Securonix SNYPR Training

SNYPR Bootcamp

Duration: 4 days
Format: Instructor-led
Exam format: Online examination

Description

This course teaches users how to configure SNYPR, integrate data to support the use cases in the SNYPR environment, and manage, monitor, and troubleshoot the platform. It features an introduction to the use case development process and describes the analytics that content developers can apply to detect specific threats, and it describes SNYPR's threat management capabilities from end to end.

Workshop Objectives

- Identify SNYPR components and deployment options
- Identify Spark apps used for each stage in the analytics pipeline
- Install and configure remote ingestion node from RIN package
- Manage the remote ingestion node using SNYPR gateway
- Provision access for Roles, Users, and Groups
- Configure SNYPR Hadoop and application settings
- Troubleshoot Hadoop and SNYPR components by monitoring end to end data flow and SNYPR-Eye
- Standardize and normalize attributes, devices, and events using the OEF
- Configure Data Types to support the use cases in your environment
- Design use cases to meet your business requirements
- Write policies and threat models to support the use cases using the available analytics
- Prioritize threats with risk scores
- Boot risk scores and identify sophisticated attacks with Threat Models
- Use custom dashboards to gain insight into your organization
- Hunt for threats using the various tools in SNYPR
- Configure Workflows to guide incident management
- Manage threats from detection to resolution using the Security Command Center and Incident Management Dashboard
- Monitor and audit the activity in SNYPR to meet compliance regulations
- Run ad-hoc and scheduled reports from built-in templates
- Identify and remediate rogue and outlier access

Workshop Topics

1. SNYPR Architecture
2. Data Flow and Spark jobs
3. Remote Ingestion
4. Access Control
5. Application Settings
6. Platform Monitoring
7. Open Event Format
8. Data Types Overview

9. SNYPR Content
10. Use Case Development Overview
11. Analytics
12. Risk Scoring
13. Threat Models
14. White Lists
15. Security Command Center
16. Data Insights
17. Threat Hunting with Investigation Workbench and Spotter
18. Incident Management
19. Reports and Audit Logs
20. Access Outlier Dashboard
21. Access Review Dashboard

Hands-on Lab Exercises

1. Configure Access Control
2. Configure Application
3. Create Email Templates
4. Import User Data
5. Import Data to Enrich Events
6. Import Activity Data to Support Use Cases
7. Develop Content for Custom Use Case
8. Create Threat Models
9. Reduce the Risk Score of a Violation
10. Create Customized Dashboards
11. Hunt for Threats using Spotter
12. Create a Workflow
13. Manage a Threat from Detection to Resolution
14. Run Categorized and Spotter Reports
15. Investigate Access Outliers

Workshop Requirements

Required Knowledge

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

Technical Requirements

- Laptop
- Reliable Internet connection (LAN/Wi-Fi)
- Most current web browser (Mozilla Firefox, Google Chrome recommended)
- Cisco WebEx Meetings desktop app (for remote workshops only) from https://www.webex.com/downloads.html