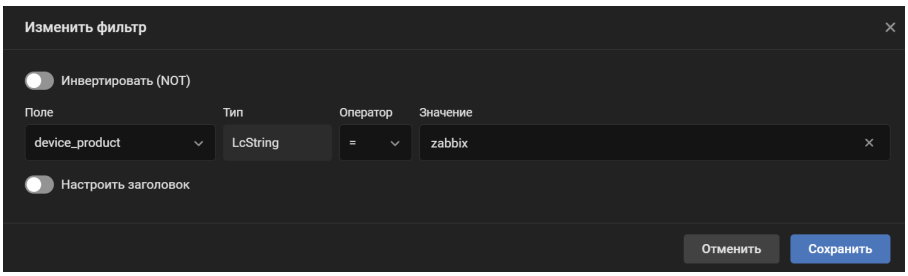
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Zabbix.

Найти события Zabbix в хранилище можно по следующему фильтру:

```
device_product = "zabbix"
```



Системы обнаружения и предотвращения вторжений (IDS/IPS)

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых систем обнаружения и предотвращения вторжений:

- ИнфоТеКС ViPNet IDS NS
- ИнфоТеКС ViPNet TIAS

ИнфоТеКС ViPNet IDS NS

- ИнфоТеКС ViPNet IDS NS: настройка источника

ИнфоТеКС ViPNet IDS NS: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий ViPNet IDS NS в R-Vision SIEM.

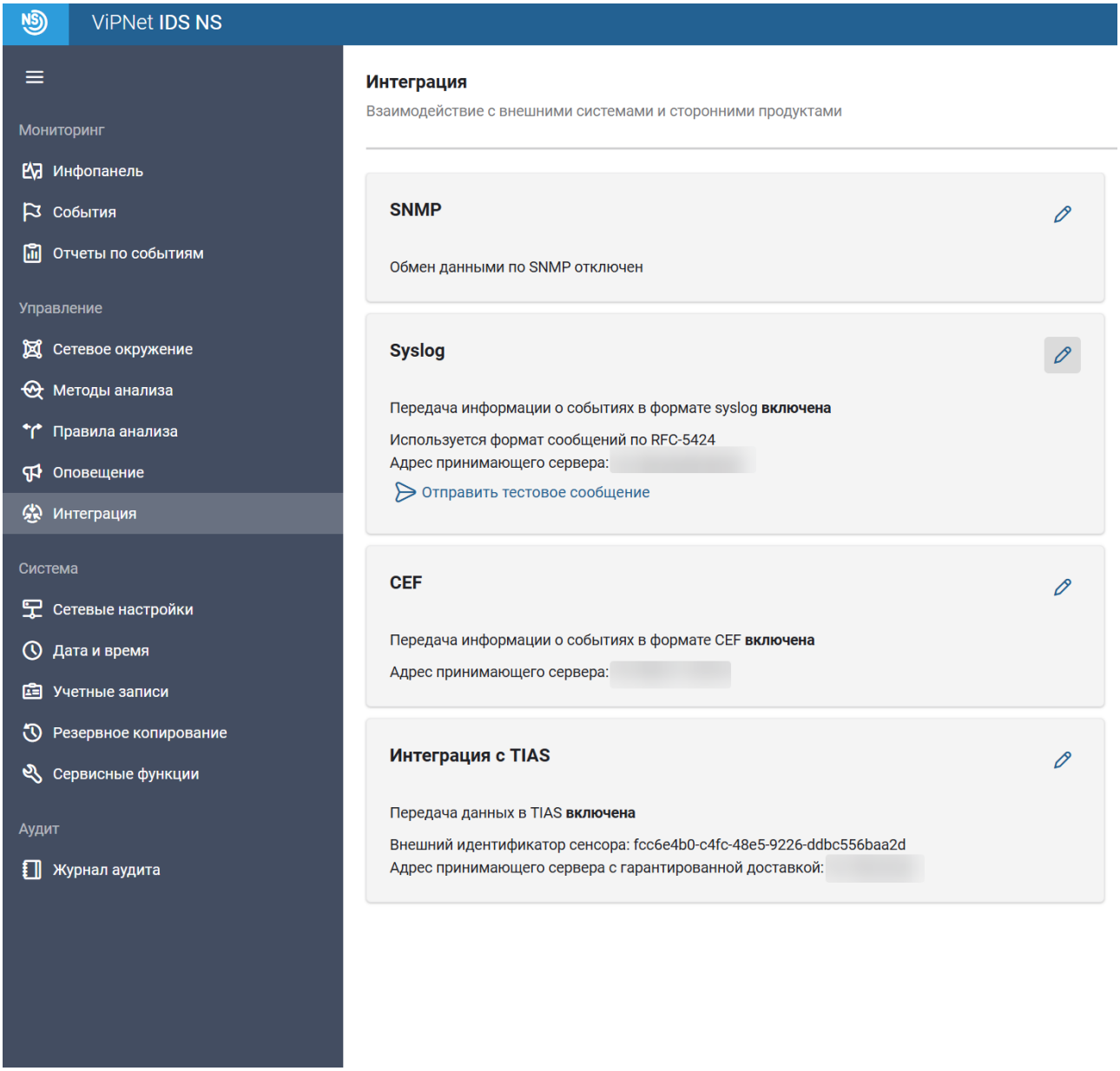
Предварительные требования

- Сетевая доступность сервера ViPNet IDS NS по целевому порту и протоколу до коллектора, который будет принимать события.

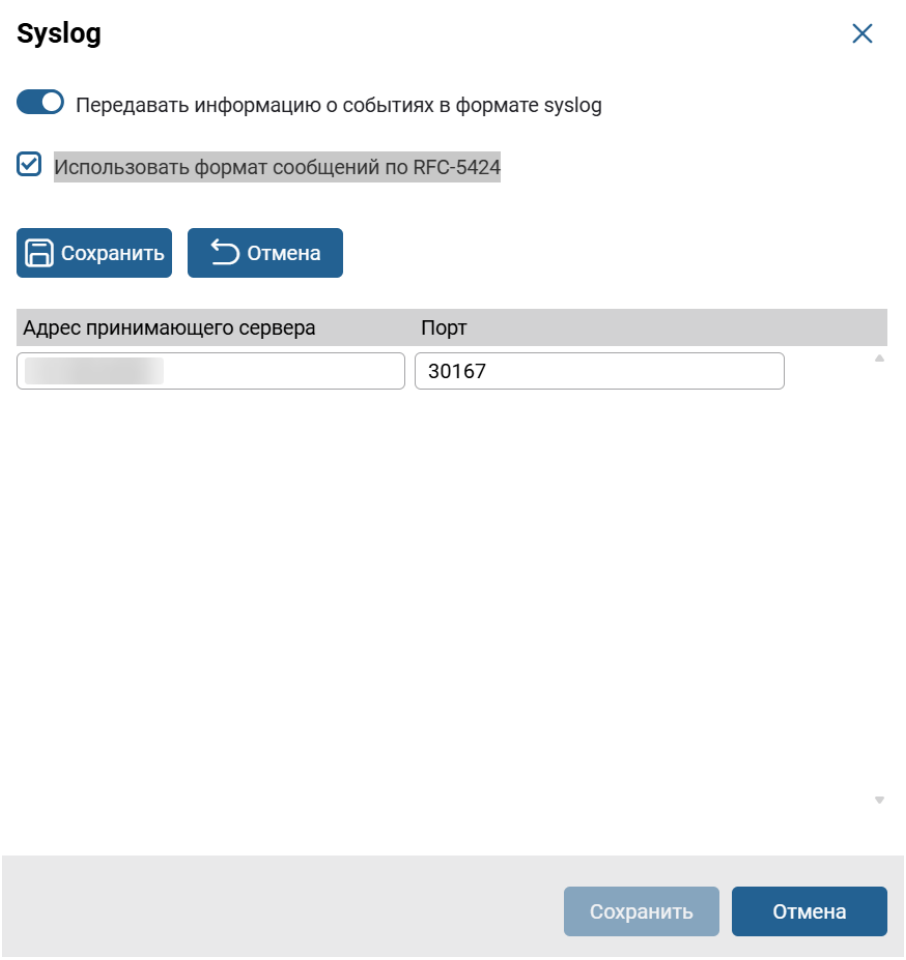
Настройка ViPNet IDS NS

Для настройки отправки событий ViPNet IDS NS в SIEM-систему в формате `syslog` выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet IDS NS.
2. В боковом меню откройте раздел **Интеграция**.
3. В форме **Syslog** откройте окно редактирования.



4. В открывшемся окне установите переключатель **Передавать информацию о событиях в формате syslog** в активное положение.
5. Нажмите на кнопку **Добавить**.
6. Установите флажок **Использовать формат сообщений по RFC-5424**.
7. В поле **Адрес принимающего сервера** введите IP-адрес коллектора R-Vision SIEM, в рамках которого планируется осуществлять сбор событий ViPNet IDS NS.
8. В поле **Порт** введите значение порта (рекомендуется использовать любой свободный порт больше 30000). В качестве транспортного протокола будет использоваться UDP.



9. Нажмите на кнопку **Сохранить**.

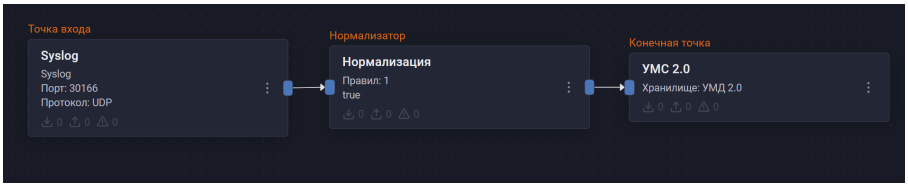
Настройка на стороне ViPNet IDS NS завершена.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне источника.
   - Протокол: выберите вариант в соответствии с настройками на стороне источника.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **ViPNet IDS NS** (идентификатор правила: **RV-N-281**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

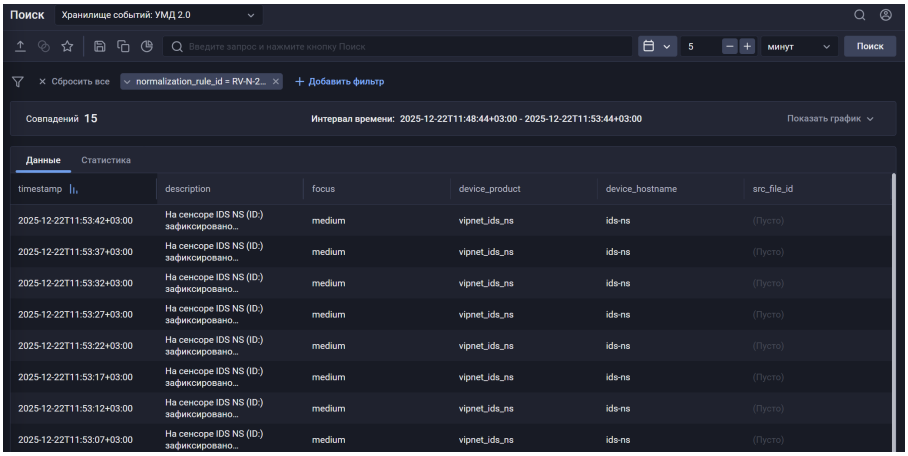
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события из ViPNet IDS NS.

Найти события ViPNet IDS NS в хранилище можно по следующему фильтру:

```
normalization_rule_id = "RV-N-281"
```



ИнфоТеКС ViPNet TIAS

- ИнфоТеКС ViPNet TIAS: настройка источника

ИнфоТеКС ViPNet TIAS: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий системы обнаружения компьютерных атак ViPNet TIAS в R-Vision SIEM.

Предварительные требования

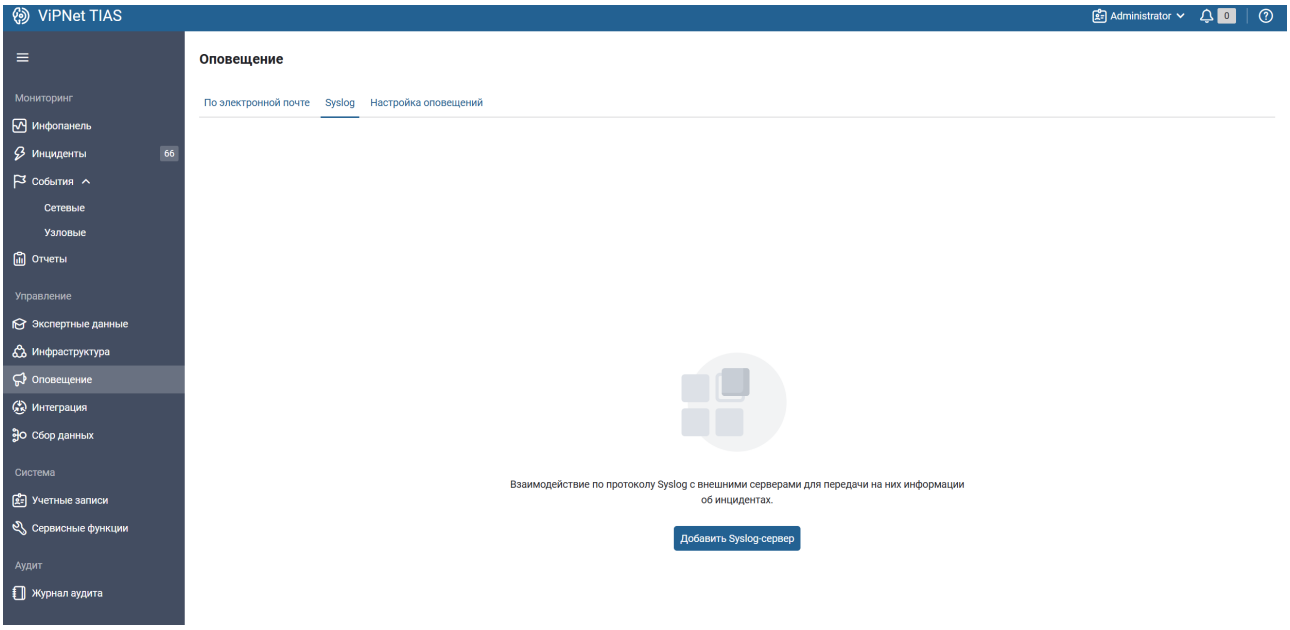
- Сетевая доступность сервера ViPNet TIAS по целевому порту и протоколу до коллектора, который будет принимать события.

Настройка ViPNet TIAS

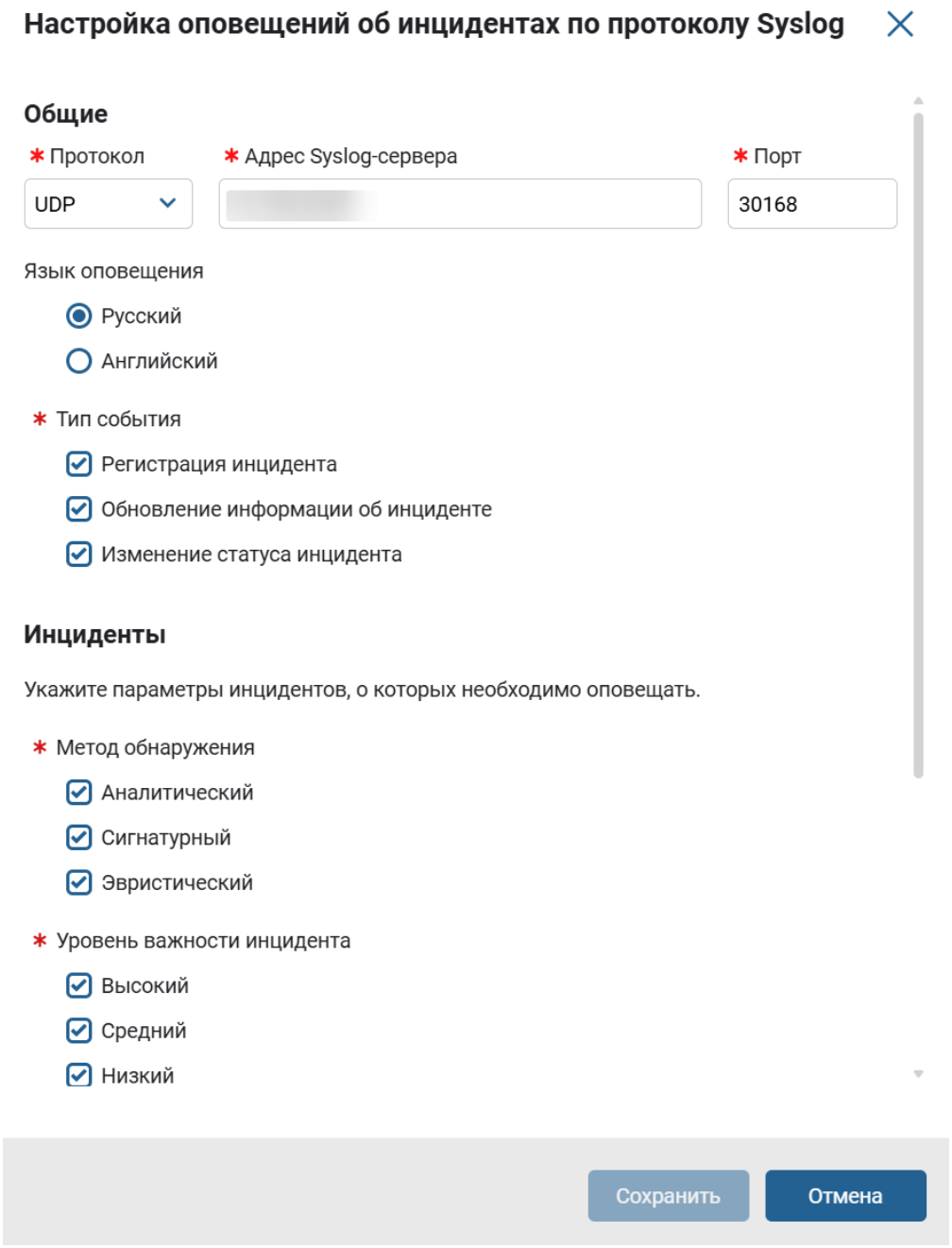
Для настройки отправки событий ViPNet TIAS в SIEM-систему в формате `syslog` выполните следующие действия:

1. Войдите в веб-интерфейс ViPNet TIAS.
2. В боковом меню откройте раздел **Оповещение**.

3. На вкладке **Syslog** нажмите на кнопку **Добавить Syslog-сервер**. Откроется окно настроек оповещений об инцидентах по протоколу Syslog.



4. В поле **Протокол** выберите значение TCP или UDP.
5. В поле **Адрес Syslog-сервера** введите адрес коллектора R-Vision SIEM, в рамках которого планируется осуществлять сбор событий ViPNet TIAS.
6. Введите значение порта (рекомендуется использовать порт больше 30000).
7. Выберите русский язык для оповещения.
8. Установите флажки в остальных полях.
9. Выберите необходимые объекты инфраструктуры.
10. Нажмите на кнопку **Сохранить**.



Настройка на стороне ViPNet TIAS завершена.

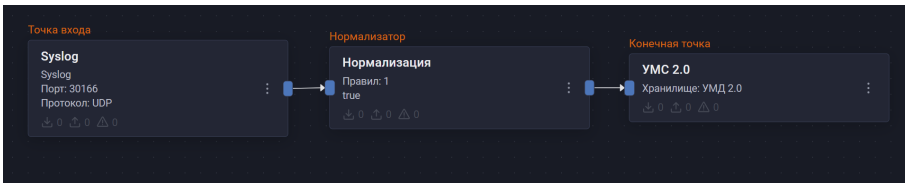
Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне источника.
   - Протокол: выберите вариант в соответствии с настройками на стороне источника.

3. Добавьте на конвейер элемент **Нормализатор** с правилом **ViPNet TIAS** (идентификатор правила: **RV-N-283**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

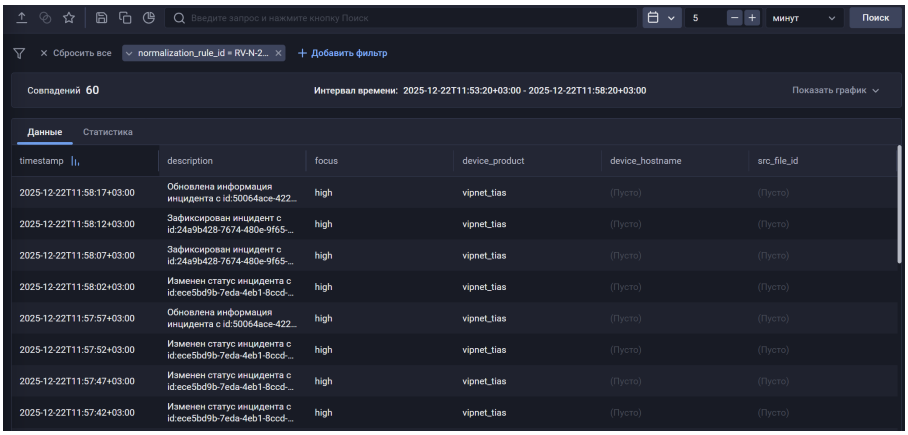
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события из ViPNet TIAS.

Найти события ViPNet TIAS в хранилище можно по следующему фильтру:

```
normalization_rule_id = "RV-N-283"
```



Системы организации терминального доступа

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых систем организации терминального доступа:

- Microsoft Windows Terminal Services

Microsoft Windows Terminal Services

- Microsoft Windows Terminal Services: настройка источника

Microsoft Windows Terminal Services: настройка источника

Данное руководство описывает процесс отправки событий из журналов Windows Terminal Services в R-Vision SIEM с помощью продукта R-Vision EVO.

Настройка Microsoft Windows Terminal Services

Настройка журналирования не требуется. События источника сохраняются в журнале Windows.

Установка и подключение агента R-Vision EVO

Установите агент R-Vision EVO на целевой хост, следуя официальной инструкции.

После установки настройте подключение агента к менеджеру агентов R-Vision SIEM в соответствии с инструкцией.

Настройка политики сбора событий в R-Vision SIEM

Для сбора событий журналов Microsoft Windows Terminal Services создайте политику сбора и добавьте в нее требуемый узел. Информацию о работе с группами агентов можно найти в инструкции по настройке групп.

Чтобы настроить сбор событий из журналов **Terminal Services**, выполните следующие шаги:

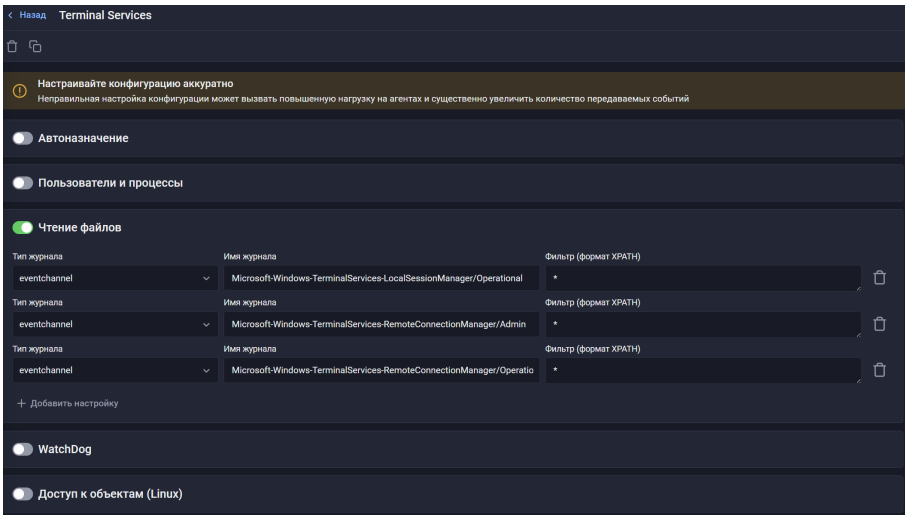
1. Перейдите к настройке нужной группы агентов.
2. Убедитесь, что переключатель **Чтение файлов** установлен в активное положение.
3. Добавьте новый элемент:
   - **Тип журналов**: `eventchannel`.
   - **Имя журналов**: `Microsoft-Windows-TerminalServices-LocalSessionManager/Operational`, `Microsoft-Windows-TerminalServices-RemoteConnectionManager/Admin`, `Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational`.
   - **Фильтр (формат XPath)**:
     - для сбора всех событий укажите символ *;
     - для сбора конкретных событий задайте XPath-фильтр.



Информацию о формировании корректных XPath-фильтров можно найти

в документации по синтаксису XPath.

Пример конфигурации:

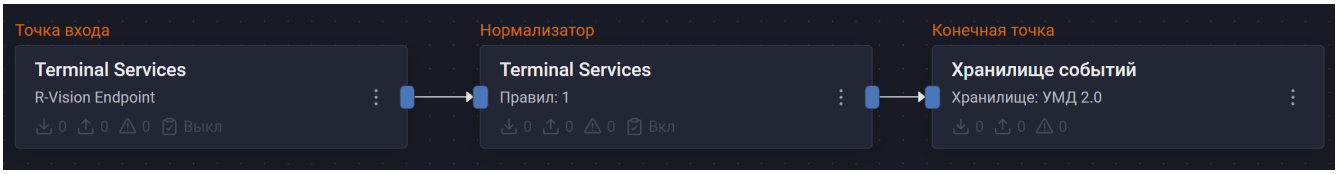


Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **R-Vision Endpoint**.
   - Домен: введите значение `gw-<your_gateway_id>`, где `<your_gateway_id>` — ID вашего шлюза.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Microsoft Windows TS RCM LSM** (идентификатор правила: **RV-N-310**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

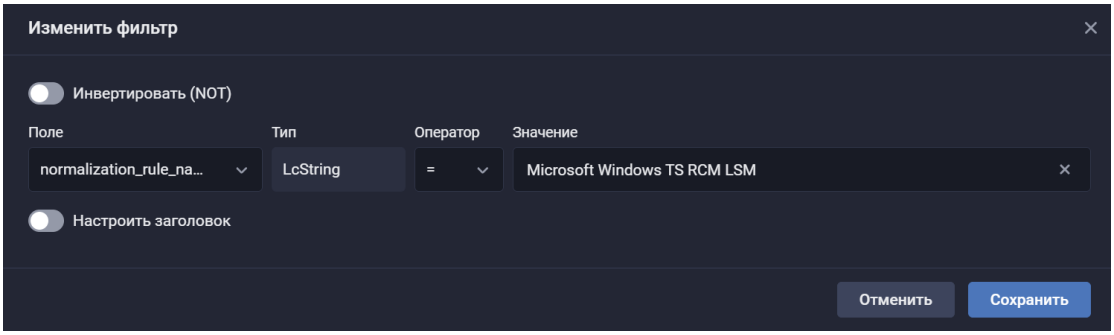
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Microsoft Windows Terminal Services.

Найти события Microsoft Windows Terminal Services в хранилище можно по следующему фильтру:

```
normalization_rule_name = "Microsoft Windows TS RCM LSM"
```



Системы организации удаленного доступа

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых систем организации удаленного доступа:

- OpenVPN
- VMware Horizon

OpenVPN

- OpenVPN: настройка источника
- OpenVPN и OpenVPN Access Server: правила корреляции

OpenVPN: настройка источника

Данное руководство описывает процесс настройки сбора событий с сервера OpenVPN и их отправки в хранилище R-Vision SIEM.

Настройка OpenVPN



Журналирование событий сервиса OpenVPN по умолчанию ведется в директории `/var/log/openvpn`. Дополнительных действий по настройке журналирования не требуется.

События сервера OpenVPN могут отправляться на централизованный сервер syslog или напрямую в систему SIEM. Далее рассмотрим оба варианта настройки.

Описание подсистемы журналирования OpenVPN

Если события сначала отправляются на сервер syslog, настройте отправку логов с сервера в SIEM. Для этого выполните следующие шаги:

1. Откройте конфигурационный файл rsyslog (`/etc/rsyslog.conf` или `/etc/rsyslog.d/`).
2. Добавьте в файл следующее правило:

```
# Укажите адрес IP-адрес SIEM и порт, куда будут отправляться события.
if $syslogtag contains 'openvpn' then {
  action(type="omfwd" target="<kub-node-fqdn>" port="<entrypoint-port>"
protocol="tcp")
  stop
}
```

Здесь:

- `<kube-node-fqdn>` — IP-адрес или полное доменное имя (FQDN) узла SIEM.
- `<entrypoint-port>` — порт точки входа, настроенный в соответствии с R-Vision SIEM

3. Перезапустите rsyslog, чтобы изменения вступили в силу:

```
sudo systemctl restart rsyslog
```

Отправка событий OpenVPN

Чтобы настроить отправку событий сервера OpenVPN, выполните следующие шаги:

1. Откройте конфигурационный файл rsyslog (`/etc/rsyslog.conf` или `/etc/rsyslog.d/`).
2. Добавьте в файл следующие правила:

```
module(load="imfile" PollingInterval="10")
input(type="imfile"
      File="/var/log/openvpn/openvpn.log"
      Tag="openvpn")
input(type="imfile"
      File="/var/log/openvpn/openvpn-status.log"
      Tag="openvpn-stat")
if $syslogtag contains 'openvpn' then {
  action(type="omfwd" target="<target>" port="<port>" protocol="udp")
  stop
}
```

   Здесь:

   - `<target>`: введите IP-адрес или полное доменное имя (FQDN) сервера syslog или узла кластера Kubernetes, на котором запущен коллектор SIEM.
   - `<port>`: для отправки событий на конвейер SIEM укажите порт точки входа Syslog — значение в диапазоне 30000—32767.

3. Перезапустите rsyslog, чтобы изменения вступили в силу:

```
sudo systemctl restart rsyslog
```

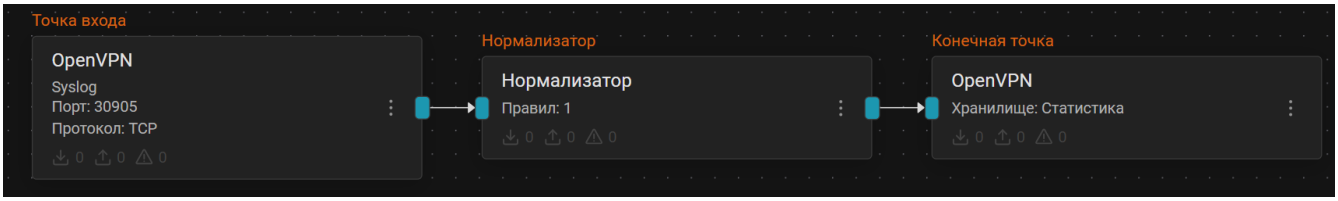
Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** типа **Syslog** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне сервера syslog.
   - Протокол: выберите вариант в соответствии с настройками на стороне сервера syslog.

3. Добавьте на конвейер элемент **Нормализатор** с одним из следующих правил:
    - **OpenVPN** (идентификатор правила: **RV-N-225**);
    - **OpenVPN** (идентификатор правила: **RV-N-226**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

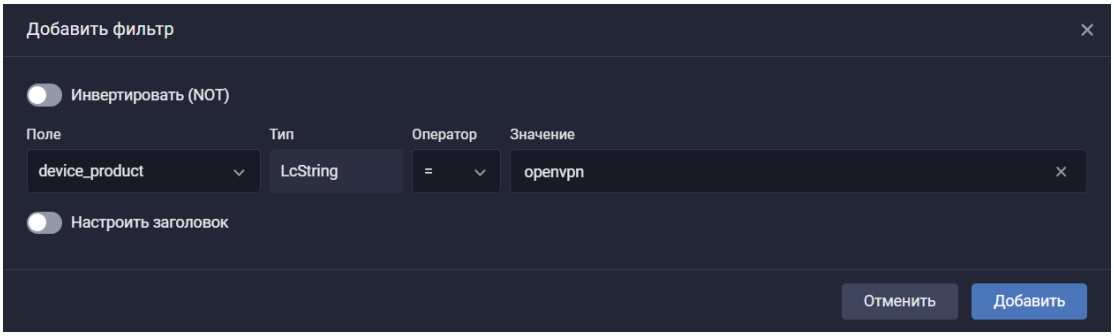
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события OpenVPN.

Найти события OpenVPN в хранилище можно по следующему фильтру:

```
device_product = "openvpn"
```



Типы обрабатываемых событий

- Warning events
- Peer info events
- Channel events
- MULTI events
- PUSH events
- SENT CONTROL events
- Verify events
- TLS events
- Connection reset events

- Client-instance restarting events
- Peer connection initiated events
- Connection established events

OpenVPN и OpenVPN Access Server: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1239	Изменение конфигурации OpenVPN Access Server	Атакующий может попытаться изменить конфигурационный файл OpenVPN Access Server с целью отключения логирования, изменения параметров аутентификации, маршрутизации или управления подключениями пользователей. Подобные изменения могут привести к скрытию его действий, снижению уровня безопасности и затруднению обнаружения подозрительной активности. Данное правило выявляет попытки изменения файла конфигурации `as.conf`.	• Defense Evasion (TA0005) • Impair Defenses (T1562)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1242	Доступ к файлу с ключами и сертификатами OpenVPN	Данное правило направлено на защиту конфиденциальных файлов OpenVPN, содержащих ключи и сертификаты, которые могут быть использованы атакующими для проведения атак типа Man-in-the-Middle (MitM), расшифровки TLS-пакетов или создания поддельных авторизационных токенов. При получении доступа к этим файлам атакующий может подписывать свои собственные сертификаты и выдать себя за доверенное соединение, что критично для безопасности VPN-сети. При срабатывании правила необходимо уточнить у пользователя легитимность активности. Важно учитывать контекст события, например, запуск команд копирования в рамках резервного копирования или административных задач. Если обращение к файлу происходит в нестандартное время, с необычного хоста или от учетной записи, не связанной с обслуживанием OpenVPN, это может указывать на попытку компрометации.	• Resource Development (TA0042) • Collection (TA0009) • Data Staged (T1074) • Develop Capabilities (T1587) • Digital Certificates (T1587.003) • Obtain Capabilities (T1588) • Digital Certificates (T1588.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1316	Подбор пароля клиента OpenVPN	Множество неудачных попыток аутентификации OpenVPN-клиента могут указывать на попытку перебора пароля или brute-force-атаку, направленную на получение несанкционированного доступа к VPN. Такое поведение свидетельствует о возможных действиях атакующего, который пытается подключиться к серверу OpenVPN, используя .ovpn-профиль с подбором учетных данных. Если атакующий успешно подберет пароль, это может привести к компрометации учетной записи VPN-пользователя и доступу к внутренним ресурсам компании, что создаст угрозу утечки данных или последующих атак внутри сети.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)
RV-D-1320	Подбор пароля в веб-консоль OpenVPN AS	Множество неудачных попыток входа могут указывать на попытку подобрать пароль или осуществить брутфорс-атаку, направленную на кражу учетных записей. Такое поведение указывает на возможное вмешательство атакующего, который пытается получить несанкционированный доступ к веб-консоли OpenVPN Access Server. Если атакующий получит успешный доступ к веб-консоли OpenVPN Access Server, это может привести к компрометации учетных данных, созданию или модификации VPN-пользователей, изменению настроек VPN-сервера, перехвату и анализу трафика, а также развитию атаки внутри сети, что поставит под угрозу внутренние ресурсы компании.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1321	Подключение OpenVPN за пределами России	OpenVPN широко используется для создания защищенных каналов связи через Интернет, обеспечивая шифрование и аутентификацию трафика. Однако в корпоративных сетях важно контролировать географию подключений, так как удаленный доступ из-за пределов России может указывать на компрометацию учетных данных, обход корпоративных ограничений или несанкционированную активность. Данное правило обнаруживает успешные подключения к OpenVPN из геолокации, не принадлежащей России.	• Initial Access (TA0001) • Valid Accounts (T1078) • External Remote Services (T1133)
RV-D-1322	Множество неуспешных HTTP-запросов к OpenVPN AS	Правило предназначено для выявления множества неуспешных HTTP-запросов (например, с кодом 404) к админ-панели OpenVPN Access Server. Это может указывать на попытки сканирования или активного поиска уязвимостей в публично доступном приложении. Такая активность часто исходит из Интернета и может быть признаком попытки эксплуатации или DDoS-атаки.	• Reconnaissance (TA0043) • Initial Access (TA0001) • Exploit Public-Facing Application (T1190) • Active Scanning (T1595) • Wordlist Scanning (T1595.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1324	Аномальный HTTP-запрос к webUI Access Server	Данное правило корреляции предназначено для выявления аномальных HTTP-запросов к административной панели Access Server OpenVPN. Админ-панель OpenVPN Access Server представляет собой веб-интерфейс, используемый администраторами для управления серверами OpenVPN, настройками пользователей и мониторингом сессий. Правило выявляет попытки доступа к админ-панели Access Server, которые не соответствуют профилю легитимных администраторов. Сравнение осуществляется по IP-адресу.	• Initial Access (TA0001) • Valid Accounts (T1078) • External Remote Services (T1133)

VMware Horizon

- VMware Horizon: настройка источника

VMware Horizon: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий VMware Horizon в R-Vision SIEM.

Предварительные требования

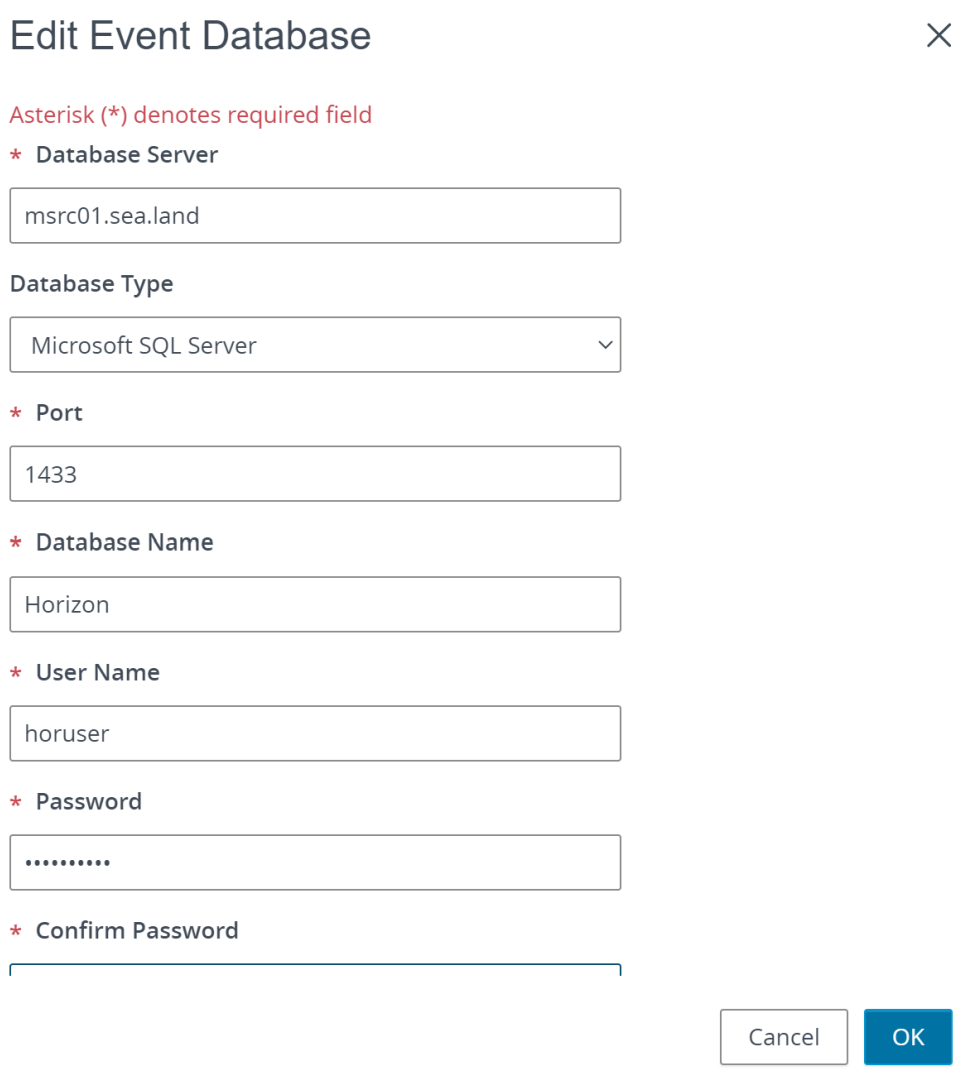
Перед настройкой пересылки событий в R-Vision SIEM убедитесь в выполнении следующих условий:

- Создана учетная запись с правами администратора VMware Horizon для настройки отправки событий.
- Сетевая связность между сервером VMware Horizon и SIEM (или промежуточным syslog-сервером) обеспечена, а необходимые порты открыты.

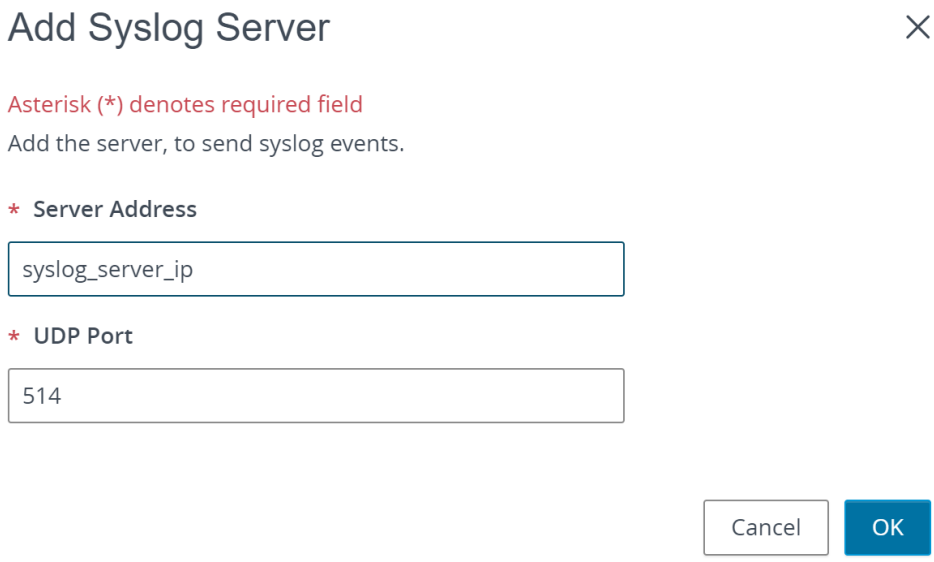
Настройка VMware Horizon

Для настройки источника выполните следующие шаги:

1. Войдите в веб-интерфейс VMware Horizon.
2. Перейдите в раздел **Settings** → **Event Configuration**.
3. На вкладке **Event Database** нажмите на кнопку **Edit**.
4. В открывшемся окне заполните данные о вашей базе данных для сохранения событий.



5. На вкладке **Syslog** нажмите на кнопку **Add**.
6. В открывшемся окне укажите следующие параметры:
   a. Server Address: укажите IP-адрес или FQDN коллектора SIEM или централизованного syslog-сервера.
   b. UDP Port: укажите порт коллектора SIEM или централизованного syslog-сервера.



7. Нажмите на кнопку **OK**.

Отправка событий VMware Horizon в SIEM настроена.

Настройка в R-Vision SIEM

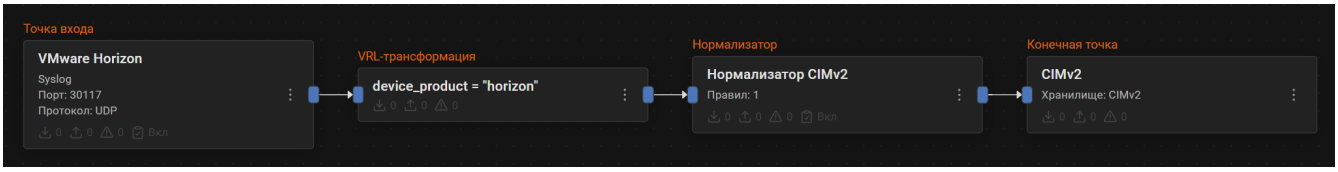
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне VMware Horizon.
   - Протокол: выберите вариант в соответствии с настройками на стороне VMware Horizon.
3. Добавьте VRL-трансформацию:

```
.device_product = "horizon"
```

4. Соедините добавленную точку входа и VRL-трансформацию.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **VMware Horizon** (идентификатор правила: **RV-N-295**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Установите конфигурацию конвейера.

Пример конфигурации конвейера:

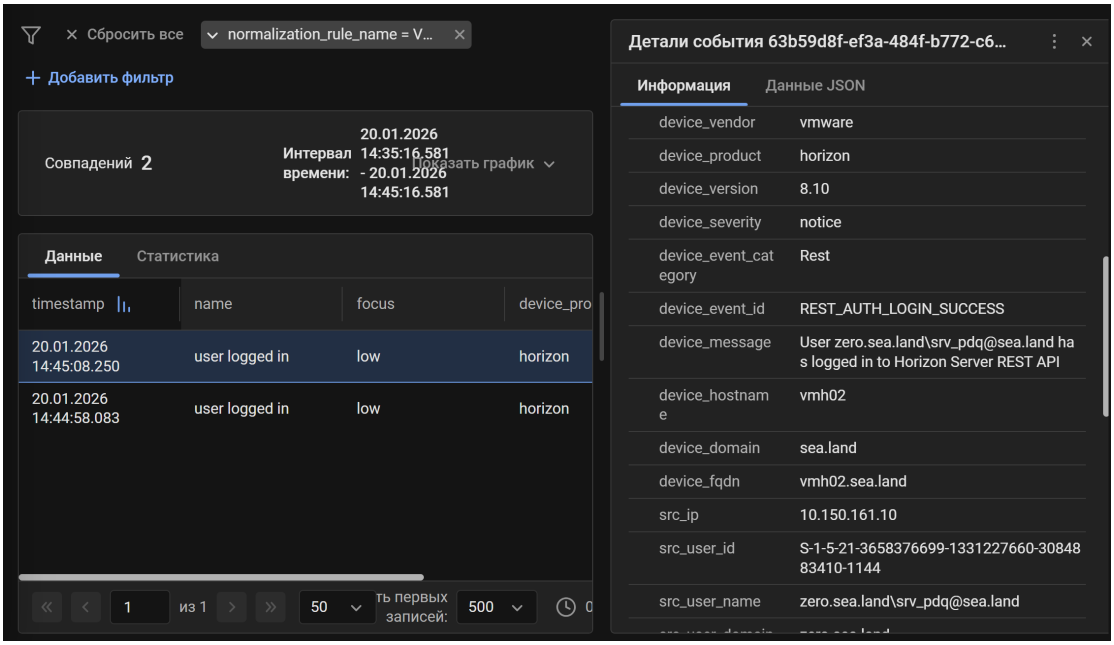


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события VMware Horizon.



