

ThreatQuotient

A Securonix Company



Rapid7 insightVM Cloud CDF

Version 1.0.0

October 13, 2026

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147



ThreatQ Supported

Support

Email: tq-support@securonix.com

Web: <https://ts.securonix.com>

Phone: 703.574.9893

Contents

Warning and Disclaimer	3
Support	4
Integration Details	5
Introduction	6
Prerequisites	7
Installation	8
Configuration	9
Rapid7 insightVM Cloud - Assets	9
Rapid7 insightVM Cloud - Vulnerabilities	10
ThreatQ Mapping	12
Rapid7 InsightVM Cloud - Assets	12
Related Finding Mapping	15
Rapid7 insightVM Cloud - Vulnerabilities	16
CVSS v3 Mapping	17
Average Feed Run	19
Rapid7 insightVM Cloud - Assets	19
Rapid7 insightVM Cloud - Vulnerabilities	20
Change Log	21

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 © 2026 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: tq-support@securonix.com

Support Web: <https://ts.securonix.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	>= 6.11.0
Support Tier	ThreatQ Supported

Introduction

The Rapid7 InsightVM Cloud integration retrieves asset and vulnerability intelligence from the Rapid7 InsightVM Cloud Integration API and ingests it into ThreatQ. It helps security teams correlate asset exposure, vulnerability findings, associated CVEs, and remediation guidance with their broader threat intelligence workflows.

The integration provides the following feeds:

- **Rapid7 insightVM Cloud - Assets** - ingests matching Rapid7 assets, asset reports, associated CVE indicators, vulnerabilities, and courses of action.
- **Rapid7 insightVM Cloud - Vulnerabilities** - ingests Rapid7 vulnerability definitions and their associated CVE indicators.

The integration ingests the following system object types:

- Assets
 - Asset Attributes
- Courses of Action
 - Course of Action Attributes
- Indicators (CVEs)
- Reports
 - Report Attributes
- Tags
- Vulnerabilities
 - Vulnerability Attributes

Prerequisites

The following is required to run the integration:

- A Rapid7 Platform API key, either an organization key or user key.
- Read permission for Rapid7 InsightVM.
- The region assigned to your Rapid7 InsightVM Cloud tenant.

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 yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration yaml file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the file on your local machine
6. Select the individual feeds to install, when prompted and click **Install**.



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.

The feed(s) 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:

Rapid7 insightVM Cloud - Assets

PARAMETER	DESCRIPTION
API Region	Select the Rapid7 tenant region. Options include US, US2, EU, Canada, Australia, and Japan. Default: US.
Rapid7 Platform API Key	Required. Enter an organization or user API key with InsightVM read permissions.
Minimum Risk Score Threshold	Required. Enter a numeric risk score value. The current configuration requests assets with a risk score lower than the specified value (<code>asset.riskScore < <value></code>), so this parameter functions as an exclusive upper limit rather than a minimum threshold. The default value of 0 can exclude assets with non-negative risk scores.
Vulnerability Filter	Select one or more vulnerability severity levels to ingest. Options include Critical , Severe , and Moderate . All options are selected by default.

PARAMETER	DESCRIPTION
Only Ingest Vulnerable Assets	Select this option to exclude assets with no vulnerabilities and assets whose processed new and same vulnerability lists are empty. Default: <code>True</code> .
Include Unchanged Vulnerabilities	Select this option to include unchanged vulnerabilities. When enabled, the integration uses <code>asset.lastScanTime</code> as the source time filter and sends <code>includeSame=True</code> . When disabled, it uses <code>asset.vulnerability.firstFound</code> and sends <code>includeSame=False</code> . Default: <code>False</code> .
Verify SSL Certificate	Determines whether the integration verifies the server SSL certificate. Enabled by default.
Disable Proxies	Select this option to prevent the feed from using proxies configured in ThreatQ. Disabled by default.

