

## Developing SOAR Applications




### Summary

This course is for Security Engineers and IT Engineers.

As an IT or security engineer, you want to plan, design, develop and debug basic apps for Splunk SOAR. Apps enable Splunk SOAR to interact with services in order to enrich events, such as geo locating an IP, or respond to a threat, such as resetting a user's password. Apps are already available for many common services. If your Splunk SOAR needs to interact with a service for which no suitable app is available, learn how to create the required app in this course.

### Prerequisites

- To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:
  - Advanced SOAR Implementation
- Additional courses and/or knowledge in these areas are also highly recommended:
  - Basic understanding of programming in Python

	<b>Format:</b> <ul style="list-style-type: none"><li>• Self-paced eLearning</li></ul>
	<b>Duration:</b> 8 Hours
	<b>Audience:</b> <ul style="list-style-type: none"><li>• IT Engineers</li><li>• Security Engineers</li></ul>

### Course Outline

#### Module 1 – Introduction to SOAR Application Development

- Describe SOAR application architecture
- Examine application development documentation
- Configure an environment to develop applications
- Design applications
- Use the App Wizard to start a new app development project

#### Module 2 – Configure a New Application

- List application dependencies and paths
- Map application actions to python functions
- Map application function results to data paths
- Identify steps to code an application

#### Module 3 – Versioning, Debugging, Output Mapping

- Clone apps
- Publish apps to new versions
- Debug apps in the App Wizard
- Map action results to data paths

## 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).