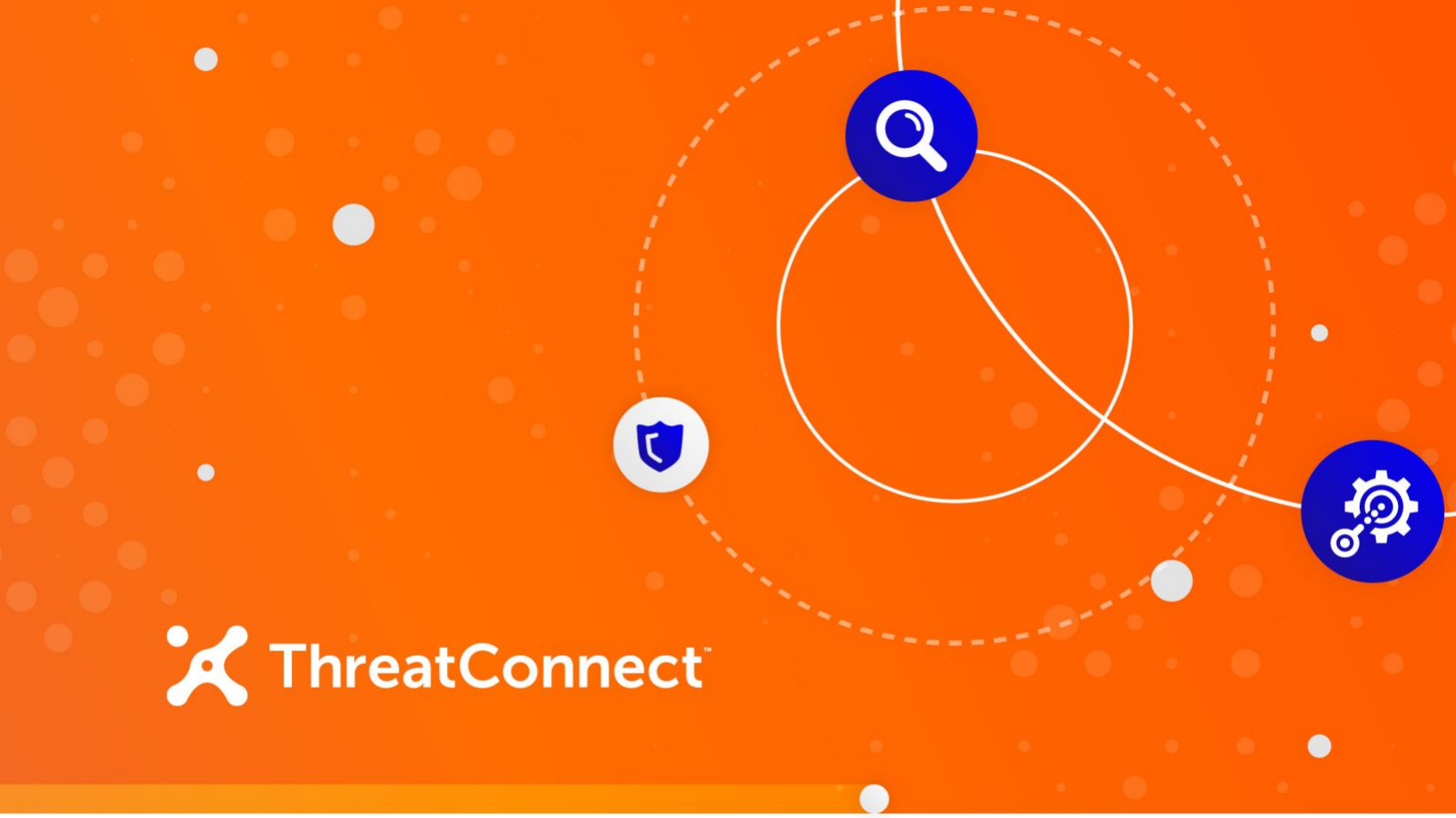

Micro Focus® ArcSight ESM - CEF Integration

Installation and Configuration Guide

May 10, 2021

30005-04 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) - Common Event Format (CEF) allows ArcSight ESM users to interact with threat intelligence in ThreatConnect directly from the ArcSight Console. This 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 Indicators to and remove them from ArcSight Active Lists, and a set of ArcSight integration commands that allow users to interact with ThreatConnect using the ArcSight Console application (e.g., retrieve Indicator details, report observations and false positives to ThreatConnect).

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

DEPENDENCIES

ThreatConnect Dependencies

ThreatConnect Job App

- ThreatConnect Environment Server, if applicable
- ThreatConnect Job App: **Micro Focus ArcSight ESM - CEF**
- ThreatConnect installation zip file: **ThreatConnect-ArcSight-Package_v1.0.zip**
- ArcSight Console
- ThreatConnect version 6.0 or newer

ThreatConnect Playbook App

- ThreatConnect Playbooks functionality enabled
- ThreatConnect Environment Server, if applicable
- ThreatConnect Playbook App: **Micro Focus ArcSight ESM - CEF**
- ThreatConnect installation zip file: **ThreatConnect-ArcSight-Package_v1.0.zip**
- ArcSight Console
- ThreatConnect version 6.0 or newer

NOTE: Users running on a Dedicated 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 utilize a user interface (UI) to execute jobs using ThreatConnect integration applications available from TC Exchange™. 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.

CONFIGURATION PARAMETERS

Parameter Definition

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

Table 1

Name	Description	Required
Syslog Server Hostname or IP	This parameter is the syslog server hostname or IP address.	True
Syslog Server Port	This parameter is the syslog server port.	True
Syslog Server Protocol	This parameter is the protocol used to communicate with the syslog server ("UDP" or "TCP").	True
Syslog Facility	This parameter is the syslog facility (LOCAL_0 to LOCAL_7).	True
Owners	This parameter is a list of Organizations, Communities, and Sources to be exported.	True
Indicator Types	This parameter is a list of Indicators to be exported.	True
Minimum Confidence	This parameter exports an Indicator when its Confidence	False

	Rating is greater than or equal to the specified value.	
Minimum Rating	This parameter exports an Indicator when its Threat Rating is greater than or equal to the specified value.	False
Minimum ThreatAssess Score	This parameter exports an Indicator when its ThreatAsses Score is greater than or equal to the specified value.	False
Minimum False Positive Count	This parameter exports an Indicator when its False Positive count is greater than or equal to the specified value.	False
Export Indicators with Tag	This parameter exports Indicators that have the specified Tag applied to them.	False
CSV string containing key pair mapping as “ownerName:deviceCustomString2”	This parameter is a comma-delimited key-pair mapping.	True
Send delete lines	This parameter sends records as **DELETE** if any exist.	False
Remove https:// or http:// from TC weblink	This parameter removes URL protocols from ThreatConnect weblinks.	False
Modified Since	This parameter returns Indicators that were modified since the specified date.	False
Logging Level	This parameter is the logging level to use for the job.	False

Indicators are selected based on a time range and converted to CEF using fields that ArcSight ESM is able to ingest. The CEF header is made up of eight sections that are pipe delimited and then prepended by a timestamp when pushed to the syslogger. The following is an example:

```
CEF Header: Fields:
CEF:Version |Device Vendor |Device Product |DeviceVersion  |Signature ID
|Name |Severity  |[Extension]

ThreatConnect Values:
CEF:0 |threatconnect |threatconnect |3 |DB ID #  |Owner |Skull Rating x 2
|Key Pair Values using above mappings
```

The final field ([Extension]) is where the values pulled from ThreatConnect via the API (e.g., confidence:50) are written. The renaming occurs at this point so that the data are not dropped at the ArcSight ESM connector. Data are sent in User Datagram Protocol (UDP) format, and the connector type in ArcSight ESM is the syslog SmartConnector. The connector is very explicit when checking for types on incoming data—an example of which is the Confidence value. When populated, it returns an integer value of between 0 and 100. The Custom Number attribute (cn1) is not used for this value because it holds a "long" rather than an integer, and the connector drops the data. When mapped into an unused value that is an integer (deviceProcessId (dvcpid)), the value is able to pass through the connector. The names of fields are remapped when written into an Active List. Table 2 displays the current listing of ThreatConnect's name mappings.

