ThreatQuotient

Intel 471 Vulnerability Reports CDF Guide

Version 1.1.2

February 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

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	1.1.2
Compatible with ThreatQ Versions	>= 4.28.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/intel471-vulnerability-reports

Introduction

Intel471 Vulnerability Reports CDF for ThreatQ ingests a comprehensive list of Vulnerability Reports and their related Context.

The integration ingests threat intelligence data from the following endpoint:

- **Intel 471 Vulnerability Reports** - `https://api.intel471.com/v1/cve/reports`

The integration ingests the following system objects:

- Indicators
  - Indicator Attributes
- Vulnerabilities
  - Vulnerability Attributes

Important Notes

- Time constrained data fetching is possible.
- Uses basic HTTP authentication based on email address and API key.

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 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
Email Address	You Intel 471 account email address.
API Key	Your Intel 471 API Key.
Save CVE Data As	Select whether to ingest CVEs as ThreatQ Vulnerability objects, Indicator objects, or both. The default selection is Indicator objects.

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

Intel 471 Vulnerability Reports

`GET https://api.intel471.com/v1/cve/reports`

Sample Response:


```
{
   "cveReportsTotalCount":1,
   "cveReports":[
      {
         "data":{
            "cve_report":{
               "risk_level":"high",
               "name":"CVE-2018-20250",
               "activity_location":{
                  "location_opensource":true,
                  "location_underground":true
               },
               "vendor_name":"RARLab",
               "exploit_status":{
                  "available":true,
                  "productized":true
               },
               "titan_links":[
                  {
                     "title":"WinRAR CVE-2018-20250 Exploit | Spread FAST",
                     "url":"https://titan.intel471.com/post_thread/4c30f13ded0db96f789f2eeaf3d45020?
post_uid=6a29bf81f82bda975124aeb32a7074ba"
                  },
                  {
                     "title":"WINRAR EXPLOIT!! CVE 2018 20250 | FAST SPREADING| 500 MILLION USERS EXPOSED",
                     "url":"https://titan.intel471.com/post_thread/61bead81b9eee36fde5add081a3425f9?
post_uid=c63793e2625349e8f741ebc01f85f151"
                  },
                  {
                     "title":"Критическая уязвимость в WinRAR ставит под угрозу более 500 млн пользователей",
                     "url":"https://titan.intel471.com/post_thread/b81726a9d01dcb4e5734dda1f666f8b6?
post_uid=15c55952778dc4103bc04df8200c9ebc"
                  }
               ],
               "patch_status":"available",
               "poc":"observed",
               "counter_measures":"The impacted vendor released patching information for impacted products and
corresponding versions. The vendor likely addressed the vulnerability in a version update.",
               "interest_level":{
                  "disclosed_publicly":true,
                  "researched_publicly":true,
                  "exploit_sought":true
               },
               "product_name":"WinRAR",
               "cve_type":"Path traversal",
               "poc_links":[
```

```
                {
                   "title":"Exploit status ",
                   "url":" https://www.exploit-db.com/exploits/46756"
                }
             ],
             "detection":"available",
             "cvss_score":{
                "v2":6.8,
                "v3":7.8
             },
             "underground_activity_summary":"Intel 471 did not observe weaponization or productization of
CVE-2018-20250 in the underground. Intel 471 observed several actors post links to open-source articles and a PoC for
CVE-2018-20250.",
             "cve_status":"status_historical",
             "underground_activity":"observed",
             "cpe":{
                "cve_data_version":"4.0",
                "nodes":[
                   {
                      "operator":"OR",
                      "cpe_match":[
