PALO ALTO NETWORKS: CORTEX® XSIAM™ FOR SECURITY OPERATIONS AND AUTOMATION (EDU-270)

Course Code: 842002

Explore the key features of Cortex XSIAM, the AI-Driven security operations platform for the modern SOC.

Cortex® 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 four-day course is designed to enable cybersecurity professionals, particularly those in SOC/CERT/CSIRT and Security Engineering roles, to use XSIAM
It 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.

What You'll Learn

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

Who Needs to Attend

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: CORTEX® XSIAM™ FOR SECURITY OPERATIONS AND AUTOMATION (EDU-270)

Course Code: 842002

VIRTUAL CLASSROOM LIVE	$5,200 CAD	4 Day

Virtual Classroom Live Outline

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

May 12 - 15, 2025 | 8:30 AM - 4:30 PM EDT

PALO ALTO NETWORKS: CORTEX® XSIAM™ FOR SECURITY OPERATIONS AND AUTOMATION (EDU-270)

Course Code: 842002

PRIVATE GROUP TRAINING	4 Day

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

Date created: 4/19/2025 10:03:10 AM