Table 2

ThreatConnect	ArcSight ESM Key	ArcSight ESM Name	Data Type
confidence	dvcpid	deviceProcessId	integer
dateAdded	deviceCustomDate1	deviceCustomDate1	date
owner	remapped to name field in header*	name	string
hostname	cs5	deviceCustomString5	string
ip	cs5	deviceCustomString5	address
lastModified	deviceCustomDate2	deviceCustomDate2	date

ownerName	cs2	deviceCustomString2	string
type	cat	deviceEventCategory	string
weblink	cs4	deviceCustomString4	string
text	cs5	deviceCustomString5	string
sha256	fileHash	fileHash	string
sha1	oldFileHash	oldFileHash	string
md5	cs5	deviceCustomString5	string
size	fsize	fileSize	integer
source	cs6	deviceCustomString6	string
address	cs5	deviceCustomString5	string
id	spid	sourceProcessId	integer
summary	cs3	deviceCustomString3	string
threatAssessRating	cfp1	deviceCustomFloating Point1	floating point
threatAssessConfidence	cfp2	deviceCustomFloating Point2	floating point

** For more information about CEF mappings, see the following link: https://community.softwaregrp.com/t5/ArcSight-Connectors/ArcSight-Common-Event-Format-CEF-Implementation-Standard/ta-p/1645557.*

USING AN ARB FILE TO LOAD ARCSIGHT CONTENT

A ThreatConnect-provided ARB file can be used to install the default rules, filters, channels, lists, and field sets necessary for the ThreatConnect ArcSight ESM - CEF integration.

1. Once the ARB file is received, open the ArcSight ESM console, select the **Packages** tab under the **Navigator** bar, and click the **Import** button (Figure 1).

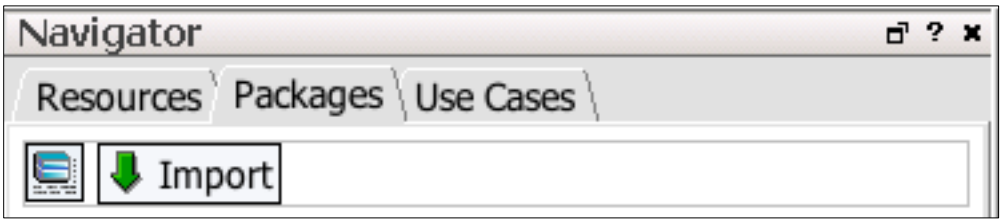

Figure 1

2. A file selection dialog box will be displayed. Locate and select the **.arb** file for import, and then click the **Open** button (Figure 2).

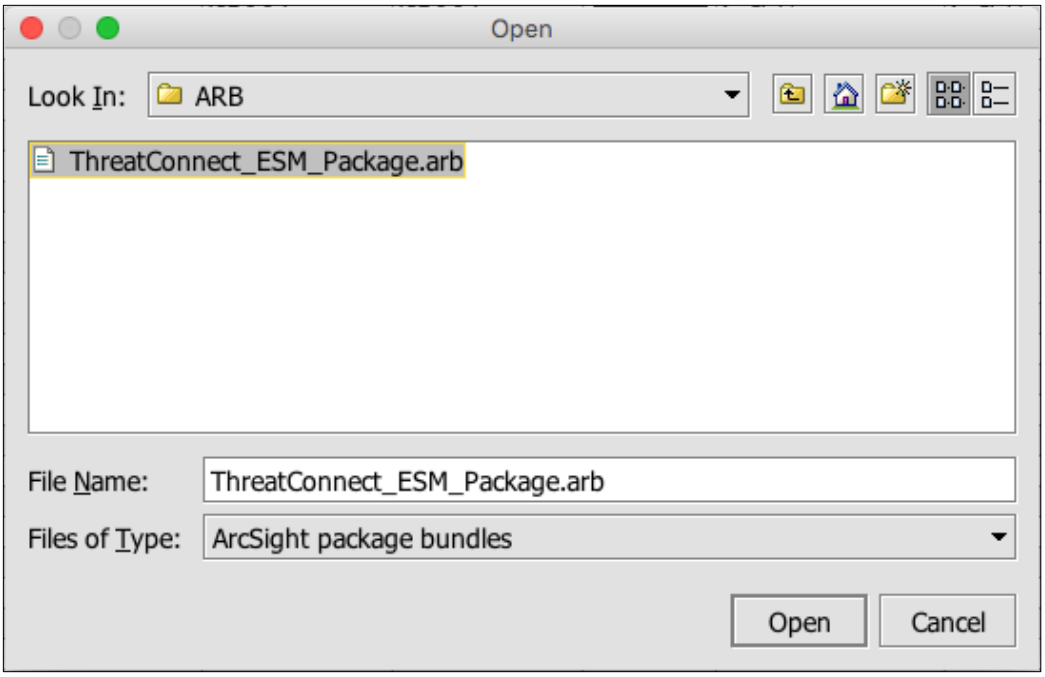

Figure 2

3. A new dialog box will be displayed in which the package to be installed can be selected. Verify that the **Install** checkbox is selected, and then click the **Next** button (Figure 3).

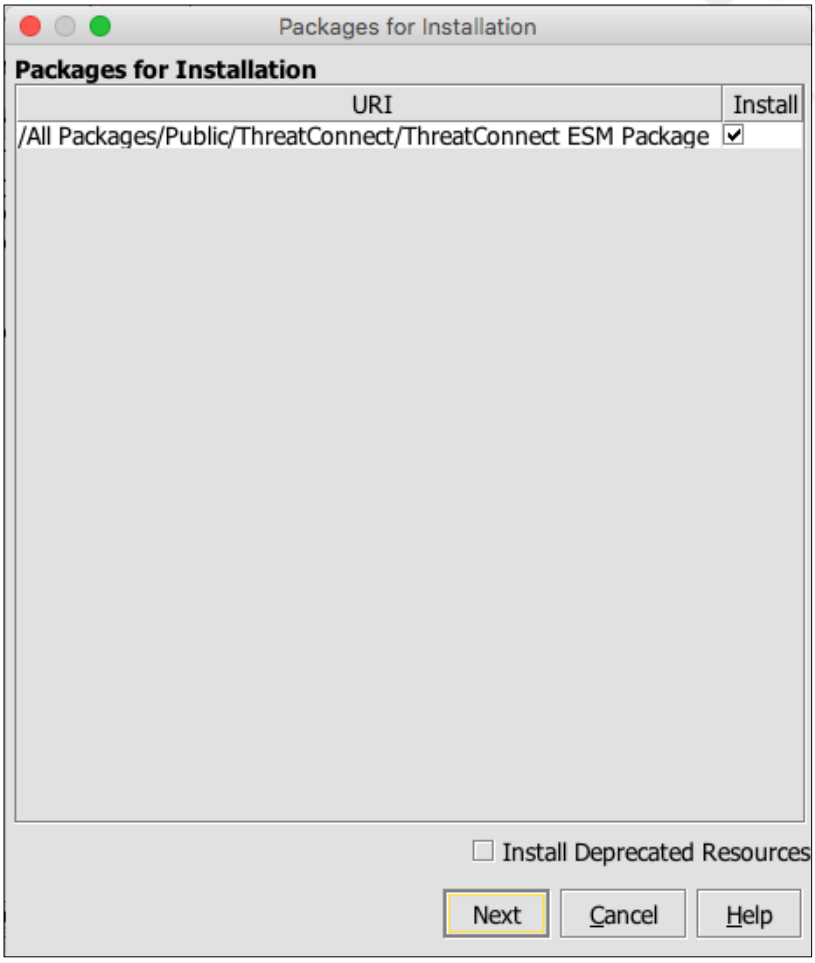

Figure 3

4. A dialog box with the results of the installation will be displayed (Figure 4). Click the **OK** button to continue.

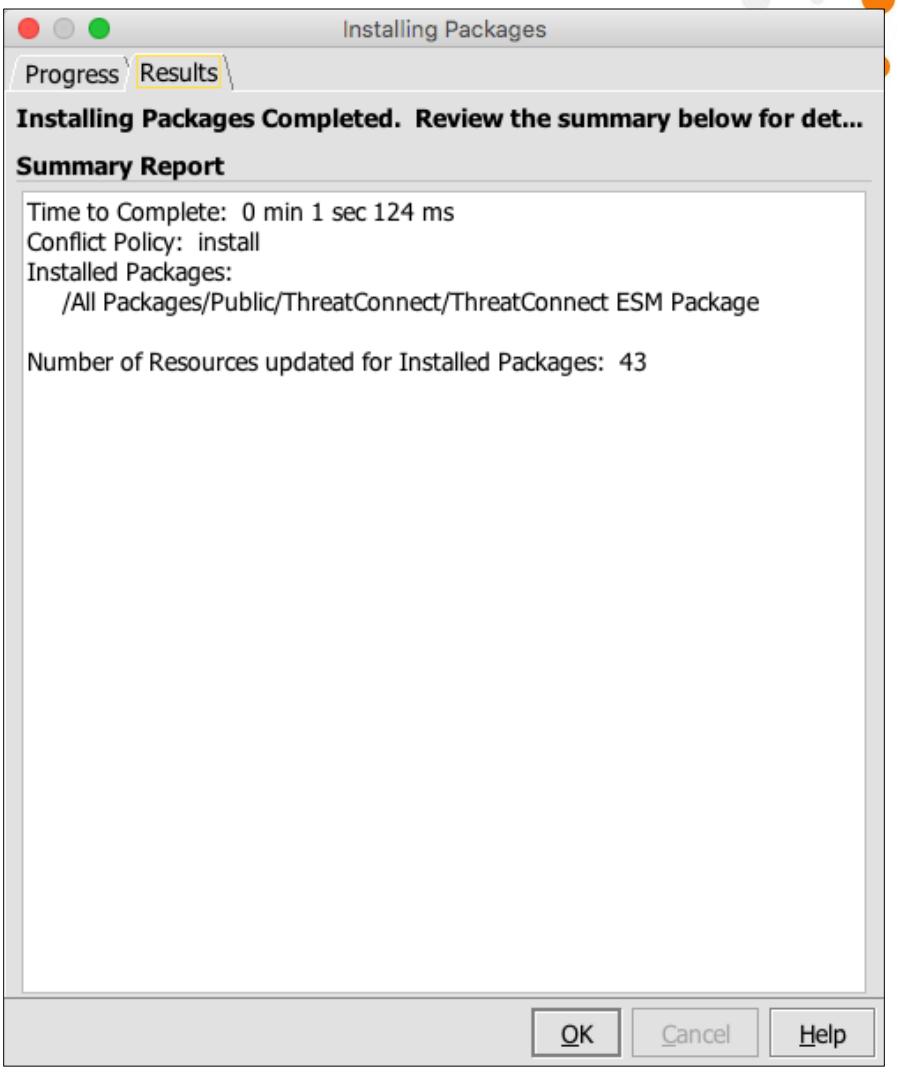

Figure 4

5. After installation, the package can be viewed from the **Packages** tab under **Packages > Shared > All Packages > Public >ThreatConnect**. Each type of object is available under the associated object type in the newly created directory **../Public/ThreatConnect** (Figure 5).

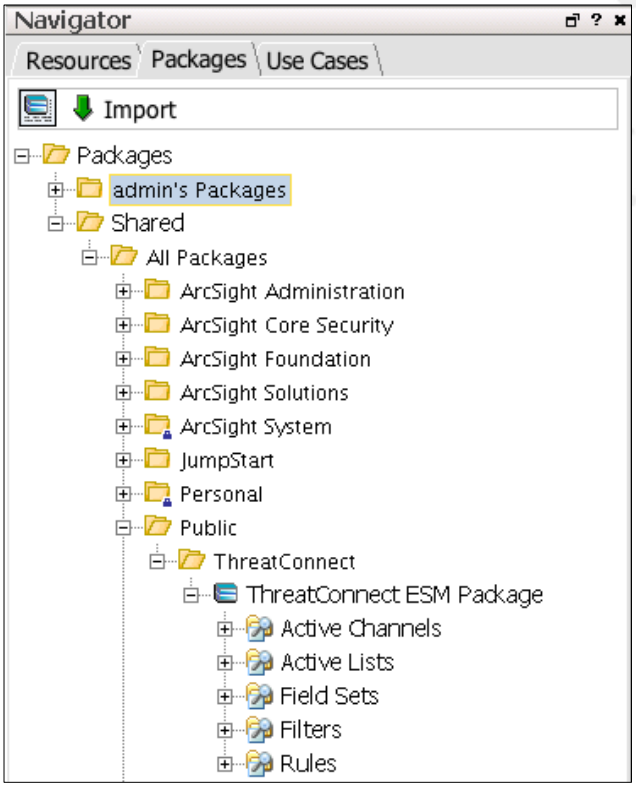

Figure 5

6. The Active Channel can be used to verify that data have arrived in ArcSight after being sent from ThreatConnect (Figure 6).

   NOTE: For the included rules to begin populating Active Lists, the rules must be moved from** ../Public/ThreatConnect **to the Real-time Rules directory.

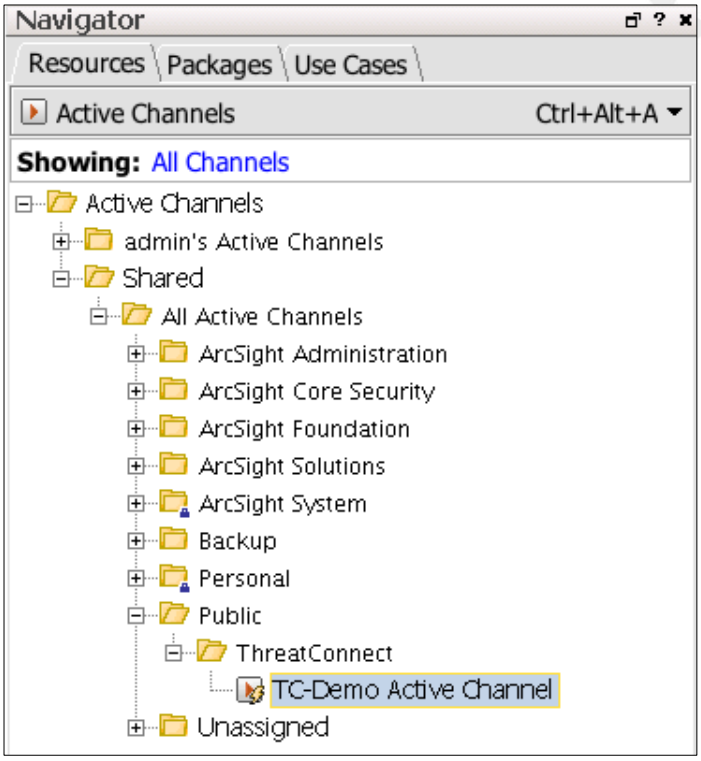
Navigator
Resources
Packages
Use Cases
Active Channels
Ctrl+Alt+A
Showing: All Channels
Active Channels
admin's Active Channels
Shared
All Active Channels
ArcSight Administration
ArcSight Core Security
ArcSight Foundation
ArcSight Solutions
ArcSight System
Backup
Personal
Public
ThreatConnect
TC-Demo Active Channel
Unassigned

Figure 6

CREATING AN ACTIVE CHANNEL AND VALIDATING DATA

1. On the ArcSight ESM Main screen, click the **New Item** icon at the top left (Figure 7), and the **New Active Channel** screen will be displayed (Figure 8).

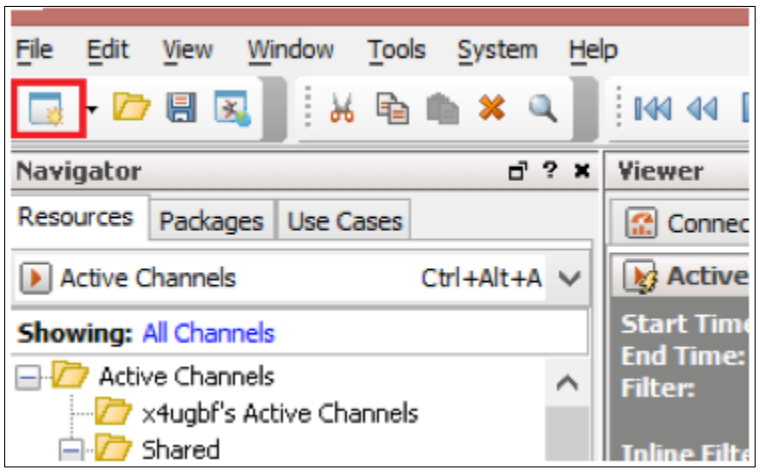

Figure 7

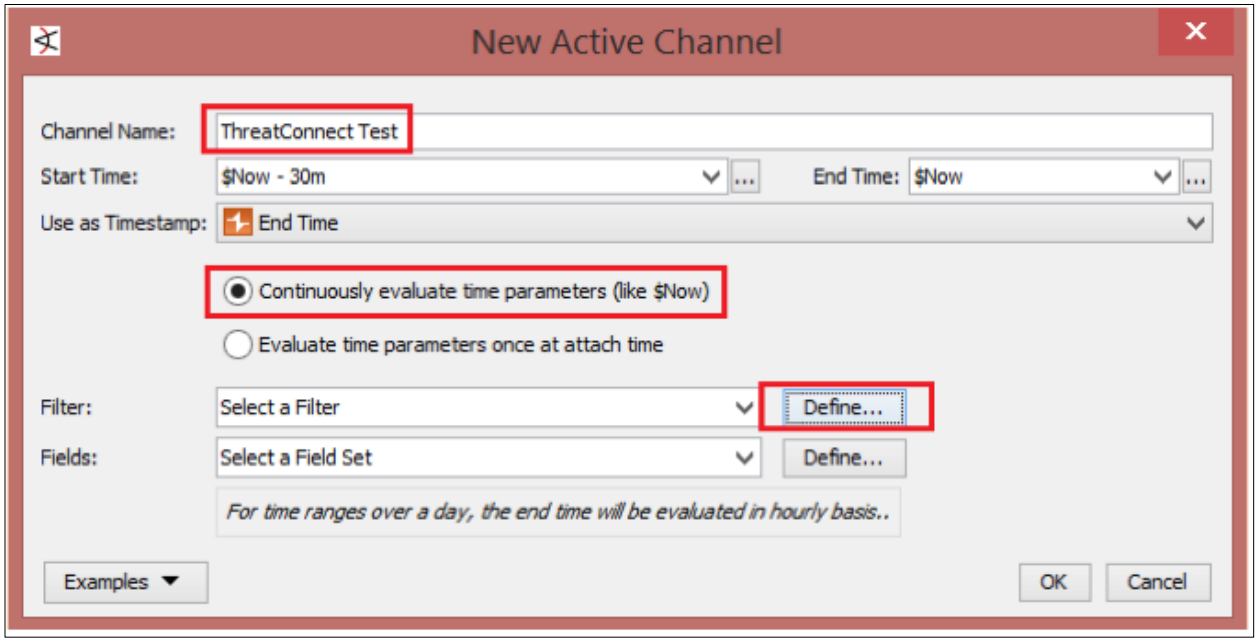

Figure 8

2. Fill in the necessary fields for the Active Channel:
3. Enter a name for the channel in the **Channel Name** box, and select the **Continuously evaluate time parameters** radio button.

   Then, click the **Define...** button next to the **Filter** dropdown menu to create a rule that will generate alerts in the new channel. A window will be displayed from which two conditions can be added that will be checked by the "and" logic gate (Figure 9).

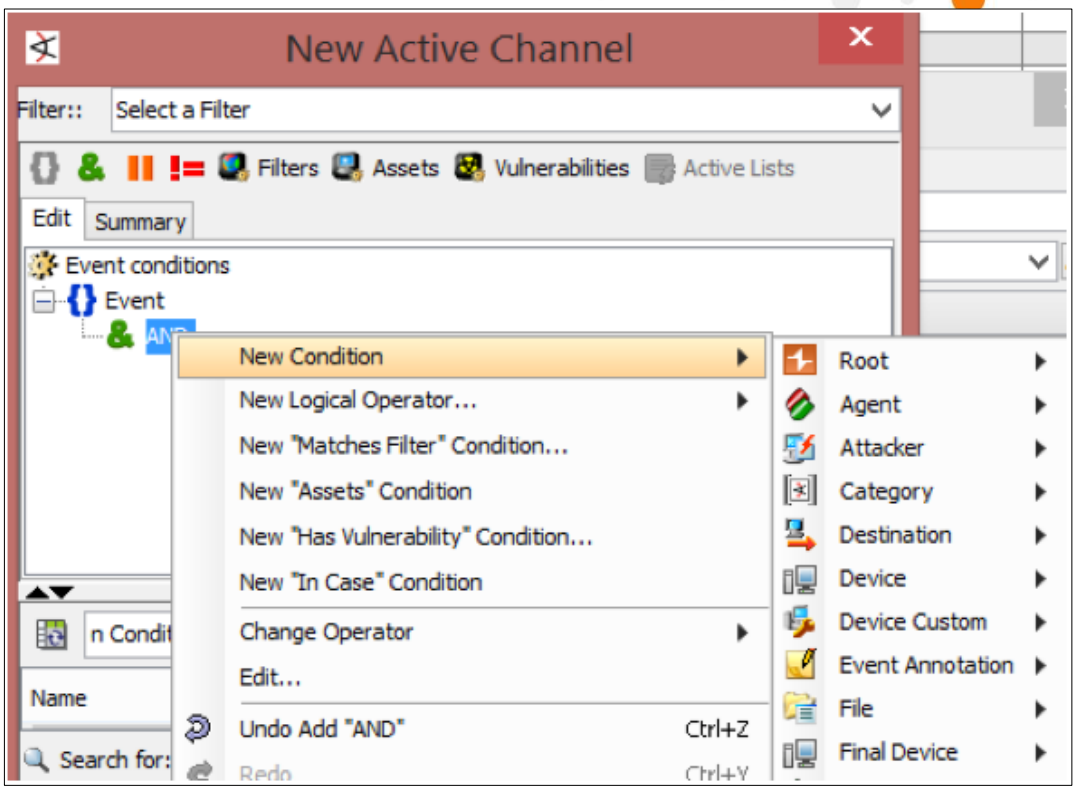

Figure 9

4. Click the green **Ampersand** button to add a Boolean "and" to the rule.
5. Right-click the **AND** text next to the green ampersand for a list of optional components to add.
6. In the **New Condition** dropdown menu, hover over **Device**, select both **Device Vendor** and **Device Product**, and set them both equal to **threatconnect** (Figure 10).

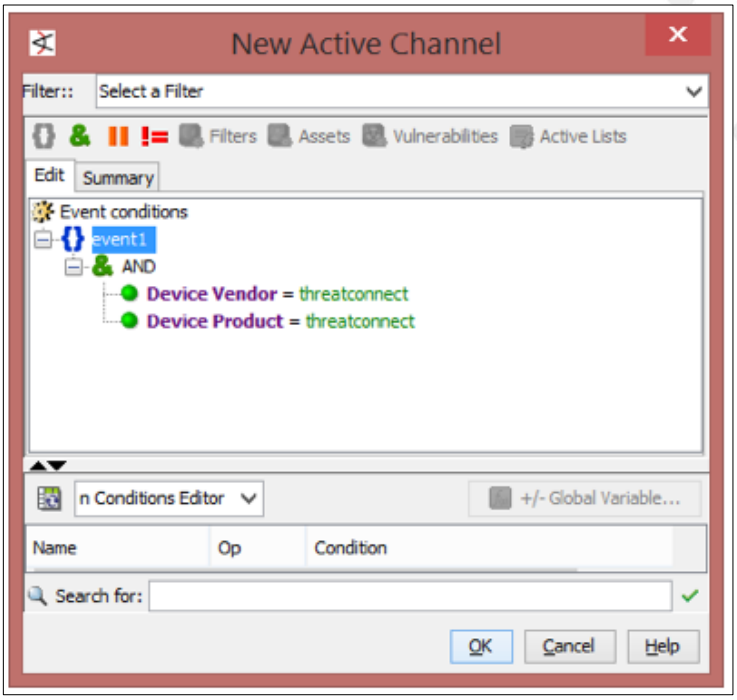

Figure 10

7. Click the **OK** button to create the filter and then again to create the channel. The new channel will be available in the user's Active Channels.
8. Select the channel to bring it up, and then execute the TC CEF Syslog job in ThreatConnect. Alerts will begin populating the Active Channel as data arrive (Figure 11).

   NOTE: This process can take up to a minute, depending on system load.

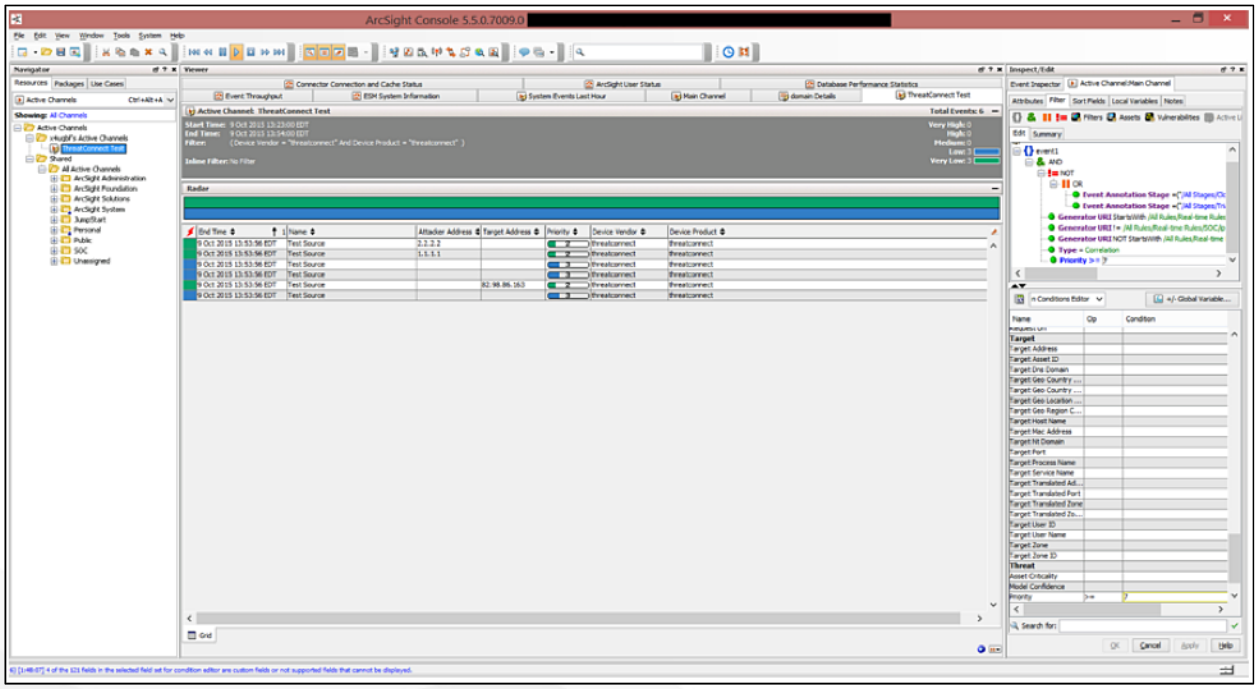

Figure 11

9. Select one of the events to verify that data are arriving correctly. The pane located at the right side of the screen will change to display the details of the selected event. Scrolling down will show that some of the fields have been populated. In particular, check the **Device Custom** fields to make sure that the data arrived (Figure 12).

