Michael Brunner, Andrea Mussmann

Information Security Management meets OpenReq

2nd Hamburg Requirements Engineering Symposium, Hamburg, 04.09.2019

Agenda

QE LaB Business Services

Context and Goals

- Information Security Management
- ADAMANT

Implementation and Results

- OpenReq Technologies
- Showcases
- Evaluation

Conclusion and Future Work

QE LaB Business Services GmbH – Customers

Stadt Bern

ARZ

SECURE SHOPPING
Die App zum Bezahlen.

HILTI

oncotyrol
Center for Personalized Cancer Medicine

tiroler wasser kraft

ÖBB INFRA

Farm Facts
A BayWa Company

FELDER GRUPPE

LIEBHERR

itsv

bachmann.

softwareONE

Founded 2012, University of Innsbruck Spin-Off

QE LaB Business Services GmbH – Range of Services

Systems Design

- Business Processes
- Architectures
- Model-driven Development
- Code Analysis

Quality Engineering

- Requirements Engineering
- Test Management & Automation
- Metrics
- Software Infrastructure

IT Security Engineering

- Security Analysis & Audits
- Security Requirements
- Security Testing
- Information Security Management

Processes and Services

- Process Assessment
- Process Improvement
- Service Evaluation
- Data Analytics

Workshops | **Individual Projects** | **Partnerships**

Agenda

QE LaB Business Services

Context and Goals

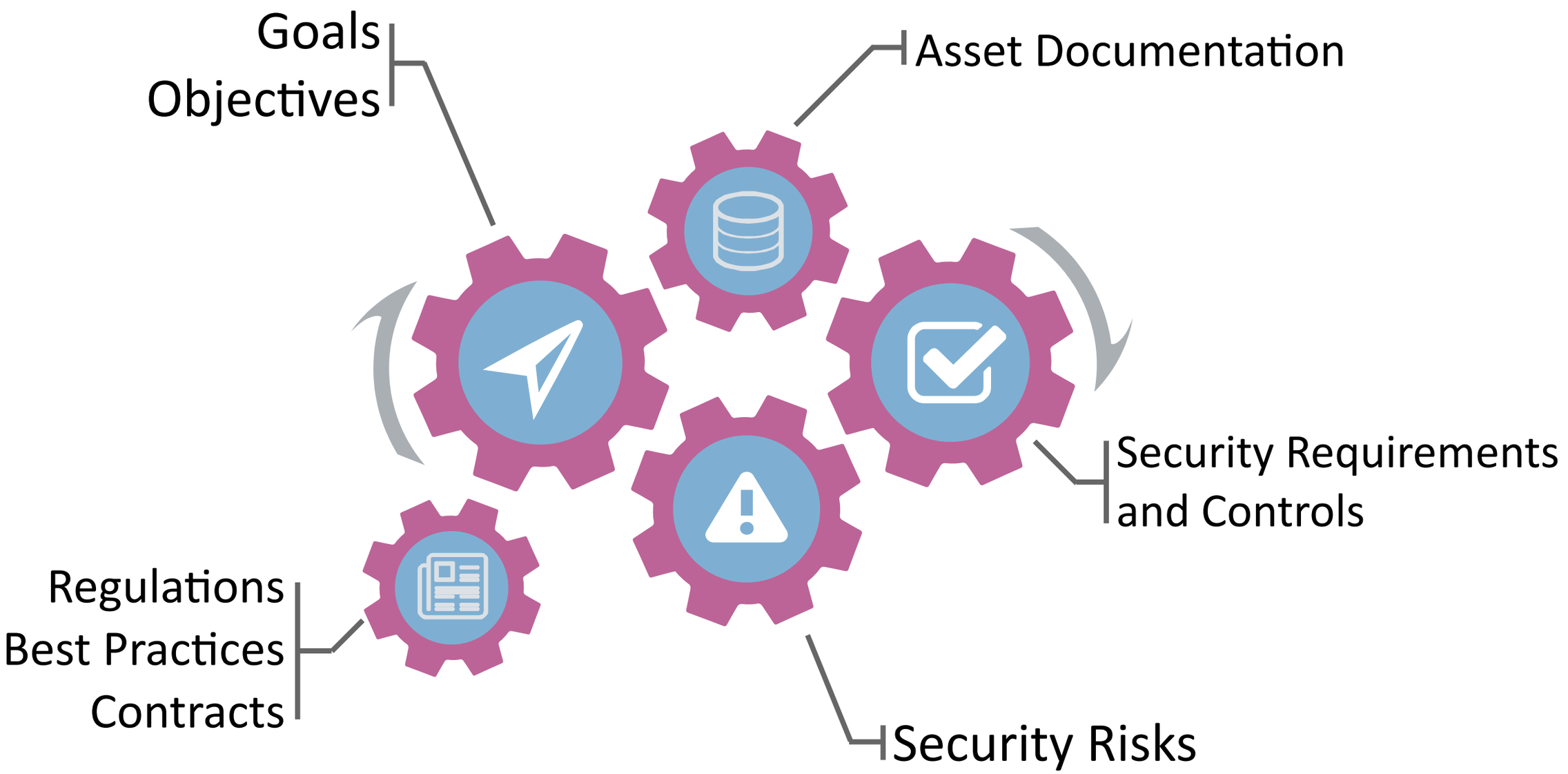
- Information Security Management
- ADAMANT

