Cortex XSIAM: Security Operations, Integration and Automation

Category: Networking & Security | **Vendor:** Palo Alto Networks

Duration: 24.00 hours (3 days) **19.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

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.

With this release, Palo Alto are now replacing Cortex XSIAM for Security Operations and Automation (EDU-270) with the following two courses:

- Cortex XSIAM for Investigation and Analysis (2- day course for XSIAM analysts)
- Cortex XSIAM: Security Operations, Integration, and Automation (3-day course for XSIAM engineers)

Students may wish to take only one or both courses as applicable to their role

About This Course

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

Who Should Attend

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 & Entry Requirements

General Prerequisites:

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

Learning Outcomes

Upon successful completion of this course, participants will be able to:

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.

Skills You Will Learn:

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.

Frequently Asked Questions

Q: What delivery options are available for Cortex XSIAM: Security Operations, Integration and Automation?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 3-day Cortex XSIAM: Security Operations, Integration and Automation course provides up to 19.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Cortex XSIAM: Security Operations, Integration and Automation training?

The training takes place over 3 day(s), with each day lasting approximately 24.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Cortex XSIAM: Security Operations, Integration and Automation?

Yes, we provide corporate training, dedicated training, and closed classes for Cortex XSIAM: Security Operations, Integration and Automation. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Cortex XSIAM: Security Operations, Integration and Automation, Palo Alto Networks, XSIAM-SOIA

Q: Why choose Nexus Human for Cortex XSIAM: Security Operations, Integration and Automation?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Cortex XSIAM: Security Operations, Integration and Automation training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)