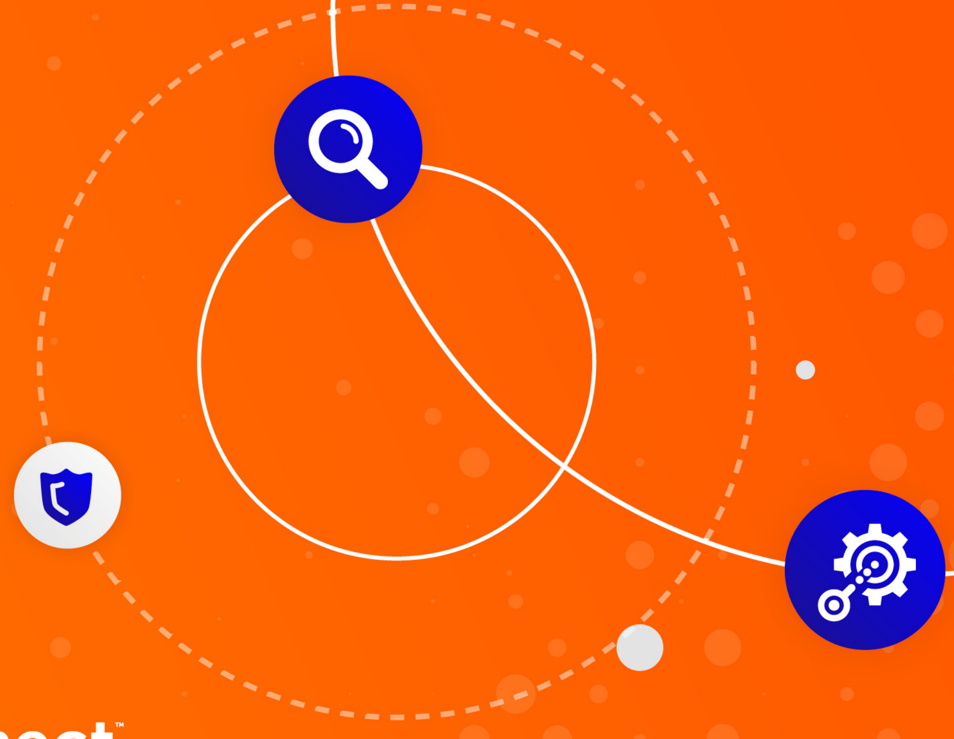

ThreatConnect™

# Accenture™ DeepSight™ Intelligence Integration

## Installation and Configuration Guide

**Software Version 1.0**

**June 1, 2020**

30033-02 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 Accenture's DeepSight Intelligence leverages the information provided by the DeepSight feed. The integration allows customers to seamlessly analyze and act on Accenture DeepSight Advanced IP and Advanced Domain/URL Datafeeds inside ThreatConnect.

# DEPENDENCIES

## ThreatConnect Dependencies

- Active ThreatConnect Application Programming Interface (API) User
- **attributes.csv** file for uploading into the target Organization (see the "Organization Configuration"  section later in this article for more details)

***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.***

# 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 Access ID | *Required* – This parameter is the ThreatConnect API Access ID. |
| ThreatConnect API Secret Key | *Required* – This parameter is the ThreatConnect API Secret Key created via the ThreatConnect Web UI. |
| ThreatConnect Default Org Name | *Required* – This parameter is the Organization name with which the incoming Indicators will be associated. |
| Accenture DeepSight User ID | *Required* – This parameter is the user ID used when connecting to Accenture. |
| Accenture DeepSight User PW | *Required* – This parameter is the password used when connecting to Accenture. |
| The default rating for an Indicator | This parameter is the default Threat Rating for an Indicator. It is used if a value is not contained in the feed. |
| The default confidence for an Indicator | This parameter is the default Confidence Rating for an Indicator. It is used if a value is not contained in the feed. |
| Sequence number of the IP file to pull | This parameter is the distinct sequence number of the file to be imported. A value of -1 will import the most recent file. The value of this parameter defaults to -1 on install. This value is used for those feeds that support IP data. |

| | |
|---|---|
| Sequence number of the URL file to pull | This parameter is the distinct sequence number of the file to be imported. A value of -1 will import the most recent file. The value of this parameter defaults to -1 on install. This value is used for those feeds that support URL data. |
| Use the proxy settings to connect to ThreatConnect (if available) | This parameter is a checkbox that should be enabled if ThreatConnect installations requires a proxy. |
| Feed | *Required* – This parameter is used to select one of the many feeds Accenture offers that will be ingested by this job. |
| Logging Level | This parameter is the logging level. The default value is "Info", but different logging levels can be selected. |

## Sequence-Number Configuration

As mentioned in the "CONFIGURATION PARAMETERS"  section, a user can specify the exact file being pulled into ThreatConnect by providing a sequence number. In most cases, the default value of -1 can be used. This value indicates that the latest file that Accenture has published for the specified feed should be retrieved. But if a specific historical file is desired, then a sequence number must be provided.

