

# Cortex XSOAR Cloud Reference Architecture

## Use Cases & Capabilities

Created by: [Recorded Future Professional Services](#)

Published: October, 2023

Updated: July, 2024

<b>Summary.....</b>	<b>3</b>
<b>Integration Overview.....</b>	<b>3</b>
<b>Content Packs.....</b>	<b>4</b>
<b>Use Cases.....</b>	<b>5</b>
Artifact Enrichment.....	6
Use Case Summary.....	6
Issue.....	6
Solution.....	6
Threat Map Hunting.....	7
Use Case Summary.....	7
Issue.....	7
Solution.....	7
Sandbox Detonation.....	8
Use Case Summary.....	8
Issue.....	8
Solution.....	8
Recorded Future Alert Management.....	9
Use Case Summary.....	9
Issue.....	9
Solution.....	9
Vulnerability Alert Handling.....	10
Use Case Summary.....	10
Issue.....	10
Solution.....	10
Watch List Management.....	11
Use Case Summary.....	11
Issue.....	11
Solution.....	11
Dynamic Blocking.....	12
Use Case Summary.....	12
Issue.....	12
Solution.....	12
Custom File Ingestion.....	13
Security Control Feed Ingestion.....	13
Identity Exposure.....	14
Use Case Summary.....	14
Issue.....	14
Solution.....	14
Collective Insights.....	15
Use Case Summary.....	15
Issue.....	15
Solution.....	15
Technical References Commands and Outputs.....	16
Intelligence Content Pack.....	16
Enrichment.....	16
Technical Links.....	18
Legacy & Playbook Alert Management.....	19
List Management.....	21
Threat Actor Maps with Enrichment.....	22
Sandbox Content Pack.....	23
Identity Content Pack.....	24
Feed Content Pack.....	25
Risk List Ingestion.....	25
<b>Additional Reading.....</b>	<b>26</b>
<b>Professional Services Assistance.....</b>	<b>26</b>

# Summary

This reference architecture aims to give the reader an understanding of the use cases and capabilities achievable with the Recorded Future integration into Cortex XSOAR. This document also outlines useful commands and their outputs within the 'Technical References - Commands and Outputs' section. This document will also highlight the different content packs available in the Cortex XSOAR Marketplace.

## Integration Overview

Overwhelmed by manual processes and high alert volume, security teams are unable to take advantage of the breadth of intelligence available, instead they focus only on internal logs and data. Security teams need a platform that centralizes intelligence in real-time and harnesses that information to drive action across security infrastructures. To meet these challenges, Recorded Future empowers security teams with improved threat visibility and accelerated incident response. Combining comprehensive, real-time threat intelligence with the security orchestration and automation power of Cortex XSOAR, the following areas are the primary focus:

**Threat Triage** With the Recorded Future and Cortex XSOAR integration, analysts see which alerts should be prioritized based on a real-time risk score that is backed by transparent evidence. An enrichment playbook automatically prioritizes alerts, quickly discounts false positives, identifies the most significant threats, and takes immediate action alongside the capability to upload file samples and submit URLs to the Sandbox for deeper triage analysis.

**Threat Detection** The explosive growth of indicators makes detecting real threats extremely resource-intensive for already overwhelmed security teams. Recorded Future connects the dots between the broadest range of sources across every language. This intelligence and critical context enables Cortex XSOAR to automatically analyze and identify IOCs related to phishing attacks, malware, and command-and-control servers, empowering security teams to automate responses and reduce risk for the organization.

**Threat Hunting** Armed with proprietary, evidence-based findings, organizations can automatically identify and block high-risk IPs, URLs, hashes, and domains at the perimeter, minimize false positive blocking, automate incident response, and improve overall security posture.

**Vulnerability Prioritization** Recorded Future provides necessary, real-time context around disclosed vulnerabilities based on the organization's technologies, industry, company, and more. By positioning direct access to evidence on the new and exploited vulnerabilities impacting their assets within Cortex XSOAR, organizations are enabled to produce deeper analysis and prioritize CVEs faster.

**Real-Time Alert Ingestion** Having the ability to take action based on context provided in Recorded Future alert details, is paramount to staying ahead and being informed of the latest threats to your organization. Pulling down Recorded Future alert context can be used for automating tasks, analyst notification, and historical knowledge. Analysts can use this added context with their existing workflow, saving time and resources.

**Identity Exposure** Ingest alerts for Identity breaches quickly and efficiently to prevent threat actors from utilizing freshly extracted credentials. Identify whether the credential is valid through the comparison of full and partial Hash data and take action to protect the associated identity.

# Content Packs

There are multiple content packs empowering many use cases when implementing Recorded Future Intelligence for orchestration and automation. These packs can be found within the Cortex XSOAR Marketplace.

This document provides an overview of the capabilities for each Recorded Future content pack:

## Content Packs

- **[Recorded Future Intelligence](#)**
  - Automate enrichment of IPs, URLs, domains, and file hashes as playbook-driven tasks within Cortex XSOAR
  - Access technical links for an indicator including threat actors and associated malware for deeper context
  - Ingest multiple types of Recorded Future alerts and run response actions using alert details for justification
  - Enrich vulnerability data and prioritize your patch management cycle
  - Retrieve threat actors from the Threat Map associated with your organization
- **[Hatching Triage \(Recorded Future Sandbox\)](#)**
  - Submit a high volume of samples to run in a sandbox and retrieve the reports for further analysis and investigation
- **[Recorded Future Feed](#)**
  - Utilize risk lists and fusion files to proactively identify, alert, and block IOCs in your environment
- **[Recorded Future Identity](#)**
  - Utilize the Identity module and commands to identify the identities exposed that meet the client's requirements and lookup contextual details for each identity / exposure
- **[Recorded Future Attack Surface Intelligence](#)**
  - Ingest ASI alerts with relevant details

# Use Cases

Recorded Future owns and maintains a library of template playbooks available for download on our [support site](#).

Utilizing Recorded Future Intelligence within a SOAR environment is extremely flexible. The following Use Cases are neither exhaustive nor extensive in scope and are designed to portray common Use Cases and provide a quick overview of the capabilities of Cortex XSOAR combined with Recorded Future to gain immediate value from the content packs.

Associated with these Use Cases are Recorded Future's Template Playbooks which can be found within each content pack. By utilizing playbooks, clients can chain together and pass data from one action to another.

Recorded Future provides a custom Use Case Development service 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 Cortex XSOAR Use Case development, assistance with creation of custom Use Cases and implementation, please contact your sales rep and arrange a conversation with Professional Services at Recorded Future to see how we can help.

