paloalto NETWORKS | CYBERSECURITY PARTNER OF CHOICE

Cortex® XSIAM for Security Operations and Automation (EDU-270)

XSIAM is the industry's most comprehensive security incident and asset management platform, offering extensive coverage for securing and managing infrastructure, workloads, and applications across multiple environments.

Throughout this course, you will explore the key features of Cortex XSIAM.

This course is designed to enable you to:

- Deploy, configure, and install XDR agents and configure Agent Groups and profiles
- Investigate incidents, examine assets and artifacts, and understand the causality chain
- Create correlation rules, use XQL to query logs, and analyze incidents using available tools and resources

Course Modules

1 - Introduction to Cortex XSIAM
2 - Elements of Security Operations
3 - Maturity Model
4 - Agent Deployment and Configuration
5 - Data Source Ingestion
6 - Visibility
7 - Data Model
8 - Analytics
9 - Alerting and Detecting
10 - Attack Surface Management
11 - Automation
12 - Incident Handling / SOC

Scope

- Duration: 4 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 Security Engineering roles, to use XSIAM.

The course reviews XSIAM intricacies, from fundamental components to advanced strategies and automation techniques, including skills needed to navigate incident handling, optimize log sources, and orchestrate cybersecurity excellence.

Target Audience

SOC/CERT/CSIRT/XSIAM engineers and managers, MSSPs and service delivery partners/system integrators, internal and external professional-services consultants and sales engineers, incident responders and threat hunters.

Prerequisites

Participants must be familiar with enterprise product deployment, networking, and 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 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