paloalto NETWORKS | CYBERSECURITY PARTNER OF CHOICE

Cortex XDR: Investigation and Analysis

XDR is the industry's most powerful extended detection and response platform. You will gain hands-on expertise in endpoint management, case management, forensic analysis and platform automation. Throughout this course, you will explore the key features of Cortex XDR.
This course is designed to enable you to:

- Investigate cases, analyze key assets and artifacts, and interpret the causality chain.
- Query and analyze logs using XQL to extract meaningful insights.
- Utilize advanced tools and resources for comprehensive case analysis.

Course Modules

1 - Introduction to Cortex XDR

2 - Endpoints

3 - XQL

4 - Alerting and Detection

5 - Vulnerability & Forensics

6 - Platform Automation

7 - Case Management

8 - Dashboards & Reports

Scope

- **Duration: 2 days**
- **Format: Lecture and hands-on simulations**
- **Platform support: Cortex**

Objectives

The course is designed to enable cybersecurity professionals, particularly those in SOC/CERT/CSIRT and Security Analysts roles, to use XDR.

The course reviews XDR intricacies, from fundamental components to advanced strategies and techniques, including skills needed to navigate case management, platform automation, and orchestrate cybersecurity excellence.

Target Audience

This course is for a wide range of security professionals, including SOC, CERT, CSIRT, and XDR analysts, managers, incident responders, and threat hunters. It is also well-suited for professional-services consultants, sales engineers, and service delivery partners.

Prerequisites

Participants should have a foundational understanding of cybersecurity principles and experience with analyzing incidents and using security tools for investigation.

Palo Alto Networks Education

The technical curriculum developed by Palo Alto Networks and delivered by Palo Alto Networks Authorized Training Partners helps provide the knowledge and expertise you need to protect our digital way of life. Our trusted certifications validate your knowledge of the Palo Alto Networks product portfolio and your ability to help prevent successful cyberattacks.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: **+1.408.753.4000**
Sales: **+1.866.320.4788**
Support: **+1.866.898.9087**

www.paloaltonetworks.com