ThreatQuotient

Hybrid Analysis CDF

Version 1.2.3

July 01, 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	1.2.3
Compatible with ThreatQ Versions	>= 5.11.0
Support Tier	ThreatQ Supported

Introduction

The Hybrid Analysis CDF for ThreatQ allows a ThreatQ user to ingest sample reports from the public feed, as well as automatically ingest reports for samples submitted through ThreatQ, via the Hybrid Analysis Operation.

The CDF provides the following feeds:

- **Hybrid Analysis Public Feed** - enables the ingestion of public reports from Hybrid Analysis using their public feed.
- **Hybrid Analysis Submissions Feed** - enables the ingestion of reports from samples submitted through the Hybrid Analysis Operation from the ThreatQ platform.
- **Hybrid Analysis Quick Scans** - ingests quick scan results and sandbox reports for samples or URLs submitted by the Hybrid Analysis Operation.

The CDF ingests the following system objects:

- Attack Patterns
  - Attack Pattern Attributes
- Indicators
  - Indicator Attributes

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 integration yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the yaml 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
6. Select the feed(s) to install when prompted and click on **Install**.

   > 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.

7. The feed(s) will be added to the integrations page. You will still need to configure and then enable the feed(s).

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:

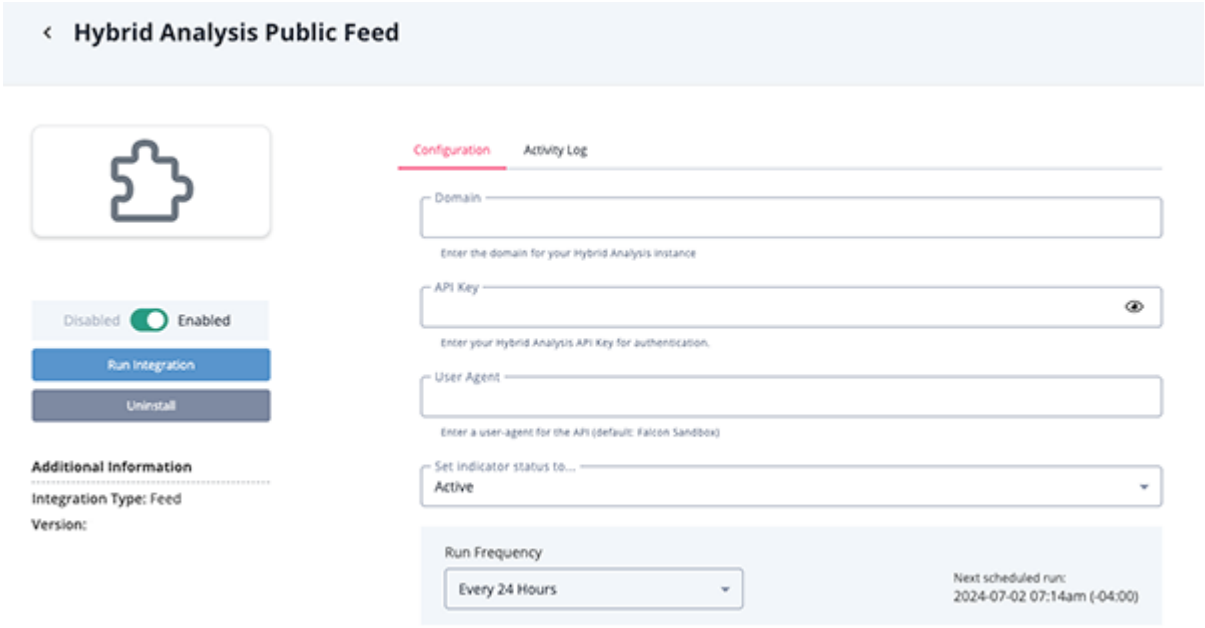
1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** option from the *Category* dropdown (optional).

