Recorded Future®

LogRhythm Integration

Installation Instructions

Table of Contents

Introduction

Recorded Future integrates seamlessly with LogRhythm, delivering intelligence that is timely, accurate, and actionable. By enriching your LogRhythm workflow with real-time intelligence from Recorded Future, you can expect to identify more security threats before impact, resolve security threats faster, and increase team efficiency.

This installation guide will walk you step by step through a basic installation of Recorded Future Threat Intelligence via LogRhythm's Threat Intelligence Service Manager. Recorded Future has many sets of malicious indicators (aka "collections") available via its STIX/TAXII server; this installation guide will help you install two important collections. Once installed, these (and other collections you configure) can be used to setup AI Engine Rules to trigger alarms in LogRhythm. Recorded Future provides high risk indicators for the following entity types:

- IP Addresses
- Domains
- URLs
- Files Hashes

You are encouraged to view this guide as a starting point, and as you grow the use of Threat Intelligence in your Security Operations workflows, we recommend that you revisit this integration to refine the threat intelligence being used and the specific correlation rules that are setup.

In addition, the Recorded Future browser extension provides automatic threat intelligence enrichment of any alerts or events in LogRhythm that include IPs, Domains, and Hashes. The section on "IOC Enrichment" has more detail about this, including where to find the browser extensions for download.

System Requirements

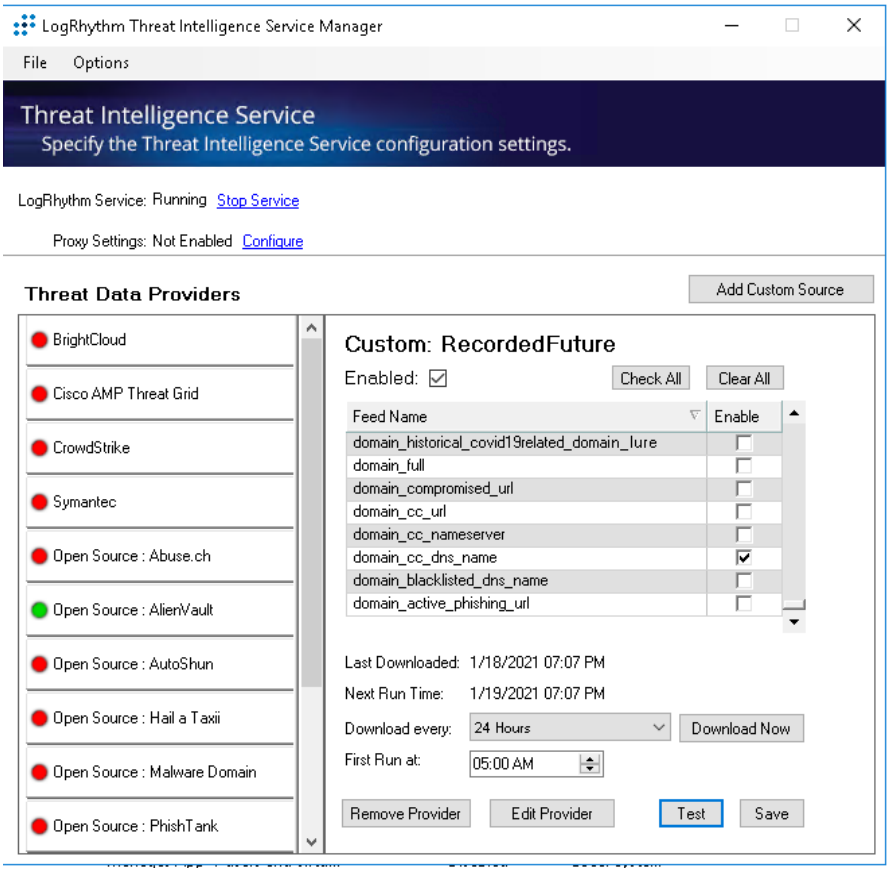
- LogRhythm version 7.6.0.9 or greater
- LogRhythm Threat Intelligence Service (TIS) Manager 1.9.3.1008 or greater
- Recorded Future subscription for the LogRhythm integration
- Access to https://api.recordedfuture.com/taxii enabled on the client firewall and proxy
- The Recorded Future browser extension (for IOC enrichment) is supported on the following browsers:
    - Google Chrome
    - Mozilla Firefox
    - Chromium-based Microsoft Edge browsers

Setting Up Threat Intelligence from Recorded Future

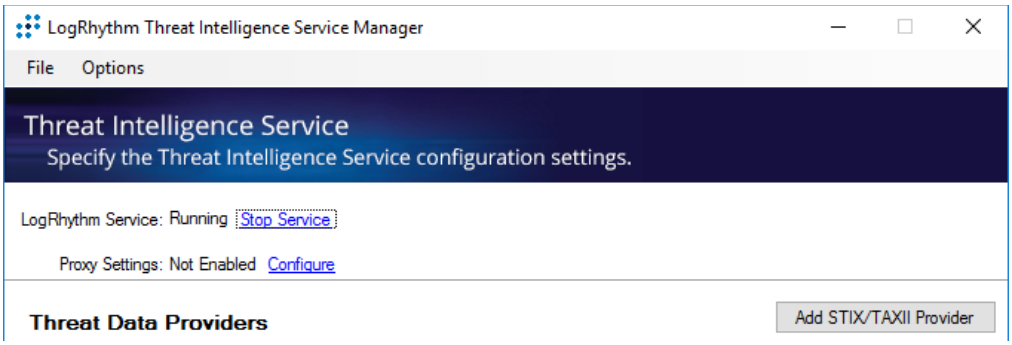
Example collection setup: malicious IPs

1. Confirm that you have installed and are running the “LogRhythm Threat Intelligence Service Manager”.
2. Obtain a Recorded Future API Token
    a. Ask your Recorded Future account team to provide one for you.
3. Login into the LogRhythm Server.

4. Open the "LogRhythm Threat Intelligence Service Manager".

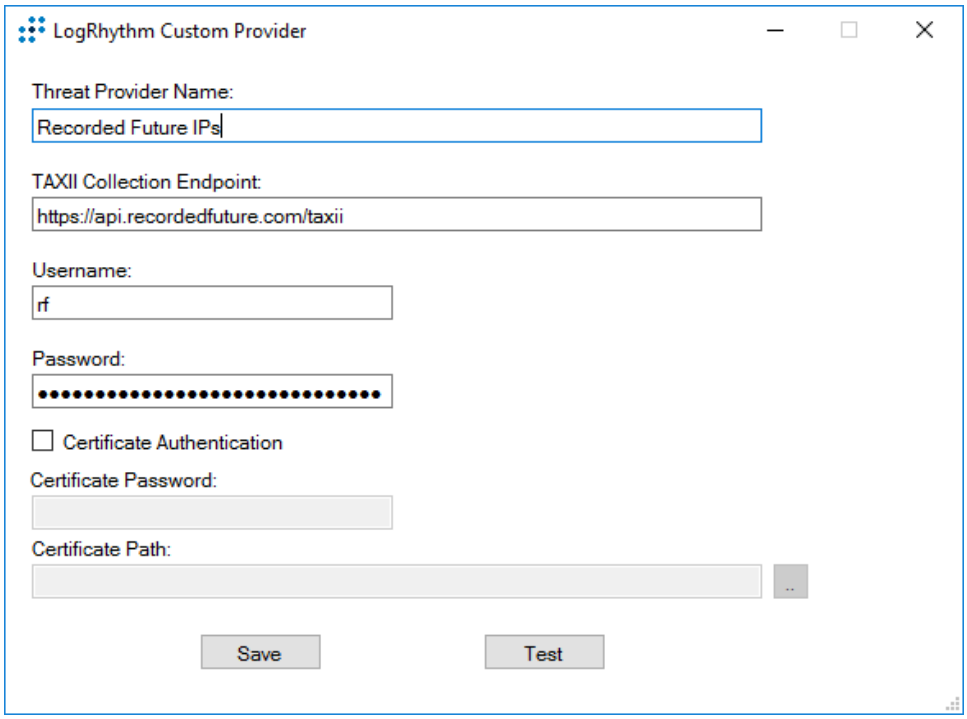


5. Click on the "Add STIX/TAXII Provider" button[1].

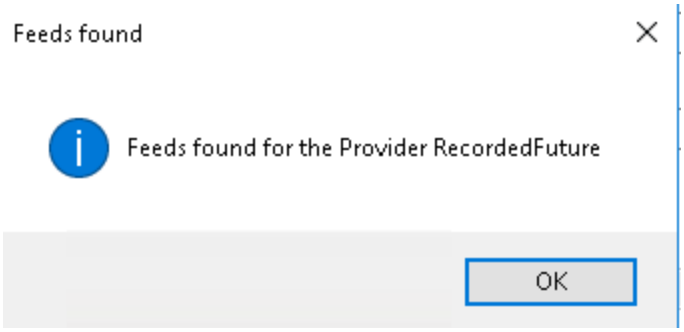


[1] For ease of maintenance, we recommend that you create separate STIX/TAXII providers for each indicator type (e.g., domains) you wish to utilize with Recorded Future Threat Intelligence. At present, the Recorded Future STIX TAXII server includes threat intelligence for IP addresses, domains, URLs, hashes, and vulnerabilities.

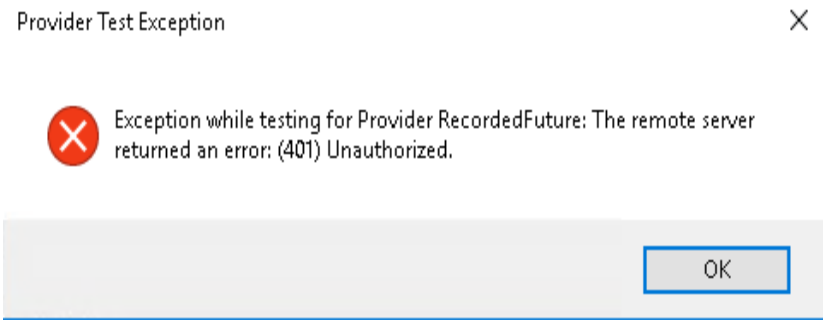
6. Fill in the following fields in the “LogRhythm Custom Provider”; here we will create a provider for high-risk IP Addresses.
    a. Threat Provider Name: Recorded Future IPs
    b. TAXII Collection Endpoint: https://api.recordedfuture.com/taxii
    c. Username: rf
    d. Password: {Recorded Future API token} (this is what you obtained in step 2 above)
7. Leave the rest of the Certificate fields blank



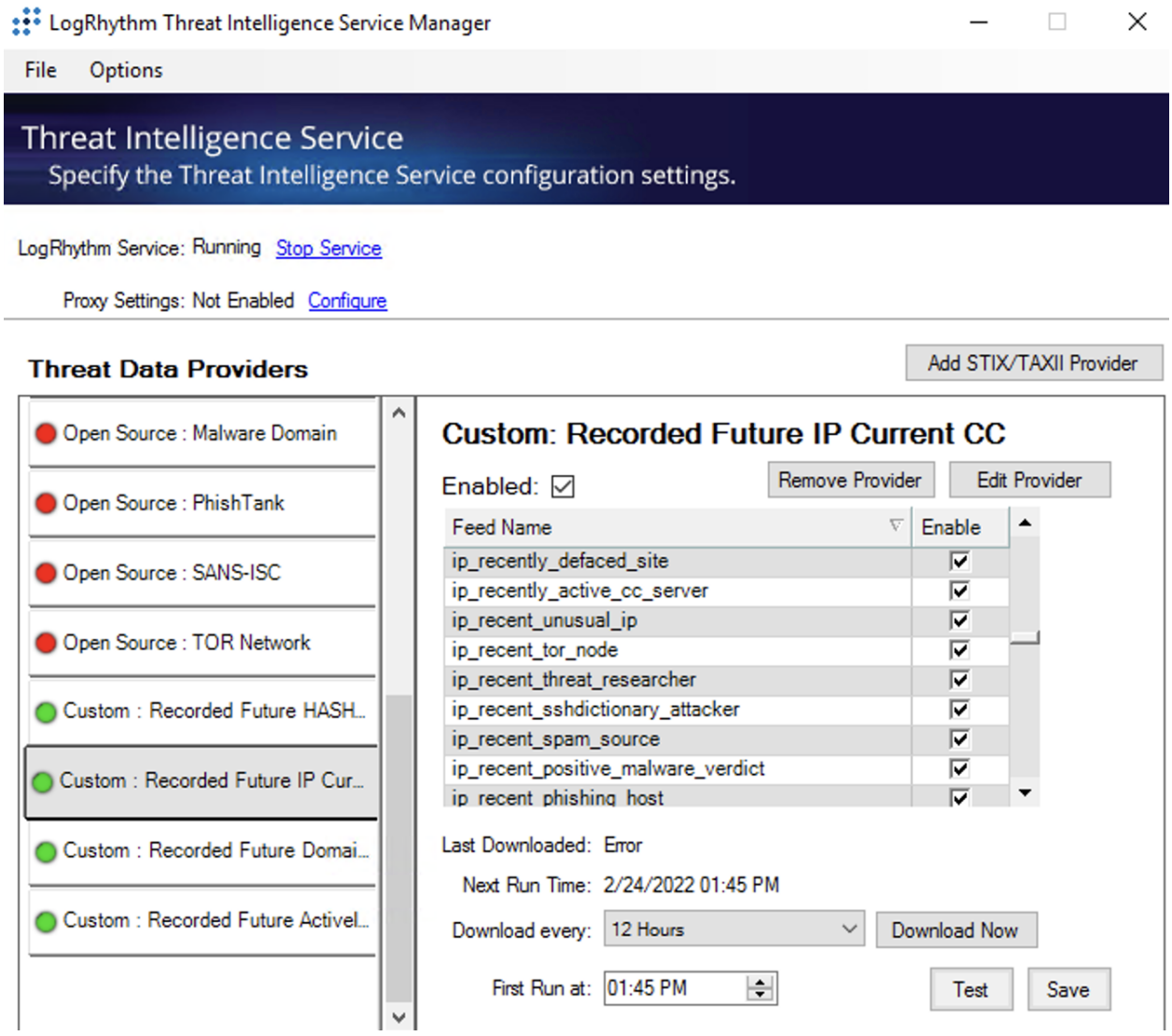
8. Click “Test” if the success popup will appear click “Save”.



