ELASTIC SECURITY FOR SIEM

This course is built for analysts who utilize the Elastic Security for SIEM solution. Elastic Security for SIEM walks you through the architecture behind the Elastic Stack, Fleet, and Elastic Agent. You will then learn how to create visualizations and dashboards and how to use Lens before diving into the Security App. Finally, you will conduct a threat hunting capstone exercise to tie everything together.

LESSONS

Some lessons include a hands-on lab.

Stack Overview

Identify the various components of the Elastic Stack, as well as how data flows through it. Gain an understanding of the different data sources utilized in security use cases. Recognition of Fleet architecture and how it manages Elastic Agents. Configure an Agent policy, install integrations, and deploy an Elastic Agent.

Elastic Common Schema

Examine the application of the Elastic Common Schema (ECS). Discuss the fundamentals of logging and data structures. Identify how ECS normalizes data.

Security App

Recognize the capabilities of Attack Discovery and AI empowered workflows. Identify the use cases for AI Assistant. Summarize relevant information within the Host, Network, and User pages. Identify how the Detection Engine searches activity and generates alerts. Construct custom detection rules with KQL, EQL, Lucene and ES|QL. Analyze Alerts that are generated from Detection rules. Correlate relevant data using Timeline and track security events using Cases. Monitor security related events with Dashboards in the Security App.

Continued on next page

COURSE INFORMATION

Audience

- Professionals who use Elastic Security as their SIEM.
- Cybersecurity analysts who are responsible for monitoring and investigating logs in a SOC environment.

Duration

24 hours

Language

English

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

ELASTIC SECURITY FOR SIEM

LESSONS

Some lessons include a hands-on lab.

Discover
Discuss how Kibana displays data in Discover and customize the Discover interface to search for data. Construct queries using KQL/Lucene to view relevant data.

Visualizations
Interpret data within visualizations. Identify best practices for creating aggregation-based visualizations. Create aggregation-based and Lens visualizations for security use cases. Demonstrate the use of additional features in Lens.

Dashboards
Interpret data using relevant Dashboards. Demonstrate best practices for pivoting between apps in Kibana. Identify best practices for creating Dashboards. Create Dashboards for security use cases.

Hunt capstone
Work through a series of hunt missions designed to gain an understanding of hunt tools and techniques. 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.

COURSE INFORMATION

Prerequisites
A basic understanding of:

Networking
- TCP/IP
- Common ports and protocols
- Common networking devices (routers, switches, firewalls)

Common Network Monitoring Tools
- IDS (Suricata)
- Zeek
- Packet Capture Tool

Operating Systems
- Windows and Linux
- File systems and permissions
- Command line navigation

Vulnerabilities and Exploit Methodology
- Reconnaissance
- Command and Control (C2)
- Data Exfiltration

elastic