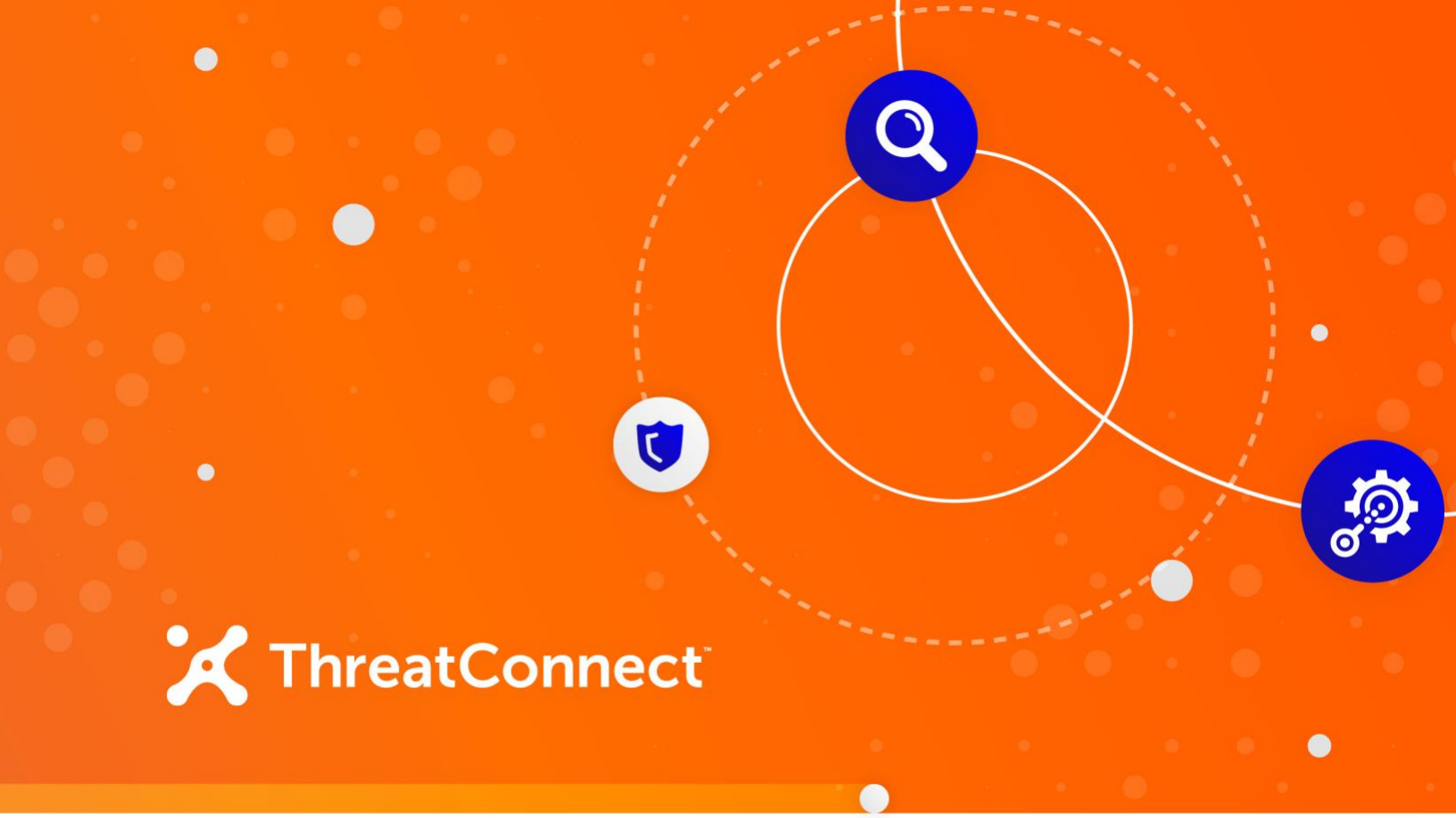

Micro Focus® ArcSight ESM - API Integration

Installation and Configuration Guide

May 10, 2021

30048-05 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 package for Micro Focus® ArcSight Enterprise Security Management (ESM) - Application Programming Interface (API) allows ArcSight ESM users to interact with threat intelligence in ThreatConnect directly from the ArcSight Console. The integration has three main components: an automated ThreatConnect Job App to add and remove Indicators between ThreatConnect and the ArcSight Active Lists, ThreatConnect Playbook-based applications to add and remove Indicators from ArcSight Active Lists, and a set of ArcSight integration commands that allow the user to interact with ThreatConnect within the ArcSight Console application (e.g., retrieve Indicator details, report observations and false positives to ThreatConnect).

