← 7 LogRhythm[™]

LogRhythm Integration

Installation Instructions

Table of Contents

Introduction	3
System Requirements	3
Setting Up Threat Intelligence from Recorded Future	4
Example collection setup: malicious IPs	4
Example collection setup: malicious domains	9
Best Practices for Setting Up Data Providers	9
Confirm Recorded Future Threat Intelligence is loading correctly	10
Entity List Mapping	10
Retire Unused Lists	11
Set up Time to Live (TTL)	11
Using Threat Intelligence from Recorded Future	12
Example AI Engine Rule Setup - Recorded Future Malicious IPs	12
Example AI Engine Rule Setup - Recorded Future Malicious Domains	18
IOC Enrichment	23
Appendix A	26
What if a collection name changes on the Recorded Future STIX/TAXII server?	26
Appendix B	30
What to do when there are no entities in a collection?	30
Appendix C	32
How to set custom download frequencies	32
Appendix D	33
How to Increase the Entity Download Limit	33

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 "<u>IOC Enrichment</u>" 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".

File Options Intreat Intelligence Service configuration settings. LogRhythm Service: Running Stop Service Proxy Settings: Not Enabled Configure Threat Data Providers Add Custom Source Bright/Cloud Cisco AMP Threat Grid Custom: RecordedFuture Cisco AMP Threat Grid Custom: RecordedFuture Cisco AMP Threat Grid Custom: RecordedFuture Cisco AMP Threat Grid Custom: Recorded future Open Source : Abuse.ch domain_tistical_convid Stelated_domain_lure Open Source : AlueShun Last Downloaded: 1/18/2021 07:07 PM Open Source : Hail a Taxii Open Source : Hail a Taxii Open Source : PhishTank W	📫 LogRhythm Threat Intelligence Service Manager	_		Х
Chreat Intelligence Service Specify the Threat Intelligence Service configuration settings. LogRhythm Service: Running Stop Service Proxy Settings: Not Enabled Configure Threat Data Providers Add Custom Source BrightCloud Cisco AMP Threat Grid Cisco AMP Threat Grid Symantec Open Source : Abuse.ch Open Source : AlienYoult Open Source : AutoShun Open Source : Hail a Taxii Open Source : Hail a Taxii Open Source : Malware Domain Open Source : PhishTank.	File Options			
LogRhythm Service: Running Stop Service Proxy Settings: Not Enabled Configure Threat Data Providers BightCloud BightCloud Cisco AMP Threat Grid CrowdStrike Open Source : Abuse.ch Open Source : AlienVault Open Source : AlienVault Open Source : Hail a Taxii Open Source : Malware Domain Open Source : PhishTank	Threat Intelligence Service Specify the Threat Intelligence Service configuration settings.			
Proxy Settings: Not Enabled Configure Add Custom Source BrightCloud Custom: RecordedFuture Enabled: Check All Clear All Cisco AMP Threat Grid Feed Name Enabled: CrowdStrike Condician Covid19related_domain_lure Covid19related_domain_lure Open Source : Abuse.ch Open Source : Abuse.ch Comain_co_nameserver Codician Open Source : AtienVault Last Downloaded: 1/18/2021 07:07 PM Next Run Time: 1/19/2021 07:07 PM Open Source : Hail a Taxii Open Source : Malware Domain Remove Provide Edit Provider Test Save	LogRhythm Service: Running Stop Service			
Threat Data Providers Add Custom Source BrightCloud Cisco AMP Threat Grid Cisco AMP Threat Grid CrowdStrike CrowdStrike Symantec Open Source : Abuse.ch Open Source : AlienVault Open Source : AutoShun Open Source : Hail a Taxii Open Source : Malware Domain Open Source : PhishTank. Add Custom Source Enabled: Cisco AMP Threat Grid Cisco AMP Threat Grid Cisco AMP Threat Grid Cisco AMP Threat Grid Symantec Open Source : Abuse.ch Open Source : AlienVault Open Source : Hail a Taxii Open Source : Hail a Taxii Open Source : Malware Domain Remove Provider Edit Provider Test Save 	Proxy Settings: Not Enabled Configure			
 BrightCloud Cisco AMP Threat Grid Cisco AMP Threat Grid CrowdStrike CrowdStrike Symantec Open Source : Abuse.ch Open Source : AlienVault Open Source : AutoShun Open Source : Hail a Taxii Open Source : Malware Domain Open Source : PhishTank. 	Threat Data Providers	Add Cu	stom Souri	ce
Cisco AMP Threat Grid Enabled: C Check All Clear All CrowdStrike domain_historical_covid19related_domain_lure domain_clar Symantec domain_compromised_url domain_compromised_url Open Source : Abuse.ch domain_cc_nameserver domain_clar Open Source : AlienVault Open Source : AutoShun Last Downloaded: 1/18/2021 07:07 PM Next Run Time: 1/19/2021 07:07 PM Download every: 24 Hours Download Now Open Source : Malware Domain First Run at: 05:00 AM Open Source : PhishTank V Edit Provider Test Save	BrightCloud Custom: RecordedFuture			
CrowdStrike Image: Construct of the second seco	Cisco AMP Threat Grid Enabled: Check All	Clear A		
Symantec Image: Compromised_url Open Source : Abuse.ch Image: Compromised_url Open Source : Abuse.ch Image: Compromised_url Open Source : AlienVault Image: Compromised_url Open Source : AlienVault Image: Compromised_url Open Source : AlienVault Image: Compromised_url Open Source : AutoShun Image: Compromised_url Open Source : Hail a Taxii Image: Compromised_url Open Source : Malware Domain Image: Compromised_url Open Source : PhishTank Image: Compromised_url	CrowdStrike domain_historical_covid19related_domain_lure domain_full			
Open Source : Abuse.ch Open Source : AlienVault Open Source : AlienVault Open Source : AutoShun Open Source : AutoShun Open Source : Hail a Taxii Open Source : Hail a Taxii Open Source : Malware Domain Open Source : PhishTank	Symantec Symantec			
Open Source : AlienVault Open Source : AutoShun Open Source : AutoShun Open Source : Hail a Taxii Open Source : Hail a Taxii Open Source : Malware Domain Open Source : PhishTank	Open Source : Abuse.ch domain_cc_nameserver domain_cc_dns_name			
Open Source : AutoShun Open Source : Hail a Taxii Open Source : Malware Domain Open Source : PhishTank V	Open Source : AlienVault domain_blacklisted_dns_name domain_active_phishing_url			
Open Source : Hail a Taxii Open Source : Malware Domain Open Source : PhishTank	Open Source : AutoShun Last Downloaded: 1/18/2021 07:07 PM			
Open Source : Malware Domain Open Source : PhishTank First Run at: 05:00 AM Remove Provider Edit Provider Test Save	Open Source : Hail a Taxii Open Source : Hail a Taxii	Download I	٩ow	
Open Source : PhishTank Remove Provider Edit Provider Test Save	Open Source : Malware Domain First Run at: 05:00 AM			
	Open Source : PhishTank Remove Provider Edit Provider Te	est S	ave	

5. Click on the "Add STIX/TAXII Provider" button¹.



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

LogRhythm Custom Provider	_	×
Threat Provider Name:		
Recorded Future IPs]	
TAXII Collection Endpoint:		
https://api.recordedfuture.com/taxii		
Username:		
rf		
Password:		
•••••		
Certificate Authentication		
Certificate Password:		
Certificate Path:	1	
Save Test		

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

LogRhythm Threat Intelligence Service Manager	-	\times
File Options		
Threat Intelligence Service Specify the Threat Intelligence Service configuration settings.		

LogRhythm Service: Running Stop Service

Proxy Settings: Not Enabled Configure

Threat Data Providers

Add STIX/TAXII Provider

Open Source : Malware Domain	`
Open Source : PhishTank	
Open Source : SANS-ISC	
Open Source : TOR Network	
Custom : Recorded Future HASH	
Custom : Recorded Future IP Cur	
Custom : Recorded Future Domai	
Custom : Recorded Future Activel	
	Y

Custom: Recorded Futu	Ire IP Curr	ent CC	
Enabled: 🗹	Remove Provide	er Edit	Provider
Feed Name	∇	Enable	•
ip_recently_defaced_site			1
ip_recently_active_cc_server			
ip_recent_unusual_ip		\checkmark	
ip_recent_tor_node			
ip_recent_threat_researcher		\checkmark	
ip_recent_sshdictionary_attacker			
ip_recent_spam_source			
ip_recent_positive_malware_verdict			
ip recent phishing host		V	•
Last Downloaded: Error			
Next Run Time: 2/24/2022 01:45 PI	И		
Download every: 12 Hours	✓ Do	wnload No	w
First Run at: 01:45 PM 🚖	1	Test	Save

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

Enabled: 🗹	Remove Provide	r Edit	Provider
Feed Name	∇	Enable	
ip_recently_linked_to_apt		Г	
ip_recently_defaced_site		Γ	·
ip_recently_active_cc_server		V	_
ip_recent_unusual_ip			
ip_recent_tor_node			
ip_recent_threat_researcher			
ip_recent_sshdictionary_attacker			
ip_recent_spam_source			
ip recent positive malware verdict			•

Custom: Recorded Future IP Current CC

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

Enabled: 🗹	Remove Provide	r Edit Provider
Feed Name	∇	Enable 🔺
ip_recently_linked_to_apt		
ip_recently_defaced_site		
ip_recently_active_cc_server		V
ip_recent_unusual_ip		
ip_recent_tor_node		
ip_recent_threat_researcher		
ip_recent_sshdictionary_attacker		
ip_recent_spam_source		
ip recent positive malware verdict		
Last Downloaded: Error		
Next Run Time: 2/24/2022 01:45 P	м	
Download every: 12 Hours	 ✓ Do 	wnload Now
First Run at: 01:45 PM 📑		Test Save

Custom: Recorded Future IP Current CC

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 page³; 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

Enabled: 🗹	Remove Provide	er Edit	t Provider
Feed Name	∇	Enable	^
domain_recent_malware_analysis_c	Ins_name		
domain_recent_fast_flux_dns_name			
domain_recent_covid19related_dom	nain_lure_susp		
domain_recent_covid19related_dom	nain_lure_mali		
domain_recent_cc_dns_name		V	
domain_no_risk_observed			
domain_newly_registered_certificat	e_with_potenti		_
domain_newly_registered_certificat	e_with_potenti		
domain large		٣	-

Custom: Recorded Future Domain CC

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.

E Log	Rhythm My Lo	n Console - [Lisi ogRhythm Tou & Person:	t Manager) ols Window Help al Dashboard 🔍 Investigate 🥥 Tail 🏽 💩 Re	port Center	🔳 List Manager 🛛 🏓	neployme	ent Monitor 🧃	j Deployment Manager		
Diag	Action	List Tupo		Entry Count	Lies Contaute	Auto Import	Import Options	Import Filonamo	Postricted Road	Description
	Action	сізстуре	Name	Endy Count	USE CORREXIS	Automport	Import options	Import riename	Hestildted Head	Description
🛛 🗛				=						
		General Value	RecordedFuture IP : Email Address : Suspicious : All	0	DomainImpacted, URL		Replace	RecordedFuture-IP-EmailAddress-Threat-All.txt		
		General Value	RecordedFuture IP : File Hash : Suspicious : All	36	DomainImpacted, URL		Replace	RecordedFuture-IP-FileHash-Threat-AII.txt		
۱.		General Value	RecordedFuture IP : Filepath : Malware : All	4	Object		Replace	RecordedFuture-IP-Filepath-Malware-AII.txt		
		General Value	RecordedFuture IP : URL : Suspicious : All	5089	DomainImpacted, URL		Replace	RecordedFuture-IP-URL-Suspicious-All.txt		
		Host	RecordedFuture : Domains: Full	3473	Host		Append	RecordedFuture-Domains-Full.txt		
		Host	RecordedFuture IP : IP : Suspicious : All	8662	Host		Replace	RecordedFuture-IP-IP-Suspicious-All.txt		

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

List Properties					×
asic Configuration	List Items	Additional S	ettings		
List Type					
Host					
List Name					
RF IP C2:IP:	Suspicious :	All			
Brief Description					
1					
Permissions			0		
Permissions Read Access			Owner	 _	
Permissions Read Access Public All Users		~	Owner LogRhythmAdmin		
Permissions Read Access Public All Users Write Access		~	Owner LogRhythmAdmin Default Entity		
Permissions Read Access Public All Users Write Access Public Global Ac	ministrator	~	Owner LogRhythmAdmin Default Entity Global Entity		
Permissions Read Access Public All Users Write Access Public Global Ac	Iministrator	~	Owner LogRhythmAdmin Default Entity Global Entity	1.2°	
Permissions Read Access Public All Users Write Access Public Global Ad	Iministrator	~	Owner LogRhythmAdmin Default Entity Global Entity	1.12	
Permissions Read Access Public All Users Write Access Public Global Ac	Iministrator	~	Owner LogRhythmAdmin Default Entity Global Entity	1.2	
Permissions Read Access Public All Users Write Access Public Global Ac Bestricted R Auto Import	Iministrator	~	Owner LogRhythmAdmin Default Entity Global Entity		

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".

ager
ager
- 3.5
+
on Mod
tic

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"

	- 🗆	×
Data Source		
Choose a data source for this rule block.		
Data Processor Logs 🗸		
Primary Filters		
Create Primary Criteria filters that identify logs to consider for the rule block. At least one Primary Criteria filter must be specified, and a log will not be considered Criteria filters are matched. Primary Criteria filters are evaluated after Day and Time Criteria and Log Source Criteria filters, and before Include and Exclude filters	unless all Prir 8.	nary
🕒 New 🔪 Edit 🚯 Add Saved Filter 🔕 Delete	-	
New Edit P Add Saved Filter On Delete	Record Typ	pe
New Edit Image: Add Saved Filter Image: Delete Fields Finew On	Record Typ	pe
New Edit Add Saved Filter Delete Fields Filters On Primary Criteria Include Filters Exclude Filters Day and Time Criteria Log Source Criteria Group By AlE Summary Fields Information	Record Typ	pe

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

😲 Log Me	ssage Filter							
t t		Add N	ew Field Filter:		\sim	Edit Values	Dele	ete
Operator	Field	Filter Mode	Filtered Values					
						OK	Cano	cel

Next to "Add New Field Filter" choose "Vendor Message $\ensuremath{\mathsf{ID}}\xspace$. 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"

t t		Add N	New Field Filter: V Edit Values Delete
Operator	Field	Filter Mode	Filtered Values
•	Vendor Messag	ls	permitted outbound traffic
	::· Field Filter	Values	– 🗆 X
	Vendor Me Filter Mode Filter In () Filter Out Filter in	Is) (Is Not) Null values?	
	Add Item		
	Regular Exp	oression 🔽 Ig	Ignore Case
		Add Item	Add List
	permitted	outbound traffic	fic

Click OK again to get to this screen again

Al Engine Rule Block Wizard - Log Observed			×								
Data Source Choose a data source for this rule block.											
Data Processor Logs 🗸											
Primary Filters Create Primary Criteria filters that identify logs to consider for the rule block. At least one Primary Criteria filter must be specified, and a log will not be considered unless all Primary Criteria filters are matched. Primary Criteria filters are evaluated after Day and Time Criteria and Log Source Criteria filters, and before Include and Exclude filters.											
🚱 New 🔪 Edit 🚱 Add Saved Filter 🛛 🔕 Delete											
Fields Filtered On	Recor	d Type									
▶ Vendor Message ID	Custor	n									
Primary Criteria Include Filters Exclude Filters Day and Time Criteria Log Source Criteria Group By AIE Summary Fields Information											
< Back Next > OK		Cance	el								

- 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

👪 Al Engine Rule Block Wizard - Log	Ob Field Filter Values	— 🗆	×	— 🗆 🗙			
Al Engine Rule Block Wizard - Log Observed							×
Include Filters							
Create filters that must be matched to consider a log for to be considered for the rule block . Include filters are	the rule block. If Include filters are spe evaluated after Day and Time Criteria,	ecified, then logs must r Log Source Criteria, an	natch all I d Primary	Primary Criteria filters and at le Criteria filters, and before Ex	east one lr clude filter	nclude filte s.	er
😯 New 🔪 Edit 🚯 Add Saved Filter 🚺	Delete						
Fields Filtered On					Rec	ord Type	
Vendor Message ID					Cus	tom	
Primary Crit	Remove Filt	er		OK Cancel			
- may cit							
< Back Next >		OK Cance		OK Cancel]		

- 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

Al Engine Rule Block Wizard	l - Log Observed		— [o x
Group By Fields				
Group logs with identical values	in the following fields. Logs without a value t	for a selected Group By field will be excluded		
* indicates fields not written to th	e AIE Event AIE Drilldown will work, but th	e field is not available for Smart Response or Event queries.		
	Leastian (Impacted)	Recipient Zone (Impacted) Zone (Opicie) *		
	Location (Impacted)			
	Log Source Entity *			
Common Event *	Log Source Boot Entity *			
Country (Impacted)	MAC Address (Impacted)	Sender Identity		
Country (Origin)	MAC Address (Origin)	Serial Number		
I CVE	MPE Rule Name	Session		
Direction	NAT IP Address (Impacted)	Session Type		
Domain Impacted	NAT IP Address (Origin)	Severity		
Domain Origin	NAT TCP/UDP Port (Impacted) Status		
Entity (Impacted) *	NAT TCP/UDP Port (Origin)	Subject		
Entity (Origin) *	Network (Impacted)	TCP/UDP Port (Impacted)		
Group	Network (Origin)	TCP/UDP Port (Origin)		
Hash	Object	Threat ID		
Host (Impacted)	Object Name	Threat Name		
Host (Origin)	Object Type			
HostName (Impacted)	Parent Process ID	User (Impacted)		
HostName (Origin)	Parent Process Name	User (Impacted) Identity		
Interface (Impacted)	Parent Process Path	User (Origin)		
Interface (Origin)	Policy	User (Origin) Identity		
IP Address (Impacted)	Process ID	User Agent		
IP Address (Origin)	Process Name	Vendor Info		
Known Application		Vendor Message ID		
Known Host (Impacted)	Reason	Version		
Primary Criteria Include Filters	Exclude Filters Day and Time Criteria	Log Source Criteria Group By AlE Summary Fields Information	1	
< Back Next >			OK	Cancel
			UK	Cancer

- 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.

👬 Al Engine Rule Wizard	
New Event Settings	
Common Event Name	Event Suppression
AIE: Recorded Future Malicious IPs	Enable suppression
Sync with rule name	Suppression Multiple: 60 🖨
Classification: Security : Failed Malware	x Suppression Interval: 00:00:01
	= Suppression Period: 00:01:00
Risk Rating: 9 - High-High 🗸	
	Forward AIE Event to Flatform Manager
New Alarm Settings	
Alam on event occurrence	
Notification Settings	
Number of decimal places to print for quantitative values: 2	
Pula Sattinga	
ndie Seuligs	Advanced Settings
False Positive Probability (FPP): 5 - Medium-Medium	Rule Set: Default Bulo Set
Environmental Dependence Factor (EDF): None ~	Runtime Priority: Normal V
Expiration Date	Data Segregation
Specify the date and time when the Rule should be automatically disabled.	Segregate log data by Entity when processed by the rule and output as an Event or an Alarm.
No expiration	None
O Expires on 1/28/2019 5:34 PM	O Log Source Entity
	C Las Sauras Bast Fathu

Example AI Engine Rule Setup - Recorded Future Malicious

LogRhythm Console - [Deployment Manager]									
🕼 Eile Edit View My LogRhythm Tools Window Help									
🙆 🤱 Personal Dashboard 🔍 Investigate 🔊 Iail 👋 Report Center 📃 List Manager 🏂 Deployment Monitor 🗊 Deployment Manager									
Entities Platform Manager Data Processors Al Engine Network Mon	itors System M	Ionitors Log S	Sources Log Proces	sing Policies Alarn	n Rules People				
Al Engine									
🛟 🚯 Actions - View: EC2AMAZ-HFJ6 - 🍢 Restart AI Eng	ine Servers								
Drag a column header here to group by that column.									
Action Al Engine Rule Name	Rule Status ∇	Restart	Activation	Expiration	Data Segregation Mode	Alarm Status			
I I Recorded Future - Malicious IP II									
Recorded Future - Malicious IP Detected	Enabled		N/A	N/A	None	Enabled			

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 "Al Engine" Tab.
- 3. In the white space, right click, "New".

LogRhythm Console - [Deployment Manager]

			-						
🚮 File E	Edit View MyLo	gRhythm Tools	Window H	elp					
0	Personal Dashbo	ard 🔍 Investig	ate ৶ Ta	il 🔹 Report C	enter 📃 List N	lanager 🛛 🏂	Deployment Monitor	访 Deployme	ent Manager
Entities	Platform Manager	Data Processors	Al Engine	Network Monitors	System Monitors	Log Sources	Log Processing Policies	Alarm Rules	People
Al Engine									
•	Actions• View	EC2AMAZ-HFJ6	▼ № F	Restart Al Engine S	ervers				
Drag a	column header he	ere to group by tha	t column.						
Action	Al Engine Rule I	Name		A Rule	e Status ⊽ Restart	Activati	on Expiration	Data Se	gregation Mod
	🔳 Z			~ 🛛 🗖		=	=		
	😳 New		Ctrl+N	L					
	Clone	1							

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

Al Engine Rule Wi	zard		$ \Box$ \times
Rule Block Types	Rule Block Designer		Rule Block Summary
Log	Add a Rule Block Type to begin.	Log Observed The Rule Block observed.	will signal when the specified logs are
Observed		Data Source – Data Process	tor Logs
		Group By	
	tit Al Engine Rule Block Wizard - Log Observed	\Box \times	
Not Observed Compound	Data Source Choose a data source for this rule block. Data Processor Logs		
	Primary Filters		
Not Observed Scheduled	Create Primary Criteria filters that identify loge to consider for the rule block. At least one Primary Criteria filter must be specified, and a log will not be considered unk Criteria filters are matched. Primary Criteria filters are evaluated after Day and Time Criteria and Log Source Criteria filters, and before Include and Exclude filters.	ess all Primary	
	Fields Filtered On Re	ecord Type	
1			1

5. In the "Primary Criteria" tab, click "New".

Al Engine Rule Block Wizard - Log Observed		×
Data Source		
Choose a data source for this rule block.		
Data Processor Logs V		
Primary Filters		
Create Primary Criteria filters that identify logs to consider for the rule block. At least one Primary Criteria filter must be specified, and a log will not be considered Criteria filters are matched. Primary Criteria filters are evaluated after Day and Time Criteria and Log Source Criteria filters, and before Include and Exclude filters	unless all I	Primary
🚱 New 🔨 Edit 🚯 Add Saved Filter 🔯 Delete		
Fields Fi New On	Record 1	Гуре
Primary Criteria Include Filters Exclude Filters Day and Time Criteria Log Source Criteria Group By AlE Summary Fields Information		
< Back Next > OK		Cancel

- 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"

Log Mess	age Filter								
t 1]		Add Ne	ew Field Filter:				\sim	Edit
Operator	Field		Filter Mode	Filtered Values					
•	Domain Ir	mpacted	ls	RecordedFutu	e : URL : Susp	icious : All			
		Fiel	d Filter Values				×		
		Doma Filter M FIC FI FIC FI	i n Impacted ode ilter In (Is) ilter Out (Is Not) Filter in Null value	es?					
		Add Iten	n ular Expression Add Item ecordedFuture : L	✓ Ignore Case JRL : Suspicious	e 	Add List.			

- 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"

Al Engine Rule Block Wizard - Log Observed		×
Include Filters Create filters that must be matched to consider a log for the rule block. If Include filters are specified, then logs must match all Primary Criteria filters and at least to be considered for the rule block . Include filters are evaluated after Day and Time Criteria, Log Source Criteria, and Primary Criteria filters, and before Exclude Wew Set Constraints and Saved Filter Set Constraints and Set Constraints	one Include fil filters.	ter
Fields Filtered On Vendor Message ID	Record Typ Custom	в 🗌

- 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.