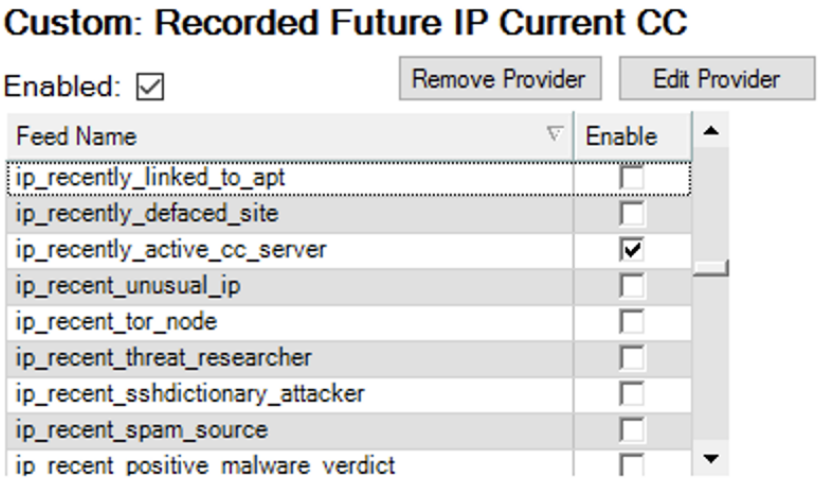
If you can receive an error message, double check the values you entered and try again.



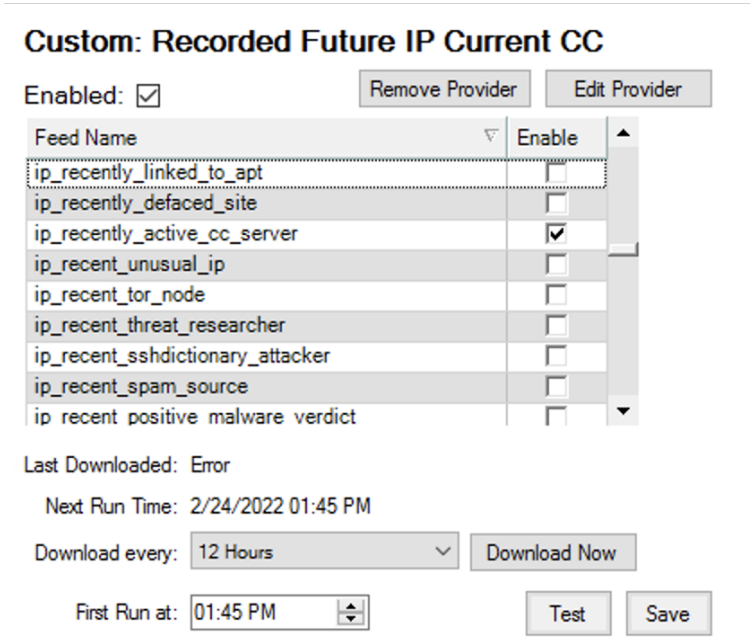
9. Click the “Enabled” button to turn on the regular import of Recorded Future Threat Intelligence



10. By default, all collections (aka "Feeds") are selected; uncheck all of the feeds except “ip_recently_active_cc_server”[2]



11. Make sure that the download frequency is set to “24 Hours” and click “Save”



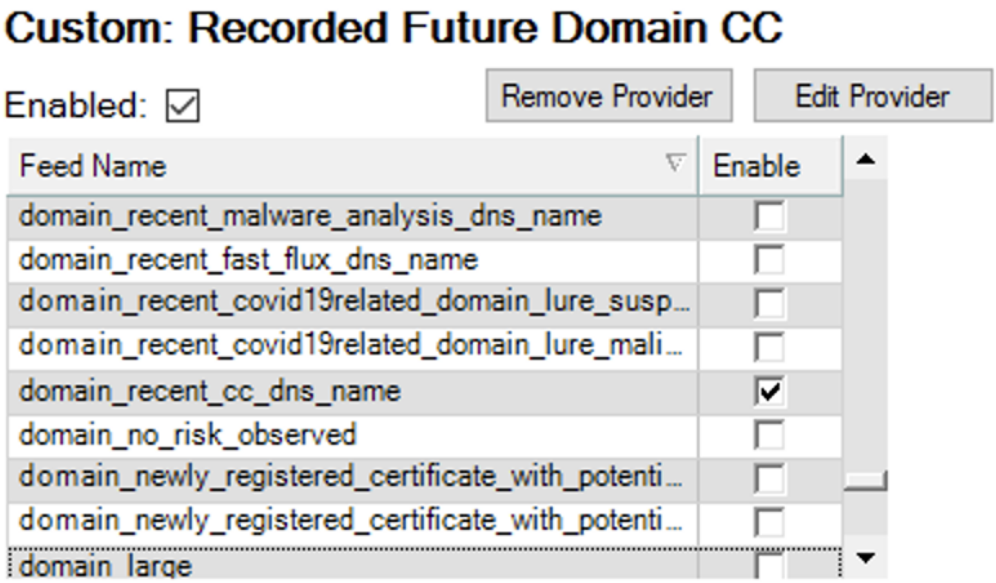
12. Congratulations! You have set up a daily recurring import of IP addresses associated with c2 servers; the available "feeds" on the Recorded Future STIX/TAXII server are associated with different "risk rules" that are used to identify

[2] This is a known behavior of LogRhythm, namely, when connecting to a new STIX TAXII service, LogRhythm will automatically try to download all available collections by default. In this example, we are showing how to set up LogRhythm to only download a single high risk set of IP addresses, with high confidence, that are known to be used for Command-and-Control (C2) servers.

risk. General information about risk rules is available on this support page[3]; specific details about IP address risk rules are here, and are represented by the different collections available. Analysts and security engineers may also want to look at this support page, which describes several common detection use cases and notes which Recorded Future collections best fulfill those use cases.

Example collection setup: malicious domains

1. To set up the ingest of another Threat Intelligence collection from Recorded Future, we will repeat steps 5-11 above except:
2. Use a different Threat Provider name for Step 6a, i.e., "Recorded Future Domains."
3. Uncheck all of the feeds except “domain_recent_cc_dns_name.”[4]



At this point, both STIX/TAXII feeds are set up.

Best Practices for Setting Up Data Providers

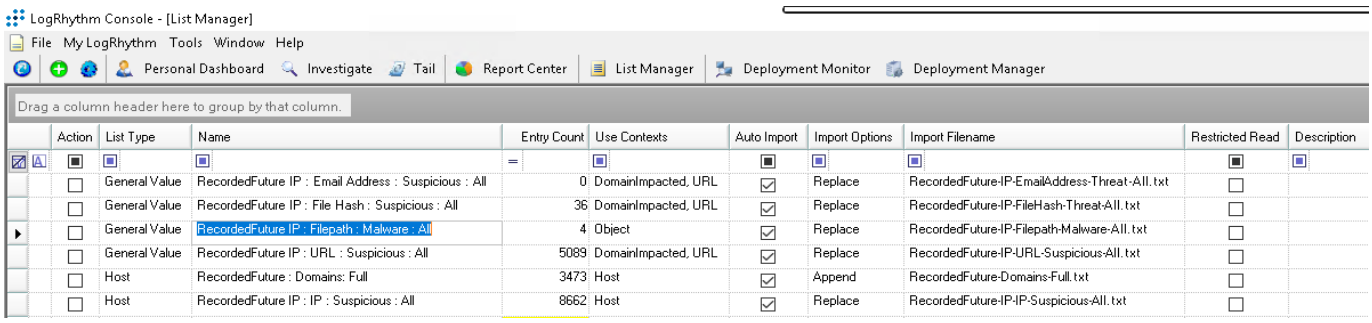
[3] Available to users with Recorded Future portal access.
[4] All collections on the Recorded Future STIX/TAXII server are prefaced with the indicator type name (e.g., "domains_") *except* IP addresses. This is because the STIX/TAXII server was originally set up with *only* IP address threat intelligence, and hence a type identifier prefix was unnecessary.

When setting up which feeds you would like to bring in, it can be helpful to go through the list of risk rules for each IOC type to figure out which rules or risk scores help to solve your organization's use cases. We typically recommend one data provider per use case, and naming the data providers something related to the feeds you are pulling (see examples in the "Integration Implementation" section) to make building out AI Engine Rules easier.

Confirm Recorded Future Threat Intelligence is loading correctly

Once the Recorded Future Threat Intelligence collections are configured in LogRhythm's TIS, you can log into the "LogRhythm Console" to view the lists and make sure they are populating correctly.

1. Once logged in, we can see the feeds we enabled being populated:



For each Threat Data Provider (defined in the Threat Intelligence Service Manager), LogRhythm will automatically create 5 corresponding lists in LogRhythm named similar to the Threat Data Provider. Depending on the type of Recorded Future Risk Lists selected for a specific Threat Data Provider, the corresponding LogRhythm list will be automatically populated. For example, when you select multiple data sets of the same type, or if you have a data set with both URLs and domains within a single Threat Data Provider, the IOCs get aggregated under the same LogRhythm list, as detailed below:

a. **[Name of Threat Data Provider] : File Hash : Suspicious : All** - will be populated with hash indicators if hash related risk lists are selected from Recorded Future
b. **[Name of Threat Data Provider] : URL : Suspicious : All** - will be populated with domains or URLs if domain or URL related risk lists are selected from Recorded Future
c. **[Name of Threat Data Provider] : IP : Suspicious : All** - will be populated with IP indicators if IP related risk lists are selected from Recorded Future

Entity List Mapping

The name of the Threat Data Provider sets the stage for which fields map to which lists when building out AI Engine Rules. It is important to note that if you use “IP” anywhere in the Threat Data Provider name, it will automatically set the List Type to “Host”, which locks the “Use Contexts” fields under “Additional Settings” in “List Properties”. This means that if you have anything other than IP feeds coming from this IP Threat Data Provider, they will not be categorized correctly by LogRhythm and therefore you will not be able to use them to correlate against entity types other than IP in the AI Engine Rules.

To get around this, we suggest naming your Threat Data Providers without specifying IP in the name, unless you know that a particular Threat Data Provider will be making only IP feeds available. Including other IOC types in the name, or not specifying an IOC type at all, will store the File Hash and URL lists as “General Value” List Types, and the IP list as a “Host” List Type. This allows you to correlate against any IOC type when creating AI Engine Rules. Since the IP list is of type “Host” it can still only be correlated against IPs, but the lists LogRhythm creates for the other IOC types will be free to correlate against any other field. Entity types that are not IPs cannot be correlated against lists that have a “Host” List Type.

