ELASTIC SIEM FUNDAMENTALS

A powerful SIEM is one of the most important tools a security analyst can wield. In this self-paced, on-demand course, you’ll learn how to leverage Elastic SIEM to drive your security operations and threat hunting. This course is designed for security analysts and practitioners who have used other SIEMs or are familiar with SIEM concepts. As a security analyst, you will learn how to stand up and use Elastic SIEM, including exploring its interface, configuring data ingestion, and leveraging prebuilt machine learning jobs to hunt down anomalies. By the end of this course, you will be ready to use Elastic SIEM to detect threats to your infrastructure, enabling you to protect and respond at the speed of Elasticsearch.

LESSONS

All lessons include a hands-on lab.

Elastic SIEM UI
Get an introduction and an overview to Elastic SIEM. Learn about the user interface and how to use it in analysis of host-related and network-related security events as part of alert investigations or interactive threat hunting.

Getting SIEM data in
Learn how to populate the SIEM app with hosts and network security events using various beats. Understand how Elastic Common Schema (ECS) enables SIEM to work with custom and third-party data sources in addition to those supported by Beats.

Anomaly detection
Discover the potential of using machine learning anomaly detection functionality within the SIEM app to complement analysis. Get an overview of prebuilt jobs that can automatically detect file system and network anomalies on hosts.

COURSE INFORMATION

Audience
Security Analysts and practitioners that has a basic understanding of SIEM in general

Duration
2-3 hours

Language
English

Prerequisites
Basic understanding of what a SIEM is and typical data involved

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

elastic.co | © 2020 Elasticsearch B.V. All rights reserved.