ThreatQuotient

IBM X-Force Premium Threat Intelligence CDF Guide

Version 1.0.0

April 11, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support

Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

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

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ⚠ ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 4.45.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/ibm-x-force-premium-threat-intelligence-cdf

Introduction

The IBM X-Force Premium Threat Intelligence for ThreatQ enables analysts to automatically ingest reports collected by IBM Security X-Force since the 1990s.

The integration provides the following feeds:

- **IBM X-Force Premium Threat Intelligence Industries** - retrieves all the available industry-based analysis reports.
- **IBM X-Force Premium Threat Intelligence Malware Analysis** - retrieves all the available malware analysis reports.
- **IBM X-Force Premium Threat Intelligence Threat Activities** - retrieves new and existing threat activity reports.
- **IBM X-Force Premium Threat Intelligence Threat Groups** - retrieves reports about cyber threat groups tracked within IBM.

The integration ingests the following system objects:

- Reports
    - Report Attributes

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.

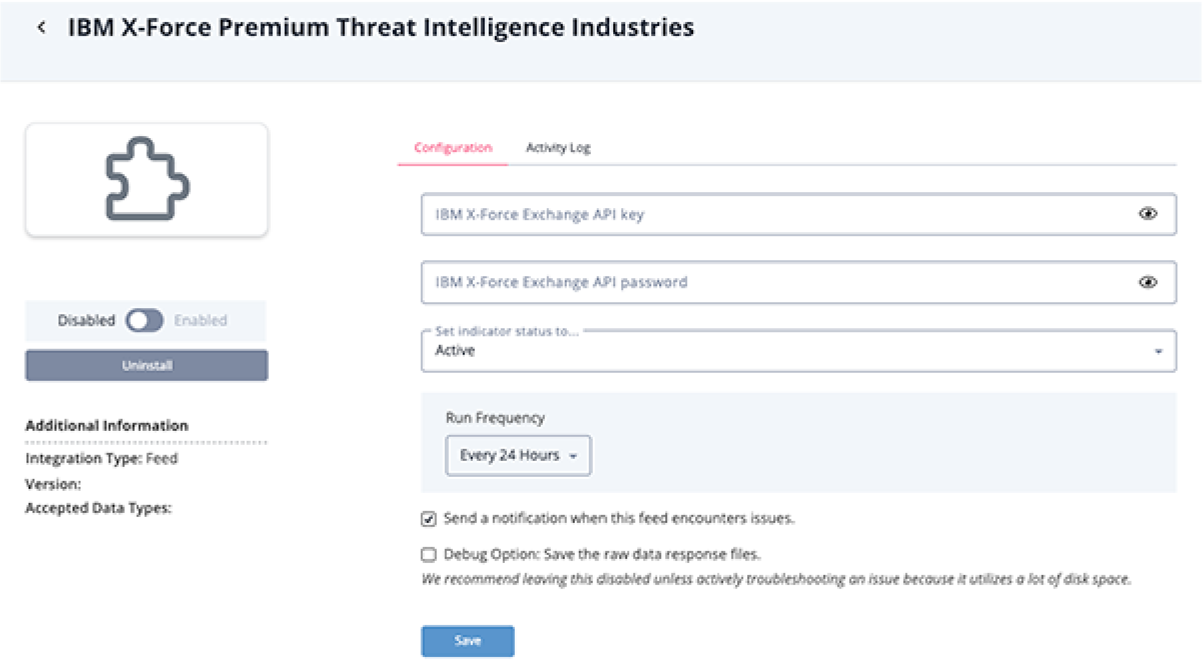
To configure the integration:

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
IBM X-Force Exchange API Key	Your IBM X-Force Exchange API Key.
IBM X-Force Exchange API Password	Your IBM X-Force Exchange API password.



IBM X-Force Premium Threat Intelligence Industries

Configuration | Activity Log

IBM X-Force Exchange API key

IBM X-Force Exchange API password

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.

