ThreatQuotient

TeamT5 ThreatVision Action Bundle

Version 1.1.0

November 19, 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.

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	>= 5.12.1
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The TeamT5 ThreatVision Action Bundle enables the automatic extraction of FQDNs (or IP Addresses) from URLs within your Threat Library.

The integration provides the following actions:

- **TeamT5 ThreatVision - ITM Enrichment** - uses the TeamT5 ThreatVision's ITM API to fetch enrichment for network indicators (IPs & Domains).
- **TeamT5 ThreatVision - Sample Enrichment** - uses the TeamT5 ThreatVision's Sample API to fetch enrichment for file indicators (MD5, SHA1, SHA256).

The action is compatible with the following indicator types:

- IP Address
- FQDN
- URL
- MD5
- SHA-1
- SHA-256

The action returns the following enriched indicator types:

- IP Address
- FQDN
- URL
- MD5
- SHA-1
- SHA-256

This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- A ThreatVision License & API Keys

  > ThreatVision API Keys can be generated from **My Account -> API** in the ThreatVision Portal.

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing the following indicator types:
  - IP Address
  - FQDN
  - URL
  - MD5
  - SHA-1
  - SHA-256

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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
    - Drag and drop the zip file into the dialog box
    - Select **Click to Browse** to locate the zip file on your local machine

> ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to configure the action.

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:

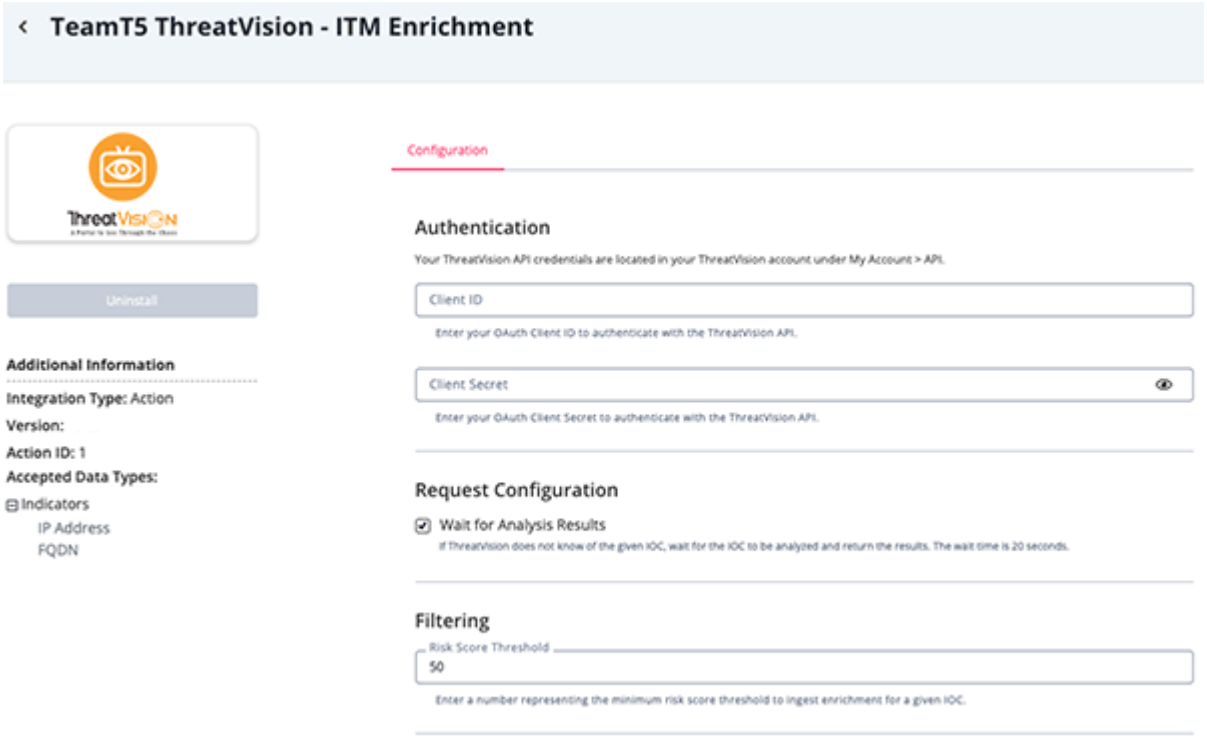
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

ITM Enrichment

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.
Wait for Analysis Results	If ThreatVision does not know of the given IOC, wait for the IOC to be analyzed and return the results. The wait time is 20 seconds. This parameter is enabled by default.
Risk Score Threshold	Enter a number representing the minimum risk score threshold to ingest enrichment for a given IOC. The default value is 50.
Additional Enrichment	Select the additional pieces of enrichment you want to ingest into ThreatQ. As of this publication, **Related Samples** is only option available.

