ThreatQuotient

Rapid7 InsightVM CDF User Guide

Version 1.0.0 rev-e

September 06, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

Not Actively Supported

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.

Copyright © 2023 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.

Support

This integration is designated as **Not Actively Supported**.

Integrations, apps, and add-ons designated as **Not Actively Supported** are not supported by ThreatQuotient's Customer Support team.

While you can report issues to ThreatQ's Customer Support team regarding the integration/app/add-on, you are solely responsible for ensuring proper functionality and version compatibility of Not Supported designations with the applicable ThreatQuotient software.

If unresolvable functional or compatibility issues are encountered, you may be required to uninstall the integration/app/add-on from your ThreatQuotient environment in order for ThreatQuotient to fulfill support obligations.

> For ThreatQuotient Hosted instance customers, the Service Level Commitment and Service Level Credit in the ThreatQuotient Service Level Schedule will not apply to issues caused by Not Actively Supported integrations/apps/add-ons.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 4.35.0
Support Tier	Not Actively Supported

Introduction

The Rapid7 insightVM integration for ThreatQ provides you with the ability to automatically track sites & assets registered within Rapid7 insightVM to monitor their vulnerabilities and overall risk.

The integration ingests threat intelligence data from the following endpoints:

- **Rapid7 insightVM - Sites** - automatically pulls sites & assets registered with Rapid7 insightVM.
- **Get Site Assets (supplemental)** - fetches the associated assets for a given site.
- **Get Asset Vulnerabilities (supplemental)** - fetches the vulnerabilities for a given asset.
- **Get Tags (supplemental)** - fetches the tags for a given asset or site.

The integration ingests the following system object types:

- Assets
  - Asset Attributes
- Indicators
  - Indicator Attributes
- Reports
  - Report Attributes

Prerequisites

Review the following prerequisites before attempting to install the integration.

Asset Object

The integration requires the Asset object. The Asset installation files are included with the integration download on the ThreatQ Marketplace. The Asset object must be installed prior to installing the integration.

> ⚠ You do not have to install the Asset object if you are running ThreatQ version 5.10.0 or greater as the object has been seeded as a default system object.

Use the steps provided to install the Asset custom object.

> ⚠ When installing the custom objects, be aware that any in-progress feed runs will be cancelled, and the API will be in maintenance mode.

1. Download the integration zip file from the ThreatQ Marketplace and unzip its contents.
2. SSH into your ThreatQ instance.
3. Navigate to tmp directory:

   ```
   cd /tmp/
   ```

4. Create a new directory:

   ```
   mkdir rapid7_cdf
   ```

5. Upload the **asset.json** and **install.sh** script into this new directory.
6. Create a new directory called **images** within the rapid7_cdf directory.

   ```
   mkdir images
   ```

7. Upload the asset.svg.
8. Navigate to the **/tmp/rapid7_cdf**.

   The directory should resemble the following:

   - tmp
     - **rapid7_cdf**
       - **asset.json**
       - **install.sh**
       - **images**
         - **asset.svg**

9. Run the following command to ensure that you have the proper permissions to install the custom object:

```
chmod +x install.sh
```

10. Run the following command:

```
sudo ./install.sh
```

> You must be in the directory level that houses the install.sh and json files when running this command.

The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

```
Installing Custom Objects - Step 1 of 5 (Entering Maintenance Mode)

Application is now in maintenance mode.
Installing Custom Objects - Step 2 of 5 (Installing the Asset Custom Object)
Installing Custom Objects - Step 3 of 5 (Configuring image for Asset Custom
Object)
Installing Custom Objects - Step 4 of 5 (Updating Permissions in ThreatQ)
Installing Custom Objects - Step 5 of 5 (Exiting Maintenance Mode)

Application is now live.
```

11. Remove the temporary directory, after the custom object has been installed, as the files are no longer needed:

```
rm -rf rapid7_cdf
```

Installation

> The CDF requires the installation of a custom object before installing the actual CDF if your are on ThreatQ version 5.9.0 or earlier. See the Prerequisites chapter for more details. The custom object must be installed prior to installing the CDF. Attempting to install the CDF without the custom object will cause the CDF install process to fail.

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.

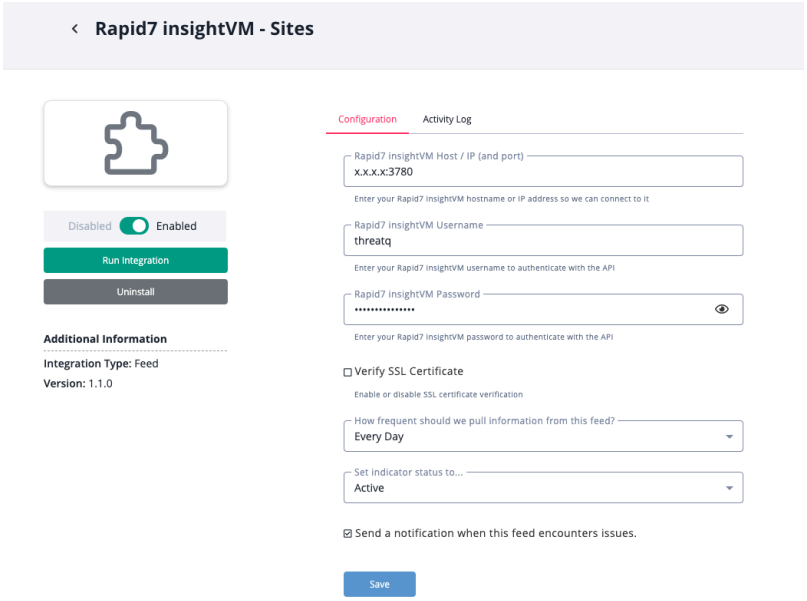
To configure the integration:

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 entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Rapid7 insightVM Host / IP (and port)	Enter your Rapid7 insightVM hostname or IP address.
Rapid7 insightVM Username	Enter your Rapid7 insightVM username to authenticate with the API.
Rapid7 insightVM Password	Enter your Rapid7 insightVM password to authenticate with the API.
Verify SSL Certificate	Enable or disable SSL certificate verification. This option is enabled by default.



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

Rapid7 insightVM - Sites (Feed)

This feed automatically pulls sites & assets registered with Rapid7 insightVM

`GET https://<host>:<port>/api/3/sites`

Sample Response:


```
{
  "resources": [
    {
      "assets": 1,
      "id": 2,
      "importance": "high",
      "lastScanTime": "2019-03-22T17:36:39.122Z",
      "links": [
        {
          "href": "https://10.13.0.65:3780/api/3/sites/2",
          "rel": "self"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/2/alerts",
          "rel": "Alerts"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/2/scan_engine",
          "rel": "Scan Engine"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/2/scan_schedules",
          "rel": "Schedules"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/2/organization",
          "rel": "Organization"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/2/tags",
          "rel": "Tags"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/2/users",
          "rel": "Users"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/2/scan_template",
          "rel": "Template"
```

```
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/2/site_credentials",
          "rel": "Site Credentials"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/2/shared_credentials",
          "rel": "Assigned Shared Credentials"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/2/web_authentication/
html_forms",
          "rel": "Web HTML Forms Authentication"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/2/web_authentication/
http_headers",
          "rel": "Web HTTP Headers Authentication"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/2/assets",
          "rel": "Assets"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/2/included_targets",
          "rel": "Included Targets"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/2/excluded_targets",
          "rel": "Excluded Targets"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/2/
included_asset_groups",
          "rel": "Included Asset Groups"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/2/
excluded_asset_groups",
          "rel": "Excluded Asset Groups"
        }
      ],
      "name": "ThreatQ Instance (ESXi)",
      "riskScore": 13107.0,
      "scanEngine": 3,
      "scanTemplate": "full-audit-without-web-spider",
      "type": "static",
      "vulnerabilities": {
        "critical": 0,
        "moderate": 9,
```

```
      "severe": 24,
      "total": 33
    }
  },
  {
    "assets": 1,
    "id": 1,
    "importance": "high",
    "lastScanTime": "2019-03-25T05:03:54.400Z",
    "links": [
      {
        "href": "https://10.13.0.65:3780/api/3/sites/1",
        "rel": "self"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/sites/1/alerts",
        "rel": "Alerts"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/sites/1/scan_engine",
        "rel": "Scan Engine"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/sites/1/scan_schedules",
        "rel": "Schedules"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/sites/1/organization",
        "rel": "Organization"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/sites/1/tags",
        "rel": "Tags"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/sites/1/users",
        "rel": "Users"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/sites/1/scan_template",
        "rel": "Template"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/sites/1/site_credentials",
        "rel": "Site Credentials"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/sites/1/shared_credentials",
        "rel": "Assigned Shared Credentials"
      },
```

```
        {
          "href": "https://10.13.0.65:3780/api/3/sites/1/web_authentication/
html_forms",
          "rel": "Web HTML Forms Authentication"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/1/web_authentication/
http_headers",
          "rel": "Web HTTP Headers Authentication"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/1/assets",
          "rel": "Assets"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/1/included_targets",
          "rel": "Included Targets"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/1/excluded_targets",
          "rel": "Excluded Targets"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/1/
included_asset_groups",
          "rel": "Included Asset Groups"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/sites/1/
excluded_asset_groups",
          "rel": "Excluded Asset Groups"
        }
      ],
      "name": "ThreatQ Website",
      "riskScore": 7405.0,
      "scanEngine": 3,
      "scanTemplate": "full-audit-without-web-spider",
      "type": "static",
      "vulnerabilities": {
        "critical": 5,
        "moderate": 2,
        "severe": 22,
        "total": 29
      }
    }
  ],
  "page": {
    "number": 0,
    "size": 10,
    "totalResources": 2,
```

```
    "totalPages": 1
  },
  "links": [
    {
      "href": "https://10.13.0.65:3780/api/3/sites?page=0&size=10&sort=id,asc",
      "rel": "self"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
`vulnerability.*`	Description	Report	N/A	N/A	N/A	HTML is built from the fields in this dict.
`.tags[]`	Tag	N/A	N/A	N/A	N/A	N/A
`.name`	Value	Report	Concatenated with `Rapid7 insightVM Site Report:`	`.lastScanTime`	N/A	N/A
`.importance`	Attribute	Importance	Title-cased	N/A	`High`	N/A
`.scanTemplate`	Attribute	Scan Template	N/A	N/A	N/A	N/A
`.type`	Attribute	Scan Type	N/A	N/A	`static`	N/A
`.vulnerabilities.total`	Attribute	Total Vulnerabilities	N/A	N/A	`32`	N/A
`.id`	Attribute	Site Link	Concatenated with `host` user field	N/A	N/A	N/A

Get Site Assets (Supplemental)

This supplemental feed will fetch the associated assets for a given site

`GET https://<host>:<port>/api/3/sites/<id>/assets`

Sample Response:


```
{
  "resources": [
    {
      "addresses": [
        {
          "ip": "10.12.0.101"
        }
      ],
      "assessedForPolicies": false,
      "assessedForVulnerabilities": true,
      "history": [
        {
          "date": "2019-03-22T17:11:00.842Z",
          "scanId": 1,
          "type": "SCAN",
          "version": 1
        },
        {
          "date": "2019-03-23T05:03:42.208Z",
          "scanId": 3,
          "type": "SCAN",
          "version": 2
        },
        {
          "date": "2019-03-24T05:03:37.782Z",
          "scanId": 4,
          "type": "SCAN",
          "version": 3
        },
        {
          "date": "2019-03-25T05:03:37.458Z",
          "scanId": 5,
          "type": "SCAN",
          "version": 4
        }
      ],
      "hostName": "threatq.com",
      "hostNames": [
        {
          "name": "threatq.com",
          "source": "user"
        }
```

```
    ],
    "id": 1,
    "ip": "10.12.0.101",
    "links": [
      {
        "href": "https://10.13.0.65:3780/api/3/assets/1",
        "rel": "self"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/assets/1/software",
        "rel": "Software"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/assets/1/files",
        "rel": "Files"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/assets/1/users",
        "rel": "Users"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/assets/1/user_groups",
        "rel": "User Groups"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/assets/1/databases",
        "rel": "Databases"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/assets/1/services",
        "rel": "Services"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/assets/1/tags",
        "rel": "Tags"
      }
    ],
    "os": "Linux 2.6.X",
    "osFingerprint": {
      "description": "Linux 2.6.X",
      "family": "Linux",
      "id": 4,
      "product": "Linux",
      "systemName": "Linux",
      "type": "General",
      "vendor": "Linux",
      "version": "2.6.X"
    },
    "rawRiskScore": 7404.6845703125,
    "riskScore": 7404.6845703125,
```

```
      "services": [
        {
          "configurations": [
            {
              "name": "bind.version",
              "value": "9.9.4-RedHat-9.9.4-61.el7"
            }
          ],
          "family": "BIND",
          "links": [
            {
              "href": "https://10.13.0.65:3780/api/3/assets/1/services/udp/53",
              "rel": "self"
            },
            {
              "href": "https://10.13.0.65:3780/api/3/assets/1/services/udp/53/
configurations",
              "rel": "Configurations"
            },
            {
              "href": "https://10.13.0.65:3780/api/3/assets/1/services/udp/53/
databases",
              "rel": "Databases"
            },
            {
              "href": "https://10.13.0.65:3780/api/3/assets/1/services/udp/53/
users",
              "rel": "Users"
            },
            {
              "href": "https://10.13.0.65:3780/api/3/assets/1/services/udp/53/
user_groups",
              "rel": "User Groups"
            },
            {
              "href": "https://10.13.0.65:3780/api/3/assets/1/services/udp/53/
web_applications",
              "rel": "Web Applications"
            }
          ],
          "name": "DNS",
          "port": 53,
          "product": "BIND",
          "protocol": "udp",
          "version": "9.9.4-RedHat-9.9.4-61.el7"
        },
        {
          "configurations": [
            {
              "name": "bind.version",
```

```
              "value": "9.9.4-RedHat-9.9.4-61.el7"
            }
          ],
          "family": "BIND",
          "links": [
            {
              "href": "https://10.13.0.65:3780/api/3/assets/1/services/tcp/53",
              "rel": "self"
            },
            {
              "href": "https://10.13.0.65:3780/api/3/assets/1/services/tcp/53/
configurations",
              "rel": "Configurations"
            },
            {
              "href": "https://10.13.0.65:3780/api/3/assets/1/services/tcp/53/
databases",
              "rel": "Databases"
            },
            {
              "href": "https://10.13.0.65:3780/api/3/assets/1/services/tcp/53/
users",
              "rel": "Users"
            },
            {
              "href": "https://10.13.0.65:3780/api/3/assets/1/services/tcp/53/
user_groups",
              "rel": "User Groups"
            },
            {
              "href": "https://10.13.0.65:3780/api/3/assets/1/services/tcp/53/
web_applications",
              "rel": "Web Applications"
            }
          ],
          "name": "DNS",
          "port": 53,
          "product": "BIND",
          "protocol": "tcp",
          "version": "9.9.4-RedHat-9.9.4-61.el7"
        },
        {
          "links": [
            {
              "href": "https://10.13.0.65:3780/api/3/assets/1/services/udp/
123",
              "rel": "self"
            },
            {
              "href": "https://10.13.0.65:3780/api/3/assets/1/services/udp/123/
```

