

ThreatQuotient



Cybersixgill Darkfeed CDF

Version 1.1.1

September 17, 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	3
Support	4
Integration Details.....	5
Introduction	6
Prerequisites	7
Compromised Account Custom Object	7
ThreatQ V6 Steps.....	7
ThreatQ v5 Steps	8
Installation.....	10
Configuration	11
All Feeds	11
Cybersixgill Darkfeed.....	11
Cybersixgill DVE.....	12
Cybersixgill Alerts.....	13
Cybersixgill Compromised Accounts.....	14
Cybersixgill Compromised Emails	14
ThreatQ Mapping.....	16
Cybersixgill Darkfeed.....	16
Cybersixgill DVE.....	19
Cybersixgill Alerts.....	23
Cybersixgill Compromised Accounts.....	25
Cybersixgill Compromised Emails	26
Get Feed Data (Supplemental).....	27
Acknowledge Feed Data (Supplemental)	27
Cybersixgill - Get Alert by ID (Supplemental).....	27
Cybersixgill - Fetch Compromised Accounts (Supplemental)	29
Cybersixgill - Fetch Compromised Emails (Supplemental)	30
Average Feed Run.....	32
Cybersixgill Darkfeed.....	32
Cybersixgill DVE.....	32
Cybersixgill Alerts.....	33
Cybersixgill Compromised Accounts.....	33
Cybersixgill Compromised Emails	34
Known Issues	35
Change Log	36

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.

Copyright © 2024 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Support

This integration is designated as **Developer Supported**.

Support Email: support@rstcloud.net

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 1.1.1

**Compatible with ThreatQ
Versions** $\geq 5.12.1$

Support Tier Developer Supported

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 high-fidelity Threat Intelligence indicators. Get IOCs such as domains, URLs, hashes, and IP addresses straight into the ThreatQuotient platform. Receive updates for the latest vulnerabilities. And, stay on top of your organization's attack surface by monitoring for alerts and compromised credentials.

This integration provides the following feeds:

- [Cybersixgill Darkfeed](#) - ingests IOCs and related data
- [Cybersixgill DVE](#) - ingests CVEs and related events
- [Cybersixgill Alerts](#) - ingest alerts and related data
- [Cybersixgill Compromised Accounts](#) - ingests compromised accounts and related data
- [Cybersixgill Compromised Emails](#) - ingests compromised emails and related data

The integration ingests the following system objects:

- Indicators
- Attack patterns
- Adversaries
- CVEs
- Vulnerabilities
- Events




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

Prerequisites

- The Compromised Account custom object is required and must be installed on your ThreatQ instance prior to attempting to install the integration.

Compromised Account Custom Object

Use the steps provided to install the Compromised Account custom object.

 When installing the custom objects, be aware that any in-progress feed runs will be cancelled, and the API will be in maintenance mode.

ThreatQ V6 Steps

Use the following steps to install the custom object in ThreatQ v6:

1. Download the integration bundle from the ThreatQ Marketplace.
2. Unzip the bundle and locate the custom object files.



The custom object files will typically consist of a JSON definition file, install.sh script, and a images folder containing the svg icons.

3. SSH into your ThreatQ instance.
4. Navigate to the tmp folder:

```
cd /var/lib/threatq/misc/
```

5. Upload the custom object files, including the images folder.

The directory structure should be as the following:

- misc
 - install.sh
 - <custom_object_name>.json
 - images (directory)
 - <custom_object_name>.svg

6. Run the following command:

```
kubectl exec -it deployment/api-schedule-run -n threatq -- sh /var/lib/threatq/misc/install.sh /var/lib/threatq/misc
```



The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

7. Delete the `install.sh`, `definition.json` file, and `images` directory from the `misc` directory after the object has been installed as these files are no longer needed.

ThreatQ v5 Steps

Use the following steps to install the custom object in ThreatQ v5:

1. Download the integration zip file from the ThreatQ Marketplace and unzip its contents.
2. SSH into your ThreatQ instance.
3. Navigate to `tmp` directory:

```
cd /tmp/
```

4. Create a new directory:

```
mkdir cybersixgill_cdf
```

5. Upload the **account.json** and **install.sh** script into this new directory.
6. Create a new directory called **images** within the `cybersixgill_cdf` directory.

```
mkdir images
```

7. Upload the `account.svg`.
8. Navigate to the `/tmp/cybersixgill_cdf`.

The directory should resemble the following:

- `tmp`
 - `cybersixgill_cdf`
 - `account.json`
 - `install.sh`
 - `images`
 - `account.svg`

9. Run the following command to ensure that you have the proper permissions to install the custom object:

```
chmod +x install.sh
```

10. Run the following command:

```
sudo ./install.sh
```



You must be in the directory level that houses the install.sh and json files when running this command.