Найти события VMware Horizon в хранилище можно по следующему фильтру:

```
normalization_rule_name = "VMware Horizon"
```


Сбросить все
normalization_rule_name = V...
Добавить фильтр
Совпадений 2
Интервал времени: 20.01.2026 14:35:16.581 - 20.01.2026 14:45:16.581
Показать график
Данные
Статистика
timestamp
name
focus
device_pro
20.01.2026 14:45:08.250
user logged in
low
horizon
20.01.2026 14:44:58.083
user logged in
low
horizon
1
из 1
50
ть первых записей:
500
Детали события 63b59d8f-ef3a-484f-b772-c6...
Информация
Данные JSON
device_vendor
vmware
device_product
horizon
device_version
8.10
device_severity
notice
device_event_category
Rest
device_event_id
REST_AUTH_LOGIN_SUCCESS
device_message
User zero.sea.land\srv_pdq@sea.land has logged in to Horizon Server REST API
device_hostname
vmh02
device_domain
sea.land
device_fqdn
vmh02.sea.land
src_ip
10.150.161.10
src_user_id
S-1-5-21-3658376699-1331227660-3084883410-1144
src_user_name
zero.sea.land\srv_pdq@sea.land

Системы предотвращения утечек данных (DLP)

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых систем предотвращения утечек данных:

- InfoWatch Traffic Monitor
- Solar Dozor
- Гарда DLP
- СёрчИнформ КИБ

InfoWatch Traffic Monitor

- InfoWatch Traffic Monitor: настройка источника

InfoWatch Traffic Monitor: настройка источника

Данная инструкция описывает настройку сбора событий на сервере InfoWatch Traffic Monitor и последующую отправку в R-Vision SIEM.

Предварительные требования

Чтобы работать с InfoWatch Traffic Monitor, убедитесь, что у вас имеется:

- сетевой доступ к БД;
- учетная запись в СУБД с правами на чтение таблиц **arc_view_audit_log** и **arc_view_objects2**.

Настройка InfoWatch Traffic Monitor

Описание подсистемы журналирования

InfoWatch Traffic Monitor записывает свои события в таблицы **arc_view_audit_log** и **arc_view_objects2** базы данных Postgres.

Чтобы настроить сбор логов из базы данных, необходимо к ней подключиться, используя специальную сервисную учетную запись (далее — УЗ).

Создание сервисной учетной записи в PostgreSQL

Чтобы создать сервисную УЗ, подключитесь к СУБД с правами администратора. Для этого выполните следующие действия на сервере с установленной СУБД:

1. Выполните следующую команду от имени пользователя postgres:

   ```
   sudo -u postgres psql
   ```

2. Создайте сервисную учетную запись, выполнив следующие команды:

```
CREATE USER "infowatch";
ALTER ROLE infowatch WITH PASSWORD 'passw0rd';
```

3. Выдайте созданной УЗ права на подключение к базе и чтение таблицы:

```
GRANT CONNECT ON DATABASE postgres to infowatch;
GRANT SELECT ON arc_view_audit_log TO infowatch;
GRANT SELECT ON arc_view_objects2 TO infowatch;
```

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте секрет со строкой подключения. Для этого:
   a. Перейдите в раздел **Ресурсы** → **Секреты** и нажмите на кнопку **Создать**.
   b. В раскрывшемся окне создания секрета заполните поля:
      - Описание (опционально): опишите, для чего будет использоваться секрет.
      - Тип секрета: выберите вариант **Строка подключения**.
      - Строка подключения: введите строку вида:

```
jdbc:postgresql://<address>:<port>/<database>?user=<user>&password=<password
>
```

        где:

        - `<address>` — адрес сервера базы.
        - `<port>` — порт подключения.
        - `<database>` — имя базы событий аудита.
        - `<user>` — логин пользователя базы.
        - `<password>` — пароль пользователя базы.

        Пример 2. Пример строки подключения

```
jdbc:postgresql://DBSERVER:5432/postgres?user=infowatch&password=passw0rd
```

   c. Нажмите на кнопку **Создать**.
2. Перейдите в раздел **Ресурсы** → **Коллекторы** и создайте новый конвейер в коллекторе.
3. Добавьте на конвейер элементы **Точка входа**. Понадобится создать две точки входа, для таблицы **arc_view_audit_log** и **arc_view_objects2**. Поля для обеих точек идентичны, за исключением SQL-запроса:
   - Название: название точки входа.

- Тип точки входа: Database.
- SQL-запрос для таблицы **arc_view_audit_log**: события InfoWatch TM:

```
SELECT CAST(AUDIT_LOG_ID AS bigint) AS AUDIT_LOG_ID_KF,
change_date,
operation,
entity_type,
entity_display_name,
entity_id,
property_changes,
user_login,
user_fullname,
user_email FROM iwtm.arc_view_audit_log WHERE change_date >
(SELECT CURRENT_TIMESTAMP - INTERVAL '1 minutes') ORDER BY AUDIT_LOG_ID LIMIT
1000;
```

- SQL-запрос для таблицы **arc_view_objects2**: аудит пользователей InfoWatch TM:

```
SELECT cast(insert_date as VARCHAR(26)) AS "EVENT_DATE_KF",
insert_date AS "INSERT_DATE",
capture_server_hostname AS "CAPTURE_SERVER_HOSTNAME",
capture_server_ip AS "CAPTURE_SERVER_IP",
categories AS "CATEGORIES",
date_of_capture AS "DATE_OF_CAPTURE",
device AS "DEVICE_NAME",
filepath AS "FILEPATH",
fingerprints AS "FINGERPRINTS",
monitorcode AS "MONITOR_CODE",
object_id AS "OBJECT_ID",
perimetersin AS "PERIMETERSIN",
perimetersout AS "PERIMETERSOUT",
policies AS "POLICIES",
protecteddocuments AS "PROTECTED_DOCUMENTS",
protocol AS "PROTOCOL",
recipientscontacts AS "RECIPIENTSCONTACTS",
recipientsfullname AS "RECIPIENTSFULLNAME",
sendermachinecontacts AS "SENDERMACHINECONTACTS",
sendermachinefullname AS "SENDERMACHINEFULLNAME",
senderscontacts AS "SENDERSCONTACTS",
sendersfullname AS "SENDERSFULLNAME",
tags AS "TAGS",
text_objects AS "TEXT_OBJECTS",
url AS "URL",
userdecision AS "USER_DECISION",
verdict AS "VERDICT",
violationtype AS "VIOLATION_TYPE",
websource AS "WEBSOURCE" FROM iwtm.arc_view_objects2
WHERE insert_date > cast('EVENT_DATE_KF' as timestamp)
```

```
ORDER BY insert_date LIMIT 10000;
```

- База данных: PostgreSQL.
- Интервал запроса: от 15 до 60.
- Поле идентификатора:
  - Ключ: `EVENT_DATE_KF`.
  - Значение: `1970-01-01 00:00:00`.
- Строка подключения в секрете:

  ```
  jdbc:postgresql://<address>:<port>/postgres?user=infowatch&password=passw0rd
  ```

  Здесь:

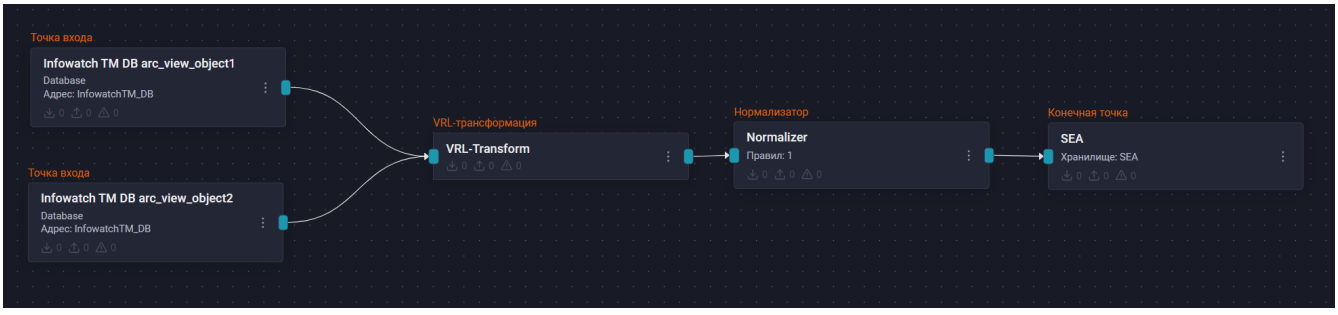
  - `<address>` — FQDN или IP-адрес сервера СУБД.
  - `<port>` — порт подключения.

4. Добавьте VRL-трансформацию:

   ```
   .device_product = "Traffic Monitor"
   ```

5. Соедините добавленную точку входа и VRL-трансформацию.
6. Добавьте нормализатор с правилом **InfoWatch Traffic Monitor** (**RV-N-198**).
7. Соедините нормализатор с VRL-трансформацией.
8. Добавьте конечную точку типа **Хранилище событий**.
9. Соедините конечную точку с нормализатором.
10. Установите конфигурацию конвейера.

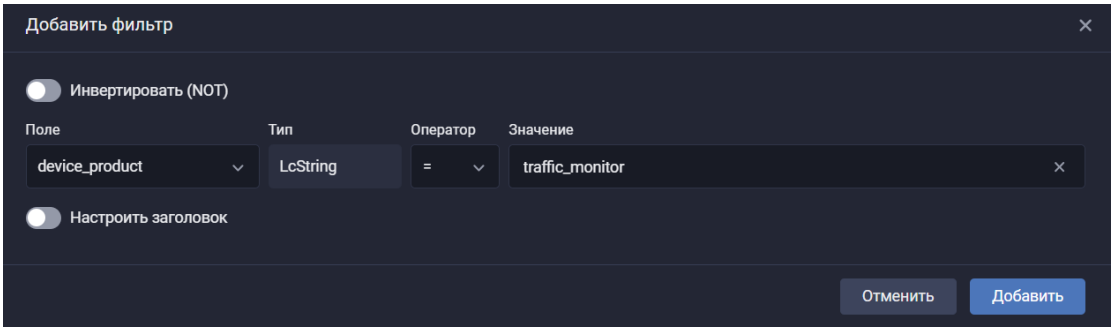
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события InfoWatch.

Найти события источника в хранилище можно по следующему фильтру:

```
device_product = "traffic_monitor"
```



InfoWatch Traffic Monitor: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1519	Password Spraying в InfoWatch TM	Правило обнаруживает неудачные попытки аутентификации с разными учетными записями в InfoWatch TM. В случае возникновения активности необходимо опросить ответственного за хост, инициирующий запросы аутентификации.	• Credential Access (TA0006) • Brute Force (T1110) • Password Spraying (T1110.003)
RV-D-1555	Атака Brute Force к InfoWatch TM	Правило обнаруживает множественные неудачные попытки подключения к InfoWatch TM от одной учетной записи.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1556	Создание администратора в InfoWatch TM	Атакующий в рамках закрепления может создать новую учетную запись и выдать ей права администратора на случай, если скомпрометированную УЗ ограничат. Права в системе InfoWath TM представляют собой различные роли, которые имеют определенные привилегии. Выдача новой роли с одной из критичных административных привилегий может указывать на вредоносную активность, так как доступ к компонентам системы основывается на ролевой системе разграничения прав доступа.	• Persistence (TA0003) • Valid Accounts (T1078) • Default Accounts (T1078.001) • Local Accounts (T1078.003) • Create Account (T1136) • Local Account (T1136.001)
RV-D-1559	Создание роли администратора в InfoWatch TM	Атакующий в рамках закрепления может создать новую учетную запись и выдать ей права администратора на случай, если скомпрометированную УЗ ограничат. Правило обнаруживает создание новой роли с правами Администратора и назначение её пользователю в панели InfoWatch TM.	• Persistence (TA0003) • Valid Accounts (T1078) • Default Accounts (T1078.001) • Local Accounts (T1078.003) • Account Manipulation (T1098)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1560	Массовое удаление пользователей	Атакующие могут сделать системы и сетевые ресурсы недоступными, препятствуя доступу к учетным записям легитимных пользователей. Для предотвращения доступа к учетным записям они могут быть удалены, заблокированы или изменены (например, могут быть изменены их учетные данные). Правило обнаруживает множественные удаления учетных записей в InfoWatch TM от одной учетной записи.	• Impact (TA0040) • Account Access Removal (T1531)
RV-D-1561	Отключение политики защиты данных в InfoWatch TM	Политики — совокупность правил, в соответствии с которыми проводится анализ и обработка объектов перехвата. Правило состоит из набора условий, по которым выполняется проверка объекта, и действий, осуществляемых при выполнении или невыполнении заданных условий. Политика реагирует на предполагаемые действия персон в соответствии с заданным алгоритмом ответных действий системы, которые были заданы офицером безопасности или администратором. Правило обнаруживает отключение политики защиты данных в панели InfoWatch TM и применение конфигурации.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)
RV-D-1564	Успешная атака Brute Force к InfoWatch TM	Правило детектирует успешный вход в панель управления InfoWatch TM после нескольких попыток неудачной аутентификации.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)

Solar Dozor

- Solar Dozor: настройка источника

Solar Dozor: настройка источника

Данное руководство содержит инструкции по настройке подключения Solar Dozor к системе R-Vision SIEM.

Настройка Solar Dozor

Для передачи событий Solar Dozor в систему R-Vision SIEM необходим инструмент `syslog-ng`.

Если в вашей системе не установлен `syslog-ng`, выполните следующие шаги:

1. Установите `syslog-ng` с помощью команды:

```
apt install syslog-ng
```



Учетная запись должна иметь привилегии для установки сторонних пакетов.

2. Создайте конфигурацию источника, как описано в документации Dozor.
3. Разместите конфигурацию источника в файле `/etc/syslog-ng/conf.d/dozor.conf`.
4. Если настройка выполнена корректно, то записанные события будут собираться в директории `/var/log/dozor`.

Пример 3. Пример конфигурации

```
@define allow-config-dups 1
# Адрес и порт сервера syslog:
@define REMOTE_SERVER "c7-syslog.example.com"
@define REMOTE_PORT 10514
filter f_dozor_unit {match("dozor" value (".journald._SYSTEMD_UNIT"));};
filter f_syslog3 { not facility(auth, authpriv, mail) and not filter(f_debug) and
not filter(f_dozor_unit);
};
destination d_tcp_q {
    syslog("`REMOTE_SERVER`" transport("tcp") port(`REMOTE_PORT`)
    disk-buffer(
        reliable(yes)
        dir("/var/lib/syslog-ng")
        disk-buf-size(524288000)
        mem-buf-size(134217728)
        qout-size(10000)
        )
    );
};
destination d_dozor {
    file("/var/log/dozor/${PROGRAM}.log"
```

```
    create-dirs(yes) dir-group("dozor") dir-owner("dozor") dir-perm(0755)
    group("dozor") owner("dozor") perm(0640)
    );
};
log {
    source(s_src); filter(f_dozor_unit); destination(d_dozor);
};
log {
    source(s_src);
    filter(f_dozor_unit);
    destination(d_tcp_q);
    flags(final,flow-control);
};
```

5. Найдите все необходимые файлы логов в директории `/var/log/dozor` с помощью следующей команды:

```
find /var/log/dozor -type f -printf 'file("%p" flags(no-parse));\n
```

6. Дополните файл `dozor.conf` следующим содержимым:

```
    source sys_input {
        file("/var/log/dozor/software-center-database.log" flags(no-parse));
        <files>
};

destination d_siem {
    network("<target>" port(<port>) transport(<protocol>));
};

log {
        source(sys_input);
        destination(d_siem);
};
```

   Здесь:

   - `<files>` — источники `file()` с указанием путей к файлам, полученным на предыдущем шаге.
   - `<target>` — IP-адрес или полное доменное имя кластера Kubernetes, где будет запущен конвейер для обработки событий.
   - `<port>` — порт, на который принимаются события.
   - `<protocol>` — используемый протокол (`tcp` или `udp`).

7. Перезагрузите службу `syslog-ng` с помощью команды:

```
systemctl restart syslog-ng
```

8. Проверьте, что события отправляются, с помощью команды:

```
tail -f /var/log/syslog
```

Настройка на стороне источника завершена.

Настройка в R-Vision SIEM

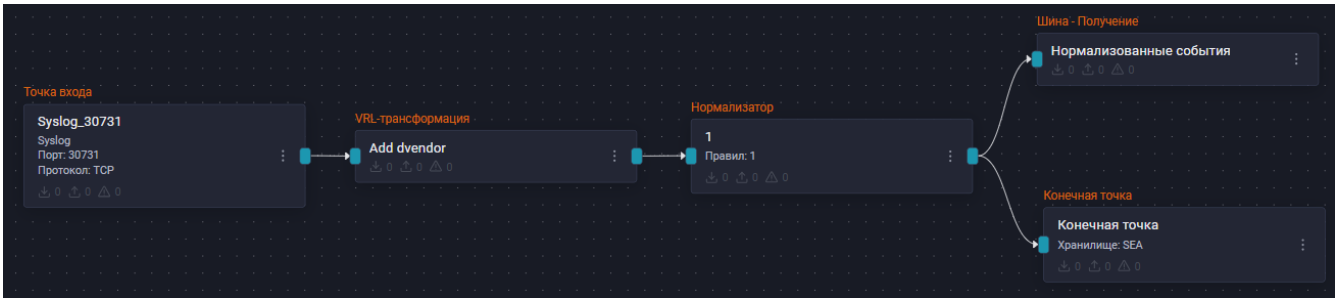
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне сервера syslog.
   - Протокол: выберите вариант в соответствии с настройками на стороне сервера syslog.
3. Добавьте на конвейер элемент **VRL-трансформация** со следующим кодом:

```
.device_vendor = "solar"
.device_product = "dozor"
```

4. Соедините VRL-трансформацию с точкой входа.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **Solar Dozor** (идентификатор правила: **RV-N-219**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Для отправки событий в коррелятор добавьте на конвейер шину, настроенную на получение.
10. Соедините шину с нормализатором.
11. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

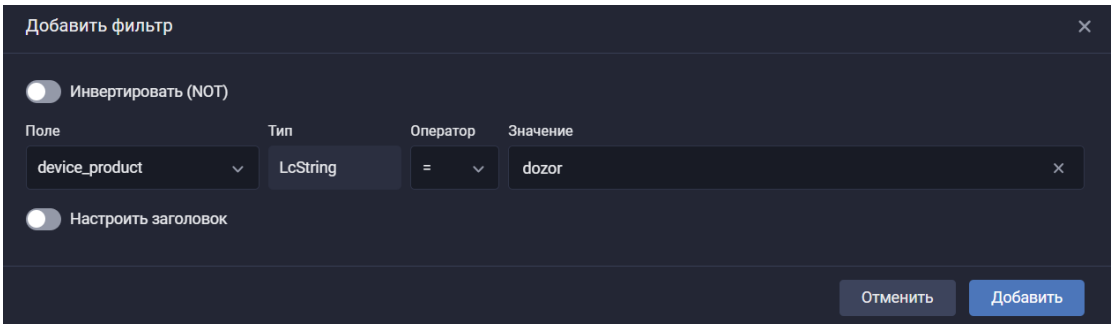


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут

поступать события Solar Dozor.

Найти события Solar Dozor в хранилище можно по следующему фильтру:

```
device_product = "dozor"
```



Гарда DLP

- Гарда DLP: настройка источника

Гарда DLP: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий комплекса Гарда DLP в R-Vision SIEM.

Предварительные требования

Перед настройкой сбора событий в R-Vision SIEM убедитесь в выполнении следующих условий:

- Сетевая связность между сервером Гарда DLP или промежуточным сервером `syslog` обеспечена, а необходимые порты открыты.

Настройка Гарда DLP

Система позволяет отправлять события безопасности во внешние системы посредством `syslog`. Для настройки передачи система требует ввести шаблон сообщения `syslog`. В рамках инструкции подготовлены шаблоны для передачи событий, генерируемых профилями безопасности по умолчанию.

Для настройки передачи событий `syslog` в Гарда DLP:

1. Войдите в консоль администратора Гарда DLP.
2. Перейдите по пути **Настройки** → **Экспорт в SIEM**.
3. Нажмите на кнопку **Добавить новый шаблон экспорта в SIEM**, чтобы создать шаблоны экспорта под каждый профиль по умолчанию.
4. Заполните общие поля для создаваемого шаблона:
    - **IP-адрес**: укажите IP-адрес коллектора SIEM.

- **Порт**: укажите порт, который настроен в SIEM для приема событий с источника.
- **Протокол**: выберите протокол, настроенный в SIEM.
- **Формат**: выберите вариант `CEF`.

5. Укажите шаблон сообщения для каждого профиля:
   - Для профиля **ПДН в почте, мессенджерах, загрузка на сайты** используйте следующий шаблон:

```
src=$Garda.uni_ip dst=$Garda.peer_ip sport=$Garda.uni_port
dport=$Garda.peer_port suser=$Garda.account cs1=$Garda.action_type
action=$Garda.user_action objType=$Garda.type count_pages=$Garda.count
name=$Garda.name time=$Garda.time time_real=$Garda.time_real
time_start=$Garda.time_start time_stop=$Garda.time_stop
uni_email=$Garda.uni_email peer_email=$Garda.peer_email
have_attach=$Garda.have_attach url=$Garda.url content_type=$Garda.content_type
http_type=$Garda.http_type size=$Garda.size web_obj_id=$Garda.web_obj_id
web_parent_id=$Garda.web_parent_id web_object_type=$Garda.web_object_type
result_code=$Garda.result_code referer=$Garda.referer
content_encoding=$Garda.content_encoding web_uni_id=$Garda.web_uni_id
web_peer_id=$Garda.web_peer_id web_source_id=$Garda.web_source_id
protocol=$Garda.protocol proto_descr=$Garda.proto_descr channel=$Garda.channel
uni_ident=$Garda.uni_ident peer_ident=$Garda.peer_ident subject=$Garda.subject
login=$Garda.login chat_id=$Garda.chat_id send_time=$Garda.send_time
mail_partid=$Garda.mail_partid mail_flags=$Garda.mail_flags
uni_is_server=$Garda.uni_is_server uni_is_sender=$Garda.uni_is_sender
blocking_action=$Garda.blocking_action
cat="ПДН_в_почте,_мессенджерах,_загрузка_на_сайты" uni_phone=$Garda.uni_phone
peer_phone=$Garda.peer_phone account=$Garda.account
user_action=$Garda.user_action type_action=$Garda.type_action
prop_text_part=$Garda.prop_text_part
```

   - Для профиля **Использование подозрительного ПО** используйте следующий шаблон:

```
src=$Garda.uni_ip dst=$Garda.peer_ip sport=$Garda.uni_port
dport=$Garda.peer_port suser=$Garda.account cs1=$Garda.action_type
action=$Garda.user_action objType=$Garda.type count_pages=$Garda.count
name=$Garda.name time=$Garda.time time_real=$Garda.time_real
time_start=$Garda.time_start time_stop=$Garda.time_stop
process_name=$Garda.process_name process_id=$Garda.process_id
action_type=$Garda.action_type user_action=$Garda.user_action
device_name=$Garda.device_name serial_id=$Garda.serial_id
protocol=$Garda.protocol proto_descr=$Garda.proto_descr channel=$Garda.channel
uni_is_server=$Garda.uni_is_server uni_is_sender=$Garda.uni_is_sender
blocking_action=$Garda.blocking_action cat="Использование_подозрительного_ПО"
```

   - Для профиля **Документы и архивы с паролем** используйте следующий шаблон:

```
src=$Garda.uni_ip dst=$Garda.peer_ip sport=$Garda.uni_port
dport=$Garda.peer_port suser=$Garda.account cs1=$Garda.action_type
action=$Garda.user_action objType=$Garda.type count_pages=$Garda.count
name=$Garda.name time=$Garda.time time_real=$Garda.time_real
time_start=$Garda.time_start time_stop=$Garda.time_stop
uni_email=$Garda.uni_email peer_email=$Garda.peer_email
have_attach=$Garda.have_attach path=$Garda.path file_size=$Garda.file_size
process_name=$Garda.process_name flags=$Garda.flags
device_name=$Garda.device_name serial_id=$Garda.serial_id url=$Garda.url
content_type=$Garda.content_type http_type=$Garda.http_type size=$Garda.size
web_obj_id=$Garda.web_obj_id web_parent_id=$Garda.web_parent_id
web_object_type=$Garda.web_object_type result_code=$Garda.result_code
referer=$Garda.referer content_encoding=$Garda.content_encoding
web_uni_id=$Garda.web_uni_id web_peer_id=$Garda.web_peer_id
web_source_id=$Garda.web_source_id protocol=$Garda.protocol
proto_descr=$Garda.proto_descr channel=$Garda.channel login=$Garda.login
chat_id=$Garda.chat_id send_time=$Garda.send_time mail_partid=$Garda.mail_partid
mail_flags=$Garda.mail_flags uni_is_server=$Garda.uni_is_server
uni_is_sender=$Garda.uni_is_sender blocking_action=$Garda.blocking_action
cat="Документы_и_архивы_с_паролем"
```

- Для профиля **Выгрузка БД на внешние носители** используйте следующий шаблон:

```
src=$Garda.uni_ip dst=$Garda.peer_ip sport=$Garda.uni_port
dport=$Garda.peer_port suser=$Garda.account cs1=$Garda.action_type
action=$Garda.user_action objType=$Garda.type count_pages=$Garda.count
name=$Garda.name time=$Garda.time time_real=$Garda.time_real
time_start=$Garda.time_start time_stop=$Garda.time_stop path=$Garda.path
file_size=$Garda.file_size process_name=$Garda.process_name flags=$Garda.flags
device_name=$Garda.device_name serial_id=$Garda.serial_id
protocol=$Garda.protocol proto_descr=$Garda.proto_descr channel=$Garda.channel
uni_is_server=$Garda.uni_is_server uni_is_sender=$Garda.uni_is_sender
blocking_action=$Garda.blocking_action cat="Выгрузка_БД_на_внешние_носители"
```

- Для профиля **ПДН на внешних носителях и в печати** используйте следующий шаблон:

```
src=$Garda.uni_ip dst=$Garda.peer_ip sport=$Garda.uni_port
dport=$Garda.peer_port suser=$Garda.account cs1=$Garda.action_type
action=$Garda.user_action objType=$Garda.type count_pages=$Garda.count
name=$Garda.name time=$Garda.time time_real=$Garda.time_real
time_start=$Garda.time_start time_stop=$Garda.time_stop path=$Garda.path
file_size=$Garda.file_size process_name=$Garda.process_name flags=$Garda.flags
device_name=$Garda.device_name serial_id=$Garda.serial_id
protocol=$Garda.protocol proto_descr=$Garda.proto_descr channel=$Garda.channel
uni_is_server=$Garda.uni_is_server uni_is_sender=$Garda.uni_is_sender
blocking_action=$Garda.blocking_action cat="ПДН_на_внешних_носителях_и_в_печати"
prop_text_part=$Garda.prop_text_part
```

- Для профиля **Блокировка фразы** используйте следующий шаблон:

```
src=$Garda.uni_ip dst=$Garda.peer_ip sport=$Garda.uni_port
dport=$Garda.peer_port suser=$Garda.account cs1=$Garda.action_type
action=$Garda.user_action objType=$Garda.type count_pages=$Garda.count
name=$Garda.name time=$Garda.time time_real=$Garda.time_real
time_start=$Garda.time_start time_stop=$Garda.time_stop url=$Garda.url
content_type=$Garda.content_type http_type=$Garda.http_type size=$Garda.size
process_name=$Garda.process_name web_obj_id=$Garda.web_obj_id
web_parent_id=$Garda.web_parent_id web_object_type=$Garda.web_object_type
result_code=$Garda.result_code referer=$Garda.referer
content_encoding=$Garda.content_encoding web_uni_id=$Garda.web_uni_id
web_peer_id=$Garda.web_peer_id web_source_id=$Garda.web_source_id
protocol=$Garda.protocol proto_descr=$Garda.proto_descr channel=$Garda.channel
uni_is_server=$Garda.uni_is_server uni_is_sender=$Garda.uni_is_sender
blocking_action=$Garda.blocking_action cat="Блокировка_фразы"
uni_phone=$Garda.uni_phone peer_phone=$Garda.peer_phone account=$Garda.account
user_action=$Garda.user_action type_action=$Garda.type_action
prop_text_part=$Garda.prop_text_part
```

- Для профиля **Передача исполняемых файлов в почте** используйте следующий шаблон:

```
src=$Garda.uni_ip dst=$Garda.peer_ip sport=$Garda.uni_port
dport=$Garda.peer_port suser=$Garda.account cs1=$Garda.action_type
action=$Garda.user_action objType=$Garda.type count_pages=$Garda.count
name=$Garda.name time=$Garda.time time_real=$Garda.time_real
time_start=$Garda.time_start time_stop=$Garda.time_stop
uni_email=$Garda.uni_email peer_email=$Garda.peer_email
have_attach=$Garda.have_attach subject=$Garda.subject
content_type=$Garda.content_type size=$Garda.size send_time=$Garda.send_time
mail_partid=$Garda.mail_partid mail_flags=$Garda.mail_flags
protocol=$Garda.protocol proto_descr=$Garda.proto_descr channel=$Garda.channel
uni_is_server=$Garda.uni_is_server uni_is_sender=$Garda.uni_is_sender
blocking_action=$Garda.blocking_action path=$Garda.path
file_size=$Garda.file_size mime_type=$Garda.mime_type hash=$Garda.hash
prop_text_part=$Garda.prop_text_part prop_guid=$Garda.prop_guid
prop_blob_id=$Garda.prop_blob_id cat="Передача_по_почте_исполняемого_файла"
```

- Для профиля **Кредитные карты** используйте следующий шаблон:

```
src=$Garda.uni_ip dst=$Garda.peer_ip sport=$Garda.uni_port
dport=$Garda.peer_port suser=$Garda.account cs1=$Garda.action_type
action=$Garda.user_action objType=$Garda.type count_pages=$Garda.count
name=$Garda.name time=$Garda.time time_real=$Garda.time_real
time_start=$Garda.time_start time_stop=$Garda.time_stop
uni_email=$Garda.uni_email peer_email=$Garda.peer_email
have_attach=$Garda.have_attach path=$Garda.path file_size=$Garda.file_size
process_name=$Garda.process_name flags=$Garda.flags
```

```
device_name=$Garda.device_name serial_id=$Garda.serial_id url=$Garda.url
content_type=$Garda.content_type http_type=$Garda.http_type size=$Garda.size
web_obj_id=$Garda.web_obj_id web_parent_id=$Garda.web_parent_id
web_object_type=$Garda.web_object_type result_code=$Garda.result_code
referer=$Garda.referer content_encoding=$Garda.content_encoding
web_uni_id=$Garda.web_uni_id web_peer_id=$Garda.web_peer_id
web_source_id=$Garda.web_source_id protocol=$Garda.protocol
proto_descr=$Garda.proto_descr channel=$Garda.channel uni_ident=$Garda.uni_ident
peer_ident=$Garda.peer_ident subject=$Garda.subject login=$Garda.login
chat_id=$Garda.chat_id send_time=$Garda.send_time mail_partid=$Garda.mail_partid
mail_flags=$Garda.mail_flags uni_is_server=$Garda.uni_is_server
uni_is_sender=$Garda.uni_is_sender blocking_action=$Garda.blocking_action
cat="Кредитные_карты" uni_phone=$Garda.uni_phone peer_phone=$Garda.peer_phone
account=$Garda.account user_action=$Garda.user_action
type_action=$Garda.type_action prop_text_part=$Garda.prop_text_part
```

- Для профиля **Использование удаленного доступа** используйте следующий шаблон:

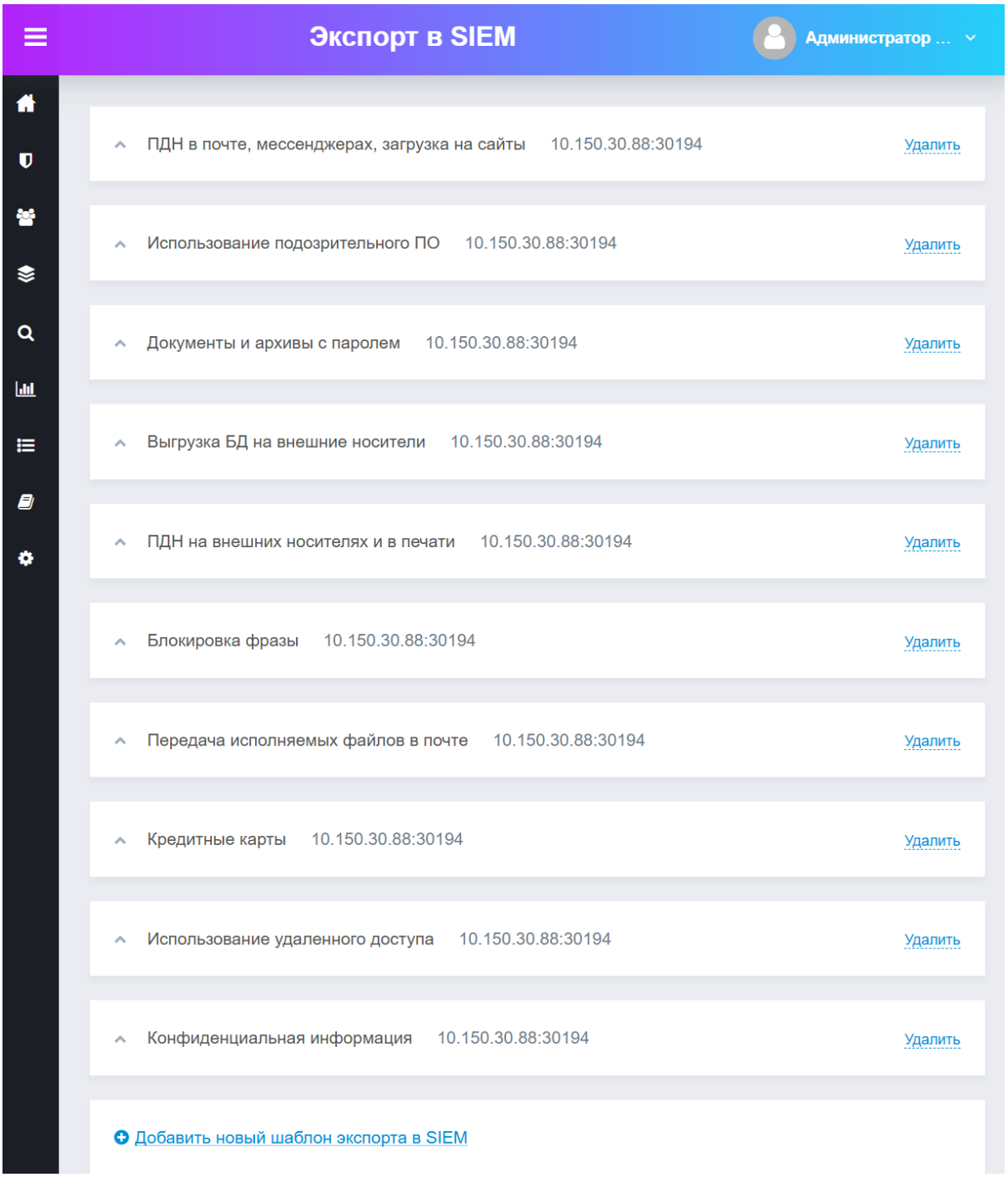
```
src=$Garda.uni_ip dst=$Garda.peer_ip sport=$Garda.uni_port
dport=$Garda.peer_port suser=$Garda.account cs1=$Garda.action_type
action=$Garda.user_action objType=$Garda.type count_pages=$Garda.count
name=$Garda.name time=$Garda.time time_real=$Garda.time_real
time_start=$Garda.time_start time_stop=$Garda.time_stop
process_name=$Garda.process_name process_id=$Garda.process_id
action_type=$Garda.action_type user_action=$Garda.user_action
device_name=$Garda.device_name serial_id=$Garda.serial_id
protocol=$Garda.protocol proto_descr=$Garda.proto_descr channel=$Garda.channel
uni_is_server=$Garda.uni_is_server uni_is_sender=$Garda.uni_is_sender
blocking_action=$Garda.blocking_action
cat="Использование_программы_удаленного_доступа"
```

- Для профиля **Конфиденциальная информация** используйте следующий шаблон:

```
src=$Garda.uni_ip dst=$Garda.peer_ip sport=$Garda.uni_port
dport=$Garda.peer_port suser=$Garda.account cs1=$Garda.action_type
action=$Garda.user_action objType=$Garda.type count_pages=$Garda.count
name=$Garda.name time=$Garda.time time_real=$Garda.time_real
time_start=$Garda.time_start time_stop=$Garda.time_stop
uni_email=$Garda.uni_email peer_email=$Garda.peer_email
have_attach=$Garda.have_attach path=$Garda.path file_size=$Garda.file_size
process_name=$Garda.process_name flags=$Garda.flags
device_name=$Garda.device_name serial_id=$Garda.serial_id url=$Garda.url
content_type=$Garda.content_type http_type=$Garda.http_type size=$Garda.size
web_obj_id=$Garda.web_obj_id web_parent_id=$Garda.web_parent_id
web_object_type=$Garda.web_object_type result_code=$Garda.result_code
referer=$Garda.referer content_encoding=$Garda.content_encoding
web_uni_id=$Garda.web_uni_id web_peer_id=$Garda.web_peer_id
web_source_id=$Garda.web_source_id protocol=$Garda.protocol
proto_descr=$Garda.proto_descr channel=$Garda.channel uni_ident=$Garda.uni_ident
```

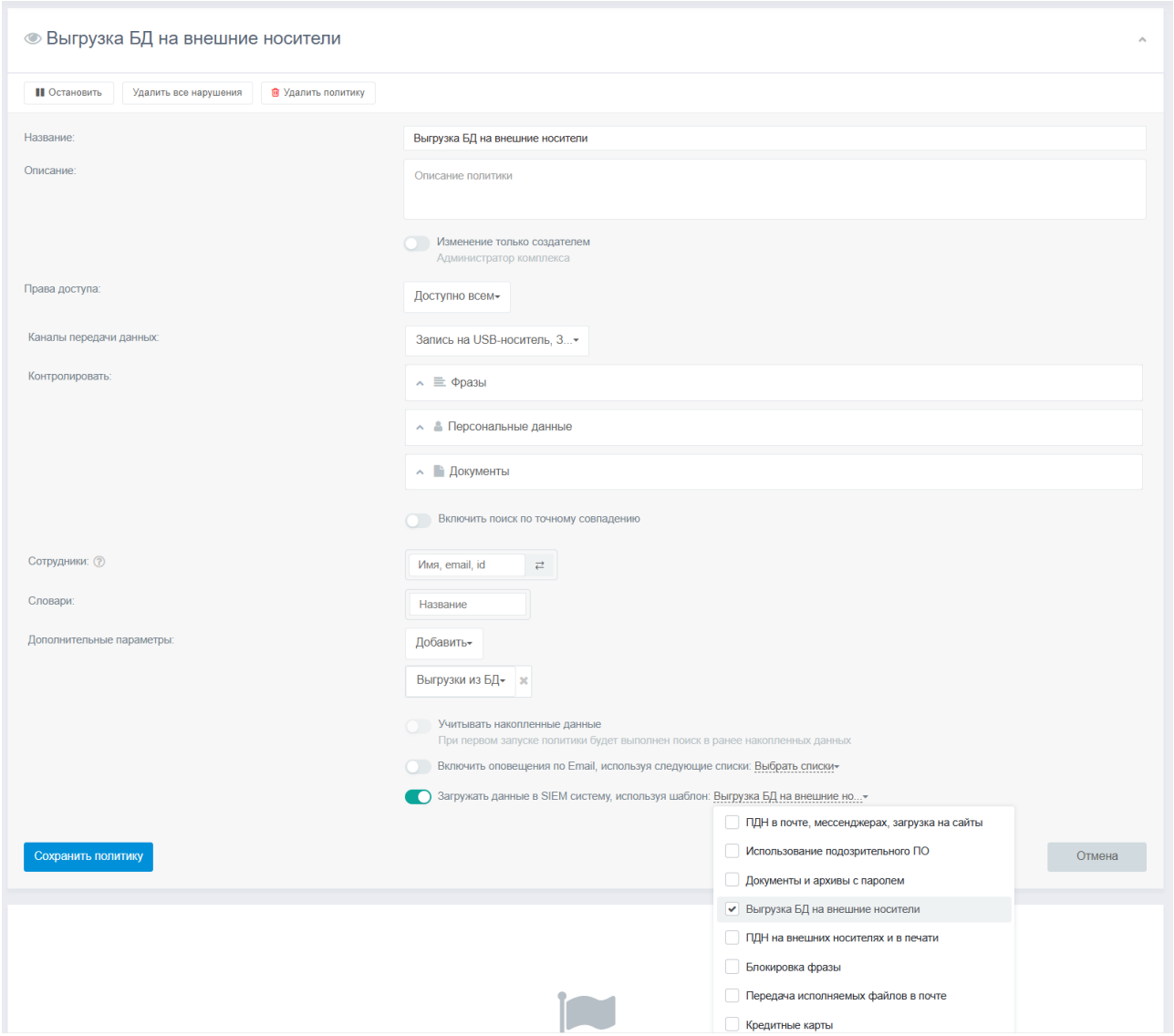
```
peer_ident=$Garda.peer_ident subject=$Garda.subject login=$Garda.login
chat_id=$Garda.chat_id send_time=$Garda.send_time mail_partid=$Garda.mail_partid
mail_flags=$Garda.mail_flags uni_is_server=$Garda.uni_is_server
uni_is_sender=$Garda.uni_is_sender blocking_action=$Garda.blocking_action
cat="Конфиденциальная_информация" uni_phone=$Garda.uni_phone
peer_phone=$Garda.peer_phone account=$Garda.account
user_action=$Garda.user_action type_action=$Garda.type_action
prop_text_part=$Garda.prop_text_part
```

6. Убедитесь, что в результате получилось 10 шаблонов:



7. Перейдите на вкладку **Политики**.
8. Выберите одну из политик по умолчанию.

9. В открывшемся окне включите функцию **Загружать данные в SIEM систему, используя шаблон**.
10. Выберите шаблон, соответствующий политике:



11. Повторите настройку для оставшихся политик.

Настройка Гарда DLP завершена.

Настройка в R-Vision SIEM

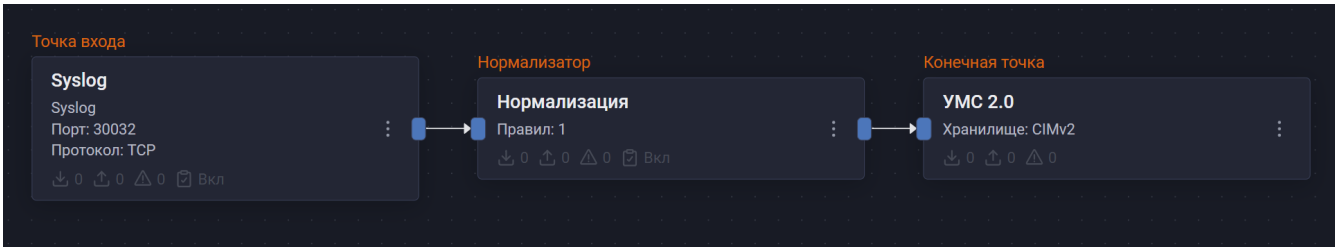
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне Гарда DLP.
   - Протокол: выберите вариант в соответствии с настройками на стороне Гарда DLP.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Garda DLP** (идентификатор правила:

RV-N-326).

4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

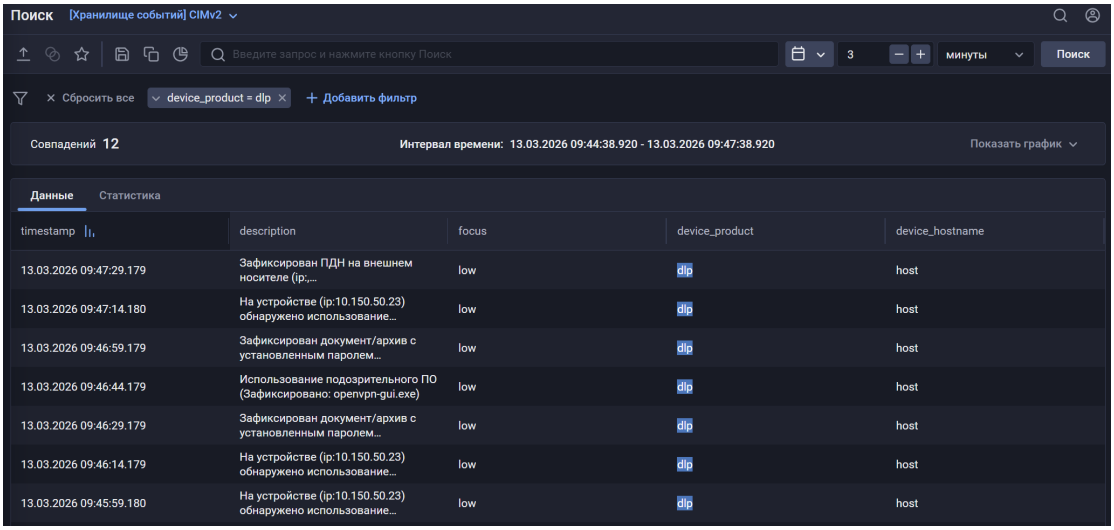
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Гарда DLP.

