ThreatQuotient

Rapid7 InsightVM Operation Guide

Version 1.1.0

December 13, 2021

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

Not 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.

Support

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

Integrations, apps, and add-ons designated as **Not 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 Supported integrations/apps/add-ons.

Versioning

- Current integration version: `1.1.0`
- Compatible with ThreatQ versions >= `4.35.0`

Introduction

The Rapid7 InsightVM Operation allows a ThreatQ user to execute CVE actions on their Rapid7 InsightVM instance.

The integration allows users to query for CVE details in their Rapid7 InsightVM instance. This action will return information on the vulnerability such as the scores and solutions.

The integration also allows users to query Rapid7 InsightVM to see if any configured sites or assets are vulnerable to a specific CVE. This action will show information on the asset as well as solutions to the vulnerability.

This integration requires the use of a custom object: Asset. See the Prerequisites chapter for more details.

Prerequisites

The Rapid7 InsightVM Operation requires the installation of the following custom object:

- Asset

The files associated with the custom object are included in the integration zip file downloaded from the ThreatQ Marketplace.

Custom Object Installation

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. Locate the custom object files in the zip file you downloaded from the ThreatQ Marketplace. Custom Object files include:
   - asset.json
   - asset.svg
2. SSH into your ThreatQ instance
3. Unzip and then copy the custom objects files to directory of your choice.

   > ThreatQuotient recommends uploading the files to the `/var/www/api/database/seeds/data/custom_objects/`.

4. Navigate to the API directory:

   ```
   <> cd /var/www/api
   ```

5. Put your ThreatQ instance into maintenance mode:

   ```
   <> sudo php artisan down
   ```

6. Run the following command to install the Custom Object Definition:

   ```
   <> sudo php artisan threatq:make-object-set --file=<Path To JSON
      File>

      sudo php artisan threatq:object-settings --code=object --
      icon=<Path To Icon Folder>/asset.svg --background-
      color='#03ac14'
   ```

7. Clear the ThreatQ object cache and update permissions:

```
<> sudo php /var/www/api/artisan cache:clear sudo php /var/www/
   api/artisan threatq:update-permissions
```

8. Take your ThreatQ instance out of maintenance mode and restart Dynamo:

```
<> sudo php artisan up sudo systemctl restart threatq-dynamo
```

Installation

> The operation requires the installation of a custom object before installing the actual operation.
> See the Prerequisites chaper for more details. The custom object must be installed priot to installing the operation. Attempting to install the operation without the custom object
> will cause the 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 operation 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 operation and will require user confirmation before proceeding.

6. You will still need to configure and then enable the operation.

Configuration

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

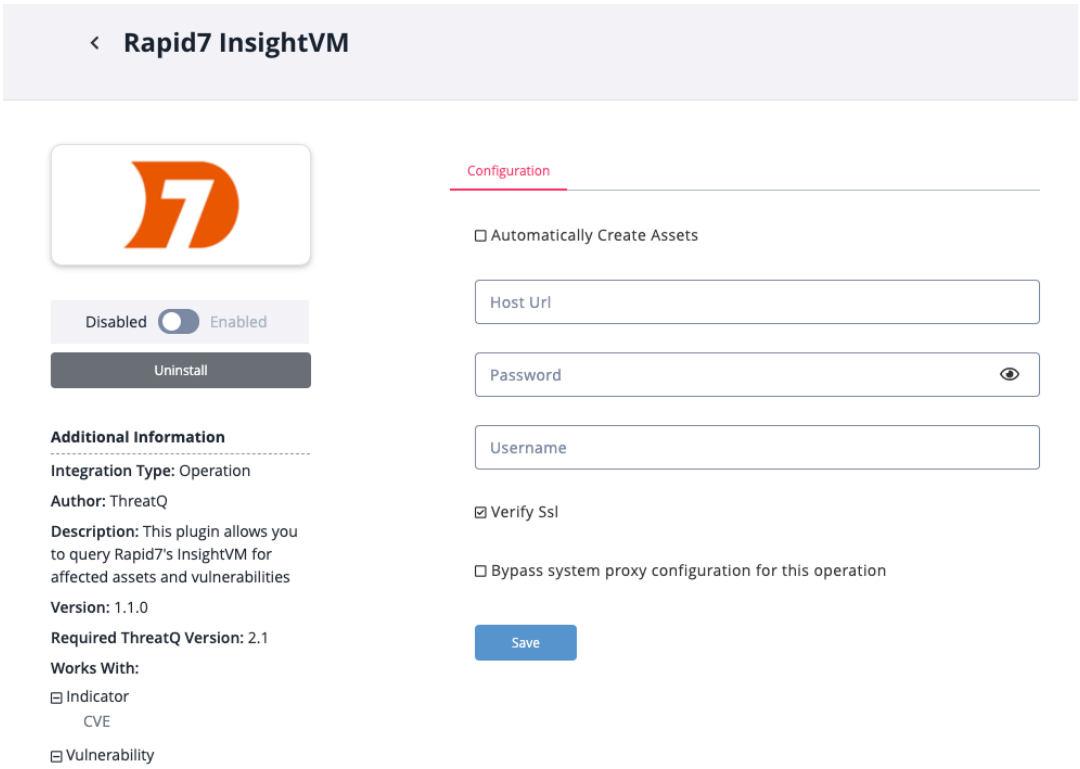
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Operation** option from the *Type* 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
Auto Create Assets	Use the checkbox provided to select whether or not to automatically create and relate asset objects to the CVEs.
Host URL	The Host or IP of your Rapid7 InsightVM instance including the port.
Username	Your Rapid7 InsightVM username to use with the API.
Password	Your Rapid7 InsightVM password associated with the above username.
Verify SSL	Use the checkbox provided to verify the host's SSL certificate when requesting it.



