Splunk SOAR Reference Architecture

Capabilities and Benefits

Created by: Recorded Future Professional Services

Published: October, 2023
Updated: January, 2024

Summary 2
Integration 3
Overview 3
Apps 4
Recorded Future for Splunk SOAR 4
Recorded Future Sandbox 4
Playbooks 5
Use Cases 8
Artifact Enrichment 8
Use Case Summary 8
Issue 8
Solution 8
Threat Map Hunting 10
Use Case Summary 10
Issue 10
Solution 10
Sandbox Detonation 13
Use Case Summary 13
Issue 14
Solution 14
Watch List Management 15
Use Case Summary 15
Issue 15
Solution 15
Dynamic Blocking 17
Use Case Summary 17
Issue 17
Solution 17
Vulnerability Alert Handling 21
Use Case Summary 21
Issue 21
Solution 21
Leaked Credential Alert Handling 23
Use Case Summary 23
Issue 23
Solution 23
Additional Reading 25
Professional Services Assistance 25

Summary

This reference architecture aims to give the reader an understanding of the capabilities achievable with the Recorded Future integration into the Splunk SOAR. This document also outlines use cases implemented by our customers in the field.

Recorded Future provides two separate apps available in the Splunk SOAR marketplace.

The Recorded Future for Splunk SOAR app provides many actions that enable the creation of playbooks to automate enrichment, threat hunting, alert handling, maintaining watchlists, and more. *This app can be found on Splunkbase here.*

The Recorded Future Sandbox for Splunk SOAR app can submit and detonate both files and URLs to the Recorded Future Sandbox and fetch reports back into the Splunk SOAR container. *This app can be found on Splunkbase here.*

Integration

This section provides the reader an understanding of the Recorded Future for Splunk SOAR integrations and available playbooks to download.

Overview

Security Operation teams require external and internal threat intelligence to rapidly identify and respond to known threats, eliminating the need for redundant analysis that specialized intelligence organizations have already performed.

Security teams can use multiple Recorded Future apps within Splunk SOAR to leverage Recorded Future's APIs for premium threat intelligence within existing workflows. The below Recorded Future features can integrate into Splunk SOAR.

- **Recorded Future Alerts**
  Both traditional and playbook alerts are compatible for ingestion and support write-back capability from Splunk SOAR. Write-back capabilities include modifying the alert status and writing back notes/comments.

- **Recorded Future Enrichment**
  Enrichment is the most common integration use case. Typically, a partner application workflow may lead to a single or small set of entities that require additional context (e.g., an IP address from which suspicious traffic has been observed or an unpatched server with a known vulnerability of unknown risk).

  Enrichment taps into Recorded Future's extensive and rich context to pull in risk scores, risk evidence, related entities, and example references from various source types (e.g., social media, security research blogs, dark web).

- **Recorded Future Lists**
  The List API, built into the integration, allows clients to create and update lists in the Recorded Future Portal. These are typically custom lists or Watch Lists that power custom queries, threat views, and alerts. The app's actions complement and extend the ability for users to maintain these lists.

- **Recorded Future Collective Insights**
  Collective Insights aggregates detections across your Splunk SOAR incidents to show trends across all detections. By prioritizing your actions based on which observed correlations and TTPs are most common across your organization, Collective Insights helps you better protect your infrastructure. Submitting your detections to Collective insights, you will power your Threat Maps to the fullest.

- **Recorded Future Threat Maps**
  The Threat Actor threat map provides a structured, repeatable method of identifying and prioritizing threat actors relevant to your enterprise and plotting them based on their values for potential intent and estimated opportunity.

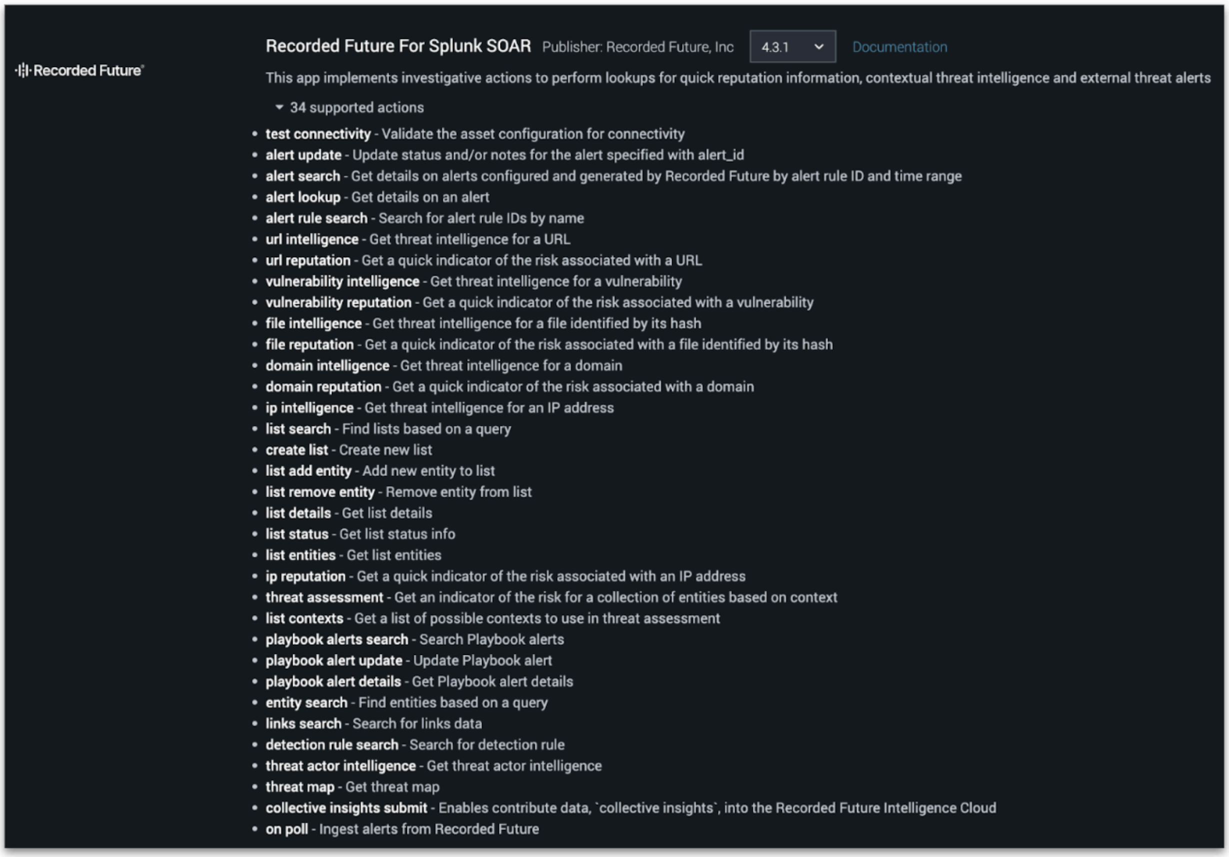
  With the integration, you can ingest the threat map into your Splunk SOAR containers to facilitate automated threat hunts. A Threat Actor enrichment action exists to compliment this.

Apps

Recorded Future built and maintains two apps in the Splunk SOAR marketplace.

Recorded Future for Splunk SOAR

The Recorded Future for Splunk SOAR app is at the core of this integration, enabling Recorded Future intelligence to propagate into and out of containers. This app utilizes several Recorded Future API endpoints to pull and push intelligence back and forth between Splunk SOAR and Recorded Future.



Recorded Future For Splunk SOAR Publisher: Recorded Future, Inc

This app implements investigative actions to perform lookups for quick reputation information, contextual threat intelligence and external threat alerts

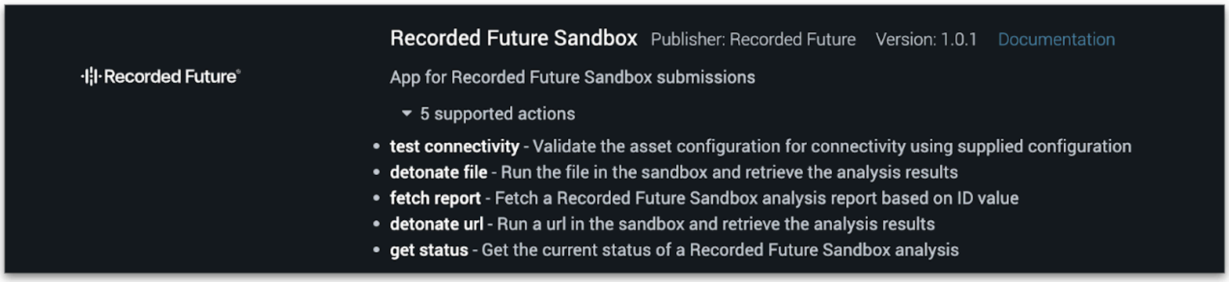
34 supported actions

- **test connectivity** - Validate the asset configuration for connectivity
- **alert update** - Update status and/or notes for the alert specified with alert_id
- **alert search** - Get details on alerts configured and generated by Recorded Future by alert rule ID and time range
- **alert lookup** - Get details on an alert
- **alert rule search** - Search for alert rule IDs by name
- **url intelligence** - Get threat intelligence for a URL
- **url reputation** - Get a quick indicator of the risk associated with a URL
- **vulnerability intelligence** - Get threat intelligence for a vulnerability
- **vulnerability reputation** - Get a quick indicator of the risk associated with a vulnerability
- **file intelligence** - Get threat intelligence for a file identified by its hash
- **file reputation** - Get a quick indicator of the risk associated with a file identified by its hash
- **domain intelligence** - Get threat intelligence for a domain
- **domain reputation** - Get a quick indicator of the risk associated with a domain
- **ip intelligence** - Get threat intelligence for an IP address
- **list search** - Find lists based on a query
- **create list** - Create new list
- **list add entity** - Add new entity to list
- **list remove entity** - Remove entity from list
- **list details** - Get list details
- **list status** - Get list status info
- **list entities** - Get list entities
- **ip reputation** - Get a quick indicator of the risk associated with an IP address
- **threat assessment** - Get an indicator of the risk for a collection of entities based on context
- **list contexts** - Get a list of possible contexts to use in threat assessment
- **playbook alerts search** - Search Playbook alerts
- **playbook alert update** - Update Playbook alert
- **playbook alert details** - Get Playbook alert details
- **entity search** - Find entities based on a query
- **links search** - Search for links data
- **detection rule search** - Search for detection rule
- **threat actor intelligence** - Get threat actor intelligence
- **threat map** - Get threat map
- **collective insights submit** - Enables contribute data, `collective insights`, into the Recorded Future Intelligence Cloud
- **on poll** - Ingest alerts from Recorded Future

Recorded Future for Splunk SOAR Actions

Recorded Future Sandbox

The Recorded Future Sandbox for Splunk SOAR app provides additional capabilities separate from the Recorded Future for Splunk SOAR app. These actions include submitting files and URLs to the Recorded Future sandbox for static and dynamic behavioral analysis and fetching the reports into Splunk SOAR.



Recorded Future Sandbox Publisher: Recorded Future Version: 1.0.1

App for Recorded Future Sandbox submissions

5 supported actions

- **test connectivity** - Validate the asset configuration for connectivity using supplied configuration
- **detonate file** - Run the file in the sandbox and retrieve the analysis results
- **fetch report** - Fetch a Recorded Future Sandbox analysis report based on ID value
- **detonate url** - Run a url in the sandbox and retrieve the analysis results
- **get status** - Get the current status of a Recorded Future Sandbox analysis

Recorded Future Sandbox for Splunk SOAR Actions

Playbooks

Playbooks allow clients to unlock the full value of the Recorded Future for Splunk SOAR integration. By utilizing playbooks, clients can chain together and pass data from one action to another.

