ThreatQuotient

TeamT5 ThreatVision CDF

Version 1.1.0

November 12, 2024

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.

Copyright © 2024 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: 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	1.1.0
Compatible with ThreatQ Versions	>= 6.5.0
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 - IOC Bundles** - fetches STIX IOC bundles from the ThreatVision API.
- **TeamT5 ThreatVision - Patch Management Reports** - ingests vulnerability advisories that are produced by TeamT5.
- **TeamT5 ThreatVision - Adversaries** - ingests Adversaries that are produced by TeamT5.
- **TeamT5 ThreatVision - Malware** - ingests Malware that is produced by TeamT5.

The integration ingests the following system objects:

- Adversaries
- Attachments
- Attack Pattern
- Indicators
- Malware
- Reports
- Signatures
- Tool
- Vulnerabilities

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.

7. The feed(s) will be added to the integrations page. You will still need to configure and then enable the feed(s).

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).

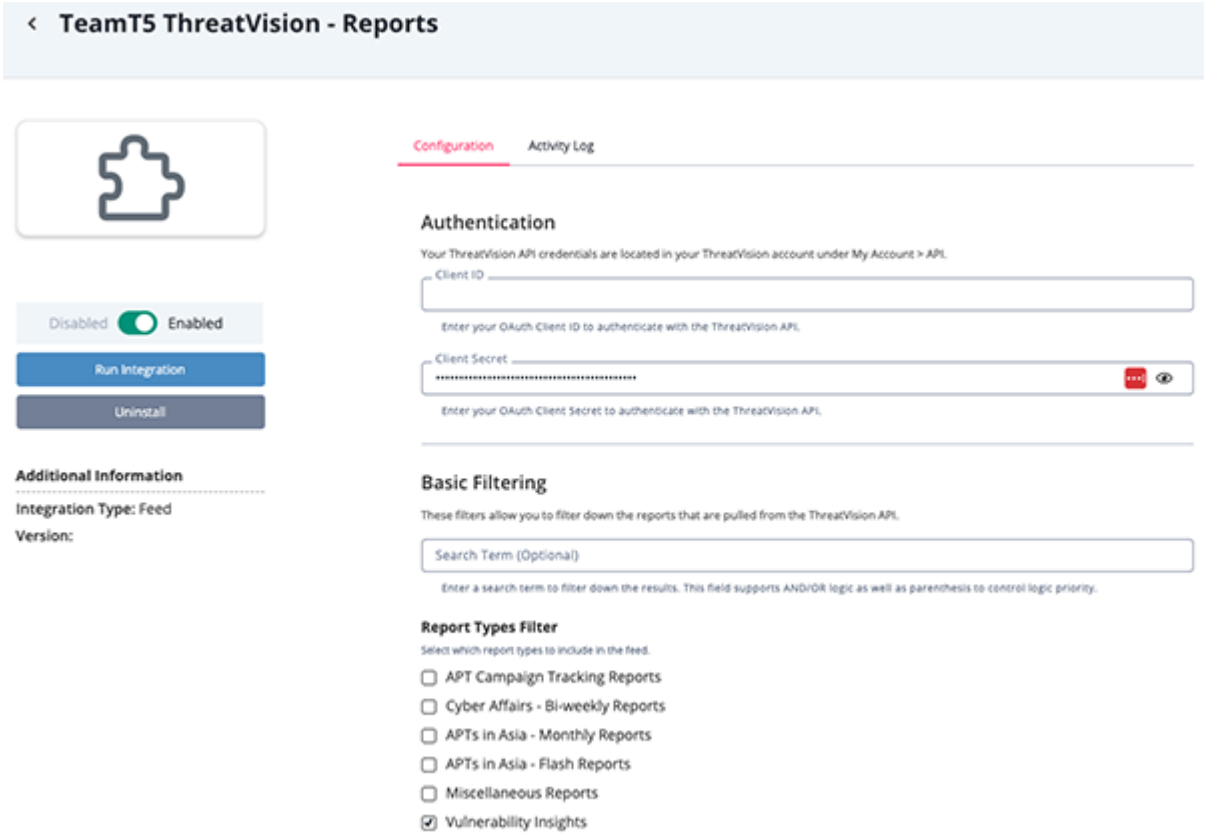
   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

TeamT5 ThreatVision - Reports Parameters

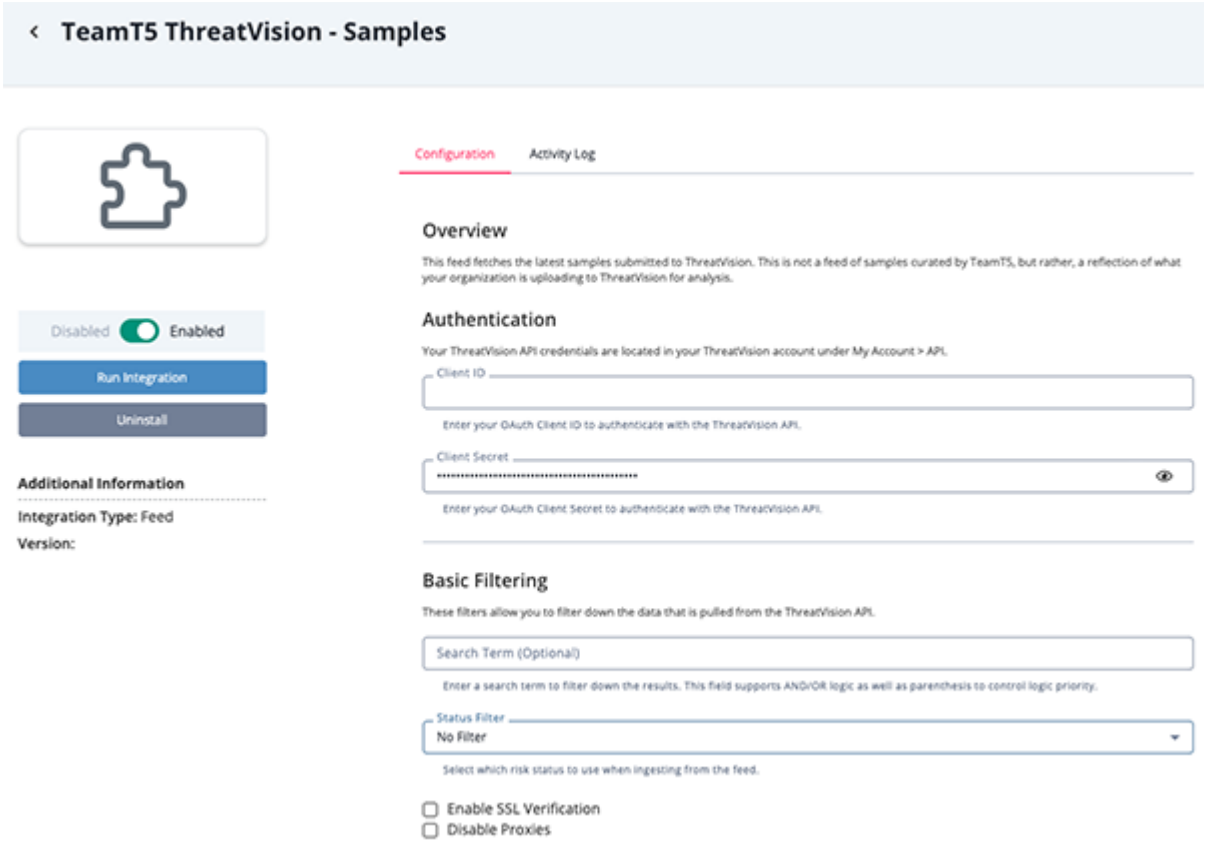
PARAMETER	DESCRIPTION
Client ID	Enter your OAuth Client ID to authenticate with the ThreatVision API.
Client Secret	Enter your OAuth Client Secret to authenticate with the ThreatVision API.
Search Term	Optional - Enter a search term to filter down the results. > This parameter supports AND/OR logic as well as parenthesis to control logic priority.
Report Types Filter	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) ◦ Vulnerability Insights (default)

PARAMETER	DESCRIPTION
Tag Filter	Enter a line-separated list of tags to use for filtering the reports.
Ingest PDF Reports	Enable this option to fetch and download the associated PDF reports with each report. This will only ingest the PDFs for scheduled runs and not manual runs.
Enable SSL Verification	Enable this for the feed to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.



