

securonix

300 Data Integrator

Securonix Training





Overview

Duration: 2 hours

Format: Self-Paced Learning

Exam format: Online Examination

Labs: Demos and Lab Simulations

Audience: Administrators and Data Integrators

Platform Version: 6.3.1

Description

For data integrators who need to import the data to support the use cases in your environment.

Develop the fundamental skills to identify the types of data sources used in the SNYPR and how to configure those data sources to support your use cases. Learn how to use existing and custom connectors to ingest security events from various log sources and enrich the event data with meaningful user, access, asset, lookup, and geolocation context.

Course Topics

1. Securonix Open Event Format.
2. Data Types Overview.
3. Remote Ingestion of Datasources.
4. Activity Data.
5. User Data.
6. Peer Groups.
7. Access Data.
8. Enrichment Data.
9. Job Monitor.

Course Objectives

- Use the Securonix Open Event Format to Standardize and Normalize Attributes, Devices, and Events in SNYPR.
- Identify the Different Data Types Used in SNYPR to Support Use Cases.



- Configure the Remote Ingestion Node (RIN) to Receive Data from Datasources and Forward the Data to SNYPR.
- Use Existing and Custom Connectors to Ingest Data.
- Identity and Ingest Data to Enrich Events.
- Ingest and Configure Activity Event Data to Support the Use Cases in Your Environment.

Labs

1. Configure RIN to ingest data sources.
2. Import data to enrich events using existing and custom connectors.
3. Import Activity data using existing connectors.
4. Import and configure a custom activity data source.

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 Hadoop big data framework.
- Basic understanding of SNYPR Platform and functionality from 100 online courses, Industry SIEM analyst training, and certifications.

Technical Requirements

- Laptop/Desktop - Mac OS or Windows.
- Environment with dual screens.
- Reliable Internet connection (LAN/Wi-Fi).
- Most current web browser (Google Chrome Recommended).