Retire Unused Lists

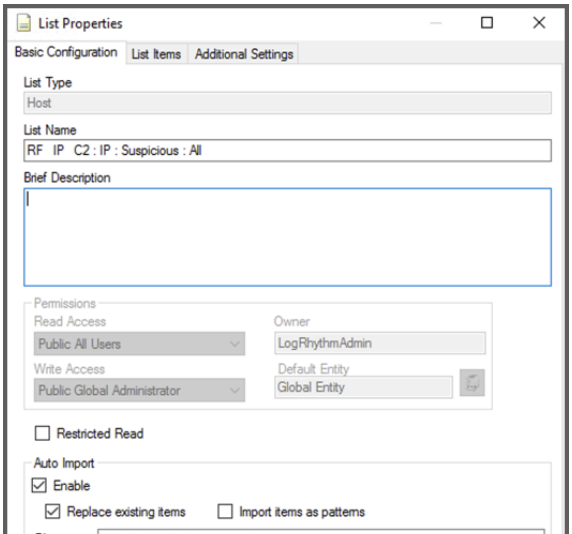
We recommend retiring unused lists in LogRhythm, or those with 0 entities.

1. In the LogRhythm Console, go to List Manager
2. Check the “Action” box next to the feeds you would like to get rid of
3. Right click anywhere on the screen
4. Go to Actions -> Retire -> Select “Yes”

Set up Time to Live (TTL)

To get rid of old lists as new ones are ingested, we need to set the TTL.

1. Open up the List Properties by double clicking on the list(s) with entries in them
2. Scroll down to TTL, check the “Expiring Items” box, and set the time of expiration
    a. We recommend setting this time somewhere around the same time interval you have set for the list to be ingested

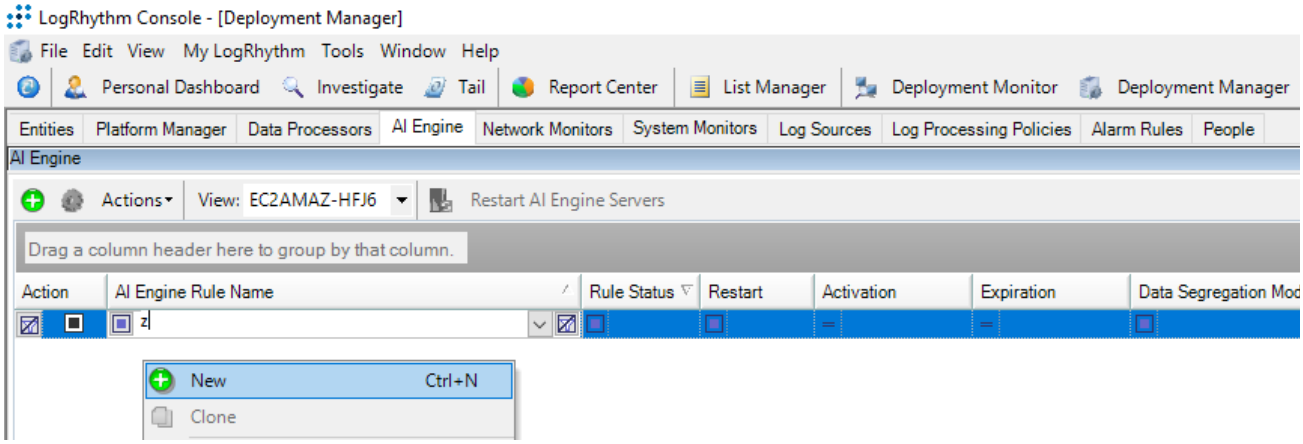


Using Threat Intelligence from Recorded Future

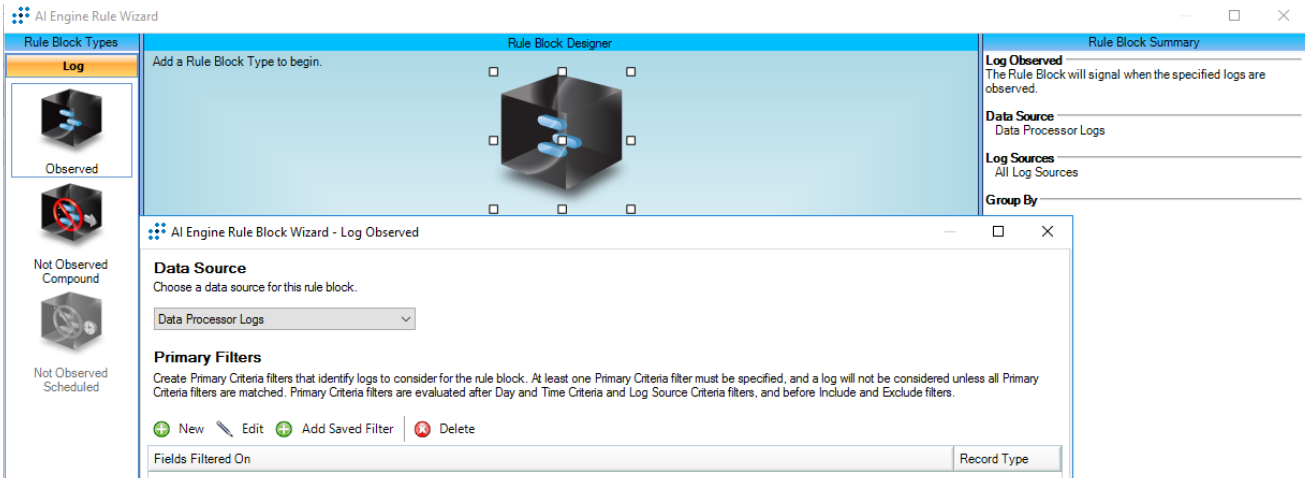
Example AI Engine Rule Setup - Recorded Future Malicious IPs

With Recorded Future Threat Intelligence being downloaded by LogRhythm, you can now create AI Engine rules to detect possible malicious traffic in your network.

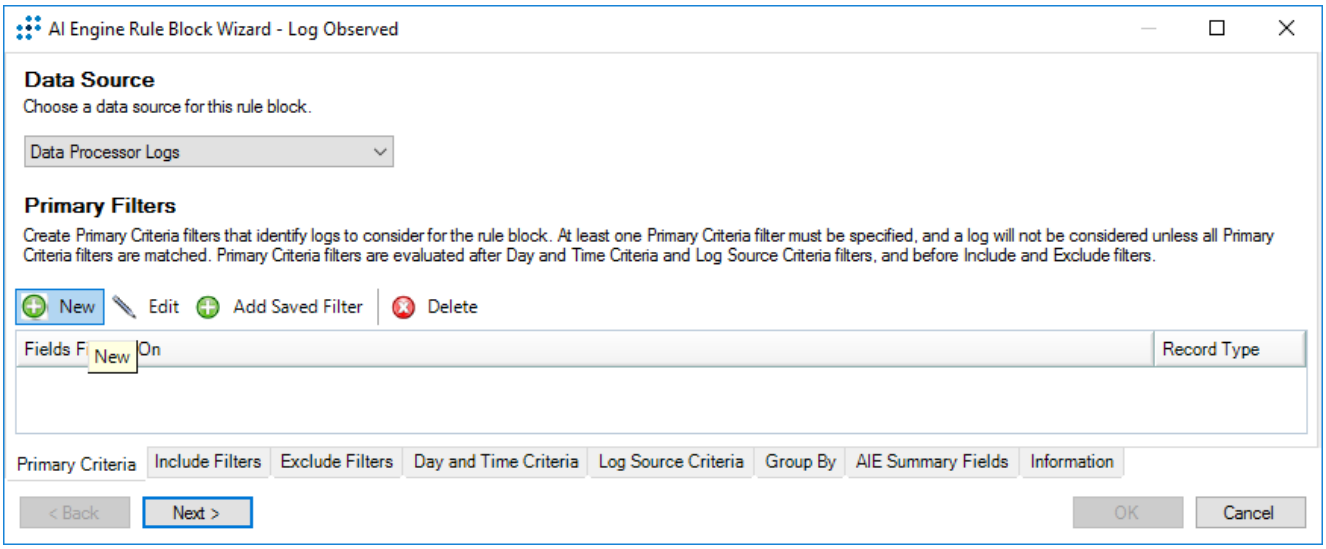
1. Navigate to the “AI Engine” Tab in the “Deployment Manager”.
2. In the white space below the list, right click to pull up a pop-up dialog box, and then click “New”.



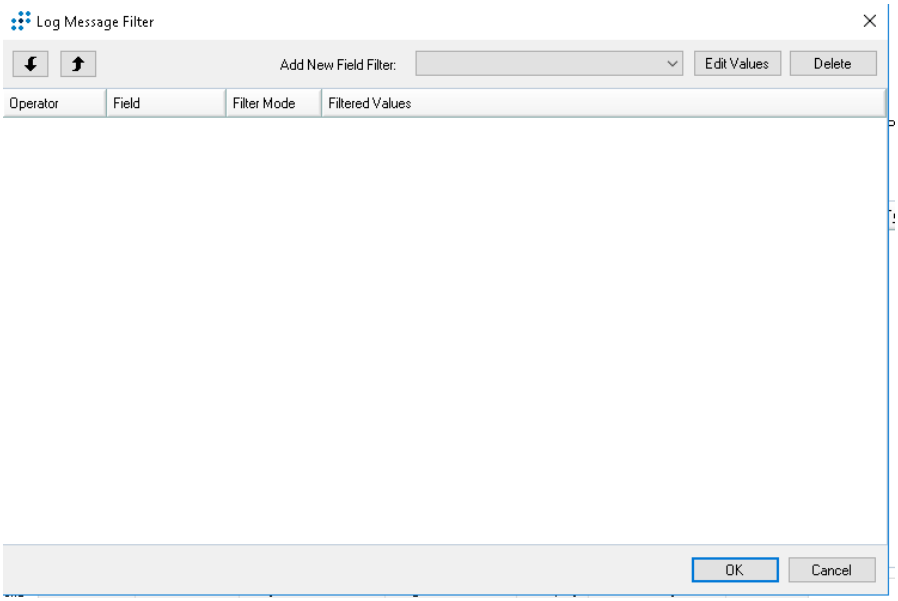
3. Drag the “Observed” cube on the left pane to the blue “Rule Block Designer” and double click the “Block”.



