Developing SOAR Playbooks

(SP-DSOARP)

COURSE OVERVIEW

This 9-hour introductory module 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 module 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 (ASOAR)
- Additionally, experience with Python programming is useful, but not required.

COURSE OBJECTIVES

- Automation best practices
- The visual playbook editor
- Creating automation and input playbooks
- Using actions and decisions
- Using action results
- Testing and debugging playbooks
- User interaction
- Output formatting
- Complex logic
- Interacting with artifacts
- Using files in a playbook
- Custom lists
- Data filtering

COURSE OUTLINE

Module 1 - Introduction to Playbooks

- Understand automation best practices
- Design playbooks
- Python support
- Use the playbook manager

Developing SOAR Playbooks (SP-DSOARP)

COURSE OUTLINE

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

Module 6 - Custom Lists and Filters

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