Additional Information

Integration Type: Feed

Version:

Accepted Data Types:

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

IBM X-Force Premium Threat Intelligence Industries

This Industries feed ingests all industry-based analysis reports collected by IBM Security X-Force.

```
GET https://api.xforce.ibmcloud.com/api/industries?limit=1&skip=0
```

Sample Response:

```
{
    "rows": [
        {
            "id": "guid:cda08d2b0b07a2818aeec9d321d2d87d",
            "reportId": "report--151fa1d9-e561-4297-9a05-8c741a4bfd8a",
            "created": "2022-05-11T00:18:28Z",
            "name": "Utilities Industry Profile",
            "modified": "2023-04-02T23:30:21Z",
            "published": "2022-05-11T00:18:28Z",
            "shortDescription": "The utilities industry—responsible for providing electricity, water, sewer, and
other utilities—occupies an essential element in a modern society critical to its day-to-day operation and survival.
Active campaigns against the industry have the potential to [cripple an entire nation](https://www.bloomberg.com/
news/features/2022-01-26/what-happens-when-russian-hackers-cyberattack-the-u-s-electric-power-grid#xj4y7vzkg).
\n\nIncreasing global competition in the industry fostered by deregulation has helped the industry achieve lower
costs and increased efficiency through technology upgrades. These innovations, while beneficial, can potentially
increase risk as more cyber threat groups actively seek to exploit the utilities industry. Malicious actors such as
nation-state actors and organized cybercriminals are [increasing their focus](https://www.utilitydive.com/news/
sophisticated-hackers-could-crash-the-us-power-grid-but-money-not-sabotag/603764/) on the utilities industry to not
only exploit but also disrupt networks, setting a worrying trend about the future security of the industry. \n\nDue
to the uniqueness of the utilities sector’s role in society, a single incident of data loss could have ripple effects
beyond monetary loss, impacting the greater national critical infrastructure framework. Adversaries could also use
stolen data, such as credentials, to either gain an initial foothold or to move laterally in a network and cause
eventual disruption to utilities operations. The [2023 X-Force Threat Intelligence Index](https://www.ibm.com/
reports/threat-intelligence) found that energy was the fourth-most attacked industry, receiving 10.7% of all attacks
on the top ten industries, up from 8.2% the year prior. In addition, the [2022 IBM-sponsored Ponemon Cost of a Data
Breach Study](https://www.ibm.com/reports/data-breach) found that the energy sector, a parent to the utilities
industry sector, has the fifth-highest total cost of a data breach at $4.72 million per incident, on average.\n\nIBM
X-Force assesses that the utilities industry may face considerable threats from a variety of adversaries and
recommends that the industry take heightened precautions to mitigate against future risks.",
            "locked": true,
            "statement": "premium"
        }
    ],
    "previousPage": "",
    "nextPage": "/industry?limit=1&skip=1"
}
```

> Endpoint called only to fetch all the .rows[].id that will be further used in the IBM X-Force Premium Threat Intelligence Details supplemental feed.

IBM X-Force Premium Threat Intelligence Malware Analysis

The Malware Analysis feed ingests all the malware analysis reports collected by IBM Security X-Force.

```
GET https://api.xforce.ibmcloud.com/api/malware_analysis?limit=1&skip=0
```

Sample Response:

```
{
    "rows": [
        {
            "id": "guid:5e71d1a65fe92a0b78104079c5b63eb2",
            "reportId": "report--907d8ca1-bc9b-435f-8966-204d45168e74",
            "created": "2023-03-22T19:52:12Z",
            "name": "Black Basta Malware Profile",
            "modified": "2023-03-29T16:51:01Z",
            "published": "2023-03-22T19:52:12Z",
            "shortDescription": "Black Basta is a ransomware family that has been used since April 2022. The
ransomware family is compiled as C++ executables for Windows and Linux operating systems. The known Linux variants
target VMWare ESXi systems.\n\nCurrently there are two versions of Black Basta in the wild. Each version has a
variant that targets Windows and Linux operating systems. These versions are referred to as Black Basta *version 1
(V1)* and Black Basta *version 2 (V2)* in this report.\n\nBlack Basta V1 typically accepts one command line argument,
`\"-forcedpath\"`, that instructs the ransomwareto encrypt the specified path, while Black Basta V2 contains
significant updates such as the number of command line arguments accepted and the encryption scheme.\n\nBased on the
samples analyzed, Black Basta V2 accepts multiple command line arguments, however, despite the presence of the
commands, not all of them have been implemented. Depending on the variant, Black Basta V2 may have the following
functionality implemented:\n\n*   Encrypt systems connected to the compromised system\n*   Encrypt a specific file
path or file\n*   Specify the number of threads used during execution\n*   Skip creating a mutex\n\nOther Black Basta
V2 updates include:\n\n*   Changes in the encryption scheme that utilize Elliptic Curve Cryptography (ECC) and
XChaCha20 from the CryptoPP library (<https://cryptopp.com/>).\n*   Black Basta V1 uses ChaCha20 and RSA from the GNU
Multiple Precision Arithmetic Library(GMP) library.\n\nBlack Basta V1 appends the file extension **.basta** to the
end of files while Black Basta V2 has been observed appending varying file extensions, reportedly varying per
victim.",
            "locked": true,
            "statement": "premium"
        }
    ],
    "previousPage": "",
    "nextPage": "/malware?limit=1&skip=1"
}
```

> Endpoint called only to fetch all the .rows[].id that will be further used in the IBM X-Force Premium Threat Intelligence Details supplemental feed.

IBM X-Force Premium Threat Intelligence Threat Activities

The Threat Activities feed ingests all the threat activity reports collected by IBM Security X-Force.

```
GET https://api.xforce.ibmcloud.com/api/threat_activities?limit=1&skip=0
```

Sample Response:

```
{
    "rows": [
        {
            "id": "guid:a5c1d6aeb5f5cb144b13d3d2c4af50c5",
            "reportId": "report--90702a16-5bb1-4913-8bf1-60ec417f882b",
            "created": "2023-03-30T10:07:31Z",
            "name": "3CXDesktopApp Becomes Trojanized in Multi-Stage Attack",
            "modified": "2023-03-31T22:14:49Z",
            "published": "2023-03-30T10:07:31Z",
            "shortDescription": "SentinelOne detected suspicious behavior from 3CXDesktopApp, a video conferencing
software product, on March 22nd. The app had become trojanized as the first stage in a multi-stage attack, with
research ongoing on how the installer became malicious.",
            "locked": true,
            "statement": "premium"
        }
    ],
    "previousPage": "",
    "nextPage": "/threat_activities?limit=1&skip=1"
}
```

> Endpoint called only to fetch all the .rows[].id that will be further used in the IBM X-Force Premium Threat Intelligence Details supplemental feed.

IBM X-Force Premium Threat Intelligence Threat Groups

The Threat Groups feed ingests all the reports about cyber threat groups collected by IBM Security X-Force.

```
GET https://api.xforce.ibmcloud.com/api/threat_groups?limit=1&skip=0
```

Sample Response:

```
{
    "rows": [
        {
            "id": "guid:28d5c141467b2a2f92d18aca0ad76024",
            "reportId": "report--213ce5bb-287f-48b2-9620-d5d6ff56a75c",
            "created": "2020-08-22T03:06:38Z",
            "name": "ITG05 Threat Group Profile",
            "modified": "2023-02-01T17:01:25Z",
            "published": "2020-08-22T03:06:38Z",
            "shortDescription": "IBM tracks ITG05 as a likely Russian state-sponsored umbrella group, which
encompasses potentially multiple actors and unique activities. ITG05 has a strong overlap with the industry-
identified threat actor groups APT28, Fancy Bear, and STRONTIUM.",
            "locked": true,
            "statement": "premium"
        }
    ],
    "previousPage": "",
    "nextPage": "/threatgroup?limit=1&skip=1"
}
```

> Endpoint called only to fetch all the .rows[].id that will be further used in the IBM X-Force Premium Threat Intelligence Details supplemental feed.