Recorded Future owns and maintains a library of template playbooks available to download for client use on our support site. The table below outlines each of these playbooks, their capabilities and dependant modules:

Playbook Name	Playbook Description	Module Dependencies
Artifact Enrichment	Enrich ingested artifacts containing file hashes, IP addresses, domain names, or URLs via CEF fields. This enrichment pulls a variety of threat intelligence details from Recorded Future into the investigation, allowing further analysis and contextual actions.	SecOps Intelligence or Threat Intelligence
Recorded Future Sandbox Detonation and Enrichment	Submit a URL or File to the Recorded Future Sandbox, detonate the samples, and return the reports.	SecOps Intelligence or Threat Intelligence
Threat Hunting	Starting with a single IP address, this playbook gathers a list of linked IP addresses, domain names, file hashes, URLs, and vulnerability CVEs from Recorded Future. Then Splunk is used to build threat hunting lookup tables and search across multiple data sources for events containing the linked entities. Lastly, IP addresses are blocked if approved by an analyst and an email is sent to notify a responder of the activity.	SecOps Intelligence or Threat Intelligence and Vulnerability Intelligence (for CVE enrichment)

Playbook Name	Playbook Description	Module Dependencies
Automated Hunting with Recorded Future Threat Maps	**recorded_future_threat_map_pull:** This playbook will pull the Recorded Future threat map, extract each Threat Actor, create an artifact for each Threat Actor (threat_actor), and create new events/cases for any Threat Actor with an intent or opportunity score >= 90 and apply the threat actor label to newly created containers. **recorded_future_threat_map_actor_hunt:** Events/Cases with the Threat Actor label, with threat_actor artifacts, will trigger this playbook and search your Splunk instance for any links related to the threat_actor. The Splunk searches will use data models. If there are matches, they will be enriched with Recorded Future and pinned to the HUD.	Threat Intelligence and Vulnerability Intelligence (for CVE enrichment)
Leaked Credential Alert Handling	This playbook shows suggested steps triaging traditional leaked credential alerts regarding active directory.	Brand Intelligence
Typosquat Alert Handling	This playbook shows suggested steps for triaging traditional typosquat alerts.	Brand Intelligence
Vulnerability Alert Handling Vulnerability Playbook Alert Handling	Ingest the CVE alert into a Splunk SOAR container utilizing the Recorded Future app's fetch feature and extract the evidence details. Each CVE contained in the vulnerability alert is extracted and formatted into a Splunk search and ran against the Splunk instance.	Vulnerability Intelligence

Playbook Name	Playbook Description	Module Dependencies
List Management	Two template playbooks demonstrating maintaining Recorded Future watch lists. The Update List playbook is used as a sub-playbook in other automation workflows and will either add or remove an entity based on the input. The Vulnerability Watch List playbook demonstrates using the sub-playbook to add and remove hypothetical vulnerability scans to and from a Vulnerability Watch List.	SecOps Intelligence or Threat Intelligence and Vulnerability Intelligence (for vulnerability playbook)

Use Cases

This section provides an overview of the use cases that Recorded Future builds and maintains for clients. Use cases are broken down by:

- Summary or Purpose of the identified use case
- Issue Description
- Proposed Solution

For any custom use cases contact Professional Services at Recorded Future.

Artifact Enrichment

This use case describes automating artifact enrichment for use within the triage and analysis stages of an investigation.

Use Case Summary

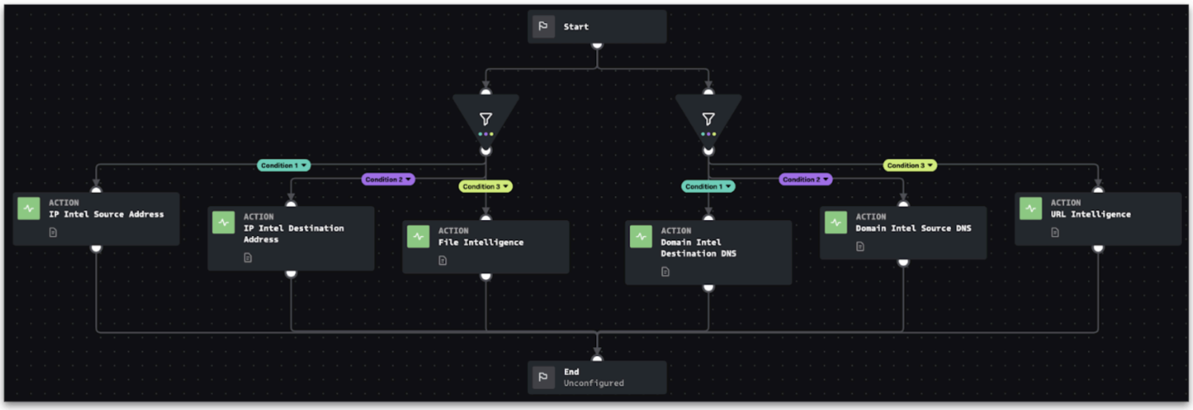
One of the main use cases for any SOAR tool is to automate enriching indicators with threat intelligence. Automating this process is practicable and will reduce cycle time for analysts when assessing the severity of incidents.

Issue

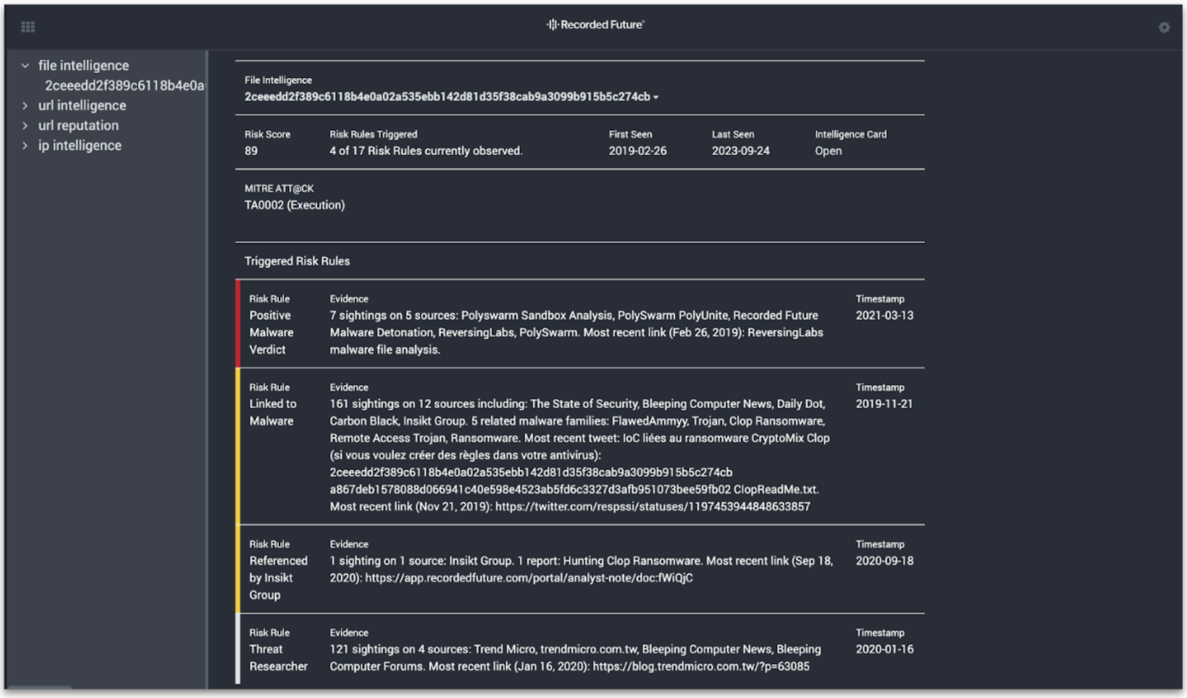
Without automation, the typical process for enriching an indicator can take minutes. At first, minutes may not seem a lot, but this will add up to hours of analyst work considering a typical day may involve investigating dozens if not hundreds of indicators.

Solution

This playbook automatically enriches artifacts containing file hashes, IP addresses, domain names, and URLs via CEF fields. This enrichment pulls a variety of threat intelligence details from Recorded Future into the investigation, allowing further analysis and contextual actions including: Risk Score, Risk Rules, Evidence Details.



Recorded Future Artifact Enrichment Playbook



File Intelligence
2ceeedd2f389c6118b4e0a02a535ebb142d81d35f38cab9a3099b915b5c274cb

Risk Score	Risk Rules Triggered	First Seen	Last Seen	Intelligence Card
89	4 of 17 Risk Rules currently observed.	2019-02-26	2023-09-24	Open

MITRE ATT@CK
TA0002 (Execution)

Triggered Risk Rules

Risk Rule	Evidence	Timestamp
Positive Malware Verdict	7 sightings on 5 sources: Polyswarm Sandbox Analysis, PolySwarm PolyUnite, Recorded Future Malware Detonation, ReversingLabs, PolySwarm. Most recent link (Feb 26, 2019): ReversingLabs malware file analysis.	2021-03-13
Linked to Malware	161 sightings on 12 sources including: The State of Security, Bleeping Computer News, Daily Dot, Carbon Black, Insikt Group. 5 related malware families: FlawedAmmyy, Trojan, Clop Ransomware, Remote Access Trojan, Ransomware. Most recent tweet: IoC liées au ransomware CryptoMix Clop (si vous voulez créer des règles dans votre antivirus): 2ceeedd2f389c6118b4e0a02a535ebb142d81d35f38cab9a3099b915b5c274cb a867deb1578088d066941c40e598e4523ab5fd6c3327d3afb951073bee59fb02 ClopReadMe.txt. Most recent link (Nov 21, 2019): https://twitter.com/respssi/statuses/1197453944848633857	2019-11-21
Referenced by Insikt Group	1 sighting on 1 source: Insikt Group. 1 report: Hunting Clop Ransomware. Most recent link (Sep 18, 2020): https://app.recordedfuture.com/portal/analyst-note/doc:fWiQjC	2020-09-18
Threat Researcher	121 sightings on 4 sources: Trend Micro, trendmicro.com.tw, Bleeping Computer News, Bleeping Computer Forums. Most recent link (Jan 16, 2020): https://blog.trendmicro.com.tw/?p=63085	2020-01-16

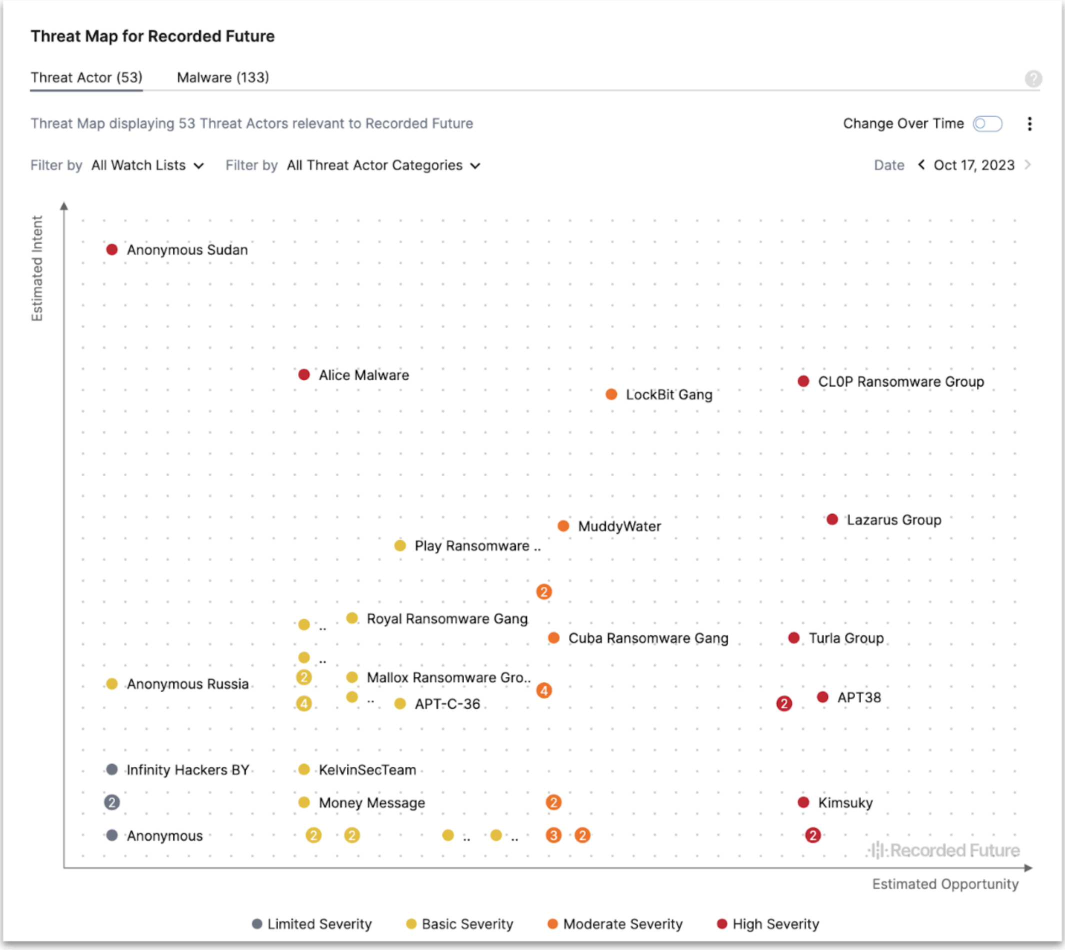
Recorded Future Intelligence Enrichment

Threat Map Hunting

This use case describes how to automate hunting within Splunk SOAR and Splunk Enterprise via the use of Recorded Future Threat Maps.

