

ThreatQuotient



ThreatQuotient for LogRhythm Implementation Guide

Version 1.0.1

Thursday, March 12, 2020

ThreatQuotient

11400 Commerce Park Dr., Suite 200
Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2019 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Last Updated: Thursday, March 12, 2020

Contents

ThreatQuotient for LogRhythm Implementation Guide	1
Warning and Disclaimer	2
Contents	3
Introduction	5
Requirements	6
Versioning	6
Users	6
Pre-installation	7
Creating an API User for LogRhythm	7
Installing Python2	8
Installation	12
Recurring Execution: tq-logrhythym.exe	14
Configuration	18
Advanced Search Mapping	19
Lists	21
Smart Response Plugins	24
Installation of SRPs	25
Using a Smart Response Plugin	26

Using the ThreatQ Add Sighting	31
Uninstallation	35
Testing the LogRhythm Integration	37
Prerequisites	37
Testing Custom Connector (Sync)	37
Testing the SRP Actions (Contextual Actions)	38

Introduction

The LogRhythm integration is a single install Windows based python2 integration between ThreatQ and the LogRhythm Platform Manager (PM).

This integration uses 2 main integration points with LogRhythm, listed below:

- **Admin REST API:** This REST API (available as of 7.4.x) allows for the creation and management of Lists with LogRhythm using REST. Currently, ThreatQ leverages this to export data from Advanced Search Saved Searches to LogRhythm for use in correlations.
- **SmartResponsePlugins:** Several SmartResponsePlugins have been created to allow for the context of an IoC within ThreatQ to be exported to LogRhythm, and to allow LogRhythm to export context around detections back to ThreatQ.

The required version of LogRhythm for this integration to work is 7.4.x. This is due to the reliance on the Admin REST API.

Requirements

The following are requirements for the ThreatQuotient for LogRhythm integration.

Versioning

- LogRhythm Version 7.4.x or newer
- Python2 version 2.7.12 or newer installed on the LogRhythm Platform Manager



This integration is not compatible with Python3

- ThreatQ Version 4.23.0 or newer
- ThreatQ SDK Version 1.7 or newer (Installed Automatically)
- ThreatQ CC Version 1.3 or newer (Installed Automatically)
- Indicators loaded into the ThreatQ Appliance
- Saved Searches readied for export

Users

- LogRhythm API User - See the [Creating an API User for LogRhythm](#) section.
- ThreatQ User of at least Primary Contributor (User to generate saved searches with and to use as connection).
 - It is suggested to create a user for this purpose (username like log-rhythm@company.com).
 - Throughout the rest of this documentation, this user will be referred to as the "LogRhythm ThreatQ User" to differentiate it from admin level users.

Pre-installation

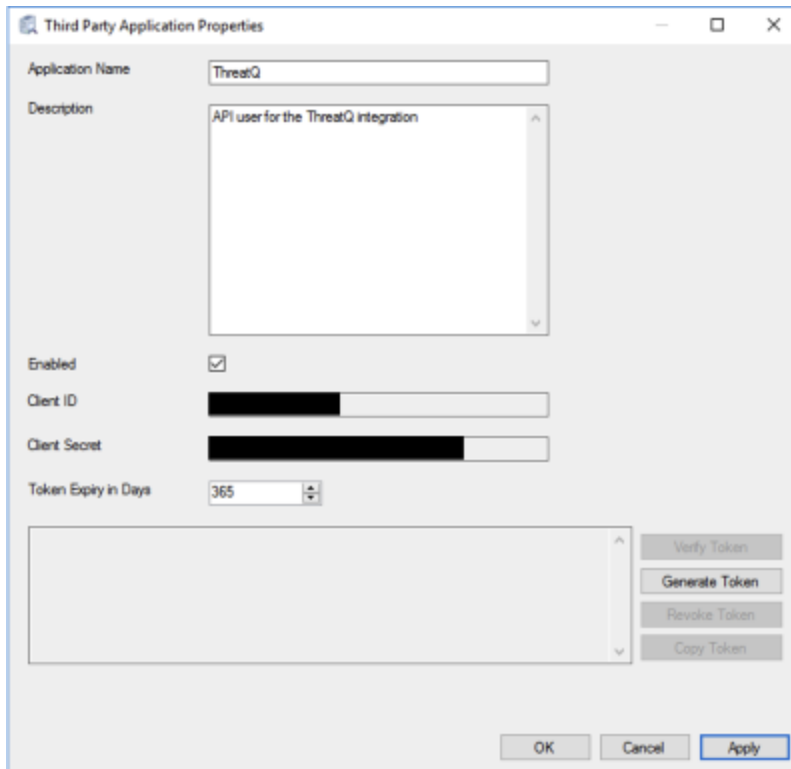
As noted in the [Requirements](#) section, this integration requires Python2 version 2.7.12 or later and a Log Rhythm API User. This section will provide the steps necessary to meet the requirements.

Creating an API User for LogRhythm

This section will describe how to create an API user to use with the ThreatQ integration.

1. Log into the VM where your LogRhythm instance is installed.
2. Open up your LogRhythm Console Within the LogRhythm Console.
3. Go to the Deployment Manager tab and then click on Third Party Applications.
4. Select the **Third Party Application** tab
5. Right click the page and select "New" to create a new app.

6. Configure your application like so:



7. Click **Generate Token** to generate a new JWT (token) to use for authentication



If the **Generate Token** button is greyed out, Apply your changes and re-open the properties dialog.

8. Copy the JWT down somewhere to use with the ThreatQ integration.

Installing Python2

If Python 2.7.12 or newer has not been installed on the Platform Manager, follow the instructions below to install Python 2.7.12 or newer.

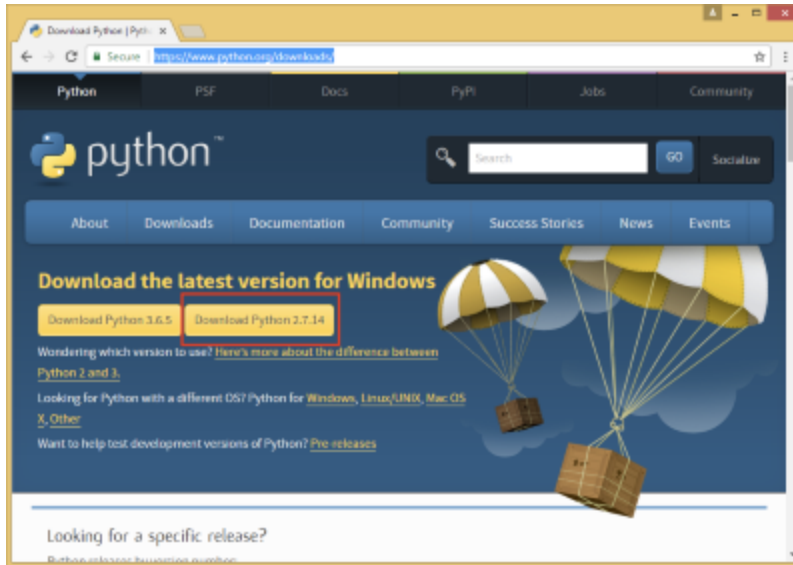


As of the release of this document, Python 2.7.14 is the newest Python2 version.

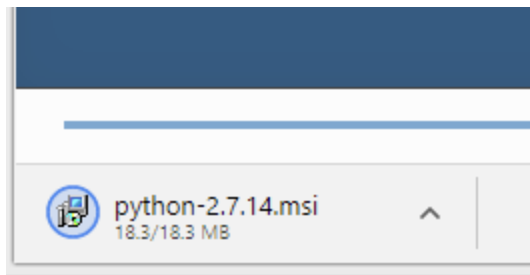


This integration is not compatible with Python3.

1. Navigate to The Python Downloads Page - <https://www.python.org/downloads/>.
2. Select **Download Python 2.7.X**.



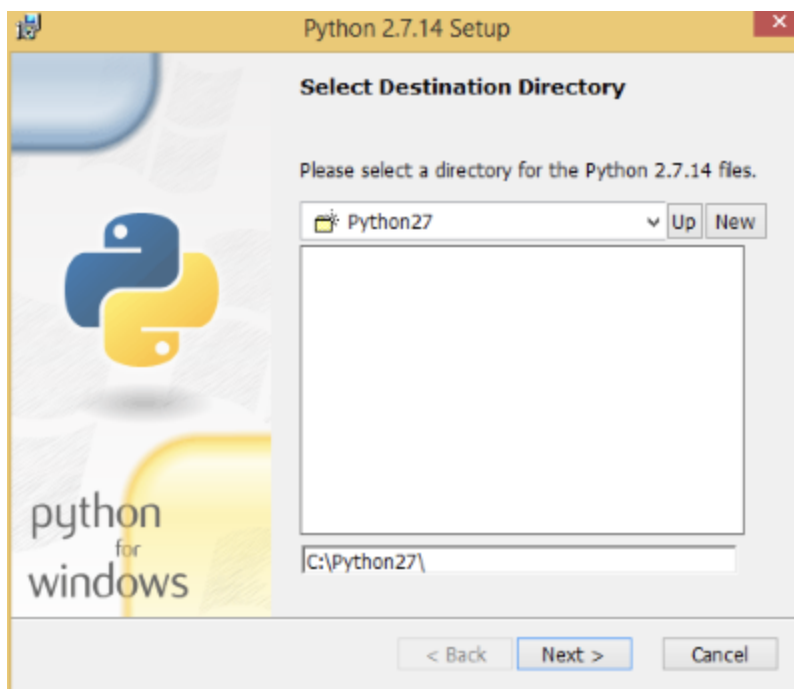
3. Click on the **Downloaded Python MSI**.



