ThreatQuotient

TeamT5 ThreatVision Operation

Version 1.1.0

November 24, 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

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.

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.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.1.0
Compatible with ThreatQ Versions	>= 5.20.0
Support Tier	ThreatQ Supported

Introduction

The TeamT5 ThreatVision Operation enables the enrichment of IOCs in ThreatQ using the TeamT5 ThreatVision API.

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 operation provides the following action:

- **Enrich** - enriches an indicator with context from ThreatVision.

The operation is compatible with the following indicator types:

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

Prerequisites

The following is required in order to use the operation:

- A ThreatVision License and API Key. ThreatVision API Keys can be generated from `My Account -> API` in the ThreatVision Portal.

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

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

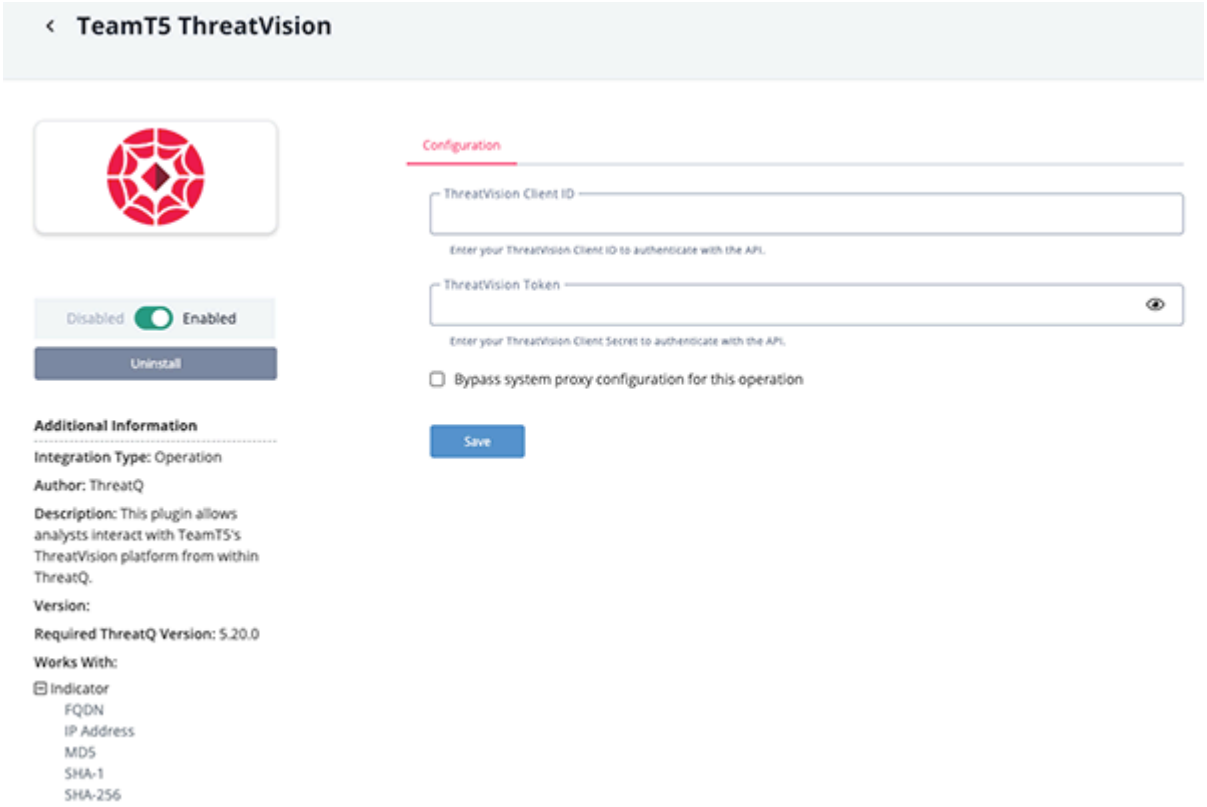
Configuration

> 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 **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

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



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.

Actions

The operation provides the following action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Enrich	Enriches an IOC with context from ThreatVision.	Indicator	IP Address, FQDN, MD5, SHA-1, SHA-256

Enrich

The Enrich action enriches an IOC with context from ThreatVision. Network IOCs will be enriched using the ITM module's API, and sample IOCs will be enriched using the sample information API.

Sample IOCs (MD5, SHA-1, SHA-256)

