

PALO ALTO NETWORKS: CORTEX XSIAM FOR INVESTIGATION AND ANALYSIS

Course Code: 842007

Designed to enable cybersecurity professionals, particularly those in SOC/CERT/CSIRT and Security Analysts roles, to use XSIAM

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.

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

What You'll Learn

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.

Who Needs to Attend

This course is intended for 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 foundational understanding of cybersecurity principles and experience with analyzing incidents and using security tools for investigation.



PALO ALTO NETWORKS: CORTEX XSIAM FOR INVESTIGATION AND ANALYSIS

Course Code: 842007

VIRTUAL CLASSROOM LIVE

\$2,000 USD

2 Day

Virtual Classroom Live Outline

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

Jul 21 - 22, 2025 | 8:30 AM - 4:30 PM EDT

Sep 8 - 9, 2025 | 8:30 AM - 4:30 PM EDT

Nov 10 - 11, 2025 | 8:30 AM - 4:30 PM EST

Jan 12 - 13, 2026 | 8:30 AM - 4:30 PM EST

Mar 2 - 3, 2026 | 8:30 AM - 4:30 PM EST

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 7/1/2025 8:50:08 AM

Copyright © 2025 Global Knowledge Training LLC. All Rights Reserved.

