

ThreatQuotient



Talos Intelligence CDF Guide

Version 1.1.0

June 29, 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.

Copyright © 2021 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Contents

Versioning..... 4

Introduction..... 5

Installation 6

Configuration..... 7

ThreatQ Mapping..... 8

Average Feed Run 9

Change Log..... 10

Versioning

- Current integration version: 1.1.0
- Supported on ThreatQ versions \geq 4.38.0

Introduction

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

- <https://snort.org/downloads/ip-block-list>

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 **OSINT** 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. Review the feed settings, make any changes if needed, and click on **Save**.
5. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

<https://snort.org/downloads/ip-block-list>

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



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.

METRIC	RESULT
Run Time	1 min
Indicators	920

Change Log

- **Version 1.1.0**
 - Updated feed url.
- **Version 1.0.0**
 - Initial Release