Al Engine Rule Block Wizard - Log Ol	bserved		— 🗆	×
Group By Fields				
Group logs with identical values in the follo	wing fields I ogs without a value fo	r a selected Group By field will be excluded		
* indicates fields not written to the AIE Eve	nt AIE Drilldown will work, but the	field is not available for Smart Response or Event queries.		
Action	Known Host (Ungin)	Recipient Zone (Impacted) Zone (Visia)		
City (Impacted)	Location (Impacted)			
City (Drigin)	Log Source *	Begion (Origin)		
	Log Source Entity *			
Command	Log Source Host *	Result		
Common Event *	Log Source Root Entity *	Sender		
Country (Impacted)	MAC Address (Impacted)	Sender Identity		
Country (Origin)	MAC Address (Origin)	Serial Number		
CVE [MPE Rule Name	Session		
Direction	NAT IP Address (Impacted)	Session Type		
Domain Impacted	NAT IP Address (Origin)	Severity		
Domain Origin	NAT TCP/UDP Port (Impacted)	Status		
Entity (Impacted)	NAT ICP/UDP Port (Origin)			
	Network (Impacted)	TCP/UDP Port (Impacted)		
	Network (Ongin)			
	_ Object Name			
Host (Drigin)	Object Type			
Host (ongin)	Parent Process ID	User (Impacted)		
HostName (Origin)	Parent Process Name	User (Impacted) Identity		
Interface (Impacted)	Parent Process Path	User (Origin)		
Interface (Origin)	Policy	User (Origin) Identity		
IP Address (Impacted)	Process ID	User Agent		
IP Address (Origin)	Process Name	Vendor Info		
Known Application	Protocol	Vendor Message ID		
Known Host (Impacted)	Reason	Version		
Primary Criteria Include Filters Exclude	Filters Day and Time Criteria	Log Source Criteria Group By AlE Summary Fields Information		
		Louoge CY.1		
< Back Next >			ок с	ancel

- 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

New Event Settings Event Suppression AlE: Recorded Future Malicious Domainal Image: Enable suppression Sync with rule name Suppression Multiple: 60 Cassification: Security : Failed Malware 60 Image: Suppression Nultiple: Rak: 9 - High-High Image: Suppression Nultiple: 60 Image: Suppression Nultiple: Rak Rating: 9 - High-High Image: Suppression Period: 00:00:00 New Alam Settings Alam on event occurrence. Notification Settings Number of decimal places to print for quantitative values: 2 Image: Suppression Suppression Suppression Manager Rule Settings False Positive Probability (FPP): 5 - Medum-Medum Suppression Suppression Suppression Suppression Suppression Suppression Manager Rule Settings False Positive Probability (FPP): 5 - Medum-Medum Rule Set: Default RuleSet Image: Suppression Suppre	Al Engine Rule Wizard	
Common Event Name Event Suppression AlE: Recorded Future Malicious Domains AlE: Prevent Suppression Sync with rule name Suppression Multiple: Cassification: Security : Failed Malware Bits Becuity : Failed Malware Risk Rating: 9-High-High New Alam Settings Alam on event occurrence. Notification Settings Number of decimal places to print for quantitative values: 2 Rule Settings Advanced Settings False Postive Probability (FPP): 5- Medium-Medium Environmental Dependence Factor (EDF): None Specify the date and time when the Rule should be automatically disabled. Segregate log data by Entity when processed by the rule and output as an Event or an Align Surgerspation Specify the date and time when the Rule should be automatically disabled. So None No sepiration Cassification Expiration Cassification	New Event Settings	
AIE: Recorded Future Malicious Domains! Image: Classification: Suppression Suppression Suppression Classification: Security: Failed Malware Image: Classification: Suppression Suppression Multiple: 60 Image: Classification: Suppression Risk Rating: 9-High-High Image: Classification: Suppression Automatication: Suppression	Common Event Name	Event Suppression
□ Sync with rule name Suppression Multiple: 60 • Classification: Security : Failed Malware € Risk Rating: 9 - High-High • Attach Suppression Period: 00:00:01 Risk Rating: 9 - High-High • New Alam Settings • AlE Event Forwarding □ Alam on event occurrence. • Proward AlE Event to Platform Manager Number of decimal places to print for quantitative values: 2 • Rule Settings • False Positive Probability (FPP): 5 - Medium-Medium Environmental Dependence Factor (EDF): None Specify the date and time when the Rule should be automatically disabled. • • No expiration •	AIE: Recorded Future Malicious Domains	
Classification: Security : Failed Malware Risk Rating: 9 - High-High New Alam Settings Alam on event occurrence. Notification Settings Number of decimal places to print for quantitative values: Palse Postive Probability (FPP): 5 - Medium-Medium Rule Settings Advanced Settings False Postive Probability (FPP): 5 - Medium-Medium Rule Set: Default Rule Set Environmental Dependence Factor (EDF): None Specify the date and time when the Rule should be automatically disabled. Image: None Image: None Image: Data Segregation Segregate log data by Entity when processed by the rule and output as an Event or an Align None Image: Data Segregation Segregate log data by Entity when processed by the rule and output as an Event or an Align None Image: Data Segregation Segregate log data by Entity when processed by the rule and output as an Event or an Align None Image: Data Segregation Segregate log data by Entity when processed by the rule and output as an Event or an Align None Image: Data Segregation	Sync with rule name	Suppression Multiple: 60 🚖
Risk Rating: 9 - High-High = Suppression Period: 00:01:00 AIE Event Forwarding Forward AIE Event to Platform Manager New Alarm Settings Forward AIE Event to Platform Manager New Alarm on event occurrence. Notification Settings Number of decimal places to print for quantitative values: 2 Rule Settings Advanced Settings False Positive Probability (FPP): 5 - Medium-Medium ▼ Environmental Dependence Factor (EDF): None Expiration Date Data Segregation Specify the date and time when the Rule should be automatically disabled. Segregate log data by Entity when processed by the rule and output as an Event or an A None Log Source Entity Log Source Entity 	Classification: Security : Failed Malware	x Suppression Interval: 00:00:01
Hisk Rating: 9 - High-High ✓ All Event Forwarding ✓ Forward AlE Event to Platform Manager New Alam Settings Alam on event occurrence. Notification Settings Number of decimal places to print for quantitative values: Palse Positive Probability (FPP): 5 - Medium-Medium ✓ Environmental Dependence Factor (EDF): None Specify the date and time when the Rule should be automatically disabled. Image: None Image: None<		= Suppression Period: 00:01:00
New Alam Settings Alam on event occurrence. Notification Settings Number of decimal places to print for quantitative values: Palse Settings Rule Settings False Positive Probability (FPP): 5 - Medium-Medium Environmental Dependence Factor (EDF): None Specify the date and time when the Rule should be automatically disabled. Image: Popple of the date and time when the Rule should be automatically disabled. Image: Popple of the date and time when the Rule should be automatically disabled. Image: Popple of the date and time when the Rule should be automatically disabled. Image: Popple of the date and time when the Rule should be automatically disabled. Image: Popple of the date and time when the Rule should be automatically disabled. Image: Popple of the date and time when the Rule should be automatically disabled. Image: Popple of the date and time when the Rule should be automatically disabled. Image: Popple of the date and time when the Rule should be automatically disabled. Image: Popple of the date and time when the Rule should be automatically disabled. Image: Popple of the date and time when the Rule should be automatically disabled. Image: Popple of the date and time when the Rule should be automatically disabled. Image: Popple of the date and time when the Rule should be automatically disabled. Image: Popple of the date and time when the Rule should be automatically disabled. Image: Popple of the date and time when the Rule should be automatically disabled. Image: Popple of the date and time when the Rule	Risk Rating: 9 - High-High V	AIE Event Forwarding
New Alam Settings Alam on event occurrence. Notification Settings Number of decimal places to print for quantitative values: 2 Rule Settings False Positive Probability (FPP): 5 - Medium-Medium Environmental Dependence Factor (EDF): None Specify the date and time when the Rule should be automatically disabled. Image: Image		Forward AIE Event to Platform Manager
Advanced Settings False Positive Probability (FPP): 5 - Medium-Medium Environmental Dependence Factor (EDF): None Expiration Date Data Segregation Specify the date and time when the Rule should be automatically disabled. Segregate log data by Entity when processed by the rule and output as an Event or an A No expiration Expires on 1/28/2019 8:49 PM C Log Source Entity 	Number of decimal places to print for quantitative values: 2	
False Positive Probability (FPP): 5 - Medium-Medium Rule Set: Default RuleSet [[]] Environmental Dependence Factor (EDF): None Runtime Priority: Normal Image: Comparison of the comparison		Advanced Settings
Environmental Dependence Factor (EDF): None Runtime Priority: Normal Expiration Date Data Segregation Specify the date and time when the Rule should be automatically disabled. Segregate log data by Entity when processed by the rule and output as an Event or an A No expiration Expires on 1/28/2019 8:49 PM O Log Source Entity 	False Positive Probability (FPP): 5 - Medium-Medium	Rule Set: Default RuleSet
Expiration Date Data Segregation Specify the date and time when the Rule should be automatically disabled. Segregate log data by Entity when processed by the rule and output as an Event or an A No expiration Expires on 1/28/2019 8:49 PM O Expires on 1/28/2019 8:49 PM 	Environmental Dependence Factor (EDF): None ~	Runtime Priority: Nomal V
Specify the date and time when the Rule should be automatically disabled. Segregate log data by Entity when processed by the rule and output as an Event or an A No expiration Expires on 1/28/2019 8:49 PM O Expires on 1/28/2019 8:49 PM O Expires on 1/28/2019 8:49 PM 	Expiration Date	Data Segregation
No expiration No expiration Expires on 1/28/2019 8:49 PM C	Specify the date and time when the Rule should be automatically disabled.	Segregate log data by Entity when processed by the rule and output as an Event or an Alarm.
○ Expires on 1/28/2019 8:49 PM □ ○ Log Source Entity	No expiration	None
	O Expires on 1/28/2019 8:49 PM	O Log Source Entity
◯ Log Source Root Entity		O Log Source Root Entity

