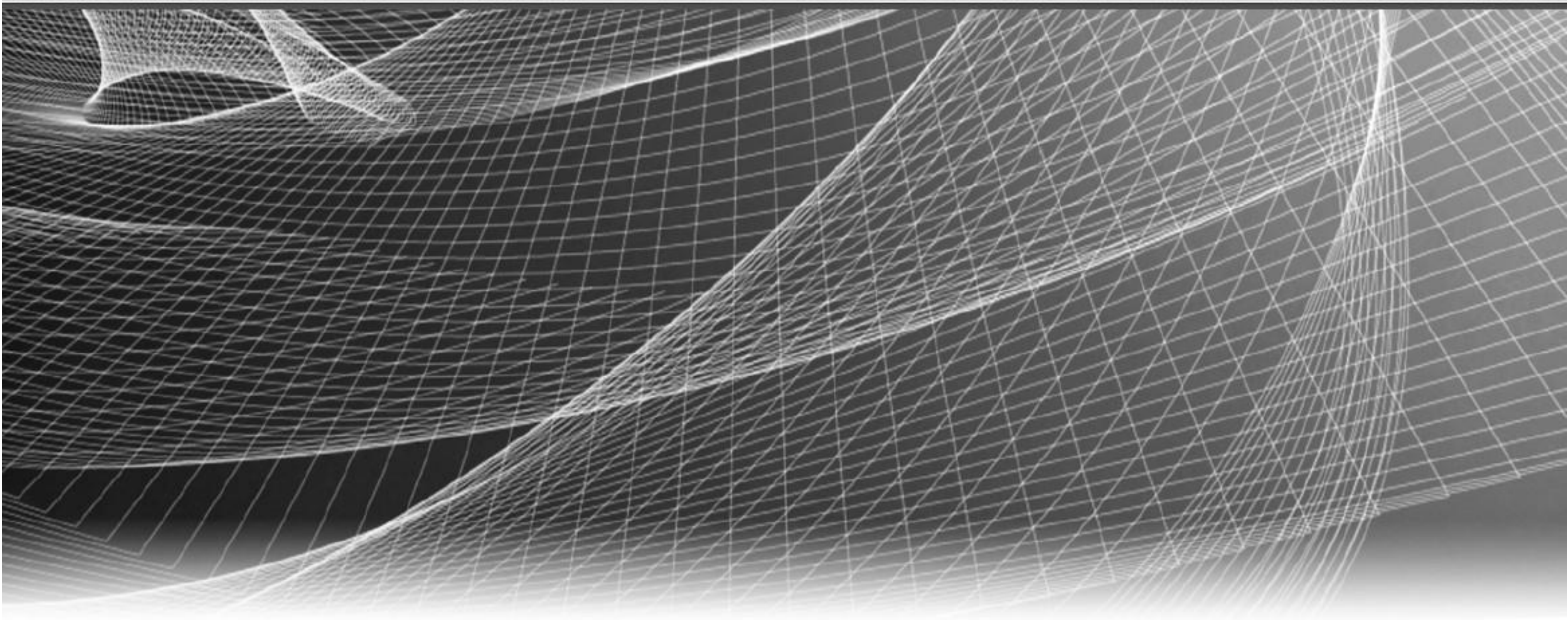


RSA Security Analytics

RSA NetWitness & LogRythm Integration Guide

Trademarks

RSA, the RSA Logo and DELL/EMC are either registered trademarks or trademarks of DELL/EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of DELL/EMC trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm.

License Agreement

This software and the associated documentation are proprietary and confidential to DELL/EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by DELL/EMC.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed in the thirdpartylicenses.pdf file.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any DELL/EMC software described in this publication requires an applicable software license. DELL/EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." DELL/EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Table of Contents

Table of Contents

Overview

The following document will describe how to configure integrations between RSA NetWitness and LogRythm.

Version Testing

LogRythm

This guide was created and tested on LogRythm Version 7.1.9, and it may work on versions as old as 7.0.0

RSA NetWitness

This was created and tested on RSA NetWitness 10.6.1.1, but it should work on versions of RSA NetWitness going back to 10.5.0.0.

Getting Started

Right-Click Integrations

Critical Start Threat Analytics Google Chrome Extensionension

RSA NetWitness has the ability to conduct investigations via a web interface. Many other security tools (SIEM, IPS, threat feeds, etc.) also use a web interface. Critical Start released their Threat Analytics Search extension for Chrome that allows integration of 3rd party (web GUI) security tools with RSA NetWitness.

If you aren't familiar with the extension, it can be summarized as a:

"Tool for security analysts, malware hunters, and incident responders that allows the use the of right-click menu in Chrome to conduct single or group searches for selected text such as file hash, IP address, or domain. The extension reduces time analysts spend visiting the same websites repeatedly to gather information about IP addresses, websites, file hashes, and domains."

source: https://community.fireeye.com/people/criticalstart1/blog/2014/03/31/fireeye-integration-with-rsa-netwitnesssecurity-analytics

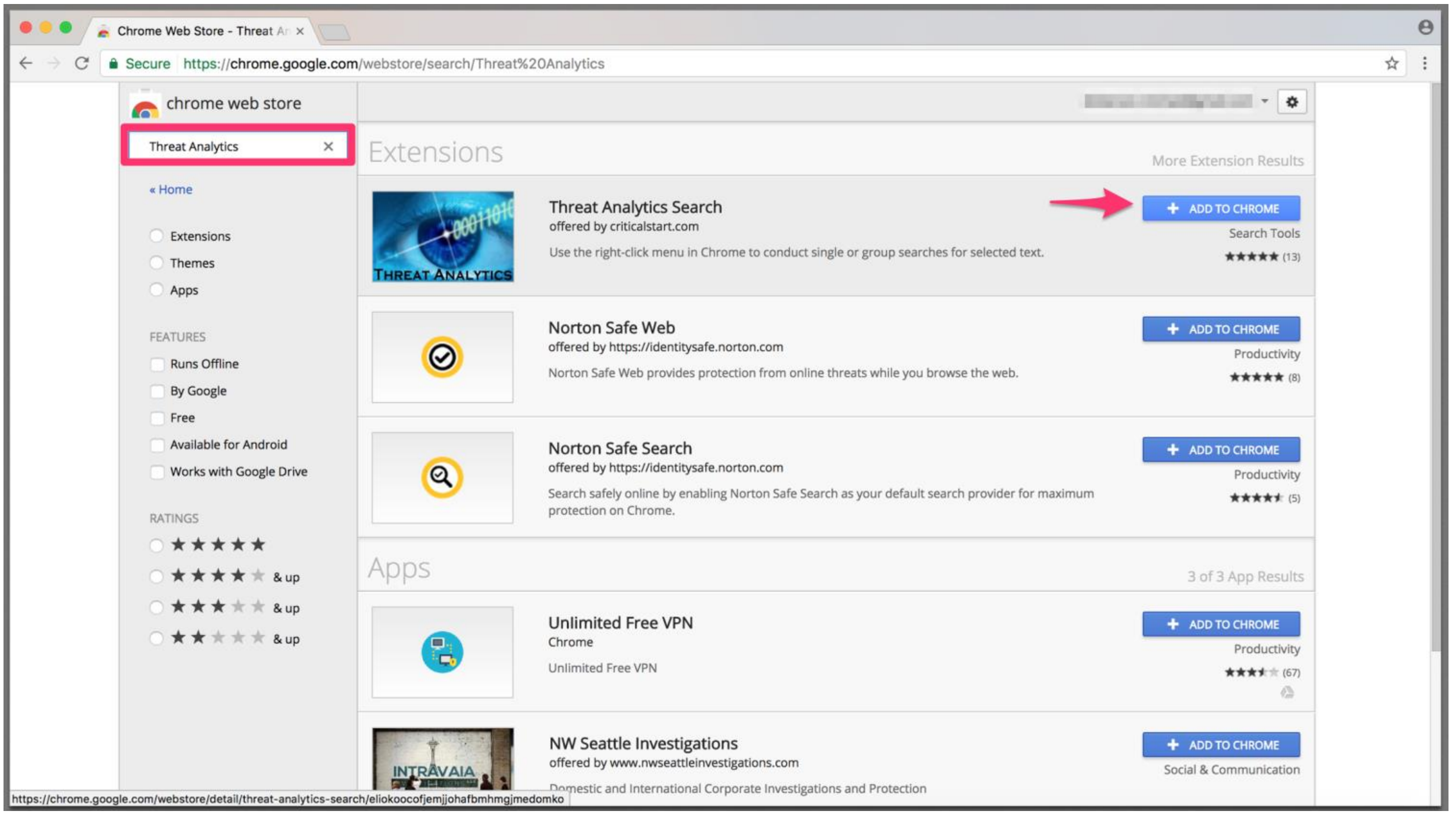
Configuring the Critical Start extension is very simple. A detailed instructional video is located here: https://community.rsa.com/videos/21070. There is also a configuration guide on RSA Link that focuses entirely on configuring the plugin located here: https://community.rsa.com/docs/DOC-63056.

This extension allows a user to right click and drill into virtually any piece of metadata in RSA NetWitness while in virtually any one of your existing security tools while using Google Chrome.

Setting up the Critical Start Plugin

Install the Plugin

1. Go to https://chrome.google.com/webstore/category/extensions and type 'Threat Analytics' in the search bar and hit enter. Then click on the + ADD TO CHROME button.



Chrome Web Store - Threat A

Secure https://chrome.google.com/webstore/search/Threat%20Analytics

chrome web store

Threat Analytics

Extensions — More Extension Results

Threat Analytics Search
offered by criticalstart.com
Use the right-click menu in Chrome to conduct single or group searches for selected text.
+ ADD TO CHROME — Search Tools ★★★★★ (13)

Norton Safe Web
offered by https://identitysafe.norton.com
Norton Safe Web provides protection from online threats while you browse the web.
+ ADD TO CHROME — Productivity ★★★★★ (8)

Norton Safe Search
offered by https://identitysafe.norton.com
Search safely online by enabling Norton Safe Search as your default search provider for maximum protection on Chrome.
+ ADD TO CHROME — Productivity ★★★★★ (5)

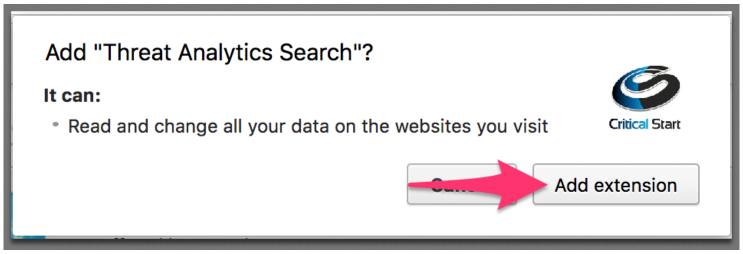
Apps — 3 of 3 App Results

Unlimited Free VPN
Chrome
Unlimited Free VPN
+ ADD TO CHROME — Productivity ★★★★☆ (67)

NW Seattle Investigations
offered by www.nwseattleinvestigations.com
Domestic and International Corporate Investigations and Protection
+ ADD TO CHROME — Social & Communication

https://chrome.google.com/webstore/detail/threat-analytics-search/eliokoocofjemjjohafbmhmgjmedomko

2. Click 'Add Extension'…

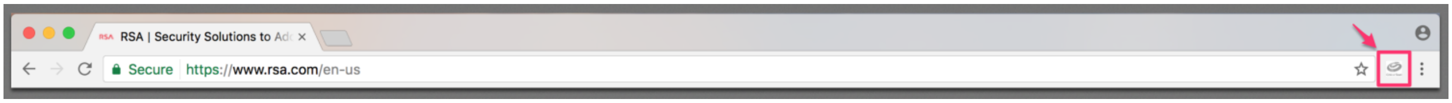


Add "Threat Analytics Search"?

