Using playbooks in SOAR

Playbooks automate security actions at machine speed. Playbooks execute a series of actions across your tools in seconds, versus hours or longer if performed manually. For instance, a playbook can tell your sandbox to detonate a suspected malicious file, while also telling your endpoint security tool to quarantine a device.

Use the following links to access and work with playbooks:

- Playbooks on the Splunk SOAR community (requires an account)
- Playbooks on Splunk Docs
- Splunk SOAR Feature Video: Playbooks

The following are two high-value playbooks to get you started.

AWS IAM find and disable inactive users

This playbook finds AWS user accounts that have the password last used “older than 90 days”, followed by a second playbook that disables the users identified from the first playbook.

Splunk Lantern also features a use case for this playbook that explains more about how to use it.

Malware triage using Crowdstrike Falcon endpoint security

The combination of Crowdstrike and Splunk SOAR allows for a smoother operational flow from detecting endpoint security alerts to operationalizing threat intelligence and automatically taking the first few response steps. This out-of-the-box playbook triages malware detections from Crowdstrike and automates a variety of responses based on an informed decision by an analyst.

Splunk Lantern also features a use case for this playbook that explains more about how to use it.

Indicator Enrichment Playbook

In this short video, you'll learn about the Splunk Intelligence Management Indicator Enrichment playbook for Splunk SOAR.
Additional resources

- Support Docs:
  - Splunk Intelligence Management - SOAR user guide
  - SOAR (Phantom) docs for TruSTAR App

- Blog:
  - SOAR in seconds