Corelight Training

Three day course

Delivered onsite or virtually

Our most in-depth offering gives your team three days of hands-on training with world-class Corelight experts. Help your organization realize the full potential of Zeek®, Suricata and Corelight with customizable, interactive learning sessions. Students should be comfortable with networking protocols (e.g., IP, TCP, UDP, DNS, HTTP) and standard workflows within a SOC.

Designed for incident responders, threat hunters, and penetration testers who are not necessarily familiar with Zeek. We start off training you to deploy and use a sensor. Next, we'll focus on understanding what the data is telling us. Finally, you'll take part in multiple Capture the Flag exercises that give you the opportunity to test your skills against real-world attacks.

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 discusses visibility into specific network segments, before comparing SPAN ports, taps, and packet brokers.

COURSE MODULES *(continued)*

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.
REST API	An introduction to our REST API with several examples to monitor dataflow into your SIEM and manage configuration of the sensor.
Deploying Fleet Manager	Fleet Manager provides a unified portal to manage and monitor Corelight Sensors. We'll demonstrate how to deploy and configure Fleet Manager.
Managing Fleet Manager	We will learn how to use Fleet Manager to adjust sensor configuration, standardize policies, and enable packages at scale.
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.
Levels of Zeek	We will discuss the typical progression from introductory Corelight/Zeek users to power users to deep expert users/developers.
Deep Dive Into Logs	We will cover the following logs in detail: conn, http, dns, ssl, x509, smb, kerberos, ntlm, dce_rpc, notice, weird, and dpd.
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.
Capture the Flag Competition	We will apply Corelight data in a variety of scenarios, including internal hosts compromised by malware infections, and externally-exposed hosts being compromised. Participants need speed and precision to find artifacts and assemble the attack's storyline and workflow. An instructor is available to answer 1:1 questions and guide students through the challenge questions.

COURSE MODULES *(continued)*

Incident Response with Corelight Data	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.
Threat hunting with Corelight data	We will use the MITRE ATT&CK® matrix to guide our search for malicious activity, spanning back months using dns, smb, and ssh logs. You can't threat hunt without data, and Corelight data is the best source. We'll introduce the Threat Hunting Guide, then walk through real-world examples.
Intro to Zeek Scripting	In this module we will discuss how to begin writing a Zeek script, and introduce the Zeek scripting language through examples.
Capstone CTF	Find artifacts of real-world attacks, assembling the storyline and workflow of the attack, with an instructor available to answer 1:1 questions. Dig into real-world datasets with fresh knowledge, putting some of our tools and processes into action.
More Zeek Scripting	Take what you have learned in the Intro to Zeek scripting module to the next level by practicing and building more scripts with practical use cases.
Software Sensor	We will cover the Software Sensor and its designed use cases, performance and feature comparison, and cover useful commands.
Intel framework	In this module we will go over what the intel framework is and how indicators and data records are stored. We will also cover how to extend it by adding meta fields into intel logs and adding approved lists.
Input and config Framework	In this module we will discuss the configuration framework, package framework, how to add custom scripts, input framework, and reading tables.

OPTIONAL MODULES

Zeek Architecture	Zeek has dozens of protocol parsers that write metadata to Zeek logs. We will learn how they work and how Corelight makes it easy.

COURSE MODULES *(continued)*

Network Operations	We will find versions of software on our clients, monitor SSL/TLS certificate hygiene, and troubleshoot network protocols and routing issues.
Smart PCAP	In this module we will cover the origins of Smart PCAP, prerequisites for enabling SmartPCAP, use cases for PCAP rules, rules and rule files, rule levers, and end with PCAP retrieval.
More Suricata	We will take Suricata to the next level teaching you how to read headers, write rules/signature, chat about content modifiers, cover keywords, and go over examples of single and multi conditional rules/signatures.

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