Implementation and Results

- OpenReq Technologies
- Showcases
- Evaluation

Conclusion and Future Work

Information Security Management



Systematically address challenges with regard to *confidentiality*, *integrity* and *availability* of *information and information processing facilities* on *organizational level.* Relevant Standards are ISO 27k or BSI IT Baseline Protection Methodology.

ADAMANT – Efficient Information Security, Data Privacy and Compliance Management

ADAMANT is a tool-supported framework enabling continuous information security management by de-emphasizing preset audit cycles

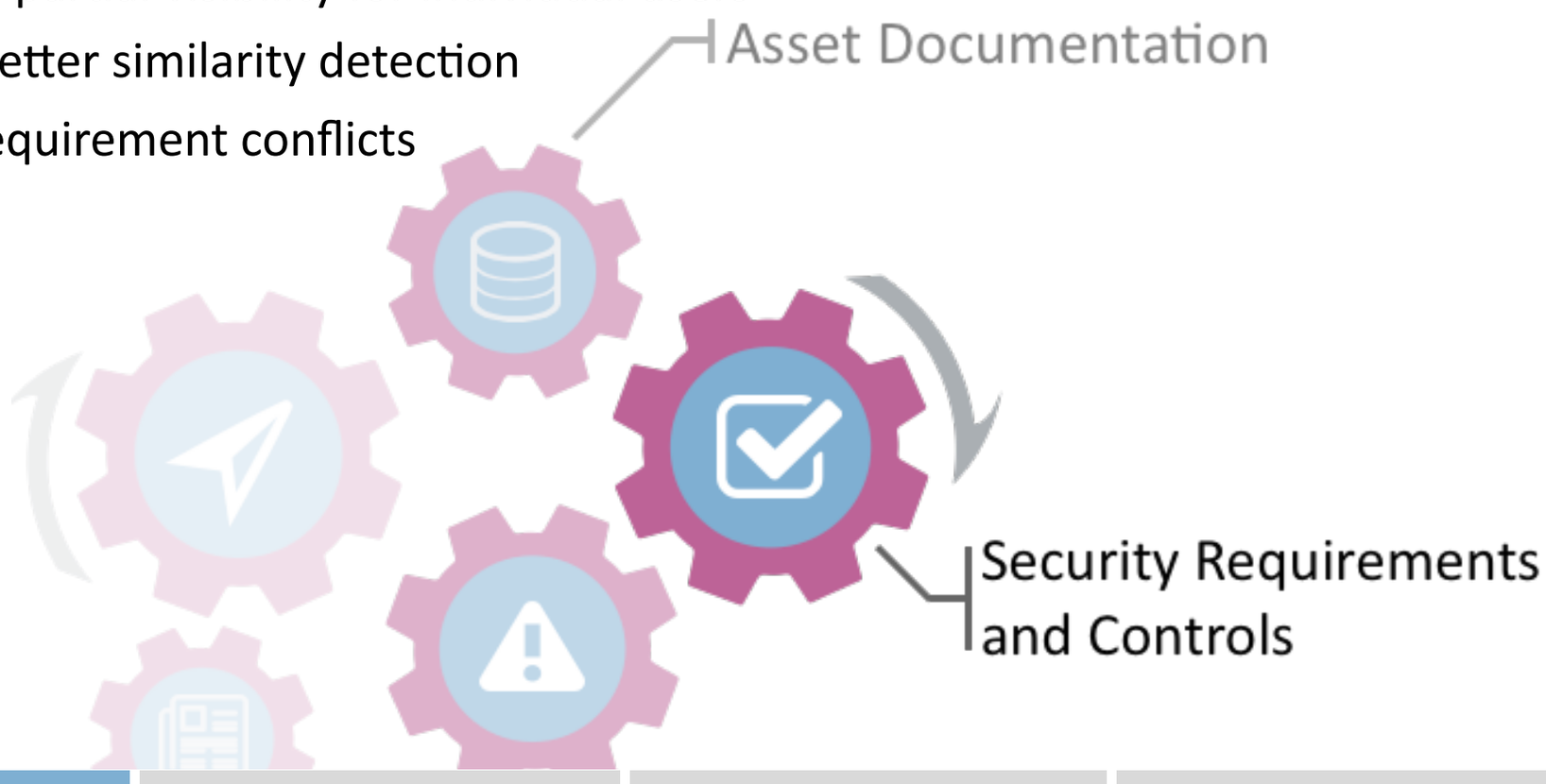
- Systematic handling of changes within highly interconnected asset, risk and security models
- Efficient organization of stake-holder collaboration in intra- and extra-organizational workflows
- Provide suitable automation facilities to reduce costs