Найти события Гарда DLP в хранилище можно по следующему фильтру:

```
device_product = "dlp"
```



СёрчИнформ КИБ

- СёрчИнформ КИБ: настройка источника

СёрчИнформ КИБ: настройка источника

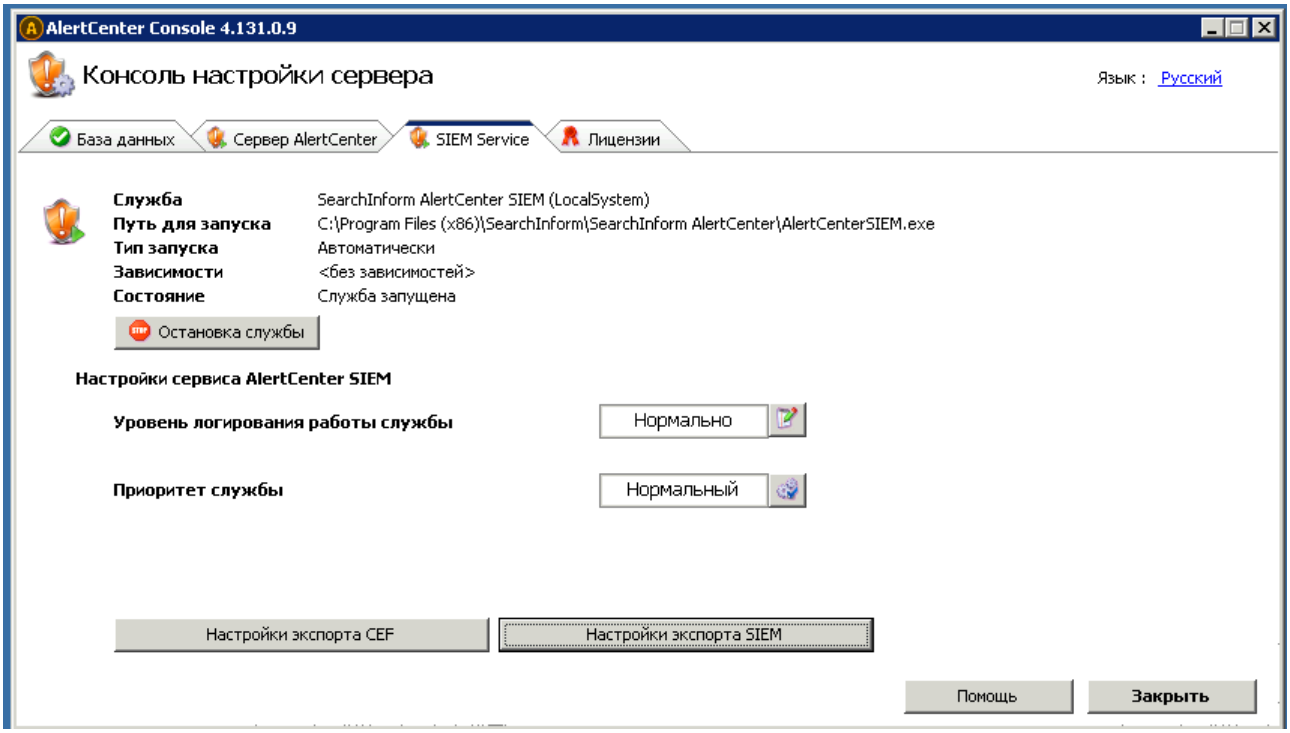
Данное руководство содержит инструкции по настройке подключения СёрчИнформ КИБ к системе R-Vision SIEM.

Предварительные требования

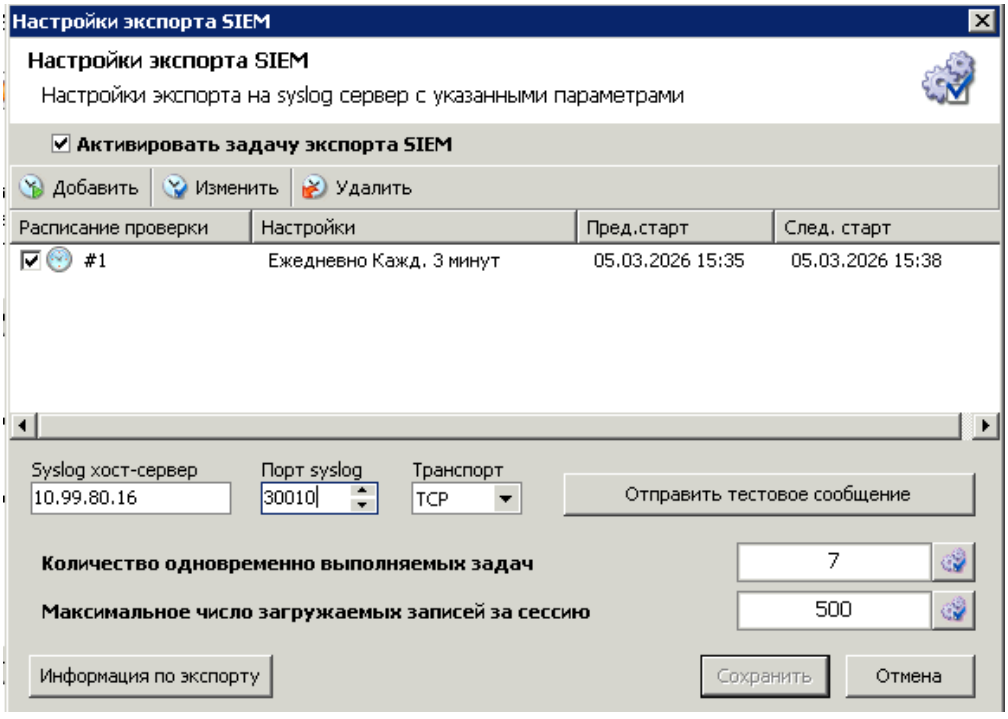
Перед настройкой пересылки событий в R-Vision SIEM убедитесь, что установлена сетевая связность между сервером AlertCenter и SIEM по целевому порту и протоколу.

Настройка СёрчИнформ КИБ

1. На сервере SearchInform откройте консоль AlertCenter и перейдите на вкладку **SIEM Service**.



2. Нажмите на кнопку **Настройки экспорта SIEM**.
3. В открывшемся окне создания задачи экспорта нажмите на кнопку **Добавить** и создайте задачу экспорта с требуемой периодичностью.



4. Укажите требуемые значения в полях **Syslog хост-сервер**, **Порт syslog** и **Транспорт**.
5. Сохраните изменения.

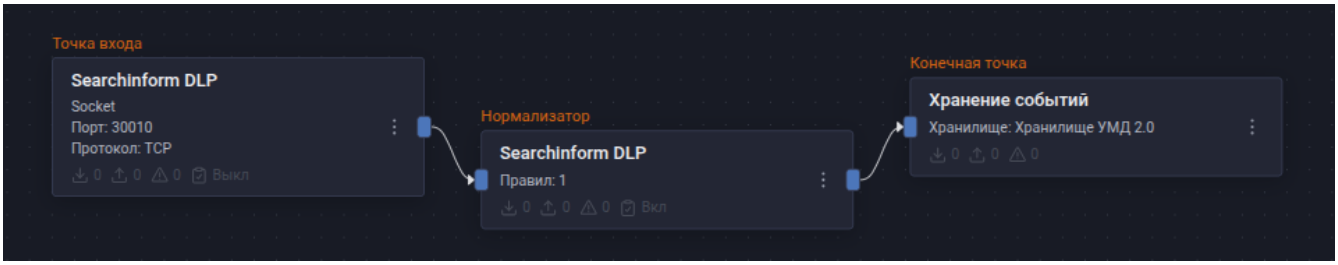
Настройка на стороне источника завершена.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Socket**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне источника.
   - Протокол: выберите вариант в соответствии с настройками на стороне источника.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Searchinform DLP** (идентификатор правила: **RV-N-312**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

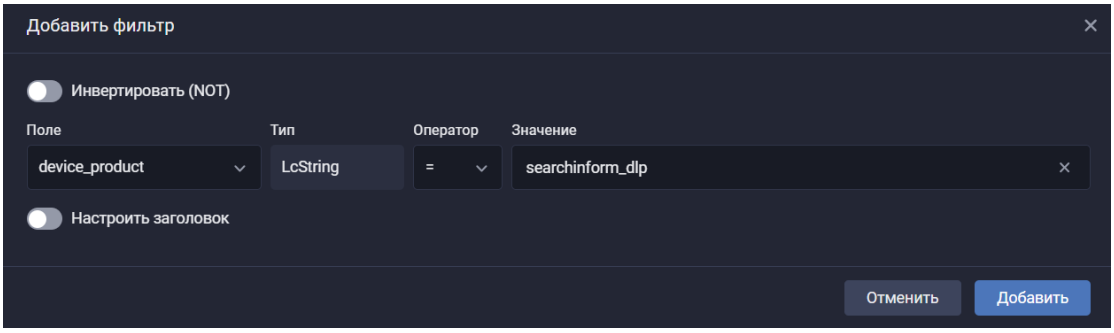
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события СёрчИнформ КИБ.

Найти события СёрчИнформ КИБ в хранилище можно по следующему фильтру:

```
device_product = "searchinform_dlp"
```


Добавить фильтр
Инвертировать (NOT)
Поле
Тип
Оператор
Значение
device_product
LcString
=
searchinform_dlp
Настроить заголовок
Отменить
Добавить

Системы резервного копирования и восстановления

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых систем резервного копирования и восстановления:

- Veeam Backup & Replication

Veeam Backup & Replication

- Veeam Backup & Replication: настройка источника

Veeam Backup & Replication: настройка источника

Данное руководство описывает процесс отправки событий Veeam Backup & Replication в R-Vision SIEM.

Настройка Veeam Backup & Replication

Настройка журналирования Veeam Backup & Replication

Программное обеспечение Veeam Backup & Replication пишет события в журнал Veeam Backup, находящийся в каталоге `C:\Windows\System32\winevt\Logs\Veeam Backup`.

Перед подключением сбора логов с сервера Veeam Backup & Replication под управлением ОС Windows Server, начиная с Windows Server 2012 R2, необходимо установить и настроить агент R-Vision EVO (далее — агент) согласно руководству пользователя продукта R-Vision EVO. Все дальнейшие настройки производятся в веб-консоли сервера управления R-Vision EVO (далее — менеджер).

Настройка в R-Vision SIEM

Настройка отправки событий в R-Vision SIEM

1. В веб-интерфейсе R-Vision SIEM перейдите в раздел **Агенты** → **Группы агентов**.
2. Создайте группу агентов и добавьте в нее узел, на котором установлен агент.
3. В созданной группе узлов в секции **Чтение файлов** нажмите на кнопку **Добавить настройку** (+).
4. В выпадающем списке **Тип журнала** выберите вариант **eventlog**.
5. В поле **Имя журнала** введите значение `Veeam Backup` (имя журнала событий).
6. Если фильтрация не требуется, то в поле **Фильтр (формат XPATH)** необходимо поставить знак *. Если необходимо выбирать события по определенным критериям, введите в это поле выражение XPath.
7. Нажмите на кнопку **Сохранить и применить**.
8. Дождитесь применения политики группы на узле. Сбор событий настроен.

Настройка обработки событий в R-Vision SIEM

В R-Vision SIEM уже должен быть настроен конвейер с точкой входа типа R-Vision EVO.

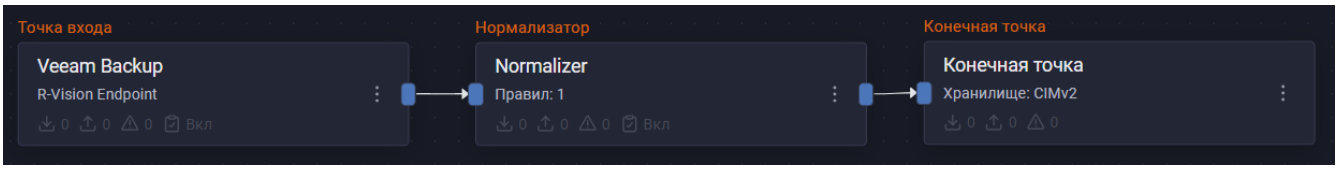


Для настройки интеграции продуктов R-Vision SIEM и R-Vision EVO обратитесь к документации продукта R-Vision SIEM.

Для настройки обработки событий Veeam Backup & Replication в R-Vision SIEM:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе (или откройте существующий).
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **R-Vision Endpoint**.
   - Домен: введите значение в формате `gw-<your_gateway_id>`, где `<your_gateway_id>` — ID шлюза.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Veeam Backup** (идентификатор правила: **RV-N-246**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

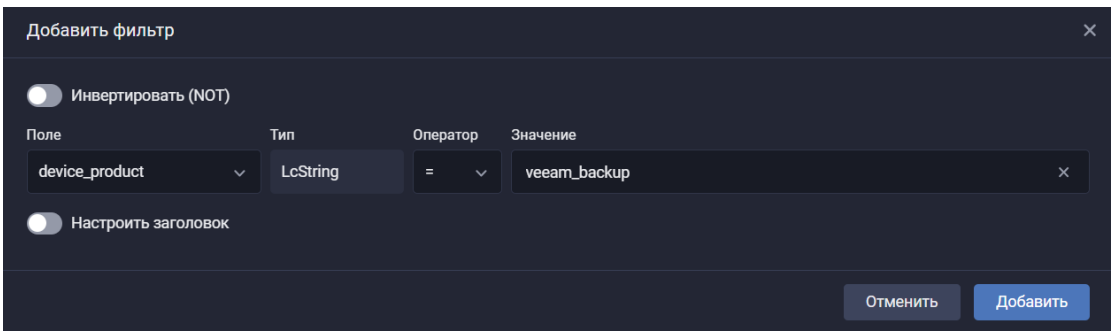


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события хоста под управлением Veeam Backup & Replication.



Найти события хоста под управлением Veeam Backup & Replication в хранилище можно по следующему фильтру:

```
device_product = "veeam_backup"
```



Системы управления базами данных (СУБД)

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых систем управления базами данных:

- Apache Cassandra
- ClickHouse
- MariaDB
- Microsoft SQL Server
- MongoDB
- Oracle Database
- Oracle MySQL
- PostgreSQL
- РЕД База Данных
- СберТех Platform V Pangolin DB

Apache Cassandra

- Apache Cassandra: настройка источника

Apache Cassandra: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий СУБД Apache Cassandra в R-Vision SIEM.

Настройка Apache Cassandra

Настройка журналирования

Для настройки журналирования событий Apache Cassandra выполните следующие шаги:

1. Убедитесь, что на сервере, где установлена Apache Cassandra, доступно не менее пяти ГБ дискового пространства.
2. Подключитесь к серверу Apache Cassandra под учетной записью с правами администратора.
3. Перед внесением изменений создайте резервные копии следующих конфигурационных файлов:
   - `/etc/cassandra/cassandra.yaml` или `/etc/alternatives/cassandra/cassandra.yaml`;
   - `/etc/cassandra/logback.xml` или `/etc/alternatives/cassandra/logback.xml`.
4. Убедитесь, что параметры конфигурационного файла `cassandra.yaml` имеют следующие значения, и при необходимости измените их:
   - в секции `audit_logging_options`: `enabled = true`;
   - в секции `logger`: `class_name = FileAuditLogger`;
   - `authorizer` установлен в значение `CassandraAuthorizer`.

5. В конфигурационный файл `logback.xml` добавьте следующий фрагмент:

```
<appender name="AUDIT" class="ch.qos.logback.core.rolling.RollingFileAppender">
    <file>${cassandra.logdir}/audit/audit.log</file>
    <rollingPolicy
class="ch.qos.logback.core.rolling.SizeAndTimeBasedRollingPolicy">
        <!-- rollover daily -->
        <fileNamePattern>${cassandra.logdir}/audit/audit.log.%d{yyyy-MM-
dd}.%i.zip</fileNamePattern>
        <!-- each file should be at most 50MB, keep 30 days worth of history, but
at most 5GB -->
        <maxFileSize>50MB</maxFileSize>
        <maxHistory>30</maxHistory>
        <totalSizeCap>5GB</totalSizeCap>
    </rollingPolicy>
    <encoder>
        <pattern>%-5level [%thread] %date{ISO8601} %F:%L - %msg%n</pattern>
    </encoder>
</appender>
<!-- Audit Logging additivity to redirect audt logging events to audit/audit.log
-->
<logger name="org.apache.cassandra.audit" additivity="false" level="INFO">
    <appender-ref ref="AUDIT"/>
</logger>
```

6. Сохраните изменения в конфигурационном файле.
7. Перезапустите службу Apache Cassandra с помощью следующих команд:

```
sudo systemctl stop cassandra.service
sudo systemctl start cassandra.service
```

8. После перезапуска проверьте статус Apache Cassandra с помощью следующей команды:

```
sudo systemctl status cassandra.service
```

   Убедитесь, что вывод команды содержит следующее сообщение:

```
Active: active (running)
```

Настройка передачи событий Apache Cassandra завершена. Передаваемые события будут сохраняться в файле `/var/log/cassandra/audit/audit.log`.

Настройка службы rsyslog

Чтобы настроить службу rsyslog, выполните следующие шаги:

1. Создайте файл конфигурации rsyslog:

```
sudo nano /etc/rsyslog.d/01-cassandra.conf
```

2. Добавьте в созданный файл следующее правило:

```
module(load="imfile" PollingInterval="10")

input(type="imfile"
      File="/var/log/cassandra/audit/audit.log"
      startmsg.regex="INFO  "
      readTimeout="1"
      escapeLF="off"
      Tag="cassandra-audit")

if $syslogtag contains 'cassandra' then {
   action(type="omfwd" target="<target>" port="<port>" protocol="<protocol>")
   stop
}
```

   Здесь:

   - `<target>` — IP-адрес или полное доменное имя (FQDN) централизованного syslog-сервера, с которого будет осуществляться отправка сообщений в SIEM.
   - `<port>` — порт точки входа Syslog на конвейере SIEM: значение в диапазоне 30000—32767.
   - `<protocol>` — `tcp` или `udp`.

Настройка syslog-сервера

Для настройки syslog-сервера выполните следующие шаги:

1. Откройте конфигурационный файл rsyslog (`/etc/rsyslog.conf` или `/etc/rsyslog.d/`).
2. Добавьте следующее правило:

```
if $syslogtag contains 'cassandra' then {
  action(type="omfwd" Target="<target>" Port="<port>" Protocol="tcp")
  stop
}
```

   Здесь:

   - `<target>` — IP-адрес или полное доменное имя (FQDN) централизованного syslog-сервера, с которого будет осуществляться отправка сообщений в SIEM.
   - `<port>` — порт точки входа Syslog в конвейере SIEM — любой свободный порт больше 30000.

3. Перезапустите rsyslog для применения изменений:

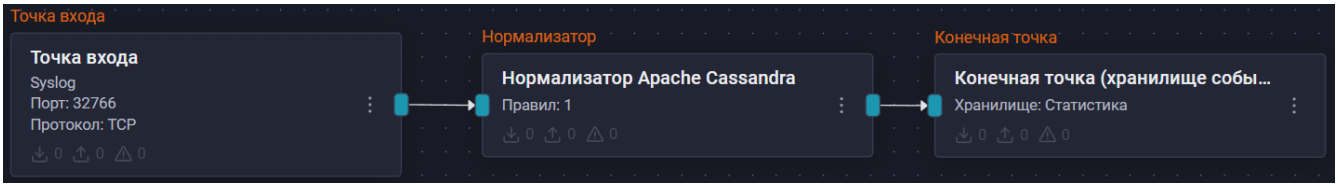
```
sudo systemctl restart rsyslog
```

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне syslog-сервера.
   - Протокол: выберите вариант **TCP**.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Apache Cassandra** (идентификатор правила: **RV-N-343**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

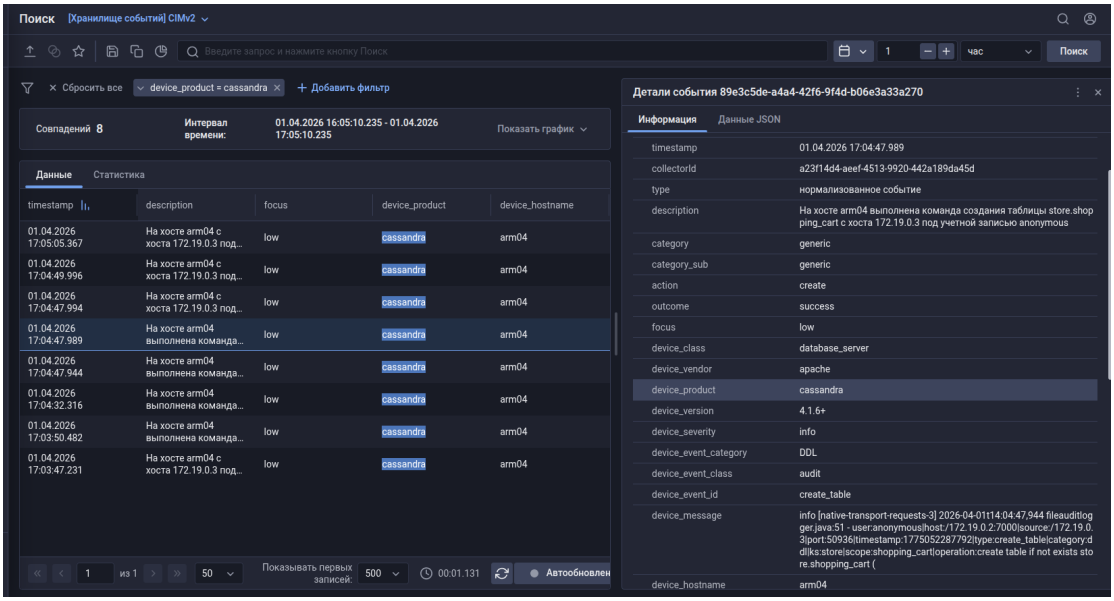
Пример конфигурации конвейера:



Если настройка передачи событий выполнена корректно, в хранилище начнут поступать события Apache Cassandra.

Найти события Apache Cassandra в хранилище можно по следующему фильтру:

```
device_product = "cassandra"
```



ClickHouse

- ClickHouse: настройка источника
- ClickHouse: правила корреляции

ClickHouse: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий ClickHouse в R-vision SIEM.

Настройка ClickHouse

Настройте передачу событий из файла. Для этого отредактируйте файл `/etc/clickhouse-server/config.xml`:

1. Раскомментируйте таблицы, название которых оканчивается на `_log`.
2. Задайте нужный уровень: `level = 8`.

СУБД ClickHouse сохраняет логи в разные таблицы системной БД system, например:

- `query_log` — лог запросов к СУБД.
- `backup_log` — логи резервного копирования. Подробнее о настройке резервного копирования см. в официальной документации ClickHouse.
- `session_log` — логи входа в систему и выхода из системы.

С полным списком системных таблиц можно ознакомиться в официальной документации ClickHouse.

Настройка в R-Vision SIEM

Настройка подключения ClickHouse в качестве источника на конвейере R-Vision SIEM сводится к подключению в качестве точек входа нескольких системных таблиц.

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте секрет со строкой подключения. Для этого:
   a. Перейдите в раздел **Ресурсы** → **Секреты**.
   b. Нажмите на кнопку **Создать** (+).
   c. В раскрывшемся окне создания секрета заполните поля:
      - Название: введите название секрета.
      - Описание (опционально): опишите, для чего будет использоваться секрет.
      - Тип секрета: выберите вариант **Строка подключения**.
      - Строка подключения: введите строку вида:

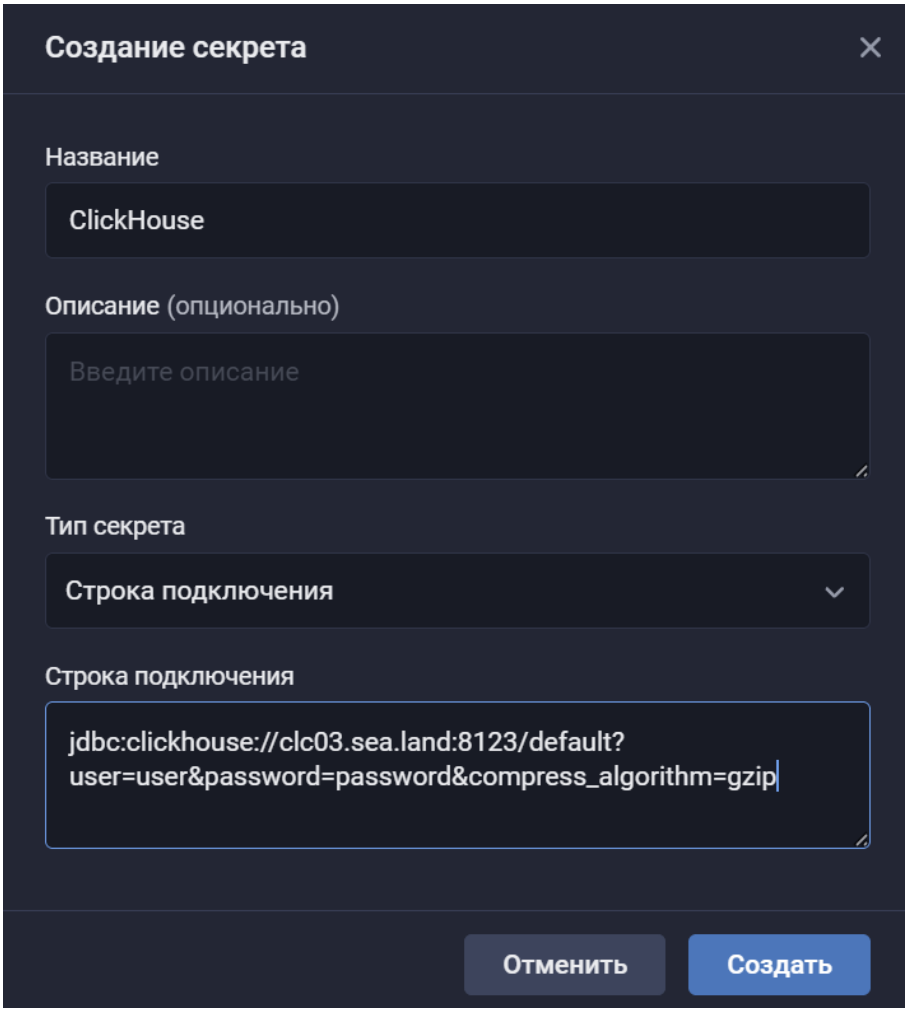
        ```
        jdbc:clickhouse://<address>:<port>/default?user=<user>&password=<password>&c
        ompress_algorithm=gzip
        ```

        Здесь:

        - `<address>` — адрес сервера базы данных.
        - `<port>` — порт подключения.
        - `<user>` — логин пользователя базы данных.
        - `<password>` — пароль пользователя базы данных.

        Пример 4. Пример строки подключения:

        ```
        jdbc:clickhouse://clc03.sea.land:8123/default?user=user&password=password
        &compress_algorithm=gzip
        ```



d. Нажмите на кнопку **Создать**.

2. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
3. Добавьте на конвейер элемент **Точка входа** для каждой таблицы со следующими параметрами.
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Database**.
   - Драйвер базы данных: выберите вариант **ClickHouse**.
   - Адрес подключения: выберите секрет, созданный ранее.
   - SQL-запрос: для каждой таблицы введите отдельный SQL-запрос:
     a. Таблица `system.query_log`:

```
SELECT FQDN() AS hostname, 'clickhouse' AS appname, 'query_log' AS at, type,
event_time AS timer, query_start_time,current_database, query, query_kind,
databases, tables, user, query_id, address, port, initial_user,
initial_query_id, initial_port, interface, is_secure, os_user,
client_hostname, client_name, http_user_agent FROM system.query_log WHERE
timer > FROM_UNIXTIME(toInt32(?)) ORDER BY timer ASC LIMIT 50;
```

     b. Таблица `system.session_log`:

```
SELECT FQDN() AS hostname, 'clickhouse' AS appname, 'session_log' AS at,
type, auth_id, event_time AS timer, user, auth_type, profiles, roles,
client_address, client_port, interface, failure_reason FROM
system.session_log WHERE timer > FROM_UNIXTIME(toInt32(?)) ORDER BY timer
ASC LIMIT 50;
```

c. Таблица `system.backup_log`:

```
SELECT FQDN() AS hostname, 'clickhouse' AS appname, 'backup_log' AS at,
hostname AS dvchost, id AS externalId, base_backup_name AS objPath,
event_time_microseconds AS timer, 'Info' AS severity, status AS act, error
AS reason, name AS objName FROM system.backup_log WHERE timer >
FROM_UNIXTIME(toInt32(?)) ORDER BY timer ASC LIMIT 10;
```



Оператор `LIMIT` в запросах — обязательный параметр, определяющий выводимое число строк. Конкретное число строк для ограничения значения `LIMIT` подбирается индивидуально по загруженности СУБД. Если на эксплуатируемой СУБД количество возвращаемых строк в результате выполнения запроса больше, чем то, которое указано в запросе, то примерно оценить `LIMIT` можно через запрос, описанный ниже.

В приложении DBeaver выполните SQL-запрос, чтобы узнать, сколько примерно строк возвращается за 15 секунд, именно такой интервал указывается при настройке точки входа. Если у вас иной интервал, нужно учесть его в запросе. Для этого измените значение `toInt32(INTEGER)` на свой интервал.

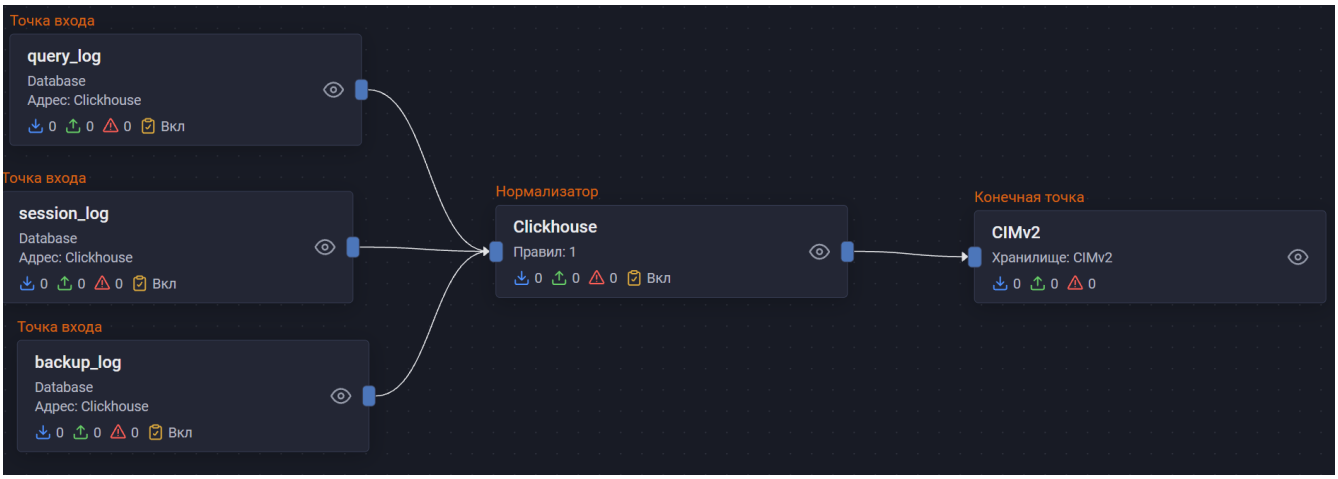
```
SELECT event_time AS rt, level AS severity, logger_name AS
aid, message AS msg FROM system.text_log WHERE rt >
FROM_UNIXTIME(toInt32(1712239973)) AND rt <=
FROM_UNIXTIME(toInt32(1712239988)) ORDER BY rt DESC;
```

- Поле идентификатора: введите ключ `timer` со значением, указывающим момент времени в формате **Unix time**. Можно воспользоваться конвертером.
- Интервал запроса, секунд: введите значение `15`. Можно выставить иной интервал.
- Максимальное количество строк (опционально): введите значение `100`. Можно выставить иное значение.

4. Добавьте на конвейер элемент **Нормализатор** с правилом **ClickHouse** (идентификатор правила: **RV-N-193**).
5. Соедините нормализатор с точками входа.
6. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
7. Соедините конечную точку с нормализатором.

8. Сохраните и установите конфигурацию конвейера.

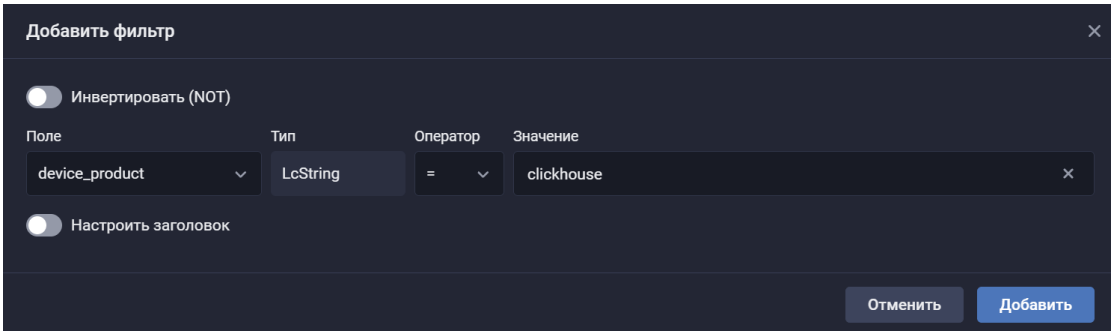
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события ClickHouse.

Найти события ClickHouse в хранилище можно по следующему фильтру:

```
device_product = "clickhouse"
```



ClickHouse: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1465	Подбор пароля к СУБД ClickHouse	Правило обнаруживает множественные неудачные попытки подключения к СУБД ClickHouse от одной учетной записи, учитывая попытки с разных хостов.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1468	Успешный подбор пароля к СУБД ClickHouse	Правило обнаруживает успешную попытку входа после множественных неудачных попыток подключения к СУБД ClickHouse от одной учетной записи, учитывая попытки с разных узлов.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)
RV-D-1469	Атака Password Spraying на СУБД ClickHouse	Правило обнаруживает множественные неудачные попытки подключения к СУБД ClickHouse от одного хоста к множеству учетных записей.	• Credential Access (TA0006) • Brute Force (T1110) • Password Spraying (T1110.003)
RV-D-1474	Получение информации о системе в ClickHouse	Атакующему может понадобиться получить дополнительные сведения о скомпрометированной системе. Правило обнаруживает попытку просмотра информации о системе, конфигурации и версии базы данных (БД).	• Discovery (TA0007) • System Information Discovery (T1082) • File and Directory Discovery (T1083)
RV-D-1476	Попытка удаления нескольких таблиц в ClickHouse	Атакующий с целью нарушения функционирования системы может попытаться удалить значимые таблицы в базе данных. Правило обнаруживает удаление 5 таблиц в течении минуты в ClickHouse с помощью характерного запроса.	• Impact (TA0040) • Data Destruction (T1485)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1477	Получение информации о структуре Clickhouse	В целях получения информации о пользователях и таблицах базы данных атакующий может провести разведку. Правило обнаруживает попытку просмотра информациии о пользователях, их привилегиях и таблицах в базе данных.	• Credential Access (TA0006) • Discovery (TA0007) • OS Credential Dumping (T1003) • Permission Groups Discovery (T1069) • Local Groups (T1069.001) • System Information Discovery (T1082) • Account Discovery (T1087) • Local Account (T1087.001) • Domain Account (T1087.002)
RV-D-1478	Создание дампа таблиц в ClickHouse	Атакующий может сохранить конфиденциальную информацию из базы данных для дальнейшей ее обработки на удаленном хосте. Правило обнаруживает попытку сохранения таблицы из базы данных ClickHouse в файл.	• Credential Access (TA0006) • Collection (TA0009) • OS Credential Dumping (T1003) • Data from Local System (T1005) • Data Staged (T1074) • Local Data Staging (T1074.001)
RV-D-1485	Изменение или удаление таблицы аудита ClickHouse	Атакующий для сокрытия своих действий может удалить или изменить значения в таблицах аудита `system.query_log` и `system.session_log`, в которых логируются выполненные запросы и события авторизации.	• Defense Evasion (TA0005) • Impact (TA0040) • Indicator Removal (T1070) • Data Manipulation (T1565) • Stored Data Manipulation (T1565.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1486	Использование LIKE для разведки в Clickhouse	Атакующий для сбора информации о таблицах в ClickHouse может использовать запрос, содержащий `where name like`. Правило обнаруживает использование данной строки в SQL запросе к системным таблицам `columns` или `tables`.	• Collection (TA0009) • Data from Local System (T1005)
RV-D-1491	Небезопасный способ аутентификации пользователя ClickHouse	Атакующий для получения доступа к базе данных ClickHouse может использовать учетные данные без использования пароля или с незашифрованным паролем. Правило обнаруживает попытку создания или модификации пользователя с установкой способа аутентификации `no_password` или `plaintext_password`.	• Persistence (TA0003) • Credential Access (TA0006) • Account Manipulation (T1098) • Create Account (T1136) • Local Account (T1136.001) • Unsecured Credentials (T1552)
RV-D-1494	Создание привилегированного пользователя в ClickHouse	В целях закрепления атакующий может создать пользователя и выдать ему привилегии. Правило обнаруживает попытку создания пользователя и выдачу ему максимальных привилегий.	• Persistence (TA0003) • Account Manipulation (T1098) • Create Account (T1136) • Local Account (T1136.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1495	Изменение конфигурации базы данных ClickHouse	Атакующий может попытаться изменить конфигурацию базы данных ClickHouse для получения информации об учетных данных, закрепления в системе или иных целей. Правило обнаруживает изменение файла конфигурации `keeper_config`, `configl`, `user` для базы данных ClickHouse.	• Persistence (TA0003) • Defense Evasion (TA0005) • Credential Access (TA0006) • Discovery (TA0007) • OS Credential Dumping (T1003) • Account Discovery (T1087) • Modify Authentication Process (T1556) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)
RV-D-1500	Вход привилегированного пользователя в ClickHouse	Атакующий может получить привилегированные учетные данные и попытаться авторизоваться с контролируемого им хоста. Правило обнаруживает попытку авторизации привилегированного пользователя с неизвестного хоста.	• Initial Access (TA0001) • Valid Accounts (T1078) • Local Accounts (T1078.003)
RV-D-1502	Попытка удаления базы данных в ClickHouse	Атакующий с целью нарушения функционирования системы может попытаться удалить базу данных. Правило обнаруживает удаление базы данных в ClickHouse с помощью характерного запроса.	• Impact (TA0040) • Data Destruction (T1485)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1503	Взаимодействие с файловой системой из БД ClickHouse	Атакующий может попытаться прочитать или записать данные в файл или попытаться выполнить скрипт. Правило обнаруживает использование функций `file` и `executable`, применяемых для взаимодействия с файловой системой.	• Execution (TA0002) • Discovery (TA0007) • Impact (TA0040) • Command and Scripting Interpreter (T1059) • Python (T1059.006) • File and Directory Discovery (T1083) • Data Manipulation (T1565) • Stored Data Manipulation (T1565.001)

MariaDB

- MariaDB: настройка источника

MariaDB: настройка источника

Данное руководство описывает процесс настройки сбора событий MariaDB и их отправки в R-Vision SIEM.

Предварительные требования

Перед началом настройки убедитесь, что выполнены следующие условия:

- На машине, с которой планируется сбор событий, установлен сервис rsyslog или syslog-ng.
- Пользователь, выполняющий настройку, имеет права администратора.

Настройка MariaDB

Настройка журналирования

Процесс настройки журналирования MariaDB отличается в зависимости от версии.

Настройка сбора событий MariaDB версии 10 и выше

Настройте логирование событий в системный журнал. Для этого выполните следующие шаги:

1. Проверьте, есть ли модуль аудита на вашем сервере:

```
SHOW VARIABLES LIKE 'plugin_dir';
```

2. Проверьте, есть ли .so-файл на сервере:

```
ls /path/to/plugin/from/previous/step | grep audit
```

3. После этого должен отобразиться файл `server_audit.so`.
4. Если данного файла нет, установите пакет с помощью команды:

```
sudo dnf install MariaDB-server-audit
```

5. Создайте отдельный файл для настройки конфигурации аудита:

```
sudo nano /etc/my.cnf.d/server_audit.cnf
```



Путь к файлу конфигурации может отличаться в зависимости от используемой операционной системы. В данном руководстве рассматривается настройка сбора событий с RED OS.

6. Добавьте секцию:

```
[mysqld]
# Загрузка плагина при старте.
plugin_load_add = server_audit

# Включение аудита.
server_audit_logging = ON

# Виды событий для логирования.
server_audit_events = CONNECT,QUERY,QUERY_DDL,QUERY_DML,QUERY_DCL

# Запись логов в системный журнал.
server_audit_output_type = SYSLOG
server_audit_syslog_facility = LOG_LOCAL6
server_audit_syslog_priority = LOG_INFO
```

7. Сохраните файл.
8. Перезапустите MariaDB:

```
sudo systemctl restart mariadb
```

9. Проверьте работу плагина аудита:

```
SELECT PLUGIN_NAME, PLUGIN_STATUS, LOAD_OPTION FROM
information_schema.plugins WHERE PLUGIN_NAME = 'server_audit';
```

10. Вы должны получить следующий вывод:

```
+--------------+---------------+-------------+
| PLUGIN_NAME  | PLUGIN_STATUS | LOAD_OPTION |
+--------------+---------------+-------------+
| SERVER_AUDIT | ACTIVE        | ON          |
+--------------+---------------+-------------+
```

Настройка сбора событий MariaDB версии 5.7 и ниже

Настройте логирование событий в системный журнал. Для этого выполните следующие шаги:

1. Проверьте, есть ли модуль аудита на вашем сервере:

```
SHOW GLOBAL VARIABLES LIKE 'plugin_dir';
```

2. Проверьте, есть ли .so-файл на сервере:

```
ls /path/to/plugin/from/previous/step | grep audit
```

3. После этого должен отобразиться файл `server_audit.so`.
4. Если файла нет, установите пакет с помощью команды:

```
sudo yum install MariaDB-server-audit
```

5. Если плагин присутствует, подключитесь к MariaDB с правами администратора и выполните следующий запрос:

```
INSTALL SONAME 'server_audit';
```

6. Создайте отдельный файл для настройки конфигурации аудита:

```
sudo nano /etc/my.cnf.d/server_audit.cnf
```



Путь к файлу конфигурации может отличаться в зависимости от используемой операционной системы. В данном руководстве рассматривается настройка сбора событий с CentOS 7.

7. Добавьте секцию:

```
[mysqld]
server_audit_logging=1

server_audit_events=connect,table,query_ddl,query_dml,query_dcl

server_audit_output_type=SYSLOG

server_audit_syslog_facility=LOG_SYSLOG
```

8. Сохраните файл.
9. Перезапустите MariaDB:

```
sudo systemctl restart mariadb
```

10. Проверьте работу плагина аудита:

```
SELECT PLUGIN_NAME, PLUGIN_STATUS, LOAD_OPTION FROM
information_schema.plugins WHERE PLUGIN_NAME = 'server_audit';
```

11. Вы должны получить следующий вывод:

```
+--------------+---------------+-------------+
| PLUGIN_NAME  | PLUGIN_STATUS | LOAD_OPTION |
+--------------+---------------+-------------+
| SERVER_AUDIT | ACTIVE        | ON          |
+--------------+---------------+-------------+
```

Настройка отправки событий в R-Vision SIEM



В настоящем руководстве рассматривается передача событий с помощью сервиса rsyslog.

События сервера MariaDB могут отправляться на централизованный сервер syslog или напрямую в систему SIEM. Далее рассмотрим оба варианта настройки.

Чтобы настроить отправку событий сервера MariaDB, выполните следующие шаги:

1. Создайте конфигурационный файл rsyslog в директории `/etc/rsyslog.d/`.
2. Добавьте в файл следующие правила:

```
if $syslogtag == 'mysql-server_auditing' or $programname == 'mysql-server_auditing'
then {
  action(type="omfwd" target="<target>" port="<port>" protocol="<protocol>")
  stop
```

```
}
```

Здесь:

- <target>: введите IP-адрес или полное доменное имя (FQDN) сервера syslog или узла кластера Kubernetes, на котором запущен коллектор SIEM.
- <port>:
  - При отправке событий на сервер rsyslog укажите порт 514.
  - При отправке событий на конвейер SIEM укажите порт точки входа Syslog — любой свободный порт со значением больше 30000.
- <protocol>: укажите протокол, используемый для точки входа на конвейере SIEM.

3. Перезапустите rsyslog, чтобы изменения вступили в силу:

```
sudo systemctl restart rsyslog
```

Настройка сбора событий источника на сервере syslog

Если события сначала отправляются на сервер syslog, настройте отправку логов с сервера в SIEM:

1. Откройте конфигурационный файл rsyslog (/etc/rsyslog.conf или /etc/rsyslog.d/).
2. Добавьте в файл следующее правило:

```
# Укажите IP-адрес SIEM и порт, куда будут отправляться события.
if $syslogtag == 'mysql-server_auditing' or $programname == 'mysql-server_auditing'
then {
  action(type="omfwd" target="<target>" port="<port>" protocol="<protocol>")
  stop
}
```

Здесь:

- <target>: введите IP-адрес или полное доменное имя (FQDN) узла кластера Kubernetes, на котором запущен коллектор SIEM.
- <port>: укажите порт точки входа Syslog — любой свободный порт со значением больше 30000.
- <protocol>: укажите протокол, используемый для точки входа на конвейере SIEM.