This version of the integration uses the ArcSight REST API to add Indicators from ThreatConnect to ArcSight ESM as well as to remove them. If you prefer to deploy Indicators via common event format (CEF)-formatted syslog, please use the CEF integration for Micro Focus ArcSight ESM.

DEPENDENCIES

ThreatConnect Job App

- ThreatConnect Environment Server, if applicable
- ThreatConnect Job App: **Micro Focus ArcSight ESM - API**
- ArcSight Console
- ArcSight version that supports REST API v1
- ThreatConnect version 6.0 or newer

ThreatConnect Playbook Apps

- ThreatConnect Playbooks functionality enabled
- ThreatConnect Environment Server, if applicable
- ThreatConnect Playbook App: **Micro Focus ArcSight ESM - API**
- ThreatConnect installation zip file: **ThreatConnect-ArcSight-Package_v2.0.zip**
- ArcSight Console
- ArcSight version that supports REST API v1
- ThreatConnect version 6.0 or newer

ThreatConnect ArcSight Integration Commands

- Active ThreatConnect Application Programming Interface (API) user
- Active ThreatConnect API key
- FlexConnector CounterACT
- ThreatConnect installation zip file: **ThreatConnect-ArcSight-Package_v2.0.zip**
- ArcSight Console
- Java 1.8

ThreatConnect ArcSight Monitor Package

- ThreatConnect installation zip file: **ThreatConnect-ArcSight-Package_v2.0.zip**
- ArcSight Console
- ArcSight 6.8/6.11

NOTE: Users running on a Dedicated Cloud instance of ThreatConnect should have the ThreatConnect Environment Server installed in order to use the ArcSight Integration Package. The Environment Server allows an organization to execute jobs using ThreatConnect integration applications available from TC Exchange™ via a user interface. For example, if data need to be pushed to a device such as a SIEM-, firewall-, or host-based system, the Environment Server runs as an intermediary between the external ThreatConnect instance and the user's internal network.

INSTALLATION

ThreatConnect-to-ArcSight Indicator Upload

ThreatConnect Automated Job Installation

Follow standard ThreatConnect procedures for setting up and configuring the automated ThreatConnect Job. The name of the application is **TC_-_ArcSight_Integration**. See *Creating Jobs Using TC Exchange Apps* for more information.

ThreatConnect Active List ARB Package

Importing the associated ThreatConnect Active List ARB package into ArcSight creates the ThreatConnect Active Lists that will contain the Indicators from the automated ThreatConnect Job.

Follow these steps to import the ThreatConnect Active List ARB package:

1. The ThreatConnect installation zip file contains a directory named **ArcSightFiles** that contains ArcSight ARB files. Extract the file named **ThreatConnect_ActiveLists.arb**, and place it on a desktop where the ArcSight Console application is running.
2. Open the ArcSight Console application.
3. In the **Navigator** panel, select the **Packages** tab and then click the **Import** button.
4. Browse to the **.arb** file downloaded in Step 1 and click **Open**.
5. After the package is imported, click **Install**.
6. Once the installation is complete, click **OK**. ThreatConnect ARB files are configured to have their contents imported into a ThreatConnect group within the public group in ArcSight. The package and Active List results should look like the examples in Figure 1 and Figure 2, respectively.

