# Splunk SOAR

## Course Topics

- Soar topics and concepts
- Installation
- Initial configuration
- Apps and assets
- User management
- Ingesting data
- Events and containers
- Mission control
- Running actions and playbooks
- Case management
- Multi tenancy

## Course Prerequisites

To be successful, students should have a solid understanding of the following:

- Familiarity with Python programming
- Administering in Splunk
- Security in Splunk

## Class Format

Instructor-led lecture with labs. Delivered via virtual classroom or at your site.

## Course Objectives

### Module 1 – Introduction to SOAR

- Describe Phantom operating concepts
- Identify documentation and community resources
- Identify installation options
- Perform initial configuration

### Module 2 – Overview and Features

- Describe SOAR operating concepts
- Identify documentation and community resources

### Module 3 – Why SOAR (Old vs new methodologies)

- Product settings
- Access control
- Authentication settings
- Response settings
- Understanding roles
- Creating users
- Managing user access

## Module 4 – Installation of SOAR

- Identify installation options
- Perform initial configuration

## Module 5 – Architecture Overview

- Splunk Architecture
- Soar Architecture

## Module 6 – Getting Data In

- Identify options to ingest data
- How to do configuration

## Module 7 – Discussion on Investigations and UI

- SOAR investigation concepts
- ROI view
- Using the Analyst Queue
- Using indicators
- Using search

## Module 8 – Discussion on Playbook

- Understand automation best practices
- Design playbooks
- Python support
- Use the playbook manager

## Module 9 – Creation of Playbooks

- Use the visual playbook editor
- Use actions and decisions
- Process action results
- Test new playbooks
- User Interaction and Logic
- Accessing and Formatting Data
- Playbook Development

## Module 10 – Customizations and Monitoring

- Use the SOAR to monitor
- Actions and decisions

## Module 11 – Artifacts in Splunk

- Actions and Customizations
- Reports and Alerts

## Module 12 – Apps and Assets

- Describe how apps and assets work in Phantom
- Add and configure new apps
- Configure assets

**********