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
Kibana for operators
This lesson builds on existing Kibana knowledge and teaches how to use Kibana to support hunting. You will learn about security-focused Beats and their dashboards, perform graph analytics, employ machine learning for threat hunting, and use alerts for automation.

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.