

## Certified SNYPR Security Analyst

**Duration:** Self-Paced

**Format:** Online

**Exam format:** Online examination

### Description

For information 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.

### Workshop 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 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
- Identify and remediate rogue and outlier access

### Workshop Topics

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

## Hands-on Lab Exercises

1. Reduce 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

## Workshop Requirements

### Required Knowledge

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

### Technical Requirements

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