Rapid7 insightVM Cloud - Vulnerabilities

PARAMETER	DESCRIPTION
API Region	Select the Rapid7 tenant region. Options include <code>US</code> , <code>US2</code> , <code>EU</code> , <code>Canada</code> , <code>Australia</code> , and <code>Japan</code> . Default: <code>US</code> .
Rapid7 Platform API Key	Required. Enter an organization or user API key with InsightVM read permissions.
Vulnerability Filter	Select one or more vulnerability severity levels to ingest. Options include Critical , Severe , and Moderate . All options are selected by default.
For Each Vulnerability Found, Return the Following	Select the vulnerability details to retrieve. Options include <code>CVSS v3 Score</code> , <code>Description</code> , <code>Reference Information</code> , and <code>Severity</code> . All options are selected by default.

PARAMETER	DESCRIPTION
Verify SSL Certificate	Determines whether the integration verifies the server SSL certificate. Enabled by default.
Disable Proxies	Select this option to prevent the feed from using proxies configured in ThreatQ. Disabled 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 Cloud - Assets

The Rapid7 InsightVM Cloud - Assets feed retrieves asset details and associated vulnerability findings from Rapid7 InsightVM. For each matching asset, the feed creates an Asset and related Report in ThreatQ.

The source response can include new, same, and remediated vulnerability arrays. The feed processes findings in the new and same arrays only. Each supported finding is ingested as a related Vulnerability and, when the finding ID contains a valid CVE, as a related CVE Indicator. Findings that include solution data also create related Courses of Action.

POST https://{api_region}.api.insight.rapid7.com/vm/v4/integration/assets

Sample Response:

```
{
  "data": [
    {
      "id": "a8bd9d81-6983-4c87-9b3a-1c58ed51b1a2",
      "ip": "198.51.100.42",
      "host_name": "app01.example.test",
      "type": "Server",
      "risk_score": 985.4,
      "total_vulnerabilities": 2,
      "new": [
        {
          "vulnerability_id": "CVE-2024-3094",
          "status": "VULNERABLE"
        }
      ],
      "same": [
        {
          "vulnerability_id": "CVE-2023-44487",
          "status": "VULNERABLE_VERSION"
        }
      ]
    }
  ],
}
```

```
"metadata": {
  "totalPages": 1
}
```

