Palo Alto Networks: Cortex XSIAM: Security Operations, Integration and Automation (CXSIAM)

Duration: 3 Days **Course Code: PAN-CXSIAMSOIA**

Overview:

Designed to enable cybersecurity professionals, particularly those in SOC/CERT/CSIRT and engineering roles, to use XSIAM. XSIAM is the industry's most comprehensive security incident and asset management platform, offering extensive coverage for securing and managing infrastructure, workloads, and applications across multiple environments.

Target Audience:

This course is intended for SOC/CERT/CSIRT/XSIAM engineers and managers, MSSPs and service delivery partners/system integrators, internal and external professional services consultants and sales engineers, SIEM and automation engineers.

Objectives:

- This course is designed to enable you to:
- Describe how endpoint agents, XDR collectors, NGFWs, and Broker VMs secure networks and devices.
- Query and analyze logs using XQL for data ingestion and detection.
- Configure Threat Intel Management features, automate workflows, and apply EDLs and indicator rules.
- The course reviews XSIAM intricacies, from fundamental components to advanced strategies and techniques, including skills needed to configure security integrations, develop automation workflows, manage indicators, and optimize dashboards for enhanced security operations.

Prerequisites:

- Participants should have foundational understanding of cybersecurity principles and experience with analyzing incidents and using security tools for investigation.

Testing and Certification

- Palo Alto Networks Certified XSIAM Engineer

Content:

Course Modules

- Course Overview
- Overview of Cortex XSIAM
- Software Components
- XQL
- Detection Engineering
- Integrations
- Automation
- Threat Intel Management
- Attack Surface Management
- UI Customizations

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/