Cortex XDR: Investigation and Response

Kód kurzu: EDU-262

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- datacollection capabilities, including the use of Cortex XDR API to receive external alerts.

Pre koho je kurz určený

- Cybersecurity analysts and engineers
- Security operations specialists

Čo Vás naučíme

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

- Investigate and manage incidents
- Describe the Cortex XDR causality and analytics concepts
- An alyze 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 an dIOC
- 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

Požadované vstupné znalosti

Participants must have comlpleted EDU-260 (Cortex XDR: Prevention and Deployment).

Osnova kurzu

- 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

Palo Alto Networks Education

The technical curriculum developed and authorized by Palo Alto Networks and delivered by Palo Alto Networks Authorized Training Partners helps provide the knowledge and expertise that prepare you to protect our digital way of life. Our trusted certifications validate your knowledge of the Palo Alto Networks product portfolio and your ability to help prevent successful cyberattacks, safely enable applications, and automate effective responses to security events.

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk