Cortex XSIAM: Security Operations and Automation (EDU-270)

Course Description

The Palo Alto Networks **Cortex XSIAM: Security Operations and Automation** (EDU-270) course is an instructor-led training that will help you to:

- Deploy, configure, and install XDR agents and configure Agent Groups and profiles
- Investigate incidents, examine assets and artifacts, and understand the causality chain
- Create correlation rules, use XQL to query logs, and analyze incidents using available tools and resources

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

The course reviews XSIAM intricacies, from fundamental components to advanced strategies and automation techniques, including skills needed to navigate incident handling, optimize log sources, and orchestrate cybersecurity excellence.

Prerequisites

No previous Palo Alto Networks experience is required to take this Cortex XSIAM EDU 270 Palo Alto course while familiarity with enterprise product deployment, networking, and security concepts is recommended.

Course Duration:

4 days

Course Outline:

Agent Deployment and Configuration

- Agent Deployment and Configuration Overview
- Profiles and Policies
- Deployment Requirements

Data Source Ingestion

- Introduction to Data Source Ingestion
- Syslog and API Collections Methods
- Parsers vs. Data Models
- Log Collection Strategy

Visibility

- Log Source Best Practices
- Onboarding Strategy
- Customizing Dashboards for SOC Needs

Data Model

- Data Model Overview
- Process/Approach to Map Events
- Components of a Data Model

Analytics

- Analytics Overview
- Analytics vs. Correlations
- EALs

Alerting and Detecting

- XQL
- Pseudocode
- Use Case Development Workflow

Attack Surface Management

- Attack Surface Management Overview
- Playbooks/Marketplace Content
- Enable/Disable Attack Surface Rules

Automation

- Automation Overview
- Marketplace
- Playbooks
- Designing, Building, and Testing Playbooks
- Using OOTB Content

Incident Handling / SOC

- Incident Overview
- Investigative Techniques
- Remediation of Incidents
- Workflow Utilization

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, incident responders and threat hunters.