THREAT HUNTING WITH KIBANA

This course is designed for security analysts interested in using Kibana to hunt threats to their data and systems. You will start with an introduction to threat hunting, including how it's different from other security analysis processes, and then move onto an introduction to the Elastic Stack and the powerful set of tools it offers. You will then learn essential Kibana features for analyzing security data, followed by an in-depth look at our network data sources, including learning about ways to enrich them. You will then learn about threat hunting philosophy, workflow, models, techniques and how it can help improve the effectiveness of security operations center. All of this will then be followed by a guided hunt exercise to put your new skills to the test.

LESSONS

All lessons include a hands-on lab.

Introduction

Start by looking at today's threat landscape to better understand advanced persistent threats and the need for threat hunting. Explore fundamentals of threat hunting and how it's different from other security analysis processes. Get an overview of different components of Elastic Stack. Learn about our security data sets and how to use essential Kibana features for analyzing them.

Network data

Start with an overview of network data and how it can be useful in security analysis. Take an in depth look at data generated by Zeek NSM and Suricata IDS. Explore the concept of flow and the benefits of collecting and analyzing flow data.

Continued on next page

COURSE INFORMATION

Audience
Security analysts

Duration
2 days | 8 hours per day

Language
English

Prerequisites

- No prior knowledge of the Elastic Stack required
- Familiarity with basic networking and network security, as well as logging and incident response concepts

Requirements

- 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

THREAT HUNTING WITH KIBANA

LESSONS (CONTINUED)

All lessons include a hands-on lab.

Data enrichment

Understand the value of enrichment during the data analysis process, as well as the different objects that can be enriched using different sources during different stages of your ETL process. Explore various enrichment tools and the value they offer in security analysis.

Threat hunting

Dive deeper into threat hunting, its philosophies, and the benefits of undertaking such an initiative. Learn the workflow, models, and techniques for hunting threats.

Guided hunt

Challenge yourself in this actual exercise of threat hunting with instructor guidance (as needed).