SOAR
SOLUTION
OVERVIEW

# Splunk SOAR: Recorded Future Vulnerability Alert Handling

## Use Case

Timely and accurate vulnerability assessment is critical. The security gained by remediating some vulnerabilities is dramatically higher than remediating others. Security Intelligence helps identify which vulnerabilities are relevant to your organization's attack surface so you can focus patching and remediation on what matters the most to you.

Recorded Future provides vulnerability alerts on predefined criteria. To name a few are vulnerabilities targeting products in your organization’s tech stack, critical or pre NVD vulnerabilities, or sourced directly from Insikt Group research. These alerts will provide your organization with relevant vulnerabilities to be searched for within your environment.

## Issue

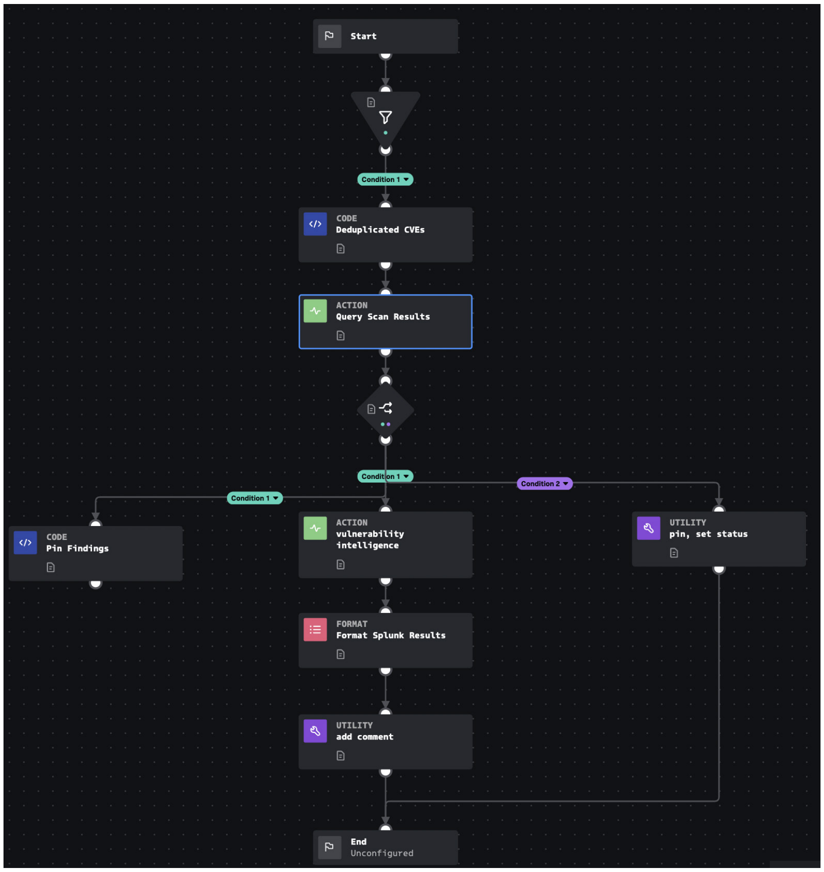
Vulnerability management, Security Operations, and Threat Intelligence teams are often siloed from one another. A Threat Intelligence or Security Operations team needs a way to instantly check if a vulnerability impacts an asset in their environment without needing to manually verify with a human, which can often take hours or days.

## Solution

This playbook responds to several Recorded Future’s vulnerability alerts including:

- Global Vulnerability Risk, New Critical or Pre NVD Vulnerabilities
- Global Vulnerability Risk, Vulnerabilities Recently Linked to Malware
- Global Vulnerability Risk, Vulnerabilities, New Exploit Chatter

The alert ingests into a Splunk SOAR container utilizing the Recorded Future app’s fetch feature. All evidence details within the alert are parsed and added as artifacts, automatically. Each CVE contained in the Vulnerability alert extracts and formats into a Splunk search. Assuming the organization's vulnerability scan results are ingested and indexed within Splunk, the search runs and looks for matches. Any matches return into the Splunk SOAR container. This process eliminates any manual searching or communication between teams for vulnerabilities existing in the environment.



## Technical

From a technical perspective the integration will need configured:

- Splunk Enterprise with read capability from Splunk SOAR
- Vulnerability scans from your vendor ingested into Splunk Enterprise
- The Recorded Future app for Splunk SOAR installed and configured **https://splunkbase.splunk.com/app/6050**

**This service will require the Recorded Future Vulnerability Intelligence Module, the Splunk SOAR Integration, and a Splunk Enterprise / Enterprise Security instance with connectivity to Splunk SOAR. The playbook will be included with the Recorded Future App on Splunk SOAR.**

### ABOUT RECORDED FUTURE

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries. Learn more at recordedfuture.com.

www.recordedfuture.com @RecordedFuture