# ThreatQuotient

## Brandefense CDF

**Version 1.0.0**

October 21, 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**
Organization Custom Object ..... 7
ThreatQ V6 Steps ..... 7
ThreatQ v5 Steps ..... 8
**Installation** ..... **10**
**Configuration** ..... **11**
Brandefense Incident Parameters ..... 11
Brandefense Indicators of Compromise Parameters ..... 12
Brandefense CTI Rules Parameters ..... 13
Brandefense Assets Parameters ..... 14
**ThreatQ Mapping** ..... **15**
Brandefense Incidents ..... 15
Fetch Incidents ..... 15
Fetch Incident Details ..... 16
Fetch Incident Related Indicators ..... 17
Brandefense Indicators of Compromise ..... 22
Brandefense CTI Rules ..... 24
Brandefense Assets ..... 26
**Average Feed Run** ..... **29**
Brandefense Incidents ..... 29
Brandefense Indicators of Compromise ..... 30
Brandefense CTI Rules ..... 30
Brandefense Assets ..... 30
**Change Log** ..... **31**

# 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** | 1.0.0 |
| **Compatible with ThreatQ Versions** | >= 5.24.0 |
| **Support Tier** | ThreatQ Supported |

# Introduction

The Brandefense CDF provides users with ability to ingest data from Brandefense.

The integration provides the following feeds:

- **Brandefense Incidents** - ingests Incidents from Brandefense back to ThreatQ.
- **Brandefense Indicators of Compromise** - ingests IOCs from Brandefense back to ThreatQ.
- **Brandefense CTI Rules** - ingests YARA Signatures from Brandefense back to ThreatQ.
- **Brandefense Assets** - ingests Assets from Brandefense back to ThreatQ.

The feeds included with this integration ingest the following object types:

- Assets
  - Assets Attributes
- Incidents
  - Incidents Attributes
- Indicators
  - Indicator Attributes
- Organizations
  - Organization Attributes
- Signatures
  - Signatures Attributes

# Prerequisites

The integration requires the following:

- Brandefense Token
- Organization Custom Object

> The Organization custom object must be installed prior to installing the CDF.

## Organization Custom Object

The integration requires the Organization custom object.

Use the steps provided to install the Organization 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

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 following location:

   ```
   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
     - organization.json
     - images (directory)
       - organization.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

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 brandefense_cdf
   ```

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

   ```
   mkdir images
   ```

7. Upload the organization.svg.
8. Navigate to the **/tmp/brandefense_cdf**.

   The directory should resemble the following:

