Cortex XSIAM for Investigation and Analysis

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

Duration: 16.00 hours (2 days) **13.0 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:

- 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.

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.

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:

- 1- Introduction to Cortex XSIAM
- 2- Endpoints
- 3- XQL
- 4- Alerting and Detection
- 5- Forensics
- 6- Threat Intel Management
- 7- Automation
- 7- Case Management
- 9- Dashboards and Reports

Who Should 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 & Entry Requirements

General Prerequisites:

Participants should have foundational understanding of cybersecurity principles and experience with analyzing incidents and using security tools for investigation.

Frequently Asked Questions

Q: What delivery options are available for Cortex XSIAM for Investigation and Analysis?

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 2-day Cortex XSIAM for Investigation and Analysis course provides up to 13.0 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Cortex XSIAM for Investigation and Analysis training?

The training takes place over 2 day(s), with each day lasting approximately 16.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Cortex XSIAM for Investigation and Analysis?

Yes, we provide corporate training, dedicated training, and closed classes for Cortex XSIAM for Investigation and Analysis. 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 for Investigation and Analysis, Palo Alto Networks, XSIAM-IA

Q: Why choose Nexus Human for Cortex XSIAM for Investigation and Analysis?

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 for Investigation and Analysis 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 1 889 8700 (Ireland) | +44 20 8142 8961 (UK)

© 2026 Nexus Human. All rights reserved. This brochure was generated on 13/11/2026.