3. Перезапустите rsyslog, чтобы изменения вступили в силу:

```
sudo systemctl restart rsyslog
```

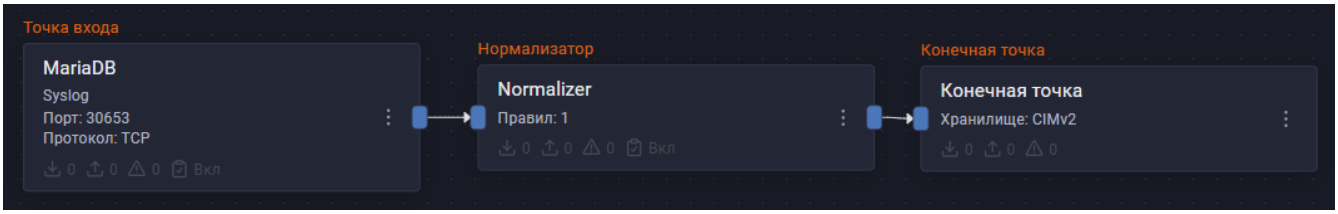
Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие

шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне сервера syslog.
   - Протокол: выберите вариант в соответствии с настройками на стороне сервера syslog.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **MariaDB** (идентификатор правила: **RV-N-236**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

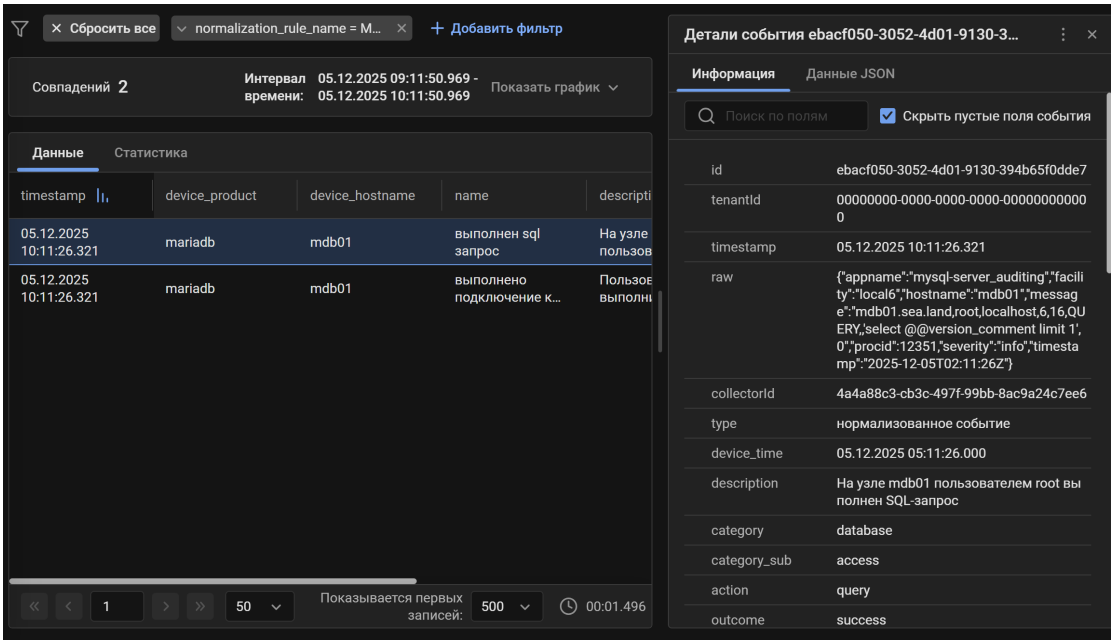
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события MariaDB.

Найти события MariaDB в хранилище можно по следующему фильтру:

```
normalization_rule_name = "MariaDB"
```



Microsoft SQL Server

- Microsoft SQL Server: настройка источника
- Microsoft SQL Server: правила корреляции

Microsoft SQL Server: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Microsoft SQL Server (MS SQL) в R-Vision SIEM.

Предварительные требования

- Сетевая доступность сервера СУБД (Microsoft SQL Server) источника по целевому порту и протоколу для каждой ноды кластера SIEM.
- Учетная запись в СУБД с правами на чтение базы данных.

Настройка MS SQL

Описание подсистемы журналирования MS SQL

Журналирование событий источника может осуществляться двумя путями:

1. Запись в журнал событий. Например, события журналов сервера Microsoft SQL Server записываются в журнал `Application`.

   Настройка сбора событий журнала Windows SQL Server с помощью агента платформы R-Vision EVO включает в себя установку агента на хост и настройку политики.

2. Отдельная настройка журналирования событий. Например, отдельно настраиваются события аудита команд SQL Server.

Создание учетной записи в СУБД MS SQL

Для отправки событий аудита команд создайте сервисную учетную запись в СУБД MS SQL и предоставьте ей права на просмотр всех сеансов на сервере:

```
GRANT VIEW SERVER STATE TO [имя пользователя];
```

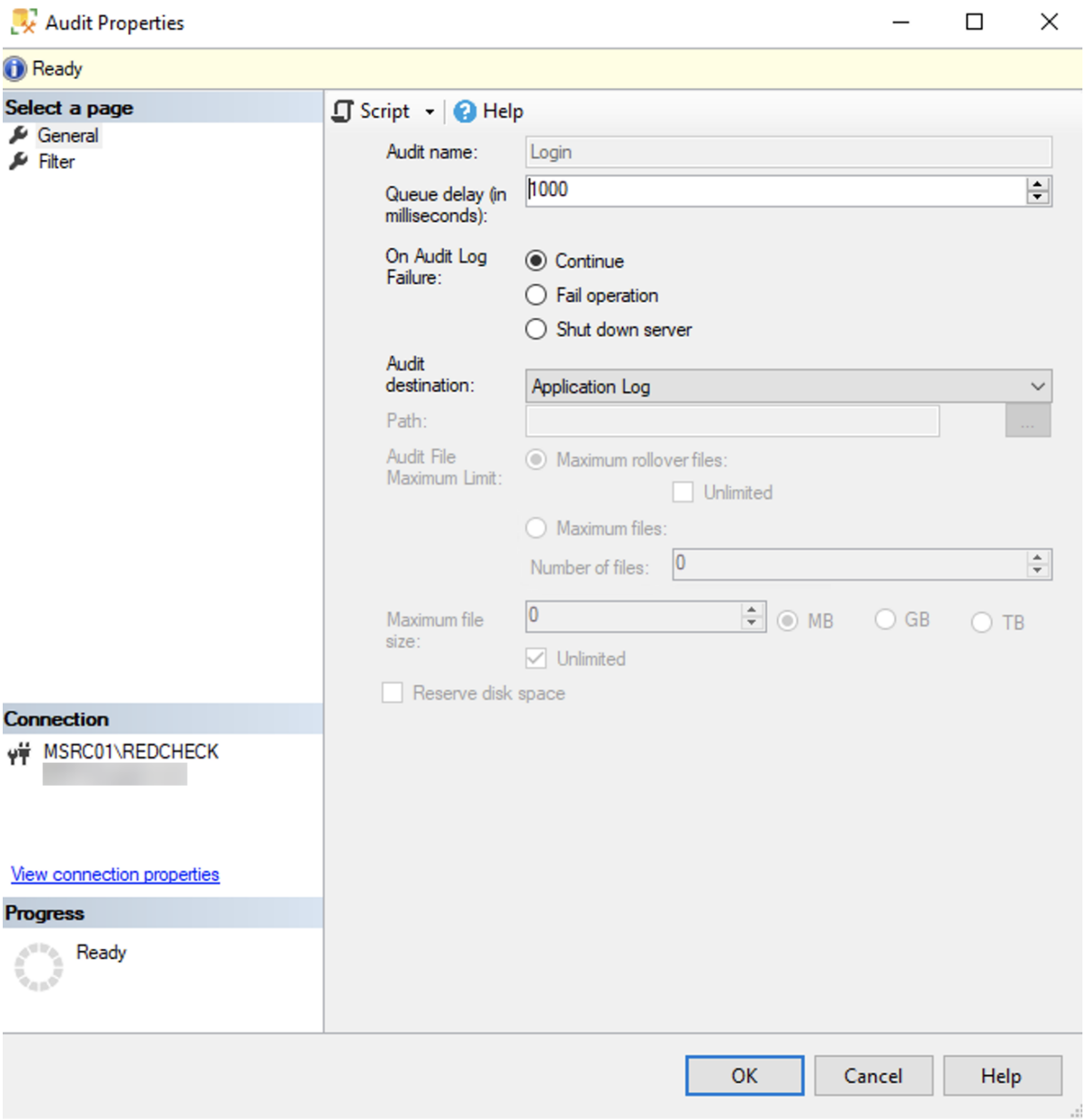
Настройка аудита MS SQL



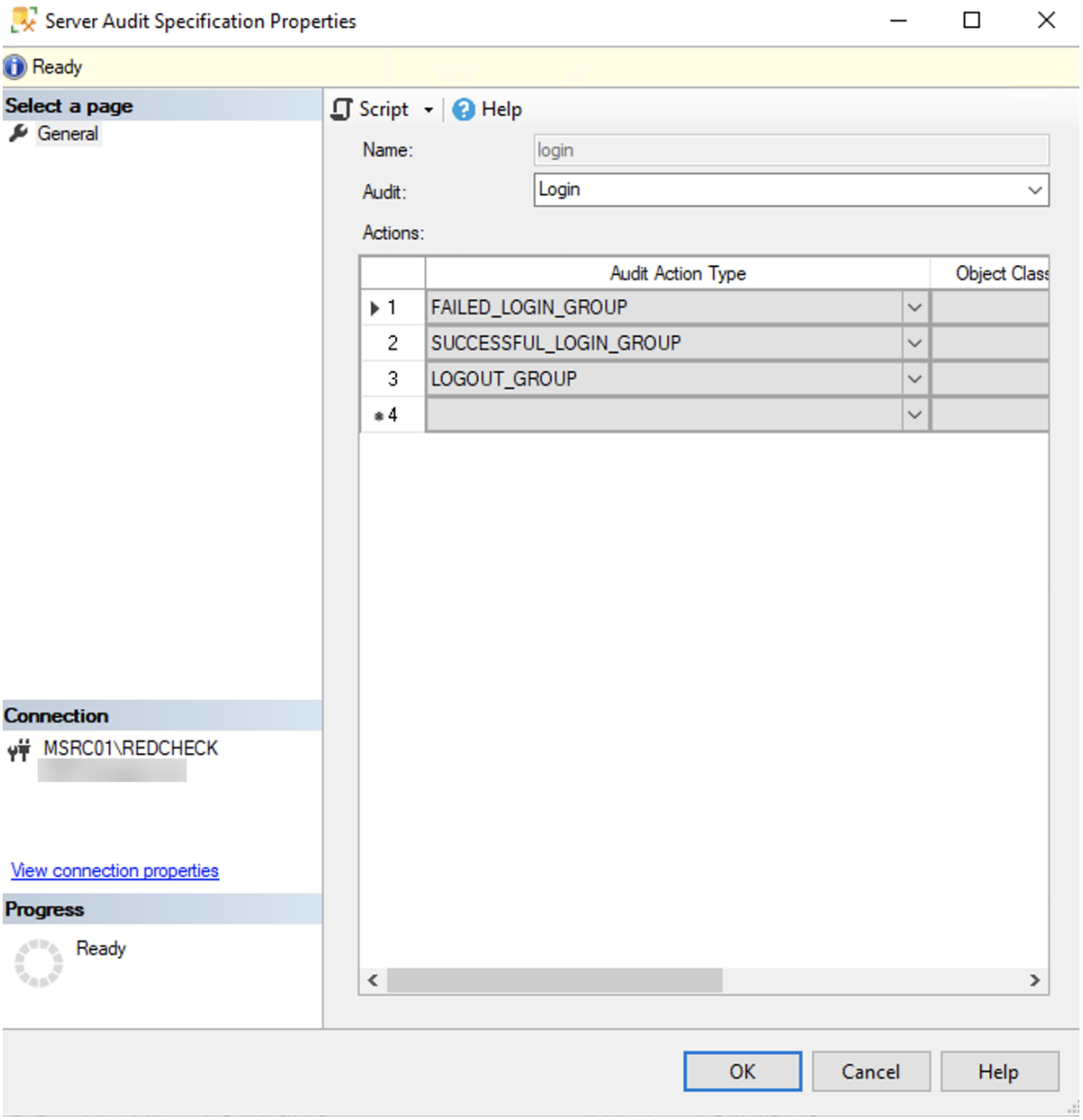
Если нет необходимости анализировать запросы к продуктовым базам, аудит действий с ними можно не настраивать. При этом для работы правил корреляции следует обязательно контролировать запросы к базе master.

Для настройки аудита на уровне сервера выполните следующие шаги:

1. Откройте **SQL Server Management Studio**.
2. В боковом меню перейдите в раздел **Security**.
3. Откройте контекстное меню **Audits** и выберите вариант **New Audit…**. Будет создан новый объект аудита SQL Server.
4. Выберите действие, которое будет запущено при сбое журнала аудита:
   - продолжить;
   - остановить операции с базой данных, которые проверяются;
   - завершить работу сервера.
5. В качестве назначения аудита выберите из выпадающего списка вариант **Application Log**.



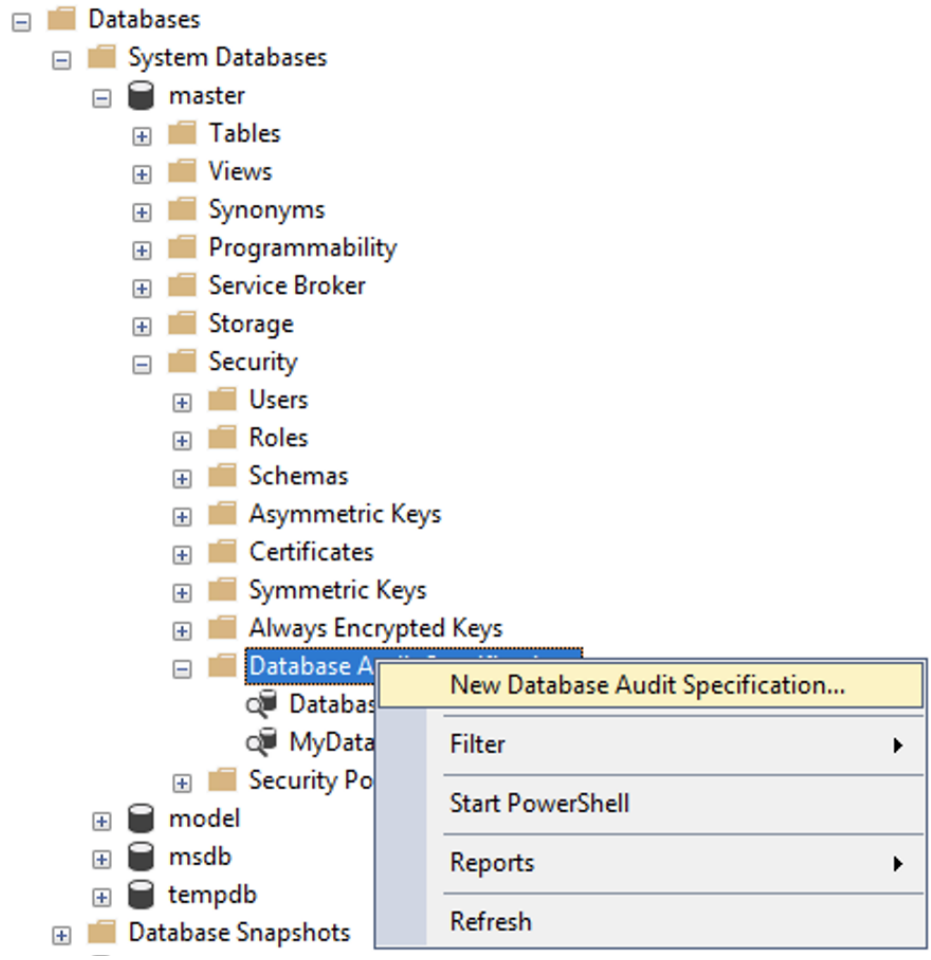
6. Нажмите на кнопку **OK**.
7. Откройте контекстное меню созданного аудита и выберите вариант **Enable Audit**.
8. Откройте контекстное меню **Server Audit Specifications** и выберите вариант **New Server Audit Specification...**. Откроется окно настроек нового объекта спецификации аудита SQL Server.
9. Введите название аудита.
10. Выберите аудит, созданный на уровне сервера.
11. Укажите в таблице типы событий, которые необходимо логировать.



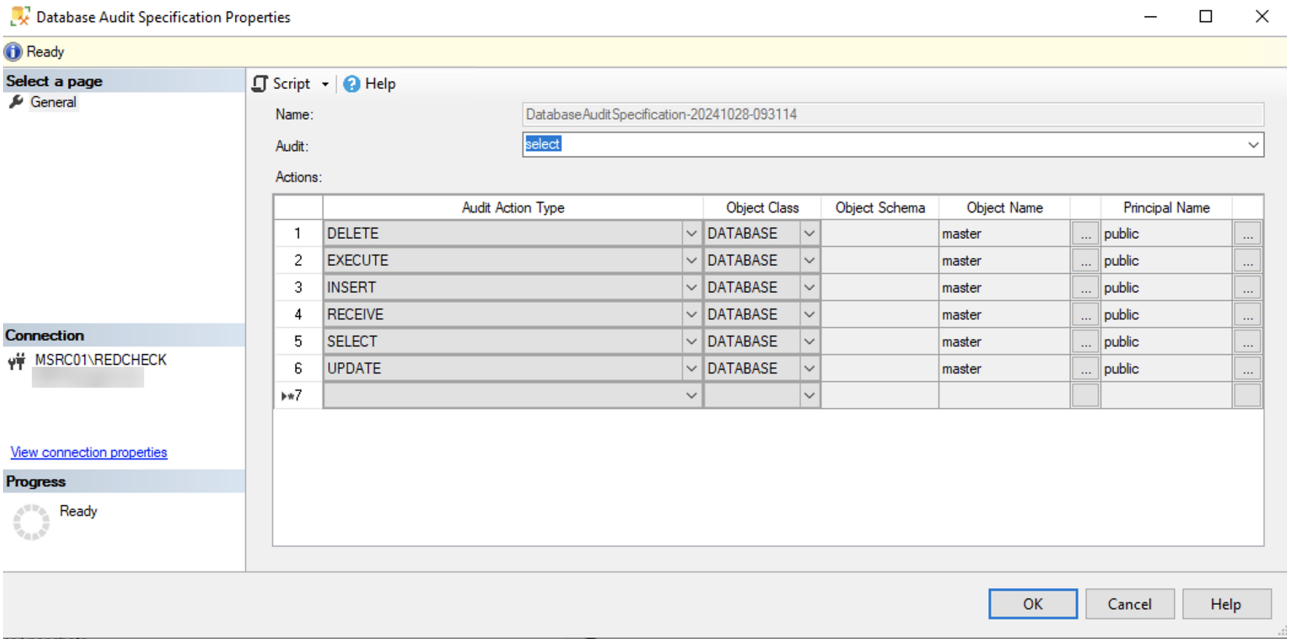
12. Нажмите на кнопку **OK**.

Для настройки аудита на уровне базы данных выполните следующие шаги:

1. Откройте **SQL Server Management Studio**.
2. Подключитесь к базе данных, для которой необходимо включить аудит.
3. В боковом меню перейдите в раздел **Security** выбранной базы данных.
4. Откройте контекстное меню папки **Database Audit Specifications** и выберите вариант **New Database Audit Specification...**. Откроется окно настроек нового объекта аудита SQL Server.



5. Введите имя аудита.
6. Выберите аудит, созданный на уровне сервера.
7. Укажите типы событий, которые необходимо логировать.



8. Нажмите на кнопку **OK**.

Настройка аудита выгрузки ключей и сертификатов MS SQL

Для настройки аудита выгрузки ключей и сертификатов MS SQL выполните следующие шаги:

1. Откройте **SQL Server Management Studio**.
2. Создайте Extended Events-сессию с логированием в файл:

```
DROP EVENT SESSION IF EXISTS TrackBackupCryptoFile ON SERVER;
GO

CREATE EVENT SESSION TrackBackupCryptoFile
ON SERVER
ADD EVENT sqlserver.sql_statement_completed
(
    ACTION (
        sqlserver.sql_text,
        sqlserver.username,
        sqlserver.client_hostname,
        sqlserver.nt_username
    )
    WHERE
        sqlserver.sql_statement_completed.statement LIKE '%BACKUP%CERTIFICATE%' OR
        sqlserver.sql_statement_completed.statement LIKE
'%BACKUP%SERVICE%MASTER%KEY%' OR
        sqlserver.sql_statement_completed.statement LIKE '%BACKUP%MASTER%KEY%' OR
        sqlserver.sql_statement_completed.statement LIKE '%BACKUP%SYMMETRIC%KEY%'
)
ADD TARGET package0.event_file
(
    SET filename = 'C:\AuditLogs\TrackBackupCrypto.xel',
        max_file_size = 10,
        max_rollover_files = 5
);
GO

ALTER EVENT SESSION TrackBackupCryptoFile ON SERVER STATE = START;
```

3. Создайте представление для просмотра событий из файла:

```
CREATE VIEW dbo.BackupCryptoAuditLogView AS
SELECT
    event_xml.value('(event/@timestamp)[1]', 'datetime') AS EventTime,
    ISNULL(event_xml.value('(event/action[@name="username"]/value)[1]',
'nvarchar(100)'), 'N/A') AS SqlLogin,
    ISNULL(event_xml.value('(event/action[@name="client_hostname"]/value)[1]',
'nvarchar(100)'), 'N/A') AS HostName,
    ISNULL(event_xml.value('(event/action[@name="nt_username"]/value)[1]',
'nvarchar(100)'), 'N/A') AS WindowsUser,
    ISNULL(event_xml.value('(event/data[@name="statement"]/value)[1]',
```

```
'nvarchar(max)'), 'N/A') AS Statement,
    ISNULL(event_xml.value('(event/action[@name="sql_text"]/value)[1]',
'nvarchar(max)'), 'N/A') AS FullSQL
FROM sys.fn_xe_file_target_read_file('C:\AuditLogs\TrackBackupCrypto*.xel', NULL,
NULL, NULL) AS xelog
CROSS APPLY (SELECT CAST(xelog.event_data AS XML) AS event_xml) AS evt;
GO
```

4. Настройте автозапуск при старте SQL Server:

```
-- Создаем процедуру автозапуска
CREATE PROCEDURE StartTrackBackupCrypto
AS
BEGIN
    IF NOT EXISTS (
        SELECT * FROM sys.dm_xe_sessions WHERE name = 'TrackBackupCryptoFile'
    )
    BEGIN
        ALTER EVENT SESSION TrackBackupCryptoFile ON SERVER STATE = START;
    END
END;
GO

-- Включаем запуск при старте SQL Server
EXEC sp_procoption 'StartTrackBackupCrypto', 'startup', 'on';
```

5. Предоставьте необходимые права для просмотра представления сервисной учетной записи, созданной ранее:

```
GRANT SELECT ON dbo.BackupCryptoAuditLogView TO [имя пользователя];
EXEC sp_addrolemember 'db_datareader', [имя пользователя];
EXEC sp_addsrvrolemember 'VIEW SERVER STATE', [имя пользователя];
```

Установка агента



Для установки агента обратитесь к документации продукта R-Vision SIEM.

Установите агент R-Vision EVO на станцию и настройте его связь с R-Vision SIEM. После этого в веб-интерфейсе R-Vision SIEM в разделе **Агенты** появится информация о подключенном хосте.

Добавьте хост в группу, в которой настроен сбор журнала `Application`.

Настройка в R-Vision SIEM

Настройка отправки событий в R-Vision SIEM

1. В веб-интерфейсе R-Vision SIEM перейдите в раздел **Агенты** → **Группы агентов**.
2. Создайте группу и добавьте в нее узел, на котором установлен агент.

3. В созданной группе узлов в секции **Чтение файлов** нажмите на кнопку **Добавить настройку** (+).
4. В выпадающем списке **Тип журнала** выберите вариант **eventchannel**.
5. В поле **Имя журнала** введите значение `Application`.
6. Если необходимо выбирать события по определенным критериям, введите в поле **Фильтр (формат XPATH)** выражение XPath. Если фильтр не нужен, введите символ `*`.
7. Нажмите на кнопку **Сохранить**.
8. Дождитесь применения политики группы на узле. Сбор событий настроен.

Настройка обработки событий в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте секрет со строкой подключения. Для этого:
   a. Перейдите в разделы **Ресурсы** → **Секреты** → **Создать**:
   b. В раскрывшемся окне создания секрета заполните поля:
      - **Название**: введите название секрета.
      - **Описание (опционально)**: опишите, для чего будет использоваться секрет.
      - **Тип секрета**: выберите вариант **Строка подключения**.
      - **Строка подключения**: введите строку вида:

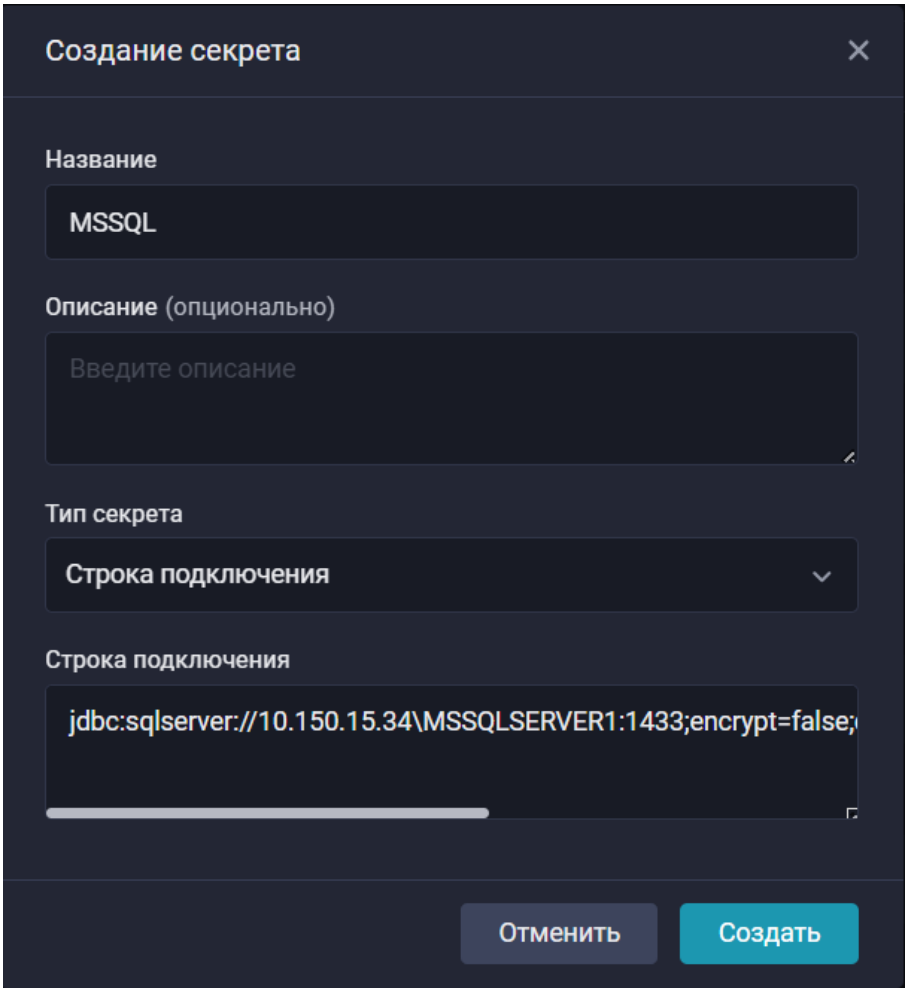
```
jdbc:sqlserver://<address>\<instance>:<port>;encrypt=false;databaseName=<dat
abase>;user=<user>;password=<password>;applicationName=SIEM_MONITOR
```

      где:

      - `<address>` — адрес сервера базы данных.
      - `<instance>` — опциональная сущность сервера СУБД. Для использования сущность должна быть заранее создана с помощью `SQL Server Management Studio`.
      - `<port>` — порт подключения.
      - `<database>` — имя базы событий аудита.
      - `<user>` — логин пользователя базы данных.
      - `<password>` — пароль пользователя базы данных.

        Пример 5. Пример строки подключения:

```
jdbc:sqlserver://10.150.15.34\MSSQLSERVER1:1433;encrypt=false;databaseNam
e=master;user=user;password=P@ssw0rd;applicationName=SIEM_MONITOR
```



c. Нажмите на кнопку **Создать**.

2. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
3. Добавьте на конвейер элемент **Точка входа** для событий аудита команд MS SQL со следующими параметрами:
   - **Название**: введите название точки входа.
   - **Тип точки входа**: выберите вариант **Database**.
   - **Драйвер базы данных**: выберите вариант **MS SQL**.
   - **Адрес подключения**: выберите секрет, созданный ранее.
   - **SQL-запрос**: введите SQL-запрос.

   Пример 6. Пример запроса:

```
DECLARE @appname NVARCHAR(15) = N'MSSQL';

;WITH RecentSessions AS (
    SELECT
        c.session_id,
        c.most_recent_sql_handle,
        c.client_net_address AS src,
        c.client_tcp_port AS spt,
        c.local_net_address AS dst,
        c.local_tcp_port AS dpt,
```

```
        c.auth_scheme,
        s.login_name,
        s.status,
        s.login_time,
        s.program_name,
        s.last_request_start_time AS rt,
        s.host_process_id,
        s.nt_domain,
        s.nt_user_name,
        s.host_name AS shost
    FROM sys.dm_exec_connections AS c
    INNER JOIN sys.dm_exec_sessions AS s
        ON c.session_id = s.session_id
    WHERE s.last_request_start_time >= DATEADD(SECOND, -15, GETDATE())
      AND s.program_name <> 'SIEM_MONITOR'
      AND s.program_name <> 'SQLServerCEIP'
      AND c.most_recent_sql_handle IS NOT NULL
)
SELECT
    rs.session_id,
    @@SERVERNAME AS dvchost,
    rs.login_name,
    rs.status,
    st.text AS query,
    rs.login_time,
    rs.program_name,
    rs.rt,
    rs.auth_scheme,
    rs.host_process_id,
    rs.nt_domain,
    rs.nt_user_name,
    rs.shost,
    rs.src,
    rs.spt,
    rs.dst,
    rs.dpt,
    @appname AS appname
FROM RecentSessions AS rs
CROSS APPLY sys.dm_exec_sql_text(rs.most_recent_sql_handle) AS st
ORDER BY rs.rt DESC;
```

- Интервал запроса, секунд: введите значение 15.

4. Добавьте на конвейер дополнительный элемент **Точка входа** для событий выгрузки ключей и сертификатов со следующими параметрами:
   - **Название**: введите название точки входа.
   - **Тип точки входа**: выберите вариант **Database**.
   - **Драйвер базы данных**: выберите вариант **MS SQL**.
   - **Адрес подключения**: выберите секрет, созданный ранее.

- **SQL-запрос**: введите SQL-запрос.

  Пример 7. Пример запроса:

  ```
  DECLARE @dproduct NVARCHAR(50);
  DECLARE @appname NVARCHAR(15);

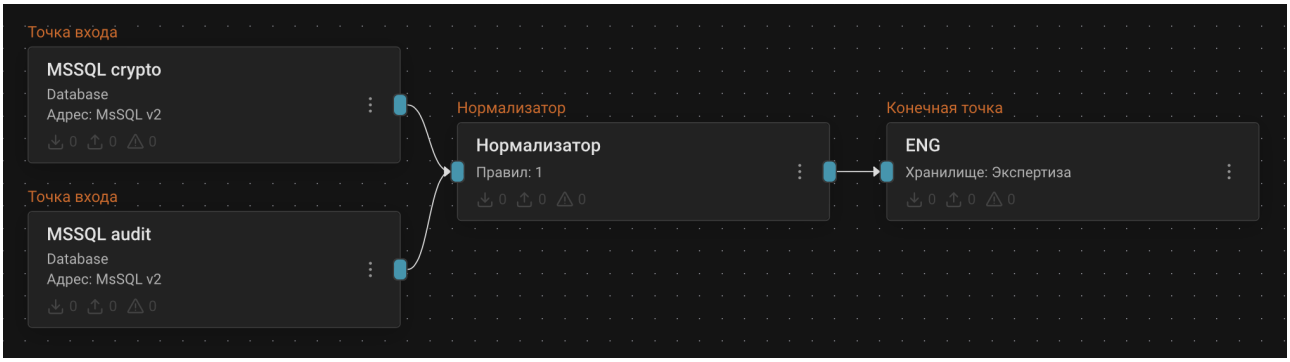
  SET @dproduct = N'SQL Server Crypto';
  SET @appname = N'MSSQL';

  SELECT
      bcalv.*,
      @dproduct AS device_product,
      @appname AS appname,
      @@SERVERNAME AS dvchost
  FROM dbo.BackupCryptoAuditLogView bcalv
  WHERE EventTime > DATEADD(S, CONVERT(INT, ?)+1, '1970-01-01') ORDER BY
  bcalv.EventTime ASC;
  ```

  - **Поле идентификатора**: введите ключ `EventTime` со значением текущего времени в формате UNIX-time.
  - **Интервал запроса, секунд**: введите значение 15.

5. Добавьте на конвейер элемент **Нормализатор** с правилом **Microsoft SQL Server** (идентификатор правила: **RV-N-192**).
6. Соедините нормализатор с точками входа.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

   Пример конфигурации конвейера:



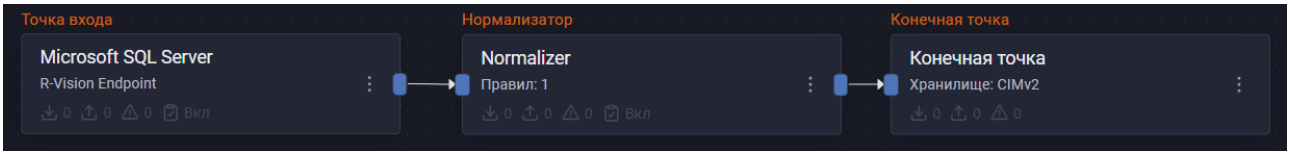
Нормализацию событий из других журналов, которые собираются с помощью агента R-Vision EVO, настройте на отдельном конвейере. Для этого:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - **Название**: введите название точки входа.

- **Тип точки входа**: выберите вариант **R-Vision Endpoint**.
- **Домен**: введите значение в формате `gw-<your_gateway_id>`, где `<your_gateway_id>` — ID шлюза.

3. Добавьте на конвейер элемент **Нормализатор** с правилом **Microsoft SQL Server** (идентификатор правила: **RV-N-212**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

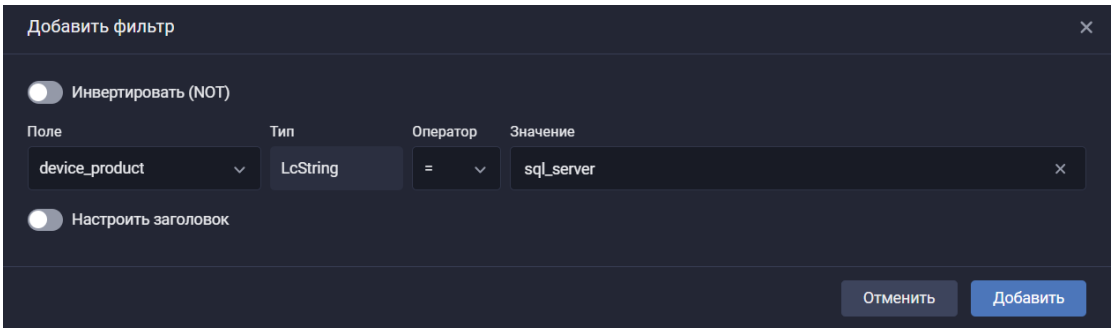
   Пример конфигурации конвейера:



После настройки передачи событий если настройка выполнена корректно, в хранилище начнут поступать события из журналов SQL Server.

Найти события источника в хранилище можно по фильтру:

```
device_product = "sql_server"
```



Microsoft SQL Server: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-784	Создание резервных копий MS SQL средствами PowerShell	Данное правило направлено на обнаружение создания резервной копии базы данных через PowerShell. В случае срабатывания правила необходимо запросить информацию о причинах активности у ответственного за учетную запись. Если легитимность подтвердить не удалось, рекомендуется временно заблокировать учетную запись, ограничить доступ к узлу, на котором произошли подозрительные действия, и инициировать внутреннее расследование.	• Collection (TA0009) • Data Staged (T1074) • Data from Information Repositories (T1213)
RV-D-1401	Создание резервной копии БД MS SQL Server	Атакующий может сохранить конфиденциальную информацию из базы данных для дальнейшей ее обработки на удаленном хосте. Правило обнаруживает попытку сохранения таблицы из базы данных SQL Server в файл.	• Credential Access (TA0006) • Collection (TA0009) • OS Credential Dumping (T1003) • Data from Local System (T1005) • Data Staged (T1074) • Local Data Staging (T1074.001)
RV-D-1402	Подбор пароля к MS SQL Server	Правило обнаруживает множественные неудачные попытки подключения к СУБД SQL Server от одной учетной записи, учитывая попытки с разных хостов.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)
RV-D-1411	Атака Password Spraying на MS SQL Server	Правило обнаруживает множественные неудачные попытки подключения к СУБД SQL Server от одного хоста к множеству учетных записей.	• Credential Access (TA0006) • Brute Force (T1110) • Password Spraying (T1110.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1412	Успешный подбор пароля MS SQL Server	Правило обнаруживает успешную попытку входа после множественных неудачных попыток подключения к СУБД SQL Server от одной учетной записи, учитывая попытки с разных узлов.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)
RV-D-1414	Получение хеша пароля пользователей MSSQL	Атакующий может получить информацию о хешах паролей пользователей MSSQL. Данная атака может помочь заполучить доступ к учетной записи с высокими привилегиями для дальнейшего закрепления. Детектирование происходит через выполнение запросов по определенным функциям.	• Credential Access (TA0006) • OS Credential Dumping (T1003)
RV-D-1419	Попытка получить состояние службы Windows	Атакующие могут злоупотреблять хранимыми процедурами SQL для установления постоянного доступа либо же в рамках выполнения разведки. В данном правиле отслеживается попытки получить состояние Windows-службы из базы данных с использованием расширенной хранимой процедуры `xp_servicecontrol`.	• Discovery (TA0007) • System Service Discovery (T1007) • Server Software Component (T1505) • SQL Stored Procedures (T1505.001)
RV-D-1439	Получение информации о версии MSSQL	Атакующий может получить информацию о версии MSSQL для эксплуатации потенциальных уязвимостей и последующего развития атаки. Обнаружение активности происходит на основании выполненных запросов, содержащих `SELECT` и одной из функции version или serverproperty.	• Discovery (TA0007) • System Information Discovery (T1082)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1447	Получение информации о привилегиях пользователя MSSQL	Атакующий может получить информацию о привилегиях пользователя MSSQL. Данная атака может помочь в получении информации о системе для дальнейшего закрепления. Детектирование происходит через выполнение команд по определенным функциям и процедурам.	• Discovery (TA0007) • Account Discovery (T1087)
RV-D-1449	Получение информации о пользователях ОС	Атакующий может получить информацию о пользователях windows средствами MSSQL. Данная атака может помочь в получении информацию о системе для дальнейшего развития атаки. Обнаружение активности происходит на основании выполненных запросов содержащие определённые функции.	• Discovery (TA0007) • Account Discovery (T1087)
RV-D-1450	Доступ к локальной файловой системе MSSQL	Данное правило направлено на обнаружение поиска информации или изменения файлов в локальной файловой системе из СУБД MSSQL. Обнаружение осуществляется на основании запроса, содержащего команду EXEC и одну из функций `xp_dirtree` или `xp_cmdshell`.	• Discovery (TA0007) • File and Directory Discovery (T1083) • Data Manipulation (T1565)
RV-D-1455	Получение информации об алгоритме шифрования БД	Шифрование баз данных – это метод защиты информации, хранящейся в базе данных, посредством преобразования данных в нечитаемый формат. Transparent Data Encryption (TDE) обеспечивает защиту данных «на диске» от несанкционированного доступа в случае физической компрометации носителей.	• Discovery (TA0007) • System Information Discovery (T1082) • Software Discovery (T1518) • Security Software Discovery (T1518.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1457	Поиск пользователей с административными правами в MSSQL	Атакующий может получить информацию о пользователях с административными правами MSSQL, для последующего развития атаки. Обнаружение осуществляется на основание запроса, содержащего оператор `SELECT`, и далее одну из функций, позволяющую получить информацию о пользователях с административными правами.	• Discovery (TA0007) • Account Discovery (T1087)
RV-D-1461	Получение информации об аудите MS SQL Server	Атакующий может получить информацию о текущем состоянии аудита на уровне сервера или базы данных. Правило отслеживает характерные запросы, которые содержат одно из представлений `dm_server_audit_status`, `server_audit_specifications`, `server_audit_specification_details`, позволяющее получить различную информацию о состоянии аудита.	• Discovery (TA0007) • Software Discovery (T1518) • Security Software Discovery (T1518.001)
RV-D-1466	Чтение ключа реестра средствами MSSQL	Атакующие могут читать ключи и значения реестра Windows для сбора информации о конфигурации системы и установленном ПО, используя встроенные процедуры MSSQL - `xp_regread` и `xp_instance_regread`. Данное правило отслеживает попытки прочитать значение ключа реестра из базы данных.	• Discovery (TA0007) • Query Registry (T1012) • System Information Discovery (T1082)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1470	Поиск резервных копий базы данных	Атакующие могут использовать встроенные механизмы MSSQL для получения информации о расположении резервных копий баз данных. Доступ к этим данным позволяет подготовиться к компрометации критически важных резервных копий, их удалению, подмене или извлечению конфиденциальной информации. Данное правило корреляции отслеживает запросы типа `SELECT` к таблице `backupmediafamily`. При срабатывании правила необходимо проверить учетную запись, выполнявшую запрос, и установить, соответствует ли ее активность типичным действиям администратора или базы данных. Если запрос был выполнен неожиданным пользователем или в необычное время, следует изучить дополнительные события в журналах MSSQL, включая историю команд и возможные попытки удаления или копирования резервных копий.	• Persistence (TA0003) • Discovery (TA0007) • File and Directory Discovery (T1083)
RV-D-1471	Получение информации о пользователях MSSQL	Атакующий может получить информацию о пользователях MSSQL для последующего развития атаки. Обнаружение осуществляется на основании запроса, содержащего оператор `SELECT` и далее одну из функций, позволяющую получить информацию о пользователях.	• Discovery (TA0007) • Account Discovery (T1087)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1480	Вход привилегированного пользователя в MS SQL Server	Атакующий может получить привилегированные учетные данные и попытаться авторизоваться с контролируемого им хоста. Правило обнаруживает попытку авторизации привилегированного пользователя с неизвестного хоста в SQL Server.	• Initial Access (TA0001) • Valid Accounts (T1078) • Local Accounts (T1078.003)
RV-D-1481	Использование процедур для локального выполнения кода	Хранимая процедура – это заранее скомпилированный набор SQL-операторов, который хранится в базе данных. Возможности, предоставляемые хранимыми процедурами, могут быть использованы не только для легитимных административных задач, но и для выполнения системных команд, позволяющих напрямую обращаться к операционной системе.	• Execution (TA0002) • Command and Scripting Interpreter (T1059)
RV-D-1482	Установка небезопасного свойства MS SQL	Отключение шифрования базы данных и включение параметра `TRUSTWORTHY` могут привести к созданию потенциальных уязвимостей и дать атакующим дополнительные возможности для несанкционированного доступа к данным или обхода механизмов безопасности.	• Defense Evasion (TA0005) • Subvert Trust Controls (T1553) • Weaken Encryption (T1600)
RV-D-1483	Запись ключа реестра средствами MSSQL	Использование хранимых процедур `xp_regwrite` и `xp_instance_regwrite` позволяет взаимодействовать с реестром Windows непосредственно из SQL Server. Запись в реестр может быть признаком попытки изменения конфигурации системы или для закрепления в системе. Данное правило отслеживает попытки записать значение ключа реестра из базы данных.	• Defense Evasion (TA0005) • Modify Registry (T1112)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1489	Попытка включить смешанную аутентификацию MS SQL	SQL Server поддерживает два основных режима аутентификации - только Windows-аутентификация и смешанный режим (Windows + SQL Server аутентификация). По умолчанию используется Windows-аутентификация, которая базируется на механизмах контроля доступа в домене и считается более безопасной. Смешанный режим же включает возможность входа через логины SQL Server, включая встроенную учетную запись sa (System Administrator). При обнаружении активности требуется опросить владельца учетной записи инициатора активности о причинах смены режима аутентификации. В случае отсутствия подтверждения легитимности данной активности произвести блокировку учетной записи инициатора активности и восстановить прежнюю конфигурацию системы.	• Defense Evasion (TA0005) • Modify Registry (T1112) • Modify Authentication Process (T1556)
RV-D-1490	Отключение политики входа пользователей MS SQL	Отключение проверки срока действия пароля и политики сложности в Microsoft SQL Server делает пароли потенциально слабыми и бесконечно долгоживущими. Атакующий может воспользоваться этим, чтобы легко подобрать пароль и получить несанкционированный доступ к серверу.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Account Manipulation (T1098) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1492	Изменение аудита базы данных MS SQL Server	Атакующий может изменить состояния текущего аудита на уровне сервера или базы данных. Правило отслеживает характерные запросы, которые позволяет изменить действующую политику аудита.	• Defense Evasion (TA0005) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001) • Spoof Security Alerting (T1562.011)
RV-D-1493	Включение небезопасных параметров в конфигурации MSSQL	Включение потенциально опасных параметров конфигурации в MSSQL может привести к эскалации привилегий, удаленному выполнению команд или обходу механизмов безопасности. Атакующие могут использовать эти параметры для закрепления в системе или выполнения вредоносных действий.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Defense Evasion (TA0005) • Create or Modify System Process (T1543) • Windows Service (T1543.003) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1497	Использование хранимых процедур `sp_proxy` и `sp_grant_proxy`	Атакующие могут злоупотреблять хранимыми процедурами SQL для получения привилегий и выполнения команд от имени привилегированных учетных записей. Одним из таких механизмов является использование proxy-аккаунтов в SQL Server Agent. Proxy-аккаунты позволяют запускать задания SQL Server Agent с повышенными привилегиями, обходя стандартные ограничения учетных записей. Атакующий может создать или назначить proxy-аккаунт с привилегиями, которых нет у его основной учётной записи, и выполнить действия от имени этой учётной записи, тем самым обходя контроль доступа. Наибольшую опасность представляют proxy, привязанные к подсистемам CmdExec, PowerShell и SSIS, так как они позволяют выполнить произвольный код с привилегиями proxy-пользователя. Данное правило обнаруживает вызовы хранимых процедур `sp_add_proxy` и `sp_grant_proxy_to_subsystem`.	• Persistence (TA0003) • Defense Evasion (TA0005) • Server Software Component (T1505) • SQL Stored Procedures (T1505.001) • Abuse Elevation Control Mechanism (T1548)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1498	Назначена роль администратора пользователю MS SQL Server	Правило обнаруживает присвоение привилегированной роли для учетной записи в СУБД SQL Server на основании событий, содержащих соответствующий SQL запрос. При обнаружении событии требуется уточнить у ответственного за учетную запись или сервер о причинах присвоения привилегированной роли. В случае если легитимность вышеуказанных действий подтвердить не удалось требуется заблокировать учетную запись до определения обстоятельств инцидента.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Account Manipulation (T1098)
RV-D-1501	Изменение пароля привилегированной УЗ MS SQL Server	Правило обнаруживает изменение паролей привилегированных учетных записей в СУБД SQL Server на основе событий проверки парольной политики или событий, содержащих SQL запрос на изменение пароля.	• Persistence (TA0003) • Account Manipulation (T1098)
RV-D-1504	Попытка изменить состояние службы Windows	В данном правиле отслеживается попытка изменить состояние Windows-сервиса из базы данных с использованием расширенной хранимой процедуры `xp_servicecontrol`. Атакующие могут использовать данный метод для запуска или остановки критически важных сервисов, таких как SQL Server Agent, что позволяет им влиять на работу системы и скрывать вредоносную активность.	• Execution (TA0002) • Impact (TA0040) • Service Stop (T1489) • System Services (T1569) • Service Execution (T1569.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1506	Отправка результатов SQL-запроса почтой	В MS SQL Server существует встроенная функциональность — Database Mail, которая позволяет отправлять электронные письма прямо из базы данных. Это может быть полезно администраторам для автоматической отправки отчетов, результатов мониторинга или оповещений о сбоях. Но также может использоваться атакующими для передачи информации.	• Exfiltration (TA0010) • Exfiltration Over Web Service (T1567)
RV-D-1507	Удаление базы данных в MS SQL Server	Данное правило направлено на обнаружение деструктивных операций в MS SQL Server, связанных с удалением баз данных (команда `DROP DATABASE`). Выполнение таких команд ведет к немедленной потере доступности информационных активов и может являться признаком критического инцидента безопасности. Подобная активность характерна для финальных стадий атак, направленных на саботаж работы организации, уничтожение следов присутствия атакующих в системе или реализацию угроз в рамках атак программ-вымогателей.	• Impact (TA0040) • Data Destruction (T1485)
RV-D-1508	Удаление нескольких таблиц в MS SQL Server	Атакующий с целью нарушения функционирования системы может попытаться удалить значимые таблицы в базе данных. Правило обнаруживает удаление 5 таблиц в течении минуты в SQL Server с помощью характерных запросов.	• Impact (TA0040) • Data Destruction (T1485)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1510	Попытка подключения к СУБД через DAC	Dedicated Admin Connection – это соединение в SQL Server, которое резервируется для подключения администратора. `DAC` используется только в том случае, если сервер находится под массивной нагрузкой, соединиться обычными способами не получается. Если атакующий получает доступ к `DAC`, он может использовать его для скрытого управления сервером, обходя стандартный мониторинг. Это позволяет ему запускать вредоносные команды через `xp_cmdshell`, загружать и исполнять бэкдоры, а также стирать важные логи с помощью `xp_delete_file`, затрудняя расследование инцидента. Что становится серьезным риском, так как в распоряжении атакующего полный контроль над SQL Server. Данное правило отслеживает попытки подключения через `DAC`, используя события `33205`, которые содержат информацию об успешных и неуспешных попытках авторизации на СУБД.	• Persistence (TA0003) • Server Software Component (T1505)

MongoDB

- MongoDB: настройка источника

MongoDB: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий MongoDB в R-Vision SIEM.

