EDU-262: Palo Alto Networks: Cortex XDR 3.0: Investigation and Response

Price: 1995

Duration:

Delivery Methods: Virtual

Overview

The first part of this instructor-led training enables you to investigate attacks from Cortex XDR management console pages, including the Incidents page and specialized artifact analysis views such as the IP View. In the first part, you will also learn how to run remote Python scripts on your endpoints.
The second part of the training enables you to work with Cortex XDR data processing capabilities to protect your environment against advanced threats such as fileless attacks. For example, in this part you will analyze alerts in the Causality View. Also, you will learn about Cortex XDR data collection capabilities, including Cortex XDR API for ingesting external alerts, and leverage the data to investigate threats. The training ends up with introductory modules to XDR Query Language XQL and two Pro features based-on Cortex XDR XQL engine.

Objectives

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

- Investigate attacks on the incidents page, and score, assign, and close them
- Investigate artifacts using the specialized views such as IP View and Hash View
- Work with Cortex XDR Pro actions: the remote script execution and EDL service
- Describe the Cortex XDR causality and analytics concepts
- Analyze alerts using the Causality and Timeline Views
- Create and manage on-demand and scheduled search queries in the Query Center

- Create and manage the Cortex XDR rules BIOC and IOC
- Work with the Cortex XDR’s external data ingestion support
- Write XQL queries to search datasets and visualize the result sets
- Create simple Correlation Rules and Parsing Rules using XQ

Target Audience

- Cybersecurity analysts and engineers, and security operations specialists

Prerequisites

- Participants must have taken the course EDU-260 (Cortex XDR: Prevention and Deployment).

Course Modules

- Cortex XDR Incidents
- Investigation Views
- Advanced Response Actions
- Causality and Analytics Concepts
- Causality Analysis of Alerts
- Building Basic Search Queries
- Building Basic XDR Rules
- External Data Collection
- Introduction to XQL
- Correlation and Parsing Rules

Course Schedule

Date	Time	Price	Options

Why Professional Choose TOPTALENT?

Dedicated Texas-Based Support

Get assistance every step of the way from our **Texas-based team**, ensuring your training experience is hassle-free and aligned with your goals.

3000+ Curated Professional Courses

Access an extensive portfolio of over 3000 courses across IT, Business Application and Leadership – Designed to meet evolving Industry demands

95% Client Approval Rating

Trusted by professionals nationwide our 95% approval rating reflects consistent quality, measurable impact and exceptional service.

Certified Industry Instructor

Learn from professionaly certified experts with real world experience and a proven commitment to learner success.

For questions

call:

(469) 721-6100

Email:

info@toptalentlearning.com

Find More Training

FAQ

What if I have to reschedule my class due to conflict?

Ten (10) business days' notice is required to reschedule a class with no additional fees. Notify TOPTALENT LEARNING as soon as possible at 469-721-6100 or by written notification to info@toptalentlearning.com to avoid rescheduling penalties.

How do I enroll for this class?

Please contact our team at 469-721-6100; we will gladly guide you through the online purchasing process.

What happens once I purchase a class?

You will receive a receipt and an enrollment confirmation sent to the email you submitted at purchase. Your enrollment email will have instructions on how to access the class. Any additional questions our team is here to support you. Please call us at 469-721-6100.

What is your late policy?

If a student is 15 minutes late, they risk losing their seat to a standby student. If a student is 30 minutes late or more, they will need to reschedule. A no-show fee will apply. Retakes are enrolled on a stand-by basis. The student must supply previously issued courseware. Additional fees may apply.

What happens when I finish my class?

You will receive a ‘Certificate of Completion’ once you complete the class. If you purchased an exam voucher for the class, a team member from TOPTALENT LEARNING will reach out to discuss your readiness for the voucher and make arrangements to send it.