ThreatQuotient

VirusTotal Operation Guide

Version 2.3.0

December 21, 2020

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

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

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.

Contents

Versioning

- **Operation Version:** `2.3.0`
- **Minimum ThreatQ Version:** `4.22.0`

Introduction

The VirusTotal operation enriches ThreatQ objects with context obtained from the VirusTotal API.

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

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 operation:

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

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

3. Click on the operation to open its details page.
4. Enter the following configuration parameter:

PARAMETER	DESCRIPTION
API Key	Your private or public VirusTotal API Key.
Automatically Add Attributes	If checked, indicator attributes are added automatically.
Automatically Add Indicators	If checked, related indicators, along with their attributes, are added automatically. If not checked, the user can select which indicators to be added (without their attributes).

5. Click on **Save** to save your settings.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

The VirusTotal operation offers the following actions:

- submit_ip
- submit_domain
- submit_url
- submit_file
- submit_hash

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
submit_ip	Submits IP for analysis	Indicator	IP
submit_domain	Submits domain for analysis	Indicator	FQDN
submit_url	Submits URL for analysis	Indicator	URL
submit_file	Submits file for analysis	ThreatFile	
submit_hash	Submits hash for analysis	Indicator	MD5, SHA-1, SHA-256

submit_ip

The submit_ip action uses the `https://www.virustotal.com/vtapi/v2/ip-address/report` endpoint.

TQ	TQ ATTRIBUTE NAME	VIRUSTOTAL	INDICATOR TYPE
Related Indicators	N/A	`undetected_downloaded_samples[].sha256`, `detected_downloaded_samples[].sha256`, `detected_referrer_samples[].sha256`, `undetected_referrer_samples[].sha256`, `detected_communicating_samples[].sha256`, `undetected_communicating_samples[].sha256`	SHA-256
Related Indicator Attributes	Positives	`undetected_downloaded_samples[].positives`, `detected_downloaded_samples[].positives`, `detected_referrer_samples[].positives`, `undetected_referrer_samples[].positives`, `detected_communicating_samples[].positives`, `undetected_communicating_samples[].positives`, `detected_urls[].positives`	N/A
Related Indicator Attributes	Total	`undetected_downloaded_samples[].total`, `detected_downloaded_samples[].total` , `detected_referrer_samples[].total` , `undetected_referrer_samples[].total` , `detected_communicating_samples[].total` , `undetected_communicating_samples[].total` , `detected_urls[].total`	N/A
Related Indicator Attributes	Date	`undetected_downloaded_samples[].date`, `detected_downloaded_samples[].date` , `detected_referrer_samples[].date` , `detected_communicating_samples[].date` , `undetected_communicating_samples[].date` , `detected_urls[].scan_date`	N/A
Related Indicators	N/A	`resolutions[].hostname`	FQDN
Related Indicator Attributes	Last Resolved	`resolutions[].last_resolved`	N/A
Related Indicators	N/A	`detected_urls[].url`	URL
Indicator Attribute	VirusTotal AS Owner	`as_owner`	N/A
Related Indicator	N/A	`asn`	ASN
Indicator Attribute	VirusTotal Whois	`whois`	N/A
Indicator Attribute	VirusTotal Country	`country`	N/A
Indicator Attribute	VirusTotal Verbose Response	`verbose_msg`	N/A
Indicator Attribute	VirusTotal Continent	`continent`	N/A
Indicator Attribute	VirusTotal Whois Timestamp	`whois_timestamp`	N/A
Indicator Attribute	VirusTotal Network	`network`	N/A
Indicator Attribute	VirusTotal: HTTPS Certificate Date	`https_certificate_date`	N/A
Indicator Attribute	Public Key Algorithm	`last_https_certificate.public_key.algorithm`	N/A

TQ	TQ ATTRIBUTE NAME	VIRUSTOTAL	INDICATOR TYPE
Indicator Attribute	Public Key RSA	`last_https_certificate.public_key.rsa`	N/A
Indicator Attribute	Public Key EC	`last_https_certificate.public_key.ec`	N/A
Related Indicator	N/A	`last_https_certificate.thumbprint_sha256`	SHA-256
Indicator Attribute	Tag	`last_https_certificate.tags`	N/A
Indicator Attribute	Signature Algorithm	`last_https_certificate.signature_algorithm`	N/A
Indicator Attribute	Certificate Subject	`last_https_certificate.subject`	N/A
Indicator Attribute	Certificate Validity	`last_https_certificate.validity`	N/A
Indicator Attribute	Certificate Version	`last_https_certificate.version`	N/A
Indicator Attribute	Certificate Policies	`last_https_certificate.extensions.certificate_policies`	N/A
Indicator Attribute	Extended Key Usage	`last_https_certificate.extensions.extended_key_usage`	N/A
Indicator Attribute	Subject Alternative Name	`last_https_certificate.extensions.subject_alternative_name`	N/A
Indicator Attribute	Tag	`last_https_certificate.extensions.tags`	N/A
Indicator Attribute	Certificate Subject Key Identifier	`last_https_certificate.extensions.subject_key_identifier`	N/A
Indicator Attribute	CRL Distribution Points	`last_https_certificate.extensions.crl_distribution_points`	N/A
Indicator Attribute	Key Usage	`last_https_certificate.extensions.key_usage`	N/A
Indicator Attribute	CA	`last_https_certificate.extensions.CA`	N/A
Indicator Attribute	CA Information Access	`last_https_certificate.extensions.ca_information_access`	N/A
Indicator Attribute	Certificate Signature	`last_https_certificate.cert_signature`	N/A
Indicator Attribute	Certificate Serial Number	`last_https_certificate.serial_number`	N/A
Indicator Attribute	Certificate Thumbprint	`last_https_certificate.thumbprint`	N/A
Indicator Attribute	Certificate Issuer	`last_https_certificate.issuer`	N/A
Indicator Attribute	Certificate Size	`last_https_certificate.size`	N/A
Indicator Attribute	Positives	`positives`	N/A

TQ	TQ ATTRIBUTE NAME	VIRUSTOTAL	INDICATOR TYPE
Indicator Attribute	Scan Date	`date`	N/A
Indicator Attribute	Total	`total`	N/A

submit_domain

The submit_domain action uses the `https://www.virustotal.com/vtapi/v2/domain/report` endpoint.

TQ	TQ ATTRIBUTE NAME	VIRUSTOTAL	INDICATOR TYPE
Related Indicators	N/A	`detected_downloaded_samples[].sha256`, `undetected_referrer_samples[].sha256`, `undetected_downloaded_samples[].sha256`, `detected_referrer_samples[].sha256`, `undetected_communicating_samples[].sha256`, `detected_communicating_samples[].sha256`	SHA-256
Related Indicator Attributes	Positives	`detected_downloaded_samples[].positives` , `undetected_referrer_samples[].positives` , `undetected_downloaded_samples[].positives` , `detected_referrer_samples[].positives` , `undetected_communicating_samples[].positives` , `detected_communicating_samples[].positives` , `detected_urls[].positives`	N/A
Related Indicator Attributes	Total	`detected_downloaded_samples[].total` , `undetected_referrer_samples[].total` , `undetected_downloaded_samples[].total` , `detected_referrer_samples[].total` , `undetected_communicating_samples[].total` , `detected_communicating_samples[].total` , `detected_urls[].total`	N/A
Related Indicator Attributes	Date	`detected_downloaded_samples[].date` , `undetected_referrer_samples[].date` , `undetected_downloaded_samples[].date` , `detected_referrer_samples[].date` , `undetected_communicating_samples[].date` `detected_communicating_samples[].date` `detected_urls[].scan_date`	N/A
Related Indicators	N/A	`resolutions[].ip_address`	IP Address
Related Indicator Attributes	Last Resolved	`resolutions[].last_resolved`	N/A
Related Indicators	N/A	`domain_siblings[]`	FQDN
Related Indicators	N/A	`subdomains[]`	FQDN
Related Indicators	N/A	`detected_urls[].url`	URL
Indicator Attribute	VirusTotal Category	`categories`	N/A
Indicator Attribute	VirusTotal Whois Timestamp	`whois_timestamp`	N/A
Indicator Attribute	VirusTotal Whois	`whois`	N/A
Indicator Attribute	VirusTotal BitDefender category	`BitDefender category`	N/A
Indicator Attribute	VirusTotal Dr.Web category	`Dr.Web category`	N/A
Indicator Attribute	VirusTotal Opera domain info	`Opera domain info`	N/A
Indicator Attribute	VirusTotal Websense ThreatSeeker category	`Websense ThreatSeeker category`	N/A

TQ	TQ ATTRIBUTE NAME	VIRUSTOTAL	INDICATOR TYPE
Indicator Attribute	VirusTotal Webutation Domain Info Safety score	`Webutation Domain Info.Safety score`	N/A
Indicator Attribute	VirusTotal Webutation Domain Info Adult content	`Webutation Domain Info.Adult content`	N/A
Indicator Attribute	VirusTotal Webutation Domain Info Verdict	`Webutation Domain Info.Verdict`	N/A
Indicator Attribute	VirusTotal Verbose Response	`verbose_msg`	N/A
Indicator Attribute	VirusTotal Alexa Category	`Alexa category`	N/A
Indicator Attribute	VirusTotal Dns Records Date	`dns_records_date`	N/A
Indicator Attribute	Public Key Algorithm	`last_https_certificate.public_key.algorithm`	N/A
Indicator Attribute	Public Key RSA	`last_https_certificate.public_key.rsa`	N/A
Indicator Attribute	Public Key EC	`last_https_certificate.public_key.ec`	N/A
Related Indicator	N/A	`last_https_certificate.thumbprint_sha256`	SHA-256
Indicator Attribute	Tag	`last_https_certificate.tags`	N/A
Indicator Attribute	Signature Algorithm	`last_https_certificate.signature_algorithm`	N/A
Indicator Attribute	Certificate Subject	`last_https_certificate.subject`	N/A
Indicator Attribute	Certificate Validity	`last_https_certificate.validity`	N/A
Indicator Attribute	Certificate Version	`last_https_certificate.version`	N/A
Indicator Attribute	Certificate Policies	`last_https_certificate.extensions.certificate_policies`	N/A
Indicator Attribute	Extended Key Usage	`last_https_certificate.extensions.extended_key_usage`	N/A
Indicator Attribute	Subject Alternative Name	`last_https_certificate.extensions.subject_alternative_name`	N/A
Indicator Attribute	Tag	`last_https_certificate.extensions.tags`	N/A
Indicator Attribute	Certificate Subject Key Identifier	`last_https_certificate.extensions.subject_key_identifier`	N/A
Indicator Attribute	CRL Distribution Points	`last_https_certificate.extensions.crl_distribution_points`	N/A
Indicator Attribute	Key Usage	`last_https_certificate.extensions.key_usage`	N/A
Indicator Attribute	CA	`last_https_certificate.extensions.CA`	N/A

TQ	TQ ATTRIBUTE NAME	VIRUSTOTAL	INDICATOR TYPE
Indicator Attribute	CA Information Access	`last_https_certificate.extensions.ca_information_access`	N/A
Indicator Attribute	Certificate Signature	`last_https_certificate.cert_signature`	N/A
Indicator Attribute	Certificate Serial Number	`last_https_certificate.serial_number`	N/A
Indicator Attribute	Certificate Thumbprint	`last_https_certificate.thumbprint`	N/A
Indicator Attribute	Certificate Issuer	`last_https_certificate.issuer`	N/A
Indicator Attribute	Certificate Size	`last_https_certificate.size`	N/A
Indicator Attribute	VirusTotal Wot Domain Info	`WOT domain info`	N/A
Indicator Attribute	Websense ThreatSeeker Category	`Websense ThreatSeeker Category`	N/A
Indicator Attribute	VirusTotal HTTPS Certificate Date	`https_certificate_date`	N/A
Indicator Attribute	VirusTotal Alexa Domain Info	`Alexa Domain Info`	N/A
Indicator Attribute	VirusTotal Bitdefender Domain Info	`BitDefender domain info`	N/A
Indicator Attribute	VirusTotal Forcepoint Threatseeker Category	`Forcepoint ThreatSeeker category`	N/A
Indicator Attribute	VirusTotal Favicon	`favicon`	N/A
Indicator Attribute	VirusTotal Trendmicro Category	`TrendMicro category`	N/A
Indicator Attribute	Majestic Rank	`popularity_ranks.Majestic.rank`	N/A
Indicator Attribute	Statvoo Ranks	`popularity_ranks.Statvoo.rank`	N/A
Indicator Attribute	Alexa Ranks	`popularity_ranks.Alexa.rank`	N/A
Indicator Attribute	Cisco Umbrella Ranks	`popularity_ranks.Cisco Umbrella.rank`	N/A
Indicator Attribute	Quantcast Ranks	`popularity_ranks.Quantcast.rank`	N/A
Indicator Attribute	DNS Records	`dns_records`	N/A
Indicator Attribute	Positives	`positives`	N/A
Indicator Attribute	Scan Date	`date`	N/A

TQ	TQ ATTRIBUTE NAME	VIRUSTOTAL	INDICATOR TYPE
Indicator Attribute	Total	`total`	N/A

submit_url

The submit_url action uses the following endpoints:

- scan - https://www.virustotal.com/vtapi/v2/url/scan
- report - https://www.virustotal.com/vtapi/v2/url/report

scan

When initially running the `submit_url` action on an indicator, the scan endpoint is used to send the url to VirusTotal for analysis, which returns a `Virus Total Scan ID` that will be used in the report endpoint in order to retrive the analysis report.

TQ	TQ ATTRIBUTE NAME	VIRUSTOTAL	INDICATOR TYPE
Indicator Attribute	VirusTotal Permanent Link	`permalink`	N/A
Indicator Attribute	VirusTotal Scan ID	`scan_id`	N/A

report

The second time the `submit_url action` is executed on the indicator, the `VirusTotal Scan ID`; attribute, obtained from the scan endpoint, is used by the `report` endpoint.

All the related indicators are related to the enriched indicator.

TQ	TQ ATTRIBUTE NAME	VIRUSTOTAL	INDICATOR TYPE
Related Indicator #1	N/A	`url`	URL
Related Indicator #1 & Indicator Attributes	first_seen	`published_at`	N/A
Related Indicator #2	N/A	`additional_info.resolution`	IP Address
Related Indicator #2 Attributes	Resolution Country	`additional_info.resolution_country`	N/A
Indicator Attribute	Positives	`positives`	N/A
Indicator Attribute	Scan date	`scan_date`	N/A
Indicator Attribute	File Scan ID	`filescan_id`	N/A
Indicator Attribute	Total	`total`	N/A
Indicator Attribute	Last Seen	`attribute`	N/A
Indicator & Related Indicator #1 Attribute	Sophos Description	`additional_info.Sophos description`	N/A
Indicator & Related Indicator #1 Attribute	Sophos Description	`additional_info.BitDefender Category`	N/A
Indicator & Related Indicator #1 Attribute	URL Contact Error	`additional_info.URL contact error`	N/A
Indicator & Related Indicator #1 Attribute	Forcepoint ThreatSeeker Category	`additional_info.Forcepoint ThreatSeeker category`	N/A

TQ	TQ ATTRIBUTE NAME	VIRUSTOTAL	INDICATOR TYPE
Indicator & Related Indicator #1 Attribute	Redirector	`additional_info.redirector`	N/A
Indicator & Related Indicator #1 Attribute	`scans[].dict_key` Scan: Did/Did NOT `(if scans.detected)` Detect - `scans.result` with detail `scans.detail`	`scans[]`	N/A
Indicator & Related Indicator #1 Attribute	VirusTotal PermaLink	`permalink`	N/A

submit_file

The submit_file action uses the following endpoints:

- scan - `https://www.virustotal.com/vtapi/v2/file/scan`
- report - `https://www.virustotal.com/vtapi/v2/file/report`

scan

When initially running the `submit_file` action on an indicator, the scan endpoint is used to send the url to VirusTotal for analysis, which returns a `VirusTotal Scan ID` that will be used in the report endpoint in order to retrive the analysis report.

TQ	TQ ATTRIBUTE NAME	VIRUSTOTAL	INDICATOR TYPE
Related Indicator	N/A	`md5`	MD5
Related Indicator	N/A	`sha1`	SHA-1
Related Indicator	N/A	`sha256`	SHA-256
Indicator Attribute	VirusTotal Permanent Link	`permalink`	N/A
Indicator & Threat File Attribute	VirusTotal Scan ID	`scan_id`	N/A

report

The second time the submit_file action is executed on the indicator, the `VirusTotal Scan ID` attribute, obtained from the scan endpoint, is used by the `report` endpoint.

All the related indicators are related to the enriched indicator.

TQ	TQ ATTRIBUTE NAME	VIRUSTOTAL	INDICATOR TYPE
Related Indicator #1	N/A	`md5`	MD5
Related Indicator #1	N/A	`sha1`	SHA-1
Related Indicator #1	N/A	`sha256`	SHA-256
Related Indicator #1	N/A	`ssdeep`	Fuzzy Hash
Related Indicator #1	N/A	`authentihash`	Fuzzy Hash
Related Indicator `authentihash` Attribute	Authenticode Hash: "Yes"	N/A	N/A
ThreatFile, Related Indicator #1 Attribute	VirusTotal File Type	`type`	N/A
ThreatFile, Related Indicator #1 Attribute	VirusTotal Unique Sources	`unique_sources`	N/A

TQ	TQ ATTRIBUTE NAME	VIRUSTOTAL	INDICATOR TYPE
ThreatFile, Related Indicator #1 Attribute	Published at	`first_seen`	N/A
ThreatFile, Related Indicator #1 Attribute	Positives	`positives`	N/A
ThreatFile, Related Indicator #1 Attribute	Total	`total`	N/A
ThreatFile, Related Indicator #1 Attribute	VirusTotal Community Reputation	`community_reputation`	N/A
ThreatFile, Related Indicator #1 Attribute	VirusTotal Harmless Votes	`harmless_votes`	N/A
ThreatFile, Related Indicator #1 Attribute	VirusTotal Malicious Votes	`malicious_votes`	N/A
ThreatFile Attribute	VirusTotal Verbose Response	`verbose_msg`	N/A
ThreatFile, Related Indicator #1 Attribute	VirusTotal PermaLink	`permalink`	N/A
ThreatFile, Related Indicator #1 Attribute	Scan Date	`scan_date`	N/A
Related Indicator #2	N/A	`submission_names`	FilePath / FileName
ThreatFile Attributes	`scans[].dict_key` Scan: `(if scans.detected) scans.result` Detected on `scans.update` with version `scans.version (else if not scans.detected) scans.version` NOT Detected on `scans.update`	`scans`	N/A
ThreatFile Attributes	Portable Executable Timestamp	`additional_info.pe-timestamp`	N/A
ThreatFile Attributes	`additional_info.exiftool.dict_key` ExifTool	`additional_info.exiftool`	N/A
Related Indicator #3	N/A	`additional_info.pe-imphash`	MD5
Related Indicator `additional_info.pe-imphash` Attribute	Import Hash: 'Yes'	N/A	N/A
ThreatFile Attributes	Portable Executable `additional_info.pe-resource-langs.dict_key` Lang	`additional_info.pe-resource-langs`	N/A
ThreatFile Attributes	DeepGuard	`additional_info.deepguard`	N/A
ThreatFile Attributes	Sigcheck `additional_info.sigcheck`	`additional_info.sigcheck`	N/A
ThreatFile Attributes	Positives Delta	`additional_info.positives_delta`	N/A
ThreatFile Attributes	Portable Executable Machine Type	`additional_info.pe-machine-type`	N/A
ThreatFile Attributes	TrID	`additional_info.trid`	N/A
ThreatFile Attributes	VirusTotal Private API Magic	`additional_info.magic`	N/A
Related Indicator #3	N/A	`additional_info.main_icon.raw_md5`	MD5

TQ	TQ ATTRIBUTE NAME	VIRUSTOTAL	INDICATOR TYPE
Related Indicator `additional_info.main_icon.raw_md5` Attribute	Main Icon: 'Yes'	N/A	N/A
Related Indicator #3 Attribute	Main Icon DHash	`additional_info.main_icon.dhash`	N/A
ThreatFile Attribute	Process Name	`additional_info.behaviour-v1.process.tree.name`	N/A
ThreatFile Attribute	Runtime DLL: Successfully Run / Failed to Run `(if additional_info.behaviour-v1.runtime-dlls.success) additional_info.behaviour-v1.runtime-dlls.file`	`additional_info.behaviour-v1.runtime-dlls`	N/A
Related Indicator #4	N/A	`additional_info.behaviour-v1.mutex.opened`	Mutex
Related Indicator `additional_info.behaviour-v1.mutex.opened` Attribute	`additional_info.behaviour-v1.mutex.opened.mutex`: Opened Mutex	N/A	N/A
Related Indicator #4	N/A	`additional_info.behaviour-v1.created`	Mutex
Related Indicator `additional_info.behaviour-v1.created` Attribute	`additional_info.behaviour-v1.created.mutex`: Created Mutex	N/A	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.opened`	FilePath
Related Indicator `additional_info.behaviour-v1.filesystem.opened` Attribute	`additional_info.behaviour-v1.filesystem.opened.path`: File Successfully Opened	N/A	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.read`	FilePath
Related Indicator `additional_info.behaviour-v1.filesystem.read` Attribute	`additional_info.behaviour-v1.filesystem.read.path`: File Successfully Read	N/A	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.moved`	FilePath
Related Indicator `additional_info.behaviour-v1.filesystem.moved` Attribute	`additional_info.behaviour-v1.filesystem.read.moved`: File Successfully Moved	N/A	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.downloaded`	FilePath
Related Indicator `additional_info.behaviour-v1.filesystem.downloaded` Attribute	`additional_info.behaviour-v1.filesystem.read.downloaded`: File Successfully Downloaded	N/A	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.written`	FilePath

TQ	TQ ATTRIBUTE NAME	VIRUSTOTAL	INDICATOR TYPE
Related Indicator `additional_info.behaviour-v1.filesystem.written` Attribute	`additional_info.behaviour-v1.filesystem.read.written`: File Successfully Written	N/A	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.replaced`	FilePath
Related Indicator `additional_info.behaviour-v1.filesystem.replaced` Attribute	`additional_info.behaviour-v1.filesystem.read.replaced`: File Successfully Replaced	N/A	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.deleted`	FilePath
Related Indicator `additional_info.behaviour-v1.filesystem.deleted` Attribute	`additional_info.behaviour-v1.filesystem.read.deleted`: File Successfully Deleted	N/A	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.copied`	FilePath
Related Indicator `additional_info.behaviour-v1.filesystem.copied` Attribute	`additional_info.behaviour-v1.filesystem.read.copied`: File Successfully Copied	N/A	N/A
ThreatFile Attribute	Portable Executable Resource Type `additional_info.pe-resource-types.dict_key`	`additional_info.pe-resource-types`	N/A
Related Indicator #4	N/A	`additional_info.network_infrastructure`	URL
ThreatFile Attribute	Portable Executable Entry Point	`additional_info.pe-entry-point`	N/A
Related Indicator #5	N/A	`additional_info.pe-resource-detail[].sha256`	SHA-256
Related Indicator #5 Attribute	Portable Executable Language"	`additional_info.pe-resource-detail[].lang`	N/A
Related Indicator #5 Attribute	Portable Executable Chi Squared"	`additional_info.pe-resource-detail[].chi2`	N/A
Related Indicator #5 Attribute	Portable Executable File Type"	`additional_info.pe-resource-detail[].filetype`	N/A
Related Indicator #5 Attribute	Portable Executable Entropy"	`additional_info.pe-resource-detail[].entropy`	N/A
Related Indicator #5 Attribute	Portable Executable Type"	`additional_info.pe-resource-detail[].type`	N/A
Related Indicator #6	N/A	`additional_info.contacted_domains`	FQDN

TQ	TQ ATTRIBUTE NAME	VIRUSTOTAL	INDICATOR TYPE
Related Indicator `additional_info.contacted_domains` Attribute	Malware Contacted Domain: Yes	N/A	N/A
ThreatFile, Related Indicator #1 Attribute	Officecheck Document Summary Info `additional_info.officecheck.document_summary_info.dict_hey`	`additional_info.officecheck.document_summary_info`	N/A
ThreatFile, Related Indicator #1 Attribute	Officecheck Summary Info `additional_info.officecheck.summary_info.dict_hey`	`additional_info.officecheck.summary_info`	N/A
ThreatFile, Related Indicator #1 Attribute	Library imported from `additional_info.imports.dict_hey`	`additional_info.imports`	N/A

submit_hash

The submit_hash action uses the `https://www.virustotal.com/vtapi/v2/file/report endpoint.`

Mapping for this action is the same as submit_file - report.

Change Log

- **Version 2.3.0**
  - `Submit URL` - FQDN indicators can't be submitted through this action anymore
  - `Submit IP` - `.asn` attribute ingested as ASN indicator
  - Minor tweaking for ingested attributes
- **Version 2.2.2**
  - Minor UI Enhancements
  - Improved error handling
  - Removed `.undetected_urls` parsing for IPs and FQDNs
  - Added `Automatically add attributes` and `Automatically add indicators` user fields
- **Version 2.2.1**
  - Improved enrichment attributes UI formatting
- **Version 2.2.0**
  - Improve UI messages, add new user field, mapping changes
- **Version 1.0.0**
  - Initial release