It can:

- Read and change all your data on the websites you visit

3. You will now see that the extension is installed to the right of your browsers address bar

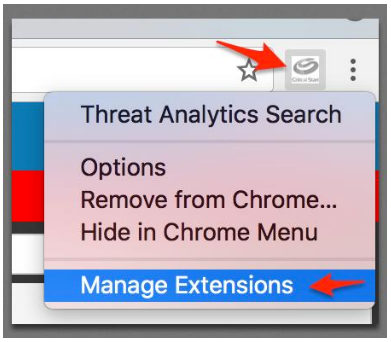


RSA | Security Solutions to Ad

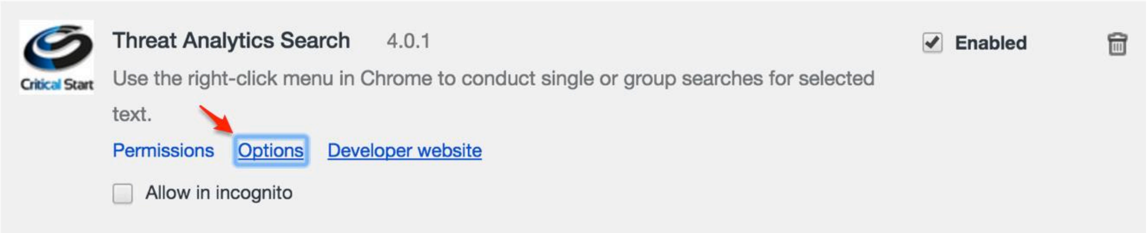
Secure https://www.rsa.com/en-us

Configuring the Plugin

1. Next click on the ‘Threat Analytics’ icon to the right of your browsers address bar and then click ‘Manage Extensions’



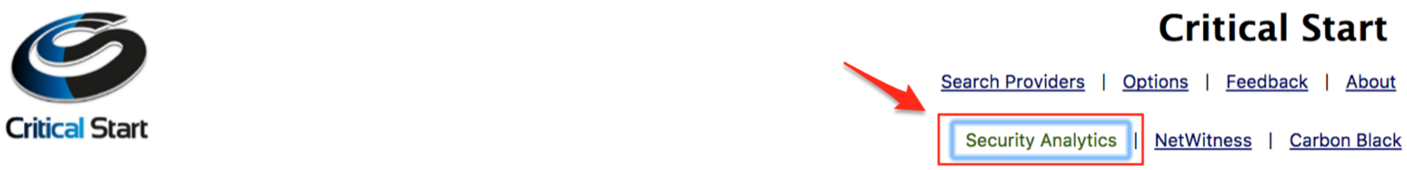
2. Next click on ‘Options’



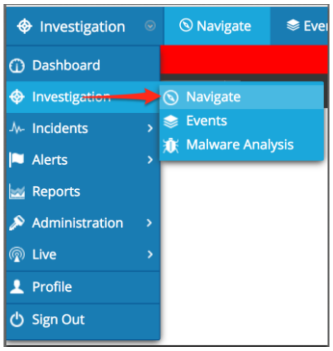
Threat Analytics Search 4.0.1

Use the right-click menu in Chrome to conduct single or group searches for selected text.

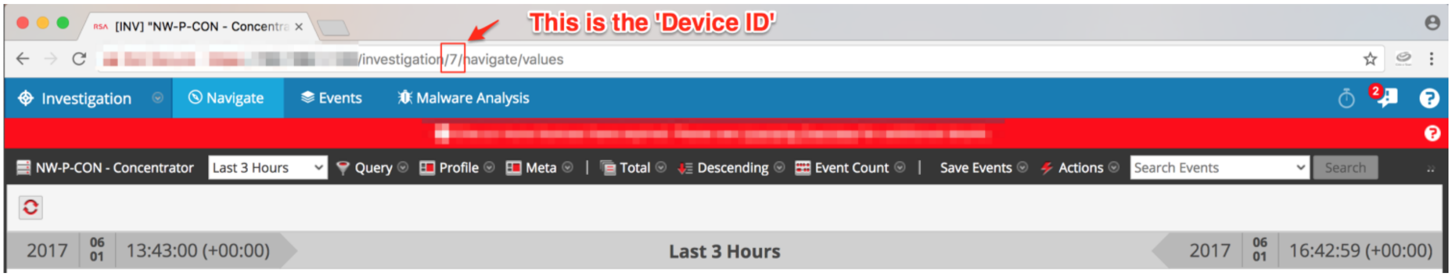
3. Next click the ‘Security Analytics’ link


Critical Start
Critical Start
Search Providers | Options | Feedback | About
Security Analytics | NetWitness | Carbon Black

4. Next you will need to get some information from Netwitness to complete the setup. Login into the Netwitness UI and open an Investigation.



5. Here you will be looking to obtain the RSA Netwitness Device ID. It will be the number between investigation and navigate in your browsers address bar. In this case it is <7>, but each case will likely be different.



This is the 'Device ID'

[INV] "NW-P-CON - Concentra

[redacted]/investigation/7/navigate/values

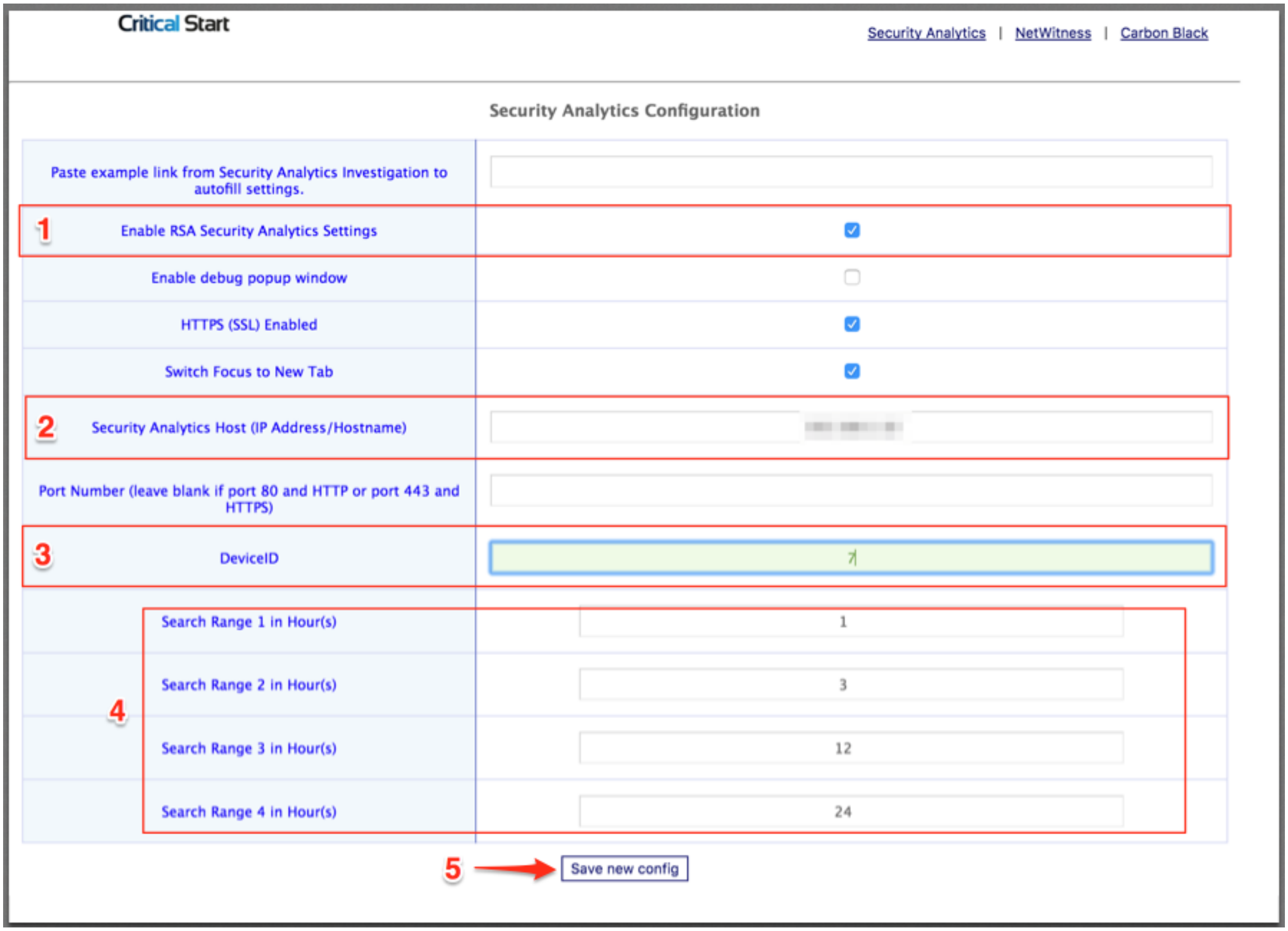
[redacted]

NW-P-CON - Concentrator | Last 3 Hours

2017 06 01 13:43:00 (+00:00) | Last 3 Hours | 2017 06 01 16:42:59 (+00:00)

6. Next you will fill in the appropriate information to complete the setup of the Threat Analytics plugin.

   a. Click checkbox to enable the Security Analytics plugin.
   b. Enter the IP address of your RSA Netwitness instance.
   c. Enter the Device ID you obtained from the step above.
   d. To make it easy, change the 'Search Range' options to (1)(3)(12)(24), these are time ranges in hours that will be queried, and can be set to whatever your requirements are.
   e. Click 'Save new config' to SAVE your configuration.



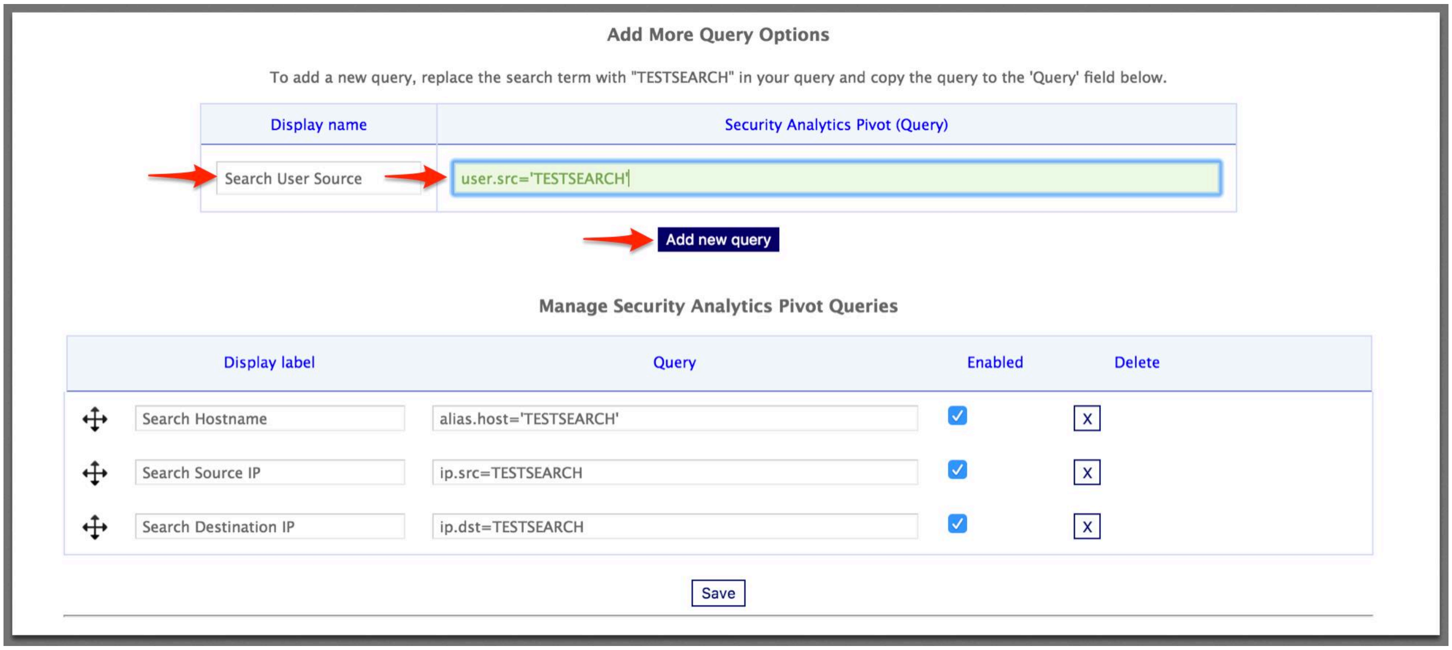
Security Analytics Configuration

Paste example link from Security Analytics Investigation to autofill settings.	
1 Enable RSA Security Analytics Settings	☑
Enable debug popup window	□
HTTPS (SSL) Enabled	☑
Switch Focus to New Tab	☑
2 Security Analytics Host (IP Address/Hostname)	[redacted]
Port Number (leave blank if port 80 and HTTP or port 443 and HTTPS)	
3 DeviceID	7
4 Search Range 1 in Hour(s)	1
Search Range 2 in Hour(s)	3
Search Range 3 in Hour(s)	12
Search Range 4 in Hour(s)	24