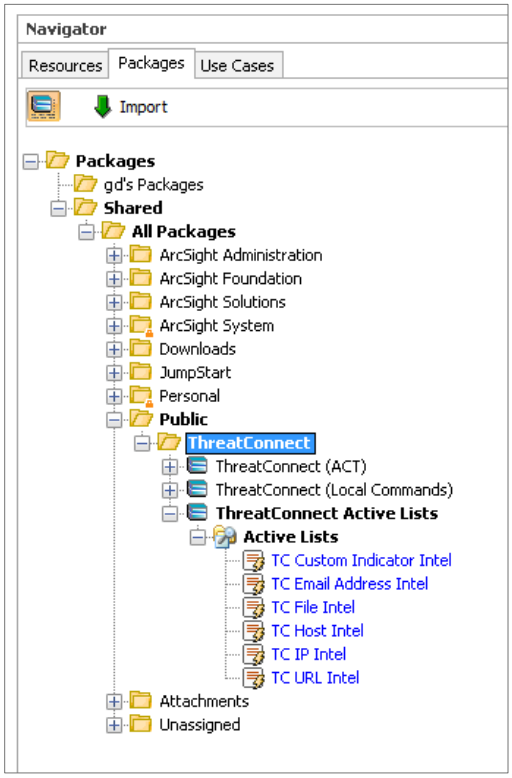

Figure 1

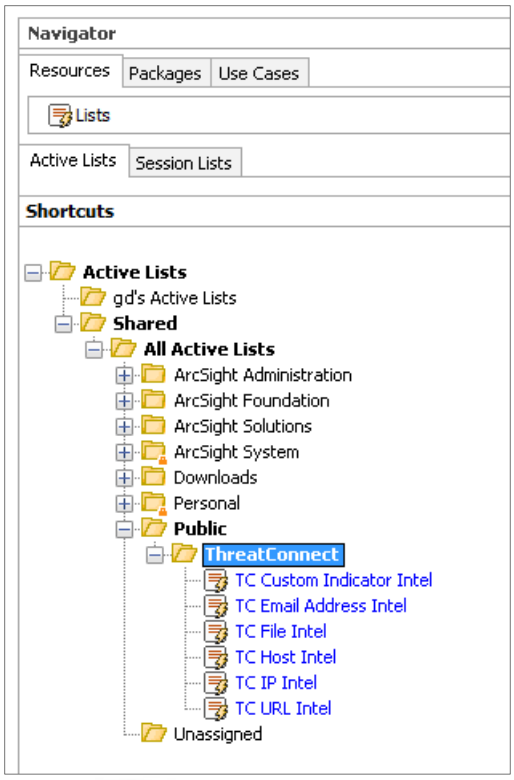

Figure 2

ThreatConnect Playbook Configuration

The ThreatConnect ArcSight Playbook applications are installed, configured, and run in the same manner as all Playbook applications. See the "Apps and Jobs" section of the *ThreatConnect System Administration Guide* and *Playbooks* for more information.

There are two ArcSight Playbook applications: **Deploy to ArcSight**, which adds a new Indicator to ArcSight, and **Remove from ArcSight**, which removes an Indicator from ArcSight. For example, the Playbook in Figure 3 uses a UserAction Trigger to send an Indicator to ArcSight.

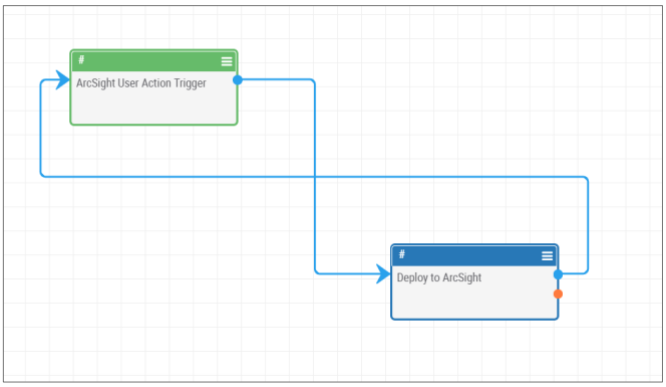

Figure 3

Integration Commands: ArcSight-to-ThreatConnect Indicator Upload and Enrichment

ArcSight integration commands perform a number of functions, including creating Indicators in ThreatConnect, retrieving more information about an Indicator, and reporting an observation.

There are two possible configuration options when using the ThreatConnect integration from within the ArcSight Console. The first option is to install an Action Connector (an instance of an ArcSight SmartConnector) on an ArcSight server, which allows the integration commands to run remotely and be centrally managed. The second option is to install the integration scripts on each workstation that runs the ArcSight Console.

If running the commands remotely, follow the steps in the next section. Otherwise, skip to the "Running Integration Commands Locally" section.

Running Integration Commands Remotely

ArcSight has various connectors that are installed separately from the base product and add functionality. Some connectors receive Indicators via the CEF format using SysLog as the transport mechanism. Others connect to a database to import Indicators.