PARAMETER	DESCRIPTION
	Each selection will result in additional API calls.
Context Filter	Select the pieces of enrichment context you want to ingest into ThreatQ. Options include: ◦ Risk Score (default) ◦ Risk Types (default) ◦ Location ◦ Related Adversaries (default) ◦ Labels (default)
Sample Context Filter	Select the pieces of enrichment context you want to ingest into ThreatQ with the related Samples. Options include: ◦ MD5 (default) ◦ SHA-256 (default) ◦ Filename ◦ Related Malware (default) ◦ Risk Level (default) ◦ ThreatVision Link
Enable SSL Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Objects Per Run	The number of objects to process per run of the workflow. The default value is 10000.

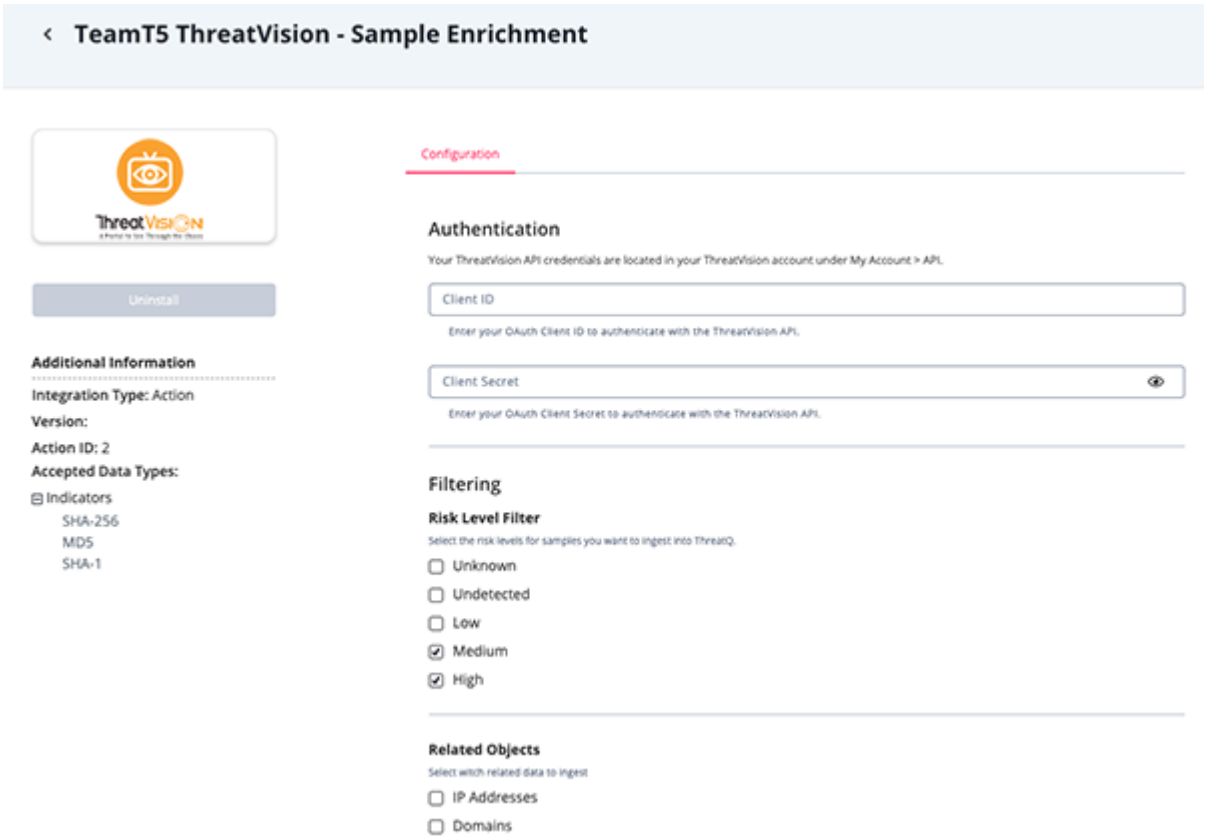


Sample Enrichment

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.
Risk Level Filter	Select the risk levels for samples you want to ingest into ThreatQ. Options include: ◦ Unknown ◦ Undetected ◦ Low ◦ Medium (default) ◦ High (default)
Context Filter	Select the pieces of enrichment context you want to ingest into ThreatQ. Options include:

PARAMETER	DESCRIPTION
	◦ Risk Level (default) ◦ Related Adversaries (default) ◦ Malware Family (Attribute) (default) ◦ File Type (default) ◦ First Seen ◦ ThreatVision Link
Sample Aliases	Select which sample aliases you want to ingest into ThreatQ. Options include: ◦ MD5 ◦ SHA-256 ◦ SHA-1 ◦ Filename ◦ File Path
Context Filter (VirusTotal)	Select the pieces of VirusTotal context you want to ingest into ThreatQ. Options include: ◦ Tags (default) ◦ Detection Rate (default) ◦ In-the-Wild URLs (default) ◦ In-the-Wild Filenames & File Paths (default)
Malicious Count Threshold (VirusTotal)	Enter the number of malicious detections required to mark a sample with a "Malicious" attribute. Enter 0 to disable. The default value is 10.
IOC Status (VirusTotal)	Select the status to assign to VirusTotal IOCs. Options include: ◦ Review (default) ◦ Active ◦ Indirect
Context Filter (Cuckoo)	Select the pieces of Cuckoo Sandbox context you want to ingest into ThreatQ. Options include: ◦ Network IOCs (IPs & FQDNs) ◦ Mutexes
IOC Status (Cuckoo)	Select the status to assign to Cuckoo Sandbox IOCs. Options include: (default: Review) ◦ Review (default)

PARAMETER	DESCRIPTION
	◦ Active ◦ Indirect
Enable SSL Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Objects Per Run	The number of objects to process per run of the workflow. The default value is 10000.



5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following actions are available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
TeamT5 ThreatVision - ITM Enrichment	Enrich network IOCs using ThreatVision's ITM module	Indicator	IP Address, FQDN, URL
TeamT5 ThreatVision - Sample Enrichment	Enrich file IOCs using ThreatVision's Sample module	Indicator	MD5, SHA-1, SHA-256

ITM Enrichment

The ThreatVision ITM Enrichment action will use TeamT5 ThreatVision's ITM API to fetch enrichment for network indicators (IPs & Domains), automatically adding the selected context to the indicator.

`https://api.threatvision.org/api/v2/network/{{ ioc.type }}/{{ ioc.value }}/samples`

Sample Response:


```
{
  "success": true,
  "analysis_status": true,
  "risk_score": 5,
  "adversaries": [],
  "attributes": [
    {
      "name": "Malware C2",
      "first_seen": "2022-12-15T15:34:06.071Z",
      "last_seen": "2023-04-14T05:54:22.454Z"
    }
  ],
  "risk_types": [
    "other"
  ],
  "ip_sharing": [
    {
      "name": "Hosting",
      "first_seen": "2023-08-29T11:42:27.576Z",
      "last_seen": "2023-08-29T11:42:27.576Z"
    }
  ],
  "services": [],
  "location": "West Chicago, United States of America",
  "summary": {
    "whois": true,
    "related_adversaries": 0,
    "related_reports": 0,
    "related_samples": 0,
    "dns_records": 7,
    "osint": 0
  }
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.location	Indicator.Attribute	Detection Rate	N/A	West Chicago, United States of America	If `Location` option is selected in `Ingestion Options` configuration section
.risk_score	Indicator.Attribute	Risk Score	N/A	5	If `Risk Score` option is selected in `Ingestion Options` configuration section. Will be updated if the value is changed
.risk_types[]	Indicator.Attribute	Risk Type	N/A	other	If `Risk Types` option is selected in `Ingestion Options` configuration section. Formatted according to the `Risk Types Table Mapping` bellow
.attributes[].name	Indicator.Attribute	Label	N/A	Malware C2	If `Labels` option is selected in `Ingestion Options` configuration section
.adversaries[]	Related Adversary.Value	N/A	N/A	N/A	If `Related Adversaries` option is selected in `Ingestion Options` configuration section. Formatted as `https://threatvision.org/samples/{.data.sha256 }`

ITM Relations Supplemental

`https://api.threatvision.org/api/v1/network/{{ ioc.type }}/{{ ioc.value }}/relations`

ThreatQuotient provides the following default mapping for this supplemental action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.sample.risk_level	Related Indicator.Attribute	Risk Level	N/A	middle	If `Risk Level` option is selected in `Sample Context Filter` configuration section
.sample.url	Related Indicator.Attribute	ThreatVision Link	N/A	N/A	If `ThreatVision Link` option is selected in `Sample Context Filter` configuration section
.sample.malwares[]	Related Indicator.Attribute	Malware Family	N/A	Malware C2	If `Related Malware` option is selected in `Sample Context Filter` configuration section
.sample.md5	Related Indicator.Value	MD5	N/A	cba74e507e9741740d251b1fb34a1874	If `MD5` option is selected in `Sample Context Filter` configuration section
.sample.sha256	Related Indicator.Value	SHA-256	N/A	56ee57de81ecea6a2c83d5430238fa98a041e8eb	If `SHA-256` option is selected in `Sample Context Filter` configuration section
.sample.filename	Related Indicator.Value	Filename	N/A	vti-rescan	If `Filename` option is selected in `Sample Context Filter` configuration section

Risk Types Mapping Table

.RISK_TYPES VALUE	RISK TYPE VALUE
ce	Cyber Espionage
cc	Cyber Crime
other	Other

Sample Enrichment

The ThreatVision Sample Enrichment action will use TeamT5 ThreatVision's Samples API to fetch enrichment for file indicators (MD5, SHA-1, SHA-256), automatically adding the selected context to the indicator.

`https://api.threatvision.org/api/v1/samples/{{ ioc.value }}`

Sample Response:


```
{
    "success": true,
    "sample": {
        "sha256":
"755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63",
        "md5": "cba74e507e9741740d251b1fb34a1874",
        "sha1": "56ee57de81ecea6a2c83d5430238fa98a041e8eb",
        "crc32": "984C2375",
        "tlshash":
"62752331b142443bc0a209785947a3b6b636fb081b3c69df73dd58acc93735a2a663d9",
        "ssdeep": "24576:pAT8QE+kzjj/
IxaSyRBCy6qqY1da7ZE+3BxNERNR700TVQtJmQtWadWPMmuioG5:pAI+M/
IaSueDYOmilISMasPMmuLG5",
        "risk_level": "middle",
        "adversaries": [],
        "malwares": [],
        "file_type": "Win32 EXE",
        "size": 1580101,
        "tlp": "green",
        "first_seen": 1599480594,
        "meta_timestamp": 708992537,
        "auto_analysis": {
            "cuckoo": {
                "last_succeed_at": 1599481494
            },
            "vt_hunt": {
                "last_succeed_at": 1676469410
            },
            "vt_info": {
                "last_succeed_at": 1660301165
            },
            "filetype": {
                "last_succeed_at": 1676472007
            },
            "file_hash": {
                "last_succeed_at": 1676471995
            },
            "pe_file": {
                "last_succeed_at": 1676472022
            },
```

```
            "yara_scan": {
                "last_succeed_at": 1676472021
            },
            "exiftool": {
                "last_succeed_at": 1676472022
            }
        },
        "related_samples": [
            {
                "sha256":
"05ff897f430fec0ac17f14c89181c76961993506e5875f2987e9ead13bec58c2",
                "md5": "0b4ad1bd093e0a2eb8968e308e900180",
                "file_type": "WIN32_EXE",
                "file_name": null,
                "relations": "Drops",
                "first_seen": 1569479863,
                "url": "https://api.threatvision.org/samples/
05ff897f430fec0ac17f14c89181c76961993506e5875f2987e9ead13bec58c2"
            }
        ],
        "virus_total": {
            "file_type": null,
            "tags": [
                "peexe",
                "overlay",
                "bobsoft",
                "runtime-modules",
                "detect-debug-environment",
                "direct-cpu-clock-access",
                "checks-user-input"
            ],
            "itw_urls": [
                "http://83.149.110.52/dzKuxMHj5HVzcoWU3KsWwhjyfzgTqY"
            ],
            "itw_filenames": [
                "/var/www/clean-mx/virusesevidence/output.180503168.txt"
            ],
            "positive": "49/75",
            "first_seen": 1441253114,
            "last_seen": 1660630051
        },
        "cuckoo_sandbox": {
            "network": [
                "193.104.215.66"
            ],
            "mutexes": [
                "!IECompat!Mutex",
                "Local\\__DDrawCheckExclMode__"
            ],
            "self_copy": [],
```