                         {
                            "vulnerable":true,
                            "cpe23Uri":"cpe:2.3:a:rarlab:winrar:*:*:*:*:*:*:*:*",
                            "versionEndIncluding":"5.61"
                         }
                      ]
                   }
                ]
             },
             "summary":"CVE-2018-20250 is a path traversal vulnerability impacting the WinRAR data compression
tool’s archive file format (ACE). A proof of concept (PoC) was observed publicly or in the underground."
          }
       },
       "last_updated":1570813574273,
       "uid":"daa5170f9d73629908d8a9170b6c3066",
       "classification":{
          "intel_requirements":[
             "2.1.2.2",
             "2.2.1"
          ]
       },
       "activity":{
          "first":1570556602000,
          "last":1570556602000
       }
    }
 ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
.cveReports[].data.uid	vulnerability.attribute/ indicator.attribute	Report UID	.cveReports[].data.cve_ report.activity.first	daa5170f9d73629908 d8a9170b6c3066
.cveReports[].data.cve_ report.name	vulnerability.value/ indicator.value	N/A	.cveReports[].data.cve_ report.activity.first	CVE-2018-20250
.cveReports[].data.cve_ report.risk_level	vulnerability.attribute/ indicator.attribute	Risk Level	.cveReports[].data.cve_ report.activity.first	low
.cveReports[].data.cve_ report.cve_type	vulnerability.attribute/ indicator.attribute	CVE Type	.cveReports[].data.cve_ report.activity.first	Path traversal
.cveReports[].data.cve_ report.vendor_name	vulnerability.attribute/ indicator.attribute	Vendor Name	.cveReports[].data.cve_ report.activity.first	Vendor Name
.cveReports[].data.cve_ report.product_name	vulnerability.attribute/ indicator.attribute	Product Name	.cveReports[].data.cve_ report.activity.first	WinRAR
.cveReports[].data.cve_ report.detection	vulnerability.attribute/ indicator.attribute	Detection	.cveReports[].data.cve_ report.activity.first	available
.cveReports[].data.cve_report. undeground_activity_summary	vulnerability.attribute/ indicator.attribute	Underground Activity Summary	.cveReports[].data.cve_ report.activity.first	Intel 471 did not observe weaponization
.cveReports[].data.cve_report.cve_status	vulnerability.attribute/ indicator.attribute	CVE Status	.cveReports[].data.cve_ report.activity.first	status_historical
.cveReports[].data.cve_report.interest _level.disclosed_publicly	vulnerability.attribute/ indicator.attribute	Disclosed Publicly	.cveReports[].data.cve_ report.activity.first	true
.cveReports[].data.cve_report.interest _level.researched_publicly	vulnerability.attribute/ indicator.attribute	Researched Publicly	.cveReports[].data.cve_ report.activity.first	true
.cveReports[].data.cve_report.interest _level.exploit_sought	vulnerability.attribute/ indicator.attribute	Exploit Sought	.cveReports[].data.cve_ report.activity.first	true
.cveReports[].data.cve_report.activity _location.location_opensource	vulnerability.attribute/ indicator.attribute	Activity Location Opensource	.cveReports[].data.cve_ report.activity.first	true
.cveReports[].data.cve_report.activity _location.location_underground	vulnerability.attribute/ indicator.attribute	Activity Location Underground	.cveReports[].data.cve_ report.activity.first	true
.cveReports[].data.cve_report.activity _location.location_private	vulnerability.attribute/ indicator.attribute	Activity Location Private	.cveReports[].data.cve_ report.activity.first	true
.cveReports[].data.cve_report.exploit _status.available	vulnerability.attribute/ indicator.attribute	Exploit Status Available	.cveReports[].data.cve_ report.activity.first	true
.cveReports[].data.cve_report.exploit _status.weaponized	vulnerability.attribute/ indicator.attribute	Exploit Status Weaponized	.cveReports[].data.cve_ report.activity.first	true
.cveReports[].data.cve_report.exploit _status.productized	vulnerability.attribute/ indicator.attribute	Exploit Status Productized	.cveReports[].data.cve_ report.activity.first	true
.cveReports[].data.cve_report.exploit _status.not_observed	vulnerability.attribute/ indicator.attribute	Exploit Status Not Observed	.cveReports[].data.cve_ report.activity.first	true
