

Developing Splunk SOAR Playbooks in the Visual Playbook Editor

Summary

This course is for SOAR developers, analysts, and automation engineers.

The course prepares security practitioners to plan, design, create, and test basic Splunk SOAR playbooks in the Visual Playbook Editor (VPE).

Prerequisites

To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:

- Administering Splunk SOAR

Course Outline

Module 1 – Introduction to Playbook Development

- Explain best practice of Splunk SOAR Playbook development
- Identify triggers for playbook execution in Splunk SOAR
- Demonstrate the use of Splunk SOAR playbooks
- Explain playbook concurrency in Splunk SOAR

Module 2 – The Visual Playbook Editor (VPE)

- Navigate the VPE
- Create and configure a playbook using the VPE
- Use the Debugger to test playbooks

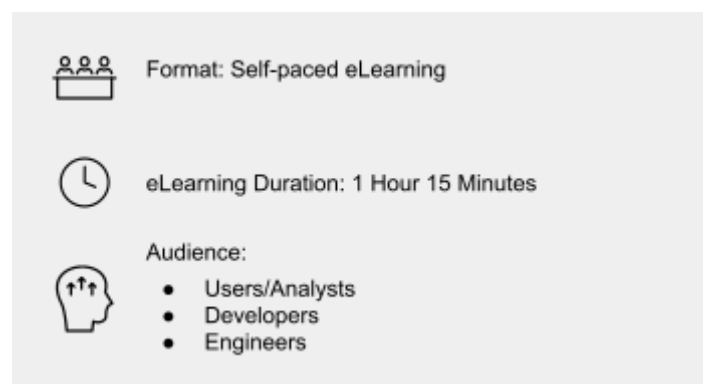
Module 3 – Playbook Data


- Access and navigate different types of data available to a playbook
- Format playbook data


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.



 Format: Self-paced eLearning

 eLearning Duration: 1 Hour 15 Minutes

 Audience:

- Users/Analysts
- Developers
- Engineers