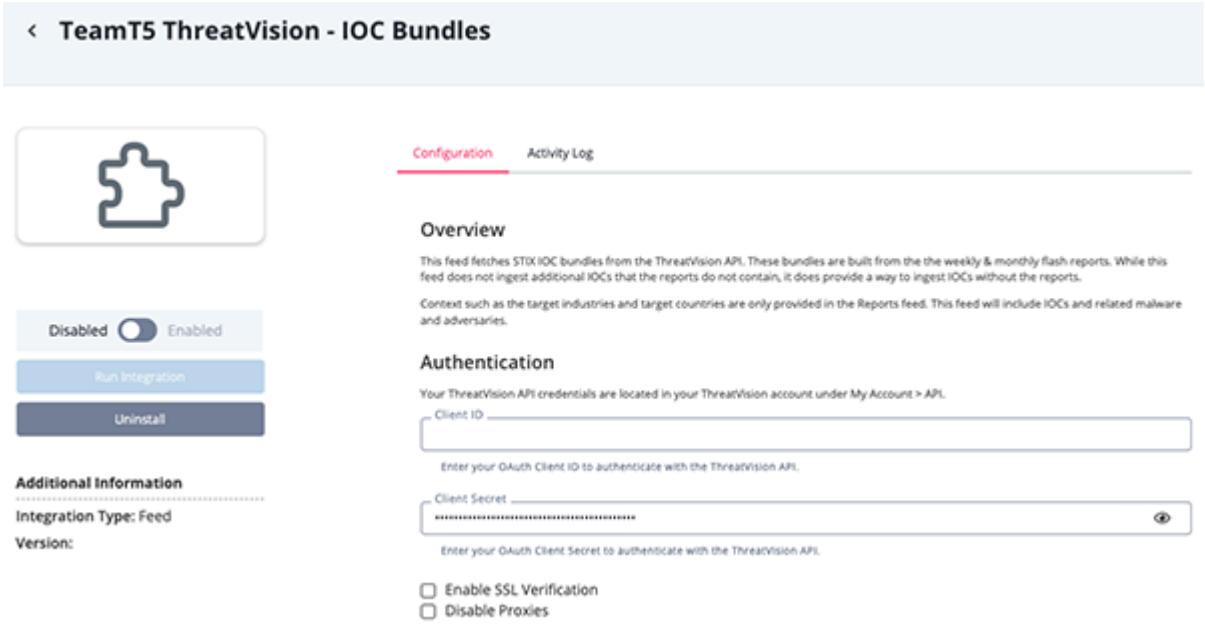
TeamT5 ThreatVision - Samples Parameters

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	Optional - Enter a search term to filter down the results.  This parameter supports AND/OR logic as well as parenthesis to control logic priority.
Status Filter	Select the risk status to use when ingesting data. Options include: ◦ High Risk ◦ Medium Risk ◦ Low Risk ◦ Undetected ◦ No Filter (default)
Enable SSL Verification	Enable this for the feed to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.



TeamT5 ThreatVision - IOC Bundles Parameters

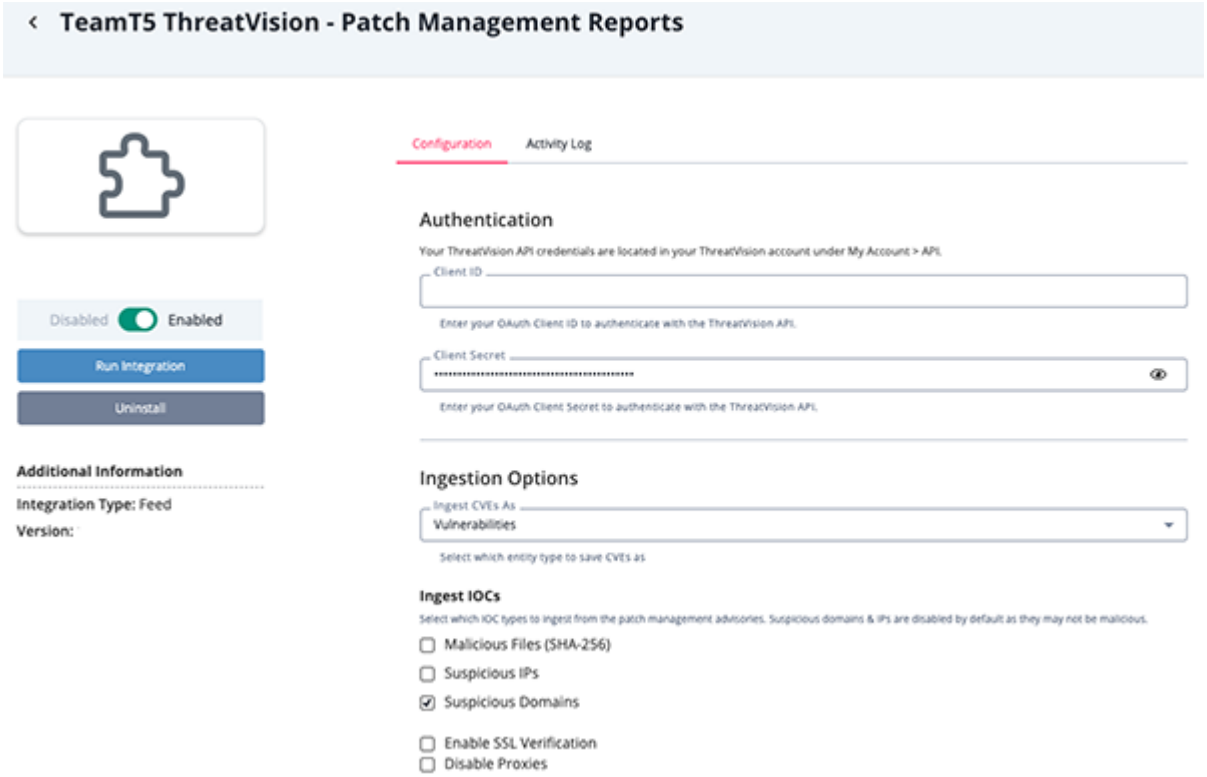
PARAMETER	DESCRIPTION
Client ID	Enter your OAuth Client ID to authenticate with the ThreatVision API.
Client Secret	Enter your OAuth Client Secret to authenticate with the ThreatVision API.
Enable SSL Verification	Enable this for the feed to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.



TeamT5 ThreatVision - Patch Management Reports Parameters

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.
Ingest CVEs As	Select which entity type to save CVEs as on the ThreatQ platform. Options include: ◦ Vulnerabilities (default) ◦ Indicators (Type: CVE)
Ingest IOCs	Select which IOC types to ingest from the patch management advisories. Options are: ◦ Malicious Files (SHA-256) (default) ◦ Suspicious IPs (default) ◦ Suspicious Domains (default)

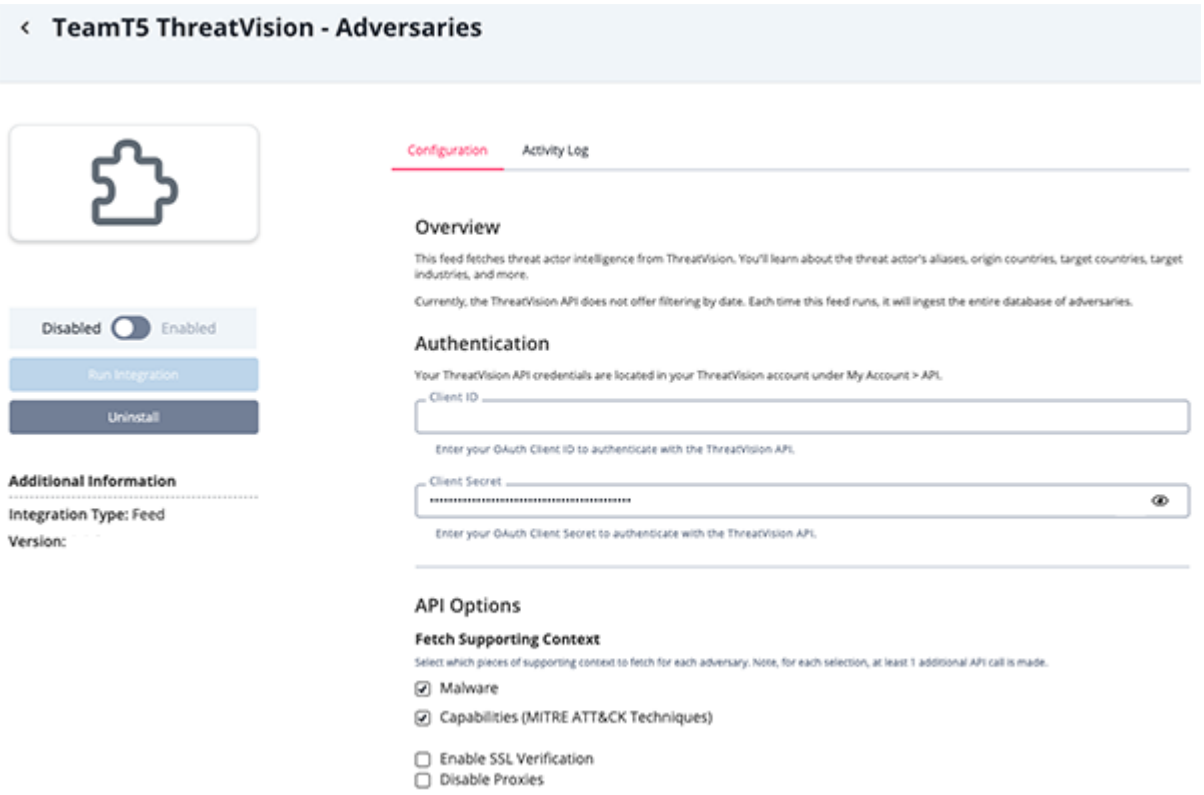
PARAMETER	DESCRIPTION
	Suspicious domains and IPs are disabled by default as they may not be malicious.
Enable SSL Verification	Enable this for the feed to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.



TeamT5 ThreatVision - Adversaries Parameters

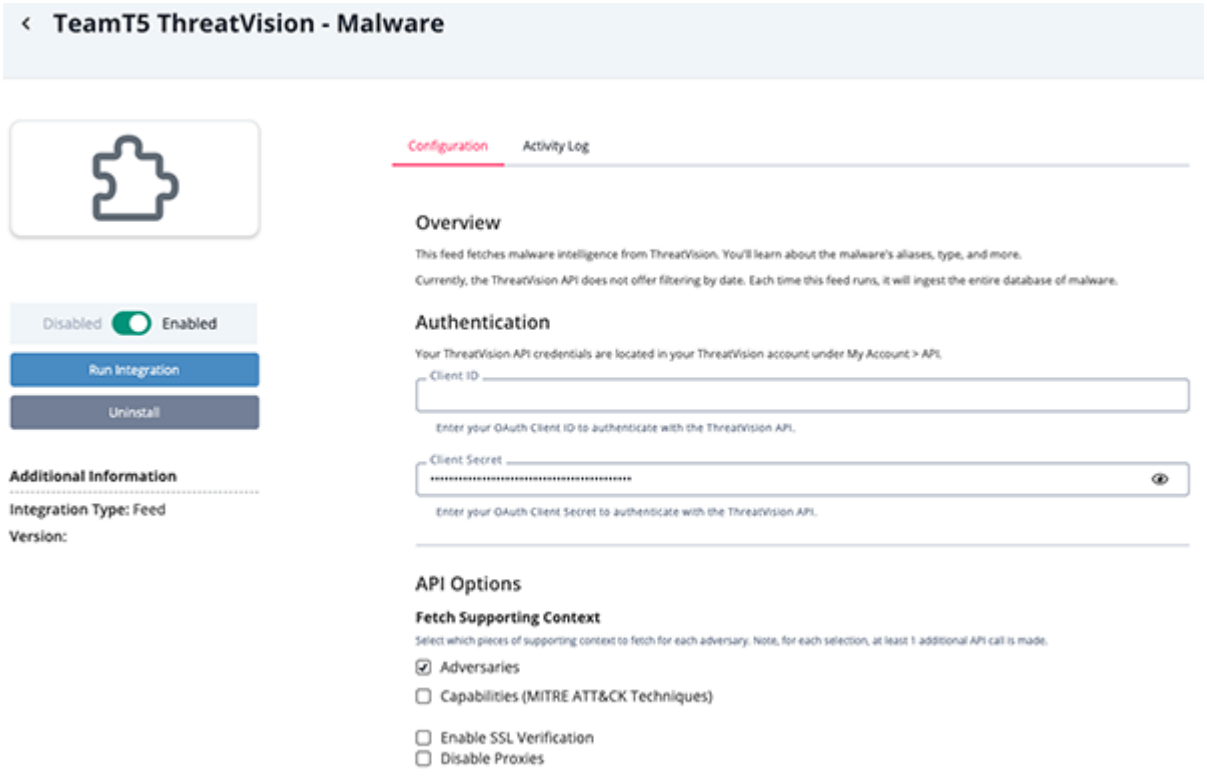
PARAMETER	DESCRIPTION
Client ID	Enter your OAuth Client ID to authenticate with the ThreatVision API.

PARAMETER	DESCRIPTION
Client Secret	Enter your OAuth Client Secret to authenticate with the ThreatVision API.
Fetch Supporting Context	Select which pieces of supporting context to fetch for each adversary. Options include: ◦ Malware ◦ Capabilities (MITRE ATT&CK Techniques) At least 1 additional API call is made for each selection.
Enable SSL Verification	Enable this for the feed to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.



TeamT5 ThreatVision - Malware Parameters

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.
Fetch Supporting Context	Select which pieces of supporting context to fetch for each adversary. Options include: ◦ Adversaries ◦ Capabilities (MITRE ATT&CK Techniques)
Enable SSL Verification	Enable this for the feed to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.



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/v2/reports`

Sample Response:


```
{
  "success": true,
  "reports": [
    {
      "title": "Flash Report 20241011 - ç¹é«”ä¸æ–‡ç‰ˆ",
      "date": 1728613800,
      "type": "flash",
      "adversaries": [],
      "malwares": ["M2Forward"],
      "targeted_countries": ["Taiwan"],
      "targeted_industries": ["Think tank"],
      "capability": ["T1606", "T1567", "T1566", "T1048"],
      "digest": "10 æœˆåˆï¼ŒTeamT5 çš„é™æ¸¬æˆªç²ä¸€èµ·é‡å°å°ç£æ™ºåº«å-
®ä½çš„é‡£éšæ”»æ“Šã€‚åœ¨é€™èµ·æ”»æ“Šä¸ï¼Œæ”»æ“Šè€…åˆ©ç”¨ Mail2000 çš„é›¶æ—¥æ¼æ´ž
T5-VUL-104083[^1] ä¾†éƒ¨ç½²æ–°çš„è³‡è¨Šç«Šå–ç¨‹å¼ M2Forwardã€‚æ ¹æ“šæˆ‘å€‘å¯é
çš„ç·šå ±ï¼Œæˆ‘å€‘æœ‰é«˜åº¦ä¿¡å¿ƒé€™èµ·æ”»æ“Šæ˜¯ä¸åœ‹è„…è¡Œå‹•è€…æ‰€ç™¼èµ·ã€‚",
      "pdf_url": "https://api.threatvision.org/api/v2/reports/
flash_report-20241009032116.pdf",
      "stix_url": "https://api.threatvision.org/api/v2/reports/
flash_report-20241009032116.stix"
    },
    {
      "title": "Flash Report 20241011",
      "date": 1728610200,
      "type": "flash",
      "adversaries": [],
      "malwares": ["M2Forward"],
      "targeted_countries": ["Taiwan"],
      "targeted_industries": ["Think tank"],
      "capability": ["T1606", "T1567", "T1566", "T1048"],
      "digest": "In early October, TeamT5â€™s telemetry intercepted a phishing
attack against a think tank in Taiwan. In the attack, the actor exploited a 0-
day vulnerability in Mail2000, T5-VUL-104083[^1], to deploy a new infostealer,
M2Forward. According to our reliable source, we hold high confidence that the
attack was launched by the Chinese actor.",
      "pdf_url": "https://api.threatvision.org/api/v2/reports/
flash_report-20241008072253.pdf",
```

```
      "stix_url": "https://api.threatvision.org/api/v2/reports/
flash_report-20241008072253.stix"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

> The mapping for this feed is based on the primary data provided by this feed. This API also provides a STIX file, which we fetch and parse using the ThreatQ STIX Parser. The STIX mappings are not included here.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title`	Report.Value	N/A	`.date`	`Flash Report 20241011`	N/A
`.digest`	Report.Description	N/A	`.date`	`In early October, TeamT5â€™s`	N/A
`.type`	Report.Attribute	Type	`.date`	`flash`	N/A
`.targeted_industries[]`	Attribute	Target Industry	`.date`	`Think tank`	Applied to report & relationships
`.targeted_countries[]`	Attribute	Target Country	`.date`	`Taiwan`	Applied to report & relationships
`.capability[]`	Attack-Pattern.Value	N/A	`.date`	`T1606 - <value>`	N/A
`.malwares[]`	Malware.Value	N/A	`.date`	`M2Forward`	N/A
`.adversaries[]`	Adversary.Value	N/A	`.date`	N/A	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.

If you would like to ingest the full analysis details, please utilize the `TeamT5 ThreatVision Action`, found on the Marketplace. This action enables the automatic enrichment of any hash within your Threat Library.

`GET https://api.threatvision.org/api/v2/samples`

Sample Response:

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

For each sample, the summary information is fetched with the following request:

`GET https://api.threatvision.org/api/v2/samples/{sha256}`

```
{
  "success": true,
  "sample": {
    "sha256":
"b266294a0412c8e79528ea222cf4bc90105584ae2f548d05093b38e6ea045650",
    "md5": "7a5fac637a6f6aac29578d69c427a2cd",
    "sha1": "93da433114992af31f2183b97f14328f2afd2645",
    "crc32": "D412656D",
    "tlshash":
"a514af35da01c434e2a302b5b26d2b7b443d0d352354b1aae3e55ae1aef49e5b13d31f",
    "ssdeep":
"3072:jyM00Fy8hVbUDwkRDRF7AzPtwvfc6zhhmN88dSEWCi4sI0yG37iZzJE:jyKhBUsCUDinc4eS8
dSzAsIzUc+",
    "risk_level": "high",
    "adversaries": [],
    "malwares": ["XLoader"],
    "file_type": "Win32 EXE",
    "size": 192512,
```

```
  "tlp": "green",
  "first_seen": 1681493828,
  "meta_timestamp": 1194567124,
  "auto_analysis": {
    "filetype": {
      "last_succeed_at": 1681493891
    },
    "file_hash": {
      "last_succeed_at": 1695863560
    },
    "pe_file": {
      "last_succeed_at": 1681494087
    },
    "yara_scan": {
      "last_succeed_at": 1695864431
    },
    "exiftool": {
      "last_succeed_at": 1681493909
    }
  },
  "related_samples": [],
  "virus_total": {
    "file_type": null,
    "tags": null,
    "positive": "/",
    "first_seen": null,
    "last_seen": null
  },
  "cuckoo_sandbox": {
    "network": [],
    "mutexes": [],
    "self_copy": [],
    "screenshot": []
  },
  "microsoft_office_meta": {
    "author": null,
    "code_page": null,
    "ole_path": [],
    "samba_strings": null,
    "created_at": null,
    "updated_at": null
  },
  "email_info": {
    "from": null,
    "to": null,
    "subject": null,
    "header": {
      "sender": null,
      "sender_ip": null,
      "received": null
```

```
      },
      "attachments": [],
      "html_object_tags": null
    },
    "file_names": [],
    "file_paths": []
  }
}
```

ThreatQuotient provides the following default mapping for this feed:

> The mapping for this feed is based on each item within the `samples` list. Indexes represent which request it came from.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`[1].sha256`	Indicator.Value	SHA-256	`.uploaded_date`	9032bc51fdf9335357dca6d7131f7bb8236dec67c068f920cb46afc98af239d8	N/A
`[1].sha1`	Indicator.Value	SHA-1	`.uploaded_date`	93da433114992af31f2183b97f14328f2afd2645	N/A
`[1].md5`	Indicator.Value	MD5	`.uploaded_date`	7a5fac637a6f6aac29578d69c427a2cd	N/A
`[1].sha256`	Indicator.Value	SHA-256	`.uploaded_date`	9032bc51fdf9335357dca6d7131f7bb8236dec67c068f920cb46afc98af239d8	N/A
`[0].filename`	Indicator.Value	Filename	`.uploaded_date`	2493882-0.jpg	N/A
`[1].sha256`	Indicator.Attribute	ThreatVision Link	`.uploaded_date`	`https://threatvision.org/samples/9032bc51fdf9335357dca6d7131f7bb8236dec67c068f920cb46afc98af239d8`	N/A
`[1].malwares[]`	Indicator.Attribute	Malware Family	`.uploaded_date`	N/A	N/A
`[1].adversaries[]`	Adversary.Value	N/A	`.uploaded_date`	N/A	N/A
`[1].risk_level`	Indicator.Attribute	Risk	`.uploaded_date`	`High`	N/A

TeamT5 ThreatVision - IOC Bundles

The TeamT5 ThreatVision - IOC Bundles feed ingests hashes, domains, IPs, and other IOCs that are produced from TeamT5's weekly & monthly reports.

> The indicators ingested by this feed will also be ingested if you have the `TeamT5 ThreatVision - Reports` feed enabled. Use this feed if you are not using the Reports feed and/or only care about the indicators.

`GET https://api.threatvision.org/api/v2/ioc_bundles`

Sample Response:


```
{
  "success": true,
  "ioc_bundles": [
    {
      "id": "Q2FzZUZpbGUvMTQ3MzQ=",
      "name": "Flash Report 20241011",
      "type": "Report IoC List",
      "created_at": 1728610200,
      "stix_url": "https://api.threatvision.org/api/v2/ioc_bundles/
Q2FzZUZpbGUvMTQ3MzQ=.stix"
    },
    {
      "id": "Q2FzZUZpbGUvMTQ3MzE=",
      "name": "Monthly Report 2024 October",
      "type": "Report IoC List",
      "created_at": 1728545249,
      "stix_url": "https://api.threatvision.org/api/v2/ioc_bundles/
Q2FzZUZpbGUvMTQ3MzE=.stix"
    },
    {
      "id": "Q2FzZUZpbGUvMTQ3Mjk=",
      "name": "Flash Report 20241010",
      "type": "Report IoC List",
      "created_at": 1728523875,
      "stix_url": "https://api.threatvision.org/api/v2/ioc_bundles/
Q2FzZUZpbGUvMTQ3Mjk=.stix"
    },
    {
      "id": "Q2FzZUZpbGUvMTQ2ODg=",
      "name": "Flash Report 20241004",
      "type": "Report IoC List",
      "created_at": 1728009407,
      "stix_url": "https://api.threatvision.org/api/v2/ioc_bundles/
Q2FzZUZpbGUvMTQ2ODg=.stix"
    },
    {
```

```
      "id": "Q2FzZUZpbGUvMTQ2NzM=",
      "name": "Flash Report 20241003",
      "type": "Report IoC List",
      "created_at": 1727920833,
      "stix_url": "https://api.threatvision.org/api/v2/ioc_bundles/
Q2FzZUZpbGUvMTQ2NzM=.stix"
    },
    {
      "id": "Q2FzZUZpbGUvMTQ2NjM=",
      "name": "VIR 2024 September H2: T5-VUL-104083",
      "type": "Report IoC List",
      "created_at": 1727763922,
      "stix_url": "https://api.threatvision.org/api/v2/ioc_bundles/
Q2FzZUZpbGUvMTQ2NjM=.stix"
    },
    {
      "id": "Q2FzZUZpbGUvMTQ2MzE=",
      "name": "Flash Report 20240927",
      "type": "Report IoC List",
      "created_at": 1727405760,
      "stix_url": "https://api.threatvision.org/api/v2/ioc_bundles/
Q2FzZUZpbGUvMTQ2MzE=.stix"
    },
    {
      "id": "Q2FzZUZpbGUvMTQ2MjI=",
      "name": "Flash Report 20240926",
      "type": "Report IoC List",
      "created_at": 1727320200,
      "stix_url": "https://api.threatvision.org/api/v2/ioc_bundles/
Q2FzZUZpbGUvMTQ2MjI=.stix"
    },
    {
      "id": "Q2FzZUZpbGUvMTQ1ODU=",
      "name": "Flash Report 20240920",
      "type": "Report IoC List",
      "created_at": 1726799967,
      "stix_url": "https://api.threatvision.org/api/v2/ioc_bundles/
Q2FzZUZpbGUvMTQ1ODU=.stix"
    },
    {
      "id": "Q2FzZUZpbGUvMTQ1NzI=",
      "name": "Flash Report 20240919",
      "type": "Report IoC List",
      "created_at": 1726714871,
      "stix_url": "https://api.threatvision.org/api/v2/ioc_bundles/
Q2FzZUZpbGUvMTQ1NzI=.stix"
    },
    {
      "id": "Q2FzZUZpbGUvMTQ1NTM=",
      "name": "VIR 2024 September H1: CVE-2024-7593",
```

```
      "type": "Report IoC List",
      "created_at": 1726482360,
      "stix_url": "https://api.threatvision.org/api/v2/ioc_bundles/
Q2FzZUZpbGUvMTQ1NTM=.stix"
    },
    {
      "id": "Q2FzZUZpbGUvMTQ1Mzg=",
      "name": "Flash Report 20240913",
      "type": "Report IoC List",
      "created_at": 1726195315,
      "stix_url": "https://api.threatvision.org/api/v2/ioc_bundles/
Q2FzZUZpbGUvMTQ1Mzg=.stix"
    },
    {
      "id": "Q2FzZUZpbGUvMTQ1MjU=",
      "name": "Flash Report 20240912",
      "type": "Report IoC List",
      "created_at": 1726111530,
      "stix_url": "https://api.threatvision.org/api/v2/ioc_bundles/
Q2FzZUZpbGUvMTQ1MjU=.stix"
    },
    {
      "id": "Q2FzZUZpbGUvMTQ1MDU=",
      "name": "Monthly Report 2024 September",
      "type": "Report IoC List",
      "created_at": 1725953309,
      "stix_url": "https://api.threatvision.org/api/v2/ioc_bundles/
Q2FzZUZpbGUvMTQ1MDU=.stix"
    },
    {
      "id": "Q2FzZUZpbGUvMTQ0ODM=",
      "name": "Flash Report 20240906",
      "type": "Report IoC List",
      "created_at": 1725593315,
      "stix_url": "https://api.threatvision.org/api/v2/ioc_bundles/
Q2FzZUZpbGUvMTQ0ODM=.stix"
    },
    {
      "id": "Q2FzZUZpbGUvMTQ0NzM=",
      "name": "Flash Report 20240905",
      "type": "Report IoC List",
      "created_at": 1725508920,
      "stix_url": "https://api.threatvision.org/api/v2/ioc_bundles/
Q2FzZUZpbGUvMTQ0NzM=.stix"
    }
  ]
}
```


For each of the IOC bundles, the feed will fetch the STIX file and parse the IOCs from the STIX file.

```
GET https://api.threatvision.org/api/v2/ioc_bundles/{id}.stix
```

Sample Response:


```
{
  "type": "bundle",
  "id": "bundle--63616333-6236-4961-a661-393264623461",
  "objects": [
    {
      "spec_version": "2.1",
      "type": "indicator",
      "name": "hash: fdd3c00b63c356f9b73f034898aa3dbe",
      "description": "",
      "valid_from": "2024-09-15T06:36:15.3Z",
      "pattern_type": "stix",
      "pattern": "[file:hashes.md5 = 'fdd3c00b63c356f9b73f034898aa3dbe' OR
file:hashes.sha1 = 'fa78de28ead9b01c8bd5a91c48a62336b94c0d8c' OR
file:hashes.sha256 =
'03dd55afbd770c167df3f9d6d73152bf5f0a921f72bfcd7b6bcce9dd7f902048']",
      "id": "indicator--33666233-6630-4932-b936-306263666536",
      "created": "2024-10-11T01:30:00.000Z",
      "modified": "2024-10-11T01:30:20.036Z"
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this feed:

> The mapping for this feed is based on the ThreatQ native STIX parser. Documentation & mappings can be found in the ThreatQ Help Center.

