Advanced SOAR Implementation

This 13.5-hour course is intended for experienced SOAR consultants who are responsible for complex SOAR solution development, and will prepare the attendee to integrate SOAR with Splunk as well as develop playbooks requiring custom coding and REST API usage.

Potential attendees have received a passing grade in all prerequisite courses and must ensure they can devote all of their attention to the class, as the coursework is very challenging. Students will develop a custom solution with SOAR, Splunk, and custom Python code. The labs provide requirements for the solution; the student must plan and execute the development. This will require thoughtful focus, experimentation, and problem-solving skills.

Course Topics

- Using external Splunk search in SOAR
- Sending events from Splunk to SOAR
- Updating Splunk events from SOAR
- Running SOAR reports on Splunk
- Executing SOAR playbooks from Splunk
- Searching Splunk from SOAR playbooks
- Writing custom code for use in SOAR Playbooks
- Using the SOAR REST API in SOAR Playbooks

Prerequisite Knowledge

Attendees for this class must ensure that they meet all course prerequisites. This is a challenging, advanced class that draws on technical knowledge from many areas in Splunk and SOAR, and the demanding labs and course schedule leave little time to learn the basics.

To be successful, students should have a solid understanding of the following:

- Experience with Python programming
- Administering Splunk SOAR
- Developing Splunk SOAR Playbooks
- Enterprise Splunk Data Administration
- Enterprise Splunk System Administration
- *Either* Using *or* Administering Splunk Enterprise Security

Course Format

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

Course Objectives

Module 1 – Implementing Splunk and SOAR

- Review of SOAR UI and concepts
- Describe interactions between Splunk and SOAR
- Identify key concepts and data flows
- Prerequisites for integration

Module 2 – Configuring External Splunk Search

- Describe the benefits of externalizing search to Splunk
- Configure the SOAR instance for externalization
- Configure the Splunk instance for externalization
- Use the Splunk app for SOAR Reporting

Module 3 – Sending Splunk Events to SOAR

- Configure the SOAR Add-on for Splunk
- Map CIM fields to CEF
- Send Enterprise Security notables to SOAR
- Automatically trigger SOAR playbooks for Splunk notables

Module 4 – Accessing Splunk from SOAR

- Install and configure the SOAR App for Splunk
- Ingest Splunk events into SOAR
- Use Splunk search from playbooks
- Update Splunk notable events

Module 5 – Custom Coding in Playbooks

- SOAR coding best practices
- Writing, using and managing custom functions
- Using the SOAR API in custom code
- Store and retrieve persistent data

Module 5 – Using SOAR REST

- Use Django queries to search for data in SOAR
- Use REST to access SOAR data
- Use the HTTP app to execute REST from playbooks

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