

## Developing SOAR Playbooks

### Summary

This 9 hour introductory course prepares IT and security practitioners to plan, design, create and debug basic playbooks for SOAR. Students will learn fundamentals of SOAR playbook capabilities, creation and testing. This course is a pre-requisite for the Advanced SOAR Implementation course.

### Prerequisites

- To be successful, students must have a working understanding of these courses:
  - Administering Splunk SOAR
- Additionally, experience with Python programming is useful, but not required.

### Course Outline

#### Module 1 – Introduction to Playbooks

Understand automation best practices

- Design playbooks
- Python support
- Use the playbook manager

#### Module 2 – Visual Playbook Editor

- Use the visual playbook editor
- Use actions and decisions
- Process action results
- Test new playbooks

#### Module 3 – User Interaction and Logic

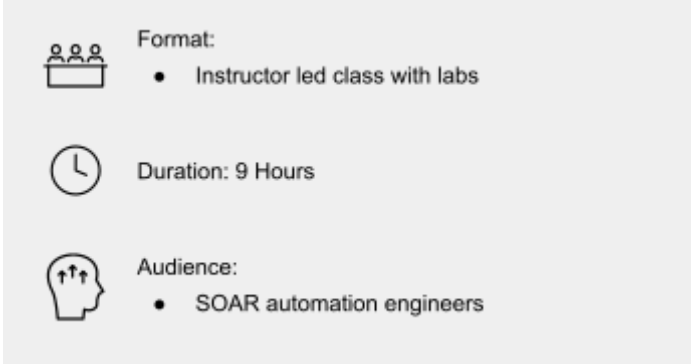
- Interact with users during playbook execution
- Format outputs
- Use decision blocks

#### Module 4 – Accessing and Formatting Data

- Accessing action results
- Accessing artifact and container data
- Formatting data

#### Module 5 – Modular Playbook Development

- Creating input playbooks
- Calling other playbooks
- Passing data between playbooks



**Format:**

- Instructor led class with labs

**Duration:** 9 Hours

**Audience:**

- SOAR automation engineers

## Module 6 – Custom Lists and Filters

- Custom list concepts
- Create custom lists
- Access lists from playbooks
- Use filters

### 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](mailto:education@splunk.com).