ELASTIC ENDPOINT SECURITY 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 Endpoint Security 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
All lessons include hands-on components.

What is a hunt and how do we do it?
Learn what a hunt is, as well as the different types available: data-driven, TTP-driven, and intelligence-driven. Understand how to measure the success of a hunt. Get familiar with Event Query Language (EQL), including its syntax, order of operations, and data pipes. Explore data-driven hunting with Endpoint Security by manipulating collected data, turning analytics into EQL queries, and then looking outside of analytics.

Advanced EQL use cases
Perform intelligence-driven hunts, turning intelligence reports into EQL queries. Perform TTP-driven hunts, translating MITRE ATT&CK techniques into EQL queries.

COURSE INFORMATION

Audience
Security analysts who are responsible for threat hunting on the Elastic Endpoint Security solution

Duration
Classroom - 2 days | 8 hours per day
Virtual - 4 days | 4 hours per day

Language
English

Prerequisites
Complete either of the following:
• Elastic Endpoint Security
• Elastic Endpoint Security Triage and Response

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