ThreatQuotient

Cybersixgill Darkfeed CDF Guide

Version 1.0.4

January 17, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

Developer Supported

Support

Email: support@cybersixgill.com
Web: N/A
Phone: N/A

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 **Developer Supported**.

Support Email: support@cybersixgill.com
Support Web: N/A
Support Phone: N/A

Integrations designated as **Developer Supported** are supported and maintained by the developer who submitted the integration to the ThreatQ Marketplace. The developer's contact information can be found on the integration’s download page within the Marketplace as well as in this guide.

You are responsible for engaging directly with the developer of Developer Supported integrations/apps/add-ons to ensure proper functionality and version compatibility with the applicable ThreatQuotient Software.

If functional or compatibility issues that may arise are not resolved, you may be required to uninstall the app or add-on from their ThreatQuotient environment in order for ThreatQuotient to fulfill support obligations.

For ThreatQuotient Hosted instance customers, the Service Level Commitment and Service Level Credit in the ThreatQuotient Service Level Schedule will not apply for any issues caused by Developer Supported integrations/apps/add-ons.

ThreatQuotient reserves the right to remove the Developer-Supported designation of third-party apps and add-ons if the developer is not, in ThreatQuotient’s determination, fulfilling reasonable obligations for support and maintenance.

> Failure by the developer to update compatibility of an app or add-on within 90 days of the release of a new version of applicable ThreatQuotient Software will result in reclassification to Not Actively Supported.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.4
Compatible with ThreatQ Versions	>= 4.34.0
Support Tier	Developer Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/Cybersixgill-darkfeed

Introduction

Delivering the next generation of deep & dark web threat intelligence feeds, Cybersixgill tailors threat intelligence to customers' intelligence needs, maximizing effective mitigation and remediation. Using an agile collection methodology and its proprietary collection automation algorithm, Cybersixgill provides broad coverage of exclusive-access deep and dark web sources, as well as relevant surface web sources. Cybersixgill harnesses artificial intelligence and machine learning to automate the production cycle of cyber intelligence from monitoring through extraction to production - unleashing both existing platforms' and teams' performance.

Leverage the power of Cybersixgill to supercharge ThreatQuotient with real-time Threat Intelligence indicators. Get IOCs such as domains, URLs, hashes, and IP addresses straight into the ThreatQuotient platform.

The integration provides the **Cybersixgill Darkfeed** feed that utilizes the following endpoints:

- **Cybersixgill Darkfeed** - returns an OAuth2 token.
- **Get Feed Data (Supplemental)** - returns the Darkfeed threat intelligence IOCs and related information.
- **Acknowledge Feed Data (Supplemental)** - acknowledges that you consumed a batch of IOC items after running the ioc endpoint.

The integration ingests the following system objects:

- Adversaries
- Attack Patterns
- Indicators
    - Indicator Attributes
- TTPs Attributes

> ⚠ The Sixgill Darkfeed CDF is now known as Cybersixgill Darkfeed CDF.

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 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.

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

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 integration-related credentials.

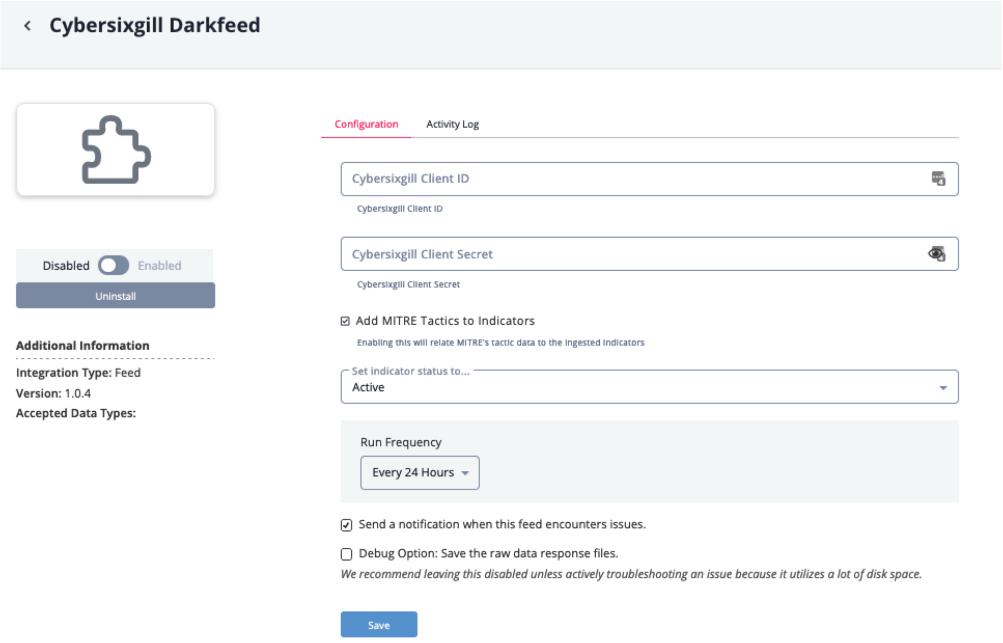
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** 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:

PARAMETER	DESCRIPTION
Cybersixgill Client ID	Your Cybersixgill Client ID.
Cybersixgill Client Secret	Your Cybersixgill Client Secret.
Add MITRE Tactics to Indicators	Enable/disable to set whether MITRE Attack Patterns will be related to ingested indicators from Cybersixgill.



