Securonix SNYPR Training

Certified SNYPR Content Developer

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

Description

For content developers who need to use the SNYPR platform to develop content to detect the threats to your organization.

Develop the fundamental skills to identify the use cases unique to your environment, integrate the datasources required to support the use cases, and use the advanced analytics and threat modeling features of SNYPR to develop content to detect the behaviors that indicate a threat.

Workshop Objectives

- Design use cases to meet your business requirements
- Configure Data Types to suppose the use cases in your environment
- Use out of the box content to support your business requirements
- Write policies to support the use cases using the available analytical techniques in SNYPR
- Prioritize threats with Risk Scoring
- Use Threat Models to boost risk scores
- Build threat models to identify specific patterns of behavior that indicate an advanced threat

Workshop Topics

1. Use Case Development
2. Data Types Overview
3. Data Integration for Content Developers
4. SNYPR Content
5. Analytics
6. Risk Scoring
7. Threat Models

Hands-on Lab Exercises

1. Develop Content for Custom Datasource
2. Create Rule-based Policy
3. Create Behavior-based Policy
4. Create Threat Models

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 understand 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)