Recorded Future Risk List Integration

Installation and Configuration Guide

Software Version 1.0

July 29, 2020

30040-03 EN Rev. A

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 | F: .703.229.4489
www.ThreatConnect.com

Table of Contents

OVERVIEW

The ThreatConnect® integration with the Recorded Future Risk List allows ThreatConnect to ingest Address, Host, URL, and File Indicators that Recorded Future has added to its Risk List and enriches the Indicators with sourcing information, allowing analysts to have an improved context as well as a place to start their research when correlating Indicators from an incident.

DEPENDENCIES

ThreatConnect Dependencies

- ThreatConnect version 5.6 or newer
- Active ThreatConnect Application Programming Interface (API) key

NOTE: All ThreatConnect dependencies will be provided by default to subscribing ThreatConnect Cloud customers. Private Instance customers can enable these settings during configuration under the *Account Settings* ***menu within their Private Instance of ThreatConnect or locally in their On Premises setup. Job creation can be done either in an On Premises installation or on a ThreatConnect Environment Server.***

Recorded Future Dependencies

- An active Recorded Future API token

APPLICATION SETUP AND CONFIGURATION

Use the ThreatConnect Feed Deployer to set up and configure the Recorded Future Risk List Integration app, or follow the steps in the "Creating a Source" section of the ***ThreatConnect Account Administration Guide*** to create and configure the Recorded Future Source, the “Creating API Accounts” section of the ***ThreatConnect Organization Administration Guide*** to generate an API key set for the ThreatConnect Organization, and the “Creating a Job” section of the ***ThreatConnect Organization Administration Guide*** to add a Job, which will activate the Recorded Future app and pull down Indicators.

CONFIGURATION PARAMETERS

Parameter Definition

The parameters defined in Table 1 apply to the configuration parameters during the job-creation process.

Table 1

Name	Description
ThreatConnect API User	This parameter is the API user that will retrieve data from ThreatConnect.
ThreatConnect Default Org Name	This parameter is the owner to which the Indicators will be added.
Logging Level	This parameter is the level used to determine the verbosity of the logging output for the application.
Recorded Future Token	This parameter is the Recorded Future API token. It is used for authentication.
Recorded Future Feed	This parameter is a multi-select list of the Recorded Future Risk List feeds that will be downloaded.

RECOMMENDATIONS

It is recommended that Address, Host, and URL feeds are scheduled for updates every 4 hours. File feeds should be updated every 24 hours.

TROUBLESHOOTING

Refer to the following steps if Indicators are not arriving in the configured data owner:

1. Verify that the API information is correct in the job parameters (for both ThreatConnect and Recorded Future).
2. If these items have been verified and you are still experiencing issues, contact your Customer Success Engineer for assistance.