ThreatConnect™

ThreatConnect® SmartResponse™ Plugin LogRhythm®

User Guide

Software Version 1.0

August 4, 2020

30051-02 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

THREAT CONNECT™

www.ThreatConnect.com
info@threatconnect.com

TOLL FREE: 1.800.965.2708
LOCAL: +1.703.229.4240
FAX: +1.703.229.4489

THREATCONNECT, INC.
3865 WILSON BLVD., SUITE 550
ARLINGTON, VA 22203

Table of Contents

OVERVIEW

The ThreatConnect integration package for LogRhythm allows LogRhythm users to interact with threat intelligence in ThreatConnect directly from the LogRhythm Console by using a set of LogRhythm plugin actions. The integration package can perform functions such as retrieving Indicator details and reporting observations and false positives to ThreatConnect.

DEPENDENCIES

ThreatConnect Dependencies

- Active ThreatConnect Application Programming Interface (API) user and 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.

- ThreatConnect installation zip file (contains ThreatConnect LogRhythm plugin actions): **ThreatConnect-LogRhythm-Package_vX.X**

LogRhythm Dependencies

- LogRhythm Console (web and PC based)
- PowerShell v4+ installed on Platform Manager

INSTALLATION

Plugin Actions: LogRhythm-to-ThreatConnect Indicator Upload and Enrichment

LogRhythm plugin actions perform a number of functions, including creating Indicators in ThreatConnect, getting more information about an Indicator, and reporting an observation. These actions are bundled within a LogRhythm SmartResponse. Before these plugins can be created, the ThreatConnect file must be configured.

File Configuration

Follow these steps to configure the ThreatConnect file:

1. Unzip the provided ThreatConnect file, **ThreatConnect-LogRhythm-Package_vX.X.zip**, into any folder.
2. One of the files within the zip file is named **tc.conf.default**. Rename the file to **tc.conf**.
3. This file controls various aspects of the integration commands. Edit the file, and update the required value and any of the optional values. Detailed information about the settings is in the file itself.

Creating a SmartResponse Plugin

Follow these steps to create the SmartResponse plugin:

1. Run the LogRhythm PC Console application.
2. Open the Deployment Manager.
3. Click on the **Tools** menu, and then choose **Administration > SmartResponse Plugin Manager** (Figure 1).

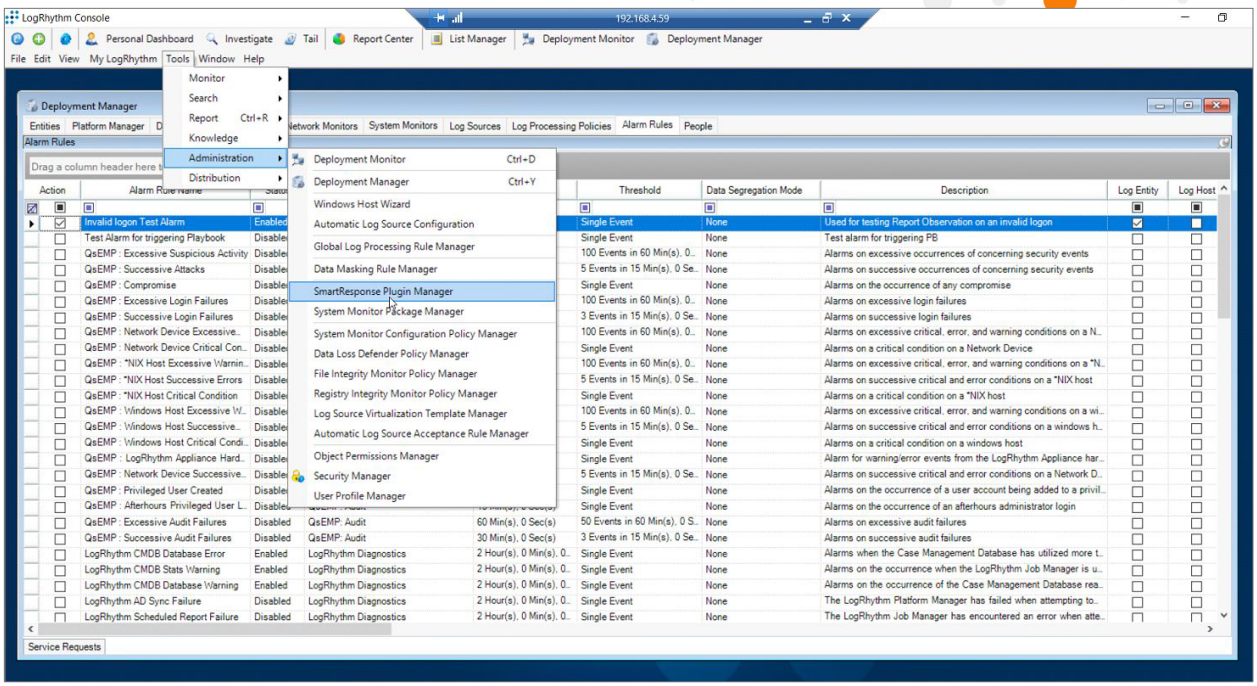

Figure 1

4. Select the **Create Plugin** menu option (Figure 2).

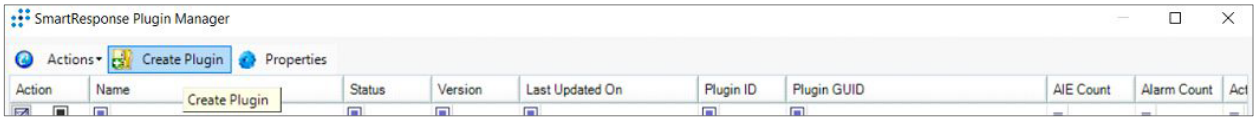

Figure 2

5. Select the folder that contains all the unzipped contents of **ThreatConnect-LogRhythm-Package_vX.X.zip**, including the **tc.conf** file that was renamed and edited during the file configuration process.
6. Click the **Validate** button. A "Success" message will appear (Figure 3).

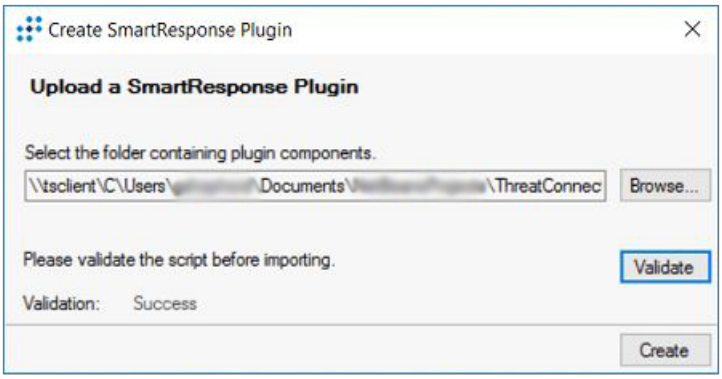

Figure 3

7. Click the **Create** button, and then choose a folder in which to save the plugin.
8. The SmartResponse plugin will be created with a name similar to the following: **ARPlugin_00000000-0000-0000-0000-000000000000_20180118.lpi**.

NOTE: The date is the last part of the filename, so if another SmartResponse plugin is created on the same day, the original file will be overwritten.

Importing the SmartResponse Plugin

1. From the **Actions** menu, choose the Import option (Figure 4).

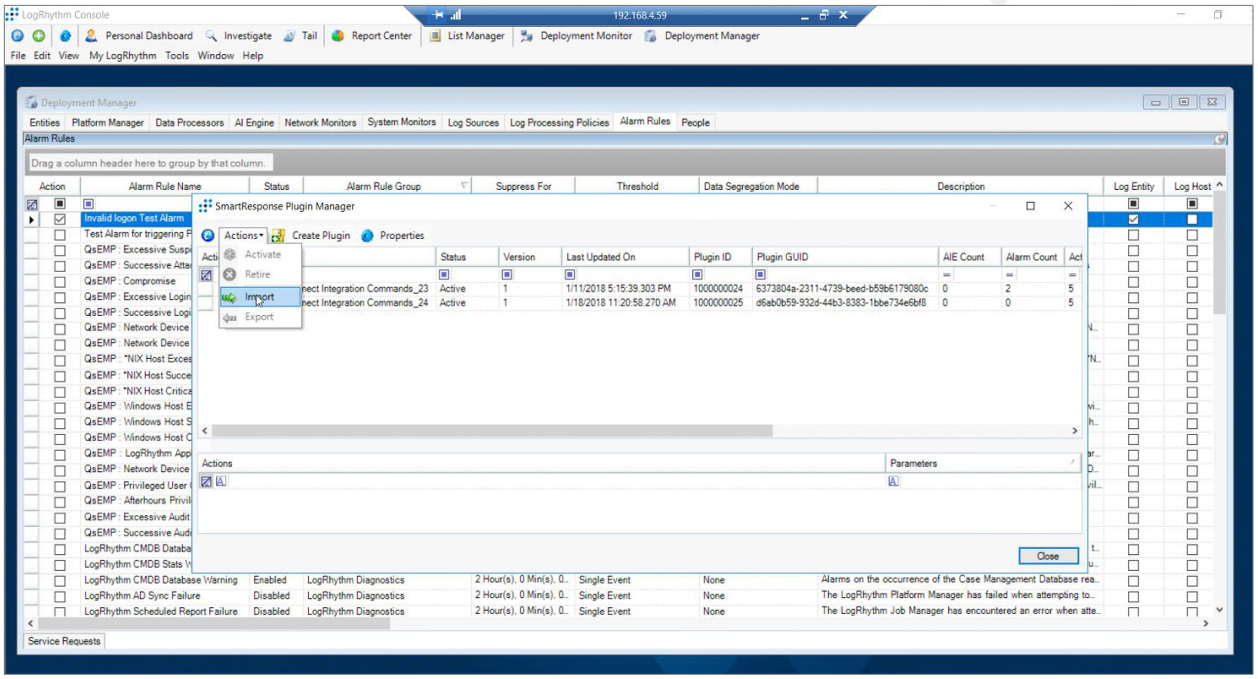

Figure 4

2. Select the file created in the "Creating a SmartResponse Plugin" section.
3. If a window appears warning that the GUID is already being used and asking if you would like to import with a new GUID (Figure 5), click the **Yes** button.

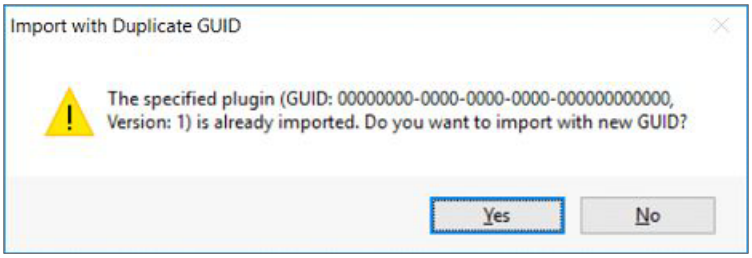

Figure 5

4. The new SmartResponse will be reflected in the window (Figure 6).

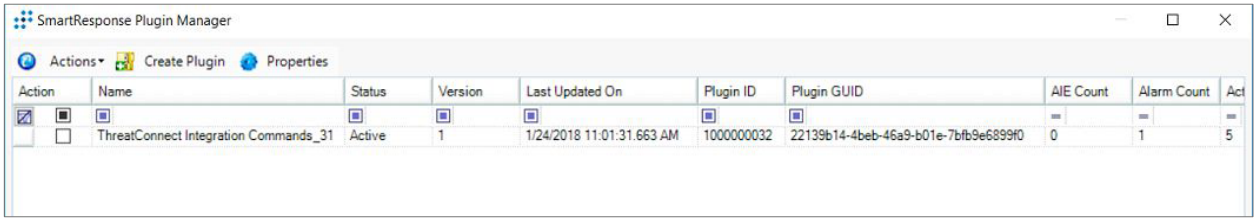

Figure 6

Testing Plugin Actions

The SmartResponse plugin has five possible actions:

- **Create Indicator**: Creates an Indicator in ThreatConnect.
- **Lookup Indicator**: Retrieves information about an Indicator (if it exists) in ThreatConnect.
- **Report False Positive**: Increments the False Positive count for the given Indicator in ThreatConnect.
- **Report Observation**: Increments the Observation count for the given Indicator in ThreatConnect.
- **Trigger Playbook**: Triggers a Playbook within ThreatConnect. A data value can be passed to the Playbook.

Each action can be tested within LogRhythm to determine whether the connections between systems are working and to demonstrate the use of each action.

NOTE: If a plugin action affects data in ThreatConnect, which is the case for all of the actions except Lookup Indicator, then testing the action will cause the data in ThreatConnect to be updated accordingly.

1. Open the SmartResponse Plugin Manager.
2. Select the SmartResponse in the top half of the window. The plugin actions to be tested will show in the list at the bottom of the window. In this example, the **ThreatConnect: Lookup Indicator** action is selected (Figure 7). This action is the simplest to test because it involves only data retrieval and thus does not change any of the data within ThreatConnect.

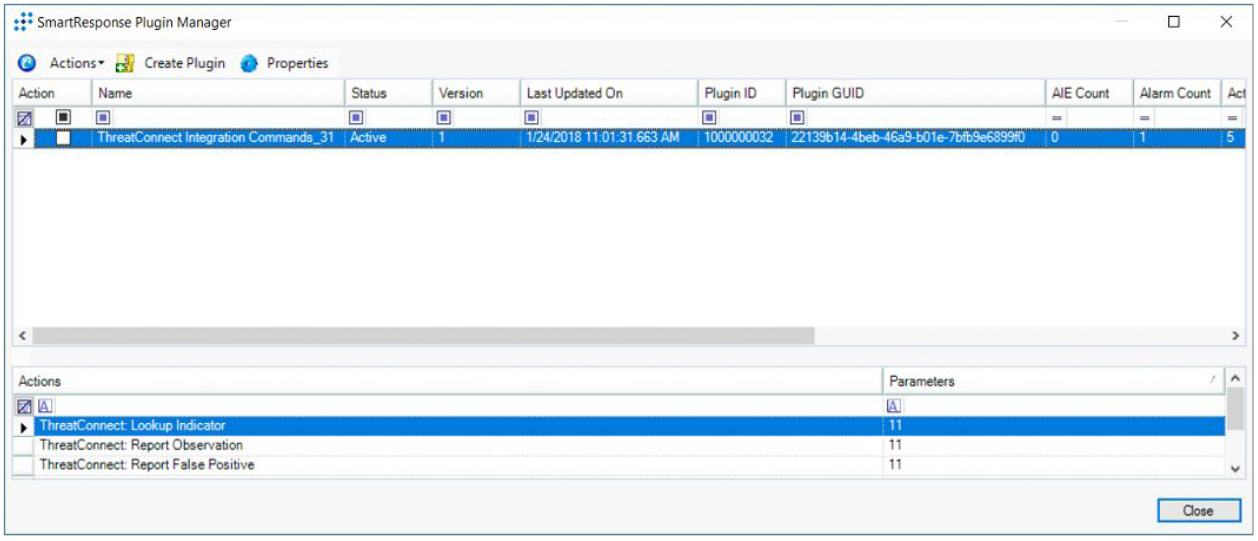

Figure 7

3. Double click the selected line, and a window showing all of the parameters that the action takes will appear (Figure 8).

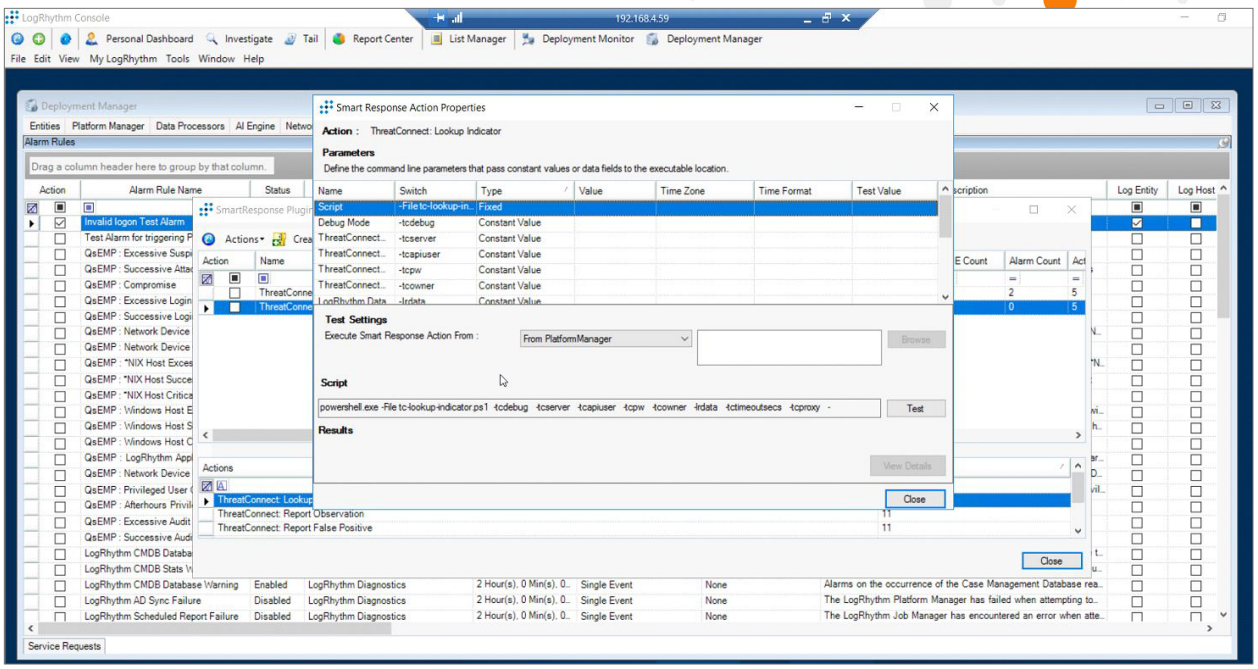

Figure 8

4. Set values for each parameter in this window. Most of the parameters are self-explanatory and mirror those in the **tc.conf** file setup. Values entered in this window will override the corresponding values in **tc.conf**. Note the following information about two of the parameters:
   - **-tcdebug** controls whether debug information is shown or not. The values follow the PowerShell values for log outputs. The most commonly used value is **Continue** (shows all debug log lines, but does not interrupt the program from running). The default value is **SilentlyContinue…** (no log lines are output, and the program is not interrupted).
   - **-lrdata** is the LogRhythm data used by the action. In most cases, it will be an Indicator value (e.g., IP Address, Host). It is a required value.
5. Once value(s) have been entered and another field has been clicked in, the **Script** section of the window will reflect the changes (Figure 9). Typically, all the values mirrored in **tc.conf** were already set when the plugin was created, and so the only value that must be set here is **-lrdata**.

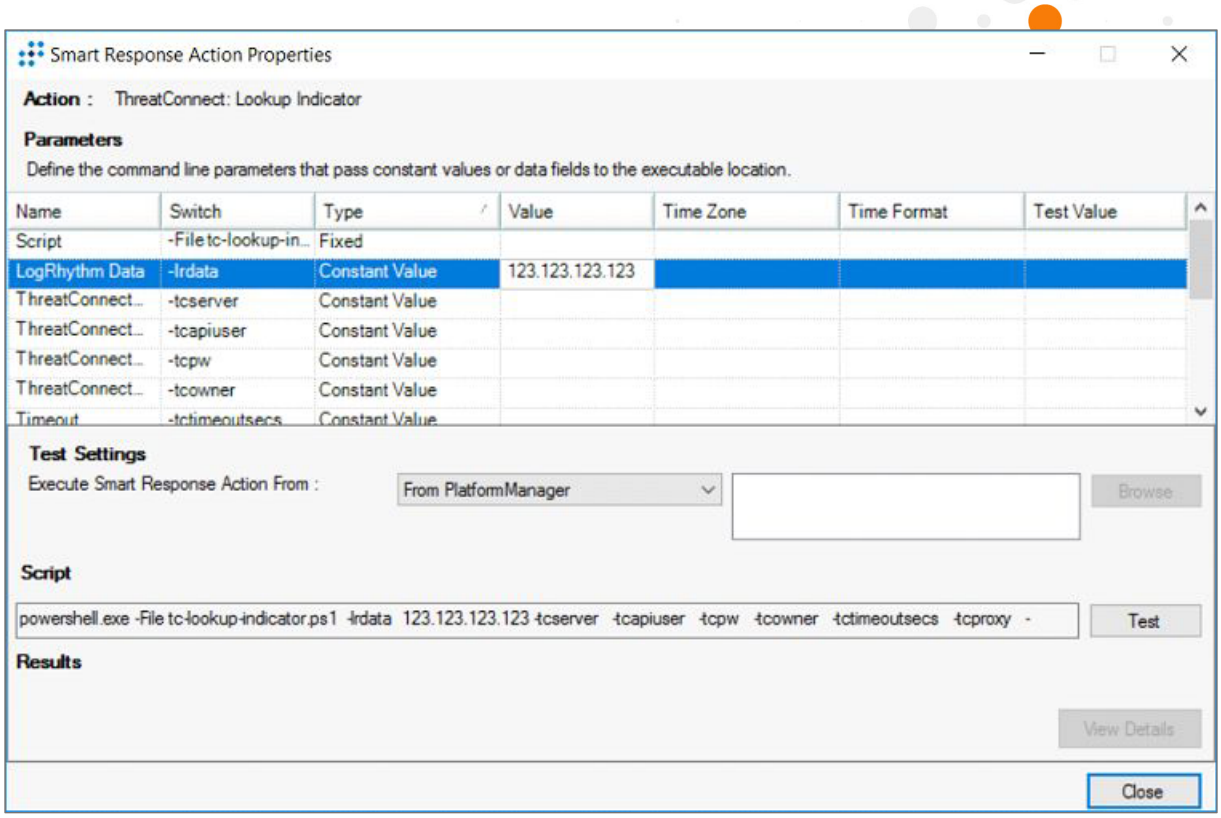

Figure 9

6. Once all parameter values have been entered, click the **Test** button towards the bottom right of the window. Click the **Yes** button on the next two dialog boxes (Figure 10 and Figure 11), and then the script will run.

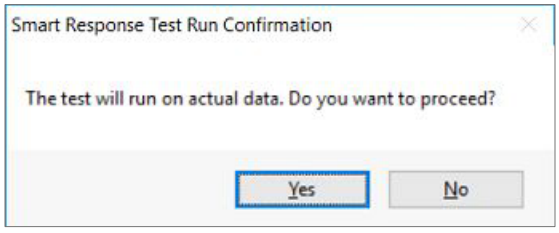

Figure 10

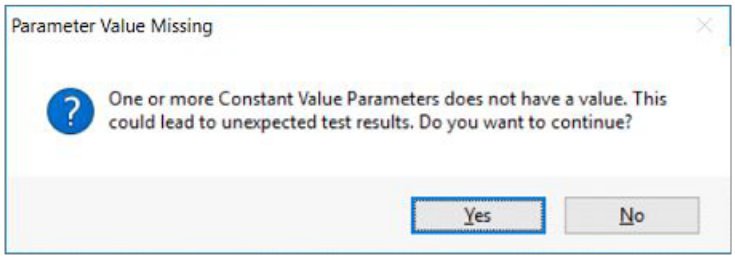

Figure 11

7. The **Results** should show the following: **Executed: Success** (Figure 12).

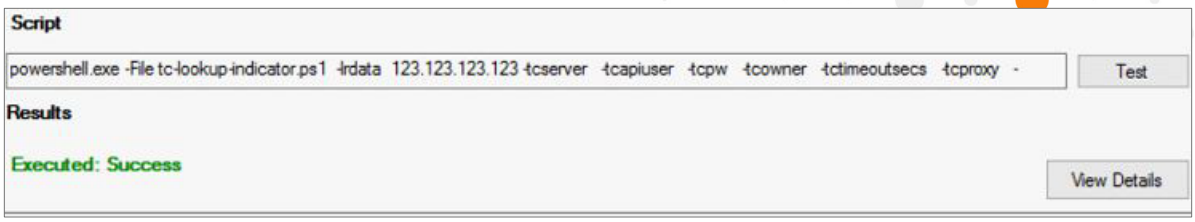

Figure 12

8. Click the **View Details** button to view any output, including debug statements.

Using Plugin Actions

The most common way to use the plugin actions is to have an Alarm Rule auto-execute them within LogRhythm. The following example demonstrates how to trigger a Playbook to execute within ThreatConnect when an Indicator from incoming LogRhythm data matches an Indicator existing in a LogRhythm List:

1. This example assumes that LogRhythm has an existing List, shown in Figure 13, that contains two Indicators (IP Addresses in this example). For details on how to set up external sources that would fill such Lists, please refer to the LogRhythm documentation.

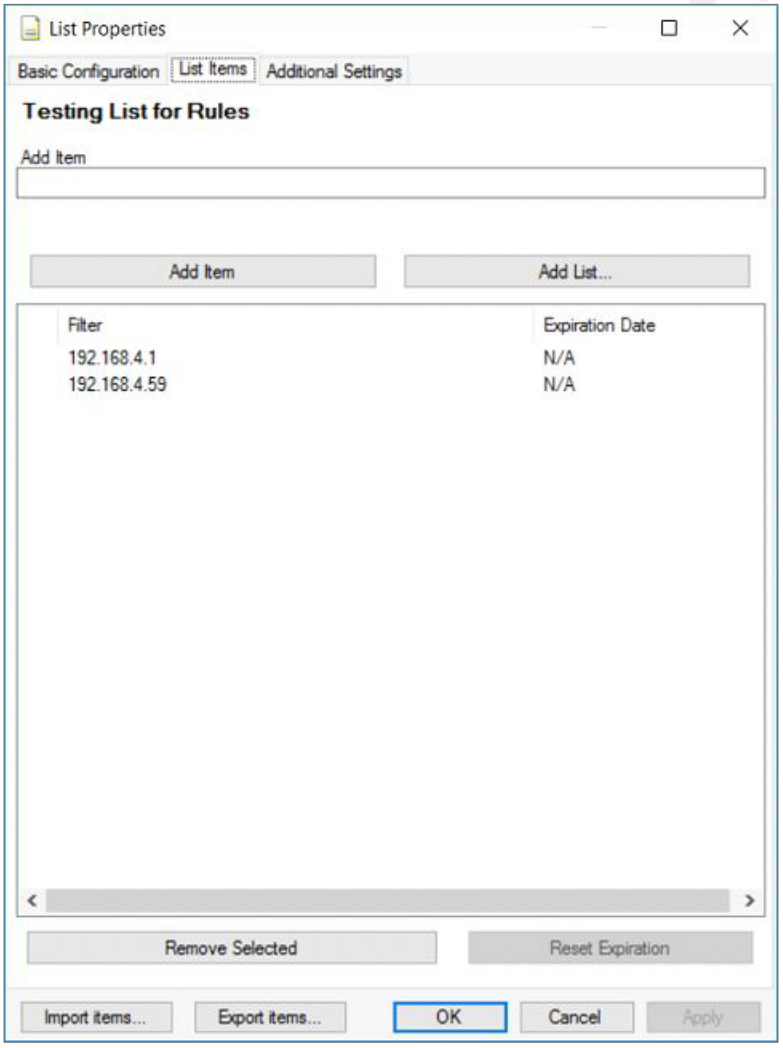

Figure 13

2. Open the Deployment Manager, and click the **Alarm Rules** tab.
3. Click the **+** button to create a new rule. A window for the rule will open (Figure 14).

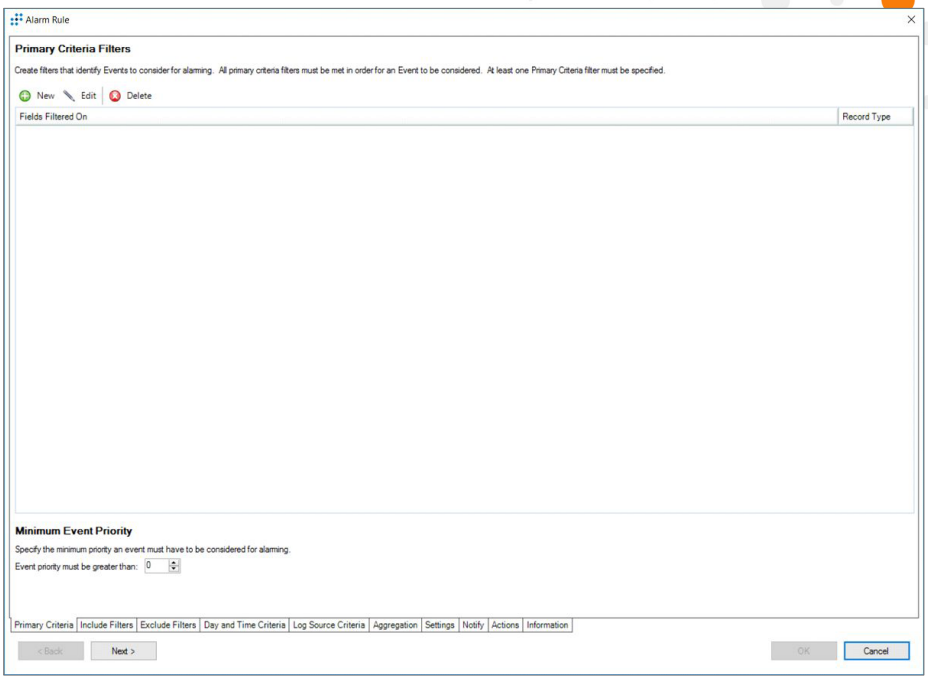

Figure 14

4. On the first tab shown at the bottom of the window, **Primary Criteria**, add a filter that compares the value in the **IP Address (Origin)** column (this column is for the incoming LogRhythm data) with any value in the List (Figure 15). Note that the term **Is** in the **Filter Mode** column indicates that a comparison/IN operation should be performed.

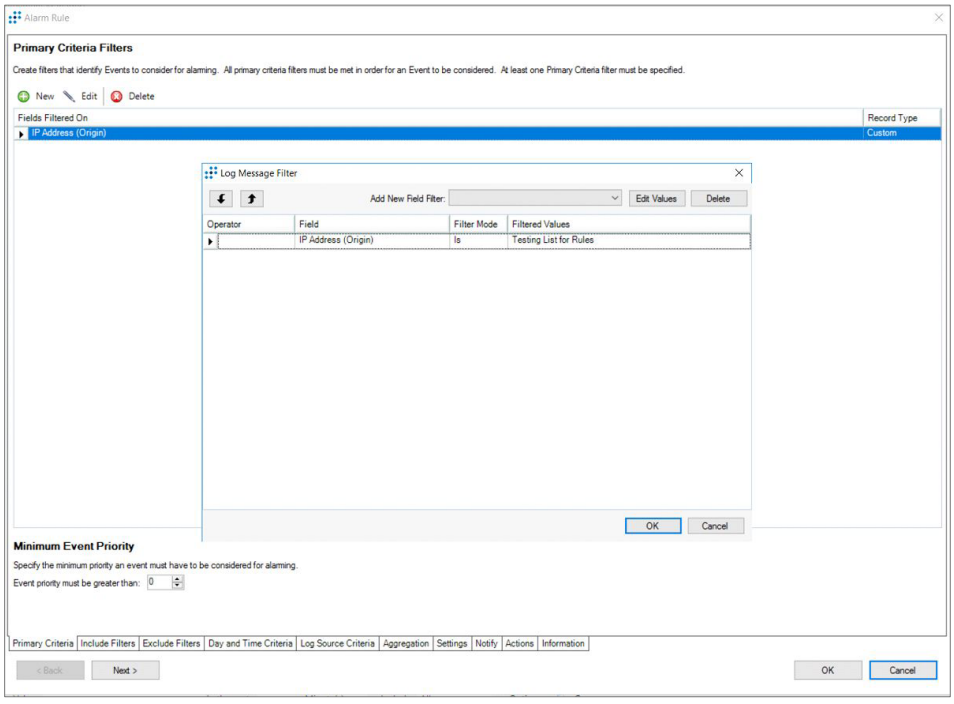

Figure 15

5. Click on the **Actions** tab at the bottom of the screen. This tab is where the SmartResponse plugin is chosen and the values are set. In this example, the action is **Report Observation**, and the **LogRhythm Data** parameter is set to **IP Address (Origin)** (Figure 16).

   NOTE: Make sure to click the Save Action button on this screen before moving on.

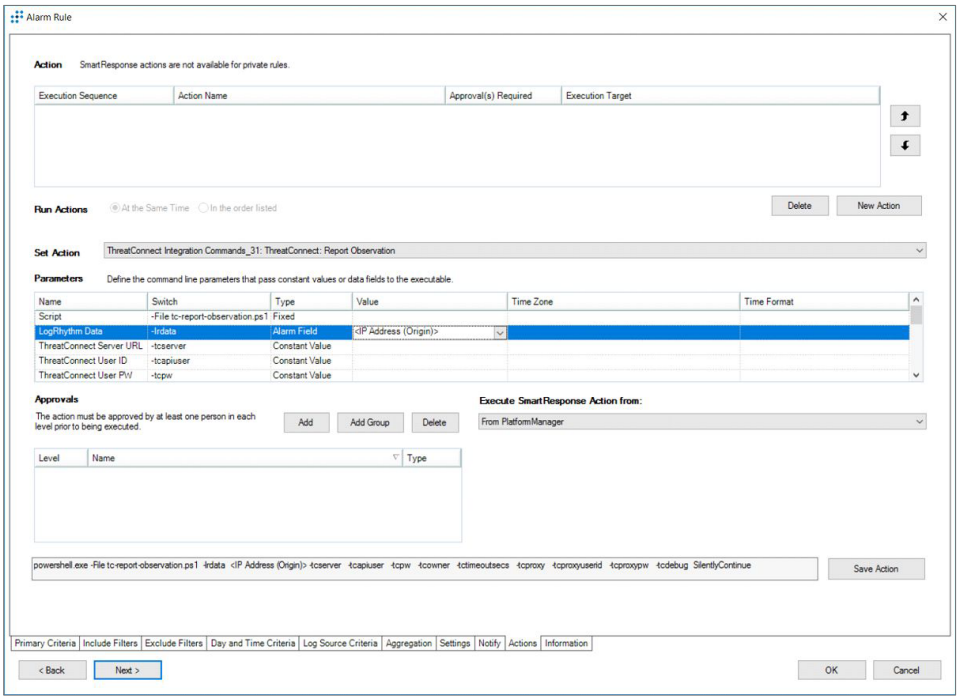

Figure 16

6. The rest of the tabs can be configured as needed for notifications, rule active time frames, etc. Please refer to LogRhythm documentation for full details.

Another way to use plugin actions is to run a SmartResponse Action within the web console to show more data about an Indicator:

1. Open the web console (dashboard) and log in. A screen similar to the one in Figure 17 will appear.

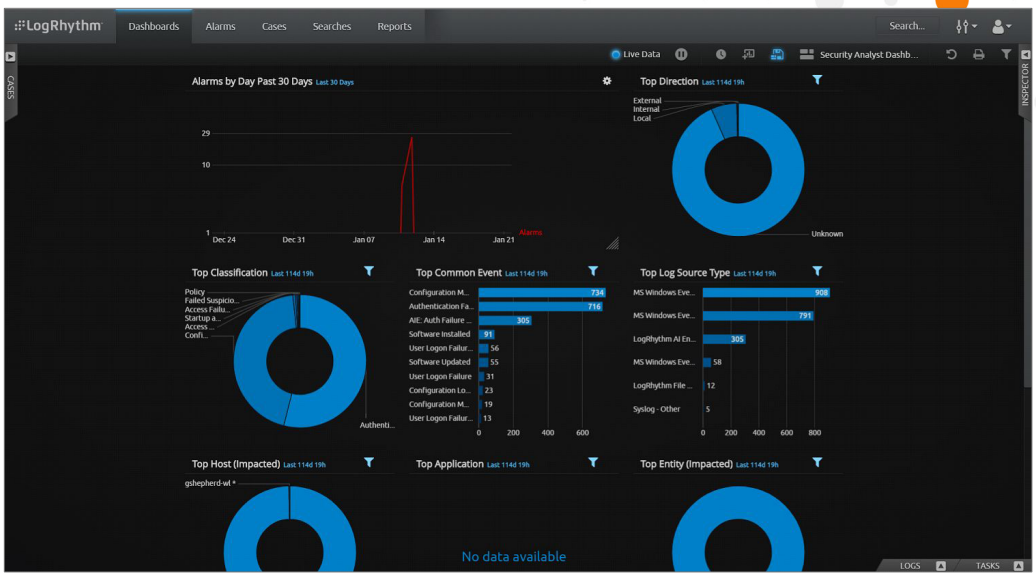

Figure 17

2. Click the **Logs** option in the bottom right-hand corner.
3. The resulting screen will show the events that have been captured. The columns can be filtered, marked as favorites, or displayed in themed groups (e.g., Application, Hosts, Location). The example in Figure 18 shows **IP Address (Origin)**, **IP Address (Impacted)**, and **Host (Impacted)** as favorite columns. It also displays the results of a filter that shows only log lines for which **IP Address (Origin)** is not blank.

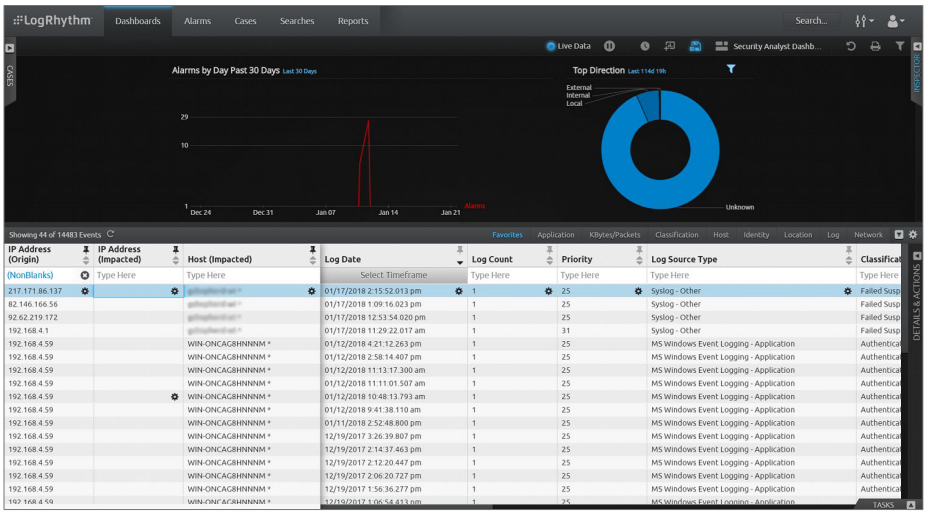

Figure 18

4. To find ThreatConnect information about a particular IP Address, select a cell on the row that contains the IP Address in question, and then click on one of the gear icons.
5. A panel will open on the right-hand side of the screen (Figure 19). Under the **Actions** tab, click the down arrow for the **SmartResponse** section. Then choose a plugin action that will show all the parameters to be passed. Make sure the **LogRhythm Data** field is filled in with the IP Address in question. LogRhythm will list all available options when that field is selected.