To understand how the sequence numbers work, it is necessary to understand how the Accenture feeds work. There are 12 feeds across the seven feed types (Attack, Bot, CnC, Fraud, Malware, Phishing, and Spam). Most types (for example, Attack) are pulling two feeds from Accenture: one for address (IP) data and one for host (URL) data. Two of the feeds (Bot and Spam) pull only IP data. Each separate IP or URL data file has a sequence number.

Accenture updates the feeds four times a day, or every 6 hours: at noon, midnight, 6 AM, and 6 PM GMT. When each feed is updated, the sequence number is increased by 1. To figure out a specific file sequence, start with the current sequence number and subtract 4 for each day back. For example, if today's sequence number is 2000, the sequence number from 8 days ago would be calculated as follows: 2000 – (8 * 4) = 1968.

The current sequence number for a particular feed is output in the feed for that log. An example of this part of a log is as follows:

```
INFO  16:51:02 com.threatconnect.app.symantecds.impl.SymantecDSSoapDataSource
- Sequence Number for file type: 44 is: 2690
```

Here, the sequence number is 2690, and the value of the file type is 44. These numbers are Accenture-specific values that can be looked up in the Accenture file-type lookup table, provided in Table 2.

Table 2

| File Type | Description |
|---|---|
| 26 | Advanced IP Reputation Attack XML |
| 29 | Advanced IP Reputation Bot XML |
| 32 | Advanced IP Reputation CnC XML |
| 35 | Advanced IP Reputation Fraud XML |
| 38 | Advanced IP Reputation Malware XML |
| 41 | Advanced IP Reputation Phishing XML |
| 44 | Advanced IP Reputation Spam XML |
| 47 | Advanced URL Reputation Attack XML |
| 50 | Advanced URL Reputation CnC XML |
| 53 | Advanced URL Reputation Fraud XML |
| 56 | Advanced URL Reputation Malware XML |
| 59 | Advanced URL Reputation Phishing XML |

As mentioned previously, most clients use the default value of -1, which will pull the latest file available. Because the files are updated every 6 hours, it is recommended that the job be scheduled to run every 6 hours.

Note that the files contain not just the last 6 hours of data, but actually the last 24 hours of data. In other words, each file contains a snapshot of the last 24 hours. As a result, data are duplicated between files. ThreatConnect handles this condition by updating any existing IP or URL file with the latest data.

## Organization Configuration

The target Organization within ThreatConnect must have the Attributes required by the Accenture feed imported. Otherwise, Indicators using unavailable Attributes will fail to load into the target Organization. These Attributes can be loaded by importing the **attributes.csv** file or by clicking the **Plus (+)** button when configuring the job within ThreatConnect. The following is a list of all required Attributes:

- Consecutive Listings
- Listing Ratio
- Reputation Rating
- Date First Seen
- Date Last Seen
- ASN
- Organization
- Organization Location
- Connection Details
- Attack Names
- Bot Names
- CNC Names
- Malware Names

# DATA MAPPING

## Advanced Domain/URL Reputation

Table 3

| Key | ThreatConnect Mapping |
|---|---|
| domain: name | indicator: name |
| domain: hostility | indicator: rating |
| domain: confidence | indicator: confidence |
| domain: consecutive_listings | indicator: attribute: “Consecutive Listings” |
| domain: listing_ratio | indicator: attribute: “Listing Ratio” |
| domain: reputation_rating | indicator: attribute: “Reputation Rating” |
| domain: first_seen | indicator: attribute: “Date First Seen” |
| domain: last_seen | indicator: attribute: “Date Last Seen” |
| domain: registration | indicator: attribute: “Domain Registration Details” |
| domain: attack_names: attack_name | indicator: attribute: “Attack Names” |
| domain: bot_names: bot_name | indicator: attribute: “Bot Names” |
| domain: cnc_names: cnc_name | indicator: attribute: “CNC Names” |
| domain: malware_names: malware_name | indicator: attribute: “Malware Names” |

## Advanced IP Reputation

Table 4

| Key | ThreatConnect Mapping |
|---|---|
| ipAddress: address | indicator: name |
| ipAddress: consecutive_listings | indicator: attribute: “Consecutive Listings” |
| ipAddress: listing_ratio | indicator: attribute: “Listing Ratio” |
| ipAddress: reputation_rating | indicator: attribute: “Reputation Rating” |
| ipAddress: hostility | indicator: rating |
| ipAddress: confidence | indicator: attribute: confidence |
| ipAddress: first_seen | indicator: attribute: “Date First Seen” |
| ipAddress: last_seen | indicator: attribute: “Date Last Seen” |
| ipAddress: asn | indicator: attribute: “ASN” |
| ipAddress: organization | indicator: attribute: “Organization” |
| ipAddress: location | indicator: attribute: “Organization Location” |
| ipAddress: connection | indicator: attribute: “Connection Details” |
| ipAddress: attack_names: attack_name | indicator: attribute: “Attack Names” |
| ipAddress: bot_names: bot_name | indicator: attribute: “Bot Names” |

| | |
|---|---|
| ipAddress: cnc_names: cnc_name | indicator: attribute: “CNC Names” |
| ipAddress: malware_names: malware_name | indicator: attribute: “Malware Names” |