Developing SOAR Playbooks

Course Description:

This 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.

Course Duration:

2 Days

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 Outlines:

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

Module 6 – Custom Lists and Filters

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

Target Audience:

- SOAR Automation Engineers