Use Case Summary

The Threat Actor Threat Map provides a structured, repeatable method of identifying and prioritizing threat actors relevant to your enterprise and plotting them based on their values for potential intent and estimated opportunity. These threat actors are often associated with indicator links which can be used to hunt for activity in your environment. Sandbox and collective insight submissions influence the threat actor's opportunity and intent scores.



Threat Map for Recorded Future

Threat Actor (53) Malware (133)

Threat Map displaying 53 Threat Actors relevant to Recorded Future

Change Over Time

Filter by All Watch Lists Filter by All Threat Actor Categories

Date Oct 17, 2023

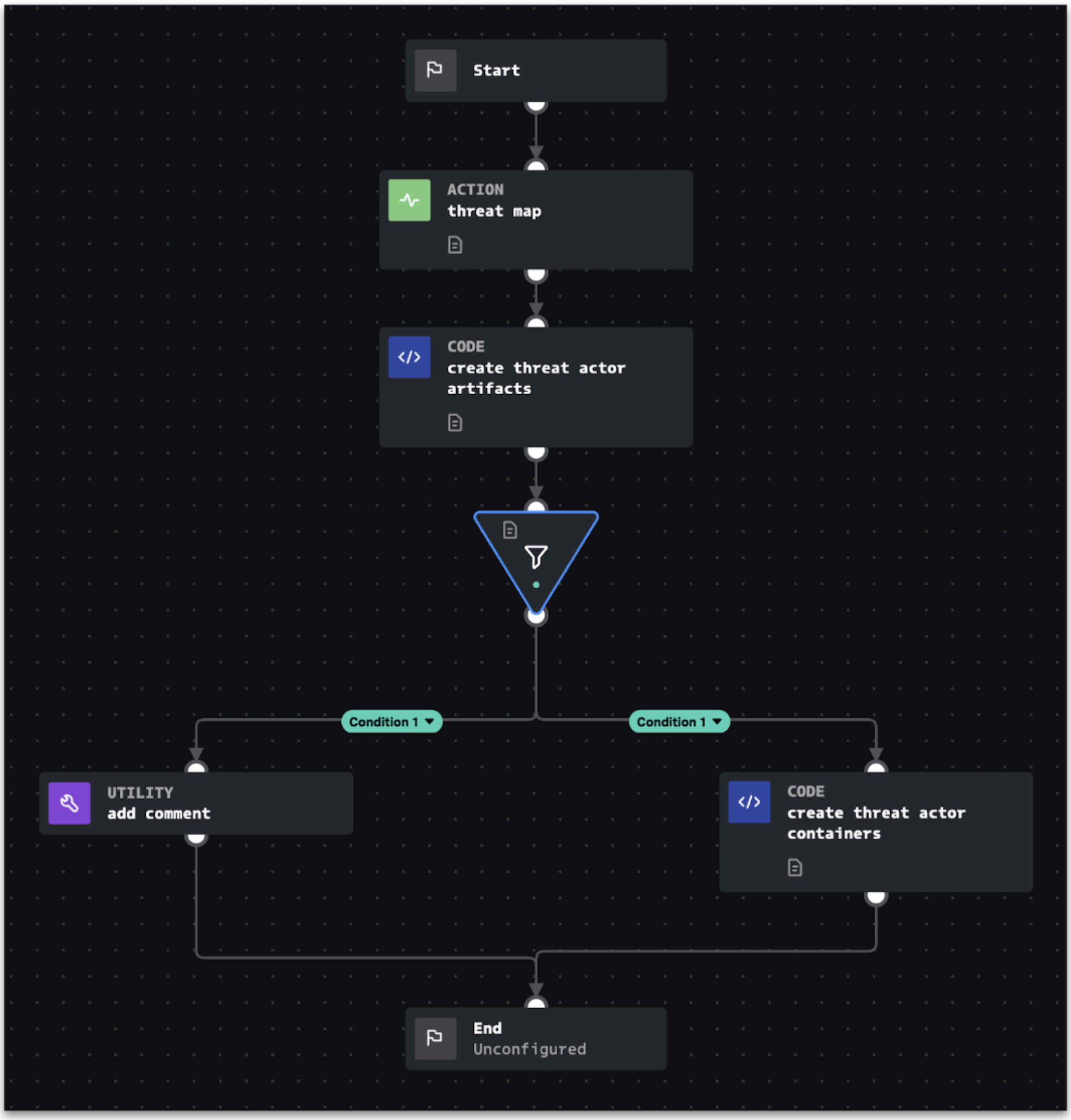
Recorded Future Threat Map

Issue

Organizations with a lack of speciality identifying attack linkages or a shortage of resources need help to reduce the time involved with proactive threat hunting. Often, a single threat actor may have dozens of indicators linked to them. Strained for resources, running dozens of manual Splunk searches can be time-consuming.

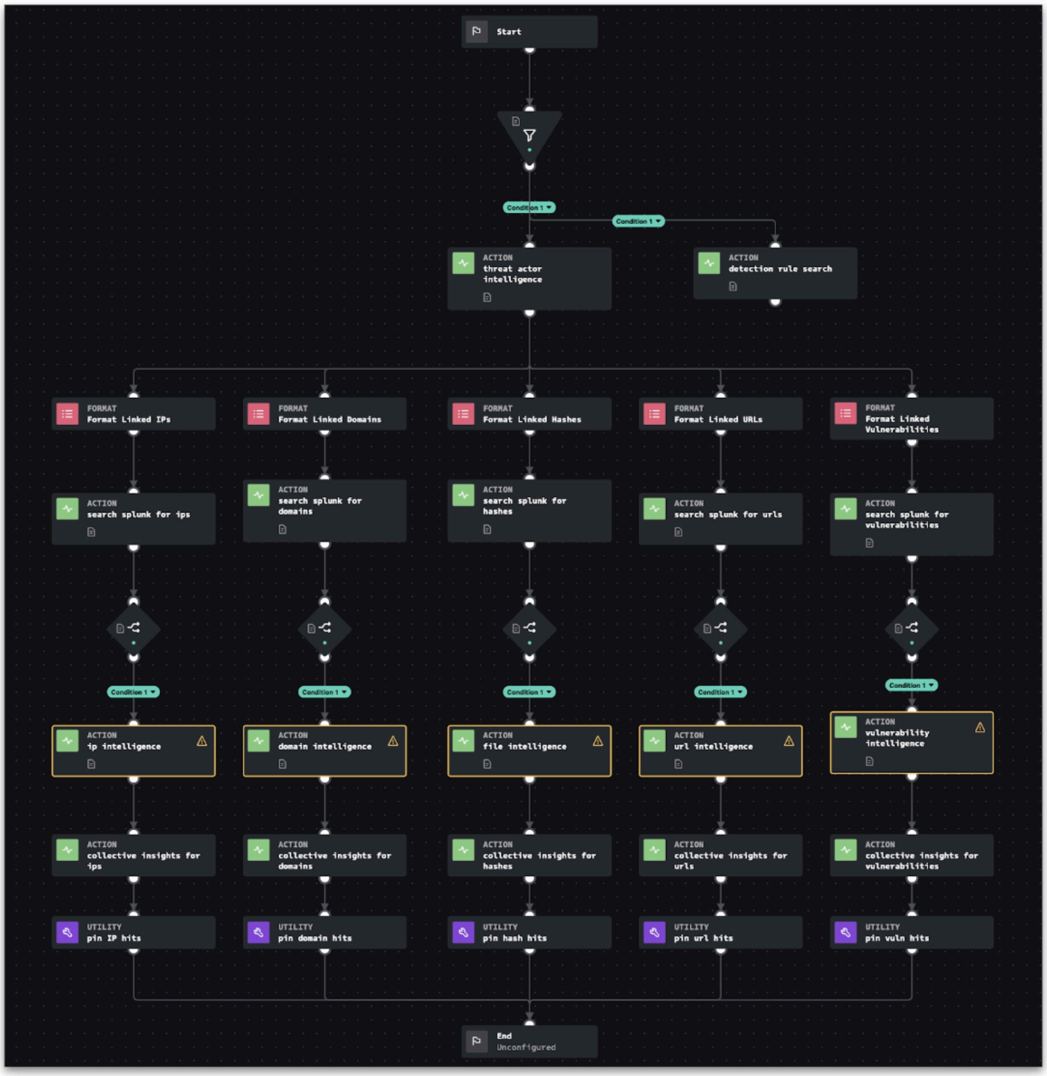
Solution

With two playbooks, you can automatically hunt for threat actor activity using Recorded Future's threat map in combination with Splunk SOAR and Splunk Enterprise. The first playbook ingests the Recorded Future threat map into Splunk SOAR. A container will populate and store the entire Threat Map. Then, the playbook creates individual containers for each threat actor whose opportunity or intent score satisfies a threshold for hunting. These events will trigger the second playbook.

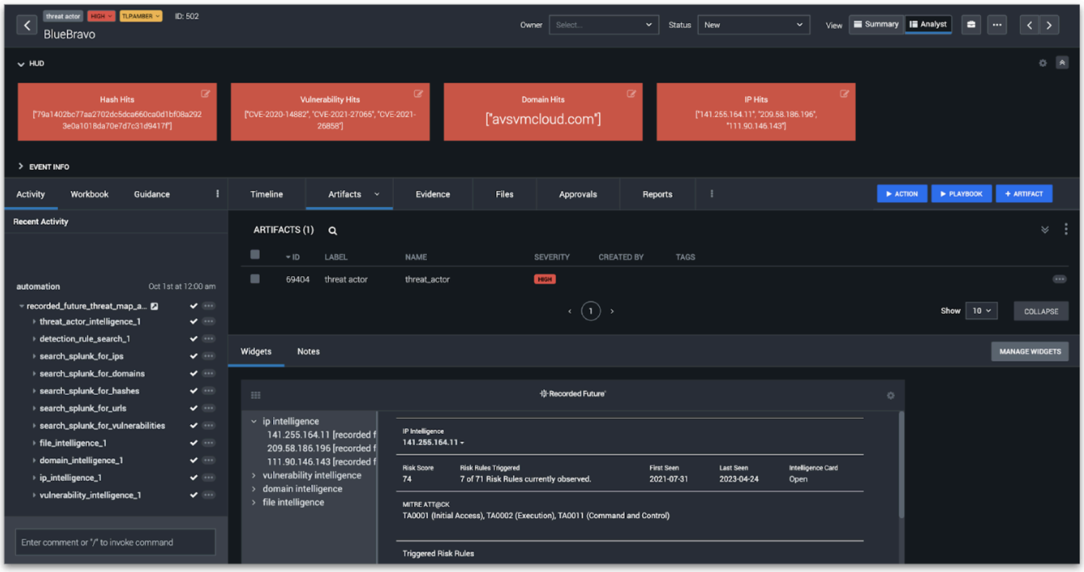


[Recorded Future Threat Map Pull](#)

The second playbook will enrich each Threat Actor with technical links and then format the links into Splunk search queries to run across your Splunk instance. Splunk SOAR will fetch the results, download YARA, Sigma, and Snort detection rules, and attach them to the vault.