4. In the “Primary Criteria” tab click “New”

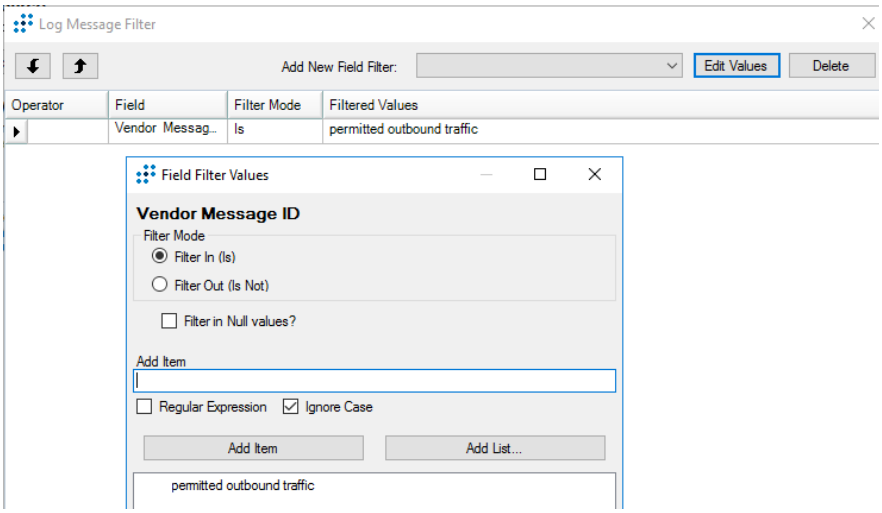


5. Then under “Add New Field Filter” choose “Vendor Message ID”

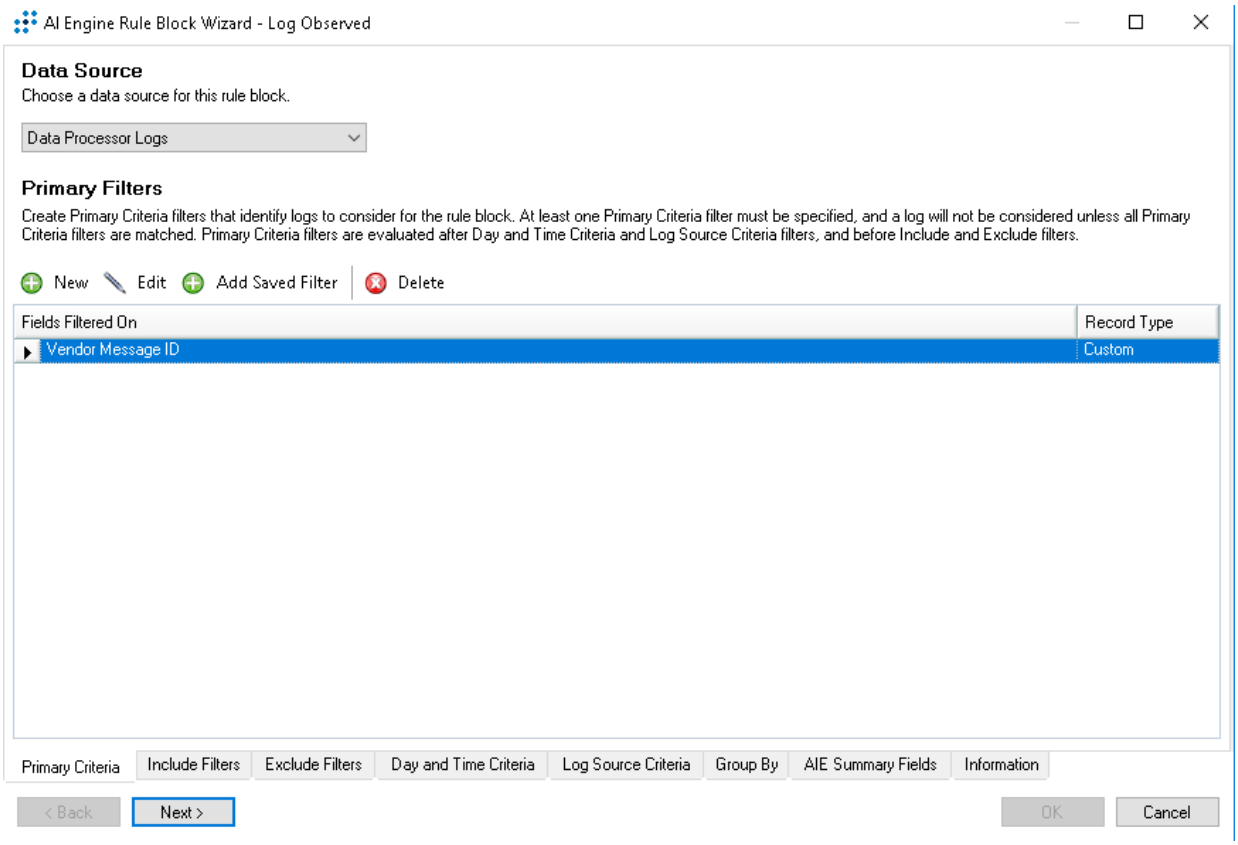


Next to “Add New Field Filter” choose “Vendor Message ID” . Then double click on white place

a. Filter Mode = Filter In (Is)
b. Under “Add Item” type “Permitted Outbound Traffic”
c. Click “Add Item”
d. Click “OK”

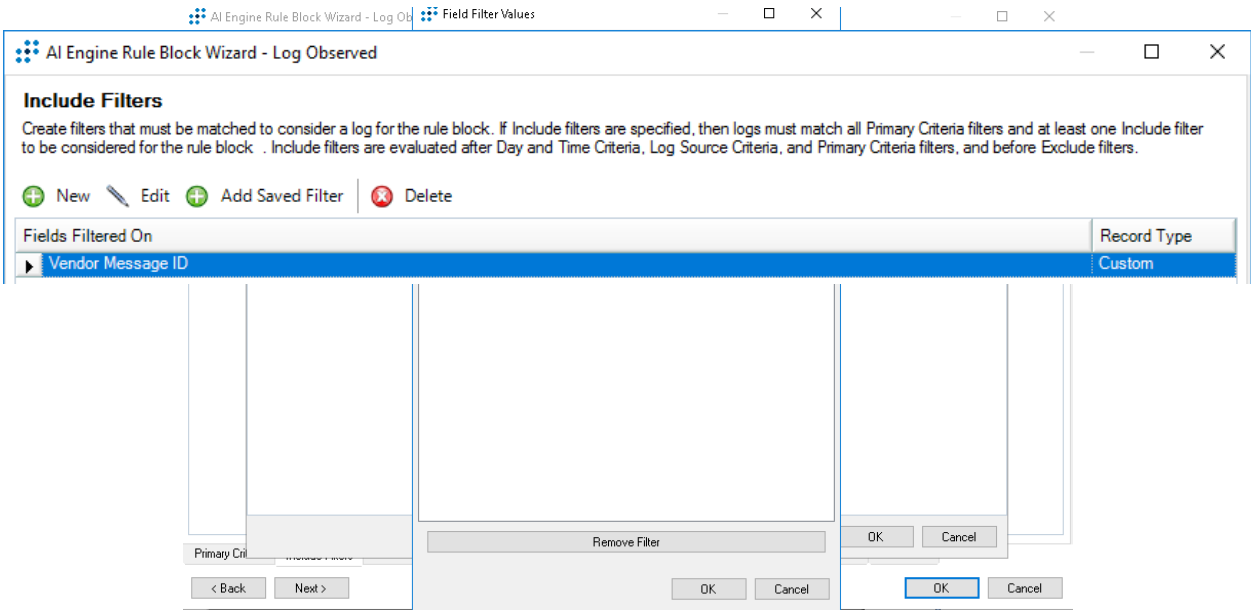


Click OK again to get to this screen again



6. Next click on the “Include Filters” tab and Click “New”
    a. Under “Add New Field Filter” choose “Host (Impacted)”
    b. Filter Mode = Filter In (Is)
    c. Under “Add List” choose the Recorded Future IP list:

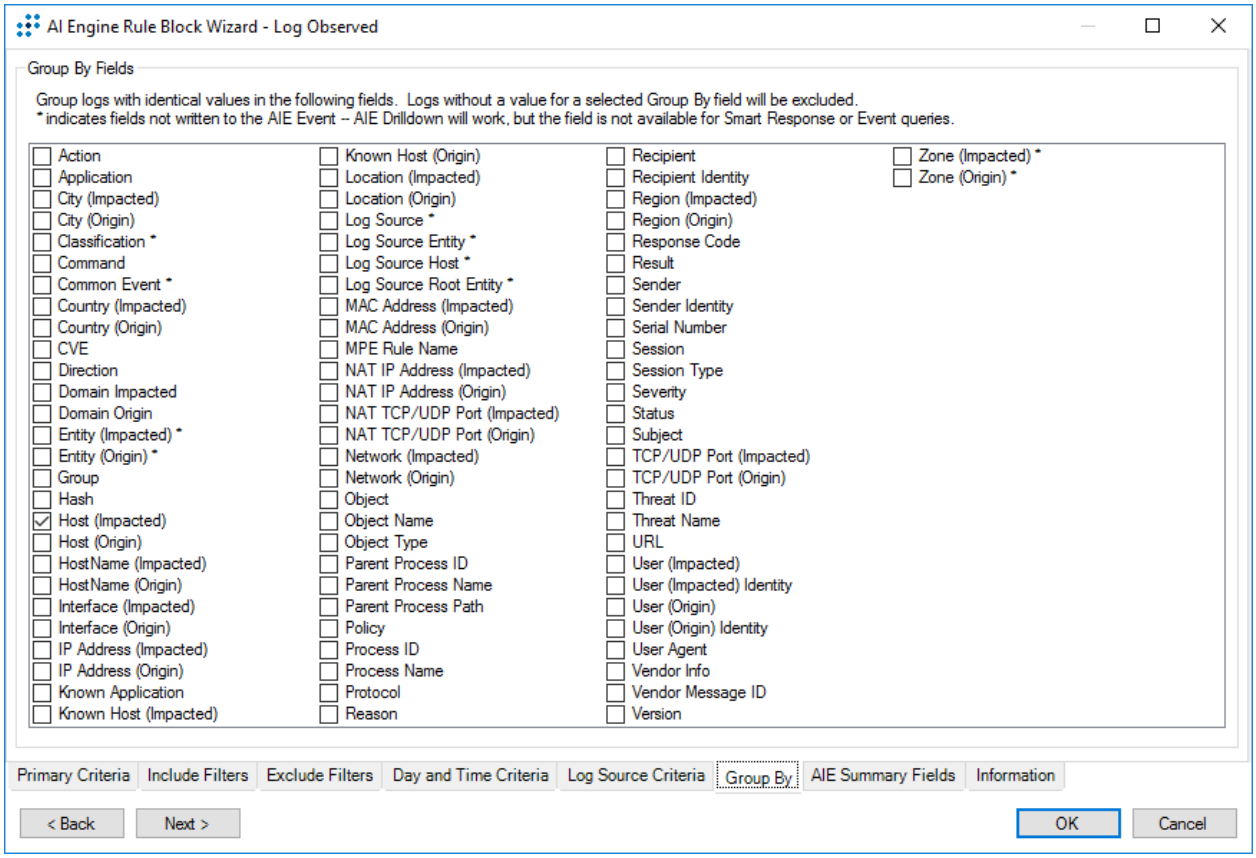
i. RecordedFuture IP : IP : Suspicious : All



d. Click “OK”

7. Next, we do not need to add anything to the “Exclude Filters” and “Day and Time Criteria” tabs
8. In the “Log Source Criteria” tab, please choose the log source(s) that you would like to compare against the Recorded Future IP Threat Intelligence.

9. In the “Group By” and “AIE Summary Fields” tab, check mark the “Host (Impacted)” box

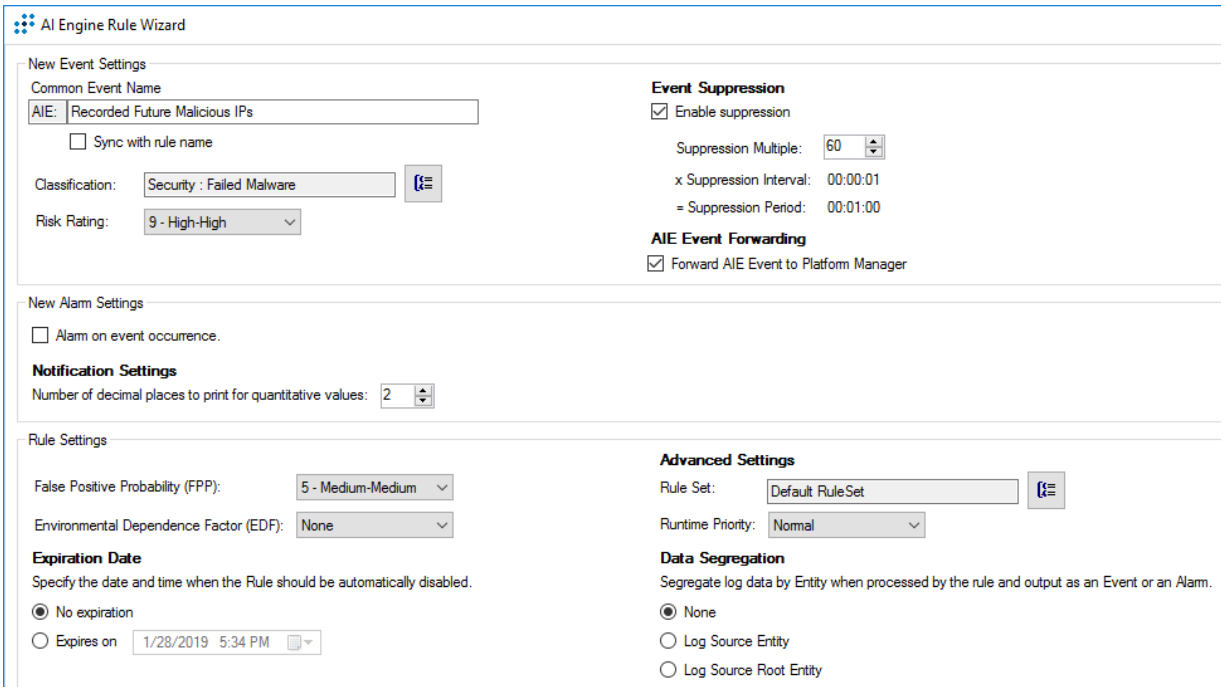


10. In the “Information” tab, please add in any related information for this correlation rule
11. Click “OK”

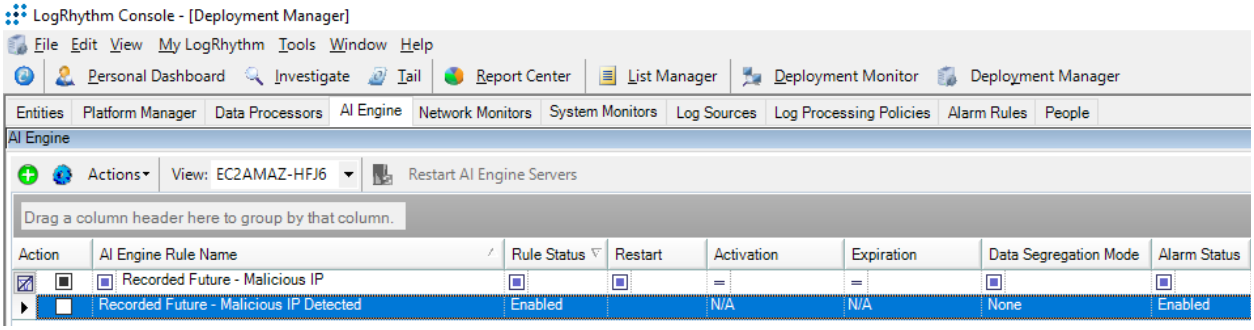
12. Choose the “Settings” tab (Next to the “Rule Block” tab)
    a. Add a “Common Event Name” by unchecking the “Sync with rule name”
        i. The “Common Event Name” = “Recorded Future Malicious IPs”
    b. Classification = “Security : Failed Malware”
    c. Risk Rating = 9 - High-High
13. No changes to the “Notify” and “Actions” tab are necessary

14. In the “Information” tab, please add a “AI Engine Rule Name” and any other relevant information in the “Brief Description” and “Additional Details”
    a. The “AI Engine Rule Name” can be “Recorded Future Malicious IPs”

15. Click “OK”. Congratulations, you have now configured an IP AI Engine rule!
    a. You will begin to see alarms being generated in the LogRhythm WebGUI when a match is found between your log source and the Recorded Future IP Threat Intelligence.

