ThreatQuotient

ThreatQuotient for LogRhythm Guide Guide

Version 1.4.0

March 16, 2021

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.

Contents

Introduction

The LogRhythm integration is a single install Windows based python 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 a data collection created via the Threat Library in ThreatQ to LogRhythm for use in correlations
- **Smart Response Plugins:** Several Smart Response Plugins 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
- Python
    - Python2 - version 2.7.12 or newer installed on the LogRhythm Platform Manager
    - Python3 if using the python3 version of the integration
- 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
- ThreatQ data collections 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 data collections with and to use as connection).
    - It is suggested to create a user for this purpose (username like logrhythm@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 chapter, based on the integration version you have downaloded, the integration requires either Python2 (version 2.7.12+) or Python3 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.

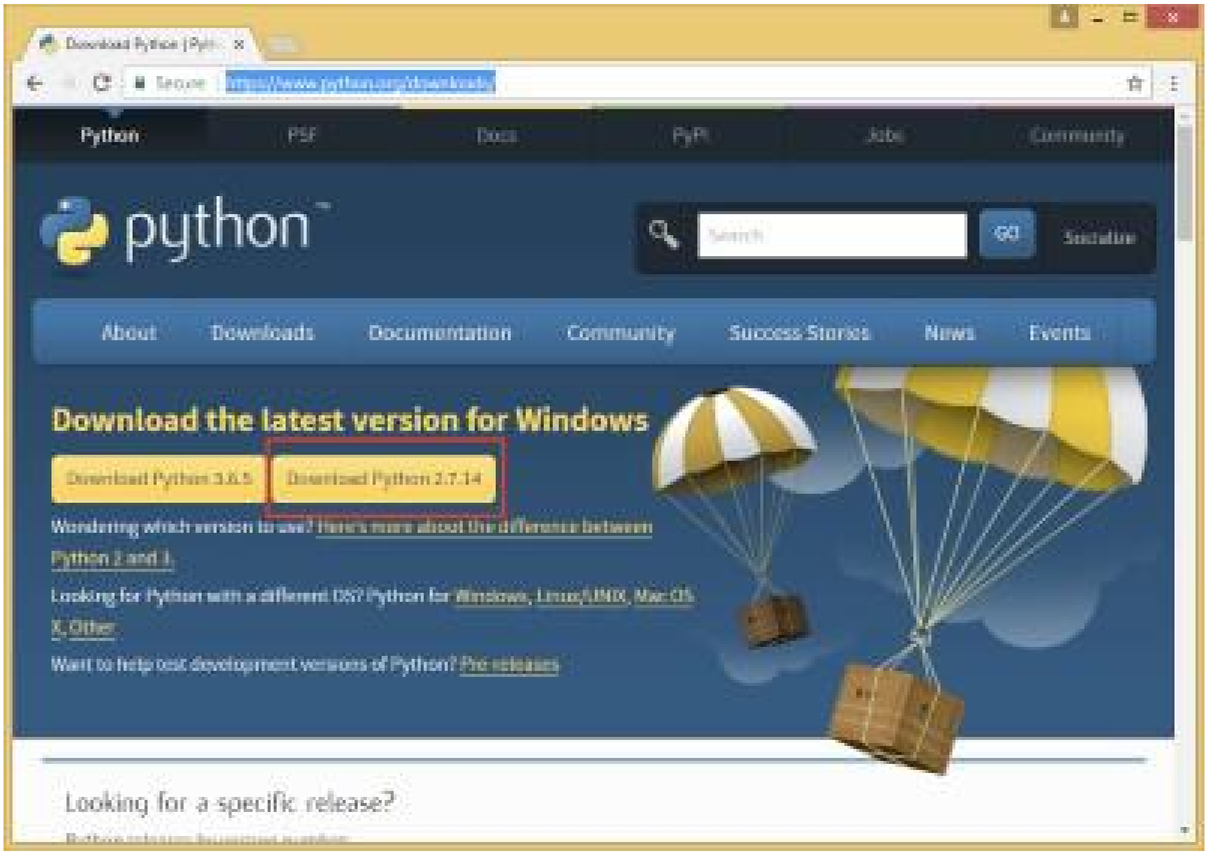
1. Log into the VM where your LogRhythm instance is installed
2. Open up your LogRhythm Console Within the LogRhythm Console
3. Go to the Deployment Manager tab and then click on Third Party Applications
4. Select the Third Party Application tab
5. Right click the page and select "New" to create a new app
6. Click Generate Token to generate a new JWT (token) to use for authentication
7. Copy the JWT down somewhere to use with the ThreatQ integration

Installing Python2

If using the Python 2 version of the integration and 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.

> ⚠ These steps are for Python 2 users only.

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



Download the latest version for Windows

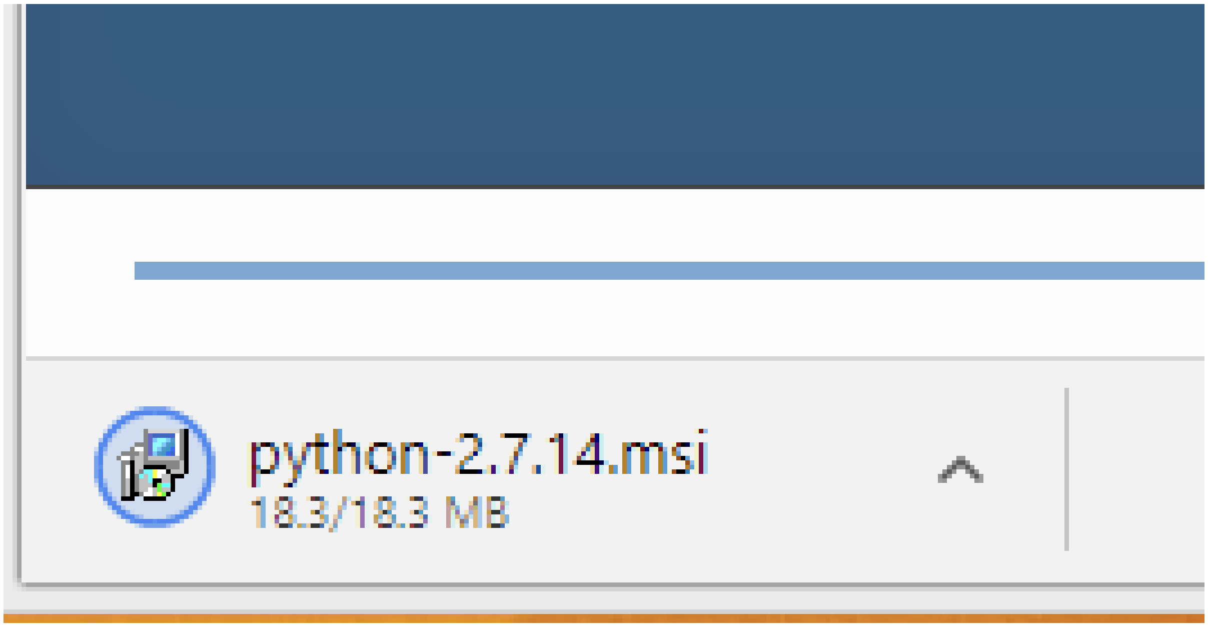
Wondering which version to use? Here's more about the difference between Python 2 and 3.

Looking for Python with a different OS? Python for Windows, Linux/UNIX, Mac OS X, Other

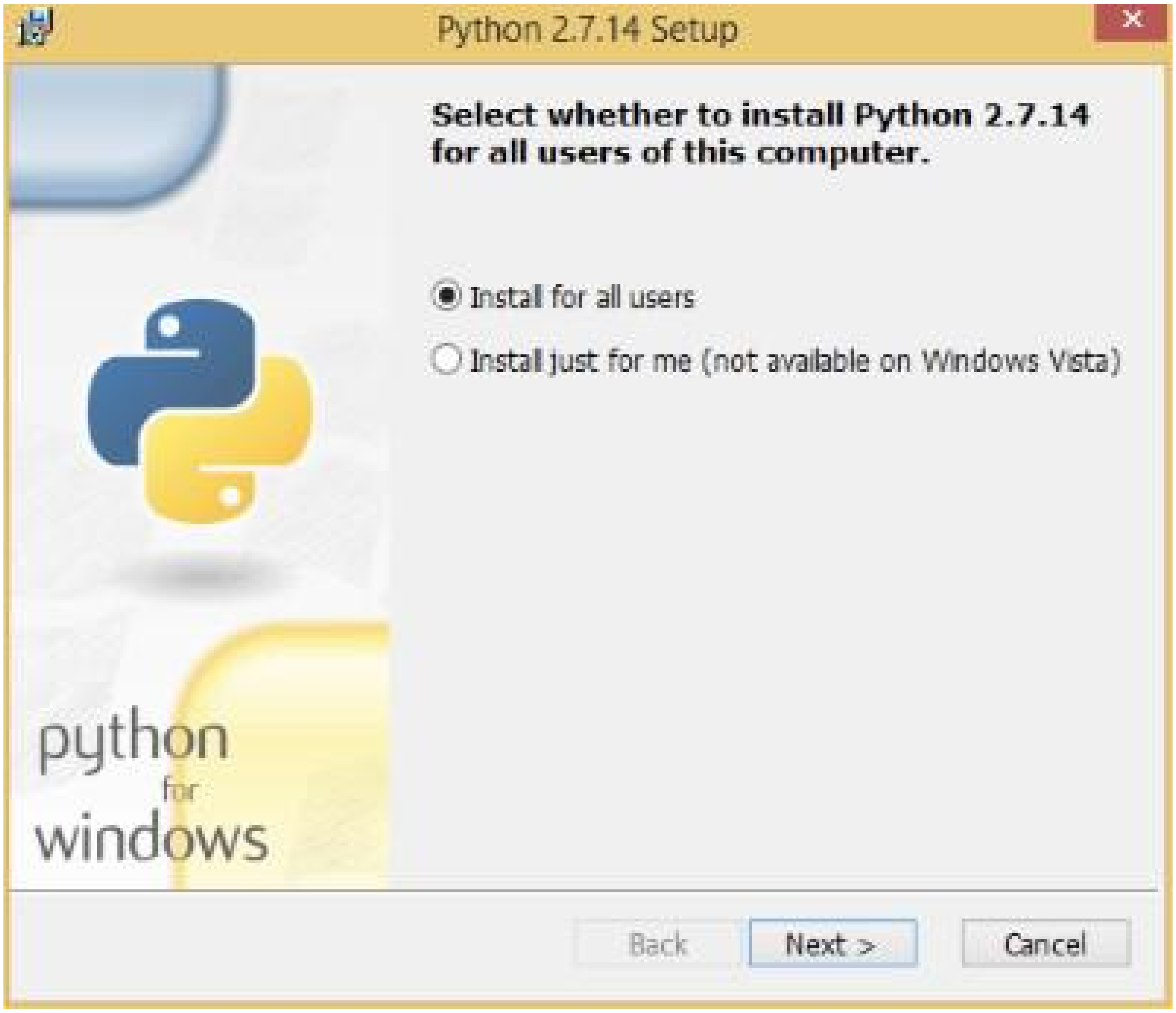
Want to help test development versions of Python? Pre-releases

Looking for a specific release?