```
            "screenshot": [
                "https://api.threatvision.org/samples/
755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63/screenshots/
10"
            ]
        },
        "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": {
                "received": null
            },
            "attachments": [],
            "html_object_tags": null
        },
        "file_names": [
            "600347.exe"
        ],
        "file_paths": [
            "/var/www/clean-mx/virusesevidence/output.180503168.txt"
        ]
    }
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.sample.virus_total.tags[]	Indicator.Tag, Related Indicator.Tag	N/A	N/A	peexe	If `Tags` option is selected in `VirusTotal Ingestion Options` configuration section
.sample.virus_total.positive	Indicator.Attribute, Related Indicator.Attribute	Detection Rate	N/A	32/74	If `Detection Rate` option is selected in `VirusTotal Ingestion Options` configuration section. Will be updated if the values is changed
.sample.virus_total.detection_count	Indicator.Attribute, Related Indicator.Attribute	Malicious	N/A	true	`True` if `.sample.virus_total.detection_count >= Malicious Count Threshold` configuration configuration.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					Will be updated if the values is changed
.sample.risk_level	Indicator.Attribute, Related Indicator.Attribute	Risk Level	N/A	middle	If `Risk Level` option is selected in `ThreatVision Ingestion Options` configuration section. Will be updated if the values is changed
.sample.malwares[]	Indicator.Attribute, Related Indicator.Attribute	Malware Family	N/A	N/A	If `Malware Family (Attribute)` option is selected in `ThreatVision Ingestion Options` configuration section
.sample.first_seen	Indicator.Attribute, Related Indicator.Attribute	First Seen	N/A	1680849173	If `First Seen` option is selected in `ThreatVision Ingestion Options` configuration section
.sample.file_type	Indicator.Attribute, Related Indicator.Attribute	File Type	N/A	Ms Word Document	If `First Seen` option is selected in `ThreatVision Ingestion Options` configuration section
.sample.sha256	Indicator.Attribute, Related Indicator.Attribute	ThreatVision Link	N/A	5b81f8f1208d2dfccb4dd6946102b61ad8f220c7b1c0a80f7be3ca23e6e59b3e	If `ThreatVision Link` option is selected in `ThreatVision Ingestion Options` configuration section. Formatted as `https://threatvision.org/samples/{.data.sha256 }`
.sample.adversaries[]	Related Adversary.Value	N/A	N/A	Polaris	If `Related Adversaries` option is selected in `ThreatVision Ingestion Options` configuration section. Formatted as `https://threatvision.org/samples/{.data.sha256 }`
.sample.cuckoo_sandbox.network[]	Related Indicator.Value	URL / FQDN	N/A	systeminfothai.gotdns.ch	If `Network IOCs (IPs & FQDNs)` option is selected in `Cuckoo Sandbox Ingestion Options` configuration section
.sample.cuckoo_sandbox.mutexes[]	Related Indicator.Value	Mutex	N/A	!IECompat!Mutex	If `Mutexes` option is selected in `Cuckoo Sandbox Ingestion Options` configuration section
.sample.virus_total.itw_urls[]	Related Indicator.Value	URL	N/A	http://adjutant.rta.mi.th/home.php	If `In-The-Wild URLs` option is selected in `VirusTotal Ingestion Options` configuration section
.sample.virus_total.itw_filenames[]	Related Indicator.Value	Filename / File Path	N/A	flashplayer18_a_install.exe	If `In-The-Wild Filenames & File Paths` option is selected in `VirusTotal Ingestion Options` configuration section
.sample.virus_total.tags	Related Indicator.Value	CVE	N/A	N/A	If `Tags` option is selected in `VirusTotal Ingestion Options` configuration section.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					Obtained by removing the `CVE-` prefix
.sample.file_names[]	Related Indicator.Value	Filename	N/A	vti-rescan	If `Filename` option is selected in `Sample Aliases` configuration section
.sample.file_paths[]	Related Indicator.Value	File Path	N/A	/var/www/clean-mx/virusesevidence/output.180503168.txt	If `File Path` option is selected in `Sample Aliases` configuration section
.sample.md5	Related Indicator.Value	MD5	N/A	cba74e507e9741740d251b1fb34a1874	If `MD5` option is selected in `Sample Aliases` configuration section
.sample.sha256	Related Indicator.Value	SHA-256	N/A	56ee57de81ecea6a2c83d5430238fa98a041e8eb	If `SHA-256` option is selected in `Sample Aliases` configuration section
.sample.sha1	Related Indicator.Value	SHA-1	N/A	755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63	If `SHA-1` option is selected in `Sample Aliases` configuration section

Enriched Data

> Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

ITM Enrichment

METRIC	RESULT
Run Time	2 minutes
Indicators	3,376
Indicator Attributes	6,703

Sample Enrichment

METRIC	RESULT
Run Time	1 minute
Indicators	393
Indicator Attributes	643

Change Log

- **Version 1.1.0**
  - Updated the actions to use version 2 of the TeamT5 API endpoints.
  - Added the following configuration parameters:
    - Enable SSL Verification
    - Disable Proxies
- **Version 1.0.0**
  - Initial release