ThreatConnect™

Intel 471 Adversary Intelligence Integration

Configuration Guide

Software Version 1.0

June 17, 2020

30021-03 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 Intel 471 Adversary Intelligence ingests Reports, Adversaries, and Indicators from Intel 471 into ThreatConnect. These Groups and Indicators are stored and associated in ThreatConnect with all their relevant context.

DEPENDENCIES

ThreatConnect Dependencies

- 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 on the** Account Settings **screen within their Private Instance of ThreatConnect.

Intel 471 Dependencies

- Active Intel 471 API key

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 Owner	*Required* – This parameter is the destination owner in which to write Groups and Indicators.
Intel 471 Username	*Required* – This parameter is the Intel 471 username.

Intel 471 API Key	*Required* – This parameter is the Intel 471 API key.
Last Run	*Required* – This parameter is the epoch timestamp of the last time the job was run to pull from Intel 471 into ThreatConnect. ***NOTE: The** Last Run **parameter should be edited only in two situations: when determining how far back to pull data during the initial run or when re-ingesting historic data during troubleshooting. In either of these situations, it is possible to use Epoch Time in Year/Month/Day format (YYYY-MM-DD) or Relative Time (e.g.,** 30 days ago**).***
Default Threat Rating	*Optional* – This parameter is the Threat Rating value to be applied to all imported Indicators. The default value is 3.
Default Confidence	*Optional* – This parameter is the default Confidence Rating value to be applied to all imported Indicators. The default value is 50.
Logging Level	*Optional* – This parameter is the logging level for the script. The default value is "info."