   - tmp
     - **brandfense_cdf**
       - **organization.json**
       - **install.sh**
       - **images**
         - **organization.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 brandefense_cdf
```

# Installation

> The integration requires that the Organization custom object be installed on the ThreatQ platform first. Attempting to install the integration prior to installing Organization custom object will result in failure.

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 zip file.
3. Extract and install the Organization custom object if you have not done so already.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the integration 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
7. Select the individual feeds to install, when prompted 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.

The feed(s) 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:

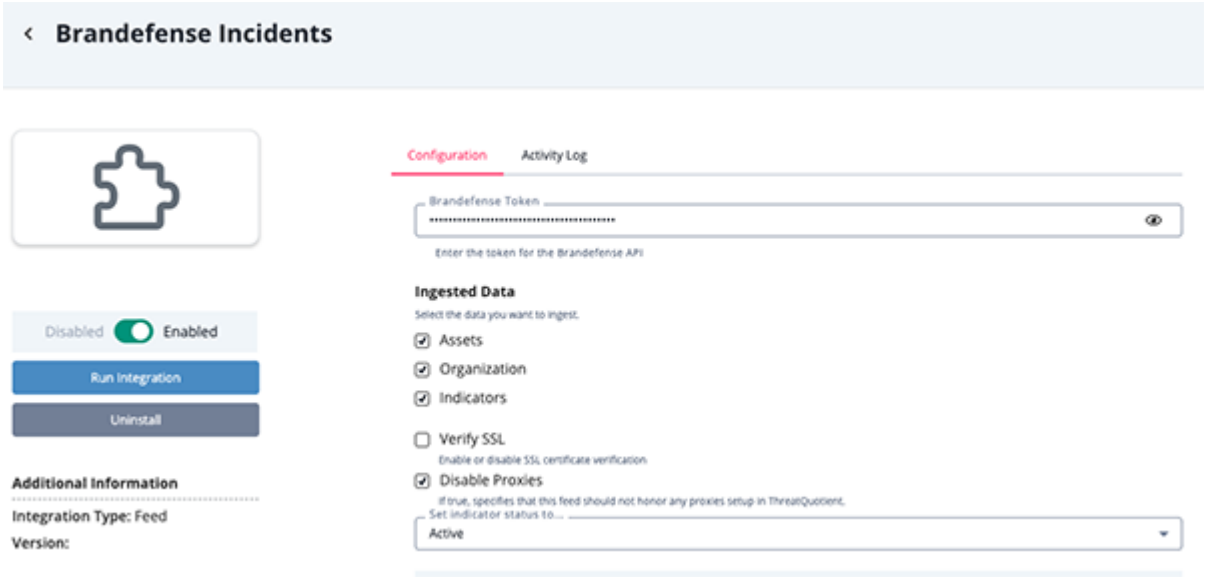
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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:

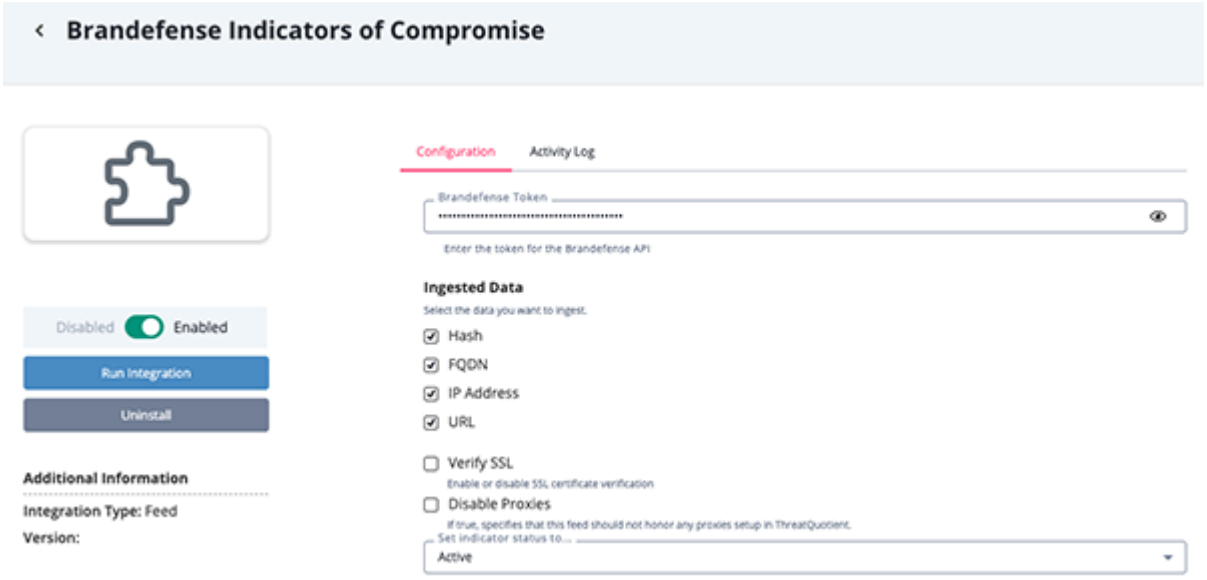
## Brandefense Incident Parameters

| PARAMETER | DESCRIPTION |
|---|---|
| **Brandefense Token** | Your Brandefense Token. |
| **Ingested Data** | Select the data to ingest. Options include:<br>◦ Assets<br>◦ Organization<br>◦ Indicators |
| **Disable Proxies** | Enable this option to have the feed ignore proxies set in the ThreatQ UI. |
| **Verify SSL** | Enable this option if the feed should verify the SSL certificate. |