Device Custom	
Device Custom Date1.	6 Oct 2015 13:59:13 EDT
Device Custom Date2.	6 Oct 2015 13:59:20 EDT
Device Custom Number1.	73
Device Custom String2.	Test
Device Custom String3.	Address

Figure 12

CREATING AN AUTO-POPULATED ACTIVE LIST

There are two components to include when creating an Active List: a rule and the Active List itself. First create the Active List, so that the rule can add new Indicators to it.

Creating an Active List

1. On the ArcSight ESM **Main** screen, click the **New Item** icon at the top left (Figure 13).

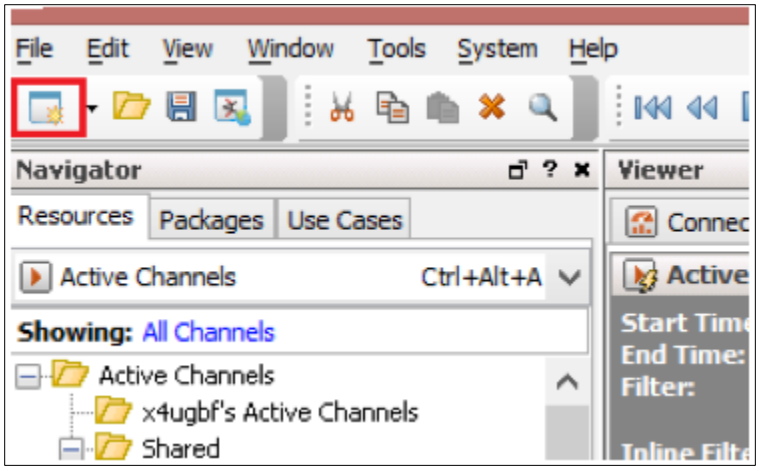

Figure 13

2. Select **Active List**, and an **Active List Editor** tab will open in the pane located at the right side of the screen (Figure 14).

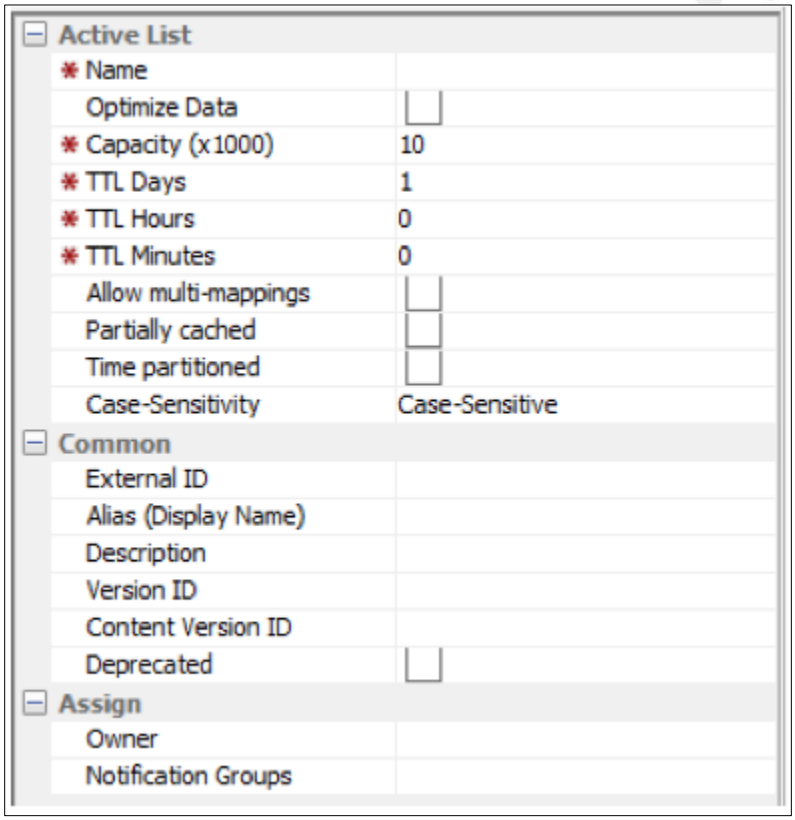

Figure 14

3. Most of the fields are not necessary; their use depends on the customer's ArcSight ESM setup. It is important to provide a **Name** for the Active List, to modify the **Capacity** as necessary, and to change the **TTL** values. The **TTL** values determine how long an item will remain on the Active List. If the values are changed to 0, Indicators will not be removed.

   NOTE: The Capacity value is given in thousands.

4. Below the **Active List** section, in the same pane, is the **Data** section, where fields that will be included in each row of the list are defined (Figure 15). Select the **Fields-based** radio button, and check the **Key Fields** box.

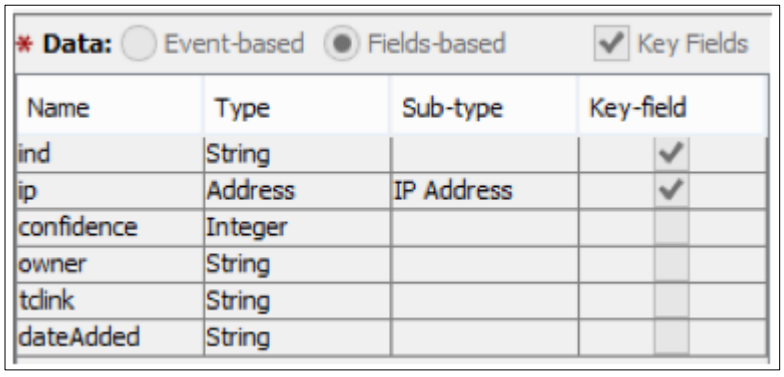

Figure 15

5. To type-match the data, the **Type** column must contain the type of data expected to be found in a field that will map to this field (accomplished by the rule created after this list).

Also, there are some reserved words in ArcSight that cannot be used as a field name. Aside from those words, users can name each field as they desire.

6. In the **Key-field** column, select the fields that will be used to join the data from an event to fields on the Active List. If an IP address is added twice, for example, the Active List will increment a count field and then overwrite non–Key Fields with changed data in the newly arriving event.
7. Click the **OK** button on the bottom to save the Active List.

Creating a Rule

1. On the ArcSight ESM **Main** screen, click the **New Item** button on the upper left (Figure 13), and then select **Rule** to open a **Rule Editor** tab in pane located at the right side of the screen (Figure 16).

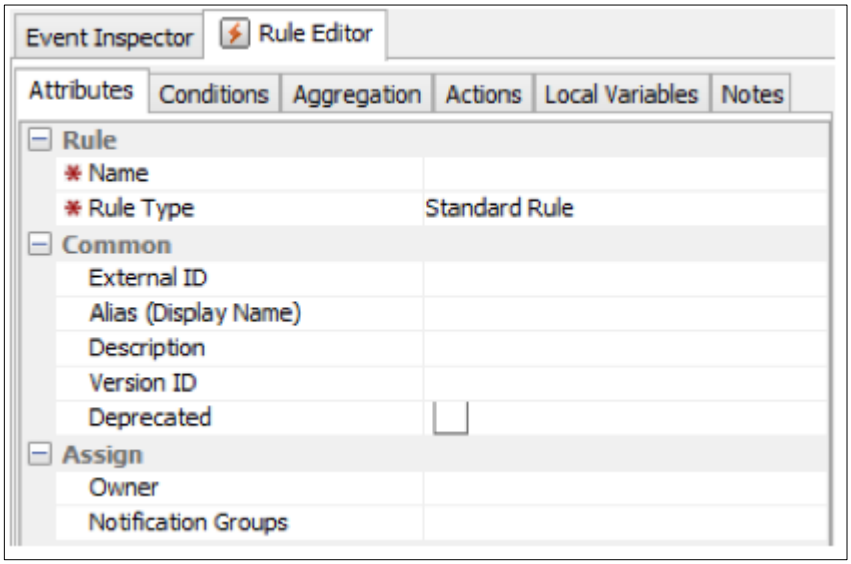

Figure 16

2. Enter a **Name** for the rule, and then select a **Rule Type.**
   - **Lightweight Rule:** A Lightweight Rule does not generate an event when an item is added to a list. Lightweight Rules are used only for adding items to and removing items from an Active List.
   - **Standard Rule**: A Standard Rule generates an event when an item is added to a list. If an integration command will be added to a rule as an action event (such as writing back an observation), then Standard Rule needs to be selected, as Lightweight Rules do not allow integration commands to be added as action events.
3. Click on the **Conditions** tab, and the **Conditions** screen will be displayed (Figure 17).

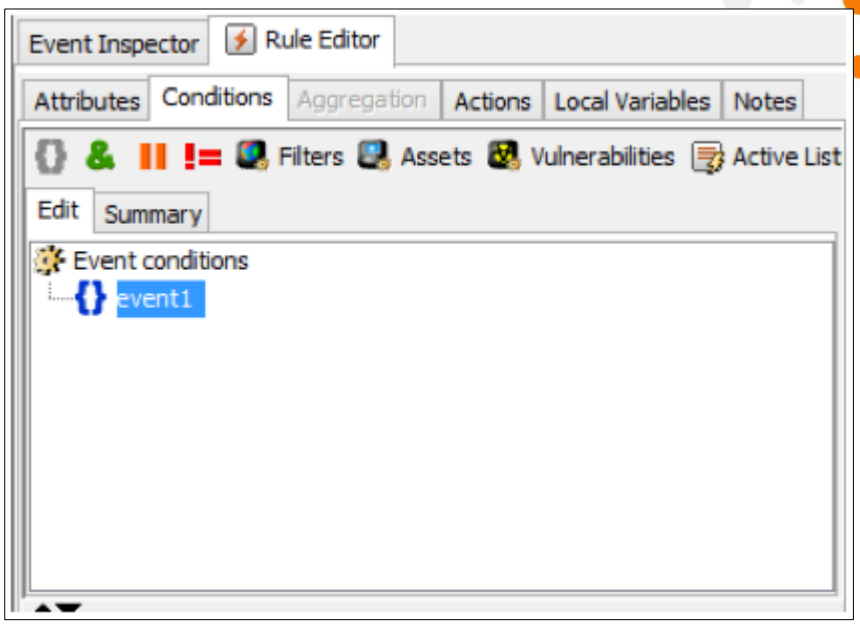

Figure 17

4. Add the same two fields used to pick up data sent from ThreatConnect when validating the data: **Device Vendor = threatconnect** and **Device Product = threatconnect**.
5. Add another field as follows: **Type != Correlation** (Figure 18). This field ensures that the rule will fire only on base events—those events coming in through connectors—and not on events that have been generated by a rule. If desired, change the Boolean operator by clicking on the equals sign and selecting a specific operator.

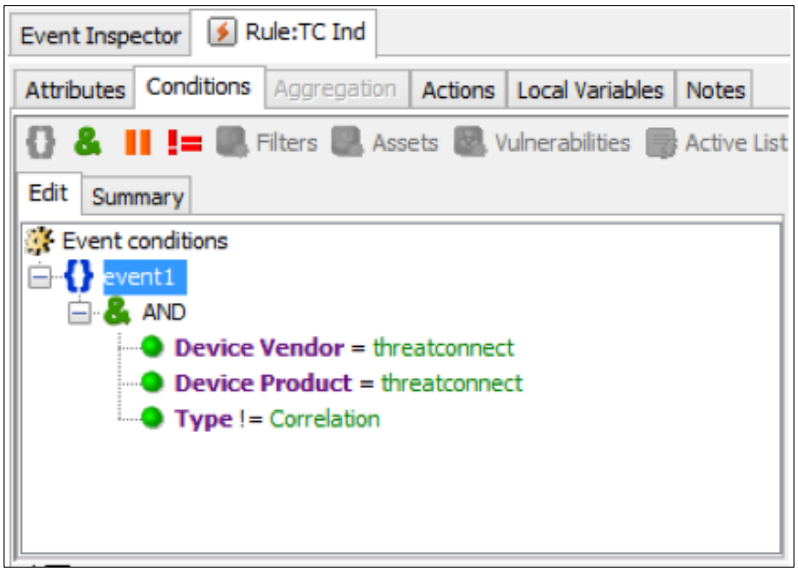

Figure 18

6. Click the **Actions** tab to add an action to this rule in order to write the detected event into the Active List previously created. This tab holds a list of event situations where an action will occur. Right-click **On Every Event**, and select **Add > Active List > Add To Active List** (Figure 19).

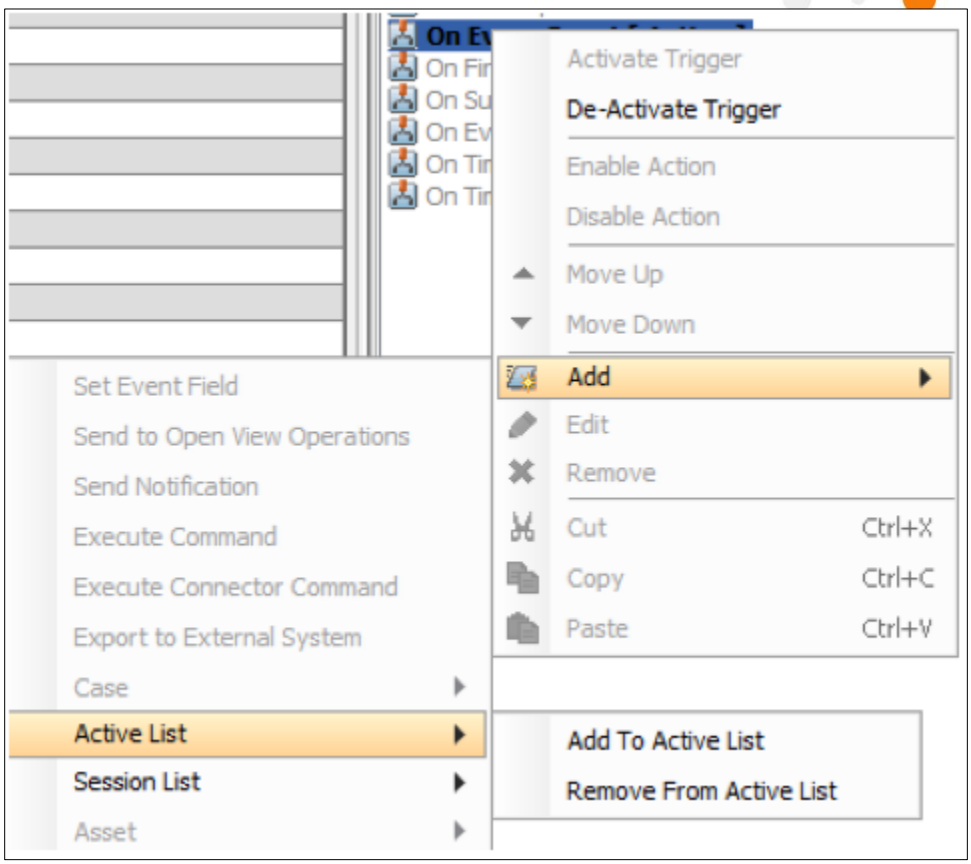

Figure 19

7. A window will be displayed from which an Active List can be selected. Select the list that was previously created to hold the inbound data, and the fields that require mapping in the Active List will be displayed (Figure 20). Matching ArcSight fields that hold the necessary data must then be selected.

   NOTE: Only fields of matching data types may be selected.

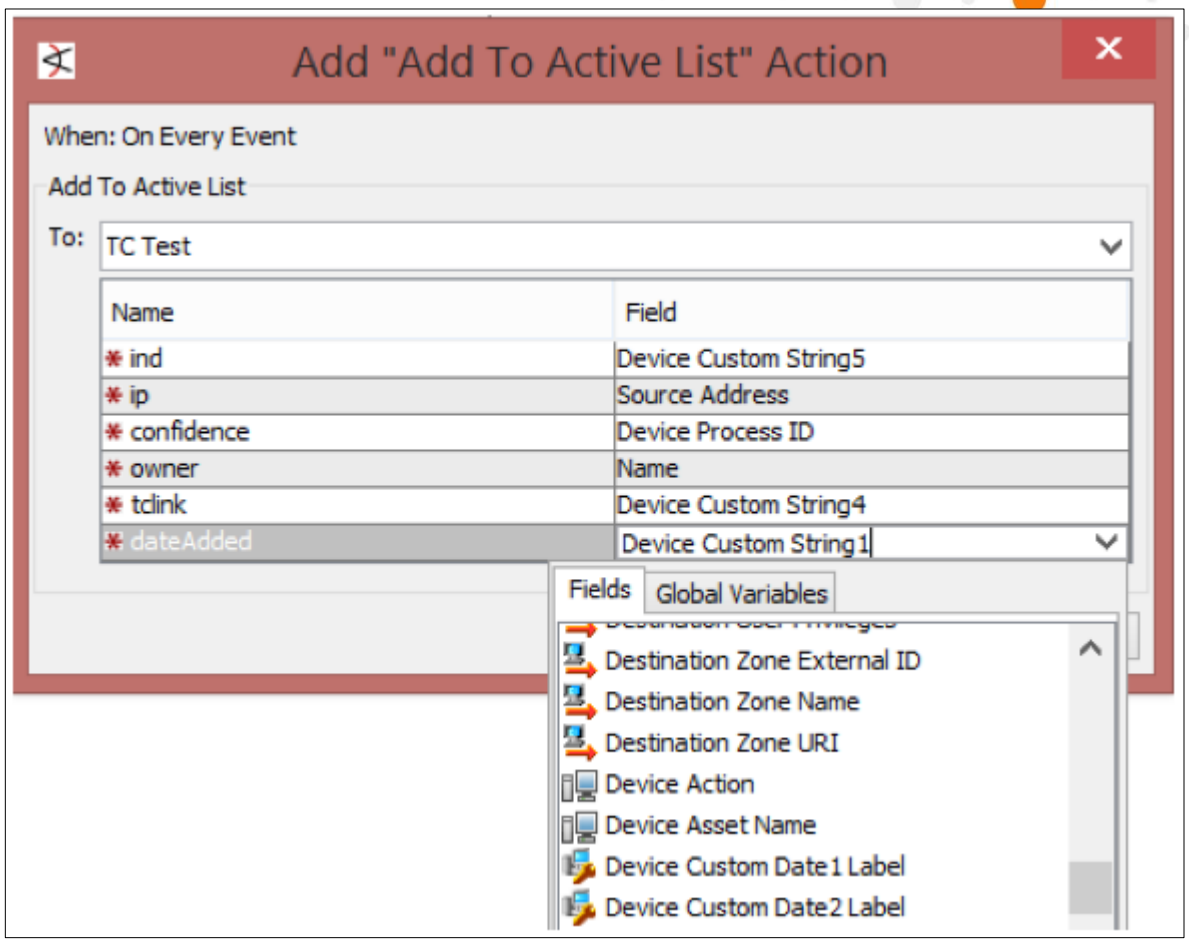

Figure 20

8. Once all of the fields have been mapped, click the **OK** button. The field mappings will be added to the **Actions** tab within the rule (Figure 21).

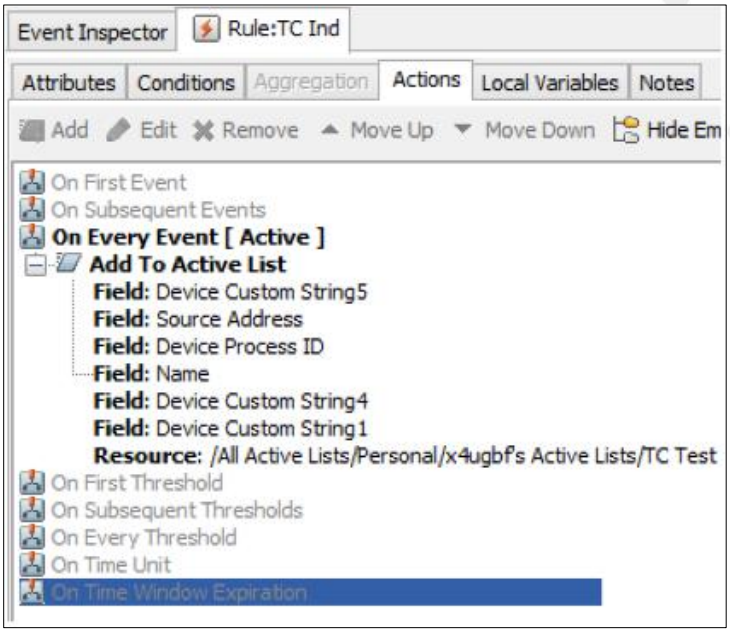

Figure 21

9. Click the **OK** button at the bottom of the pane to save the rule.
10. Although the rule has been created, it still will not be firing in real time against inbound data. To initiate this process, copy the rule from a personal directory to the **Shared > Real-time Rules** directory in the navigation pane located at the left side of the screen (Figure 22).

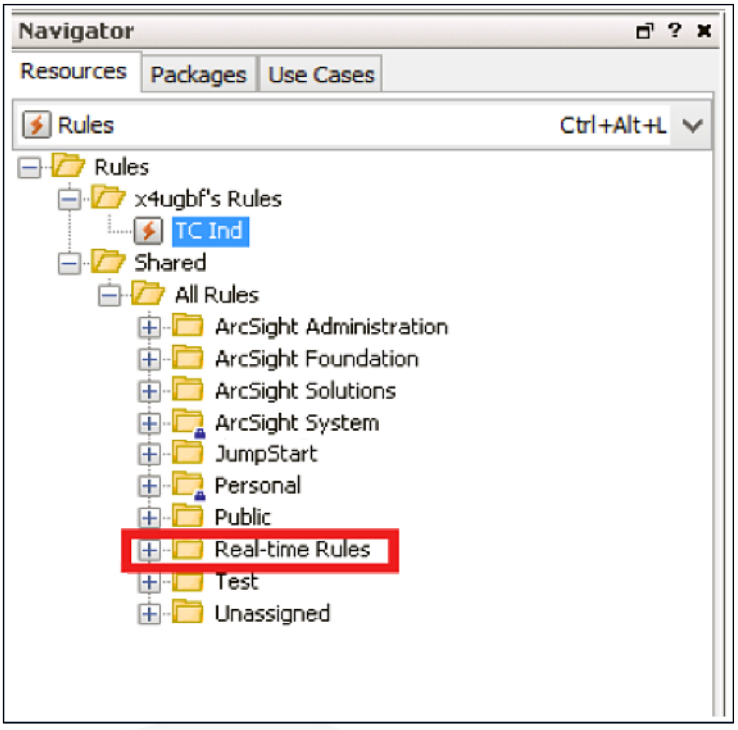

Figure 22

11. With the rule and Active List now in place, the Active List will be auto-populated by daily pushes from ThreatConnect. To test this condition, execute the **TC CEF Syslog** job in ThreatConnect to push Indicators into ArcSight ESM, or allow the `cron` job to run if using the Environment Server.
12. In the navigation pane located at the left side of the screen, go to **Lists** and right-click the Active List in the user's private list.
13. Select **Show Entries** to see what has been added to the Active List (Figure 23).

NOTE: It may take up to a minute after pushing the data for the entries to show, depending on system load. If data are taking too long to arrive, click the Refresh button located at the top right.

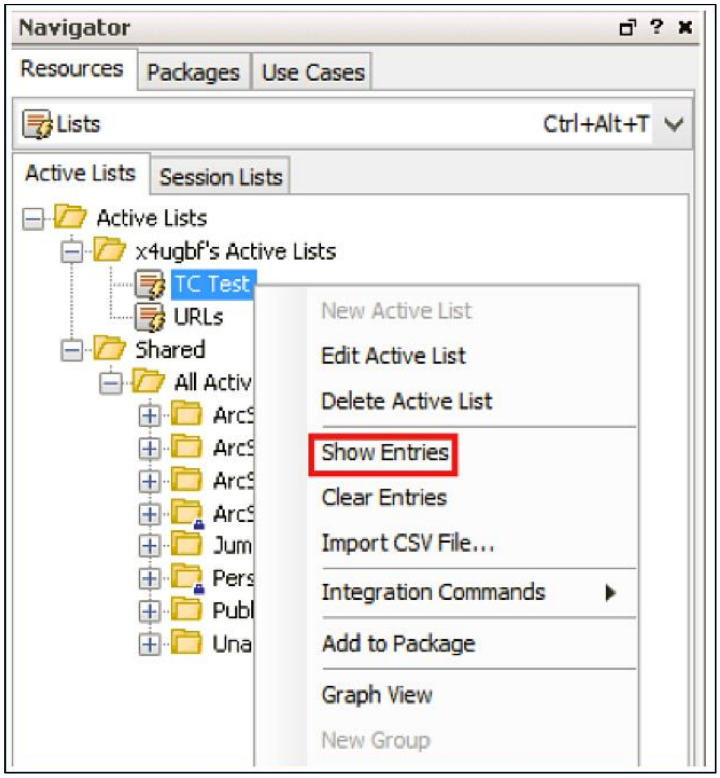

Figure 23

14. Use this list in rules matching events against this Active List, and display the events generated from the rule in an Active Channel for real-time alerts (Figure 24).