5 Save new config

7. Next you can configure advanced query options. There are (3) out of the box Pivot Queries included, but you can add as many as you would like. If you can query for it in Netwitness you can add an option for it in the Threat Analytics plugin. The example below will illustrate adding the user.src Meta Key.

   a. Under 'Display Name' enter <Search User Source>
   b. Under 'Security Analytics Pivot (Query)' enter <user.src='TESTSEARCH'>
   c. Click 'Add new query'



Add More Query Options

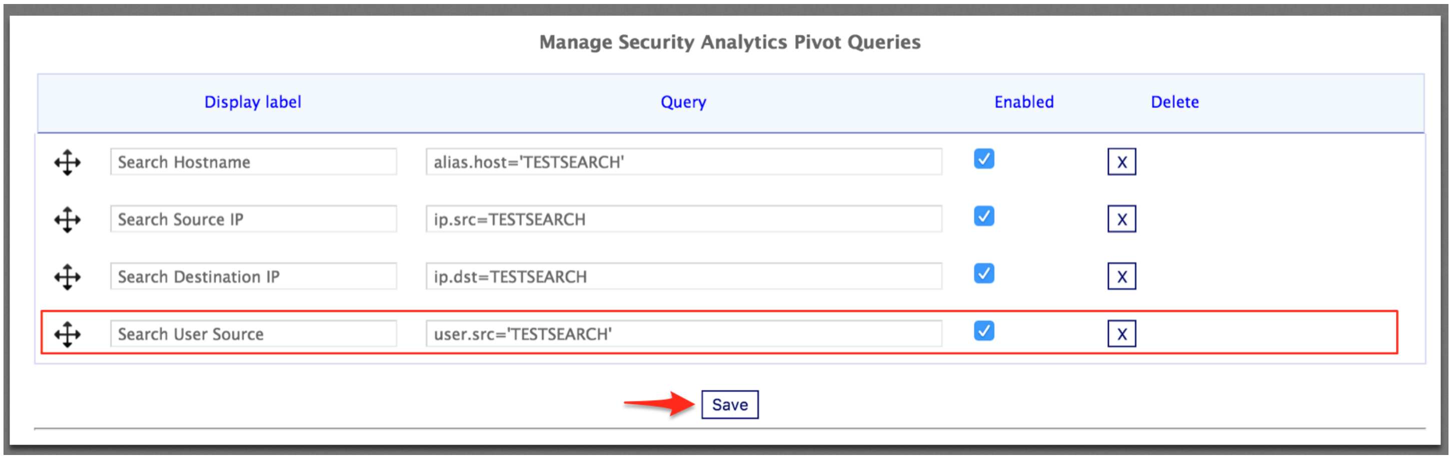
To add a new query, replace the search term with "TESTSEARCH" in your query and copy the query to the 'Query' field below.

Display name	Security Analytics Pivot (Query)
Search User Source	user.src='TESTSEARCH'

Manage Security Analytics Pivot Queries

	Display label	Query	Enabled	Delete
✥	Search Hostname	alias.host='TESTSEARCH'	☑	X
✥	Search Source IP	ip.src=TESTSEARCH	☑	X
✥	Search Destination IP	ip.dst=TESTSEARCH	☑	X

8. Now you should see your new quiery below. You can add as many additional Pivot Queries as you would like. Click the 'Save' button when you are done to save your configuration. You may also quickly export your configuration and import it on another machine, give it to your co-workers, SOC analysts, etc.

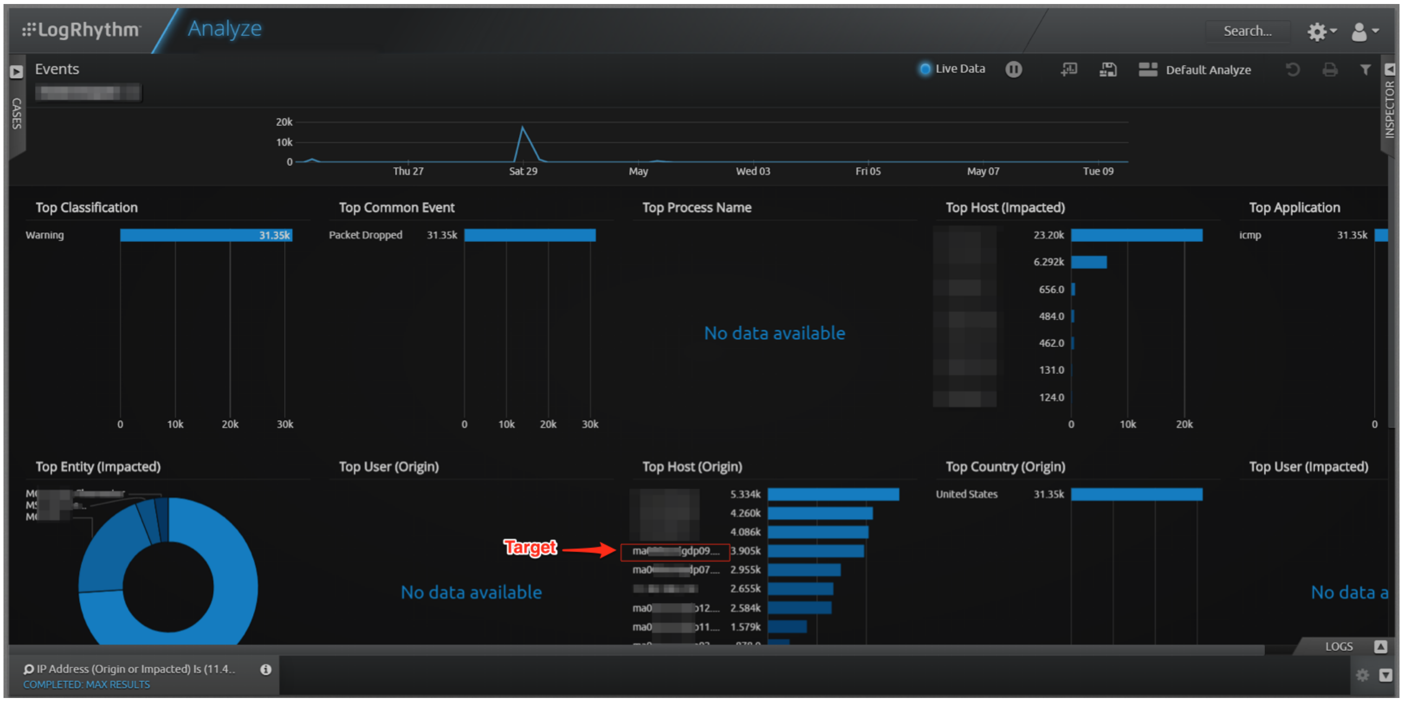


Manage Security Analytics Pivot Queries

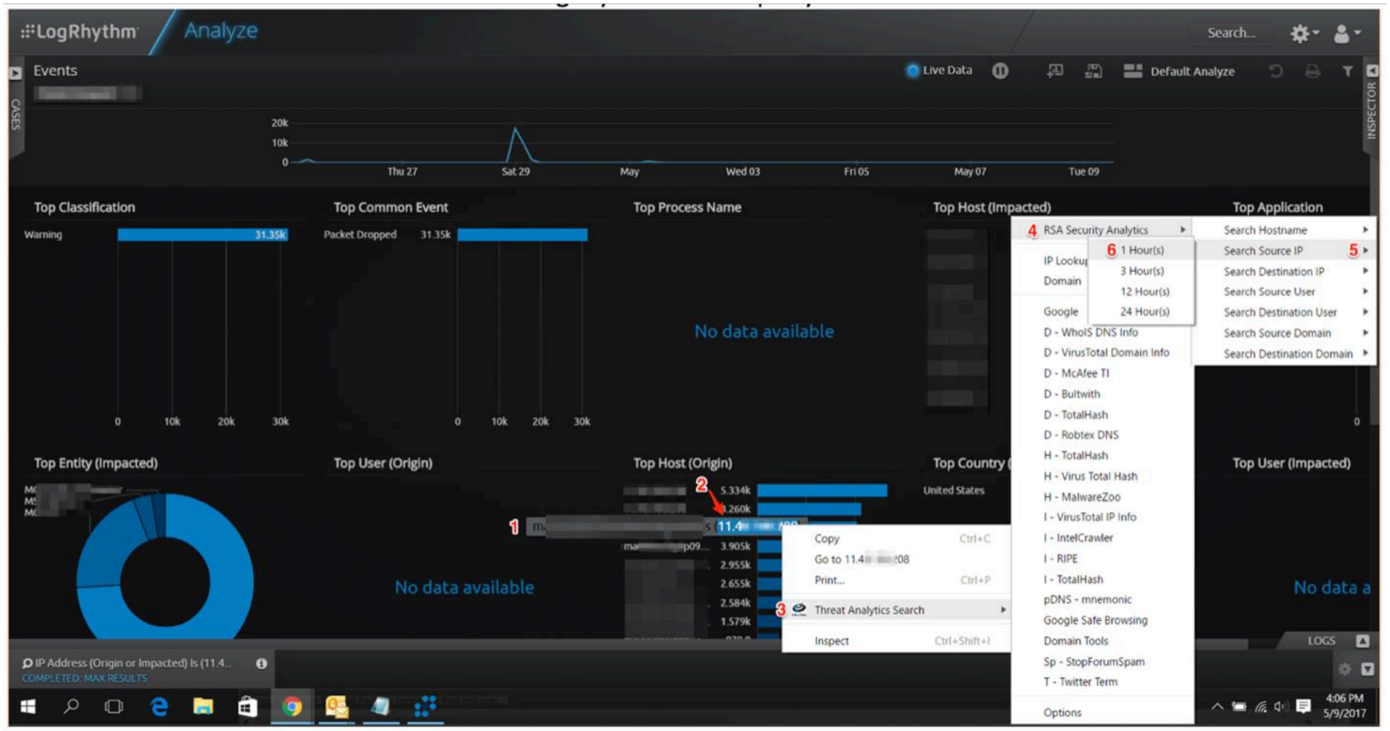
	Display label	Query	Enabled	Delete
✥	Search Hostname	alias.host='TESTSEARCH'	☑	X
✥	Search Source IP	ip.src=TESTSEARCH	☑	X
✥	Search Destination IP	ip.dst=TESTSEARCH	☑	X
✥	Search User Source	user.src='TESTSEARCH'	☑	X

