# RSA NetWitness Platform

Event Source Log Configuration Guide



## **ThreatQuotient Threat Intelligence Platform**

Last Modified: Thursday, February 13, 2020

**Event Source Product Information:** 

Vendor: ThreatQuotient Event Source: Threat Intelligence Platform Versions: 4.0

**RSA Product Information:** 

Supported On: NetWitness Platform 10.0 and later Feed Format: csv Collection Method: HTTP Feed Collection Frequency: Hourly, Daily, or Weekly

### About ThreatQuotient

ThreatQuotient delivers an open and extensible threat intelligence platform (TIP) with Threat Management and Operation characteristics. It provides defenders the context, customization, prioritization and collaboration needed for increased security effectiveness and efficient threat operations and management.

ThreatQ accelerates the transformation of threat data into actionable threat intelligence by giving defenders control through a self-tuning threat library, an adaptive workbench and an open exchange API to ensure that intelligence is accurate, relevant and timely to the business. With ThreatQ, customers can dramatically reduce the time to define and detect, increase productivity, and make the most of the existing defense infrastructure



ThreatQ Architecture Diagram

### ThreatQ Configuration

This section provides instructions for configuring the ThreatQuotient Threat Intelligence Platform with RSA NetWitness.

#### **Before You Start**

This document is not intended to suggest optimum installations or configurations. It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components. All ThreatQuotient Threat Intelligence Platform components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Intelligence Feed	File Function
Feed Contents	IP Address or Domain Name, ThreatQuotient Link, ThreatQuotient ID, Score, ThreatQuotient Status, and Detected Time.

#### **Configure ThreatQuotient**

The ThreatQuotient Threat Intelligence Platform allows threat data to be exported in a variety of different ways. This is accomplished by using the **Exports** feature.

To configure the feed for NetWitness Platform, perform these steps:

1. Log into the ThreatQ Platform and navigate to the Exports page as below:

THREATQ 🔰 🚯 Threat Library 🗛 Investigations 🕍 Analytics	1	+ Create Q 🌲 💠
Overview O Add Dishboard		User Management Incoming Feeds
Overview	to Watchlist Activity You currently don't have any items on your watchlist.	Data Management Exports Operations Management Report Options System Configurations Notification Settings Job Management About
Leading	⊘ Tasks	My Open Tasks (0) All Open Tasks (0)
	D - NAME 5 ASSIGNED TO 8 DUE DATE 8	status ÷

2. From the Exports page, click the green Add New Export button.

THREATQ 🍞	i Threat Library	A Investigations	네 Analytics	+ Create	Q 🌢	•
Ехро	orts		Need help? Click here for Exports docun	nentation.	dd New Export	Û
٥	FF/ON NAME •	URL	CONNECTION	OUTPUT FORMAT	ACTIO	25 •

After you click the button, a wizard is launched that takes you through the steps to configure the NetWitness Export.

3. Define Export Name and Token.

Select a name and token. The name should be short and descriptive, for example, "RSA NetWitness IP Feed." The token is used to authorize a connection to view the data in this feed. This is randomly generated, and should not be changed.

- a. Enter a name. The name should be short and descriptive, for example, "RSA NetWitness IP Feed."
- b. The token is used to authorize a connection to view the data in this feed. This is randomly generated, and should not be changed.

THR	EATQ 🕻	] Indicators	Events	Adversaries	Files	Signatures		Create ~	Q	<b>0</b> ~	۰.
Expo	orts						Need help? Click here for Exports do	cumentation. Ad	d New E	export	
Showing	1 to 25 of 47	,	CONN Export Nar	NECTION ne:	I SET	TINGS	×		Row	count: 2	25 🗘
	Off / On	Name	RSA Ne	tWitness IP Fe	ed			out Format			
		Search	Token:								
0		ArcSight	LqIN5fcs	y2WmSMBGdwl	9				du	plicate	
101		ArcSight Email /	Next Ste	or Cancel					du	plicate	
0	0	ArcSight Email	IGHINGHIS	ahvev	houwaroong	manaciman	connection certifys	_	du	plicate	
(D.)	0	ArcSight Email Sut	oject	api/ex	port/arcsig	phtsubject	connection settings		du	plicate	
(0)	0	ArcSight FQDN		api/ex	port/arcsig	ghtfqdn	connection settings		du	plicate	
/Ø/	0	ArcSight IP Addres	s	api/ex	port/arcsig	ghtip	connection settings		du	plicate	
10	0	ArcSight MD5		api/ex	port/arcsic	htmd5	connection settings		du	plicate	

- 4. Click Next Step to proceed.
- 5. Configure Output Format.

