Recorded Future®

SOAR
SOLUTION
OVERVIEW

# Splunk SOAR: Playbooks to Update Recorded Future Watchlists

## Use Case

Many Recorded Future alerts are driven and powered by watch lists. Oftentimes, these watch lists store information like Vulnerabilities, IP addresses, or even AWS keys.

## Issue

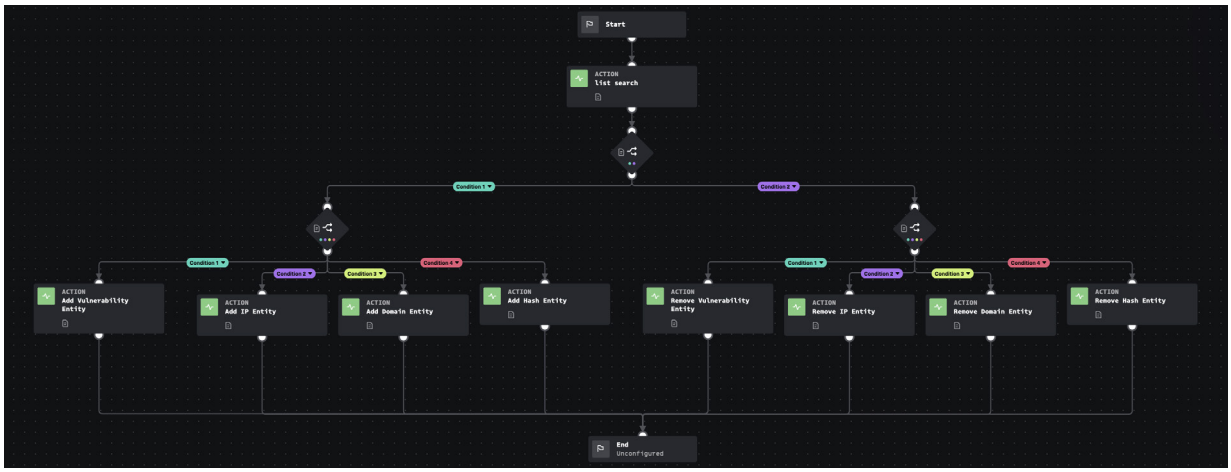
All organizations want alerts generated based on accurate and up to date watch lists. Without automation, watch lists become stale and out of date. Relying on manual intervention to update watch lists can become unreliable and will oftentimes go forgotten.

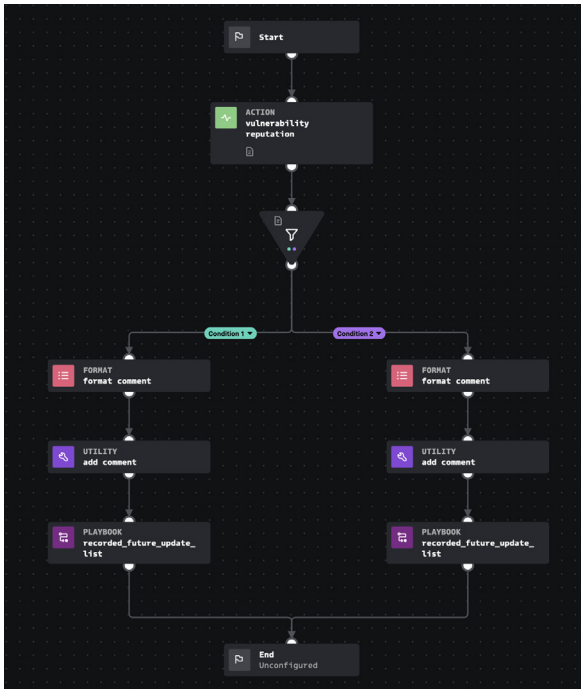
## Solution

These playbooks can be used to update your organization's watch lists in an automated manner resulting in fresh and accurate information. Included are two playbooks.

The first playbook is designed to be a sub-playbook used in other workflows. The sub-playbook accepts 4 inputs: Entity Name, Entity Type, List Name, and Operation (add/remove)

The second playbook demonstrates enriching vulnerabilities from a hypothetical vulnerability scanner and adding all vulnerabilities with a risk score greater than 90 to a Vulnerability Watch List. The playbook appears simple due to utilizing the sub-playbook previously mentioned.




## Technical

From a technical perspective this playbook will need the following configured:

- The Recorded Future for Splunk SOAR installed and configured **https://splunkbase.splunk.com/app/5908**

**This service will require the Threat Intelligence Module, Vulnerability Intelligence Module (For the Vulnerability playbook), and the Splunk SOAR integration. The playbooks will be included with the Recorded Future App on the Splunk SOAR marketplace and on the Recorded Future support site.**