Предварительные требования

- Сетевая связность между сервером СУБД (MongoDB) и SIEM (или промежуточным syslog-сервером) обеспечена, а необходимые порты открыты.
- Создана учетная запись с правами администратора для изменения конфигурации MongoDB и rsyslog.

Настройка MongoDB

Настройка аудита



Данная настройка приведена для MongoDB Enterprise Edition. MongoDB Community Edition не поддерживает функцию auditLog.

Для настройки аудита MongoDB выполните следующие шаги:

1. Откройте конфигурационный файл `/etc/mongod.conf`:

```
nano /etc/mongod.conf
```

2. Отредактируйте следующие блоки:

```
systemLog:
  verbosity: 0
  destination: syslog
  timeStampFormat: iso8601-local
  component:
    accessControl:
      verbosity: 1
    command:
      verbosity: 0
    network:
      verbosity: 0

security:
  authorization: enabled

## Enterprise-Only Options
# Включение auditLog.
auditLog:
  destination: file
  format: JSON
  path: /var/log/mongodb/audit.log
  filter: |
    {
      "$and": [
        { "param.command": { "$nin": ["hello", "ping"] } },
        { "$or": [
            { "atype": { "$in": ["authenticate","authCheck"] } },
            { "atype": { "$in":
["createUser","dropUser","grantRolesToUser","revokeRolesFromUser","updateUser"] }
},
            { "param.command": { "$in":
["insert","update","delete","find","findAndModify","drop","dropDatabase"] } },
            { "param.command": { "$in":
["shutdown","replSetInitiate","replSetReconfig","setParameter","enableSharding"] }
```

```
}
          ]
        }
      ]
    }

# Включение логирования успешных операций.
setParameter:
  auditAuthorizationSuccess: true
```

3. Перезапустите сервис MongoDB:

```
systemctl restart mongod
```

4. Настройте logrotate для файлов аудита. Пример `/etc/logrotate.d/mongodb-audit`:

```
/var/log/mongodb/audit.log {
    daily
    rotate 7
    compress
    delaycompress
    missingok
    notifempty
    copytruncate
}
```

Настройка службы rsyslog

Чтобы настроить службу rsyslog, выполните следующие действия:

1. Создайте файл конфигурации rsyslog:

```
sudo nano /etc/rsyslog.d/10-siem.conf
```

2. Добавьте в созданный файл следующее правило:

```
module(load="imfile" PollingInterval="10")  # Модуль для файлов.
input(type="imfile"
      File="/var/log/mongodb/audit.log"
      Tag="mongod"
      Severity="info"
      Facility="local0"
      PersistStateInterval="200")

if $programname == 'mongod' or $programname == 'mongos' or $syslogtag == 'mongod'
then {
  action(type="omfwd" Target="<target>" Port="<port>" Protocol="<protocol>")
```

```
  stop
}
```

Здесь:

- `<target>` — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- `<port>` — порт точки входа Syslog на конвейере SIEM.
- `<protocol>` — сетевой протокол: `tcp` или `udp`.

3. Перезапустите rsyslog для применения изменений:

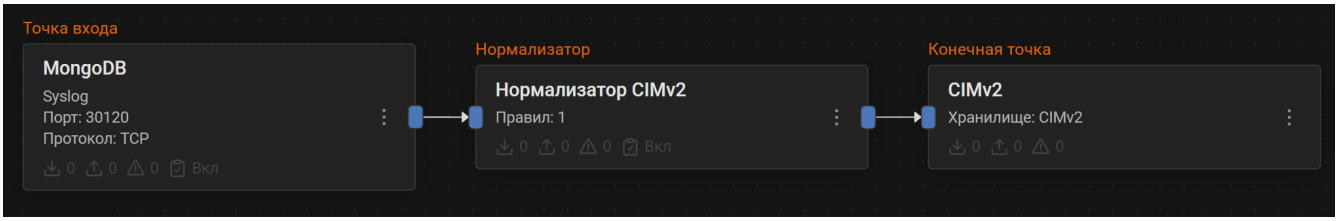
```
sudo systemctl restart rsyslog
```

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне MongoDB.
   - Протокол: выберите вариант в соответствии с настройками на стороне MongoDB.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **MongoDB** (идентификатор правила: **RV-N-293**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Установите конфигурацию конвейера.

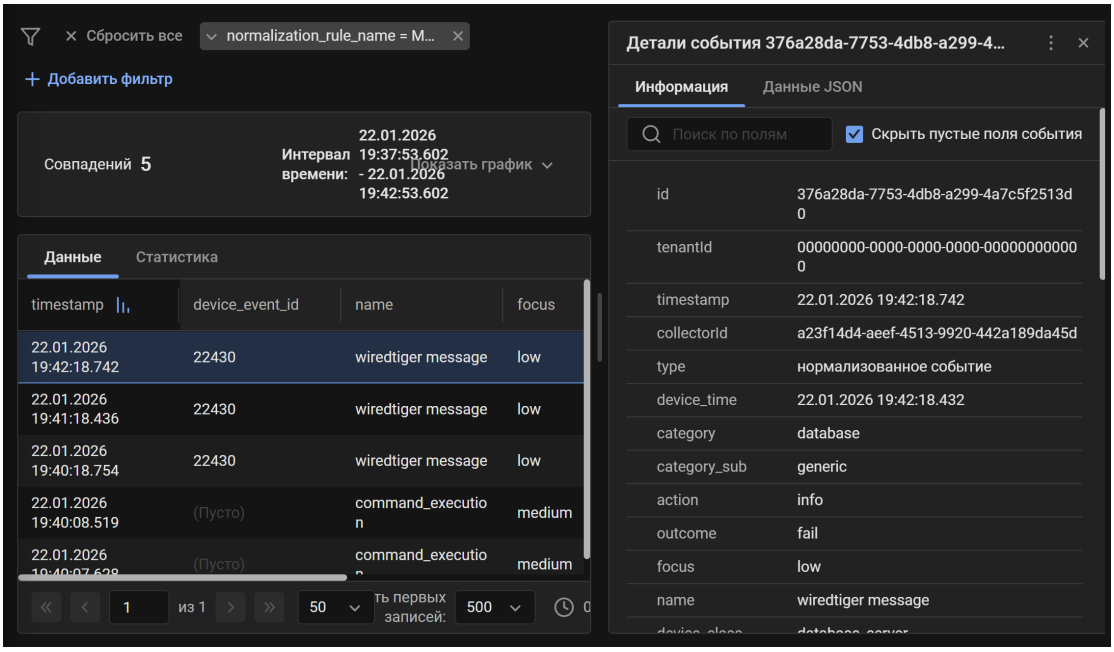
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события MongoDB.

Найти события MongoDB в хранилище можно по следующему фильтру:

```
normalization_rule_name = "MongoDB"
```



Oracle Database

- Oracle Database: настройка источника
- Oracle Database (syslog): настройка источника
- Oracle Database: правила корреляции

Oracle Database: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Oracle Database в R-Vision SIEM.

Предварительные требования

Перед началом настройки убедитесь, что выполнены следующие условия:

- Пользователь, выполняющий настройку, имеет права администратора.
- Создана сервисная учетная запись с правами на чтение таблицы `UNIFIED_AUDIT_TRAIL` и просмотр аудита (`AUDIT_VIEWER`).

Настройка Oracle Database

Настройка журналирования

В версиях 23ai и 26ai `Unified Auditing` включен по умолчанию. Проверьте статус:

```
SQL> SELECT value FROM v$option WHERE parameter = 'Unified Auditing';
```

1. Создайте политику аудита сессий через `Unified Auditing`:

```
SQL> CREATE AUDIT POLICY audit_sessions ACTIONS LOGON,LOGOFF;
```

2. Примените политику к пользователям:

```
SQL> AUDIT POLICY audit_sessions;
```

3. Аналогично создайте политику для DDL:

```
SQL> CREATE AUDIT POLICY audit_ddl
    ACTIONS CREATE TABLE, ALTER TABLE, DROP TABLE,
            CREATE VIEW, DROP VIEW,
            CREATE SYNONYM, CREATE SEQUENCE;
SQL> AUDIT POLICY audit_ddl;
```

4. Создайте политику аудита DML для чувствительных таблиц (рекомендуется выбирать только критичные таблицы для снижения объема логов):

```
SQL> CREATE AUDIT POLICY audit_dml
    ACTIONS SELECT, INSERT, UPDATE, DELETE ON <таблица>;
SQL> AUDIT POLICY audit_dml;
```

5. Создайте политику аудита привилегий:

```
SQL> CREATE AUDIT POLICY audit_privileges
    ACTIONS GRANT, REVOKE, CREATE USER, DROP USER, ALTER USER, CREATE ROLE, DROP
ROLE;
SQL> AUDIT POLICY audit_privileges;
```

6. Проверьте активные политики `Unified Auditing`:

```
SQL> SELECT policy_name, enabled_option, entity_name, success, failure
    FROM audit_unified_enabled_policies;
```

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

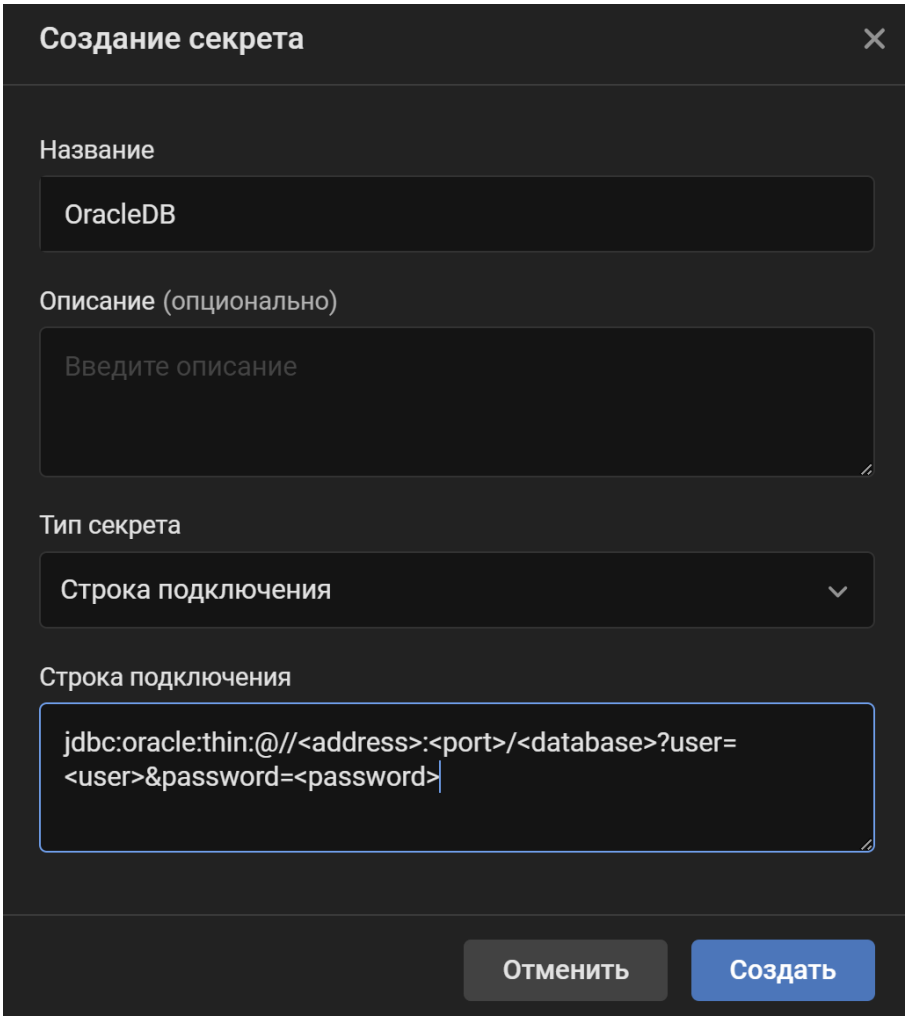
1. Скачайте драйвер `ojdbc11.jar` (из состава Oracle 23ai или 26ai) с официального сайта Oracle JDBC Downloads.
2. В интерфейсе R-Vision SIEM загрузите драйвер БД согласно официальной инструкции.

3. Перезагрузите коллектор, через который планируется подключение точки входа.
4. В интерфейсе R-Vision SIEM создайте секрет со строкой подключения. Для этого:
    a. Перейдите в раздел **Ресурсы** → **Секреты** → **Создать**.
    b. В раскрывшемся окне создания секрета заполните поля:
        - Название: введите название секрета.
        - Описание (опционально): опишите, для чего будет использоваться секрет.
        - Тип секрета: выберите вариант **Строка подключения**.
        - Строка подключения: введите строку вида:

```
jdbc:oracle:thin:@//<address>:<port>/<database>?user=<user>&password=<passwo
rd>
```

Здесь:

- `<address>`: адрес сервера базы данных.
- `<port>`: порт подключения.
- `<database>`: имя базы данных.
- `<user>`: логин пользователя базы данных.
- `<password>`: пароль пользователя базы данных.



c. Нажмите на кнопку **Создать**.

5. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
6. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Database**.
   - Драйвер базы данных: выберите вариант **Oracle Database**.
   - Адрес подключения: выберите секрет, созданный ранее.
   - SQL-запрос: введите запрос вида:

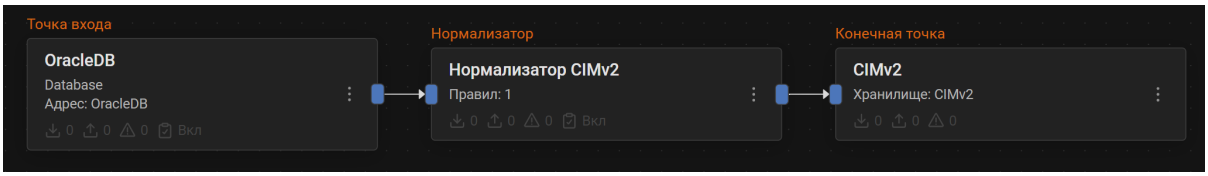
```
SELECT
    'oracledb' AS DATASOURCE,
    SYS_CONTEXT('USERENV', 'SERVER_HOST') AS DB_SERVER_NAME,
    EVENT_TIMESTAMP,
    DBUSERNAME,
    ACTION_NAME,
    OBJECT_NAME,
    OBJECT_SCHEMA,
    USERHOST,
    SYSTEM_PRIVILEGE_USED,
    RETURN_CODE,
    SESSIONID,
```

```
    SQL_TEXT,
    ENTRY_ID,
    SCN
FROM UNIFIED_AUDIT_TRAIL
WHERE SCN > ?
ORDER BY SCN ASC
```

- Поле идентификатора: введите ключ `SCN` со значением `0`.
- Интервал запроса, секунд: введите значение `15`.

7. Добавьте на конвейер элемент **Нормализатор** с правилом **Oracle Database** (идентификатор правила: **RV-N-319**).
8. Соедините нормализатор с точкой входа.
9. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
10. Соедините конечную точку с нормализатором.
11. Сохраните и установите конфигурацию конвейера.

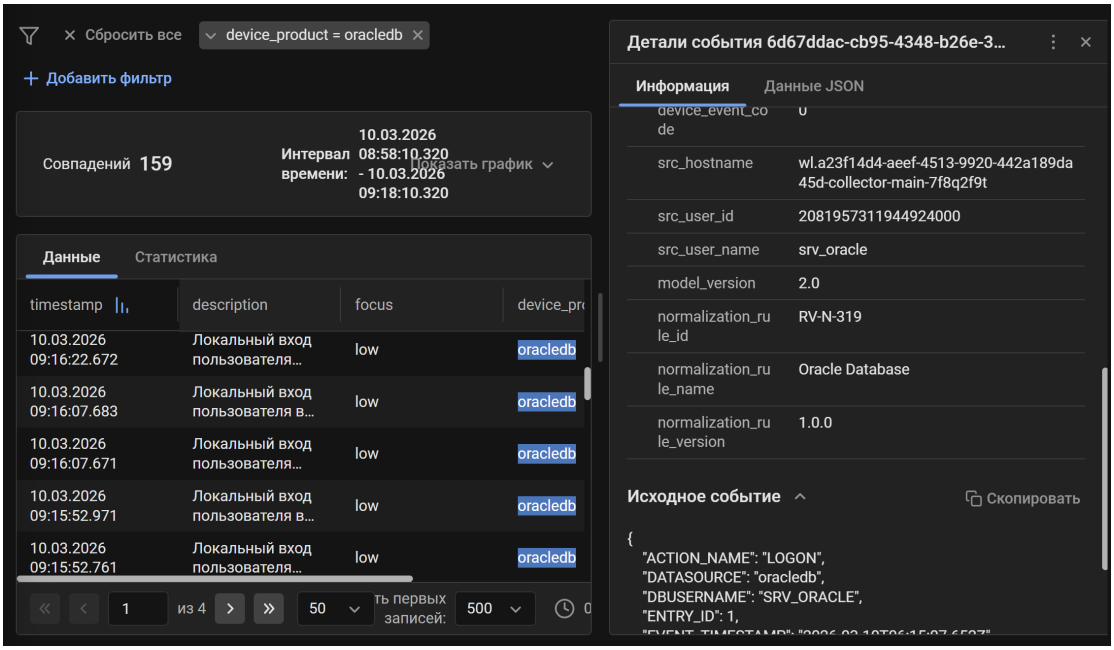
    Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Oracle Database.

Найти события Oracle Database в хранилище можно по следующему фильтру:

```
device_product = "oracledb"
```



Oracle Database (syslog): настройка источника

Данное руководство описывает процесс настройки сбора событий Oracle Database с помощью протокола `syslog` и их отправки в R-Vision SIEM.

Предварительные требования

Перед началом настройки убедитесь, что выполнены следующие условия:

- На машине, с которой планируется сбор событий, установлен сервис `rsyslog` или `syslog-ng`.
- Пользователь, выполняющий настройку, имеет права администратора.

Настройка Oracle Database

Настройка журналирования

В версиях 23ai и 26ai `Unified Auditing` включен по умолчанию. Проверьте статус:

```
SQL> SELECT value FROM v$option WHERE parameter = 'Unified Auditing';
```

1. Создайте политику аудита сессий через `Unified Auditing`:

   ```
   SQL> CREATE AUDIT POLICY audit_sessions ACTIONS LOGON,LOGOFF;
   ```

2. Примените политику к пользователям:

   ```
   SQL> AUDIT POLICY audit_sessions;
   ```

3. Аналогично создайте политику для DDL:

   ```
   SQL> CREATE AUDIT POLICY audit_ddl
       ACTIONS CREATE TABLE, ALTER TABLE, DROP TABLE,
               CREATE VIEW, DROP VIEW,
               CREATE SYNONYM, CREATE SEQUENCE;
   SQL> AUDIT POLICY audit_ddl;
   ```

4. Создайте политику аудита DML для чувствительных таблиц (рекомендуется выбирать только критичные таблицы для снижения объема логов):

   ```
   SQL> CREATE AUDIT POLICY audit_dml
       ACTIONS SELECT, INSERT, UPDATE, DELETE ON <таблица>;
   SQL> AUDIT POLICY audit_dml;
   ```

5. Создайте политику аудита привилегий:

```
SQL> CREATE AUDIT POLICY audit_privileges
    ACTIONS GRANT, REVOKE, CREATE USER, DROP USER, ALTER USER, CREATE ROLE, DROP
ROLE;
SQL> AUDIT POLICY audit_privileges;
```

6. Проверьте активные политики `Unified Auditing`:

```
SQL> SELECT policy_name, enabled_option, entity_name, success, failure
    FROM audit_unified_enabled_policies;
```



В версии 23ai режим записи в базу данных и в `syslog` обычно исключают друг друга для минимизации нагрузки. Настраивайте `unified_audit_systemlog`, если вас интересует сбор событий только через `syslog`.

Чтобы Oracle начал писать события в системный лог, измените параметры инициализации базы:

1. В базе (под `SYS`):

```
SQL> ALTER SYSTEM SET audit_syslog_level='local1.info' SCOPE=SPFILE;
```

2. Примените изменения, перезапустив базу:

```
SQL> SHUTDOWN IMMEDIATE;
SQL> STARTUP;
```

Настройка отправки событий в R-Vision SIEM



В настоящем руководстве рассматривается передача событий с помощью сервиса `rsyslog`.

События сервера Oracle Database могут отправляться на централизованный сервер `syslog` или напрямую в систему R-Vision SIEM.

Чтобы настроить отправку событий сервера Oracle Database, выполните следующие шаги:

1. Создайте конфигурационный файл `rsyslog` в директории `/etc/rsyslog.d/`.
2. Добавьте в файл следующие правила:

```
if $programname startswith 'oracle' then {
  action(type="omfwd" target="<target>" port="<port>" protocol="<protocol>")
  stop
}
```

Здесь:

- `<target>`: IP-адрес или полное доменное имя (FQDN) коллектора R-Vision SIEM.
- `<port>`: порт точки входа `Syslog` на конвейере R-Vision SIEM.
- `<protocol>`: сетевой протокол (`tcp` или `udp`).

3. Перезапустите службу `rsyslog` для применения изменений:

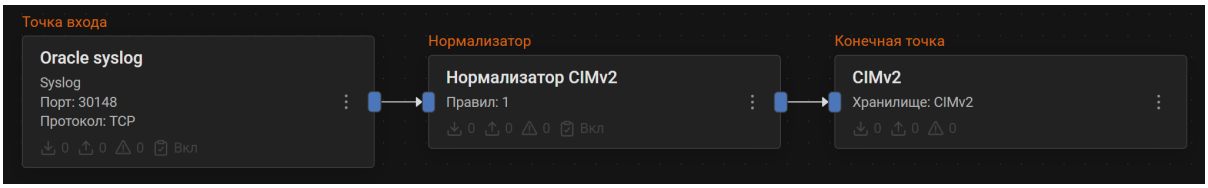
```
sudo systemctl restart rsyslog
```

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне источника.
   - Протокол: выберите вариант в соответствии с настройками на стороне источника.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Oracle Database** (идентификатор правила: **RV-N-210**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

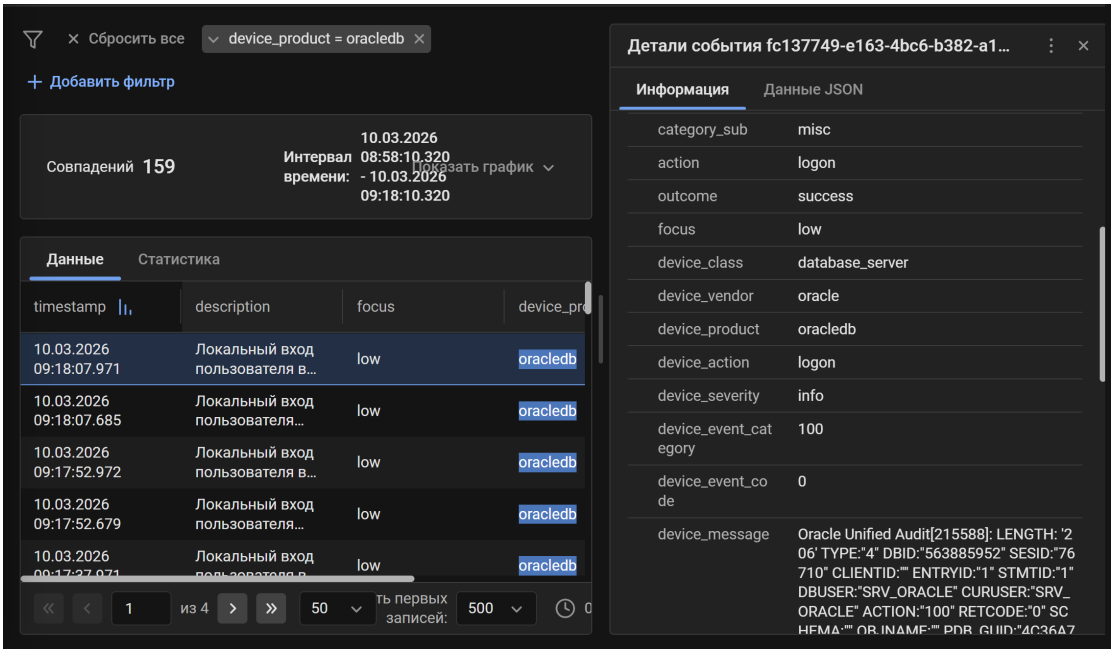


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Oracle Database.



Найти события Oracle Database в хранилище можно по следующему фильтру:

```
device_product = "oracledb"
```



Oracle Database: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1574	Подбор пароля к СУБД Oracle	Данное правило направлено на обнаружение подозрительных действий, связанных с попытками перебора (bruteforce) учетных данных для доступа к базе данных Oracle. Такие действия могут включать многократные неудачные попытки входа в систему с использованием стандартных инструментов, таких как `sqlplus`, или автоматизированных скриптов для подбора паролей. Детектирование происходит за счет множества событий (от пяти) неудачного входа. Эксплуатация данной техники может привести к компрометации учетных записей и несанкционированному доступу к конфиденциальным данным.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1576	Успешный подбор пароля к СУБД Oracle	Данное правило направлено на обнаружение подозрительных действий, связанных с успешным перебором (bruteforce) учетных данных для доступа к базе данных Oracle. Такие действия могут включать успешный вход в систему после серии неудачных попыток, что может свидетельствовать о том, что атакующему удалось подобрать правильную комбинацию логина и пароля. Детектирование происходит за счет анализа событий входа, где успешная аутентификация следует за множеством неудачных попыток (например, пять или более). Эксплуатация данной техники может привести к компрометации учетных записей и несанкционированному доступу к конфиденциальным данным, что представляет серьезную угрозу для безопасности базы данных. Успешный `bruteforce` часто является результатом слабых паролей, отсутствия ограничений на количество попыток ввода или недостаточного мониторинга подозрительной активности.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1582	Атака Password Spraying на OracleDB	Данное правило направлено на обнаружение подозрительных действий, связанных с атакой Password Spraying на базу данных Oracle. Password Spraying — это метод атаки, при котором атакующий использует небольшое количество распространенных паролей для попытки доступа к множеству учетных записей. В отличие от классического bruteforce, где атакующий перебирает множество паролей для одной учетной записи, Password Spraying позволяет избежать блокировки учетных записей за счет распределения попыток входа по времени.	• Credential Access (TA0006) • Brute Force (T1110) • Password Spraying (T1110.003)
RV-D-1585	Вход привилегированного пользователя в СУБД Oracle	Данное правило направлено на обнаружение попыток входа под учетными записями администратора Oracle. Доступ к таким учетным записям предоставляет атакующему полный контроль над базой данных, что может привести к утечке конфиденциальной информации, изменению критически важных данных или уничтожению структуры базы. Детектирование осуществляется путем анализа событий аутентификации, фиксирующих успешные попытки входа под административными учетными записями. Подозрительной активностью могут считаться входы с нестандартных устройств.	• Initial Access (TA0001) • Valid Accounts (T1078)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1586	Поиск информации о структуре в OracleDB	Данное правило направлено на обнаружение подозрительных действий, связанных с поиском информации о структуре базы данных Oracle. Атакующие могут выполнять SQL-запросы к системным представлениям (`DBA_TABLES`, `ALL_TABLES`, `USER_TABLES`, `DBA_OBJECTS`, `ALL_TAB_COLUMNS` и др.) с целью получения сведений о таблицах, колонках и других объектах БД. Эти данные могут быть использованы для подготовки дальнейших атак, таких как SQL-инъекции, несанкционированное чтение данных или обход механизмов контроля доступа. Детектирование данной активности основано на анализе запросов, обращающихся к системным таблицам, содержащим метаданные о структуре базы данных.	• Discovery (TA0007) • System Information Discovery (T1082)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1587	Поиск информации о конфигурации OracleDB	Данное правило направлено на обнаружение подозрительных действий, связанных с поиском информации о конфигурации базы данных Oracle. Атакующие могут выполнять SQL-запросы к системным представлениям (`V$VERSION`, `V$INSTANCE`, `PRODUCT_COMPONENT_VERSION`, `V$PARAMETER`, `V$OPTION`) с целью получения сведений о версии базы данных, установленных компонентах, параметрах конфигурации и доступных опциях. Эти данные могут быть использованы для анализа текущего состояния системы, выявления уязвимостей и подготовки дальнейших атак, таких как использование специфичных для версии уязвимостей или настройка атак с учетом доступных опций. Детектирование данной активности основано на анализе запросов, обращающихся к критически важным конфигурационным таблицам и представлениям Oracle.	• Discovery (TA0007) • System Information Discovery (T1082)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1590	Получение информации о пользователях СУБД Oracle	Данное правило направлено на обнаружение подозрительных действий, связанных с поиском информации о пользователях в базе данных Oracle. Атакующие могут выполнять SQL-запросы к системным представлениям (`DBA_USERS`, `ALL_USERS`, `USER_USERS`, `SYS.USER$`) с целью сбора данных об учетных записях, их статусе, привилегиях и ролях. Полученная информация может быть использована для дальнейших атак, таких как эскалация привилегий или подбор учетных данных. Детектирование данной активности основано на анализе запросов, обращающихся к системным таблицам, содержащим информацию о пользователях и их правах.	• Discovery (TA0007) • System Owner/User Discovery (T1033)
RV-D-1592	Манипуляция с учетными данными СУБД Oracle	Данное правило направлено на обнаружение подозрительных действий, связанных с созданием, изменением и удалением учетных записей в OracleDB. Атакующие могут использовать SQL-команды `CREATE USER`, `DROP USER`, `ALTER USER` и `GRANT DBA` для создания скрытых учетных записей, эскалации привилегий или удаления учетных записей с целью сокрытия своей активности. Эти действия могут указывать на попытку несанкционированного доступа, закрепления в системе или подготовки к дальнейшим атакам.	• Persistence (TA0003) • Account Manipulation (T1098)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1595	Экспорт базы данных Oracle	Данное правило направлено на обнаружение подозрительных действий, связанных с экспортом базы данных в СУБД Oracle. Атакующие могут использовать стандартные утилиты `Oracle exp`, `expdp` для экспорта базы данных. Эта активность может свидетельствовать о финальном этапе атаки, после которого данные могут быть зашифрованы/удалены. Детектирование данной активности основано на анализе запуска утилиты и определенных аргументов.	• Exfiltration (TA0010) • Automated Exfiltration (T1020)

Oracle MySQL

- Oracle MySQL: настройка источника
- Oracle MySQL: правила корреляции

Oracle MySQL: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Oracle MySQL в R-Vision SIEM.

Предварительные требования

- Сетевая связность между сервером СУБД (Oracle MySQL) и SIEM (или промежуточным syslog-сервером) обеспечена, а необходимые порты открыты.
- Настроена учетная запись с правами администратора для установки плагина аудита и изменения конфигурации rsyslog.

Настройка MySQL

Установка плагина для ведения журнала аудита

Для настройки аудита MySQL установите плагин для ведения журнала аудита, разработанный компанией Percona. Он поддерживает полный аудит в различных форматах, таких как XML, JSON и CSV, а также регистрирует события, связанные с аутентификацией.



Плагин поддерживается в MySQL версии 8.0 и выше.

Чтобы установить плагин аудита Percona, выполните следующие действия:

1. Скачайте архив с плагином, выполнив следующую команду:

```
wget https://downloads.percona.com/downloads/Percona-Server-8.0/Percona-Server-8.0.36-28/binary/tarball/Percona-Server-8.0.36-28-Linux.x86_64.glibc2.35.tar.gz
```

2. Распакуйте архив с плагином:

```
tar -xvf Percona-Server-8.0.36-28-Linux.x86_64.glibc2.35.tar.gz --wildcards --no-anchored '*audit_log.so*'
```

3. Получите путь к директории, в которой располагаются плагины MySQL. Для этого:

   a. Войдите в консоль MySQL:

   ```
   mysql -u root -p -h localhost
   ```

   b. Выполните следующий запрос:

   ```
   SHOW GLOBAL VARIABLES LIKE 'plugin_dir';
   ```

   ▼ *Пример вывода запроса пути к директории плагинов*

   ```
   +---------------+--------------------------+
   | Variable_name | Value                    |
   +---------------+--------------------------+
   | plugin_dir    | /usr/lib64/mysql/plugin/ |
   +---------------+--------------------------+
   1 row in set (0.00 sec)
   ```

   Здесь `/usr/lib64/mysql/plugin/` — директория плагинов.

4. Скопируйте плагин в директорию плагинов:

```
cp Percona-Server-8.0.36-28-Linux.x86_64.glibc2.35/lib/plugin/audit_log.so <plugin-dir>
```

Здесь `<plugin-dir>` — директория плагинов, полученная на шаге 3.

5. Установите плагин. Для этого:

   a. Войдите в консоль MySQL:

   ```
   mysql -u root -p -h localhost
   ```

   b. Выполните следующий запрос:

```
INSTALL PLUGIN audit_log SONAME 'audit_log.so';
```

Если плагин установлен успешно, отобразится сообщение:

```
Query OK, 0 rows affected (0.02 sec)
```

6. Добавьте настройки плагина в раздел `_[mysqld]_` в файле `my.cnf`:

```
[mysqld]
audit_log_format = JSON
audit_log_policy = ALL
audit_log_handler = SYSLOG
```

7. Перезапустите сервер MySQL:

```
systemctl restart mysqld
```

Настройка службы rsyslog

Чтобы настроить службу rsyslog, выполните следующие действия:

1. Создайте файл конфигурации rsyslog:

```
sudo nano /etc/rsyslog.d/10-siem.conf
```

2. Добавьте в созданный файл следующее правило:

```
if $syslogtag == 'mysqld' or $syslogtag == 'percona-audit' then {
   action(type="omfwd" target="<target>" port="<port>" protocol="<protocol>")
   stop
}
```

Здесь:

- `<target>` — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- `<port>` — порт точки входа Syslog на конвейере SIEM.
- `<protocol>` — сетевой протокол: `tcp` или `udp`.

3. Перезапустите rsyslog для применения изменений:

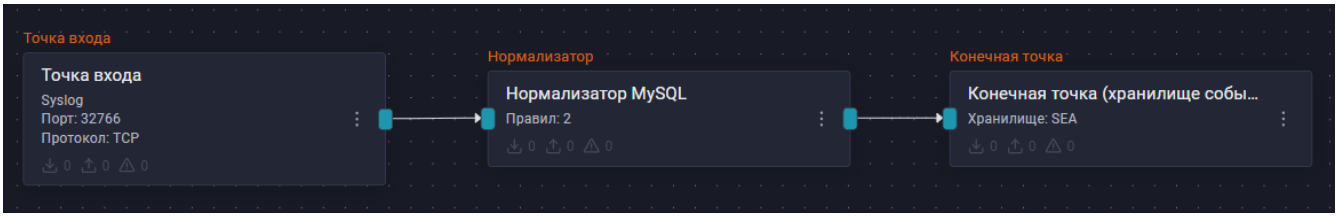
```
sudo systemctl restart rsyslog
```

Настройка в R-Vision SIEM

Для интеграции источника с R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне Oracle MySQL.
   - Протокол: выберите вариант в соответствии с настройками на стороне Oracle MySQL.
3. Добавьте на конвейер элемент **Нормализатор** с правилами **Oracle MySQL** (идентификаторы правил: **RV-N-194** и **RV-N-195**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Установите конфигурацию конвейера.

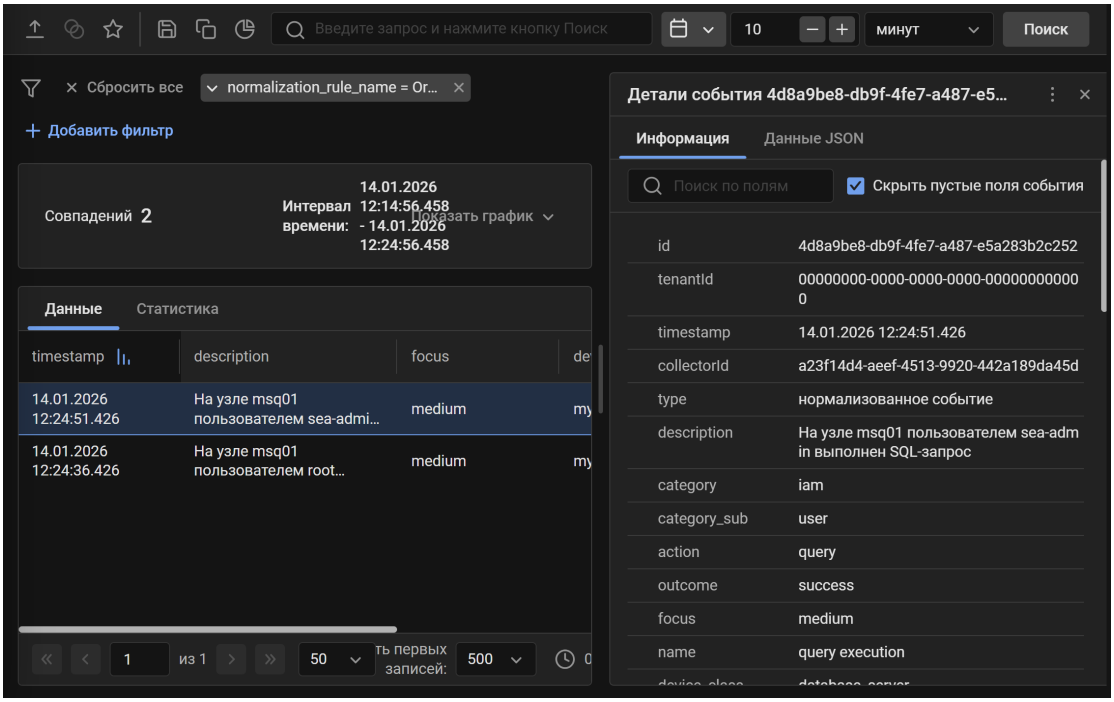
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Oracle MySQL.

Найти события Oracle MySQL в хранилище можно по следующему фильтру:

```
normalization_rule_name = "Oracle MySQL"
```



Oracle MySQL: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1453	Просмотр пользовательских данных MySQL	Атакующие могут попытаться получить несанкционированный доступ к системным таблицам, содержащим учетные записи пользователей, их привилегии и хэшированные пароли.	• Credential Access (TA0006) • Discovery (TA0007) • Collection (TA0009) • OS Credential Dumping (T1003) • Proc Filesystem (T1003.007) • Account Discovery (T1087) • Local Account (T1087.001) • Domain Account (T1087.002) • Data from Information Repositories (T1213)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1456	Получение списка подключений к MySQL	Атакующий может просмотреть, какие есть активные сессии в СУБД для последующего взаимодействия с учетными записями. В MySQL есть два способа просмотра активных сессий - встроенной командой или SQL-запросом таблиц.	• Discovery (TA0007) • System Network Connections Discovery (T1049)
RV-D-1459	Получение информации о версии MySQL	Запрос версии базы данных MySQL может быть как частью легитимных административных задач, так и частью разведки атакующего. Зная точную версию MySQL, атакующий может идентифицировать уязвимости в используемой версии и подобрать эксплойты, определить конфигурационные особенности, которые могут упростить атаку и оценить уровень обновлений и патчей сервера перед дальнейшими атаками.	• Discovery (TA0007) • Software Discovery (T1518)
RV-D-1462	Создание резервной копии MySQL	Атакующий может сохранить конфиденциальную информацию из базы данных MySQL, создав ее резервную копию или экспортировав данные в файл. Это может привести к утечке данных, если доступ к системе получен несанкционированно.	• Credential Access (TA0006) • Collection (TA0009) • OS Credential Dumping (T1003) • Data from Local System (T1005) • Data Staged (T1074) • Local Data Staging (T1074.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1463	Изменение/удаление таблицы аудита MySQL	Атакующие могут попытаться отключить\удалить или изменить систему аудита MySQL, чтобы скрыть свою активность и избежать обнаружения.	• Defense Evasion (TA0005) • Impact (TA0040) • Indicator Removal (T1070) • Clear Windows Event Logs (T1070.001) • Impair Defenses (T1562) • Disable or Modify Tools (T1562.001) • Data Manipulation (T1565) • Stored Data Manipulation (T1565.001)
RV-D-1464	Массовое удаление таблиц MySQL	Массовое удаление таблиц MySQL представляет серьезную угрозу для целостности данных и работоспособности сервисов. Подобные действия могут выполняться легитимно при очистке БД перед миграцией новых структур или удалении старой информации.	• Impact (TA0040) • Data Manipulation (T1565) • Stored Data Manipulation (T1565.001)
RV-D-1467	Удаление базы данных в MySQL	Атакующий с целью нарушения функционирования системы может попытаться удалить базу данных. Правило обнаруживает удаление базы данных в MySQL с помощью характерного запроса.	• Impact (TA0040) • Data Destruction (T1485)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1472	Назначение прав администратора MySQL	Правило детектирует создание новых пользователей с административными привилегиями или эскалацию прав у существующих пользователей. Если атакующему удастся успешно выполнить такие действия, он получит полный контроль над базами данных, что может привести к краже, модификации или уничтожению данных.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Account Manipulation (T1098)
RV-D-1473	Остановка сессии пользователя в MySQL	Атакующий может просмотреть, какие есть активные сессии в СУБД для последующего нарушения доступности БД путем блокирования доступа от учетных записей, используемых легитимными пользователями.	• Impact (TA0040) • Account Access Removal (T1531)
RV-D-1475	Изменение пароля учетной записи MySQL	Атакующий может изменить пароль учетной записи базы данных, чтобы закрепиться в системе или получить доступ к другому пользователю, например, учетной записи с максимальными привилегиями.	• Persistence (TA0003) • Privilege Escalation (TA0004) • Account Manipulation (T1098)
RV-D-1479	Атака Password Spraying на СУБД MySQL	Правило обнаруживает множественные неудачные попытки подключения к СУБД MySQL от одного хоста к множеству учетных записей.	• Credential Access (TA0006) • Brute Force (T1110) • Password Spraying (T1110.003)
RV-D-1484	Подбор пароля к СУБД MySQL	Правило обнаруживает множественные неудачные попытки подключения к СУБД MySQL от одной учетной записи, учитывая попытки с разных хостов.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)
RV-D-1487	Успешный подбор пароля к СУБД MySQL	Правило обнаруживает успешную попытку входа после множественных неудачных попыток подключения к СУБД MySQL от одной учетной записи, учитывая попытки с разных узлов.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1488	Вход привилегированного пользователя в MySQL	Атакующий может получить привилегированные учетные данные и попытаться авторизоваться с контролируемого им хоста. Правило обнаруживает попытку авторизации привилегированного пользователя с неизвестного хоста в СУБД MySQL.	• Initial Access (TA0001) • Valid Accounts (T1078) • Local Accounts (T1078.003)
RV-D-1509	Чтение журналов MySQL	Атакующие могут выполнять SQL-запросы к таблицам журналирования и представлениям, содержащим историю активности MySQL, с целью получения информации о ранее выполненных операциях, пользователях и административных действиях. Доступ к таким источникам, как general_log, slow_log, audit_log, а также представлениям performance_schema.events_statements_*, позволяет атакующему проводить разведку внутри СУБД, выявлять поведение администраторов и подготавливать дальнейшие этапы атаки.	• Discovery (TA0007) • Log Enumeration (T1654)

PostgreSQL

- PostgreSQL: настройка источника
- PostgreSQL: правила корреляции

PostgreSQL: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий СУБД PostrgeSQL в R-Vision SIEM.