# Artifact Enrichment

## Use Case Summary

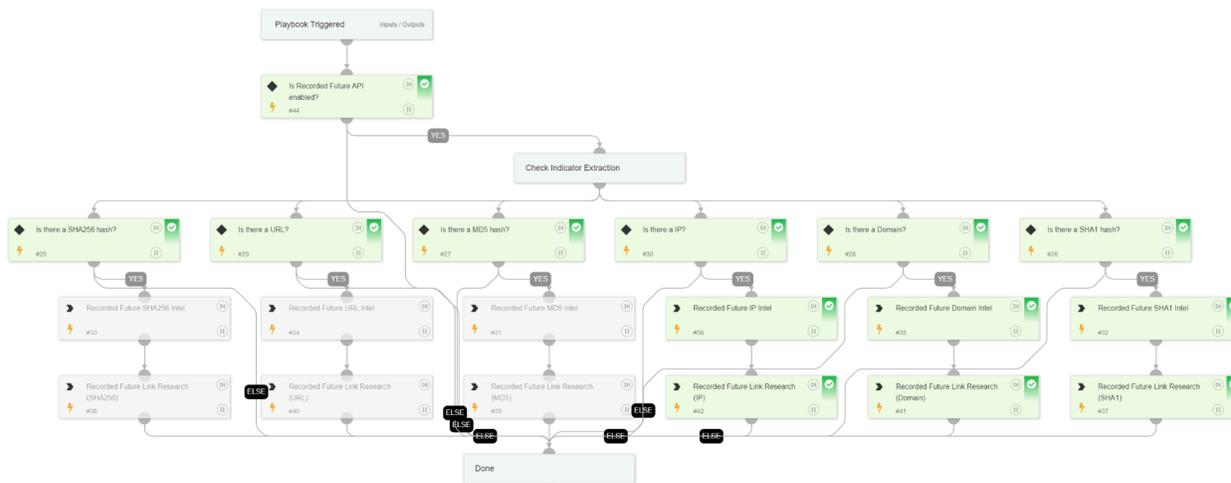
Enrichment capabilities include gathering Technical links and the associated risk scores and risk rules attached to those to understand the potential impact or attribution of a threat. These additional indicators and attributions can aid in understanding the threat.

## Issue

Typically identifying technically related indicators following an incident takes time and effort by the Forensic analysis team. The time taken to identify additional indicators can give the attackers time to spread wider or achieve objectives before the incident is fully investigated and mitigated.

## Solution

Utilizing Recorded Futures technical links can provide associated threat actors, vulnerabilities, malware and IOCs for the analyst to attribute to previous Incidents (Campaigns & Actors) or perform manual hunting activities on the EDR and / or SIEM to determine if any of the associated indicators are present to extend the detection of the active threat. [Template Playbook](#)



# Threat Map Hunting

## Use Case Summary

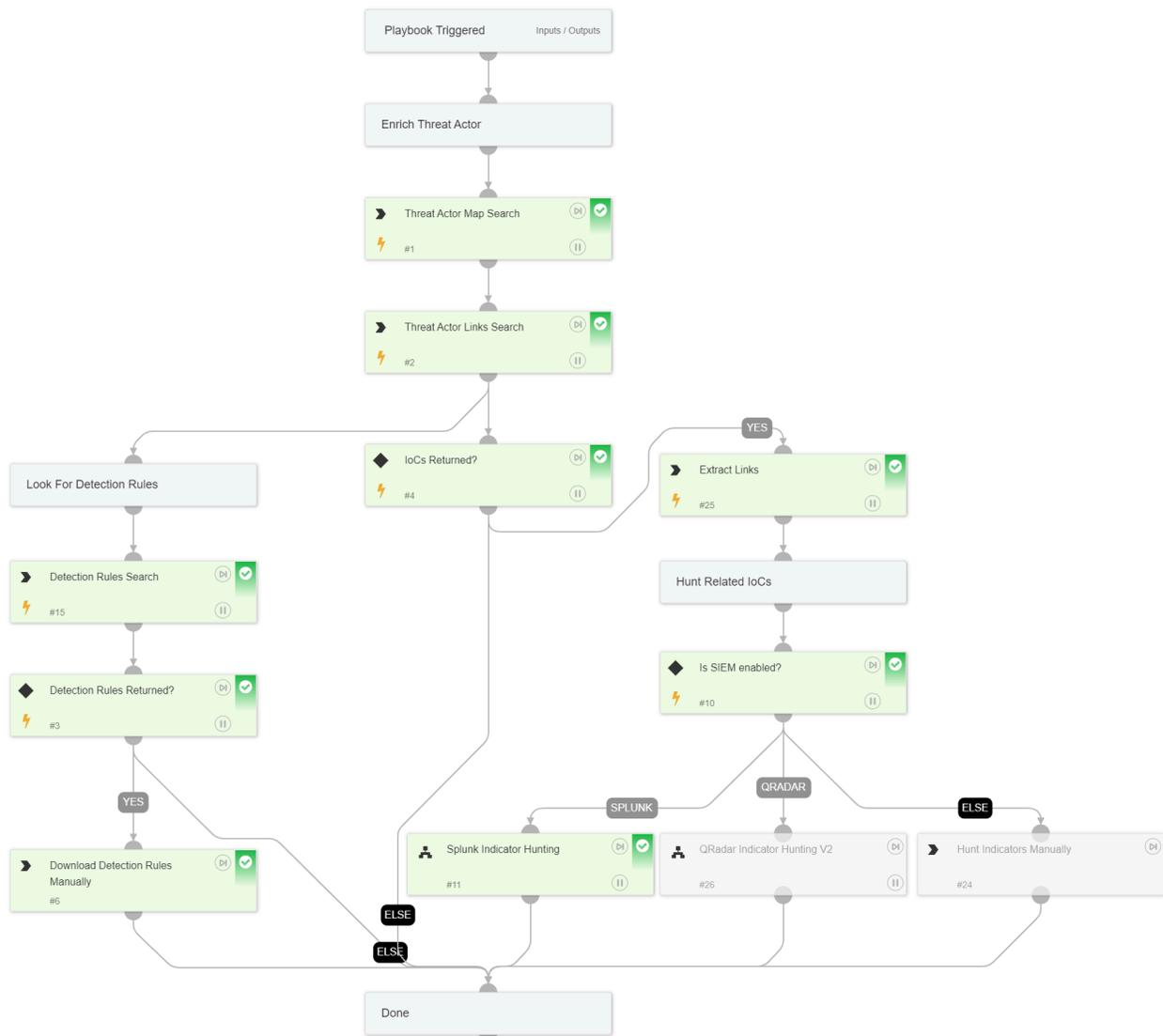
Recorded Future can assist with Threat Hunting utilizing Intelligence led Threat Maps, Threat Actor Indicators and Technical Links to identify new threats previously not detected by SIEM correlation rules.

## Issue

Detections are governed by strict syntax and are prone to generate noise and unwanted alerts. Tuning is time consuming and detection can be problematic. Threat Hunting provides a more robust detection method however it is time consuming and doesn't provide timely detection.

