Cortex XDR: Security Operations and Integration

Duration: 3 Days

Course Description:

This 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. Throughout this course you will explore the key features of Cortex XDR.

This course is designed to enable you to:

- 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.

Target Audience:

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

Prerequisites:

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

Course Objectives:

The course is designed to enable cybersecurity professionals, particularly those in SOC/CERT/CSIRT and engineering roles, to use XDR. 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.

Course Outlines:

- Course Overview
- Overview of Cortex XDR 2
- Software Components
- Integrations
- XQL
- Detection Engineering
- System Optimization
- Dashboards and Reports