Настройка PostgreSQL

В настоящем руководстве рассматривается передача событий с помощью службы rsyslog. Предполагается, что rsyslog на станции с ОС Linux уже установлен.

Настройка журналирования PostgreSQL

Для настройки аудита выберите один из подходящих вариантов: **Вариант А** (встроенный аудит PostgreSQL) или **Вариант Б** (универсальный pgaudit).

Вариант А: Настройка встроенного аудита PostgreSQL

1. В файле postgresql.conf настройте параметры безопасности и вывода:

```
log_destination = 'syslog'
logging_collector = on
log_min_messages = warning
log_min_error_statement = error
log_checkpoints = on
log_connections = on
log_disconnections = on
log_error_verbosity = verbose
log_line_prefix = '%m [%p] %u %r '

# These are relevant when logging to syslog:
syslog_facility = 'LOCAL0'
syslog_ident = 'postgres'

syslog_split_messages = off
```

Вариант Б: Настройка модуля pgaudit

Этот вариант обеспечивает детальный аудит SQL-запросов в формате CSV.

1. Установите модуль pgaudit (название модуля будет отличаться в зависимости от версии PostgreSQL и ОС):

```
yum install -y pgaudit16_14
```

2. В конфигурационном файле postgresql.conf отредактируйте параметры:

```
log_destination = 'syslog'
logging_collector = on
log_connections = on
log_disconnections = on
log_line_prefix = '%m [%p] %u %r '
log_min_messages = warning

# Подключение модуля
shared_preload_libraries = 'pgaudit'

# These are relevant when logging to syslog:
syslog_facility = 'LOCAL0'
syslog_ident = 'postgres'
```

```
syslog_split_messages = off
```

3. Перезапустите сервис PostgreSQL для примененения настроек:

```
systemctl restart postgresql-14
```

4. Только для Варианта Б (pgaudit) включите расширение в базе данных:

```
sudo -u postgres psql -c "CREATE EXTENSION pgaudit;"
sudo -u postgres psql -c "ALTER SYSTEM SET pgaudit.log = 'all';"
sudo -u postgres psql -c "SELECT pg_reload_conf();"
```

Отправка событий PostgreSQL

Чтобы настроить отправку событий PostgreSQL:

1. Создайте файл **/etc/rsyslog.d/60-postgres.conf** со следующим содержимым:

```
if $programname == 'postgres' or $syslogtag == 'postgres' then {
  action(type="omfwd" Target="<target>" Port="<port>" Protocol="<protocol>")
  stop
}
```

   Здесь:

   - `<target>` — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
   - `<port>` — порт точки входа Syslog в конвейере SIEM.
   - `<protocol>` — сетевой протокол: `tcp` или `udp`.

2. Перезапустите службу rsyslog.service с помощью команды:

```
systemctl restart rsyslog.service
```

Настройка интеграции с R-Vision SIEM

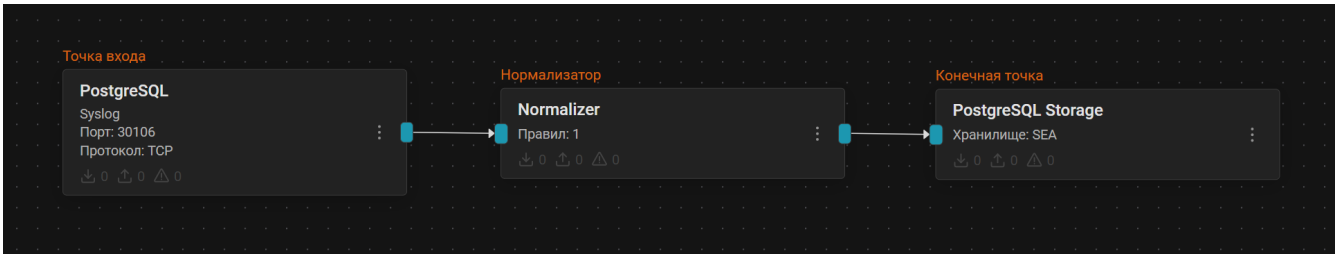
Для настройки сбора событий от источника в R-Vision SIEM выполните следующие шаги:

1. В веб-интерфейсе R-Vision SIEM перейдите в раздел **Ресурсы** → **Коллекторы** и создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - **Название**: введите произвольное, понятное название.
   - **Тип точки входа**: выберите вариант **Syslog**.
   - **Порт точки входа**: введите значение в соответствии с настройками на стороне PostgreSQL.

- **Протокол**: выберите вариант в соответствии с настройками на стороне PostgreSQL.

3. Добавьте на конвейер элемент **Нормализатор** с правилом **PostgreSQL** (идентификатор правила: **RV-N-189**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

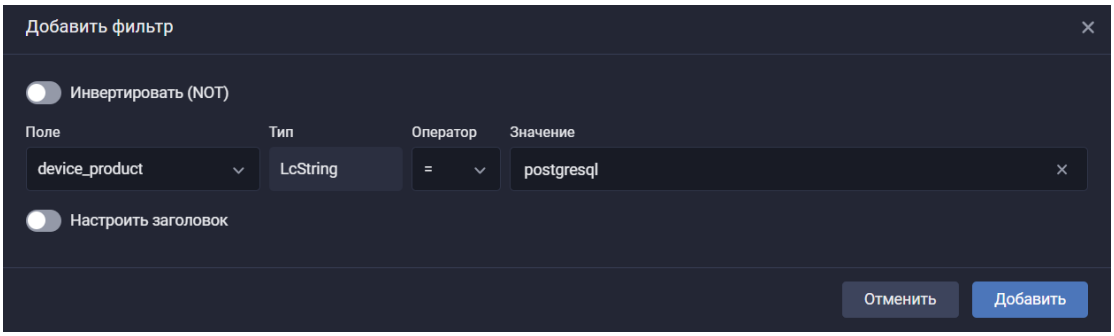
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события PostgreSQL.

Найти события PostgreSQL в хранилище можно по следующему фильтру:

```
device_product = "postgresql"
```



PostgreSQL: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1418	Атака типа Password Spraying к СУБД PostgreSQL	Правило обнаруживает множественные неудачные попытки подключения к PostgreSQL от одного хоста к множеству учетных записей.	• Credential Access (TA0006) • Brute Force (T1110) • Password Cracking (T1110.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1421	Изменение файла конфигурации базы данных PostgreSQL	Правило обнаруживает изменение файлов конфигурации `postgresql.conf` и `postgresql.auto.conf` для базы данных PostgreSQL.	• Impact (TA0040) • Data Manipulation (T1565)
RV-D-1427	Попытка удаления базы данных в PostgreSQL	Правило обнаруживает удаление базы данных в PostgreSQL с помощью характерного запроса.	• Impact (TA0040) • Data Destruction (T1485)
RV-D-1428	Получение информации о существующих учетных записях в PostgreSQL	Правило обнаруживает получение информации о существующих учетных записях и их атрибутах в PostgreSQL.	• Discovery (TA0007) • Account Discovery (T1087)
RV-D-1429	Взаимодействие с файловой системой из базы данных PostgreSQL	Правило обнаруживает взаимодействие с файловой системой из базы данных PostgreSQL с помощью характерных запросов, может говорить о попытке разведки на узле, например, для дальнейшего повышения привилегий.	• Discovery (TA0007) • File and Directory Discovery (T1083)
RV-D-1430	Новая учетная запись с правами superuser в PostgreSQL	Правило обнаруживает создание учетной записи с правами superuser или выдачу прав уже существующей учетной записи в PostgreSQL.	• Persistence (TA0003) • Create Account (T1136)
RV-D-1433	Изменение параметров аудита базы данных PostgreSQL	Правило обнаруживает изменение параметров аудита базы данных и конфигурации PostgreSQL.	• Defense Evasion (TA0005) • Impair Defenses (T1562)
RV-D-1436	Вход привилегированного пользователя с неизвестного хоста	Правило детектирует вход на СУБД Postgres привилегированного пользователя с неизвестного хоста.	• Initial Access (TA0001) • Valid Accounts (T1078) • Local Accounts (T1078.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1437	Разведка структуры базы данных PostgreSQL	Данное правило обнаруживает SQL-запросы, потенциально указывающие на попытки разведки структуры базы данных PostgreSQL — ключевого этапа подготовительной фазы атаки, направленного на сбор сведений о внутреннем устройстве системы. Правило отслеживает SQL-запросы, обращающиеся к системным каталогам и служебным схемам, таким как pg_catalog и information_schema, для получения сведений о таблицах, ролях и базах данных.	• Discovery (TA0007) • System Information Discovery (T1082)
RV-D-1438	Успешный перебор пароля к СУБД PostgreSQL	Правило обнаруживает успешную попытку входа после множественных неудачных попыток подключения к PostgreSQL от одной учетной записи, учитывая попытки с разных узлов.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)
RV-D-1440	Множественные неудачные попытки подключения к PostgreSQL	Правило обнаруживает множественные неудачные попытки подключения к PostgreSQL от одной учетной записи, учитывая попытки с разных хостов.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)
RV-D-1496	Изменен пароль от учетной записи с правами superuser в PostgreSQL	Правило обнаруживает изменение пароля от учетной записи с правами superuser в PostgreSQL.	• Persistence (TA0003) • Account Manipulation (T1098)

РЕД База Данных

- РЕД База Данных: настройка источника

РЕД База Данных: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий РЕД База Данных в R-Vision SIEM.

Предварительные требования

Перед началом настройки убедитесь, что выполнены следующие условия:

- Сетевая связность между сервером СУБД (РЕД База Данных) и SIEM (или промежуточным syslog-сервером) обеспечена, а необходимые порты открыты.
- На машине, с которой планируется сбор событий, установлен сервис rsyslog или syslog-ng.
- Создана учетная запись с правами администратора для изменения конфигурации РЕД База Данных и rsyslog.

Настройка РЕД База Данных

В настоящем руководстве рассматривается передача событий с помощью службы rsyslog.

Настройка журналирования РЕД База Данных

Для настройки источника выполните следующие действия:

1. В конфигурационном файле раскомментируйте следующую строку:

```
    AuditTraceConfigFiles = fbtrace.conf;
```

2. В конфигурационном файле `fbtrace.conf` найдите и отредактируйте параметры:

```
database
{
        enabled = true
        format = system
        include_filter =
"%(SELECT|INSERT|UPDATE|DELETE|DROP|ALTER|CREATE|GRANT|REVOKE)%"
        log_connections = true
        log_transactions = true
        log_statement_finish = true
        log_errors = true
        log_warnings = true
        print_hostname = true
}
```

3. Перезапустите сервис базы данных командой:

```
systemctl restart firebird
```

Отправка событий РЕД База Данных

Чтобы настроить отправку событий РЕД База Данных:

1. Создайте файл `/etc/rsyslog.d/10-reddb.conf` со следующим содержимым:

```
if $programname == 'RedDatabase' or $syslogtag == 'RedDatabase' then {
  action(type="omfwd" Target="<target>" Port="<port>" Protocol="<protocol>")
  stop
```

```
}
```

Здесь:

- `<target>` — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- `<port>` — порт точки входа Syslog в конвейере SIEM.
- `<protocol>` — сетевой протокол: `tcp` или `udp`.

2. Перезапустите службу rsyslog.service с помощью команды:

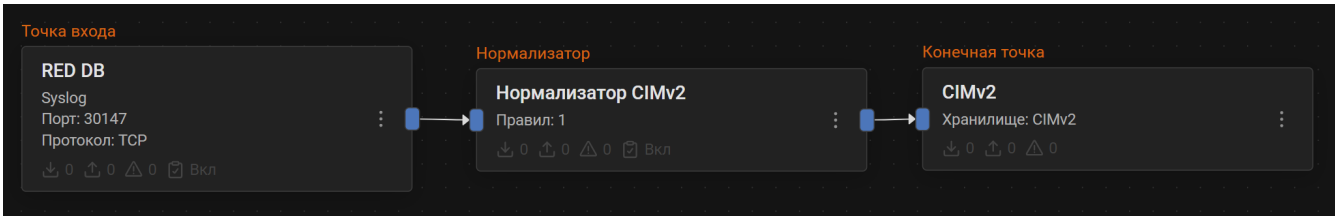
```
systemctl restart rsyslog.service
```

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне РЕД База Данных.
   - Протокол: выберите вариант в соответствии с настройками на стороне РЕД База Данных.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **RED SOFT RED Database** (идентификатор правила: **RV-N-318**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

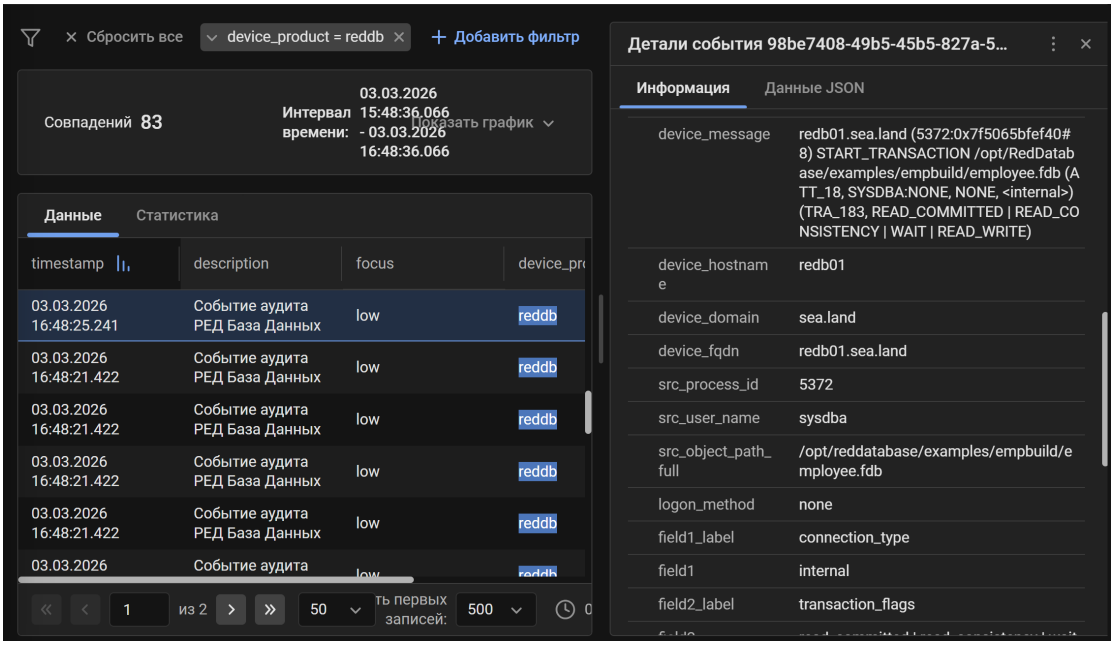
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события РЕД База Данных.

Найти события РЕД База Данных в хранилище можно по следующему фильтру:

```
device_product = "reddb"
```



СберТех Platform V Pangolin DB

- СберТех Platform V Pangolin DB: настройка источника

СберТех Platform V Pangolin DB: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Platform V Pangolin DB в R-Vision SIEM.

Настройка СберТех Platform V Pangolin DB

В настоящем руководстве рассматривается передача событий с помощью службы rsyslog. Предполагается, что rsyslog на станции с ОС Linux уже установлен.

Настройка журналирования

Для настройки аудита выберите один из подходящих вариантов: **Вариант А** (встроенный аудит СберТех Platform V Pangolin DB) или **Вариант Б** (универсальный pgaudit).

Вариант А: Настройка встроенного аудита СберТех Platform V Pangolin DB

Чтобы настроить встроенный аудит СберТех Platform V Pangolin DB, в файле `postgresql.conf` настройте параметры безопасности и вывода:

```
log_destination = 'syslog'
logging_collector = on
log_min_messages = warning
log_min_error_statement = error
log_checkpoints = on
```

```
log_connections = on
log_disconnections = on
log_error_verbosity = verbose
log_line_prefix = '%m %p %u %r '
log_statement = 'all'

syslog_facility = 'LOCAL0'
syslog_ident = 'postgres'

syslog_split_messages = off
```

Вариант Б: Настройка модуля pgaudit

Этот вариант обеспечивает детальный аудит SQL-запросов в формате CSV.

В конфигурационном файле `postgresql.conf` отредактируйте параметры:

```
log_destination = 'syslog'
log_connections = on
log_disconnections = on
log_line_prefix = '%m %p %u %r '
log_min_messages = warning
log_statement = 'NONE'

syslog_facility = 'LOCAL0'
syslog_ident = 'pangolin'

syslog_split_messages = off

# Подключение модуля.
shared_preload_libraries = 'pgaudit'

pgaudit.log = 'all'
pgaudit.log_catalog = on
pgaudit.log_parameter = on
pgaudit.log_relation = on
```

Затем перезапустите сервис СберТех Platform V Pangolin DB для примененения настроек (путь может отличаться):

```
/opt/pangolin-dbms-server-7/bin/pg_ctl -D /var/lib/pangolin/data7 restart
```

Отправка событий

Чтобы настроить отправку событий СберТех Platform V Pangolin DB:

1. Создайте файл `/etc/rsyslog.d/60-pangolin.conf` со следующим содержимым:

```
if $programname == 'pangolin' or $syslogtag == 'pangolin' then {
  action(type="omfwd" Target="<target>" Port="<port>" Protocol="<protocol>")
  stop
}
```

Здесь:

- `<target>` — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- `<port>` — порт точки входа Syslog в конвейере SIEM.
- `<protocol>` — сетевой протокол: `tcp` или `udp`.

2. Перезапустите службу `rsyslog.service` с помощью команды:

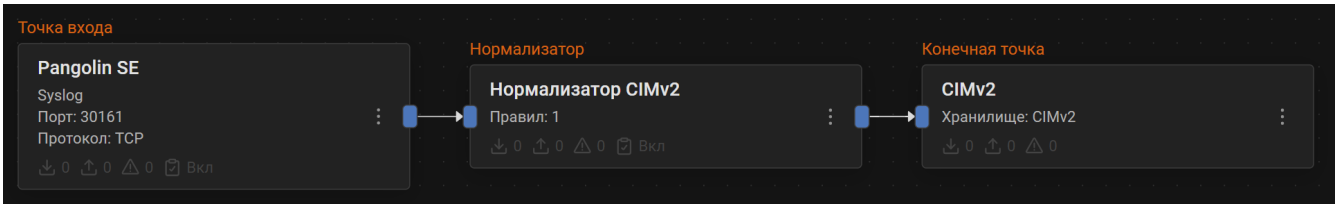
```
systemctl restart rsyslog.service
```

Настройка интеграции с R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В веб-интерфейсе R-Vision SIEM перейдите в раздел **Ресурсы** → **Коллекторы** и создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - **Название**: введите произвольное, понятное название.
   - **Тип точки входа**: выберите вариант **Syslog**.
   - **Порт точки входа**: введите значение в соответствии с настройками на стороне СберТех Platform V Pangolin DB.
   - **Протокол**: выберите вариант в соответствии с настройками на стороне СберТех Platform V Pangolin DB.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **SberTech Pangolin SE** (идентификатор правила: **RV-N-350**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

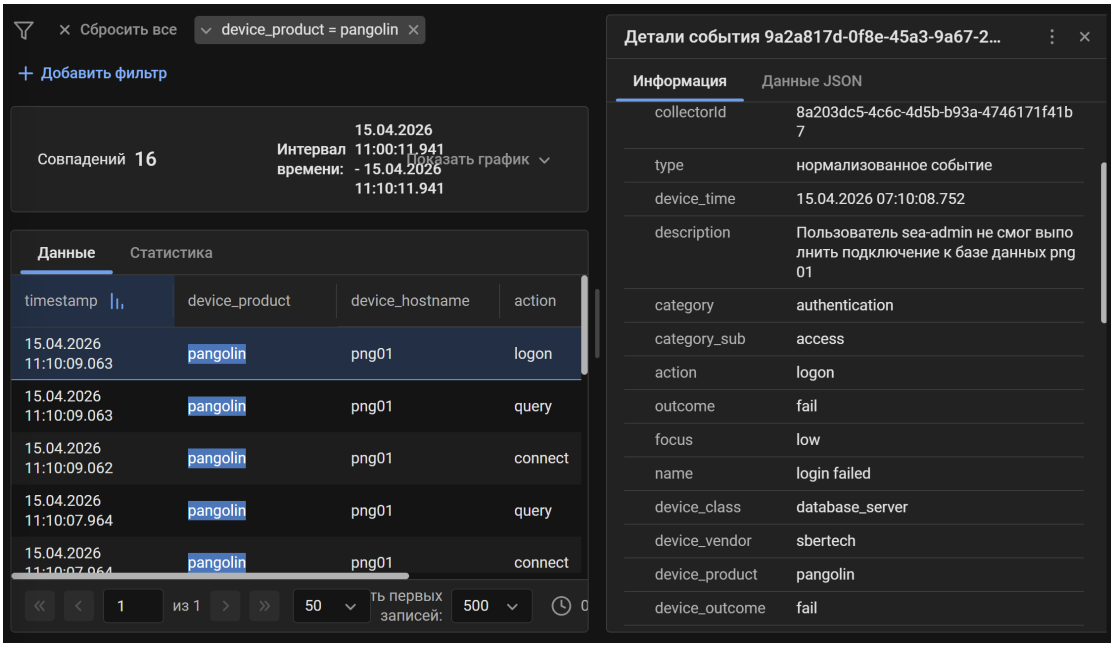
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события СберТех Platform V Pangolin DB.

Найти события СберТех Platform V Pangolin DB в хранилище можно по следующему фильтру:

```
device_product = "pangolin"
```



Системы управления инцидентами ИБ

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых систем управления инцидентами ИБ:

- R-Vision SOAR

R-Vision SOAR

- R-Vision SOAR: настройка источника

R-Vision SOAR: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий R-Vision SOAR в R-Vision SIEM.

Предварительные требования

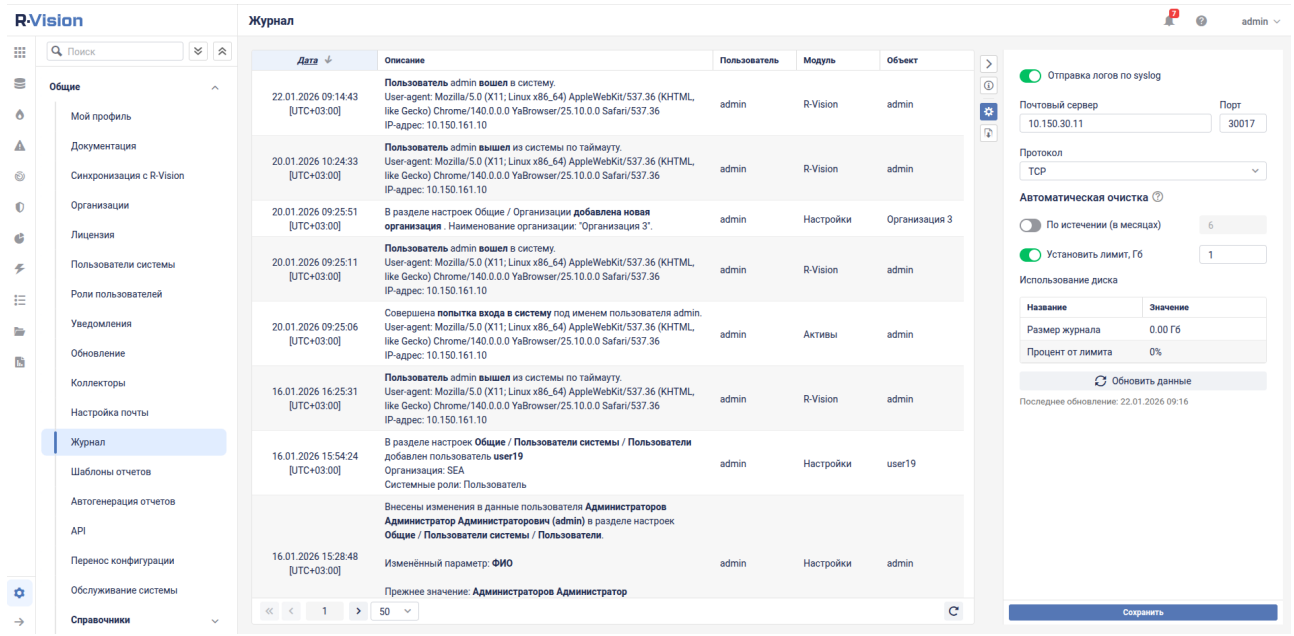
Сетевая доступность узлов кластера SIEM по целевому порту и протоколу для источника или сетевая доступность централизованного Syslog-сервера.

Настройка R-Vision SOAR

Настройка отправки событий в R-Vision SIEM

Чтобы настроить отправку событий R-Vision SOAR в R-Vision SIEM, выполните следующие шаги:

1. Войдите в веб-интерфейс R-Vision SOAR под учетной записью администратора.
2. Перейдите в раздел **Настройки системы** → **Общие** → **Журнал**.
3. В карточке журнала перейдите на вкладку **Настройки**.
4. Установите переключатель **Отправка логов по syslog** в активное положение.
5. Введите IP-адрес сервера rsyslog.
6. Введите значение порта сервера rsyslog.
7. Выберите из выпадающего списка протокол **TCP**.
8. Сохраните изменения.

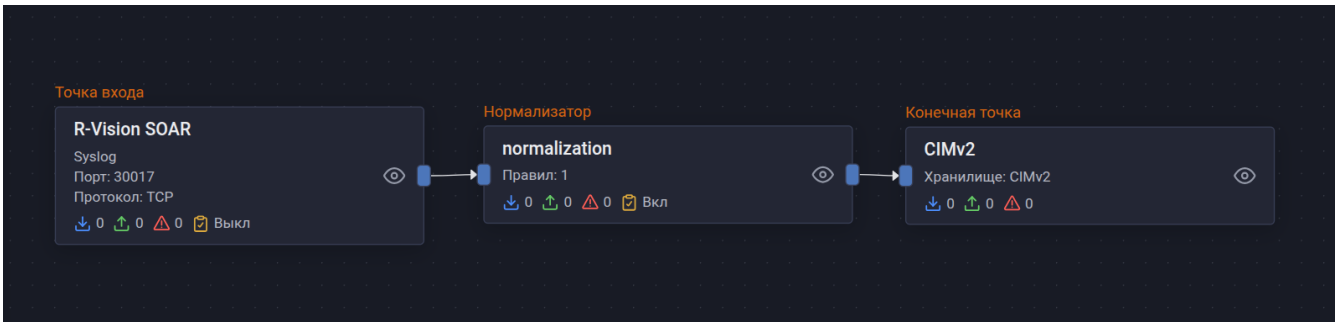


Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне R-Vision SOAR.
   - Протокол: выберите из выпадающего списка вариант **TCP**.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **R-Vision SOAR** (идентификатор правила: **RV-N-292**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:

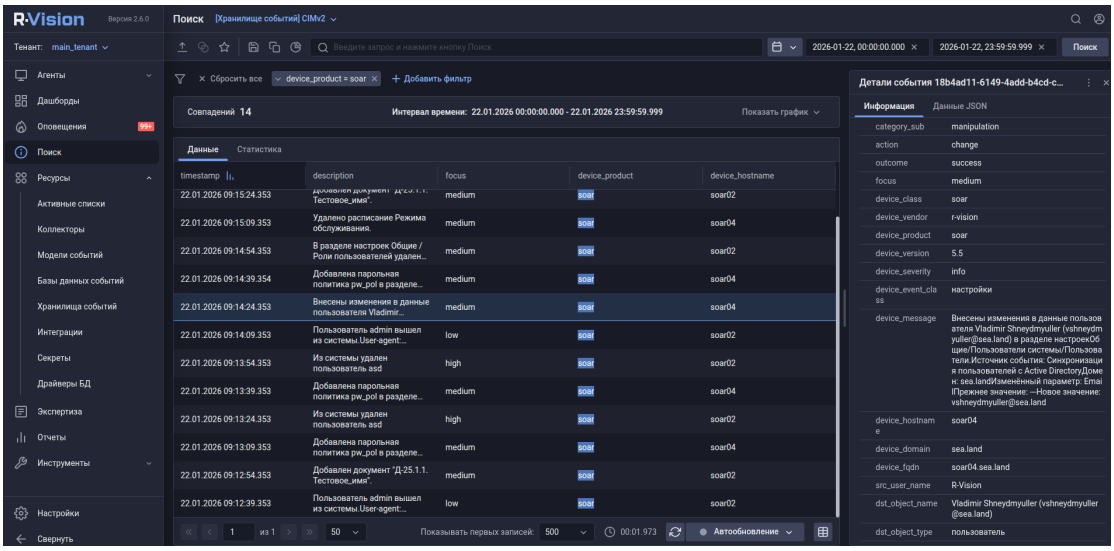


После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут

поступать события R-Vision SOAR.

Найти события R-Vision SOAR в хранилище можно по следующему фильтру:

```
device_product = "soar"
```



Системы управления ложными сетевыми объектами

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых систем управления ложными сетевыми объектами:

- R-Vision TDP
- Xello Deception

R-Vision TDP

- R-Vision TDP: настройка источника

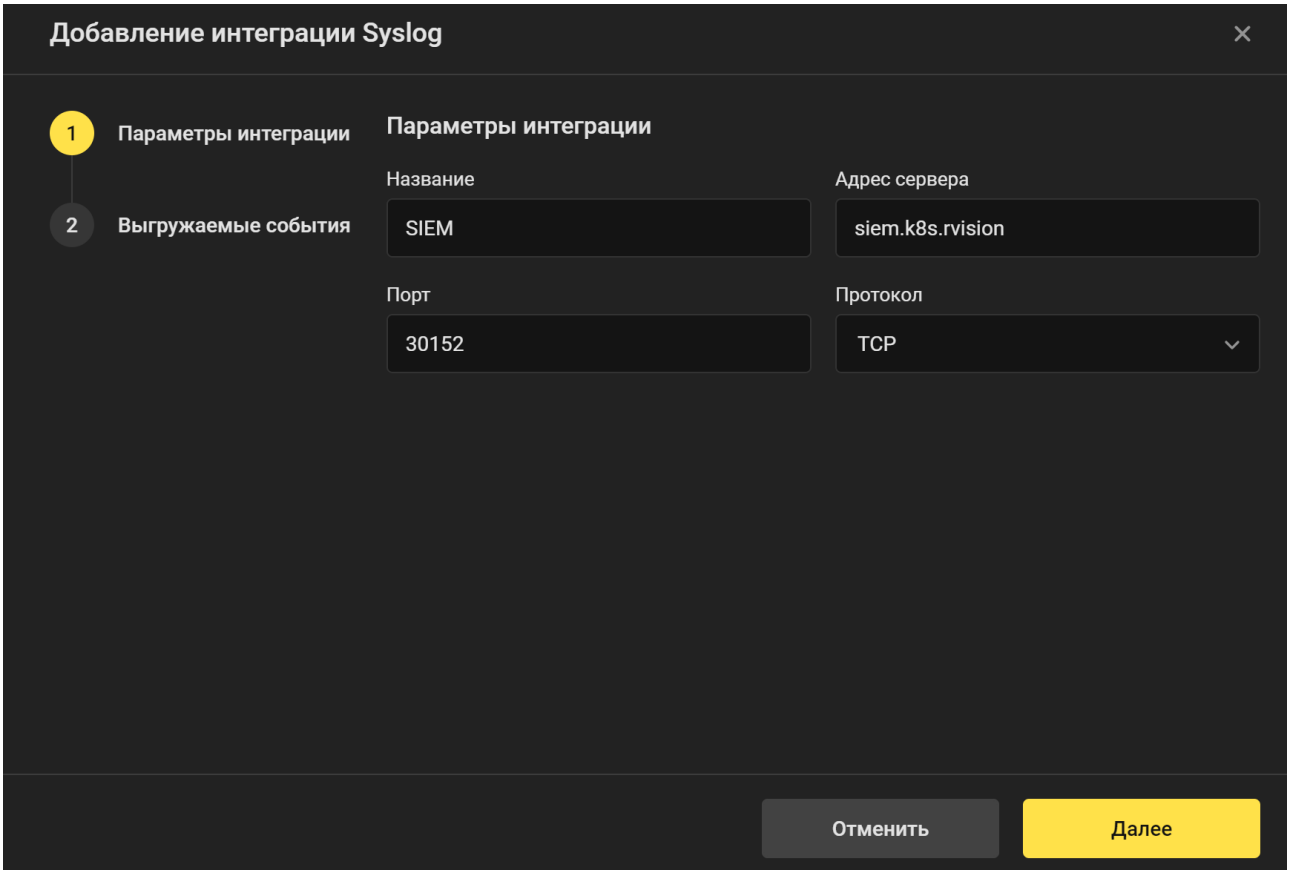
R-Vision TDP: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий R-Vision Threat Deception Platform (R-Vision TDP) в R-Vision SIEM.

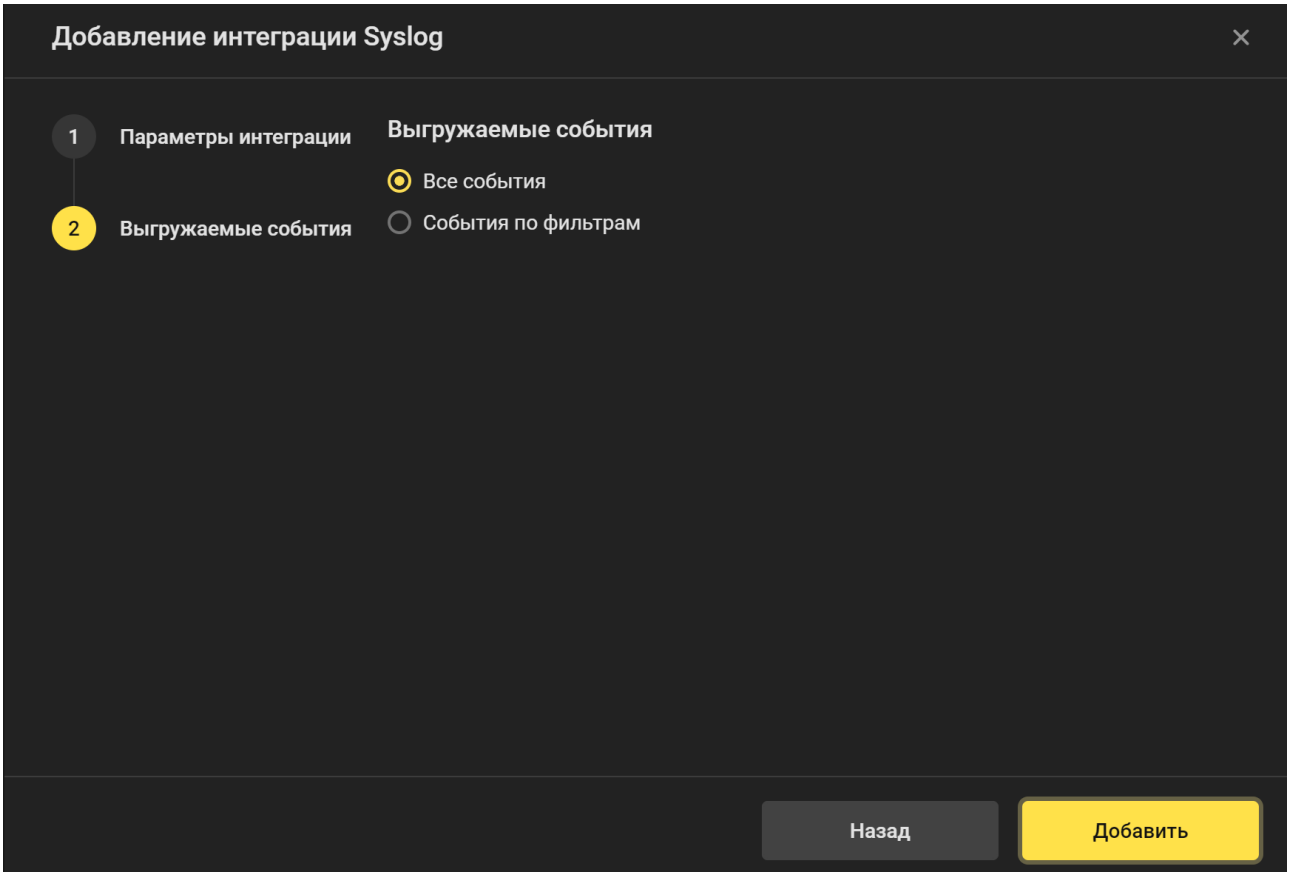
Настройка R-Vision TDP

Для настройки отправки событий выполните следующие действия:

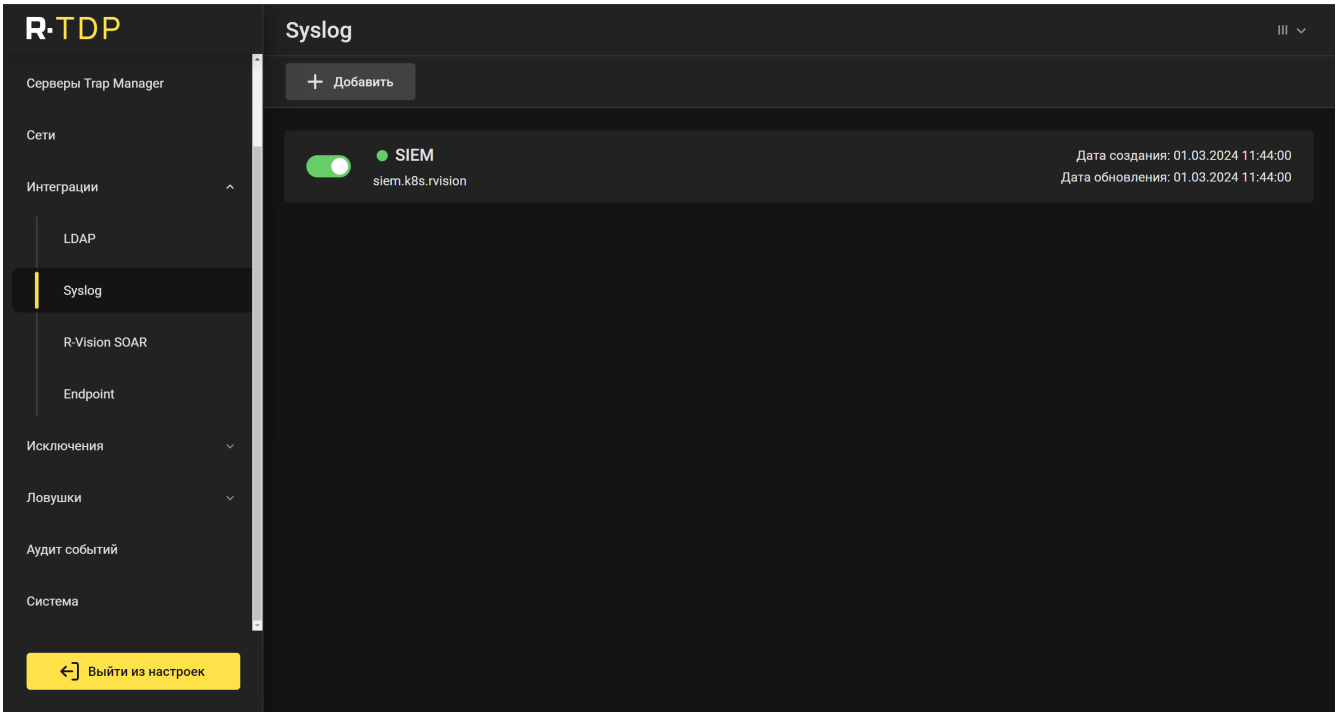
1. Войдите в веб-интерфейс R-Vision TDP.
2. Перейдите в раздел **Настройки** → **Интеграции** → **Syslog**.
3. В открывшейся вкладке нажмите на кнопку **Добавить** (+).
4. В текущем окне заполните параметры интеграции:
   - **Название** — название системы.
   - **Адрес сервера** — IP-адрес или FQDN узла кластера R-Vision SIEM.
   - **Порт** — порт Syslog-сервера.
   - **Протокол** — сетевой протокол (**TCP** или **UDP**).
5. Нажмите на кнопку **Далее**.



6. Выберите типы событий для отправки.
7. Нажмите на кнопку **Добавить**.



Если настройка на стороне R-Vision TDP проведена корректно, в разделе **Интеграции** → **Syslog** отобразится добавленная вами интеграция.

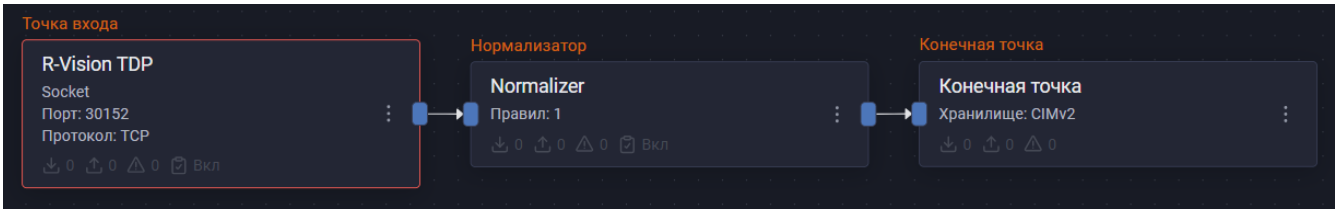


Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Socket**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне R-Vision TDP.
   - Протокол: выберите вариант в соответствии с настройками на стороне R-Vision TDP.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **R-Vision TDP** (идентификатор правила: **RV-N-287**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

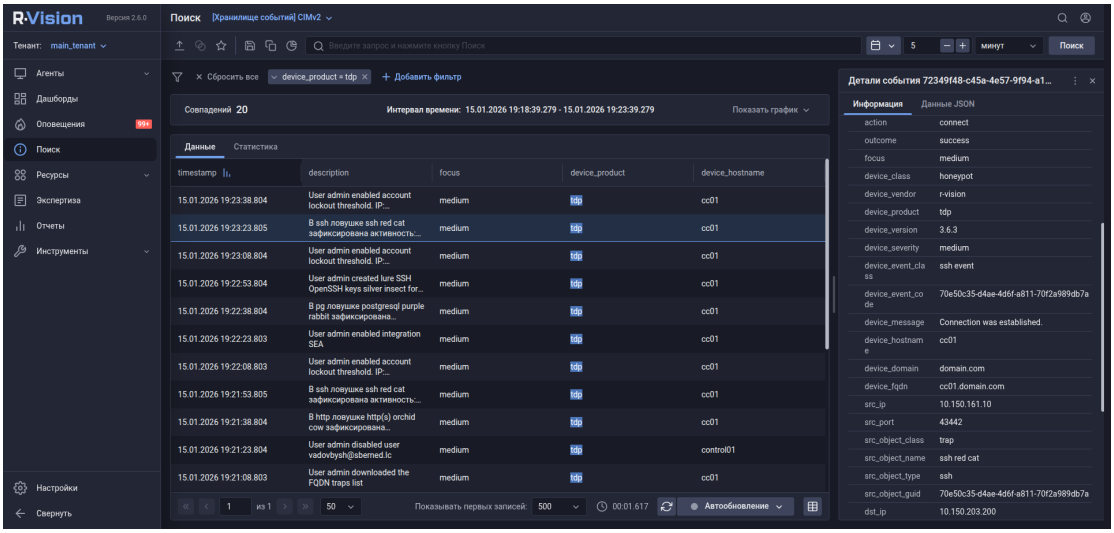
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события R-Vision TDP.

Найти события R-Vision TDP в хранилище можно по следующему фильтру:

```
device_product = "tdp"
```



Xello Deception

- Xello Deception: настройка источника

Xello Deception: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Xello Deception в R-Vision SIEM.

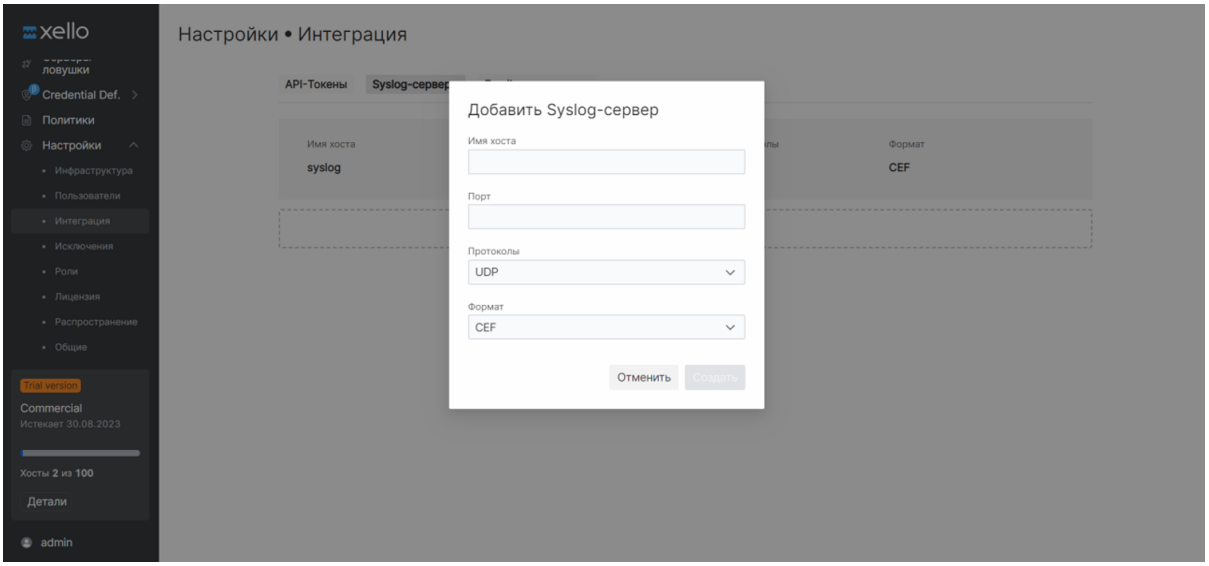
Предварительные требования

Необходима сетевая доступность между Xello Deception и коллектором R-Vision SIEM.