The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

11. Remove the temporary directory, after the custom object has been installed, as the files are no longer needed:

```
rm -rf cybersixgill_cdf
```

Installation



The CDF requires the installation of the Compromised Account custom objects before installing the actual CDF. See the [Prerequisites](#) chapter for more details.

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
6. Select the individual feeds to install and click **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 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:

All Feeds

PARAMETER	DESCRIPTION
Cybersixgill Client ID	Your Cybersixgill Client ID.
Cybersixgill Client Secret	Your Cybersixgill Client Secret.

Cybersixgill Darkfeed

PARAMETER	DESCRIPTION
Add MITRE Tactics to Indicators	Enable/disable to set whether MITRE Attack Patterns will be related to ingested indicators from Cybersixgill.
Context Selection	<p>Select the context you want to bring in with each indicator. This will allow you to curate which pieces of information your organization cares about, and which pieces of information you want to ignore.</p> <ul style="list-style-type: none"> Labels (Tags) (<i>default</i>)

PARAMETER

DESCRIPTION

- Confidence (*default*)
- Severity (*default*)
- Cybersixgill Feed Name
- Cybersixgill Post Link
- Cybersixgill Source
- Cybersixgill Post Title
- Revoked (*default*)
- VirusTotal Link
- VirusTotal Positive Rate (*default*)
- Related Threat Actor (*default*)
- Related MITRE Techniques (*default*)

Cybersixgill DVE

PARAMETER

DESCRIPTION

Ingest CVE Events

Enable this option to ingest the associated events for each CVE. For example, when a CVE was mentioned on Twitter, when a score was changed, or when NVD published a new CVE. (default: false)

Ingest CVEs As

Select the entity type you would like your CVEs ingested as:

- Indicators
- Vulnerabilities (*default*)

Context Selection

Select the context you want to bring in with each CVE. This will allow you to curate which pieces of information your organization cares about, and which pieces of information you want to ignore.

- Attribution (*default*)
- CVSSv3 Score (*default*)
- CVSSv3 Severity (*default*)
- CVSSv3 Vector
- CVSSv2 Score
- CVSSv2 Severity
- CVSSv2 Vector
- Current Rating (*default*)
- Highest Rating (*default*)
- Previously Exploited
- Affected Vendors (*default*)
- Affected Products (*default*)

PARAMETER	DESCRIPTION
	<ul style="list-style-type: none"> ◦ Affected Packages (<i>default</i>) ◦ External References

Cybersixgill Alerts

PARAMETER	DESCRIPTION
Ingest CVEs As	Select the entity type you would like your CVEs ingested as: <ul style="list-style-type: none"> • Indicators • Vulnerabilities (<i>default</i>)
Threat Level Filter	Select the threat levels for alerts you want to ingest into ThreatQ. <ul style="list-style-type: none"> ◦ Imminent (<i>default</i>) ◦ Emerging (<i>default</i>)
Context Selection	Select the context you want to bring in with each indicator. This will allow you to curate which pieces of information your organization cares about, and which pieces of information you want to ignore. <ul style="list-style-type: none"> • Labels (Tags) (<i>default</i>) • Confidence (<i>default</i>) • Severity (<i>default</i>) • Cybersixgill Feed Name • Cybersixgill Post Link • Cybersixgill Source • Cybersixgill Post Title • Revoked (<i>default</i>) • VirusTotal Link • VirusTotal Positive Rate (<i>default</i>) • Related Threat Actor (<i>default</i>) • Related MITRE Techniques (<i>default</i>)

Cybersixgill Compromised Accounts

PARAMETER	DESCRIPTION
Host Domains	Enter a line-separated list of host domains to search for. By default, at least one host domain is required to be searched on. You may enter multiple if you'd like to monitor multiple domains for breaches.
Require Compromised Password	If enabled, only credentials that have an associated compromised password will be ingested into ThreatQ. This will allow you to ignore credentials that have been compromised but do not have a password associated with them. <i>(default: False)</i>
Context Selection	<p>Select the context you want to bring in with each compromised credential. This will allow you to curate which pieces of information your organization cares about, and which pieces of information you want to ignore.</p> <ul style="list-style-type: none"> ◦ Credential Domain <i>(default)</i> ◦ Impacted Domain <i>(default)</i> ◦ Impacted URL ◦ Password ◦ Password Hash Type ◦ Name <i>(default)</i> ◦ Breach Name (Tag) <i>(default)</i> ◦ Breached At <i>(default)</i>