Using the Plugin in LogRythm

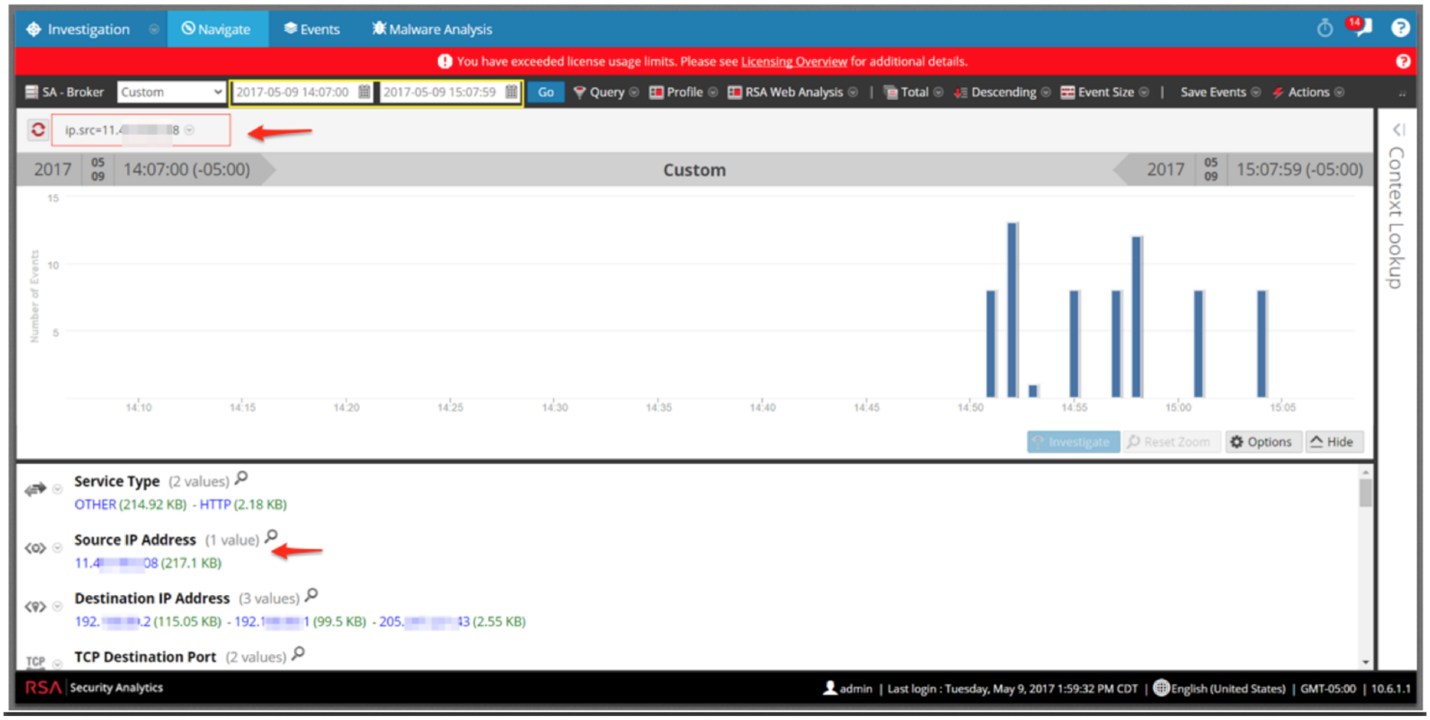
1. From the LogRythm UI identify an IP address that you would like to further investigate and hover your mouse over it.



2. Hover your mouse over the target and the IP address will pop-out. Use your mouse to 'highlight' the IP address and 'Right-Click' it, select 'Threat Analytics' > 'RSA Security Analytics' > Choose the Meta Key Pivot you'd like to search on > then choose the 'Time Range' you'd like to query on.



3. A web query will be automatically sent to RSA Netwitness and an investigation window will automatically open. See below that the IP 11.4x.xxx.x08 was queried by ip.src, for the previous 3 hours. You can now drill into a more comprehensive investigation, export the PCAP, etc…



You have exceeded license usage limits. Please see Licensing Overview for additional details.

2017-05-09 14:07:00 – 2017-05-09 15:07:59

ip.src=11.[redacted]8

2017 05 09 14:07:00 (-05:00) Custom 2017 05 09 15:07:59 (-05:00)

Service Type (2 values)
OTHER (214.92 KB) - HTTP (2.18 KB)

Source IP Address (1 value)
11.4[redacted]08 (217.1 KB)

Destination IP Address (3 values)
192.[redacted].2 (115.05 KB) - 192.1[redacted]1 (99.5 KB) - 205.[redacted]43 (2.55 KB)

TCP Destination Port (2 values)

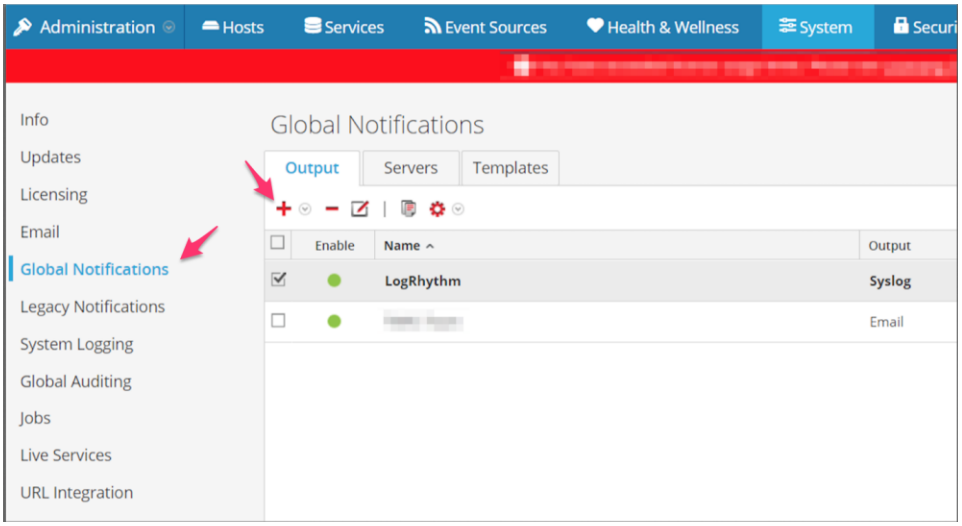
admin | Last login : Tuesday, May 9, 2017 1:59:32 PM CDT | English (United States) | GMT-05:00 | 10.6.1.1

4. Anywhere in LogRythm that you can highlight an IP address, you can right-click and pivot into a RSA Netwitness investigation. You can configure virtually any query in Threat Analytics that you can create in RSA Netwitness. Once the Threat Analytics plugin is configured, you can use it in any web-based tool that you use within your organization.

Send RSA Netwitness Audit Logs and ESA Alerts to LogRythm

This section will walk you through sending Netwitness Audit Logs and ESA Alerts to a centra lized location or log repository. This is helpful for decreasing the number of places you have to look for system alerts.

1. Log into the RSA NetWitness GUI with "Administrative" Credentials
2. Go to: Administration>System>Global Notifications

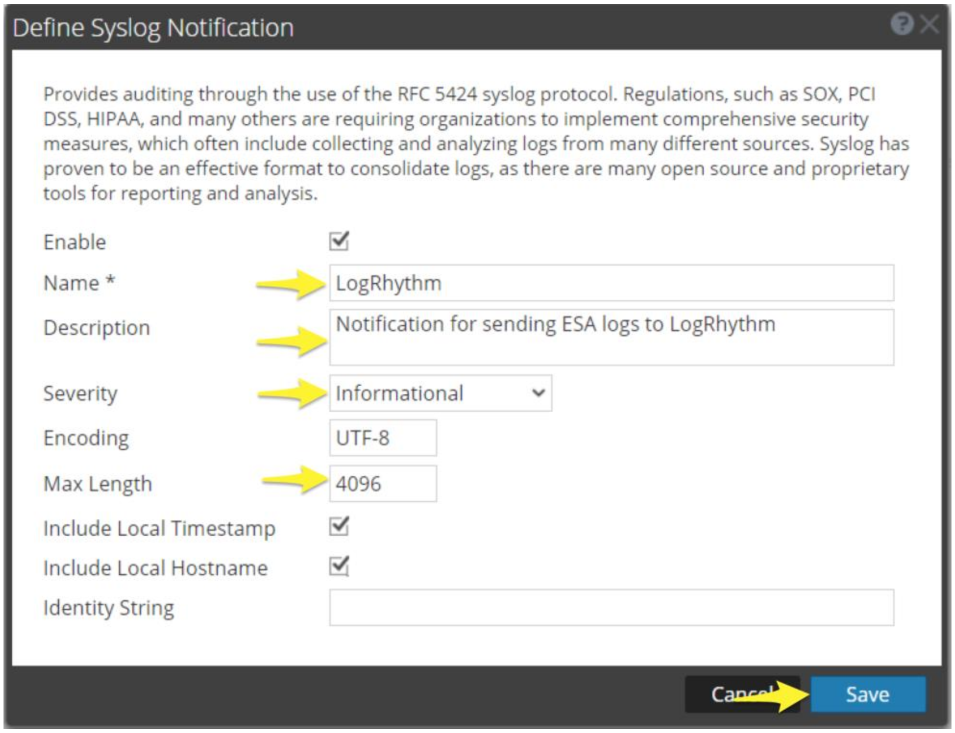


[redacted]

Global Notifications

☐	Enable	Name ^	Output
☑	●	LogRhythm	Syslog
☐	●	[redacted]	Email

3. Click "Output" and then click the "+" Sign and choose "Syslog". Ensure configuration matches image below:

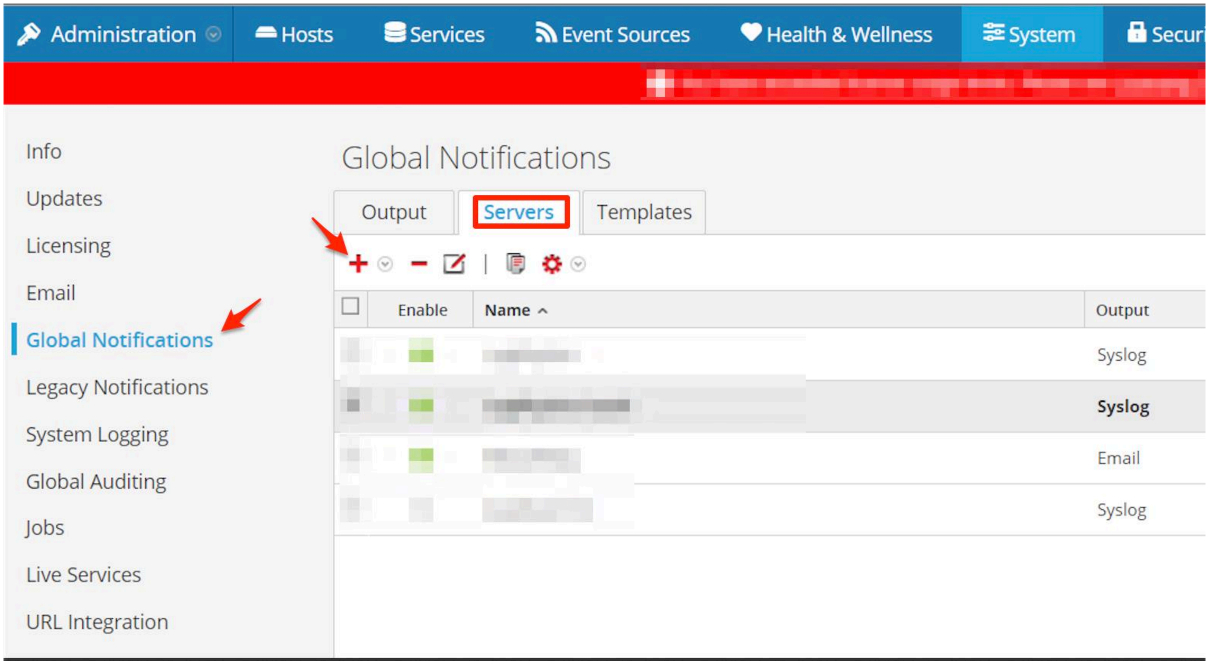


Define Syslog Notification

Provides auditing through the use of the RFC 5424 syslog protocol. Regulations, such as SOX, PCI DSS, HIPAA, and many others are requiring organizations to implement comprehensive security measures, which often include collecting and analyzing logs from many different sources. Syslog has proven to be an effective format to consolidate logs, as there are many open source and proprietary tools for reporting and analysis.

