ThreatQuotient

RSA NetWitness Incidents CDF Guide

Version 1.1.0

October 25, 2021

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

ThreatQ Supported

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

Contents

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.

Support

This integration is designated as **ThreatQ Supported**.

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

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ⚠ ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Versioning

- Current integration version `1.1.0`
- Supported on ThreatQ versions >= `4.35.0`

Introduction

The RSA NetWitness Incidents CDF for ThreatQuotient enables ThreatQ to automatically ingest incidents and their related indicators from RSA NetWitness.

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the integration file on your local machine

   > ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.
6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to configure and then enable the feed.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
RSA NetWitness Hostname/IP (and port)	Your RSA NetWitness Hostname/IP, along with the port (if applicable).
RSA NetWitness Login	Your RSA NetWitness Login (username) to authenticate with the API.
RSA NetWitness Password	Your RSA NetWitness Login (password) to authenticate with the API.
Alert Rules	An optional comma-delimited list of alert rules. This will limit the ingested incidents only to ones created by these rules.
Priority Filter	The incident priorities to be ingested. Options include: • Low • Medium (default)

PARAMETER	DESCRIPTION
	• High (default) • Critical (default)
Minimum Risk Score Threshold	The minimum risk score threshold for incidents to be ingested. The default setting is **50**.
Skip Closed Incidents	Checkbox to control whether to ingest close incidents. The default setting is **false**.
Skip Remediated Incidents	Checkbox to control whether to ingest remediated incidents. The default setting is **false**.
Verify SSL Certificate	Checkbox to enable or disable SSL certificate verification.

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

RSA NetWitness Incidents (Feed)