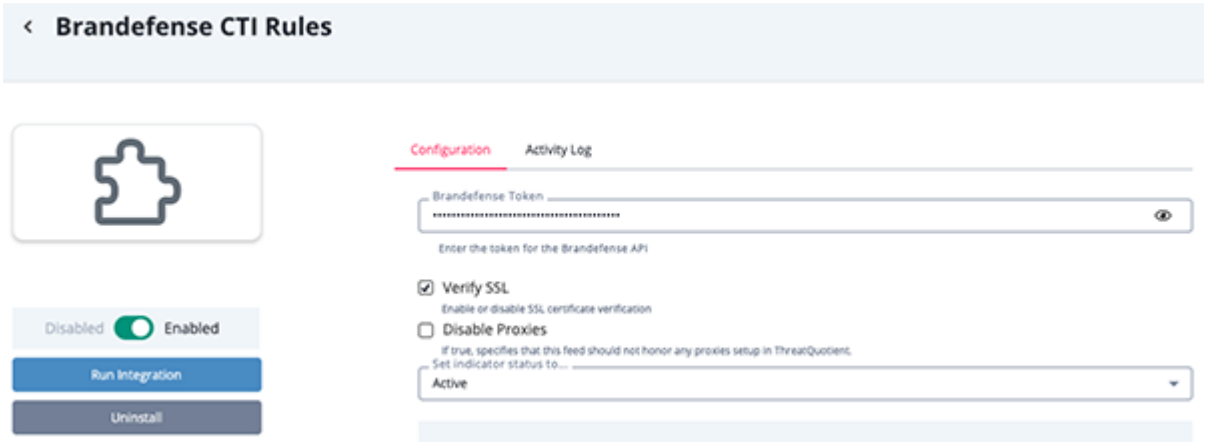

# Brandefense Indicators of Compromise Parameters

| PARAMETER | DESCRIPTION |
|---|---|
| **Brandefense Token** | Your Brandefense Token. |
| **Ingested Data**<br>*(Incident & Indicator of Compromise feeds only)* | Select the data to ingest. Options include:<br>◦ Hash<br>◦ FQDN<br>◦ IP Address<br>◦ URL |
| **Disable Proxies** | Enable this option to have the feed ignore proxies set in the ThreatQ UI. |
| **Verify SSL** | Enable this option if the feed should verify the SSL certificate. |



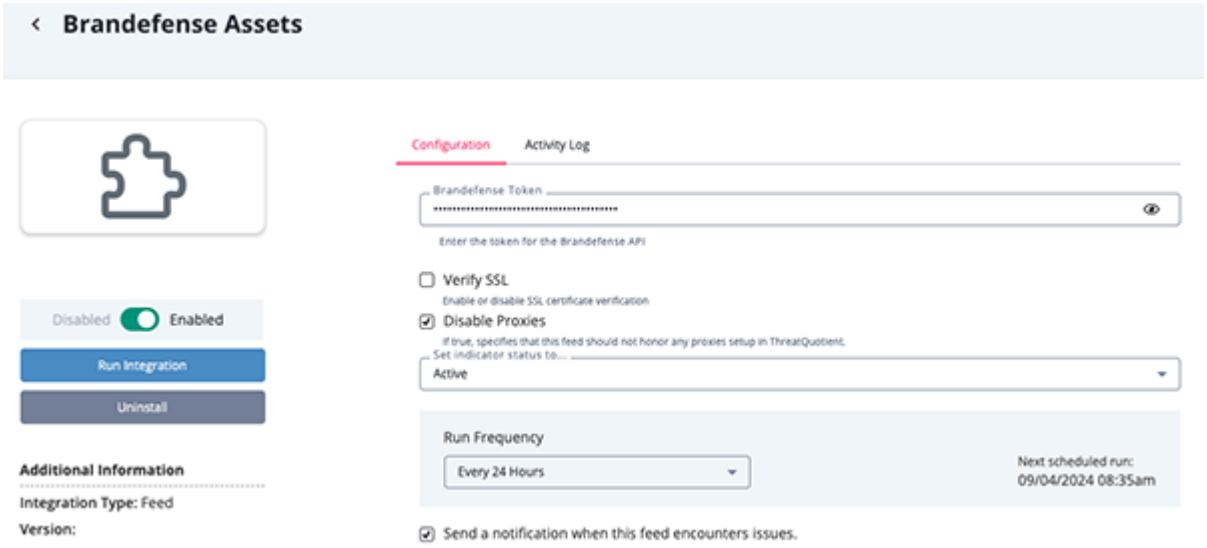

# Brandefense CTI Rules Parameters

| PARAMETER | DESCRIPTION |
|---|---|
| **Brandefense Token** | Your Brandefense Token. |
| **Disable Proxies** | Enable this option to have the feed ignore proxies set in the ThreatQ UI. |
| **Verify SSL** | Enable this option if the feed should verify the SSL certificate. |



# Brandefense Assets Parameters

| PARAMETER | DESCRIPTION |
|---|---|
| **Brandefense Token** | Your Brandefense Token. |
| **Disable Proxies** | Enable this option to have the feed ignore proxies set in the ThreatQ UI. |
| **Verify SSL** | Enable this option if the feed should verify the SSL certificate. |




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

## Brandefense Incidents

The Brandfense Incidents feed ingests Incident and Incident related indicators into the ThreatQ platform

### Fetch Incidents

`GET https://api.brandefense.io/api/v1/incidents`

**Sample Response:**