Used in security consulting projects and for dedicated information security management trainings

OpenReq Open Call Project Goals

Extend security requirements engineering platform

- Quality checks for security requirement texts
  - Model-based approach with natural language descriptions for security goals, requirements and controls
  - Direct feedback on natural language texts
- Extend conflict/similarity detection
  - Collaborative approach with partial visibility for individual users
  - Support QA activities with better similarity detection
  - Identify potential security requirement conflicts



Agenda

QE LaB Business Services

Context and Goals

- Information Security Management
- ADAMANT

Implementation and Results

- OpenReq Technologies
- Showcases
- Evaluation

Conclusion and Future Work

OpenReq Technologies and Services

OpenReq Improving Requirements Quality

- Find language issues in requirements
  - Weak language
  - Ambiguous words

OpenReq Requirements Classifier

- Train informativeness classifier
- Classify requirements sentences

OpenReq Similarity Detection

- Detect similar requirements for each asset
- Resolve similarity conflicts

adamant

Edit | New Sub-Requirement | Delete | Operationalize | OpenReq | Back

Verify that all input validation controls are not affected by any malicious code

Verify that all input validation controls are not affected by any malicious code.

Rationale: risk analysis

Source: OWASP Application Security Verification Standard (2014) [OTHER]

Tags: OWASP ASVS | OWASP ASVS:Level 3 - Advanced

Stakeholders:

OpenReq Text Quality Analysis

OpenReq text quality analysis identified **7 potential issues**

1. Type: **Pronoun**
   "[..] that [..]"
   Description: Potentially unclear reference.
2. Type: **Dangerous Plural**
   "[..] all [..]"
   Description: Potentially dangerous plural.
3. Type: **Ambiguous Compound Nouns**
   "[..] input validation controls [..]"
   Description: A sequence of more than two consecutive nouns may have more than one interpretation depending on the possible associations between the words.
4. Type: **Ambiguous Nominalization**
   "[..] input validation [..]"
   Description: A nominalization means the use of the

