Securonix SNYPR Training

Certified SNYPR Data Integrator

Duration: Self-paced
Format: Online
Exam format: Online examination

Description

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

Develop the skills to identify the types of datasources used in SNYPR and how to configure those datasources 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, geolocation,

Workshop 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 RIN to receive data drom datasources and forward the data to SNYPR
- Use existing and custom connectors to ingest data
- Identify and ingest data to enrich events
- Ingest and configure activity event data to support the use cases in your environment

Workshop 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

Hands-on Lab Exercises

1. Configure RIN to ingest datasources
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 datasource

Certified SNYPR Data Integrator

Workshop Requirements

Required Knowledge

- Basic understanding of networking and network security
- Basic understanding of Hadoop big data framework
- Basic understanding of SNYPR platform from the 100 series online course
- Basic understanding of SNYPR functionality from the 200 series online course

Technical Requirements

- Laptop or workstation
- Reliable Internet connection (LAN/Wi-Fi)
- Updated web browser (Mozilla Firefox, Google Chrome recommended)