```
{
    "count": 7890,
    "next": "https://api.brandefense.io/api/v1/incidents?page=2",
    "previous": null,
    "results": [
        {
            "id": 545052,
            "code": "BRNDE-ASM-306",
            "created_at": "2024-08-21T00:59:42.148079Z",
            "status": "OPEN",
            "asset": {
                "id": 1639,
                "asset": "brandefense.io",
                "type": "DOMAIN",
                "status": "ACTIVE"
            },
            "organization": {
                "id": 15,
                "name": "PS BRANDEFENSE DEMO",
                "short_code": "BRNDE",
                "code": "brandefense-demo",
                "is_active": true,
                "is_mssp": false,
                "license_type": "LICENSED"
            },
            "title": "Daily Discovered Entity Updates",
            "assignees": [],
            "indicator_count": 45,
            "attachment_count": 0,
            "comment_count": 0,
            "category": "EXPOSURE_MANAGEMENT",
            "module": "ATTACK_SURFACE",
            "network_type": "SURFACE_WEB",
            "type": "SECURITY_SCAN",
```

```
            "tags": [],
            "mitre_tactics": [
                "RECONNAISSANCE",
                "DISCOVERY"
            ],
            "severity": "INFO"
        }
    ]
}
```


## Fetch Incident Details

`GET https://api.brandefense.io/api/v1/incidents/{code}`

**Sample Response:**


```
{
    "id": 545052,
    "code": "BRNDE-ASM-306",
    "created_at": "2024-08-21T00:59:42.148079Z",
    "status": "OPEN",
    "risk_score": 15,
    "asset": {
        "id": 1639,
        "asset": "brandefense.io",
        "type": "DOMAIN",
        "status": "ACTIVE"
    },
    "organization": {
        "id": 15,
        "name": "PS BRANDEFENSE DEMO",
        "short_code": "BRNDE",
        "code": "brandefense-demo",
        "is_active": true,
        "is_mssp": false,
        "license_type": "LICENSED"
    },
    "title": "Daily Discovered Entity Updates",
    "description": "<p>This incident provides an overview of the latest
findings in the attack surface monitoring over the last 24 hours. It includes
details of exposed panels, new JavaScript files, subdomain changes, SSL
certificate registrations, DNS record updates, open ports, service changes on
ports and WHOIS record modifications.</p>",
    "evidence": {
        "Total_Entity_Count": "<a href=\"/modules/attack-surface/entities/ip-
addresses?
page=1&page_size=20first_seen__range=2024-08-20T01:00:48.779Z,2024-08-21T00:59:
41.538Z\">Exposed IP Address: 1/<a><br><a href=\"/modules/attack-surface/
entities/dns-records?
page=1&page_size=20first_seen__range=2024-08-20T01:00:48.779Z,2024-08-21T00:59:
```

```
41.539Z\">DNS Record Found: 45</a><br>",
        "Daily_Discovered_Entity_Details": "<a href=\"/modules/attack-surface/
updates?
page=1&page_size=20last_seen__range=2024-08-20T01:00:48.779Z,2024-08-21T00:59:4
1.550Z\"> See All</a>"
    },
    "solution_title": "Verify and Approve Daily Discovered Entity Updates",
    "solution": "
```


This incident report uses a general overview and consolidates various findings into categories, offering a structured method for reporting daily attack surface discoveries. Therefore, it is strongly advised to:

- **Verify and Investigate:** All new findings should be thoroughly verified and investigated to determine their authenticity and potential security impact.
- **Secure and Monitor:** Implement necessary security measures to protect against identified risks and continuously monitor for any suspicious activity.
- **Update and Patch:** Ensure all systems and software are up to date with the latest patches to mitigate vulnerabilities.


```
", "assignees": [], "indicator_count": 45, "attachment_count": 0,
"comment_count": 0, "category": "EXPOSURE_MANAGEMENT", "module":
"ATTACK_SURFACE", "network_type": "SURFACE_WEB", "type": "SECURITY_SCAN",
"tags": [], "mitre_tactics": [], "severity": "INFO" }
```


## Fetch Incident Related Indicators

```
GET https://api.brandefense.io/api/v1/incidents/{code}/indicators
```

**Sample Response:**


```
{
    "next": null,
    "previous": null,
    "count": 45,
    "results": [
        {
            "_id": 117704372,
            "Date": "2024-08-20T07:04:53",
            "Entity": "docs.brandefense.io",
            "Finding": "DNS Record Found",
            "Description": "New A Record: 34.251.194.182 found on
docs.brandefense.io",
            "_entity_params": [
                "Entity"
            ]
        },
        {
            "_id": 1177042,
            "Domain": "docs.brandefense.io"
```

```
        },
        {
            "id": 171096,
            "created_at": "2023-07-18T09:46:06.584460Z",
            "content_object": [
                {
                  "data": "pncbankartscenter.org",
                  "data_source": "certstream",
                  "detection_id": 16441,
                  "detection_date": "2021-09-29",
                  "is_domain": true,
                  "register_date": "2012-03-30",
                  "risk_score": 55,
                  "last_analyze_date": "2021-09-29"
                },
                {
                    "botnet_id": "",
                    "breached_date": "2023-11-05",
                    "data": "",
                    "id": 5168943,
                    "username": "olivier.pacaud@threatq.com"
                }
            ],
            "status": "POTENTIAL",
            "takedown_status": "NOT_REQUESTED"
        },
        {
                "IP_Address": "3.217.205.239",
                "_id": 121212336
        }
    ]
}{
    "next": null,
    "previous": null,
    "count": 45,
    "results": [
        {
            "_id": 117704372,
            "Date": "2024-08-20T07:04:53",
            "Entity": "docs.brandefense.io",
            "Finding": "DNS Record Found",
            "Description": "New A Record: 34.251.194.182 found on
docs.brandefense.io",
            "_entity_params": [
                "Entity"
            ]
        },
        {
            "_id": 1177042,
            "Domain": "docs.brandefense.io"
```