   > 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 parameters under the **Configuration** tab:

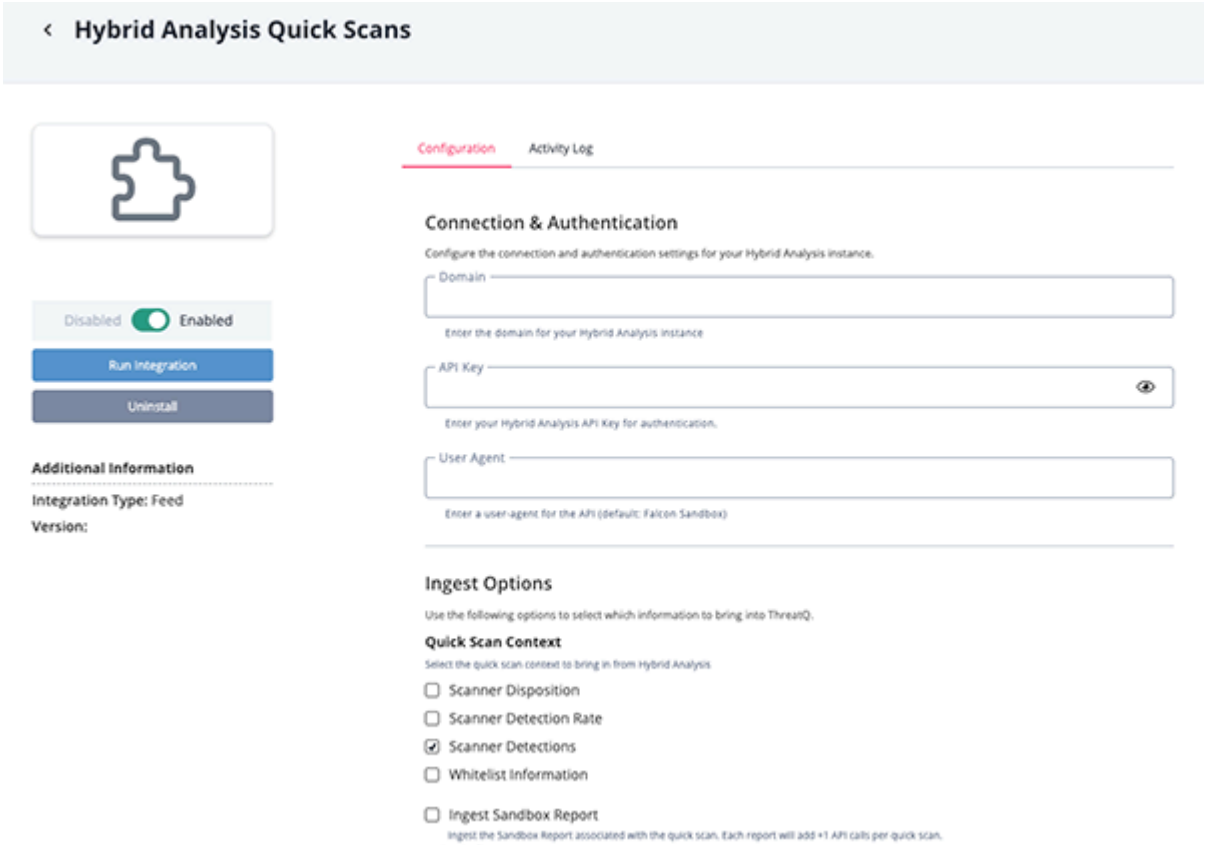
Public Feed and Submissions Parameters

PARAMETER	DESCRIPTION
Domain	The domain of your Hybrid Analysis instance.
API Key	Your Hybrid Analysis API Key for authentication.
User Agent	The User-agent for the API. The default setting is Falcon Sandbox.



Quick Scans Parameters

PARAMETER	DESCRIPTION
Domain	The domain of your Hybrid Analysis instance
API Key	Your Hybrid Analysis API Key for authentication.
User Agent	The User-agent for the API. The default setting is Falcon Sandbox.
Quick Scan Context	Select the pieces of information about a quick to bring in from Hybrid Analysis.
Ingest Sandbox Report	Ingest the Sandbox Report associated with the quick scan. Each report will add +1 API calls per quick scan.



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

ThreatQuotient provides feed urls, sample responses, and default ThreatQ mapping.

Hybrid Analysis Public Feed

The Hybrid Analysis Public Feed enables the ingestion of public reports from Hybrid Analysis using their public feed.

`GET https://hybrid-analysis.com/api/v2/feed/latest`

Sample Response:


```
{
  "count": 174,
  "status": "ok",
  "data": [
    {
      "job_id": "5ebeb84be7702b60fe113eeb",
      "md5": "3e7488819b26ac88e372ac19d415d445",
      "sha1": "f5d5ad71a231afe21f5ba045ec5b597ebdcc4786",
      "sha256":
"b71f228ade7b30e6e431c872a53b007d6bf7ff8604255c4e6a9276ca13651440",
      "interesting": false,
      "analysis_start_time": "2020-05-15 15:42:09",
      "threat_score": 18,
      "threat_level": 1,
      "threat_level_human": "suspicious",
      "unknown": true,
      "submit_name": "https://medium.com/@kopapic176/watch-britains-got-talent-
season-14-episodes-6-6b83e2bce89e",
      "url_analysis": true,
      "domains": [
        "a16180790160.cdn.optimizely.com",
        "cdn-client.medium.com",
        "cdn-static-1.medium.com",
        "cdn.optimizely.com",
        "glyph.medium.com",
        "logx.optimizely.com",
        "medium.com",
        "miro.medium.com",
        "ocsp.pki.goog"
      ],
      "hosts": [
        "104.16.123.127",
        "104.16.120.145",
        "104.16.119.145",
        "104.16.118.145",
```

```
        "172.217.7.174",
        "172.217.15.99",
        "34.199.177.216"
      ],
      "hosts_geolocation": [
        {
          "ip": "104.16.123.127",
          "latitude": "37.7621",
          "longitude": "-122.3971",
          "country": "USA"
        },
        {
          "ip": "104.16.120.145",
          "latitude": "37.7621",
          "longitude": "-122.3971",
          "country": "USA"
        },
        {
          "ip": "104.16.119.145",
          "latitude": "37.7621",
          "longitude": "-122.3971",
          "country": "USA"
        }
      ],
      "environment_id": 100,
      "environment_description": "Windows 7 32 bit",
      "shared_analysis": false,