4. Select **Install for all users** and click **Next**.



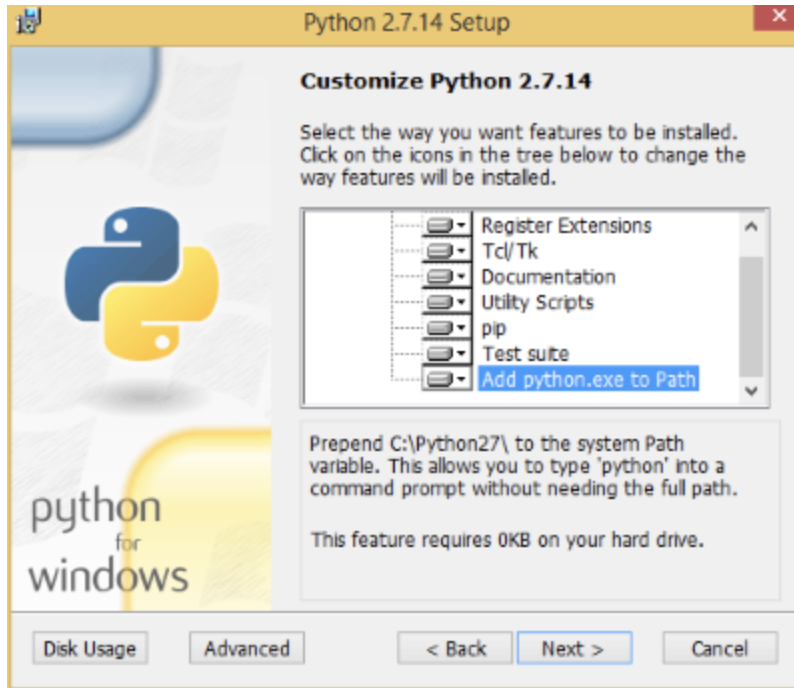
5. Select the installation location.





It is suggested that the default C:\Python27 is used.

6. Verify that **Add python.exe to Path** is selected and click **Next**.



7. Click on the **Finish** button after the installation is complete.

Once complete, you should be able to navigate to C:\Python27 and execute the python program



Type `exit()` to exit the shell.

Installation

The command `pip` is used to install the ThreatQ Integration on the LogRhythm server.

To install this, open a command prompt `Windows Key + R: cmd` as an administrator.

The instructions below assume that Python 2.7.12 or newer has been installed on the system. If it has not, please refer to the [Installing Python2](#) section.



Python must be installed in the Python27 directory for this to operate correctly. If another installation directory is used, replace `C:\Python27` with the correct directory. A specific SRP bundle will have to be generated for this configuration. Contact support@threatq.com.

1. Log into the VM where LogRhythm is installed.
2. Open the command line from the start menu.
3. Navigate to the Python Directory `C:\Python27`.
4. Navigate to the **Scripts** directory.
5. Execute the following command:

With Internet Access

If your LogRhythm instance has access to the internet:

```
pip install -i  
https://<USERNAME>:<PASSWORD>@extensions.threat  
q.com/threatq/integrations tqLogRhythm
```



<USERNAME> and <PASSWORD> are the username and password used to get updates from ThreatQ on the main appliance (The ThreatQ Credentials entered during setup).

This will install several command line tools.

Without Internet Access

Download the installable with its dependencies on an instance with access to the internet, transfer all the files to LogRhythm, and run pip install:

```
mkdir /tmp/logrhythm

pip download tqLogRhythm -d /tmp/logrhythm
```

Transfer the tqLogRhythm whl, and its dependencies to the LogRhythm instance in the Downloads folder.

```
pip install C:\Downloads\tqLogRhythm-1.0.1-py2-
none-any.whl --no-index --find-links
C:\Downloads
```

6. Optional - Add `C:\Python27` to your Windows Path. This will allow you to execute commands without having to specify the directory.
7. Create a new folder in your **Log Files** disk called **ThreatQ**.

Example Path: L:\ThreatQ

8. Check if there is a route to ThreatQ from LogRhythm.




Do not continue past this point until you have confirmed that LogRhythm can reach ThreatQ.

```
C:\ping <ThreatQ Host>
```

9. Execute the following command:

```
C:\Python27\Scripts\tq-logrhythm.exe -ll  
L:\ThreatQ\ -v 3
```

10. Complete the following fields:

Field	Description
ThreatQ Host	This is the hostname or IP Address of the ThreatQ appliance.
ClientID	This is the OAuth Client ID, found by going to Gear → OAuth Credentials in the ThreatQ Appliance.
Email Address	The e-mail address of the LogRhythm ThreatQ User.
Password	The password of the LogRhythm ThreatQ User.
Status	<div>The status of newly created IoCs.  It is recommended to select the Active status.</div>

Once complete, the configuration will be stored in `HKEY_LOCAL_MACHINE\Software\ThreatQuotient\LogRhythm` and will be available to this system

Once the system has been installed on the LogRhythm Platform Manager, the user must configure the integration in the ThreatQ UI.

Recurring Execution: tq-logrhythym.exe

One of the commands provided during the installation is the `tq-logrhythm.exe` command. This command is what is used to read the configuration set in the UI of the ThreatQ

appliance, generate, and maintain lists.

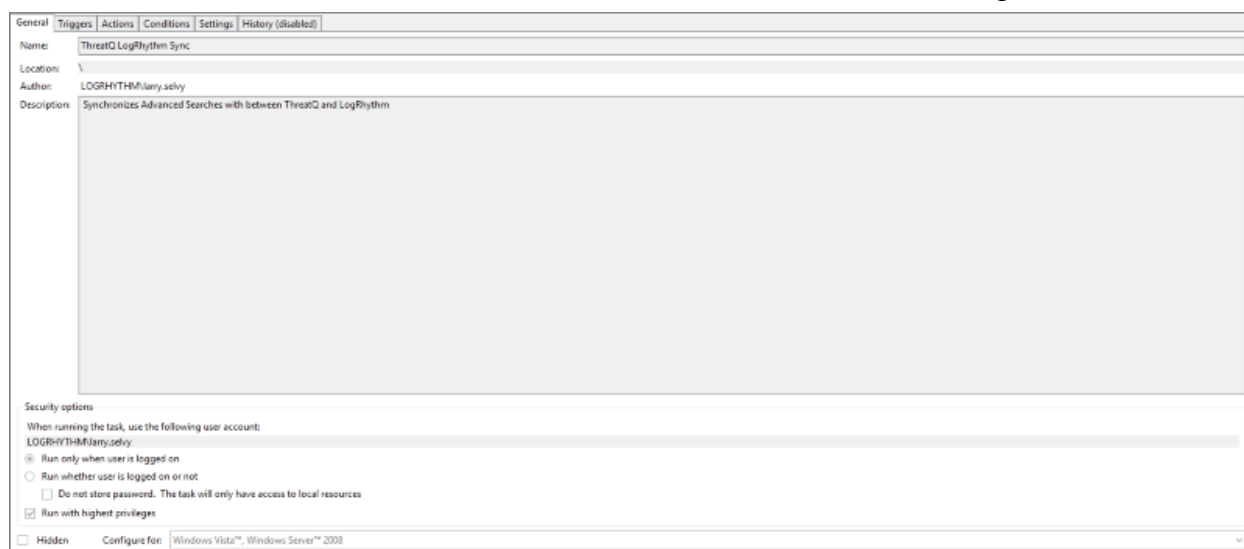
During the execution of tq-logrhythm.exe, the UI fields are read, lists are created, and all lists are compared against what is in the content of the Advanced Search Saved Searches - see the [Advanced Search Mapping](#) section.

Each Indicator of Compromise listed in the Saved Advanced Search is compared to the contents of the associated list. If the IoC is not in the list, it is added during the Synchronization step.

When each IoC has been compared to the list, those IoCs which are no longer in the Advanced Search Saved Search, but are in the list in LogRhythm, are tagged for deletion during the Synchronization step.

Finally, each list is Synchronized.

This must be setup on a recurring basis to keep the data in the lists synchronized to the data in the Advanced Searches. To do this, use the Task Scheduler, and configure it as below:



The screenshot shows the 'General' tab of a Windows Task Scheduler task. The task name is 'ThreatQ LogRhythm Sync'. The location is set to the root of the drive (represented by a backslash). The author is 'LOGRHYTHM\jany.schly'. The description is 'Synchronizes Advanced Searches with between ThreatQ and LogRhythm'. Under 'Security options', the user account 'LOGRHYTHM\jany.schly' is specified. The task is configured to 'Run only when user is logged on', with the option to 'Do not store password' selected. The 'Run with highest privileges' checkbox is checked. The 'Hidden' checkbox is unchecked, and the task is configured for 'Windows Vista™, Windows Server™ 2008'.

General
Triggers
Actions
Conditions
Settings
History (disabled)

When you create a task, you can specify the conditions that will trigger the task. To change these triggers, open the task property pages using the Properties command.

Trigger	Details	Status
Daily	At 6:26 PM every day - After triggered, repeat every 1 hour for a duration of 1 day.	Enabled

General
Triggers
Actions
Conditions
Settings
History (disabled)

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

Action	Details
Start a program	C:\Python27\Scripts\lq-logrhythm.exe -ll C:\Python27\Scripts\ -v 3

General Triggers Actions Conditions Settings History (disabled)

Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition specified here is not true. To change these conditions, open the task property pages using the Properties command.

Idle

☐ Start the task only if the computer is idle for: 10 minutes

Wait for idle for: 1 hour

☒ Stop if the computer ceases to be idle

☐ Restart if the idle state resumes

Power

☒ Start the task only if the computer is on AC power

☒ Stop if the computer switches to battery power

☒ Wake the computer to run this task

Network

☐ Start only if the following network connection is available:

Any connection

General Triggers Actions Conditions Settings History (disabled)

Specify additional settings that affect the behavior of the task. To change these settings, open the task property pages using the Properties command.