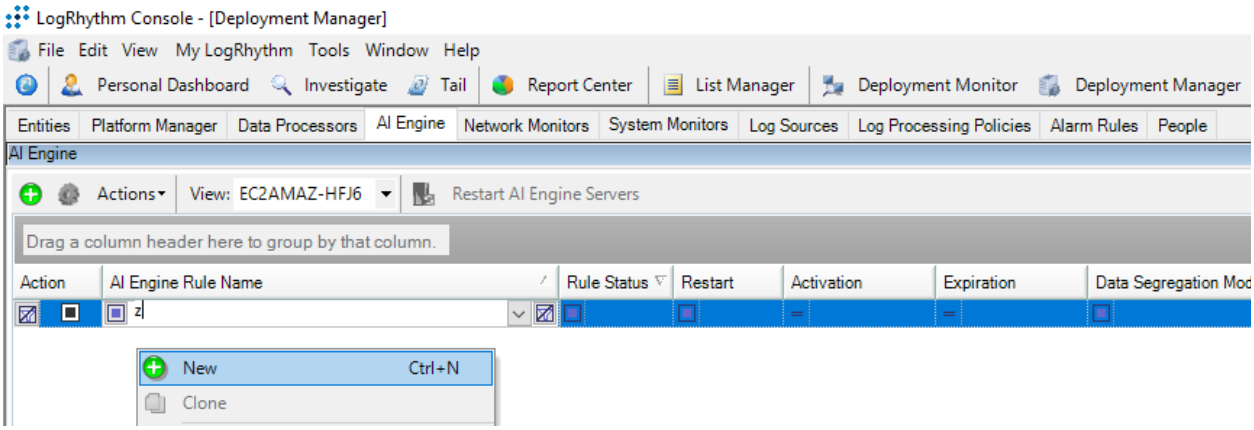


Example AI Engine Rule Setup - Recorded Future Malicious

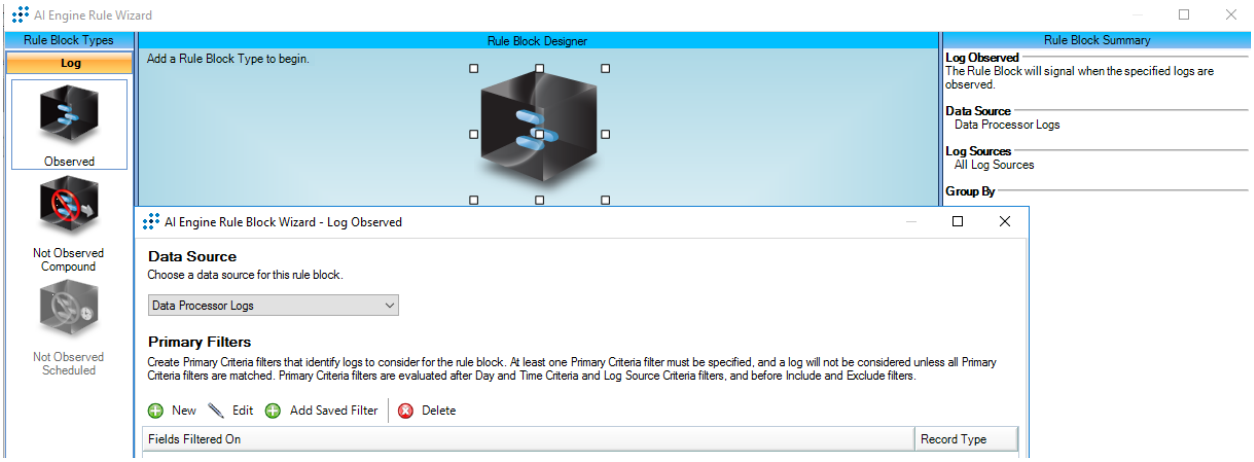


Domains

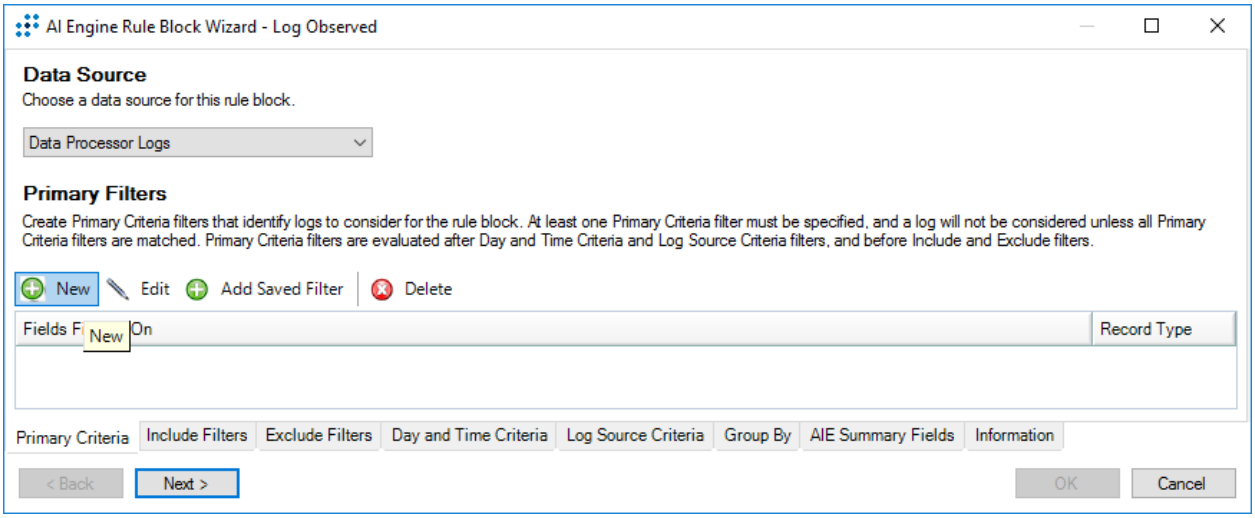
1. We can create AI Engine rules between the Recorded Future data and the data within LogRhythm for Domains.
2. Navigate to the “Deployment Manager” then “AI Engine” Tab.
3. In the white space, right click, “New”.



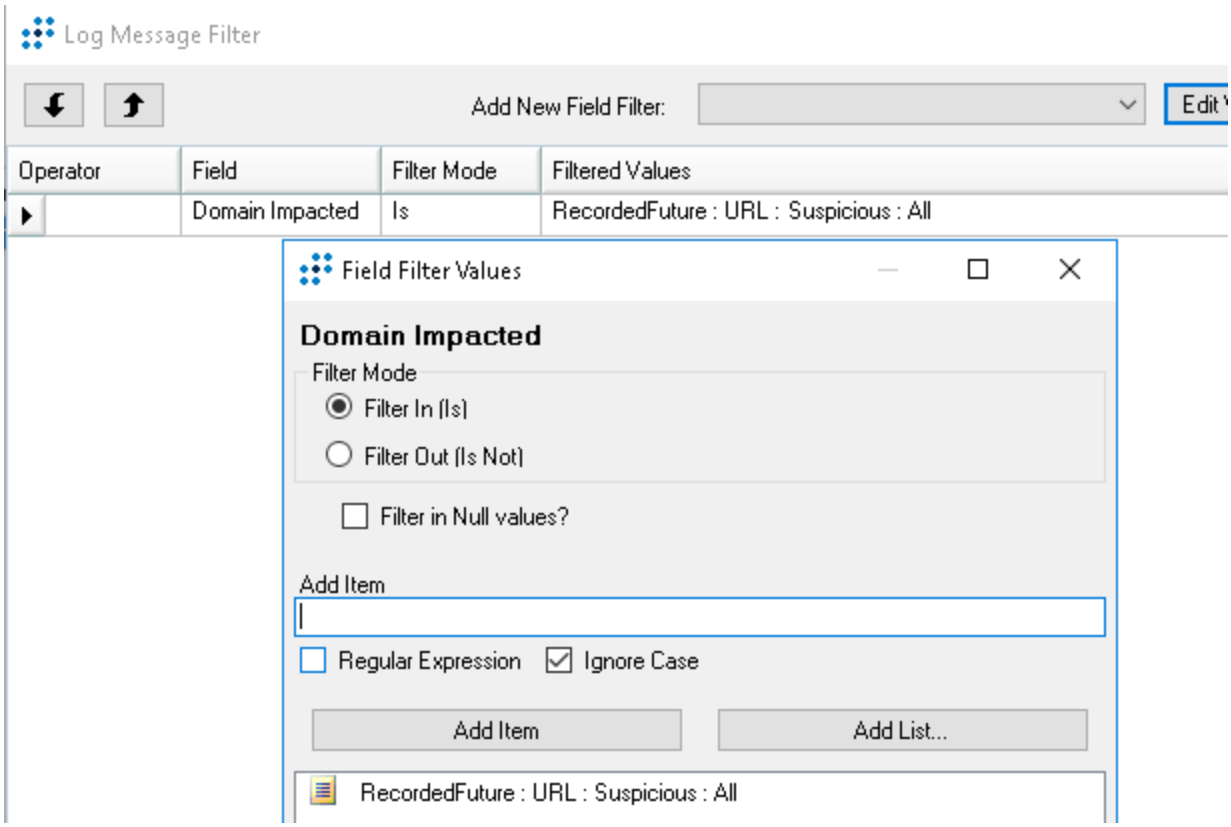
4. Drag the “Observed” cube from the left pane to the blue “Rule Block Designer” and double click the “Block”.



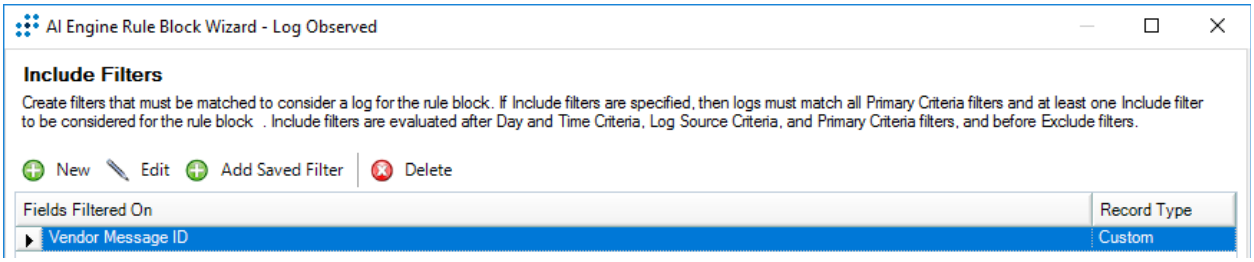
5. In the “Primary Criteria” tab, click “New”.



