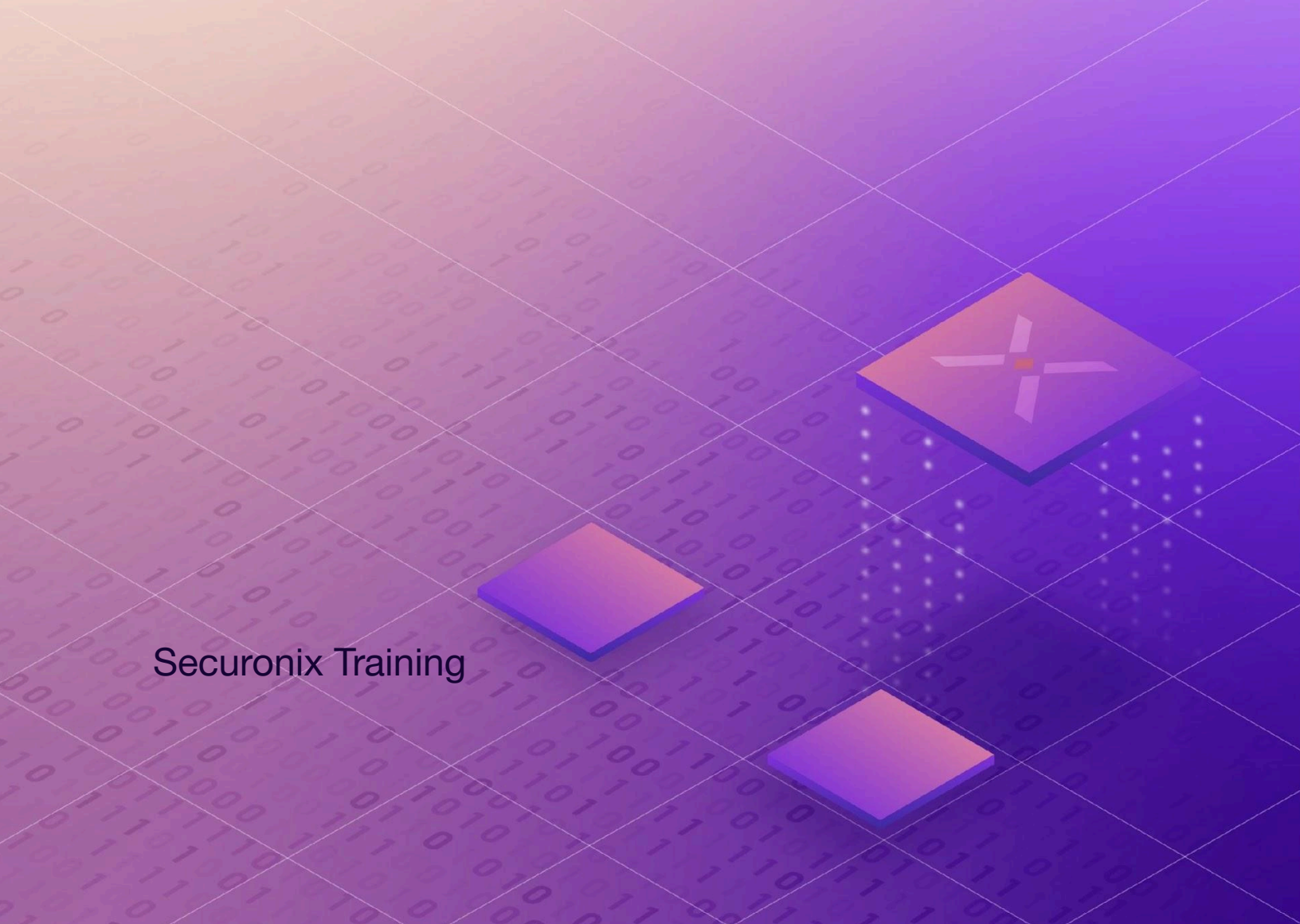
securonix

300 Security Analyst



Securonix Training

securonix

Overview

Duration: 6.5 hours
Format: Self-Paced Learning
Exam format: Online Examination
Labs: Demos and Lab Simulations
Audience: Security Analysts, Incident Handlers, and Threat Hunters
Platform Version: 6.3.1

Description

For informing security professionals and security analysts who need to use the SNYPR Platform to identify and manage threats.

Learn how to interpret and identify threats to your organization, take action on threats, create workflows to manage incidents from detection to resolution, identify rogue or outlier access, and investigate potential threats using the SNYPR search and link analysis features.

Course Topics

1. Analytics.
2. Risk Scoring.
3. Threat Models.
4. White Lists.
5. Security and Command Center.
6. Data Insights.
7. Threat Hunting.
8. Incident Management.
9. Report and Audit Logs.
10. Access Outliers
11. Access Reviews.

© Copyright Securonix 2025. All Rights Reserved.

securonix

Course Objectives

- Understand the Analytical Types Used to Detect Threats in SNYPR.
- Prioritize Threats with Risk Scoring.
- Use Threat Models to Boost Risk Scores.
- Exempt Entities from Monitoring Using White Lists.
- Manage Threats from Detection to Resolution Using the Security and Command Center and Incident Management Dashboard.
- Use Custom Dashboards to Gain Insights Into Your Organization.
- Hunt for Threats Using the Various Tools in SNYPR.
- Manage the Incident Management Lifecycle using workflows.
- Run Ad-hoc and Scheduled Reports from Built-in Templates and Custom Requirements.
- Identity and Remediate Rogue and Outlier Access.

Labs

1. Reduce the risk score of a policy violation.
2. Create customized dashboards.
3. Hunt for threats and perform basic searches using Spotter.
4. Create a custom workflow.
5. Manage a threat from detection to resolution.
6. Run categorized and Spotter reports.
7. Investigate Access Outliers.

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).

© Copyright Securonix 2025. All Rights Reserved.