```
        },
        {
            "id": 171096,
            "created_at": "2023-07-18T09:46:06.584460Z",
            "content_object": [
                {
                  "data": "pncbankartscenter.org",
                  "data_source": "certstream",
                  "detection_id": 16441,
                  "detection_date": "2021-09-29",
                  "is_domain": true,
                  "register_date": "2012-03-30",
                  "risk_score": 55,
                  "last_analyze_date": "2021-09-29"
                },
                {
                    "botnet_id": "",
                    "breached_date": "2023-11-05",
                    "data": "",
                    "id": 5168943,
                    "username": "olivier.pacaud@threatq.com"
                }
            ],
            "status": "POTENTIAL",
            "takedown_status": "NOT_REQUESTED"
        },
        {
                "IP_Address": "3.217.205.239",
                "_id": 121212336
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| `results[].code + results[].title` | Incident.Value | N/A | `results[].created_at` | `BRNDE-ASM-306 - Daily Discovered Entity Updates` | The value of the Incident is formed by concatenating both keys |
| `results[].created_at` | Incident.Published_at | N/A | `results[].created_at` | `2024-08-21T00:59:42.148079Z` | N/A |
| `results[].created_at` | Incident.Started_at | N/A | `results[].created_at` | `2024-08-21T00:59:42.148079Z` | N/A |
| `results[].created_at` | Incident.Ended_at | N/A | `results[].created_at` | `2024-08-21T00:59:42.148079Z` | N/A |
| `results[].description + results[].evidence.description + results[].solution_title + results[].solution` | Incident.Description | N/A | `results[].created_at` | `This incident provides an overview...` | The description of the Incident is formed by concatenating the keys |
| `results[].code` | Incident.Attribute | Code | `results[].created_at` | `BRNDE-ASM-306` | N/A |
| `results[].status` | Incident.Attribute | Incident Status | `results[].created_at` | `OPEN` | Updatable |
| `results[].risk_score` | Incident.Attribute | Incident Risk Score | `results[].created_at` | `15` | Updatable |
| `results[].category` | Incident.Attribute | Incident Category | `results[].created_at` | `EXPOSURE_MANAGEMENT` | N/A |
| `results[].module` | Incident.Attribute | Incident Module | `results[].created_at` | `ATTACK_SURFACE` | N/A |
| `results[].network_type` | Incident.Attribute | Incident Network Type | `results[].created_at` | `SURFACE_WEB` | N/A |
| `results[].type` | Incident.Attribute | Incident Type | `results[].created_at` | `SECURITY_SCAN` | N/A |
| `results[].severity` | Incident.Attribute | Incident Severity | `results[].created_at` | `INFO` | Updatable |
| `results[].asset.asset` | Related Asset.Value | N/A | `results[].created_at` | `brandefense.io` | N/A |
| `results[].asset.type` | Related Asset.Attribute | Asset Type | `results[].created_at` | `DOMAIN` | N/A |
| `results[].asset.status` | Related Asset.Attribute | Asset Status | `results[].created_at` | `ACTIVE` | N/A |
| `results[].organization.name` | Related Organization.Value | N/A | `results[].created_at` | `PS BRANDEFENSE DEMO` | N/A |
| `results[].organization.short_code` | Related Organization.Attribute | Organization Short Code | `results[].created_at` | `BRNDE` | N/A |
| `results[].organization.code` | Related Organization.Attribute | Organization Code | `results[].created_at` | `brandefense-demo` | N/A |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| `results[].organization.license_type` | Related Organization.Attribute | Organization License Type | `results[].created_at` | `LICENSED` | N/A |
| `results[].Entity` | Related Indicator.Value | FQDN | `results[].Date` | `docs.brandefense.io` | N/A |
| `results[].Finding` | Related Indicator.Attribute | Indicator Finding | `results[].Date` | `DNS Record Found` | N/A |
| `results[].Description` | Related Indicator.Description | N/A | `results[].Date` | `New A Record: 34.251.194.182 found on docs.brandefense.io` | N/A |
| `results[].content_object.data` | Related Indicator.Value | FQDN | `results[].created_at` | `pncbankartscenter.org` | N/A |
| `results[].content_object.data_source` | Related Indicator.Attribute | Indicator Data Source | `results[].created_at` | `certstream` | N/A |
| `results[].content_object.risk_score` | Related Indicator.Attribute | Indicator Risk Score | `results[].created_at` | `55` | N/A |
| `results[].status` | Related Indicator.Attribute | Indicator Status | `results[].created_at` | `POTENTIAL` | N/A |
| `results[].takedown_status` | Related Indicator.Attribute | Indicator Takedown Status | `results[].created_at` | `NOT_REQUESTED` | N/A |
| `results[].IP_Address` | Related Indicator.Value | IP Address | `results[].created_at` | `3.217.205.239` | N/A |
| `results[].content_object.username` | Related Indicator.Value | Email Address | `results[].created_at` | `demo@threatq.com` | N/A |

# Brandefense Indicators of Compromise

The Brandefense Indicators of Compromise feed ingests indicators into the ThreatQ platform.

```
GET https://api.brandefense.io/api/v1/threat-intelligence/iocs?
ioc_type={ioc_type}
```

**Sample Response:**


```
{
    "count": 282082,
    "previous": null,
    "next": "https://api.brandefense.io/api/v1/threat-intelligence/iocs?
ioc_type=ip_address&page=2",
    "results": [
        {
            "data": "104.210.133.240",
            "type": "ipv4",
            "category": "online_scanners",
            "module": "sans_research",
            "severity": "medium",
            "data_source_type": "isc.sans.edu",
            "extras": {
                "added_date": "2024-08-21",
                "type": "openai",
                "as": "AS8075 Microsoft Corporation",
                "asname": "MICROSOFT-CORP-MSN-AS-BLOCK",
                "country": "United States",
                "countryCode": "US",
                "isp": "Microsoft Corporation",
                "lat": 29.4167,
                "lon": -98.5
            },
            "last_seen": "2024-08-22T09:29:03.564998+00:00",
            "first_seen": "2024-08-22T09:29:03.564998+00:00",
            "count": 1
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| `results[].data` | Indicator.Value | `results[].type` | `results[].first_seen` | `104.210.133.240` | We use the value on `results[].type` to determinate the IOC type |
| `results[].category` | Indicator.Attribute | Indicator Category | `results[].first_seen` | `online_scanners` | N/A |
| `results[].module` | Indicator.Attribute | Indicator Module | `results[].first_seen` | `sans_research` | N/A |
| `results[].severity` | Indicator.Attribute | Indicator Severity | `results[].first_seen` | `sans_research` | Updatable |
| `results[].data_source_type` | Indicator.Attribute | Indicator Data Source Type | `results[].first_seen` | `isc.sans.edu` | N/A |
| `results[].extras.type` | Indicator.Attribute | Type | `results[].first_seen` | `openai` | N/A |
| `results[].extras.as` | Indicator.Attribute | AS | `results[].first_seen` | `AS8075 Microsoft Corporation` | N/A |
| `results[].extras.asname` | Indicator.Attribute | AS Name | `results[].first_seen` | `MICROSOFT-CORP-MSN-AS-BLOCK` | N/A |
| `results[].extras.country` | Indicator.Attribute | Country | `results[].first_seen` | `United States` | N/A |
| `results[].extras.countryCode` | Indicator.Attribute | Country Code | `results[].first_seen` | `US` | N/A |
| `results[].extras.isp` | Indicator.Attribute | ISP | `results[].first_seen` | `Microsoft Corporation` | N/A |
| `results[].extras.lat` | Indicator.Attribute | Latitude | `results[].first_seen` | `29.4167` | N/A |
| `results[].extras.lon` | Indicator.Attribute | Longitude | `results[].first_seen` | `-98.5` | N/A |

# Brandefense CTI Rules

The Brandefense CTI Rules feed ingests signatures.

`GET https://api.brandefense.io/api/v1/threat-intelligence/rules`

**Sample Response:**


