

# Recorded Future Configuration Guide

## App Configuration

Recorded Future's connector app is available in Cyware Threat Intelligence eXchange (CTIX) and security teams can easily leverage it by adding their authentication credentials. Follow the below steps to activate and get started.

1. Navigate to the **Integration Management** module and select the **Enrichment Tools** section. This section displays the list of all available apps.
2. Use the search bar to locate "**Recorded Future**" and click on the app to open the configurations page.
3. Now, click on the "**Edit**" button adjacent to Settings and enter API credentials, which include Base URL and API Key. Base URL and API Key details are shared by Recorded Future.
4. After finishing, click "**Save Settings**". Now you will be able to configure available Actions and make the app "**Active**".
5. Use the "**status toggle switch**" on the top of the page to activate the app.

## Recorded Future Configuration

1. Base URL and API Key must be obtained from Recorded Future.

## Action Configuration

The **Actions** section displays the list of actions/endpoints that are configured for the app. Click on the "**Configuration**" button to perform the following activities.

The below screenshot shows an intel feed received from Recorded Future

## Intel Packages

Refresh



Source Recorded Future X



| <input type="checkbox"/> | Title                                             | Source          | Created on ^           | Received on            | Actions |
|--------------------------|---------------------------------------------------|-----------------|------------------------|------------------------|---------|
| <input type="radio"/>    | IP Address 213.159.203.51 ....and more.           | Recorded Future | Jun 09, 2020, 02:42 PM | Jun 09, 2020, 03:23 PM | ...     |
| <input type="radio"/>    | Domain www.abuseipdb.com ....and more.            | Recorded Future | May 29, 2020, 01:55 PM | May 29, 2020, 02:54 PM | ...     |
| <input type="radio"/>    | IP Address 46.26.39.151 ....and more.             | Recorded Future | May 29, 2020, 01:42 PM | May 29, 2020, 01:52 PM | ...     |
| <input type="radio"/>    | SHA-256-hash a0fea4a4a71c69311f23b170c3d38...     | Recorded Future | May 29, 2020, 01:10 PM | May 29, 2020, 02:14 PM | ...     |
| <input type="radio"/>    | Vulnerability CVE-2019-19781 ....and more.        | Recorded Future | May 29, 2020, 12:15 PM | May 29, 2020, 01:25 PM | ...     |
| <input type="radio"/>    | URL http://mrscrowe.net/p66/9hgdfyr6 ....and m... | Recorded Future | May 29, 2020, 11:28 AM | May 29, 2020, 01:21 PM | ...     |
| <input type="radio"/>    | IP Address 46.26.39.151 ....and more.             | Recorded Future | May 27, 2020, 11:42 PM | May 28, 2020, 12:09 AM | ...     |

## Available Actions

### Retrieve Domain Feeds Data

This action can be used to get domain data types from the Recorded Future API endpoint.

1. Click on the Configuration button to configure Collections and Risk List Types.
2. Collections - These are used to group intel feeds received from sources. Multiple Collections can be associated with a Source. Enter a name to create a Collection. The below screenshot shows an Intel package received in Domain Data Collection from Recorded Future.

## &lt; Domain www.abuseipdb.com ....and more.

0 Duplicate(s) Found



## Basic Details

## Basic Details

Domain Objects

Package ID  
package-29636f85-7fb9-4165-a167-3396a7bef72b

Geo-IP Map

STIX Visualization

Description

HTML View Fang-Defang

Notes

Recorded Future STIX

Created on  
May 29, 2020, 01:55 PM

Received on  
May 29, 2020, 02:54 PM

Categorization  
Select Category v

Source(s)  
Recorded Future

Collection(s)  
Domain Feeds

TLP  
NONE

STIX  
1.x

3. Risk List Types - Risk Lists can be used to correlate and enrich events. Each domain data point in the risk list contains a risk score and the information which is contributed to its risk score. The available Risk List Types for Domain Data Endpoint can be selected from the drop-down list.

**Note:** Enter the required Risk List Types to this field to start receiving relevant feeds from this source. The below screenshot shows an example configuration for this action.

Action Configuration

×

☒ Automatic ☐ Manual

Polling Time (seconds)

600

Collection Name

Domain Feed

Risk List Type

Recent Typosquat Similarity - Typo or Homograph ×

▼

Cancel

Save Configuration

## Retrieve URL Feeds Data

This action can be used to get URL data types from the Recorded Future API endpoint.

1. Click on the Configuration button to configure Collections and Risk List Types.
2. Collections - These are used to group intel feeds received from Sources. Multiple Collections can be associated with a Source. Enter a name to create a Collection. The below screenshot shows the threat intel package received in the URL Data Collection from Recorded Future.

&lt; URL http://mrscrowe.net/p66/9hgfdy6r6 ....and more.

0 Duplicate(s) Found



**Basic Details**

Domain Objects

Geo-IP Map

STIX Visualization

Notes

Package ID  
package-e8509391-d794-4183-abe1-5c90dec21c3b

Description  
Recorded Future STIX

Created on  
May 29, 2020, 11:28 AM

Received on  
May 29, 2020, 01:21 PM

Source(s)  
Recorded Future

Collection(s)  
URL Feeds

TLP  
NONE

STIX  
1.x

HTML View

Fang-Defang

Categorization  
Select Category

- Risk List Types - Risk Lists can be used to correlate and enrich events. Each URL data in the risk list contains a risk score and the information which contributed to the risk score. The available Risk List Types for URL Data Endpoint can be selected from the drop-down list.

**Note:** Enter the required Risk List Types into this field to start receiving relevant feeds from this Source. The screenshot below shows an example configuration for this action.

Action Configuration ×

☒ Automatic ☐ Manual

Polling Time (seconds)  
600

Collection Name  
URL Feeds

Risk List Type  
Ransomware Distribution URL × ▼

Cancel

Save Configuration

## Retrieve Vulnerability Feeds Data

This action can be used to get Vulnerability data types from the Recorded Future API endpoint.

1. Click on the Configuration button to configure Collections and Risk List Types.
2. Collections - These are used to group intel feeds received from Sources. Multiple Collections can be associated with a Source. Enter a name to create a Collection. The screenshot below shows the threat intel package received in the URL Data Collection from Recorded Future.

Collection / Intel Packages / Vulnerability CVE-2019-19781 ....and mor... / Basic Details

< Vulnerability CVE-2019-19781 ....and more. 0 Duplicate(s) Found

Basic Details

Domain Objects

Geo-IP Map

STIX Visualization

Notes

Basic Details

Package ID  
package-ef9c5d79-0ac8-423b-9ae0-7eae6c5c5441

Description  
Recorded Future STIX

Created on  
May 29, 2020, 12:15 PM

Received on  
May 29, 2020, 01:25 PM

Categorization  
Select Category

Source(s)  
Recorded Future

Collection(s)  
Vulnerability Feeds

TLP  
NONE

STIX  
1.x

3. Risk List Types - Risk Lists can be used to correlate and enrich events. Each Vulnerability data in the risk list contains a risk score and the information which contributed to its risk score. The available Risk List Types for Vulnerability Data Endpoint can be selected from the drop-down list.

**Note:** Enter the required Risk List Types to this field to start receiving relevant feeds from this source. The below screenshot shows an example configuration for this action.

## Action Configuration



☒ Automatic ☐ Manual

Polling Time (seconds)

600

Collection Name

Vulnerability Feeds

Risk List Type

Recently Observed Exploit/Tool Development in the Wild ×

Cancel

Save Configuration

## Retrieve IP Feeds Data

This action can be used to get IP data types from the Recorded Future API endpoint.

4. Click on the Configuration button to configure Collections and Risk List Types.
5. Collections - These are used to group intel feeds received from Sources. Multiple Collections can be associated with a Source. Enter a name to create a Collection. The screenshot below shows the threat intel package received in IP Data Collection from Recorded Future.

