Cortex XSIAM: Security Operations, Integration, and Automation

COURSE DETAILS

Delivery Type: Instructor-Led
Duration: 3 Days

COURSE PREREQUISITES

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

COURSE CONTENT

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.

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 OUTLINE

1. Course Overview
2. Overview of Cortex XSIAM
3. Software Components
4. XQL
5. Detection Engineering
6. Integrations
7. Automation
8. Threat Intel Management
9. Attack Surface Management
10. UI Customizations

WHO SHOULD ATTEND

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.