Palo Alto Networks: Cortex XDR Security Operations and Integration

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

Overview:

Gain hands-on expertise in security operations, incident investigation, and system optimization to effectively protect modern environments. This 3-day instructor-led course provides in-depth training on Cortex XDR, Palo Alto Networks' powerful extended detection and response platform. You will gain hands-on expertise in security operations, incident investigation, and system optimization to effectively protect modern environments.
The course reviews XDR intricacies, from fundamental components to advanced strategies and techniques, including skills needed to configure security integrations, develop workflows, manage indicators, and optimize dashboards for enhanced security operations.

Target Audience:

- SOC/CERT/CSIRT/XDR engineers and managers
- MSSPs and service delivery partners/system integrators
- Security consultants and sales engineers.

Objectives:

- Describe the role of Cortex XDR components, including endpoint agents, XDR collectors, NGFWs, and Broker VMs, in securing networks and devices.
- Utilize XQL to query and analyze logs for effective data ingestion and threat detection.
- Design and implement workflows to streamline security operations.
- Apply External Dynamic Lists and indicator rules to enforce security policies.

Prerequisites:

- Attendees should possess a solid understanding of cybersecurity principles, including network and endpoint security concepts.

Testing and Certification

- Palo Alto Networks Certified XDR Engineer

Content:

Course Modules

0 - Course Overview

1 - Overview of Cortex XDR

2 - Software Components

3 - Integrations

4 - XQL

5 - Detection Engineering

6 – Platform Automation

7 - System Optimization

8 - Dashboards and Reports

9 – Email Security

Additional Information:

Palo Alto Networks Education:
The technical curriculum developed by Palo Alto Networks and delivered by Palo Alto Networks Authorized Training Partners helps provide the knowledge and expertise you need 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 cyberattack

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/