



# Administering Splunk SOAR

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

## Course Topics

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

## Prerequisite Knowledge

- *Investigating Incidents with Splunk SOAR*

## Course Format

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

## Course Objectives

### 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

### 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

## About Splunk Education

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

### Certification Tracks

Our certification tracks provide comprehensive education for Splunk customer and partner personnel according to their areas of responsibility.

To view all Splunk Education's course offerings, or to register for a course, go to <http://www.splunk.com/education>

To contact us, email [Education\\_AMER@splunk.com](mailto:Education_AMER@splunk.com)

Splunk, Inc.

270 Brannan St. San Francisco, CA 94107

+1 866.GET.SPLUNK (1 866.438.7758)

[Contact sales](#)