- 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.

LogRhyt	LogRhythm Console - [Deployment Manager]										
🚮 <u>F</u> ile <u>E</u> d	🕼 Eile Edit View My LogRhythm Iools Window Help										
0 2	<u>P</u> ersonal Dashboard 🔍 <u>I</u> nvestiga	ate 🙋 <u>T</u> ail 🌔 <u>R</u> ep	ort Center	📕 List Manag	er <u>为</u> eployme	ent Monitor 🛛 🖏 D	eplo <u>y</u> ment Manager				
Entities F	Platform Manager Data Processors	Al Engine Network Mon	itors System	Monitors Log	Sources Log Proce	ssing Policies Alarr	n Rules People				
Al Engine											
0 🐵	🔁 🚳 Actions 🛛 View: EC2AMAZ-HFJ6 🔽 🔣 Restart Al Engine Servers										
Drag a co	olumn header here to group by that	t column.									
Action	Al Engine Rule Name	Ζ.	Rule Status ∇	Restart	Activation	Expiration	Data Segregation Mode	Alarm Status			
	Recorded Future - Malicious Doma	ain 🗸 🗹			=						
	Recorded Future - Malicious Domain	n Detected	Enabled		N/A	N/A	None	Enabled			

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 <u>link</u> and Mozilla Firefox at this <u>link</u>). More information about the Recorded Future Browser Extension is available on this <u>support</u> 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
 - 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

			Search	ii - ≗- 0
	🧿 Paused 🕨 🕨	۵	Inspector	
Fri 25 Jan 27 Tue 29 Closed		Id: 2341 A	AIE: Recorded Fu IP Detected	ıture - Malicious d
Group: Any 🔻 🛛 Alarm Id: Any 🔻 🛛 In a Case: Any 💙	 Reset Filters 	Data, C	omments &	Al Engine
Sort By Please Select 👻		C	Details	Rule
RISK 01/30/2019 5:01:48 pm ld: 2344		Event Data		_
		Alarm ID	2341	
SmartResponse Not Set	7	Alarm Dat	e 01/30/20	19 5:01:48 pm
New 🔻 🔝 🗊 🔘	-	Alarm Nan	ne AIE: Reco Malicious	rded Future - IP Detected
AIE: Recorded Future - Malicious IP		Classificat	ion Suspiciou	s
Global Entity RISK Global Entity		Log Source	e Al Engine	
SmartResponse Not Set		Zone (Impacted	External)	
New ▼		Entity (Origin)	Global En	tity
AIE: Recorded Future - Malicious IP		Entity (Impacted	Global En)	tity
Global Entity RISK 01/30/2019 5:01:48 pm Id: 2338		Host (Impacted	185.38.24)	9.242