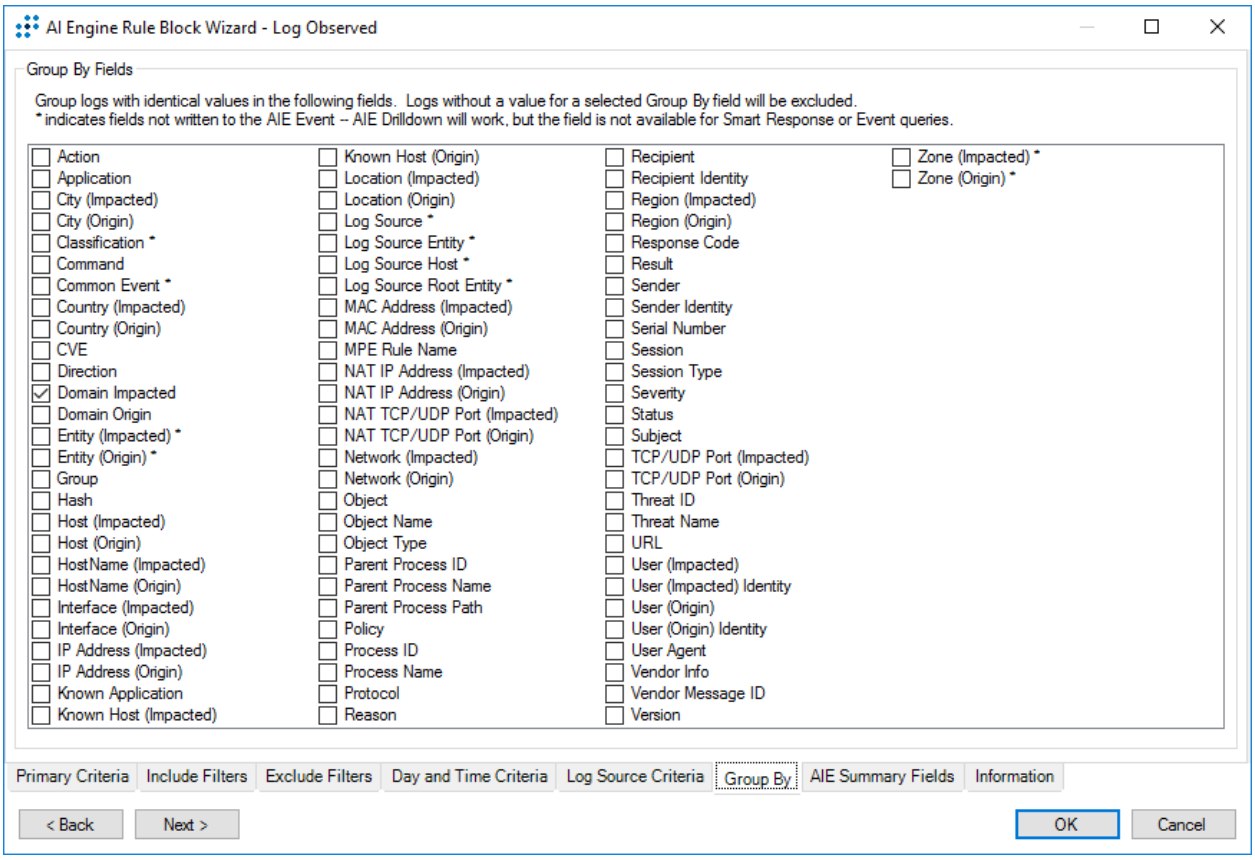
6. Under “Add New Field Filter” choose “Vendor Message ID”.
    a. Filter Mode = Filter In (Is)
    b. Under “Add Item” type “C&C DNS Name”
    c. Click “Add Item”
    d. Click “OK”



7. Next click on the “Include Filters” tab and Click “New”.
    a. Under “Add New Field Filter” choose “Domain Impacted”
    b. Filter Mode = Filter In (Is)
    c. Under “Add List” choose the Recorded Future list name:
        i. RecordedFuture : URL : Suspicious : All
    d. Click “OK”

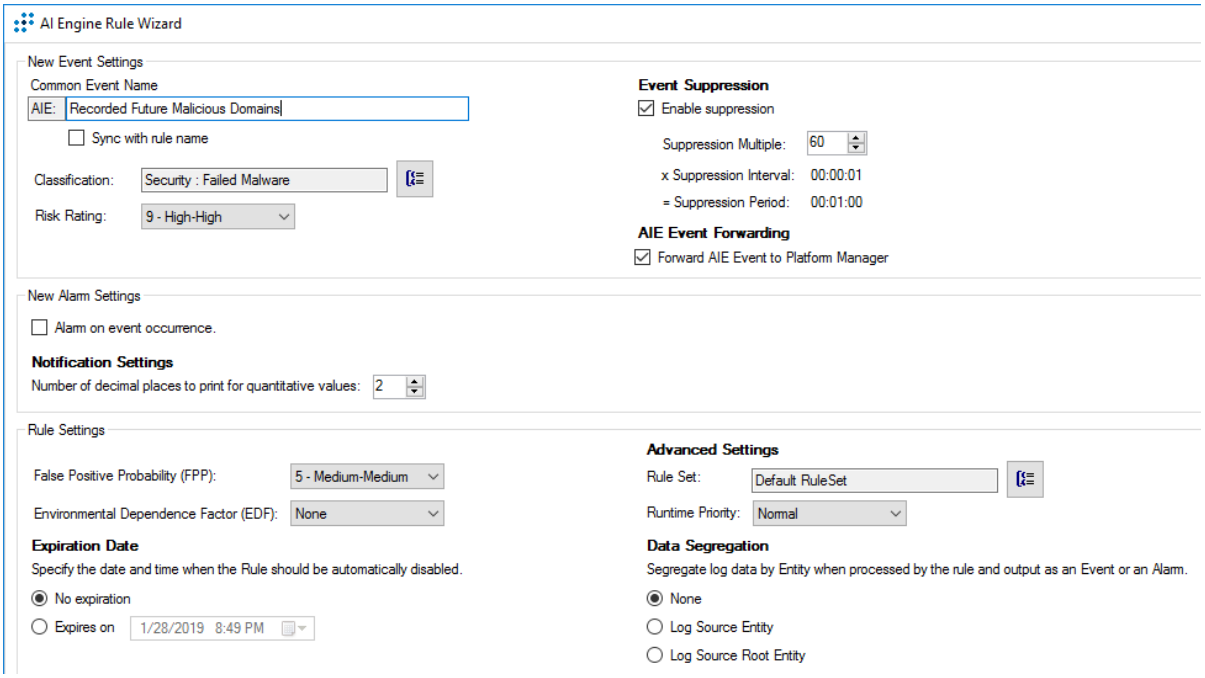


8. Next, we do not need to add anything to the “Exclude Filters” and “Day and Time Criteria” tabs.
9. In the “Log Source Criteria” tab, please choose the log source(s) that you would like to alert on in relation to domains.
10. In the “Group By” and “AIE Summary Fields” tab, check mark the “Domain Impacted” box.

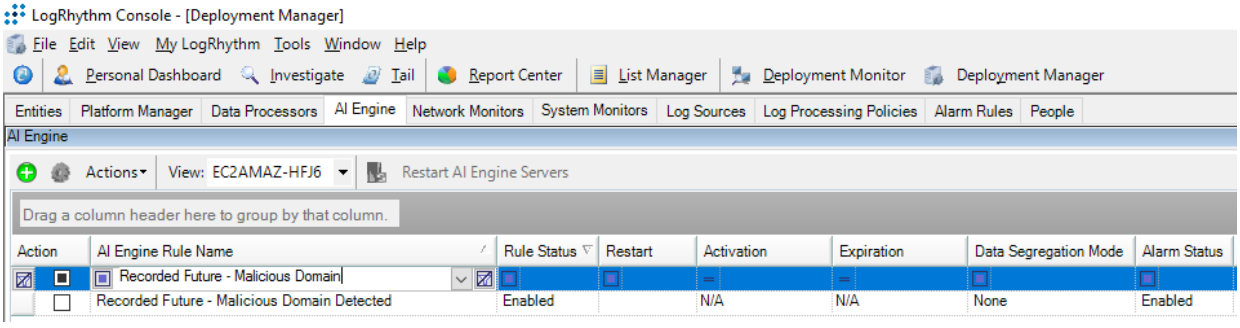


11. In the “Information” tab, please add in any related information for this correlation rule.
12. Click “OK”.
13. Choose the “Settings” tab (Next to the “Rule Block” tab).
    a. Add a “Common Event Name” by unchecking the “Sync with rule name”
        i. The “Common Event Name” = “Recorded Future Malicious Domains”
    b. Classification = “Security : Failed Malware”
    c.

d. Risk Rating = 9 - High-High



14. No changes to the "Notify" and "Actions" tab are necessary.
15. In the "Information" tab, please add "AI Engine Rule Name" and any other relevant information in the "Brief Description" and "Additional Details".
    a. The "AI Engine Rule Name" can be "Recorded Future Malicious Domains"
16. Click "OK" and now the Domain AI Engine rule is configured.
    a. You will begin to see alarms in the LogRhythm WebGUI when match(es) between Recorded Future Threat Intelligence and your related (domain) log sources are found.

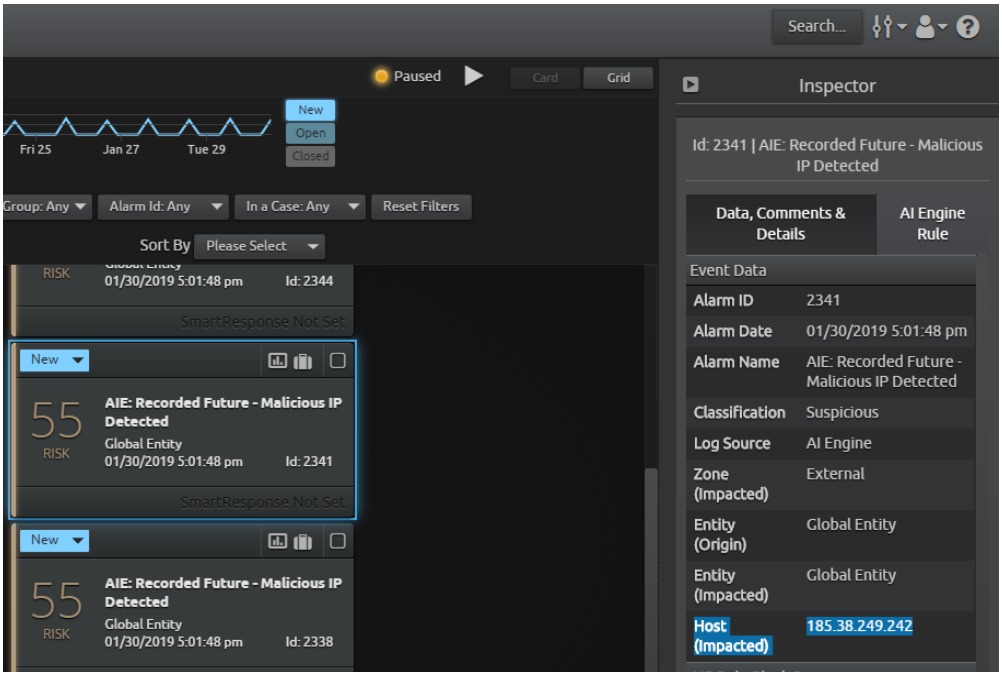


IOC Enrichment

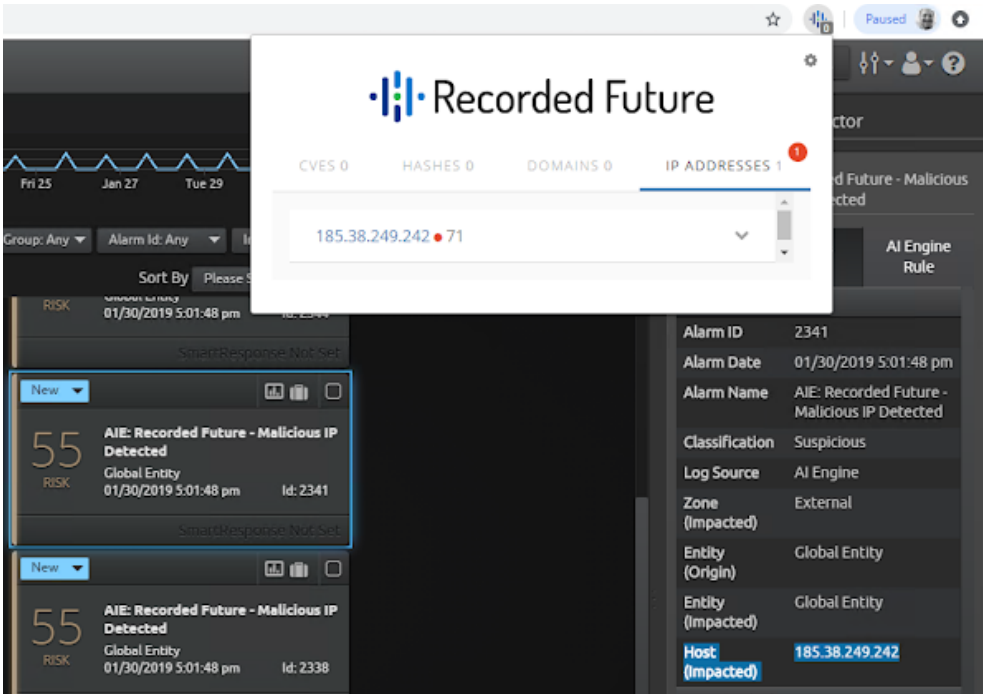
As LogRhythm users investigate alarms and other anomalous network traffic, it can often be very useful to find out what information Recorded Future may have about one or more indicators, be they IP addresses, domains, or hashes. In particular, Recorded Future is collecting information about threats from hundreds of thousands of sources all over the web and analyzing this raw information in real-time to provide actionable insights. SOC analysts can often gain indicator context from Recorded Future to determine whether an alarm warrants further investigation or can simply be filed away as 'low risk'.

