ThreatQuotient

VirusTotal IOC Stream CDF

Version 1.0.1

June 07, 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	1.0.1
Compatible with ThreatQ Versions	>= 5.22.0
Support Tier	ThreatQ Supported

Introduction

The VirusTotal IOC Stream CDF returns different types of objects (files, URLs, domains, IP addresses) coming from multiple origins. Depending on the origin of the notification there will be different context attributes added to these objects.

The integration provides the following feed:

- **VirusTotal IOC Stream** - ingests IOCs from the VirusTotal IOC Stream feed and stores them along with selected Context attributes.

The integration ingests following object types:

- Indicators
  - Filename
  - Fuzzy Hash
  - IP Address
  - MD5
  - SHA-1
  - SHA-256
- Malware

Prerequisites

The integration requires a VirusTotal API key.

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 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. 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.

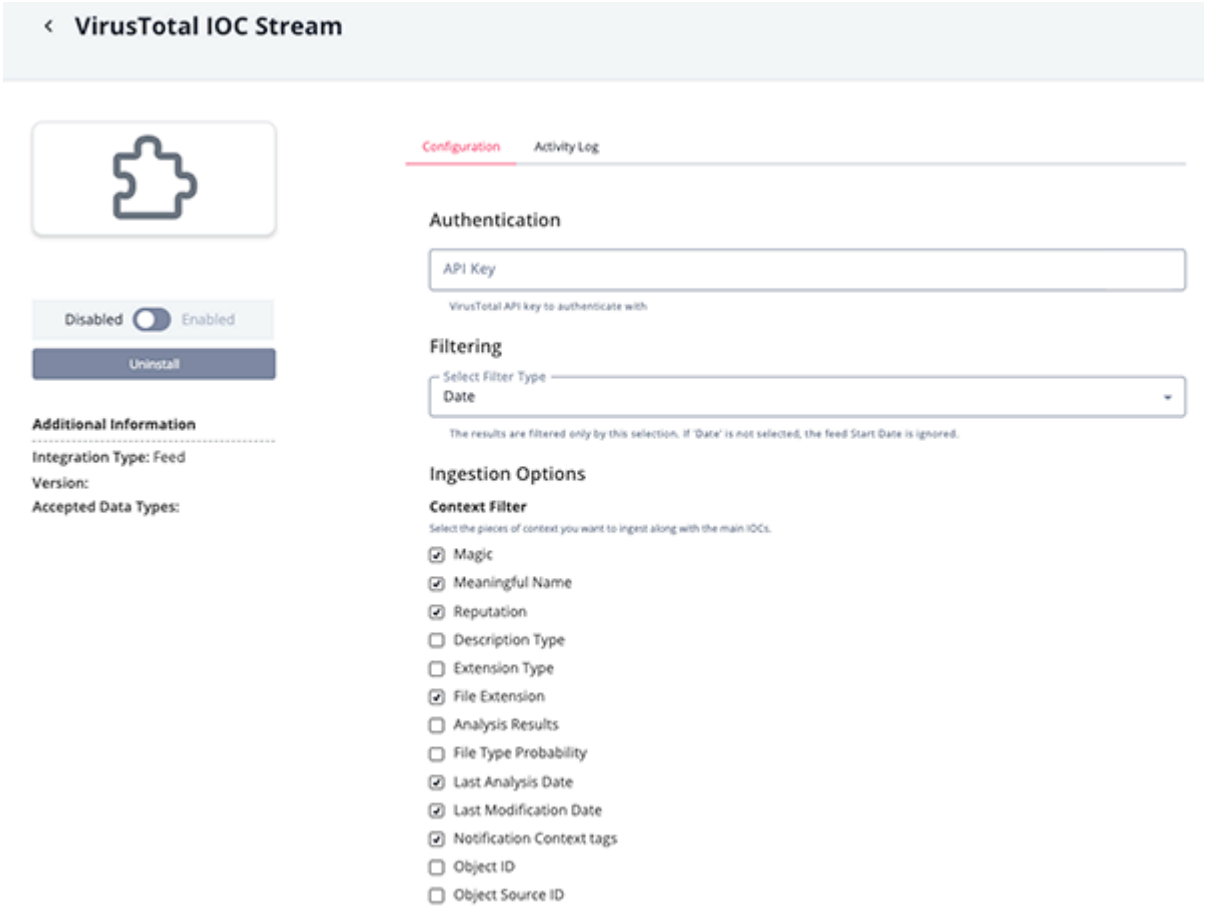
To configure the integration:

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
API Key	Enter your VirusTotal API key.
Context Filter	Select the pieces of context you want to ingest along with the IPs. Options include: ◦ Magic (default) ◦ Meaningful Name (default) ◦ Reputation (default) ◦ Description Type ◦ Extension Type ◦ File Extension (default) ◦ Analysis Result ◦ File Type Probability ◦ Last Analysis Date (default) ◦ Last Modification Date (default) ◦ Notification Context Tags (default) ◦ Object ID ◦ Object Source ID



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

VirusTotal IOC Stream

The VirusTotal IOC Stream feed ingests IOCs from the VirusTotal IOC Stream feed and stores them along with selected Context attributes.

```
GET https://www.virustotal.com/api/v3/ioc_stream
```

Sample Response:


```
{
  "meta": {
    "cursor": "eJyrCa9yNfIPSTf1DXE09M1KLvZ09qzwzYqs9HdJNvEPSTbxdfZKAQDpQQwc",
    "count": 76
  },
  "data": [
    {
      "attributes": {
        "whois": "NetRange: 10.0.0.0 - 10.255.255.255\nCIDR:
10.0.0.0/8\nNetName: PRIVATE-ADDRESS-ABLK-RFC1918-IANA-RESERVED\nNetHandle:
NET-10-0-0-0-1\nParent: ()\nNetType: IANA Special Use\nOriginAS:
\nOrganization: Internet Assigned Numbers Authority (IANA)\nRegDate: \nUpdated:
2013-08-30\nComment: These addresses are in use by many millions of
independently operated networks, which might be as small as a single computer
connected to a home gateway, and are automatically configured in hundreds of
millions of devices. They are only intended for use within a private context
and traffic that needs to cross the Internet will need to use a different,
unique address.\r\nComment: \r\nComment: These addresses can be used by anyone
without any need to coordinate with IANA or an Internet registry. The traffic
from these addresses does not come from ICANN or IANA. We are not the source of
activity you may see on logs or in e-mail records. Please refer to http://
www.iana.org/abuse/answers\r\nComment: \r\nComment: These addresses were
assigned by the IETF, the organization that develops Internet protocols, in the
Best Current Practice document, RFC 1918 which can be found at:\r\nComment:
http://datatracker.ietf.org/doc/rfc1918\nRef: https://rdap.arin.net/registry/
ip/10.0.0.0\nOrgName: Internet Assigned Numbers Authority\nOrgId:
IANA\nAddress: 12025 Waterfront Drive\r\nAddress: Suite 300\nCity: Los
Angeles\nStateProv: CA\nPostalCode: 90292\nCountry: US\nRegDate: \nUpdated:
2012-08-31\nRef: https://rdap.arin.net/registry/entity/IANA\nOrgAbuseHandle:
IANA-IP-ARIN\nOrgAbuseName: ICANN\nOrgAbusePhone: +1-310-301-5820
\nOrgAbuseEmail: abuse@iana.org\nOrgAbuseRef: https://rdap.arin.net/registry/
entity/IANA-IP-ARIN\nOrgTechHandle: IANA-IP-ARIN\nOrgTechName:
ICANN\nOrgTechPhone: +1-310-301-5820 \nOrgTechEmail:
abuse@iana.org\nOrgTechRef: https://rdap.arin.net/registry/entity/IANA-IP-
ARIN\n",
        "whois_date": 1652963616,
        "last_analysis_date": 1698893708,
```

```
      "tags": [
        "private"
      ],
      "last_analysis_stats": {
        "harmless": 56,
        "malicious": 0,
        "suspicious": 0,
        "undetected": 33,
        "timeout": 0
      },
      "threat_severity": {
        "threat_severity_level": "SEVERITY_NONE",
        "threat_severity_data": {
          "has_bad_communicating_files_high": true,
          "has_bad_communicating_files_medium": true
        },
        "last_analysis_date": "1698894041",
        "version": "I2",
        "level_description": "Severity NONE because it has no detections."
      },
      "reputation": 0,
      "last_analysis_results":
      {
        "Bkav": {
          "category": "undetected",
          "result": "unrated",
          "method": "blacklist",
          "engine_name": "Bkav"
        },
        "CMC Threat Intelligence":
        {
            "category": "harmless",
            "result": "clean",
            "method": "blacklist",
            "engine_name": "CMC Threat Intelligence"
        }
      },
      "last_modification_date": 1698921525,
      "total_votes": {
        "harmless": 0,
        "malicious": 0
      }
    },
    "type": "ip_address",
    "id": "10.127.0.3",
    "links": {
      "self": "https://www.virustotal.com/api/v3/ip_addresses/10.127.0.3"
    },
    "context_attributes": {
      "notification_id": "12558362696",
```

```
        "origin": "hunting",
        "hunting_info": {
          "rule_name": "IpsContactedByADetectedFile"
        },
        "tags": [
          "untitled_yara_ruleset",
          "ipscontactedbyadetectedfile"
        ],
        "sources": [
          {
            "type": "hunting_ruleset",
            "id": "12682106570",
            "label": "Untitled YARA ruleset"
          }
        ],
        "notification_date": 1698921520
      }
    }
  ],
    "links": {
        "self": "https://www.virustotal.com/api/v3/ioc_stream",
        "next": "https://www.virustotal.com/api/v3/ioc_stream?
cursor=eJyrCa9yNfIPSTf1DXE09M1KLvZ09qzwzYqs9HdJNvEPSTbxdfZKAQDpQQwc"
    }
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].id	Indicator Value	IP Address	.data[].attributes.last_submission_date	'10.127.0.3'	If type is not `file`
.data[].attributes.type_description +"_"+ data[].attributes.tlsh	Indicator Value	Filename	.data[].attributes.last_submission_date	N/A	If type is `file`
.data[].attributes.magic	Indicator Attribute	Magic	.data[].attributes.last_submission_date	N/A	
.data[].attributes.meaningful_name	Indicator Attribute	Meaningful Name	.data[].attributes.last_submission_date	N/A	
.data[].attributes.reputation	Indicator Attribute	Reputation	.data[].attributes.last_submission_date	'0'	
.data[].attributes.type_description	Indicator Attribute	Description Type	.data[].attributes.last_submission_date	N/A	
.data[].attributes.type_extension	Indicator Attribute	Extension Type	.data[].attributes.last_submission_date	N/A	
.data[].attributes.last_analysis_date	Indicator Attribute	Last Analysis Date	.data[].attributes.last_submission_date	'1698894041'	Timestamp format. Updates at ingestion time.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].attributes.last_modification_date	Indicator Attribute	Last Modification Date	.data[].attributes.last_submission_date	N'1698921525'	Timestamp format. Updates at ingestion time.
.data[].attributes.trid[].file_type + .data[].attributes.trid[].probability	Indicator Attribute	File Type Probability	.data[].attributes.last_submission_date	N/A	
.data[].attributes.exiftool.FileTypeExtension	Indicator Attribute	File Extension	.data[].attributes.last_submission_date	n/A	
.data[].attributes.last_analysis_results.(key).result	Indicator Attribute	(key) Analysis Result	.data[].attributes.last_submission_date	'unrated'	The name of this attribute is dynamically set with the value found on (key). We only add this attribute if the value is not null.
.data[].attributes.tags[]	Indicator Tag	N/A	.data[].attributes.last_submission_date	'apk'	
.data[].attributes.last_analysis_results.(key).result	Related.Malware	N/A	.data[].attributes.last_submission_date	'clean'	If the value corresponds to a type of malware, then a Malware object is ingested instead of ingesting the '(key) Analysis Result' signature attribute.
.data[].attributes.last_analysis_results.(key).engine_name	Related.Malware.Attribute	Analysis Engine	.data[].attributes.last_submission_date	'CMC Threat Intelligence'	
.data[].attributes.md5	Related.Indicator	MD5	.data[].attributes.last_submission_date	N/A	
.data[].attributes.sha1	Related.Indicator	SHA-1	.data[].attributes.last_submission_date	N/A	
.data[].attributes.sha256	Related.Indicator	SHA-256	.data[].attributes.last_submission_date	N/A	
.data[].attributes.ssdeep	Related.Indicator	Fuzzy Hash	.data[].attributes.last_submission_date	N/A	
.data[].attributes.main_icon.raw_md5	Related.Indicator	MD5	.data[].attributes.last_submission_date	N/A	
.data[].attributes.tlsh	Related.Indicator	Fuzzy Hash	.data[].attributes.last_submission_date	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.

METRIC	RESULT
Run Time	3 minutes
Indicators	3,026
Indicator Attributes	3,655
Malware	3,962
Malware Attributes	4,687

Known Issues / Limitations

- When filtering the results by any context information other than `Date`, the feed's `Start Date` will be ignored and the results will not be filtered by `Date`.
- The API will occasionally respond with a 500 error when the feed times run long.

Change Log

- **Version 1.0.1**
  - Resolved a parsing attribute issue that would cause a `Cannot parse argument of type None` error.
- **Version 1.0.0**
  - Initial release