3. Click on the Downloaded Python MSI.



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



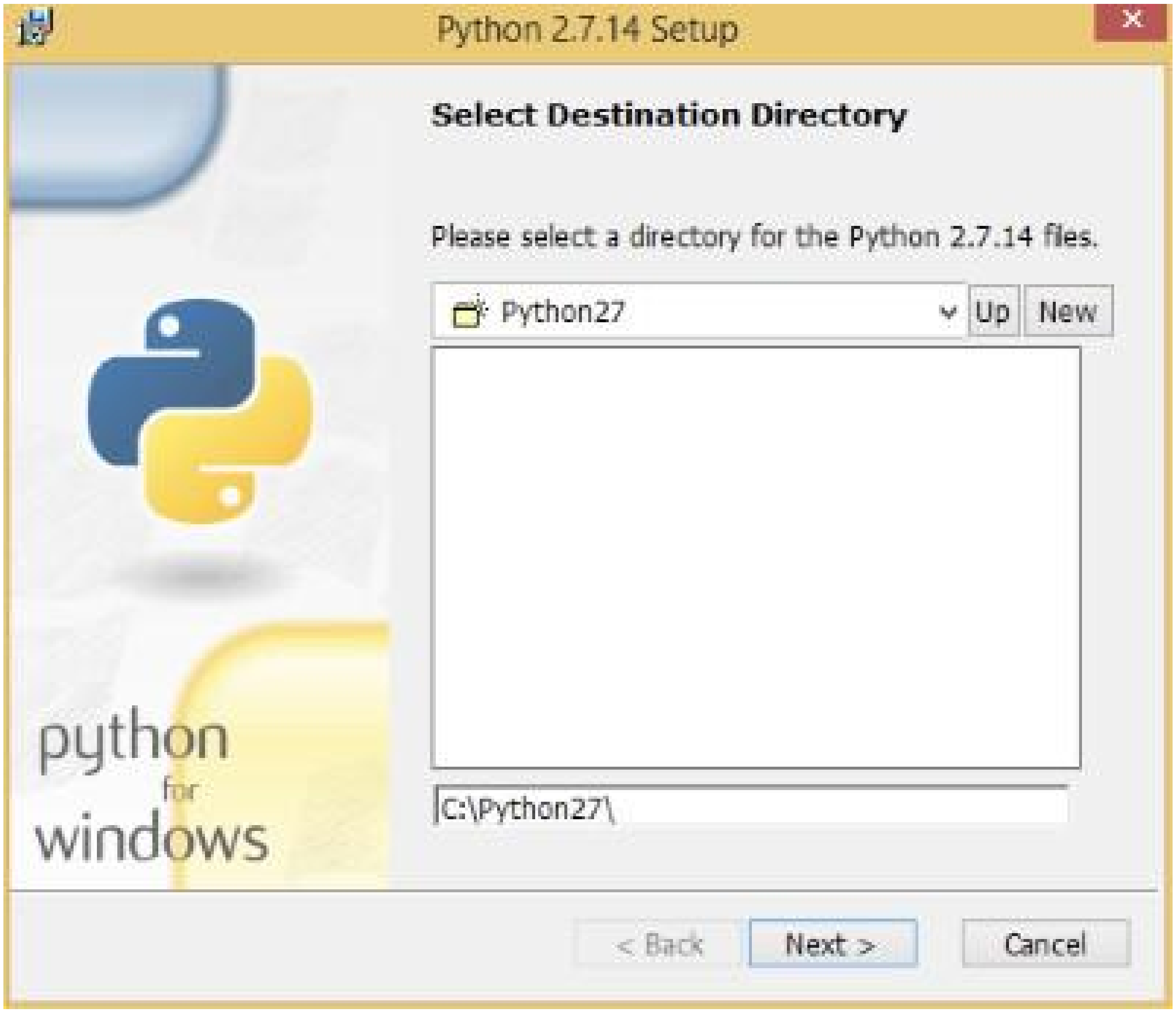
Python 2.7.14 Setup

Select whether to install Python 2.7.14 for all users of this computer.

● Install for all users

○ Install just for me (not available on Windows Vista)

5. Select the installation location.



Python 2.7.14 Setup

Select Destination Directory

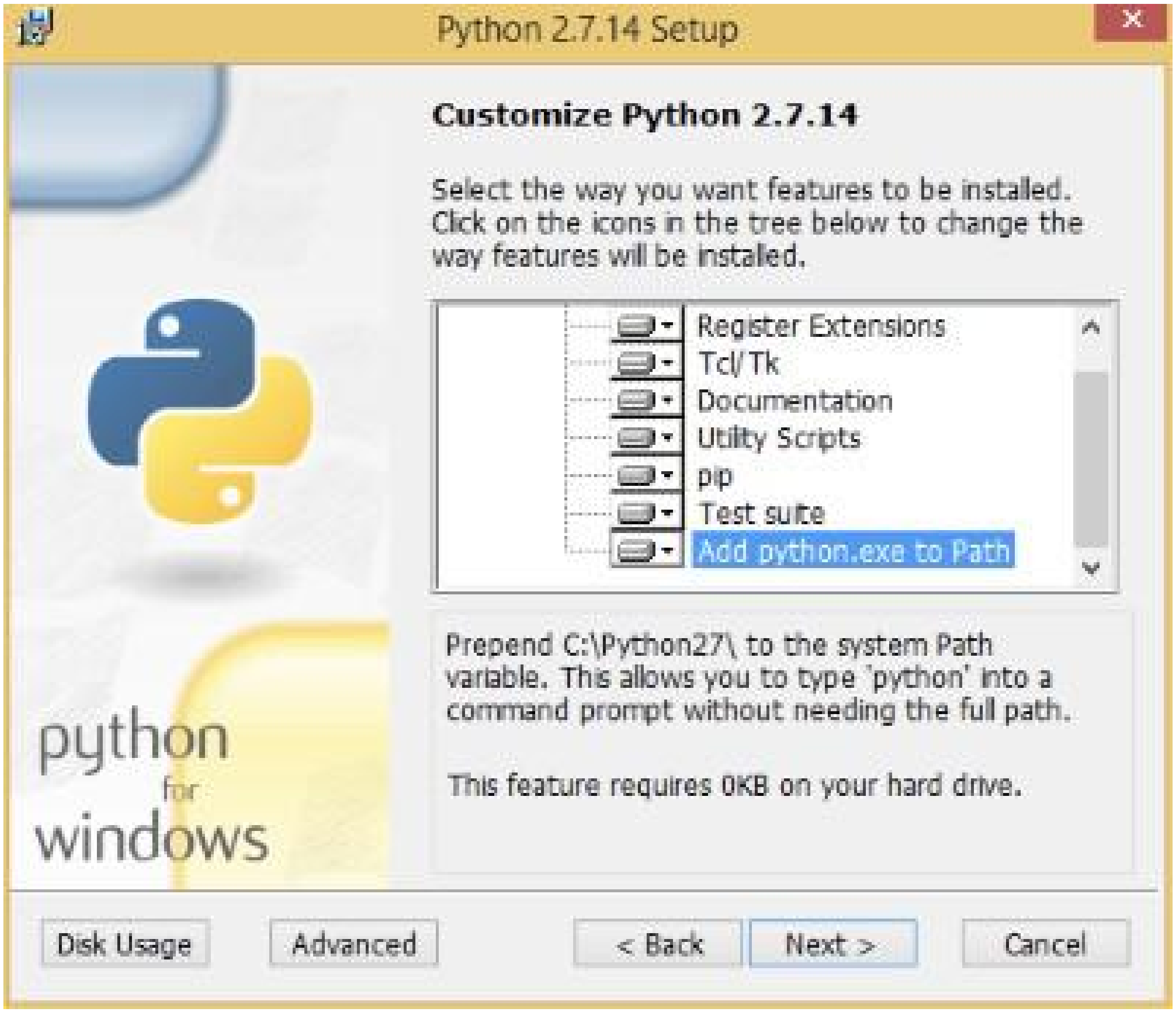
Please select a directory for the Python 2.7.14 files.

Python27

C:\Python27\

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

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



Customize Python 2.7.14

Select the way you want features to be installed. Click on the icons in the tree below to change the way features will be installed.

- Register Extensions
- Tcl/Tk
- Documentation
- Utility Scripts
- pip
- Test suite
- Add python.exe to Path

Prepend C:\Python27\ to the system Path variable. This allows you to type 'python' into a command prompt without needing the full path.

This feature requires 0KB on your hard drive.

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.

8. Type exit() to exit the shell.

Installation

⚠ Upgrading Users: If you are ungrading from a previous version of the integration, review the change log for any changes regarding configuration parameters. If there are any parameter changes listed, then you must first delete the configuration file from the pervious version before proceeding with the steps below. Failure to delete this file will result in the integration falling.

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, refer to the Installing Python2 section of the Pre-Installation chapter.

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.

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

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\Scripts.
4. Execute the following command:

   With Internet Access

   If your LogRhythm instance has access to the internet:

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

> <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 tq_conn_logrhythm -d /tmp/logrhythm
```

Transfer the tq_conn_logrhythm-<version>-py2-none-any.whl, and its dependencies to the Downloads folder on the LogRhythm instance.

```
pip install C:\Downloads\tq_conn_logrhythm-1.4.0-py2-none-any.whl --no-index
--find-links C:\Downloads
```

5. Optional - Add C:\Python27 to your Windows Path. This will allow you to execute commands without having to specify the directory.
6. Create new folders in your Log Files disk to store the integration's logs and config. For example:

   Config: L:\ThreatQ\config
   Logs: L:\ThreatQ\logs
7. Check if there is a route to ThreatQ from LogRhythm.

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

8. Execute the following command. If you are using different paths for the config and logs folder, please change the respective values below:

```
C:\Python27\Scripts\tq-conn-logrhythm.exe -c L:\ThreatQ\config\ -ll L:
\ThreatQ\logs\ -v3
```

9. Complete the following fields:

PARAMETER	DESCRIPTION
ThreatQ Host	This is the hostname or IP Address of the ThreatQ appliance
Client ID	This is the OAuth Client ID, found by going to Gear → OAuth Credentials in the ThreatQ Appliance
Email Address	The email address of the LogRhythm ThreatQ User
Password	The password of the LogRhythm ThreatQ User
Status	The status of newly created IOCs. It is recommended to select the Active status

Once complete, the log and config paths, and the verbosity level will be stored in HKEY_LOCAL_MACHINE\Software\ThreatQuotient\LogRhythm and will be available to this system.

After the integration is installed on the LogRhythm Platform Manager, the user must configure the integration in the ThreatQ UI.

Configuration

To configure the connector:

1. Navigate to your integrations management page in ThreatQ.
2. Select Labs for the Category dropdown.
3. Click on the integration to open its details page.
4. Enter the following parameters under the Configuration tab:

PARAMETER	DESCRIPTION
LogRhythm Host	The Hostname of IP Address of the LogRhythm Platform Manager
LogRhythm 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
Check this box if LogRhythm is version 7.5.1 or higher	Due to a change in the LogRhythm API, this box needs to be checked if your version is 7.5.1 or above
Name of the LogRhythm user owning the Threat Lists in LogRhythm NOT the username, but the name of the user as it appears in LogRhythm	Name of the LogRhythm user who will own the threat list. This is usually the LogRhythm Administrator. The name can be found by navigating to LogRhythm Console -> Deployment Manager -> People. Enter the name as see in the first column, NOT the username.
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)
A ThreatQ data collection with IOCs to add to LogRhythm	This is the mapping of data collections to LogRhythm lists, explained in detail in the ThreatQ Data Collection section of this document

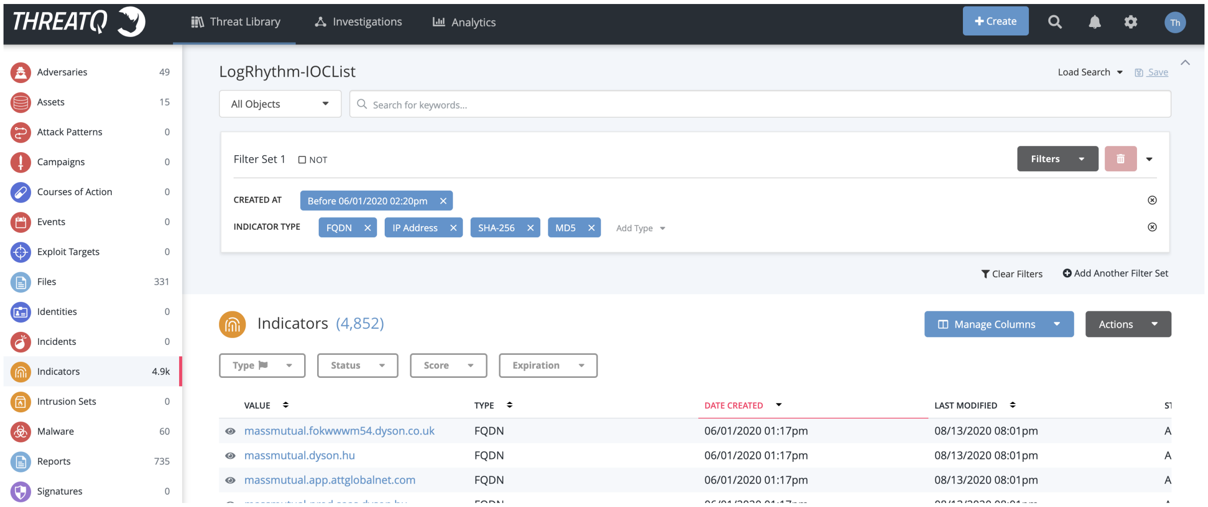
5. Click on **Save Changes**.

6. Click on the toggle switch, located above the Additional Information section, to enable the integration.

ThreatQ Data Collection

This section explains how to configure a Data Collection in ThreatQ. Go to the ThreatQ Library in ThreatQ and enter the search parameters for the indicators you would like to send to LogRhythm. The IOCs should be of the following types – IP Address, FQDN, MD5, SHA-1, and SHA-256.

This is an example of a data collection called “LogRhythm-IOCList” that includes IP Address, FQDN, SHA-256 and MD5 created before 06/01/2020 at 2:20pm:



Adversaries	49
Assets	15
Attack Patterns	0
Campaigns	0
Courses of Action	0
Events	0
Exploit Targets	0
Files	331
Identities	0
Incidents	0
Indicators	4.9k
Intrusion Sets	0
Malware	60
Reports	735
Signatures	0

LogRhythm-IOCList

Filter Set 1 □ NOT

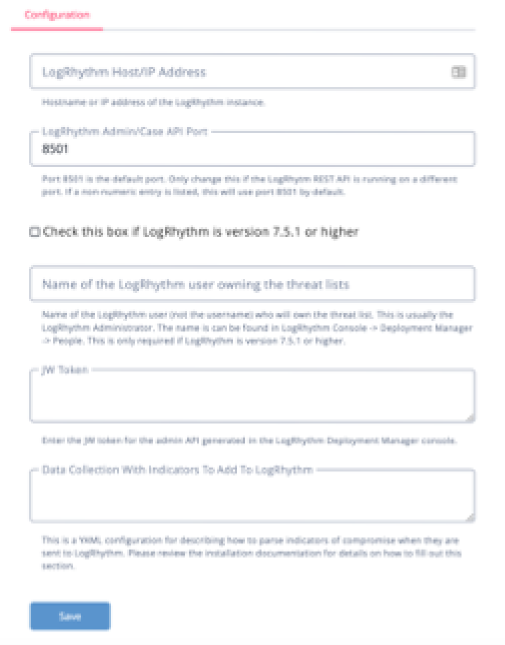
CREATED AT: Before 06/01/2020 02:20pm

INDICATOR TYPE: FQDN, IP Address, SHA-256, MD5

Indicators (4,852)

VALUE	TYPE	DATE CREATED	LAST MODIFIED	ST
massmutual.fokwwwm54.dyson.co.uk	FQDN	06/01/2020 01:17pm	08/13/2020 08:01pm	A
massmutual.dyson.hu	FQDN	06/01/2020 01:17pm	08/13/2020 08:01pm	A
massmutual.app.attglobalnet.com	FQDN	06/01/2020 01:17pm	08/13/2020 08:01pm	A

Once the search is configured, from the top menu navigate to Integrations -> Feeds & Connectors and click on LogRhythm. Open the card for LogRhythm and enable it by moving the slider to the right.



Configuration

LogRhythm Host/IP Address

Hostname or IP address of the LogRhythm instance.

LogRhythm Admin/Case API Port: 8501

Port 8501 is the default port. Only change this if the LogRhythm REST API is running on a different port. If a non numeric entry is listed, this will use port 8501 by default.

□ Check this box if LogRhythm is version 7.5.1 or higher

Name of the LogRhythm user owning the threat lists

Name of the LogRhythm user (not the username) who will own the threat list. This is usually the LogRhythm Administrator. The name is can be found in LogRhythm Console -> Deployment Manager -> People. This is only required if LogRhythm is version 7.5.1 or higher.

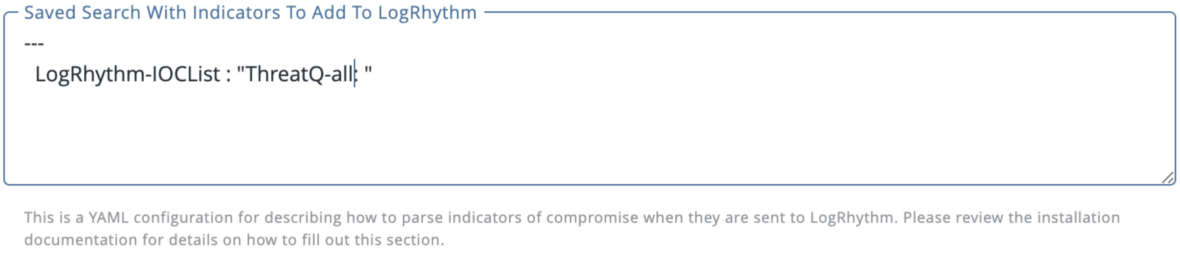
JW Token

Enter the JW token for the admin API generated in the LogRhythm Deployment Manager console.

Data Collection With Indicators To Add To LogRhythm

This is a YAML configuration for describing how to parse indicators of compromise when they are sent to LogRhythm. Please review the installation documentation for details on how to fill out this section.

Fill out the required information for host, LogRhythm user who will own the lists, and the JW Token. In the Data Collection box, enter the name of the data collection search followed by the name of the threat intel list you would like to create in LogRhythm similar to the syntax below, including the three dashes on the first line:



Saved Search With Indicators To Add To LogRhythm

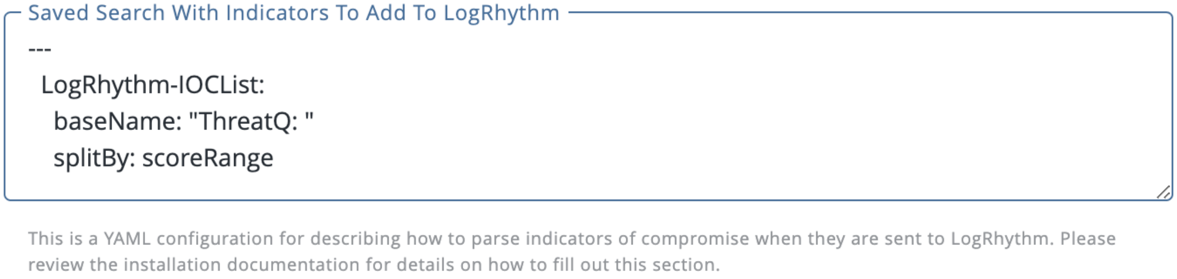
```
---
 LogRhythm-IOCList : "ThreatQ-all: "
```

This is a YAML configuration for describing how to parse indicators of compromise when they are sent to LogRhythm. Please review the installation documentation for details on how to fill out this section.

In the line above, “LogRhythm-IOCList” is the name of the Data Collection in ThreatQ. The phrase "ThreatQ-all: " is the basename of a family of lists in LogRhythm. All of the lists will have the prefix “ThreatQ-all:” 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.

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



