ThreatQuotient

Disconnect.me CDF User Guide

Version 1.0.0

December 19, 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	1.0.0
Compatible with ThreatQ Versions	>= 5.12.0
Support Tier	ThreatQ Supported

Introduction

The Disconnect.me CDF for ThreatQ enables the automatic ingestion of domains related to tracking services, into ThreatQ. This allows you to automatically create indicators for these domains as well as review and block them.

Disconnect.me is a site that maintains a list of services that track users online. Tracking may be done via ads, finger printers, and cryptominers.

The integration provides the following feed:

- **Disconnect.me Trackers** - ingests domains related to tracking services.

The integration ingests indicators and indicator attributes.

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.

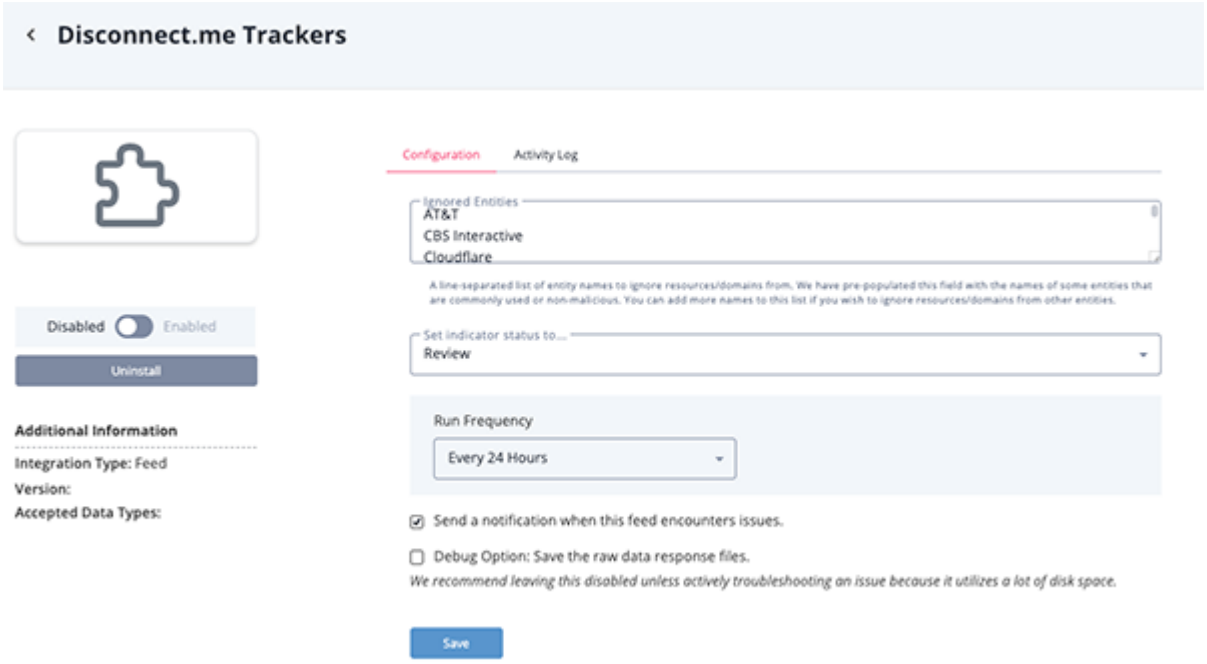
To configure the integration:

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 parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
Ignored Entities	Enter a line-separated list of entity names to ignore resources/domains from. The integration provides pre-populated entities with the names of some entities that are commonly used or non-malicious. You can add more names to this list if you wish to ignore resources/domains from other entities. Pre-populated names provided are: ◦ Amazon.com ◦ AT&T ◦ CBS Interactive ◦ Cloudflare ◦ eBay ◦ Experian ◦ Facebook ◦ Google ◦ HubSpot ◦ HP ◦ Microsoft ◦ Neustar ◦ Opera ◦ Oracle ◦ Pinterest ◦ Salesforce ◦ SAP ◦ SolarWinds ◦ Twitter ◦ Twilio ◦ Vimeo ◦ Walmart ◦ Web.com ◦ Zendesk ◦ ZoomInfo



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

Disconnect.me Trackers

The Disconnect.me Trackers feed ingests domains related to tracker services.

`GET https://raw.githubusercontent.com/disconnectme/disconnect-tracking-protection/master/entities.json`

Sample Response:


```
{
  "license": "Copyright 2010-2023 Disconnect, Inc. / Licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International license (the â€œLicenseâ€). A summary of the License is available here: https://creativecommons.org/licenses/by-nc-sa/4.0/. The text version of the License is here: https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode.txt. Please see the License for the specific language governing permissions and limitations under the License. Unless agreed to in writing or required by law, software distributed under the License on an \"as is\" basis without warranties or conditions of any kind, either express or implied. This license does not apply to any Disconnect logos or marks contained in this repo.",
  "entities": {
    "10Web": {
      "properties": ["10web.io"],
      "resources": ["10web.io"]
    },
    "121Marketing": {
      "properties": ["1-2-1marketing.com"],
      "resources": ["1-2-1marketing.com"]
    },
    "1plusx": {
      "properties": ["1plusx.com"],
      "resources": ["opecloud.com"]
    }
  }
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.[entity].properties[]`, `.[entity].resources[]`	Indicator.Value	FQDN	N/A	`1plusx[.]com`	N/A
`.[entity]`	Indicator.Attribute	Entity	N/A	`Google`	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.

METRIC	RESULT
Run Time	2 minutes
Indicators	3,146
Indicator Attributes	412

Known Issues / