Cortex XSIAM: Security Operations, Integration, and Automation

Duration: 3 Days

Course Description:

The 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. Throughout this course, you will explore the key features of Cortex XSIAM.

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.

Target Audience:

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.

Prerequisites:

Participants should have a foundational understanding of cybersecurity principles and experience with network and endpoint security fundamentals.

Course Objectives:

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

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.

Course Outlines:

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