The Output Format page allows you to describe the feed in detail. Here, we set the type of information to "Indicators", the Output Type to "text/csv", the special parameters and output format shown below.

'hreat Library	스 Investigations 네 Analytics		
Exports		Output Format	orts docum
OFF / ON	NAME *	Type of information you would like to export? Indicators Output type Custom	• •
	Start typing  ArcSight	text/csv	tings
	ArcSight Email Address	<ul> <li>Special Parameters (optional)</li> <li>indicator.status=Active&amp;indicator.deleted=N&amp;indicator.type=IP</li> <li>Address&amp;indicator.class=network</li> </ul>	tings
	ArcSight Email Subject		tings
	ArcSight FQDN ArcSight IP Address	Provide URL Parameters to further refine information being exported: See examples.	tings
	ArcSight MD5 ArcSight String	#indicator, id, link, score, status, last_detected_at, sources {foreach_\$data as \$indicator} {\$indicator.value}, {\$indicator.idh.https://{\$http.hostVindicators/{\$indicator.id}/details_	tings
	ArcSight URL ArcSight URL Path	{\$indicator.score},{\$indicator.status},{\$indicator.last_detected_at},{foreach \$indicator.Sources as \$source name= <u>'sourceloop</u> }{\$source.value}{if i\$smarty.foreach.sourceloop.last}/(/if){foreach}	tings
	ArcSight User-Agent	Vioreduly	tings
	C2 IP Addresses	Save Settings Cancel	tings

6. Click Save Settings.

The new export is saved, and you can then find this export by using the search bar on the Exports page.

7. Enable and Get Connection Information.

After the Export has been saved, you need to go get its URL and enable the feed. To do that, just search for it on the Exports page.

THREAT	? 🍠	👬 Threat Library	A Investigations	님 Analytics				l	+ Create	۹	•	۵
Exports					Need help?	Click here for Exports docum	entation. Add New	Export				
								25 •				
OFF / ON	Q Secur				URL	CONNECTION	OUTPUT FORMAT	ACTIONS				
	RSA NetWitness	IP Feed			apl/export/c0115bc194cd9d8fef d7cfddd22a73cc	connection settings	output format	duplicate				
Previous								Next				

8. To enable the feed, click the Off/On toggle. Record the URL, as it is needed during the RSA NetWitness configuration.

**Note:** If you click on the URL, the system downloads the feed into a CSV, however, it will only take the top 10 indicators. To get the full list of indicators, right click the URL, and select "Copy Link Address".

The configuration of the ThreatQuotient IP Feed is now complete. You can repeat the steps above for any type of indicator (for example FQDNs).

### **RSA NetWitness Custom Feed Configuration**

Depending on your deployment and if you have elected to add an RSA NetWitness Log Decoder and/or Packet Decoder follow the steps below for your integration.

For reference, this procedure is available in the RSA NetWitness Online Documentation here: Create a Custom Feed.

#### To create a custom feed:

1. From the main NetWitness menu, go to Configure > CUSTOM FEEDS.

The Custom Feeds view is displayed.

2. In the toolbar, click **†**.

The Setup Feed dialog is displayed.

3. To select the feed type, click Custom Feed and Next.

The Configure a Custom Feed wizard is displayed, with the Define Feed form open.

4. Select **Adhoc** if you are uploading the file once or **Recurring** if you plan to automate the feed. Enter the URL of the Feed provider and select how often to pull the feed by setting the **Recur Every** option and select **Next**.

