WE GET HOW TO PROVIDE YOU WITH THE SKILLS YOU NEED FOR XDR.

CDW Amplified™ Information Security

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

The Palo Alto Networks Cortex XDR: Investigation and Response course teaches participants 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.

Palo Alto Networks Cortex XDR: Investigation and Response can help you:

- Maximize ROI
- Acquire Skills
- Prepare for Certification

Course Overview

The Palo Alto Networks Cortex XDR: Investigation and Response course combines instructor-led training and interactive hands-on labs to teach students 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 concludes with Cortex XDR external-data collection capabilities, including the use of Cortex XDR API to receive external alerts. The training will help you to:

- Differentiate the architecture and components of Cortex XDR
- Investigate and manage incidents
- Work with Cortex XDR Pro actions such as remote script execution
- Create and manage the Cortex XDR rules BIOC and IOC
- Work with Cortex XDR assets and inventories
- Write XQL queries to search data sets and visualize the result sets
- Work with Cortex XDR's external data collection

CDW is an Authorized Training Partner of Palo Alto Networks. All courses are delivered and taught by certified instructors through CDW's workforce development arm, Focal Point Academy. The technical curriculum has been developed and authorized by Palo Alto Networks and helps provide the knowledge and expertise to prepare you to protect your digital way of life.

Target Audience and Prerequisites

This course is ideal for cybersecurity analysts, engineers and security operations specialists.

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

COURSE SNAPSHOT

- **Level:** Advanced
- **Duration:** 2 days
- **Format:** Lecture and hands-on labs
- **Platform support:** Palo Alto Networks Cortex XDR Pro per Endpoint

CDW GETS PALO ALTO NETWORKS

Palo Alto Networks enables you to secure access, protect users and applications, and control data – from anywhere. With our deep expertise in providing Palo Alto Networks solutions, CDW can assist with all aspects of your Palo Alto Networks environment.

In addition to deep services expertise, CDW is a Palo Alto Networks Authorized Training Partner. Our instructors have been certified by Palo Alto Networks, having demonstrated exceptionally high levels of technical and presentation skills.

Furthermore, CDW has been named Palo Alto Networks State, Local and Education Government Partner of the Year, Federal Partner of the Year, Americas Partner of the Year, Global Partner of the Year and is a Diamond Innovator Partner.

CDW's full lifecycle of Services can support your organization no matter where you are on your journey

Design → Orchestrate → Manage → On-Premises → On-Journey → Cloud-Based

CDW AMPLIFIED™ SERVICES

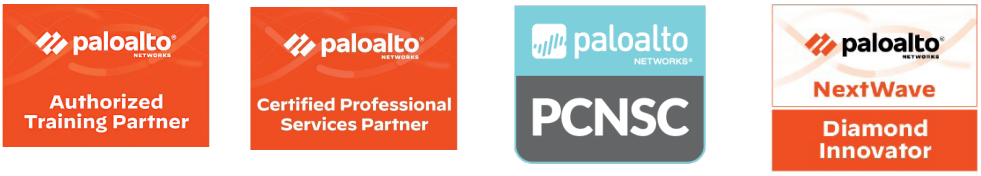
Course Modules

The Cortex XDR: Investigation and Response course includes the following modules:

Course Module	Module Name
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

Certifications

CDW has achieved numerous certifications from Palo Alto Networks, including:



Proofpoints

2021

Global Partner of the Year

5x

Americas Partner of the Year

48

Trained Palo Alto Networks Services personnel

2,600+

Palo Alto Networks customers

2,000+

Palo Alto Networks field service projects implemented

paloalto NETWORKS

Services-KS-060322

Contact your CDW account team or email authorizedtraining@cdw.com.

CDW AMPLIFIED™ SERVICES