This course is only offered privately. Please contact your sales representative or email us at sales@elastic.co to schedule a training.

Overview
This instructor-led course is designed for analysts that currently use, or are interested in using, the Elastic Stack for security event collection and analytics. You will start with an overview of the Elastic Stack, exploring the various components and some of the use cases they can serve. The remainder of this course will take an in-depth look at several security related data sources and how to gain value from them with the Elastic Stack. As you learn about these data sources, we will mix in instruction on the various components of Kibana, including basic discovery, visualizations and dashboards, and advanced components like Graph and machine learning. After completing each module, you will apply what you have learned in a series of hands-on labs. By the end of the training, you will be able to use the Elastic Stack to analyze the data sources from your network and various systems in order to paint a more complete security picture.

Audience
Security analysts who are researching, building, or leveraging search and analytics solutions using the Elastic Stack

Duration
3 Days | 8 hours per day

Language
English

Prerequisites
No prior knowledge of the Elastic Stack required

Requirements
• Stable internet connection
• Mac, Linux, or Windows
• A modern web browser
ELASTIC SECURITY ANALYTICS

Modules

Day 1

Introduction to the Elastic Stack
• Learn about the products that make up the Elastic Stack and when you might choose one tool vs. another.

Threat Detection
• Review common approaches to threat hunting and learn about how the tools in the Elastic Stack can help compliment these proven methods.

Bro Basics
• Understand what Bro data is, how to capture it, and leverage it for security operations.
• Hands-On Lab: Explore Bro data from the command line and move to analyzing the same dataset using Kibana.

Suricata IDS
• Suricata is a popular Intrusion Detection System (IDS). Learn how to analyze the alerts and flow data that it can provide.
• Hands-On Lab: Analyze alerts and flow data generated from Suricata.

Day 2

Windows Host Data
• Learn all about how Windows stores event logs and how to use the Elastic Stack to centralize and search them.
• Hands-On Lab: Analyze Windows host logs that have been collected using Winlogbeat.

Linux Host Data
• Review common log collection points within Linux operating systems and how to analyze them for threats using the Elastic Stack.
• Hands-On Lab: Analyze a variety of Linux host logs that have collected using Filebeat and Auditbeat.

Enriching Host Data
• Gain insight into common approaches for enriching host data, both pre and post collection. This will be a high-level overview of the approaches available.
• Hands-On Lab: Analyze Windows host logs that have been enriched using Sysmon.
ELASTIC SECURITY ANALYTICS

Day 3

Guided Analysis

• Spend a full day applying the concepts that you have learned in class. This is designed to be very hands-on and flexible to the needs and desires of the students.

• The typical flow is to spend 30 minutes looking for anomalies in the data and then regroup and review as a class what everyone has found.