Cortex XDR: Investigation and Response (EDU-262)

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 analyse 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 demonstrates how to use specialised investigation views to visualise 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 data collection capabilities, including the use of Cortex XDR API to receive external alerts.

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**

› **Analyse 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 Centre**

› **Create and manage the Cortex XDR rules BIOC and IOC**

› **Work with Cortex XDR assets and inventories**

› **Write XQL queries to search datasets and visualise the result sets**

› **Work with Cortex XDR's external-data collection**

Target Audience

› **Cybersecurity Analysts**

› **Cybersecurity Engineers**

› **Security Operations Specialists**

Prerequisites

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

Course Outline:

Day 1

› **Cortex XDR Incidents**

› **Causality and Analytics Concepts**

› **Causality Analysis of Alerts**

› **Advanced Response Actions**

› **Building Search Queries**

Day 2

› **Building XDR Rules**

› **Cortex XDR Assets**

› **Introduction to XQL**

› **External Data Collection**

Scope

› **Level:** Advanced

› **Duration:** 2 days

› **Format:** Lecture and hands-on labs

› **Platform support:** Cortex XDR Pro per Endpoint

Palo Alto Networks Education

The technical curriculum developed and authorised by Palo Alto Networks and delivered by Exclusive Networks as a Palo Alto Networks Authorised Training Partner helps provide the knowledge and expertise that prepare you to protect our digital way of life. These trusted certifications validate your knowledge of the Palo Alto Networks product portfolio and your ability to help prevent successful cyberattacks and safely enable applications.

View our latest training schedule.

› Visit: **https://training.exclusive-networks.com/**

› Select your country in the top right

› Choose Palo Alto Networks in the Vendor options, and hit search.