Cortex™ XSOAR 6.2: Automation and Orchestration

Kód kurzu: EDU-380

The Cortex™ XSOAR 6.2: Automation and Orchestration (EDU-380) course is four days of instructor-led training that will help you:Configure integrations, create tasks, and develop playbooksBuild incident layouts that enable analysts to triage and investigate incidents efficientlyIdentify how to categorize event information and map that information to display fieldsDevelop automations, manage content, indicator data, and artifact stores, schedule jobs, organize users and user roles, oversee case management, and foster collaboration

Pro koho je kurz určen

Security-operations (SecOps), or security, orchestration, automation, and response (SOAR) engineers, managed security service providers (MSSPs), service delivery partners, system integrators, and professional services engineers.

Co Vás naučíme

This training is designed to enable a SOC, CERT, CSIRT, or SOAR engineer to start working with Cortex XSOAR integrations, playbooks, incident-page layouts, and other system features to facilitate resource orchestration, process automation, case management, and analyst workflow.
The third module of the course demonstrates a complete playbook-development process for automating a typical analyst workflow to address phishing incidents. This end-to-end view of the development process provides a framework for more focused discussions of individual topics that are covered in subsequent modules.

Požadované vstupní znalosti

Participants must complete the Cortex XSOAR Analyst digital learning. Participants who have experience with scripting, the use of Python and JavaScript, and the use of JSON data objects will likely be able to apply what they learn more quickly than participants without such experience. However, completion of the course does not require proficiency in writing code.

Osnova kurzu

- Core Functionality and Feature Sets
- Enabling and Configuring Integrations
- Playbook Development
- Classification and Mapping
- Layout Builder
- Solution Architecture
- Docker
- Automation Development and Debugging
- The Marketplace and Content Management
- Indicators and Threat Intelligence Management
- Jobs and Job Scheduling
- Users and Role-Based Access Controls (RBAC)
- Integration Development

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