Cybersixgill Compromised Emails

PARAMETER	DESCRIPTION
Host Domains	Enter a line-separated list of host domains to search for. By default, at least one host domain is required to be searched on. You may enter multiple if you'd like to monitor multiple domains for breaches.
Require Compromised Password	If enabled, only credentials that have an associated compromised password will be ingested into ThreatQ. This will allow you to ignore credentials that have been compromised but do not have a password associated with them. <i>(default: False)</i>

PARAMETER	DESCRIPTION
Context Selection	<p>Select the context you want to bring in with each compromised credential. This will allow you to curate which pieces of information your organization cares about, and which pieces of information you want to ignore.</p> <ul style="list-style-type: none">◦ Credential Domain (<i>default</i>)◦ Password◦ Password Hash Type◦ Name (<i>default</i>)◦ Breach Name (Tag) (<i>default</i>)◦ Breached At (<i>default</i>)

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

This feed pulls the indicators of compromise (IOCs) from the Cybersixgill Darkfeed. This may include indicators such as URLs, FQDNs, IP Addresses, and Hashes. Indicators will be brought in with context such as the Confidence and Severity.

The feed will then make a request using the *supplemental feed*, `Get Feed Data`, to retrieve the IOCs.

GET <https://api.cybersixgill.com/darkfeed/ioc>

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 Sixgill 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": "bded5cfc05b917ac80c7a0aaac45a2fffb26ce4",
    "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"
}

```

Lastly, it will acknowledge that the batch of IOCs was consumed using the *supplemental feed*, Acknowledge Feed Data.

POST <https://api.cybersixgill.com/darkfeed/ioc/ack>

ThreatQuotient provides the following default mapping for this feed:



The following mapping is based on each item within the objects array.

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

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

Cybersixgill DVE

This feed pulls emerging CVEs and related events from the Cybersixgill DVE feed. This may include indicators such as CVEs, CVSS scores, affected vendors/products, and more.

The feed will then make a request using the *supplemental feed*, `Get Feed Data`, to retrieve the IOCs.

GET <https://api.cybersixgill.com/dvefeed/ioc>

Sample Response:

```
{
  "id": "bundle--cf118a51-eb64-4aa2-b929-51f91a643495",
  "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 Sixgill 2020. All rights reserved."
  },
  "definition_type": "statement",
  "id": "marking-definition--41eaaf7c-0bc0-4c56-abdf-d89a7f096ac4",
  "type": "marking-definition"
},
{
  "created": "2020-09-06T20:33:33.538Z",
  "external_references": [
    {
      "external_id": "CVE-2020-15392",
      "source_name": "cve"
    }
  ],
  "id": "cveevent--a26f4710-0d64-4a76-ae27-6ac038e7536b",
  "modified": "2020-09-06T20:33:33.538Z",
  "object_marking_refs": [
    "marking-definition--41eaaf7c-0bc0-4c56-abdf-d89a7f096ac4",
    "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"
  ],
  "spec_version": "2.0",
  "type": "x-cybersixgill-com-cve-event",
  "x_sixgill_info": {
    "event": {
      "_id": "5f1f17164731b1cef86c8aaf",
      "action": "trend",
      "description": "Trend of Github commits related to CVE-2020-15392",
      "event_datetime": "2020-06-30T00:00Z",
      "name": "trend_Github_commits",
      "prev_level": "prev_level",
      "type": "github_authoring"
    },
    "nvd": {
      "base_score_v3": 5.3,
      "base_severity_v3": "MEDIUM",
      "link": "https://nvd.nist.gov/vuln/detail/CVE-2020-15392",
      "modified": "2020-07-15T16:52Z",
      "published": "2020-07-07T14:15Z",

```

