ThreatQuotient

A Securonix Company

Hybrid Analysis Operation

Version 1.2.0

June 15, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.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: tq-support@securonix.com
Support Web: https://ts.securonix.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	1.2.0
Compatible with ThreatQ Versions	>= 4.34.0
Support Tier	ThreatQ Supported

Introduction

The Hybrid Analysis Operation for ThreatQuotient enables a ThreatQ user to interact with Hybrid Analysis by fetching reports and submitting samples.

The operation provides the following actions:

- **Quick Scan** - sends an IOC or attachment to be quickly scanned by Hybrid Analysis and its' integrated scan engines.
- **Sandbox** - sends an IOC or attachment to the Hybrid Analysis Sandbox for a complete detonation.
- **Get Reports** - retrieves reports from Hybrid Analysis scans.

The operation is compatible with the following system objects:

- Files (Attachments)
- Indicators (FQDN, URL, Filename, SHA-1, SHA-256, IP Address)

Prerequisites

The following is required to use the integration:

- A Hybrid Analysis domain name and 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 whl file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the whl file using one of the following methods:
    - Drag and drop the file into the dialog box
    - Select **Click to Browse** to locate the file on your local machine

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

The operation is now installed and will be displayed in the ThreatQ UI. 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 integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Key	Your Hybrid Analysis API Token.
Domain	The domain name associated with Hybrid Analysis.

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.

Actions

The operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Quick Scan	Sends an IOC or attachment to be quickly scanned by Hybrid Analysis and its' integrated scan engines.	Indicators, Files	FQDN, URL (Indicators)
Sandbox	Sends an IOC or attachment to the Hybrid Analysis Sandbox for a complete detonation.	Indicators, Files	FQDN, URL (Indicators)
Get Reports	Retrieves reports from Hybrid Analysis scans.	Indicators, Files	FQDN, URL, Filename, MD5, SHA-1, SHA-256, IP Address

Quick Scan

The Quick Scan action sends an IOC or attachment to be quickly scanned by Hybrid Analysis and its' integrated scan engines.

`POST https://hybrid-analysis.com/api/v2/quick-scan/{file-type}`

Sample Response:


```
  {
  "submission_type": "page_url",
  "id": "63b6f74f9e9d70709b420acb",
  "sha256": "8906304c8b5db5f96eb7236e6074510f8ca07d47afed20a6da2468ab26f3e383",
  "scanners": [
    {
      "name": "VirusTotal",
      "status": "in-queue",
      "error_message": null,
      "progress": 0,
      "total": null,
      "positives": null,
      "percent": null,
      "anti_virus_results": []
    },
    {
      "name": "urlscan.io",
      "status": "in-queue",
      "error_message": null,
      "progress": 0,
      "total": null,
      "positives": null,
      "percent": null,
      "anti_virus_results": []
    }
  ],
  "whitelist": [],
  "reports": [],
  "finished": false
}
```

ThreatQ provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
id	Indicator Attribute	Hybrid Analysis Quick Scan ID	N/A	63b6f74f9e9d70709b420acb	N/A
.scanners_v2[].{SCANNER_NAME}.status	Indicator Attribute	{SCANNER_NAME} Disposition	N/A	In Queue	Mapped using the table `Hybrid Analysis Scan Status`
.scanners_v2[].{SCANNER_NAME}.percent	Indicator.Attribute	{SCANNER_NAME} Detection Rate	N/A	`0%`	`%` is appended
.scanners_v2[].{SCANNER_NAME}.positives, .scanners_v2[].{SCANNER_NAME}.total	Indicator.Attribute	{SCANNER_NAME} Detections	N/A	`0/23`	Concatenated using `/`
.whitelist[].id, .whitelist[].value	Indicator.Attribute	{WHITELIST_ID} Whitelisted	N/A	`No`	Mapped to `Yes` or `No`.

The JSON key `.sha256` hash is used for a supplemental call to get additional report data. See below Get Reports Action for additional mapping.

Hybrid Analysis Scan Status

HYBRID ANALYSIS SCAN STATUS	THREATQ DISPOSITION ATTRIBUTE
no-result	No Result
no-classification	No Classification
in-queue	In Queue
clean	Clean
malicious	Malicious
unsure	Unsure

Run Configuration Options

> The following configuration option is set after selecting the action to run against an object and are not set from the operation's configuration screen.

The following configuration options are available for this operation action:

OPTION	DESCRIPTION
Default URL Scheme	Select the default URL scheme to use for the scan. This will be used if no scheme is provided in the URL or the attributes of the object. The default is HTTP.
Default Port	Enter the default port to use for the scan when scanning an IP Address. If this field is left blank, no port will be used.
Share with Third Parties	Enabling this will allow the sample to be shared with Hybrid Analysis' partners.
Scan Publicly	Enabling this will make all your scanned samples publicly viewable.

Sandbox

The Sandbox action sends an IOC or attachment to the Hybrid Analysis Sandbox for a complete analysis.

```
POST https://hybrid-analysis.com/api/v2/submit/{file-type}
```

Sample Response:

```
{
  "submission_type": "page_url",
  "job_id": "63b6fc72ebdd090dc9451590",
  "submission_id": "63b6fc72ebdd090dc9451591",
  "environment_id": 120,
  "sha256": "8906304c8b5db5f96eb7236e6074510f8ca07d47afed20a6da2468ab26f3e383"
}
```

Run Configuration Options

The following configuration option is set after selecting the action to run against an object and are not set from the operation's configuration screen.

The following configuration options are available for this operation action:

OPTION	DESCRIPTION
Environment	Select which environment you want your sample detonated in. Options include: • Windows 7 32 bit • Windows 7 32 bit (HWP Support) • Windows 7 64 bit (default) • Windows 11 64 bit • Windows 10 64 bit • Android Static Analysis • Linux (Ubuntu 24.04 64 bit) • macOS Tahoe

OPTION	DESCRIPTION
Action Script	Optional - select an action script to use during the detonation. Options include: • Default • Max Anti-Evasion • Random Files • Random Theme • Open Internet Explorer
Network Settings	Select network settings to use during analysis.
Password	The password for the file if you are using one for an Adobe/ Office file.
Default URL Scheme	Select the default URL scheme to use for the scan. This will be used if no scheme is provided in the URL or the attributes of the object. The default is `HTTP`.
Default Port	Enter the default port to use for the scan when scanning an IP Address. If this field is left blank, no port will be used.
Share with Third Parties	Enabling this will allow the sample to be shared with Hybrid Analysis' partners.
Scan Publicly	Enabling this will make all your scanned samples publicly viewable.

Get Reports

The Get Reports action sends the hash of an IOC or attachment to the Hybrid Analysis Sandbox for a summary.

`GET https://hybrid-analysis.com/api/v2/search/hash?hash={hash}`

The action searches uses the following for URL, FQDN, IP Address, and Filename indicators:

`POST https://hybrid-analysis.com/api/v2/search/terms`

Sample Response:


```
 [
 {
   "classification_tags": [],
   "tags": [],
   "submissions": [
     {
       "submission_id": "63b7bc54abedbd2ade303544",
       "filename": null,
       "url": "http://promocioninmobiliaria.cl/upl.txt",
       "created_at": "2023-01-06T06:14:44+00:00"
     }
   ],
   "machine_learning_models": [],
   "crowdstrike_ai": null,
   "job_id": null,
   "environment_id": null,
   "environment_description": "Static Analysis",
   "size": null,
   "type": null,
   "type_short": [],
   "target_url": null,
   "state": "SUCCESS",
   "error_type": null,
   "error_origin": null,
   "submit_name": "http://promocioninmobiliaria.cl/upl.txt",
   "md5": "bc3c087c7e45854c1999401d2edd9e19",
   "sha1": "00abc96e13fce7e94ad9958671da99da2cdb0c4c",
   "sha256": "40b28ef29b4ce766ddc150156204cffc6a6c29070d405bdf98878835f5dbfdca",
   "sha512":
"9119ad7a7ab8c8120bdd0f0bc5e430278914421e4e06f3a5d6847a06d6056d8302c05da65f
              4d55413fb1322d0dad01003041ed5d6169cd0720cc7f8bca2d332a",
   "ssdeep": null,
   "imphash": null,
   "entrypoint": null,
   "entrypoint_section": null,
   "image_base": null,
```

```
    "subsystem": null,
    "image_file_characteristics": [],
    "dll_characteristics": [],
    "major_os_version": null,
    "minor_os_version": null,
    "av_detect": 5,
    "vx_family": null,
    "url_analysis": true,
    "analysis_start_time": "2023-01-06T05:49:35+00:00",
    "threat_score": null,
    "interesting": false,
    "threat_level": 2,
    "verdict": "malicious",
    "certificates": [],
    "domains": [],
    "compromised_hosts": [],
    "hosts": [],
    "total_network_connections": 0,
    "total_processes": 0,
    "total_signatures": 0,
    "extracted_files": [],
    "file_metadata": null,
    "processes": [],
    "mitre_attcks": [],
    "network_mode": "default",
    "signatures": []
  }
]
```


ThreatQ provides the following default mapping for this Action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].md5	Related Indicator	MD5	N/A	bc3c087c7e45854c1999401d2edd9e19	N/A
[].sha1	Related Indicator	SHA1	N/A	00abc96e13fce7e94ad9958671da99da2cdb0c4c	N/A
[].sha512	Related Indicator	SHA512	N/A	9119ad7a7ab8c8120bdd0f0bc5e430278914421e4e06f3a5d6847a06d6056d8302c05da65f4d55413fb1322d0dad01003041ed5d6169cd0720cc7f8bca2d332a	N/A
[].submit_name	Related Indicator	URL	N/A	http://promocioninmobiliaria.cl/upl.txt	N/A
[].sha256, [].environment_id	Indicator.Attribute	Scan Link	N/A	https://hybrid-analysis.com/sample/40b28ef29b4ce766ddc150156204cffc6a6c29070d405bdf98878835f5dbfdca?environmentId=100	Composed using domain user field, [].sha256 and environment_id if [].environment_id is not null
[].sha256	Indicator.Attribute	Scan Link	N/A	https://hybrid-analysis.com/sample/40b28ef29b4ce766ddc150156204cffc6a6c29070d405bdf98878835f5dbfdca	Composed using domain user field and [].sha256 if [].environment_id is null
[].verdict	Indicator.Attribute	Hybrid Analysis Verdict	N/A	malicious	N/A
[].environment_description	Indicator.Attribute	Scan Environment	N/A	Static Analysis	N/A
[].av_detect	Indicator.Attribute	Detection rate	N/A	5	N/A
[].threat_level	Indicator.Attribute	Threat Level	N/A	2	N/A
[].type	Indicator.Attribute	File Type Description	N/A	N/A	If [].type is not null
[].type_short[]	Indicator.Attribute	File Type	N/A	N/A	If [].type_short[] is not empty
[].vx_family	Indicator.Attribute	Malware Family	N/A	N/A	If [].vx_family is not null
[].threat_score	Indicator.Attribute	Threat Score	N/A	N/A	If [].threat_score is not null
[].tags[]	Indicator.Attribute	Tag	N/A	N/A	If [].tags[] is not empty

Run Configuration Options

The following configuration option is set after selecting the action to run against an object and are not set from the operation's configuration screen.

The following configuration options are available for this operation action:

OPTION	DESCRIPTION
Default URL Scheme	Select the default URL scheme to use for the scan. This will be used if no scheme is provided in the URL or the attributes of the object. The default is HTTP.
Default Port	Enter the default port to use for the scan when scanning an IP Address. If this field is left blank, no port will be used.

Change Log

- **Version 1.2.0**
  - Updated the endpoint used by the **Get Report** action. The endpoint used by the action previously has been deprecated.
  - Enhanced support for IP Address indicators, including improved handling of HTTP schemes and port values.
  - Updated processing of `POST /search/terms` responses to align with current API response schemas.
  - Resolved an issue affecting the **Indirect Indicator Add** action.
  - Refreshed available Sandbox environment options to reflect current provider offerings
- **Version 1.1.1**
  - Updated the `Verdict` attribute to `Hybrid Analysis Verdict` for the Get Reports action.
- **Version 1.1.0**
  - Added a new action parameter, **Network Settings**, to replace the **Offline Analysis** field for the Sandbox action.
  - Resolved an issue for the Quick Scan action regarding FQDNs. If a domain was not found, the service would respond with an error.
  - Added improved error handling for actions.
- **Version 1.0.0**
  - Initial release