To run ThreatConnect integration commands remotely, the ArcSight FlexConnector CounterACT connector must be installed. This installation follows the standard ArcSight installation procedures. Please refer to Chapter 2, "Installing the FlexCounter ACT Connector," of the *ArcSight Action Center documentation* for details.

NOTE: The directory where the ArcSight Connectors will be installed should be of the form** /opt/arcsight/connectors**. Within that directory, create a directory named** threatconnect**. This directory is where the ArcSight Connector and, later, ThreatConnect-specific code will be installed.

NOTE: When prompted for the configuration file name, use the name** threatconnect.counteract.properties**. The next section covers the installation and configuration of this file.

ThreatConnect ArcSight Connector Configuration

The configuration file **threatconnect.counteract.properties** is used to tell the connector what remote commands are available. An example template file is included in the ThreatConnect installation zip file within the **threatconnect** directory.

Follow these steps to install the configuration file:

1. Extract the **threatconnect.counteract.properties-template** file from the ThreatConnect installation zip file.
2. Rename the file to **threatconnect.counteract.properties**.
3. Move the file to the ArcSight server where the connector is installed. Depending on the name of the directory created during the installation of the FlexConnector CounterACT connector, the directory to move the file into will look something like **/opt/arcsight/connectors/threatconnect/current/user/agent/flexagent/**.
4. Restart the connector for the changes to take effect.

ThreatConnect Integration Command Code and Configuration

The ThreatConnect integration command code consists of two parts: a configuration file and the Java **.jar** file. Both exist within the ThreatConnect installation zip file.

Follow these steps to install and configure the command code:

1. Extract the file **tc.conf-template** from the installation zip file.
2. Rename the file to **tc.conf**.
3. Edit the file to provide parameter values. The following values are required:
   a. **api_access_id:** The ThreatConnect API access ID.
   b. **api_secret_key:** The ThreatConnect API secret key.
   c. **api_base_url:** The ThreatConnect base URL. This URL will include **http** or **https** (e.g., **https://my.threatconnect.com/api**).
   d. **Owner**: The name of the owner in ThreatConnect to be used for the integration commands.
   e. **playbook_key:** If using Playbooks and an HttpLink Trigger Playbook, this parameter is the ThreatConnect Trigger token or key that is displayed within active Playbooks. For example, if the HttpLink Trigger is **https://<TCInstance>/api/playbook/f3e58bce-**

7036-43da-a68e-e0e8a0569a9c, then the key is **f3e58bce-7036-43da-a68e-e0e8a0569a9c**.

4. Extract the **ThreatConnect-jar-with-dependencies.jar** file from the installation zip file.
5. Based on the directory created during the installation of the FlexConnector CounterACT connector, the directory where the ArcSight Connector is installed will look something like **/opt/arcsight/connectors/threatconnect/current/.** Create a directory named **threatconnect-arcsight** to contain the ThreatConnect code. The full path for the file will be similar to **/opt/arcsight/connectors/threatconnect/current/threatconnect-arcsight.**
6. Move the modified **tc.conf** file and**. ThreatConnect-jar-with-dependencies.jar** file into the directory created in the previous step.
7. Restart the connector for the changes to take effect.

ThreatConnect Integration Commands ARB Package

Follow these steps to install the ThreatConnect integration commands into the ArcSight Console:

1. Extract the **ThreatConnect_(ACT).arb** file from the ThreatConnect installation zip file. This file is within the **ThreatConnect/ArcSightFiles** directory.
2. Open the ArcSight Console, and import the **.arb** file downloaded in the previous step. ArcSight ARB files are configured to have their contents imported into a ThreatConnect group within the public group in ArcSight. The package and integration commands results should look like the examples in Figure 4 and Figure 5, respectively.