```

    "score_2_0": 5.0,
    "severity_2_0": "MEDIUM",
    "vector_v2": "AV:N/AC:L/Au:N/C:P/I:N/A:N",
    "vector_v3": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N"
  },
  "rating": {
    "current": 0.02,
    "highest": {
      "date": "2020-07-27T00:00Z",
      "value": 0.02
    },
    "previouslyExploited": 0.07
  }
}
]
}

```

Lastly, it will acknowledge that the batch of IOCs was consumed using the *supplemental feed*, Acknowledge Feed Data.

POST <https://api.cybersixgill.com/dvfeed/ioc/ack>

ThreatQ provides the following default mapping for this feed:

The following mapping is based on each item within the `objects` array.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.external_references[].external_id</code>	Indicator Value	CVE	<code>.created</code>	N/A	N/A
<code>.x_sixgill_info.event.action</code>	Attribute	Event Action	<code>.x_sixgill_info.event.event_datetime</code>	N/A	N/A
<code>.x_sixgill_info.event.name</code>	Attribute	Event Name	<code>.x_sixgill_info.event.event_datetime</code>	N/A	N/A
<code>.x_sixgill_info.nvd.base_score_v3</code>	Attribute	CVSS v3 Score	<code>.x_sixgill_info.nvd.modified</code>	N/A	N/A
<code>.x_sixgill_info.nvd.base_severity_v3</code>	Attribute	CVSS v3 Severity	<code>.x_sixgill_info.nvd.modified</code>	N/A	N/A
<code>.x_sixgill_info.nvd.link</code>	Attribute	Reference	<code>.x_sixgill_info.nvd.modified</code>	N/A	N/A
<code>.x_sixgill_info.nvd.score_2_0</code>	Attribute	CVSS v2 Score	<code>.x_sixgill_info.nvd.modified</code>	N/A	N/A
<code>.x_sixgill_info.nvd.severity_2_0</code>	Attribute	CVSS v3 Severity	<code>.x_sixgill_info.nvd.modified</code>	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.x_sixgill_info.nvd.vector_v2</code>	Attribute	CVSS v2 Vector	<code>.x_sixgill_info.nvd.modified</code>	N/A	N/A
<code>.x_sixgill_info.nvd.vector_v3</code>	Attribute	CVSS v3 Vector	<code>.x_sixgill_info.nvd.modified</code>	N/A	N/A
<code>.x_sixgill_info.nvd.base_score_v3</code>	Attribute	CVSS v3 Score	<code>.x_sixgill_info.nvd.modified</code>	N/A	N/A
<code>.x_sixgill_info.current.rating</code>	Attribute	Current Score	<code>.x_sixgill_info.event.event_datetime</code>	N/A	N/A
<code>.x_sixgill_info.highest.value</code>	Attribute	Highest Score	<code>.x_sixgill_info.event.event_datetime</code>	N/A	N/A
<code>.x_sixgill_info.cpe_match[].vendor</code>	Attribute	Affected Vendor	<code>.x_sixgill_info.nvd.modified</code>	qlik	N/A
<code>.x_sixgill_info.cpe_match[].product</code>	Attribute	Affected Product	<code>.x_sixgill_info.nvd.modified</code>	qlik_sense	N/A
<code>.x_sixgill_info.affected_packages[].ecosystem,</code> <code>.x_sixgill_info.affected_packages[].name</code>	Attribute	Affected Package	<code>.x_sixgill_info.nvd.modified</code>	Alpine:v3.18/vim	Keys are concatenated, separated by a / character
<code>.x_sixgill_info.attributes[].name</code>	Attribute	Attribution	<code>.x_sixgill_info.nvd.modified</code>	Has_POC_exploit_attribute	When <code>x_sixgill_info.attributes[].value == True</code>
<code>.x_sixgill_info.rating.previously Exploited</code>	Attribute	Previously Exploited	<code>.x_sixgill_info.event.event_datetime</code>	N/A	Bool -> Yes/No
<code>.x_sixgill_info.event.description</code>	Event Title	N/A	<code>.x_sixgill_info.event.event_datetime</code>	N/A	N/A
<code>.x_sixgill_info.event.level</code>	Attribute	Level	<code>.x_sixgill_info.event.event_datetime</code>	N/A	N/A
<code>.x_sixgill_info.event.previous_level</code>	Attribute	Previous Level	<code>.x_sixgill_info.event.event_datetime</code>	N/A	N/A
<code>.x_sixgill_info.event.new_base_score</code>	Attribute	New Base Score	<code>.x_sixgill_info.event.event_datetime</code>	N/A	N/A
<code>.x_sixgill_info.event.old_base_score</code>	Attribute	Old base Score	<code>.x_sixgill_info.event.event_datetime</code>	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.x_sixgill_info.event.type	Attribute	Event Type	.x_sixgill_info.event. event_datetime	N/A	N/A

Cybersixgill Alerts

This feed pulls alerts from your Cybersixgill portal. These alerts may be regarding compromised accounts, leaked credentials, or other security incidents. Using this feed will help you stay up to date with your attack surface, within ThreatQ.

The first request will fetch the list of alerts by date using the *primary feed*.

GET <https://api.cybersixgill.com/alerts/actionable-alert>

Sample Response:

```
[
  {
    "alert_name": "Recent mentions of your organization in the underground",
    "alert_type_id": "619d013e9a1c16790fc6f4be",
    "content": ",compound,img,false,32,2023-06-28,2023-06-28,\n31,11,https://www.@sixgill-start-highlight@acme@sixgill-end-highlight@.com/@sixgill-start-highlight@acme@sixgill-end-highlight@-missing-link-partnership/,Linking-Up to Strengthen Threat Operations in Australia,www.@sixgill-start-highlight@acme@sixgill-end-highlight@.com,https://www.themissinglink.com.au/,The Missing Link,branded,a,false,32,2023-03-30,2023-11-28,\n73,26,https://nvd.nist.gov/vuln/detail/CVE-2022-40288,NVD - CVE-2022-40288,nvd.nist.gov,https://www.themissinglink.com.au/se ...",
    "date": "2024-01-31 06:09:18",
    "es_id": "2d5aa1ae0aca7ef07cce3648c502a0ab40094a61",
    "id": "65b9e418168d64d1d32e93b2",
    "matched_assets": {
      "organization_aliases": ["acme"],
      "organization_name": ["acme"]
    },
    "read": true,
    "severity": 1,
    "site": "github",
    "status": {
      "name": "treatment_required"
    },
    "threat_level": "emerging",
    "threats": ["General Mentions"],
    "title": "Mentions of acme on underground sites",
    "user_id": "5f8fe7a1701ecb000f063250"
  },
  {
    "alert_name": "Compromised Accounts are Discussed in the Underground",
    "alert_type_id": "5f27fd269f94fd3b9d1acb71",

```

```

    "content": "... e/,Security
Testing,money,a,false,78,2023-09-19,2023-11-15,\nfor-review,2,0,https://
www.1001firms.com/list-of-companies/all/cyber_assurance/contact,Cyber assurance
- List of Companies,www.10...www.@sixgill-start-highlight@acme@sixgill-end-
highlight@.com",
    "date": "2024-01-30 11:51:07",
    "es_id": "2d5aa1ae0aca7ef07cce3648c502a0ab40094a61",
    "id": "65b8e2ad168d64d1d32e78be",
    "matched_assets": {
      "organization_aliases": ["acme"],
      "organization_name": ["acme"],
      "products": []
    },
    "read": true,
    "severity": 1,
    "site": "github",
    "status": {
      "name": "treatment_required"
    },
    "threat_level": "emerging",
    "threats": ["Compromised Accounts"],
    "title": "Underground discussion of acme accounts",
    "user_id": "5f8fe7a1701ecb000f063250"
  }
]

```

For each of those alerts, it will fetch the full details of it using the *supplemental feed*, *Cybersixgill - Get Alert by ID*.

ThreatQ provides the following default mapping for this feed:

The following mapping is based on each item returned by the Cybersixgill - Get Alert by ID supplemental feed

FEED DATA	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.matched_assets.organization_name[], .matched-assets.domain_names[], .matched-assets.cves[], .asset_information.asset_value	Asset Value, Vulnerability/ Indicator Value	N/A	.create_time	N/A	Object type depends on if the asset is a CVE or not
.title, .threat_level, .alert_id	Event Title	Alert	.create_time	N/A	Keys concatenated together to form Event Title
.actor_information	Adversary Name	N/A	.create_time	N/A	N/A
.es_item.tags[]	Event Tags	N/A	.create_time	N/A	N/A
.status.name	Event Attribute	Status	.create_time	treatment_required	Updatable

FEED DATA	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.category	Event Attribute	Category	.create_time	regular	Updatable
.alert_name	Event Attribute	Alert Type	.create_time	IabAlertRule	N/A
.threat_level	Event Attribute	Threat level	.create_time	Imminent	Title-cased
.threats[]	Event Attribute	Threat	.create_time	General Mention	N/A
.available_services[]	Event Attribute	Available Service	.create_time	purchase	N/A
.sub_alerts_length	Event Attribute	Is Aggregate Alert	.create_time	true	If value > 0
.asset_information.asset_type	Asset Attribute	Type	.create_time	domain	N/A
.asset_information.asset_subtypes	Event Attribute	Subtype	.create_time	email	N/A
.asset_information.importance	Event Attribute	Importance	.create_time	High	Updatable; Mapped from integer to human-readable string
.asset_information.risk_score	Event Attribute	Risk	.create_time	N/A	Updatable; Mapped from integer to human-readable string
.actor_information.actor_name	Adversary Attribute	Category	.create_time	N/A	N/A

Cybersixgill Compromised Accounts

This feed pulls compromised accounts from Cybersixgill. This may include accounts that have been breached, leaked, or otherwise compromised. This feed is not limited to compromised emails, but rather is more broad in scope, capturing accounts stolen by malware and other means.

The primary feed does not make an API call, but rather the *supplemental feed*, *Cybersixgill - Fetch Compromised Accounts*, is used to fetch results for each of your selected domains.

ThreatQ provides the following default mapping for this feed:

The following mapping is based on each item within the objects array, returned by the Cybersixgill - Fetch Compromised Accounts supplemental feed

FEED DATA	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.username	Compromised Account Value	N/A	.create_time	john.doe@gmail.com	N/A

FEED DATA	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.stealer_malware	Malware Value	N/A	.create_time	REDLINE	If enabled
.breach_name	Tag	N/A	N/A	stealer-malware-logs	If enabled
.domain	Attribute	Credential Domain	.create_time	gmail.com	If enabled
.host_domain	Attribute	Impacted Domain	.create_time	facebook.com	If enabled
.host	Attribute	Impacted URL	.create_time	https://facebook.com/login	If enabled
.password	Attribute	Password	.create_time	hunter2	If enabled
.hash_type	Attribute	Password Hash Type	.create_time	plain	If enabled
.name	Attribute	Name	.create_time	N/A	If enabled
.breach_date	Attribute	Breached At	.create_time	N/A	If enabled

Cybersixgill Compromised Emails

This feed pulls compromised emails from Cybersixgill. This feed typically includes emails that have been leaked or phished, and may include passwords or other related information.

The primary feed does not make an API call, but rather the *supplemental feed, Cybersixgill - Fetch Compromised Emails*, is used to fetch results for each of your selected domains.

ThreatQ provides the following default mapping for this feed:

*The following mapping is based on each item within the `objects` array, returned by the *Cybersixgill - Fetch Compromised Emails* supplemental feed*

FEED DATA	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.username	Compromised Account Value	N/A	.create_time	john.doe@gmail.com	N/A
.breach_name	Tag	N/A	N/A	stealer-malware-logs	If enabled
.domain	Attribute	Credential Domain	.create_time	gmail.com	If enabled
.password	Attribute	Password	.create_time	hunter2	If enabled
.hash_type	Attribute	Password Hash Type	.create_time	plain	If enabled
.name	Attribute	Name	.create_time	N/A	If enabled
.breach_date	Attribute	Breached At	.create_time	N/A	If enabled

Get Feed Data (Supplemental)

Fetches data from a specific Cybersixgill feed.

GET `https://api.cybersixgill.com/{{feed name}}/ioc`

Sample Response:

See sample data from specific primary feed

Acknowledge Feed Data (Supplemental)

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/{{feed name}}/ioc/ack`

Sample Response:

```
1000
```

Cybersixgill - Get Alert by ID (Supplemental)

Fetches the full details for an alert by its ID

GET `https://api.cybersixgill.com/alerts/actionable_alert/{{alert ID}}`

Sample Response:

```
{
  "actor_information": {
    "active_since": "2023-09-28T14:34:29",
    "activity": 1,
    "actor_name": "pbscybsec",
    "languages": ["en"],
    "reputation": 1,
    "site": "github"
  },
  "additional_info": {
    "asset_attributes": ["organization_aliases", "organization_name"],
    "assets_counter": {
      "organization_aliases": {
        "acme": 1
      },
      "organization_name": {
        "acme": 1
      }
    },
    "excluded_assets": {},
    "matched_organization_aliases": ["acme"],
    "matched_organization_name": ["acme"],
    "organization_aliases": ["acme"],
    "organization_name": "acme",
    "query_attributes": ["organization_aliases", "organization_name"],
  }
}
```