```
configurations",
              "rel": "Configurations"
            },
            {
              "href": "https://10.13.0.65:3780/api/3/assets/1/services/udp/123/
databases",
              "rel": "Databases"
            },
            {
              "href": "https://10.13.0.65:3780/api/3/assets/1/services/udp/123/
users",
              "rel": "Users"
            },
            {
              "href": "https://10.13.0.65:3780/api/3/assets/1/services/udp/123/
user_groups",
              "rel": "User Groups"
            },
            {
              "href": "https://10.13.0.65:3780/api/3/assets/1/services/udp/123/
web_applications",
              "rel": "Web Applications"
            }
          ],
          "name": "NTP",
          "port": 123,
          "protocol": "udp"
        }
      ],
      "vulnerabilities": {
        "critical": 5,
        "exploits": 6,
        "malwareKits": 0,
        "moderate": 2,
        "severe": 22,
        "total": 29
      }
    }
  ],
  "page": {
    "number": 0,
    "size": 10,
    "totalResources": 1,
    "totalPages": 1
  },
  "links": [
    {
      "href": "https://10.13.0.65:3780/api/3/sites/1/assets?
page=0&size=10&sort=id,asc",
      "rel": "self"
    }
```

```
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
`.vulnerability.*`	Description	Asset	N/A	N/A	N/A	HTML is built from the fields in this dict
`.tags[]`	Tag	N/A	N/A	N/A	N/A	N/A
`.tags[]`	Attribute	`<Tag Type>`	Ignored if type is `custom`	N/A	N/A	`Tag Type` is determined by the `.tags[].type` field
`.services[].vendor/product/name`	Attribute	Installed Service	Keys are concatenated together if they exist	N/A	`OpenBSD - OpenSSH - SSH`	N/A
`.ip/hostName`	Asset	Value	N/A	N/A	N/A	`<hostName> (<ip>)` if hostName exists, otherwise, just `<ip>`
`.ip`	Attribute	IP Address	N/A	N/A	N/A	N/A
`.hostName`	Attribute	Hostname	N/A	N/A	N/A	N/A
`.id`	Attribute	ID	N/A	N/A	N/A	N/A
`.id`	Attribute	insightVM Link	Concatenated with the user field, `host`	N/A	N/A	N/A
`.os`	Attribute	Operating System	N/A	N/A	N/A	N/A
`.type`	Attribute	Asset Type	N/A	N/A	N/A	N/A
`.vulnerabilities.total`	Attribute	Total Vulnerabilities	N/A	N/A	N/A	N/A
`.assessedForPolicies`	Attribute	Assessed for Policies	bool -> string	N/A	N/A	N/A
`.assessedForVulnerabilities`	Attribute	Assessed for Vulnerabilities	bool -> string	N/A	N/A	N/A

These mappings are based on the data pulled from the `resources` list from the API response.

Get Asset Vulnerabilities (Supplemental)