ThreatQuotient provides the following default mapping for each entry in `.data[]`.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.host_name</code> and <code>.ip</code>	Asset	Asset value	N/A	app01.example.test (198.51.100.42)	Uses <code><host_name></code> (<code><ip></code>) when <code>host_name</code> is present; otherwise uses <code>ip</code> , or <code>Unknown</code> .
Derived from vulnerability counts and <code>.last_assessed_for_vulnerabilities</code>	Asset, Report	Description	N/A	Vulnerability Overview	HTML summary includes total vulnerabilities and non-zero severity, exploit, and malware-kit counts. It is limited to 32,590 characters.
<code>.tags[].name</code>	Asset.Tag, Report.Tag	Tag	N/A	Production	Each tag name is limited to 50 characters.
<code>.tags[].type</code> and <code>.tags[].name</code>	Asset.Attribute, Report.Attribute	<code><Type></code>	N/A	Location: Production	The tag type is title-cased to form the attribute key. Custom tags remain tags but do not create attributes.
<code>.ip</code>	Asset.Attribute, Report.Attribute	IP Address	N/A	198.51.100.42	Ingested for every processed asset.
<code>.host_name</code>	Asset.Attribute, Report.Attribute	Hostname	N/A	app01.example.test	Asset attribute is conditional on a non-empty value.
<code>.id</code> and selected API region	Asset.Attribute, Report.Attribute	InsightVM Link	N/A	https://us.insight.rapid7.com/vm#/assets/a8bd...	Derived link to the InsightVM asset.
<code>.total_vulnerabilities</code>	Asset.Attribute, Report.Attribute	Total Vulnerabilities	N/A	2	Ingested as 0 when the source field is absent.
<code>.risk_score</code>	Asset.Attribute, Report.Attribute	Risk Score	N/A	985.4	Ingested as 0 when the source field is absent.
<code>.os_description</code>	Asset.Attribute, Report.Attribute	Operating System	N/A	Ubuntu Linux 22.04	Ingested when available.
<code>.id</code>	Asset.Attribute	Asset ID	N/A	a8bd9d81-...	Rapid7 asset identifier.
<code>.os_family</code>	Asset.Attribute	OS Family	N/A	Linux	Ingested when available.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.os_vendor</code>	Asset.Attribute	OS Vendor	N/A	Canonical	Ingested when available.
<code>.services[]</code>	Asset.Attribute	Installed Service	N/A	nginx - nginx - HTTPS	Concatenates non-empty vendor, product, and name values with <code>-</code> .
<code>.type</code>	Asset.Attribute	Asset Type	N/A	Server	Ingested when available.
<code>.critical_vulnerabilities</code>	Asset.Attribute	Critical Vulnerabilities	N/A	1	Ingested as 0 when absent.
<code>.severe_vulnerabilities</code>	Asset.Attribute	Severe Vulnerabilities	N/A	1	Ingested as 0 when absent.
<code>.moderate_vulnerabilities</code>	Asset.Attribute	Moderate Vulnerabilities	N/A	0	Ingested as 0 when absent.
<code>.exploits</code>	Asset.Attribute	Exploits	N/A	1	Ingested as 0 when absent.
<code>.malware_kits</code>	Asset.Attribute	Malware Kits	N/A	0	Ingested as 0 when absent.
<code>.assessed_for_vulnerabilities</code>	Asset.Attribute	Assessed for Vulnerabilities	N/A	Yes	Boolean is converted to Yes or No.
<code>.assessed_for_policies</code>	Asset.Attribute	Assessed for Policies	N/A	No	Boolean is converted to Yes or No.
<code>.last_scan_start</code>	Asset.Attribute	Last Scan Start	N/A	2026-10-01T01:00:00.000Z	Ingested when available.
<code>.last_scan_end</code>	Asset.Attribute	Last Scan End	N/A	2026-10-01T01:20:00.000Z	Ingested when available.
<code>.last_assessed_for_vulnerabilities</code>	Asset.Attribute	Last Assessed for Vulnerabilities	N/A	2026-10-01T01:20:00.000Z	Also supplies the Report published date.
<code>.mac</code>	Asset.Attribute	MAC Address	N/A	00:11:22:33:44:55	Ingested when available.
Constant value	Asset.Attribute	Hack	N/A	Yes	The current YAML always adds this attribute with the value Yes.
Derived asset name	Report	Report value	<code>.last_assessed_for_vulnerabilities</code>	Rapid7 insightVM Cloud Asset Report: <code>app01.example.test (198.51.100.42)</code>	Each processed asset creates one related Report.

Related Finding Mapping

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.cvss_v3_exploit_score	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Exploitability Score	.published	3.9	The YAML defines this same mapping twice.
.cvss_v3_impact_score	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Impact Score	.published	6.0	Ingested when present.
.cvss_v3_vector	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Vector String	.published	CVSS:3.1/AV:N/...	Ingested when present.
.cvss_v3_attack_vector	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Attack Vector	.published	NETWORK	Ingested when present.
.cvss_v3_attack_complexity	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Attack Complexity	.published	HIGH	Ingested when present.
.cvss_v3_privileges_required	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Privileges Required	.published	NONE	Ingested when present.
.cvss_v3_user_interaction	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 User Interaction	.published	NONE	Ingested when present.
.cvss_v3_scope	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Scope	.published	UNCHANGED	Ingested when present.
.cvss_v3_confidentiality_impact	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Confidentiality Impact	.published	HIGH	Ingested when present.
.cvss_v3_integrity_impact	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Integrity Impact	.published	HIGH	Ingested when present.
.cvss_v3_availability_impact	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Availability Impact	.published	HIGH	Ingested when present.
.cvss_v3_score	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Base Score	.published	10.0	Ingested when present.

Rapid7 insightVM Cloud - Vulnerabilities

The Rapid7 InsightVM Cloud - Vulnerabilities feed ingests vulnerability definitions as Vulnerability objects, relates associated CVEs as CVE Indicators, and can include selected description, severity, reference, and CVSS v3 details.