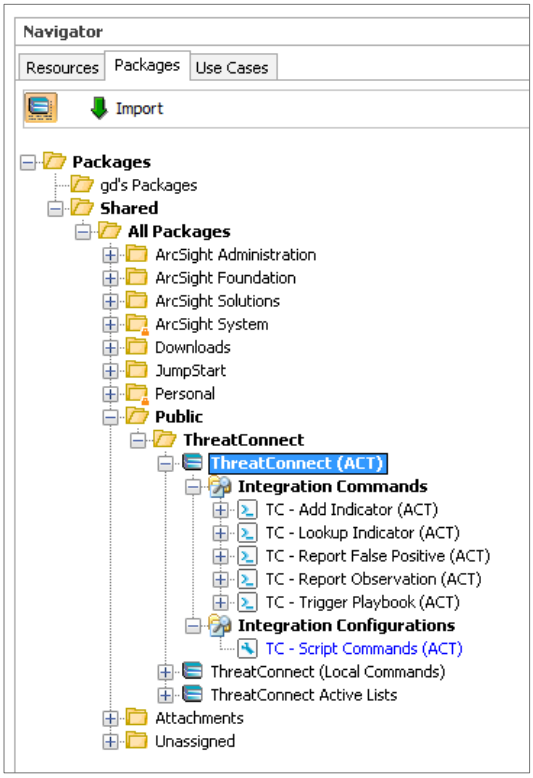

Figure 4

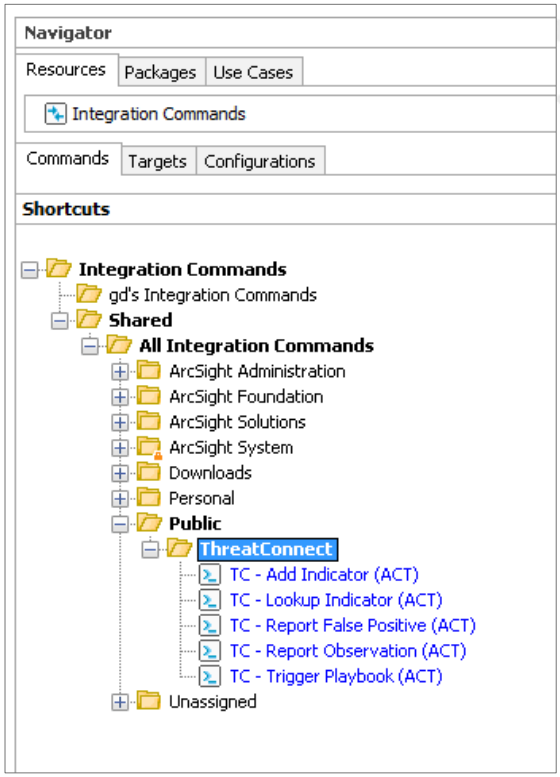

Figure 5

3. To run a command, open any view within the Console that shows Indicator data, right-click the cell with those data, and select **Integration Commands > TC - Script Commands (ACT).** The **TC – Script Commands (ACT)** window will be displayed (Figure 6). Select the desired command options, and click **OK.**

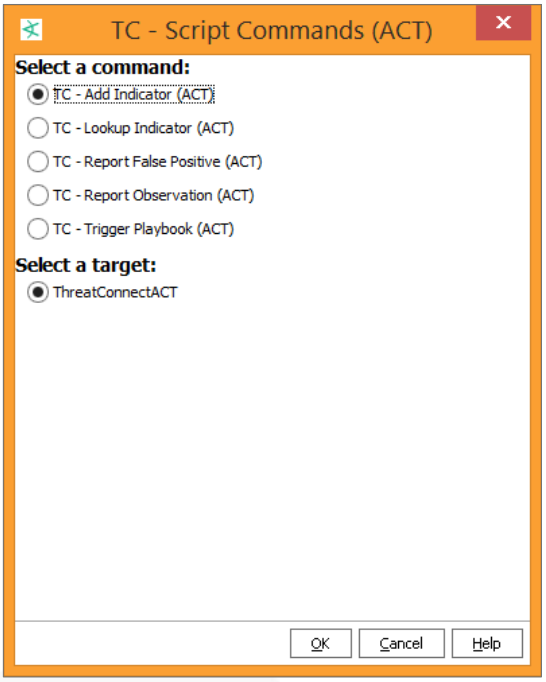

Figure 6

Running Integration Commands Locally

For ease of installation, ThreatConnect integration commands may be run locally. This method does not require a new ArcSight Connector to be installed and configured. The code is local to each user's workstation that runs the ArcSight Console.

ThreatConnect Integration Command Code and Configuration

The code consists of two parts: a configuration file and the Java **.jar** file. Both exist within the ThreatConnect installation zip file.

Follow these steps to install and configure the command code:

1. Extract the **tc.conf-template** file from the installation zip file.
2. Rename the file to **tc.conf**.
3. Edit the file to provide parameter values. The following values are required:
   a. **api_access_id**: The ThreatConnect API access ID.
   b. **api_secret_key:** The ThreatConnect API secret key.
   c. **api_base_url:** The ThreatConnect base URL. This URL will include **http://** or **https://** (e.g., https://my.threatconnect.com/api).
   d. **Owner:** The name of the owner in ThreatConnect to be used for the integration commands.
   e. **playbook_key:** If using Playbooks and the Playbooks integration command, this parameter is the ThreatConnect Trigger token or key that is displayed within active Playbooks.
4. On the workstation, create a local directory off the root called **threatconnect.** This directory is referenced in the commands, so the syntax must match exactly. An example on a Windows box would be **C:\threatconnect.** A Linux-based OS would use **\threatconnect.**
5. Extract the **ThreatConnect-jar-with-dependencies.jar** file from the installation zip file.
6. Move the modified **tc.conf** file and the **ThreatConnect-jar-with-dependencies.jar** file into the directory created in the previous step.

ThreatConnect Integration Commands ARB Package

Follow these steps to import the ThreatConnect integration commands into the ArcSight Console:

1. Extract the **ThreatConnect_(Local_Commands).arb** file from the ThreatConnect installation zip file. This file is found within the **ThreatConnect/ArcSightFiles** directory.
2. Open the ArcSight Console and import the **.arb** file downloaded in the previous step. ArcSight ARB files are configured to have their contents imported into a ThreatConnect group within the public group in ArcSight. The package and integration commands results should look like the examples in Figure 7 and Figure 8, respectively.

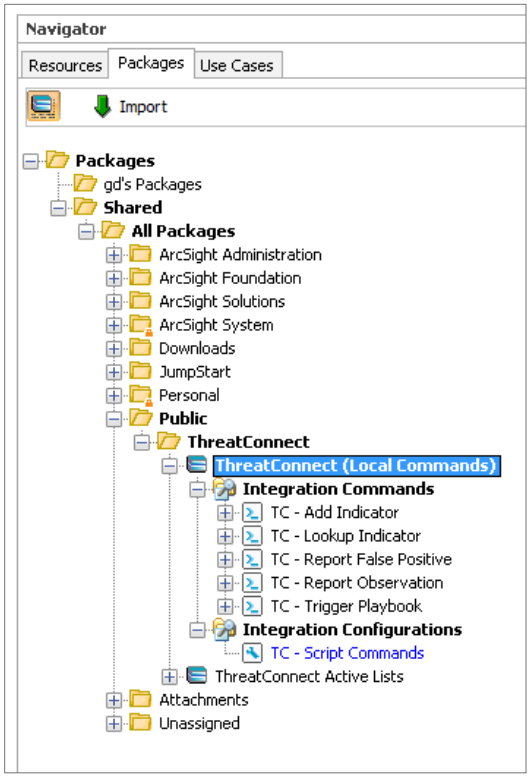

Figure 7

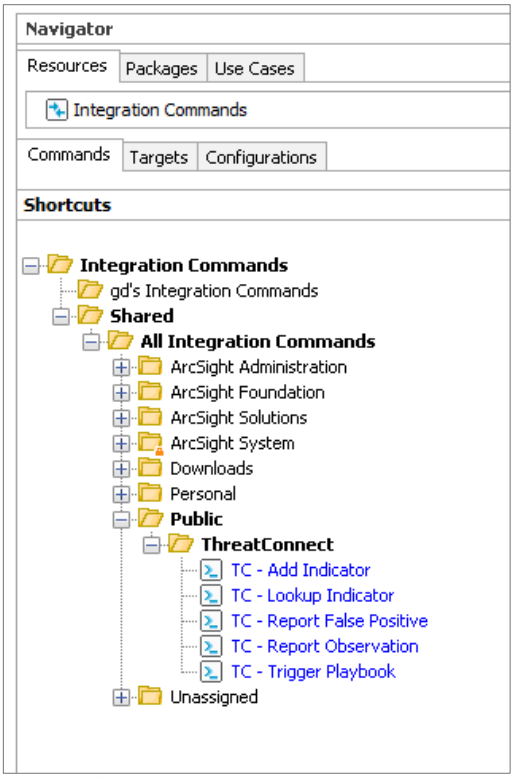

Figure 8

3. When running one of the integration commands, the **Parameters** window may be displayed (Figure 9). Providing the parameters in this window is optional if they are defined within the **tc.conf** file mentioned in the "ThreatConnect Integration Command Code and Configuration" section.