```
{
    "count": 8169,
    "previous": null,
    "next": "https://api.brandefense.io/api/v1/threat-intelligence/rules?
page=2",
    "results": [
        {
            "tags": [
                "Oyster Backdoor"
            ],
            "id": 16025,
            "type": "rule_yara",
            "identifier": "RULE_YARA-8035",
            "source": "BRANDEFENSE",
            "content": "rule MAL_Backdoor_Oyster_Backdoor_Win_DLL_July26{\n
meta:\n        author = \"Gokhan FIRAT\"\n        source = \"brandefense.io\"\n
date = \"26.07.2024\"\n    strings:\n        $s1 = \"Boost.Beast/351\" ascii\n
$s2 = \"C:\\\\Users\\\\postman\\\\Desktop\\\\NZT\\\\ProjectD_cpprest\\\\\n
CleanUp\\\\Release\\\\CleanUp.pdb\" ascii\n        $s3 = \"WORKGROUP\" wide\n
$h1 = { 0F B6 02 8D 52 FF 8A 0C 37 0F B6 80 ?? ?? ?? ?? 88 04 37 46 0F B6 C1 0F
B6 80 ?? ?? ?? ?? 88 42 01 3B 75 B4 7C DA }\n        $h2 = { 8A 0C 38 8D 52 FF
0F B6 42 01 8B 75 FC 0F B6 80 ?? ?? ?? ?? 88 04 3E 47 0F B6 C1 0F B6
80 ?? ?? ?? ?? 88 42 01 8B C6 3B FB 7C D5 }\n        $h3 = { 0F B6 02 8D 52 FF
8A 0C 37 8A 80 ?? ?? ?? ?? 88 04 37 46 0F B6 C1 8A 80 ?? ?? ?? ?? 88 42 01 3B
B5 54 FE FF FF 7C D9 }\n    condition:\n        uint16(0) == 0x5A4D and\n
any of ($s*) and\n        2 of ($h*)\n}",
            "created_at": "2024-08-19T06:17:27.257113+00:00",
            "updated_at": "2024-08-19T06:17:27.257113+00:00"
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| `results[].content` | Signature.Name | N/A | `results[].created_at` | `MAL_Backdoor_Oyster_Backdoor_Win_DLL_July26` | We extract the name from `results[].content` |
| `results[].content` | Signature.Value | N/A | `results[].created_at` | `rule MAL_Backdoor_Oyster_Backdoor_Win_DLL_July26...` | N/A |
| `results[].tags` | Signature.Tag | N/A | `results[].created_at` | `Oyster Backdoor` | N/A |
| `results[].identifier` | Signature.Attribute | Identifier | `results[].created_at` | `RULE_YARA-8035` | N/A |
| `results[].source` | Signature.Attribute | External Source | `results[].created_at` | `BRANDEFENSE` | N/A |

# Brandefense Assets

The Brandefense Assets feed ingests assets and related organizations into the ThreatQ platform.