TeamT5 ThreatVision - Patch Management Reports

The TeamT5 ThreatVision - Patch Management Reports feed ingests vulnerability advisories that are produced by TeamT5. These advisory reports will detail the vulnerability, corresponding CVE, and any other relevant information such as CVSS score, affected products, and remediation steps.

```
GET https://api.threatvision.org/api/v2/vulnerability/advisory_lists
```

Sample Response:


```
{
  "success": true,
  "advisories": [
    {
      "identification": "CVE-2024-43047",
      "release_date":1727827204,
      "report_urls": null,
      "is_new": true,
      "vendor": "Qualcomm",
      "product": "Multiple Chipsets ",
      "product_list": [],
      "cvss": 7.8,
      "cvss_vector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H",
      "description": {
        "title": null,
        "detail": "Multiple Qualcomm chipsets contain a use-after-free
vulnerability due to memory corruption in DSP Services while maintaining memory
maps of HLOS memory. "
      },
      "threat_level": "HIGH",
      "poc": [],
      "publicly_disclosed": false,
      "updated_at": 1728428472,
      "patch": "Apply remediations or mitigations per vendor instructions or
discontinue use of the product if remediation or mitigations are unavailable.",
      "references": [
        "https://docs.qualcomm.com/product/publicresources/securitybulletin/
october-2024-bulletin.html"
      ],
      "malicious_files": null,
      "suspicious_domains": null,
      "suspicious_ips": null,
      "exploited": true
    },
    {
      "identification": "CVE-2024-43572",
      "report_urls": [],
      "is_new": true,
      "vendor": "Microsoft",
      "product": "Windows",
```

```
      "product_list": [
        "Windows 10 Version 1809 for 32-bit Systems",
        "Windows 10 Version 1809 for x64-based Systems",
        "Windows Server 2019",
        "Windows Server 2019 (Server Core installation)",
        "Windows Server 2022",
        "Windows Server 2022 (Server Core installation)",
        "Windows 11 version 21H2 for x64-based Systems",
        "Windows 11 version 21H2 for ARM64-based Systems",
        "Windows 10 Version 21H2 for 32-bit Systems",
        "Windows 10 Version 21H2 for ARM64-based Systems",
        "Windows 10 Version 21H2 for x64-based Systems",
        "Windows 11 Version 22H2 for ARM64-based Systems",
        "Windows 11 Version 22H2 for x64-based Systems",
        "Windows 10 Version 22H2 for x64-based Systems",
        "Windows 10 Version 22H2 for ARM64-based Systems",
        "Windows 10 Version 22H2 for 32-bit Systems",
        "Windows 11 Version 23H2 for ARM64-based Systems",
        "Windows 11 Version 23H2 for x64-based Systems",
        "Windows Server 2022, 23H2 Edition (Server Core installation)",
        "Windows 11 Version 24H2 for ARM64-based Systems",
        "Windows 11 Version 24H2 for x64-based Systems",
        "Windows 10 for 32-bit Systems",
        "Windows 10 for x64-based Systems",
        "Windows 10 Version 1607 for 32-bit Systems",
        "Windows 10 Version 1607 for x64-based Systems",
        "Windows Server 2016",
        "Windows Server 2016 (Server Core installation)",
        "Windows Server 2008 for 32-bit Systems Service Pack 2",
        "Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core
installation)",
        "Windows Server 2008 for x64-based Systems Service Pack 2",
        "Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core
installation)",
        "Windows Server 2008 R2 for x64-based Systems Service Pack 1",
        "Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server
Core installation)",
        "Windows Server 2012",
        "Windows Server 2012 (Server Core installation)",
        "Windows Server 2012 R2",
        "Windows Server 2012 R2 (Server Core installation)"
      ],
      "cvss": 7.8,
      "cvss_vector": "CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H",
      "description": {
        "title": "Microsoft Management Console Remote Code Execution
Vulnerability",
        "detail": "Microsoft Windows Management Console contains unspecified
vulnerability that allows for remote code execution."
      },
```

```
      "threat_level": "HIGH",
      "poc": [],
      "publicly_disclosed": true,
      "updated_at": 1728428411,
      "patch": "Affected Versions:\n10.0.17763.6414 10.0.20348..2762
10.0.22000.3260 10.0.19044.5011 10.0.22621.4317 10.0.19045.5011 10.0.22631.4317
10.0.25398.1189 10.0.26100.2033 10.0.10240.20796 10.0.14393.7428 6.0.6003.22918
6.0.6003.22918 6.1.7601.27366 6.1.7601.27366 6.2.9200.25118
6.3.9600.22221\nMore details can be found at: https://msrc.microsoft.com/
update-guide/vulnerability/CVE-2024-43572\n",
      "references": [
        "https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572"
      ],
      "malicious_files": [
        "6be4dd9af27712f5ef6dc7d684e5ea07fa675b8cbed3094612a6696a40c664ce",
        "77373a220e74824d641faac62c6b82835935f94254bd663b060bb3885746aa6d",
        "ca05513c365c60a8fdabd9e21938796822ecda03909b3ee5f12eb82fefa34d84",
        "eae187a91f97838dbb327b684d6a954beee49f522a829a1b51c1621218039040",
        "f1d519f43c36e24a89b351f00059a1bdb9afc2a339f7301117babb484e2cc555",
        "fb640cfb9a86b9dc6806b048c6a88ef6ff546ca830a147322b4e3a3646b70942"
      ],
      "suspicious_domains": ["lokjopppkuimlpo.shop"],
      "suspicious_ips": [],
      "exploited": true
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this feed:

> The mapping for this feed is based on each item within the samples list. Indexes represent which request it came from.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`[1].description.title`	Vulnerability.Value	N/A	`.release_date`	CVE-2024-43047	N/A
`[1].identification`	Indicator.Value / Vulnerability.Value	CVE	`.release_date`	CVE-2024-43047	N/A
`[1].exploited`	Tag.Value	N/A	N/A	Exploited	N/A
`[1].malicious_files`	Related Indicator.Value	SHA-256	`.release_date`	6be4dd9af27712f5ef6dc7d684e5ea07fa675b8cbed3094612a6696a40c664ce	N/A
`[1].suspicious_ips`	Related Indicator.Value	IP Addresses	`.release_date`	N/A	N/A
`[1].suspicious_domains`	Related Indicator.Value	FQDN	`.release_date`	lokjopppkuimlpo.shop	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`[1].report_urls`	Related Reports	N/A	N/A	N/A	We use the stix parser to ingest the data
`[1].cvss`	Indicator/ Vulnerability.Attribute	CVSS Score	`.release_date`	7.8	Updatable
`[1].cvss_vector`	Indicator/ Vulnerability.Attribute	CVSS Vector String	`.release_date`	CVSS:3.1/AV:L/ AC:L/P R:L/UI:N/S:U/C:H/ I:H/A:H	N/A
`[1].threat_level`	Indicator/ Vulnerability.Attribute	Threat Level	`.release_date`	High	Updatable
`[1].product`	Indicator/ Vulnerability.Attribute	Affected Product	`.release_date`	Windows	N/A
`[1].vendor`	Indicator/ Vulnerability.Attribute	Affected Vendor	`.release_date`	Microsoft	N/A
`[1].publicly_disclosed`	Indicator/ Vulnerability.Attribute	Is Publicly Disclosed	`.release_date`	True	Updatable
`[1].exploited`	Indicator/ Vulnerability.Attribute	Exploited	`.release_date`	True	Updatable

TeamT5 ThreatVision - Adversaries

The TeamT5 ThreatVision - Adversaries feed fetches threat actor intelligence from ThreatVision. You'll learn about the threat actor's aliases, origin countries, target countries, target industries, and more.

> Currently, the ThreatVision API does not offer filtering by date. Each time this feed runs, it will ingest the entire database of adversaries.

`GET https://api.threatvision.org/api/v2/adversaries`

Sample Response:


```
{
  "success": true,
  "adversaries": [
    {
      "name": "Amoeba",
      "aliases": [
        "Winnti",
        "APT41",
        "Barium",
        "Wicked Panda",
        "Earth Baku",
        "Double Dragon"
      ],
      "origin_countries": ["China"],
      "targeted_countries": [
        "Taiwan",
        "Japan",
        "South Korea",
        "United States of America",
        "Thailand",
        "Singapore",
        "India",
        "Malaysia",
        "Hong Kong",
        "China"
      ],
      "targeted_industries": [
        "Media",
        "Education",
        "Energy",
        "Government",
        "Critical Infrastructure",
        "Telecommunication",
        "Gambling",
        "Semiconductor",
        "Financial Institution",
        "Healthcare",
```

