PALO ALTO NETWORKS: CORTEX™ XDR: INVESTIGATION AND RESPONSE (EDU-262)

Course Code: 821506

Learn causality chains, detectors in the Analytics Engine, alerts versus logs, log stitching, and the concepts of causality and analytics.

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-data collection capabilities, including the use of Cortex XDR API to receive external alerts.

What You'll Learn

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
- 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

Who Needs to Attend

- Cybersecurity analysts and engineers
- Security operations specialists

Prerequisites

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

skillsoft
global
knowledge™

PALO ALTO NETWORKS: CORTEX™ XDR: INVESTIGATION AND RESPONSE (EDU-262)

Course Code: 821506

CLASSROOM LIVE	$2,600 CAD	2 Day

Classroom Live Outline

- Module 1: Cortex XDR Incidents
- Module 2: Causality and Analytics Concepts
- Module 3: Causality Analysis of Alerts
- Module 4: Advanced Response Actions
- Module5: Building Search Queries
- Module 6 : Building XDR Rules
- Module 7: Investigation Views
- Module 8: Introduction to XQL
- Module 9: External Data Collection

skillsoft
global
knowledge™

PALO ALTO NETWORKS: CORTEX™ XDR: INVESTIGATION AND RESPONSE (EDU-262)

Course Code: 821506

VIRTUAL CLASSROOM LIVE	$2,600 CAD	2 Day

Virtual Classroom Live Outline

- Module 1: Cortex XDR Incidents
- Module 2: Causality and Analytics Concepts
- Module 3: Causality Analysis of Alerts
- Module 4: Advanced Response Actions
- Module5: Building Search Queries
- Module 6 : Building XDR Rules
- Module 7: Investigation Views
- Module 8: Introduction to XQL
- Module 9: External Data Collection

Aug 7 - 8, 2025 | 9:00 AM - 5:00 PM EDT

Oct 16 - 17, 2025 | 8:30 AM - 4:30 PM EDT

Dec 11 - 12, 2025 | 9:00 AM - 5:00 PM EST

PALO ALTO NETWORKS: CORTEX™ XDR: INVESTIGATION AND RESPONSE (EDU-262)

Course Code: 821506

PRIVATE GROUP TRAINING	2 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 7/1/2025 9:22:08 AM