   If the parameters are specified in the **Parameters** window, the values entered will override the values in the **tc.conf** file. Selecting the checkbox in the **Save to User** column will cause the value to be stored within the ArcSight User Configuration, and the value will not be asked for again until it is deleted within the ArcSight User Configuration. These options allow multiple ways to configure and use the local ThreatConnect integration commands.

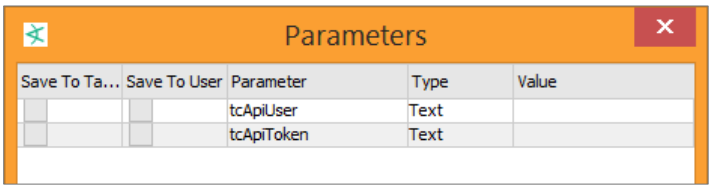

Figure 9

ThreatConnect ArcSight Monitor Package

ThreatConnect provides a Monitor Package that includes dashboards, data monitors, reports, and rules for use within the ArcSight Console. These features can be used "out of the box" or built upon for customer-specific requirements.

The Monitor Package depends on the ThreatConnect Active List ARB Package already installed. Refer to the "ThreatConnect Active List ARB Package" section for installation steps.

Follow these steps to import the ThreatConnect ArcSight Monitor Package:

1. The ThreatConnect installation zip file contains a directory named **ArcSightFiles** that contains ArcSight ARB files. Extract the **ThreatConnect_Monitoring.arb** file, and place it on a desktop where the ArcSight Console application is running.
2. Open the ArcSight Console.
3. In the **Navigator** panel, select the **Packages** tab, and then click the **Import** button.
4. Browse to the **.arb** file downloaded in Step 1 and click **Open**.
5. After the package is imported, click **Install**.
6. When the installation completes, click **OK**.

ThreatConnect ARB files are configured to have their contents imported into a ThreatConnect group within the public group in ArcSight. The Monitor Package should look like the example in Figure 10.

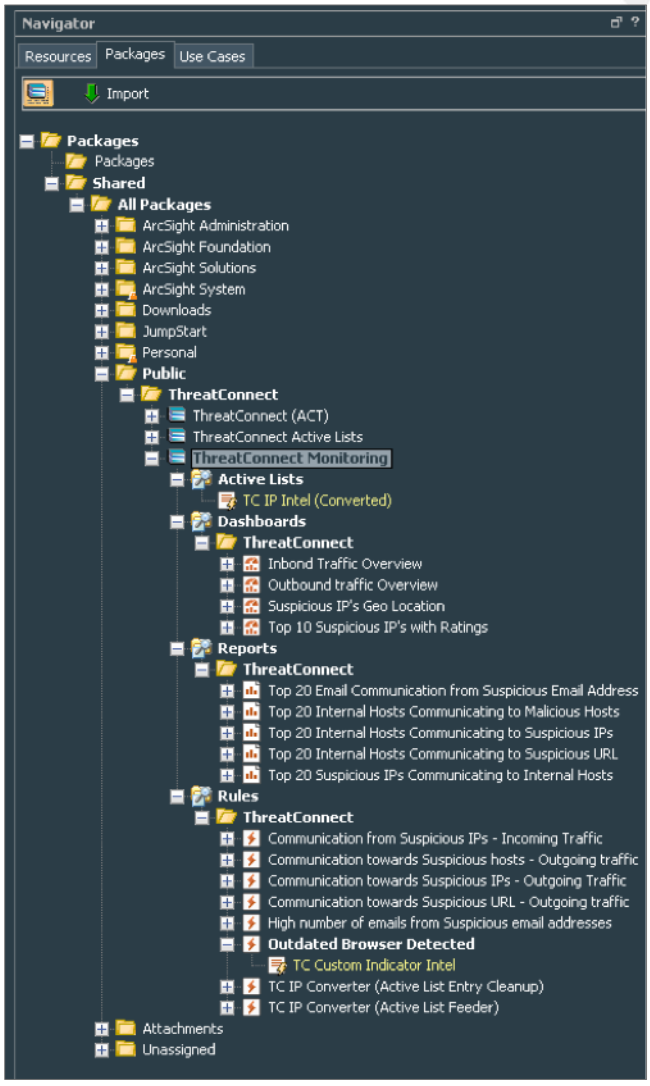

Figure 10

Dashboards can be used for real-time monitoring of events, while reports can be used for timeframe snapshots of events. Rules serve as examples that can be used in notification alerts. Knowledge of ArcSight is required in order to modify these objects.

