ThreatQuotient

VirusTotal Action Bundle

Version 1.1.3

April 22, 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	1.1.3
Compatible with ThreatQ Versions	>= 5.19.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The VirusTotal Action Bundle submits a collection of FQDN and supported objects to the VirusTotal API in individual HTTP Requests. VirusTotal returns a response for each object containing any information it has about the indicator.

The integration provides the following actions:

- **VirusTotal** - enriches supported objects with attributes and related objects describing the Indicator of Compromise.
- **VirusTotal Submit URLs** - submits URL indicators to VirusTotal to be analyzed.

The action is compatible with the following indicator types:

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

The action returns the following enriched indicator objects:

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

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

Prerequisites

The action requires the following:

- A VirusTotal API Key.
- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the following indicator objects:
  - FQDN
  - IP Address
  - MD5
  - SHA-256
  - SHA-1
  - URL

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 file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action 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 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.

PARAMETER	DESCRIPTION
VirusTotal API Key	Your VirusTotal API Key.
Malicious Verdict Threshold *(VT action only)*	The minimum number of AV scans reporting the IOC as malicious. Passing this threshold will result in an attribute of "Malicious: True" to be added.
AV Scan Information *(VT action only)*	The number of reports from URL scanners marking it as harmless, suspicious, malicious or undetected. Options include: ◦ Harmless Count ◦ Malicious Count (default) ◦ Suspicious Count (default) ◦ Undetected Count ◦ VirusTotal GUI Link ◦ Return Individual AV Scan Information
FILE HASH SUBMISSION	
Supporting Context *(VT action only)*	Select the which date should be used to enrich the IoC for hash submission. Options include:

PARAMETER	DESCRIPTION
	◦ Basic Properties (default) ◦ Last Analysis Result ◦ Names ◦ VirusTotal Link
Synonymous Hashes *(VT action only)*	Select the IOC types that will be ingested in ThreatQ for the file hash submission. Options include: ◦ MD5 ◦ SHA-1 ◦ SHA-256
Set Synonymous Hash Status to *(VT action only)*	Set the status of the ingested IOCs. Options include: ◦ Active (default) ◦ Expired ◦ Indirect ◦ Review ◦ Whitelisted
FQDN SUBMISSION	
Supporting Context *(VT action only)*	Select which data should be used to enrich the IOC for FQDN Submission. There is currently one option: ◦ DNS NS, SOA, andMX Records *
Relationships *(VT action only)*	Select the Relationships data to be retrieved from VirusTotal. Options include: ◦ Immediate Parent ◦ Parent ◦ Siblings ◦ Subdomains ◦ URLs *
Set Related Indicator Status to *(VT action only)*	Set the status of the related indicators. Options include: ◦ Active ◦ Expired ◦ Indirect ◦ Review ◦ Whitelisted

PARAMETER	DESCRIPTION
IP ADDRESS SUBMISSION	
Supporting Context *(VT action only)*	Select which data should be used to enrich the IOC for IP Address Submission. Options include: ◦ Basic Properties (default) ◦ Last SSL Certificate ◦ Historical SSL Certificates *
Relationships *(VT action only)*	Select the relationships data to be retrieved from VirusTotal. There is currently one option: ◦ URLs *
Set Related Indicator Status to *(VT action only)*	Set the status of the related indicators. Options include: ◦ Active ◦ Expired ◦ Indirect ◦ Review ◦ Whitelisted
URL SUBMISSION	
Supporting Context *(VT action only)*	Select which data should be used to enrich the IOC for URL Submission. Options include: ◦ Basic Properties
Relationships *(VT action only)*	Select the relationships data to be retrieved from VirusTotal. Options include: ◦ Contacted Domains * ◦ Redirecting URLs * ◦ Referrer Files * ◦ Referrer URLs *
Set Related Indicator Status to *(VT action only)*	Set the status of the related indicators. Options include: ◦ Active ◦ Expired ◦ Indirect ◦ Review ◦ Whitelisted

PARAMETER	DESCRIPTION
Requests per minute *(VT action only)*	Set the maximum number of requests to make to DomainTools per-minute. The default value is 100.
Add Last Submission Date *(VT Submit action only)*	Enabling this option will add the attribute, `Last TQO Submission Date`, to the submitted indicator record in ThreatQ.
Objects per run	Set the maximum number of objects to send to DomainTools per-run. The default value is 5,000.

* Items marked with an * require an API call.

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

Actions

The bundle provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
VirusTotal	Queries the VirusTotal API for context.	Indicator	FQDN, IP Address, MD5, SHA-256, SHA-1, URL
VirusTotal Submit URLs	Submits a URL to VirusTotal API for analysis.	Indicator	URL

VirusTotal

The VirusTotal action enriches supported objects with attributes and related objects describing the Indicator of Compromise.

```
GET https://www.virustotal.com/api/v3/{{vt_collection_name}}/{{ioc_value}}
```

> `vt_collection_name` represents the plural form of the object type as it appears in VirusTotal, while `ioc_value` represents the actual value of the objects for all indicators except for URLs. The URLs are first encoded to Base64.

Sample Response:


```
{
  "data": {
    "attributes": {
      "type_description": "DOS EXE",
      "tlsh": "T178445B4972A43CF9ECA7C239C657461BEFF27C664630D35F03641A9A4F233A1622E752",
      "exiftool": {
        "MIMEType": "application/octet-stream",
        "FileType": "DOS EXE",
        "FileTypeExtension": "exe"
      },
      "trid": [
        {
          "file_type": "DOS Executable Generic",
          "probability": 100
        }
      ],
      "crowdsourced_yara_results": [
        {
          "description": "Detects Meterpreter Beacon - file K5om.dll",
          "source": "https://github.com/Neo23x0/signature-base",
          "author": "Florian Roth",
          "ruleset_name": "apt_apt19",
          "rule_name": "Beacon_K5om",
          "ruleset_id": "000f28467c"
        }
      ],
      "names": [
        "e2f6cdade9be842ebd160634c30f1e16.virus"
      ],
      "last_modification_date": 1654841377,
      "type_tag": "mz",
      "times_submitted": 1,
      "total_votes": {
        "harmless": 0,
        "malicious": 0
      },
      "size": 263358,
      "popular_threat_classification": {
        "suggested_threat_label": "trojan.cobaltstrike",
        "popular_threat_category": [
          {
            "count": 4,
            "value": "trojan"
          }
        ],
        "popular_threat_name": [
```

```
          {
            "count": 4,
            "value": "cobaltstrike"
          }
        ]
      },
      "last_submission_date": 1653524502,
      "last_analysis_results": {
        "ClamAV": {
          "category": "malicious",
          "engine_name": "ClamAV",
          "engine_version": "0.105.0.0",
          "result": "Win.Trojan.CobaltStrike-8091534-0",
          "method": "blacklist",
          "engine_update": "20220609"
        },
        "FireEye": {
          "category": "undetected",
          "engine_name": "FireEye",
          "engine_version": "35.24.1.0",
          "result": null,
          "method": "blacklist",
          "engine_update": "20220610"
        }
      },
      "downloadable": true,
      "sha256": "56e784268807ee237adebd98046f0090ceecdfde6d2e1326afd3670e4e3ffd23",
      "type_extension": "exe",
      "tags": [
        "mz"
      ],
      "last_analysis_date": 1654834036,
      "unique_sources": 1,
      "first_submission_date": 1653524502,
      "ssdeep": "3072:3sYckn3Xzq4IDwSK2Mbn/
gprEJwJNJsCwQTIfXouPruOOTR09BQYJerCo2e:3sYwjwIGIprEJweGTIDjhOTRqQ8I",
      "md5": "e2f6cdade9be842ebd160634c30f1e16",
      "sha1": "ccbbc621afe012b358ed2e13875f1581b944dd25",
      "magic": "MS-DOS executable, MZ for MS-DOS",
      "last_analysis_stats": {
        "harmless": 0,
        "type-unsupported": 11,
        "suspicious": 0,
        "confirmed-timeout": 0,
        "timeout": 0,
        "failure": 2,
        "malicious": 5,
        "undetected": 54
      },
      "meaningful_name": "e2f6cdade9be842ebd160634c30f1e16.virus",
      "reputation": 0
    },
    "type": "file",
    "id": "56e784268807ee237adebd98046f0090ceecdfde6d2e1326afd3670e4e3ffd23",
    "links": {
      "self": "https://www.virustotal.com/api/v3/files/
56e784268807ee237adebd98046f0090ceecdfde6d2e1326afd3670e4e3ffd23"
    }
  }
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.attributes.last_analysis_stats.malicious	Indicator.Attribute, Related Indicator.Attribute	Malicious Count	.attributes.creation_date or .attributes.first_submission_date	10	If `Malicious Count` user option is checked. For all indicator types.
.attributes.last_analysis_stats.harmless	Indicator.Attribute, Related Indicator.Attribute	Harmless Count	.attributes.creation_date or .attributes.first_submission_date	23	If `Harmless Count` user option is checked. For all indicator types.
.attributes.last_analysis_stats.suspicious	Indicator.Attribute, Related Indicator.Attribute	Suspicious Count	.attributes.creation_date or .attributes.first_submission_date	8	If `Suspicious Count` user option is checked. For all indicator types.
.attributes.last_analysis_stats.undetected	Indicator.Attribute, Related Indicator.Attribute	Undetected Count	.attributes.creation_date or .attributes.first_submission_date	0	If `Undetected Count` user option is checked. For all indicator types.
.attributes.last_analysis_stats.malicious	Indicator.Attribute, Related Indicator.Attribute	Malicious	.attributes.creation_date or .attributes.first_submission_date	True	If `.attributes.malicious_count` is greater then the `Malicious Verdict Treshold` value.
.attributes.type_description	Indicator.Attribute, Related Indicator.Attribute	File Type	.attributes.creation_date or .attributes.first_submission_date	DOS EXE	For File Hashes. If `Basic Properties` user option is checked
.attributes.first_submission_date	Indicator.Attribute, Related Indicator.Attribute	First Published Date	.attributes.creation_date or .attributes.first_submission_date	1581118958	For File Hashes and URLs. If `Basic Properties` user option is checked

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.attributes.last_analysis_results.result	Indicator.Attribute, Related Indicator.Attribute	Last Analysis Result	.attributes.creation_date or .attributes.first_submission_date	clean	For File Hashes. If `Last Analysis Result` user option is checked.
.attributes.meaningful_name	Indicator.Attribute, Related Indicator.Attribute	Meaningful Name	.attributes.creation_date or .attributes.first_submission_date	e2f6cdade9be842ebd160634c30f1e16.virus	For File Hashes. If `Basic Properties` user option is checked
.attributes.md5	Related Indicator.Value	N/A	.attributes.creation_date or .attributes.first_submission_date	e2f6cdade9be842ebd160634c30f1e16	For File Hashes. If `MD5` user option is checked
.attributes.md5	Related Indicator.Attribute	VirusTotal Link	.attributes.creation_date or .attributes.first_submission_date	e2f6cdade9be842ebd160634c30f1e16	For File Hashes. If `MD5` user option is checked, formatted as `https://www.virustotal.com/gui/file/{.attributes.md5}`
.attributes.sha1	Related Indicator.Value	N/A	.attributes.creation_date or .attributes.first_submission_date	ccbbc621afe012b358ed2e13875f1581b944dd25	For File Hashes. If `SHA-1` user option is checked
.attributes.sha1	Related Indicator.Attribute	VirusTotal Link	.attributes.creation_date or .attributes.first_submission_date	ccbbc621afe012b358ed2e13875f1581b944dd25	For File Hashes. If `SHA-1` user option is checked, formatted as `https://www.virustotal.com/gui/file/{.attributes.sha1}`
.attributes.sha256	Related Indicator.Value	N/A	.attributes.creation_date or .attributes.first_submission_date	56e784268807ee237adebd98046f0090ceecdfd	For File Hashes. If `SHA-256`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
				e6d2e1326afd3670e4e3ffd23	user option is checked
.attributes.sha256	Related Indicator.Attribute	VirusTotal Link	.attributes.creation_date or .attributes.first_submission_date	56e784268807ee237adebd98046f0090ceecdfde6d2e1326afd3670e4e3ffd23	For File Hashes. If `SHA-256` user option is checked, formatted as `https://www.virustotal.com/gui/file/{.attributes.sha256}`
.attributes.names[]	Indicator.Attribute, Related Indicator.Attribute	Name	.attributes.creation_date or .attributes.first_submission_date	e2f6cdade9be842ebd160634c30f1e16.virus	For File Hashes. If `Names` user option is checked
.attributes.asn	Indicator.Attribute	ASN	.attributes.creation_date or .attributes.first_submission_date	39798	For IP Addresses. If `Basic Properties` user option is checked
.attributes.as_owner	Indicator.Attribute	AS Owner	.attributes.creation_date or .attributes.first_submission_date	MivoCloud SRL	For IP Addresses. If `Basic Properties` user option is checked
.attributes.last_https_certificate	Indicator.Attribute	Last SSL certificate	.attributes.creation_date or .attributes.first_submission_date	1581118958	For IP Addresses. If `Last SSL certificate` user option is checked

IOC Type Mapping

ThreatQ provides the following ThreatQ IOC Type to VirusTotal Collection Name mapping.

THREATQ IOC TYPE	VIRUSTOTAL COLLECTION NAME
FQDN	domains
IP Address	ip_addresses
SHA-256	files
SHA-1	files
MD5	files
URL	urls

Supplemental Calls

VirusTotal objects contain relationships with other objects in the dataset that can be retrieved with the supplemental call endpoint.

`GET https://www.virustotal.com/api/v3/{{vt_collection_name}}/{{ioc_value}}/{{relationship}}`

Sample Response:


```
{
    "meta": {
        "count": 1
    },
    "data": [
        {
            "attributes": {
                "last_dns_records": [
                    {
                        "type": "CNAME",
                        "value": "rigpriv.com",
                        "ttl": 599
                    },
                    {
                        "type": "NS",
                        "value": "jm2.dns.com",
                        "ttl": 21600
                    }
                ],
                "jarm": "28d28d28d00028d1ec28d28d28d28de9ab649921aa9add8c37a8978aa3ea88",
                "whois": "Creation Date: 2022-06-29T16:00:00Z\nCreation Date:
2022-06-30T02:32:32Z\nDNSSEC: unsigned\nDomain Name: RIGPRIV.COM\nDomain Status: ok https://
icann.org/epp#ok\nName Server: JM1.DNS.COM\nName Server: JM2.DNS.COM\nRegistrant City:
7145b6c7c70448a6\nRegistrant Country: CN\nRegistrant Email: 5c0a26a8248bb13fs@\nRegistrant State/
Province: 4f3a9c87b8ed6c6a\nRegistrar Abuse Contact Email: domainabuse@35.cn\nRegistrar Abuse
Contact Phone: +86.4001353511\nRegistrar Abuse Contact Phone: +86.4006003535\nRegistrar IANA ID:
1316\nRegistrar Registration Expiration Date: 2023-06-30T04:00:00Z\nRegistrar URL: http://
www.35.com\nRegistrar WHOIS Server: whois.35.com\nRegistrar: Xiamen 35.Com Technology Co.,
Ltd\nRegistrar: Xiamen 35.Com Technology Co., Ltd.\nRegistry Domain ID: 2707568686_DOMAIN_COM-
VRSN\nRegistry Expiry Date: 2023-06-30T02:32:32Z\nRegistry Registrant ID: Not Available From
Registry\nUpdated Date: 2022-06-30T02:43:05Z\nUpdated Date: 2022-08-21T16:00:00Z",
                "last_https_certificate_date": 1660080390,
                "tags": [],
                "popularity_ranks": {},
                "last_dns_records_date": 1660080390,
                "last_analysis_stats": {
                    "harmless": 86,
                    "malicious": 0,
                    "suspicious": 0,
                    "undetected": 8,
                    "timeout": 0
                },
                "creation_date": 1656556352,
                "reputation": 0,
                "registrar": "Xiamen 35.Com Technology Co., Ltd",
                "last_analysis_results": {
                    "CMC Threat Intelligence": {
                        "category": "harmless",
                        "result": "clean",
                        "method": "blacklist",
                        "engine_name": "CMC Threat Intelligence"
                    }
```

```
                },
                "last_update_date": 1661097600,
                "last_modification_date": 1660080390,
                "last_https_certificate": {
                    "size": 1159,
                    "public_key": {
                        "ec": {
                            "oid": "secp256r1",
                            "pub":
"0481596f6c64661ffb6a79fce6cba763d9ee961778b6e21f93eca791db1bb8fa401bbda5b35fc3874e0577444
8520d600e5f041b35257c4d7b428390afac0d514e"
                        },
                        "algorithm": "EC"
                    },
                    "thumbprint_sha256":
"2a676d52b302af217fd08e64dca3a5635bd8eea0d19ad91a50c518da2e26acc4",
                    "tags": [],
                    "cert_signature": {
                        "signature":
"6902093866e2a299575f2c04f852aaf3c2789cf53687873d4e6f599ea9140101e9be50dd8774f01b30115ca72
1561416a4d03d316b146844a3b819ec235346bb2ddc7cf3a17592a142c6b303080b18cd801d28bf7738ffb3e51
3059d8c0664783bc7edaf3711c1e6062eb20abedada8c0c8f5b2a1be20519b3056422f3c92b02c4190f649189e
a4ed07d2f9e3e87839bb180afe9a81e36f28a826400eee290775b2035bb37b681424d8224e5c8955d5ce21ecf0
475a7670f772fe16e5133176fd6dc0cc538c3d459faa72f7ffec06c4c1f9f2578cb168f82c56e10a0ffa77365d
b3378f6f55fbb1144465011a0cadb2d72658fc59b54958b0f34a89de56d640c",
                        "signature_algorithm": "sha256RSA"
                    },
                    "validity": {
                        "not_after": "2022-10-20 12:54:43",
                        "not_before": "2022-07-22 12:54:44"
                    },
                    "version": "V3",
                    "extensions": {
                        "certificate_policies": [
                            "2.23.140.1.2.1",
                            "1.3.6.1.4.1.44947.1.1.1"
                        ],
                        "extended_key_usage": [
                            "serverAuth",
                            "clientAuth"
                        ],
                        "authority_key_identifier": {
                            "keyid": "142eb317b75856cbae500940e61faf9d8b14c2c6"
                        },
                        "subject_alternative_name": [
                            "m.rigpriv.com",
                            "rigpriv.com",
                            "wap.rigpriv.com",
                            "www.rigpriv.com"
                        ],
                        "tags": [],
                        "subject_key_identifier": "48a87063dd6dc4462b432889e1615c2ce20f118d",
                        "key_usage": [
                            "ff"
                        ],
                        "1.3.6.1.4.1.11129.2.4.2":
"0481f100ef007500dfa55eab68824f1f6cadeeb85f4e3e5aeacda212a46a5e8e",
                        "CA": true,
                        "ca_information_access": {
                            "CA Issuers": "http://r3.i.lencr.org/",
                            "OCSP": "http://r3.o.lencr.org"
                        }
                    },
                    "signature_algorithm": "sha256RSA",
```

```
                    "serial_number": "044be080e3027b8cbf43952e34f00ce03492",
                    "thumbprint": "de1cabd8d7c8b5e3b9ef2d8899b2f148390fa3d2",
                    "issuer": {
                        "C": "US",
                        "CN": "R3",
                        "O": "Let's Encrypt"
                    },
                    "subject": {
                        "CN": "m.rigpriv.com"
                    }
                },
                "categories": {},
                "total_votes": {
                    "harmless": 0,
                    "malicious": 0
                }
            },
            "type": "domain",
            "id": "wap.rigpriv.com",
            "links": {
                "self": "https://www.virustotal.com/api/v3/domains/wap.rigpriv.com"
            }
        }
    ],
    "links": {
        "self": "https://www.virustotal.com/api/v3/domains/rigpriv.com/subdomains?limit=10"
    }
}
```


ThreatQuotient provides the following default mapping for this function:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
attributes.url	Related Indicator.Value	N/A	N/A	www.rigpriv.com/upload	For `URLs` relationships
.attributes.md5	Related Indicator.Value	N/A	N/A	e2f6cdade9be842ebd160634c30f1e16	For `Referrer File` relationship
.attributes.sha1	Related Indicator.Value	N/A	N/A	ccbbc621afe012b358ed2e13875f1581b944dd25	For `Referrer File` relationship
.attributes.sha256	Related Indicator.Value	N/A	N/A	56e784268807ee237adebd98046f0090ceecdfde6d2e1326afd3670e4e3ffd23	For `Referrer File` relationship
.context_attributes.first_seen_date	Indicator.Attribute	Historical SSL certificate	N/A	1591571057	For `Historical SSL certificate` relationship
.id	Related Indicator.Value	View the Relationships table above	N/A	www.rigpriv.com	For all other relationships
N/A	Related Indicator.Attribute	VirusTotal Link	N/A	https://www.virustotal.com/gui/ip-address/194.180.191.124	Formatted based on the type of the indicator and it's value. For URL indicators the url is encoded using `base64` format

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
N/A	Related Indicator.Attribute	`Relationship`	N/A	True	Represents the relationship with the data collection indicator as it appears in the ThreatQ Configuration column from the Relationship table above.

Relationships Type Mapping Table

ThreatQ provides the following relationships mapping:

VIRUS TOTAL COLLECTION NAME	VIRUS TOTAL RELATIONSHIP	THREATQ CONFIGURATION	ACCESSIBILITY
domains	ns_records	DNS NS	VT Premium users only
domains	soa_records	SOA	VT Premium users only
domains	mx_records	MX Records	VT Premium users only
domains	urls	Immediate Parent	Everyone
domains	parent	Parent	Everyone
domains	siblings	Siblings	Everyone
domains	immediate_parent	Immediate Parent	Everyone
domains	subdomains	Subdomains	Everyone
domains	urls	URLs	VT Premium users only
ip_addresses	historical_ssl_certificates	Historical SSL certificates	Everyone
ip_addresses	urls	URLs	VT Premium users only

VIRUS TOTAL COLLECTION NAME	VIRUS TOTAL RELATIONSHIP	THREATQ CONFIGURATION	ACCESSIBILITY
urls	last_serving_ip_address	Last Serving IP address	Everyone
urls	contacted_domains	Contacted Domains	VT Premium users only
urls	redirecting_urls	Redirecting URLs	VT Premium users only
urls	referrer_files	Referrer Files	VT Premium users only
urls	referrer_urls	Referrer URLs	VT Premium users only

VirusTotal Submit URLs

The Virus Total Submit URLS action enriches IPs using the VirusTotal API.

`POST https://www.virustotal.com/api/v3/urls/{{ioc_value}}/analyse`

Sample Response:

```
{
  "data": {
    "type": "analysis",
    "id": "u-d0e196a0c25d35dd0a84593cbae0f38333aa58529936444ea26453eab28dfc86-1677067101"
  }
}
```

ThreatQ provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
run_meta.started_at	Indicator.Attribute	Last TQO Submission Date	N/A	2023-02-22 12:15:00-00:00	Only gets ingested if the user selects the `Add Last Submission Date as Attribute` option.

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.

VirusTotal

METRIC	RESULT
Run Time	1 minute
Indicators	61
Indicator Attributes	352

VirusTotal Submit URLs

METRIC	RESULT
Run Time	1 minute
Indicators	57
Indicator Attributes	57

Use Case Example

1. A Threat Analyst identifies a collection of supported objects they would like to enrich.
2. The Threat Analyst adds the VirusTotal Action to a Workflow
3. The Threat Analyst configures the action with the desired parameters, and enables the Workflow
4. The Workflow executes all Actions in the graph, including VirusTotal
5. The action returns the documented Attributes from the provider, and the Workflow ingests this data into the ThreatQ platform.

Known Issues / Limitations

- The VirusTotal API is limited to 50 lookups per day.

Change Log

- **Version 1.1.3**
  - Hashes - the `Last Analysis Result` attribute is no longer ingested when `Basic Properties` is enabled for the **Supporting Context** configuration field. A new option is now available for this configuration: `Last Analysis Result`.
- **Version 1.1.2**
  - Resolved a filter mapping issue when the API response is missing fields.
- **Version 1.1.1**
  - You can now retrieve information about an individual AV scan.
    - Added new **AV Scan Information** option: **Return Individual AV Scan Information**.
  - Updated minimum ThreatQ version to 5.19.0.
- **Version 1.1.0**
  - Added support for resubmitting URLs to VirusTotal to be analyzed via VirusTotal Submit URL function.
- **Version 1.0.5**
  - Resolved an issue ingesting historical SSL attributes.
- **Version 1.0.4**
  - Initial release to ThreatQ Marketplace.