Administering SOAR

This 9-hour course prepares IT and security practitioners to install, configure, and use SOAR in their environment and will prepare developers to attend the playbook development course.

Course Topics

- SOAR modules and concepts
- Installation
- Initial configuration
- Apps and assets
- User management
- Ingesting data
- Investigations
- Running actions and playbooks
- Case management & workflows
- Multi-tenancy & clustering

Prerequisite Knowledge

- None

Course Format

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

Course Objectives

Module 1 – Introduction, Deployment and Installation

- Describe SOAR operating concepts
- Identify documentation and community resources
- Identify installation and upgrade options
- SOAR & Splunk Architecture
- Splunk/SOAR relationships

Module 2 – Initial Configuration

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

Module 3 – Apps, Assets and Playbooks

- Describe how apps and assets work in SOAR
- Add and configure new apps
- Configure assets
- Manage playbooks
- Module 4 –Ingesting Data
- Assets as data sources
- Configuring data polling
- Labels and tags
- Data ingestion management
- Event settings

Module 4 – Ingesting Data

- Assets as data sources
- Configuring data polling
- Labels and tags
- Data ingestion management
- Event settings

Module 5 – Analyst Queue

- Work with the analyst queue
- Filtering and sorting
- Using search
- Container export and import
- Aggregation settings

Module 6 – Investigations

- Use the Investigation page to work on events
- Use indicators to find matching artifacts in multiple events
- Using the heads-up display
- Using notes

Module 7 – Actions, Playbooks and Files

- Manually run actions and examine action results
- Manually run playbooks
- Store related files in events

Module 8 – Case Management and Workbooks

- Use case management for complex investigations
- Use case workflows
- Define new workbooks
- Customize case management

Module 9 – Customization

- Create custom severity levels
- Create custom status levels
- Add custom fields and CEF settings
- Create custom workbooks

Module 10 – Additional Topics

- Run reports
- Use SOAR audit tools
- Monitor system health
- Define clustering best practices
- Configure multi-server SOAR clusters
- Configure multi-tenancy
- Backup/restore

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

Splunk, Inc.

270 Brannan St. San Francisco, CA 94107

+1 866.GET.SPLUNK (1 866.438.7758)

Contact sales