```
        "Aerospace",
        "Manufacturing",
        "Gaming",
        "Chemicals",
        "Information Technology"
      ],
      "overview": "Amoeba is a Chinese adversary group widely known as
â€œWinnti,â€ named after one of its most infamous RATs. Although the Amoeba
group is best known for its preference for attacking gaming industry, it has
now expanded its scope to other sectors including telecommunication, chemistry,
pharmacy, aviation, etc. In 2020, the U.S. government indicted five Amoeba
actors, pointing out that the group has strong connections with China's
Ministry of State Security (MSS), the top intelligence agency of the Chinese
government. "
    }
  ]
}
```


Depending on your user-field selection, and which supporting context you have enabled, the feed will make additional API requests to fetch relational data for each adversary.

Fetching Related Malware

```
GET https://api.threatvision.org/api/v2/adversaries/{adversary_name}/malwares
```


```
{
  "success": true,
  "id": "Polaris",
  "malwares": [
    {
      "name": "TVLoad",
      "aliases": [],
      "type": "Loader",
      "attribution": "Polaris",
      "overview": "TVLoad is a loader used by the Chinese APT group Polaris.
The loader usually use the path \"%Public%\\Libraries\" for persistence and
load the embedded AES-encrypted RAT. It was observed to load CobaltStrike
Stager and NoFive. This name comes from that it usually create a directory with
string \"tv\"."
    },
    {
      "name": "CobaltStrike Beacon",
      "aliases": [],
      "type": "RAT",
      "attribution": "shared",
      "overview": "CobaltStrike Beacon is the payload of Cobalt Strike, a
commercial penetration testing software used by various red teams, ethical
hackers, and threat actors. It is highly customizable with features such as key
logging, file transfer, SOCKS proxying, privilege escalation, and mimikatz.
CobaltStrike is a legitimate tool used by ethical hackers as well as cyber
arsenal used by threat actors to launch real attacks against companies and
organizations."
```

```
    }
  ]
}
```

Fetching Related Capabilities (MITRE ATT&CK Techniques)

`GET https://api.threatvision.org/api/v2/adversaries/{adversary_name}/capabilities`


```
{
  "success": true,
  "id": "Polaris",
  "techniques": [
    {
      "main_value": "T1005",
      "name": "Data from Local System",
      "description": "Adversaries may search local system sources, such as file systems and configuration files or local databases, to find files of interest and sensitive data prior to Exfiltration.\n\nAdversaries may do this using a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), such as [cmd](https://attack.mitre.org/software/S0106) as well as a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008), which have functionality to interact with the file system to gather information.(Citation: show_run_config_cmd_cisco) Adversaries may also use [Automated Collection](https://attack.mitre.org/techniques/T1119) on the local system.\n",
      "last_modified": 1681343679,
      "published_at": 1496266220,
      "version": "1.6",
      "tactics": [
        {
          "tactic_name": "Collection",
          "tactic_serial": "TA0009"
        }
      ],
      "sub_techniques": []
    },
    {
      "main_value": "T1008",
      "name": "Fallback Channels",
      "description": "Adversaries may use fallback or alternate communication channels if the primary channel is compromised or inaccessible in order to maintain reliable command and control and to avoid data transfer thresholds.",
      "last_modified": 1594756187,
      "published_at": 1496266221,
      "version": "1.0",
      "tactics": [
        {
          "tactic_name": "Command and Control",
          "tactic_serial": "TA0011"
        }
      ],
```

```
      "sub_techniques": []
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

> The mapping for this feed is based on each item within the corresponding list keys returned by the API. Indexes represent which request it came from.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`[0].name`	Adversary.Name	N/A	N/A	`Polaris`	N/A
`[0].overview`	Adversary.Description	N/A	N/A	N/A	N/A
`[0].aliases[]`	Adversary.Attribute	Alias	N/A	`APT1`	N/A
`[0].origin_countries[]`	Adversary.Attribute	Origin Country	N/A	`North Korea`	N/A
`[0].targeted_countries[]`	Adversary.Attribute	Target Country	N/A	`Taiwan`	N/A
`[0].targeted_industries[]`	Adversary.Attribute	Target Industry	N/A	`Education`	N/A
`[1].name`	Malware.Value	N/A	N/A	`Amoeba`	User-configurable
`[1].overview`	Malware.Description	N/A	N/A	N/A	User-configurable
`[1].aliases[]`	Malware.Attribute	Alias	N/A	N/A	User-configurable
`[1].type`	Malware.Attribute	Malware Type	N/A	`RAT`	User-configurable
`[2].main_value`, `[2].name`	Attack-Pattern.Value	N/A	N/A	`T1008 - Fallback Channels`	User-configurable
`[2].tactics[].tactic_name`	Attack-Pattern.Attribute	Tactic	`Reconnaissance`	N/A	User-configurable
`[2].overview`	Attack-Pattern.Description	N/A	N/A	N/A	User-configurable

TeamT5 ThreatVision - Malware

The TeamT5 ThreatVision - Malware feed etches malware intelligence from ThreatVision. You'll learn about the malware's aliases, type, and more.

> ⚠ Currently, the ThreatVision API does not offer filtering by date. Each time this feed runs, it will ingest the entire database of malware.

`GET https://api.threatvision.org/api/v2/malwares`

Sample Response:


```
{
  "success": true,
  "malwares": [
    {
      "name": "ChatLoader",
      "aliases": [],
      "type": "Loader",
      "attribution": "Amoeba",
      "overview": "ChatLoader is a loader which has many functionalities, like
ETW bypass, dll hollwing. The name \"chat\" loader is named from the ChaCha20
algorithm which chatloader used to decrypt the payload."
    },
    {
      "name": "RevbShell",
      "aliases": [],
      "type": "RAT",
      "attribution": "shared",
      "overview": "RevbShell is a Visual Basic Script based open source remote
administration tool. Its client will connect to a python based server and fetch
commands periodically. "
    }
  ]
}
```


Depending on your user-field selection, and which supporting context you have enabled, the feed will make additional API requests to fetch relational data for each malware.

Fetching Related Adversaries

`GET https://api.threatvision.org/api/v2/malware/{malware_name}/adversaries`


```
{
  "success": true,
  "id": "ChatLoader",
  "adversaries": [
    {
      "name": "Amoeba",
      "aliases": [
        "Winnti",
```

```
        "APT41",
        "Barium",
        "Wicked Panda",
        "Earth Baku",
        "Double Dragon"
      ],
      "origin_countries": ["China"],
      "targeted_countries": [
        "Taiwan",
        "Japan",
        "South Korea",
        "United States of America",
        "Thailand",
        "Singapore",
        "India",
        "Malaysia",
        "Hong Kong",
        "China"
      ],
      "targeted_industries": [
        "Media",
        "Education",
        "Energy",
        "Government",
        "Critical Infrastructure",
        "Telecommunication",
        "Gambling",
        "Semiconductor",
        "Financial Institution",
        "Healthcare",
        "Chemical",
        "Aerospace",
        "Manufacturing",
        "Gaming",
        "Information Technology"
      ],
      "overview": "Amoeba is a Chinese adversary group widely known as
â€œWinnti,â€ named after one of its most infamous RATs. Although the Amoeba
group is best known for its preference for attacking gaming industry, it has
now expanded its scope to other sectors including telecommunication, chemistry,
pharmacy, aviation, etc. In 2020, the U.S. government indicted five Amoeba
actors, pointing out that the group has strong connections with China's
Ministry of State Security (MSS), the top intelligence agency of the Chinese
government. "
    }
  ]
}
```