This supplemental feed will fetch the vulnerabilities for a given asset

`GET https://<host>:<port>/api/3/assets/<id>/vulnerabilities`

Sample Response:


```
{
  "resources": [
    {
      "id": "apache-httpd-cve-2016-4975",
      "instances": 3,
      "links": [
        {
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
apache-httpd-cve-2016-4975",
          "rel": "self"
        },
        {
          "id": "apache-httpd-cve-2016-4975",
          "href": "https://10.13.0.65:3780/api/3/vulnerabilities/apache-httpd-
cve-2016-4975",
          "rel": "Vulnerability"
        },
        {
          "id": "apache-httpd-cve-2016-4975",
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
apache-httpd-cve-2016-4975/validations",
          "rel": "Vulnerability Validations"
        },
        {
          "id": "apache-httpd-cve-2016-4975",
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
apache-httpd-cve-2016-4975/solution",
          "rel": "Vulnerability Solutions"
        }
      ],
      "results": [
        {
          "port": 8443,
          "proof": "<p><ul><li>Running HTTPS service</li><li>Product HTTPD
exists -- Apache HTTPD 2.4.6</li><li>Vulnerable version of product HTTPD found
-- Apache HTTPD 2.4.6</li></ul></p>",
          "protocol": "tcp",
          "since": "2019-03-22T17:36:22.611Z",
          "status": "vulnerable-version"
        },
        {
          "port": 443,
```

```
          "proof": "<p><ul><li>Running HTTPS service</li><li>Product HTTPD
exists -- Apache HTTPD 2.4.6</li><li>Vulnerable version of product HTTPD found
-- Apache HTTPD 2.4.6</li></ul></p>",
          "protocol": "tcp",
          "since": "2019-03-22T17:36:22.611Z",
          "status": "vulnerable-version"
        },
        {
          "port": 80,
          "proof": "<p><ul><li>Running HTTP service</li><li>Product HTTPD
exists -- Apache HTTPD 2.4.6</li><li>Vulnerable version of product HTTPD found
-- Apache HTTPD 2.4.6</li></ul></p>",
          "protocol": "tcp",
          "since": "2019-03-22T17:36:22.611Z",
          "status": "vulnerable-version"
        }
      ],
      "since": "2019-03-22T17:36:22.611Z",
      "status": "vulnerable"
    },
    {
      "id": "apache-httpd-cve-2017-15710",
      "instances": 3,
      "links": [
        {
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
apache-httpd-cve-2017-15710",
          "rel": "self"
        },
        {
          "id": "apache-httpd-cve-2017-15710",
          "href": "https://10.13.0.65:3780/api/3/vulnerabilities/apache-httpd-
cve-2017-15710",
          "rel": "Vulnerability"
        },
        {
          "id": "apache-httpd-cve-2017-15710",
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
apache-httpd-cve-2017-15710/validations",
          "rel": "Vulnerability Validations"
        },
        {
          "id": "apache-httpd-cve-2017-15710",
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
apache-httpd-cve-2017-15710/solution",
          "rel": "Vulnerability Solutions"
        }
      ],
      "results": [
        {
```

```
          "port": 8443,
          "proof": "<p><ul><li>Running HTTPS service</li><li>Product HTTPD
exists -- Apache HTTPD 2.4.6</li><li>Vulnerable version of product HTTPD found
-- Apache HTTPD 2.4.6</li></ul></p>",
          "protocol": "tcp",
          "since": "2019-03-22T17:36:22.611Z",
          "status": "vulnerable-version"
        },
        {
          "port": 443,
          "proof": "<p><ul><li>Running HTTPS service</li><li>Product HTTPD
exists -- Apache HTTPD 2.4.6</li><li>Vulnerable version of product HTTPD found
-- Apache HTTPD 2.4.6</li></ul></p>",
          "protocol": "tcp",
          "since": "2019-03-22T17:36:22.611Z",
          "status": "vulnerable-version"
        },
        {
          "port": 80,
          "proof": "<p><ul><li>Running HTTP service</li><li>Product HTTPD
exists -- Apache HTTPD 2.4.6</li><li>Vulnerable version of product HTTPD found
-- Apache HTTPD 2.4.6</li></ul></p>",
          "protocol": "tcp",
          "since": "2019-03-22T17:36:22.611Z",
          "status": "vulnerable-version"
        }
      ],
      "since": "2019-03-22T17:36:22.611Z",
      "status": "vulnerable"
    },
    {
      "id": "apache-httpd-cve-2018-1301",
      "instances": 3,
      "links": [
        {
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
apache-httpd-cve-2018-1301",
          "rel": "self"
        },
        {
          "id": "apache-httpd-cve-2018-1301",
          "href": "https://10.13.0.65:3780/api/3/vulnerabilities/apache-httpd-
cve-2018-1301",
          "rel": "Vulnerability"
        },
        {
          "id": "apache-httpd-cve-2018-1301",
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
apache-httpd-cve-2018-1301/validations",
          "rel": "Vulnerability Validations"
```

```
        },
        {
          "id": "apache-httpd-cve-2018-1301",
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
apache-httpd-cve-2018-1301/solution",
          "rel": "Vulnerability Solutions"
        }
      ],
      "results": [
        {
          "port": 8443,
          "proof": "<p><ul><li>Running HTTPS service</li><li>Product HTTPD
exists -- Apache HTTPD 2.4.6</li><li>Vulnerable version of product HTTPD found
-- Apache HTTPD 2.4.6</li></ul></p>",
          "protocol": "tcp",
          "since": "2019-03-22T17:36:22.611Z",
          "status": "vulnerable-version"
        },
        {
          "port": 443,
          "proof": "<p><ul><li>Running HTTPS service</li><li>Product HTTPD
exists -- Apache HTTPD 2.4.6</li><li>Vulnerable version of product HTTPD found
-- Apache HTTPD 2.4.6</li></ul></p>",
          "protocol": "tcp",
          "since": "2019-03-22T17:36:22.611Z",
          "status": "vulnerable-version"
        },
