ThreatQuotient

VirusTotal Operation Implementation Guide

Version 2.1.0

Monday, March 30, 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.

Last Updated: Monday, March 30, 2020

Contents

Versioning

- **Operation Version**: 2.1.0
- **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 or upgrade the VirusTotal operation.

1. Log into https://marketplace.threatq.com.
2. Locate and download the VirusTotal operation file.
3. Navigate to your ThreatQ instance.
4. From the ThreatQ navigation menu, choose the **Settings** icon > **Operations Management**.
5. Click on the **Install Operation** button.
6. Perform one of the following options:
   - Drag and drop the operation file into the dialog box.
   - Select **Click to browse** to locate the operation file on your local machine.

   

   If the operation already exists on the platform, ThreatQ will inform you that the operation already exists on the platform and will require confirmation to continue with the installation process.

   The Operation will appear in your list of installed operations once the installation process has completed. You will still need to configure and then enable the operation.

Operation Configuration

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

To Configure the VirusTotal Operation:

1. Click on the **Settings** icon and select **Operations Management**
2. Locate the **VirusTotal** operation and click on **Operation Settings**.
3. Enter the following configuration parameters:

Parameter	Description
API Key	The private or public VirusTotal API key.
Auto Enrichment	If checked, indicator attributes are added automatically.

4. Click on **Save Changes** then click on the toggle switch next to the operation name to enable the operation.

Actions

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, FQDN
submit_file	Submits file for analysis	ThreatFile	
submit_hash	Submits hash for analysis	Indicator	MD5, SHA-1, SHA-256

submit_ip

Uses the https://www.virustotal.com/vtapi/v2/ip-address/report endpoint

ThreatQ	ThreatQ 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`,	N/A

ThreatQ	ThreatQ Attribute Name	VirusTotal	Indicator Type
		`detected_communicating_samples[].positives`, `undetected_communicating_samples[].positives`, `detected_urls[].positives`	
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`,	N/A

ThreatQ	ThreatQ Attribute Name	VirusTotal	Indicator Type
		`detected_referrer_samples[].date`, `detected_communicating_samples[].date`, `undetected_communicating_samples[].date`, `detected_urls[].scan_date`	
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
Indicator Attribute	VirusTotal ASN	`asn`	N/A
Indicator Attribute	VirusTotal Whois	`whois`	N/A
Indicator Attribute	VirusTotal Country	`country`	N/A
Indicator Attribute	VirusTotal Verbose Response	`verbose_msg`	N/A

submit_domain

Uses the https://www.virustotal.com/vtapi/v2/domain/report endpoint.

ThreatQ	ThreatQ Attribute Name	Virus Total	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_`	N/A

ThreatQ	ThreatQ Attribute Name	Virus Total	Indicator Type
		`samples[].positives`, `detected_communicating_samples[].positives`, `detected_urls[].positives`	
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`	N/A

ThreatQ	ThreatQ Attribute Name	Virus Total	Indicator Type

		`[].date`,
		`detected_referrer_samples[].date`,
		`undetected_communicating_samples[].date`
		`detected_communicating_samples[].date`
		`detected_urls[].scan_date`	

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	VirusTotal Whois	`whois_timestamp`	N/A

ThreatQ	ThreatQ Attribute Name	Virus Total	Indicator Type
Attribute	Timestamp		
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
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

submit_url

Uses the https://www.virustotal.com/vtapi/v2/url/scan and https://www.virustotal.com/vtapi/v2/url/report endpoints.

scan

By running the action the first time on an indicator, the 'scan' endpoint is used to send the url to VirusTotal for analysis, returning a scan ID that will be used in the report endpoint in order to retrieve the analysis report.

ThreatQ	ThreatQ 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 action is executed on the indicator that has a 'VirusTotal Scan ID' attribute, the 'report' endpoint is used.

All the related indicators are related to the enriched indicator and the report object.

ThreatQ	ThreatQ Attribute Name	VirusTotal	Indicator Type
Related Indicator #1	N/A	`url`	URL

ThreatQ	ThreatQ Attribute Name	VirusTotal	Indicator Type
Related Indicator #1 & Indicator Attributes	first_seen	`published_at`	N/A
Related Indicator #2	N/A	`additional_info.resolution`	IP Address
Related Indicator #2 Attrib-utes	Resolution Country	`additional_info.resolution_country`	N/A
Report	"VirusTotal Report for `Indicator.value`"	N/A	N/A
Related Attribute	Positives	`positives`	N/A
Related Attribute	File Scan ID	`filescan_id`	N/A
Related Attribute	Total	`total`	N/A
Related Attribute	Last Seen	`attribute`	N/A
Report & Related	Sophos Description	`additional_info.Sophos`	N/A

ThreatQ	ThreatQ Attribute Name	VirusTotal	Indicator Type
Indicator #1 Attribute		`description`	
Report & Related Indicator #1 Attribute	Sophos Description	`additional_info.BitDefender Category`	N/A
Report & Related Indicator #1 Attribute	URL Contact Error	`additional_info.URL contact error`	N/A
Report & Related Indicator #1 Attribute	Forcepoint ThreatSeeker Category	`additional_info.Forcepoint ThreatSeeker category`	N/A
Report & Related Indicator #1 Attribute	Redirector	`additional_info.redirector`	N/A
Report & Related	`scans[].dict_key` Scan: Did/Did NOT `(if scans.detected)`	`scans[]`	N/A

ThreatQ	ThreatQ Attribute Name	VirusTotal	Indicator Type
Indicator #1 Attribute	Detect - `scans.result` with detail `scans.detail`		

submit_file

Uses the https://www.virustotal.com/vtapi/v2/file/report and https://www.virustotal.com/vtapi/v2/file/scan endpoints.

scan

By running the action the first time on an indicator, the 'scan' endpoint is used to send the file to VirusTotal for analysis, returning a scan ID that will be used in the report endpoint in order to retrieve the analysis report.

ThreatQ	ThreatQ 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

All the related indicators are related to the enriched indicator and the report object.

ThreatQ	ThreatQ Attribute Name	VirusTotal
Related Indicator #1	N/A	`md5`
Related Indicator #1	N/A	`sha1`
Related Indicator #1	N/A	`sha256`
Related Indicator #1	N/A	`ssdeep`
Related Indicator #1	N/A	`authentihash`
Related Indicator `authentihash` Attribute	Authenticode Hash: "Yes"	N/A
Report	"VirusTotal Report for `ThreatFile.title`"	N/A
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal File Type	`type`
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal Unique Sources	`unique_sources`
ThreatFile, Related Indicator #1 Attribute	Published at	`first_seen`
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal Number of Positives	`positives`

ThreatQ	ThreatQ Attribute Name	VirusTotal
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal Community Reputation	`community_reputation`
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal Harmless Votes	`harmless_votes`
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal Malicious Votes	`malicious_votes`
Report Attribute	VirusTotal Verbose Response	`verbose_msg`
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal PermaLink	`permalink`
ThreatFile, Report, Related Indicator #1 Attribute	VirusTotal Scan Date	`scan_date`
Related Indicator #2	N/A	`submission_names`
Report Attributes	`scans[].dict_key` Scan: `(if scans.detected)` `scans.result`Detected on `scans.update` with version `scans.version(else if not scans.detected)`	`scans`

ThreatQ	ThreatQ Attribute Name	VirusTotal
	`scans.version` NOT Detected on `scans.update`	
Report Attributes	Portable Executable Timestamp	`additional_info.pe-timestamp`
Report Attributes	`additional_info.exiftool.dict_key` ExifTool	`additional_info.exiftool`
Related Indicator #3	N/A	`additional_info.pe-imphash`
Related Indicator `additional_info.pe-imphash` Attribute	Import Hash: 'Yes'	N/A
Report Attributes	Portable Executable `additional_info.pe-resource-langs.dict_key` Lang	`additional_info.pe-resource-langs`
Report Attributes	DeepGuard	`additional_info.deepguard`
Report Attributes	Sigcheck `additional_info.sigcheck`	`additional_info.sigcheck`
Report Attributes	Positives Delta	`additional_info.positives_delta`
Report Attributes	Portable Executable Machine Type	`additional_info.pe-machine-type`

ThreatQ	ThreatQ Attribute Name	VirusTotal
Report Attributes	TrID	`additional_info.trid`
Report Attributes	VirusTotal Private API Magic	`additional_info.magic`
Related Indicator #3	N/A	`additional_info.main_icon.raw_md5`
Related Indicator `additional_info.main_icon.raw_md5` Attribute	Main Icon: 'Yes'	N/A
Related Indicator #3 Attribute	Main Icon DHash	`additional_info.main_icon.dhash`
Report Attribute	Process Name	`additional_info.behaviour-v1.process.tree.name`
Report 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`
Related Indicator #4	N/A	`additional_info.behaviour-v1.mu-`

ThreatQ	ThreatQ Attribute Name	VirusTotal
		tex.opened
Related Indicator addi-tional_info.be-haviour-v1.mutex.opened Attribute	additional_info.be-haviour-v1.mu-tex.opened.mutex: Opened Mutex	N/A
Related Indicator #4	N/A	additional_info.be-haviour-v1.created
Related Indicator addi-tional_info.be-haviour-v1.created Attribute	additional_info.be-haviour-v1.cre-ated.mutex: Created Mutex	N/A
Related Indicator #2	N/A	additional_info.be-haviour-v1.-filesystem.opened
Related Indicator addi-tional_info.be-haviour-v1.-filesystem.opened Attribute	additional_info.be-haviour-v1.-filesys-tem.opened.path: File Successfully Opened	N/A
Related Indicator #2	N/A	additional_info.be-haviour-v1.-filesystem.read
Related Indicator addi-	additional_info.be-	N/A

ThreatQ	ThreatQ Attribute Name	VirusTotal
tional_info.be-haviour-v1.mu-tex.opened Attribute	haviour-v1.-filesystem.read.path: File Successfully Read	
Related Indicator #2	N/A	additional_info.be-haviour-v1.-filesystem.moved
Related Indicator addi-tional_info.be-haviour-v1.-filesystem.opened Attribute	additional_info.be-haviour-v1.-filesystem.read.moved: File Successfully Moved	N/A
Related Indicator #2	N/A	additional_info.be-haviour-v1.-filesys-tem.downloaded
Related Indicator addi-tional_info.be-haviour-v1.-filesys-tem.downloaded Attribute	additional_info.be-haviour-v1.-filesys-tem.read.downloaded: File Successfully Down-loaded	N/A
Related Indicator #2	N/A	additional_info.be-haviour-v1.-filesystem.written

ThreatQ	ThreatQ Attribute Name	VirusTotal
Related Indicator `additional_info.behaviour-v1.filesystem.written` Attribute	`additional_info.behaviour-v1.filesystem.read.written`: File Successfully Written	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.replaced`
Related Indicator `additional_info.behaviour-v1.filesystem.replaced` Attribute	`additional_info.behaviour-v1.filesystem.read.replaced`: File Successfully Replaced	N/A
Related Indicator #2	N/A	`additional_info.behaviour-v1.filesystem.deleted`
Related Indicator `additional_info.behaviour-v1.filesystem.deleted` Attribute	`additional_info.behaviour-v1.filesystem.read.deleted`: File Successfully Deleted	N/A
Related Indicator #2	N/A	`additional_info.be-`

ThreatQ	ThreatQ Attribute Name	VirusTotal
		haviour-v1.-filesystem.copied
Related Indicator additional_info.behaviour-v1.-filesystem.copied Attribute	additional_info.behaviour-v1.-filesystem.read.copied: File Successfully Copied	N/A
Report Attribute	Portable Executable Resource Type additional_info.pe-resource-types.dict_key	additional_info.pe-resource-types
Related Indicator #4	N/A	additional_info.network_infrastructure
Report Attribute	Portable Executable Entry Point	additional_info.pe-entry-point
Related Indicator #5	N/A	additional_info.pe-resource-detail[].sha256
Related Indicator #5 Attribute	Portable Executable Language"	additional_info.pe-resource-detail[].lang
Related Indicator #5 Attribute	Portable Executable Chi Squared"	additional_info.pe-resource-detail

ThreatQ	ThreatQ Attribute Name	VirusTotal
		`[].chi2`
Related Indicator #5 Attribute	Portable Executable File Type"	`additional_info.pe-resource-detail [].filetype`
Related Indicator #5 Attribute	Portable Executable Entropy"	`additional_info.pe-resource-detail [].entropy`
Related Indicator #5 Attribute	Portable Executable Type"	`additional_info.pe-resource-detail [].type`
Related Indicator #6	N/A	`additional_info.-contacted_domains`
Related Indicator `addi-tional_info.-contacted_domains` Attribute	Malware Contacted Domain: Yes	N/A
ThreatFile, Related Indicator #1 Attribute	Officecheck Document Summary Info `additional_info.of-ficecheck.document_sum-mary_info.dict_hey`	`additional_info.of-ficecheck.document_summary_info`
ThreatFile, Related Indicator #1 Attribute	Officecheck Summary Info `additional_info.of-ficecheck.summary_`	`additional_info.of-ficecheck.summary_info`

ThreatQ	ThreatQ Attribute Name	VirusTotal
	`info.dict_hey`	
ThreatFile, Report, Related Indicator #1 Attribute	Library imported from `additional_info.imports.dict_hey`	`additional_info.imports`

submit_hash

Uses the https://www.virustotal.com/vtapi/v2/file/report endpoint

Mapping is the same as submit_file - report.