Enable	☑
Name *	LogRhythm
Description	Notification for sending ESA logs to LogRhythm
Severity	Informational
Encoding	UTF-8
Max Length	4096
Include Local Timestamp	☑
Include Local Hostname	☑
Identity String	

4. Click “Servers” tab and then click the “+” Sign and choose “Syslog” from the menu.

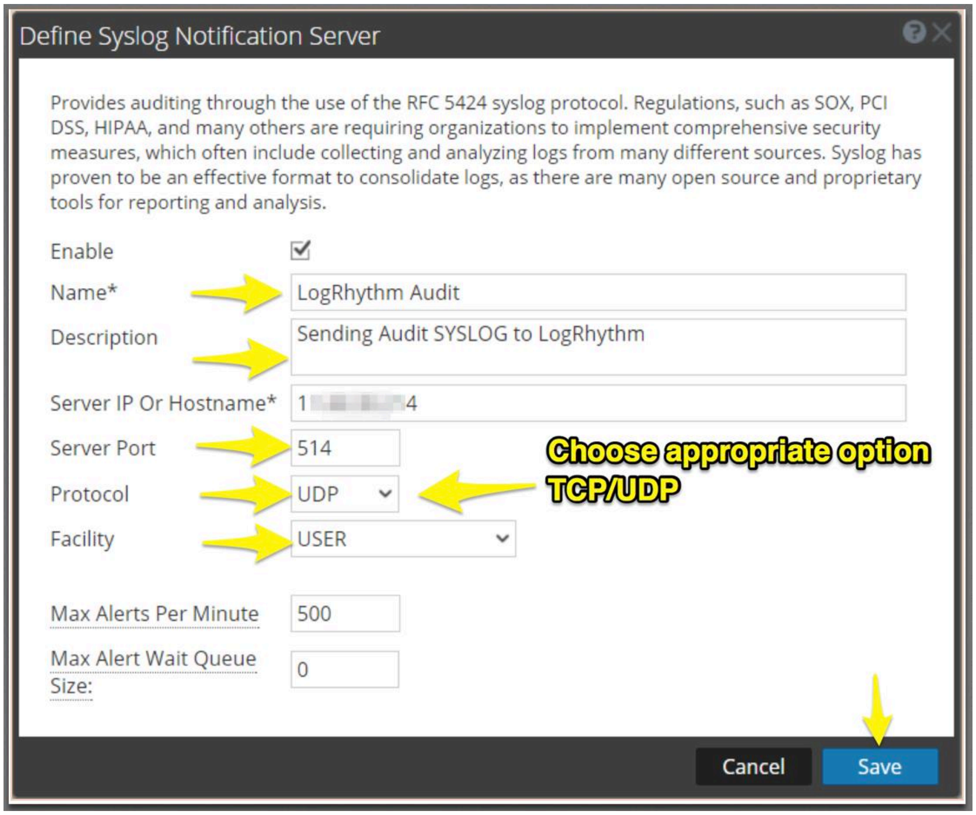


[redacted]

Global Notifications

□	Enable	Name ^	Output
[redacted]	[redacted]	[redacted]	Syslog
[redacted]	[redacted]	[redacted]	Syslog
[redacted]	[redacted]	[redacted]	Email
[redacted]	[redacted]	[redacted]	Syslog

5. Ensure you update the values highlighted below. The Server IP address will be the IP Address of your LogRythm Syslog SmartConnector



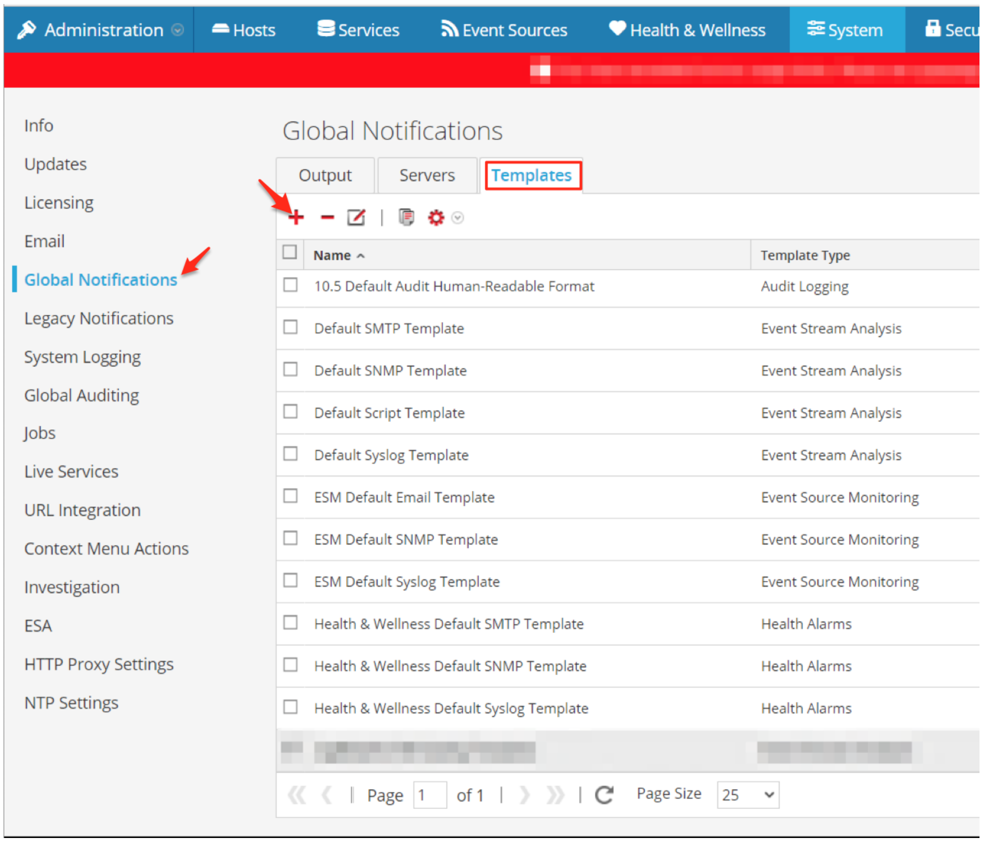
Define Syslog Notification Server

Provides auditing through the use of the RFC 5424 syslog protocol. Regulations, such as SOX, PCI DSS, HIPAA, and many others are requiring organizations to implement comprehensive security measures, which often include collecting and analyzing logs from many different sources. Syslog has proven to be an effective format to consolidate logs, as there are many open source and proprietary tools for reporting and analysis.

Enable	☑
Name*	LogRhythm Audit
Description	Sending Audit SYSLOG to LogRhythm
Server IP Or Hostname*	1[redacted]4
Server Port	514
Protocol	UDP
Facility	USER
Max Alerts Per Minute	500
Max Alert Wait Queue Size:	0

Choose appropriate option TCP/UDP

6. Click the “Templates” Tab, then click “+”

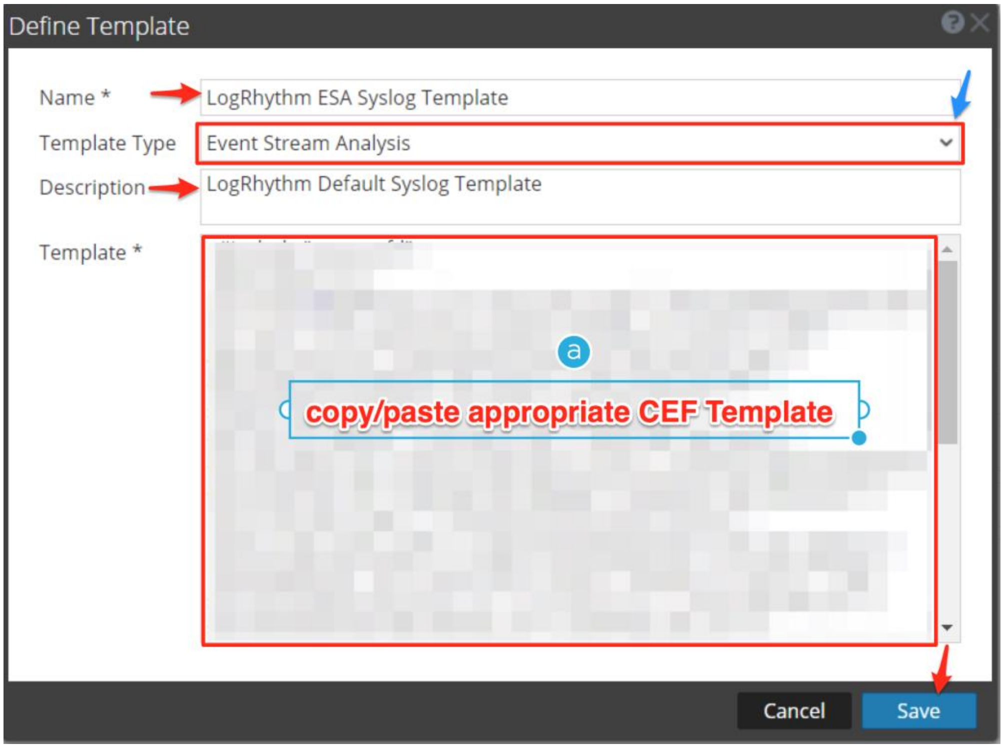


[redacted]

Global Notifications

☐	Name ^	Template Type
☐	10.5 Default Audit Human-Readable Format	Audit Logging
☐	Default SMTP Template	Event Stream Analysis
☐	Default SNMP Template	Event Stream Analysis
☐	Default Script Template	Event Stream Analysis
☐	Default Syslog Template	Event Stream Analysis
☐	ESM Default Email Template	Event Source Monitoring
☐	ESM Default SNMP Template	Event Source Monitoring
☐	ESM Default Syslog Template	Event Source Monitoring
☐	Health & Wellness Default SMTP Template	Health Alarms
☐	Health & Wellness Default SNMP Template	Health Alarms
☐	Health & Wellness Default Syslog Template	Health Alarms
[redacted]	[redacted]	[redacted]

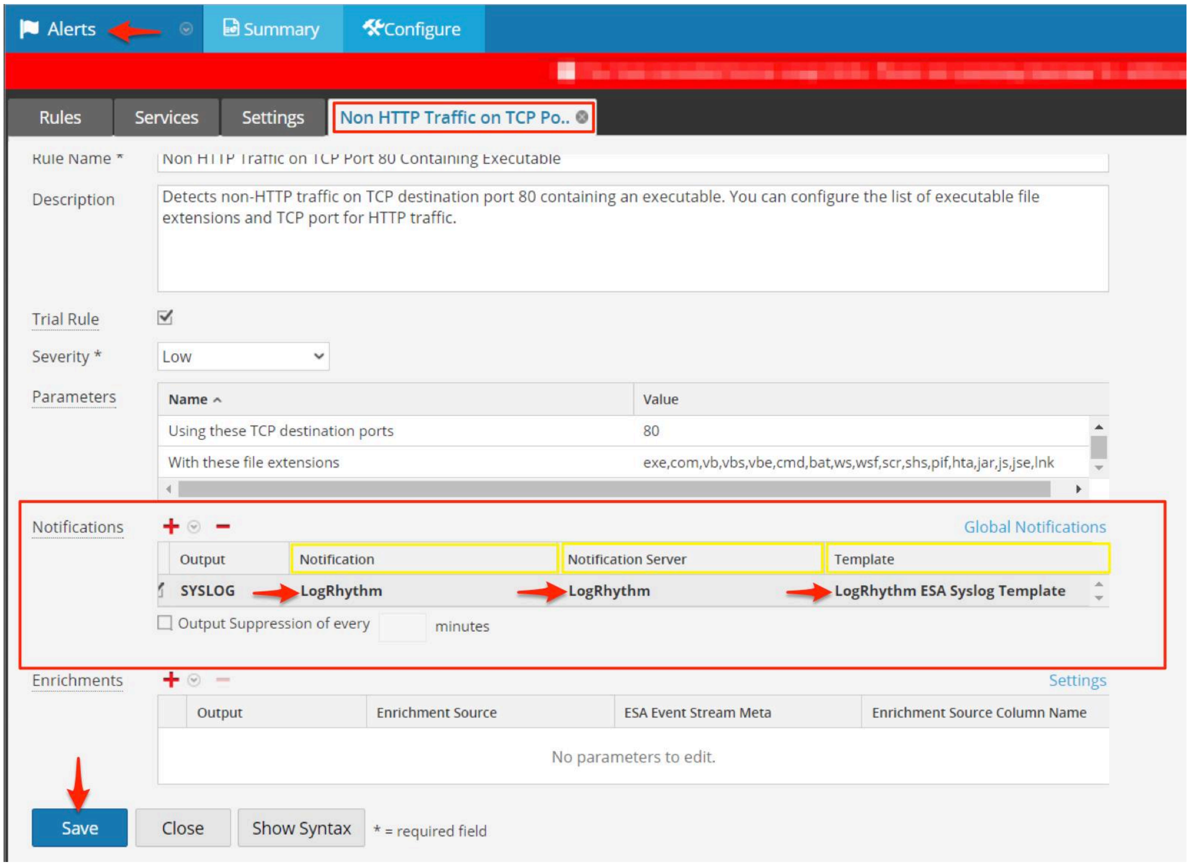
7. Fill out the “Define Template” field as illustrated below and click “Save”.