## Solution

Recorded Future can automate Threat Hunting utilizing Threat Map data derived from your curated watch lists, known threat actors targeting your industry or organization and Recorded Future Analyst driven data to proactively detect threats in your event logs via hunting from the SOAR to the SIEM based on Incident related technical links or automated search criteria utilizing Threat Actor Risk Lists or Threat Map data. [Template Playbook](#)



## Sandbox Detonation

### Use Case Summary

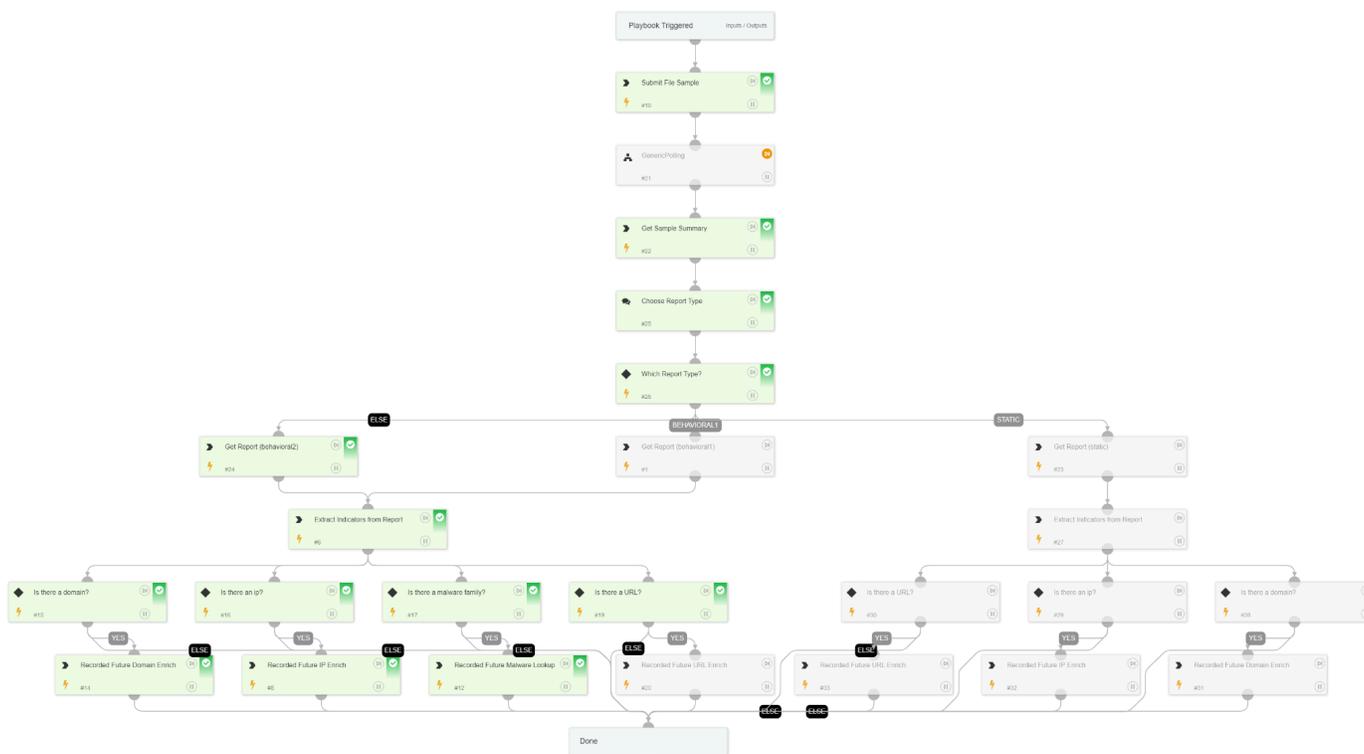
Sandbox analysis is designed to quickly triage a binary or URL to determine the threat based on active automated analysis. Recorded Future further enriches this process via matching Indicators from the sandbox analysis against available intelligence to determine an initial threat level based on risk score and risk rules.

### Issue

Typically analysts are overwhelmed with alerts, events and incidents in a SOC and have a minimal amount of time (typically 15 minutes or less) to determine if an Incident is critical, invalid or a low priority. Performing manual analysis of Binaries and URLs can be a time consuming process involving multiple analysis engines, virtual environments and following complex processes.

### Solution

Utilizing Recorded Future's Triage Sandbox, URLs and Binary payloads are detonated in a safe environment to determine known threats and further enriched with a risk scoring to determine a baseline threat level. This provides the Analyst team with a detailed analysis report along with a prioritized list of indicators to investigate. [Template Playbook](#)



# Recorded Future Alert Management

## Use Case Summary

Recorded Future provides a method to ingest all Recorded Future alerts into the SOAR for triage, investigation and management without leaving the SOAR console for a fully integrated incident management solution.

## Issue

Not all analysts may have access to the Recorded Future portal and switching to platform to manage alerts may become time consuming and be managed on a batch basis as opposed to triaging and handling / closing the alerts in a timely manner as they are produced.

## Solution

Ingesting alerts into the SOAR platform provides an opportunity to automatically assign, triage, and close or escalate alerts without the need to manage them manually in the Recorded Future Platform.

**#7 Recorded Future Playbook Alert - Domain abuse norbvpn.com - Incident Info** Source | Recorded Future Playbook Alerts

**Incident Info** | War Room | Work Plan | Evidence Board

Type	Recorded Future Domain Abuse
Severity	High
Source Brand	RecordedFuturePlaybookAlerts
Source Instance	Recorded Future Playbook Alerts
Playbook	Recorded Future Domain Abuse

Alert ID	23abac98-e75a-476a-96b6-782612b76b4b
Alert Name	norbvpn.com
Occurred	Feb 1st 2024 09:06:37
Source Priority	High

**RECORDED FUTURE EVIDENCE SUMMARY**

Description  
Alert was created as a result of a triggered typosquat detection.

Recorded Future Identified Domain

RISK SCORE	ENTITY CRITICALITY	ENTITY NAME
26	Medium	norbvpn.com

Recorded Future Whois Record Data

CREATED DATE	REGISTRAR NAME	CONTACT EMAIL	NAME SERVERS
Jun 21st 2023 20:00:...	Dynadot Inc		["ns1.dyna-ns.net";"ns2.dyna-ns.net"]

Recorded Future DNS Records

RECORD TYPE	RISK SCORE	CRITICALITY	ENTITY
A	25	Medium	34.111.46.214
NS	5	Low	ns2.dyna-ns.net
NS	5	Low	ns1.dyna-ns.net

**NOTES (1)** + Add

**DBot**  
Feb 1st 2024 09:12:42

Uploaded and commented on an image: [5d2b298e-e92f-4ef9-9dee-f161b3e87633.png](#)

[Hide Preview](#)

An image associated with the Playbook Alert

# Vulnerability Alert Handling

## Use Case Summary

Recorded Future provides vulnerability alerts against your organization's tech stack. Alerts include pre-NVD and vulnerabilities researched by the Recorded Future Insikt Group. These alerts will provide your organization with relevant vulnerability alerts for consideration of mitigation, patching, or monitoring to detect attempted exploits and protect against them.

## Issue

Vulnerability Management can be a timely and complex task to manage. Organizations typically have a disparate and varied technology stack which leads to difficulty in identifying, mitigating, and patching identified vulnerabilities.

## Solution

Performing regular asset or vulnerability scans will provide your organization with up-to-date asset repository lists, ensuring those technologies are updated to the Recorded Future Technology Stack Watch List will provide relevant alerts to assist in identifying the most pertinent vulnerabilities and also tracking the status of vulnerabilities against the vulnerability exploitability timeline from PoC to Exploited in the Wild ensuring timely and accurate assessments can be made against vulnerable assets to determine whether mitigation, patching, isolation or additional monitoring activities should be implemented to protect the asset and associated services.

