

Administering Splunk SOAR

Summary

This course prepares IT professionals to configure and manage SOAR.

Prerequisites

- To be successful, students must have a working understanding of these courses:
 - Investigating Incidents with Splunk SOAR

Course Outline

Topic 1 –Initial Configuration

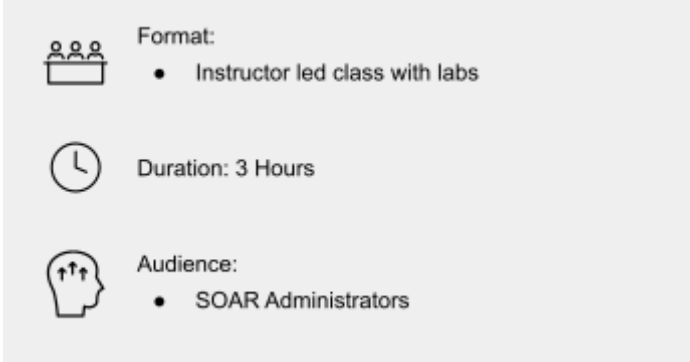
- Describe SOAR operating concepts
- Identify documentation and community resources
- SOAR & Splunk Architecture
- Product settings
- Access control
- Authentication settings
- Response settings
- Understanding roles
- Creating users
- Managing user access
- Describe SOAR Automation Broker

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



Format:

- Instructor led class with labs

Duration: 3 Hours

Audience:

- SOAR Administrators

Appendix: SOAR Automation Broker

About Splunk Education

With Splunk Education, you and your teams can learn to optimize Splunk through self-paced eLearning and instructor-led training, supported by hands-on labs. Explore learning paths and certifications to meet your goals. Splunk courses cover all product areas, supporting specific roles such as Splunk Platform Search Expert, Splunk Enterprise or Cloud Administrator, SOC Analyst or Administrator, DevOps or Site Reliability Engineer, and more. To learn more about our flexible learning options, full course catalog, and Splunk Certification, please visit <http://www.splunk.com/education>.

To contact us, email education@splunk.com.