



# Intel 471 Malware Intelligence Integration Configuration Guide

**Software Version 1.0**

**November 4, 2020**

30071-01 EN Rev. A



©2020 ThreatConnect, Inc.

ThreatConnect® is a registered trademark of ThreatConnect, Inc.





# Table of Contents

---

OVERVIEW.....	4
DEPENDENCIES.....	4
ThreatConnect Dependencies.....	4
Intel 471 Dependencies.....	4
CONFIGURATION PARAMETERS .....	4
Parameter Definition.....	4





## OVERVIEW

The ThreatConnect® integration with Intel 471 Malware Intelligence ingests Reports, Threats, 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	<i>Required</i> - This parameter is the destination owner in which to write Groups and Indicators.
Intel 471 Username	<i>Required</i> - This parameter is the Intel 471 username.



Intel 471 API Key	<i>Required</i> - This parameter is the Intel 471 API key.
Last Run	<i>Required</i> - This parameter is the epoch timestamp of the last time the job was run to pull from Intel 471 into ThreatConnect.  <b><i>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).</i></b>
Default Threat Rating	<i>Optional</i> - This parameter is the Threat Rating value to be applied to all imported Indicators.
Logging Level	<i>Optional</i> - This parameter is the logging level for the script. The default value is "info."

