ANOMALY DETECTION AND ALERTING ON LOG DATA

Overview
Indexing and storing logs in Elasticsearch is an important step in achieving visibility into your organizational log data, but what good is the data if it's not actionable? In this course, you will learn how to leverage the Elastic Stack machine learning and alerting features to help you keep a closer eye on your logs. You will learn how to configure machine learning jobs and watches to get alerted when anomalies occur. After completing this course, you’ll be to more easily focus on important issues that could otherwise be missed within gigabytes of logs.

Audience
Data Analysts, Software Developers and Engineers, Data Architects, System Administrators, DevOps

Duration
Virtual Classroom - 1 day | 2–3 hours

Language
English

Prerequisites
• We recommend you have taken Elasticsearch Engineer I and Elasticsearch Engineer II or possess equivalent knowledge. Engineer I and Engineer II teach the concepts that are the foundation upon which all specializations are built.

• We also recommend that you have taken Logging Fundamentals (another module within this specialization).

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.
ANOMALY DETECTION AND ALERTING ON LOG DATA

Modules

The Use Case for Anomaly Detection and Alerting
• Learn how to set up basic single metric machine learning jobs and threshold alerts to get started with machine learning and alerting.
  • Hands-On Lab

From Anomaly Detection to Forecasting
• Learn about the power of machine learning by configuring multi-metric jobs and creating forecasts to predict future behavior.
  • Hands-On Lab

Alerting Deep Dive
• Learn how to configure watches that go beyond basic threshold alerts to get alerted on anomalies that are important to your organization.
  • Hands-On Lab

Tying It All Together
• Apply the skills you have learned to visualize and explore anomalies in a log dataset.
  • Hands-on Lab