Corelight Training

Silver

On demand learning at your pace delivered virtually

This course teaches new-to-Corelight incident responders, threat hunters and penetration testers everything they need to know to start using this powerful tool. The course balances lectures and lab exercises while covering the need for network monitoring, how to deploy Corelight Sensors, and the value of Corelight data.

COURSE MODULES

Why NTA? Why NDR? **Why Smart PCAP?** **Why Investigator?** **Why Corelight?**	We will cover what Network Traffic Analysis and Network Detection and Response are with examples using current and relevant incidents, intrusions and compromises as use cases. This foundational model will frame the remainder of the course with context and background.
Corelight in Your Network	This interactive module covers common protocols, and data visibility across the network, leading into an overview of SPAN ports, taps, and packet brokers. We end with a walkthrough of exporting.
Sensor Types: Hardware, Virtual, Cloud Platforms	In this module we will describe the differences between hardware sensor versions including their throughput requirements and additional features and capabilities.
Diagnostic Shell	A hands-on demonstration of using the diagnostic shell and discussion of several commands useful for troubleshooting.

Corelight Training: Silver

COURSE MODULES *(continued)*

REST API	An introduction to our REST API with several examples to monitor dataflow into your SIEM and manage configuration of the sensor.
ETC and C2 Collections from Corelight Research	Corelight's research continues to enhance the visibility above and beyond open-source Zeek®. We'll highlight the latest updates to include the Encrypted Traffic Collection and Command and Control Collection of inference packages.
Use Case: Incident Response	Learn how Suricata and Zeek work together to detect, investigate and track threats in real time with Investigator. The power of Zeek, Suricata and Investigator becomes clear when used for incident response investigations. We'll complete a hands-on investigation, including file extraction and protocol logging using only network data.
Introduction to Suricata	In this module we will describe the Corelight + Suricata integration, contrast the roles of Zeek and Suricata, demonstrate multiple ways to upload rulesets, and walk through the structure of a single rule.

Corelight Training: Silver

To learn more about Corelight training, please visit **https://www.corelight.com/support/training** or the Corelight website **corelight.com**

Corelight provides security teams with network evidence so they can protect the world's most critical organizations and companies. On-prem and in the cloud, our open Network Detection and Response platform enhances visibility and analytics, leading to faster investigations and expanded threat hunting. Corelight's global customers include Fortune 500 companies, major government agencies, and large research universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the widely-used network security technology.

info@corelight.com | 888-547-9497