ThreatQuotient

TeamT5 ThreatVision CDF User Guide

Version 1.0.0

September 08, 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	>= 5.6.0
Support Tier	ThreatQ Supported

Introduction

TeamT5's ThreatVision is a customer-engaged threat intelligence platform that provides real-time alerts, technical data, OSINT analysis, and in-depth APT investigations. The TeamT5 ThreatVision CDF is an integration that ingests threat intelligence from the ThreatVision Portal such as reports, samples, and other IOCs.

The integration provides the following feeds:

- **TeamT5 ThreatVision - Reports** - ingests the STIX reports from the ThreatVision API.
- **TeamT5 ThreatVision - Samples** - ingests samples submitted by users to ThreatVision.
- **TeamT5 ThreatVision - APT Weekly IOCs** - ingests hashes, network indicators, and their context from ThreatVision's APT Weekly Feed.

The integration ingests the following system objects:

- Reports
- Adversaries
- Indicators
- Malware
- Signatures
- Tool

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:

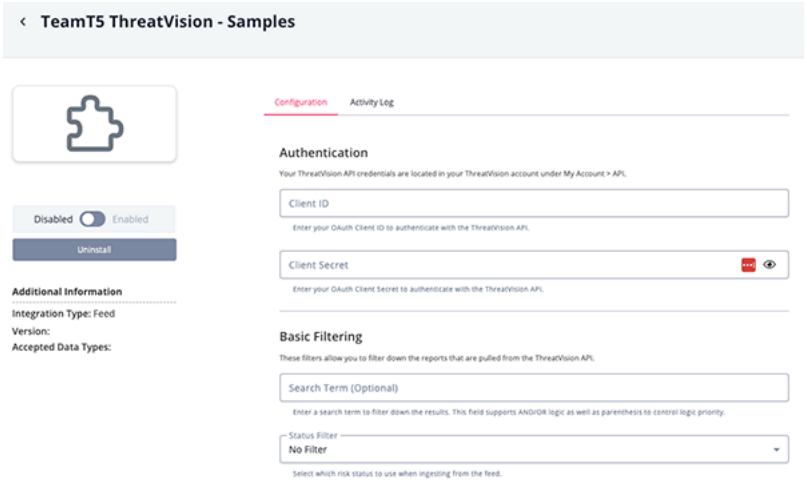
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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
Client ID	Enter your OAuth Client ID to authenticate with the ThreatVision API.
Client Secret	Enter your OAuth Client Secret to authenticate with the ThreatVision API.
Search Term *(Reports and Samples feeds only)*	Optional - Enter a search term to filter down the results. > This parameter supports AND/OR logic as well as parenthesis to control logic priority.
Report Types Filter *(Reports feed only)*	Select the report types to include. Options are: ◦ APT Campaign Tracking Reports (default) ◦ Cyber Affairs - Bi-weekly Reports (default) ◦ APTs in Asia - Monthly Reports (default) ◦ APTs in Asia - Flash Reports (default) ◦ Miscellaneous Reports (default)
Tag Filter *(Reports feed only)*	Enter a line-separated list of tags to use for filtering the reports.

PARAMETER	DESCRIPTION
Tag Mode *(Reports feed only)*	Select how the tag filter will be applied. Options include Union (OR) and Intersection (AND). The intersection option is selected by default.
Status Filter *(Samples feed only)*	Select the risk status to use when ingesting data. Options include: ◦ High Risk ◦ Medium Risk ◦ Low Risk ◦ Undetected ◦ No Filter (default)
Context Filter *(APT Weekly IOCs feed Only)*	Select the context the feed will ingest. Options include: ◦ MD5 Hash ◦ IP Address ◦ Domain ◦ Malware Family (Attribute) ◦ Target Country ◦ Target Industry ◦ SHA-256 Hash ◦ SHA-1 Hash



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

TeamT5 ThreatVision - Reports

The TeamT5 ThreatVision - Reports feed ingests the STIX reports from the ThreatVision API. The reports are filtered by the selected report types, search term, and tags.

```
GET https://api.threatvision.org/api/v1/reports
```

Sample Response:


```
{
  "success": true,
  "reports": [
    {
      "title": "Flash Report 20230414",
      "type": "flash",
      "digest": "In early April, TeamT5 detected that North Korean-nexus
APT37[^1] attacked entities in South Korea. In the attack, we identified
APT37's proprietary downloader TailDown (Sample 1).",
      "stix_url": "https://api.threatvision.org/api/v1/reports/
flash_report-20230414033309.stix",
      "pdf_url": "https://api.threatvision.org/api/v1/reports/
flash_report-20230414033309.pdf"
    },
    {
      "title": "VMRR 2023 April H1: CVE-2023-24880",
      "type": "flash",
      "digest": "The report is a sample of our upcoming new series,
\"Vulnerability Mitigation and Response Report (VMRR).\" The VMRR aims to
provide our customers with a comprehensive mitigation advisory on the most
critical vulnerabilities with our own analysis. If you are interested in
subscribing to this new report series, please contact TeamT5 for more
information.",
      "stix_url": "https://api.threatvision.org/api/v1/reports/
flash_report-20230410025354.stix",
      "pdf_url": "https://api.threatvision.org/api/v1/reports/
flash_report-20230410025354.pdf"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title`	Report Value	N/A	N/A	N/A	`VMRR 2023 April H1: CVE-2023-24880`
`.digest`	Report Description	N/A	N/A	The report is a sample of our...	N/A
`.type`	Attribute	Type	N/A	`flash`	N/A

TeamT5 ThreatVision - Samples

The TeamT5 ThreatVision - Samples feed ingests samples submitted by users to ThreatVision. Ingested metadata includes the related malware and adversaries as well as identifiers for the sample such as the SHA-256 hash and filename.

`GET https://api.threatvision.org/api/v1/samples`

Sample Response:

```
{
  "success": true,
  "samples": [
    {
      "sha256":
"9032bc51fdf9335357dca6d7131f7bb8236dec67c068f920cb46afc98af239d8",
      "filename": "2493882-0.jpg",
      "memo": null,
      "uploaded_date": 1681834433,
      "adversaries": [],
      "malwares": [],
      "url": "https://api.threatvision.org/samples/
9032bc51fdf9335357dca6d7131f7bb8236dec67c068f920cb46afc98af239d8"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.sha256`	Indicator Value	SHA-256	`.uploaded_date`	9032bc51fdf9335357dca6d7131f7bb8236dec67c068f920cb46afc98af239d8	N/A
`.filename`	Indicator Value	Filename	`.uploaded_date`	2493882-0.jpg	N/A
`.memo`	Attribute	Memo	`.uploaded_date`	N/A	N/A
`.sha256`	Attribute	ThreatVision Link	`.uploaded_date`	`https://threatvision.org/samples/9032bc51fdf9335357dca6d7131f7bb8236dec67c068f920cb46afc98af239d8`	N/A
`user_fields.risk_filter`	Attribute	Risk	`.uploaded_date`	`High`	N/A
`.malwares[]`	Attribute	Malware Family	`.uploaded_date`	N/A	N/A
`.adversaries[]`	Adversary	N/A	N/A	N/A	N/A

TeamT5 ThreatVision - APT Weekly IOCs

The TeamT5 ThreatVision - APT Weekly IOCs feed ingests hashes, network indicators, and their context from ThreatVision's APT Weekly Feed.

```
GET https://api.threatvision.org/api/v1/indicator_bundles/flash_indicators.csv
```

Sample Response:

```
hash,ip,domain,program_family,target_countries,target_industries,sha256,sha1
61402f53a8918246c791e332fb33848d,"","","",TW,Unknown,057e908cd15f95a9768989c045
5ae9a24a65c46a5022f5fa1adfe7c7a8a4b6a7,40dd7320248850588077850c2f4e9fd4ec44a951
aa756b20170aa0869d6f5d5b5f1b7c37,"",delps.scienceontheweb.net,"",KR,Think
tank,1334ef6ae02e3d0581f3ac177aec7660628e26f764ee7064d3758fc4a34e8475,371d2c652
83178192fa982671f2418c007182f3f
038c824c8394fa052fc69e30b139186c,"","",PlugX
Fast,TW,Unknown,989e56d0e9b4a7149d1a6e7ae9d04d0d8bfdf2209217d469d0ff4ea4d905547
3,78c15b34dc41189d77ba4d60e8c3bb45028cd7b7
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.hash`	Indicator Value	MD5	N/A	aa756b20170aa0869d6 f5d5b5f1b7c37	N/A
`.ip`	Indicator Value	IP Address	N/A	N/A	N/A
`.domain`	Indicator Value	FQDN	N/A	delps.scienceontheweb.net	N/A
`.program_family`	Attribute	Malware Family	N/A	`Pangolin8RAT`	N/A
`.target_countries`	Attribute	Target Country	N/A	`TW`	N/A
`.target_industries`	Attribute	Target Industry	N/A	`Healthcare`	N/A
`.sha256`	Indicator Value	SHA-256	N/A	1334ef6ae02e3d0581f3ac17 7aec7660628e26f764ee7064 d3758fc4a34e8475	N/A
`.sha1`	Indicator Value	SHA-1	N/A	371d2c65283178192fa982671 f2418c007182f3f	N/A

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.

TeamT5 ThreatVision - Reports

METRIC	RESULT
Run Time	3 minutes
Adversaries	1
Adversary Attributes	1
Indicators	1,198
Indicator Attributes	3,133
Malware	21
Malware Attributes	46
Reports	13
Report Attributes	13
Signatures	560
Signature Attributes	1,601

TeamT5 ThreatVision - Samples

METRIC	RESULT
Run Time	1 minutes
Indicators	2
Indicator Attributes	2

TeamT5 ThreatVision - APT Weekly IOCs

METRIC	RESULT
Run Time	1 minutes
Indicators	81
Indicator Attributes	96

Change Log

- **Version 1.0.0**
  - Initial release