[Recorded Future Threat Actor Hunt]()



ID: 502

BlueBravo

Status: New

Hash Hits
['79a1402bc77aa2702dc5dca660ca0d1bf08a292 3e0a1018da70e7d7c31d9417f']

Vulnerability Hits
['CVE-2020-14882', 'CVE-2021-27065', 'CVE-2021-26858']

Domain Hits
['avsvmcloud.com']

IP Hits
['141.255.164.11', '209.58.186.196', '111.90.146.143']

ARTIFACTS (1)

ID	LABEL	NAME	SEVERITY	CREATED BY	TAGS
69404	threat actor	threat_actor	HIGH		

automation Oct 1st at 12:00 am

- recorded_future_threat_map_a... ✓
  - threat_actor_intelligence_1 ✓
  - detection_rule_search_1 ✓
  - search_splunk_for_ips ✓
  - search_splunk_for_domains ✓
  - search_splunk_for_hashes ✓
  - search_splunk_for_urls ✓
  - search_splunk_for_vulnerabilities ✓
  - file_intelligence_1 ✓
  - domain_intelligence_1 ✓
  - ip_intelligence_1 ✓
  - vulnerability_intelligence_1 ✓

- ip intelligence
  - 141.255.164.11 [recorded f
  - 209.58.186.196 [recorded f
  - 111.90.146.143 [recorded f
- vulnerability intelligence
- domain intelligence
- file intelligence

IP Intelligence
141.255.164.11

Risk Score	Risk Rules Triggered	First Seen	Last Seen	Intelligence Card
74	7 of 71 Risk Rules currently observed.	2021-07-31	2023-04-24	Open

MITRE ATT@CK
TA0001 (Initial Access), TA0002 (Execution), TA0011 (Command and Control)

Triggered Risk Rules

Threat Actor Splunk SOAR Container

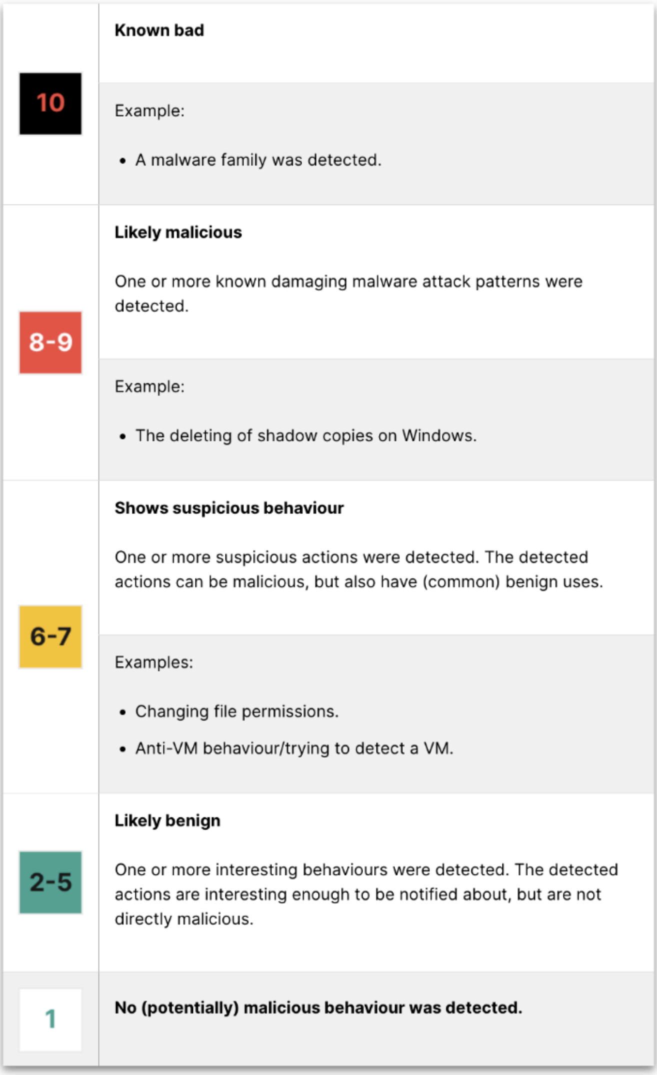
Sandbox Detonation

This use case describes how to automate submitting samples to the Recorded Future Sandbox.

Use Case Summary

End users in organizations often report phishing emails for security analysts to investigate. These emails report to a designated email inbox, often within Exchange. These emails sometimes include attachments and URLs that are dangerous to visit or explore manually. The Recorded Future Sandbox allows analysts to submit these files and URLs for analysis.

The sandbox uses 1 - 10 scoring to reflect whether something is malicious or not. The following is an explanation of what each score means and what can cause this score.



10	**Known bad** Example: • A malware family was detected.
8-9	**Likely malicious** One or more known damaging malware attack patterns were detected. Example: • The deleting of shadow copies on Windows.
6-7	**Shows suspicious behaviour** One or more suspicious actions were detected. The detected actions can be malicious, but also have (common) benign uses. Examples: • Changing file permissions. • Anti-VM behaviour/trying to detect a VM.
2-5	**Likely benign** One or more interesting behaviours were detected. The detected actions are interesting enough to be notified about, but are not directly malicious.
1	**No (potentially) malicious behaviour was detected.**

Note: *It is important to look at the actual signatures that triggered. The score is determined by these.*

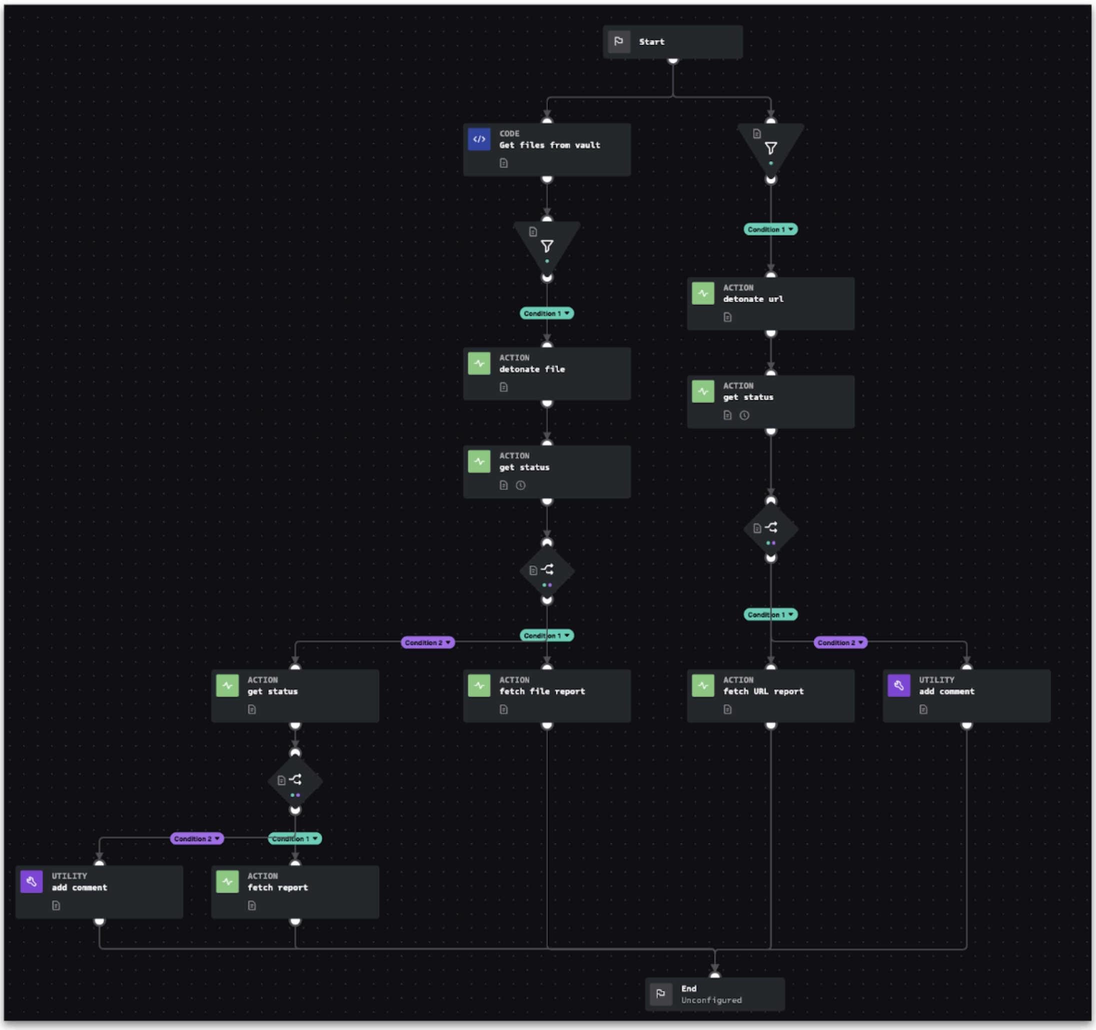
Issue

Manually submitting a handful of file submissions each day is fine. However, as the threshold of files needed to investigate rises, this process can consume hours of analyst cycle time per day. Keeping up with phishing email submissions can be tedious, mundane, and manual. Often, analysts ignore these submissions even though they can contain critical warnings of an incoming security incident.

Solution

Using the poll capability with the EWS for Office 365 app within Splunk, phishing emails can be automatically ingested into Splunk SOAR and converted into artifacts, including email headers, bodies, and file attachments. This playbook responds to these incoming emails. The playbook extracts any files that are added from the phishing email to the vault and uploads them to the Recorded Future Sandbox API for analysis. After completing the submission report, all results return to the Splunk SOAR container, and the same for any URLs referenced in the phishing email.

These results can be used to determine the maliciousness of the email and passed into further automation, such as enterprise searches throughout the organization for similar emails, blocking related URLs and IP addresses from end users' systems, or starting endpoint scans or quarantines.



Recorded Future Sandbox Detonation Playbook

Watch List Management

This use case describes how to interact with Recorded Future Watch Lists by adding and removing entities.

Use Case Summary

Many Recorded Future alerts are driven and powered by watch lists. Often, these watch lists store information like Vulnerabilities, IP addresses, or even AWS keys. This playbook is able to maintain these watch lists by adding and removing various entities.