Define Template

Name *	LogRhythm ESA Syslog Template
Template Type	Event Stream Analysis
Description	LogRhythm Default Syslog Template
Template *	[redacted]

copy/paste appropriate CEF Template

8. Configure your ESA Alert to use the new template by adjusting the following highlighted notifications settings:



[redacted]

Rule Name * Non HTTP Traffic on TCP Port 80 Containing Executable

Description: Detects non-HTTP traffic on TCP destination port 80 containing an executable. You can configure the list of executable file extensions and TCP port for HTTP traffic.

Trial Rule ☑

Severity * Low

Parameters

Name	Value
Using these TCP destination ports	80
With these file extensions	exe,com,vb,vbs,vbe,cmd,bat,ws,wsf,scr,shs,pif,hta,jar,js,jse,lnk

Notifications — Global Notifications

Output	Notification	Notification Server	Template
SYSLOG	LogRhythm	LogRhythm	LogRhythm ESA Syslog Template

□ Output Suppression of every minutes

Enrichments — Settings

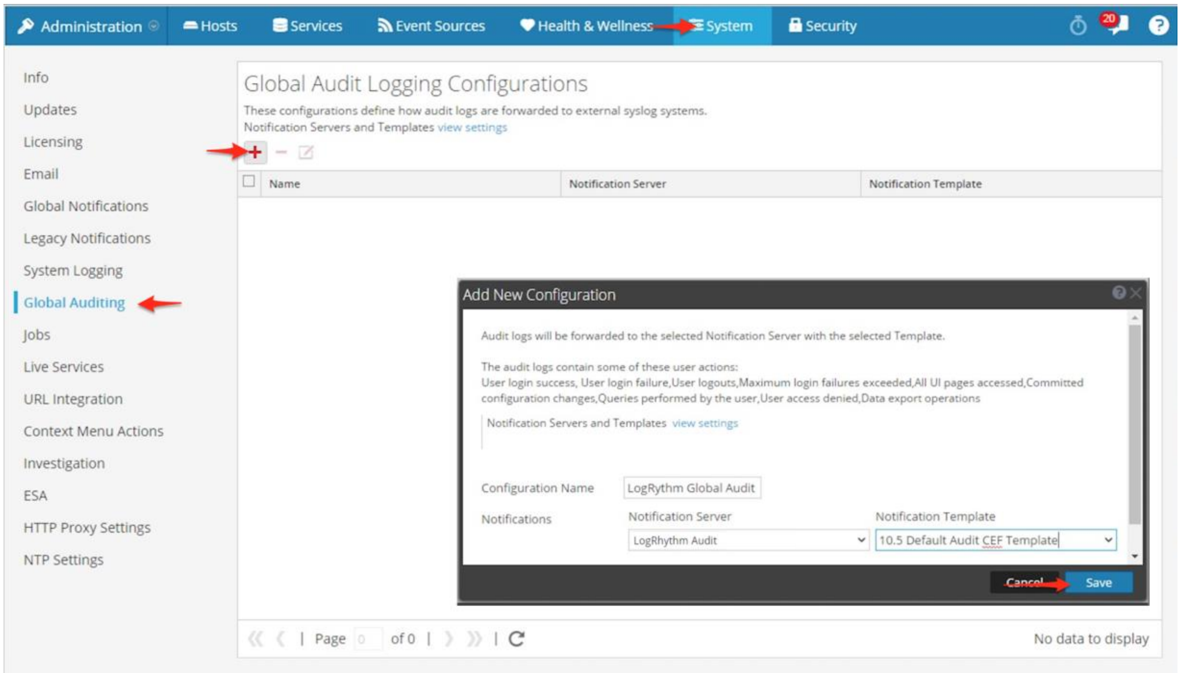
Output	Enrichment Source	ESA Event Stream Meta	Enrichment Source Column Name

No parameters to edit.

* = required field

9. Remember to re-deploy the rule to push the new notification templates.

10. Update the configuration to add and to send Global Audit Logs . Choose the Notification Sever you created in Step 4 and click ‘Save’.



Global Audit Logging Configurations

These configurations define how audit logs are forwarded to external syslog systems.
Notification Servers and Templates view settings

Name	Notification Server	Notification Template

Add New Configuration

Audit logs will be forwarded to the selected Notification Server with the selected Template.

The audit logs contain some of these user actions:
User login success, User login failure,User logouts,Maximum login failures exceeded,All UI pages accessed,Committed configuration changes,Queries performed by the user,User access denied,Data export operations

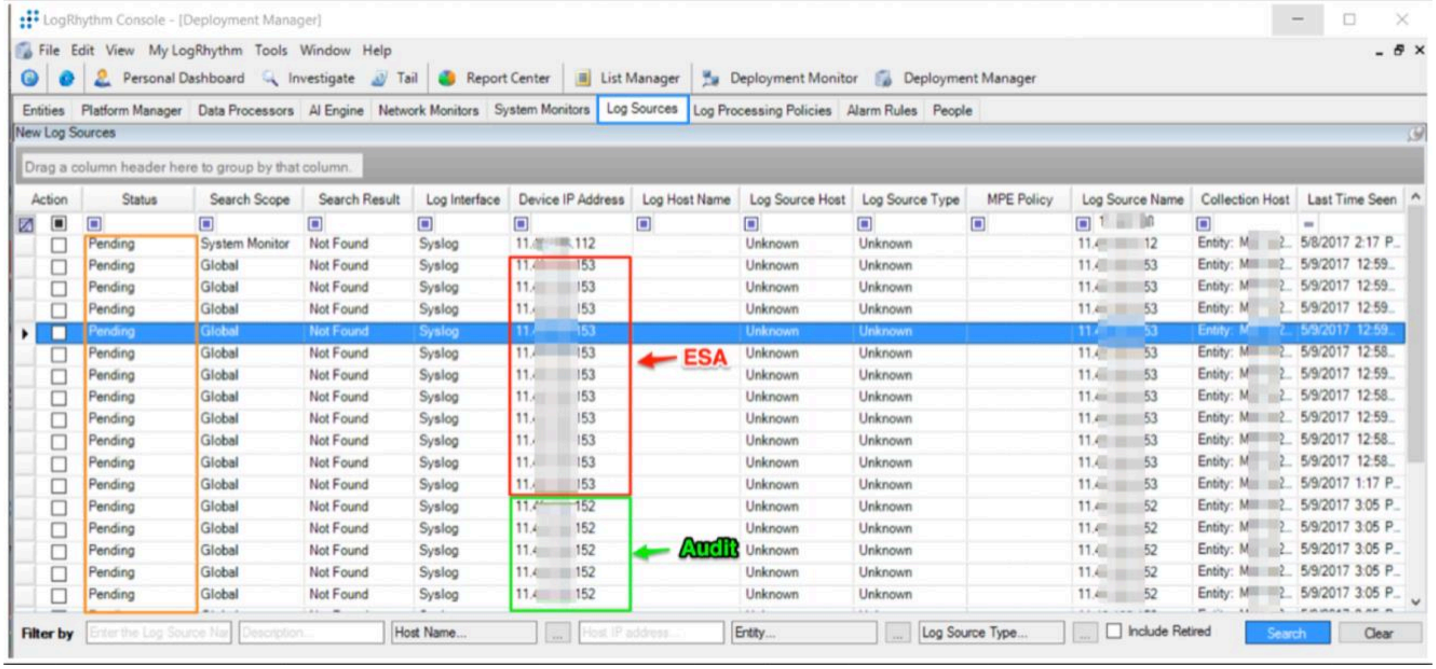
Notification Servers and Templates view settings

Configuration Name: LogRythm Global Audit

Notifications — Notification Server: LogRhythm Audit — Notification Template: 10.5 Default Audit CEF Template

No data to display

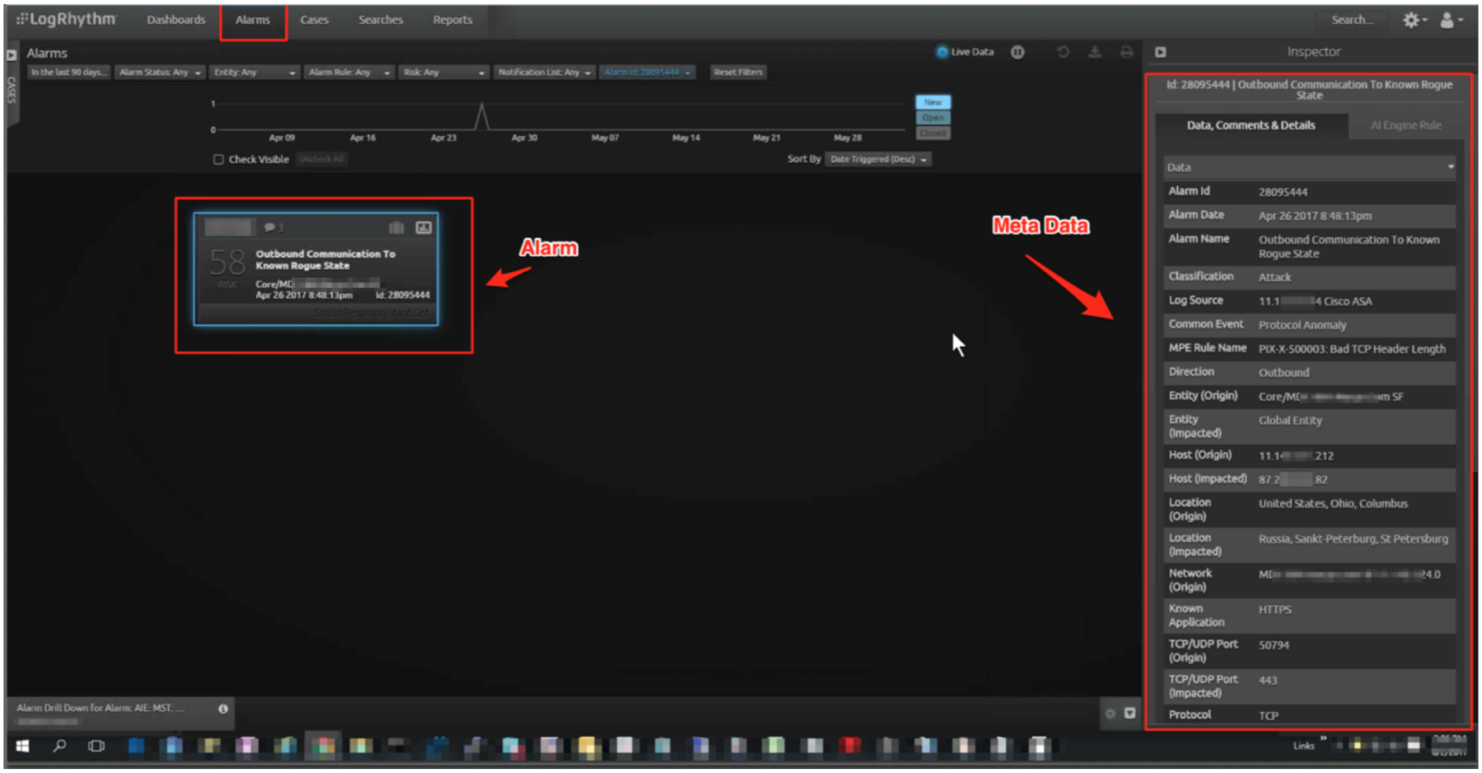
11. Once you have Audit Logs and ESA Alerts being sent to LogRythm you will need to onboard 'Netwitness' as a log source in LogRythm. In this case the .153 is from the ESA and the .152 is from the SA Server.