Some highlights of items included in the package are as follows:

Rules

- **Communication towards Suspicious IPs - Outgoing Traffic**: This rule will trigger when any internal IP address is trying to communicate with a malicious IP address present in the TC Suspicious IP Active List.
- **Communication towards Suspicious URL - Outgoing Traffic**: This rule will trigger when any internal hosts are trying to communicate with malicious URLs present in the TC URL Intel Active List.

- **High number of emails from Suspicious email addresses**: This rule will trigger when any email is observed from a suspicious email address listed in the TC Email Intel Active List.
- **Communication from Suspicious IPs - Incoming Traffic**: This rule will trigger when any malicious IP address present in the Suspicious IP Active List is trying to communicate with internal IP addresses.
- **Communication towards Suspicious Hosts - Outgoing Traffic**: This rule will trigger when any internal hosts are trying to communicate with malicious hosts present in the TC Host Intel Active List.

Data Monitors and Dashboards

- **Email from Suspicious Email Address**: This Data Monitor will reflect the top communication from a suspicious email address.
- **Inbound Suspicious Traffic**: This Data Monitor will reflect the top communication from a suspicious IP address that is present in the TC Suspicious IP Active List.
- **Outbound Suspicious Traffic**: This Data Monitor will reflect the top internal IP address trying to communicate with a suspicious IP address present in the TC Suspicious IP Active List.
- **Top Users Sending Emails to Suspicious Email Address**: This Data Monitor will reflect the top malicious email addresses to which internal users are trying to send emails.
- **Traffic to Suspicious Host**: This Data Monitor will reflect the top malicious hosts to which internal hosts are sending requests.
- **Traffic to Suspicious URL**: This Data Monitor will reflect the top malicious URLs to which internal hosts are sending requests.
- **Top 10 Suspicious IPs with Ratings**: This Data Monitor will reflect the top malicious IP addresses with their respective Threat Ratings and Confidence Ratings.
- **Suspicious IPs Geo Location**: This Data Monitor will reflect the geolocation data of the malicious IP addresses that are trying to communicate with internal IP addresses.

Reports

The following is a list of reports containing the “Top 20” traffic details from all of the ThreatConnect feeds lists:

- Top 20 Email Communication from Suspicious Email Address
- Top 20 Internal Hosts Communicating to Malicious Hosts
- Top 20 Internal Hosts Communicating to Suspicious IPs
- Top 20 Internal Hosts Communicating to Suspicious URL
- Top 20 Suspicious IPs Communicating to Internal Hosts

UPGRADE PROCESS WHEN ACTIVE LISTS CHANGE

When updates to the ThreatConnect integration for ArcSight change the Active Lists within ArcSight (e.g., by adding columns), existing data will not automatically be upgraded to include the changes, because there is no ability to update existing Active Lists in ArcSight. There are two ways in which to address this issue.

First, if the existing data do not need to be saved, uninstall and remove the current ThreatConnect ArcSight packages, and then install the updated packages, which are included with the release for the integration update. This method is the simplest way to update the structure of the Active Lists, but it is essentially starting over, and existing data will not persist.

If the existing data must be retained, then the following procedure should be used:

1. For each Active List whose data are to be preserved, export the data as a CSV file:
   a. Create a Query (tab within the Reports Resource) that pulls all the desired data from the Active List.
   b. Create a Report that uses the Query. The format should be **csv** so that the data will be saved to a file when the Report is executed.
   c. Confirm that the output file contains the data to be retained.
2. Uninstall and remove the current ThreatConnect ArcSight packages.
3. Install the updated ThreatConnect ArcSight packages.
4. Import the CSV files into the appropriate lists:
   a. Right-click the list within the console and select **Import CSV File...**.
   b. Select the Active List into which it is to be imported.
   c. Confirm that the data are correct in the preview window. New columns that were added to Active Lists with the update should be empty for existing data.