ThreatQuotient

RSA NetWitness App Guide

Version 1.0.0

July 13, 2021

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2021 ThreatQuotient, Inc.
All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Contents

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions >= `4.3.0`

Introduction

To integrate with NetWitness, ThreatQuotient developed an Output Script to send alerts/events to ThreatQ in real-time. This integration is a single-file script to handle alerts that are fired from NetWitness ESA.

Installation

In order to ingest Threat Intelligence from ThreatQ into RSA NetWitness, you must:

- Create an Export in ThreatQ.
- Edit your Log Concentrator in RSA NetWitness.
- Add the custom feed to RSA NetWitness.
- Install a script to pull all triggered alerts into ThreatQ.

Creating an Export in ThreatQ

The first step to ingesting threat intelligence into RSA NetWitness is to create the export from ThreatQ to be pulled into RSA NetWitness.

1. Log into your ThreatQ instance.
2. Click the gear icon.
3. Select the Exports option.
4. Click the **Add New Export** button.
5. Enter an export name (i.e. RSA NetWitness Custom Feed), and click the **Next Step** button.
6. Populate the Output Format form as follows:

FIELD	VALUE
Type of information you would like to export?	Indicators
Output type	Custom
Provide an output type here	text/csv
Special Parameters	Add your custom, special parameters here. For example:

FIELD	VALUE
	`indicator.deleted=N&indicator.status=Active&indicator.type=IP Address&indicator.score>=7`
Output Format Template	`{foreach $data as $indicator}{$indicator.value},https://{$http_host}/indicators/{$indicator.id}/details,{$indicator.score},{$indicator.id},{foreach $indicator.Sources as $source name='sourceloop'}{$source.value}{if !$smarty.foreach.sourceloop.last} | {/if}{/foreach}{/foreach}`

7. Click the **Save Settings** button.
8. From the Exports page, click the toggle next to the new export to enable it.
9. Test the export by clicking the link starting with `api/export/<export ID>.`

Editing Your Log Concentrator in RSA NetWitness

In order for RSA NetWitness to index the data, you must edit some custom XML files that are pushed to the Log Concentrator.

1. Log into your main RSA NetWitness instance.
2. Navigate to **Admin > System > Services**.
3. Select the gear icon next to your Log Concentrator entry.
4. Select **View > Config**.
5. Select the Files tab
6. From the drop-down list of files to edit, select `index-concentrator-custom.xml`.
7. Add the following lines within the `<language>` tags:

```
<key description="ThreatQ ID" format="UInt32" level="IndexValues" name="tq.id" valueMax="1000000000"
defaultAction="Open" />
<key description="ThreatQ Score" format="UInt8" level="IndexValues" name="tq.score" valueMax="100"
defaultAction="Open" />
<key description="ThreatQ Sources" format="Text" level="IndexValues" name="tq.sources" valueMax="250000"
defaultAction="Open" />
<key description="ThreatQ Reference" format="Text" level="IndexValues" name="tq.reference" valueMax="250000"
defaultAction="Open" />
```

7. Navigate back to **Admin > Services** and restart your Log Concentrator service.

Adding the Custom Feed in RSA NetWitness

After you configure the Concentrator to recognize the ThreatQ meta-keys, you must add the custom feed to RSA NetWitness.

1. Log into your main RSA NetWitness instance.
2. Navigate to **Configure > Custom Feeds**.
3. Click the **+** button to create a new feed.
4. Populate the Define Feed page as follows:

FIELD	VALUE
Feed Type	CSV
Feed Task Type	Recurring
Name	ThreatQ
URL	Enter your full export URL (without a limit)
Recur Every	1 Hour(s)

5. Click Next.
6. In the Select Services page, select your Log Decoder and your Context Hub.
7. Click Next.
8. Populate the Define Columns page as follows:

FIELD	VALUE
Type	IP
Index Column(s)	1
Key	Use the following meta-key names to populate the Key for each column of the CSV: ◦ tq.reference

FIELD	VALUE
	◦ tq.score ◦ tq.id ◦ tq.sources

9. Click Next.
10. On the Review page, verify the information.
11. Click Next.
12. Once saved, the feed begins pulling in threat intelligence from ThreatQ.

Script Installation

> This script brings all triggered alerts into ThreatQ from RSA NetWitness. These are *not* aggregated incidents. If you only want the incidents, install the **RSA NetWitness CDF** from the ThreatQ Marketplace.

Prerequisites

Download scripts

Before installation, you must download script files from the ThreatQ Marketplace to your PC:

1. Log into https://marketplace.threatq.com/.
2. Locate and download the following **RSA NetWitness** files:
   - rsa_nw_threatq_global_notification_output.export
   - rsa_nw_threatq_global_notification_server.export
3. Save these files to your PC.

Set up OAuth

OAuth client credentials are also required for the Alert Script. See the Help Center for detailed instructions. When setting up the credentials, enter RSA NetWitness Alerts as the name. After command execution, copy and save the credentials for use in step 6 of the script install process.

Installing the Script

1. Log into your main NetWitness instance.
2. Navigate to **Admin > System > Global Notifications > Output**.
3. Click the gear icon.
4. Select the Import option.
5. When prompted, select the `rsa_nw_threatq_global_notification_output.export` file you downloaded.
6. Once imported, edit the script, and enter in your ThreatQ authentication credentials:
    - ThreatQ Host
    - Client ID: This is generated via CLI.
    - Client Secret: This is generated via CLI.
7. Enter any configuration option changes.
8. Navigate to the Servers tab.
9. Click the gear Icon.
10. Select the Import option.
11. When prompted, select the `rsa_nw_threatq_global_notification_server.export` file you downloaded.

Applying the Script to the ESA Correlation Rule

Once the script has been imported, you must apply the notification script to your ESA Rule.

1. Log into your main NetWitness instance.
2. Navigate to **Configure > ESA Rules**.
3. Create an ESA rule. If you already have, edit the rule to which you want to apply the notification.
4. Under the Notifications section, click the **+** button to add a script notification.
5. For the Notification column, select the script you imported in the Installing the Script section.
6. For the Notification Server column, select the server that you created in the Installing the Script section.
7. For the Template column, select Default Script Template.
8. Save your rule.
9. Add the ESA rule to your deployment, then deploy your rule changes.

Troubleshooting

ThreatQ meta-keys are not indexed on the concentrator

Usually, this is an issue with NetWitness parsing the CSV feed from ThreatQ. To determine if there is an actual error with parsing:

1. SSH into your NetWitness instance running the log decoder. This may be your log-hybrid host if that was set up on the initial installation.
2. Next, `tail` the system logs and `grep` for messages pertaining to the ThreatQ Feed:
   CLI Command: `tail -n 200 /var/log/messages | grep -i threatq`
3. If you notice any logs with the following error, this most likely means there was an issue with the configuration of your ThreatQ Export. Please refer back to the Creating an Export in ThreatQ section to fix any issues.
   Error: `[FeedParser] [failure] Feedname: ThreatQ, exception: Failed to lookup handle for language key`
4. If the issue is not with your Export's configuration, it may be tied to a NetWitness service failing to communicate the feed information to the Log Decoder or Content Hub services. In that case, please open a support ticket with RSA to debug the issue with the service.

Change Log

- **Version 1.0.0**
  - Initial Release