ThreatQuotient

Hybrid Analysis Feed Guide

Version 1.0.0

Monday, August 10, 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, August 10, 2020

Contents

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions >= `4.30.0`

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.

Installation

Perform the following steps to install the feed:

The same steps can be used to upgrade the feed to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the **Hybrid Analysis** integration file.
3. Navigate to your ThreatQ instance.
4. Click on the **Settings** icon and select **Incoming feeds**.
5. Click on the **Add New Feed** button.
6. Upload the feed file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the feed file on your local machine

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.

The feeds will be added to the **OSINT** tab for Incoming Feeds. You will still need to configure and then enable the feed.

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 feed:

1. Click on the **Settings** icon and select **Incoming Feeds**.
2. Locate the feed under the **OSINT** tab.
3. Click on the **Feed Settings** link for the feed.
4. Under the **Connection** tab, enter the following configuration parameters:

Parameter	Description
API Key	Enter your Hybrid Analysis API Key for authentication.
User Agent	Enter a user-agent for the API (default: Falcon Sandbox).

5. Click on **Save Changes**.
6. Click on the toggle switch to the left of the feed name to enable the feed.

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
```


```
{
  "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/b71f228ad-
e7b30e6e431c872a53b007d6bf7ff8604255c4e6a9276ca13651440/5ebeb84be7702b60fe113eeb",
      "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:\\b71f228ad-
e7b30e6e431c872a53b007d6bf7ff8604255c4e6a9276ca13651440.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.

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

```
{
    "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/b71f228ad-
e7b30e6e431c872a53b007d6bf7ff8604255c4e6a9276ca13651440/5ebeb84be7702b60fe113eeb",
    "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:\\b71f228ad-
e7b30e6e431c872a53b007d6bf7ff8604255c4e6a9276ca13651440.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-epis-
odes-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"
    }
    ]
}
```

Default Mappings

ThreatQ provides the following default mapping for this the following feeds: `Hybrid Analysis Public Feed` & `Hybrid Analysis Sub-missions`

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
data[].mitre_attcks[].attck_id/technique	Object Value	Malware	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	Indicator	File Path	data[].ana-	N/A	N/A

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
[].file_path	Value		lysis_start_ time		
data[].extracted_files []].md5	Indicator Value	MD5	data[].ana- lysis_start_ time	N/A	N/A
data[].extracted_files []].name	Indicator Value	Filename	data[].ana- lysis_start_ time	N/A	N/A
data[].extracted_files []].sha256	Indicator Value	SHA-256	data[].ana- lysis_start_ time	N/A	N/A
data[].submit_name	Indicator Value	Filename/URL	data[].ana- lysis_start_ time	N/A	Type depends on 'url_ana- lysis' flag
data[].compromised_ hosts[]	Indicator Value	IP Address	data[].ana- lysis_start_ time	N/A	N/A

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
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	Attribute	Threat Score	data[].analysis_start_time	65	N/A
data[].threat_level	Attribute	Threat Level	data[].analysis_start_	2	Numerical representation of "verdict"

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
			time		
data[].verdict	Attribute	Verdict	data[].analysis_start_time	Malicious	Readable representation of "threat_level"
data[].environment_description	Attribute	Scan Environment	data[].analysis_start_time	Windows 7 32 bit	N/A
data[].av_detect	Attribute	Detection Rate	data[].analysis_start_time	22%	Percentage
data[].vx_family	Attribute	Malware Family	data[].analysis_start_time	Trojan.RP.Generic	N/A
data[].type_short[]	Attribute	File Type	data[].analysis_start_time	peexe	N/A
data[].size	Attribute	File Size	data[].ana-	100020	N/A

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
			lysis_start_ time		
data[].extracted_files[].de- scription	Attribute	Description	data[].ana- lysis_start_ time	N/A	N/A
data[].extracted_files []threat_level	Attribute	Threat Level	data[].ana- lysis_start_ time	1	Numerical representation of "threat_level_readable"
data[].extracted_files []threat_level_readable	Attribute	Threat Level	data[].ana- lysis_start_ time	Suspicious	Readable representation of "threat_level"
data[].extracted_files []av_label	Attribute	AV Label	data[].ana- lysis_start_ time	Unrated site	N/A
data[].extracted_files []av_matched/av_total	Attribute	Detections	data[].ana- lysis_start_ time	22 / 84	Formatted string

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
data[].extracted_files[].file_size	Attribute	File Size	data[].analysis_start_time	123455	N/A
data[].hosts_geolocation[].country	Attribute	Country	data[].analysis_start_time	USA	N/A
data[].mitre_attcks[].tactic	Attribute	Tactic	data[].analysis_start_time	N/A	N/A

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	~1200
Indicator Attributes	~4800
Attack Patterns	20
Attack Pattern Attributes	25

Hybrid Analytics Submissions

Results will vary depending on Hybrid Analysis Operation usage.

Known Issues/Limitations

- API usage is subject to Hybrid Analysis' rate limiting per-API-key. Be sure to stagger feed runs to reduce API usafe

Change Log

- **Version 1.0.0**
  - Initial Release