ELASTIC ENDGAME CORE + ADVANCED THREAT HUNTING

Endgame Core:

Elastic Endgame gives you the power to keep your endpoints safe from attack, as well as unparalleled visibility into any threat in your environment. This instructor-led course teaches you how to install, configure, and manage an Elastic Endgame solution. You will learn endpoint detection and response workflows as well as how to hunt using the platform. The coursework culminates with a Hunt module, in which you will discover and capture flags, simulating tactics from potential malicious activity. You will be able to keep your infrastructure safe from attacks, and have full visibility into how the attacks were initiated so they can be prevented in the future.

Advanced Threat Hunting:

New cybersecurity threats appear every day, as adversaries are always evolving and finding new ways to attack your network. This instructor-led course focuses on advanced threat hunting scenarios using the Elastic Endgame platform. You will learn about various types of hunts — including data-driven, technique-driven and intel-driven hunting. You will then learn how to perform these hunt types by exploring built-in investigations and analytics as well as Event Query Language (EQL) capabilities. After completing this course, you'll be able to employ these proactive methods to identify advanced threats more quickly and respond to them easily.

LESSONS

Some lessons include a hands-on lab.

Capture the flag

Leverage training from the previous modules to discover and capture flags, simulating tactics from potential malicious activity.

Continued on the next page

COURSE INFORMATION

Audience

Security analysts who are responsible for implementing an Elastic Endgame solution.

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

- Familiarity with Linux and Windows operating systems
- Basic understanding of cyber security concepts and terms

Language

English

Duration

5 days | 40 hours

elastic

ELASTIC ENDGAME CORE + ADVANCED THREAT HUNTING

LESSONS

Some lessons include a hands-on lab.

Core concepts

Gain an understanding of host-based threat hunting fundamentals. Get familiar with Event Query Language (EQL), including its syntax, order of operations, and data pipes. Learn about the various use cases of Investigations and Resolver View as well as how they can be utilized to conduct hunts with Elastic Endgame.

Types of Hunts

Learn about the different types available: data-driven, TTP-driven, and intelligence-driven. Understand how to measure the success of a hunt. Perform intelligence-driven hunts, turning intelligence reports into EQL queries. Explore data-driven hunting by manipulating data collected with Elastic Endgame and turning analytics into EQL queries. Perform TTP-driven hunts, translating MITRE ATT&CK techniques into EQL queries.
Hands-on lab