ELASTIC SECURITY FOR ENDPOINT

This course is built for analysts who utilize the Elastic Security for Endpoint solution. Elastic Security for Endpoint walks you through the components behind the Elastic Stack, Fleet, and Elastic Agent. You will then be familiarized with Elastic Security and using visualizations, dashboards, and other components of the Security App to triage alerts and investigate events in Timeline. Afterwards, you will learn about Elastic Defend and other security integrations. Finally, you will conduct a threat hunting capstone based on concepts covered during the course to reinforce the lessons learned.

LESSONS

Includes a hands-on lab.

Elastic Stack overview
Refresher of the Elastic Stack, how data flows through it, and some security use case data sources. Gain an understanding of Fleet, Fleet Server, and Elastic Agent. Configure an Agent policy, install integrations, and deploy an Elastic Agent.

Security application
Summarize relevant information within the Host, Network, and User pages. Construct custom detection and exception rules with KQL, EQL, Lucene, and ES|QL. Analyze Alerts that are generated from Detection rules. Monitor security related events with Dashboards in the Security App.

Elastic defend
Identify the type of protections available through Defend. Demonstrate the ability to modify and fine tune Protection Policies and identify additional Defend policy management options.

Elastic security enrichments
Leverage OSquery to retrieve host information to enrich relevant data. Discuss other security-centric integrations.

Threat hunting
Work through a series of hunt events and challenges designed to gain an understanding of hunt techniques. Learn to choose an appropriate action for each job, how to know when to dig deeper, response operations, and more before embarking on individual hunts.

COURSE INFORMATION

Audience
Security analysts who are responsible for monitoring and investigating host based alerts sourced from Elastic Endpoint protection capabilities

Duration
24 hours

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

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

Networking
- Common ports and protocols
- Common Networking devices

Vulnerabilities and Exploit Methodology
- Reconnaissance
- Command and control
- Persistence techniques

Language
English

elastic