corelight

THREE DAY TRAINING

Three Day Corelight / Zeek Training

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

Designed for incident responders, threat hunters, and penetration testers, who are not necessarily familiar with Zeek, we'll train 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 CTF exercises that give you the opportunity to test your skills against real-world attacks.

THREE DAY COURSE DESCRIPTION

Intro to Zeek and EternalSafety	Introduce Zeek by way of EternalSafety, a package used to detect EternalBlue. We'll cover the purpose of Zeek and the philosophy of providing non-judgemental data.
Zeek Architecture	A detailed walkthrough of Zeek internals, focusing on how connections and protocol analysis works using Dynamic Protocol Detection (DPD).
Why Zeek? Why Corelight?	How is Zeek different from other network traffic data? How does Corelight enhance Zeek? We'll dive into use cases.
Insights through Corelight Research	Corelight's research continues to enhance the visibility above-and-beyond open-source Zeek. We'll highlight the latest updates.
Corelight in Your Network	This interactive module discusses visibility into specific network segments, before comparing SPAN ports, taps, and packet brokers.
Sensors Types	A comparison of hardware platforms, virtual sensors, and cloud-based sensors, plus installation and deployment.
Corelight Diagnostic Shell (with lab)	A hands-on demonstration of using the diagnostic shell and discussion of several commands useful for troubleshooting.
Corelight REST API (with lab)	An introduction to our REST API with several examples to monitor dataflow into your SIEM and manage configuration of the sensor.

CORELIGHT, INC. | INFO@CORELIGHT.COM

Deploying Corelight Fleet Manager	Fleet provides a unified portal to manage and monitor Corelight sensors. We'll demonstrate how to deploy and configure Fleet Manager.
Managing Fleet Manager	Using Corelight Fleet Manager to adjust sensor configuration, standardize policies, and enable packages at scale.
Incident Response	The power of Zeek becomes clear when used for incident response investigations. We'll complete a hands-on investigation, including file extraction, using only network data.
Threat Hunting	We'll use the MITRE ATT&CK matrix to guide our search for malicious activity, spanning back months using DNS, SMB, and SSH logs.
Network Operations	We'll find versions of software on our clients, monitor TLS certificate hygiene, and troubleshoot network routing issues.
Capture-The-Flag Exercise	Find artifacts of real-world attacks, assembling the storyline and workflow of the attack, with an instructor available to answer 1:1 questions.
Meta-Logs	We'll dive into logs that give a high-level overview, starting with the "conn" log before pivoting into the "files" log. Finally, we'll take a look at the "notice" and "weird" logs.
HTTP and DNS (with lab)	We'll combine the most common logs, HTTP and DNS, into a demonstration of a client's workflow, focusing on configurations and identifying anomalous activity.
SSL and x509 (with lab)	We'll review a normal TLS/SSL client connection, introduce JA3 and JA3S to fingerprint the client and host, then dive into the x509 log.
SMB, NTLM, and DCE_RPC (with lab)	This walkthrough will examine normal workflows of Windows clients and identify anomalous and malicious SMB activity.
Threat Hunting with Corelight Data	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.
Data Archival with JSON and TSV	This module compares JSON and TSV, two secondary formats for archival and cold storage of logs and introduces tools for filtering them.
Capstone CTF	Dig into real-world datasets with fresh knowledge, putting some of our tools and processes into action. An instructor answers 1:1 questions.