☒ Allow task to be run on demand

☐ Run task as soon as possible after a scheduled start is missed

☒ If the task fails, restart every: 10 minutes

Attempt to restart up to: 3 times

☒ Stop the task if it runs longer than: 1 hour

☒ If the running task does not end when requested, force it to stop

☐ If the task is not scheduled to run again, delete it after: 30 days

If the task is already running, then the following rule applies:

Stop the existing instance



Each list can only have up to 1 Million IoCs in it. Any more than this and the system will be unable to synchronize correctly

The time that this repeats is at the discretion of the user, but should be no shorter than once every hour.

Other schedulers can be used, the syntax of the command above should be used in whatever scheduler is provided.

Configuration

To configure the LogRhythm feed:

1. Click on the **Settings** icon and select **Incoming Feeds**.
2. Locate the feeds under the **Labs** tab.
3. Click on the **Feed Settings** link for the feed.
4. Under the **Connection** tab, enter the following configuration parameters:

Parameter	Details
LogRhythm Host	The Hostname or IP Address of the LogRhythm Platform Manager.
LogRhythm Admin/Case API Port	This is port 8501 by default, and should not have to change. This is the port of the REST API not the SOAP API.
JW Token	This is the token that was generated during the creation of the LogRhythm API User (See this article if you need help creating this token)
Advanced Searches	This is the mapping of advanced searches to LogRhythm lists, explained in detail in the Advanced Search Mapping section of this document.

- 5.
6. Click on **Save Changes**.
7. Click on the toggle switch to the left of each feed name to enable the feed.

At this point, log out of ThreatQ as the Admin user and log into the appliance with the LogRhythm ThreatQ User. Go to the magnifying glass and click **Advanced Search**. Once in the advanced search menu, generate a search that you would like to export to LogRhythm. When this is done, save the search by going to **Recent Searches**, selecting the search

created for export, and click **Save**. Remember the name of the saved search as it will be used later.

Advanced Search Mapping

This section explains how to configure an Advanced Search mapping. This is a YAML file. It is assumed that an Advanced Search Saved Search has already been generated. If one has not, please see the [Configuration](#) section.

1. Delete the filler text that exists, except for the top three - characters.
2. Once cleared each new line should consist of the name of an Advanced Search Saved Search (generated by the user configured in the [Configuration](#) section), a list basename, and optional splitting parameters. The syntax is as follows:

```
---  
Interesting IoCs: "ThreatQ: "
```

In the line above, Interesting IoCs is the name of an Advanced Search Saved Search. The phrase "ThreatQ: " is the basename of a family of lists. All of the lists will start with the term ThreatQ: and then have the specific indicator type. For instance, FQDNs in the above list will be put into the ThreatQ: FQDN list, IP Addresses will be in the ThreatQ: IP Address list, and so on.



The splitting of IoCs into their specific indicator types is a best practice for LogRhythm, and is enforced in this integration

3. Further splitting of lists is allowed by specifying a splitBy parameter, as below:

```
---  
Interesting IoCs:  
    baseName: "ThreatQ: "  
    splitBy: scoreRange
```

This will have a similar affect above, except that it will create one more level of list. For instance, FQDNs in the above saved search, Interesting IoCs, will be saved by score range in the following lists:

- ThreatQ: FQDN: Very High
- ThreatQ: FQDN: High
- ThreatQ: FQDN: Medium
- ThreatQ: FQDN: Low
- ThreatQ: FQDN: Very Low
- ThreatQ: FQDN: Not Scored

The above lists will only be created if an FQDN of that level is in the saved search. For instance, if no Medium FQDNs are in the saved search, there will be no ThreatQ: FQDN: Medium list. At any point in the future, these will be added as necessary.

Other splitBy parameters are below:

Parameter	Details
splitBy: score	Similar to the scoreRange, except that lists are broken out by specific score (1-10).
splitBy: scoreRange	Lists are broken out by the score range on the landing page of the appliance.
splitBy: tqtype	This is the default, and breaks out lists by indicator type only.

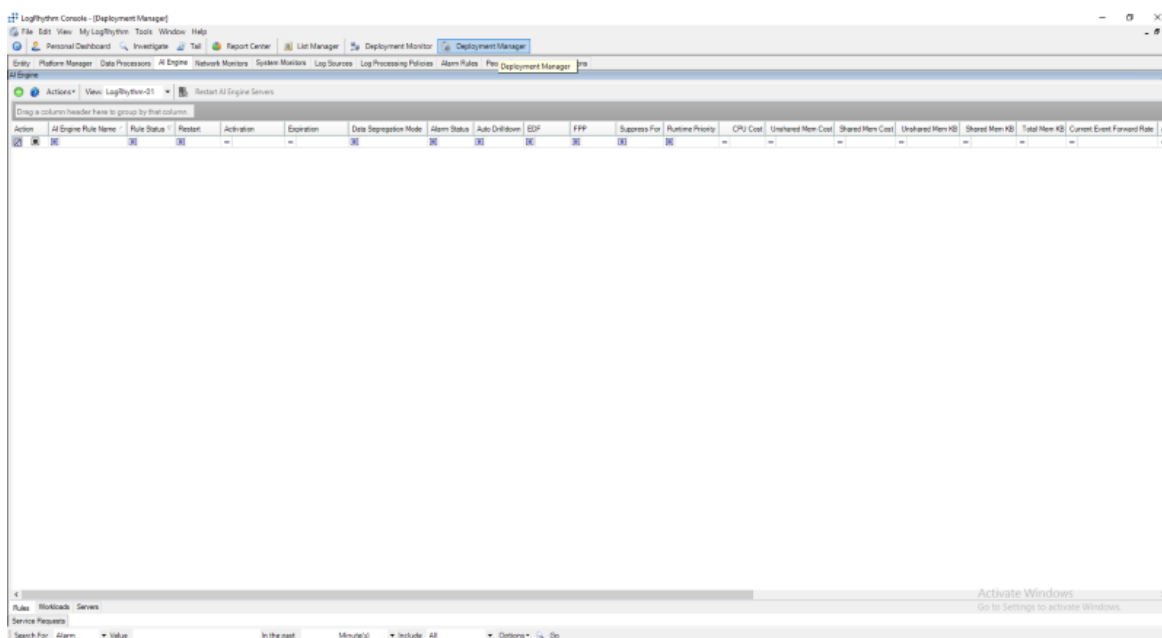
Lists

LogRhythm Lists are the primary interface for which Cyber Threat Intelligence data is stored and used in LogRhythm. These lists can come from many different locations, and can store many different data types. For the purpose of ThreatQ, lists will be dynamically generated at execution time based on configurations given on the "Incoming Feeds" page of ThreatQ. (Gear → Incoming Feeds → TQ Labs → LogRhythm).

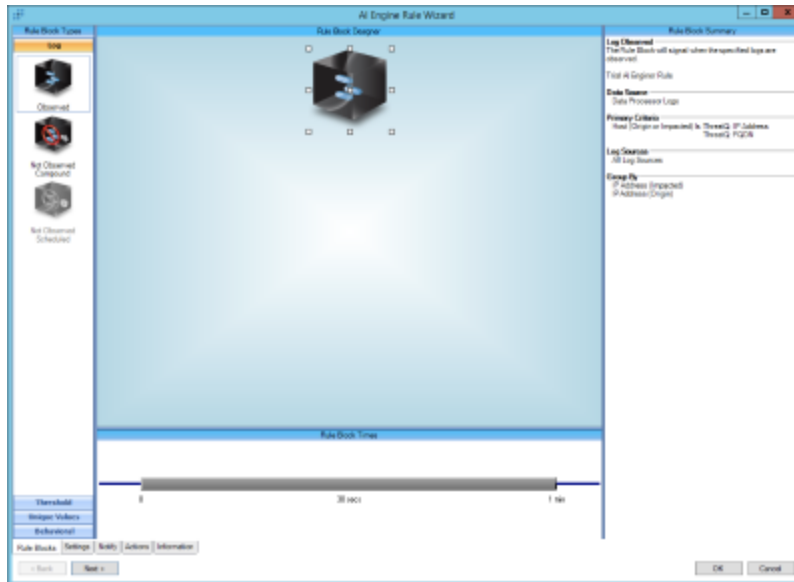
These lists can be used in conjunction with the LogRhythm AI Engine to determine correlations against incoming log data.

To configure the list to be used in the AI, do the following:

1. Open Deployment Manager and go to the **AI Engine** tab.
2. Click on the green + button in the toolbar.

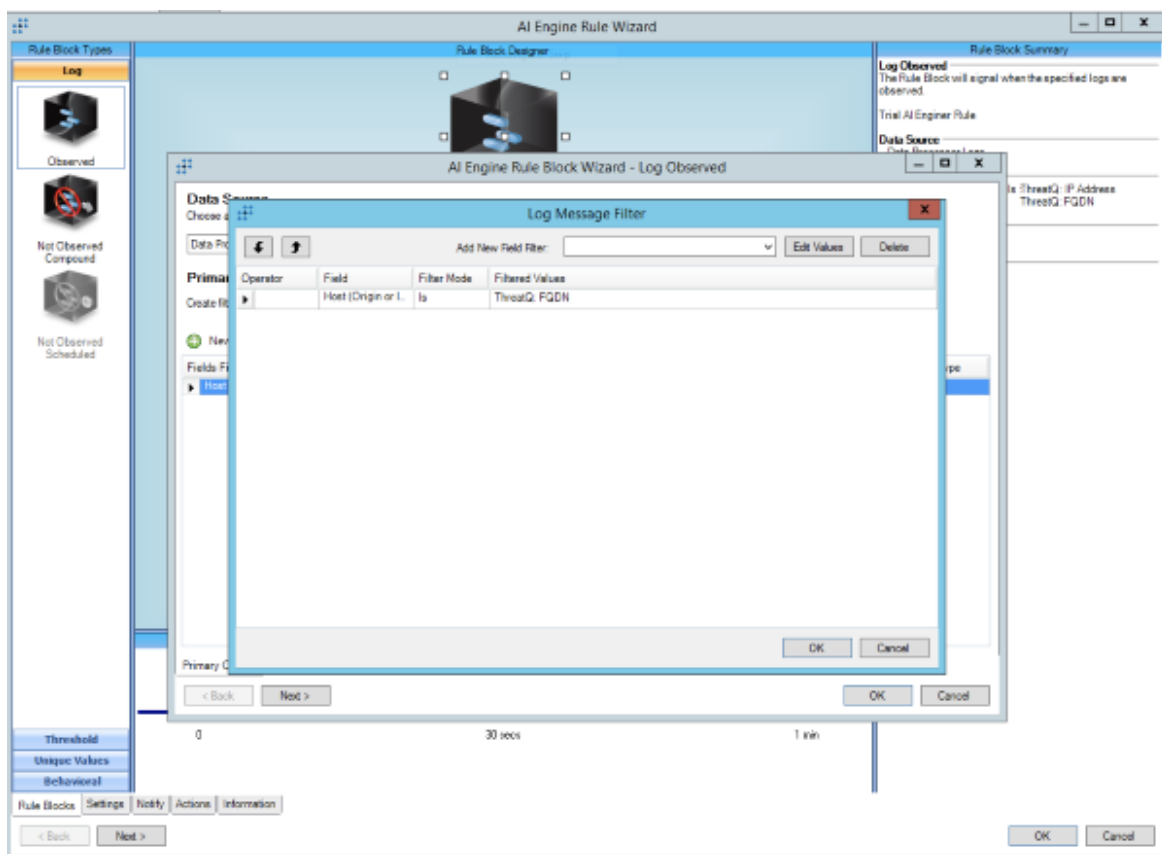


- When the AI Engine Rule Wizard opens, select the **Observed** block on the Log Section.



- Configure it as needed for detection of Cyber Threat Events. In the example given here, the Host (Origin or Impacted) Field must be in the **ThreatQ: FQDN** list. The

list names and fields will vary based on the purpose of the rule.



5. Go through the rest of the Wizard and select the required settings based on your Incident Response Manifesto

Once saved and the AI Engine Service restarted, any Log that has a host field with an Origin or Impacted Host in the **ThreatQ: FQDN** list will have the associated log alerted on.

For more information on the AI Engine and its possibilities, please consult the LogRhythm Client Console Reference Guide in the LogRhythm Administration → AI Engine Section.

Smart Response Plugins

LogRhythm allows for tools to be added to the platform to enrich data within LogRhythm. Using these tools, IoCs can also be enriched within ThreatQ. The following SmartResponsePlugins are provided with the installation. All of the can be found in the C:\Python27\Scripts directory:

Name of SRP Executable	Name of SRP Action	Description	Enrichment Destination
tq-whitelist-ioc.exe	ThreatQ Whitelist IoC	This changes the status to "Whitelisted" for an IoC within ThreatQ.	Enriches ThreatQ
tq-sight-ing.exe	ThreatQ Add Sighting	This creates a "Sighting" event within ThreatQ that associates IoCs with the LogRhythm AI Engine Event.	Enriches ThreatQ
tq-mark-true-positive.exe	ThreatQ Mark True Positive	Adds an attribute of "True Positive" with a value "Yes" to the IoC within ThreatQ. If the IoC does not exist, this will add it. This is meant to be used during score calculations.	Enriches ThreatQ
tq-mark-false-positive.exe	ThreatQ Mark False Positive	Adds an attribute of "False Positive" with a value "Yes" to the IoC within ThreatQ. If the IoC does not exist, this will add it. This is meant to be used during score calculations.	Enriches ThreatQ
tq-look-up.exe	ThreatQ Lookup IoC	Searches the ThreatQ Threat Library for an indicator with the same type and value as the indicator provided	Enriches LogRhythm

Name of SRP Executable	Name of SRP Action	Description	Enrichment Destination
tq-add-ioc.exe	ThreatQ Add IoC	Adds an IoC of the same type and value to ThreatQ from LogRhythm. If the IoC already exists, it adds LogRhythm as a source	Enriches ThreatQ

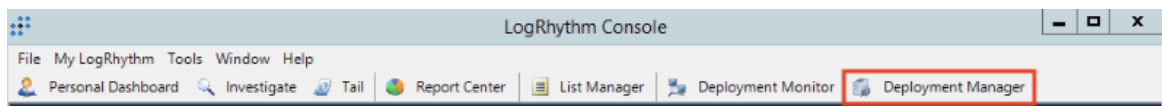
Installation of SRPs

The SPR executables are installed during the original installation of the integration.

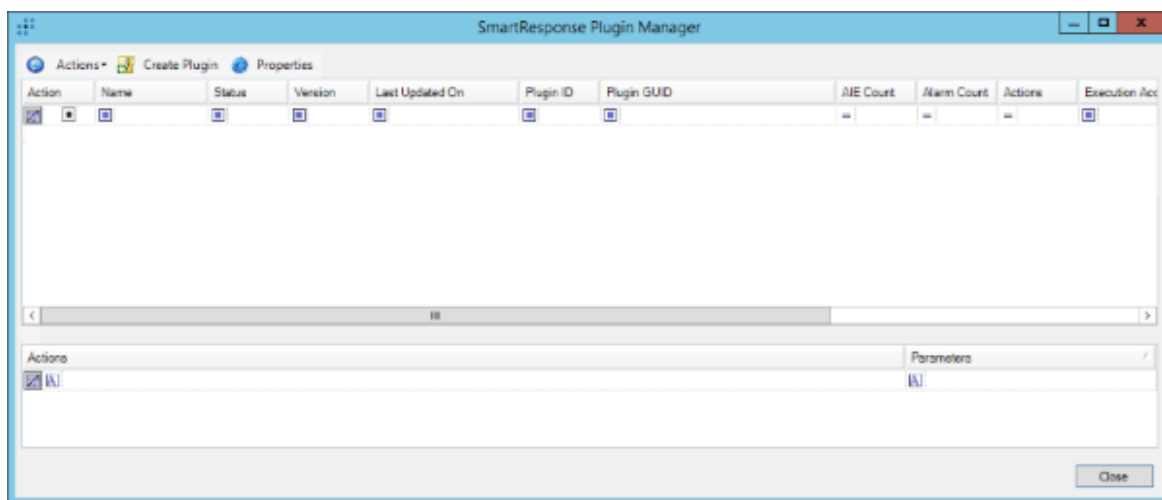
However, to enable these within LogRhythm to be used in the Client or Web Consoles, the SRP bundle has to be added. The bundle is presented as an all in one.

To install the SRP bundle:

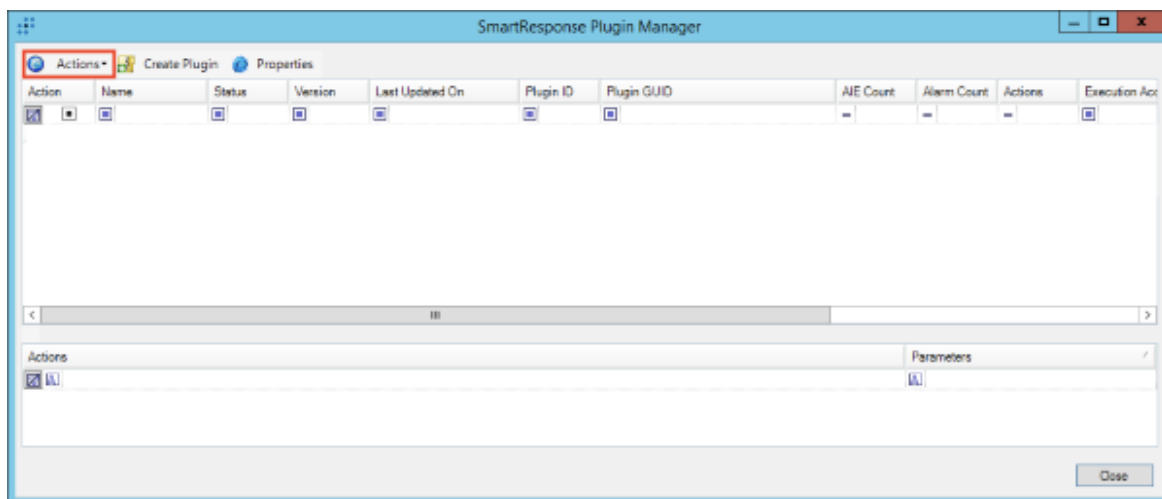
1. Open the Deployment Manager.



2. Go to Tools → Administration → SmartResponse Plugin Manager.

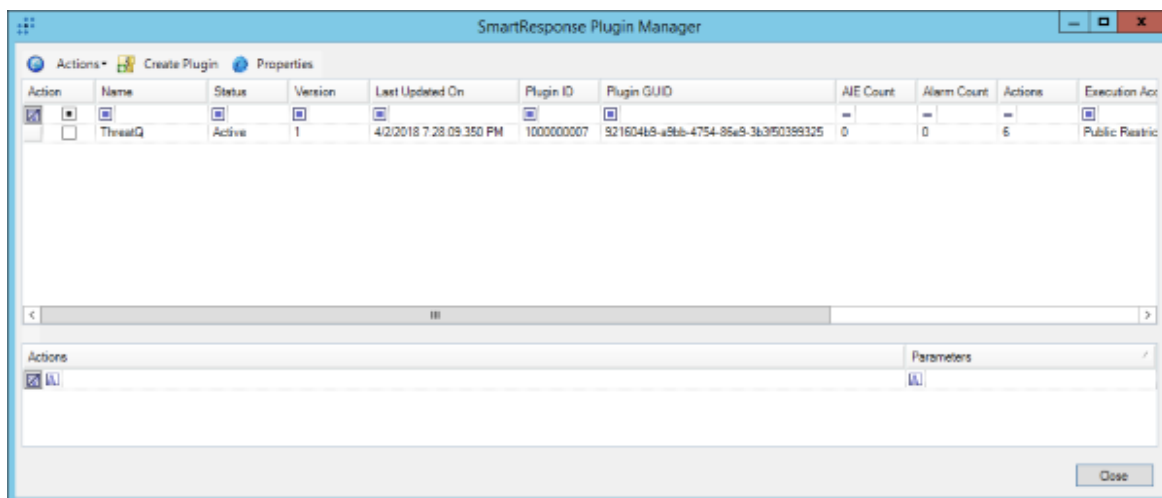


3. Click on the **Actions** button .



4. Navigate to the ThreatQ SRP bundle and click **Open**.

Once complete, the ThreatQ Smart Response Plugins list found in [Smart Response Plugins](#).

