Recorded Future®

SOAR
SOLUTION
OVERVIEW

Splunk SOAR: Recorded Future Artifact Enrichment Playbook

Use Case

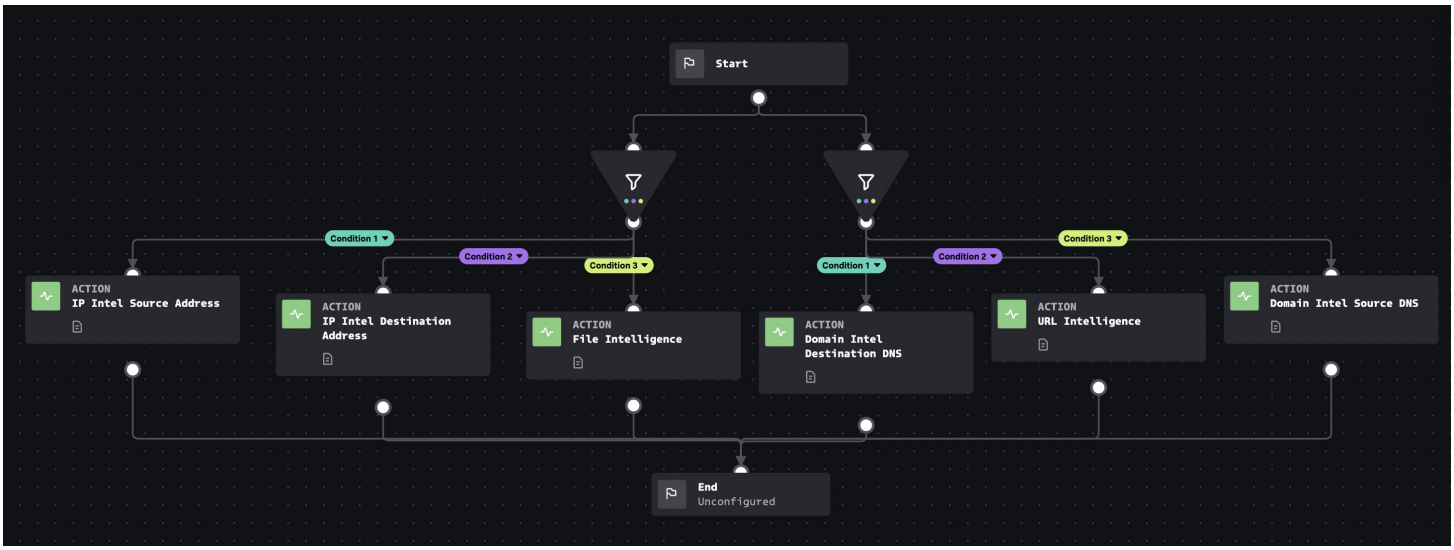
One of the first main use cases for any SOAR tool is to automate enriching indicators with threat intelligence. Automating this process is practicable and will reduce cycle time for analysts when assessing the severity of incidents.

Issue

Without automation, the typical process for enriching an indicator can take minutes. This can generate hours of analyst work when a typical day involves investigating dozens if not hundreds of indicators.

Solution

This playbook enriches ingested artifacts that contain file hashes, IP addresses, domain names, or URLs in some of the most common CEF fields. This enrichment pulls a variety of threat intelligence details from Recorded Future into the investigation, allowing further analysis and contextual actions.



Technical

From a technical perspective the integration will need configured:

- The Recorded Future app for Splunk SOAR installed and configured **https://splunkbase.splunk.com/app/6050**

This service will require the SecOps or Threat Intelligence Module, and the Splunk SOAR Integration. The playbook will be included with the Recorded Future App on the Splunk SOAR marketplace.