Cortex XDR: 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

The course is designed to enable cybersecurity professionals, particularly those in SOC/CERT/CSIRT and Security Analysts roles, to use XDR.
The course reviews XDR intricacies, from fundamental components to advanced strategies and techniques, including skills needed to navigate case management, platform automation, and orchestrate cybersecurity excellence

XDR is the industry's most powerful extended detection and response platform. You will gain hands-on expertise in endpoint management, case management, forensic analysis and platform automation. Throughout this course, you will explore the key features of Cortex XDR.

This course will utilize the Simulated Lab Environment, which is embedded within The Learning Center (TLC).

About This Course

Course Modules

- 1 - Introduction to Cortex XDR
- 2 - Endpoints
- 3 - XQL
- 4 - Alerting and Detection
- 5 - Vulnerability & Forensics
- 6 - Platform Automation
- 7 - Case Management
- 8 - Dashboards & Reports

Who Should Attend

This course is for a wide range of security professionals, including SOC, CERT, CSIRT, and XDR analysts, managers, incident responders, and threat hunters. It is also well-suited for professional-services consultants, sales engineers, and service delivery partners.

Prerequisites & Entry Requirements

General Prerequisites:

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

Learning Outcomes

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

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.

Detailed Course Outline

Module 1: Introduction to Cortex XDR

Module 2: Endpoints

Module 3: XQL

Module 4: Alerting and Detection

Module 5: Vulnerability & Forensics

Module 6: Platform Automation

Module 7: Case Management

Module 8: Dashboards & Reports

Skills You Will Learn:

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.

Frequently Asked Questions

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

Yes, we provide corporate training, dedicated training, and closed classes for Cortex XDR: 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 XDR: Investigation and Analysis, Palo Alto Networks, PCXDR-IA

Q: Why choose Nexus Human for Cortex XDR: 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 XDR: 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 14/11/2026.