```

    "template_id": "619d013e9a1c16790fc6f4be",
    "vendor": "Sixgill"
  },
  "alert_id": "62409ba14511c6c8a9f4e3e3",
  "alert_name": "Recent mentions of your organization in the underground",
  "alert_type": "PercolatedQueryBasedManagedAlertRule",
  "alert_type_id": "619d013e9a1c16790fc6f4be",
  "assessment": "",
  "asset_information": {},
  "category": "regular",
  "content_type": "search_result_item",
  "create_time": "2023-12-26 06:10:49",
  "description": "\"acme\" was recently mentioned on underground sites",
  "es_id": "330125ea0391d44882c42f0aa7a49226f388eb7a",
  "es_item": {
    "collection_date": "2023-12-25T09:38:13",
    "content": "... to various Threat intelligence domains.\n# Table of
Contents\n- [Threat Intelligence Platforms](#threat-intelligence-platforms)\n-
[Open-Source Threat Intelligence Tools](#open-source...https://www.@sixgill-
start-highlight@acme@sixgill-end-highlight@.com/",
    "content_urls": "https://www.@sixgill-start-highlight@acme@sixgill-end-
highlight@.com/",
    "creator": "pbscybsec",
    "date": "2023-09-28T14:34:29",
    "highlight": {
      "content": [
        "** Readme **\n\n# Biggest-Threat-Intelligence-Resource\nThis
repository is a comprehensive collection of the most popular and useful Threat
intelligence resources available on the internet. It includes resources related
to various Threat intelligence domains.\n\n# Table of Contents\n\n- [Threat
Intelligence Platforms](#threat-intelligence-platforms)\n- [Open-Source Threat
Intelligence Tools](#open-source"
      ],
      "content_urls": [
        "https://www.@sixgill-start-highlight@acme@sixgill-end-highlight@.com/"
      ]
    },
    "id": "330125ea0391d44882c42f0aa7a49226f388eb7a",
    "images": [],
    "lang": "en",
    "rep_grade": 5,
    "site": "github",
    "tags": ["Twitter_handle", "Hacking", "APT", "Drugs", "Malware"],
    "title": "Threat-Intelligence",
    "type": "repository"
  },
  "has_comments": false,
  "id": "658a6e6b8656daba37822554",
  "iq_information": {},
  "iq_prioritized": true,

```

```

"is_deleted": false,
"lang": "English",
"langcode": "en",
"matched_assets": {
  "organization_aliases": ["acme"],
  "organization_name": ["acme"]
},
"read": false,
"recommendations": [""],
"severity": 1,
"site": "github",
"site_information": {
  "active_since": "1970-01-01T07:00:00",
  "description": "Popular web-based hosting service for version control using
Git.",
  "languages": ["en"],
  "site_name": "github",
  "stars": 5,
  "type": "Github"
},
"status": {
  "name": "treatment_required"
},
"summary": "",
"threat_level": "emerging",
"threats": ["General Mentions"],
"title": "Mentions of acme on underground sites",
"trigger_actions": [],
"update_time": "2023-12-26 06:10:49",
"user_id": "5f8fe7a1701ecb000f063250"
}

```

Cybersixgill - Fetch Compromised Accounts (Supplemental)

Fetches compromised accounts for a given domain.

POST https://api.cybersixgill.com/data_leak/credentials/logins/search

Sample Response:

```

{
  "objects": [
    {
      "breach_id": 5670012,
      "breach_name": "stealer-malware-logs",
      "breach_description": "The following credentials were obtained using a
stealer malware, and shared on the Telegram channel \"OBSERVERCLOUD - BEST FREE
COMBO CLOUD\" (channel id: 1851318122) on 2024-03-05. They were extracted from
a file named \"@txtlog - FREE - 318.txt\", with a size of 191.7 MB.",
      "breach_publication_date": "2024-03-05",
      "domain": "",

```

```

    "hash_type": "plain",
    "name": "",
    "password": "Z$ZtP@$$1234",
    "post_id": "f28928e4fa2bfd2b05f72074f3ca5321",
    "source_name": "telegram",
    "post_title": "Daily Telegram Channel 👁 OBSERVERCLOUD - BEST FREE COMBO
CLOUD (1851318122)",
    "username": "john.doe",
    "host": "https://acme.roadrunner.com/login",
    "host_domain": "acme.roadrunner.com",
    "stealer_malware": "REDLINE",
    "create_time": "2024-03-05T20:35:35.347031"
  },
  {
    "breach_id": 5348935,
    "breach_name": "stealer-malware-logs",
    "breach_description": "The following credentials were obtained using a
stealer malware, and shared on the Telegram channel \"OBSERVERCLOUD - BEST FREE
COMBO CLOUD\" (channel id: 1851318122) on 2024-03-04. They were extracted from
a file named \"@urllogpass_diller_1000000.txt\", with a size of 75.4 MB.",
    "breach_publication_date": "2024-03-04",
    "domain": "roadrunnersystems.com",
    "hash_type": "plain",
    "name": "",
    "password": "Z*&^^VtP@$^&$",
    "post_id": "eb59ff30381b800177ddd59c7e242354",
    "source_name": "telegram",
    "post_title": "Daily Telegram Channel 👁 OBSERVERCLOUD - BEST FREE COMBO
CLOUD (1851318122)",
    "username": "john.doe@roadrunnersystems.com",
    "host": "https://acme.roadrunner.com/login",
    "host_domain": "acme.roadrunner.com",
    "stealer_malware": "",
    "create_time": "2024-03-05T09:22:56.560810"
  }
]
}

```

Cybersixgill - Fetch Compromised Emails (Supplemental)

Fetches compromised emails for a given domain.

POST https://api.cybersixgill.com/data_leak/credentials/leaks/search

Sample Response:

```

{
  "objects": [
    {
      "breach_id": 273204,
      "breach_name": "leaked-credentials",

```

```

    "breach_description": "The following credentials were shared on the
Telegram channel \"Raidforums Official\" (channel id: 2124656678) on
2024-01-22. They were extracted from a file named \"25kk By
Chucky_7_2000000.txt\", with a size of 67.3 MB.",
    "breach_publication_date": "2024-01-22",
    "email": "adam.quest@acme.com",
    "domain": "acme.com",
    "is_email_domain": true,
    "hash_type": "plain",
    "name": "",
    "password": "W3bb0y1!",
    "post_id": "d048ac18be31fd71c242a4659319f6c4",
    "source_name": "telegram",
    "post_title": "Daily Telegram Channel Raidforums Official (2124656678)",
    "create_time": "2024-01-24T01:04:50.497875"
  },
  {
    "breach_id": 254158,
    "breach_name": "leaked-credentials",
    "breach_description": "The following credentials were shared on the
Telegram channel \"CHAT | HQ COMBO | FRESH BASE http://proshoping24.ru Onlain
magazin\" (channel id: 1368172612) on 2023-11-27T18:40:32. They were extracted
from a file named \"621k no valid hq vip combo [@darkwebs_guru].txt.txt\", with
a size of 19.6 MB.",
    "breach_publication_date": "2023-11-27",
    "email": "john.doe@acme.com",
    "domain": "acme.com",
    "is_email_domain": true,
    "hash_type": "plain",
    "name": "",
    "password": "hunter2",
    "post_id": "d4d60e4da1892fdc59e4102df953b715d159e224",
    "source_name": "telegram",
    "post_title": "",
    "create_time": "2023-11-27T20:57:55.484928"
  }
]
}

```

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	2001
Indicator Attributes	30,248
Adversaries	65
Attack Patterns	2
Attack Patterns Attributes	21

Cybersixgill DVE

METRIC	RESULT
Run Time	3 minutes
Vulnerabilities	158
Vulnerability Attributes	2,404

Cybersixgill Alerts

METRIC	RESULT
Run Time	1 minute
Adversaries	4
Adversary Attributes	8
Assets	2
Asset Attributes	4
Events	13
Event Attributes	91

Cybersixgill Compromised Accounts

METRIC	RESULT
Run Time	1 minute
Compromised Accounts	5
Compromised Account Attributes	25
Malware	1

Cybersixgill Compromised Emails

METRIC	RESULT
Run Time	1 minute
Compromised Accounts	15
Compromised Account Attributes	24

Known Issues

- The Darkfeed & DVE feeds are limited to a maximum amount of items fetched per feed run:
 - Darkfeed: 100,000 items
 - DVE: 25,000 items

Change Log

- **Version 1.1.1 rev-a**
 - Guide Update - added steps for installing the Compromised Account custom object.
- **Version 1.1.1**
 - Resolved an issue where users would encounter an error if no matched assets were returned by the feed.
- **Version 1.1.0**
 - Adds Cybersixgill DVE, Cybersixgill Alerts, Cybersixgill Compromised Accounts, and Cybersixgill Compromised Emails feeds.
 - Updates to the Cybersixgill Darkfeed:
 - Adds support for additional indicator types; IPv6 Address, Email Address
 - Adds user field selections for ingested context
 - Adds TLP support
 - Renames `False Positive` attribute to `Revoked`
 - Labels will now be ingested as Tags
 - Renames `Cybersixgill Post ID` attribute to `Cybersixgill Post Link`
 - Removes `Cybersixgill Feed ID` attribute
 - Fixes issue ingesting "None" label (now a tag)
 - The feed will no longer mark Revoked indicators as Whitelisted
 - Fixes issue where the feed would not fully paginate through all the available data
 - Previous versions of the feed would stop after 2k entries
 - This feed will now ingest up to 50k entries per run
- **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