**#5 Recorded Future Playbook Alert - Vulnerability CVE-2024-23222 - Incident Info**

Incident Info | War Room | Work Plan | Evidence Board

### CASE DETAILS

Type: Recorded Future Vulnerability  
 Severity: 🔥 High  
 Source Brand: RecordedFuturePlaybookAlerts  
 Source Instance: Recorded Future Playbook Alerts  
 Playbook: Recorded Future Vulnerability

### RECORDED FUTURE ALERT OVERVIEW

Alert ID: c4d38ca0-4300-411f-82b7-9c24de874dfb  
 Alert Name: CVE-2024-23222  
 Occurred: Feb 1st 2024 09:06:35  
 Source Priority: High  
 Recorded Future Targ.: MacOS

### RECORDED FUTURE EVIDENCE SUMMARY

Recorded Future Identified CVE

RISK SCORE	ENTITY CRITICALITY	LIFECYCLE STAGE	ENTITY NAME
99	Very Critical	Exploited	CVE-2024-23222

Recorded Future Risk Rule

RULE	DESCRIPTION
Exploited in the Wild ...	1 sighting on 1 source: CISA Known Exploited Vulnerabilities Catalog: Apple Multiple Products Type Confusion Vulnerability from vendor...

Recorded Future Insikt Notes

TITLE	PUBLISHED	TOPIC	FRAGMENT
Apple Addresses CVE...	Jan 23rd 2024 11:38...	Validated Intelligence ...	On January 22, 2024, Apple patched a WebKit confusion vulnerability. tra...
Summary note for CV...	Jan 22nd 2024 20:30...	Informational	Source: Cyber Threat Cognitive Intelligence (CTCI)

### NOTES (2)

**DBot**  
 Feb 1st 2024 09:38:28  
**Task Result #16:** Enrich CVE as Note  
**Command:** recordedfuture-intelligence:profile="ALL" entity\_type="cve" entit... [Recorded Future v2]  
**Recorded Future CVE Intelligence for "CVE-2024-23222"**

Risk Score: 99  
 Summary: 7 of 23 Risk Rules currently observed.  
 Criticality Label: Very Critical  
 Total references to this entity: 1450  
 RecordedFuture AI Insights: CVE-2024-23222 is a zero-day vulnerability that has been exploited in Apple Vision Pro. Apple has released a fix for this vulnerability, which allows attackers to compromise iPhones, Macs, and Apple TVs. The vulnerability has gained attention in various online platforms such as RootTalk, 0J Pro Recently Filled, hivespro.com, Reddit, Information Security News, and FreeBufCOM. The vulnerability has been categorized as a threat with 336 references in the last 60 days. It is associated with seven malware families including Zero Day Exploit, Metasploit, Trojan, Offensive Security Tools (OST), and Out-of-Bounds Memory Access. Tenable and Recorded Future have also reported on this vulnerability, with the CVE v3.1 Score calculated at 9.5 out of 10. It is advised to prioritize patching this vulnerability as it poses a significant risk to the security of Apple devices and could potentially lead to unauthorized access or data breaches if left unpatched.  
 First reference collected on: 2024-01-12 23:50:41  
 Latest reference collected on: 2024-02-01 13:55:45

## Watch List Management

### Use Case Summary

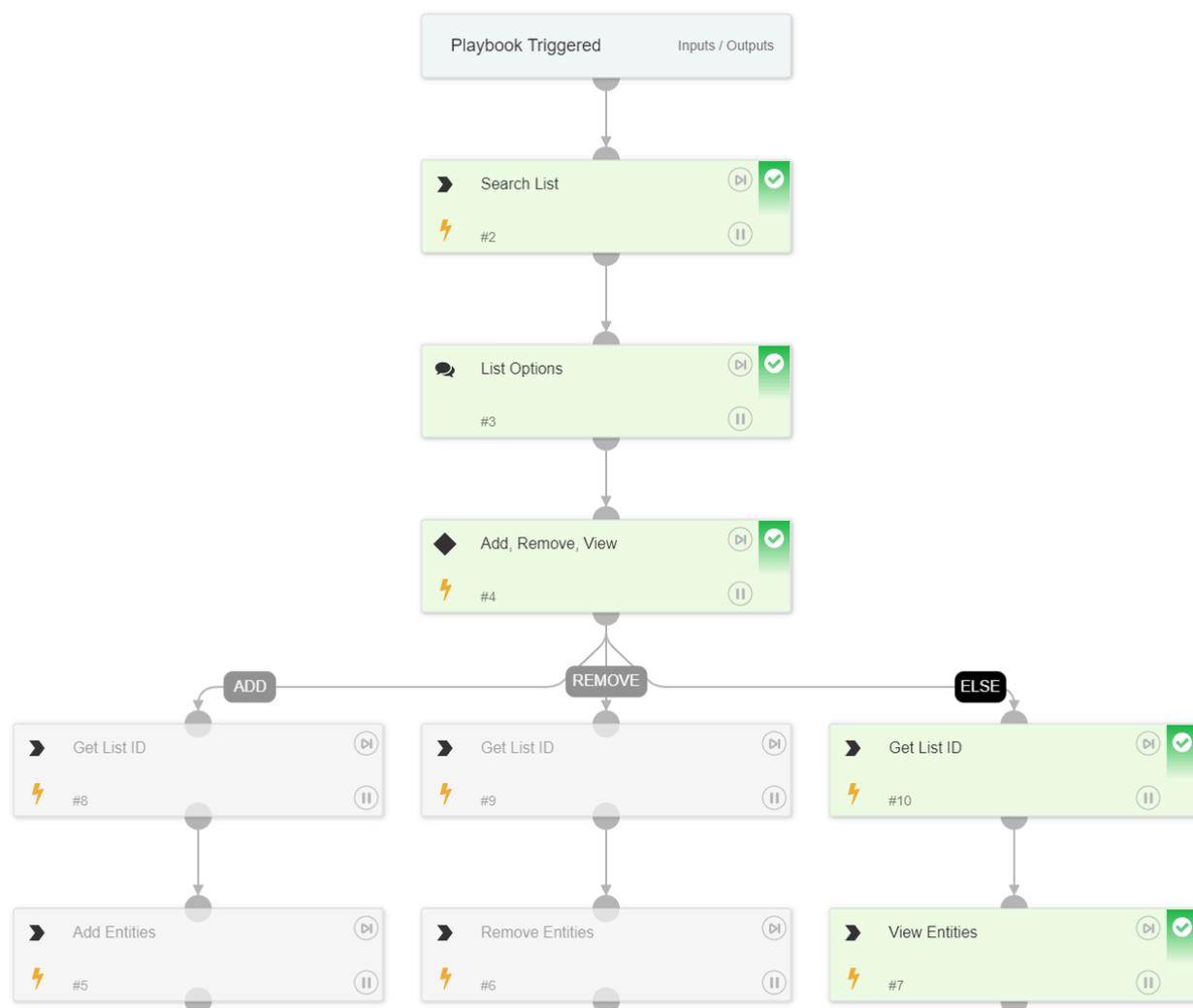
Recorded Future Watch lists help maintain relevance of Recorded Future alerts. The List API Provides a method to automatically maintain and manage these lists outside of the Recorded Future Portal.

### Issue

Not all team members may have access to the Recorded Future portal and maintenance of watch lists may be considered a time consuming task which isn't highly prioritized which leads to the watch list data becoming stale and this in turn may generate more unwanted noisy alerts.

### Solution

Managing the watch lists through the API allows the technology stacks to be maintained through asset scanners / vulnerability scanners ensuring the vulnerability alerts are always accurate and reflect potential threats to the organization. [Template Playbook](#)



# Dynamic Blocking

## Use Case Summary

Performing automated or analyst decision gated decision blocks against firewall and endpoint devices ensures accuracy and timely action is performed against known bad IOCs.