```
---
 LogRhythm-IOCList:
  baseName: "ThreatQ: "
  splitBy: scoreRange
```

This is a YAML configuration for describing how to parse indicators of compromise when they are sent to LogRhythm. Please review the installation documentation for details on how to fill out this section.

This will have a similar affect as above, except that it will create one more level of list. For instance, FQDNs in the above data collection, “LogRhythm-IOCList”, 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 data collection. For instance, if no Medium FQDNs are in the data collection, there will be no ThreatQ: FQDN: Medium list. At any point in the future, these will be added as necessary.

The following are the currently available splitBy parameters:

PARAMETER	DESCRIPTION
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

Recurring Execution

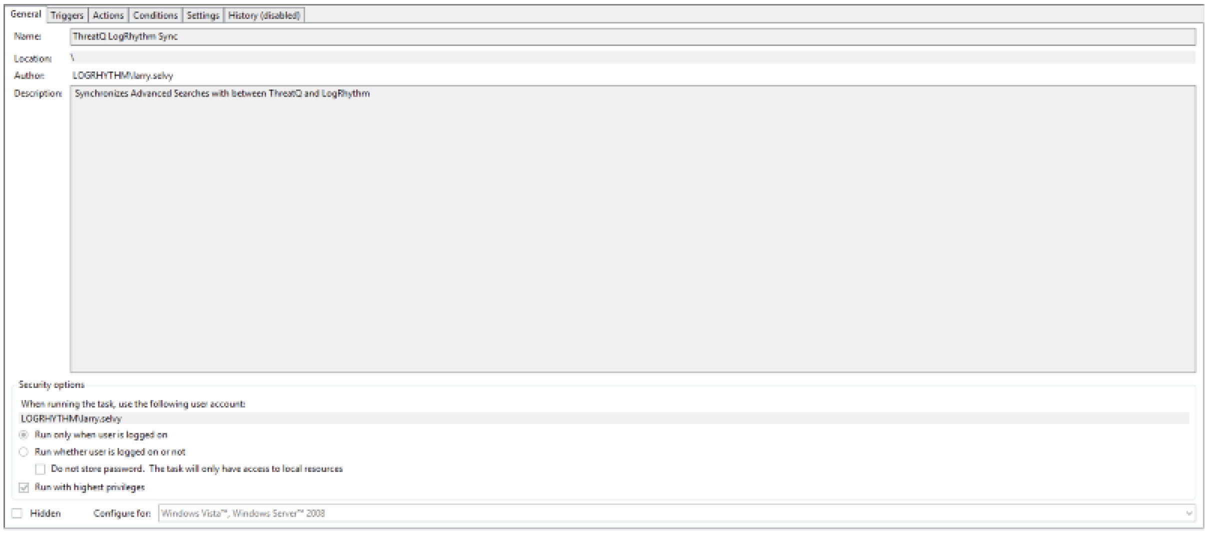
One of the commands provided during the installation is the tq-conn-logrhythm.exe command. This command is what is used to read the configuration set in the UI of the ThreatQ appliance, parse the indicators from a data collection in ThreatQ and upload those indicators to the LogRhythm lists.

During the execution of tq-conn-logrhythm.exe, the UI fields are read, lists are created, and all lists are compared against the content of the data collections in the ThreatQ's Threat Library.

Each Indicator of Compromise listed in the data collection is compared to the con- tents 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 data collection, 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 data collections. To do this, use the Task Scheduler, and configure it as below:



Name: ThreatQ LogRhythm Sync

Location: \

Author: LOGRHYTHM\larry.selvy

Description: Synchronizes Advanced Searches with between ThreatQ and LogRhythm

Security options

When running the task, use the following user account:

LOGRHYTHM\larry.selvy

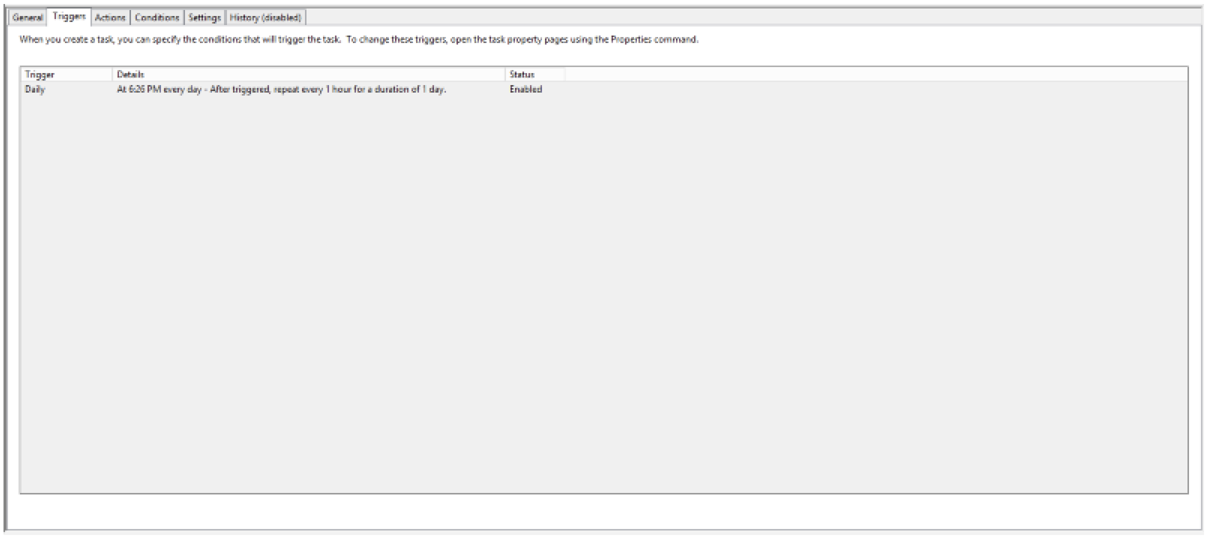
● Run only when user is logged on

○ Run whether user is logged on or not

□ Do not store password. The task will only have access to local resources

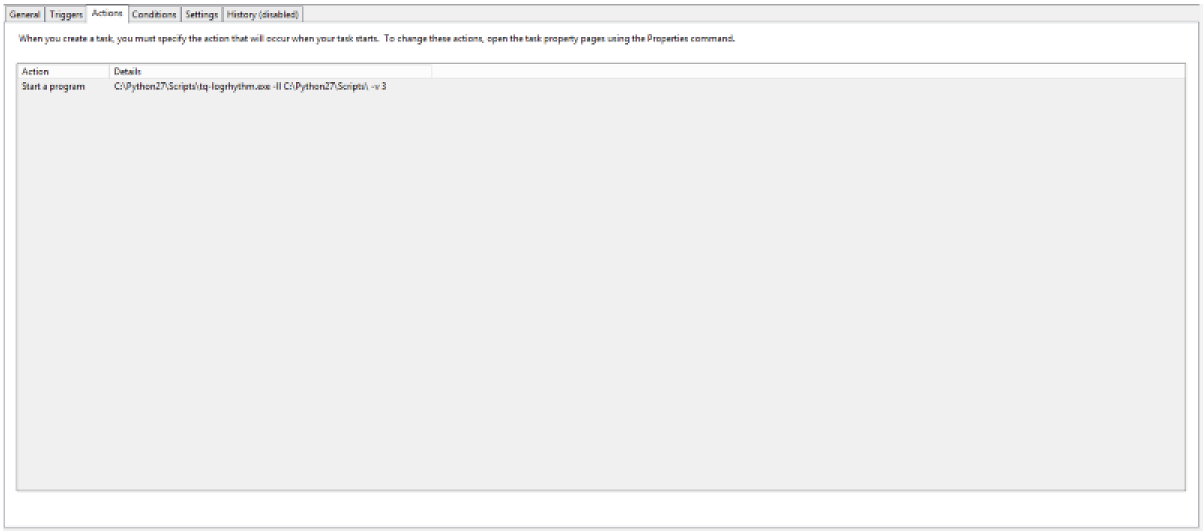
☑ Run with highest privileges

□ Hidden Configure for: Windows Vista™, Windows Server™ 2008



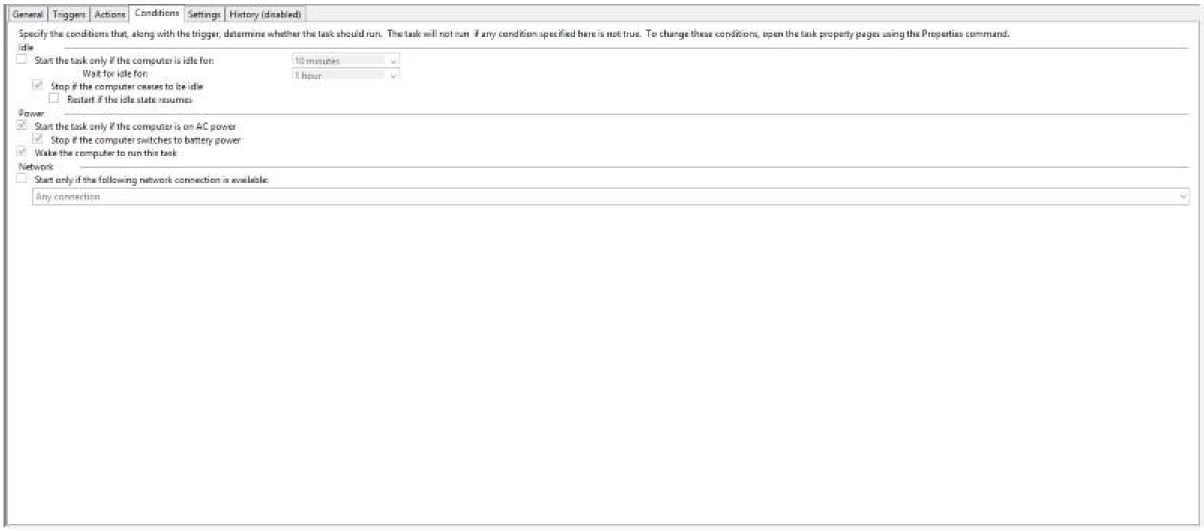
When you create a task, you can specify the conditions that will trigger the task. To change these triggers, open the task property pages using the Properties command.

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



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



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

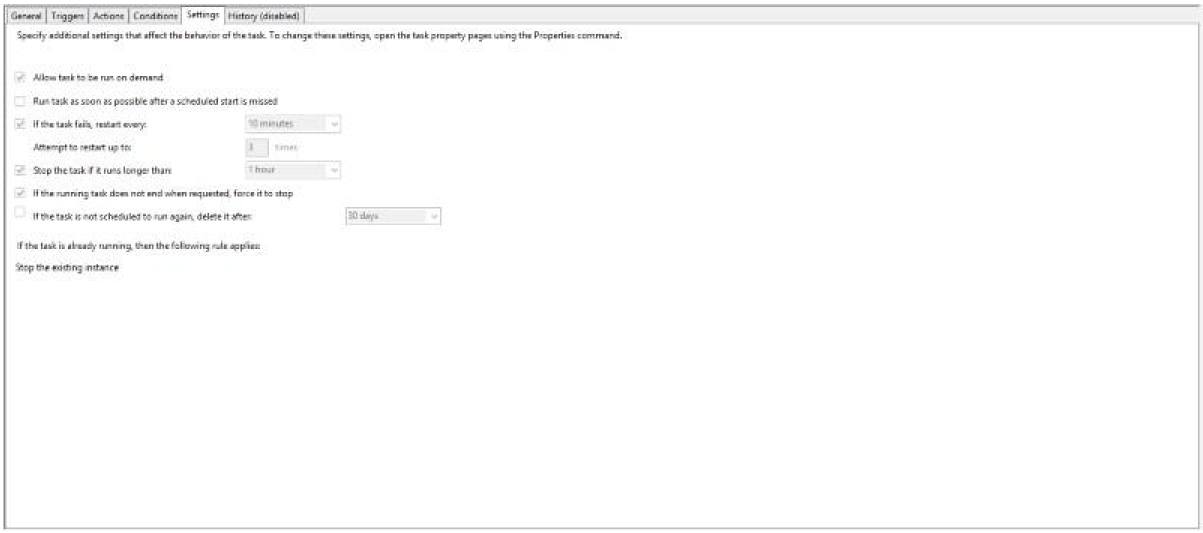
- ☐ Start the task only if the computer is idle for: 10 minutes
  - Wait for idle for: 1 hour
  - ☑ Stop if the computer ceases to be idle
    - ☐ Restart if the idle state resumes

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



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. Anymore than this and the system will be unable to synchronize correctly.

The frequency of synchronization between ThreatQ and LogRhythm is at the discretion of the user but it should be no more than once an hour.

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

Smart Response Plugin

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 SRPs are provided with the installation. All of these can be found in the C:\Python27\Scripts directory and can also be executed via the CLI on the LogRhythm host.

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-sighting.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-lookup.exe	ThreatQ Lookup IOC	Searches the ThreatQ Threat Library for an indicator with the	Enriches ThreatQ

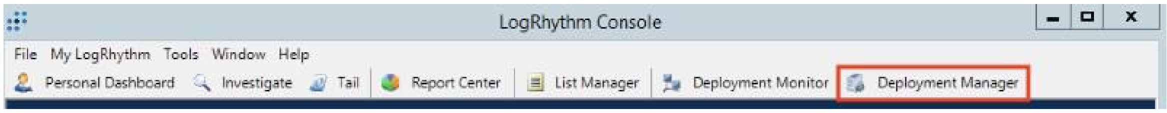
NAME OF SRP EXECUTABLE	NAME OF SRP ACTION	DESCRIPTION	ENRICHMENT DESTINATION
		same type and value as the indicator provided	
tq-add-ioc.exe	ThreatQ Add IOC	Adds an IOC of the same type and value to ThreatQ from LogRhythm. If the IOC already exists, it adds LogRhythm as a source	Enriches ThreatQ

Installation of SRPs

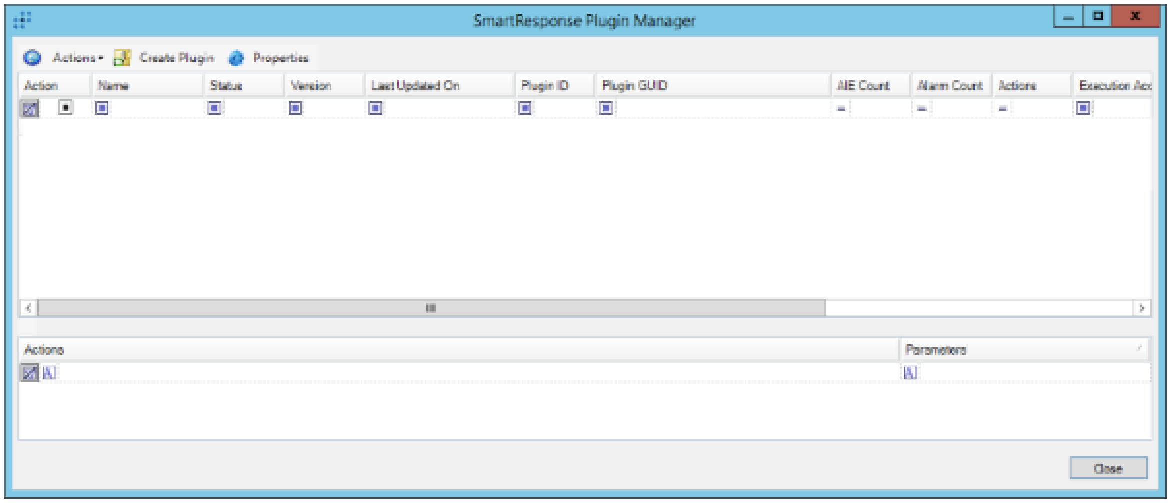
The SPR executables are installed during the original installation of the integration. However, to enable these within LogRhythm to be used in the Client or Web Consoles, the SRP bundle has to be added. The bundle is presented as an all in one.

To install the SRP bundle:

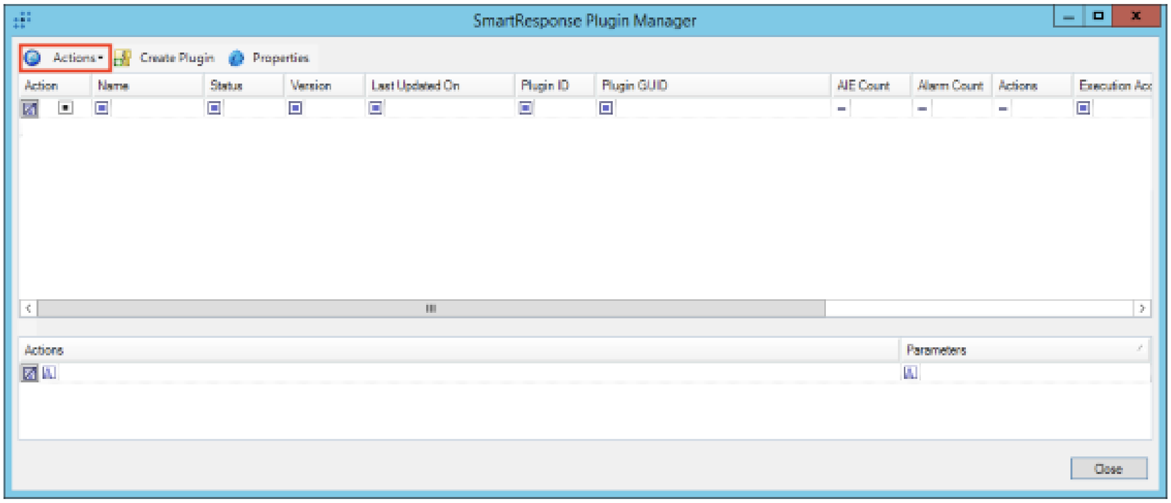
1. Login to the LogRhythm console
2. Open the Deployment Manager



3. Go to Tools → Administration → SmartResponse Plugin Manager

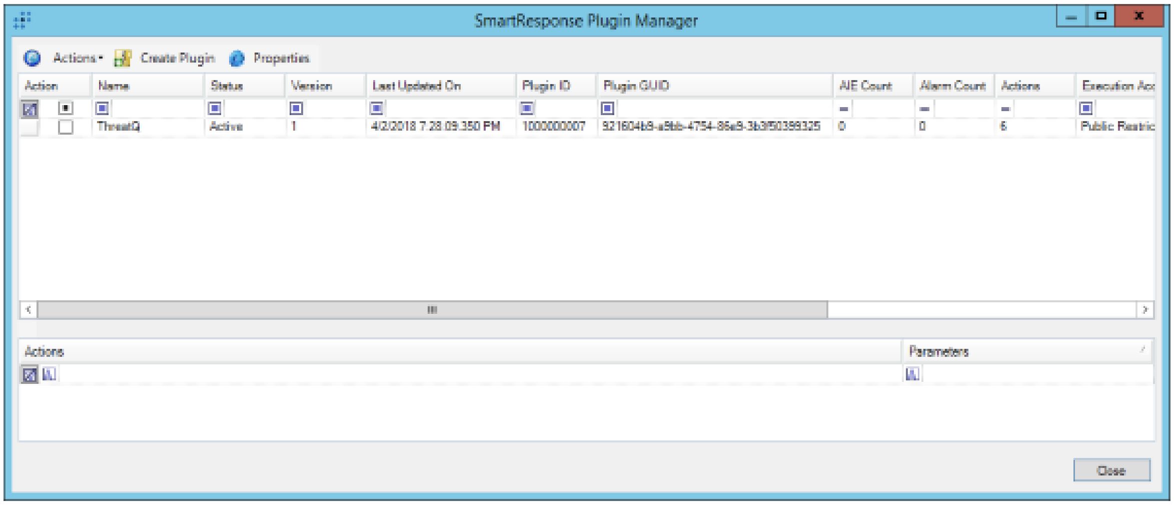


4. Click on the Actions button



5. Navigate to the ThreatQ SRP bundle and click Open.

   Once complete, the ThreatQ Smart Response Plugins list found in Smart Response Plugins.

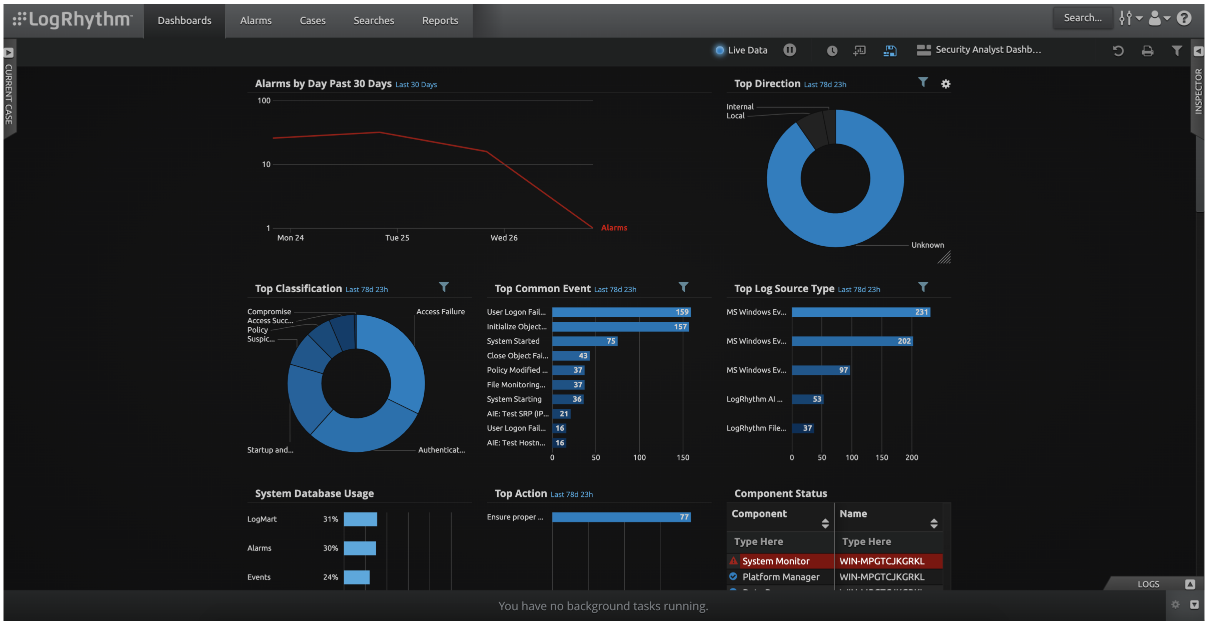


Action	Name	Status	Version	Last Updated On	Plugin ID	Plugin GUID	AIE Count	Alarm Count	Actions	Execution Acc
□	ThreatQ	Active	1	4/2/2018 7:28:09.350 PM	1000000007	921604b9-a9bb-4754-86e9-3b3f50399325	0	0	6	Public Restric

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.

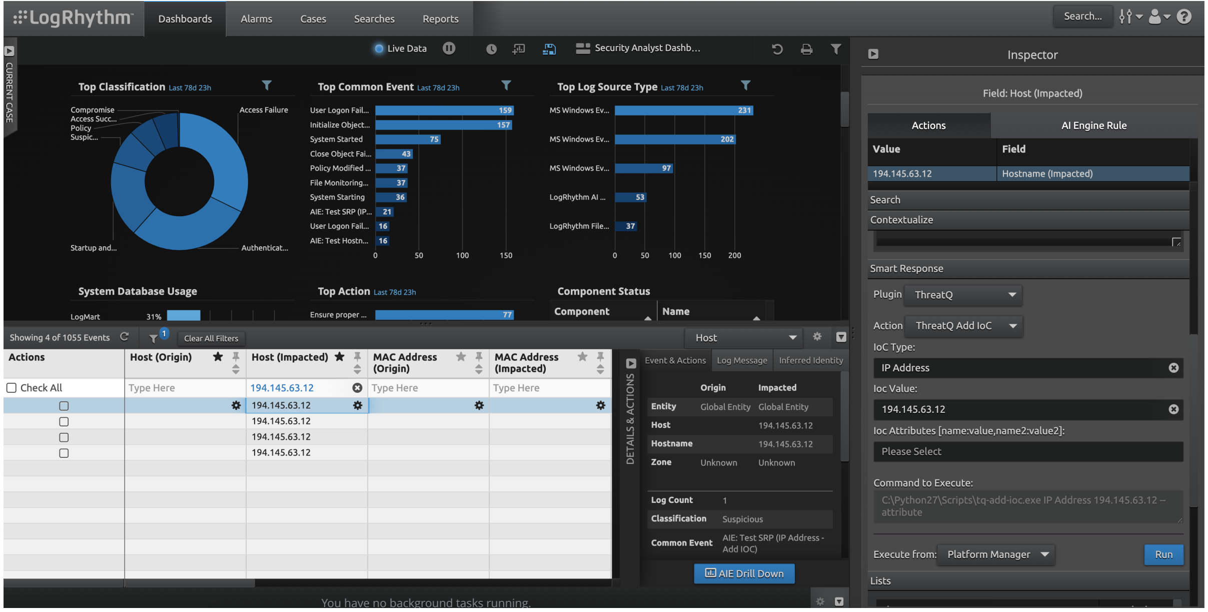


Component	Name
Type Here	Type Here
System Monitor	WIN-MPGTCJKGRKL
Platform Manager	WIN-MPGTCJKGRKL

You have no background tasks running.

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.



Inspector

Field: Host (Impacted)

Value	Field
194.145.63.12	Hostname (Impacted)

Smart Response

Plugin: ThreatQ

Action: ThreatQ Add IoC

IoC Type: IP Address

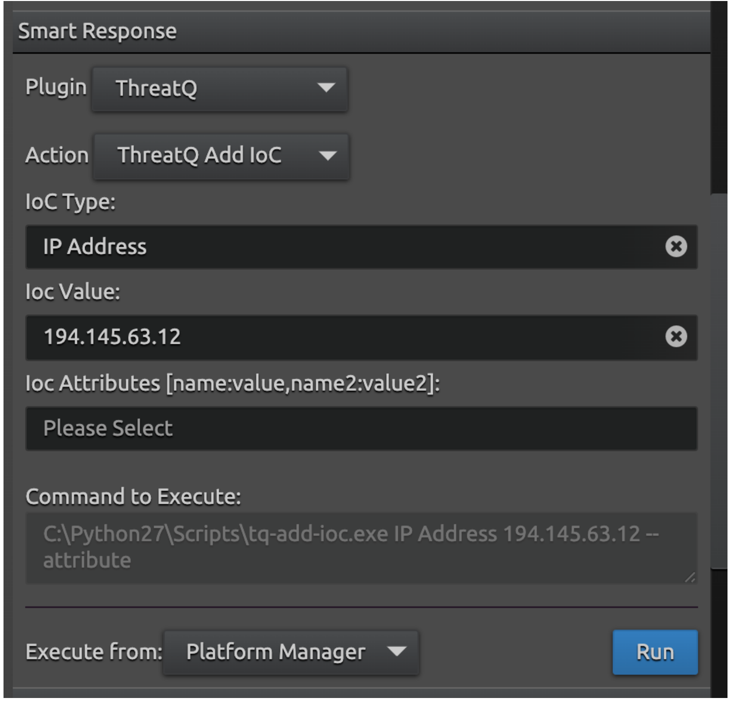
Ioc Value: 194.145.63.12

Ioc Attributes [name:value,name2:value2]: Please Select

Command to Execute: C:\Python27\Scripts\tq-add-ioc.exe IP Address 194.145.63.12 --attribute

Execute from: Platform Manager

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 Add IOC Action).
5. Fill in the appropriate Values (here an IP address is used). Depending on the action executed, different values would need to be entered in the UI
6. Ensure "Execute from: Platform Manager" is selected and click Run.



Smart Response

Plugin: ThreatQ

Action: ThreatQ Add IoC

IoC Type: IP Address

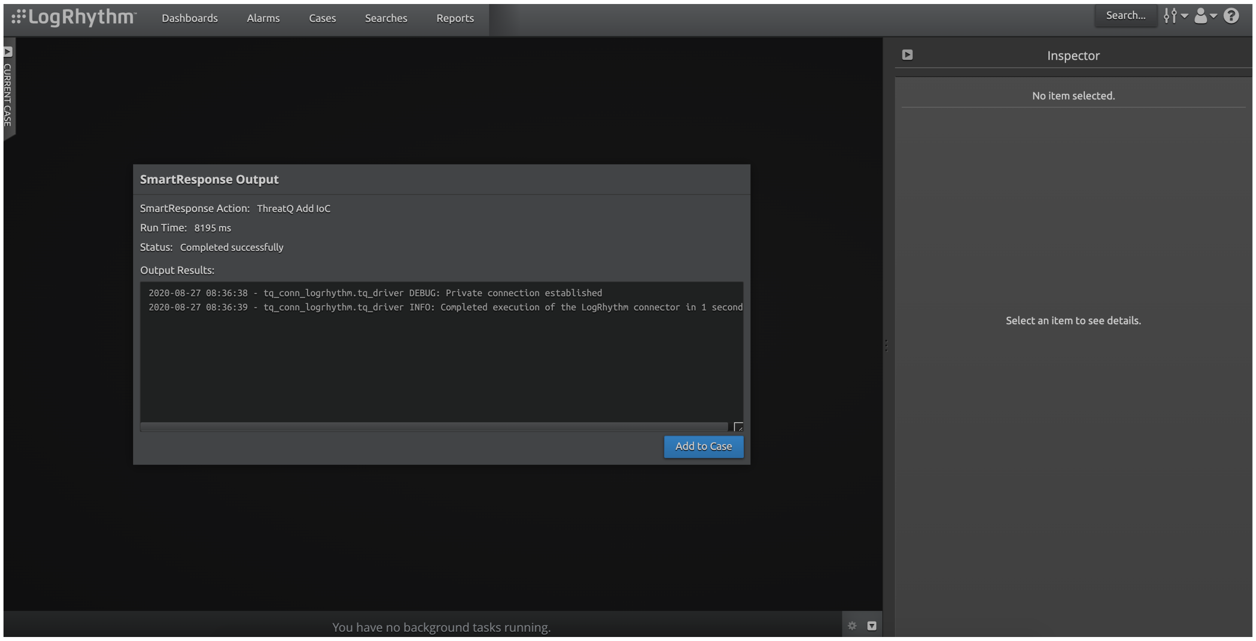
Ioc Value: 194.145.63.12

Ioc Attributes [name:value,name2:value2]: Please Select

Command to Execute: C:\Python27\Scripts\tq-add-ioc.exe IP Address 194.145.63.12 --attribute

Execute from: Platform Manager

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



SmartResponse Output

SmartResponse Action: ThreatQ Add IoC

Run Time: 8195 ms

Status: Completed successfully

Output Results:

```
2020-08-27 08:36:38 - tq_conn_logrhythm.tq_driver DEBUG: Private connection established
2020-08-27 08:36:39 - tq_conn_logrhythm.tq_driver INFO: Completed execution of the LogRhythm connector in 1 second
```

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.

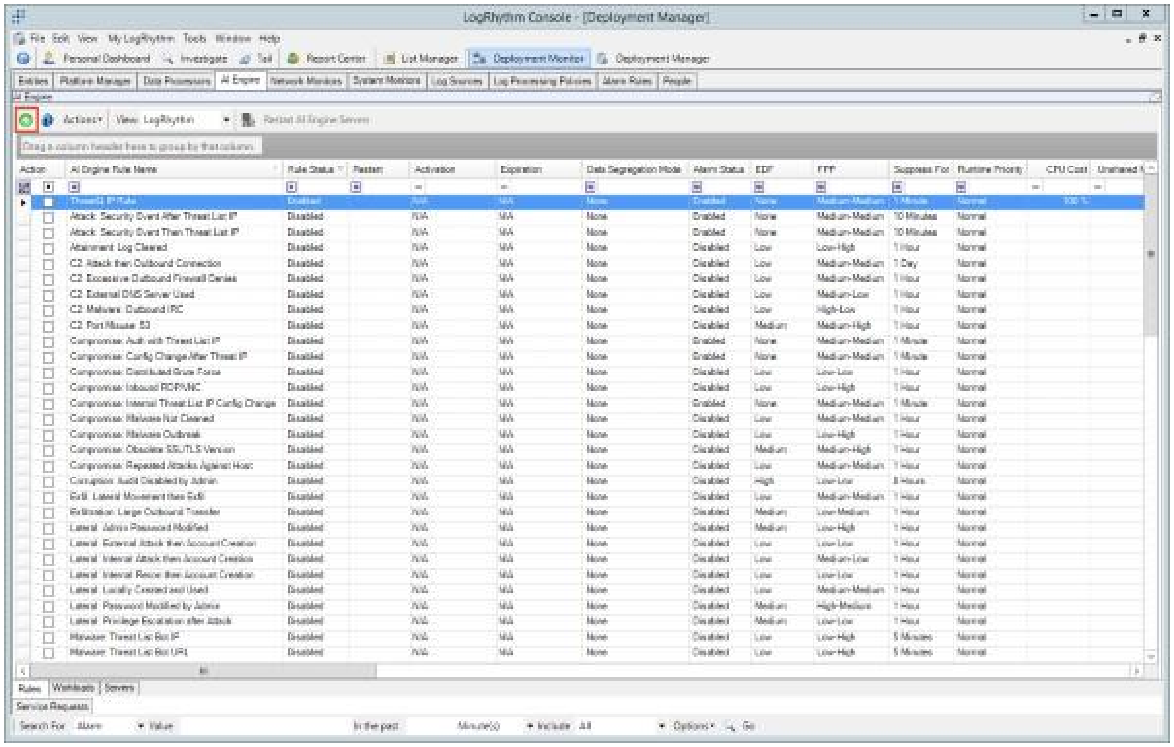
> The ThreatQ Add Sighting action is accessible through this interface but is not usable here. This action is to be used only in the Client Console when configuring AI Engine Rules. This is used to bring over a Case as a "Sighting" type Event in ThreatQ, including the observed IOCs.

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.

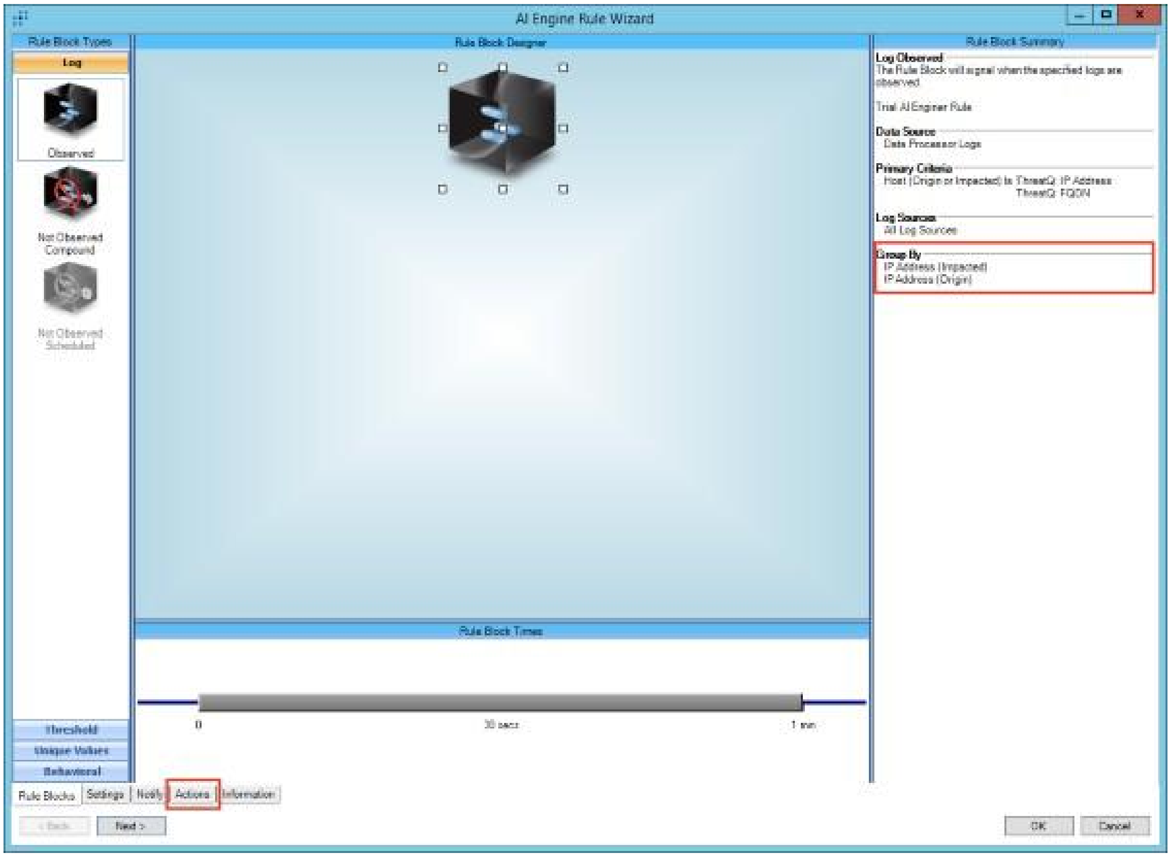
To provide the most flexible solution to capture all possible Sightings, the ThreatQ Add Sighting SRP has options for all known IOC fields. To add a rule that has uses this SRP:

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.



Action	AI Engine Rule Name	Rule Status	Restart	Activation	Expiration	Data Segregation Mode	Alarm Status	EDF	FPP	Suppress For	Runtime Priority	CPU Cost	Unshared
☐	ThreatQ IP Rule	Disabled		N/A	N/A	None	Disabled	None	Medium-Medium	1 Minute	Normal	100 %	
☐	Attack: Security Event After Threat List IP	Disabled		N/A	N/A	None	Enabled	None	Medium-Medium	10 Minutes	Normal		
☐	Attack: Security Event Then Threat List IP	Disabled		N/A	N/A	None	Enabled	None	Medium-Medium	10 Minutes	Normal		
☐	Attainment: Log Cleared	Disabled		N/A	N/A	None	Disabled	Low	Low-High	1 Hour	Normal		
☐	C2: Attack then Outbound Connection	Disabled		N/A	N/A	None	Disabled	Low	Medium-Medium	1 Day	Normal		
☐	C2: Excessive Outbound Firewall Denies	Disabled		N/A	N/A	None	Disabled	Low	Medium-Medium	1 Hour	Normal		
☐	C2: External DNS Server Used	Disabled		N/A	N/A	None	Disabled	Low	Medium-Low	1 Hour	Normal		
☐	C2: Malware: Outbound IRC	Disabled		N/A	N/A	None	Disabled	Low	High-Low	1 Hour	Normal		
☐	C2: Port Misuse: 53	Disabled		N/A	N/A	None	Disabled	Medium	Medium-High	1 Hour	Normal		
☐	Compromise: Auth with Threat List IP	Disabled		N/A	N/A	None	Enabled	None	Medium-Medium	1 Minute	Normal		
☐	Compromise: Config Change After Threat IP	Disabled		N/A	N/A	None	Enabled	None	Medium-Medium	1 Minute	Normal		
☐	Compromise: Distributed Brute Force	Disabled		N/A	N/A	None	Disabled	Low	Low-Low	1 Hour	Normal		
☐	Compromise: Inbound RDP/VNC	Disabled		N/A	N/A	None	Disabled	Low	Low-High	1 Hour	Normal		
☐	Compromise: Internal Threat List IP Config Change	Disabled		N/A	N/A	None	Enabled	None	Medium-Medium	1 Minute	Normal		
☐	Compromise: Malware Not Cleaned	Disabled		N/A	N/A	None	Disabled	Low	Medium-Medium	1 Hour	Normal		
☐	Compromise: Malware Outbreak	Disabled		N/A	N/A	None	Disabled	Low	Low-High	1 Hour	Normal		
☐	Compromise: Obsolete SSL/TLS Version	Disabled		N/A	N/A	None	Disabled	Medium	Medium-High	1 Hour	Normal		
☐	Compromise: Repeated Attacks Against Host	Disabled		N/A	N/A	None	Disabled	Low	Medium-Medium	1 Hour	Normal		
☐	Corruption: Audit Disabled by Admin	Disabled		N/A	N/A	None	Disabled	High	Low-Low	8 Hours	Normal		
☐	Exfil: Lateral Movement then Exfil	Disabled		N/A	N/A	None	Disabled	Low	Medium-Medium	1 Hour	Normal		
☐	Exfiltration: Large Outbound Transfer	Disabled		N/A	N/A	None	Disabled	Medium	Low-Medium	1 Hour	Normal		
☐	Lateral: Admin Password Modified	Disabled		N/A	N/A	None	Disabled	Medium	Low-High	1 Hour	Normal		
☐	Lateral: External Attack then Account Creation	Disabled		N/A	N/A	None	Disabled	Low	Low-Low	1 Hour	Normal		
☐	Lateral: Internal Attack then Account Creation	Disabled		N/A	N/A	None	Disabled	Low	Medium-Low	1 Hour	Normal		
☐	Lateral: Internal Recon then Account Creation	Disabled		N/A	N/A	None	Disabled	Low	Low-Low	1 Hour	Normal		
☐	Lateral: Locally Created and Used	Disabled		N/A	N/A	None	Disabled	Low	Medium-Medium	1 Hour	Normal		
☐	Lateral: Password Modified by Admin	Disabled		N/A	N/A	None	Disabled	Medium	High-Medium	1 Hour	Normal		