Issue

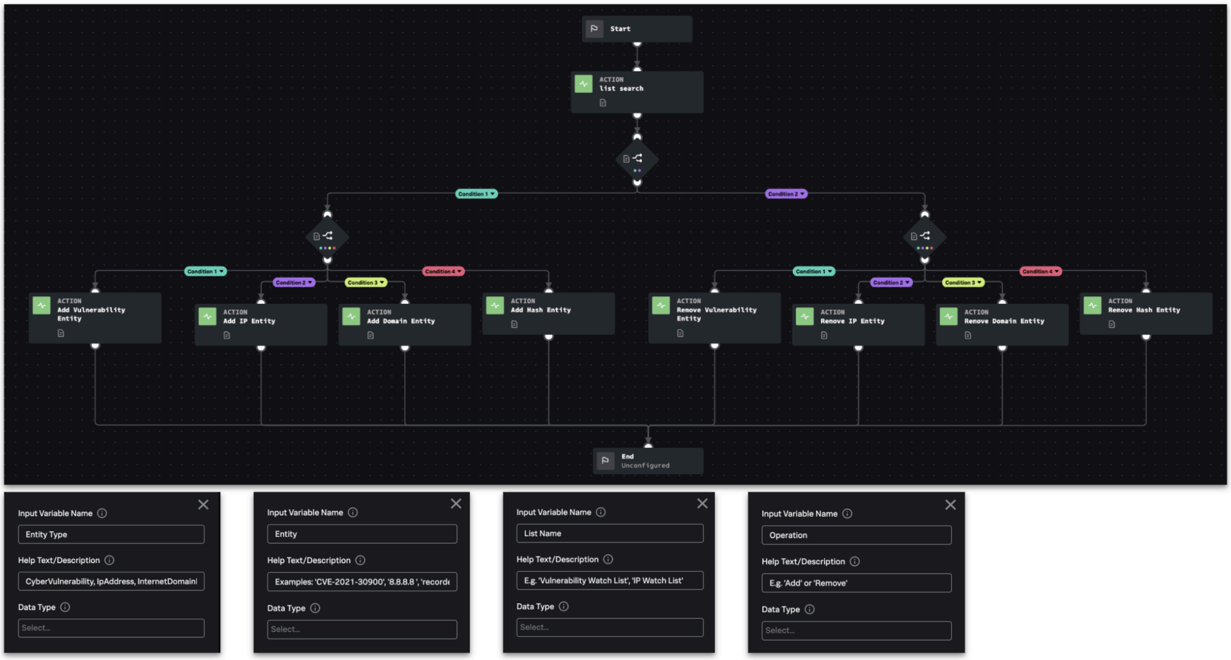
All organizations want alerts generated based on accurate and up-to-date watch lists. Without automation or manual intervention, watch lists become stale and outdated. Furthermore, relying on manual intervention to update watch lists can become unreliable and will frequently be forgotten.

Solution

Included are two playbooks. The first playbook serves as a sub-playbook for other workflows. The sub-playbook accepts four 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. Alternatively, the playbook could be adjusted to add all Vulnerabilities to the Vulnerability Watch List to power the Vulnerability Playbook Alerts to better track their “lifecycle stages”. Or, this playbook works on and enriches any artifacts containing CVEs. The playbook appears simple due to utilizing the sub-playbook mentioned above.

Organizations can use these playbooks to update watch lists in an automated manner, resulting in fresh and accurate information.



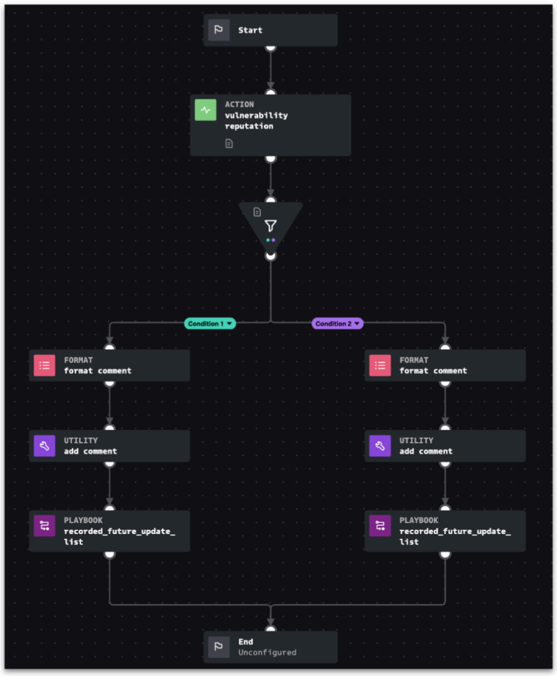
Input Variable Name ⓘ
Entity Type
Help Text/Description ⓘ
CyberVulnerability, IpAddress, InternetDomainI
Data Type ⓘ
Select...

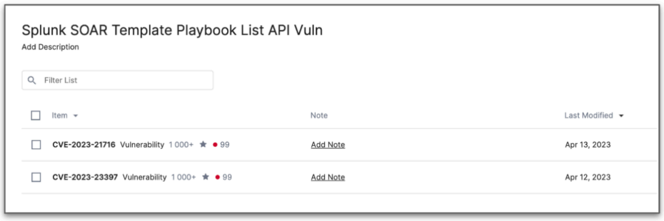
Input Variable Name ⓘ
Entity
Help Text/Description ⓘ
Examples: 'CVE-2021-30900', '8.8.8.8 ', 'record
Data Type ⓘ
Select...

Input Variable Name ⓘ
List Name
Help Text/Description ⓘ
E.g. 'Vulnerability Watch List', 'IP Watch List'
Data Type ⓘ
Select...

Input Variable Name ⓘ
Operation
Help Text/Description ⓘ
E.g. 'Add' or 'Remove'
Data Type ⓘ
Select...

Recorded Future Update List Playbook



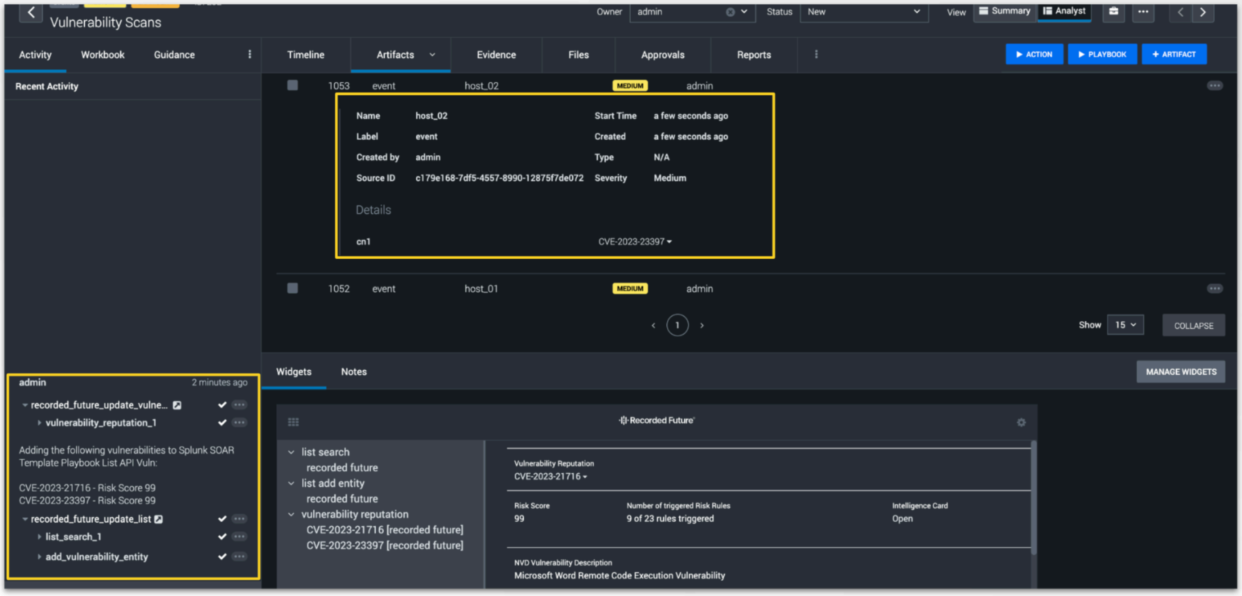


Splunk SOAR Template Playbook List API Vuln

Add Description

□	Item	Note	Last Modified
□	**CVE-2023-21716** Vulnerability 1 000+ ★ ● 99	Add Note	Apr 13, 2023
□	**CVE-2023-23397** Vulnerability 1 000+ ★ ● 99	Add Note	Apr 12, 2023

Recorded Future Update List Playbook



1053 event host_02 MEDIUM admin

Name	host_02	Start Time	a few seconds ago
Label	event	Created	a few seconds ago
Created by	admin	Type	N/A
Source ID	c179e168-7df5-4557-8990-12875f7de072	Severity	Medium

Details

cn1 CVE-2023-23397

1052 event host_01 MEDIUM admin

admin 2 minutes ago

- recorded_future_update_vulne... ✓
  - vulnerability_reputation_1 ✓

Adding the following vulnerabilities to Splunk SOAR Template Playbook List API Vuln:

CVE-2023-21716 - Risk Score 99
CVE-2023-23397 - Risk Score 99

- recorded_future_update_list ✓
  - list_search_1 ✓
  - add_vulnerability_entity ✓

- list search
  - recorded future
- list add entity
  - recorded future
- vulnerability reputation
  - CVE-2023-21716 [recorded future]
  - CVE-2023-23397 [recorded future]

Vulnerability Reputation
CVE-2023-21716

Risk Score	Number of triggered Risk Rules	Intelligence Card
99	9 of 23 rules triggered	Open

NVD Vulnerability Description
Microsoft Word Remote Code Execution Vulnerability

Adding Vulnerabilities to the Watch List

Dynamic Blocking

This use case describes how to block indicators using Recorded Future intelligence with either single or bulk lists of indicators.

Use Case Summary

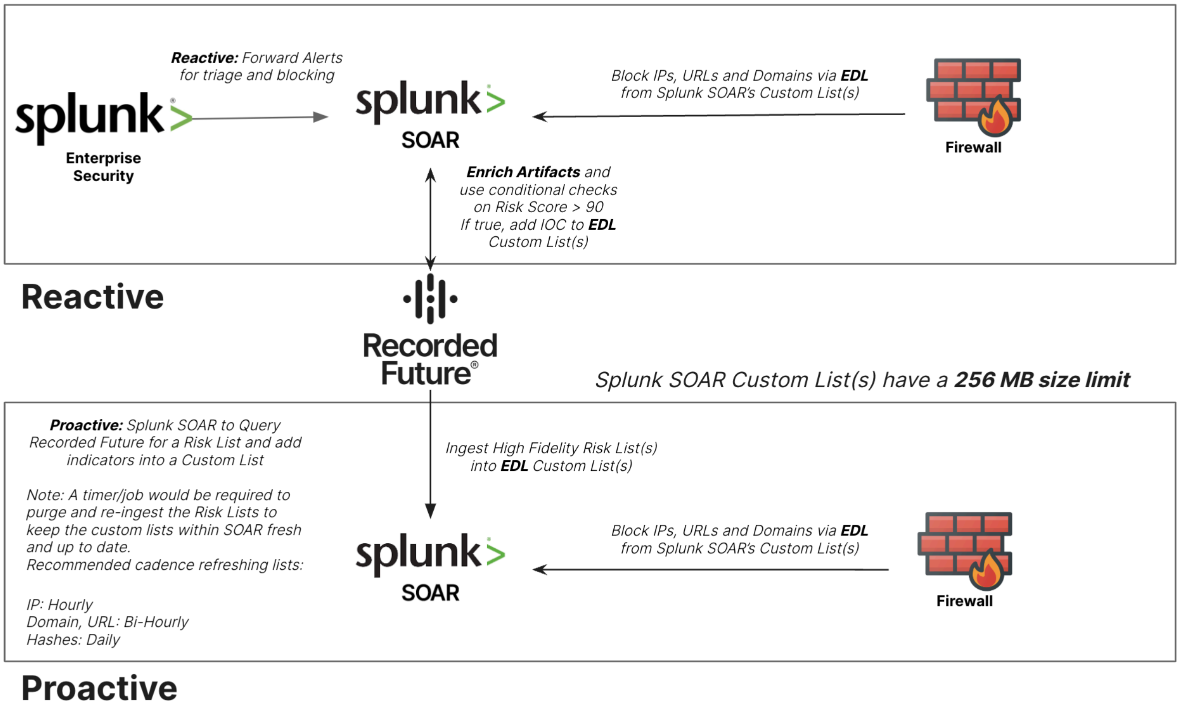
Recorded Future's enrichment and Risk Lists allow organizations to take tailored actions on indicators. Based on their needs, these actions can include blocking indicators using Risk Scores and Risk Rules. Organizations can push these indicators to Splunk SOAR's custom lists, allowing them to host them as external dynamic lists (EDL) firewalls can pull from.

Issue

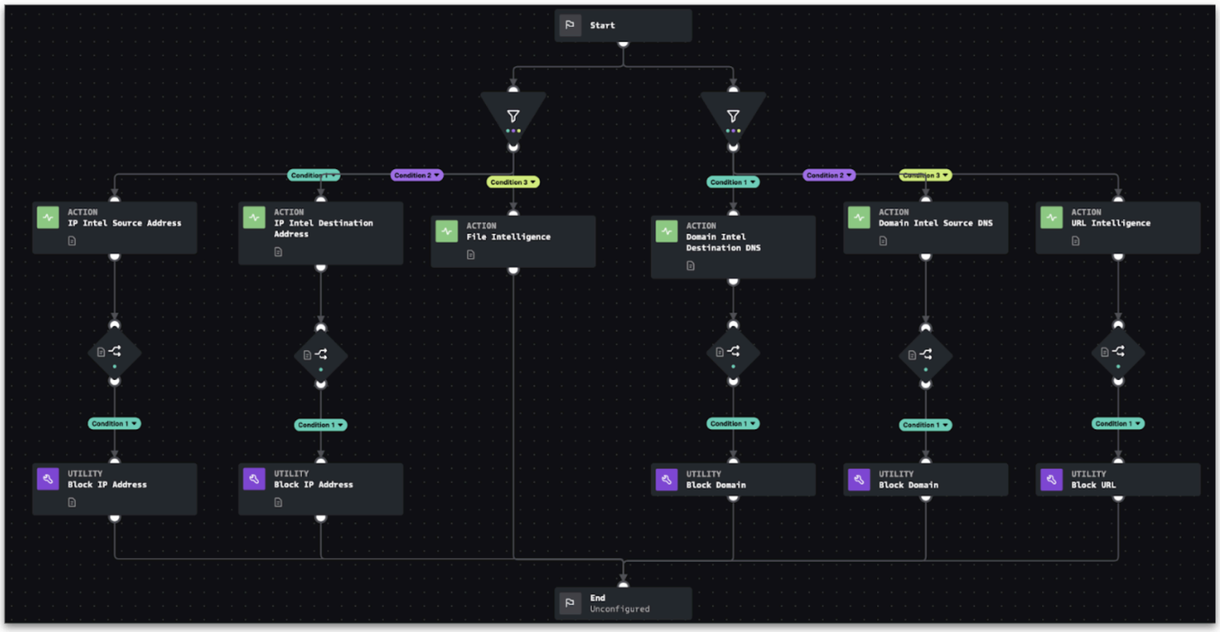
Without automation, the typical process for blocking an indicator takes minutes, assuming the analyst noticed it immediately. Threats like scanners will go unnoticed for hours, if not days, allowing the threat to probe the network continuously. Threat actors can obtain valuable information to target your organization if no proactive or reactive blocking controls are in place.

Furthermore, assuming an internal asset is infected, communication to the C2 server will allow information to relay back and forth between the two, potentially leading to data exfiltration. Considering the time between infection and exfiltration takes seconds, more than manual intervention is required.

Solution


Reactive: Forward Alerts for triage and blocking
splunk> Enterprise Security
splunk> SOAR
Block IPs, URLs and Domains via EDL from Splunk SOAR's Custom List(s)
Firewall
Enrich Artifacts and use conditional checks on Risk Score > 90 If true, add IOC to EDL Custom List(s)
Reactive
Recorded Future®
Splunk SOAR Custom List(s) have a 256 MB size limit
Proactive: Splunk SOAR to Query Recorded Future for a Risk List and add indicators into a Custom List
Note: A timer/job would be required to purge and re-ingest the Risk Lists to keep the custom lists within SOAR fresh and up to date.
Recommended cadence refreshing lists:
IP: Hourly
Domain, URL: Bi-Hourly
Hashes: Daily
Ingest High Fidelity Risk List(s) into EDL Custom List(s)
splunk> SOAR
Block IPs, URLs and Domains via EDL from Splunk SOAR's Custom List(s)
Firewall
Proactive

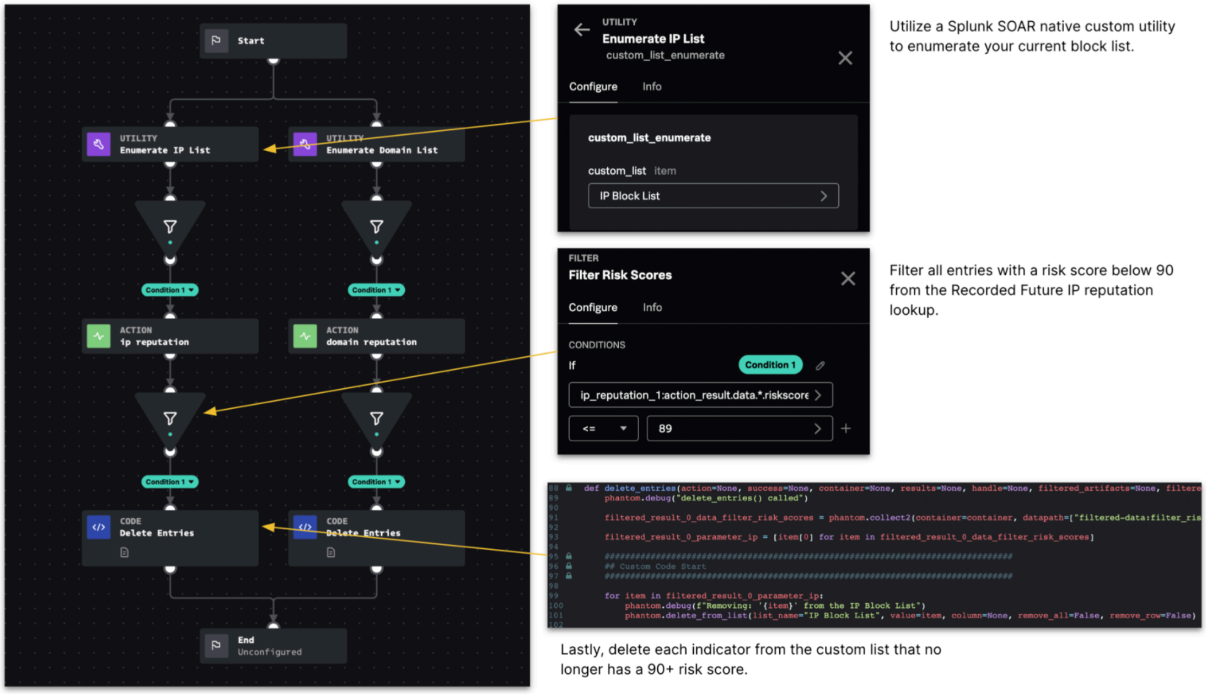
Building on the artifact enrichment playbook allows alert indicators to be blocked based on their Recorded Future Risk Score nearly instantaneously. The playbook below utilizes a decision block to check if the enriched indicators risk score is >= 90. Security engineers can also use other parameters, such as Risk Rules like Validated C&C Server, to drive decisions.



Recorded Future Enrich and Block Playbook (Reactive)

An additional playbook can run daily to keep the EDL fresh with up-to-date information by checking each indicator's risk score. The following playbook utilizes a native Splunk SOAR custom utility to enumerate the custom block list and remove all entries with a risk score below 90.

This playbook doesn't necessarily need to run on only Recorded Future-generated custom lists. Any custom list containing domains, IP addresses, or URLs can use the following logic to maintain fresh block lists.



Utilize a Splunk SOAR native custom utility to enumerate your current block list.

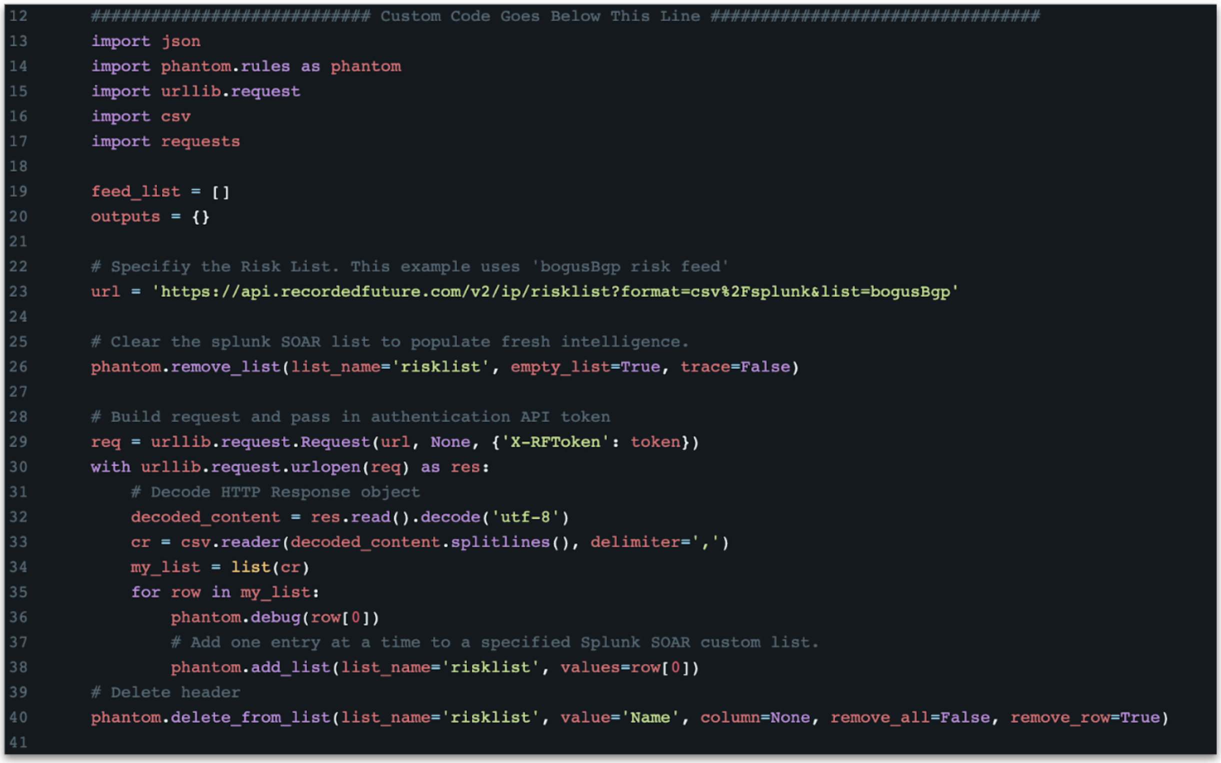
Filter all entries with a risk score below 90 from the Recorded Future IP reputation lookup.

```
def delete_entries(action=None, success=None, container=None, results=None, handle=None, filtered_artifacts=None, filtere
    phantom.debug("delete_entries() called")

    filtered_result_0_data_filter_risk_scores = phantom.collect2(container=container, datapath=["filtered-data:filter_ris

    filtered_result_0_parameter_ip = [item[0] for item in filtered_result_0_data_filter_risk_scores]

    ################################################################################
    ## Custom Code Start
    ################################################################################

    for item in filtered_result_0_parameter_ip:
        phantom.debug(f"Removing: '{item}' from the IP Block List")
        phantom.delete_from_list(list_name="IP Block List", value=item, column=None, remove_all=False, remove_row=False)
```

Lastly, delete each indicator from the custom list that no longer has a 90+ risk score.

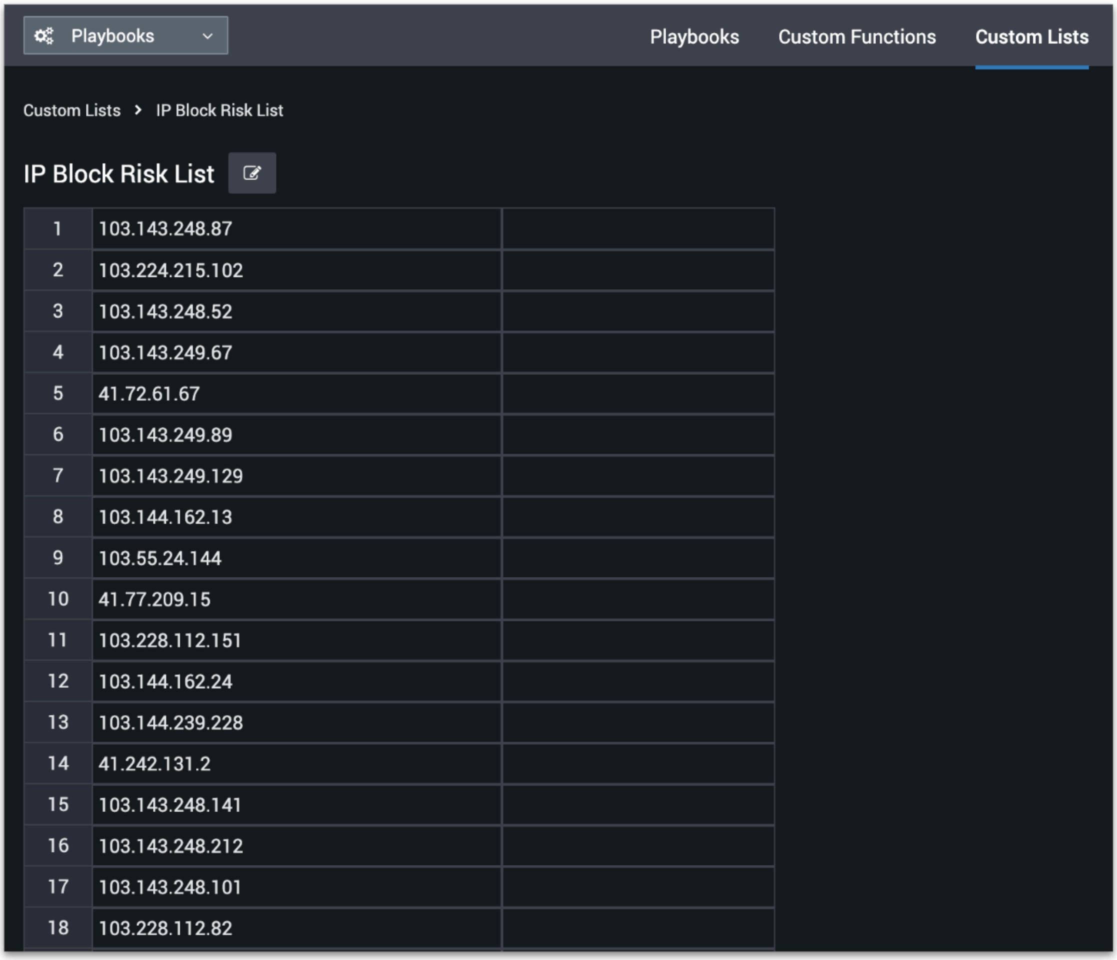
Recorded Future Refresh Block List

Lastly, deploy a custom function to ingest complete Recorded Future Risk Lists to prevent threats from communicating with your network. This custom function uses the Recorded Future Connect API risk list endpoint to 'pull' a specific list. It then iterates through the entries and uses a native Splunk SOAR function to populate a custom list.



```
############################ Custom Code Goes Below This Line #################################
import json
import phantom.rules as phantom
import urllib.request
import csv
import requests

feed_list = []
outputs = {}

# Specifiy the Risk List. This example uses 'bogusBgp risk feed'
url = 'https://api.recordedfuture.com/v2/ip/risklist?format=csv%2Fsplunk&list=bogusBgp'

# Clear the splunk SOAR list to populate fresh intelligence.
phantom.remove_list(list_name='risklist', empty_list=True, trace=False)

# Build request and pass in authentication API token
req = urllib.request.Request(url, None, {'X-RFToken': token})
with urllib.request.urlopen(req) as res:
    # Decode HTTP Response object
    decoded_content = res.read().decode('utf-8')
    cr = csv.reader(decoded_content.splitlines(), delimiter=',')
    my_list = list(cr)
    for row in my_list:
        phantom.debug(row[0])
        # Add one entry at a time to a specified Splunk SOAR custom list.
        phantom.add_list(list_name='risklist', values=row[0])
# Delete header
phantom.delete_from_list(list_name='risklist', value='Name', column=None, remove_all=False, remove_row=True)
```

Custom Function Risk List Download



Custom Lists > IP Block Risk List

IP Block Risk List

1	103.143.248.87	
2	103.224.215.102	
3	103.143.248.52	
4	103.143.249.67	
5	41.72.61.67	
6	103.143.249.89	
7	103.143.249.129	
8	103.144.162.13	
9	103.55.24.144	
10	41.77.209.15	
11	103.228.112.151	
12	103.144.162.24	
13	103.144.239.228	
14	41.242.131.2	
15	103.143.248.141	
16	103.143.248.212	
17	103.143.248.101	
18	103.228.112.82	

Populated Custom List

Vulnerability Alert Handling

This use case describes how to automatically triage Recorded Future vulnerability alerts by leveraging vulnerability scan results stored in Splunk Enterprise.

Use Case Summary

Timely and accurate vulnerability assessment is critical. The security gained by remediating some vulnerabilities is dramatically higher than remediating others. Vulnerability 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. 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 exposures to search for within your environment.

Issue

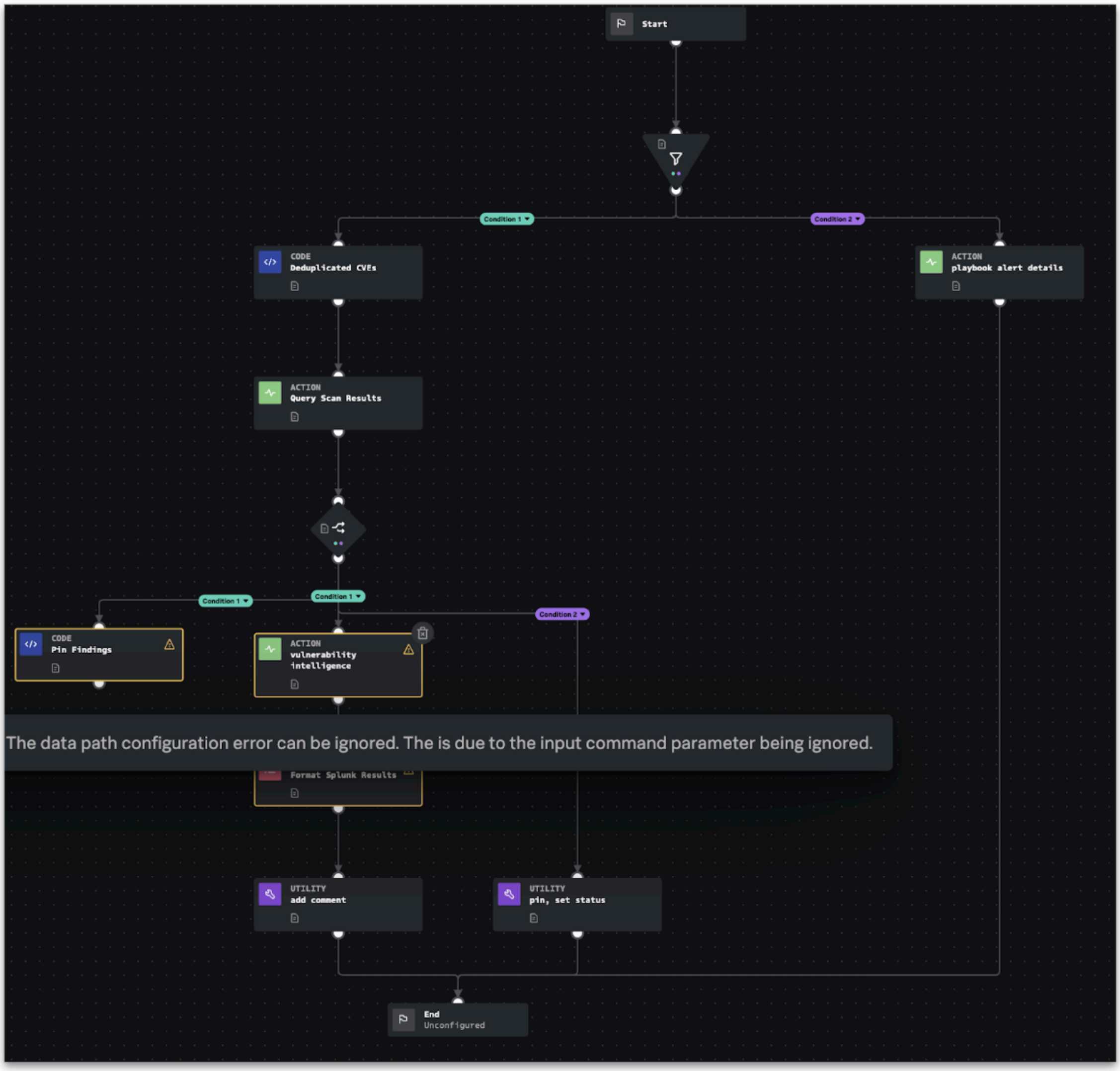
Vulnerability management, Security Operations, and Threat Intelligence teams are often siloed from one another. A Threat Intelligence or Security Operations team needs a way to instantly check if a vulnerability impacts an asset in their environment without needing to manually verify with a human, which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

Solution

The workflow assumes your Splunk Enterprise instance stores your vulnerability scan results. This playbook responds to Recorded Future's vulnerability alerts for both playbook and traditional alerts.

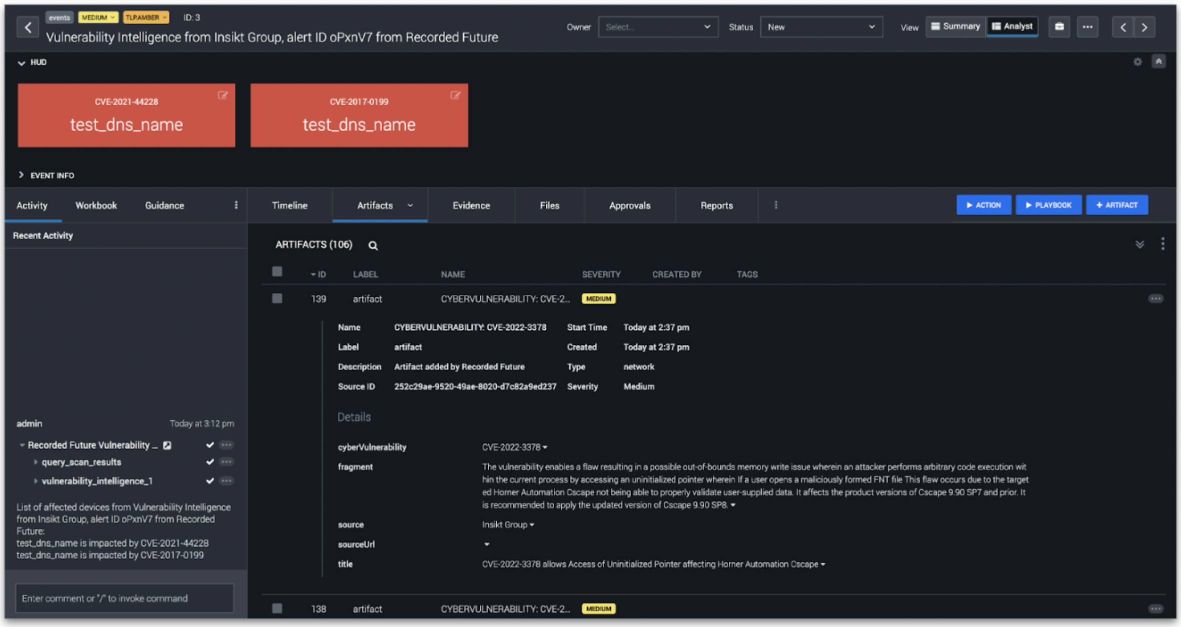
A Splunk SOAR container uses the Recorded Future app's fetch feature to ingest the Recorded Future alert. All evidence details within the alert are parsed and added as artifacts automatically. Then, each CVE contained in the Vulnerability alert extracts and formats into a Splunk search. The search runs and looks for matches within Splunk. Any matches return to the Splunk SOAR container.

This process eliminates manual searching or team communication for high-fidelity vulnerabilities in your environment and allows your organization to leverage vulnerability intelligence across team silos with one integration.



The data path configuration error can be ignored. The is due to the input command parameter being ignored.

[Recorded Future Vulnerability Alert Handling Playbook](#)



ID: 3

Vulnerability Intelligence from Insikt Group, alert ID oPxnV7 from Recorded Future

Owner Select...   Status New   View

CVE-2021-44228
test_dns_name

CVE-2017-0199
test_dns_name

Recent Activity

admin Today at 3:12 pm

- Recorded Future Vulnerability ... ✓
  - query_scan_results ✓
  - vulnerability_intelligence_1 ✓

List of affected devices from Vulnerability Intelligence from Insikt Group, alert ID oPxnV7 from Recorded Future:
test_dns_name is impacted by CVE-2021-44228
test_dns_name is impacted by CVE-2017-0199

Enter comment or "/" to invoke command

ARTIFACTS (106)

ID	LABEL	NAME	SEVERITY	CREATED BY	TAGS
139	artifact	CYBERVULNERABILITY: CVE-2...	MEDIUM		
138	artifact	CYBERVULNERABILITY: CVE-2...	MEDIUM		

Name	CYBERVULNERABILITY: CVE-2022-3378	Start Time	Today at 2:37 pm
Label	artifact	Created	Today at 2:37 pm
Description	Artifact added by Recorded Future	Type	network
Source ID	252c29ae-9520-49ae-8020-d7c82a9ed237	Severity	Medium

Details

cyberVulnerability	CVE-2022-3378 ▾
fragment	The vulnerability enables a flaw resulting in a possible out-of-bounds memory write issue wherein an attacker performs arbitrary code execution within the current process by accessing an uninitialized pointer wherein If a user opens a maliciously formed FNT file This flaw occurs due to the targeted Horner Automation Cscape not being able to properly validate user-supplied data. It affects the product versions of Cscape 9.90 SP7 and prior. It is recommended to apply the updated version of Cscape 9.90 SP8. ▾
source	Insikt Group ▾
sourceUrl	▾
title	CVE-2022-3378 allows Access of Uninitialized Pointer affecting Horner Automation Cscape ▾

Vulnerability Alert Container

Leaked Credential Alert Handling

This use case describes how to respond to Recorded Future Leaked Credential alerts using Active Directory (AD) LDAP.

Use Case Summary

Leaked credentials can provide a company insight into the future where the next business compromise impact may arise from. Often, these credentials are sold and purchased on dark web marketplace forums, harvested via malware, or dumped into cloud storage for public access.

Recorded Future's leaked credential alerts provide companies with actionable intelligence for the compromised accounts to use to reset employee or customer passwords, stopping a breach before it can happen.

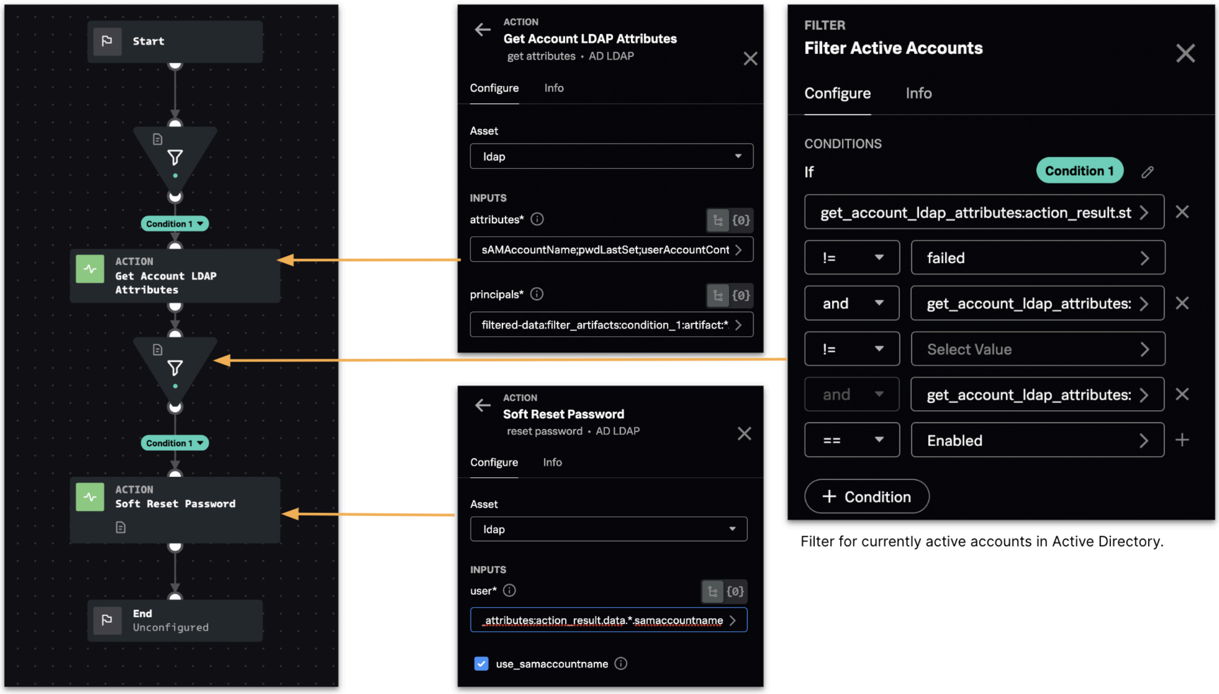
Issue

Credential leaks can be tedious to address and respond to manually. Often, security teams form separate groups with individual responsibilities. An identity management team might be disconnected from the threat intelligence team, which might be disconnected from the incident response team.

Sending a request from one team to another will consume minutes, if not hours. By automatically resetting an employee credential with a SOAR tool, a security team can respond and contain risk as soon as an alert is received.

Solution

This playbook responds to the Recorded Future monitoring of leaked credentials exposed on the internet alerts. The accounts are verified if they exist within Active Directory and are active (enabled/disabled). If an account is active, a manual prompt to 'soft reset' the account at the next login is issued. A 'soft reset' will inform the employee to reset their password the next time they log on. Depending on their comfort level, the SOAR Engineer can remove the manual prompt and replace it with an automated reset.



ACTION
Get Account LDAP Attributes
get attributes • AD LDAP

Configure | Info

Asset: ldap

INPUTS

attributes*: sAMAccountName;pwdLastSet;userAccountCont

principals*: filtered-data:filter_artifacts:condition_1:artifact:*

ACTION
Soft Reset Password
reset password • AD LDAP

Configure | Info

Asset: ldap

INPUTS

user*: _attributes:action_result.data.*.samaccountname

☑ use_samaccountname

FILTER
Filter Active Accounts

Configure | Info

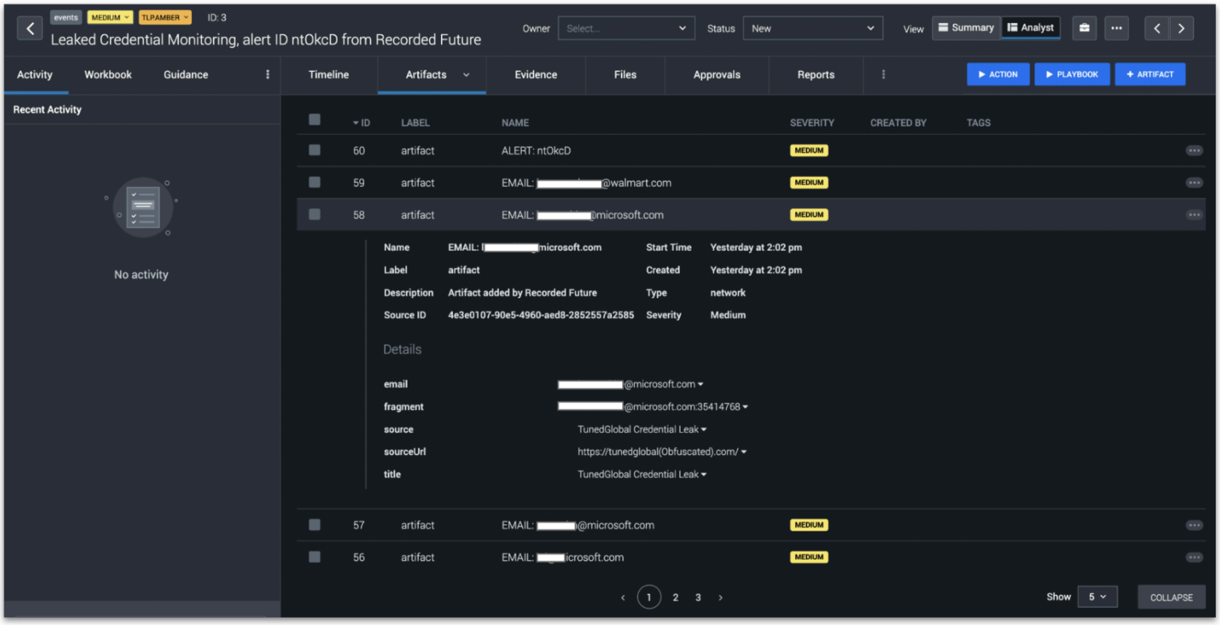
CONDITIONS

If — Condition 1

get_account_ldap_attributes:action_result.st
!= failed
and get_account_ldap_attributes:
!= Select Value
and get_account_ldap_attributes:
== Enabled

+ Condition

Filter for currently active accounts in Active Directory.



events | MEDIUM | TLP:AMBER | ID: 3

Leaked Credential Monitoring, alert ID ntOkcD from Recorded Future

Owner: Select... | Status: New | View: Summary | Analyst

ID	LABEL	NAME	SEVERITY	CREATED BY	TAGS
60	artifact	ALERT: ntOkcD	MEDIUM		
59	artifact	EMAIL: [redacted]@walmart.com	MEDIUM		
58	artifact	EMAIL: [redacted]microsoft.com	MEDIUM		

Name	EMAIL: [redacted]microsoft.com	Start Time	Yesterday at 2:02 pm
Label	artifact	Created	Yesterday at 2:02 pm
Description	Artifact added by Recorded Future	Type	network
Source ID	4e3e0107-90e5-4960-aed8-2852557a2585	Severity	Medium

Details

email	[redacted]@microsoft.com
fragment	[redacted]@microsoft.com:35414768
source	TunedGlobal Credential Leak
sourceUrl	https://tunedglobal(Obfuscated).com/
title	TunedGlobal Credential Leak

ID	LABEL	NAME	SEVERITY	CREATED BY	TAGS
57	artifact	EMAIL: [redacted]@microsoft.com	MEDIUM		
56	artifact	EMAIL: [redacted]icrosoft.com	MEDIUM		

‹ 1 2 3 › Show 5 COLLAPSE

Leaked Credential Alert Container

Additional Reading

Find below additional information of the various Recorded Future products mentioned throughout this document.

Recorded Future Sandbox FAQ
Recorded Future Vulnerability Intelligence Module
Recorded Future SecOps Module
Recorded Future Threat Intelligence Module
Recorded Future Brand Intelligence Module
Recorded Future List API
Recorded Future Entity Match API
Recorded Future Threat Map

Professional Services Assistance

Recorded Future provides a custom service for *Use Case Development* to identify and implement the capabilities outlined in this document and also develop new capabilities based on discovery workshops with customers.

For more information on Splunk SOAR use case development or assistance with creating custom use cases and implementation, please get in touch with your Sales or Intelligence Services representative and arrange a conversation with Professional Services at Recorded Future to see how we can help.