The easiest way to get Recorded Future context on indicators associated with a LogRhythm alarm is to simply download and install the Recorded Future Browser Extension (available for Chrome at this link and Mozilla Firefox at this link). More information about the Recorded Future Browser Extension is available on this support section.

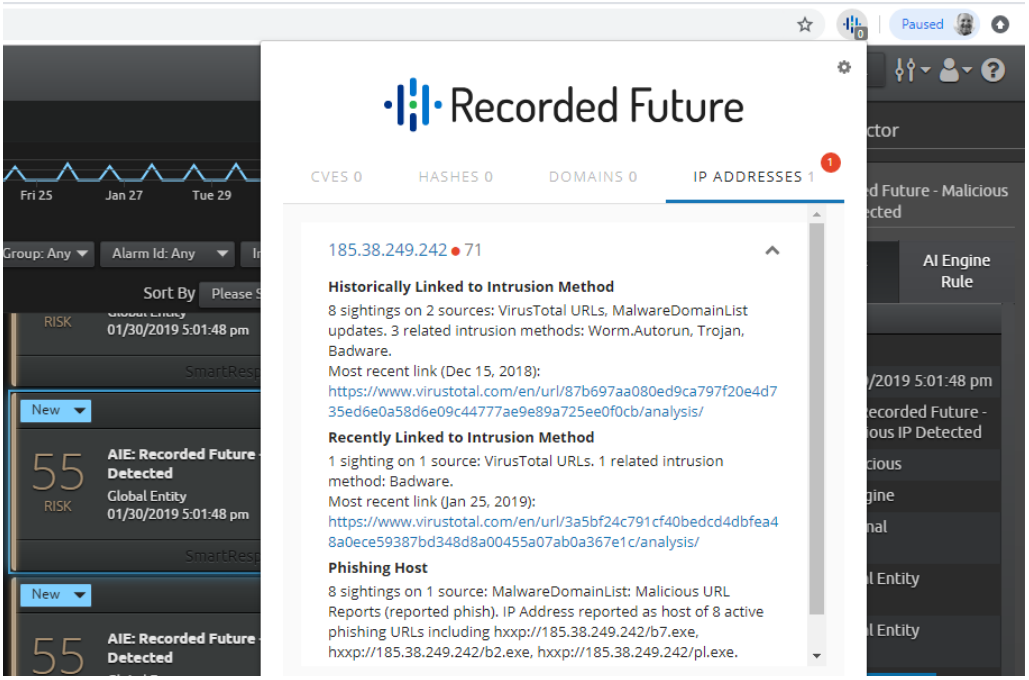
1. By default the Recorded Future Browser Extension will enrich any IoC that it finds on a particular web page; this works seamless on IOCs viewed in the LogRhythm WebGUI.
    a. The most popular use case within LogRhythm is enriching alarm IoCs
        i. For example, when an alarm such as “AIE: Recorded Future - Malicious IP Detected” pops up, we see the created “Event Data”
        ii. We can then see the “Host (Impacted)” IP address



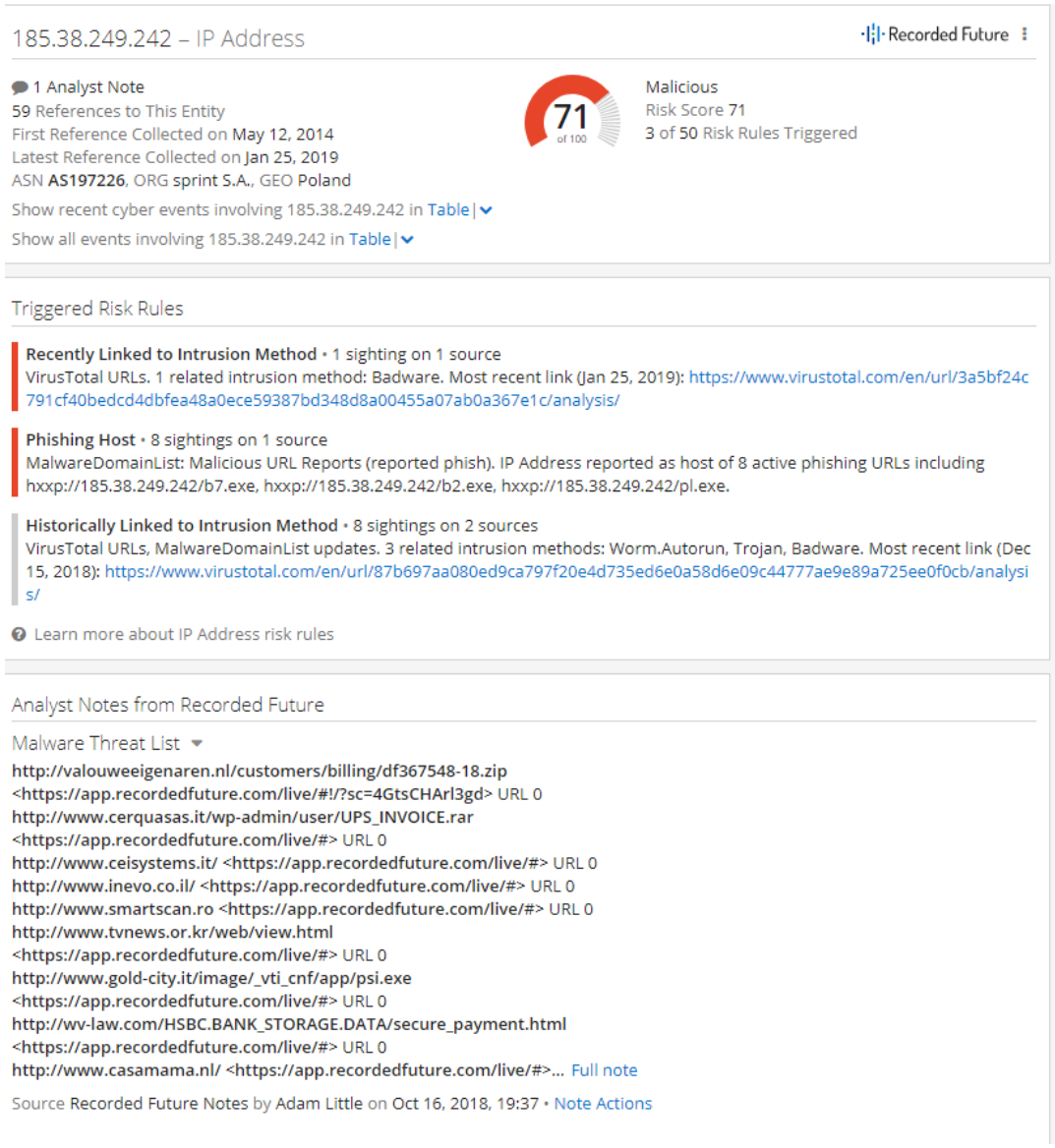
iii. Now we can click the Recorded Future Browser Extension Icon for further context



iv. We can view more enriched information by expanding the section with a click on the upside down carrot symbol on the right



v. To view all of the information Recorded Future has on a particular IoC you can click on the IoC (In this case 185.38.249.242) which will pivot to the Recorded Future Portal



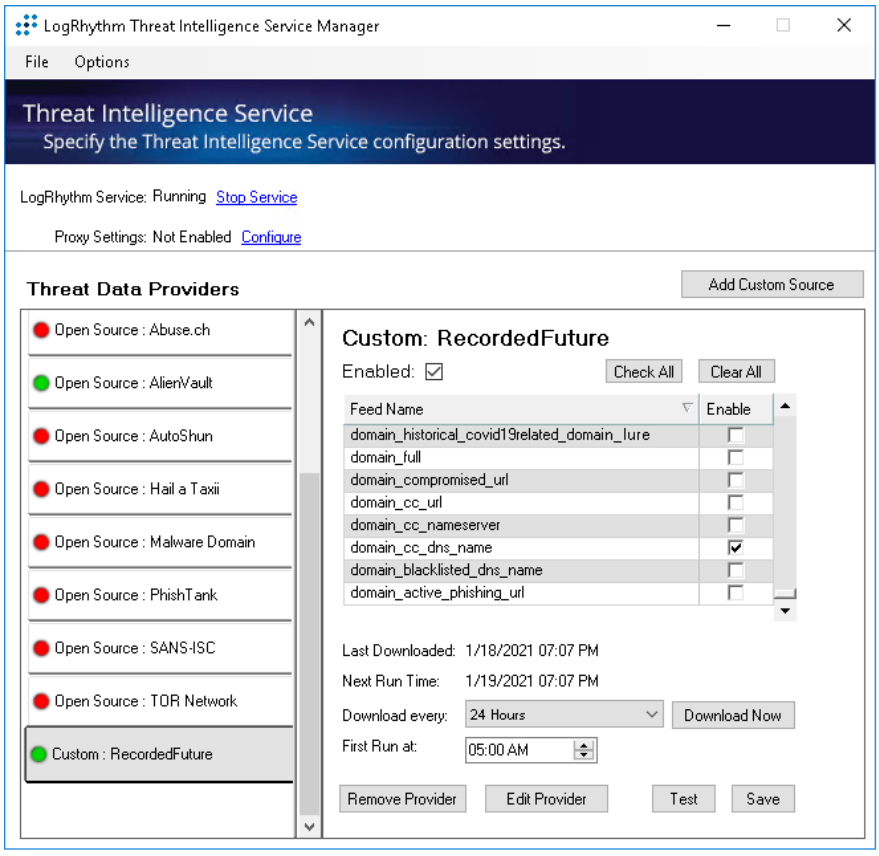
Congratulations! You have completed the Recorded Future integration for LogRhythm. If you have any questions, please reach out to your account team or submit a support request.

Appendix A

What if a collection name changes on the Recorded Future STIX/TAXII server?

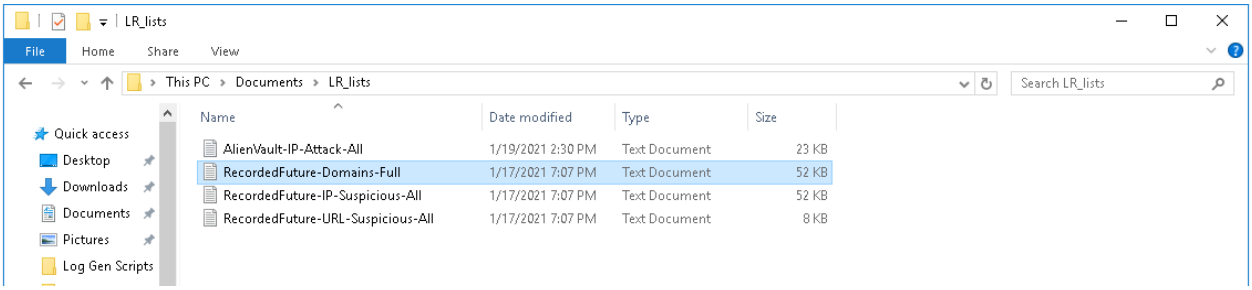
Occasionally, collection names change on the Recorded Future STIX/TAXII server and hence the old collection name will no longer be available for download. To fix that and work with a new collection name, you need to go to the LogRhythm Threat Intelligence Service Manager and perform these next steps. For example, imagine an "old collection" named ***domain_full_large*** was just changed to ***domain_full***.

