SNYPR SaaS Admin Training

Overview

Duration: 3 Days
Format: Instructor Led Training
Exam format: Online Examination
Practical: 1 Day (Hands-on, open-book assessment)

Description

The Securonix SNYPR SaaS Admin course reviews the intended deployment and administration tasks to initially configure and onboard data into your 6.4 SNYPR environment. The class materials during this course provide important terminology to understand and effectively stage and provision access to a new environment. The hand-on exercises provide you with important skills that enable you to install the Remote Ingester Node (RIN), onboard User Data from Active Directory and Activity data from common data sources. The content creation and following exercises provide the foundational framework needed to implement use case initiatives that begin once data has been onboarded. Finally, throughout this course we explore the fundamentals.

Course Objectives

- Review Securonix fundamental terminology, SaaS Architecture, and components of the enrichment framework.
- Configure the Securonix platform in a way that aligns to an organization's objectives and offerings to internal or external customers.
- Install, configure, and manage the RIN 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, syslog - 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 algorithms, core functionality and intended applications.
- Identify features available to optimize the Securonix story, including Analytic Summary, Summary View, and MITRE and kill-chain functionalities.
- Demonstrate a functional understanding of Spotter to search and visualize varying data sets.
- Create reports and dashboards that help to achieve operational and security objectives.

Course Topics

- Securonix Terminology and offerings
- RIN installation and management
- Data onboarding best practices
- Policy development and testing
- Threat hunting and reports in Spotter

Overview

Lab Exercises

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. RIN: Connecting to Bastion Host and RIN
6. RIN: Exploring Current RIN Configuration
7. RIN: RIN 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: NX Log Installation and Configuration for Local Windows Event Log Forwarding
12. Data Onboarding: Creating a Custom Datasource and Paser Management
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. Operations: Spotter Overview
17. Operations: Data Insights and Visualizations
18. Operations: Report Creation and Management

Workshop Requirements

Required Knowledge

- Basic understanding of networking and network security.
- Basic understanding of SNYPR platform and functionality from 100 series 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 datasource types required in your environment.
- Basic understanding of API authentication and collection partners.
- 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.
- 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 port 3389