NETWORK SECURITY MONITORING ENGINEER

This instructor-led course is focused around the deployment of the Elastic Stack in a security context, including how to implement the different parts of the Elastic Stack (Elasticsearch, Kibana, Beats, and Logstash) and how to tune performance. You will start with an overview of the Elastic Stack and its core components, and from there, build network security monitoring (NSM) sensors in a variety of configurations. By the end of the training, you will be able to build the Elastic Stack from the ground up to analyze the data sources from your network and various systems in order to paint a more complete security picture.

LESSONS

All lessons include hands-on labs.

Ansible
Building and configuring the sensors to use for NSM operations is done by completing a checklist of many tasks. The vast majority of these tasks are repeatable and can be completed with "Configuration Management". This lesson teaches the basics of Ansible for configuration management. You will explore Ansible, learning about environment setup, ad-hoc commands, playbooks, modules, variables, templates, and more.

Zeek install, operate, and maintain
This lesson is designed to familiarize sensor engineers with the various ways to install and configure Zeek (formerly Bro). It will also briefly cover ongoing maintenance that should be performed against an installation. Topics covered include installation and deployment options, clustering, capture methods, and more.

Continued on next page

COURSE INFORMATION

Audience
Security engineers who are responsible for installing, operating, and maintaining the Elastic Stack and network security monitoring platforms

Duration
10 days | 8 hours per day

Language
English

Prerequisites
There are no prerequisites for this course.

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
NETWORK SECURITY MONITORING ENGINEER

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

Advanced Zeek
This lesson builds on existing Zeek knowledge and teaches operators how to leverage Zeek for hunting. You will learn about Zeek scripting, the Zeek Event Engine, the Intel Framework, and the Files Framework.

Passive operations and tapping
It is important that a sensor engineer understands what a passive system is (versus active) and what that actually means. This lesson will clearly define the difference and explain how to utilize different tapping technologies so that students can weigh their options and make the best choice for their environment.

CAPES install, operate, and maintain
CAPES is a self-hosted incident response service hub, providing IR management, communication, documentation, VoIP, collaborative workspaces, indicator enrichment, data analysis, and data visualization. This lesson is designed to take an operator or analyst who has never used the CAPES technology stack and bring them up to speed with its capabilities.

Elastic Stack install, operate, and maintain
This lesson is designed to familiarize sensor engineers with the various ways to install, configure, tune, and secure the different pieces of the Elastic Stack: Elasticsearch, Kibana, Beats, and Logstash.

Suricata rule management and tuning
This lesson is designed to provide an engineer with the foundational knowledge required to: maintain up-to-date rulesets, create custom rules, and manage the performance of a Suricata sensor.

Sensor troubleshooting
This lesson is designed to provide an engineer with the foundational knowledge required to troubleshoot and correct sensor or configuration errors.

Engineer capstone event
This capstone will have an engineer build a sensor from the ground up, and will then have to troubleshoot and fix errors introduced to their sensors to return them to a working state.