## &lt; IP Address 213.159.203.51 ....and more.

0 Duplicate(s) Found



Basic Details

Domain Objects

Geo-IP Map

STIX Visualization

Notes

Package ID

package-8488c596-c227-4552-a99e-e19319b063c0

Description

Recorded Future STIX

HTML View

Fang-Defang

Created on

Jun 09, 2020, 02:42 PM

Received on

Jun 09, 2020, 03:23 PM

Categorization

Select Category

Source(s)

Recorded Future

Collection(s)

IP Feeds

TLP

NONE

STIX

1.x

6. Risk List Types - Risk Lists can be used to correlate and enrich events. Each IP data in the risk list contains a risk score and the information which contributed to its risk score. The available Risk List Types for IP Data Endpoint can be selected from the drop-down list.

**Note:** Enter the required Risk List Types to this field to start receiving relevant feeds from this Source. The below screenshot shows an example configuration for this action.

## Action Configuration

☒ Automatic ☐ Manual

Polling Time (seconds)

600

Collection Name

IP Feeds

Risk List Type

Malware Delivery ×

Historical Spam Source ×



Cancel

Save Configuration

## Retrieve Hash Feeds Data

This action can be used to get Hash data types from the Recorded Future API endpoint.

1. Click on the Configuration button to configure Collections and Risk List Types.
2. Collections - These are used to group intel feeds received from sources. Multiple Collections can be associated with a Source. Enter a name to create a Collection. The screenshot below shows the threat intel package received in Hash Data Collection from Recorded Future.

Collection / Intel Packages / SHA-256-hash 837e469561a338074a0adcda80c... / Basic Details

< SHA-256-hash 837e469561a338074a0adcda80c2e3cfc4f3997d2bf7c0bce5e405e8cdf27f [View More](#) 0 Duplicate(s) Found [Share](#) [More](#)

[Basic Details](#)  
[Domain Objects](#)  
[Geo-IP Map](#)  
[STIX Visualization](#)  
[Notes](#)

### Basic Details

Package ID  
package-6ebc3d68-0f81-47ce-abdf-644272d975a2

Description  
Recorded Future STIX

Created on  
May 27, 2020, 10:07 PM

Received on  
May 27, 2020, 11:05 PM

Categorization  
[Select Category](#) [HTML View](#) [Fang-Defang](#)

Source(s)  
Recorded Future

Collection(s)  
Hash Feeds

3. Risk List Types - Risk Lists can be used to correlate and enrich events. Each Hash data in the risk list contains a risk score and the information which contributed to its risk score. The available Risk List Types for Hash Data Endpoint can be selected from the drop-down list.

**Note:** Enter the required Risk List Types to this field to start receiving relevant feeds from this Source. The below screenshot shows an example configuration for this action.



## Action Configuration



☒ Automatic ☐ Manual

Polling Time (seconds)

600

Collection Name

Hash Feeds

Risk List Type

Linked to Cyber Attack ×



Cancel

Save Configuration

## Use Case: CTIX Threat Visualizer and Recorded Future

The Threat Visualizer feature in CTIX deduces important context from complex threat intelligence data to help analysts investigate security incidents with improved insights. Recorded Future integration can be utilized in the Threat Visualizer canvas to uncover additional context for threat indicators (IOCs) during the investigation stage of the threat intelligence lifecycle.

**Challenge:** While researching IOCs in the Threat Visualizer, analysts need access to key information in order to correlate and investigate complex and seemingly isolated data. The vast amount of data and hidden relations present in intel packages restrict analysts from uncovering threats and delay the execution of necessary actions to block the threats.

**Solution:** Using the CTIX Visualizer and Recorded Future together, analysts can effortlessly tackle this challenge. The Threat Visualizer in CTIX allows analysts to quickly gather the necessary threat intelligence from Recorded Future and get a single-pane view on the IOC relationships. Analysts can also uncover the relations between other ongoing threat activities to facilitate faster response and deploy informed actions more confidently.