corelight

ONE DAY TRAINING

One Day Corelight / Zeek Training

This course takes incident responders, threat hunters and pen testers, who are new to Zeek and teaches them everything they need to know to start using this powerful tool. Typically delivered online, it balances lectures and lab exercises and covers the need for network monitoring, the implementation of Corelight sensors, and the value of Zeek data. The day ends with a CTF exercise designed to test the skills you've just learned.

COURSE MODULES

Intro to Zeek

We'll introduce Zeek through a recent tool that detects EternalBlue (and more), then cover the purpose of Zeek, the purpose of non-judgemental data, and how users can tailor Zeek to their needs.

Why Zeek? Why Corelight?

An overview for new users on Zeek vs.other network traffic data, and how Corelight enhances Zeek. Includes use cases from incident response, threat hunting, and zero-day exploits.

Corelight in Your Network

This interactive module covers common protocols, and data visibility across the network. This leads into an overview of SPAN ports, taps, and packet brokers, and ends with a walkthrough of exporting.

Use Cases

Incident Response: Through hands-on exercises, we'll complete an investigation, including file extraction, using only network data.

Threat Hunting: We'll use the MITRE ATT&CK matrix to search for months of malicious activity on our network.

NetOps: We'll discuss the Software log, strong SSL and certificate hygiene, and troubleshooting routing issues.

Capture The Flag competition

We'll apply Corelight data in a variety of scenarios, including internal hosts compromised by malware infections and externally-exposed hosts being compromised by zero-day exploits.
Participants will need speed and precision to find artifacts and assemble the attack's storyline and workflow. An instructor will answer 1:1 questions and guide students through the challenge questions.

CORELIGHT, INC. | INFO@CORELIGHT.COM