‹ Cybersixgill Darkfeed

Disabled Enabled

Additional Information

Integration Type: Feed

Version: 1.0.4

Accepted Data Types:

Cybersixgill Client ID

Cybersixgill Client ID

Cybersixgill Client Secret

Cybersixgill Client Secret

☑ Add MITRE Tactics to Indicators

Enabling this will relate MITRE's tactic data to the ingested indicators

Set indicator status to...: Active

Run Frequency: Every 24 Hours

☑ Send a notification when this feed encounters issues.

☐ Debug Option: Save the raw data response files.

We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

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

Cybersixgill Darkfeed

The Cybersixgill Darkfeed returns an OAuth2 token based on the `Cybersixgill API ID` and `Cybersixgill API Key` user fields that will be used for authentication on the next feeds.

`POST https://api.cybersixgill.com/auth/token`

Sample Response:

```
{
    "access_token": "eyJhbG",
    "expires_in": 28800,
    "refresh_expires_in": 86400,
    "refresh_token": "eyJhbGciOiJIUzI1NiIsInR5cCIgOiAi",
    "token_type": "bearer",
    "not-before-policy": 0,
    "session_state": "11ab30c9-d947-484a-8e9b-a51071762c9e",
    "scope": "email profile"
}
```

Get Feed Data (Supplemental)

The Get Feed Data supplemental endpoint returns the Darkfeed threat intelligence IOCs and related information.

`GET https://api.cybersixgill.com/darkfeed/ioc?limit=2000`

Sample Response:

```
{
  "id": "bundle--318ed832-2b1c-4d3d-8b9f-6b4b8ef628ad",
  "objects": [
    {
      "created": "2017-01-20T00:00:00.000Z",
      "definition": {
        "tlp": "amber"
      },
      "definition_type": "tlp",
      "id": "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82",
      "type": "marking-definition"
    },
    {
      "created": "2019-12-26T00:00:00Z",
      "definition": {
        "statement": "Copyright Cybersixgill 2020. All rights reserved."
      },
      "definition_type": "statement",
      "id": "marking-definition--41eaaf7c-0bc0-4c56-abdf-d89a7f096ac4",
      "type": "marking-definition"
    },
    {
      "created": "2020-05-12T15:38:42.969Z",
      "description": "Malware available for download from file-sharing sites",
      "external_reference": [
        {
          "description": "Mitre attack tactics and technique reference",
          "mitre_attack_tactic": "Build Capabilities",
          "mitre_attack_tactic_id": "TA0024",
          "mitre_attack_tactic_url": "https://attack.mitre.org/tactics/TA0024/",
          "mitre_attack_technique": "Obtain/re-use payloads",
          "mitre_attack_technique_id": "T1346",
          "mitre_attack_technique_url": "https://attack.mitre.org/techniques/T1346/",
          "source_name": "mitre-attack"
        }
      ],
      "id": "indicator--4bf4b89b-1115-40d1-9f6c-a70405d49141",
      "labels": [
        "malicious-activity",
        "malware",
        "Build Capabilities",
        "Obtain/re-use payloads"
      ],
      "lang": "en",
      "modified": "2020-05-12T15:38:42.969Z",
      "object_marking_refs": [
        "marking-definition--41eaaf7c-0bc0-4c56-abdf-d89a7f096ac4",
        "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"
      ],
      "pattern": "[url:value = 'https://anonfile.com/te7aYaw7o9/Leeched_Combo_464705_txt']",
      "sixgill_actor": "h4ckcr4ck",
      "sixgill_confidence": 80,
      "sixgill_feedid": "darkfeed_010",
      "sixgill_feedname": "malware_download_urls",
      "sixgill_postid": "bded5cfcb05b917ac80c7a0aaac45a2fffb26ce4",
      "sixgill_posttitle": "464705 - HQ Combolist Mega, File-upload, Mediafire, 4shared",
      "sixgill_severity": 80,
      "sixgill_source": "forum_nulled",
      "spec_version": "2.0",
      "type": "indicator",
      "valid_from": "2020-05-08T05:53:26Z"
    }
  ],
  "spec_version": "2.0",
  "type": "bundle"
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.objects[].pattern`	Indicator Value	Extracted from `.objects[].pattern`	.objects[].valid_from	url:value = 'https://anonfile.com/bcqfn7ydoa/sqli_dumper_10.1_zip']	Both value and type are extracted from `.pattern`
`.objects[].modified`	Indicator Modified At	N/A	N/A	2020-05-15T12:10:28.942Z	N/A
`.objects[].revoked`	Indicator Status	N/A	N/A	False	'Active' if `.revoked` is `False` else 'Whitelisted'
`.objects[].description`	Indicator Description	N/A	N/A	Malware available for download from file-sharing sites	N/A
`.objects[].sixgill_confidence`	Indicator Attribute	Confidence	.objects[].valid_from	80	N/A
`.objects[].sixgill_severity`	Indicator Attribute	Severity	.objects[].valid_from	80	N/A
`.objects[].sixgill_feedname`	Indicator Attribute	Cybersixgill Feed Name	.objects[].valid_from	malware_download_urls	N/A
`.objects[].sixgill_feedid`	Indicator Attribute	Cybersixgill Feed ID	.objects[].valid_from	darkfeed_010	N/A
`.objects[].sixgill_postid`	Indicator Attribute	Cybersixgill Post ID	.objects[].valid_from	9528ffecd65e2a1ae9f5c3b1f5e6948e2353d620	N/A
`.objects[].sixgill_posttitle`	Indicator Attribute	Cybersixgill Post Title	.objects[].valid_from	sqli dumper 10.2 2020	N/A
`.objects[].sixgill_source`	Indicator Attribute	Cybersixgill Source	.objects[].valid_from	forum_demonforums	N/A
`.objects[].revoked`	Indicator Attribute	False Positive	.objects[].valid_from	Flase	N/A
`.objects[].labels[]`	Indicator Attribute	Label	.objects[].valid_from	malware	N/A
`.objects[].sixgill_post_virustotallink`	Indicator Attribute	VirusTotal Link	.objects[].valid_from	https://virustotal.com/#/file/e436924a2fac62b5d...	N/A
`.objects[].external_reference[].positive_rate`	Indicator Attribute	VirusTotal Positive Rate	.objects[].valid_from	low	Applicable only when `.source_name` is 'VirusTotal'
`.objects[].sixgill_actor`	Adversary Name	N/A	.objects[].valid_from	meisami2015	N/A
`.objects[].external_reference[].mitre_attack_tactic_id + mitre_attack_tactic`	TTP Value	N/A	N/A	TA0024 - Build Capabilities	Applicable only when `.source_name` is 'mitre-attack'
`.objects[].external_`	TTP Attribute	Technique ID	N/A	T1346	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`reference[].mitre_attack_technique_id`					
`.objects[].external_reference[].mitre_attack_technique`	TTP Attribute	Technique Name	N/A	Obtain/re-use payloads	N/A
`.objects[].external_reference[].mitre_attack_technique_url`	TTP Attribute	Technique External Reference	N/A	https://attack.mitre.org/techniques/T1346/	N/A
`.objects[].external_reference[].mitre_attack_tactic_id`	TTP Attribute	Tactic ID	N/A	TA0024	N/A
`.objects[].external_reference[].mitre_attack_tactic`	TTP Attribute	Tactic Name	N/A	Build Capabilities	N/A
`.objects[].external_reference[].mitre_attack_tactic_url`	TTP Attribute	Tactic External Reference	N/A	https://attack.mitre.org/tactics/TA0024/	N/A

Acknowledge Feed Data (Supplemental)

The Acknowledge Feed Data supplemental endpoint acknowledges that a batch of IOC items was consumed after running the `Get Feed Data` endpoint. On it's next call, the next bundle of IOCs will be received.

```
POST https://api.cybersixgill.com/darkfeed/ioc/ack
```

Sample Response:

```
{
  2000
}
```

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.

Cybersixgill Darkfeed

METRIC	RESULT
Run Time	7 minutes
Indicators	2,001
Indicator Attributes	30,248
Adversaries	65
Attack Patterns	2
TTPs Attributes	21

Change Log

- **Version 1.0.4**
  - Updated the labeling and description for the configuration parameters. Cybersixgill API ID is now **Cybersixgill Client ID** and Cybersixgill API Key is now **Cybersixgill Client Secret**.
- **Version 1.0.3**
  - Updating integration naming and configuration labels - Sixgill is now Cybersixgill.
- **Version 1.0.2**
  - Update support for MITRE Attack Patterns
- **Version 1.0.1**
  - Fixed error during ingestion
- **Version 1.0.0**
  - Initial release