      "reliable": true,
      "report_url": "/sample/
b71f228ade7b30e6e431c872a53b007d6bf7ff8604255c4e6a9276ca13651440/5ebeb84be7702b
60fe113eeb",
      "extracted_files": [
        {
          "name": "urlblockindex_1_.bin",
          "file_size": 16,
          "sha1": "e4f30e49120657d37267c0162fd4a08934800c69",
          "sha256":
"775853600060162c4b4e5f883f9fd5a278e61c471b3ee1826396b6d129499aa7",
          "md5": "fa518e3dfae8ca3a0e495460fd60c791",
          "type_tags": ["data"],
          "description": "data",
          "threat_level": 0,
          "threat_level_readable": "no specific threat",
          "av_matched": 0,
          "av_total": 70,
          "file_available_to_download": false
        },
        {
          "name": "en-US.2",
          "file_path": "%LOCALAPPDATA%\\Microsoft\\Internet Explorer\
```

```
\DomainSuggestions\\en-US.2",
          "file_size": 18176,
          "sha1": "3c96c993500690d1a77873cd62bc639b3a10653f",
          "sha256":
"c6a5377cbc07eece33790cfc70572e12c7a48ad8296be25c0cc805a1f384dbad",
          "md5": "5a34cb996293fde2cb7a4ac89587393a",
          "type_tags": ["data"],
          "description": "data",
          "runtime_process": "iexplore.exe",
          "threat_level": 0,
          "threat_level_readable": "no specific threat",
          "file_available_to_download": false
        }
      ],
      "processes": [
        {
          "uid": "562548150-00001272",
          "name": "rundll32.exe",
          "normalized_path": "%WINDIR%\\System32\\rundll32.exe",
          "command_line": "\"%WINDIR%\\System32\\ieframe.dll\",OpenURL C:\
\b71f228ade7b30e6e431c872a53b007d6bf7ff8604255c4e6a9276ca13651440.url",
          "sha256":
"3fa4912eb43fc304652d7b01f118589259861e2d628fa7c86193e54d5f987670"
        },
        {
          "uid": "562548293-00001964",
          "parentuid": "562548150-00001272",
          "name": "iexplore.exe",
          "normalized_path": "%PROGRAMFILES%\\Internet Explorer\\iexplore.exe",
          "command_line": "https://medium.com/@kopapic176/watch-britains-got-
talent-season-14-episodes-6-6b83e2bce89e",
          "sha256":
"8abc7daa81c8a20bfd88b6a60ecc9ed1292fbb6cedbd6f872f36512d9a194bba"
        },
        {
          "uid": "562548314-00001712",
          "parentuid": "562548293-00001964",
          "name": "iexplore.exe",
          "normalized_path": "%PROGRAMFILES%\\Internet Explorer\\iexplore.exe",
          "command_line": "SCODEF:1964 CREDAT:275457 /prefetch:2",
          "sha256":
"8abc7daa81c8a20bfd88b6a60ecc9ed1292fbb6cedbd6f872f36512d9a194bba"
        }
      ]
    }
  ]
}
```