☐	Lateral: Privilege Escalation after Attack	Disabled		N/A	N/A	None	Disabled	Medium	Low-Low	1 Hour	Normal		
☐	Malware: Threat List Bot IP	Disabled		N/A	N/A	None	Disabled	Low	Low-High	5 Minutes	Normal		
☐	Malware: Threat List Bot URL	Disabled		N/A	N/A	None	Disabled	Low	Low-High	5 Minutes	Normal		

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



Log Observed
The Rule Block will signal when the specified logs are observed

Trial AI Enginer Rule

Data Source
Data Processor Logs

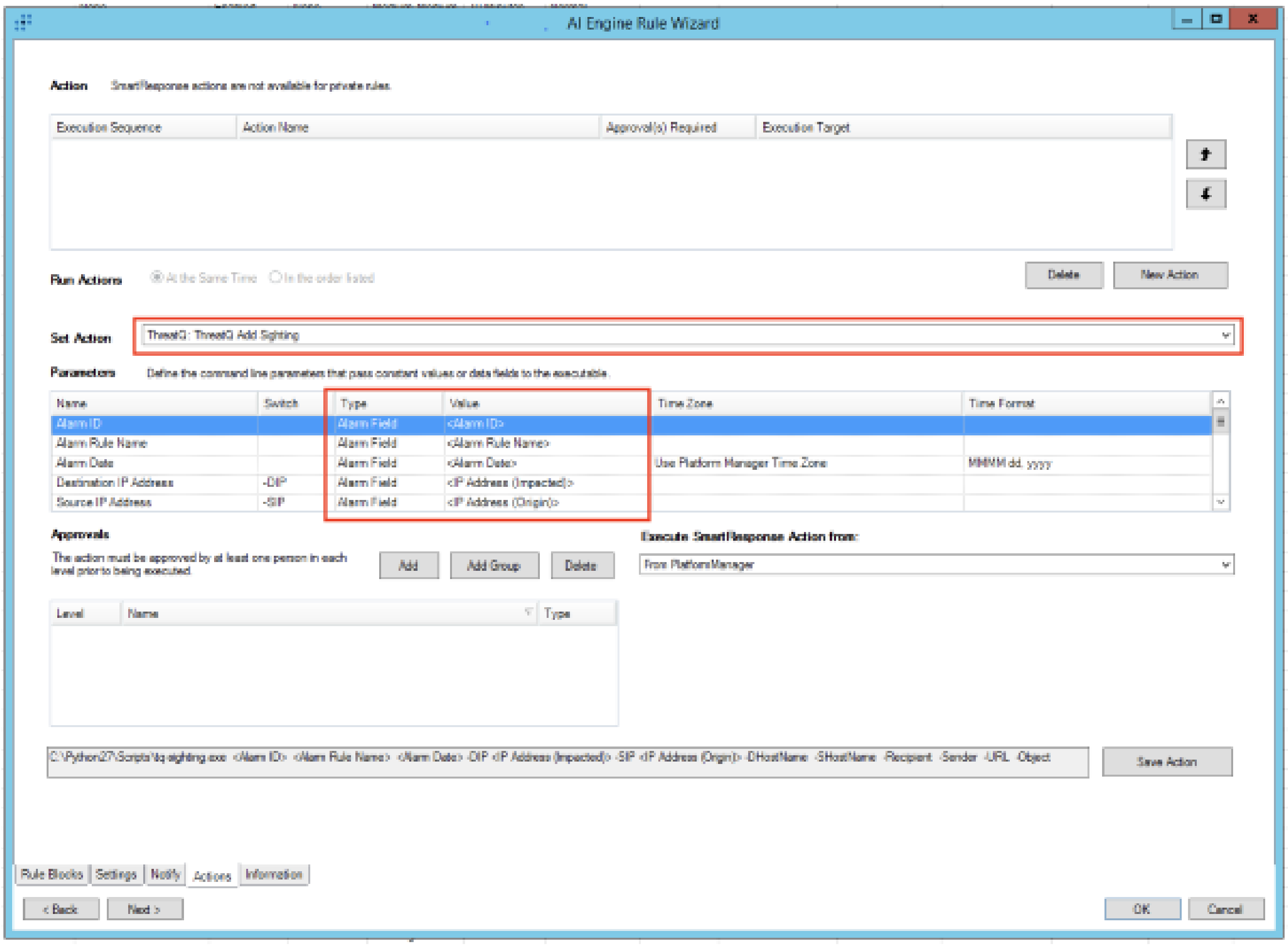
Primary Criteria
Host (Origin or Impacted) Is ThreatQ: IP Address
ThreatQ: FQDN

Log Sources
All Log Sources

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.



Action SmartResponse actions are not available for private rules.

Execution Sequence	Action Name	Approval(s) Required	Execution Target

Run Actions ● At the Same Time ○ In the order listed

Set Action: ThreatQ : ThreatQ Add Sighting

Parameters Define the command line parameters that pass constant values or data fields to the executable.

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>	Use Platform Manager Time Zone	MMMM dd, yyyy
Destination IP Address	-DIP	Alarm Field	<IP Address (Impacted)>		
Source IP Address	-SIP	Alarm Field	<IP Address (Origin)>		

Approvals

The action must be approved by at least one person in each level prior to being executed.

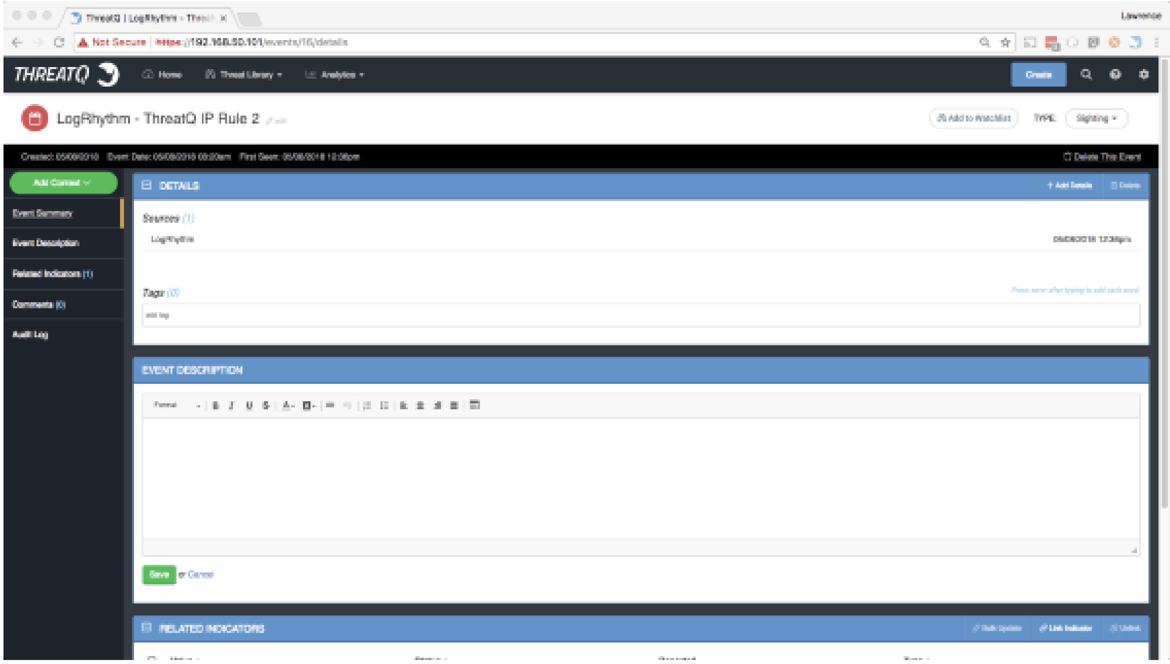
Level	Name	Type

Execute SmartResponse Action from: From PlatformManager

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

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 the Alarm Date value, modify the Time Format to yyyy-MM-dd HH:mm:ss
7. For all other fields, change the Type from Alarm Field to Constant Value. 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.

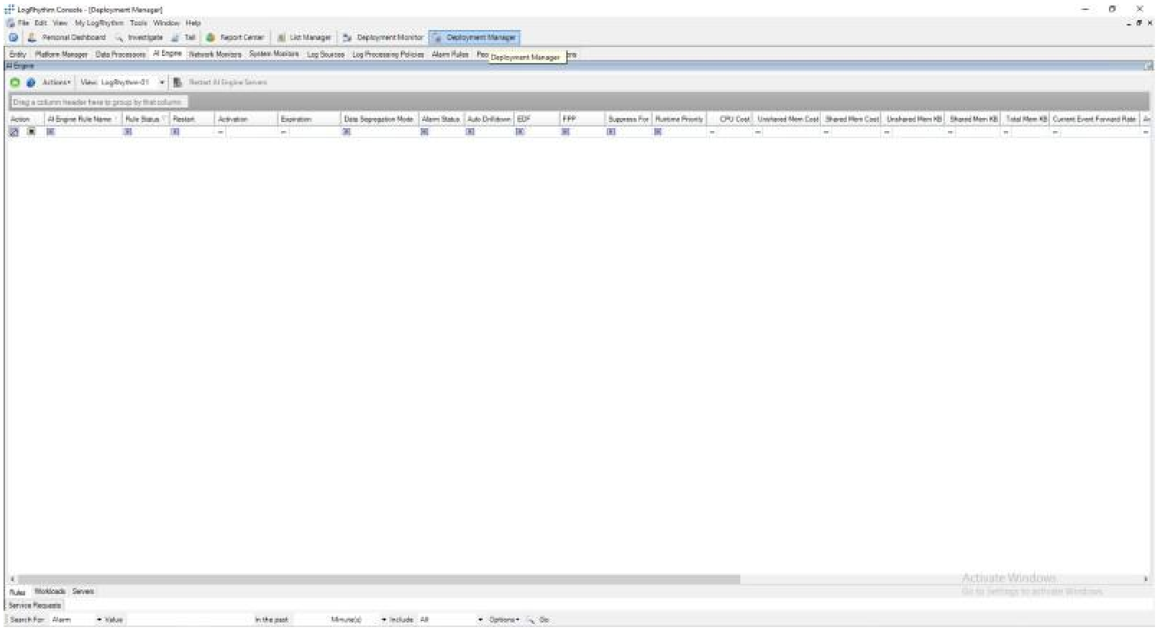
Setup Alarm Rules

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 sources, 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. (Settings → Incoming Feeds → TQ Labs → LogRhythm).

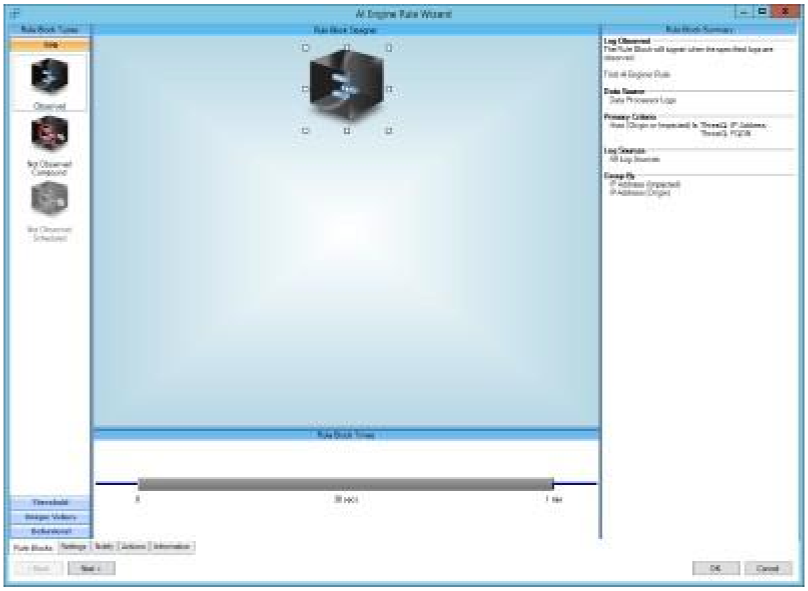
These lists can be used in conjunction with the LogRhythm AI Engine to determine correlations against incoming log data.

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.



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



Log Observed
The Rule Block will signal when the specified logs are observed

Trial AI Engine Rule

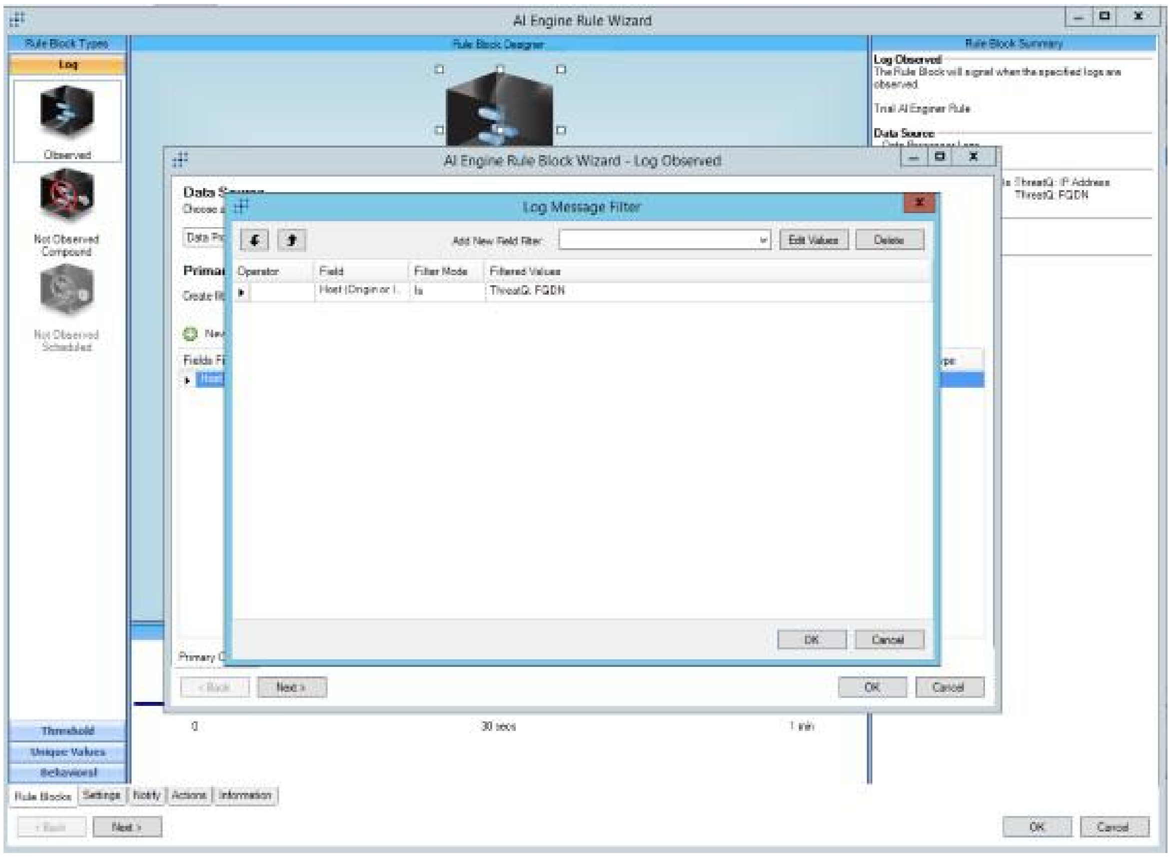
Data Source
Data Processor Logs

Primary Criteria
Host (Origin or Impacted) Is ThreatQ: IP Address,
ThreatQ: FQDN

Log Sources
All Log Sources

Group By
IP Address (Impacted)
IP Address (Origin)

4. 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.



Log Observed
The Rule Block will signal when the specified logs are observed

Trial AI Engine Rule

Data Source

Is ThreatQ: IP Address
ThreatQ: FQDN

Operator	Field	Filter Mode	Filtered Values
	Host (Origin or I...	Is	ThreatQ: FQDN

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.

Testing the 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 data collection 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 don’t yet have, please 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 (paths to the config and log folders and the verbosity level) 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.
5. Run the connector using this command
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).

    > The lists created will be determined by your YAML configuration.

    c. Make sure each list contains the same number of indicators as in the data collection

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).

1. RDP into the LogRhythm server.
2. Install the custom connector. If you don’t yet have, please 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 to ThreatQ

