ThreatQuotient

IBM X-Force Exchange Feeds Guide

Version 1.1.0

January 07, 2021

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

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

Warning and Disclaimer

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

Contents

Versioning

- Current integration version: `1.1.0`
- Supported on ThreatQ versions >= `4.31.0`

Introduction

The IBM X-Force Exchange integration ingests threat intelligence data from the following feeds:

FEED	DESCRIPTION
IBM X-Force Exchange - Anonymization Services - IPv4	`GET https://api.xforce.ibmcloud.com/xfti/anonsvcs/ipv4` Returns a list of IPv4 addresses that are categorized as anonymization services.
IBM X-Force Exchange - Anonymization Services - IPv6	`GET https://api.xforce.ibmcloud.com/xfti/anonsvcs/ipv6` Returns a list of IPv6 addresses that are categorized as anonymization services.
IBM X-Force Exchange - Anonymization Services - URL	`GET https://api.xforce.ibmcloud.com/xfti/anonsvcs/url` Returns a list of URLs that are categorized as anonymization service.
IBM X-Force Exchange - Botnet CnC Servers - IPv4	`GET https://api.xforce.ibmcloud.com/xfti/c2server/ipv4` Returns a list of IPv4 addresses that are categorized as botnet command and control servers.
IBM X-Force Exchange - Botnet CnC Servers - IPv6	`GET https://api.xforce.ibmcloud.com/xfti/c2server/ipv6` Returns a list of IPv6 addresses that are categorized as botnet command and control servers.
IBM X-Force Exchange - Botnet CnC Servers - URL	`GET https://api.xforce.ibmcloud.com/xfti/c2server/url` Returns a list of URLs that are categorized as botnet command and control servers.
IBM X-Force Exchange - Bots - IPv4	`GET https://api.xforce.ibmcloud.com/xfti/bots/ipv4` Returns a list of IPv4 addresses that are categorized as bots.
IBM X-Force Exchange - Bots - IPv6	`GET https://api.xforce.ibmcloud.com/xfti/bots/ipv6` Returns a list of IPv6 addresses that are categorized as bots.
IBM X-Force Exchange - Cryptocurrency mining - IPv4	`GET https://api.xforce.ibmcloud.com/xfti/cryptomining/ipv4` Returns a list of IPv4 addresses that are categorized as Cryptocurrency mining.
IBM X-Force Exchange - Cryptocurrency mining - IPv6	`GET https://api.xforce.ibmcloud.com/xfti/cryptomining/ipv6` Returns a list of IPv6 addresses that are categorized as Cryptocurrency mining.
IBM X-Force Exchange - Cryptocurrency mining - URL	`GET https://api.xforce.ibmcloud.com/xfti/cryptomining/url` Returns a list of URLs that are categorized as Cryptocurrency mining.
IBM X-Force Exchange - Early Warning - URL	`GET https://api.xforce.ibmcloud.com/xfti/ew/url` Returns a list of URLs that are categorized as early warning.
IBM X-Force Exchange - Malware - IPv4	`GET https://api.xforce.ibmcloud.com/xfti/mw/ipv4` Returns a list of IPv4 addresses that are categorized as malware.
IBM X-Force Exchange - Malware - IPv6	`GET https://api.xforce.ibmcloud.com/xfti/mw/ipv6` Returns a list of IPv6 addresses that are categorized as malware.
IBM X-Force Exchange - Malware - URL	`GET https://api.xforce.ibmcloud.com/xfti/mw/url` Returns a list of URLs that are categorized as malware.
IBM X-Force Exchange - Phishing - URL	`GET https://api.xforce.ibmcloud.com/xfti/phishing/url` Returns a list of URLs that are categorized as phishing.
IBM X-Force Exchange - Scanning IPs - IPv4	`GET https://api.xforce.ibmcloud.com/xfti/scanning/ipv4` Returns a list of IPv4 addresses that are categorized as scanning IPs.
IBM X-Force Exchange - Scanning IPs - IPv6	`GET https://api.xforce.ibmcloud.com/xfti/scanning/ipv6` Returns a list of IPv6 addresses that are categorized as scanning IPs.
IBM X-Force Exchange - Top Activity - URL / 10K	`GET https://api.xforce.ibmcloud.com/xfti/topact/url/10k` Returns the top ten thousand URLs rated by activity as known by X-Force Exchange.