IBM X-Force Premium Threat Intelligence Details (Supplemental)

The Supplemental feed called once per each .rows[].id returned by the feeds:

- IBM X-Force Premium Threat Intelligence Industries
- IBM X-Force Premium Threat Intelligence Malware Analysis
- IBM X-Force Premium Threat Intelligence Threat Activities
- IBM X-Force Premium Threat Intelligence Threat Groups

```
https://api.xforce.ibmcloud.com/api/{path}/{id}
```

Sample Response:

```
{
    "type": "bundle",
    "id": "bundle--b7736d42-bcd6-432c-9b0b-c7e73c9d7569",
    "spec_version": "2.0",
    "objects": [
        {
            "type": "report",
            "labels": [
                "industry"
            ],
            "name": "Information Technology Industry Profile",
            "published": "2022-01-31T19:40:24.000Z",
            "x_com_ibm_short_description": "The information technology industry is a sub-industry of the professional
services industry, which is the fifth-most attacked industry according to the 2021 IBM X-Force Threat Intelligence
Index.[\\[1\\]](#cite-summary-1-1) Information technology most likely is attractive to cyber adversaries because of
the force multiplier it can become in an attack, as access to one technology company potentially can provide
additional access to multiple downstream targets, including by infecting patch updates. In addition, some attackers
may focus on the information technology industry for the notoriety of gaining access to a technical firms’ networks,
or to exploit newly implemented software and technologies that adversaries perceive are more prone to undiscovered
vulnerabilities. X-Force assesses that the information technology industry is likely to be in the top ten attacked
industries for at least the next three years.\n\nThe IBM-sponsored Ponemon Cost of a Data Breach Study for 2021 found
that the technology industry had the fourth-highest cost per record for a data breach, at $4.88 million, on average.
[\\[2\\]](#cite-summary-2-1) By comparison, the average total cost of a data breach is $4.24 million.[\\[3\\]](#cite-
summary-3-1)",
            "id": "report--cfcc808e-a2c1-4c62-996f-51c125e4f1a2",
            "created": "2022-01-31T19:40:24.000Z",
            "modified": "2022-01-31T19:40:24.000Z",
            "x_com_ibm_tags": [
                {
                    "type": "tag",
                    "tag": "x-industry:profserv-it",
                    "entityType": "report",
                    "entityId": "industry-guid:4af7d01d1177c34fdfa70361b3a088de",
                    "commentId": "",
                    "user": "IRIS",
                    "date": "2022-12-01T11:12:03.919Z",
                    "displayName": "IBM X-Force"
                },
                {
                    "type": "tag",
                    "tag": "x-industry:profserv",
                    "entityType": "report",
                    "entityId": "industry-guid:4af7d01d1177c34fdfa70361b3a088de",
                    "commentId": "",
                    "user": "IRIS",
                    "date": "2022-12-01T11:12:03.919Z",
                    "displayName": "IBM X-Force"
                }
            ],
            "object_refs": [
                "marking-definition--51c4945c-0ced-4429-81a2-d8ced934190a"
            ]
        }
    ]
}
```

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[].name	Report.Value	N/A	.objects[].created	'Information Technology Industry Profile'	N/A
.objects[].x_com_ibm_short_description	Report.Description	N/A	N/A	'The information technology industry...'	N/A
.objects[].x_com_ibm_tags[].tag	Report.Tag	N/A	N/A	'x-industry:profserv-it,x-industry:profserv'	N/A
.objects[].labels	Report.Attribute	Report Label	.objects[].created	['industry']	N/A
.spec_version	Report.Attribute	Report Specification Version	.objects[].created	'2.0'	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.

Industries

METRIC	RESULT
Run Time	1 minute
Reports	24
Report Attributes	48

Malware Analysis

METRIC	RESULT
Run Time	6 minutes
Reports	558
Report Attributes	1,116

Threat Activities

METRIC	RESULT
Run Time	10 minutes
Reports	877
Report Attributes	1,754

Threat Groups

METRIC	RESULT
Run Time	1 minute
Reports	74
Report Attributes	148

Change Log

- **Version 1.0.0**
    - Initial release