ELASTIC ENDPOINT SECURITY

Elastic Endpoint Security 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 Endpoint Security solution. You will learn endpoint detection and response workflows as well as how to hunt using the platform. The coursework culminates with a full-day capture-the-flag exercise in which you will discover and capture flags, simulating tactics from potential malicious activity. After completing this course, 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.

LESSONS
All lessons include hands-on components.

Installation, deployment, and protection policies

Alert triage and tuning, endpoint detection and response

Hunt
Learn how to identify outliers in an environment. Explore advanced tradecraft analytics and how to enumerate malicious activity. Use Artemis and Event Query Language (EQL) to search for and identify “living off the land” techniques as well as advanced adversary tradecraft. Leverage the API for extensibility of the platform and customization of data collection. Utilize the Endpoint Security Shell — a custom python tool built to utilize the API and provide cutting-edge forensic capabilities.

Capture the flag
Leverage training from the previous three days to discover and capture flags, simulating tactics from potential malicious activity.