## Issue

Determining whether to block an entity can be a time consuming task involving checking safe lists, critical asset lists and identifying whether the entity should be blocked based on triage information and intelligence. During this time, the entity may have been utilized by more victims or the threat actor to conduct objectives.

## Solution

Automatically verify whether an entity with a high risk score is on a safe list, watchlist or no list and make appropriate decisions based on that data. For example if a high risk IP is not a safe list and the victim asset is on the critical assets list, it may be pertinent to Proactively block the IP and flag the Incident for priority triage / investigation to determine if the IP should remain blocked or be removed from the Block list. This will ensure critical assets are protected much faster and remediated quickly following automated threat mitigation.

Proactive blocking may also be utilized via pushing known high threat data to firewalls on a regular cadence. Recorded Future Security Control Feeds for example may be utilized to frequently update a known C2 Block list on a Firewall.

Batch enrichment could also be utilized to enrich large feed lists obtained from third parties with no previous context to determine a threat level and baseline to block high fidelity bad entities.

The screenshot shows the 'Indicators' section of a security dashboard. It features a search bar, several action buttons (Create incident, Edit, Delete and Exclude, Export CSV, Export STIX), and a table of indicators. The table columns are: TYPE, VALUE, VERDICT, RECORDED FUTURE RISK SCORE, SOURCE INSTANCES, SOURCE TIME STAMP, EXPIRATION STATUS, and EXPIRATION. All indicators listed are of type 'IP' and have a 'Malicious' verdict and a risk score of 99. The expiration status for all is 'Active', and the expiration date is 'Feb 9th 2024 15:08:31'.

	TYPE	VALUE	VERDICT	RECORDED FUTURE RISK SCORE	SOURCE INSTANCES	SOURCE TIME STAMP	EXPIRATION STATUS	EXPIRATION
<input type="checkbox"/>	IP	110.42.214.238	> Malicious	99	Recorded Future Default IP List...	Feb 2nd 2024 11:27:29	Active	Feb 9th 2024 15:08:31
<input type="checkbox"/>	IP	38.46.13.115	> Malicious	99	Recorded Future Default IP List...	Feb 2nd 2024 11:27:29	Active	Feb 9th 2024 15:08:31
<input type="checkbox"/>	IP	152.136.104.49	> Malicious	99	Recorded Future Default IP List...	Feb 2nd 2024 11:27:29	Active	Feb 9th 2024 15:08:31
<input type="checkbox"/>	IP	143.198.237.171	> Malicious	99	Recorded Future Default IP List...	Feb 2nd 2024 11:27:29	Active	Feb 9th 2024 15:08:31
<input type="checkbox"/>	IP	185.81.157.14	> Malicious	99	Recorded Future Default IP List...	Feb 2nd 2024 05:21:29	Active	Feb 9th 2024 15:08:31
<input type="checkbox"/>	IP	85.175.101.203	> Malicious	99	Recorded Future Default IP List...	Feb 2nd 2024 05:21:29	Active	Feb 9th 2024 15:08:31
<input type="checkbox"/>	IP	139.84.229.159	> Malicious	99	Recorded Future Default IP List...	Feb 2nd 2024 05:21:29	Active	Feb 9th 2024 15:08:31
<input type="checkbox"/>	IP	85.208.109.15	> Malicious	99	Recorded Future Default IP List...	Feb 1st 2024 17:09:29	Active	Feb 9th 2024 15:08:31

## Custom File Ingestion

Utilizing the Recorded Future Fusion API, security teams can create custom data outputs for SOAR Platforms, SIEMs, ticketing systems, endpoint security, and other analytic tools or security devices using internal client-sourced data enriched with Recorded Future's threat intelligence data. Or simply combine / augment the details available in the Recorded Future Graph API to a custom Recorded Future Risk List (for example combining multiple risk lists and reducing the fields to a simple block list)

## Security Control Feed Ingestion

Security Control Feeds are precompiled Detect and Block grade Intelligence Feeds based on Recorded Future Data generated from internally verified sources & methods to create datasets for specific security use cases. The purpose of these feeds is for proactive blocking and high fidelity detection of threats. Unlike 'Recorded Future Risk Lists', Security Control Feeds do not contain 'Risk Scores', 'Risk Rules' or 'Evidence Details'.

The Security Control Feeds do in some instances generate risk rules against data contained in the Recorded Future Intelligence Graph; this data is on the "Recorded Future Risk Lists". As such not all Security Control Feed IOCs are contained in the Recorded Future Graph and some that are may have a low risk score; this does not detract from the fidelity of the IOC being high due to inclusion in the Security Control Feed.

## External Dynamic List Integration

*External Dynamic List Credentials*

Username  
*User name*

---

Password  
*Password*

---

---

External Dynamic List - PAN-OS LEGACY ⓘ

---

Enable External Dynamic List

ⓘ Enabling External Dynamic Lists (EDL) allows integration of your defined external Domain Names and IP Addresses lists with your firewall. For more information on how EDL integrates with Palo Alto firewalls, see [Using an External Dynamic List in Policy](#).

IP ADDRESSES EDL URL:  
[https://edl-rpx1.xdr.us.paloaltonetworks.com/block\\_list?type=ip](https://edl-rpx1.xdr.us.paloaltonetworks.com/block_list?type=ip) ⓘ

DOMAIN NAMES EDL URL:  
[https://edl-rpx1.xdr.us.paloaltonetworks.com/block\\_list?type=domain](https://edl-rpx1.xdr.us.paloaltonetworks.com/block_list?type=domain) ⓘ

---

External Dynamic List - Generic Integration NEW

---

To configure External Dynamic List Integration, use the relevant ["Automation & Feed Integration"](#)



### Generic Export Indicators Service

Content Pack: [Generic Export Indicators Service](#)

Use the Generic Export Indicators Service integration to provide an endpoint with a list of indicators as a service for the system indicators. [Show less](#)

[Hide commands](#)

edl-update (Deprecated)	Updates values stored in the EDL (only available On-Demand).
export-indicators-list-update	Updates values stored in the List (only available On-Demand).

# Identity Exposure

## Use Case Summary

Credentials are commonly used to laterally move around a network undetected for long periods of time. Identifying leaked or stolen credentials early can assist with quick mitigation or identification of an asset breach.

## Issue

Commonly, data breaches are detected before identity exposures. Infostealer malware may extract credentials for resale, or to be utilized in a later attack. It can be difficult to detect and attribute credential breaches to an attack after the breach has occurred without extensive forensic analysis.

## Solution

Leverage the Recorded Future Identity Intelligence integration to proactively detect and respond to employee and customer identity compromises. By automating the collection and analysis of identity intelligence, organizations can enhance their overall security posture and minimize the risk of unauthorized access or data breaches. [Template Playbook](#)

The screenshot displays a Recorded Future alert interface with the following sections:

- Incident Info:** #96 Recorded Future Playbook Alert - Identity novel exposures ulisse611@norsego... Source | reclut identity 2/14 Actions Side panels Search in Incidents
- Incident Info Tabs:** Incident Info, War Room, Work Plan, Evidence Board
- CASE DETAILS:**
  - Type: mock Identity Exposure PBA
  - Severity: Medium
  - Source Brand: Recorded Future Identity
  - Source Instance: reclut identity
  - Playbook: proserv identity exposure pba response
- RECORDED FUTURE ALERT OVERVIEW:**
  - Alert ID: d9bc75f7-1e9c-4094-af6b-12910b155757
  - Alert Name: Novel Identity Exposure
  - Occurred: Jul 9th 2024 12:51:23
  - Source Priority: Moderate
  - Target: norsegods.online
  - Recorded Future Ident...: Malware
- RECORDED FUTURE SET ALERT STATUS:**
  - In-Progress
  - Dismissed - False Positive
  - Resolved - True Positive
  - Select Resolving Action
- IDENTITY EXPOSURE:**
  - Recorded Future Identity Dump Name: Stealer Malware Logs 2024-06-29
  - Description: This credential data was derived from stealer malware logs. These logs are legally obtained through proprietary methods from multiple underground sources. Most data is available within 48 hours after the infection. Refer to exfiltration date for each specific exposure.
  - Recorded Future Identity Name: ulisse611@norsegods.online
  - Recorded Future Identity Authorization URL: https://norsegods.online
  - Source IP: 93.45.72.190
  - Recorded Future Identity Malware Family: Stealc
  - Recorded Future Identity Compromised Host: [Table with columns OS, OS USERNAME, COMPUTER NAME, ANTI]
- EXPOSED SECRET DETAILS:**
  - Recorded Future Identity Exposed Properties: Letter, Number, UpperCase, LowerCase, AtLeast10Characters
  - Recorded Future Identity Exposed Hint: 20
  - Recorded Future Identity Exposed Secret:

ALGORITHM	HASH
SHA1	26ef12a5493c633fb942bc6fae164f78022c2ce
SHA256	acaf401c5012940299c590ea19391f996e90212379db2269d6a37f...
NTLM	71d75d94f999ee39573164fb7d228683e
- INITIATE RESPONSE TASKS:**
  - Disable Account
- WORK PLAN (1):**
  - Waiting for users (1)
  - Review account manually
  - Review the identity exposure user credential in question manually, either via Active Directory, an Identity Access Management system, or log event data within a SIEM tool.
  - View in: Tasks Pane or Work Plan
- TIMELINE INFORMATION:**
  - Occurred: Jul 9th 2024 12:51:23
  - DBot Created: Jul 9th 2024 12:51:23
  - DBot Modified: Jul 18th 2024 09:56:28

## Collective Insights

### Use Case Summary

Enriched security events serve as inputs into the Recorded Future platform, unveiling patterns and emerging trends across security tools employed by all clients. The fusion of Recorded Future Intelligence and Collective Insights from Cortex XSOAR delivers a comprehensive and holistic perspective, empowering organizations to effectively prioritize and address potential threats.

### Issue

Effective detection of emerging threats faced by organizations require proactive insights from what is happening internally, externally, and to other organizations.

### Solution

Customize insights based on internal telemetry with the new SecOps Intelligence dashboard, helping to proactively detect threats, and prioritize them based on risk factors. In addition, map detections against the MITRE ATT&CK framework to show what types of adversary TTPs are being used within the environment to prioritize mitigation techniques effectively. Collective Insights currently powers the Malware Threat Map within the Threat Intelligence module as well.

#### SecOps Intelligence

Overview Detection Activity Detection Explorer

All detections from Recorded Future integrations connected to Recorded Future Collective Insights  
Connected Integrations: Splunk Integration, XSOAR Integration +7

Detections Ignored Detections

Source Xsoar - Collective Insights Demo (+1) Entity Type All Detectors All Malware All Mitre Codes All Event Source All Reset Last 30 Days

Entity	Description	Detectors	Malware	Mitre Code	Source	Event Source	Detection Date
<input type="checkbox"/> example.net 15	Recorded Future Phishing Triage	Playbook	-	-	Xsoar - Collectiv...	-	Feb 14, 2024, 11:29
<input type="checkbox"/> norsegods.online 10	Recorded Future Phishing Triage	Playbook	T1566 (Phishing) T1566.002 (Phishing: Spearphishing Link)	-	Xsoar - Collectiv...	-	Feb 14, 2024, 11:29
<input type="checkbox"/> itaucardi23.000webhostapp.com 74	Recorded Future Phishing Triage	Playbook	TA0002 (Execution) TA0001 (Initial Access)	T1566, T1566.002, TA0002, ...	Xsoar - Collectiv...	-	Feb 14, 2024, 11:29
<input type="checkbox"/> 10.0.0.10	Recorded Future Phishing Triage	Playbook	TA0011 (Command and Control)	-	Xsoar - Collectiv...	-	Feb 14, 2024, 11:29
<input type="checkbox"/> bdbd498b740d9548856c47b1d20d270a8772b2552bae0ed1ac79de0e13f561ca 89	Recorded Future Phishing Triage	Playbook	-	TA0002	Xsoar - Collectiv...	-	Feb 14, 2024, 11:29
<input type="checkbox"/> bdbd498b740d9548856c47b1d20d270a8772b2552bae0ed1ac79de0e13f561ca 89	Recorded Future Malware Detected	Playbook	-	TA0002	Xsoar - Collectiv...	-	Feb 14, 2024, 11:29
<input type="checkbox"/> 193.142.147.59 99	Recorded Future Phishing Triage	Playbook	Raccoon Stealer	T1071, TA0011	Xsoar - Collectiv...	-	Feb 14, 2024, 11:29
<input type="checkbox"/> http://itaucardi23.000webhostapp.com/inicio.html 78	Recorded Future Phishing Triage	Playbook	-	TA0011, T1204.001, T1566...	Xsoar - Collectiv...	-	Feb 14, 2024, 11:29

# Technical References *Commands and Outputs*

## Intelligence Content Pack

Recorded Future's intelligence, related context, and technical links provide an invaluable method to utilize threat intelligence data within automation and orchestration playbooks to perform operations such as blocking, triaging, containment, and hunting with a high level of confidence.

### Enrichment

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

Commands within this pack include:

#### Reputation Command

Real-time Risk Scores, Risk Rules and Evidence Details for IP, Domain, URL, Hash, and Vulnerability

**Example:** `!ip ip="107.174.176.209"`

**Recorded Future IP reputation for 107.174.176.209**

Risk score: 31  
 Risk Summary: 3 out of 71 Risk Rules currently observed  
 Criticality: Suspicious

[Intelligence Card](#)

**Risk Rules Triggered**

[Export to CSV](#)

Criticality	Rule	Evidence	Timestamp
Suspicious	Previously Validated C&C Server	5 sightings on 1 source: <code>&lt;e id=source:qGrIFQ&gt;Recorded Future Command &amp; Control Validation&lt;/e&gt;</code> . Recorded Future analysis validated <code>&lt;e id=ip:107.174.176.209&gt;107.174.176.209&lt;/e&gt;</code> : <code>&lt;e id=mf6ngC&gt;7777&lt;/e&gt;</code> as a command and control server for <code>&lt;e id=LnK3Q6&gt;Cobalt Strike&lt;/e&gt;</code> on Oct 03, 2023	2023-10-03 08:30:47
Suspicious	Historically Reported C&C Server	6 sightings on 1 source: <code>&lt;e id=source:qU_q-9&gt;Recorded Future Command &amp; Control Reports&lt;/e&gt;</code> . <code>&lt;e id=ip:107.174.176.209&gt;107.174.176.209&lt;/e&gt;</code> : <code>&lt;e id=mf6ngC&gt;7777&lt;/e&gt;</code> was reported as a command and control server for <code>&lt;e id=LnK3Q6&gt;Cobalt Strike&lt;/e&gt;</code> on Oct 03, 2023	2023-10-17 11:03:32
Informational	Recorded Future Predictive Risk Model	High Risk activity in CIDR Block.	2023-10-17 11:03:32

**Figure 1.** IP Reputation Command with Corresponding Results

### Intelligence Command

Deeper context, Related indicators, and Associated threat actors where such data exists.

