ThreatQuotient

CI Army IPs CDF Guide

Version 1.0.0

February 07, 2022

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

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.

Versioning

- Current integration version: `1.0.0`
- Compatible with ThreatQ versions >= `4.10.0`

Introduction

The CI Army List IPs CDF for ThreatQ retrieves a list of the top 15,000 malicious IP addresses.

The integration provides the following endpoint:

- **CI Army List IPs** - retrieves a list of malicious IP addresses and ingests them as indicators into ThreatQ.

The integration ingests IP Address type indicatgors into the ThreatQ platform.

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

The CI Army List IPs feed retrieves a list of malicious IP addresses and ingests them as indicators into ThreatQ.

```
GET http://www.ciarmy.com/list/ci-badguys.txt
```

Sample Response:

```
1.116.107.130
1.116.123.100
1.116.140.153
1.116.152.38
1.116.157.87
1.116.161.241
1.116.16.205
1.116.175.214
1.116.176.122
1.116.179.58
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
1 (first token)	Indicator.Value	IP Address	223.95.205.217	N/A

Average Feed Run

METRIC	RESULT
Run Time	3 min
Indicators	15,000

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.

Change Log

- **Version 1.0.0**
  - Initial release