Palo Alto Networks: Cortex™ XSOAR: Automation and Orchestration

Duration: 4 Days **Course Code: PAN-EDU-380** **Version: 6.8**

Overview:

The Cortex™ XSOAR 6.8: Automation and Orchestration (EDU-380) course is four days of instructor-led training that will help you:
- Configure integrations, create tasks, and develop playbooks
- Build incident layouts that enable analysts to triage and investigate incidents efficiently
- Identify how to categorize event information and map that information to display fields
- Develop automations, manage content, indicator data, and artifact stores, schedule jobs, organize users and user roles, oversee case management, and foster collaboration

Target Audience:

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

Objectives:

- 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 course includes coverage of 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 the course.

Prerequisites:

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.

Content:

- 1 - Core Functionality and Feature Sets
- 2 - Enabling and Configuring Integrations
- 3 - Playbook Development
- 4 - Classification and Mapping
- 5 - Layout Builder
- 6 - Solution Architecture
- 7 - Docker
- 8 - Automation Development and Debugging
- 9 - The Marketplace and Content Management
- 10 - Indicators and Threat Intelligence Management
- 11 - Jobs and Job Scheduling
- 12 - Users and Role-Based Access Controls (RBAC)
- 13 - Integration Developmen

Additional Information:

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.

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK