ThreatQuotient

VirusTotal Retrohunt CDF Guide

Version 1.0.0

April 25, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ⚠ ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 4.45.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/virustotal-retrohunt-cdf

Introduction

The VirusTotal Retrohunt Feed fetches data related to signatures that have been pushed to VirusTotal Retrohunt via the Virtus Total Retrohunt operation.

The integration provides the following feeds:

- **VirusTotal Retrohunt** - fetches Retrohunt jobs pushed by the operation.
- **VirusTotal Retrohunt Details (supplemental)** - retrieves matching data for a Retrohunt job.

The integration ingests the following system objects:

- Signatures
  - Signature Attributes
  - Signature Tags
- Malware
  - Malware Attributes

> ⚠ This CDF must be used in together with the VirusTotal Retrohunt Operation. The operation will push YARA Signatures into VirusTotal Retrohunt and the feed will fetch data related to each pushed Signature.

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the integration file on your local machine

   > ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.
6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to configure and then enable the feed.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

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

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

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

PARAMETER	DESCRIPTION
API Key	Your VirusTotal Retrohunt API Key to be used in HTTP headers for accessing feed data.

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 Retrohunt

The VirusTotal Retrohunt feed enriches previously pushed YARA Signatures.

```
GET https://www.virustotal.com/api/v3/intelligence/retrohunt_jobs
```

Sample Response:


```
{
    "data": [
        {
            "attributes": {
                "corpus": "main",
                "creation_date": 1609749890,
                "finish_date": 1609762777,
                "notification_email": "test@test.com",
                "num_matches": 2567,
                "num_matches_outside_time_range": 5167,
                "progress": 100.0,
                "rules": "rule banbra : banker {\n\tstrings: \n$a = \"senha\" fullword nocase\ncondition:\n #a >
3}\n",
                "scanned_bytes": 743463977795058,
                "start_date": 1609749895,
                "status": "finished"
            },
            "id": "tis.threatq-1609749890",
            "links": {
                "self": "https://www.virustotal.com/api/v3/intelligence/retrohunt_jobs/tis.threatq-1609749890"
            },
            "type": "retrohunt_job"
        }
    ],
    "links": {
        "self": "https://www.virustotal.com/api/v3/users/tis.threatq/retrohunt_jobs?limit=10"
    },
    "meta": {
        "count": 2
    }
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.data[].attributes.rules	Signature.Value	YARA	'rule banbra : banker {\n\tstrings: \n$a = "senha" fullword nocase\ncondition:\n #a > 3}\n'	N/A

VirusTotal Retrohunt Details (Supplemental)

The VirusTotal Retrohunt Details supplemental feed is used to fetch the previously pushed signature details. The JSON Key from the previous feed `.data[].id` is used to call the supplemental feed.

`GET https://www.virustotal.com/api/v3/intelligence/retrohunt_jobs/{{ruleset_id}}/matching_files`

Sample Response:


```
{
    "data": [
        {
            "attributes": {
                "bundle_info": {
                    "extensions": {
                        "MF": 1,
                        "RSA": 1
                    },
                    "file_types": {
                        "DEX": 2,
                        "ELF": 5
                    },
                    "highest_datetime": "1980-00-00 00:00:00",
                    "lowest_datetime": "1980-00-00 00:00:00",
                    "num_children": 2339,
                    "type": "APK",
                    "uncompressed_size": 21842695
                },
                "capabilities_tags": [],
                "downloadable": true,
                "exiftool": {
                    "FileType": "ZIP",
                    "FileTypeExtension": "zip",
                    "MIMEType": "application/zip"
                },
                "first_submission_date": 1609751194,
                "last_analysis_date": 1609751194,
                "last_analysis_results": {
                    "ALYac": {
                        "category": "undetected",
                        "engine_name": "ALYac",
                        "engine_update": "20210102",
                        "engine_version": "1.1.3.1",
                        "method": "blacklist",
                        "result": null
                    },
                    "Bkav": {
                        "category": "malicious",
                        "engine_name": "Bkav",
                        "engine_update": "20201117",
                        "engine_version": "1.3.0.9899",
                        "method": "blacklist",
                        "result": "W32.AIDetectVM.malware2"
```

```
            },
            "Cylance": {
                "category": "malicious",
                "engine_name": "Cylance",
                "engine_update": "20201124",
                "engine_version": "2.3.1.101",
                "method": "blacklist",
                "result": "Unsafe"
            }
        },
        "last_analysis_stats": {
            "confirmed-timeout": 0,
            "failure": 0,
            "harmless": 0,
            "malicious": 0,
            "suspicious": 0,
            "timeout": 1,
            "type-unsupported": 9,
            "undetected": 65
        },
        "last_modification_date": 1609758590,
        "last_submission_date": 1609751194,
        "magic": "Zip archive data",
        "main_icon": {
            "dhash": "c4b2f8d0d4e2b2cc",
            "raw_md5": "f57cea79ec71636a99c67d5e78ffcdd9"
        },
        "md5": "b20a44d4bec61606f89b34825e080aab",
        "meaningful_name": "classes.dex",
        "reputation": 0,
        "sha1": "ad1a629afbaaf1a70a958c7a8947e5d54946f1b6",
        "sha256": "26ab6adfcdc7ba9f8074917ab1c4fcc739eebbb3da4e2920c43bf7676b3529e1",
        "size": 23179757,
        "ssdeep": "393216:6lUGcYKCjs89A90Y10PXciZy2E2dB9Q6o936cn2ioud5:6lUlwDTY10P9Wu9vcJd5",
        "tags": [
            "apk",
            "android"
        ],
        "times_submitted": 1,
        "tlsh": "T184372393F39DF82AC573D1328AB6437764A94C49CA45EB171A01B22D6DFBAC04B05FC9",
        "total_votes": {
            "harmless": 0,
            "malicious": 0
        },
        "trid": [
            {
                "file_type": "Android Package",
                "probability": 57.0
            }
        ],
        "type_description": "Android",
        "type_extension": "apk",
        "type_tag": "android",
        "unique_sources": 1,
        "vhash": "b6dc367d3c1af22b05a33edeac125a98"
    },
    "context_attributes": {
        "match_in_subfile": false,
        "rule_name": "banbra"
    },
    "id": "26ab6adfcdc7ba9f8074917ab1c4fcc739eebbb3da4e2920c43bf7676b3529e1",
```

```
            "links": {
                "self": "https://www.virustotal.com/api/v3/files/
26ab6adfcdc7ba9f8074917ab1c4fcc739eebbb3da4e2920c43bf7676b3529e1"
            },
            "type": "file"
        }
    ],
    "links": {
        "next": "https://www.virustotal.com/api/v3/intelligence/retrohunt_jobs/tis.threatq-1609749890/matching_files?
cursor=STEwCi4%3D&limit=10",
        "self": "https://www.virustotal.com/api/v3/intelligence/retrohunt_jobs/tis.threatq-1609749890/matching_files?
limit=10"
    },
    "meta": {
        "count": 2567,
        "cursor": "STEwCi4="
    }
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.data[].context_attributes.rule_name	Signature.Name	YARA	'banbra'	N/A
.data[].attributes.magic	Signature.Attribute	Magic	'Zip archive data'	N/A
.data[].attributes.meaningful_name	Signature.Attribute	Meaningful Name	'classes.dex'	N/A
.data[].attributes.reputation	Signature.Attribute	Reputation	'0'	N/A
.data[].attributes.type_description	Signature.Attribute	Description Type	'Android'	N/A
.data[].attributes.type_extension	Signature.Attribute	Extension Type	'apk'	N/A
.data[].attributes.trid[].file_type + .data[].attributes.trid[].probability	Signature.Attribute	File Type Probability	'Android Package - 57.0%'	The value of file_type and probability concatenated
.data[].attributes.exiftool.FileTypeExtension	Signature.Attribute	File Extension	'zip'	N/A
.data[].attributes.last_analysis_results.(key).result	Signature.Attribute	(key) Analysis Result	'Unsafe'	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[]	Signature.Tag	N/A	'apk'	N/A
.data[].attributes.last_analysis_results.(key).result	Malware.Value	N/A	'W32.AIDetectVM.malware2'	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	Malware.Attribute	Analysis Engine	'Bkav'	If the value corresponds to a type of malware, then a Malware object is ingested instead of ingesting the '(key) Analysis Result' signature attribute.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.data[].attributes.md5	Indicator.Value	MD5	'b20a44d4bec61606f89b34825e080aab'	N/A
.data[].attributes.sha1	Indicator.Value	SHA-1	'ad1a629afbaaf1a70a958c7a8947e5d54946f1b6'	N/A
.data[].attributes.sha256	Indicator.Value	SHA-256	'26ab6adfcdc7ba9f8074917ab1c4fcc739eebbb3da4e2920c43bf7676b3529e1'	N/A
.data[].attributes.ssdeep	Indicator.Value	Fuzzy Hash	'393216:6lUGcYKCjs89A90Y10PXciZy2E2dB9Q6o936cn2ioud5:6lUlwDTY10P9Wu9vcJd5'	N/A
.data[].attributes.main_icon.raw_md5	Indicator.Value	MD5	'f57cea79ec71636a99c67d5e78ffcdd9'	N/A
.data[].attributes.tlsh	Indicator.Value	Fuzzy Hash	'T184372393F39DF82AC573D1328AB6437764A94C49CA45EB171A01B22D6DFBAC04B05FC9'	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.

VirusTotal Retrohunt

METRIC	RESULT
Run Time	10 minutes
Signatures	2
Signature Attributes	1,435
Indicators	15,588
Malware	809
Malware Attributes	1,011

Change Log

- **Version 1.0.0**
  - Initial release