Palo Alto Networks Cortex XSIAM: Investigation and Analysis

Duration: 2 Days

Course Description:

Cortex XSIAM: Investigation and Analysis is a course designed to equip cybersecurity professionals with the knowledge and skills to effectively investigate incidents and manage security operations using Cortex XSIAM — Palo Alto Networks' next-generation SOC platform.

Participants will learn how to query and analyze logs with XQL, leverage built-in threat intelligence tools, automate investigation workflows, and visualize security data using dashboards and reports. With a strong focus on real-world application, this course combines lectures and lab-based exercises to ensure participants gain practical expertise in incident analysis and response.

Target Audience:

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.

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 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 Outlines:

- Introduction to Cortex XSIAM
- Endpoints
- XQL
- Alerting and Detection
- Threat Intel Management
- Automation
- Attack Surface Management
- Incident Handling
- Dashboards and Reports