DEPARTMENT OF DEFENSE CYBER OPERATOR

This instructor-led course teaches network and endpoint security monitoring in a simple, practical way that builds incrementally. 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 2-day, guided hunt capstone containing multiple scenarios — both as an individual hunter and as part of a DoD team — that will engage the newly learned skills to find the adversary in the traffic.

This course focuses on the Department of Defense’s mission of threat hunting in unique contested networks.

LESSONS

All lessons include hands-on labs.

Linux foundations, management, and security
This introduction is designed to equip students with basic operational skills for the Linux command line, like file system layout, using Vim, viewing logs, package management, services, SELinux, and some administration. It is not intended to make them an expert, but to familiarize them with enough Linux to succeed.

Networking foundations
This module expands upon the OSI model to give a full analysis of protocols and encapsulation. This is complemented by advanced analysis and hunting techniques with the platform.

Packet analysis
This course will introduce Operators to fine-grained packet analysis and filtering and then address strategies to analyze packets at scale using Google Stenographer.

The Elastic Stack
The Elastic Stack is integral to network security monitoring. This lesson will provide an overview and introduction to the main Elastic Stack products: Elasticsearch, Kibana, Beats, and Logstash.

Continued on next page
DEPARTMENT OF DEFENSE CYBER OPERATOR

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

The Suricata Intrusion Detection System (IDS)
This lesson will introduce operators to 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.

Zeek protocol analyzer
An understanding of Zeek is a foundational skill for NSM. This lesson is designed to take an operator or analyst who has never used Zeek and bring them up to speed with its capabilities, like analyzing packets, commands, filtering and sorting, and more.

Kibana for operators
This lesson builds on the earlier Kibana training and teaches operators how to use Kibana to support them in their 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.

Platform architecture and engineering
This module covers the engineering overview for the platform along with the necessary administrative skills required for managing the build.

Endpoint detection and response
This module will introduce operators to Endpoint Detection and Response (EDR) with the platform. The material covers baselining, capturing volatile artifacts, and basic endpoint hunt operations.

Assisted hunt
This 2-day capstone module is designed to walk an operator through a series of individual and team-based hunt missions designed to expand their understanding of the hunt techniques.