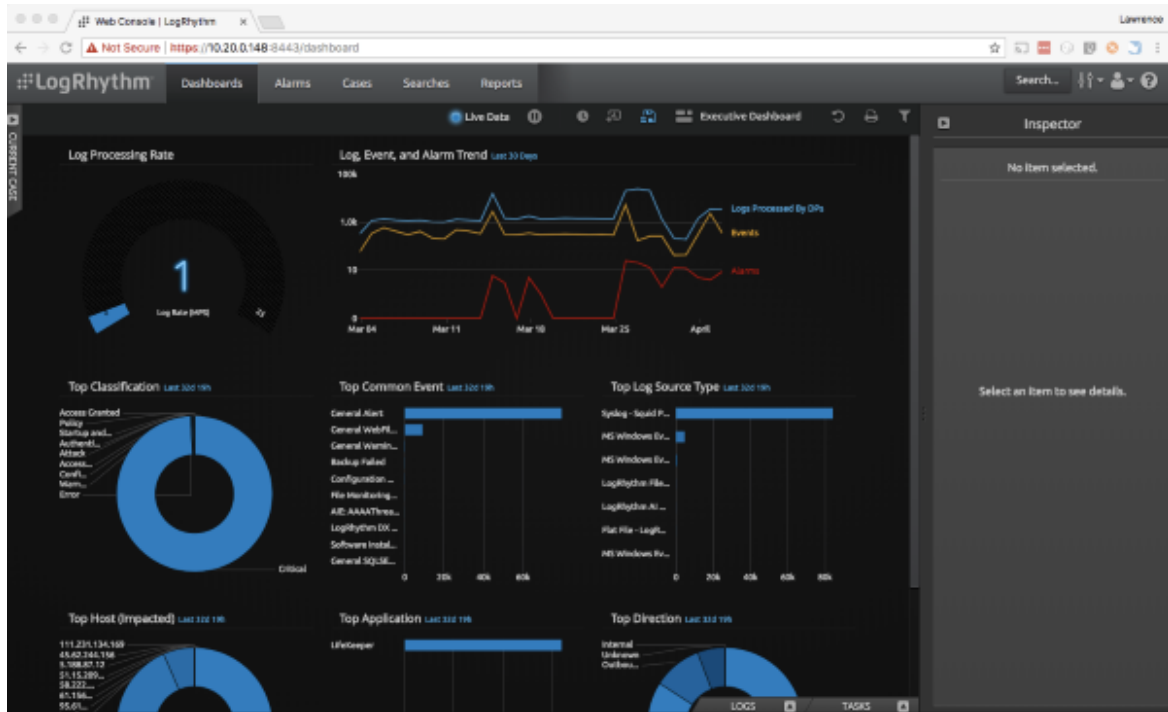


Using a Smart Response Plugin

There are several ways in which a Smart Response Plugin can be used. The first is to configure it as part of an AI Engine Rule. This will not be covered in this documentation as it is covered in depth in the LogRhythm Client Console Reference in the LogRhythm

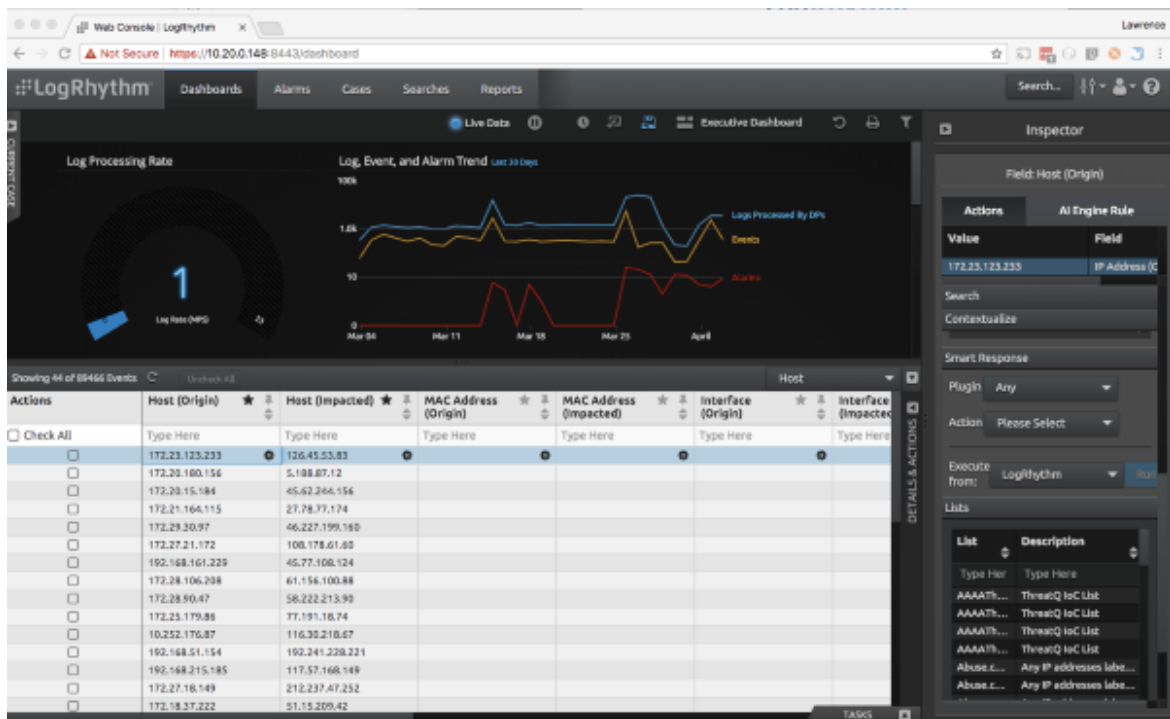
Administration → AI Engine Section. This section will focus on using the SRPs in the Web Console.

1. Log into the Web Console.



2. Open up the "Logs" pane and Navigate to a log entry that is interesting.

3. Open the "Inspector" pane if it is not already open.

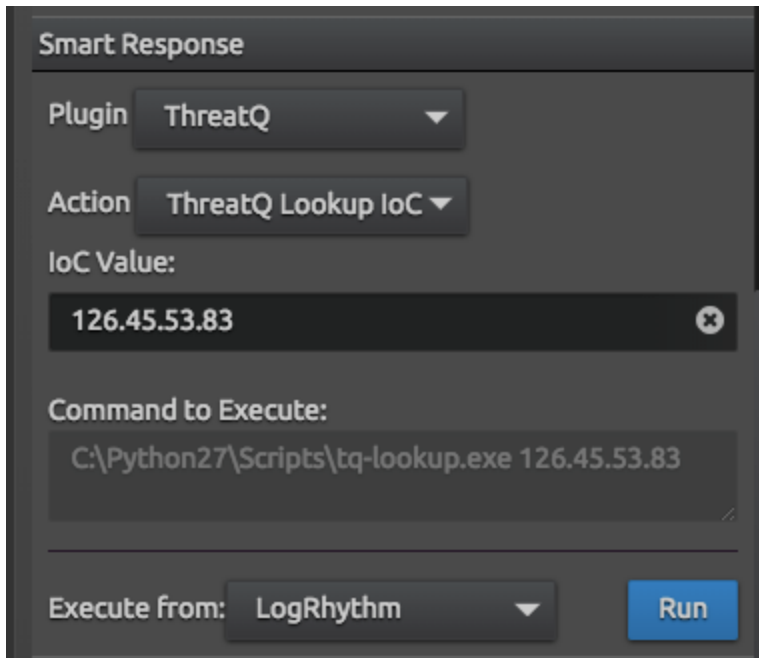


The screenshot shows the LogRhythm web interface. The main dashboard area includes a 'Log Processing Rate' gauge showing a value of 1, and a line chart titled 'Log, Event, and Alarm Trend' showing data from March 8 to April. The 'Inspector' pane on the right is active, displaying the 'Field: Host (Origin)' with a value of '172.23.123.233' and an action of 'IP Address (C)'. Below this, there are sections for 'Smart Response' and 'Lists'.

Host (Origin)	Host (Impacted)	MAC Address (Origin)	MAC Address (Impacted)	Interface (Origin)	Interface (Impacted)
Type Here	Type Here	Type Here	Type Here	Type Here	Type Here
172.23.123.233	126.45.53.83				
172.23.180.156	5.188.87.12				
172.23.15.184	45.62.246.156				
172.21.164.115	27.78.37.174				
172.29.30.97	46.227.199.169				
172.27.21.172	108.178.61.60				
192.168.161.229	45.77.108.124				
172.28.106.238	61.156.100.88				
172.28.90.47	58.222.213.99				
172.25.179.86	77.191.18.74				
10.252.176.87	116.39.218.67				
192.168.51.154	192.241.228.221				
192.168.215.185	117.57.168.149				
172.27.18.149	212.237.47.252				
172.18.37.222	51.15.209.42				

4. In the Inspector Pane, Navigate to "Smart Response."
 - a. Choose "Plugin: ThreatQ"
 - b. Choose the appropriate Action (in this example it will be the ThreatQ Lookup IoC Action).
5. Fill in the appropriate Values (here an IP address is used).

