Cortex XDR: Investigation and Analysis

Duration: 2 Days

Course Description:

XDR is the industry's most powerful extended detection and response platform. You will gain hands-on expertise in endpoint management, case management, forensic analysis and platform automation. Throughout this course, you will explore the key features of Cortex XDR. This course is designed to enable you to Investigate cases, analyze key assets and artifacts, and interpret the causality chain, query and analyze logs using XQL to extract meaningful insights and utilize advanced tools and resources for comprehensive case analysis.

Target Audience:

This course is for a wide range of security professionals, including SOC, CERT, CSIRT, and XDR analysts, managers, incident responders, and threat hunters. It is also well-suited for professional-services consultants, sales engineers, and service delivery partners.

Prerequisites:

Participants should have a foundational understanding of cybersecurity principles and experience with analyzing incidents and using security tools for investigation.

Course Objectives:

The course is designed to enable cybersecurity professionals, particularly those in SOC/CERT/CSIRT and Security Analysts roles, to use XDR. The course reviews XDR intricacies, from fundamental components to advanced strategies and techniques, including skills needed to navigate case management, platform automation, and orchestrate cybersecurity excellence.

Course Outlines:

- Introduction to Cortex XDR
- Endpoints
- XQL
- Alerting and Detection
- Vulnerability & Forensics
- Platform Automation
- Case Management
- Dashboards & Reports