Cortex XDR: Investigation and Response

Kód kurzu: EDU-262

Please Note: This course will be delivered in half-day sessions
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.Please Note: This course will be delivered in half-day sessions

Pro koho je kurz určen

Cybersecurity analysts and engineers, and security operations specialists.

Co Vás naučíme

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 XQL

Požadované vstupní znalosti

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

Osnova kurzu

- 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

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 and safely enable applications.

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