Action	Status	Search Scope	Search Result	Log Interface	Device IP Address	Log Host Name	Log Source Host	Log Source Type	MPE Policy	Log Source Name	Collection Host	Last Time Seen
☐	Pending	System Monitor	Not Found	Syslog	11.[redacted]112		Unknown	Unknown		11.[redacted]12	Entity: M[redacted]2...	5/8/2017 2:17 P...
☐	Pending	Global	Not Found	Syslog	11.[redacted]153		Unknown	Unknown		11.[redacted]53	Entity: M[redacted]2...	5/9/2017 12:59...
☐	Pending	Global	Not Found	Syslog	11.[redacted]153		Unknown	Unknown		11.[redacted]53	Entity: M[redacted]2...	5/9/2017 12:59...
☐	Pending	Global	Not Found	Syslog	11.[redacted]153		Unknown	Unknown		11.[redacted]53	Entity: M[redacted]2...	5/9/2017 12:59...
☐	Pending	Global	Not Found	Syslog	11.[redacted]153		Unknown	Unknown		11.[redacted]53	Entity: M[redacted]2...	5/9/2017 12:59...
☐	Pending	Global	Not Found	Syslog	11.[redacted]153		Unknown	Unknown		11.[redacted]53	Entity: M[redacted]2...	5/9/2017 12:58...
☐	Pending	Global	Not Found	Syslog	11.[redacted]153		Unknown	Unknown		11.[redacted]53	Entity: M[redacted]2...	5/9/2017 12:59...
☐	Pending	Global	Not Found	Syslog	11.[redacted]153		Unknown	Unknown		11.[redacted]53	Entity: M[redacted]2...	5/9/2017 12:58...
☐	Pending	Global	Not Found	Syslog	11.[redacted]153		Unknown	Unknown		11.[redacted]53	Entity: M[redacted]2...	5/9/2017 12:59...
☐	Pending	Global	Not Found	Syslog	11.[redacted]153		Unknown	Unknown		11.[redacted]53	Entity: M[redacted]2...	5/9/2017 12:58...
☐	Pending	Global	Not Found	Syslog	11.[redacted]153		Unknown	Unknown		11.[redacted]53	Entity: M[redacted]2...	5/9/2017 12:58...
☐	Pending	Global	Not Found	Syslog	11.[redacted]153		Unknown	Unknown		11.[redacted]53	Entity: M[redacted]2...	5/9/2017 1:17 P...
☐	Pending	Global	Not Found	Syslog	11.[redacted]152		Unknown	Unknown		11.[redacted]52	Entity: M[redacted]2...	5/9/2017 3:05 P...
☐	Pending	Global	Not Found	Syslog	11.[redacted]152		Unknown	Unknown		11.[redacted]52	Entity: M[redacted]2...	5/9/2017 3:05 P...
☐	Pending	Global	Not Found	Syslog	11.[redacted]152		Unknown	Unknown		11.[redacted]52	Entity: M[redacted]2...	5/9/2017 3:05 P...
☐	Pending	Global	Not Found	Syslog	11.[redacted]152		Unknown	Unknown		11.[redacted]52	Entity: M[redacted]2...	5/9/2017 3:05 P...
☐	Pending	Global	Not Found	Syslog	11.[redacted]152		Unknown	Unknown		11.[redacted]52	Entity: M[redacted]2...	5/9/2017 3:05 P...

LogRythm Advanced Integration

LogRythm generates 'Alarms' which contains Meta Data that that can be used to query against in RSA Netwitness. Below is an example the the Meta Data that is generated and populates a LogRythm Alarm.

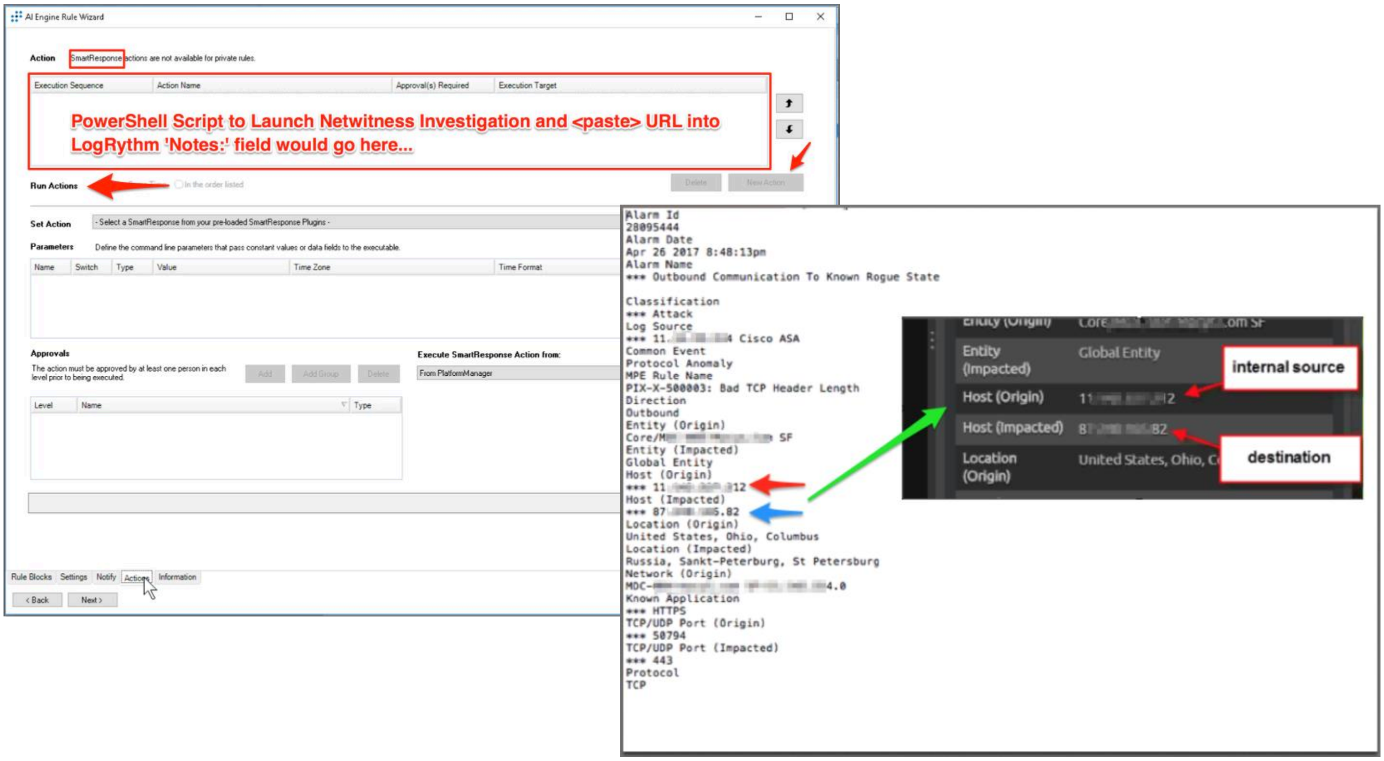


58 RISK
Outbound Communication To Known Rogue State
Core/MD[redacted]
Apr 26 2017 8:48:13pm Id: 28095444

Id: 28095444 | Outbound Communication To Known Rogue State

Alarm Id	28095444
Alarm Date	Apr 26 2017 8:48:13pm
Alarm Name	Outbound Communication To Known Rogue State
Classification	Attack
Log Source	11.1[redacted]4 Cisco ASA
Common Event	Protocol Anomaly
MPE Rule Name	PIX-X-500003: Bad TCP Header Length
Direction	Outbound
Entity (Origin)	Core/MD[redacted]m SF
Entity (Impacted)	Global Entity
Host (Origin)	11.1[redacted].212
Host (Impacted)	87.2[redacted].82
Location (Origin)	United States, Ohio, Columbus
Location (Impacted)	Russia, Sankt-Peterburg, St Petersburg
Network (Origin)	MD[redacted]24.0
Known Application	HTTPS
TCP/UDP Port (Origin)	50794
TCP/UDP Port (Impacted)	443
Protocol	TCP

LogRythm has a 'Smart Response' plugin that can run PowerShell scripts & commands and automate tasks within LogRythm. A script can be written to run a web query in RSA Netwitness searching specific Meta Keys and a write/paste the RSA Netwitness investigatuion URL into the LogRythm 'Comments' field.



SmartResponse actions are not available for private rules.

PowerShell Script to Launch Netwitness Investigation and <paste> URL into LogRythm 'Notes:' field would go here...

