

Cortex XSIAM: 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 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 XSIAM
- 2 - Endpoints
- 3 - XQL
- 4 - Alerting and Detection
- 5 - Forensics
- 6 - Threat Intel Management
- 7 - Automation
- 8 - Case Management
- 9 - Dashboards and 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 XSIAM.

The course reviews XSIAM intricacies, from fundamental components to advanced strategies and techniques, including skills needed to navigate case management, 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.