1. Open the LogRhythm Threat Intelligence Service Manager

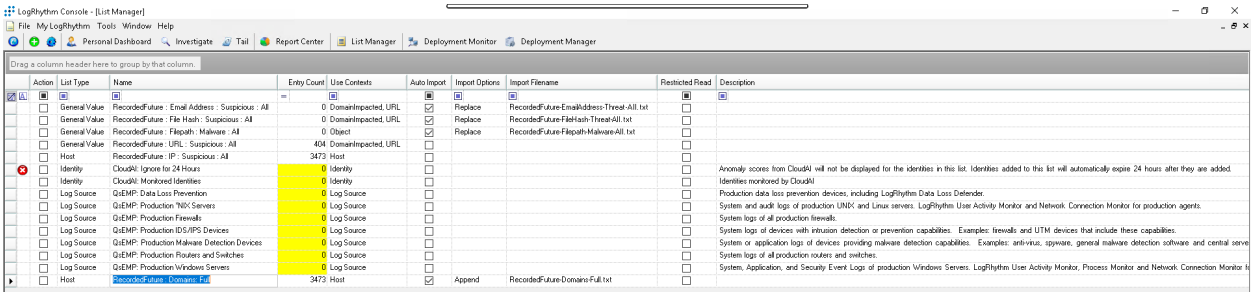


2. Threat Intelligence Service should have an auto refresh collection list, so you should be able to see the new collection name there.
3. Now you need to mark it and download it by pressing *Download Now*.
4. Check the downloaded file, that should be located in the default or custom folder for your Threat Intelligence Service, the file name according to example should be named *RecordedFuture-Domain-Full* and it should contain a list of domains. In this case it is

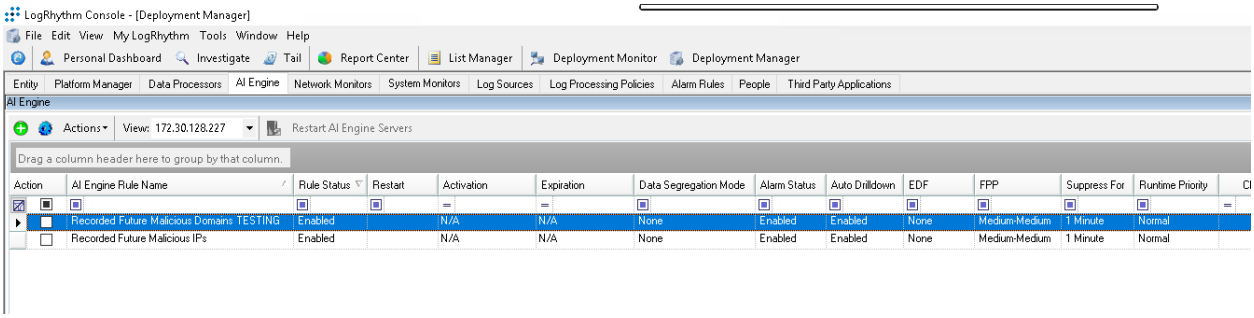
custom folder.



5. Now you should go to the LogRhythm *Console.*
6. Once logged in click the *List Manager* we can see that a new list is being populated. We need it's name for future, in this case it is *Recorded Future Domains Full.*
   Note: There can be no Entry Count, probably because we at the beginning of the setup of LogRhythm Threat Intelligence Service Manager used different folders for threat lists. And now LR can't auto import them. To fix it you need to edit the record, remove the auto import option and choose the file manually .

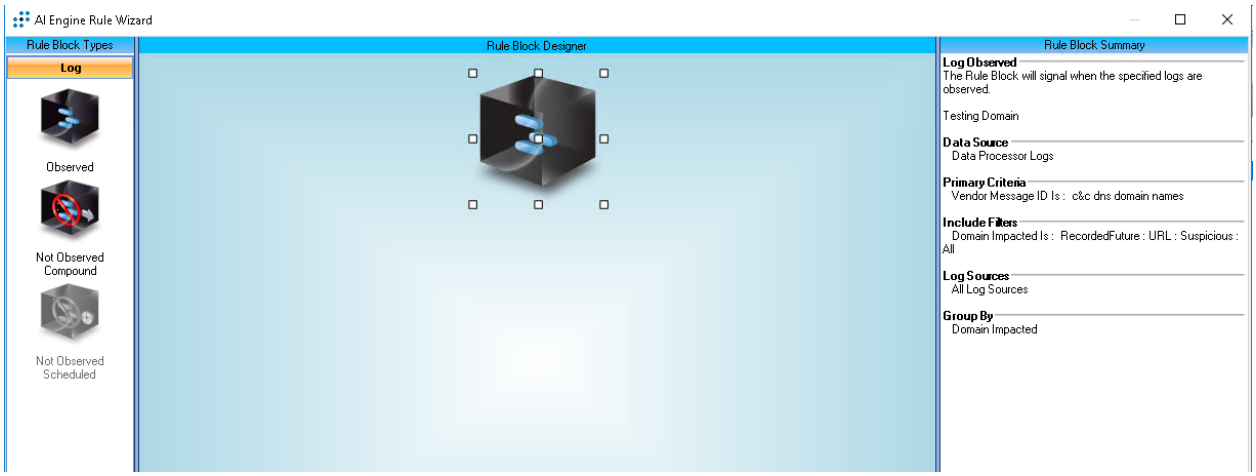


7. Now you need to make changes to the correlation rule that is using ***domain_full_large*** list.
8. Navigate to the *Deployment Manager,* then *AI Engine* tab.

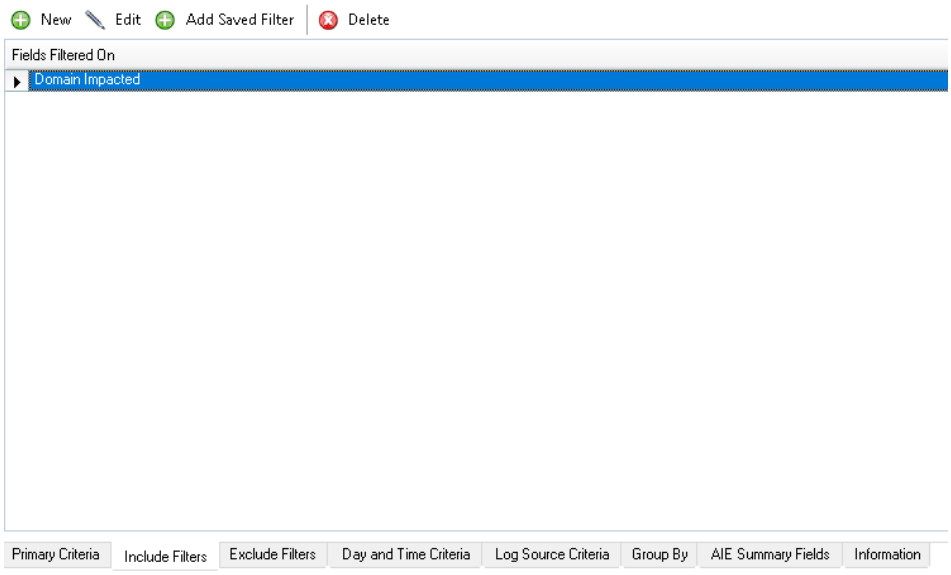


9. Then choose rule that is using old list (***domain_full_large***).

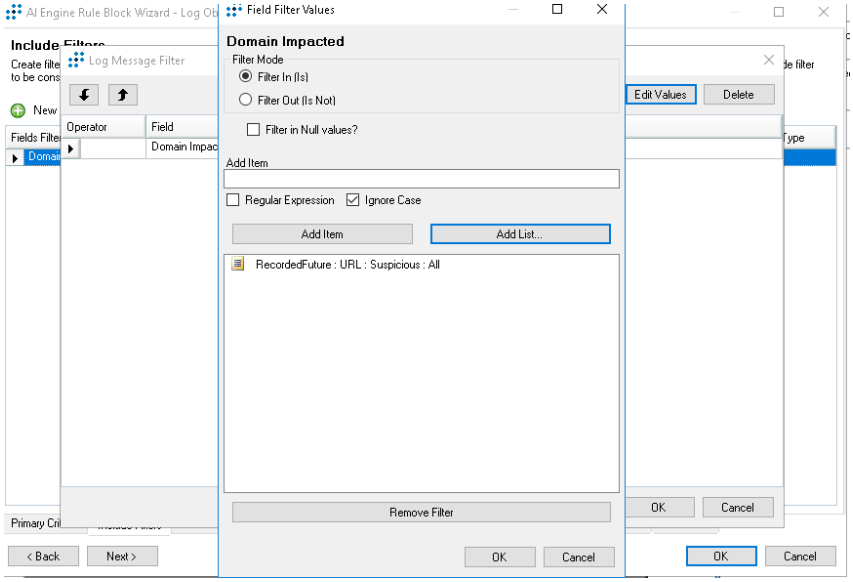
10. In the blue *Rule Block Designer* double click the *Block* for Observed.



11. Next click on the "Include Filters" tab and Click on the filter that is using ***domain_full_large***



12. In the new window Under *Add List* choose the old list and click remove filter. And then press *Add List* and choose the newly added list. And finally press *OK*



13. Now save all the changes you have made.

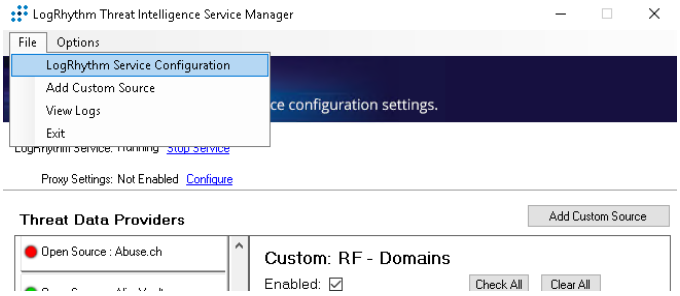
NOTE: This was just an example to illustrate the problem and has rarely happened to date.

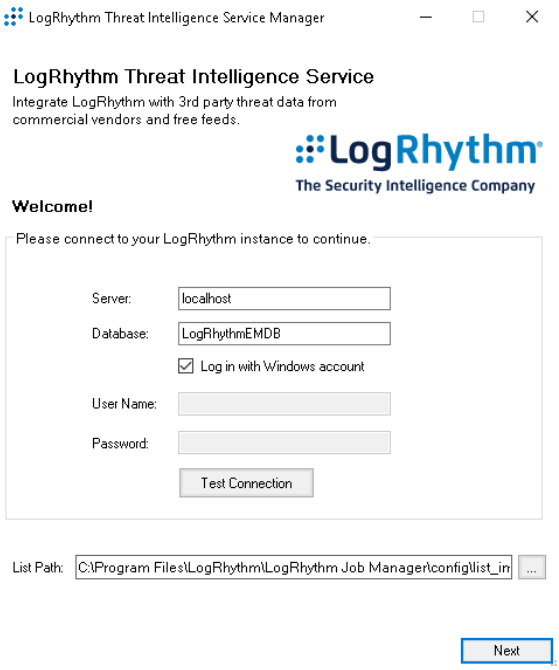
Appendix B

What to do when there are no entities in a collection?

If a collection is showing 0 entry count, it could be the case where the initial installation of LogRhythm Threat Intelligence Server was configured to a different folder for threat intelligence. As a result, LogRhythm isn't able to find and auto import the threat intelligence.

To fix this, clients need to edit the record, remove the auto import option, and choose the file manually. By default this folder is `<C:\Program Files\LogRhythm\LogRhythm Job Manager\config\list_import\>`. If this folder is used, auto import will work. If the user wants to change the folder it can be done under File → LogRhythm Service Configuration.




LogRhythm Threat Intelligence Service Manager
LogRhythm Threat Intelligence Service
Integrate LogRhythm with 3rd party threat data from commercial vendors and free feeds.
LogRhythm
The Security Intelligence Company
Welcome!
Please connect to your LogRhythm instance to continue.
Server:
localhost
Database:
LogRhythmEMDB
Log in with Windows account
User Name:
Password:
Test Connection
List Path:
C:\Program Files\LogRhythm\LogRhythm Job Manager\config\list_in
...
Next

Appendix C

How to set custom download frequencies

To set up custom pull frequencies for the feeds you're downloading into LogRhythm, follow the steps detailed below. We recommend pulling IPs once an hour (60 minute frequency), Domains and URLs once every two hours (120 minute frequency), and Hashes once a day (1440 frequency).

The pull frequencies of feeds in LogRhythm can be customized in the configuration file by going to: *C:\Program Files\LogRhythm\LogRhythm Threat Intelligence Service\config\lrtfsvcconfig.json*. Find the desired data provider (under "ProviderName" field), change the "Frequency" field (in minutes), and save the file.

Appendix D

How to Increase the Entity Download Limit

To increase the entity limit for a Threat Data Provider to greater than 100k, follow the steps detailed below. Note that as you increase the amount of entities brought into LogRhythm, this will also increase the corresponding file size.

The entity limit of feeds in LogRhythm can be customized in the configuration file by going to: *C:\Program Files\LogRhythm\LogRhythm Threat Intelligence Service\config\lrtfsvcconfig.json*. Find the desired data provider (under "ProviderName" field), change the "TopRisksList1Size" field for the appropriate LogRhythm list according to which entities you are pulling in for a specific Threat Data Provider (listed below), and save the file.

1. [Name of Threat Data Provider] : IP : Suspicious : All - This list contains all of the IP entities downloaded from Recorded Future risk lists
2. [Name of Threat Data Provider] : URL : Suspicious : All - This list contains all of the URL and domain entities downloaded from Recorded Future risk lists
3. [Name of Threat Data Provider] : File Hash : Suspicious : All - This list contains all of the hash entities downloaded from Recorded Future risk lists