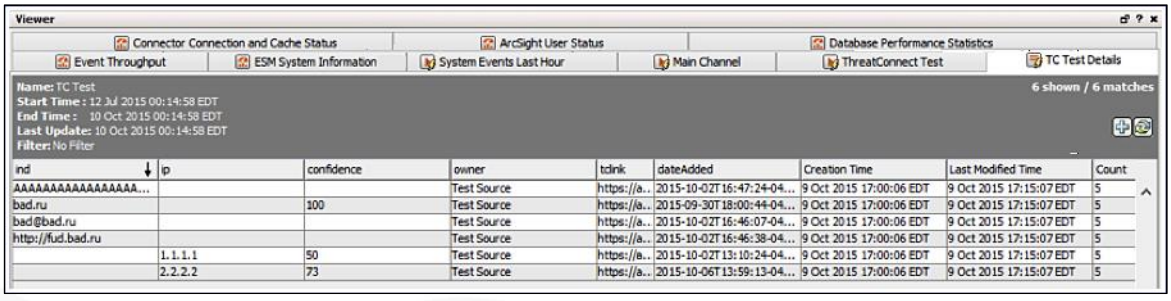

Figure 24

Using Deprecation to Remove Indicators from an Active List

Items may be removed from an Active List in much the same way that they are added to an Active List. While creating the rule to add Indicators, add a condition to check the value of **Device Process ID** (where **Device Process ID** is the Confidence Rating of the Indicator). This value needs to be greater than the last positive value an Indicator would have if being deprecated (Figure 25). For example, if an Indicator's Confidence Rating is 10 and is deprecated by 1 daily before being deleted at 0, it would need to be removed from the Active List when the Confidence Rating value reaches 1 (that is, before it is deleted and no longer sent from ThreatConnect).

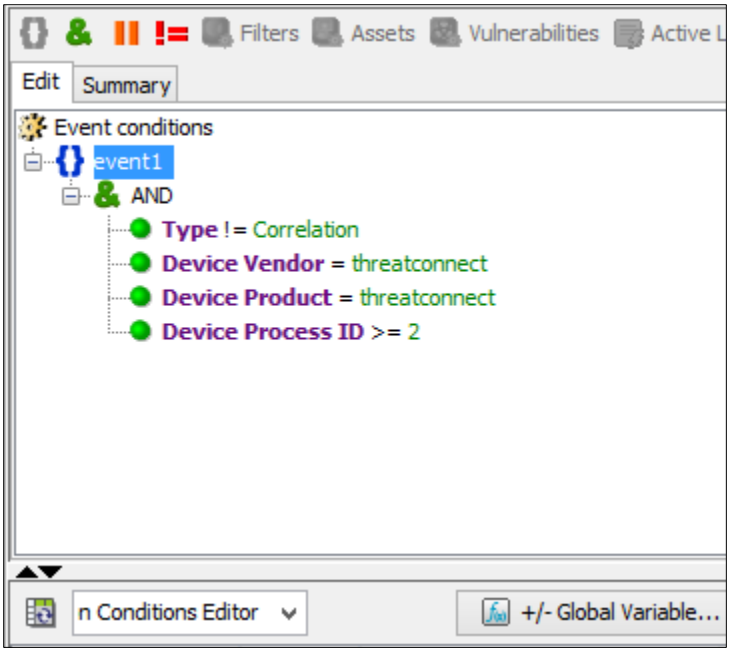

Figure 25

A second rule needs to be created to actually remove the item. This rule is built in the same way as the rule for checking **Device Process ID** against the last positive value of an Indicator that is being deprecated, but it instead checks for a **Device Process ID** value of the minimum deprecation value or less (Figure 26). The action is also changed so that it removes an item from the list rather than adding it to the list (Figure 27).

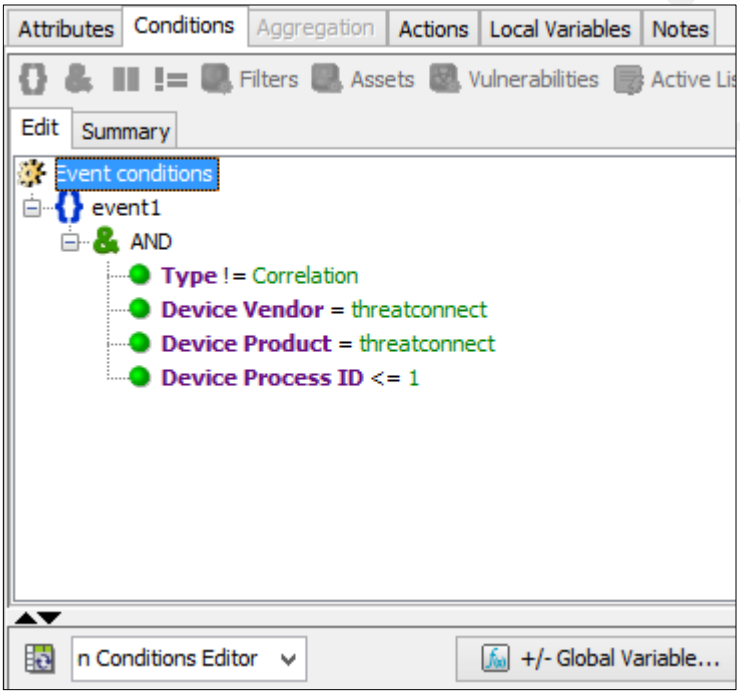

Figure 26

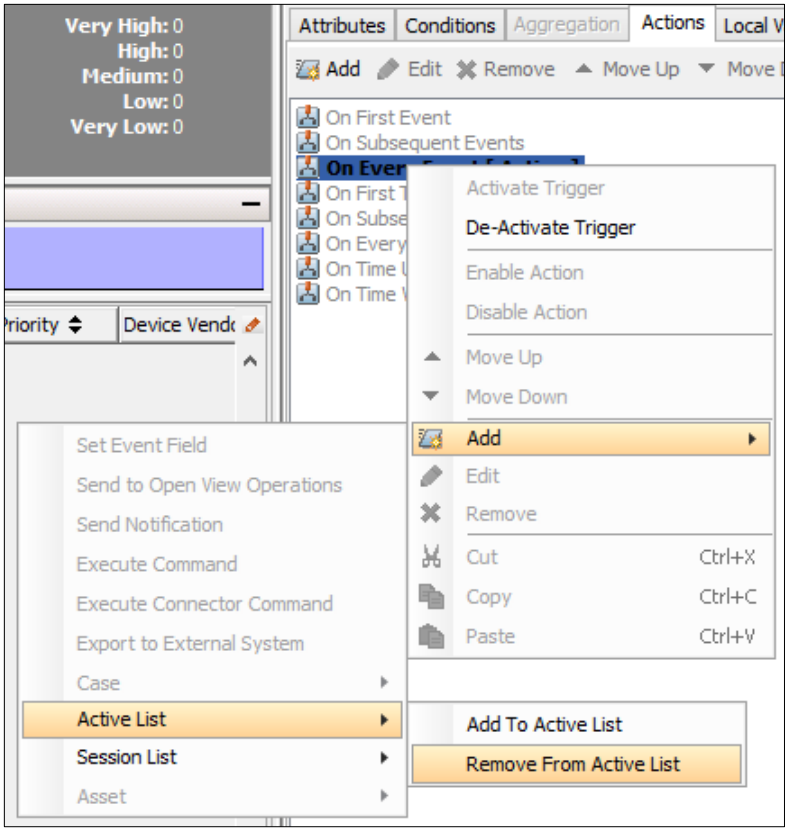

Figure 27

After selecting the items to remove from a list, select the list from which to remove the items (Figure 28). Once again, map the fields on the list to different fields, making sure to map all of the same fields that were mapped on the rule that added items to the list.

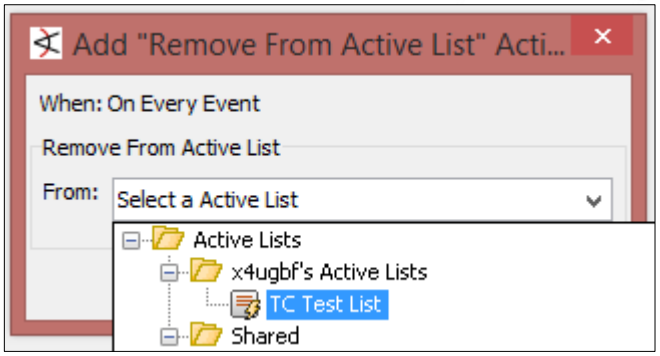

Figure 28

When both of these rules have been added to the **Real-time Rules** folder, the system will begin adding and removing items from the Active List.