6. Ensure "Execute from: LogRhythm" is selected.



The screenshot shows the "Smart Response" configuration window. It has a dark grey background with white text. At the top, the title "Smart Response" is in a bold font. Below the title, there are two dropdown menus: "Plugin" set to "ThreatQ" and "Action" set to "ThreatQ Lookup IoC". Below these, the "IoC Value:" is displayed in a text box with the value "126.45.53.83" and a small "x" icon to its right. Underneath, the "Command to Execute:" is shown in a text box with the command "C:\Python27\Scripts\tq-lookup.exe 126.45.53.83". At the bottom, there is an "Execute from:" dropdown menu set to "LogRhythm" and a blue "Run" button.

Smart Response

Plugin ThreatQ ▼

Action ThreatQ Lookup IoC ▼

IoC Value:

126.45.53.83 ✕

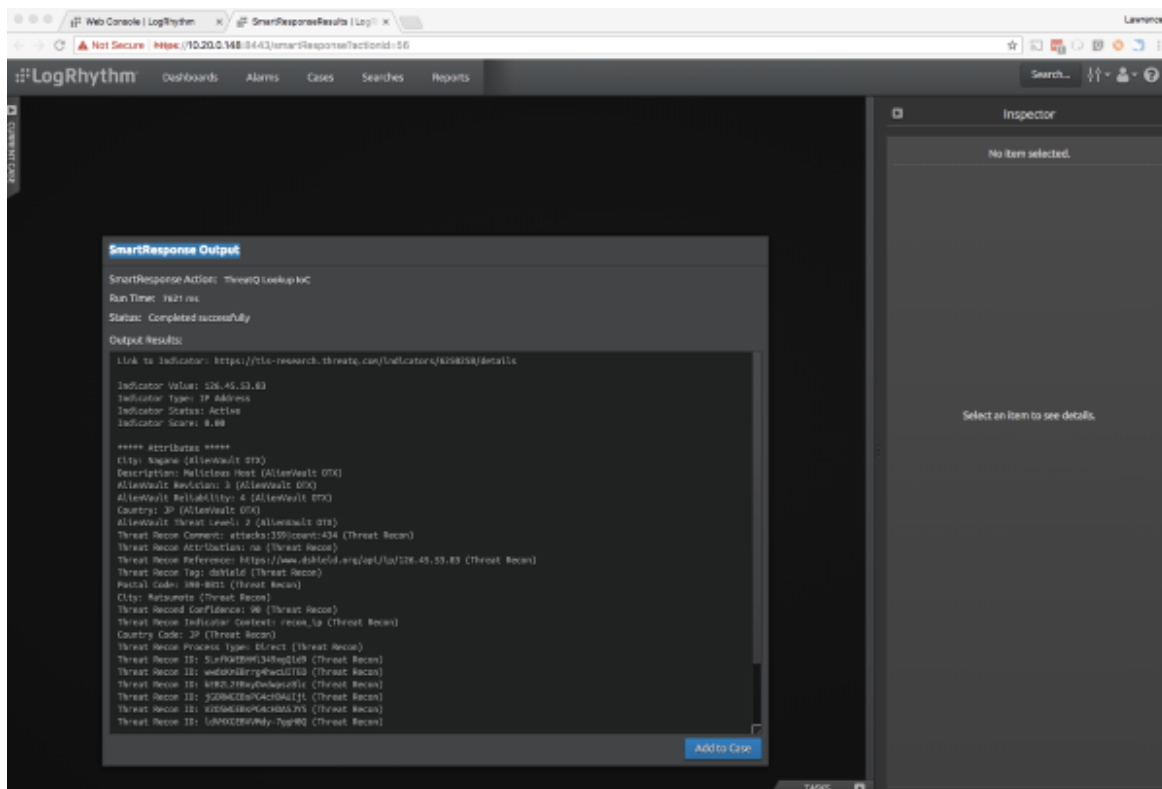
Command to Execute:

C:\Python27\Scripts\tq-lookup.exe 126.45.53.83

Execute from: LogRhythm ▼ Run

7. Click Run.

At this point LogRhythm will execute action in a separate window, retuning the results.



If a case is currently selected, this can be added to the case by clicking the **Add to Case** button. If it is added to a case, it will appear in that case as Evidence.



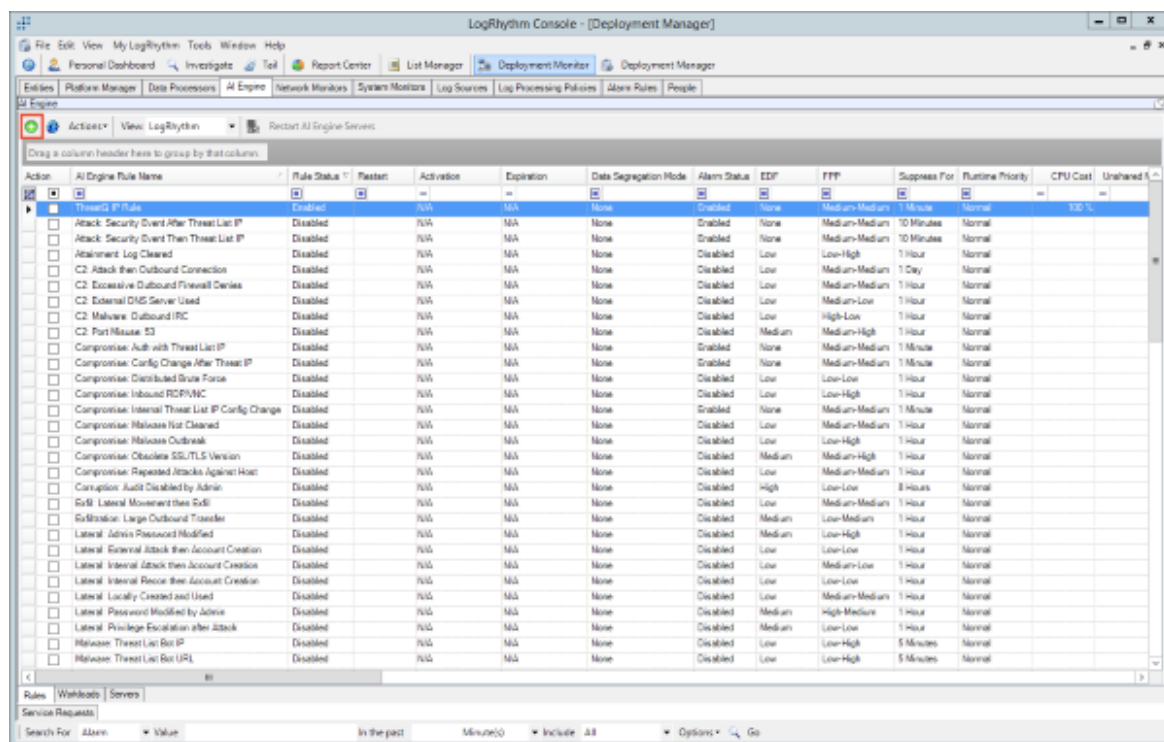
The ThreatQ Add Sighting action is accessible through this interface, but is not usable here. This action is to be used only in the Client Console when configuring AI Engine Rules. This is used to bring over a Case as a "Sighting" type Event in ThreatQ, including the observed IoCs.

Using the ThreatQ Add Sighting

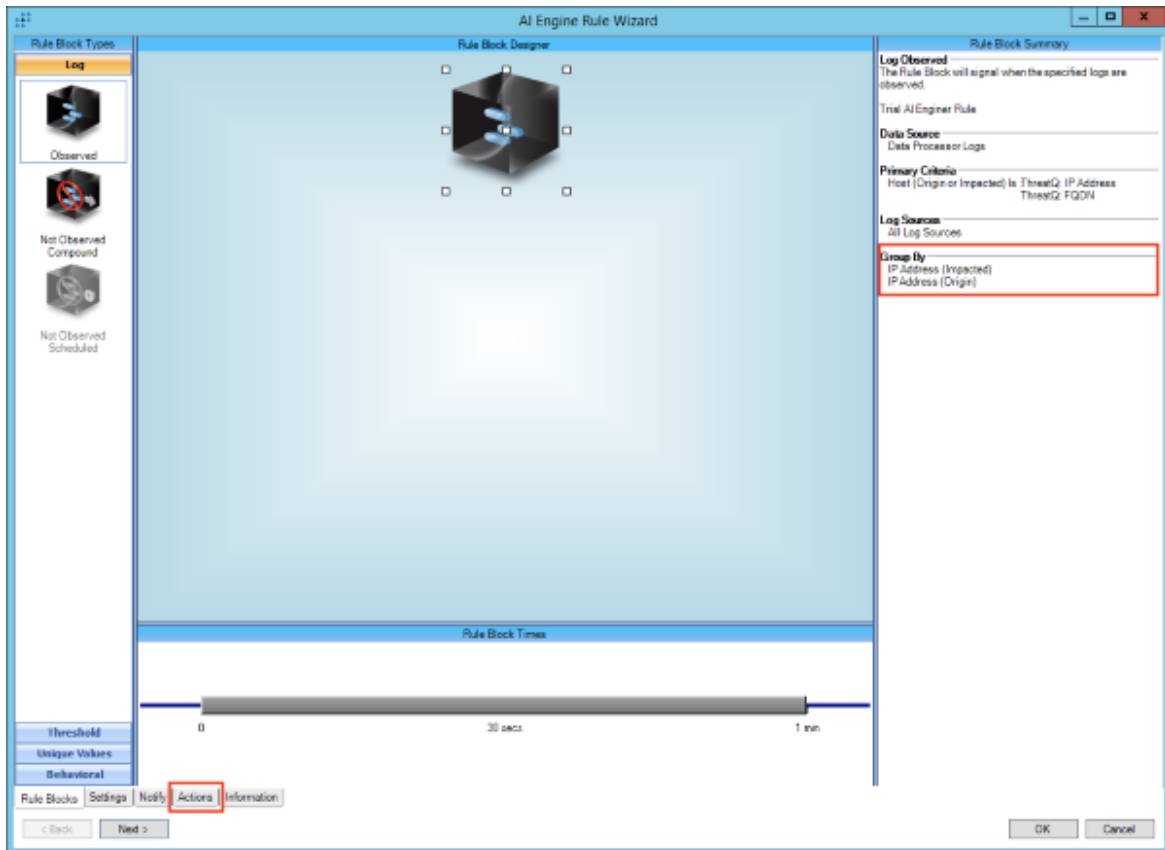
Tracking the sighting of Indicators of Compromise is an integral piece in the Threat Intelligence feedback loop. This feedback loop alerts Threat Analysts to existence of known Indicators of Compromise that have been observed in LogRhythm. Unlike the other SRPs provided above, this SRP is designed to solely be used as part of an AI Engine rule. When this rule is triggered, it creates an Event within ThreatQ with a type of "Sighting". These sightings have the AlarmID, Alarm Name, and other pieces of information configurable in the AI Engine in the LogRhythm Client Console.