Fetching Related Capabilities (MITRE ATT&CK Techniques)

```
GET https://api.threatvision.org/api/v2/malwares/{malware_name}/capabilities
```

```
{
  "success": true,
  "id": "ChatLoader",
  "techniques": [
    {
      "main_value": "T1036",
      "name": "Masquerading",
      "description": "Adversaries may attempt to manipulate features of their
artifacts to make them appear legitimate or benign to users and/or security
tools. Masquerading occurs when the name or location of an object, legitimate
or malicious, is manipulated or abused for the sake of evading defenses and
observation. This may include manipulating file metadata, tricking users into
misidentifying the file type, and giving legitimate task or service names.
\n\nRenaming abusable system utilities to evade security monitoring is also a
form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation:
LOLBAS Main Site)",
      "last_modified": 1680887074,
      "published_at": 1496266238,
      "version": "1.5",
      "tactics": [
        {
          "tactic_name": "Defense Evasion",
          "tactic_serial": "TA0005"
        }
      ],
      "sub_techniques": [
        {
          "main_value": "T1036.001",
          "name": "Invalid Code Signature",
          "description": "Adversaries may attempt to mimic features of valid
code signatures to increase the chance of deceiving a user, analyst, or tool.
Code signing provides a level of authenticity on a binary from the developer
and a guarantee that the binary has not been tampered with. Adversaries can
copy the metadata and signature information from a signed program, then use it
as a template for an unsigned program. Files with invalid code signatures will
fail digital signature validation checks, but they may appear more legitimate
to users and security tools may improperly handle these files.(Citation:
Threatexpress MetaTwin 2017)\n\nUnlike [Code Signing](https://attack.mitre.org/
techniques/T1553/002), this activity will not result in a valid signature.",
          "last_modified": 1581364367,
          "published_at": 1581364186,
          "version": "1.0",
          "tactics": [
            {
              "tactic_name": "Defense Evasion",
              "tactic_serial": "TA0005"
            }
          ],
          "parent": {
            "name": "Masquerading",
            "serial": "T1036"
```

```
          },
          "sub_techniques": []
        },
        {
          "main_value": "T1036.002",
          "name": "Right-to-Left Override",
          "description": "Adversaries may abuse the right-to-left override
(RTLO or RLO) character (U+202E) to disguise a string and/or file name to make
it appear benign. RTLO is a non-printing Unicode character that causes the text
that follows it to be displayed in reverse. For example, a Windows screensaver
executable named <code>March 25 cod.scr</code> will display as <code>March 25
rcs.docx</code>. A JavaScript file named <code>photo_high_regnp.js</code> will
be displayed as <code>photo_high_resj.png</code>.(Citation: Infosecinstitute
RTLO Technique)\n\nAdversaries may abuse the RTLO character as a means of
tricking a user into executing what they think is a benign file type. A common
use of this technique is with [Spearphishing Attachment](https://
attack.mitre.org/techniques/T1566/001)/[Malicious File](https://
attack.mitre.org/techniques/T1204/002) since it can trick both end users and
defenders if they are not aware of how their tools display and render the RTLO
character. Use of the RTLO character has been seen in many targeted intrusion
attempts and criminal activity.(Citation: Trend Micro PLEAD RTLO)(Citation:
Kaspersky RTLO Cyber Crime) RTLO can be used in the Windows Registry as well,
where regedit.exe displays the reversed characters but the command line tool
reg.exe does not by default.",
          "last_modified": 1634245319,
          "published_at": 1581364529,
          "version": "1.1",
          "tactics": [
            {
              "tactic_name": "Defense Evasion",
              "tactic_serial": "TA0005"
            }
          ],
          "parent": {
            "name": "Masquerading",
            "serial": "T1036"
          },
          "sub_techniques": []
        }
      ]
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this feed:

> The mapping for this feed is based on each item within the corresponding list keys returned by the API. Indexes represent which request it came from.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`[1].name`	Adversary.Name	N/A	N/A	`Polaris`	User-configurable
`[1].overview`	Adversary.Description	N/A	N/A	N/A	User-configurable
`[1].aliases[]`	Adversary.Attribute	Attribute	N/A	`APT1`	User-configurable
`[1].origin_countries[]`	Adversary.Attribute	Origin Country	N/A	`North Korea`	User-configurable
`[1].targeted_countries[]`	Adversary.Attribute	Target Country	N/A	`Taiwan`	User-configurable
`[1].targeted_industries[]`	Adversary.Attribute	Filename	N/A	`Education`	User-configurable
`[0].name`	Malware.Value	N/A	N/A	`Amoeba`	N/A
`[0].overview`	Malware.Description	N/A	N/A	N/A	N/A
`[0].aliases[]`	Malware.Attribute	Alias	N/A	N/A	N/A
`[0].type`	Malware.Attribute	Malware Type	N/A	`RAT`	N/A
`[2].main_value`, `[2].name`	Attack-Pattern.Value	N/A	N/A	`T1008 - Fallback Channels`	User-configurable
`[2].tactics[].tactic_name`	Attack-Pattern.Attribute	Tactic	`Reconnaissance`	N/A	User-configurable
`[2].overview`	Attack Pattern.Description	N/A	N/A	N/A	User-configurable

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 minute
Indicators	4
Indicator Attributes	4

TeamT5 ThreatVision - IOC Bundles

METRIC	RESULT
Run Time	1 minute
Indicators	374
Indicator Attributes	1,202
Malware	20
Malware Attributes	23
Tools	23
Signatures	172

TeamT5 ThreatVision - Patch Management Reports

METRIC	RESULT
Run Time	1 minute

METRIC	RESULT
Indicators	45
Indicator Attributes	188
Report	2
Report Attributes	11
Signatures	22
Signature Attributes	44
Vulnerabilities	4
Vulnerability Attributes	41

TeamT5 ThreatVision - Adversaries

METRIC	RESULT
Run Time	3 minutes
Adversaries	40
Adversary Attributes	616
Attack Patterns	286
Attack Pattern Attributes	344
Malware	243

METRIC	RESULT
Malware Attributes	259

TeamT5 ThreatVision - Malware

METRIC	RESULT
Run Time	15 minutes
Adversaries	43
Adversary Attributes	146
Attack Patterns	295
Attack Pattern Attributes	378
Malware	344
Malware Attributes	360

Known Issues / Limitations

- The MITRE filter uses cache memory to load all MITRE ATT&CK data, with the cache being refreshed every 24 hours.

Change Log

- **Version 1.1.0**
  - Resolved an issue where the report published at dates were incorrect.
  - Updated the feeds to use the ThreatVision v2 API.
  - Renamed the **TeamT5 ThreatVision - APT Weekly IOCs** feed to **TeamT5 ThreatVision - IOC Bundles**.
  - Added the following new feeds:
    - TeamT5 ThreatVision - Patch Management Reports
    - TeamT5 ThreatVision - Adversaries
    - TeamT5 ThreatVision - Malware
  - Added a new MITRE filter designed to streamline the process of handling MITRE ATT&CK data.
  - IOCs parsed from STIX bundles will now also receive attribution inherited from the parent report (Target Country & Target Industry).
  - TeamT5 ThreatVision - Reports feed
    - Added a new configuration option: **Ingest PDF Reports**. This gives users the ability to fetch and download the associated PDF reports with each report.
    - Added a new option, Vulnerabilities, to the **Report Types Filter**.
  - Updated the minimum ThreatQ version to 6.5.0.
- **Version 1.0.0**
  - Initial release