KIBANA SECURITY ANALYST

In this course we will overview the architecture of Kibana. Then we will learn how the Elastic Common Schema makes out data easier to correlate data across different data sources. We will touch on visualizations and dashboards and how they represent our network data. Finally, we will finish it up with a short guided hunt to bring it all together.

This course is part of the Elastic Network Security Analyst Learning Plan. Please review the pre-reqs section for additional information.

LESSONS

All lessons include a hands-on lab.

Kibana basics

Learn how Kibana views the data from Elasticsearch and how we correlate our log field types from our previous lessons in Zeek and Suricata.

Elastic common schema

Learn how ECS defines a common set of fields to be used when storing event data in Elasticsearch and how they map from our original Zeek and Suricata Fields.

Searching

Understand the basics of performing a query against our network security data.

Visualizations

Learn how to leverage the fields and searching lessons we just learned about to create powerful visualizations that will help analysts understand what is happening on the network.

Dashboards

Learn the basics of dashboards as a collection of visualizations. We will share some tips for creating useful dashboards for Zeek and Suricata data.

Bringing it all together

We will use kibana in a short guided hunt to reinforce the previous learning objectives.

COURSE INFORMATION

Audience

Network Analysts
Security Engineers

Duration

8 hours

Language

English

Prerequisites

- Linux Fundamentals
- Packet Analysis
- Network Protocol Analysis
- Intrusion Detection System (IDS) log analysis with Suricata
- Network Metadata log analysis with Zeek
- Kibana Security Analyst

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