paloalto NETWORKS | CYBERSECURITY PARTNER OF CHOICE

Cortex® XSIAM Security Operations, Integration, and Automation

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:

- Describe how endpoint agents, XDR collectors, NGFWs, and Broker VMs secure networks and devices.
- Query and analyze logs using XQL for data ingestion and detection.
- Configure Threat Intel Management features, automate workflows, and apply EDLs and indicator rules.

Course Modules

0 - Course Overview
1 - Overview of Cortex XSIAM
2 - Software Components
3 - XQL
4 - Detection Engineering
5 - Integrations
6 - Automation
7 - Threat Intel Management
8 - Attack Surface Management
9 - UI Customizations

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 XSIAM.

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

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, SIEM and automation engineers.

Prerequisites

Participants should have a foundational understanding of cybersecurity principles and experience with network and endpoint security fundamentals.

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

ilt-44-XSIAM-investigation-and-analysis-ds-112124

paloalto NETWORKS | CYBERSECURITY PARTNER OF CHOICE

Cortex® XSIAM for Investigation and Analysis

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:

- Investigate incidents, 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 incident analysis.

Course Modules

1 - Introduction to Cortex XSIAM
2 - Endpoints
3 - XQL
4 - Alerting and Detection
5 - Threat Intel Management
6 - Automation
7 - Attack Surface Management
8 - Incident Handling
9 - Dashboards and Reports

Scope

- Duration: 2 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 Analysts roles, to use XSIAM.

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

Target Audience

SOC/CERT/CSIRT/XSIAM analysts 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 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

ilt-46-XSIAM-investigation-and-analysis-ds-112124