Настройка Xello Deception

Для настройки отправки событий выполните следующие действия:

1. Перейдите по следующему пути: **Настройки** → **Интеграция** → **Syslog-серверы**.
2. Добавьте syslog-сервер со следующими данными:
   - **Имя хоста**: укажите FQDN или IP-адрес коллектора.
   - **Порт**: укажите порт, который слушает коллектор для приема событий.
   - **Протоколы**: укажите протокол, настроенный на коллекторе (`TCP` или `UDP`).
   - **Формат**: `CEF`.
3. Нажмите кнопку **Создать**.



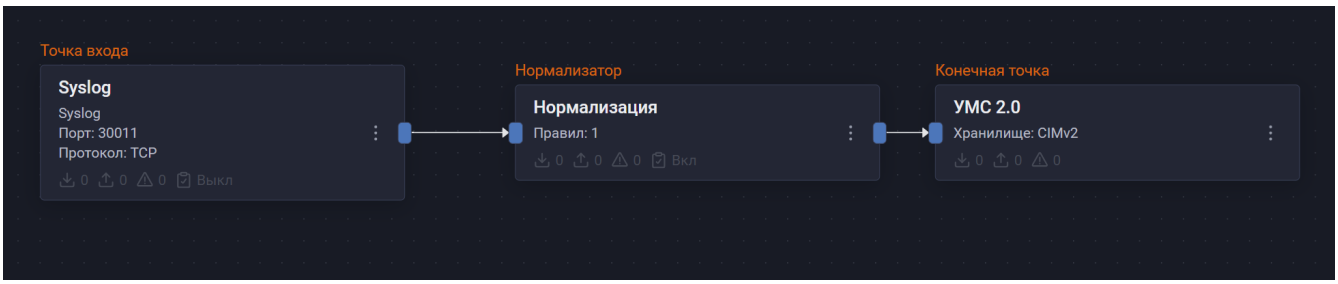
Настройка Xello Deception завершена.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне Xello Deception.
   - Протокол: выберите вариант в соответствии с настройками на стороне Xello Deception.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Xello Deception** (идентификатор правила: **RV-N-316**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

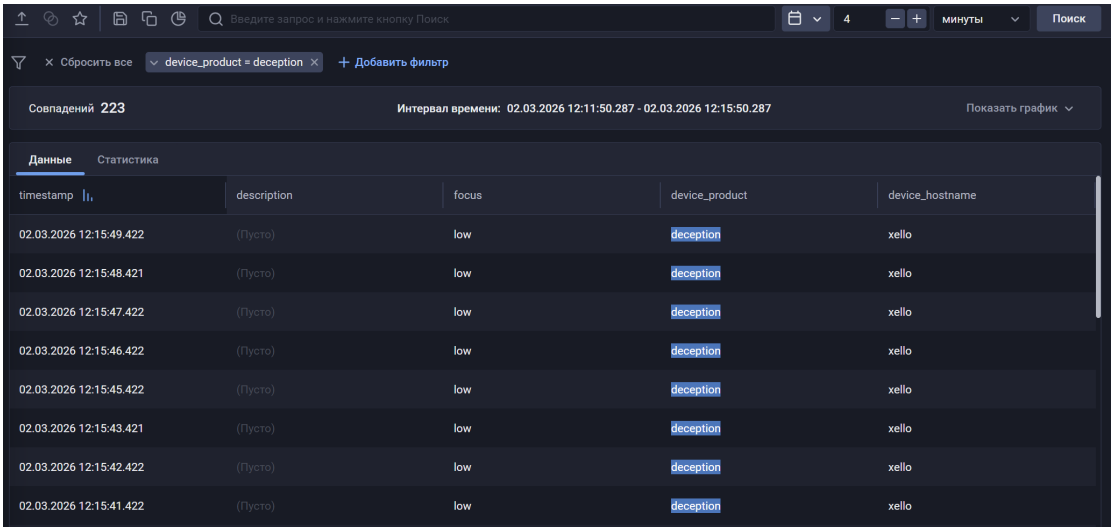
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Xello Deception.

Найти события Xello Deception в хранилище можно по следующему фильтру:

```
device_product = "deception"
```



Системы управления серверной инфраструктурой

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых систем управления серверной инфраструктурой:

- Red Hat Ansible AWX
- Red Hat Ansible Tower
- Microsoft SCOM

Red Hat Ansible AWX

- Ansible AWX: настройка источника

Ansible AWX: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Ansible AWX в R-Vision SIEM.

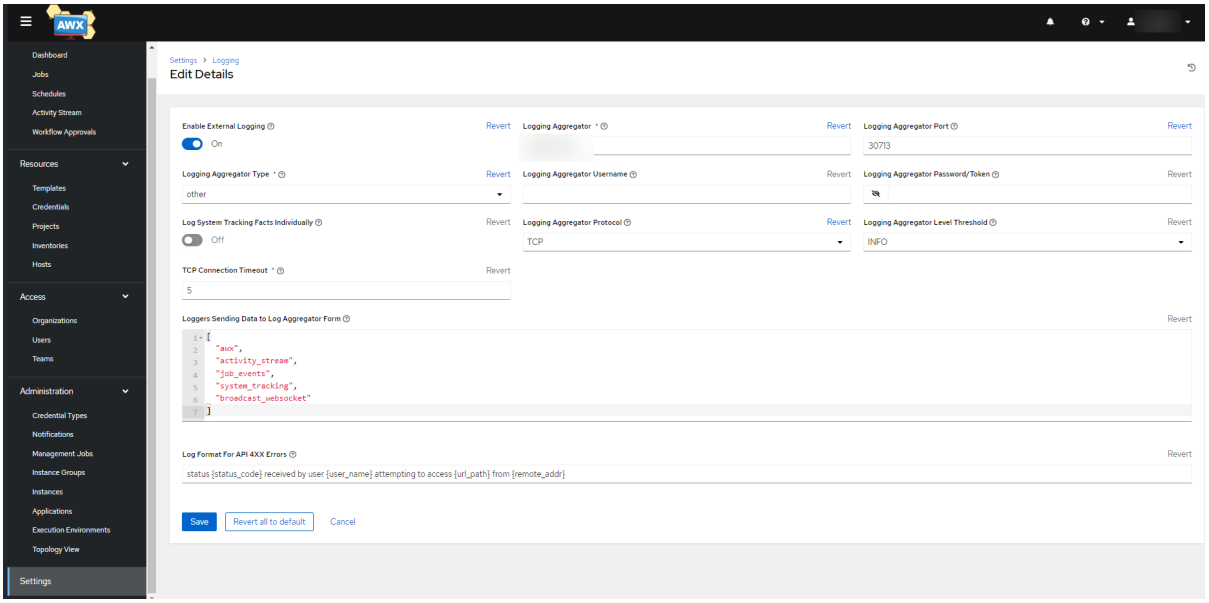
Предварительные требования

- Сетевая доступность нод кластера SIEM по целевому порту и протоколу для источника.

Настройка Ansible AWX

Чтобы настроить Ansible AWX, выполните следующие шаги:

1. Войдите в веб-интерфейс **Ansible AWX**.
2. Перейдите в раздел **Settings** → **Logging** → **Edit Details**.
3. Задайте следующие параметры:
   - **Enable External Logging**: переведите переключатель в активное положение.
   - **Logging Aggregator Type**: выберите из выпадающего списка вариант `Other`.
   - **Logging Aggregator**: введите IP-адрес коллектора SIEM.
   - **Logging Aggregator Protocol**: выберите из выпадающего списка вариант `TCP` или `UDP`.
   - **Logging Aggregator Port**: введите порт точки входа типа `Syslog`.
4. Остальные параметры оставьте без изменений.
5. Сохраните настройки, нажав на кнопку **Save**.



Настройка в R-Vision SIEM

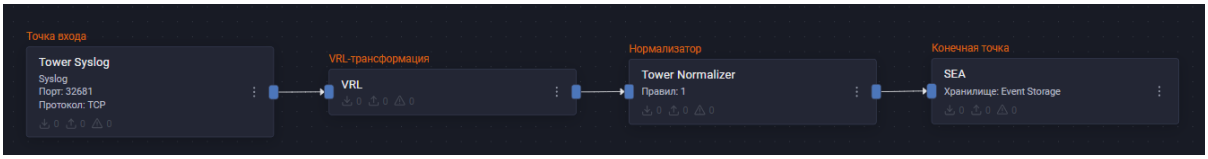
Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне Ansible AWX.
   - Протокол: выберите вариант в соответствии с настройками на стороне Ansible AWX.
3. Добавьте элемент **VRL-трансформация** со следующим кодом:

```
.device_product = "awx"
```

4. Соедините добавленную точку входа и VRL-трансформацию.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **Ansible AWX** (идентификатор правила: **RV-N-320**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

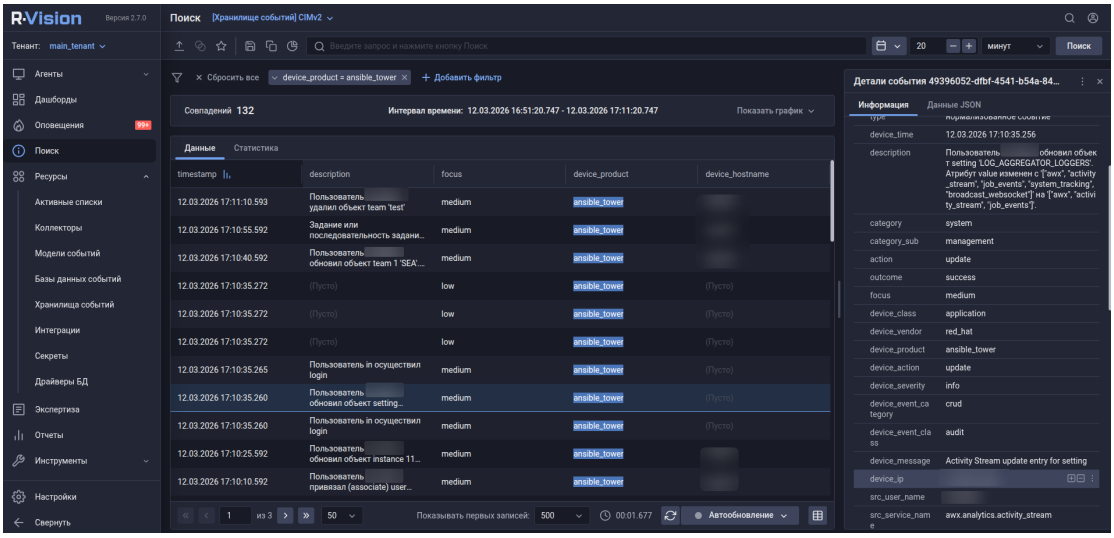
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Ansible AWX.

Найти события Ansible AWX в хранилище можно по следующему фильтру:

```
device_product = "awx"
```



Red Hat Ansible Tower

- Red Hat Ansible Automation Platform (Automation Controller): настройка источника

Red Hat Ansible Automation Platform (Automation Controller): настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий Ansible Automation Platform (Automation Controller) в R-Vision SIEM. Ранее компонент Automation Controller был отдельным продуктом и назывался Ansible Tower, поэтому всё описанное в инструкции также применимо для Ansible Tower.

Предварительные требования

- Сетевая доступность нод кластера SIEM по целевому порту и протоколу для источника.

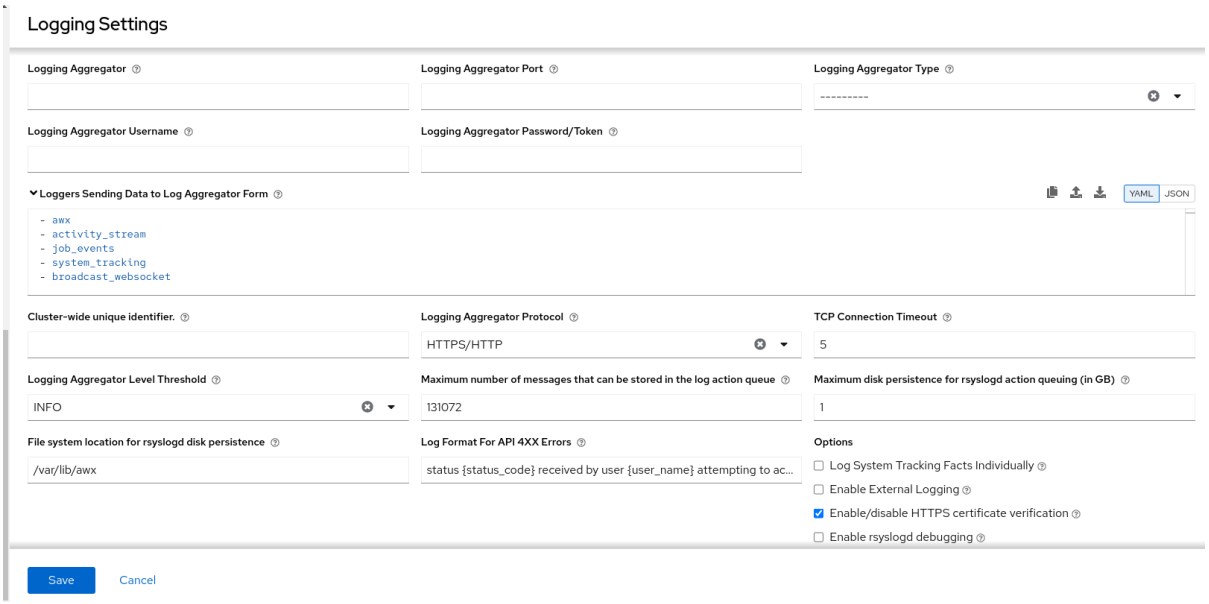
Настройка Ansible Automation Platform (Automation Controller)

Чтобы настроить Ansible Automation Platform (Automation Controller), выполните следующие шаги:

1. Войдите в веб-интерфейс **Ansible Automation Platform (Automation Controller)**.
2. Перейдите в раздел **Settings** → **Automation Execution** → **Logging** → **Edit**.
3. Задайте следующие параметры:
   - **Enable External Logging**: переведите переключатель в активное положение.
   - **Logging Aggregator Type**: выберите из выпадающего списка вариант `Other`.

- **Logging Aggregator**: введите IP-адрес коллектора R-Vision SIEM.
- **Logging Aggregator Protocol**: выберите из выпадающего списка вариант `TCP` или `UDP`.
- **Logging Aggregator Port**: введите порт точки входа типа `Syslog`.

4. Остальные параметры оставьте без изменений.
5. Сохраните настройки, нажав на кнопку **Save**.



Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

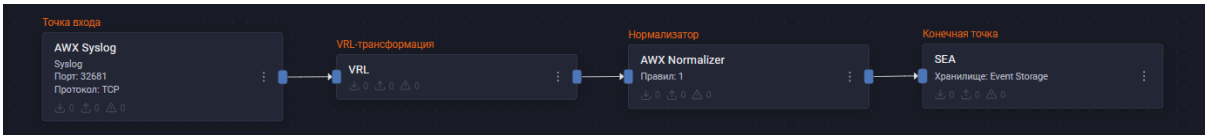
1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне Ansible Automation Platform (Automation Controller).
   - Протокол: выберите вариант в соответствии с настройками на стороне Ansible Automation Platform (Automation Controller).
3. Добавьте на конвейер элемент **VRL-трансформация** со следующим кодом:

```
.device_product = "awx"
```

4. Соедините добавленную точку входа и VRL-трансформацию.
5. Добавьте на конвейер элемент **Нормализатор** с правилом **Ansible AWX** (идентификатор правила: **RV-N-320**).
6. Соедините нормализатор с VRL-трансформацией.
7. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.

8. Соедините конечную точку с нормализатором.
9. Сохраните и установите конфигурацию конвейера.

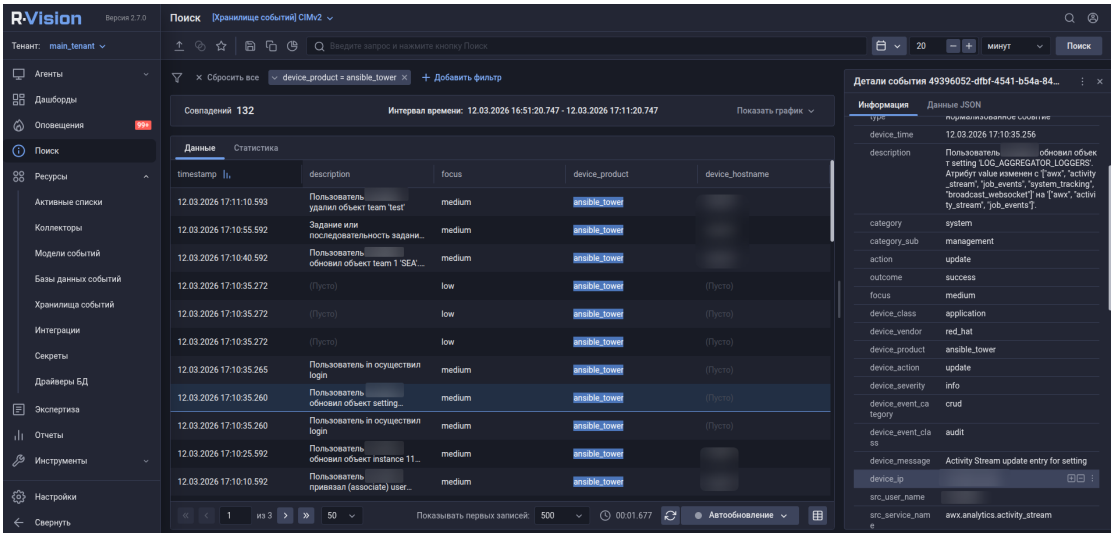
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Ansible Automation Platform (Automation Controller).

Найти события Ansible Automation Platform (Automation Controller) в хранилище можно по следующему фильтру:

```
device_product = "awx"
```



Microsoft SCOM

- Microsoft System Center Operations Manager: настройка источника

Microsoft System Center Operations Manager: настройка источника

Данное руководство описывает процесс настройки сбора событий Microsoft SCOM и их отправки в R-Vision SIEM.

Предварительные требования

Перед настройкой пересылки событий в R-Vision SIEM убедитесь в выполнении следующих условий:

- Сетевая доступность сервера СУБД источника по целевому порту и протоколу для каждой ноды кластера R-Vision SIEM.
- Учетная запись в СУБД с правами на чтение базы данных `OperationsManager`.

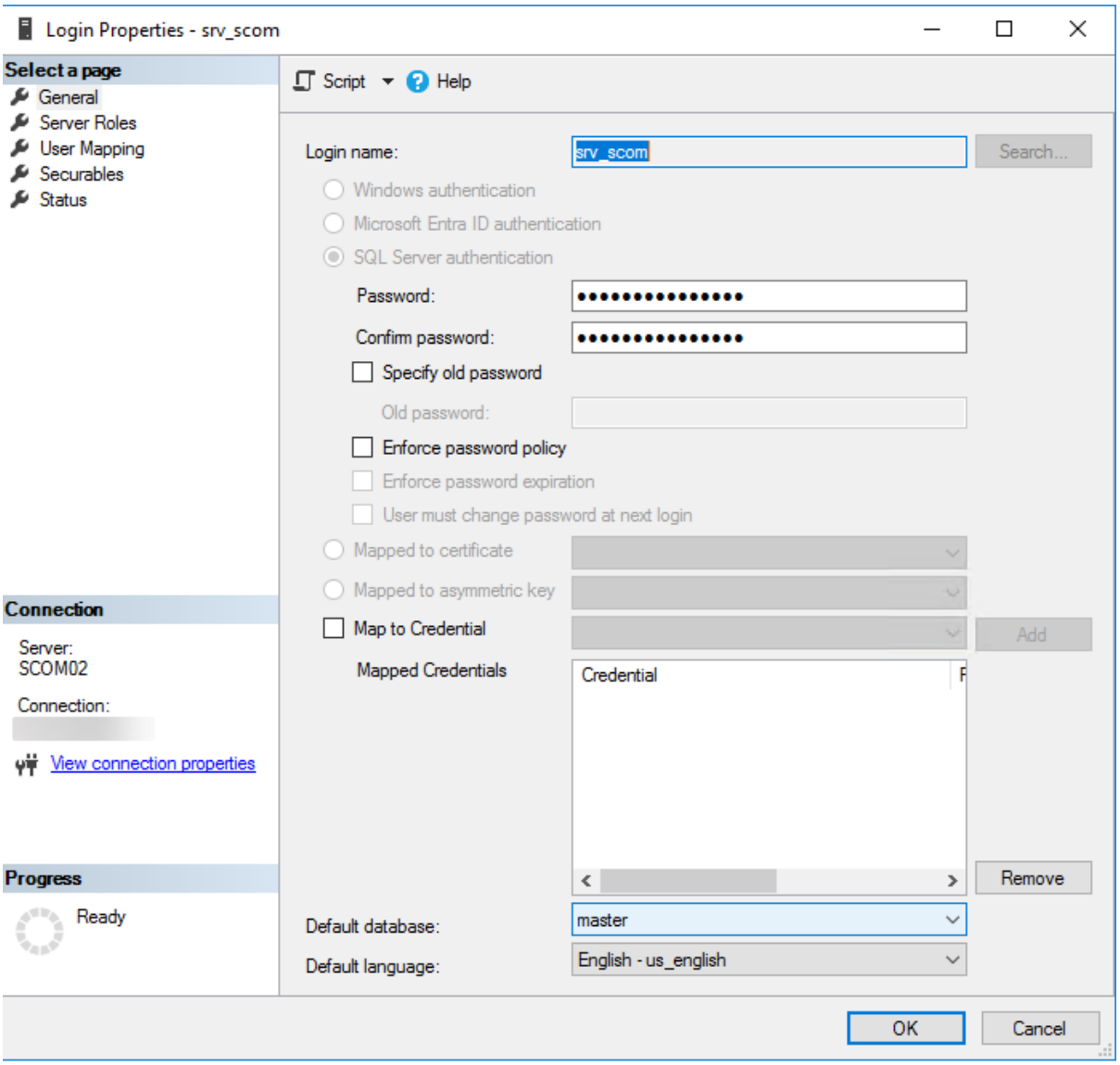
Настройка СУБД MS SQL

События Microsoft SCOM записываются в представление `RV_SCOM_ALERTS` базы данных `OperationsManager` СУБД MS SQL. Для настройки сбора логов из базы данных необходимо к ней подключиться. Используйте для подключения специально созданную сервисную учетную запись (далее — УЗ).

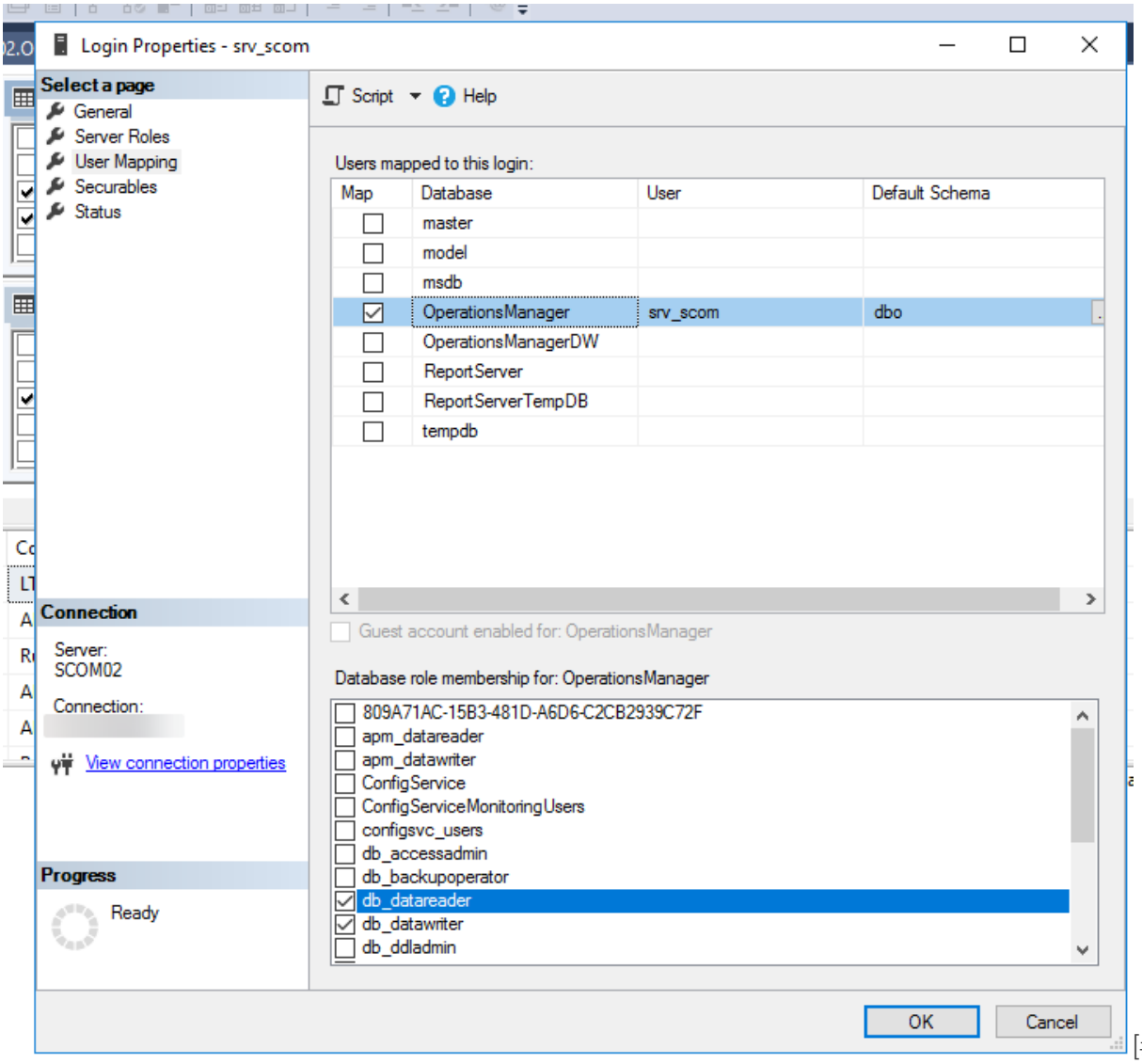
Создание учетной записи в СУБД MS SQL

Чтобы создать сервисную УЗ, подключитесь к СУБД с правами администратора. Для этого выполните следующие действия в SQL Server Management Studio:

1. Выберите **New Login** в контекстном меню для **Security/Logins**.
2. Создайте сервисную учетную запись.



3. Предоставьте учетной записи права на чтение базы `OperationsManager`.

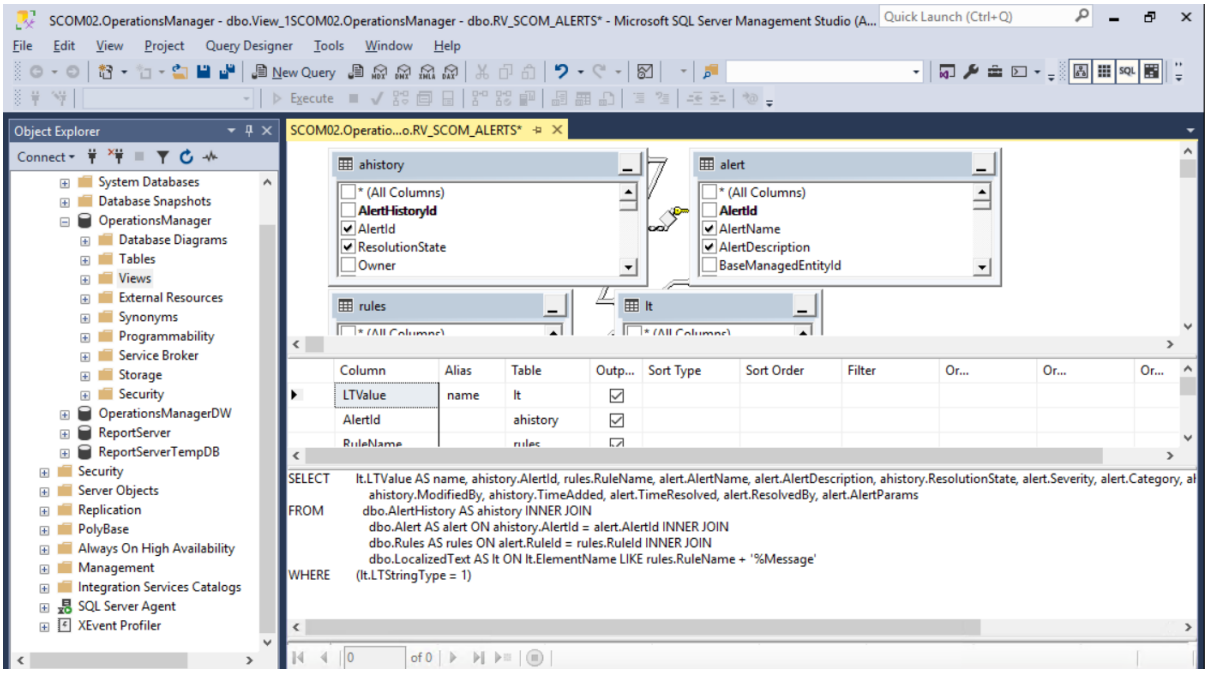


[#create-view] === Создание представления в СУБД MS SQL

Создайте представление с названием `RV_SCOM_ALERTS`. Для этого:

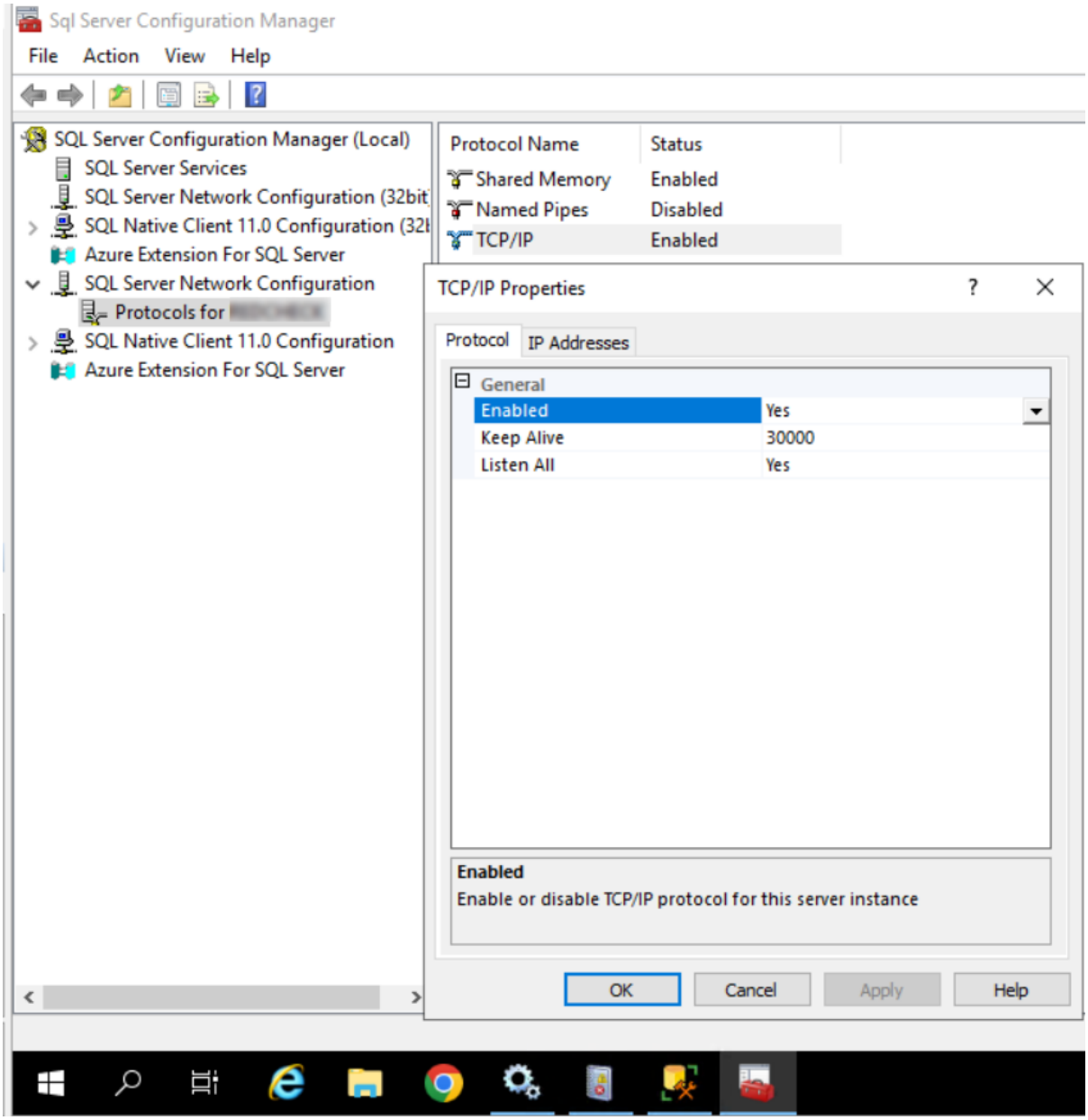
1. Выберите **New View…** в контекстном меню для **OperationsManager/Views**.
2. В окне создания нового представления в строке запроса вставьте следующий SQL-запрос:

```
SELECT          lt.LTValue AS name, ahistory.AlertId, rules.RuleName,
alert.AlertName, alert.AlertDescription, ahistory.ResolutionState,alert.Severity,
alert.Category, ahistory.Comments, ahistory.TimeModified, ahistory.ModifiedBy,
ahistory.TimeAdded, alert.TimeResolved, alert.ResolvedBy, alert.AlertParams
FROM            dbo.AlertHistory AS ahistory INNER JOIN
                         dbo.Alert AS alert ON ahistory.AlertId = alert.AlertId
INNER JOIN
                         dbo.Rules AS rules ON alert.RuleId = rules.RuleId INNER
JOIN
                         dbo.LocalizedText AS lt ON lt.ElementName LIKE
rules.RuleName + '%Message'
WHERE            lt.LTStringType = 1
```



Настройка сервера MS SQL

В настройках SQL Server Configuration Manager убедитесь, что протокол `TCP/IP` включен в конфигурации сети SQL Server.



Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте секрет со строкой подключения. Для этого:
   a. Перейдите в раздел **Ресурсы** → **Секреты**.
   b. Нажмите на кнопку **Создать** (＋).
   c. В раскрывшемся окне создания секрета заполните поля:
      - **Название**: введите название секрета.
      - **Описание** (опционально): опишите, для чего будет использоваться секрет.
      - **Тип секрета**: выберите вариант **Строка подключения**.
      - **Строка подключения**: введите строку вида:

```
jdbc:sqlserver://<DB_SERVER>\<DB_INSTANCE>:<DB_PORT>;encrypt=false;databaseN
```

```
ame=OperationsManager;user=<DB_USER>;password=<DB_PASSWORD>
```

- <DB_SERVER>: IP-адрес инстанса СУБД.
- <DB_INSTANCE>: название инстанса СУБД.
- <DB_PORT>: порт инстанса СУБД (для MS SQL стандартный порт 1433).
- <DB_USER>: системный аккаунт с правами на чтение.
- <DB_PASSWORD>: пароль системного аккаунта.

d. Нажмите на кнопку **Создать**.

2. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
3. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Database**.
   - Драйвер базы данных: выберите вариант **MS SQL**.
   - Адрес подключения: выберите секрет, созданный ранее.
   - SQL-запрос: введите запрос вида:

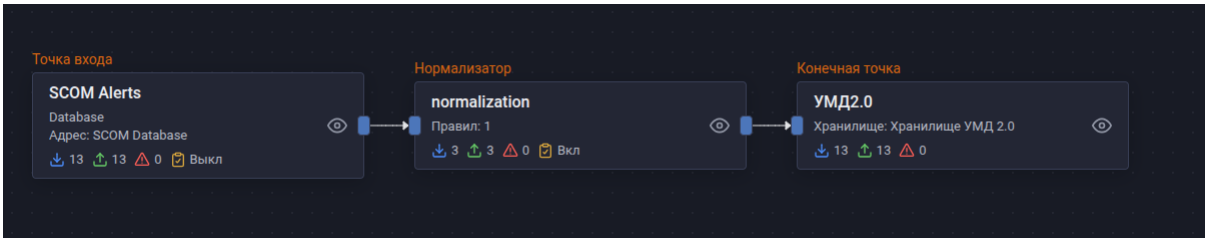
```
SELECT 'scom' AS appname, @@SERVERNAME as hostname, TimeAdded AS timer, * FROM
OperationsManager.dbo.RV_SCOM_ALERTS WHERE TimeAdded > DATEADD(S, CONVERT(INT,
?)+1, '1970-01-01') ORDER BY TimeAdded ASC;
```



При большом количестве событий в СУБД рекомендуется добавлять TOP 10000 в начало SQL-запроса.

   - Поле идентификатора: введите ключ timer со значением 1719588137.
   - Интервал запроса, секунд: введите значение 15.
4. Добавьте на конвейер элемент **Нормализатор** с правилом **Microsoft SCOM** (идентификатор правила: **RV-N-328**).
5. Соедините нормализатор с точкой входа.
6. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
7. Соедините конечную точку с нормализатором.
8. Сохраните и установите конфигурацию конвейера.

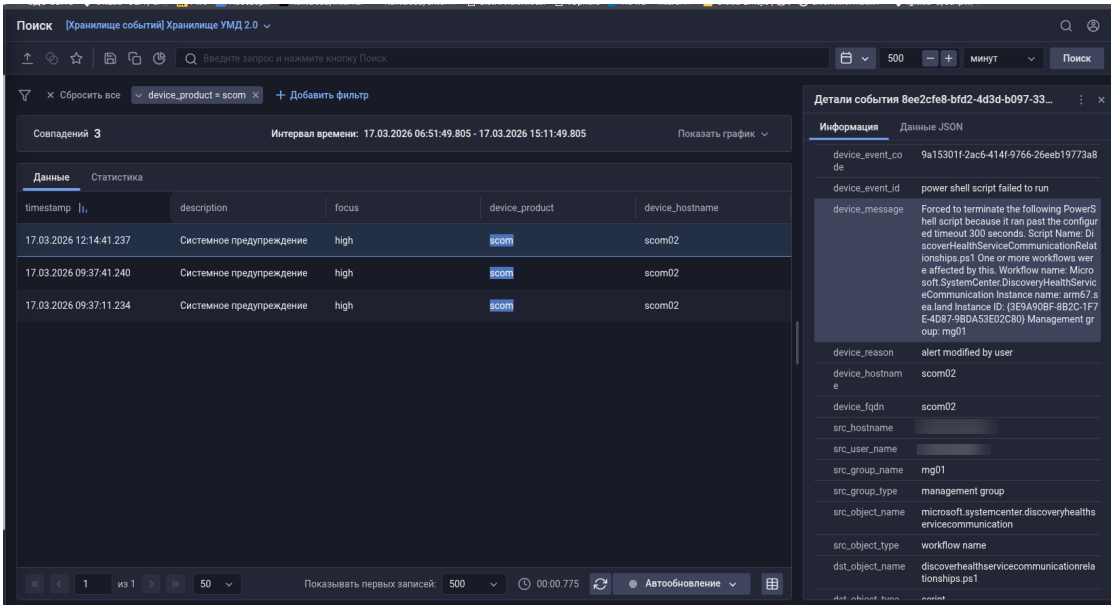
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать уведомления консоли SCOM.

Найти события Microsoft SCOM в хранилище можно по следующему фильтру:

```
device_product = "scom"
```



Службы каталогов (Directory Services)

Данный раздел содержит инструкции для настройки сбора событий с поддерживаемых служб каталогов:

- FreeIPA
- РЕД АДМ

FreeIPA

- FreeIPA: настройка источника
- FreeIPA: правила корреляции

FreeIPA: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий FreeIPA в R-Vision SIEM.

Настройка FreeIPA

Описание подсистемы журналирования FreeIPA

FreeIPA — это открытое программное обеспечение, предоставляющее специализированную службу каталогов для операционных систем на базе Linux. Оно предназначено для создания централизованной среды управления аутентификацией, авторизацией и учетными записями пользователей.

Продукт FreeIPA регистрирует события следующих служб:

- 389 DS;
- KRB5KDC;
- HTTPD.

Отправка событий FreeIPA

В настоящем руководстве рассматривается передача событий с помощью службы rsyslog. Предполагается, что rsyslog на станции с ОС Linux уже установлен.

Для настройки источника выполните следующие действия:

1. Настройте передачу событий из файлов. Для этого создайте файл конфигурации `/etc/rsyslog.d/01-freeipa.conf` со следующим содержимым:

```
module(load="imfile" mode="inotify")
input(
    type="imfile"
    File="/var/log/dirsrv/slapd-<DOMAIN>/access"
    Tag="FreeIPA-389DS-access"
```

```
    Severity="info"
    Facility="local4"
)
input(
    type="imfile"
    File="/var/log/dirsrv/slapd-<DOMAIN>/audit"
    Tag="FreeIPA-389DS-audit"
    Severity="info"
    Facility="local4"
)
input(
    type="imfile"
    File="/var/log/dirsrv/slapd-<DOMAIN>/errors"
    Tag="FreeIPA-389DS-errors"
    Severity="info"
    Facility="local4"
)

input(
    type="imfile"
    File="/var/log/httpd/error_log"
    Tag="FreeIPA-HTTPD-error_log"
    Severity="info"
    Facility="local4"
)

input(
    type="imfile"
    File="var/log/krb5kdc.log"
    Tag="FreeIPA-KDC-krb5kdc_log"
    Severity="info"
    Facility="local4"
)

if $syslogtag contains 'FreeIPA' then {
    action(type="omfwd" Target="<target>" Port="<port>" Protocol="<protocol>")
    stop
}
```

Здесь:

- `<target>` — IP-адрес или полное доменное имя (FQDN) коллектора SIEM.
- `<port>` — порт точки входа Syslog в конвейере SIEM.
- `<protocol>` — сетевой протокол: `tcp` или `udp`.
- `<DOMAIN>` — доменное имя.

2. Перезапустите службу rsyslog.service с помощью команды:

```
systemctl restart rsyslog.service
```

Для дистрибутивов на основе Debian журнал ошибок Apache по умолчанию располагается по пути `/var/log/apache2/error.log`.

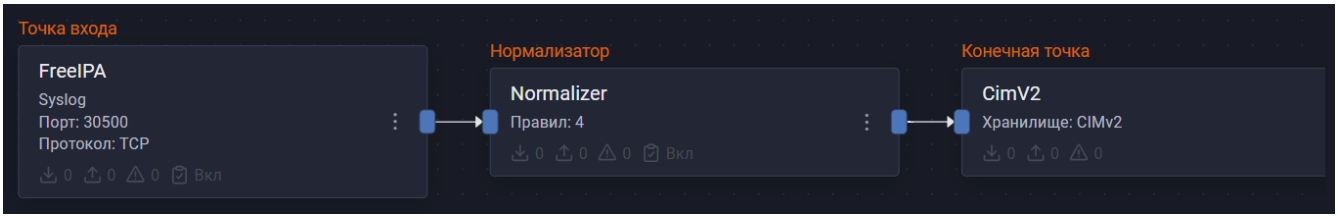
Чтобы корректно разбирать даты в журнале krb5kdc.log на системах с дистрибутивами на основе Debian, установите значение системной локали в файле `/etc/default/locale` на en_US.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Тип точки входа: Syslog.
   - Порт точки входа и протокол: в соответствии с настройками на стороне FreeIPA.
3. Добавьте на конвейер элемент **Нормализатор** с правилами **FreeIPA** (идентификаторы правил: **RV-N-206**, **RV-N-207**, **RV-N-208**, **RV-N-209**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

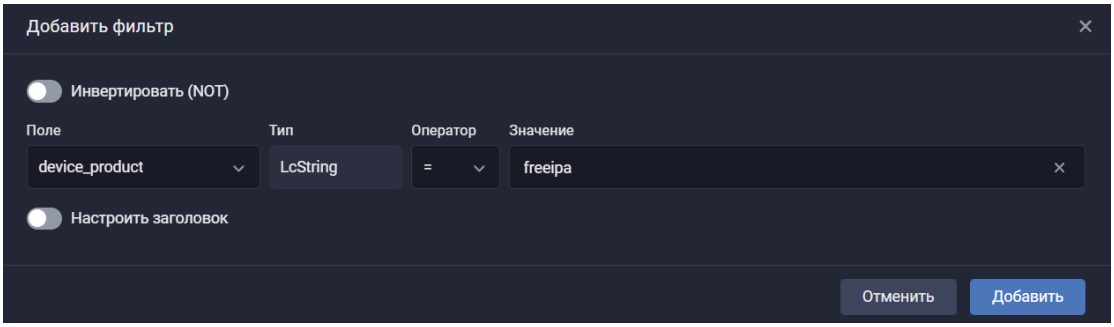
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события FreeIPA.

Найти события FreeIPA в хранилище можно по следующему фильтру:

```
device_product = "freeipa"
```



FreeIPA: правила корреляции

Таблица содержит сведения о разработанных правилах корреляции, включая их краткое описание и перечень тактик и техник MITRE ATT&CK, которые они охватывают.

