

ThreatQuotient



Rapid7 insightVM Operation User Guide

Version 1.1.1

November 06, 2023

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

 ThreatQ Supported

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Warning and Disclaimer	3
Support	4
Integration Details.....	5
Introduction	6
Prerequisites	7
Asset Object.....	7
Installation.....	9
Configuration	10
Actions	12
Get Affected Assets.....	13
Result Example	13
Query	14
Query General Result Example.....	14
Verdict Result Example	14
Solution Result Example	15
Add Tag.....	16
Action Parameters.....	16
Remove Tag	17
Action Parameters.....	17
Change Log	18

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 **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.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version 1.1.1

**Compatible with ThreatQ
Versions** $\geq 4.35.0$

Support Tier ThreatQ Supported

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.

The operation provides the following actions:

- **Get Affected Assets** - queries Rapid7 InsightVM to determine if you have any assets/sites affected by the specific CVE.
- **Query** - queries Rapid7 InsightVM to determine what information and scores it has for the vulnerability.
- **Add Tag** - adds a tag to an existing asset within Rapid7 insightVM.
- **Remove Tag** - removes a tag from an existing asset within Rapid7 insightVM.

The operation is compatible with CVE-type indicators and the Asset custom object type.




This integration requires the use of the Asset system object. See the [Prerequisites](#) chapter for more details.

Prerequisites


Review the following requirements before attempting to install or upgrade the operation.

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_op
```

5. Upload the **asset.json** and **install.sh** script into this new directory.
6. Create a new directory called **images** within the **rapid7_op** directory.

```
<> mkdir images
```

7. Upload the **asset.svg**.
8. Navigate to the **/tmp/rapid7_op**.

The directory should resemble the following:

- tmp
 - rapid7_op
 - 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.

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

```
<> rm -rf rapid7_op
```


Installation



The operation requires the installation of a custom object before installing the actual operation if you 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 operation. Attempting to install the operation without the custom object will cause the operation 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 zip file.
3. Extract the zip file's contents and install the Asset custom object if you are on ThreatQ version 5.9 or earlier.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the integration .whl file using one of the following methods:
 - Drag and drop the .whl file into the dialog box
 - Select **Click to Browse** to locate the .whl 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 operation 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.

The operation is now installed and will be displayed in the ThreatQ UI. 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).
3. Click on the integration entry 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.

< Rapid7 InsightVM



Disabled ☐ Enabled

Uninstall

Additional Information

Integration Type: Operation

Author: ThreatQ

Description: This plugin allows you to query Rapid7's InsightVM for affected assets and vulnerabilities

Version: 1.1.0

Required ThreatQ Version: 2.1

Works With:

☐ Indicator
CVE

☐ Vulnerability

Configuration

☐ Automatically Create Assets

Host Url

Password 

Username

☒ Verify Ssl

☐ Bypass system proxy configuration for this operation

Save

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.

Actions

The operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
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, Indicator	CVE
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

Operations

Select An Operation

Rapid7 InsightVM : get_affected_assets

Found 1 Asset(s) Vulnerable to this CVE

Asset Info

NAME	VALUE
Asset IP Address	10.12.0.101
Asset Risk Score	7355.5380859375
Asset Hostname	threatq.com
Asset ID	1
Asset Operating System	Linux 2.6.X
InsightVM Link	https://10.13.0.65:3780/site.jsp?siteid=1

Add Selected Attributes

Vulnerability Overview

NAME	VALUE
Moderate Vulnerabilities	2
Exploit Vulnerabilities	6
Total Vulnerabilities	29
Severe Vulnerabilities	22
Malware Kit Vulnerabilities	0
Critical Vulnerabilities	5

Add Selected Attributes

Scan History

Show

Successfully auto-related 1 assets to this CVE!

Please refresh the page to see new relationships

View: [threatq.com \(10.12.0.101\)](#)

Hide

Raw Response

Show

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

Query General Result Example

General Info

<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	Search	Search
<input type="checkbox"/>	CVE Description	In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent replay 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.
<input type="checkbox"/>	CVE Title	Alpine Linux: CVE-2018-1312: apache2 Multiple vulnerabilities
<input type="checkbox"/>	Rapid7 CVE ID	alpine-linux-cve-2018-1312
<input type="checkbox"/>	Category	Alpine Linux
<input type="checkbox"/>	Category	Apache
<input type="checkbox"/>	Category	Web
<input type="checkbox"/>	Date Added	2018-04-02
<input type="checkbox"/>	Date Published	2018-03-26

Add Selected Attributes

Verdict Result Example

CVE Verdicts

Showing 1 to 15 of 15

Row count: 25

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

Add Selected Attributes

Solution Result Example

Solutions

<input type="checkbox"/>	Solution	Time Needed
	<input type="text" value="Search"/>	<input type="text" value="Search"/>
<input type="checkbox"/>	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.

Action 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. <div> This will be ignored if a tag with the same name already exists.</div>

Remove Tag

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

Action 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 1.1.1 rev-a (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.
- **Version 1.1.1**
 - Optimized integration code to improve overall performance and upgraded support tier from Not Supported to ThreatQ Supported.
 - Updated the [Prerequisites](#) chapter in this user guide.
- **Version 1.1.0**
 - Initial Release