5. Click **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable the operation.

Actions

The Rapid7 InsightVM Operation provides the following actions:

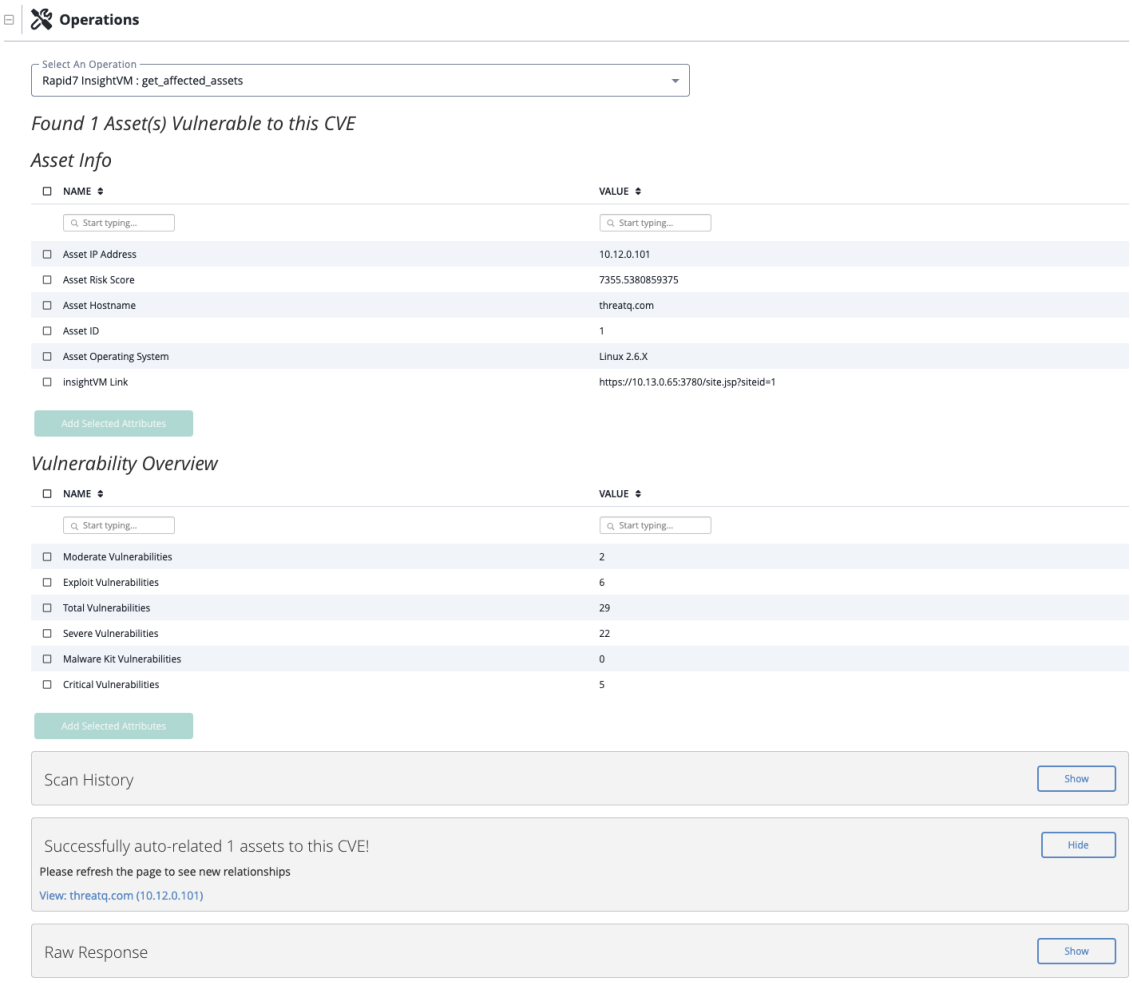
ACTION	DESCRIPTION	OBJECT TYPES	OBJECT SUB-TYPES
Get Affected Assets	Queries Rapid7 InsightVM to determine if you have any assets/sites affected by the specific CVE.	Asset, CVE	N/A
Query	Queries Rapid7 InsightVM to determine what information and scores it has for the vulnerability.	Asset, CVE	N/A
Add Tag	Adds a tag to an existing asset within Rapid7 insightVM.	Asset	N/A
Remove Tag	Remove a tag from an existing asset within Rapid7 insightVM.	Asset	N/A

