Cortex XDR: Security Operations and Integration

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

This 3-day instructor-led course provides in-depth training on Cortex XDR, Palo Alto Networks' powerful extended detection and response platform. You will gain hands-on expertise in security operations, incident investigation, and system optimization to effectively protect modern environments. Throughout this course you will explore the key features of Cortex XDR.

The course is designed to enable cybersecurity professionals, particularly those in SOC/CERT/CSIRT and engineering roles, to use XDR.
The course reviews XDR intricacies, from fundamental components to advanced strategies and techniques, including skills needed to configure security integrations, develop workflows, manage indicators, and optimize dashboards for enhanced security operations.

- Format: Lecture and hands-on simulations
- Platform support: Cortex

This is an update and replacement for the previous EDU-260 course, specifically intended for the individuals who are responsible for configuring Cortex XDR and managing integrations, data ingestion, and security policies as opposed to the analysts who investigate cases and issues.
A retirement date for the EDU-260 and EDU-262 will be announced once the replacement course for EDU-262 is released (date TBA). For now the EDU-260 and EDU-262 will remain available, in addition to this new course offering

About This Course

Course Modules:

- 0 - Course Overview
- 1 - Overview of Cortex XDR
- 2 - Software Components
- 3 - Integrations
- 4 - XQL
- 5 - Detection Engineering
- 6 - Platform Automation
- 7 - System Optimization
- 8 - Dashboards and Reports
- 9 - Email Security

Who Should Attend

SOC/CERT/CSIRT/XDR engineers and managers, MSSPs and service delivery partners/system integrators, security consultants and sales engineers.

Prerequisites & Entry Requirements

General Prerequisites:

Attendees should possess a solid understanding of cybersecurity principles, including network and endpoint security concepts.

Learning Outcomes

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

This course is designed to enable you to:

- Describe the role of Cortex XDR components, including endpoint agents, XDR collectors, NGFWs, and Broker VMs, in securing networks and devices.
- Utilize XQL to query and analyze logs for effective data ingestion and threat detection.
- Design and implement workflows to streamline security operations.
- Apply External Dynamic Lists and indicator rules to enforce security policies.

Detailed Course Outline

Module 0: Course Overview | Module 1: Overview of Cortex XDR | Module 2: Software Components | Module 3: Integrations | Module 4: XQL | Module 5: Detection Engineering | Module 6: Platform Automation | Module 7: System Optimization | Module 8: Dashboards and Reports | Module 9: Email Security

Skills You Will Learn:

This course is designed to enable you to:

- Describe the role of Cortex XDR components, including endpoint agents, XDR collectors, NGFWs, and Broker VMs, in securing networks and devices.
- Utilize XQL to query and analyze logs for effective data ingestion and threat detection.
- Design and implement workflows to streamline security operations.
- Apply External Dynamic Lists and indicator rules to enforce security policies.

Frequently Asked Questions

Q: What delivery options are available for Cortex XDR: Security Operations and Integration?

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 XDR: Security Operations and Integration 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 XDR: Security Operations and Integration 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 XDR: Security Operations and Integration?

Yes, we provide corporate training, dedicated training, and closed classes for Cortex XDR: Security Operations and Integration. 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: Security Operations and Integration, Palo Alto Networks, PCXDR-SOI

Q: Why choose Nexus Human for Cortex XDR: Security Operations and Integration?

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: Security Operations and Integration 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)