Configure a Custo	om Feed			>
Define Feed		Select Services	Define Columns	Review
Feed Task Type Name *	O Adhoc	Recurring		
URL *	https://www	threatq.com/api/exp	ort/aad4bea18bce57da407b9ce	1bdc6a19a/ Verify
Recur Every	Authentic Use proxy	ay (s)		
- O Date Range				
— 💮 Advanced Oj	ptions			
Reset			Cance	Prev Next

5. Select the services on which to deploy the feed, by selecting one or more groups from the **Groups** tab.

Co	nfigure	a Custom Feed		×
	Defi	ne Feed Select Sel	rvices Define Column	s Review
	Servi	ces Groups		
		Name ~	Address	Туре
	🗆 💋	packet decoder - Decoder	10.100.53.102	Decoder
	🗆 💋	vm3098 packet Decoder	10.100.53.98	Decoder
	🗹 💋	vm3099_log_Decoder	10.100.53.99	Log Decoder
C	Reset			Cancel Prev Next

**Note:** Netwitness installations having only a Log Decoder or a Packet Decoder display one or the other, not both. Deploying the Feed to both Log and Packet Decoders enable matching of IP event sources such as **ip.dst**, **ip-src**, **ipv6-src**, **ipv6-dst**.

6. Click Next.

The Define Columns dialog is displayed.

7. Define the **Type** as **IP** and **Index Column** 1 (IP Address Field). Set the header of each column as needed and click **Next**.

Define	Feed	$\geq$	Select Services	Define Columns	Revie
efine Inde ype	2X	● IP	O IP Range	O Non IP	
dex Colu	mn	1 ~			
Column	1 (odes)		2	3	4
Key			threatq.id	✓ threatq.link	v threatq.score
	5.9.73.22	6	8	https://www.th	reat 0.00
	23.224.1	72.71	9	https://	reat 0.00
	23.236.6	2.147	10	https://	reat 0.00
	23.247.2	0.31	11	https://	reat 0.00
	34.194.8	1.224	12	https://	reat 0.00
	34.196.14	49.119	13	https://armsth	reat 0.00
	43 741 1	96 105	14	https://www.ath	reat 0.00

**Important:** This example used in this document is IP based. Use Type **Non IP** for DNS threat intelligence Callback Key(s), for **aliashost** or **domain.dst** keys.

8. Select Finish to complete the setup of the Feed Integration.

Note that anytime before you click Finish, you can:

- Click **Cancel** to close the wizard without saving your feed definition.
- Click **Reset** to clear the data in the wizard.
- Click **Next** to display the next form (if not viewing the last form).
- Click **Prev** to display the previous form (if not viewing the first form)

Define F	eed	Select Se	rvices	Define Columns	Revi	ew
varine	inreat	QIPreea				
JRL	https:/ token=	LqIN5fcsy2Wm	tq.com/api/export SMBGdwl9	t/aad4bea18bce57	da407b9ce1bdc6a1	9a/?
lecurrence ry	e Every	T Day (S)				
Date Range	Start Da	ite	End Date			
ervice Details	S					
iervices		.og Collector - L	og Decoder			
Column Mapp	oing Details					
ndex Type	I	P				
IDR	f	alse				
alue Columns/	6					
1	2	3	4	5	6	thro-
IIIDEX	till eatquit	un eacquiris	threatquistore	tineatq.status	threatd.otcto_at	unee

9. Initially, the status appears as **Waiting** and the Progress indicator is yellow until RSA NetWitness completes the transfer of the Feed. After transfer is completed, the Status displays **Completed** and the Progress indicator turns green. Depending on the size of the feed, it may take some time for RSA NetWitness to download all Threat Intel from your provider.

Feeds						
+ - 2100						
Name	Trigger	Created	Last Run Time	Status	Progress	
RecordedFutureSALogs	Starting at 2015-Nov-04 14:34, every day	2015-11-04 09:3	2015-11-04 09:34:26		<u> </u>	_

The configuration of ThreatQ and Netwitness is complete. If there are any matches to the ThreatQ intelligence, they appear within the RSA Netwitness Investigator as part of the matched event.



Copyright © 2020 Dell Inc. or its subsidiaries. All Rights Reserved.

#### Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.