.cveReports[].data.cve_report.cvss_ score.v2	vulnerability.attribute/ i ndicator.attribute	CVSS Score V2	.cveReports[].data.cve_ report.activity.first	6.8
.cveReports[].data.cve_report.cvss_ score.v3	vulnerability.attribute/ indicator.attribute	CVSS Score v3	.cveReports[].data.cve_ report.activity.first	7.3

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
.cveReports[].data.cve_report.patch_status	vulnerability.attribute/ indicator.attribute	Patch Status	.cveReports[].data.cve_report.activity.first	available
.cveReports[].data.cve_report.underground_activity	vulnerability.attribute/ indicator.attribute	Underground activity	.cveReports[].data.cve_report.activity.first	observed
.cveReports[].data.cve_report.counter_measures	vulnerability.attribute/ indicator.attribute	POC Link Counter Measures	.cveReports[].data.cve_report.activity.first	The impact vendor released patching information for impacted product
.cveReports[].data.cve_report.summary	vulnerability.attribute/ indicator.attribute	Summary	.cveReports[].data.cve_report.activity.first	CVE-2019-5786 is a use after free vulnerability impacting Google Chrome versions
.cveReports[].data.cve_report.titan_links.title, .cveReports[].data.cve_report.titan_links.url, .cveReports[].data.cve_report.title_links.poc	vulnerability.attribute/ indicator.attribute	Titan Link Title, Titan Link URL, Titan Links POC	.cveReports[].data.cve_report.activity.first	В Google Chrome обнаружена критическая 0Day, http://some.com
.cveReports[].data.cve_report.titan_links.title, .cveReports[].data.cve_report.titan_links.url	vulnerability.attribute/ indicator.attribute	Titan Link Title, Titan Link URL	.cveReports[].data.cve_report.activity.first	
.cveReports[].data.cve_report.poc_links.title, .cveReports[].data.cve_report.poc_links.url	vulnerability.attribute/ indicator.attribute	POC Link Title, POC Link URL	.cveReports[].data.cve_report.activity.first	Chromium proof of concept
.cveReports[].data.cve_report.counter_measures_links.title, .cveReports[].data.cve_report.counter_measures_links.url	vulnerability.attribute/ indicator.attribute	Counter Measures Title, Counter Measures URL	.cveReports[].data.cve_report.activity.first	
.cveReports[].data.cve_report.patch_links.title, .cveReports[].data.cve_report.patch_links.url	vulnerability.attribute/ indicator.attribute	Patch Link Title, Patch Link URL	.cveReports[].data.cve_report.activity.first	Chrome release security fix
.cveReports[].data.cve_report.classification.intel_requirements	vulnerability.attribute/ indicator.attribute	Intel Requirements	.cveReports[].data.cve_report.activity.first	["2.1.2.1", "2.1.2.2"]
.cveReports[].data.cve_report.last_updated	vulnerability.attribute/ indicator.attribute	Last Updated At	.cveReports[].data.cve_report.activity.first	2000-01-01 21:21:21
.cveReports[].data.cve_report.activity.first	vulnerability.attribute/ indicator.attribute	Created At	.cveReports[].data.cve_report.activity.first	2000-01-01 21:21:21
.cveReports[].data.cve_report.activity.last	vulnerability.attribute/ indicator.attribute	Last Activity At	.cveReports[].data.cve_report.activity.first	2000-01-01 21:21:21
.cveReports[].data.cve_report.cpe.nodes.cpe_match.cpe23Uri, .cveReports[].data.cve_report.cpe.nodes.cpe_match.vulnerable	vulnerability.attribute/ indicator.attribute	Cpe23Uri, Vulnerability	.cveReports[].data.cve_report.activity.first	cpe:2.3:a:schben:adive:.:.:.:.:.:", true
.cveReports[].data.cve_report.cpe.nodes.children.cpe_match.cpe23Uri, .cveReports[].data.cve_report.cpe.nodes.children.cpe_match.vulnerable	vulnerability.attribute/ indicator.attribute	Cpe23Uri, Vulnerability	.cveReports[].data.cve_report.activity.first	cpe:2.3:a:schben:adive:.:.:.:.:.:", true

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.

METRIC	RESULT
Run Time	10 minutes
Indicators	569
Indicator Attributes	26,844
Vulnerabilities	759
Vulnerability Attributes	26,844

Change Log

- **Version 1.1.2**
  - Fixed a filter mapping error that would occur when the `title` for the `Poc Link Title, POC Link URL` attribute was not present.
- **Version 1.1.1**
  - Fixed a pagination bug.
- **Version 1.1.0**
  - Added 'Save CVE Data As' user configuration parameter.
- **Version 1.0.0**
  - Initial release.