        {
          "port": 80,
          "proof": "<p><ul><li>Running HTTP service</li><li>Product HTTPD
exists -- Apache HTTPD 2.4.6</li><li>Vulnerable version of product HTTPD found
-- Apache HTTPD 2.4.6</li></ul></p>",
          "protocol": "tcp",
          "since": "2019-03-22T17:36:22.611Z",
          "status": "vulnerable-version"
        }
      ],
      "since": "2019-03-22T17:36:22.611Z",
      "status": "vulnerable"
    },
    {
      "id": "apache-httpd-cve-2018-1312",
      "instances": 3,
      "links": [
        {
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
apache-httpd-cve-2018-1312",
          "rel": "self"
        },
        {
```

```
          "id": "apache-httpd-cve-2018-1312",
          "href": "https://10.13.0.65:3780/api/3/vulnerabilities/apache-httpd-
cve-2018-1312",
          "rel": "Vulnerability"
        },
        {
          "id": "apache-httpd-cve-2018-1312",
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
apache-httpd-cve-2018-1312/validations",
          "rel": "Vulnerability Validations"
        },
        {
          "id": "apache-httpd-cve-2018-1312",
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
apache-httpd-cve-2018-1312/solution",
          "rel": "Vulnerability Solutions"
        }
      ],
      "results": [
        {
          "port": 8443,
          "proof": "<p><ul><li>Running HTTPS service</li><li>Product HTTPD
exists -- Apache HTTPD 2.4.6</li><li>Vulnerable version of product HTTPD found
-- Apache HTTPD 2.4.6</li></ul></p>",
          "protocol": "tcp",
          "since": "2019-03-22T17:36:22.611Z",
          "status": "vulnerable-version"
        },
        {
          "port": 443,
          "proof": "<p><ul><li>Running HTTPS service</li><li>Product HTTPD
exists -- Apache HTTPD 2.4.6</li><li>Vulnerable version of product HTTPD found
-- Apache HTTPD 2.4.6</li></ul></p>",
          "protocol": "tcp",
          "since": "2019-03-22T17:36:22.611Z",
          "status": "vulnerable-version"
        },
        {
          "port": 80,
          "proof": "<p><ul><li>Running HTTP service</li><li>Product HTTPD
exists -- Apache HTTPD 2.4.6</li><li>Vulnerable version of product HTTPD found
-- Apache HTTPD 2.4.6</li></ul></p>",
          "protocol": "tcp",
          "since": "2019-03-22T17:36:22.611Z",
          "status": "vulnerable-version"
        }
      ],
      "since": "2019-03-22T17:36:22.611Z",
      "status": "vulnerable"
    },
```

```
    {
      "id": "centos_linux-cve-2018-17972",
      "instances": 1,
      "links": [
        {
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
centos_linux-cve-2018-17972",
          "rel": "self"
        },
        {
          "id": "centos_linux-cve-2018-17972",
          "href": "https://10.13.0.65:3780/api/3/vulnerabilities/centos_linux-
cve-2018-17972",
          "rel": "Vulnerability"
        },
        {
          "id": "centos_linux-cve-2018-17972",
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
centos_linux-cve-2018-17972/validations",
          "rel": "Vulnerability Validations"
        },
        {
          "id": "centos_linux-cve-2018-17972",
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
centos_linux-cve-2018-17972/solution",
          "rel": "Vulnerability Solutions"
        }
      ],
      "results": [
        {
          "proof": "<p><p>Vulnerable OS: CentOS Linux 7.6.1810<p></p></
p><p><ul><li><ContainerBlockElement>kernel - version 3.10.0-957.5.1.el7 is
installed</ContainerBlockElement></li></ul></p></p>",
          "since": "2019-03-22T17:36:22.611Z",
          "status": "vulnerable-version"
        }
      ],
      "since": "2019-03-22T17:36:22.611Z",
      "status": "vulnerable"
    },
    {
      "id": "centos_linux-cve-2018-18445",
      "instances": 1,
      "links": [
        {
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
centos_linux-cve-2018-18445",
          "rel": "self"
        },
        {
```

```
          "id": "centos_linux-cve-2018-18445",
          "href": "https://10.13.0.65:3780/api/3/vulnerabilities/centos_linux-
cve-2018-18445",
          "rel": "Vulnerability"
        },
        {
          "id": "centos_linux-cve-2018-18445",
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
centos_linux-cve-2018-18445/validations",
          "rel": "Vulnerability Validations"
        },
        {
          "id": "centos_linux-cve-2018-18445",
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
centos_linux-cve-2018-18445/solution",
          "rel": "Vulnerability Solutions"
        }
      ],
      "results": [
        {
          "proof": "<p><p>Vulnerable OS: CentOS Linux 7.6.1810<p></p></
p><p><ul><li><ContainerBlockElement>kernel - version 3.10.0-957.5.1.el7 is
installed</ContainerBlockElement></li></ul></p></p>",
          "since": "2019-03-22T17:36:22.611Z",
          "status": "vulnerable-version"
        }
      ],
      "since": "2019-03-22T17:36:22.611Z",
      "status": "vulnerable"
    },
    {
      "id": "centos_linux-cve-2018-9568",
      "instances": 1,
      "links": [
        {
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
centos_linux-cve-2018-9568",
          "rel": "self"
        },
        {
          "id": "centos_linux-cve-2018-9568",
          "href": "https://10.13.0.65:3780/api/3/vulnerabilities/centos_linux-
cve-2018-9568",
          "rel": "Vulnerability"
        },
        {
          "id": "centos_linux-cve-2018-9568",
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
centos_linux-cve-2018-9568/validations",
          "rel": "Vulnerability Validations"
```

```
        },
        {
          "id": "centos_linux-cve-2018-9568",
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
centos_linux-cve-2018-9568/solution",
          "rel": "Vulnerability Solutions"