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

185.38.249.242 – IP Address	·I <mark>:</mark> I·Recorded Fu
1 Analyst Note 59 References to This Entity First Reference Collected on May 12, 2014 Latest Reference Collected on Jan 25, 2019 ASN AS197226, ORG sprint S.A., GEO Poland Show recent cyber events involving 185.38.249.242 in Table	Malicious Risk Score 71 3 of 50 Risk Rules Triggered
Show all events involving 185.38.249.242 in Table ✔	
Triggered Risk Rules	
Recently Linked to Intrusion Method • 1 sighting on 1 source VirusTotal URLs. 1 related intrusion method: Badware. Most 791cf40bedcd4dbfea48a0ece59387bd348d8a00455a07ab0a	e recent link (Jan 25, 2019): https://www.virustotal.com/en/url/3a5 i367e1c/analysis/
Phishing Host • 8 sightings on 1 source MalwareDomainList: Malicious URL Reports (reported phish) hxxp://185.38.249.242/b7.exe, hxxp://185.38.249.242/b2.exe	I. IP Address reported as host of 8 active phishing URLs including 2, hxxp://185.38.249.242/pl.exe.
Historically Linked to Intrusion Method • 8 sightings on 2 so VirusTotal URLs, MalwareDomainList updates. 3 related intru 15, 2018): https://www.virustotal.com/en/url/87b697aa080ed s/	ources Jsion methods: Worm.Autorun, Trojan, Badware. Most recent lin d9ca797f20e4d735ed6e0a58d6e09c44777ae9e89a725ee0f0cb/a
O Learn more about IP Address risk rules	
Analyst Notes from Recorded Future	
Malware Threat List http://valouweeigenaren.nl/customers/billing/df367548-18.z <https: #!="" ?sc="4GtsCHArl3gd" app.recordedfuture.com="" live=""> http://www.cerquasas.it/wp-admin/user/UPS_INVOICE.rar <https: #="" app.recordedfuture.com="" live=""> URL 0 http://www.ceisystems.it/ <https: <br="" app.recordedfuture.com="" live="">http://www.inevo.co.il/ <https: <br="" app.recordedfuture.com="" live="">http://www.smartscan.ro <https: <="" app.recordedfuture.com="" live="" th=""><th>ip ∙ URL 0 /live/#> URL 0 e/#> URL 0 live/#> URL 0</th></https:></https:></https:></https:></https:>	ip ∙ URL 0 /live/#> URL 0 e/#> URL 0 live/#> URL 0

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 <u>support</u> 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

ervice Manager			_		Х
vice nce Service configu _{vice}	ration settings.				
qure					
			Add Cus	tom Sour	се
Custom:	RecordedFuture				
Enabled: 🛛	3	Check All	Clear All		
Feed Name domain_histor	ical_covid19related_domai	⊽ n_lure	Enable	•	
domain_comp domain_cc_u	romised_url I				
domain_cc_n domain_cc_d	ameserver ns_name				
domain_black domain_active	listed_dns_name e_phishing_url				
Last Download	ed: 1/18/2021 07:07 PM				
Next Run Time	y: 24 Hours	~ D	ownload N	ow	
First Run at:	05:00 AM 🚖				
Remove Provi	der Edit Provider	Tes	t Sa	ive	
	Service Manager Prvice pervice Provice Provice Provice Previce Previce Pr	Service Manager Prvice Previce Previce Provice Provice Provice Provice Previce Previce Pr	Service Manager Prvice Prote Pro	Service Manager — Prvice tence Service configuration settings. ervice nfigure Add Cus Custom: RecordedFuture Enabled: ☑ Check All Clear All Feed Name ☑ Check All Clear All Feed Name ☑ Check All Clear All Gomain_historical_covid19related_domain_lure domain_full domain_co_url domain_co_url domain_oc_url domain_oc_url domain_oc_url domain_oc_url domain_oc_url domain_oc_url domain_active_phishing_url Last Downloaded: 1/18/2021 07:07 PM Next Run Time: 1/19/2021 07:07 PM Next Run Time: 1/19/2021 07:07 PM Next Run Time: 1/19/2021 07:07 PM Download every: 24 Hours ☑ Download N First Run at: 05:00 AM ④ Remove Provider Edit Provider Test Sa	Service Manager Prvice Pervice Pervice

- 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.

📙 💆 📙 🖛 LF	R_lists						-	×
File Home	Share	View						~ 🕐
← → ~ ↑	> Thi	s PC > Documents > LR_lists				✓ Ö Search	LR_lists	Q
	^	Name	Date modified	Туре	Size			
A Quick access		📄 AlienVault-IP-Attack-All	1/19/2021 2:30 PM	Text Document	23 KB			
Desktop	*	📄 RecordedFuture-Domains-Full	1/17/2021 7:07 PM	Text Document	52 KB			
🔶 Downloads	*	RecordedFuture-IP-Suspicious-All	1/17/2021 7:07 PM	Text Document	52 KB			
😭 Documents	*	📄 RecordedFuture-URL-Suspicious-All	1/17/2021 7:07 PM	Text Document	8 KB			
📰 Pictures	*							
📙 Log Gen Scri	ipts							

- 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.

Lo	gRhythn	n Console - [Lis	t Manager]							- a ×
📄 Fil	e MyL	ogRhythm To	ols Window Help							_ 8>
0	0.	🕴 🧟 Person	al Dashboard 🔍 Investigate 🛷 Tail 🦲	Report Center	List Manager	No Deploy	ment Monitor	🕵 Deployment Manager		
-					-	1.00				
Drag	a colur	nn header here	to group by that column.							
_	Action	List Type	Name	Entry Coun	Use Contexts	Auto Import	Import Options	Import Filename	Restricted Read	Description
Z A				-						
		General Value	RecordedFuture : Email Address : Suspicious : All	1	0 DomainImpacted, URL		Replace	RecordedFuture-EmailAddress-Threat-All.txt		
		General Value	RecordedFuture : File Hash : Suspicious : All	1	0 DomainImpacted, URL		Replace	RecordedFuture-FileHash-Threat-All.txt		
		General Value	RecordedFuture : Filepath : Malware : All	1	0 Object		Replace	RecordedFuture-Filepath-Malware-All. txt		
		General Value	RecordedFuture : URL : Suspicious : All	40	4 DomainImpacted, URL					
		Host	RecordedFuture : IP : Suspicious : All	347	3 Host					
8		Identity	CloudAl: Ignore for 24 Hours		0 Identity					Anomaly scores from CloudAl will not be displayed for the identities in this list. Identities added to this list will automatically expire 24 hours after they are added.
		Identity	CloudAl: Monitored Identities		0 Identity					Identifies monitored by CloudAI
		Log Source	QsEMP: Data Loss Prevention		B Log Source					Production data loss prevention devices, including LogPihythm Data Loss Detender.
		Log Source	QsEMP: Production 'NIX Servers	1	0 Log Source					System and audit logs of production UNIX and Linux servers. LogRhythm User Activity Monitor and Network Connection Monitor for production agents.
		Log Source	QsEMP: Production Firewalls		0 Log Source					System logs of all production firewalts.
		Log Source	QsEMP: Production IDS/IPS Devices		0 Log Source					System logs of devices with intrusion detection or prevention capabilities. Examples: firewalls and UTM devices that include these capabilities.
		Log Source	QsEMP: Production Malware Detection Devices		0 Log Source					System or application logs of devices providing malware detection capabilities. Examples: anti-virus, spyware, general malware detection software and central serv
		Log Source	QsEMP: Production Routers and Switches		0 Log Source					System logs of all production routers and switches.
		Log Source	QsEMP: Production Windows Servers		0 Log Source					System, Application, and Security Event Logs of production Windows Servers. LogRhythm User Activity Monitor, Process Monitor and Network Connection Monitor
•	Ē	Host	RecordedFuture : Domains: Full	347.	3 Host	M	Append	RecordedFuture-Domains-Full.txt		

- 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.

