Cortex™ XDR 3.2: Investigation and Response

Course Description

This instructor-led course teaches you how to use the Incidents pages of the Cortex XDR management console to investigate attacks. It explains causality chains, detectors in the Analytics Engine, alerts versus logs, log stitching, and the concepts of causality and analytics.

You will learn how to analyze alerts using the Causality and Timeline Views and how to use advanced response actions, such as remediation suggestions, the EDL service, and remote script execution.

Multiple modules focus on how to leverage the collected data. You will create simple search queries in one module and XDR rules in another. The course demonstrate how to use specialized investigation views to visualize artifact-related data, such as IP and Hash Views. Additionally, it provides an introduction to XDR Query Language (XQL). The course concludes with Cortex XDR external-datacollection capabilities, including the use of Cortex XDR API to receive external alerts.

Prerequisites

Participants must have completed EDU-260 (Cortex XDR: Prevention and Deployment).

Course Duration

2 days

Objectives

Successful completion of this instructor-led course with hands-on lab activities should enable participants to:

- Investigate and manage incidents
- Describe the Cortex XDR causality and analytics concepts
- Analyze alerts using the Causality and Timeline Views
- Work with Cortex XDR Pro actions such as remote script execution
- Create and manage on-demand and scheduled search queries in the Query Center
- Create and manage the Cortex XDR rules BIOC and IOC
- Working with Cortex XDR assets and inventories
- Write XQL queries to search datasets and visualize the result sets
- Work with Cortex XDR's external-data collection

Course Outline

1. Cortex XDR Incidents
2. Causality and Analytics Concepts
3. Causality Analysis of Alerts
4. Advanced Response Actions
5. Building Search Queries
6. Building XDR Rules
7. Cortex XDR Assets
8. Introduction to XQL
9. External Data Collection

Who Should Attend

- Cybersecurity analysts and engineers
- Security operations specialists