ThreatQuotient

Rapid7 InsightVM Action Guide

Version 1.0.0

May 02, 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

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.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.14.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/rapid7-insightvm-action

Introduction

Rapid7 InsightVM is a vulnerability management solution that provides three main features: fully scan the network; prioritize risks and step-by-step directions for remediation; track and communicate the progress using dashboards. This action gets the most recent list of sites that are defined in the Rapid7 InsightVM Security Console. For each site it submits the data collection containing assets to the Rapid7 InsightVM provider. The provider starts a scan for each site on the hosts that are in the list of summited assets and returns a report for each site.

The integration provides the following action:

- **Rapid7 insightVM - Scan Sites** - scans all accessible sites on a Rapid7 insightVM instance using a threat collection of assets.

The action is compatible with the Asset object type and returns enriched Report system objects.

> This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- A Rapid7 InsightVM Security Console username and password.
- An active ThreatQ TDR Orchestrator (TQO) license.
- A ThreatQ data collection containing at least one Asset that has the attribute IP Address.

> It is recommended to build the collection using the output of Rapid7 insightVM - Sites feed from the Rapid7 InsightVM CDF.

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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action file using one of the following methods:
    - Drag and drop the zip file into the dialog box
    - Select **Click to Browse** to locate the zip file on your local machine

    > ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to configure the action.

Configuration

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

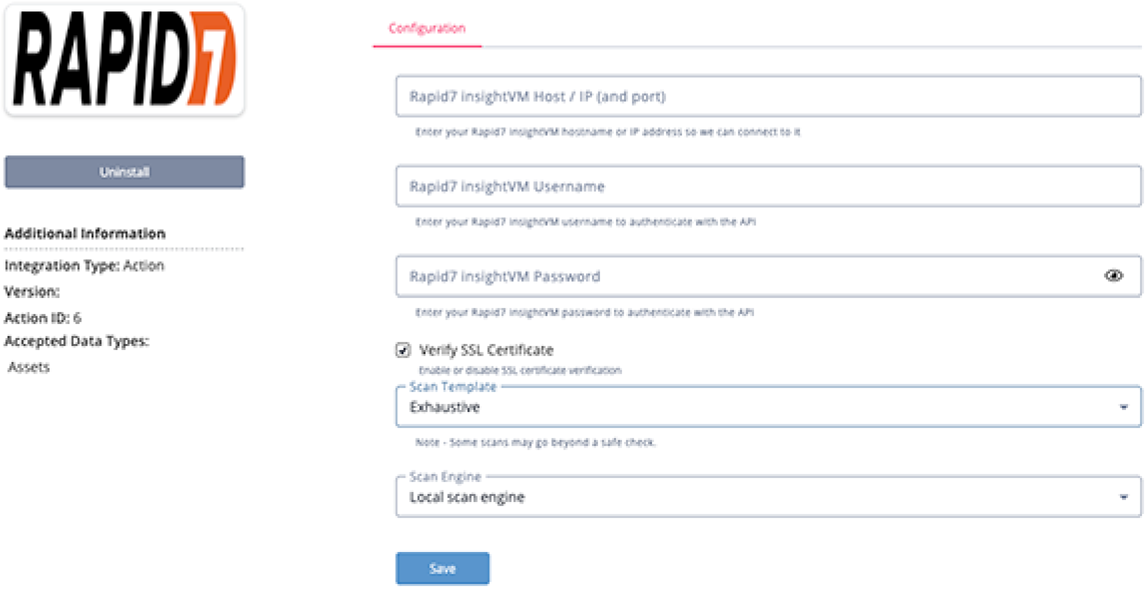
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
Host/IP: Port	Your Rapid7 insightVM instance you wish to connect.
Rapid7 InsightVM Username	Your Rapid7 InsightVM Username.
Rapid7 InsightVM Password	Your Rapid7 InsightVM Password.
Verify SSL Certificate	If checked, specifies that this connector should verify SSL connections with the Rapid7 InsightVM server
Scan Template	Select the configuration/type of scan to perform.

PARAMETER	DESCRIPTION
Scan Engine	Select the scan engine to be used.



Additional Information

Integration Type: Action

Version:

Action ID: 6

Accepted Data Types:

Assets

Rapid7 insightVM Host / IP (and port)

Enter your Rapid7 insightVM hostname or IP address so we can connect to it

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

Scan Template: Exhaustive

Note - Some scans may go beyond a safe check.

Scan Engine: Local scan engine

5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following actions are available:

FUNCTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Rapid7 InsightVM - Scan Sites	Scans all accessible sites on a Rapid7 insightVM instance using a threat collection of assets	Asset	N/A

Rapid7 InsightVM - Scan Sites

Initially, the action retrieves the most recent list of sites that are defined in the Rapid7 InsightVM Security Console. For each site, the action submits the IP Address attribute of all the assets from the data collection to Rapid7 InsightVM provider. The provider will start the scan for all the submitted IP addresses.

```
GET https://10.13.0.65:3780/api/3/sites
```

Sample Response (Truncated):

```
{
  "resources": [
    {
      "assets": 2,
      "id": 2,
      "importance": "high",
      "lastScanTime": "2023-04-18T07:40:43.082Z",
      "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"
        }
      ],
      "name": "ThreatQ Instance (ESXi)",
      "riskScore": 18116.0,
      "scanEngine": 3,
      "scanTemplate": "full-audit-without-web-spider",
      "type": "static",
      "vulnerabilities": {
        "critical": 0,
        "moderate": 10,
        "severe": 43,
        "total": 53
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.resources[].name	Report.Value	N/A	N/A	Rapid7 insightVM Site Scan(s) Started: ThreatQ Instance (ESXi)	Concatenated with `Rapid7 insightVM Site Scan(s) Started:`
.resources[].scanTemplate	Report.Attribute	Scan Template	N/A	full-audit-without-web-spider	N/A
.resources[].type	Report.Attribute	Site Type	N/A	static	N/A
.resources[].vulnerabilities.total	Report.Attribute	Total Vulnerabilities	N/A	53	N/A
.resources[].importance	Report.Attribute	Importance	N/A	High	Title-cased
.resources[].id	Report.Attribute	Site Link	N/A	https://10.13.0.65:3780/site.jsp?siteid=2	Concatenated with `host` user field

Scans

`POST https://10.13.0.65:3780/api/3/sites/{{site_id}}/scans`

POST Body

```
{
  "hosts": [
    "10.12.0.101",
    "10.13.0.12"
  ],
  "templateId": "exhaustive-audit"
}
```

Sample Response:

```
{
  "links": [
    {
      "href": "https://10.13.0.65:3780/api/3/sites/2/scans?overrideBlackout=false",
      "rel": "self"
    },
    {
      "href": "https://10.13.0.65:3780/api/3/scans/230",
      "rel": "Scan"
    }
  ],
  "id": 230
}
```

ThreatQuotient provides the following default mapping for this function:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.links[].href	Report.Description	N/A	N/A	https://10.13.0.65:3780/api/3/scans/230	If .links[].rel is Scan

Enriched Data

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

METRIC	RESULT
Run Time	1 minute
Reports	2
Report Attributes	10

Change Log

- **Version 1.0.0**
  - Initial release