ID правила	Название правила	Описание	Тактики и техники
RV-D-1048	Разведка пользователей/ролей Free IPA	Обнаружение использования команд поиска пользователей, групп и ролей в IPA. Атакующие могут попытаться получить список учетных записей домена. Далее эта информация может помочь определить, какие учетные записи домена существуют, чтобы облегчить последующее поведение, например, нацеливание на определенные учетные записи, обладающие определенными привилегиями. В случае подтверждения нелегитимной активности необходимо незамедлительно изолировать хост и отключить скомпрометированную учетную запись. Далее проверить возможные пути распространения атаки и осуществить поиск изначальной причины компрометации узла/УЗ.	• Discovery (TA0007) • Account Discovery (T1087) • Domain Account (T1087.002)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1049	Изменение оболочки входа средствами FreeIPA	Некоторые оболочки могут предоставлять больше возможностей для выполнения скриптов или команд. Атакующие могут воспользоваться изменением оболочки входа для повышения своих возможностей в системе. Данный функционал реализуется за счет функции user_mod() из функционала API FreeIPA (ipa user-mod) или при помощи смены оболочки пользователя в веб-интерфейсе. В случае возникновения активности требуется опросить пользователя, ответственного за учетную запись инициатора активности, на предмет осуществления активности. Если активность является нелегитимной, рекомендуется заблокировать учетную запись ее инициатора.	• Execution (TA0002) • Command and Scripting Interpreter (T1059) • Unix Shell (T1059.004)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1050	Остановка/перезапуск сервисов FreeIPA	FreeIPA — это набор компонентов для централизованного управления учетными записями, группами, политиками безопасности (аналог Active Directory в Windows). Для работы сервера FreeIPA по умолчанию устанавливается несколько сервисов. Для применения изменения многих конфигураций требуется перезагрузка этих сервисов. Атакующий может перезапустить или остановить сервисы для отключения функционала FreeIPA или подмены легитимных сервисов на вредоносные. В случае подтверждения нелегитимной активности, необходимо незамедлительно изолировать хост и отключить скомпрометированную учетную запись. Далее проверить возможные пути распространения атаки и осуществить поиск изначальной причины компрометации узла/УЗ.	• Impact (TA0040) • Service Stop (T1489)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1055	Изменение конфигурации sudo в FreeIPA	Обнаружение использования команд изменения конфигураций sudo в FreeIPA. Команда sudo позволяет системному администратору делегировать полномочия, чтобы предоставить определенным пользователям (или группам пользователей) возможность выполнять некоторые (или все) команды как root. Атакующие могут изменять конфигурацию sudo для закрепления в системе и повышения привилегий на доменных хостах. В случае подтверждения нелегитимной активности необходимо незамедлительно изолировать хост и отключить скомпрометированную учетную запись. Далее проверить возможные пути распространения атаки и осуществить поиск изначальной причины компрометации узла/учетной записи.	• Privilege Escalation (TA0004) • Abuse Elevation Control Mechanism (T1548) • Sudo and Sudo Caching (T1548.003)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1056	Добавление HBAC-правила через FreeIPA	HBAC (Host-based access control) — набор правил для настройки доступа пользователей или групп пользователей к определенным хостам с использованием определенных сервисов. Добавление HBAC-правил для определенного пользователя — это своего рода повышение привилегий, позволяющее изменить настройки доступа пользователей или групп пользователей к определенным хостам с использованием определенных сервисов. Создание нового HBAC-правила может нести риски по несанкционированному доступу к определенным сервисам FreeIPA. В случае возникновения активности требуется опросить пользователя, ответственного за учетную запись инициатора активности, на предмет осуществления активности. В случае если активность нелегитимна, заблокировать учетную запись инициатора активности.	• Privilege Escalation (TA0004) • Account Manipulation (T1098)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1057	Чтение Ticket CCACHE файла	Когда билеты настроены на сохранение в виде файла на диске, стандартным форматом и типом является файл CCACHE. Это простой двоичный формат файла для хранения учетных данных Kerberos. Эти файлы обычно хранятся в `/tmp` и имеют разрешения 600. С точки зрения атакующего, это важно по следующим причинам: 1. Действительные билеты могут быть использованы для аутентификации без необходимости знать пароль пользователя в открытом тексте. 2. Билеты CCACHE очень портативны. Их можно скачать и загрузить на другой хост без необходимости обновления или проверки билета. Таким образом, доступ к билетам CCACHE является критичным событием ИБ и может означать действия атакующего по разведке учетных записей и доступу к действительным билетам Kerberos. В случае возникновения инцидента необходимо опросить владельца учетной записи о причинах активности. Если легитимность активности не подтверждена, то заблокировать учетную запись, инициировать процесс расследования.	• Credential Access (TA0006) • Steal or Forge Kerberos Tickets (T1558) • Ccache Files (T1558.005)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1058	Атака Golden Ticket FreeIPA	Атака Golden Ticket предполагает, что атакующий создает поддельный Ticket Granting Ticket (TGT), который используется в Kerberos для получения доступа к ресурсам, как если бы он был законно выдан контроллером домена (KDC — Key Distribution Center). Это позволяет атакующему получать доступ ко всем ресурсам в домене без необходимости знать пароли пользователей. Атака требует наличия доступа к хэшу пароля учетной записи `krbtgt`, которая используется для подписи и верификации TGT. Эта учетная запись является критичной в Kerberos, так как ее ключ используется для подписи всех TGT, а этот поддельный билет будет принят всеми системами в домене как законный, так как он корректно подписан с использованием мастер-ключа домена. В данном правиле реализована интерпретация атаки Golden Ticket, но не подделыванием TGT, а кражей TGT-билета чужой УЗ, так как аутентификация в FreeIPA осуществляется через специализацию backend-а `ipa-kdb` без необходимости эксплуатировать хэш ключа `krbtgt`. При срабатывании данного правила необходимо связаться с владельцем УЗ. Если действия не подтверждены, то необходимо заблокировать учетную запись, от имени которой выполнялись команды для получения TGT-билета, и учетную запись `krbtgt`. Смена пароля `krbtgt` аннулирует все существующие, в том числе поддельные билеты Kerberos, которые могли быть созданы. Процесс изменения пароля `krbtgt` должен быть выполнен дважды с интервалом, чтобы убедиться, что все билеты полностью	• Credential Access (TA0006) • Steal or Forge Kerberos Tickets (T1558) • Golden Ticket (T1558.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1061	Выполнение бэкапа FreeIPA	Клонирование домена в контексте FreeIPA можно реализовать через бэкап домена при помощи команды ipa-backup с последующим развертыванием локальной копии контроллера домена. Это позволяет атакующему получить все необходимые ключи для создания билетов, в том числе золотых. Основные этапы включают получение бэкапа, восстановление бэкапа, и запуск локального контроллера домена, который будет идентичен целевому окружению. При срабатывании данного правила необходимо незамедлительно связаться с инициатором активности и с администратором контроллера домена для уточнения легитимности. В случае нелегитимности, необходимо сбросить пароль для всех пользователей в домене, так как они могли быть скомпрометированы в том числе и от УЗ Directory Manager.	• Defense Evasion (TA0005) • OS Credential Dumping (T1003) • DCSync (T1003.006)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1062	Успешный подбор пароля пользователя FreeIPA	В домене под управлением FreeIPA в качестве основного механизма аутентификации используется протокол Kerberos. Использование данного протокола позволяет производить атаки, аналогичные атакам на Active Directory. Одним из видов такой атаки является перебор паролей для учетной записи. Для получения доступа к учетной записи или хосту атакующий может попробовать подобрать пароль с помощью перебора. В случае возникновения инцидента необходимо опросить владельца учетной записи о причинах активности. Если легитимность активности не подтверждена, то заблокировать учетную запись, инициировать процесс расследования.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1063	Чтение LDAP секретов FreeIPA	Клонирование домена в контексте FreeIPA можно реализовать через экспорт LDAP-данных с последующим развертыванием локальной копии контроллера домена. Это позволяет атакующему получить все необходимые ключи для создания билетов, в том числе золотых. Основные этапы включают получение дампа LDIF, восстановление бэкапа и запуск локального контроллера домена, который будет идентичен целевому окружению. В файлах `id2entry` и `dse.ldif` хранится база LDAP, из которой можно развернуть контроллер домена в своей изолированной среде. При срабатывании данного правила необходимо незамедлительно связаться с инициатором активности и с администратором контроллера домена для уточнения легитимности. В случае нелегитимности необходимо сбросить пароль для всех пользователей в домене, так как они могли быть скомпрометированы в том числе и от УЗ Directory Manager.	• Credential Access (TA0006) • OS Credential Dumping (T1003) • DCSync (T1003.006)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1064	Атака Silver Ticket FreeIPA	Атака Silver Ticket является известной техникой, используемой для злоупотребления привилегиями в инфраструктуре, основанной на Microsoft Active Directory. FreeIPA, являясь системой управления идентификацией и аутентификацией, аналогичной Active Directory, также может быть потенциально уязвима для таких типов атак, так как система использует Kerberos. Используя поддельный билет, атакующий может получить доступ к ресурсам и услугам, для которых в иной ситуации потребовались бы легитимные учетные данные. В рамках данного правила детектируется создание keytab-файла и последующая аутентификация с запросом билета пользователя для доступа к сервису. При срабатывании данного правила необходимо связаться с владельцем УЗ, если действия не подтверждены, то необходимо заблокировать учетную запись, от имени которой выполнялись команды для получения TGS и сменить пароль скомпрометированной УЗ.	• Credential Access (TA0006) • Steal or Forge Kerberos Tickets (T1558) • Silver Ticket (T1558.002) • Ccache Files (T1558.005)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1065	Подбор пароля пользователя FreeIPA	В домене под управлением FreeIPA в качестве основного механизма аутентификации используется протокол Kerberos. Использование данного протокола позволяет производить атаки, аналогичные атакам на Active Directory. Одним из видов такой атаки является перебор паролей для учетной записи. Для получения доступа к учетной записи или хосту атакующий может попробовать подобрать пароль с помощью перебора. В случае возникновения инцидента необходимо опросить владельца учетной записи о причинах активности. Если легитимность активности не подтверждена, то заблокировать учетную запись, инициировать процесс расследования.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1066	Использование утилиты kadmin	Утилиты kadmin и kadmin.local используются для управления базой данных Kerberos. Kadmin подключается к удаленному серверу (kadmin server) и требует аутентификации для выполнения операций, а kadmin.local работает только локально на сервере, где установлена база данных Kerberos. В отличие от kadmin, kadmin.local не требует сетевого подключения и аутентификации. Доступ к данным утилитам атакующим может привести к тому, что он может скомпрометировать учетные записи и ключи, что приведет к утечке данных или несанкционированному доступу к ресурсам сети. При обнаружении несанкционированного доступа к утилитам kadmin и kadmin.local необходимо запросить информацию у пользователя, чья учетная запись обращалась к данным утилитам, при неподтверждении действий — заблокировать УЗ и проверить историю изменений в базе Kerberos от этой УЗ для предотвращения дальнейшего распространения атакующего.	• Persistence (TA0003) • Defense Evasion (TA0005) • Credential Access (TA0006) • OS Credential Dumping (T1003) • Account Manipulation (T1098) • Access Token Manipulation (T1134) • Create or Modify System Process (T1543)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1067	Изменение конфигураций FreeIPA через API	Обнаружение использования команд изменения критичных конфигураций в FreeIPA. API FreeIPA позволяет изменять все основные функции аутентификации, kerberos и других конфигураций. Атакующие могут изменять конфигурации для обхода механизмов безопасности и закрепления в системе. В случае возникновения инцидента требуется опросить пользователя, ответственного за учетную запись, на предмет осуществления активности. Если легитимность действий не подтверждена, рекомендуется заблокировать учетную запись и инициировать процесс расследования.	• Persistence (TA0003) • Modify Authentication Process (T1556) • Domain Controller Authentication (T1556.001)
RV-D-1068	Изменение файлов управления FreeIPA	FreeIPA — это набор компонентов для централизованного управления учетными записями, группами, политиками безопасности. Для управления сервером FreeIPA по умолчанию устанавливается несколько утилит для настройки и управления сервером. Атакующий может пытаться заменить данные исполняемые файлы на свои вредоносные, тем самым закрепляясь в системе. В случае возникновения инцидента требуется опросить пользователя, ответственного за учетную запись, на предмет осуществления активности. Если легитимность действий не подтверждена, рекомендуется заблокировать учетную запись и инициировать процесс расследования.	• Persistence (TA0003) • Masquerading (T1036) • Hijack Execution Flow (T1574)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1069	Изменение конфигураций разрешений в FreeIPA	Обнаружение использования команд добавления административных разрешений в FreeIPA. Атакующие могут добавлять новые административные права для закрепления в системе и повышения привилегий на доменных хостах. В случае возникновения инцидента требуется опросить пользователя, ответственного за учетную запись, на предмет осуществления активности. Если легитимность действий не подтверждена, рекомендуется заблокировать учетную запись и инициировать процесс расследования.	• Persistence (TA0003) • Account Manipulation (T1098) • Modify Authentication Process (T1556) • Domain Controller Authentication (T1556.001)
RV-D-1070	Изменение конфигураций привилегий в FreeIPA	Обнаружение использования команд добавления административных прав в привилегии FreeIPA. Атакующие могут изменять привилегии для закрепления в системе и повышения привилегий на доменных хостах. В случае возникновения инцидента требуется опросить пользователя, ответственного за учетную запись, на предмет осуществления активности. Если легитимность действий не подтверждена, рекомендуется заблокировать учетную запись и инициировать процесс расследования.	• Persistence (TA0003) • Account Manipulation (T1098) • Modify Authentication Process (T1556) • Domain Controller Authentication (T1556.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1071	Изменение конфигураций ролей в FreeIPA	Обнаружение использования команд добавления административных прав в привилегии и их назначение ролям FreeIPA. Атакующие могут изменять роли для закрепления в системе и повышения привилегий на доменных хостах. В случае возникновения инцидента требуется опросить пользователя, ответственного за учетную запись, на предмет осуществления активности. Если легитимность действий не подтверждена, рекомендуется заблокировать учетную запись и инициировать процесс расследования.	• Persistence (TA0003) • Account Manipulation (T1098)
RV-D-1072	Изменение конфигурации сервера kerberos	Kerberos – это сетевой протокол аутентификации, который позволяет передавать данные через незащищенные сети для безопасной идентификации. Протокол проверки подлинности Kerberos обычно используется для аутентификации на объектах доменной инфраструктуры, в том числе и в FreeIPA. По умолчанию конфигурационные файлы kerberos в FreeIPA хранятся в директориях `/etc/krb5.conf*` и `/etc/sysconfig/krb5kdc*`. Атакующий может изменять данные файлы, меняя тем самым настройки сервера, что позволяет ему закрепиться в домене различными способами. В случае возникновения инцидента требуется опросить пользователя, ответственного за учетную запись, на предмет осуществления активности. Если легитимность действий не подтверждена, рекомендуется заблокировать учетную запись и инициировать процесс расследования.	• Persistence (TA0003) • Modify Authentication Process (T1556) • Domain Controller Authentication (T1556.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1074	Изменение конфигурации сервера FreeIPA	По умолчанию конфигурационные файлы FreeIPA хранятся в директориях `/var/lib/ipa/` и `/etc/ipa`. Атакующий может изменять данные файлы, меняя тем самым настройки сервера, что позволяет ему закрепиться в домене различными способами. Также, например, при чтении `/var/lib/ipa/passwds` можно получить хэш пароля Directory Manager, который в последующем позволяет получить широкий спектр прав (доступ к различным ресурсам, минуя Kerberos, обращение к базе LDAP с правами создателя). В случае возникновения инцидента требуется опросить пользователя, ответственного за учетную запись, на предмет осуществления активности. Если легитимность действий не подтверждена, рекомендуется заблокировать учетную запись и инициировать процесс расследования.	• Persistence (TA0003) • OS Credential Dumping (T1003) • Create Account (T1136) • Domain Account (T1136.002) • Modify Authentication Process (T1556) • Domain Controller Authentication (T1556.001)
RV-D-1075	Изменение конфигурации сервера ldap	По умолчанию конфигурационные файлы openldap хранятся в директориях `/etc/openldap*` и `/etc/sudo-ldap.conf`. Атакующий может изменять данные файлы, меняя тем самым настройки сервера, что позволяет ему закрепиться в домене различными способами. В случае возникновения инцидента требуется опросить пользователя, ответственного за учетную запись, на предмет осуществления активности. Если легитимность действий не подтверждена, рекомендуется заблокировать учетную запись и инициировать процесс расследования.	• Persistence (TA0003) • Modify Authentication Process (T1556) • Domain Controller Authentication (T1556.001) • Steal or Forge Kerberos Tickets (T1558)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1097	Подбор пароля от FreeIPA Web UI	События множественных неудачных аутентификаций в FreeIPA Web UI могут указывать на перебор паролей учетных записей домена. Атакующие могут осуществлять подбор учетных данных для получения доступа к доменным ресурсам и привилегированным операциям.	• Credential Access (TA0006) • Brute Force (T1110) • Password Spraying (T1110.003) • Credential Stuffing (T1110.004)
RV-D-1098	Обнаружение атаки Password Spraying на FreeIPA	В домене под управлением FreeIPA в качестве основного механизма аутентификации используется протокол Kerberos. Использование данного протокола позволяет производить атаки, аналогичные атакам на Active Directory. Одним из видов такой атаки является Password Spraying учетных записей. Для получения доступа к учетной записи или хосту атакующий может попробовать подобрать пароль с помощью перебора.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)
RV-D-1102	Подбор пароля пользователя по LDAP в FreeIPA	В домене под управлением FreeIPA используется протокол LDAP для аутентификации и управления данными. Использование данного протокола позволяет производить атаки, аналогичные атакам на Active Directory. Одним из видов такой атаки является подбор паролей пользователей через LDAP-интерфейс. Для получения доступа к учетной записи или доменным ресурсам атакующий может попробовать подобрать пароль с помощью перебора по LDAP-протоколу, обходя ограничения Kerberos.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)

ID правила	Название правила	Описание	Тактики и техники
RV-D-1103	Успешный подбор пароля пользователя по LDAP в FreeIPA	В домене под управлением FreeIPA используется протокол LDAP для аутентификации и управления данными. Использование данного протокола позволяет производить атаки, аналогичные атакам на Active Directory. Одним из видов такой атаки является подбор паролей пользователей через LDAP-интерфейс. Для получения доступа к учетной записи или доменным ресурсам атакующий может попробовать подобрать пароль с помощью перебора по LDAP-протоколу, обходя ограничения Kerberos.	• Credential Access (TA0006) • Brute Force (T1110) • Password Guessing (T1110.001)
RV-D-1118	Успешный подбор пароля от FreeIPA Web UI	События множественных неудачных аутентификаций в FreeIPA Web UI с последующим успешным доступом могут указывать на перебор паролей учетных записей домена. Атакующие могут осуществлять подбор учетных данных для получения доступа к доменным ресурсам и привилегированным операциям.	• Credential Access (TA0006) • Brute Force (T1110) • Password Spraying (T1110.003) • Credential Stuffing (T1110.004)

РЕД АДМ

- РЕД АДМ: настройка источника

РЕД АДМ: настройка источника

Данное руководство описывает процесс настройки сбора и отправки событий РЕД АДМ в R-Vision SIEM.

Предварительные требования

- Настроен и сконфигурирован `rsyslog`-сервер на машине с установленным сервисом РЕД АДМ.

Настройка РЕД АДМ

Описание подсистемы журналирования РЕД АДМ

Система централизованного управления ИТ-инфраструктурой РЕД АДМ является программным продуктом, разработанным компанией РЕД СОФТ. РЕД АДМ имеет модульную структуру и агрегирует в себе множество модулей администрирования различного назначения.

Отправка событий РЕД АДМ

В настоящем руководстве рассматривается передача событий с помощью встроенного сервиса `syslog` и службы `rsyslog`. Для настройки событий авторизации, доступа к веб-интерфейсу и событий серверных служб выполните следующие действия:

1. Включите сервис в файле конфигурации `Samba`. Для этого:
   - Откройте файл конфигурации `/opt/reddc/etc/smb.conf`.
   - В секцию `[global]` в список директивы `server services` добавьте сервис `redlog`:

     ```
     server services = s3fs, rpc, nbt, wrepl, ldap, cldap, kdc, drepl, winbindd,
     ntp_signd, kcc, dnsupdate, redlog
     ```

   - Перезагрузите сервис `reddc`, чтобы изменения вступили в силу:

     ```
     systemctl restart redd
     ```

2. Создайте файл `/etc/rsyslog.d/red-log.conf` со следующим содержимым:

```
module(load="imfile") # Закомментируйте, если модуль используется в rsyslog.conf
input(type="imfile"
      file="/var/log/redadm/ldap_queries.log"
      tag="RedAdm_ldap"
      facility="local0"
      severity="info"
)
input(type="imfile"
      file="/var/log/redadm/event.log"
      tag="RedAdm_event"
      facility="local0"
      severity="info"
)
input(type="imfile"
      file="/var/log/redadm/session.log"
      tag="RedAdm_session"
      facility="local0"
      severity="info"
)
input(type="imfile"
      file="/var/log/redadm/server.log"
      tag="RedAdm_server"
      facility="local0"
```

```
      severity="info"
)
input(type="imfile"
      file="/var/log/redadm/ssh.log"
      tag="RedAdm_ssh"
      facility="local0"
      severity="info"
)
input(type="imfile"
      file="/var/log/redadm/playbook.log"
      tag="RedAdm_playbook"
      facility="local0"
      severity="info"
)
if $syslogtag contains "RedAdm" then {
        action(type="omfwd"
           target="<ip-address>"
           port="<port>"
           protocol="<proto>"
           action.resumeRetryCount="-1"  # Бесконечные попытки при ошибке сети
    )
    stop
}
```

- `<ip-address>`: IP-адрес вашей воркер-ноды R-Vision SIEM.
- `<port>`: порт точки входа, настроенной в конвейере.
- `<protocol>`: `tcp` или `udp` в зависимости от настроек на стороне R-Vision SIEM.

3. Перезагрузите rsyslog-сервер для применения конфигурации:

```
systemctl restart rsyslog.service
```

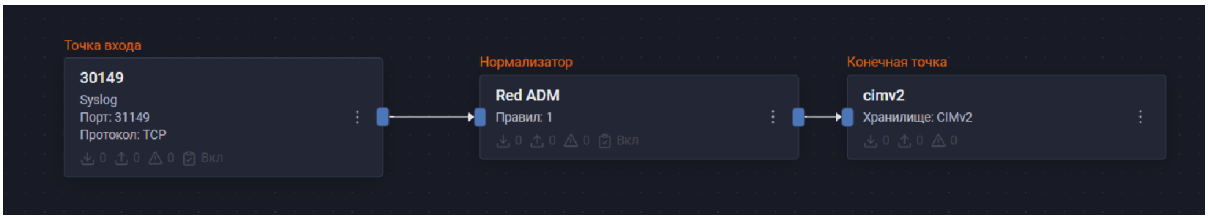
Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - **Название**: введите название точки входа.
   - **Тип точки входа**: выберите вариант **Syslog**.
   - **Порт точки входа**: введите значение в соответствии с настройками на стороне РЕД АДМ.
   - **Протокол**: выберите вариант в соответствии с настройками на стороне РЕД АДМ.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **РЕД АДМ** (идентификатор правила: **RV-N-327**).
4. Соедините нормализатор с точкой входа.

5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

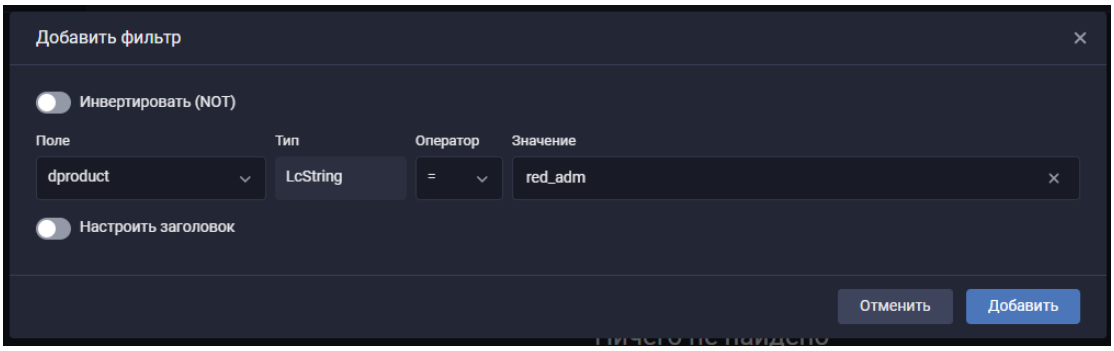
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события РЕД АДМ.

Найти события РЕД АДМ в хранилище можно по следующему фильтру:

```
device_product = "red_adm"
```



Прочие системы и источники

Данный раздел содержит инструкции для настройки сбора событий с других поддерживаемых систем и источников:

- Sonatype Nexus Repository
- АйТи Бастион СКДПУ НТ
- Универсальный коннектор CEF

Sonatype Nexus Repository

- Sonatype Nexus Repository: настройка источника

Sonatype Nexus Repository: настройка источника

Данное руководство описывает процесс настройки сбора событий Sonatype Nexus Repository и их отправки в R-Vision SIEM.

Настройка Sonatype Nexus Repository



Журналирование событий сервиса Sonatype Nexus Repository по умолчанию ведется в директории `/sonatype-work/nexus3/log/`, где установлено приложение. Дополнительных действий по настройке журналирования не требуется.

Отправка событий Sonatype Nexus Repository

Чтобы настроить отправку событий сервера Sonatype Nexus Repository, выполните следующие шаги:

1. Откройте конфигурационный файл rsyslog (`/etc/rsyslog.conf` или `/etc/rsyslog.d/`).
2. Добавьте в файл следующие правила:

```
module(load="imfile" PollingInterval="10")
input(type="imfile"
      File="/opt/sonatype-work/nexus3/log/audit/audit.log"
      Tag="nexus")
if $syslogtag contains 'nexus' then {
  action(type="omfwd" target="<target>" port="<port>" protocol="udp")
  stop
}
```

Здесь:

- `<target>` — введите IP-адрес или полное доменное имя (FQDN) сервера syslog или узла кластера Kubernetes, на котором запущен коллектор SIEM.
- `<port>` — для отправки событий на конвейер SIEM укажите порт точки входа Syslog — значение в диапазоне 30000—32767.

3. Перезапустите rsyslog, чтобы изменения вступили в силу:

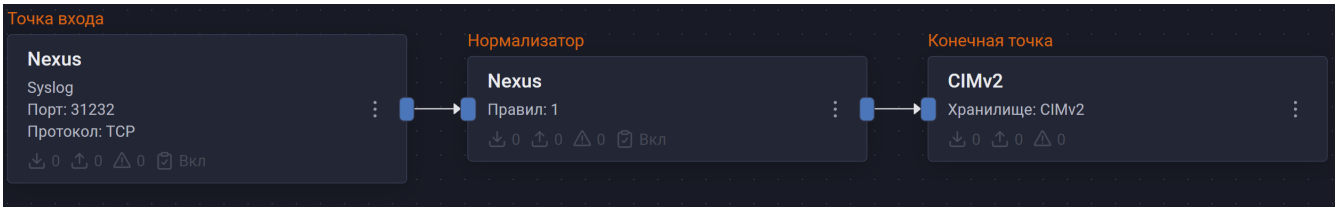
```
sudo systemctl restart rsyslog
```

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне сервера Nexus Repository.
   - Протокол: выберите вариант в соответствии с настройками на стороне сервера Nexus Repository.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Nexus** (идентификатор правила: **RV-N-304**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

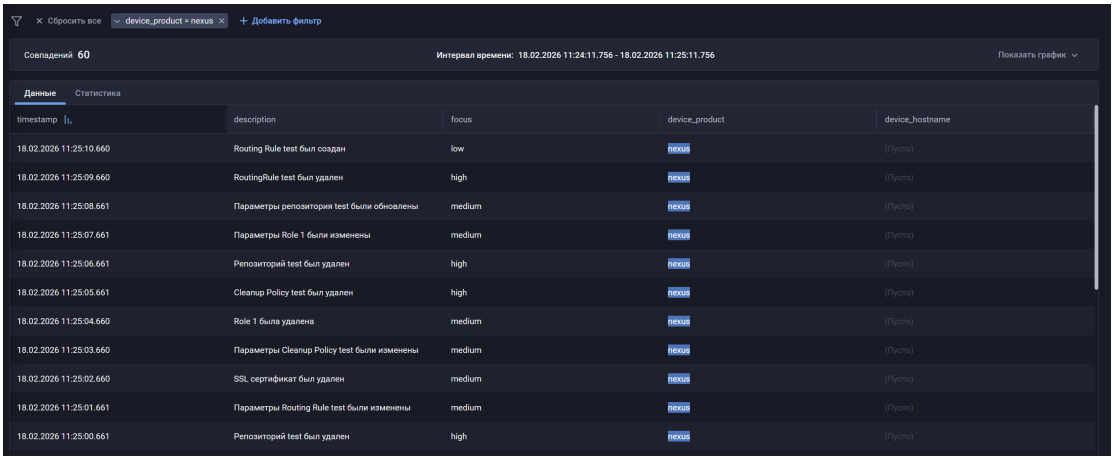
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события Sonatype Nexus Repository.

Найти события Sonatype Nexus Repository в хранилище можно по следующему фильтру:

```
device_product = "nexus"
```



АйТи Бастион СКДПУ НТ

- АйТи Бастион СКДПУ НТ: настройка источника

АйТи Бастион СКДПУ НТ: настройка источника

Данное руководство описывает процесс отправки событий АйТи Бастион СКДПУ НТ в R-Vision SIEM.

Предварительные требования

Перед настройкой отправки событий в R-Vision SIEM убедитесь в выполнении следующих условий:

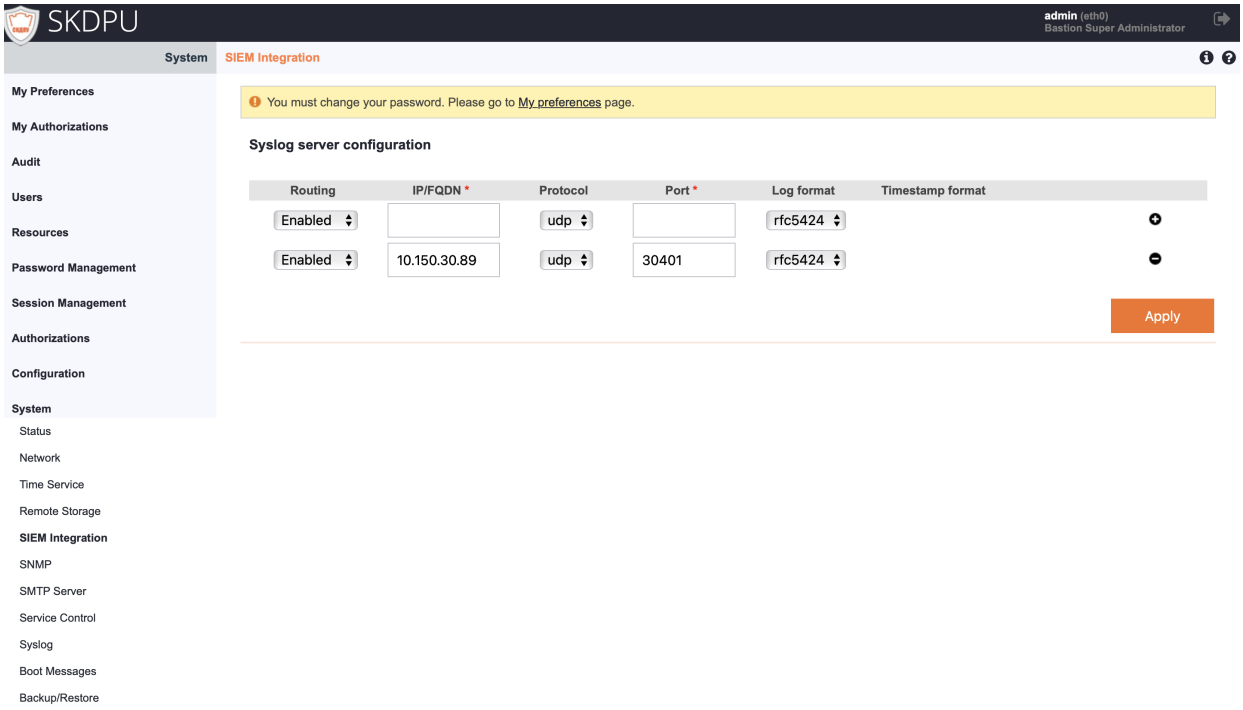
1. Пользователь, выполняющий настройку, имеет права администратора.
2. IP-адреса отправителя и получателя корректны, и между ними существует маршрут.

Настройка АйТи Бастион СКДПУ НТ

Отправка событий АйТи Бастион СКДПУ НТ

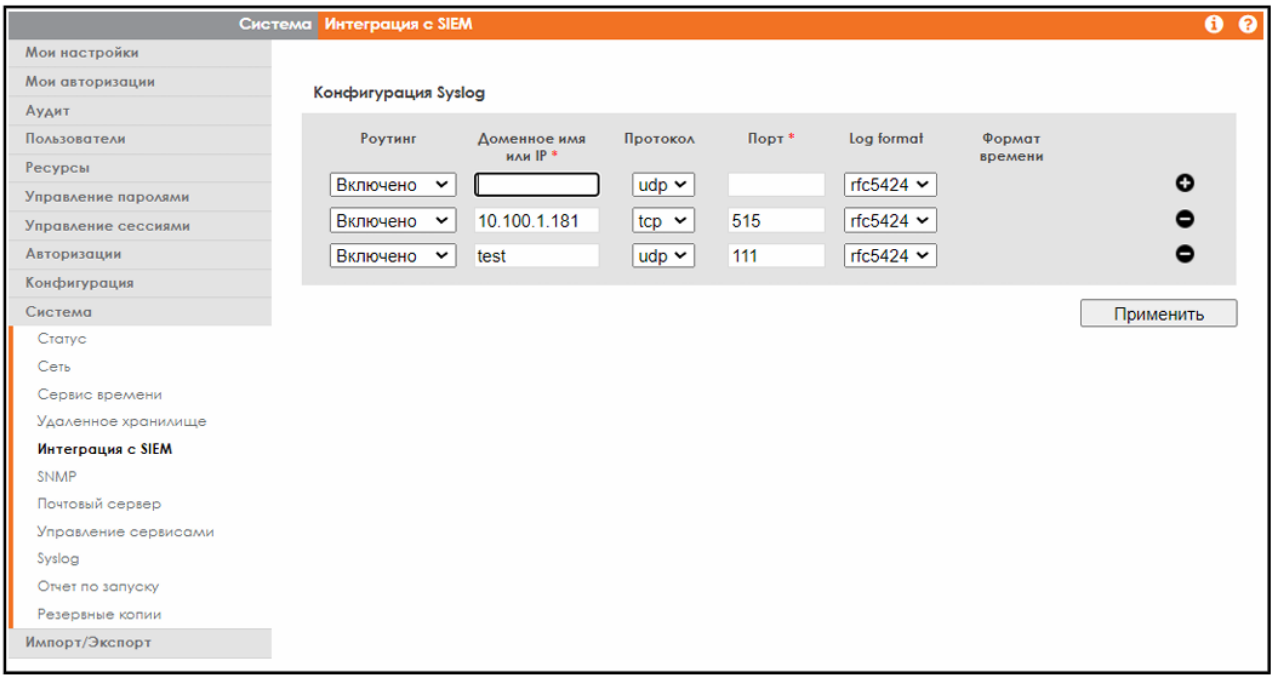
Для перенаправления журналов СКДПУ НТ GW Syslog в SIEM выполните следующие шаги:

1. В веб-интерфейсе **SKDPU** перейдите в раздел **System**.
2. Выберите пункт **SIEM Integration**.
3. Для отправки журналов, сохраненных в локальной файловой системе, настройте следующие параметры:
    - Выберите из выпадающего списка **Routing** значение **Enabled**, чтобы включить перенаправление журналов Syslog.
    - В поле **IP/FQDN** введите требуемый IP-адрес.
    - Выберите из выпадающего списка **Protocol** необходимый протокол.
    - В поле **Port** введите значение порта.
    - Выберите из выпадающего списка **Log format** требуемый формат записей.
    - Нажмите на кнопку **Apply**.



Для перенаправления журналов СКДПУ НТ Syslog в SIEM выполните следующие шаги:

1. В веб-интерфейсе **СКДПУ** перейдите в раздел **Система**.
2. Выберите пункт **Интеграция с SIEM**.
3. Настройте следующие параметры:
    - Выберите из выпадающего списка **Роутинг** значение **Включено**, чтобы включить перенаправление журналов Syslog.
    - В поле **Доменное имя или IP** введите требуемый IP-адрес.
    - Выберите из выпадающего списка **Протокол** необходимый протокол.
    - В поле **Порт** введите значение порта.
    - Выберите из выпадающего списка **Log format** требуемый формат записей.
    - Нажмите на кнопку **Применить**.



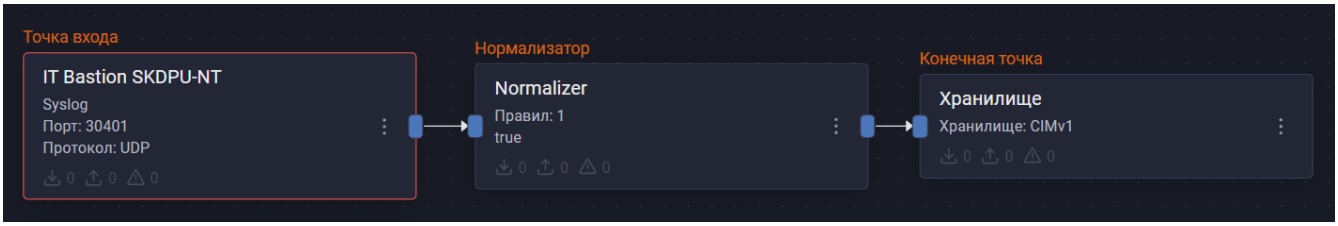
Отправка событий АйТи Бастион СКДПУ НТ настроена.

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне АйТи Бастион СКДПУ НТ.
   - Протокол: выберите вариант в соответствии с настройками на стороне АйТи Бастион СКДПУ НТ.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **IT Bastion SKDPU NT** (идентификатор правила: **RV-N-191**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

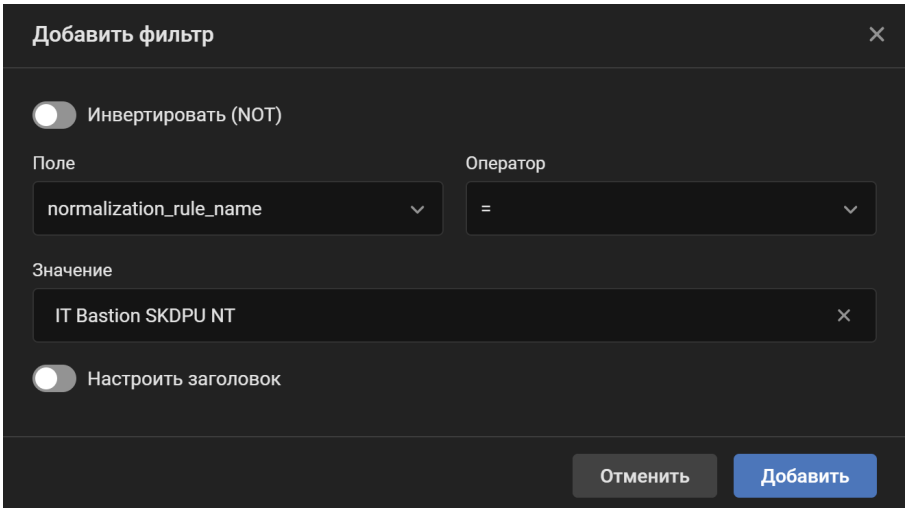
Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события АйТи Бастион СКДПУ НТ.

Найти события АйТи Бастион СКДПУ НТ в хранилище можно по следующему фильтру:

```
normalization_rule_name = "IT Bastion SKDPU NT"
```



Универсальный коннектор CEF

- Универсальный коннектор CEF: настройка источника

Универсальный коннектор CEF: настройка источника

Данное руководство содержит инструкции по настройке подключения к системе R-Vision SIEM источников событий, передающих данные в формате Common Event Format (CEF) через syslog.

Подключение источников событий, передающих данные в формате CEF, требует выполнения настроек на стороне источников, syslog-сервера и коллектора в R-Vision SIEM. После завершения настройки обеспечивается централизованный сбор, хранение и анализ событий безопасности от источников, поддерживающих логирование в формате CEF.

Корреляция событий, нормализованных универсальным коннектором CEF, в настоящий момент не поддерживается. Если для источника есть отдельные правила нормализации и корреляции, то источник следует подключать по инструкции для данного источника событий.

Предварительные требования

Настройка syslog-сервера

Для настройки syslog-сервера выполните следующие шаги:

1. Убедитесь, что syslog-сервер настроен на прослушивание порта. Как правило, для протоколов UDP и TCP используется порт 514.

2. Проверьте, что syslog-сервер принимает сообщения в формате CEF.

Настройка сетевой связности

Для настройки сетевой связности выполните следующие шаги:

1. Откройте порты 514 для UDP или TCP на сетевых устройствах.
2. Убедитесь, что источники событий имеют доступ к syslog-серверу.

Настройка источника событий

Убедитесь, что устройство или приложение поддерживает формат CEF и протокол syslog.



Способ настройки отправки событий может отличаться в зависимости от типа источника. Рекомендуем использовать официальную документацию источника при настройке логирования и отправки событий.

Для настройки источника событий для отправки сообщений в формате CEF выполните следующие шаги:

1. Укажите формат отправки — CEF.
2. Задайте адрес syslog-сервера.
3. Укажите порт. В примере ниже введен порт 514.

Пример 8. Пример команды настройки

```
log_format CEF
log_server <syslog-server-IP>
log_port 514
```

Настройка syslog-сервера

Для настройки syslog-сервера выполните следующие шаги:

1. Откройте конфигурационный файл rsyslog в директории `/etc/rsyslog.d/`.
2. Добавьте в файл правило обработки CEF-сообщений:

```
# Настройка для приема сообщений на порте 514 протокол UDP
module(load="imudp")
input(type="imudp" port="514")

# Направление CEF-сообщений в R-Vision SIEM
if $msg contains "CEF:" then {
    action(type="omfwd" Target="<siem>" Port="<port>" Protocol="tcp")
}
```

Здесь:

- `<siem>` — IP-адрес или полное доменное имя (FQDN) узла кластера Kubernetes, на котором запущен коллектор SIEM.
- `<port>` — порт точки входа Syslog для отправки событий на конвейер SIEM — любой свободный порт в диапазоне 30000—32767.

3. Перезапустите syslog-сервер с помощью команды:

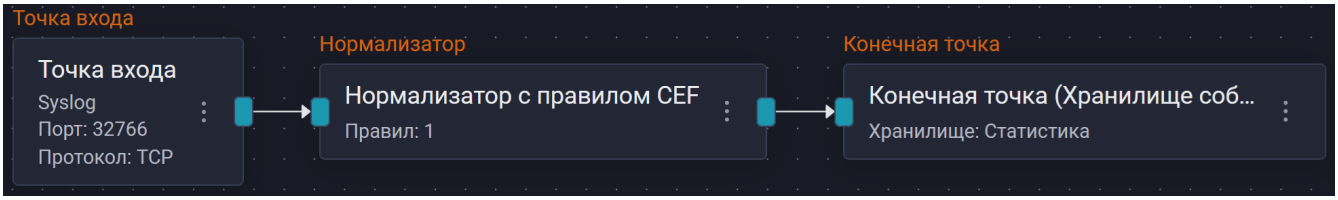
```
sudo systemctl restart rsyslog
```

Настройка в R-Vision SIEM

Для настройки сбора и нормализации событий источника в R-Vision SIEM выполните следующие шаги:

1. В интерфейсе R-Vision SIEM создайте новый конвейер в коллекторе.
2. Добавьте на конвейер элемент **Точка входа** со следующими параметрами:
   - Название: введите название точки входа.
   - Тип точки входа: выберите вариант **Syslog**.
   - Порт точки входа: введите значение в соответствии с настройками на стороне syslog-сервера.
   - Протокол: выберите вариант в соответствии с настройками на стороне syslog-сервера.
3. Добавьте на конвейер элемент **Нормализатор** с правилом **Universal CEF** (идентификатор правила: **RV-N-243**).
4. Соедините нормализатор с точкой входа.
5. Добавьте на конвейер элемент **Конечная точка** типа **Хранилище событий**.
6. Соедините конечную точку с нормализатором.
7. Сохраните и установите конфигурацию конвейера.

Пример конфигурации конвейера:



После настройки передачи событий, если настройка выполнена корректно, в хранилище начнут поступать события источника.

Найти события источника в хранилище можно по следующему фильтру:

```
device_product = "<Device Product>"
```

где `<Device Product>` — имя продукта, установленное вендором в поле `Device Product` CEF-заголовка события:

```
Jan 18 11:07:53 host CEF:Version|Device Vendor|Device Product|Device
Version|Device Event Class ID|Name|Severity|[Extension]
```

Проверка получения событий

Для проверки корректности настройки источника событий выполните следующие шаги:

1. Используйте утилиту `logger` для отправки тестового сообщения:

   ```
   logger -P 514 -n <syslog-server-IP>
   "CEF:0|Vendor|Product|Version|SignatureID|Name|Severity|Extension"
   ```

   где `<syslog-server-IP>` — адрес syslog-сервера.

2. Убедитесь, что события поступают в R-Vision SIEM и записываются в указанное хранилище.
3. Проверьте логи на syslog-сервере для подтверждения получения отправленного сообщения.
4. В случае отсутствия событий в SIEM убедитесь в корректности настроек порта, протокола и формата сообщений на стороне источника и syslog-сервера.

Решение проблем

Некорректный формат события может стать причиной неработающего правила нормализации.

Для устранения проблемы выполните следующие шаги:

1. Проверьте, соответствует ли событие одному из допустимых форматов:

   ```
   CEF:0|Vendor|Product|Version|SignatureID|Name|Severity|Extension
   'Syslog header' CEF:0|Vendor|Product|Version|SignatureID|Name|Severity|Extension
   ```

2. Удалите из события префикс `syslog` и проверьте, работает ли правило нормализации.
3. Если проблема сохраняется, проверьте событие на наличие лишних символов. Например, после разделителя `|` не должно быть пробелов.

   Пример с ошибкой:

   ```
   CEF:0|R-Vision|SEA|1.0|empty|empty|2| RealTime=09/13/2024 07:49:57
   ```

   Корректный формат:

   ```
   CEF:0|R-Vision|SEA|1.0|empty|empty|2|RealTime=09/13/2024 07:49:57
   ```

4. В RObject-конфигурации правила нормализации замените VRL-функцию `parse_cef` на `rv_parse_cef`, которая поддерживает заголовки syslog. Например:

```
normalizer: !vrl |
  # event = parse_cef(.raw.message) ?? {}
  event = rv_parse_cef(.raw.message) ?? {}
```