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

TRAINING GOALS:

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.

Objectives

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

Target Audience

- Cybersecurity analysts and engineers
- Security operations specialists

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

CONSPECT:

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

REQUIREMENTS:

Participants must have completed EDU-260 Cortex XDR: Prevention and Deployment course.

Difficulty level

CERTIFICATE:

The participants will obtain certificates signed by Palo Alto Networks (course completion).

This course also helps you prepare for the Palo Alto Networks Detection and Remediation Analyst (PCDRA). Palo Alto Networks certification exams are offered at Pearson Vue test centers worldwide https://home.pearsonvue.com/paloaltonetworks

TRAINER:

Palo Alto Networks Certified Security Platform Instructor (PCSPI)

ADDITIONAL INFORMATION:

Authorized Courseware

Each attendee will receive a student guide and lab exercise guide in the form of a secure PDF. Students will access these materials by creating an account with a third party platform, Kortext, hosted by fulfilment supplier.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

Training Credit

Palo Alto Networks Training Credits allow you a single point of purchase for training for use throughout the year. Training credits are redeemable by all employees within an organization for any Palo Alto Networks open enrollment, private on-site, or online course offered by our Authorized Training Partners (ATPs). Compendium CE accept the Training Credits issued by Palo Alto Networks. To sign-up for a course and pay using training credits, please contact with our sales team: szkolenia@compendium.pl

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007