**Example:** `!recorded-future-intelligence profile="all" entity_type="ip" entity="107.174.176.209" fetch_related_entities=yes`

#### Recorded Future IP Intelligence for "107.174.176.209"

Risk Score: 35  
 Summary: 4 of 71 Risk Rules currently observed.  
 Criticality label: Suspicious  
 Total references to this entity: 0  
 ASN and Geolocation  
 AS Number: [AS36352](#)  
 AS Name: AS-COLOCROSSING  
 CIDR: [107.174.176.0/20](#)  
 Geolocation (city): N/A  
 Geolocation (country): United States  
 First reference collected on: 2023-10-04 00:00:00  
 Latest reference collected on: 2023-10-04 23:59:59  
[Intelligence Card](#)

#### Triggered Risk Rules

Rule Criticality	Rule Triggered	Evidence Summary	Rule Triggered Time
Very Malicious	Actively Communicating Validated C&C Server	3 sightings on 1 source: Recorded Future Network Intelligence. Multiple communications observed between 73.127.52.111 on 20 ports including 47138 and 45.133.238.221 (validated Mythic C2 Server) on port 7443 on 2023-10-03 at 17:43 UTC.	2023-10-03T00:00:00.000Z

#### Related Entities

RelatedInternetDomainName	RelatedIpAddress	RelatedProduct
amazon.com, googleusercontent.com, contaboserver.net, datacheap.ru, mtc.com, ec2-13-59-188-22.us-east-2.compute.amazonaws.com, ec2-18-176-35-161.ap-northeast-1.compute.amazonaws.com, ec2-35-78-243-160.ap-northeast-1.compute.amazonaws.com, rapid7.cloud, stark-industries.solutions,	77.242.250.36, 13.82.141.216, 101.35.148.219, 109.248.6.225, 13.59.188.22, 165.227.136.106, 18.176.35.161, 31.44.184.129, 39.105.107.87, 39.105.231.22,	Akamai Connected Cloud

Figure 2. IP Intelligence command with corresponding results and related entities

## Technical Links

Technical Links are high-confidence, evidence-based, indicator linkages that are technically validated via malware sandbox analysis, infrastructure analysis, network traffic analysis, and more. Links provide a greater understanding of the threat and a pivot point for hunting related indicators, threat actors, TTPs, and much more.

### Links Command

Technical related entities from the Recorded Future sandbox, and Insikt research from the previous 30 days

---

**Example:** `!recordedfuture-links entity_type="ip" entity="123.59.211.213"`

**Insikt Group Research Links for: 123.59.211.213**

Category Actors, Tools & TTPs

Threat Actor	FIN12
<b>Malware</b>	
Cobalt Strike	
Conti Ransomware	
Ryuk Ransomware	
Trickbot	

**Figure 3.** Links Command with IP entity type and corresponding results

---

**Example:** `!recordedfuture-links entity_type="domain" entity="anbackup.com"`

**Insikt Group Research Links for: anbackup.com**

Category Actors, Tools & TTPs

Threat Actor	FIN12
<b>Malware</b>	
Cobalt Strike	
Conti Ransomware	
Ryuk Ransomware	
Trickbot	

**Figure 4.** Links Command with Domain entity type and corresponding results

## Legacy & Playbook Alert management

Alerts can be ingested as a summary from the portal against a given filter such as rule-id, Triggered-time, Assignee and Status. Additionally, the alerts can be updated with the 'recorded-future-alert-set-status' command and 'recorded-future-alert-set-note' commands. To retrieve a list of Rule IDs, use the 'recorded-future-alert-rules' command.

### Legacy Alert Command

Retrieve all or filtered Legacy Alerts over a time period

**Example:** `!recordedfuture-alerts triggered_time="1 day"`

Alert ID	Rule	Alert Title	Triggered	Status	Assignee
tDfK6B	Vidar Infrastructure Analysis	Vidar Infrastructure Analysis - 497 references	2023-10-18 12:04:09	no-action	
tDfK8C	Brand Mentions with Cyber entities	Brand Mentions with Cyber entities - 17 references	2023-10-18 12:04:19	no-action	
tDfK61	My domains on Dark Web and closed sources	My domains on Dark Web and closed sources - 2 references	2023-10-18 12:04:21	dismiss	
tDfK-u	My domains on Dark Web and closed sources	My domains on Dark Web and closed sources - 2 references	2023-10-18 12:08:13	dismiss	

### Legacy Individual Alert Command

Individual alerts can be ingested in detail from the portal against the Alert ID retrieved from the previous Alert command.

**Example:** `!recordedfuture-single-alert id=tDfK61`

### My domains on Dark Web and closed sources - 2 references

**Status:**  
dismiss

**Note:**

**Recorded Future AI Insights**

The Recorded Future AI requires more references in order to produce a summary.

**Title:** Fresh cc [fullzdumpspn,tracks 1&2western unionpaypal clone cards+ gift cards](#)

URL: [https://Card%20Villa%20Forum%20\(Obfuscated\)/help-desk/558544-fresh-cc-fullz-dumps-pin-tracks-1-2-western-union-paypal-clone-cards-gift-cards-post695033.html#post695033](https://Card%20Villa%20Forum%20(Obfuscated)/help-desk/558544-fresh-cc-fullz-dumps-pin-tracks-1-2-western-union-paypal-clone-cards-gift-cards-post695033.html#post695033)

Source: Card Villa Forum  
Source id: source:WViMED

**Entities for document** [Export to CSV](#)

fragment	id	name	type
> **US: (Bank of America,Chase,Wells Fargo...)	B_FAG	United States	Country
> **US: (Bank of America,Chase,Wells Fargo...)	ruAYO1	Wells Fargo	IndustryTerm
> **US: (Bank of America,Chase,Wells Fargo...)	B_L_k	Bank of America	Company

### Playbook Alert Command

Playbook Alerts can be ingested in summary from the portal against a given filter such as category, time-since-update, playbook-alert-status and priority. Additionally, the alerts can be updated with the 'recorded-future-alerts-update' command.

To retrieve a list of Rule IDs, use the 'recorded-future-alert-rules' command.

