ThreatQuotient

Talos Intelligence Feed Guide

Version 1.0.0

Friday, June 26, 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: Friday, June 26, 2020

Contents

Versioning

- Current Integration Version: `1.0.0`
- Supported on ThreatQ Version: >= `4.38.0`

Introduction

The Talos Intelligence feed ingests a list of known malicious network threats such as Tor exit nodes.

The Talos Intelligence feed ingests threat intelligence data from the following endpoint:

- https://talosintelligence.com/documents/ip-blacklist

Installation

Perform the following steps to install the connector:

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

1. Log into https://marketplace.threatq.com/.
2. Locate and download the **Talos Intelligence** integration 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 feed 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 **OSINT** 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 feed under the **OSINT** tab.
3. Click on the **Feed Settings** link for the feed.
4. Review the settings under the **Settings** tab.
5. Click on **Save Changes** if any fields in the previous step were updated.
6. Click on the toggle switch to the left of the feed name to enable the feed.

ThreatQ Mapping

Response sample:

```
91.236.4.234
151.80.194.85
81.90.175.7
82.160.64.45
```

ThreatQ provides the following default mapping for the feed:

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples
First Token	Indicator.Value	IP Address	61.234.32.119

Average Feed Run

Average Feed Run results for Talos Intelligence:

Metric	Result
Run Time	1 min
Indicators	920

Feed runtime is 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.

Change Log

- **Version 1.0.0**
  - Initial release