- Select a SmartResponse from your pre-loaded SmartResponse Plugins -

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

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

From PlatformManager

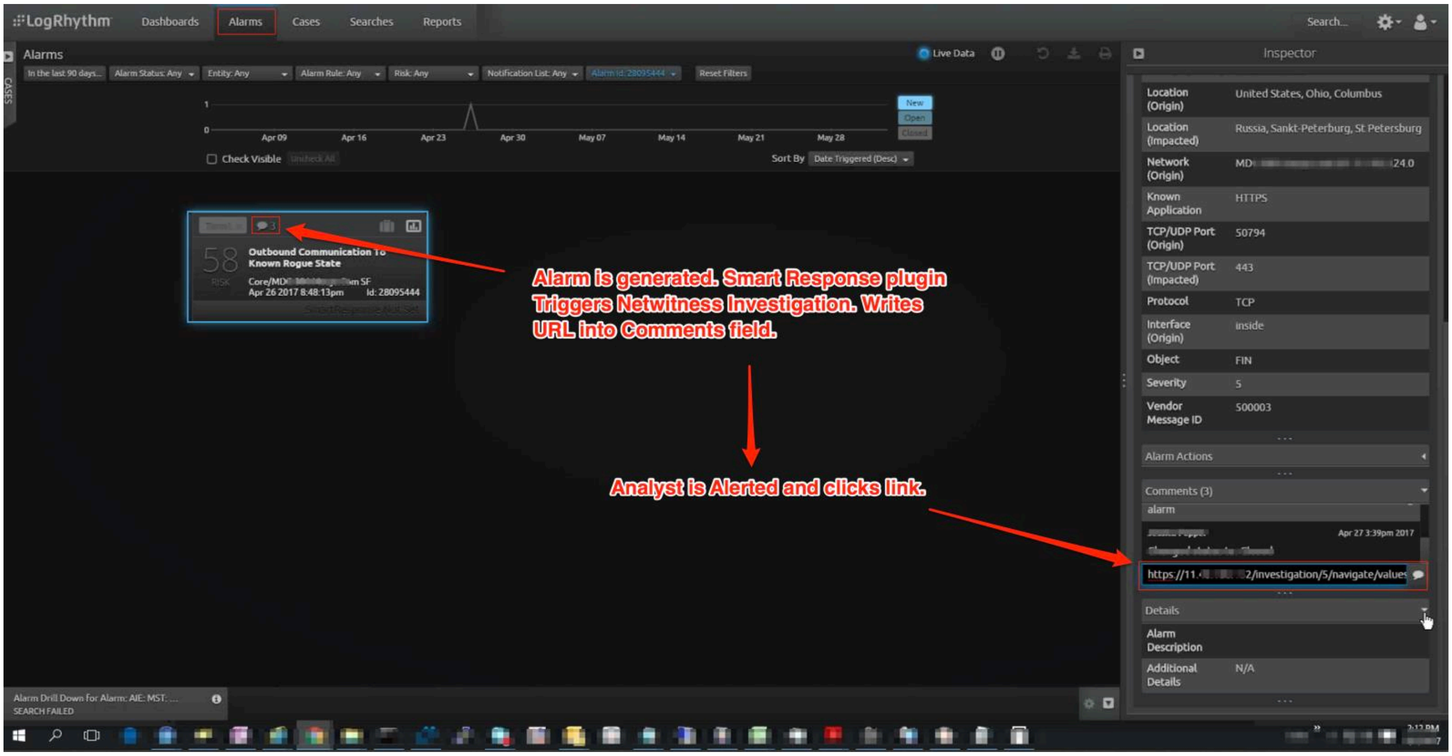
```
Alarm Id
28095444
Alarm Date
Apr 26 2017 8:48:13pm
Alarm Name
*** Outbound Communication To Known Rogue State

Classification
*** Attack
Log Source
*** 11.[redacted]4 Cisco ASA
Common Event
Protocol Anomaly
MPE Rule Name
PIX-X-500003: Bad TCP Header Length
Direction
Outbound
Entity (Origin)
Core/M[redacted] SF
Entity (Impacted)
Global Entity
Host (Origin)
*** 11[redacted]12
Host (Impacted)
*** 87[redacted]5.82
Location (Origin)
United States, Ohio, Columbus
Location (Impacted)
Russia, Sankt-Peterburg, St Petersburg
Network (Origin)
MDC-[redacted]4.0
Known Application
*** HTTPS
TCP/UDP Port (Origin)
*** 50794
TCP/UDP Port (Impacted)
*** 443
Protocol
TCP
```

Entity (Origin)	Core[redacted]om SF
Entity (Impacted)	Global Entity
Host (Origin)	11[redacted]2
Host (Impacted)	8[redacted]82
Location (Origin)	United States, Ohio, C

Use Case – Pivoting into Newitness via 'Smart Response Plugin'

The use case would be as follows; An Alarm is generated in LogRythm, the Smart Response plugin runs PowerShell script, the RSA Netwitness investigation is initiated, and the investigation URL is written into the 'Comments' of the Alarm.



58 RISK
Outbound Communication To Known Rogue State
Core/MD[redacted]m SF
Apr 26 2017 8:48:13pm Id: 28095444

Alarm is generated. Smart Response plugin Triggers Netwitness Investigation. Writes URL into Comments field.

Analyst is Alerted and clicks link.

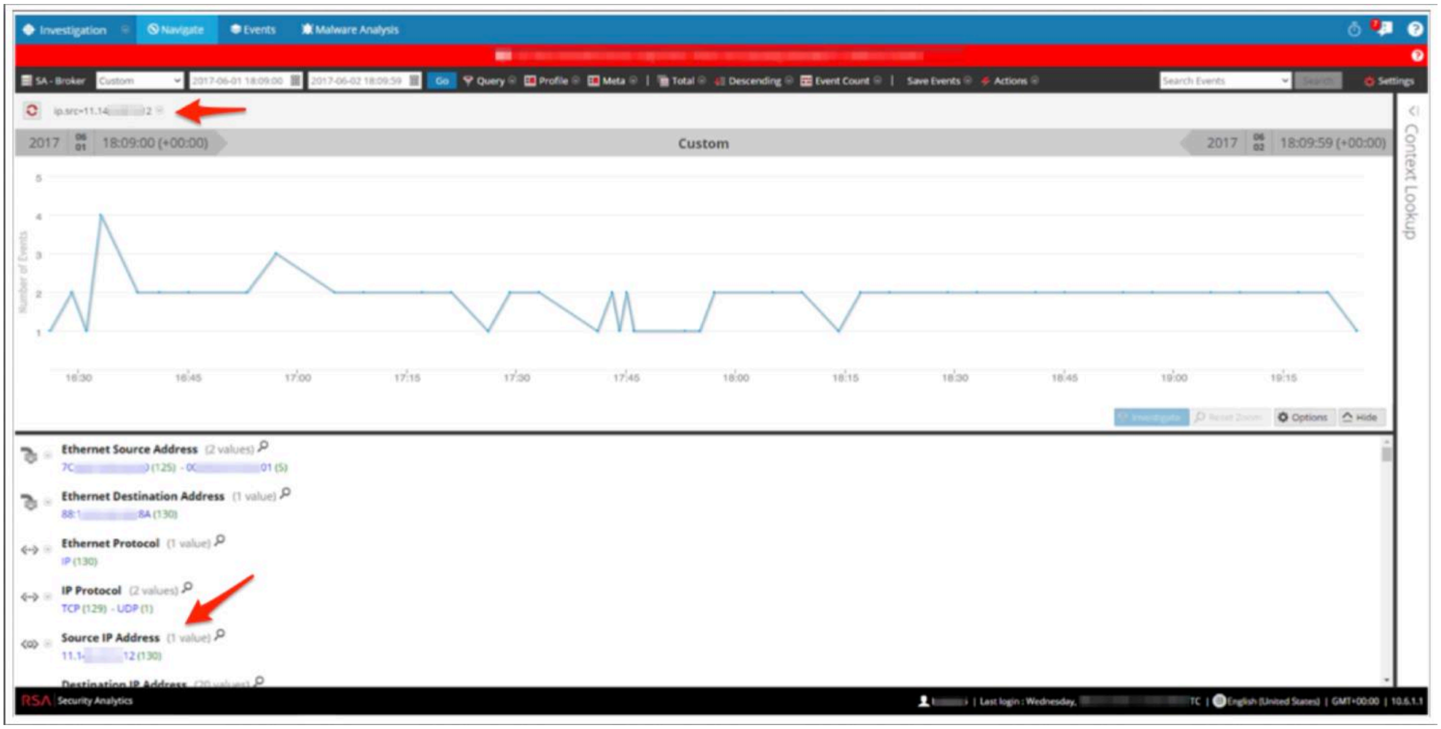
Location (Origin)	United States, Ohio, Columbus
Location (Impacted)	Russia, Sankt-Peterburg, St Petersburg
Network (Origin)	MD[redacted]24.0
Known Application	HTTPS
TCP/UDP Port (Origin)	50794
TCP/UDP Port (Impacted)	443
Protocol	TCP
Interface (Origin)	inside
Object	FIN
Severity	5
Vendor Message ID	500003

Comments (3)
alarm
[redacted] Apr 27 3:39pm 2017
[redacted]
https://11.[redacted]2/investigation/5/navigate/values

Alarm Description	
Additional Details	N/A

Alarm Drill Down for Alarm: AIE: MST: ...
SEARCH FAILED

The analyst is notified of the Alarm and can click on the URL in the Comments of the Alarm to pivot into the RSA Netwitness Investigation.



ip.src=11.14[redacted]2

Ethernet Source Address (2 values)
7C[redacted] (125) - 0C[redacted]01 (5)

Ethernet Destination Address (1 value)
88:1[redacted]8A (130)

Ethernet Protocol (1 value)
IP (130)

IP Protocol (2 values)
TCP (129) - UDP (1)

Source IP Address (1 value)
11.1[redacted]12 (130)

Destination IP Address (20 values)

[redacted] | Last login : Wednesday, [redacted] TC | English (United States) | GMT+00:00 | 10.6.1.1

References

Sample - ESA Syslog Alert Template

Do not copy and paste this directly, the formatting will be not properly convey from Word. Instead, copy and paste into Notepad++ then paste into RSA Netwitness, or import as outlined in the installation steps.

```
------------------------------------------------------------------------------------------------------------------------------------------

<#include "macros.ftl">

<#list events as x>

CEF:0|RSA|NetWitness|10.6.2|${x.event_type!""}|${moduleName}|${x.severity!""}|act="<#if
x.action?has_content><@value_of x.action /></#if>"  app=${x.protocol!""} destinationDnsDomain=${x.domain_dst!""}
destinationServiceName="${x.client!""}" dmac=${x.eth_dst!""} sntdom=${x.ad_domain_src!""} dproc="${x.process!""}"
dpt=${x.tcp_dstport!""} dst=${x.ip_dst!""} duid='${x.user_dst!""}' dvc=${x.device_ip!""} dvchost=${x.device_host!""}
endTime=${time?datetime} externalId=${x.rid!""} fileType=${x.filetype!""} fileName="${x.filename!""}"
msg="${x.event_desc!""}" transportProtocol=${x.service!""} reason="${x.result_code!""}"
requestClientApplication="${x.user_agent!""}" requestMethod="<#if x.action?has_content><@value_of x.action
/></#if>"  sourceHostName=${x.host_src!""} src=${x.ip_src!""} smac=${x.eth_src!""}
sourceDnsDomain=${x.domain_src!""} suid='${x.user_src!""}' type=${x.medium!""}
deviceCustomDate1=${x.event_time!""} deviceCustomDate1Label="Event Time"
cs2=${time?datetime?iso_m_nz("GMT+01")}  cs2Label="Custom Time String plus 1 Hour"
cs1=${time?datetime?iso_m_nz("GMT-01")}  cs1Label="Custom Time String minus 1 Hour" cat="${x.event_cat_name!""}"
spriv="${x.group!""}"  cs3="${x.alert_id!""}" cs3Label="Alert ID" cs4="${x.msg_id!""}"  cs4Label="Message ID"
cs5="${x.risk_info!""}-${x.risk_suspicious!""}-${x.risk_warning!""}"  cs5Label="Risk Categories" cs6="${x.category!""}"
cs6Label="NW Category" suser='${x.ad_username_src!""}' deviceExternalId=${x.did!""} dhost=<#if
x.alias_host?has_content><@value_of x.alias_host/></#if> spt=${x.tcp_srcport!""} duser='${x.ad_username_dst!""}'
fileSize=${x.size!""} fileHash=${x.checksum!""} outcome="${x.ec_outcome!""}"  cn1=${x.sessionid!""}
cn1Label="SessionID" </#list>

------------------------------------------------------------------------------------------------------------------------------------------
```

Additional Comments

As of June 6th 2017, the date this integreation guide was created, Right-Click context from Netwitness – LogRythm is not possible due to the process in which LogRythm creates queries in its UI. The LogRythm UI uses a query builder which then re-writes the query on the LogRythm Server in Lucene syntax and queries its database.

Also as of June 6th 2017 the date this integration guide was created it was not possible to natively Right-Click (pivot) from LogRythm to Netwitness. Much of the right-click ability/functionality within LogRythm is disabled which is why we chose to utilize the Google Chrome 'Threat Analytics' plugin.

Contact Customer Care

RSA SecureCare Online:	https://knowledge.rsasecurity.com/ or https://community.rsa.com/community/rsa-customer-support
Phone:	1-800-995-5095, option 3
International Contacts:	http://www.emc.com/support/rsa/contact/phone-numbers.htm
Email:	support@rsa.com
Community:	https://community.rsa.com/community/products/netwitness
Basic Support:	Technical Support for your technical issues is available during 8am to 5pm your local time, Monday through Friday.
Enhanced Support:	Technical Support is available by phone 24 x 7 x 365 days of the year for Severity 1 and Severity 2 issues only.

Preparing to Contact Customer Care

When you contact Customer Care, you should be at your computer. Be prepared to give the following information:

1. The version number of the RSA NetWitness product or application you are using.
2. The type of hardware you are using.