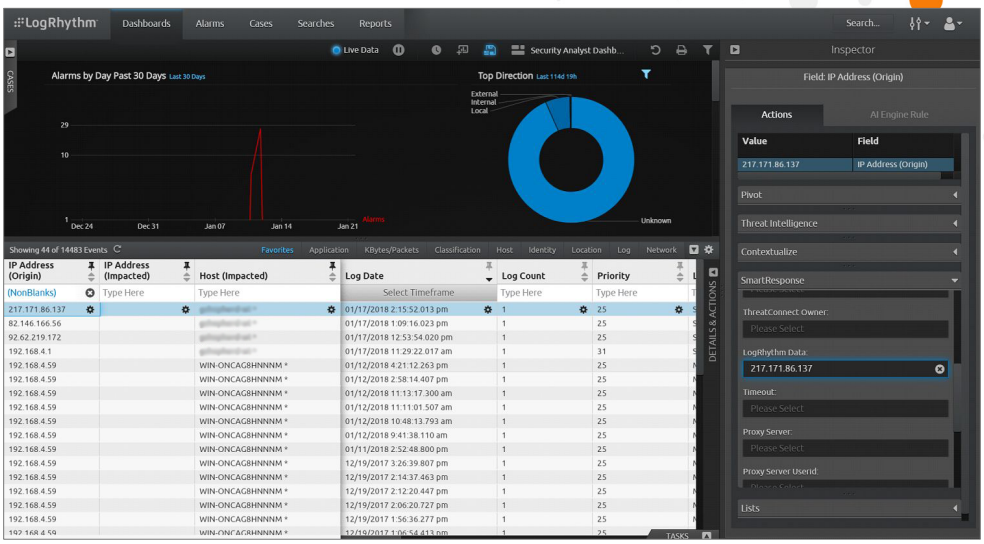

Figure 19

6. Scroll down to the bottom of the panel on the right-hand side of the screen, and click on the **Run** option (Figure 20).

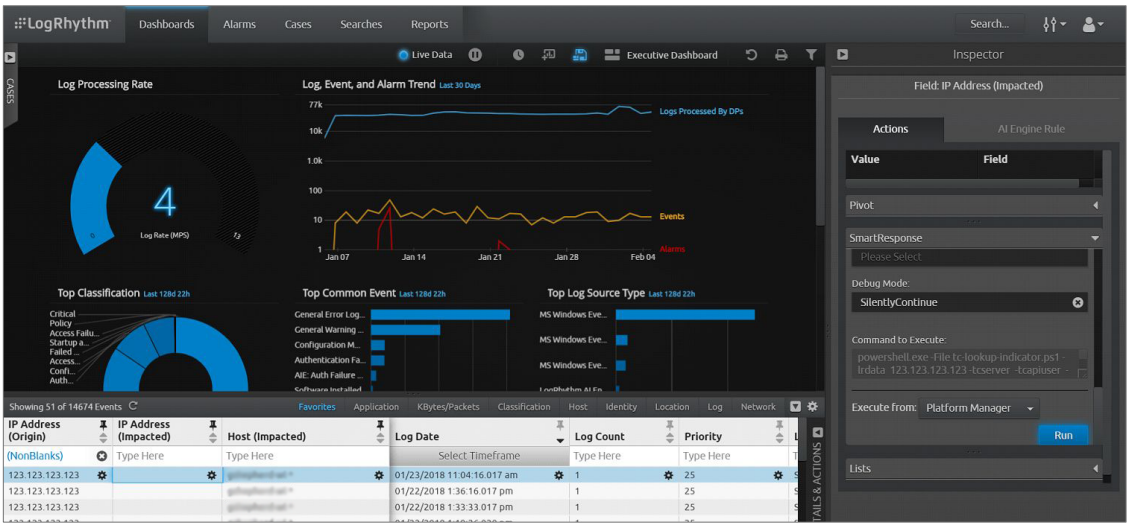

Figure 20

7. The results will open in a new browser tab (Figure 21).

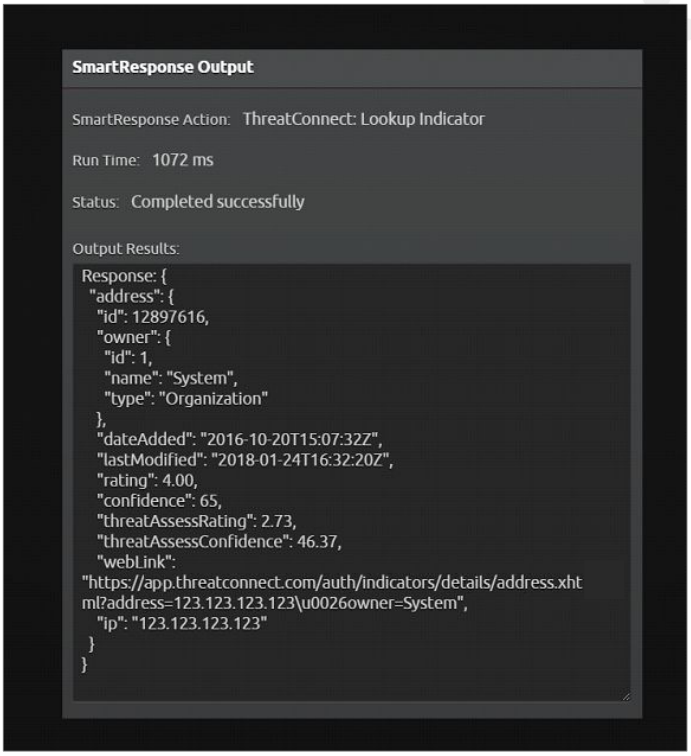
SmartResponse Output
SmartResponse Action: ThreatConnect: Lookup Indicator
Run Time: 1072 ms
Status: Completed successfully
Output Results:
Response: {
"address": {
"id": 12897616,
"owner": {
"id": 1,
"name": "System",
"type": "Organization"
},
"dateAdded": "2016-10-20T15:07:32Z",
"lastModified": "2018-01-24T16:32:20Z",
"rating": 4.00,
"confidence": 65,
"threatAssessRating": 2.73,
"threatAssessConfidence": 46.37,
"webLink":
"https://app.threatconnect.com/auth/indicators/details/address.xht
ml?address=123.123.123.123\u0026owner=System",
"ip": "123.123.123.123"
}
}

Figure 21