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

Sample Response:


```
{
    "success": true,
    "risk_level": "high",
    "md5": "0f9d9438bd628418be4e6c59094c90bb",
    "sha1": "7b9324983131c38aca79625dcb3f9c2050b673d3",
    "sha256":
"722bd8c64d76132e7163ffa9a9e22f4bfe42fe8dc5a0d2b7117a9f98b2285524",
    "first_seen": 1719872731,
    "size": 16359,
    "date": 1719876679,
    "meta": {
        "filename": {
            "original_filename": null,
            "pdb_strings": []
        },
        "document": {
            "code_page": ""
        },
        "exiftool": {
            "output": {
                "directory": "/",
                "file_name": "sample_path_in_docker",
                "file_size": "16 kB",
                "file_type": "sh script",
                "mime_type": "text/x-sh",
                "source_file": "/sample_path_in_docker",
                "file_access_date": "2024-07-31 22:25:37+0000",
                "file_modify_date": "2024-07-31 22:25:37+0000",
                "file_permissions": "rw-r--r--",
                "exif_tool_version": "11.88",
                "file_type_extension": "sh",
                "file_inode_change_date": "2024-07-31 22:25:37+0000"
            }
        },
        "file_hash": {
            "tlsh":
"7572724ba119dc3b14eacc6e3363911d8a6b94eb806b5ff5fc65b43c442d04cb619ee8",
            "crc32": "91558144",
```

```
            "entropy": 5.27684211730957
        }
    }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.meta.exiftool.output.directory	Indicator.Attribute	Directory	N/A	`/`	N/A
.meta.exiftool.output.exif_tool_version	Indicator.Attribute	Exif Tool Version	N/A	`11.88`	N/A
.meta.exiftool.output.file_name	Indicator.Attribute	File Name	N/A	`sample_path_in_docker`	N/A
.meta.exiftool.output.file_permissions	Indicator.Attribute	File Permissions	N/A	`rw-r--r--`	N/A
.meta.exiftool.output.file_size	Indicator.Attribute	File Size	N/A	`794 kB`	N/A
.meta.exiftool.output.file_type	Indicator.Attribute	File Type	N/A	`ZIP`	N/A
.meta.exiftool.output.file_type_extension	Indicator.Attribute	File Type Extension	N/A	`zip`	N/A
.meta.exiftool.output.mime_type	Indicator.Attribute	Mime Type	N/A	`application/zip`	N/A
.meta.exiftool.output.source_file	Indicator.Attribute	Source File	N/A	`/sample_path_in_docker`	N/A
.risk_level	Indicator.Attribute	Risk Level	N/A	`high`	Updatable
.size	Indicator.Attribute	Size	N/A	`813233`	N/A
.md5	Related Indicator.Value	MD5	N/A	`368a4cd9a9b34ada390c192157988921`	N/A
.sha1	Related Indicator.Value	SHA-1	N/A	`e0b5c5cd32f115b1ea4462bbbafc4cccef7d438f`	N/A
.sha256	Related Indicator.Value	SHA-256	N/A	`4bcedac20a75e8f8833f4725adfc87577c32990c3783bf6c743f14599a176c37`	N/A

Risk Level Mapping

ThreatQuotient provides the following risk level mapping.

TEAMT5 THREATVISION VALUE	THREATQ VALUE
undetected	Undetected
unknown	Unknown
low	Low
middle	Medium
high	High

Network IOCs

The operation will use different endpoints depending on if the given network IOC has related samples.

Network IOCs Summary

`GET https://api.threatvision.org/api/v2/network/ips/{ip}/summary` `GET https://api.threatvision.org/api/v2/network/domains/{domain}/summary`

Sample Response:


```
{
  "success": true,
  "analysis_status": true,
  "risk_score": 0,
  "risk_types": ["other"],
  "location": "",
  "adversaries": [],
  "attributes": [
    {
      "name": "Malware C2",
      "first_seen": "2022-12-15T15:34:06.071Z",
      "last_seen": "2023-04-14T05:54:22.454Z"
    }
  ],
  "services": [],
  "summary": {
    "whois": false,
    "related_adversaries": 0,
    "related_reports": 0,
    "related_samples": 10,
    "dns_records": 6,
    "osint": 0
  }
}
```

Network IOCs with Samples

If a given network IOC has related samples, they will be fetched using the following API:

`GET https://api.threatvision.org/api/v1/network/ips/{ip}/summary` `GET https://api.threatvision.org/api/v1/network/domains/{domain}/summary`

Sample Response:

```
{
  "success": true,
  "analysis_status": true,
  "samples": [
    {
      "sha256":
"3252345b2640efc44cdd98667dbd25806ee2316d1e01eec488fd678e885aa960",
      "md5": "8f106544bfd4755d17a353064666426a",
      "adversaries": [],
      "malwares": [],
      "filename": null,
      "risk_level": "middle",
      "network_activity": true,
      "seen": false,
      "url": "https://api.threatvision.org/samples/
3252345b2640efc44cdd98667dbd25806ee2316d1e01eec488fd678e885aa960"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.risk_score`	Indicator.Attribute	Risk Score	N/A	`45`	N/A
`.risk_types[]`	Indicator.Attribute	Risk Type	N/A	`Cyber Espionage`	N/A
`.location`	Indicator.Attribute	Location	N/A	`Richardson, United States of America`	N/A
`.attributes[].name`	Indicator.Attribute	Label	N/A	`Malware C2`	N/A
`.adversaries[]`	Indicator.Attribute	Related Adversary	N/A	N/A	N/A
`.summary.related_samples[].sha256`	Related Indicator.Value	SHA-256	N/A	`3252345b2640efc44cdd98667dbd25806ee2316d1e01eec488fd678e885aa960`	N/A
`.summary.related_samples[].md5`	Related Indicator.Value	MD5	N/A	`8f106544bfd4755d17a353064666426a`	N/A
`.summary.related_samples[].adversaries[]`	Related Indicator.Attribute	Related Adversary	N/A	N/A	N/A
`.summary.related_samples[].malwares[]`	Related Indicator.Attribute	Malware Family	N/A	N/A	N/A
`.summary.related_samples[].filename`	Related Indicator.Value	Filename	N/A	N/A	N/A
`.summary.related_samples[].risk_level`	Related Indicator.Attribute	Risk Level	N/A	`Medium`	Mapped to a standardized value using table `Risk Level Mapping`

Known Issues / Limitations

- Due to platform limitations for Indicators of type IP or FQDN an attribute is added to a related sample only if it has a value for all the entries. In other words, if a column has values for all the entries, but one, that column will not be added as an attribute.

Change Log

- **Version 1.1.0**
  - Updated the integration to use version 2 of TeamT5's API.
- **Version 1.0.0**
  - Initial release