`GET https://{{host}}/rest/api/incidents`

This endpoint will fetch all incidents from RSA NetWitness, within a given timeframe. Each incident will be parsed for metadata and related indicators, and the intelligence will be uploaded to ThreatQ.


```
{
    "items": [
        {
            "id": "INC-708",
            "title": "High Risk Alerts: ESA for 119.45.42.241",
            "summary": "",
            "priority": "High",
            "riskScore": 50,
            "status": "New",
            "alertCount": 1,
            "averageAlertRiskScore": 50,
            "sealed": false,
            "totalRemediationTaskCount": 0,
            "openRemediationTaskCount": 0,
            "created": "2021-07-08T15:16:00.696Z",
            "lastUpdated": "2021-07-08T15:16:00.696Z",
            "lastUpdatedBy": null,
            "assignee": null,
            "sources": [
                "Event Stream Analysis"
            ],
            "ruleId": "5ffdec73cf797e197669c5f0",
            "firstAlertTime": "2021-07-08T15:15:46.290Z",
            "categories": [],
            "journalEntries": null,
            "createdBy": "High Risk Alerts: ESA",
            "deletedAlertCount": 0,
            "eventCount": 1,
            "alertMeta": {
                "SourceIp": [
                    "119.45.42.241"
                ],
                "DestinationIp": [
                    "172.24.131.192"
                ]
            }
        },
        {
            "id": "INC-707",
            "title": "High Risk Alerts: ESA for 81.68.246.68",
            "summary": "",
            "priority": "High",
```

```
            "riskScore": 50,
            "status": "New",
            "alertCount": 2,
            "averageAlertRiskScore": 50,
            "sealed": false,
            "totalRemediationTaskCount": 0,
            "openRemediationTaskCount": 0,
            "created": "2021-07-08T15:16:00.677Z",
            "lastUpdated": "2021-07-08T15:16:00.677Z",
            "lastUpdatedBy": null,
            "assignee": null,
            "sources": [
                "Event Stream Analysis"
            ],
            "ruleId": "5ffdec73cf797e197669c5f0",
            "firstAlertTime": "2021-07-08T15:15:46.265Z",
            "categories": [],
            "journalEntries": null,
            "createdBy": "High Risk Alerts: ESA",
            "deletedAlertCount": 0,
            "eventCount": 2,
            "alertMeta": {
                "SourceIp": [
                    "81.68.246.68"
                ],
                "DestinationIp": [
                    "172.21.225.14",
                    "172.18.205.42"
                ]
            }
        }
    ]
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
`.id| title| riskScore |priority`	Value	Incident	Concatenated together to form a title	`.firstAlertTime`	INC-435 - High Risk Alerts: ESA for 40.73.79.203 - Score: 50 - Priority: High	N/A
`.summary`	Description	Incident	N/A	N/A	N/A	These are empty by default
`.id`	Attribute	Incident ID	N/A	`.created`	INC-123	N/A
`.id`	Attribute	Incident Link	Concatenated with an incident URL	`.created`	https://{{host}}/respond /incident/{{id}}	N/A
`.priority`	Attribute	Priority	N/A	`.created`	High	N/A
`.status`	Attribute	Status	N/A	`.created`	New	N/A
`.averageAlertRiskScore`	Attribute	Average Alert Risk Score	N/A	`.created`	50	N/A
`.sealed`	Attribute	Is Sealed	bool -> True/False	`.created`	False	N/A
`.totalRemediationTaskCount`	Attribute	Total Remediation Task Count	N/A	`.created`	0	N/A
`.openRemediationTaskCount`	Attribute	Open RemediationTaskCount	N/A	`.created`	0	N/A
`.sources[]`	Attribute	Incident ID	N/A	`.created`	Event Stream Analysis	N/A
`.ruleId`	Attribute	Triggered Rule ID	N/A	`.created`	5ffdec73cf797e197669c5f0	N/A
`.alertCount`	Attribute	Alert Count	N/A	`.created`	INC-123	N/A
`.eventCount`	Attribute	Event Count	N/A	`.created`	INC-123	N/A
`.riskScore`	Attribute	Risk Score	N/A	`.created`	INC-123	N/A
`.categories[].parent|name`	Attribute	Category	Keys, `parent` & `name` are concatenated	`.created`	Hacking - path traversal	N/A
`.createdBy`	Attribute	Triggered Rule Name	N/A	`.created`	High Risk Alerts: ESA	N/A
`.journalEntries[].notes`	Attribute	Note	N/A	`.created`	Updated status	N/A
`.journalEntries[].milestone`	Attribute	Milestone	N/A	`.created`	Reconnaisance	N/A
`.alertMeta.SourceIp |`	Value	Indicator	N/A	`.created`	N/A	Lists merged and filtered by internal vs. external IPs.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
`DestinationIp[]`						External IPs are added as indicators
`.alertMeta.SourceIp` | `DestinationIp[]`	Attribute	Internal Device ID	N/A	`.created`	N/A	Lists merged and filtered by internal vs. external IPs. Internal IPs are added as attributes

Get API Token (Supplemental)

`POST https://{{host}}/rest/api/auth/userpass`

This endpoint will authenticate using user credentials to get back an access token used for each subsequent request.


```
{
  "id": "admin",
  "roles": [
    "Administrators"
  ],
  "accessToken": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9....",
  "refreshToken":
"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE2MjgzNTA3NDc1NjUsImlzcyI6InNlY3VyaXR5LXNlcnZlciOONzdjNzgzZSOwNzlhLT
RjNWYtODdkNCO3NDBhNTc5MmUyM2UiLCJpYXQiOjE2MjU3NTg3NDc1NjUsInJlZnJlc2giOnRydWUsInVzZXJfbmFtZSI6ImFkbWluInO....."
}
```

Average Feed Run

METRIC	RESULT
Run Time	1 minute
Incidents	274
Incident Attributes	4,003
Indicators	217
Indicator Attributes	217

Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on SIEM configuration and threat landscape.

Change Log

- **Version 1.1.0**
  - Added an optional configuration parameter: **Alert Rules**.
- **Version 1.0.0**
  - Initial Release