**Example:** `!recordedfuture-playbook-alerts-search`

Playbook alert ID	Title	Category	Status	Priority	Last update
08caf711-3af3-4f0f-b304-743e988e8b5f	<a href="https://github.com/uqarni/fullharvest">https://github.com/uqarni/fullharvest</a>	Code repo leakage	New	Informational	2023-10-18, 15:16
d19fede0-012e-48d4-8c3f-07563dac3a31	<a href="https://github.com/zo-bla-kv/house-of-dogs">https://github.com/zo-bla-kv/house-of-dogs</a>	Code repo leakage	New	Moderate	2023-10-18, 15:03

### Playbook Alert Command

Retrieve playbook alert details via selecting details including: summary, whois, status, log, action and dns

**Example:** `!recordedfuture-playbook-alerts-details alert_ids="08caf711-3af3-4f0f-b304-743e988e8b5f" detail_sections=summary`

Recorded Future  
Playbook Alert / Data Leakage on Code Repository

<https://github.com/uqarni/fullharvest>

---

**Summary**

Repository owner: [uqarni](#)  
[Go to repository](#)

**Evidence**

Watch List Entity Mention: Matched keyword HubSpot  
<https://github.com/uqarni/fullharvest/commit/08caf711-3af3-4f0f-b304-743e988e8b5f>  
Published: 2023-10-18T15:14:43.431Z

```
+++ b/salesforce_client.py
@@ -1,4 +1,4 @@
-class Salesforce();
+class Hubspot();
```

## List Management

Recorded Future lists are utilized to ensure alerts are valid and targeted. For example, updating the 'tech stack watch list' ensures all vulnerability alerts are tailored to the technologies in that list. The API List endpoint enables the management and potential automation to maintain those lists.

### Lists-search Command

Show all available lists to obtain the relevant List IDs

**Example:** `!recordedfuture-lists-search`

List	Contains	Last updated	Created	ID
Tech Company Attackers	entity	2022-12-20T10:57:45.940Z	2013-11-14T20:29:31.585Z	
RF - Tech Companies	entity	2022-12-20T10:57:45.971Z	2013-11-15T23:41:59.323Z	
ICS Technology Targets	entity	2022-12-20T10:57:46.030Z	2013-11-22T02:10:22.646Z	
Tech Ontology	entity	2022-12-20T10:57:46.231Z	2014-01-08T15:45:38.440Z	
Tech Infrastructure	entity	2023-03-21T17:03:19.049Z	2014-01-22T23:51:43.151Z	

### Lists-entities Command

Show all contained entities within the Lists via List IDs

**Example:** `!!recordedfuture-lists-entities list_ids="report:abcde,report:vwxyz"`

Entity	Type	Id
Turkish Hackers	Organization	
Microsoft Digital Crimes Unit	Organization	
Nicholas Percoco	Person	
Team Madleets	Organization	
German Hackers	Organization	
Jacobson	Person	
Nunez	Person	

### Lists-add Command

Add single or multiple entities from a specific list via a comma delimited list

**Example:** `!recordedfuture-lists-add-entities list_id=abcd freetext_names="1.1.1.1" type=ip`

### Lists-remove Command

Remove single or multiple entities from a specific list via a comma delimited list

**Example:** `!recordedfuture-lists-remove-entities list_id=abcd entity_ids="vwxyz,pqrst"`

## Threat Actor Maps with Enrichment

The Recorded Future Threat Map tracks threat actor data utilizing watch lists and Insikt Group analysis. Collective Insights also feeds data to the Threat Actor Map to provide additional sourcing against the threat map data. This data identifies Threat Actors with a calculated high intent and opportunity to be considered a threat.

### Threat-Map data retrieval command

Retrieve Intelligence data and technical links related to a Threat Actor of Interest

**Example:** `!recordedfuture-threat-map include_links=true actor_name="LockBit Gang"`

### Threat actors result

Name: LockBit Gang  
 Alias: LockBit Ransomware Group, LockBit Group, LockBit 2.0 ransomware group, LockBit, White Janus, Gold Mytic, lockbit, LockBit Ransomware Gang, BITWISE SPIDER  
 Intent: 74  
 Opportunity: 57  
 Categories: Ransomware and Extortion Groups, Threat Actor

**Links:**  
 LockBit Gang/type:Organization links

URL type links [Export to CSV](#)

Name	Source	Criticality
http://lockbit-decryptor.top	technical	Malicious

## **Sandbox Content Pack**

Recorded Future's malware analysis sandbox provides a high-volume analysis capability and supports configurable malware analysis with automated Threat Intelligence enrichment to enable detection and Orchestrated action against confirmed threats. URLs and files are supported.

### **File sample submission**

Submit a file by uploading / dragging to the war room and retrieving the "id" via the 3 dots on the upper right hand side of the results.

Property	Value
Type	application/zip
Size	591,311 bytes

### **File sample submission command**

Submit the file to the Triage IO service for processing with the file ID obtained from XSOAR

**Example:** `!triage-submit-sample kind="file" interactive="false" data="258@8c8aa15c-f239-45a7-86b5-ece72ce2fe82"`

---

filename	231026-reav2sdrqd_pw_infected.zip
id	231027-q2mmpap1yt
kind	file
private	true
status	pending
submitted	2023-10-27T13:45:30Z

### **Triage Report Retrieval Command**

There are multiple task IDs related to the analysis of the file / url ("behavioral1", "behavioral2" and "static". All three task reports must be retrieved individually in order to obtain the full results.

**Example:** `!triage-get-report-triage sample_id=231027-q2mmpap1yt task_id=behavioral1`

---

## Identity Content Pack

Identity for Cortex XSOAR enables security and IT teams to detect identity compromises, for both employees and customers. Recorded Future's Identity integration continuously monitors for identity compromises, pulling in only those that align with the organization's enabled domains.

### Identity search command

Fetch the latest discovered leaked identities

**Example:** `!recordedfuture-identity-search latest-downloaded="six months ago" domain-type="Email"`

### This is search results for norsegods.online :

- `**442102344@norsegods.online**` in domain `norsegods.online`
- `**aalmidi@norsegods.online**` in domain `norsegods.online`
- `**aegir.ymirsson@norsegods.online**`
- `**ahmostafa@norsegods.online**` in domain `norsegods.online`

### Identity lookup command

Fetch specific details for a leaked credential

**Example:** `!recordedfuture-identity-lookup identities="442102344@norsegods.online" first-downloaded="six months ago" domain-type="Email"`

**Compromised credential [1]**

Rank: N/A  
 Properties: Letter, Number, Symbol, UpperCase, LowerCase, AtLeast10Characters  
 Type: clear  
 Effectively clear (i.e., password unencrypted): True  
 Password Hint: FA

[Export to CSV](#)

Hash Algorithm	Hash Value
SHA1	590555d415b0e44a8b045cc807a37e3f
SHA256	e37797d9a889efc3c1797fbcc3640d22c
NTLM	md4 no longer supported
MD5	f1db8ec5ecd3eca53c81c0fa106fc867

Authorization Service Url: <https://norsegods.online/owa/>  
 Domain: norsegods.online  
 First Downloaded: 25 Oct 2023  
 Last Downloaded: 25 Oct 2023  
 Exfiltration Date: N/A  
 Malware Family: Vidar

**Compromised credential [1] Dump Data**

Stealer Malware Logs 2023-07-12  
 Dump Downloaded Date: 25 Oct 2023

Description: This credential data was derived from stealer malware logs. These logs are legally obtained through proprietary methods from multiple underground sources. Most data is available within 48 hours after the infection. Refer to exfiltration date for each specific exposure.

Dump type: N/A

**Compromised Host**

Operating System: Windows 10 Pro [x64]  
 OS User Name: faisa  
 File Path Location: C:\Users\faisa\AppData\Local\Temp\7z083CC7746\Setup.exe  
 Time Zone: UTC+03:00  
 Name of the Machine: FAISAL  
 User Account Control Setting: N/A  
 Antivirus: N, /, A  
 IP Address: 78.95.97.175



## 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 Cortex XSOAR 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.