Course Outline

Palo Alto Networks: Cortex XDR 3.0: Investigation and Response (EDU-262)

Course Summary

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. You will learn how to use specialized investigation views to visualize artifact-related data, such as IP and Hash Views. Additionally, an introduction to XDR Query Language XQL is provided. The course concludes with Cortex XDR external data collection capabilities, including the use of Cortex XDR API to receive external alerts.

Objectives

At the end of this course, students will be able 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 the 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
- Investigate artifacts using the specialized views IP View and Hash View
- Write XQL queries to search datasets and visualize the result sets
- Work with Cortex XDR's external data collection

Topics

- Cortex XDR Incidents
- Causality and Analytics Concepts
- Causality Analysis of Alerts
- Advanced Response Actions
- Building Search Queries
- Building XDR Rules
- Building XDR Rules
- Introduction to XQL
- External Data Collection

Audience

Cybersecurity analysts and engineers and security operations specialists, as well as administrators and product deployers.

Prerequisites

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

Duration

Two days