ThreatQuotient

www.dan.me.uk TOD Node List CDF Guide

Version 2.0.2

January 17, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

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.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	2.0.2
Compatible with ThreatQ Versions	>= 4.20.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/www-dan-me-uk-tor-node-list-cdf/

Introduction

The www.dan.me.uk Tor Node List CDF for ThreatQ provides a full Tor node list (not more than one hour old) in script-readable format.

The integration provides the following feed:

- **www.dan.me.uk Tor Node List** - ingests indicators in a pipe-delimited format.

The integration ingests indicators and indicator attributes.

Important Notes:

- Nodes flagged `E` are those which allow exit from the Tor network.
- Nodes flagged `X` are those which allow exit from the Tor network, but do not publicly advertise that they do so.

> ⚠ The feed source (https://www.dan.me.uk/tornodes) can only be accessed once every 30 minutes. If accessed too often, your IP will be blocked.

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

PARAMETER	DESCRIPTION
Only Ingest Exit Nodes	If checked, the integration will only ingest nodes which allow exit from the Tor network. This parameter is unchecked by default, which results in ingesting all nodes.
Feed URL	This parameter is for UI display purposes only.
Context Filter	Select the pieces of context to ingest into the ThreatQ platform. Options include: ◦ TOR Name ◦ Router Port ◦ Directory Port ◦ Flags ◦ Version ◦ Uptime ◦ Contact Info

5. Review any additional settings, 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

www.dan.me.uk Tor Node List

The feed ingests data using the following pipe-delimited format:

```
<ip>|<name>|<router-port>|<directory-port>|<flags>|<uptime>|<version>|<contactinfo>
```

Sample Response:

```
101.100.136.62|warduckcomingatya|9001|9030|RSDV|6699668|Tor 0.4.1.6|0xFFFFFFFF Warduck <warduck@gmail.com>
103.234.220.195|ASock|443|80|EFHRSDV|1918882|Tor 0.4.1.6|dobby_potter at aol.com or send hedwig
2605:6400:0030:f8f0:b055:151e:5dcf:7ae4|ULayerManning|443|80|FGRSDV|62|Tor 0.4.1.6|noc [AT] ulayer.net
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
ip	indicator.type	IP Address/IPv6 Address	N/A	N/A
ip	indicator.value	N/A	101.100.136.62	N/A
name	indicator.attribute	TOR Name	warduckcomingatya	N/A
router-port	indicator.attribute	Router Port	9001	N/A
directory-port	indicator.attribute	Directory Port	9030	N/A
flags	indicator.attribute	Flags	RSDV	If the configuration parameter `Only Ingest Exist Nodes` is checked and `flags` contains neither `E` nor `X`, the indicator is not ingested.
version	indicator.attribute	Version	Tor 0.4.1.6	N/A
contactinfo	indicator.attribute	Contact	0xFFFFFFFF Warduck <warduck@gmail.com>	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.

www.dan.me.uk Tor Node List

METRIC	RESULT
Run Time	12 min
Indicators	8,660
Indicator Attributes	60,238

Known Issues / Limitations

- The feed source (https://www.dan.me.uk/tornodes) can only be accessed once every 30 minutes. If accessed too often, your IP will be blocked.
- ThreatQ 4x instances only - the `uptime` attribute is not updated and duplicated instead. You can use the Context Filter configuration parameter to disable the ingestion of this attribute.

Change Log

- **Version 2.0.2**
  - Resolved an issue where the integration did not respect the **Context Filter** selections set on the configuration page.
- **Version 2.0.1**
  - Added a new configuration parameter, **Context Filter**, which allows you to configure what pieces of information are ingested into the ThreatQ platform.
- **Version 2.0.0**
  - Initial release