ThreatQuotient

Project Zero: 0Day 'In the Wild' CDF Guide

Version 1.3.0

April 03, 2022

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

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.

Versioning

- Current integration version `1.3.0`
- Supported on ThreatQ versions >= `4.27.0`

Introduction

The Project Zero: 0day 'In the Wild' CDF consumes data from the Project Zero '0day in the wild' spreadsheet that tracks known cases of zero-day exploits found in the wild.

> ⚠ The data is provided by Project Zero as a community resource and not a "feed." There are no guarantees around the timeliness of the data provided and it may stop being maintained at any point.
>
> You should only enable this data source if you accept these limitations.

The spreadsheet can be found at:
https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY

The integration ingests the following system objects:

- Indicators
  - Indicator Attributes
- Vulnerabilities
  - Vulnerability Attributes

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 **OSINT** 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 to open its details page.
4. Enter the following parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
Ingest CVEs As	Select whether to ingest CVEs as ThreatQ Vulnerabilities, Indicators, or both. The default selection is to ingest as Vulnerability 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

The ThreatQ platform will ingest data from spreadsheet, provided in CSV format, that tracks known cases of zero-day exploits found in the wild.

```
GET https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/export?format=csv&gid=1190662839
```

Sample Response:

```
CVE,Vendor,Product,Type,Description,Date Discovered,Date Patched,Advisory,Analysis URL,Root Cause Analysis,Reported By
CVE-2022-26485,Mozilla,Firefox,Memory Corruption,Use-after-free inXSLT parameter processing,??? ,2022-03-05,https://www.mozilla.org/en-US/security/advisories/mfsa2022-09/,???,???,"Wang Gang, Liu Jialei, Du Sihang, Huang Yi & Yang Kang of 360 ATA"
CVE-2022-26486,Mozilla,Firefox,Memory Corruption,Use-after-free in WebGPU IPC Framework,???,2022-03-05,https://www.mozilla.org/en-US/security/advisories/mfsa2022-09/,???,???,"Wang Gang, Liu Jialei, Du Sihang, Huang Yi & Yang Kang of 360 ATA"
CVE-2022-0609,Google,Chrome,Memory Corruption,Use-after-free in Animation,2022-02-10,2022-02-15,https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop_14.html,???,???,Adam Weidemann and Clément Lecigne of Google's Threat Analysis Group
CVE-2022-22620,Apple,WebKit,Memory Corruption,Unspecified use-after-free,???,2022-02-10,https://support.apple.com/en-us/HT213093,???,???,???
CVE-2022-22587,Apple,iOS,Memory Corruption,Memory corruption in IOMobileFrameBuffer,???,2022-01-26,https://support.apple.com/en-us/HT213053,???,???,"Meysam Firouzi (@R00tkitSMM) of MBition - Mercedes-Benz Innovation Lab, Siddharth Aeri (@b1n4r1b01), & an anonymous reporter"
CVE-2022-21882,Microsoft,Windows,Memory Corruption,Win32k Elevation of Privilege,???,2022-01-11,https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21882,???,https://googleprojectzero.github.io/0days-in-the-wild//0day-RCAs/2022/CVE-2022-21882.html,Big CJTeam of Tianfu Cup & RyeLv (@b2ahex)
CVE-2021-42292,Microsoft,Office,Logic/Design Flaw,Excel security feature bypass,???,2021-11-09,https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42292 ,https://twitter.com/HaifeiLi/status/1486133229614616577,???,Microsoft Threat Intelligence Center (MSTIC)
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	Vulnerability.Value, Indicator.Value	CVE	sixth token	CVE-2022-26485	Vulnerability and Indicator objects are conditionally ingested depending on the value of the `Ingest CVEs As` configuration parameter.
1 (second token)	Vulnerability.Attribute, Indicator.Attribute	Vendor	sixth token	Mozilla	N/A
2 (third token)	Vulnerability.Attribute, Indicator.Attribute	Product	sixth token	Firefox	N/A
3 (fourth token)	Vulnerability.Attribute, Indicator.Attribute	Type	sixth token	Memory Corruption	N/A
4 (fifth token)	Vulnerability.Attribute, Indicator.Attribute	Description	sixth token	Use-after-free inXSLT parameter processing	N/A
5 (sixth token)	Vulnerability.Attribute, Indicator.Attribute	Date Discovered	sixth token	N/A	N/A
6 (seventh token)	Vulnerability.Attribute, Indicator.Attribute	Date Patched	sixth token	2022-03-05	N/A
7 (eighth token)	Vulnerability.Attribute, Indicator.Attribute	Advisory	sixth token	https://www.mozilla.org/en-US/security/advisories/mfsa2022-09/	N/A
8 (ninth token)	Vulnerability.Attribute, Indicator.Attribute	Analysis URL	sixth token	N/A	N/A
9 (tenth token)	Vulnerability.Attribute, Indicator.Attribute	Root Cause Analysis	sixth token	N/A	N/A
10 (eleventh token)	Vulnerability.Attribute, Indicator.Attribute	Reported by	sixth token	Wang Gang, Liu Jialei, Du Sihang, Huang Yi & Yang Kang of 360 ATA	N/A
N/A	Vulnerability.Attribute, Indicator.Attribute	Exploit Exists	sixth token	True	Will always be `True`
N/A	Vulnerability.Attribute, Indicator.Attribute	Observed as 0-day	sixth token	True	Will always be `True`

Any token starting with `???` will be discarded.

Average Feed Run

METRIC	RESULT
Run Time	< 1 minute
Indicators	205
Indicator Attributes	2,047
Vulnerabilities	205
Vulnerability Attributes	2,047

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.

Known Issues/Limitations

It is recommended that users run this integration no more than daily as the data from the provider is not updated frequently.

Change Log

- **Version 1.3.0**
  - Updated the integration to reflect changes to the CSV format by the provider.
- **Version 1.2.0**
  - Fixed an issue with data being falsely imported as Adversaries.
- **Version 1.1.0**
  - Updated the feed URL.
- **Version 1.0.0**
  - Initial release