```
C:\Python27\Scripts\tq-sighting.exe <Alarm ID>

<Alarm Name> <Alarm Date> -SIP <IP Address (Origin)> -DIP <IP

Address (Destination)> -DHostName -SHostName <Host (Origin)> -

Recipient -Sender -URL -Object -c <Config Location> -ll <Logs

Location> -v <Log Verbosity Level – 1,2,3>

# Example

C:\Python27\Scripts\tq-sighting.exe 123 "ThreatQ

Blocklist" "2020-08-25 20:20:20" -SIP 156.86.198.45 -DIP 157.86.198.45 -c L:
\ThreatQ\config\ -ll L:\ThreatQ\logs\ -v3
```

Add IOC to ThreatQ

```
C:\Python27\Scripts\tq-add-ioc.exe "<Indicator Type>" <Indicator Value> [--attribute
"[attr1:val1,attr2:val2]"] -c <Config Location> -ll <Logs Location> -v <Log Verbosity
Level – 1,2,3>

# Example

C:\Python27\Scripts\tq-add-ioc.exe "IP Address" 77.77.77.77 --attribute "False
Positive:Yes,Confidence:High" -c L:\ThreatQ\config\ -ll L:\ThreatQ\logs\ -v3
```

Lookup IOC from ThreatQ

```
C:\Python27\Scripts\tq-lookup.exe "<Indicator Type>" <Indicator Value> -c <Config
Location> -ll <Logs Location> -v <Log Verbosity Level – 1,2,3>

# Example

C:\Python27\Scripts\tq-lookup.exe "IP Address" 77.77.77.77 -c L:\ThreatQ\config\ -ll L:
\ThreatQ\logs\ -v3
```

Mark IOC as False Positive in ThreatQ

```
C:\Python27\Scripts\tq-mark-false-positive.exe "<Indicator Type>" <Indicator Value>
-c <Config Location> -ll <Logs Location> -v <Log Verbosity Level – 1,2,3>

# Example

C:\Python27\Scripts\tq-mark-false-positive.exe "IP Address" 77.77.77.77 -c L:
\ThreatQ\config\ -ll L:\ThreatQ\logs\ -v3
```

Mark IOC as True Positive in ThreatQ

```
C:\Python27\Scripts\tq-mark-true-positive.exe "<Indicator Type>" <Indicator Value>
-c <Config Location> -ll <Logs Location> -v <Log Verbosity Level – 1,2,3>

# Example

C:\Python27\Scripts\tq-mark-true-positive.exe "IP Address" 77.77.77.77 -c L:
\ThreatQ\config\ -ll L:\ThreatQ\logs\ -v3
```

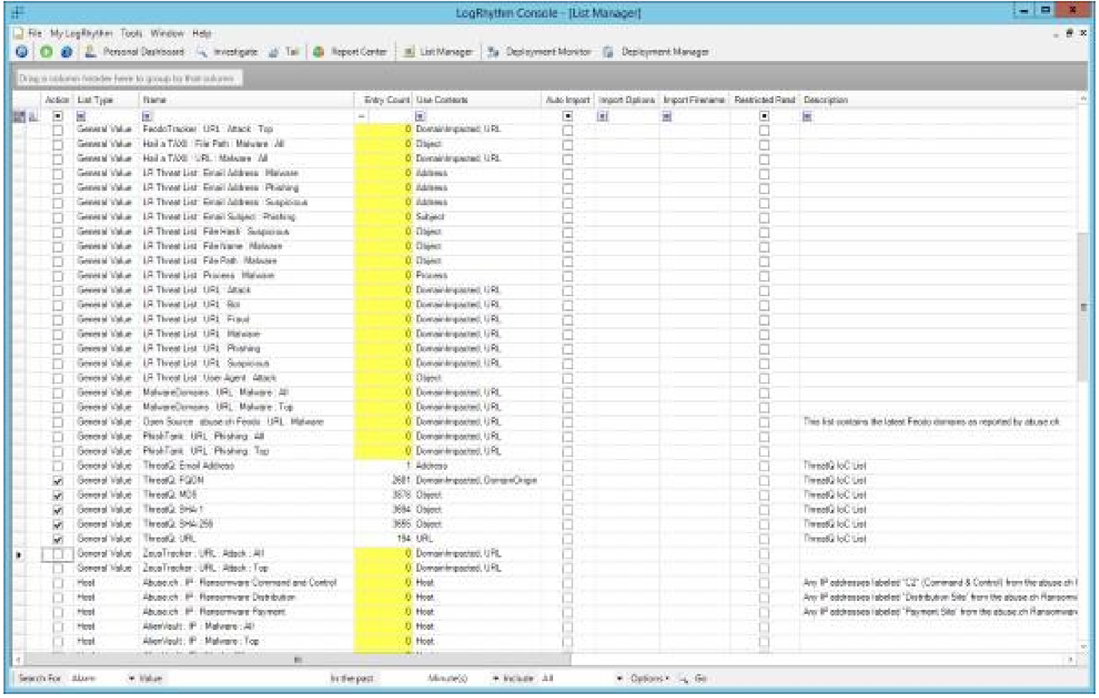
Change the Status of IOC to “Whitelist” in ThreatQ

```
C:\Python27\Scripts\tq-whitelist-ioc.exe "<Indicator Type>" <Indicator Value> -c
<Config Location> -ll <Logs Location> -v <Log Verbosity Level – 1,2,3>

# Example

C:\Python27\Scripts\tq-whitelist-ioc.exe "IP Address" -c L:\ThreatQ\config\ -ll L:
\ThreatQ\logs\ -v3
```

Uninstall Integration

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.

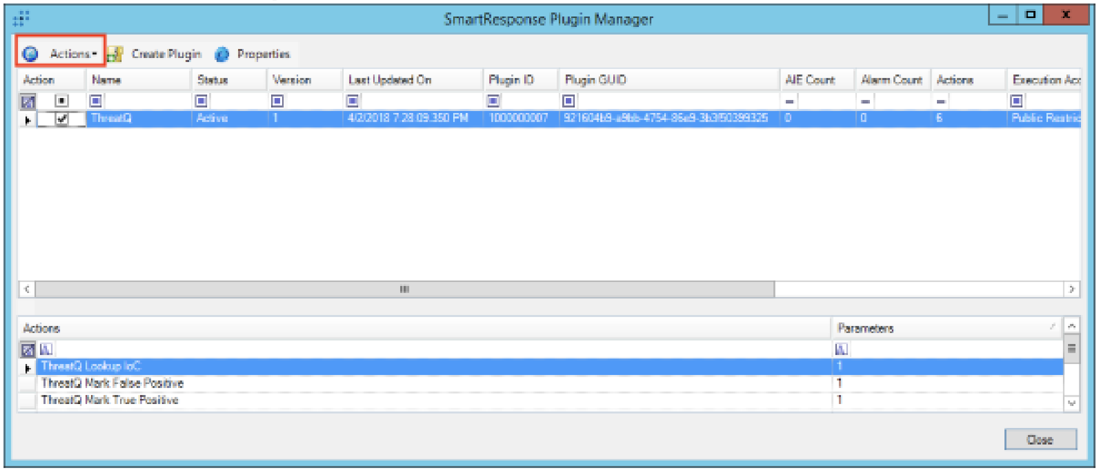
1. Stop the Windows Job for synchronization.
2. Deactivate all of the Lists created by ThreatQ.
    a. Open the List Manager.
    b. Check All Lists created by ThreatQ.



Action	List Type	Name	Entry Count	Use Contexts	Auto Import	Import Options	Import Filename	Restricted Read	Description
□	General Value	FeodoTracker : URL : Attack : Top	0	DomainImpacted, URL	□			□	
□	General Value	Hail a TAXII : File Path : Malware : All	0	Object	□			□	
□	General Value	Hail a TAXII : URL : Malware : All	0	DomainImpacted, URL	□			□	
□	General Value	LR Threat List : Email Address : Malware	0	Address	□			□	
□	General Value	LR Threat List : Email Address : Phishing	0	Address	□			□	
□	General Value	LR Threat List : Email Address : Suspicious	0	Address	□			□	
□	General Value	LR Threat List : Email Subject : Phishing	0	Subject	□			□	
□	General Value	LR Threat List : File Hash : Suspicious	0	Object	□			□	
□	General Value	LR Threat List : File Name : Malware	0	Object	□			□	
□	General Value	LR Threat List : File Path : Malware	0	Object	□			□	
□	General Value	LR Threat List : Process : Malware	0	Process	□			□	
□	General Value	LR Threat List : URL : Attack	0	DomainImpacted, URL	□			□	
□	General Value	LR Threat List : URL : Bot	0	DomainImpacted, URL	□			□	
□	General Value	LR Threat List : URL : Fraud	0	DomainImpacted, URL	□			□	
□	General Value	LR Threat List : URL : Malware	0	DomainImpacted, URL	□			□	
□	General Value	LR Threat List : URL : Phishing	0	DomainImpacted, URL	□			□	
□	General Value	LR Threat List : URL : Suspicious	0	DomainImpacted, URL	□			□	
□	General Value	LR Threat List : User Agent : Attack	0	Object	□			□	
□	General Value	MalwareDomains : URL : Malware : All	0	DomainImpacted, URL	□			□	
□	General Value	MalwareDomains : URL : Malware : Top	0	DomainImpacted, URL	□			□	
□	General Value	Open Source : abuse.ch Feodo : URL : Malware	0	DomainImpacted, URL	□			□	This list contains the latest Feodo domains as reported by abuse.ch
□	General Value	PhishTank : URL : Phishing : All	0	DomainImpacted, URL	□			□	
□	General Value	PhishTank : URL : Phishing : Top	0	DomainImpacted, URL	□			□	
□	General Value	ThreatQ: Email Address	1	Address	□			□	ThreatQ IoC List
☑	General Value	ThreatQ: FQDN	2681	DomainImpacted, DomainOrigin	□			□	ThreatQ IoC List
☑	General Value	ThreatQ: MD5	3878	Object	□			□	ThreatQ IoC List
☑	General Value	ThreatQ: SHA-1	3684	Object	□			□	ThreatQ IoC List
☑	General Value	ThreatQ: SHA-256	3685	Object	□			□	ThreatQ IoC List
☑	General Value	ThreatQ: URL	194	URL	□			□	ThreatQ IoC List
□	General Value	ZeusTracker : URL : Attack : All	0	DomainImpacted, URL	□			□	
□	General Value	ZeusTracker : URL : Attack : Top	0	DomainImpacted, URL	□			□	
□	Host	Abuse.ch : IP : Ransomware Command and Control	0	Host	□			□	Any IP addresses labeled "C2" (Command & Control) from the abuse.ch I
□	Host	Abuse.ch : IP : Ransomware Distribution	0	Host	□			□	Any IP addresses labeled "Distribution Site" from the abuse.ch Ransomw
□	Host	Abuse.ch : IP : Ransomware Payment	0	Host	□			□	Any IP addresses labeled "Payment Site" from the abuse.ch Ransomwar
□	Host	AlienVault : IP : Malware : All	0	Host	□			□	
□	Host	AlienVault : IP : Malware : Top	0	Host	□			□	

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

   c. Select the ThreatQ SRP and click Actions.



Action	Name	Status	Version	Last Updated On	Plugin ID	Plugin GUID	AIE Count	Alarm Count	Actions	Execution Acc
☑	ThreatQ	Active	1	4/2/2018 7:28:09.350 PM	1000000007	921604b9-a9bb-4754-86a9-3b3f50399325	0	0	6	Public Restric

Actions	Parameters
ThreatQ Lookup IoC	1
ThreatQ Mark False Positive	1
ThreatQ Mark True Positive	1

   d. Click Retire.

4. Uninstall the integration.
   a. Open an Administrative cmd session.
   b. Navigate to C:\Python27\Scripts.
   c. Execute pip.exe uninstall tq-conn-logrhythm.
   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.

Change Log

- **Version 1.4.0**
    - Added backward compatibility for the integration with LogRhythm versions prior to version 7.5.1
- **Version 1.3.0**
    - Updated the integration for LogRhythm v7.6
    - Added a parameter to the ThreatQ UI Configuration for the LogRhythm user that will own the threat lists
- **Version 1.2.0**
    - Released a version for Python3
    - Migrated the integration to use the latest Threat Library in the ThreatQ SDK
    - Updated the examples
- **Version 1.1.1**
    - Changed the search from the Advanced Search to the Threat Library
    - Updated the Smart Response Plugin
- **Version 1.0.1**
    - Initial Release