paloalto NETWORKS | CYBERSECURITY PARTNER OF CHOICE

Cortex XDR: Security Operations and Integration

This 3-day instructor-led course provides in-depth training on Cortex XDR, Palo Alto Networks' powerful extended detection and response platform. You will gain hands-on expertise in security operations, incident investigation, and system optimization to effectively protect modern environments. Throughout this course you will explore the key features of Cortex XDR.

This course is designed to enable you to:

- Describe the role of Cortex XDR components, including endpoint agents, XDR collectors, NGFWs, and Broker VMs, in securing networks and devices.
- Utilize XQL to query and analyze logs for effective data ingestion and threat detection.
- Design and implement workflows to streamline security operations.
- Apply External Dynamic Lists and indicator rules to enforce security policies.

Course Modules

0 - Course Overview

1 - Overview of Cortex XDR

2 - Software Components

3 - Integrations

4 - XQL

5 - Detection Engineering

6 - System Optimization

7 - Dashboards and Reports

Scope

- **Duration: 3 days**
- **Format: Lecture and hands-on labs**
- **Platform support: Cortex**

Objectives

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

The course reviews XDR intricacies, from fundamental components to advanced strategies and techniques, including skills needed to configure security integrations, develop workflows, manage indicators, and optimize dashboards for enhanced security operations.

Target Audience

SOC/CERT/CSIRT/XDR engineers and managers, MSSPs and service delivery partners/system integrators, security consultants and sales engineers.

Prerequisites

Attendees should possess a solid understanding of cybersecurity principles, including network and endpoint security concepts.

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 cyberattack.

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