THREAT HUNTING WITH CORELIGHT

In this instructor-led course, you will learn how to use Corelight with the Elastic Stack for network security monitoring. The coursework culminates with a two-day capstone event in which you will perform a series of increasingly difficult hunting operations using the Corelight data. This capstone is instructor assisted to ensure that no one is left behind. By the end of the training, you will be able to use Corelight via Zeek (formerly Bro) data and the Elastic Stack to analyze your network traffic, sniff out threats, and respond appropriately.

LESSONS

All lessons include hands-on labs.

Passive operations and tapping
Learn the difference between active and passive operations and find out how to utilize different tapping technologies in order to weigh options and make the best choice for your environment.

Introduction to Zeek
Start with system setup, a comparison with Wireshark, and an ASCII logs overview. Then get up to speed with Zeek’s capabilities, including analyzing a packet capture and filtering and sorting data. Finish with a capture the flag exercise.

Zeek performance tuning
Get a walkthrough of the ways in which sensor engineers tune Zeek for optimal performance. Find out how to monitor incoming bandwidth, identify performance bottlenecks, and filter what Zeek captures.

Advanced Zeek
This lessons teaches operators how to use Zeek for hunting. Get an overview of scripting, the Zeek event engine, and frameworks. Then delve into the Intel framework and file extraction.

COURSE INFORMATION

Audience
Security analysts who are researching, building or leveraging Corelight as a part of their security monitoring program

Duration
5 days | 8 hours per day

Language
English

Prerequisites
Familiarity with Linux, networking, and network security concepts

Requirements
- An OpenSSH-compatible secure-shell client
- Stable internet connection
- Mac, Linux, or Windows
- Latest version of Chrome or Firefox (other browsers not supported)
- Disable any ad blockers and restart your browser before class

Continued on next page
THREAT HUNTING WITH CORELIGHT

LESSONS (CONTINUED)
All lessons include hands-on labs.

**Introduction to the Elastic Stack**
Learn about the products that make up the Elastic Stack and how they interoperate. After that, you’ll get an introduction to the Kibana UI and a deep-dive on each component that is relevant to a successful hunt.

**Data ingestion**
Learn more about the all-important step of moving data from Zeek to Elasticsearch in an efficient and scalable manner. Discover how to use Logstash and Beats, and how to enrich the data along the way.

**Visualizations and dashboards**
Visualizations are a powerful way to summarize a large set of data and spot anomalies. Learn all about how to use visualizations to tell a story about your data, and also how to build dashboards focused on protocols or specific use cases.

**Assisted hunt**
Put all the skills you’ve learned to work during this threat hunting exercise. Learn how to select the right tools, when to dig deeper, and follow proper incident response operations.