Cortex XSIAM for Investigation and Analysis

COURSE DETAILS

Delivery Type: Instructor-Led
Duration: 2 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:

- 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.

COURSE 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.

COURSE OUTLINE

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

WHO SHOULD ATTEND

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.