Analyse | Edit | Close

Requirement Context

Switch to Graph View

adamant

Add Conflict Group | Run Conflict Detection for all Groups

Conflict Groups

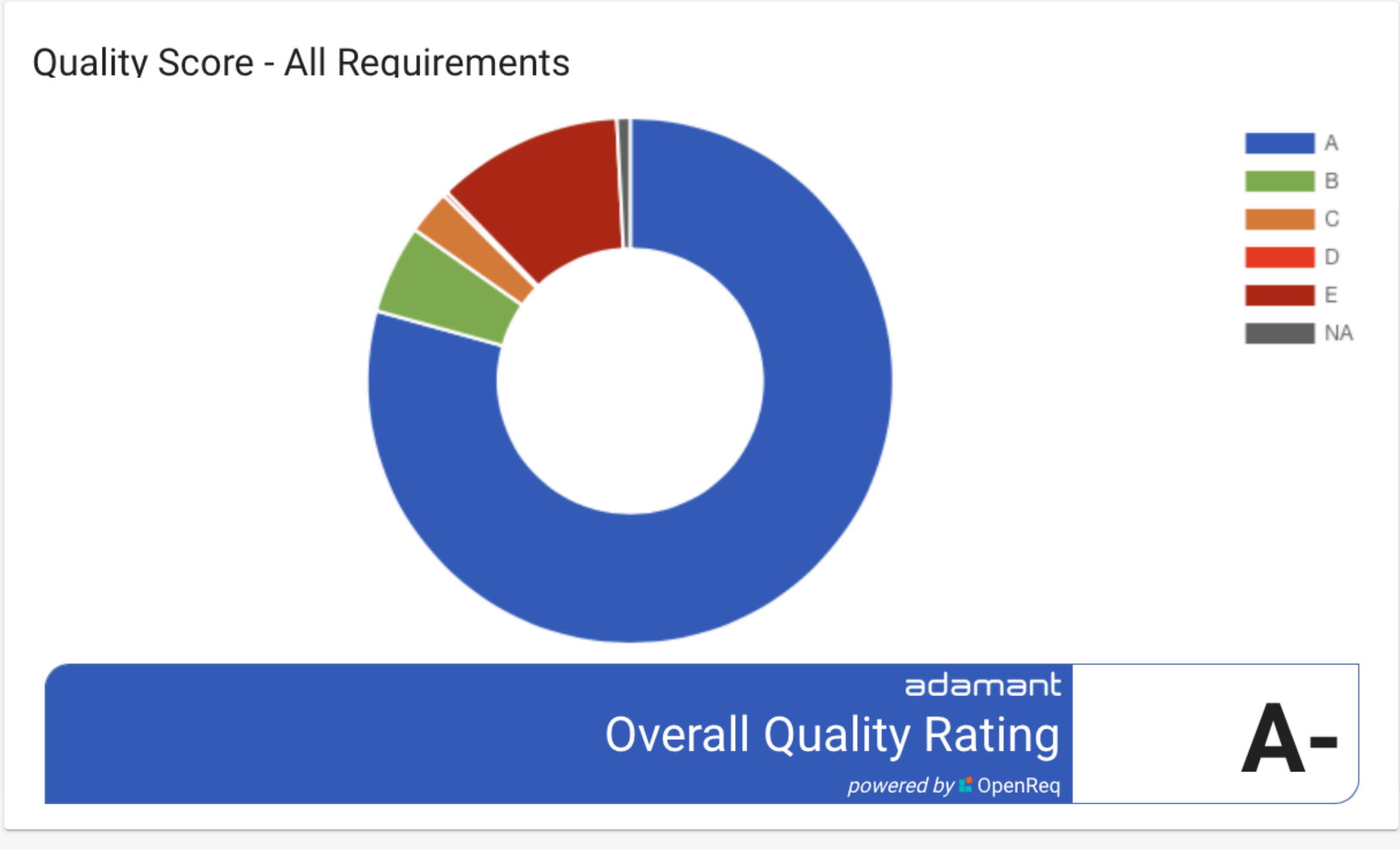
Name	Type	Responsible	Conflicts	Last Run	Commands
OpenReq Similarity Detection	openreqasset	Open Req	9 Conflicts (0 resolved)	today 13:07	
Similar Security Requirements and Controls	contentsimilarity	Open Req	5 Conflicts (0 resolved)	today 13:04	

In total there are **2** conflict groups configured.

Conflicts for Group **OpenReq Similarity Detection**

Requirement 1	Requirement 2	Identified	Resolved
Verify the use of passphrases	Verify password entry fields allow or encourage the use of passphrases	today 13:07	no
Verify that the mobile app does not store sensitive data onto potentially unencrypted shared resources on the device	Verify that the mobile app does not store sensitive data onto shared resources on the device	today 13:07	no
Verify that the application is not susceptible to LDAP Injection	Verify that the runtime environment is not susceptible to LDAP Injection	today 13:07	no
Verify that authenticated session tokens are sufficiently long and random to withstand session guessing attacks	Verify that session ids are sufficiently long, random and unique across the correct active session base	today 13:07	no
Verify that each log event includes necessary information that would allow for a detailed investigation of the timeline when an event happens	Verify that each log event includes necessary information	today 13:07	no
Verify that the list of sensitive data processed by this application is identified	Verify that the list of sensitive data processed ...	today 13:07	no
Verify that log fields from trusted and untrusted sources are distinguishable in log entries	Verify that log fields from trusted and untrusted sources are distinguishable in log entries	today 13:07	no