To provide the most flexible solution to capture all possible Sightings, the ThreatQ Add Sighting SRP has options for all known IoC fields. To add a rule that has uses this SRP:

1. Open Deployment Manager and go to the "AI Engine" tab.
2. Click on the Green "+" Button in the toolbar or navigate to the rule you wish to edit, select it, right click and select edit.



3. Configure the rule as needed, when complete select the actions tab.

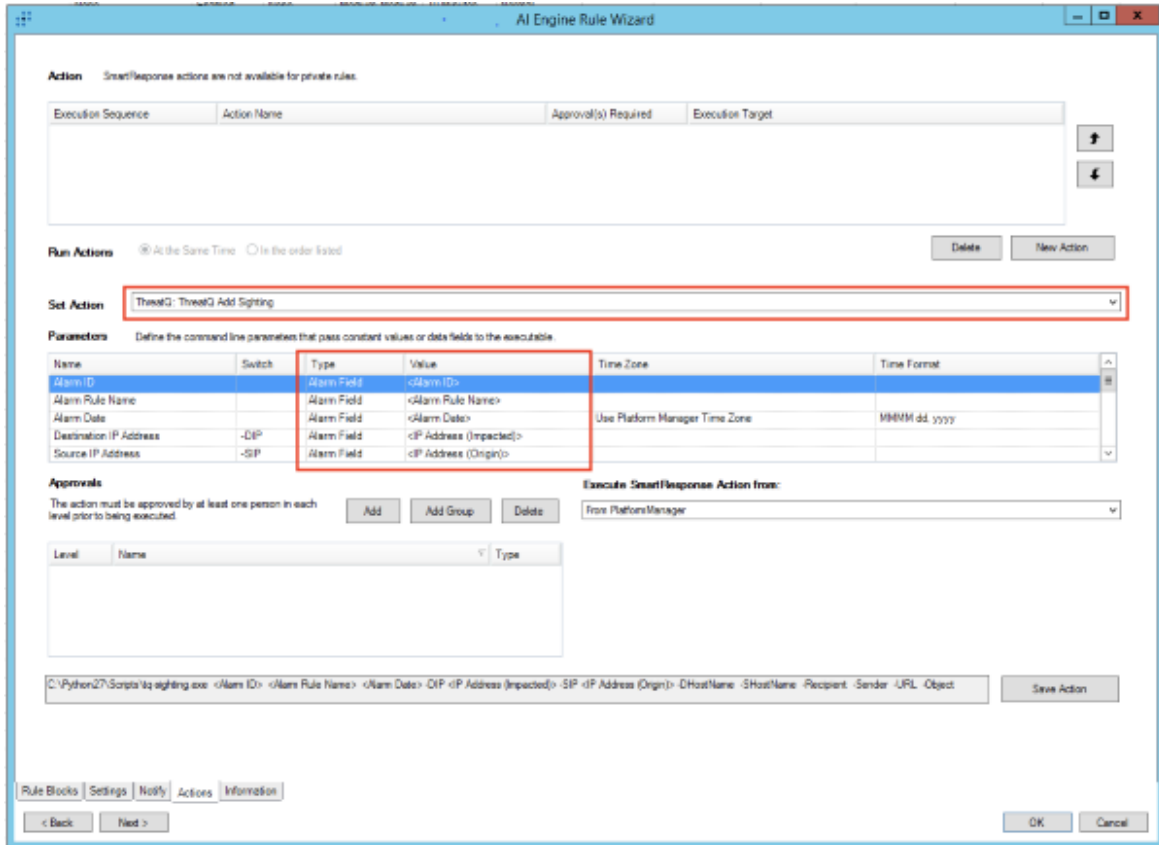


The screenshot displays the 'AI Engine Rule Wizard' interface. On the left, under 'Rule Block Types', the 'Log' category is selected, showing options like 'Observed', 'Not Observed Compound', and 'Not Observed Scheduled'. The central 'Rule Block Designer' area contains a 3D cube icon. Below this, the 'Rule Block Times' section features a horizontal timeline from 0 to 1 min, with a 30 sec mark. At the bottom, the 'Rule Block' tab is active, and the 'Actions' sub-tab is highlighted. On the right, the 'Rule Block Summary' panel provides details: 'Log Observed' (The Rule Block will signal when the specified logs are observed), 'Data Source' (Data Processor Logs), 'Primary Criteria' (Host (Origin or Impacted) is ThreatQ IP Address, ThreatQ FQDN), 'Log Sources' (All Log Sources), and 'Group By' (IP Address (Impacted), IP Address (Origin)).



Only the fields listed in the "Group By" section will be available in the Actions Menu.

4. On the Actions screen, use the Set Action drop down and select the ThreatQ: ThreatQ Add Sighting Action.



The screenshot shows the 'AI Engine Rule Wizard' window. The 'Action' section at the top states 'SmartResponse actions are not available for private rules.' Below this is a table for 'Execution Sequence' with columns for 'Action Name', 'Approval(s) Required', and 'Execution Target'. The 'Run Actions' section has two radio buttons: 'At the Same Time' (selected) and 'In the order listed'. The 'Set Action' dropdown is set to 'ThreatQ: ThreatQ Add Sighting'. The 'Parameters' section contains a table with columns: Name, Switch, Type, Value, Time Zone, and Time Format. The 'Approvals' section includes a table for approval levels and a 'Save Action' button. The bottom of the window has navigation buttons: '< Back', 'Next >', 'OK', and 'Cancel'.

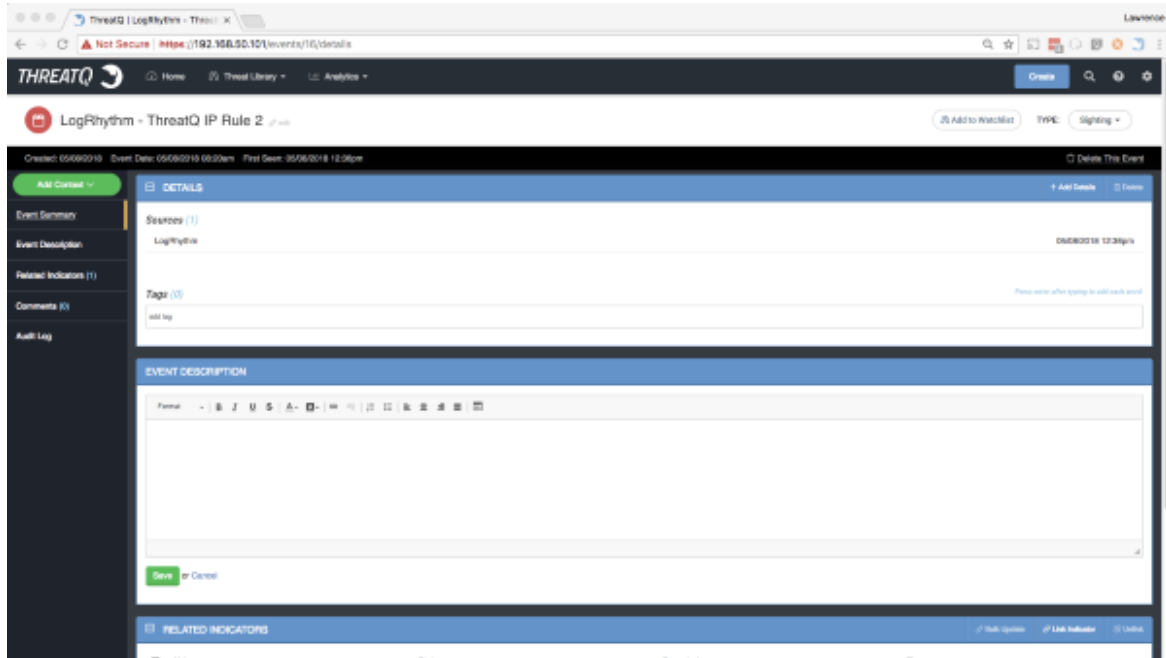
Name	Switch	Type	Value	Time Zone	Time Format
Alarm ID		Alarm Field	<Alarm ID>		
Alarm Rule Name		Alarm Field	<Alarm Rule Name>		
Alarm Date		Alarm Field	<Alarm Date>		
Destination IP Address	-DIP	Alarm Field	<IP Address (Impacted)>	Use Platform Manager Time Zone	MMMM dd, yyyy
Source IP Address	-SIP	Alarm Field	<IP Address (Origin)>		

Execute SmartResponse Action from: From Platform Manager

Save Action

5. Make sure the fields that are present in the Group by have the correct value. For instance, the Destination IP Address should have <IP Address (Impacted)> selected.
6. For all other fields, change the Type from **Alarm Field** to **Constant Value**.
7. Click the **Save Action** button.
8. You will be prompted to restart the AI Engine.