LogRh	ythm Console - [Deployment Manager]												
🚮 File E	🗊 File Edit View MyLogRhythm Tools Window Help												
۵ 🚨	Personal Dashboard 🔍 Investigate 🖉	Tail 🌖 Repo	rt Center 🛛 📕	List Manager	🗽 Deployment Mo	initor 🗊 Deployment	: Manager						
Entity	Platform Manager Data Processors Al Engine	Network Monitor	s System Mo	nitors Log Sources	Log Processing Po	licies Alarm Rules Pe	ople Third Pa	arty Applications					
Al Engine													
O 😔	Actions • View: 172.30.128.227 •	Restart Al Engir	ne Servers										
Drag a	column header here to group by that column.												
Drag a Action	column header here to group by that column. Al Engine Rule Name	 Rule Status ∇ 	Restart	Activation	Expiration	Data Segregation Mode	Alarm Status	Auto Drildown	EDF	FPP	Suppress For	Runtime Priority	CI
Drag a	column header here to group by that column. Al Engine Rule Name	′Rule Status ⊽ ■	Restart	Activation	Expiration	Data Segregation Mode	Alarm Status	Auto Drilldown	EDF	FPP	Suppress For	Runtime Priority	CI
Drag a Action	Column header here to group by that column. Al Engine Rule Name Recorded Future Malicious Domains TESTING	Rule Status ⊽ ■ Enabled	Restart	Activation = N/A	Expiration = N/A	Data Segregation Mode	Alarm Status Enabled	Auto Drilldown	EDF	FPP	Suppress For	Runtime Priority	CI =
Action	column header here to group by that column. Al Engine Rule Name Recorded Future Malicious Domains TESTING Recorded Future Malicious IPs	Rule Status ⊽ Enabled Enabled	Restart	Activation N/A N/A	Expiration N/A N/A	Data Segregation Mode None None	Alarm Status Enabled Enabled	Auto Drilldown Enabled Enabled	EDF None None	FPP Medium-Medium Medium-Medium	Suppress For I Minute 1 Minute	Runtime Priority Normal Normal	CI =
Action	column header here to group by that column. Al Engine Rule Name Recorded Future Malicious Domains TESTING Recorded Future Malicious IPs	 Rule Status ♥ Enabled Enabled 	Restart	Activation = N/A N/A	Expiration = N/A N/A	Data Segregation Mode	Alarm Status Enabled Enabled	Auto Drilldown Enabled Enabled	EDF None None	FPP Medium-Medium Medium-Medium	Suppress For Minute	Runtime Priority Normal	CI =

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.

👬 Al Engine Rule Wiz	ard	— 🗆 X
Rule Block Types	Rule Block Designer	Rule Block Summary
Log		Log Observed The Rule Block will signal when the specified logs are observed.
*		Testing Domain
Observed		Data Source Data Processor Logs
		Primary Criteria Vendor Message ID Is : c&c dns domain names
		Include Filters Domain Impacted Is : RecordedFuture : URL : Suspicious : All
Not Ubserved Compound		Log Sources All Log Sources
Bo		Group By Domain Impacted
Not Observed Scheduled		

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



Primary Criteria Include Filters Exclude Filters Day and Time Criteria Log Source Criteria Group By AIE Summary Fields Information

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*

Include: Filter Create lift: L Og Message Filter Image: Create lift: Filter Image: Create lift: Image: Create lift: I	Al Engine Rule Block Wizard - Log Ob	📫 Field Filter Values		\Box ×		_	\times
Primary Cril	Include Create file New Fields File Domain Impace	Domain Impacted Filer Mode Filer Mode Filer Uu (Is Not) Filer Uu (Is Not) Regular Expression Add Item Add Item RecordedFuture : URL : Suspicious : All RecordedFuture : URL : Suspicious : All	Add List		Edit Values	X Se fill Delete	,
<back next=""> OK Cancel OK Cancel</back>	< Back Next >		OK	Cancel		K Can	cel

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 \rightarrow LogRhythm Service Configuration.

LogRhythm Threat Intelligence Service Manager	-		\times
File Options			
LogRhythm Service Configuration			
Add Custom Source			
View Logs ce configuration settings.			
Exit			
Proxy Settings: Not Enabled Configure			
Threat Data Providers	Add Cu	stom Sour	се
Open Source : Abuse.ch Custom: RF - Domains Sechlod: 2	Clear		
	Lieal A		1

– 🗆 🗙 🟥 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 LogRhythmEMDB Database: 🗹 Log in with Windows account User Name: Password: Test Connection

List Path: C:\Program Files\LogRhythm\LogRhythm Job Manager\config\list_in

Next	
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.

"StixProviders": [ł "NumofBackDaysData": 7, "Password": "3||qHrcsB3y/UwQdOhq28any20j0oEeRbNjLlSN5v85x7/zgSuy4eJ+amEWvYw2i/P7", "LastFullDownloadOn": "5/16/2018 05:00:15 AM", "SourceURL": "https://api.recordedfuture.com/taxii", "UserName": "3||1nuo4cG0StCEfwy0vrH8NQ==", "Enabled": true, "IsFirstRun": false, "Retired": false, "Frequency": 60, "DownloadedDataOn": "5/18/2018 05:00 PM", "DownloadLastAttemptedOn": "5/18/2018 05:00 PM", "FirstRunTime": "05:00 AM", "ProviderLastUpdatedDate": "5/18/2018 05:00:25 PM", "ProviderName": "Recorded Future - Malicious IP Addresses", "CustomObjectTypes": [], "CertificateAuthentication": { "isCertificateAuthentication": false, "certificatePath": "", "certificatePassword": ""

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

