

securonix

Unified Defense SIEM Analyst Training

Securonix Training





Overview

Duration: 2 Days (4 Learning Credits)

Format: Instructor-Led Training (ILT)

Exam format: Online Examination

Audience: Security Analysts and Incident Responders

Platform Version: 6.4 or UDS

Description

The Securonix Analyst course provides analysts with the skills needed to prioritize and respond to use case objectives. Starting with security alert analysis that effectively uses Securonix features to provide user and environmental context and continuing to achieve a wider visibility of entity behavior. Analysts will obtain the ability to determine use case alignment to business objectives and optimizations available to respond to alerts effectively.

Course Topics

1. Performing Spotter Searches
2. Creating Data Insights Dashboards
3. Creating Reports in Spotter
4. Executing Advanced Spotter Searches
5. Creating Policies and Threat Models
6. Performing Threat Response and Incident Handling Activities
7. Using Unified Defense SEIM (UDS) Resources for Threat Hunting

Course Objectives

- Understanding Content Management Terminology.
- Demonstrate How to Create Policies and Threat Models.
- Configure Policy Conditions.
- Demonstrate How to Configure Risk Scoring for Policies and Threats.
- Demonstrate How to Configure Actions and remediation steps.



- Configure Policies that Engage Behavior-based Analytics.
- Identity How Behavior Profiles are Established.
- Demonstrate How to Manage the Policy Life Cycle.
- Identity Priorities in Threat Response.
- Effectivity Identity of the Securonix Story Found When Responding to Rulesets and Alignment to Business Use Cases.
- Demonstrate Incident Management Workflows.
- Demonstrate Query Syntax Usage in Structured and Unstructured Searches..
- Demonstrate the Use of Spotter Indexes in Searches.
- Identify the Common Fields of Data Queries in Spotter.
- Demonstrate the Use of Operators in Spotter Queries.
- Optimize Queries to Refine Results and Identify relevant data.
- Manage Data Insights and Create Dashboards for Reporting.

Labs

Hands-on labs are provided to reinforce the skills needed to successfully deploy and manage a Securonix Unified Defense SIEM Platform.

1. Fundamentals: Configuring Baseline View
2. Fundamentals: Configuring Tenant Baseline
3. Fundamentals: Access Control - Roles, Users and Groups
4. Content Management: Security and Command Center Overview
5. Content Management: Reducing the Risk Score of a Policy Violation
6. Content Management: Policy Configuration and Securonix Story
7. Content Management: Creating and Triggering New Policies
8. Content Management: Threat Model Configurations
9. Operations: Spotter Performing Spotter Searches
10. Operations: Executing Advanced Spotter Searches
11. Operations: Data Insights and Visualization
12. Operations: Report Creation and Management
13. Incident Handling: Creating and Managing On-demand Incidents
14. Incident Handling: Group Incident Response and Collaboration
15. Incident Handling: Performing Independent Threat Response
16. Incident Handling: Hunting for Threats



Course Requirements

Required Knowledge

The following prerequisites will ensure that trainees receive the best experience.

- Basic understanding of networking and network security.
- Basic understanding of the Unified Defense SIEM Platform and functionality from 100 online courses, Industry SIEM analyst training, and certifications.
- Basic understanding of business use case objectives and data source requirements in your environment.

Recommended Industry Analyst Training and Certifications

- SANS 504 Incident Handling, GSEC, CISSP, GCIH, or GCIA.

Technical Requirements

- Laptop/Desktop - Mac OS or Windows.
- An environment with dual screens and a headset with a microphone is recommended.
- Reliable Internet connection (LAN/Wi-Fi).
- Most current web browser (Google Chrome Recommended).
- Zoom desktop application.
- Outbound Connectivity to Amazon EC2 SNYPR over HTTPS port 443.