Administering Splunk SOAR (SP-ASOAR)

COURSE OVERVIEW

This 3 hour course prepares IT professionals to configure and manage SOAR.

PREREQUISITES

- Investigating Incidents with Splunk SOAR

COURSE OBJECTIVES

- SOAR concepts
- Initial configuration
- Apps and assets
- Configuring automation
- User management
- Ingesting data
- Customization and monitoring

COURSE OUTLINE

Topic 1 - Initial Configuration

- Describe SOAR operating concepts
- Identify documentation and community resources
- SOAR & Splunk Architecture
- Product settings
- Access control
- Authentication settings
- Response settings
- Understanding roles
- Creating users
- Managing user access
- Describe SOAR Automation Broker

Administering Splunk SOAR (SP-ASOAR)

COURSE OUTLINE

Topic 1 – Initial Configuration

- Describe SOAR operating concepts
- Identify documentation and community resources
- SOAR & Splunk Architecture
- Product settings
- Access control
- Authentication settings
- Response settings
- Understanding roles
- Creating users
- Managing user access
- Describe SOAR Automation Broker

Topic 2 – Apps, Assets and Playbooks

- Add and configure apps and assets
- Manage playbooks
- Ingesting Data
- Labels and tags
- Event settings

Topic 3 – Customization and Monitoring

- Create custom severity levels
- Create custom status levels
- Add custom fields and CEF settings
- Create custom workbooks
- Run reports
- Use SOAR audit tools
- Monitor system health