POST `https://{api_region}.api.insight.rapid7.com/vm/v4/integration/vulnerabilities`

Sample Response:

```
{
  "data": [
    {
      "id": "rapid7-cve-2024-3094",
      "description": "A malicious upstream change in xz-utils can
permit remote code execution.",
      "published": "2024-03-29T00:00:00.000Z",
      "modified": "2026-10-04T09:30:00.000Z",
      "severity": "critical",
      "severity_score": 10.0,
      "risk_score": 987.0,
      "categories": "Linux,Remote Code Execution,Supply Chain",
      "cves": "CVE-2024-3094",
      "cvss_v3_score": 10.0
    }
  ],
  "metadata": {
    "totalPages": 1
  }
}
```

ThreatQuotient provides the following default mapping for each entry in `.data[ ]`.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.id</code>	Vulnerability	Vulnerability value	N/A	rapid7-cve-2024-3094	Preserves the source value. Entries without id are skipped.
<code>.description</code>	Vulnerability	Description	N/A	A malicious upstream change...	Ingested only when Description is selected in For each vulnerability found return the following . It is limited to 32,590 characters.
<code>.categories</code>	Vulnerability Tag	Tag	N/A	Remote Code Execution	Comma-separated values are split into tags; each value is limited to 50 characters.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.cves	Related Indicator	CVE	N/A	CVE-2024-3094	Comma-separated CVE values are split into Indicators and related to the emitted Vulnerability.
.severity	Vulnerability.Attribute, Related Indicator.Attribute	Severity	N/A	critical	Ingested only when Severity is selected.
.severity_score	Vulnerability.Attribute, Related Indicator.Attribute	Severity Score	N/A	10.0	Ingested only when Severity is selected and the value is truthy.
.risk_score	Vulnerability.Attribute, Related Indicator.Attribute	Rapid7 Risk Score	N/A	987.0	Ingested whenever the value is truthy, regardless of selected data options.
.links[].href	Vulnerability.Attribute, Related Indicator.Attribute	Reference URL	.published	https://www.cve.org/CVERecord?id=CVE-2024-3094	All link URLs are ingested only when Reference Information is selected.

CVSS v3 Mapping

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.cvss_v3_exploit_score	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Exploitability Score	.published	3.9	The YAML defines this same mapping twice.
.cvss_v3_impact_score	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Impact Score	.published	6.0	Ingested when present.
.cvss_v3_vector	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Vector String	.published	CVSS:3.1/AV:N/...	Ingested when present.
.cvss_v3_attack_vector	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Attack Vector	.published	NETWORK	Ingested when present.
.cvss_v3_attack_complexity	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Attack Complexity	.published	HIGH	Ingested when present.
.cvss_v3_privileges_required	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Privileges Required	.published	NONE	Ingested when present.
.cvss_v3_user_interaction	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 User Interaction	.published	NONE	Ingested when present.
.cvss_v3_scope	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Scope	.published	UNCHANGED	Ingested when present.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.cvss_v3_confidentiality_impact	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Confidentiality Impact	.published	HIGH	Ingested when present.
.cvss_v3_integrity_impact	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Integrity Impact	.published	HIGH	Ingested when present.
.cvss_v3_availability_impact	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Availability Impact	.published	HIGH	Ingested when present.
.cvss_v3_score	Vulnerability.Attribute, Related Indicator.Attribute	CVSSv30 Base Score	.published	10.0	Ingested when present.

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 Cloud - Assets

METRIC	RESULT
Run Time	1 minute
Assets	1
Asset Attributes	26
Courses of Action	2
Course of Action Attributes	4
Indicators	2
Reports	1
Report Attributes	8
Vulnerabilities	2
Vulnerability Attributes	4

Rapid7 insightVM Cloud - Vulnerabilities

METRIC	RESULT
Run Time	1 minute
Vulnerabilities	1
CVE Indicators	2
Vulnerability Attributes	17

Change Log

- **Version 1.0.0**
 - Initial release