`GET https://api.brandefense.io/api/v1/assets`

**Sample Response:**


```
{
    "count": 227,
    "next": "https://api.brandefense.io/api/v1/assets?page=2",
    "previous": null,
    "results": [
        {
            "id": 204449,
            "status": "SUGGESTED",
            "modules": [
                {
                    "name": "Attack Surface",
                    "code": "attack-surface",
                    "short_code": "ASM",
                    "category": "exposure-management"
                }
            ],
            "created_by": {
                "id": 3,
                "name": "Automation",
                "email": "automation@brandefense.io",
                "role": "ADMIN"
            },
            "type": "DOMAIN",
            "severity": "MEDIUM",
            "organization": {
                "id": 722,
                "name": "ThreatQuotient",
                "short_code": "THRTQ",
                "code": "threatquotient",
                "is_active": true,
                "is_mssp": false,
                "license_type": "PROOF_OF_CONCEPT",
                "country": [
                    "US"
                ],
                "industries": [
                    "Technology",
                    "Retail",
                    "Information Technology",
                    "Cyber Security",
                    "Business and Legal Services"
                ]
```

```
            },
            "parent": null,
            "created_at": "2024-08-27T00:10:55.831642Z",
            "possible_types": [],
            "description": "The suggested asset was discovered on threatq.com
with reverse WHOIS searching method. It is suggested because WHOIS record
matches with the original WHOIS record's email (will.fitch@threatq.com)
value.",
            "asset": "threatq.ninja",
            "properties": {}
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| `results[].asset` | Asset.Name | N/A | `results[].created_at` | `threatq.ninja` | N/A |
| `results[].description` | Asset.Description | N/A | `results[].created_at` | `The suggested asset was discovered on threatq.com...` | N/A |
| `results[].status` | Asset.Attribute | Asset Status | `results[].created_at` | `SUGGESTED` | Updatable |
| `results[].type` | Asset.Attribute | Asset Type | `results[].created_at` | `DOMAIN` | N/A |
| `results[].severity` | Asset.Attribute | Asset Severity | `results[].created_at` | `MEDIUM` | Updatable |
| `results[].created_by.name/email/role` | Asset.Attribute | Created By | `results[].created_at` | `Automation - automation@brandefense.io - ADMIN` | We concatenate the values into one. |
| `results[].modules.name` | Asset.Attribute | Asset Module Name | `results[].created_at` | `Attack Surface` | N/A |
| `results[].modules.code` | Asset.Attribute | Asset Module Code | `results[].created_at` | `attack-surface` | N/A |
| `results[].modules.short_code` | Asset.Attribute | Asset Module Short Code | `results[].created_at` | `ASM` | N/A |
| `results[].modules.category` | Asset.Attribute | Asset Module Category | `results[].created_at` | `exposure-management` | N/A |
| `results[].organization.name` | Related Organization.Value | N/A | `results[].created_at` | `ThreatQuotient` | N/A |
| `results[].organization.short_code` | Related Organization.Attribute | Organization Short Code | `results[].created_at` | `THRTQ` | N/A |
| `results[].organization.code` | Related Organization.Attribute | Organization Code | `results[].created_at` | `threatquotient` | N/A |
| `results[].organization.license_type` | Related Organization.Attribute | Organization License Type | `results[].created_at` | `PROOF_OF_CONCEPT` | N/A |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| `results[].organization.country` | Related Organization.Attribute | Organization Country | `results[].created_at` | `US` | N/A |
| `results[].organization.industries` | Related Organization.Attribute | Organization Industry | `results[].created_at` | `Technology` | 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.

## Brandefense Incidents

| METRIC | RESULT |
|---|---|
| **Run Time** | 20 minutes |
| **Indicators** | 245 |
| **Indicator Attributes** | 320 |
| **Organizations** | 55 |
| **Organization Attributes** | 103 |
| **Assets** | 74 |
| **Asset Attributes** | 120 |
| **Incidents** | 7,890 |
| **Incident Attributes** | 9,466 |

## Brandefense Indicators of Compromise

| METRIC | RESULT |
|---|---|
| **Run Time** | 10 minutes |
| **Indicators** | 6,168 |
| **Indicator Attributes** | 26,299 |

## Brandefense CTI Rules

| METRIC | RESULT |
|---|---|
| **Run Time** | 3 minutes |
| **Indicators** | 90 |
| **Indicator Attributes** | 180 |

## Brandefense Assets

| METRIC | RESULT |
|---|---|
| **Run Time** | 3 minutes |
| **Assets** | 90 |
| **Assets Attributes** | 180 |
| **Organizations** | 90 |
| **Organization Attributes** | 180 |

# Change Log

- **Version 1.0.0**
  - Initial release