        }
      ],
      "results": [
        {
          "proof": "<p><p>Vulnerable OS: CentOS Linux 7.6.1810<p></p></
p><p><ul><li><ContainerBlockElement>kernel - version 3.10.0-957.5.1.el7 is
installed</ContainerBlockElement></li></ul></p></p>",
          "since": "2019-03-22T17:36:22.611Z",
          "status": "vulnerable-version"
        }
      ],
      "since": "2019-03-22T17:36:22.611Z",
      "status": "vulnerable"
    },
    {
      "id": "centos_linux-cve-2019-6133",
      "instances": 1,
      "links": [
        {
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
centos_linux-cve-2019-6133",
          "rel": "self"
        },
        {
          "id": "centos_linux-cve-2019-6133",
          "href": "https://10.13.0.65:3780/api/3/vulnerabilities/centos_linux-
cve-2019-6133",
          "rel": "Vulnerability"
        },
        {
          "id": "centos_linux-cve-2019-6133",
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
centos_linux-cve-2019-6133/validations",
          "rel": "Vulnerability Validations"
        },
        {
          "id": "centos_linux-cve-2019-6133",
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
centos_linux-cve-2019-6133/solution",
          "rel": "Vulnerability Solutions"
        }
      ],
      "results": [
        {
```

```
          "proof": "<p><p>Vulnerable OS: CentOS Linux 7.6.1810<p></p></
p><p><ul><li><ContainerBlockElement>polkit - version 0.112-18.el7 is
installed</ContainerBlockElement></li></ul></p></p>",
          "since": "2019-03-22T17:36:22.611Z",
          "status": "vulnerable-version"
        }
      ],
      "since": "2019-03-22T17:36:22.611Z",
      "status": "vulnerable"
    },
    {
      "id": "certificate-common-name-mismatch",
      "instances": 2,
      "links": [
        {
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
certificate-common-name-mismatch",
          "rel": "self"
        },
        {
          "id": "certificate-common-name-mismatch",
          "href": "https://10.13.0.65:3780/api/3/vulnerabilities/certificate-
common-name-mismatch",
          "rel": "Vulnerability"
        },
        {
          "id": "certificate-common-name-mismatch",
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
certificate-common-name-mismatch/validations",
          "rel": "Vulnerability Validations"
        },
        {
          "id": "certificate-common-name-mismatch",
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
certificate-common-name-mismatch/solution",
          "rel": "Vulnerability Solutions"
        }
      ],
      "results": [
        {
          "port": 8443,
          "proof": "<p><p>The subject common name found in the X.509
certificate does not seem to match the scan target:<ul><li>Subject CN
*.threatq.com does not match target name specified in the site.</li><li>Subject
CN *.threatq.com could not be resolved to an IP address via DNS lookup</
li><li>Subject Alternative Name *.threatq.com does not match target name
specified in the site.</li><li>Subject Alternative Name threatq.com does not
match target name specified in the site.</li></ul></p></p>",
          "protocol": "tcp",
          "since": "2019-03-22T17:36:22.611Z",
```

```
          "status": "vulnerable"
        },
        {
          "port": 443,
          "proof": "<p><p>The subject common name found in the X.509
certificate does not seem to match the scan target:<ul><li>Subject CN
*.threatq.com does not match target name specified in the site.</li><li>Subject
CN *.threatq.com could not be resolved to an IP address via DNS lookup</
li><li>Subject Alternative Name *.threatq.com does not match target name
specified in the site.</li><li>Subject Alternative Name threatq.com does not
match target name specified in the site.</li></ul></p></p>",
          "protocol": "tcp",
          "since": "2019-03-22T17:36:22.611Z",
          "status": "vulnerable"
        }
      ],
      "since": "2019-03-22T17:36:22.611Z",
      "status": "vulnerable"
    },
    {
      "id": "generic-icmp-timestamp",
      "instances": 1,
      "links": [
        {
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
generic-icmp-timestamp",
          "rel": "self"
        },
        {
          "id": "generic-icmp-timestamp",
          "href": "https://10.13.0.65:3780/api/3/vulnerabilities/generic-icmp-
timestamp",
          "rel": "Vulnerability"
        },
        {
          "id": "generic-icmp-timestamp",
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
generic-icmp-timestamp/validations",
          "rel": "Vulnerability Validations"
        },
        {
          "id": "generic-icmp-timestamp",
          "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities/
generic-icmp-timestamp/solution",
          "rel": "Vulnerability Solutions"
        }
      ],
      "results": [
        {
          "proof": "<p><p>Able to determine remote system time.</p></p>",
```

```
          "since": "2019-03-22T17:36:22.611Z",
          "status": "vulnerable"
        }
      ],
      "since": "2019-03-22T17:36:22.611Z",
      "status": "vulnerable"
    }
  ],
  "page": {
    "number": 0,
    "size": 10,
    "totalResources": 33,
    "totalPages": 4
  },
  "links": [
    {
      "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities?
page=0&size=10&sort=id,asc",
      "rel": "first"
    },
    {
      "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities?
page=0&size=10&sort=id,asc",
      "rel": "self"
    },
    {
      "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities?
page=1&size=10&sort=id,asc",
      "rel": "next"
    },
    {
      "href": "https://10.13.0.65:3780/api/3/assets/2/vulnerabilities?
page=3&size=10&sort=id,asc",
      "rel": "last"
    }
  ]
}
```