Hybrid Analysis Submissions

The Hybrid Analysis Submissions Feed enables the ingestion of reports from samples submitted through the Hybrid Analysis Operation within ThreatQ. In order for this feed to ingest data, it is mandatory that ThreatQ Threat Library to contain indicators that have the `Hybrid Analysis Verdict` and `Scan Link` attributes. These attributes can be added using the Hybrid Analysis ThreatQ Operation. The feed will retrieve all the indicators having these attributes and queries Hybrid Analysis to get Sandbox reports.

`GET https://hybrid-analysis.com/api/v2/report/{sha256}:{environmentId}/summary`

Sample Response:


```
{
    "job_id": "5ebeb84be7702b60fe113eeb",
    "md5": "3e7488819b26ac88e372ac19d415d445",
    "sha1": "f5d5ad71a231afe21f5ba045ec5b597ebdcc4786",
    "sha256":
"b71f228ade7b30e6e431c872a53b007d6bf7ff8604255c4e6a9276ca13651440",
    "interesting": false,
    "analysis_start_time": "2020-05-15 15:42:09",
    "threat_score": 18,
    "threat_level": 1,
    "threat_level_human": "suspicious",
    "unknown": true,
    "submit_name": "https://medium.com/@kopapic176/watch-britains-got-talent-
season-14-episodes-6-6b83e2bce89e",
    "url_analysis": true,
    "domains": [
    "a16180790160.cdn.optimizely.com",
    "cdn-client.medium.com",
    "cdn-static-1.medium.com",
    "cdn.optimizely.com",
    "glyph.medium.com",
    "logx.optimizely.com",
    "medium.com",
    "miro.medium.com",
    "ocsp.pki.goog"
    ],
    "hosts": [
    "104.16.123.127",
    "104.16.120.145",
    "104.16.119.145",
    "104.16.118.145",
    "172.217.7.174",
    "172.217.15.99",
    "34.199.177.216"
    ],
    "hosts_geolocation": [
    {
```

```
        "ip": "104.16.123.127",
        "latitude": "37.7621",
        "longitude": "-122.3971",
        "country": "USA"
    },
    {
        "ip": "104.16.120.145",
        "latitude": "37.7621",
        "longitude": "-122.3971",
        "country": "USA"
    },
    {
        "ip": "104.16.119.145",
        "latitude": "37.7621",
        "longitude": "-122.3971",
        "country": "USA"
    }
    ],
    "environment_id": 100,
    "environment_description": "Windows 7 32 bit",
    "shared_analysis": false,
    "reliable": true,
    "report_url": "/sample/
b71f228ade7b30e6e431c872a53b007d6bf7ff8604255c4e6a9276ca13651440/5ebeb84be7702b
60fe113eeb",
    "extracted_files": [
    {
        "name": "urlblockindex_1_.bin",
        "file_size": 16,
        "sha1": "e4f30e49120657d37267c0162fd4a08934800c69",
        "sha256":
"775853600060162c4b4e5f883f9fd5a278e61c471b3ee1826396b6d129499aa7",
        "md5": "fa518e3dfae8ca3a0e495460fd60c791",
        "type_tags": ["data"],
        "description": "data",
        "threat_level": 0,
        "threat_level_readable": "no specific threat",
        "av_matched": 0,
        "av_total": 70,
        "file_available_to_download": false
    },
    {
        "name": "en-US.2",
        "file_path": "%LOCALAPPDATA%\\Microsoft\\Internet Explorer\
\DomainSuggestions\\en-US.2",
        "file_size": 18176,
        "sha1": "3c96c993500690d1a77873cd62bc639b3a10653f",
        "sha256":
"c6a5377cbc07eece33790cfc70572e12c7a48ad8296be25c0cc805a1f384dbad",
        "md5": "5a34cb996293fde2cb7a4ac89587393a",
```

```
        "type_tags": ["data"],
        "description": "data",
        "runtime_process": "iexplore.exe",
        "threat_level": 0,
        "threat_level_readable": "no specific threat",
        "file_available_to_download": false
    }
    ],
    "processes": [
    {
        "uid": "562548150-00001272",
        "name": "rundll32.exe",
        "normalized_path": "%WINDIR%\\System32\\rundll32.exe",
        "command_line": "\"%WINDIR%\\System32\\ieframe.dll\",OpenURL C:\
\b71f228ade7b30e6e431c872a53b007d6bf7ff8604255c4e6a9276ca13651440.url",
        "sha256":
"3fa4912eb43fc304652d7b01f118589259861e2d628fa7c86193e54d5f987670"
    },
    {
        "uid": "562548293-00001964",
        "parentuid": "562548150-00001272",
        "name": "iexplore.exe",
        "normalized_path": "%PROGRAMFILES%\\Internet Explorer\\iexplore.exe",
        "command_line": "https://medium.com/@kopapic176/watch-britains-got-
talent-season-14-episodes-6-6b83e2bce89e",
        "sha256":
"8abc7daa81c8a20bfd88b6a60ecc9ed1292fbb6cedbd6f872f36512d9a194bba"
    },
    {
        "uid": "562548314-00001712",
        "parentuid": "562548293-00001964",
        "name": "iexplore.exe",
        "normalized_path": "%PROGRAMFILES%\\Internet Explorer\\iexplore.exe",
        "command_line": "SCODEF:1964 CREDAT:275457 /prefetch:2",
        "sha256":
"8abc7daa81c8a20bfd88b6a60ecc9ed1292fbb6cedbd6f872f36512d9a194bba"
    }
    ]
}
```

Public Feed and Submissions Mapping

The Hybrid Analysis Public Feed and Submissions feed share the same mapping table listed below.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
data[].mitre_attcks[].attck_id/technique	Related Attack Pattern	N/A	data[].analysis_start_time	T100 - Some MITRE Technique	Formatted string
data[].processes[].normalized_path	Indicator Value	File Path	data[].analysis_start_time	N/A	N/A
data[].domains[]	Indirect Indicator Value	FQDN	data[].analysis_start_time	blahblah.google.com	Indirect because they may be common hosts
data[].hosts_geolocation[].ip	Indirect Indicator Value	IP Address	data[].analysis_start_time	N/A	Indirect because they may be common host IPs
data[].extracted_files[].file_path	Indicator Value	File Path	data[].analysis_start_time	N/A	N/A
data[].extracted_files[].md5	Indicator Value	MD5	data[].analysis_start_time	N/A	N/A
data[].extracted_files[].name	Indicator Value	Filename	data[].analysis_start_time	N/A	N/A
data[].extracted_files[].sha256	Indicator Value	SHA-256	data[].analysis_start_time	N/A	N/A
data[].submit_name	Indicator Value	Filename/URL	data[].analysis_start_time	N/A	Type depends on 'url_analysis' flag
data[].compromised_hosts[]	Indicator Value	IP Address	data[].analysis_start_time	N/A	N/A
data[].md5	Indicator Value	MD5	data[].analysis_start_time	N/A	N/A
data[].sha1	Indicator Value	SHA-1	data[].analysis_start_time	N/A	N/A
data[].sha256	Indicator Value	SHA-256	data[].analysis_start_time	N/A	N/A
data[].sha512	Indicator Value	SHA-512	data[].analysis_start_time	N/A	N/A
data[].threat_score	Indicator Attribute	Threat Score	data[].analysis_start_time	65	If the attribute already exists, the value will be updated
data[].threat_level	Indicator Attribute	Threat Level	data[].analysis_start_time	2	Numerical representation of "verdict"
data[].verdict	Indicator Attribute	Hybrid Analysis Verdict	data[].analysis_start_time	Malicious	Readable representation of "threat_level", if the attribute already exists, the value will be updated
data[].environment_description	Indicator Attribute	Scan Environment	data[].analysis_start_time	Windows 7 32 bit	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
data[].av_detect	Indicator Attribute	Detection Rate	data[].analysis_start_time	22%	Percentage
data[].vx_family	Indicator Attribute	Malware Family	data[].analysis_start_time	Trojan.RP.Generic	N/A
data[].type_short[]	Indicator Attribute	File Type	data[].analysis_start_time	peexe	N/A
data[].size	Indicator Attribute	File Size	data[].analysis_start_time	100020	N/A
data[].extracted_ files[].description	Indicator Attribute	Description	data[].analysis_start_time	N/A	N/A
data[].extracted_ files[].threat_level	Indicator Attribute	Threat Level	data[].analysis_start_time	1	Numerical representation of "threat_level_readable"
data[].extracted_ files[].threat_level_ readable	Indicator Attribute	Hybrid Analysis Verdict	data[].analysis_start_time	Suspicious	Readable representation of "threat_level", if the attribute already exists, the value will be updated
data[].extracted_ files[].av_label	Indicator Attribute	AV Label	data[].analysis_start_time	Unrated site	N/A
data[].extracted_ files[].av_matched/ av_total	Indicator Attribute	Detections	data[].analysis_start_time	22 / 84	Formatted string
data[].extracted_ files[].file_size	Indicator Attribute	File Size	data[].analysis_start_time	123455	N/A
data[].hosts_ geolocation[].country	Indicator Attribute	Country	data[].analysis_start_time	USA	N/A
data[].mitre_attcks[].tactic	Attack Pattern Attribute	Tactic	data[].analysis_start_time	N/A	N/A

Hybrid Analysis Quick Scans

The Hybrid Analysis Quick Scans Feed enables the ingestion of quick scan results and sandbox reports for samples or URLs submitted through the Hybrid Analysis Operation within ThreatQ. For this feed to ingest data it is mandatory that ThreatQ Library contains indicators having the attribute `Hybrid Analysis Quick Scan ID`. This attribute can be added using the Hybrid Analysis ThreatQ Operation. The feed gets all the indicators having this attribute and queries Hybrid Analysis to get quick scan results.

`GET https://hybrid-analysis.com/api/v2/quick-scan/{hybdrid_analysis_quick_scan_id}`

Sample Response:


```
{
  "id": "667d15f7e46d689e7e0ac4b6",
  "sha256": "a2a28705f577b928c211130f2d779604c58c7ea82a25dfae7f29308d0e166d69",
  "scanners": [
    {
      "name": "Metadefender",
      "status": "clean",
      "error_message": null,
      "progress": 100,
      "total": 23,
      "positives": 0,
      "percent": 0,
      "anti_virus_results": []
    }
  ],
  "scanners_v2": {
    "crowdstrike_ml": null,
    "virustotal": null,
    "metadefender": {
      "name": "Metadefender",
      "status": "clean",
      "error_message": null,
      "progress": 100,
      "total": 23,
      "positives": 0,
      "percent": 0,
      "anti_virus_results": []
    }
  },
  "whitelist": [
    {
      "id": "internal",
      "value": false
    }
  ],
  "reports": [
```

```
    "5b8413ab7ca3e13e5c4aece3"
  ],
  "finished": true
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.scanners_v2[].{SCANNER_NAME}.status	Indicator.Attribute	{SCANNER_NAME} Disposition	N/A	`Clean`	Mapped using the table `Hybrid Analysis Scan Status`. If enabled in used config.
.scanners_v2[].{SCANNER_NAME}.percent	Indicator.Attribute	{SCANNER_NAME} Detection Rate	N/A	`0%`	`%` is appended. If enabled in used config.
.scanners_v2[].{SCANNER_NAME}.positives, .scanners_v2[].{SCANNER_NAME}.total	Indicator.Attribute	{SCANNER_NAME} Detections	N/A	`0/23`	Concatenated using `/`. If enabled in used config.
.whitelist[].id, .whitelist[].value	Indicator.Attribute	{WHITELIST_ID} Whitelisted	N/A	`No`	Mapped to `Yes` or `No`.
.sha256	Related Indicator.Value	SHA-256	N/A	`a2a28705f577b928c211130f2d779604c58c7ea82a25dfae7f29308d0e166d69`	N/A

If the **Ingest Sandbox Report** configuration option is enabled, .sha256 is used to get the Sandbox Report. The SandBox Report has the same mapping as **Hybrid Analysis Submissions** feed.

Hybrid Analysis Scan Status Mapping

The following table outlines the Hybrid Analysis Scan Status to ThreatQ Disposition Attribute mapping.

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

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.

Hybrid Analytics Public Feed

METRIC	RESULT
Run Time	2 minutes
Indicators	1,200
Indicator Attributes	4,800
Attack Patterns	20
Attack Pattern Attributes	25

Hybrid Analytics Submissions

METRIC	RESULT
Run Time	2 minutes
Indicators	1,200
Indicator Attributes	4,800
Attack Patterns	20
Attack Pattern Attributes	25

Hybrid Analytics Quick Scans

METRIC	RESULT
Run Time	2 minutes
Indicators	500
Indicator Attributes	7,00

Known Issues / Limitations

- API usage is subject to Hybrid Analysis' rate limiting per-API-key. You should stagger feed runs to reduce API usage.

Change Log

- **Version 1.2.3**
  - Added a new feed: Hybrid Analysis Quick Scans.
- **Version 1.2.2**
  - Added ingest rules for the `Hybrid Analysis Verdict` and `Threat Score` attributes.
  - Rename the `Verdict` attribute to `Hybrid Analysis Verdict`.
- **Version 1.2.1**
  - Upgraded the integration for compatibility with ThreatQ version 5.22.0 and later.
  - Updated the minimum ThreatQ version to 5.11.0.
- **Version 1.2.0**
  - Fixed a bug that that would result in calling an endpoint without the required query parameters.
  - Added improvement safeguards for the integration.
- **Version 1.1.0**
  - Fixed a filter mapping bug.
- **Version 1.0.0**
  - Initial release