Once completed, when that Rule is executed, a sighting should be added that looks similar to the following:

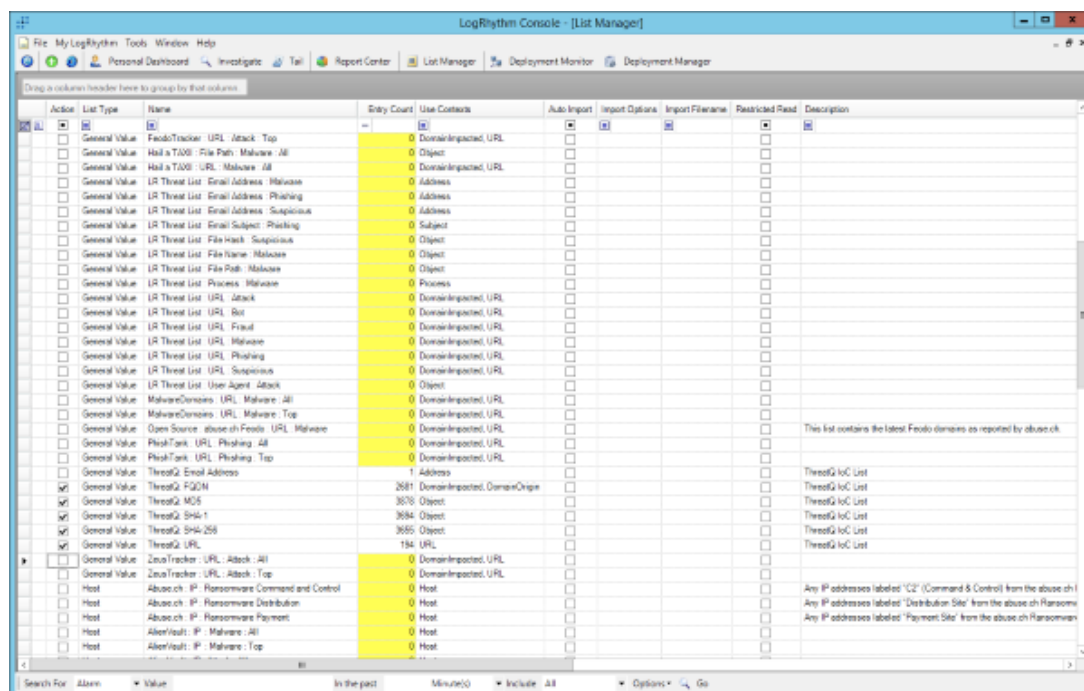


Currently, this only records the actual IoCs associated with the sighting itself. In the future, more attributes and details will be added.

Uninstallation

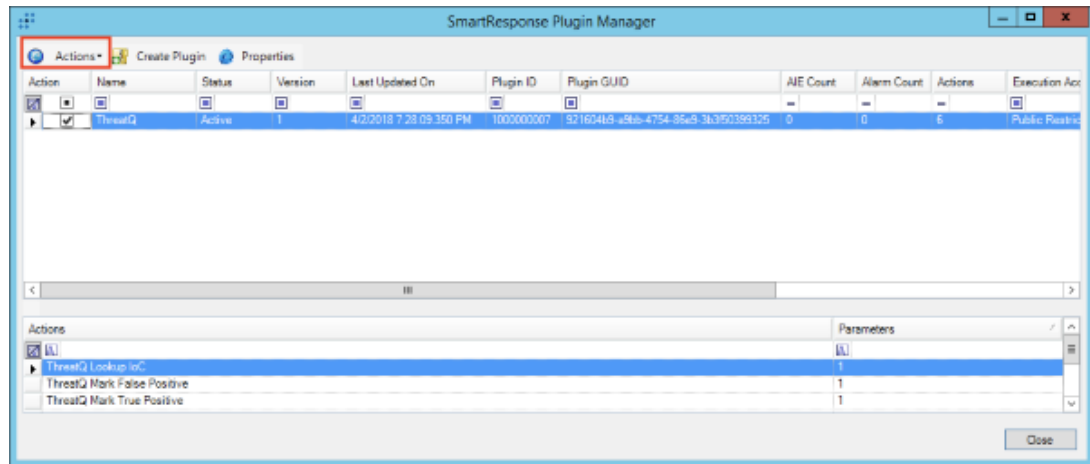
If it is decided that the integration needs to be removed, there are three main steps to uninstalling the integration. Due to audit requirements, however, it is not possible to delete the created Lists. Lists can only be disabled.

1. Stop the Windows Job for synchronization.
2. Deactivate all of the Lists created by ThreatQ.
 - a. Open the List Manager.
 - b. Check All Lists created by ThreatQ.



- c. Right Click → Actions → Retire.
 - d. Confirm Retirement.
3. Uninstall the SRPs.
 - a. Open the Deployment Manager.
 - b. Naviagte to Tools → Administration → SmartResponse Plugin Manager.

- c. Select the ThreatQ SRP and click Actions.



- d. Click Retire.

4. Uninstall the integration.

- a. Open an Administrative cmd session.
- b. Navigate to C:\Python27\pip.
- c. Execute pip.exe uninstall tqLogRhythm.
- d. Confirm removal.

5. Clean up Windows Registry.

- a. Click Windows Key + R and type regedit.
- b. Navigate to HKEY_LOCAL_MACHINE → SOFTWARE.
- c. Delete the ThreatQuotient key and all sub keys.

Testing the LogRhythm Integration

Prerequisites

- LogRhythm is installed.
- RDP is enabled for LogRhythm.
- ThreatQ integration is installed.
 - Custom connector
 - SRP (Smart Response Plugin) Actions

Testing Custom Connector (Sync)

This part of the integration downloads a ThreatQ saved search (Indicator search; Not Threat Library) and uploads the intelligence to lists in LogRhythm. Here is how to test the integration.

1. RDP into the LogRhythm server.
2. Install the custom connector if you have not see the [Installation](#) section.
3. Run the custom connector for the first time to install it into ThreatQ.
 - a. If it's already installed, the custom connector connection settings (client ID, client secret, and host) are stored in the Windows Registry.
 - b. To reset the connected ThreatQ host, you will need to remove the registry keys. See step 5 in the [Uninstallation](#) section.
4. Configure the connector using this guide: see the [Configuration](#) section.



The saved-search field is a YAML, not a comma-separated list of hashes. Follow these instructions to configure the YAML:[Advanced Search Mapping](#).

5. Run the connector using this command

```
C:\Python27\Scripts\tq-logrhythm.exe -ll  
L:\ThreatQ\ -v 3
```

6. Here is a quick checklist on what to look out for:

- a. The connector runs with no errors.
- b. The connector creates LogRhythm lists to store the indicators (if it hasn't already).
 - i. The lists created will be determined by your YAML configuration.
- c. Make sure each list contains the same number of indicators as in the saved search (indicator search)



You might need to check the indicator types individually since not all types will get ingested into LogRhythm.



LogRhythm now supports more types, it might be worth updating the integration to support them

Testing the SRP Actions (Contextual Actions)

This part of the integration allows you to execute specific actions on alarms or individual indicators within the LogRhythm platform. They can also be used in the "AI Engine" to perform automatic actions when an alarm is triggered. This is usually the case for the "ThreatQ: Add Sighting" Action. Since logs are slightly complicated to get into the LogRhythm platform,

we can test the actual script directly (as if LogRhythm was calling it).



This testing guide will not require any logs.

1. RDP into the LogRhythm server.
2. Install the custom connector if you have not then see the [Installation](#) section.
3. Run the custom connector for the first time to authenticate and install it into ThreatQ.
4. Test each of the SRP actions by running the action command (with the required parameters). Here are some examples (replace <> text):

Add Sighting

```
C:\Python27\Scripts\tq-sighting.exe <Alarm ID>
<Alarm Name> <Alarm Date> -DIP -SIP <IP Address
(Origin)> -DHostName -SHostName <Host (Origin)> -
Recipient -Sender -URL -Object

# Example
C:\Python27\Scripts\tq-sighting.exe 123 "ThreatQ
Blocklist" "2019-01-17 01:00:00" -DIP -SIP
55.55.55.55 -DHostName -SHostName badhost.com -
Recipient -Sender -URL -Object
```

Add IoC

```
C:\Python27\Scripts\tq-add-ioc.exe "<Indicator
Type>" <Indicator Value> [--attribute "
[attr1:val1,attr2:val2]" ]
```

```
# Example
C:\Python27\Scripts\tq-add-ioc.exe "IP Address"
77.77.77.77 --attribute "False Positive:
Yes,Confidence:High"
```

Lookup IoC

```
C:\Python27\Scripts\tq-lookup.exe <Indicator Value>

# Example
C:\Python27\Scripts\tq-lookup.exe 77.77.77.77
```

Mark as False Positive

```
C:\Python27\Scripts\tq-mark-false-positive.exe
<Indicator Value>

# Example
C:\Python27\Scripts\tq-mark-false-positive.exe
77.77.77.77
```

Mark as True Positive

```
C:\Python27\Scripts\tq-mark-true-positive.exe
<Indicator Value>

# Example
C:\Python27\Scripts\tq-mark-true-positive.exe
77.77.77.77
```


Create Sighting

```
C:\Python27\Scripts\tq-whitelist-ioc.exe <Indicator  
Value>
```

```
# Example
```

```
C:\Python27\Scripts\tq-whitelist-ioc.exe  
77.77.77.77
```