ThreatQuotient 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`	Indicator Value	CVE	N/A	N/A	N/A	Parsed from the ID of the vulnerability
`.proof[]`	Description	Asset	N/A	N/A	N/A	HTML is built from the values within the `proof` key

These mappings are based on the data pulled from the `resources` list from the API response.

Get Tags (Supplemental)

This supplemental feed will fetch the tags for a given asset or site

`GET https://<host>:<port>/api/3/<entity type>/<id>/tags`

Sample Response:


```
{
  "resources": [
    {
      "color": "default",
      "created": "2019-03-21T21:02:38.439Z",
      "id": 2,
      "links": [
        {
          "href": "https://10.13.0.65:3780/api/3/tags/2",
          "rel": "self"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/tags/2/assets",
          "rel": "Tag Assets"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/tags/2/asset_groups",
          "rel": "Tag Asset Groups"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/tags/2/sites",
          "rel": "Tag Sites"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/tags/2/search_criteria",
          "rel": "Tag Search Criteria"
        },
        {
          "href": "https://10.13.0.65:3780/api/3/users/0",
          "rel": "Tag Creator"
        }
      ],
      "name": "High",
      "riskModifier": "1.5",
      "source": "built-in",
      "sources": [
        {
          "source": "tag"
        }
      ],
      "type": "criticality"
    },
```

```
{
  "color": "default",
  "created": "2021-11-22T18:32:31.590Z",
  "id": 7,
  "links": [
    {
      "href": "https://10.13.0.65:3780/api/3/tags/7",
      "rel": "self"
    },
    {
      "href": "https://10.13.0.65:3780/api/3/tags/7/assets",
      "rel": "Tag Assets"
    },
    {
      "href": "https://10.13.0.65:3780/api/3/tags/7/asset_groups",
      "rel": "Tag Asset Groups"
    },
    {
      "href": "https://10.13.0.65:3780/api/3/tags/7/sites",
      "rel": "Tag Sites"
    },
    {
      "href": "https://10.13.0.65:3780/api/3/tags/7/search_criteria",
      "rel": "Tag Search Criteria"
    },
    {
      "href": "https://10.13.0.65:3780/api/3/users/1",
      "rel": "Tag Creator"
    }
  ],
  "name": "on-prem",
  "source": "custom",
  "sources": [
    {
      "source": "tag"
    }
  ],
  "type": "location"
},
{
  "color": "default",
  "created": "2021-11-22T18:32:35.543Z",
  "id": 8,
  "links": [
    {
      "href": "https://10.13.0.65:3780/api/3/tags/8",
      "rel": "self"
    },
    {
      "href": "https://10.13.0.65:3780/api/3/tags/8/assets",
```

```
        "rel": "Tag Assets"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/tags/8/asset_groups",
        "rel": "Tag Asset Groups"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/tags/8/sites",
        "rel": "Tag Sites"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/tags/8/search_criteria",
        "rel": "Tag Search Criteria"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/users/1",
        "rel": "Tag Creator"
      }
    ],
    "name": "TIE",
    "source": "custom",
    "sources": [
      {
        "source": "tag"
      }
    ],
    "type": "owner"
  },
  {
    "color": "blue",
    "created": "2021-11-22T18:32:45.337Z",
    "id": 9,
    "links": [
      {
        "href": "https://10.13.0.65:3780/api/3/tags/9",
        "rel": "self"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/tags/9/assets",
        "rel": "Tag Assets"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/tags/9/asset_groups",
        "rel": "Tag Asset Groups"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/tags/9/sites",
        "rel": "Tag Sites"
      },
      {
```

```
        "href": "https://10.13.0.65:3780/api/3/tags/9/search_criteria",
        "rel": "Tag Search Criteria"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/users/1",
        "rel": "Tag Creator"
      }
    ],
    "name": "threatq-demo",
    "source": "custom",
    "sources": [
      {
        "source": "tag"
      }
    ],
    "type": "custom"
  },
  {
    "color": "orange",
    "created": "2021-11-22T18:33:03.265Z",
    "id": 10,
    "links": [
      {
        "href": "https://10.13.0.65:3780/api/3/tags/10",
        "rel": "self"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/tags/10/assets",
        "rel": "Tag Assets"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/tags/10/asset_groups",
        "rel": "Tag Asset Groups"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/tags/10/sites",
        "rel": "Tag Sites"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/tags/10/search_criteria",
        "rel": "Tag Search Criteria"
      },
      {
        "href": "https://10.13.0.65:3780/api/3/users/1",
        "rel": "Tag Creator"
      }
    ],
    "name": "validated",
    "source": "custom",
    "sources": [
```

```
        {
          "source": "tag"
        }
      ],
      "type": "custom"
    }
  ],
  "links": [
    {
      "href": "https://10.13.0.65:3780/api/3/assets/2/tags",
      "rel": "self"
    }
  ]
}
```

Average Feed Run

> Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

Rapid7 insightVM - Sites

METRIC	RESULT
Run Time	1 minute
Assets	2
Asset Attributes	24
Indicators	45
Reports	2
Report Attributes	10

Change Log

- **Version 1.0.0 rev-e (Guide Update)**
  - Updated the Prerequisites chapter regarding the Asset object. ThreatQ version 5.10.0 introduced the Asset object as a seeded default system object. Users on ThreatQ 5.10.0 or later do not have to install the Asset custom object prior to installing the integration.
  - Corrected support tier to Not Actively Supported.
- **Version 1.0.0**
  - Initial release