NETWORK SECURITY MONITORING CYBER OPERATOR

This instructor-led course is designed for operators that serve or are interested in serving as the "human-in-the-loop" to a suite of cybersecurity tools. While focused primarily on the best of breed open source security tools, the knowledge gained aims to be tool agnostic. You will learn to use the Elastic Stack along with security tools like Zeek (formerly Bro) and Suricata to perform full-spectrum threat detection and hunting. The course ends with a guided hunt capstone containing multiple scenarios — both as an individual hunter and as part of a team — that will engage the newly learned skills to find the adversary in the traffic.

LESSONS

All lessons include hands-on labs.

Introduction to packet analysis

This lesson will introduce operators to doing fine-grained packet analysis, using Berkeley Packet Filters, and addressing strategies to analyze packets at scale using Docket and Google Stenographer.

Protocol analysis with Zeek

This lesson introduces the Zeek protocol analyzer and teaches operators how to leverage Zeek for hunting. You will learn about Zeek data flow, Zeek logging, Zeek file types, and Zeek protocol analysis.

Intrusion detection systems (IDS)

This lesson will cover what message queuing is all about and how it is used. This lesson also introduces the leading IDS — Suricata — and cover when and how to employ an IDS to support hunt operations. You will look at signature writing, Suricata vs. Snort, and IDS dashboards within Kibana.

Continued on next page

COURSE INFORMATION

Audience

Cybersecurity operators who need to work as part of a team to analyze data to find bad actors lurking in their network as part of a machine-assisted, human-driven operation

Duration

5 days | 8 hours per day

Language

English

Prerequisites

- Familiarity with Linux, networking, and network security concepts
- Basic operational knowledge of Kibana
- Foundational Zeek knowledge

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

elastic

NETWORK SECURITY MONITORING CYBER OPERATOR

LESSONS (CONTINUED)

All lessons include hands-on labs.

Kibana UI for Security

This module walks you through the basics of Kibana architecture, how to create Visualizations and Dashboards, and use the Security app. You will get hands-on experience with searching through data and logs to perform network and host analyses, as well as performing a short guided hunt that simulates real-world activity.

Assisted hunt

This capstone lesson is designed to walk an operator through a series of hunt missions designed to expand their understanding of the hunt tools and techniques. You will learn to choose the right tool for each job, how to know when to dig deeper, response operations, and more before embarking on individual and team hunts. Hunts include: find the beacons, enemy objectives, applying the kill chain, and full-spectrum adversary detection.