Palo Alto Networks: Cortex XDR 3.2: Investigation and Response(EDU-262)

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

This instructor-led course teaches you how to use the Incidents pages of the Cortex XDR management console to investigate attacks. It explains causality chains, detectors in the Analytics Engine, alerts versus logs, log stitching, and the concepts of causality and analytics. You will learn how to analyze alerts using the Causality and Timeline Views and how to use advanced response actions, such as remediation suggestions, the EDL service, and remote script execution. Multiple modules focus on how to leverage the collected data. You will create simple search queries in one module and XDR rules in another. The course demonstrate how to use specialized investigation views to visualize artifact-related data, such as IP and Hash Views. Additionally, it provides an introduction to XDR Query Language (XQL). The course concludes with Cortex XDR external-data collection capabilities, including the use of Cortex XDR API to receive external alerts.This class is powered by Cloud Harmonics.

About This Course

This instructor-led course teaches you how to use the Incidents pages of the Cortex XDR management console to investigate attacks. It explains causality chains, detectors in the Analytics Engine, alerts versus logs, log stitching, and the concepts of causality and analytics. You will learn how to analyze alerts using the Causality and Timeline Views and how to use advanced response actions, such as remediation suggestions, the EDL service, and remote script execution.

Multiple modules focus on how to leverage the collected data. You will create simple search queries in one module and XDR rules in another. The course demonstrate how to use specialized investigation views to visualize artifact-related data, such as IP and Hash Views. Additionally, it provides an introduction to XDR Query Language (XQL). The course concludes with Cortex XDR external-data collection capabilities, including the use of Cortex XDR API to receive external alerts.

This class is powered by Cloud Harmonics.

Who Should Attend

Cybersecurity analysts and engineers

Security operations specialists

Learning Outcomes

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

Successful completion of this instructor-led course with hands-on lab activities should enable participants to:

Investigate and manage incidents

Describe the Cortex XDR causality and analytics concepts

Analyze alerts using the Causality and Timeline Views

Work with Cortex XDR Pro actions such as remote script execution

Create and manage on-demand and scheduled search queries in the Query Center

Create and manage the Cortex XDR rules BIOC and IOC

Working with Cortex XDR assets and inventories

Write XQL queries to search datasets and visualize the result sets

Work with Cortex XDR’s external-data collection

Additional Course Details

Nexus Humans Palo Alto Networks: Cortex XDR 3.2: Investigation and Response(EDU-262) training program is a workshop that presents an invigorating mix of sessions, lessons, and masterclasses meticulously crafted to propel your learning expedition forward.

This immersive bootcamp-style experience boasts interactive lectures, hands-on labs, and collaborative hackathons, all strategically designed to fortify fundamental concepts.

Guided by seasoned coaches, each session offers priceless insights and practical skills crucial for honing your expertise. Whether you're stepping into the realm of professional skills or a seasoned professional, this comprehensive course ensures you're equipped with the knowledge and prowess necessary for success.

While we feel this is the best course for the Palo Alto Networks: Cortex XDR 3.2: Investigation and Response(EDU-262) course and one of our Top 10 we encourage you to read the course outline to make sure it is the right content for you.

Additionally, private sessions, closed classes or dedicated events are available both live online and at our training centres in Dublin and London, as well as at your offices anywhere in the UK, Ireland or across EMEA.

Frequently Asked Questions

Q: What delivery options are available for Palo Alto Networks: Cortex XDR 3.2: Investigation and Response(EDU-262)?

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 Palo Alto Networks: Cortex XDR 3.2: Investigation and Response(EDU-262) 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 Palo Alto Networks: Cortex XDR 3.2: Investigation and Response(EDU-262) 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 Palo Alto Networks: Cortex XDR 3.2: Investigation and Response(EDU-262)?

Yes, we provide corporate training, dedicated training, and closed classes for Palo Alto Networks: Cortex XDR 3.2: Investigation and Response(EDU-262). 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: Why choose Nexus Human for Palo Alto Networks: Cortex XDR 3.2: Investigation and Response(EDU-262)?

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 Palo Alto Networks: Cortex XDR 3.2: Investigation and Response(EDU-262) 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)