Get Affected Assets

The Get Affected Assets action allows you to query Rapid7 InsightVM and see if you have any assets/sites affected by the specific CVE.

> If there are no assets affected by the vulnerability, you will receive a message saying there are no affected assets.

Result Example



Query

The Query action allows you to query your Rapid7 InsightVM to see what information and scores it has for the vulnerability.

> If there are no CVEs found, you will receive a message saying the CVE does not exist in Rapid7 InsightVM

Result Examples

Query General Results

General Info

	Name	Value
	Search	Search
☐	CVE Description	In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.
☐	CVE Title	Alpine Linux: CVE-2018-1312: apache2 Multiple vulnerabilities
☐	Rapid7 CVE ID	alpine-linux-cve-2018-1312
☐	Category	Alpine Linux
☐	Category	Apache
☐	Category	Web
☐	Date Added	2018-04-02
☐	Date Published	2018-03-26

Add Selected Attributes

Verdict Results

CVE Verdicts

Showing 1 to 15 of 15 Row count: 25

Name	Value
Search	Search
Severity	Severe
PCI Compliance Status	Fail
PCI Severity Score	4
PCI CVSS Score	6
Number of Exploits	0
Severity Score	7
Rapid7 Risk Score	327.09
Denial of Service	False
Number of Malware Kits	0
CVSS v2 Impact Score	5.8731
CVSS v2 Exploit Score	3.887
CVSS v2 Score	9.8
CVSS v2 Impact Score	6.443
CVSS v2 Score	6.8
CVSS v2 Exploit Score	8.5888

Add Selected Attributes

Solutions Results

Solutions

Solution	Time Needed
Search	Search
Use 'apk update' and 'apk upgrade' to upgrade all packages to the latest version. To only update apache2 use the commands 'apk update' and 'apk add --upgrade apache2'.	PT15M

Add Selected Attributes

Add Tag

The Add Tag action allows you to add a tag to an existing asset within Rapid7 insightVM.

Parameters

ThreatQ provides the following parameters for this Action:

PARAMETER	DESCRIPTION
Name	Enter a tag name to apply to the given asset.
Tag Type	Select the type of tag you want this tag to be.  This will be ignored if a tag with the same name already exists.

Remove Tag

The Remove Tag action allows you to remove a tag from an existing asset within Rapid7 insightVM.

Parameters

ThreatQ provides the following parameter for this Action:

PARAMETER	DESCRIPTION
Name	Enter a tag name to remove from the given asset.

Change Log

- **Version 1.1.0**
  - Initial Release