ThreatQuotient

IBM X-Force Exchange (Feed) Implementation Guide

Version 1.0.0

Wednesday, March 18, 2020

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.

Last Updated: Wednesday, March 18, 2020

Contents

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions >= `4.31.0`

Introduction

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

- Anonymization Services - IPv4
- Anonymization Services - IPv6
- Anonymization Services - URL
- Botnet CnC Servers - IPv4
- Botnet CnC Servers - IPv6
- Botnet CnC Servers - URL
- Bots - IPv4
- Bots - IPv6
- Cryptocurrency mining - IPv4
- Cryptocurrency mining - IPv6
- Cryptocurrency mining - URL
- Early Warning - URL
- Malware - IPv4
- Malware - IPv6
- Malware - URL
- Phishing - URL
- Scanning IPs - IPv4
- Scanning IPs - IPv6
- Top Activity - URL / 10K

An API key and API password are used for HTTP basic authentication.

Installation

Perform the following steps to install the feeds:

The same steps can be used to upgrade the feed to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the **IBM X-Force Exchange** feeds file.
3. Navigate to your ThreatQ instance.
4. Click on the **Settings** icon and select **Incoming feeds**.
5. Click on the **Add New Feed** button.
6. Upload the feeds file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the feed 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.

   The feed will be added to the **Commercial** tab for Incoming Feeds. 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 feed-related credentials.

To configure the feed:

1. Click on the **Settings** icon and select **Incoming Feeds**.
2. Locate the feeds under the **Commercial** tab.
3. Click on the **Feed Settings** link for each feed.
4. Under the **Connection** tab, enter the following configuration parameters:

Parameter	Description
API Key	IBM X-Force Exchange account API key.
API Password	IBM X-Force Exchange account API password.

5. Click on **Save Changes**.
6. Click on the toggle switch to the left of each feed name to enable the feeds.

ThreatQ Mapping

All the feeds use the same mapping table - the only difference is the type of indicator ingested.

Endpoint Example:


```
{
  "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"
  ]
}
```

All the feeds use the same mapping table - the only difference is the type of indicator ingested.

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples
.data	indicator.value	Indicator Value	["109.75.183.124", "109.74.194.75"]
.FeedType	indicator.type	Indicator Type	"IPv4" / "IPv6" / "URL"
.CreationDate	indicator.published_at	Indicator Published At	"2020-02-20T08:05:30.597Z"
.FeedCategory	indicator.attribute	Feed Category	"Anonymization Services"
.Version	indicator.attribute	Version	"0000043381"
.PartNo	indicator.attribute	Part Number	"D01VKZX"
.Copyright	indicator.attribute	Copyright	"(C) Copyright IBM Corp...."

Notes

- The .FeedType JSON key is mapped to TQ indicator types "IP Address", "IPv6 Address" and "URL".
- The .CreationDate is formatted as a timestamp and is assigned to each attribute
- The .data array could contain IPv4, IPv6 or URL values.