Palo Alto Networks: Cortex XSIAM for Investigation and Analysis (XSIAM-IA)

Duration: 2 Days **Course Code: PAN-XSIAM-IA**

Overview:

XSIAM is the industry's most comprehensive security incident and asset management platform, offering extensive coverage for securing and managing infrastructure, workloads, and applications cross multiple environments.
Throughout this course, you will explore the key features of Cortex XSIAM.
This course is designed to enable you to:
- Investigate incidents, analyze key assets and artifacts, and interpret the causality chain.
- Query and analyze logs using XQL to extract meaningful insights.
- Utilize advanced tools and resources for comprehensive incident analysis.

Target Audience:

SOC/CERT/CSIRT/XSIAM analysts and managers, MSSPs and service delivery partners/system integrators, internal and external professional-services consultants and sales engineers, incident responders and threat hunters.

Objectives:

- The course is designed to enable cybersecurity professionals, particularly those in SOC/CERT/CSIRT and Security Analysts roles, to use XSIAM.
- The course reviews XSIAM intricacies, from fundamental components to advanced strategies and techniques, including skills needed to navigate incident handling, automation, and orchestrate cybersecurity excellence.

Prerequisites:

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

Testing and Certification

There is no online exit exam for this course, but there is a related certification: XSIAM Analyst

Content:

Course Modules

1- Introduction to Cortex XSIAM

2- Endpoints

3- XQL

4- Alerting and Detection

5- Threat Intel Management

6- Automation

7- Attack Surface Management

8- Incident Handling

9- Dashboards and Reports

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/