Evaluation – Results: Quality Analysis of OWASP ASVS

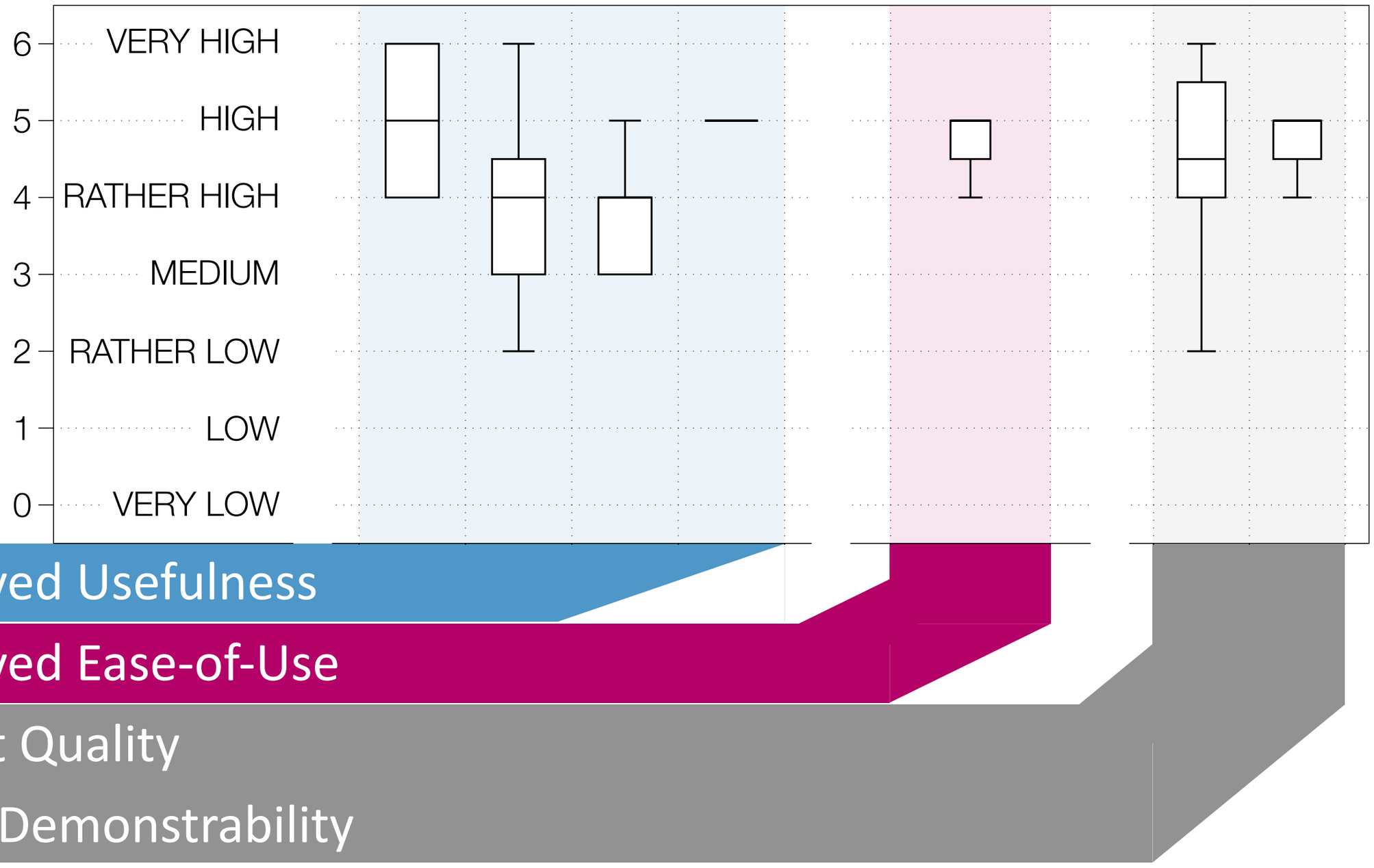


Am

Cc

Evaluation – User Feedback

User Perception of ADAMANT OpenReq Extension (TAM)



Agenda

QE LaB Business Services

Context and Goals

- Information Security Management
- ADAMANT

Implementation and Results

- OpenReq Technologies
- Showcases
- Evaluation

Conclusion and Future Work

Conclusion and Future Work

OpenReq services allowed the easy integration of new features into ADAMANT. We still see some areas for future improvement.

Enhance training data for OpenReq requirement classifier

- Use multiple standards
- Implement more classifiers and improve ADAMANT quality rating

Further use of similarity detection in research and practice

- Support template creation and management process
- Investigate security standards overlap
- Master thesis on security standard mappings

QE LaB Business Services GmbH

Michael Brunner (michael.brunner@qe-lab.com)

Andrea Mussmann (andrea.mussmann@qe-lab.com)

Technikerstraße 21a

A-6020 Innsbruck

www.qe-lab.com

https://adamant.work

https://openreq.adamant.work