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 to open its details page.
4. Enter the following parameters under the **Configuration** tab:

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

5. Review the **Settings** configuration, 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

All feeds except **IBM X-Force Exchange - Top Activity - URL / 10K** use the same mapping table. **IBM X-Force Exchange - Top Activity - URL / 10K** has a different Feed Data Path for accessing Indicator Values, has a static Indicator Type of URL and Default Indicator Status of Review, and ingests the "Feed Category" Attribute.

All Feeds (Except Top Activity - URL / 10K)

JSON response sample (specifically from "IBM X-Force Exchange - Anonymization Services - IPv4"):


```
{
  "FeedCategory": "Anonymization Services",
  "FeedType": "IPv4",
  "Version": "0000043381",
  "CreationDate": "2020-02-20T08:05:30.597Z",
  "IndicatorCount": "3",
  "PartNo": "D01VKZX",
  "Copyright": "(C) Copyright IBM Corp. 2019, 2020. All Rights Reserved.",
  "data": [
        "109.75.183.124",
        "109.74.194.75",
        "107.148.6.184"
  ]
}
```


ThreatQ provides the following default mapping for these feeds:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
.data[]	Indicator.Value	See .FeedType	.CreationDate	109.74.194.75
.FeedType	Indicator.Type	See Indicator Type Mapping table below	N/A	"IPv4" / "IPv6" / "URL"

Indicator Type Mapping

IBM X-FORCE EXCHANGE INDICATOR TYPE	THREATQ INDICATOR TYPE	NOTES
IPv4	IP Address	N/A
IPv6	IPv6 Address	N/A
URL	URL or FQDN	By default, URL Indicators that are actually FQDNs will be ingested as FQDN Indicators via normalization.

IBM X-Force Exchange - Top Activity - URL / 10K

Returns the top ten thousand URLs rated by activity as known by X-Force Exchange. The URLs provided by this feed are not guaranteed to be malicious or non-malicious. As a result, the default indicator status for the URL or FQDN Indicators ingested by this feed is Review.

```
GET https://api.xforce.ibmcloud.com/xfti/topact/url/10k
```

JSON response sample:


```
{
  "FeedCategory": "Top-Volume Domains",
  "FeedType": "URL",
  "Version": "0000000372",
  "CreationDate": "2020-12-16T00:23:01.497Z",
  "IndicatorCount": "10000",
  "PartNo": "D01VKZX",
  "Copyright": "(C) Copyright IBM Corp. 2019, 2020. All Rights Reserved.",
  "data": [
    {
      "url": "google.com",
      "categories": [
        "Search Engines / Web Catalogues / Portals"
      ]
    },
    {
      "url": "netflix.com",
      "categories": [
        "Cinema / Television"
      ]
    },
    {
      "url": "microsoft.com",
      "categories": [
        "Software / Hardware",
        "General Business"
      ]
    }
  ]
}
```


ThreatQ provides the following default mapping for the feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].url	Indicator.Value	URL or FQDN	.CreationDate	google.com	By default, URL Indicators that are actually FQDNs will be ingested as FQDN Indicators via normalization.
.data[].categories[]	Indicator.Attribute	Feed Category	.CreationDate	"Search Engines / Web Catalogues / Portals"	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.

IBM X-Force Exchange - Anonymization Services - IPv4

METRIC	RESULT
Run Time	11 minutes
Indicators	22,301

IBM X-Force Exchange - Anonymization Services - IPv6

METRIC	RESULT
Run Time	< 1 minute
Indicators	604

IBM X-Force Exchange - Anonymization Services - URL

METRIC	RESULT
Run Time	67 minutes
Indicators	149,568
Indicator Attributes	18,659 (derived from URLs)

IBM X-Force Exchange - Botnet CnC Servers - IPv4

METRIC	RESULT
Run Time	2 minutes
Indicators	3,266

IBM X-Force Exchange - Botnet CnC Servers - IPv6

METRIC	RESULT
Run Time	< 1 minute
Indicators	10

IBM X-Force Exchange - Botnet CnC Servers - URL

METRIC	RESULT
Run Time	103 minutes
Indicators	240,129
Indicator Attributes	59 (derived from URLs)

IBM X-Force Exchange - Bots - IPv4

METRIC	RESULT
Run Time	25 minutes
Indicators	62,706

IBM X-Force Exchange - Bots - IPv6

METRIC	RESULT
Run Time	< 1 minute
Indicators	39

IBM X-Force Exchange - Cryptocurrency mining - IPv4

METRIC	RESULT
Run Time	< 1 minute
Indicators	373

IBM X-Force Exchange - Cryptocurrency mining - IPv6

METRIC	RESULT
Run Time	< 1 minute
Indicators	18

IBM X-Force Exchange - Cryptocurrency mining - URL

METRIC	RESULT
Run Time	< 1 minute
Indicators	844
Indicator Attributes	82 (derived from URLs)

IBM X-Force Exchange - Early Warning - URL

METRIC	RESULT
Run Time	> 8 hours
Indicators	807,652
Indicator Attributes	1,687 (derived from URLs)

IBM X-Force Exchange - Malware - IPv4

METRIC	RESULT
Run Time	< 1 minute
Indicators	812

IBM X-Force Exchange - Malware - IPv6

METRIC	RESULT
Run Time	< 1 minute
Indicators	7

IBM X-Force Exchange - Malware - URL

METRIC	RESULT
Run Time	33 minutes
Indicators	43,409
Indicator Attributes	35,129 (derived from URLs)

IBM X-Force Exchange - Phishing - URL

METRIC	RESULT
Run Time	28 minutes
Indicators	38,105
Indicator Attributes	18,599 (derived from URLs)

IBM X-Force Exchange - Scanning IPs - IPv4

METRIC	RESULT
Run Time	106 minutes
Indicators	235,413

IBM X-Force Exchange - Scanning IPs - IPv6

METRIC	RESULT
Run Time	< 1 minute
Indicators	0

- At the time these feed run metrics were gathered, this feed returned only a single IPv6 address: `2001:db8:1234::3`. Reserved IPv6 addresses are not ingested by ThreatQ, and any addresses matching the CIDR Block `2001:db8::/32` are reserved per RFC 3949.

IBM X-Force Exchange - Top Activity - URL / 10K

METRIC	RESULT
Run Time	6 minutes
Indicators	9,596
Indicator Attributes	9,662

Known Issues/Limitations

- Streaming errors that occur between the X-Force Exchange server and ThreatQ, after the HTTP status code 200 was received by ThreatQ, will cause the stream to end. This will cause the following feed run error as seen in the ThreatQ UI: `Error fetching data from provider: 524, message='None'`. This corresponds to a 524 Timeout Occurred error. The user can disable and re-enable the feed in order to kick off another scheduled run to try again. This error may occur several times in a row.
  - This error is also documented in the IBM X-Force Exchange documentation.
- Due to the amount of data provided by the feed **IBM X-Force Exchange - Early Warning - URL**, users may experience ThreatQ system performance issues, such as failed batches due to timeout errors. There is not much one can do to completely mitigate this, but some suggestions are:
  - Make sure **IBM X-Force Exchange - Early Warning - URL** is the only feed enabled when one wants to run it.
  - Do not leave **IBM X-Force Exchange - Early Warning - URL** enabled for consecutive daily runs. Periodically re-enable it to ingest the latest data. Each run will attempt to consume over 800k URL Indicators.

Change Log

- **Version 1.1.0**
  - Removed ingesting the following attributes from all IBM X-Force Exchange feeds:
    - Feed Type
    - Copyright
    - Version
    - Part Number
  - Removed the Feed Category attribute from all feeds (except for IBM X-Force Exchange - Top Activity - URL / 10k).
  - Improved efficiency of IBM X-Force Exchange - Top Activity - URL / 10K.
  - By default, all Indicators ingested via IBM X-Force Exchange - Top Activity - URL / 10K will have the Review Indicator Status since the URLs provided by this feed are not guaranteed to be malicious or non-malicious.
- **Version 1.0.0**
  - Initial release