

securonix

Unified Defense SIEM SaaS Admin Training Training

Securonix Training





Overview

Duration: 3 Days (6 Learning Credits)

Format: Instructor-Led Training (ILT)

Exam format: Online Examination

Labs: Demos, Hands-on labs

Practical: 1 Day (Optional, Hands-on, open-book assessment and certification)

Audience: Administrators

Platform Version: 6.4 or UDS

Description

The Securonix SaaS Admin course reviews the intended deployment and administration tasks to initially configure and onboard data into your Unified Defense SIEM (UDS) environment. The class material during this course provides important terminology to understand and effectively stage and provide access to a new environment. The hands-on exercises provide you with important skills that enable you to install the Securonix Hub, onboard User Data from Active Directory, and Activity data from common data sources. The content creation and following exercises provide the foundational framework to implement use case initiatives that begin once data has been onboarded.

Course Topics

1. Securonix Terminology and Offerings
2. Hub Installation and Management
3. Data Onboarding Best Practices
4. Parsing and Mapping Leveraging Data Dictionary
5. Policy Development and Implementing a Policy Lifecycle
6. Leveraging Content Management Updates
7. Creating Efficient Search Queries
8. Building Effective Dashboards and Reports



Course Objectives

- Review Securonix's fundamental terminology, SaaS Architecture, and components of the enrichment framework.
- Configure the Securonix Unified Defense SIEM in a way that aligns with an organization's objectives and offerings to internal or external customers.
- Install, configure, and manage the Securonix Hub from preparation to validation.
- Leverage Securonix Best Practices for collection and configuration considerations that enable upstream enrichment and true positive targets.
- Identify and implement common collection methods, including Active Directory Imports, Windows Data, and API collection.
- Identify and effectively use the data onboarding steps, including parser management and identity attribution, to optimize the onboarding and enrichment of data sources.
- Identify available Securonix Behavioral algorithms, core functionality, and intended applications.
- Identify features available to optimize the Securonix Story, including Analytic Summary, Summary View, MITRE, and kill-chain functionalities.
- Demonstrate a functional understanding of Spotter to search and visualize data sets.
- Create reports and dashboards that help to achieve operational and security objectives.

Labs

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

1. Fundamentals: Accessing the SNYPR Training Lab
2. Fundamentals: Configuring Baseline View
3. Fundamentals: Configuring Tenant Baseline
4. Fundamentals: Access Control - Roles, Users and Groups
5. Securonix Hub: Connecting to Bastion Host and Hub Agent
6. Securonix Hub: Exploring current Hub Configuration
7. Securonix Hub: Hub Preparation, Installation, and Post-installation Actions
8. Data Onboarding: User Data Management - Active Directory
9. Data Onboarding: Staging - Creating a Discovery Queue
10. Data Onboarding: Windows Domain Controller Security Event Logs
11. Data Onboarding: NXLog Installation and Configuring for Local Windows Event Forwarding
12. Data Onboarding: API Collection - AWS CloudTrail
13. Content Management: Security and Command Center Overview
14. Content Management: Policy Configuration and Securonix Story
15. Content Management: Creating and Triggering New Policies
16. Content Management: Threat Model Configurations
17. Operations: Spotter Performing Spotter Searches
18. Operations: Executing Advanced Spotter Searches



- 19. Operations: Data Insights and Visualization
- 20. Operations: Report Creation and Management

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 administration training, and certifications.
- Basic functional understanding of Unix and command line functions.
- Familiarity with accessing Unix-based systems using SSH or Putty.
- Basic understanding of SIEM collection mechanisms and data flow.
- Basic understanding of data sources and objectives with bringing data into your environment.
- Familiarity with the data source types required in your environment.
- Basic understanding of API authentication and collection parameters.
- Experience with Windows, including administrative tasks, privilege elevation, and event logging.
- Basic understanding of data sources and objectives with bringing data into your environment.

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.
- Outbound RDP Connectivity to Amazon EC2 bastion over TCP 3389.