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
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.
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.

---

**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.
3. **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.
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.

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.
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.
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.
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.

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.
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.