ELASTIC MACHINE LEARNING FOR CYBERSECURITY

Overview
Network security analysts have the daunting daily task of identifying potential threats in an endless ocean of network security data. In this class, you'll see how Elastic machine learning can help you quickly and efficiently detect those threats, regardless of how much data you need to analyze. Elastic machine learning features can automatically model the behavior of your network security data trends, periodicity, and more, all in real time to identify issues faster, streamline root cause analysis, and reduce false positives. After completing this course, you'll be able to use the powerful features of Elastic machine learning for identifying anomalies in your security data.

Audience

Duration
2–3 hours

Language
English

Prerequisites
• We recommend you have taken Kibana Data Analysis and Elasticsearch Engineer I or possess equivalent knowledge.

• General familiarity around security log data

• Basic networking knowledge

Requirements
• Stable internet connection

• Mac, Linux, or Windows

• Latest version of Chrome or Firefox (Safari is not 100% supported)

• Due to virtual classroom JavaScript requirements, we recommend that you disable any ad-blockers and restart your browser before class.
ELASTIC MACHINE LEARNING FOR CYBERSECURITY

Modules

Introduction to Elastic Machine Learning
- Learn about the Elastic Stack machine learning functionality and discuss security use cases for machine learning. Explore the security threat landscape and see how machine learning can help. Get familiar with our security dataset.

- Hands-On Lab: Students will explore and get familiar with our security dataset.

Configuring Elastic ML
- Configure Elastic machine learning jobs for detecting anomalies in our security dataset.

- Hands-On Lab: Students will learn how to configure machine learning jobs for detecting suspicious login activity within the SSH Logs dataset.

Detecting DNS Data Exfiltration
- Explore DNS Data Exfiltration use case and how Elastic can help detect it. Also discuss creating advanced jobs, configurations and navigation of results.

- Hands-On Lab: Students will learn to use Elastic machine learning to detect DNS data exfiltration from within a private network.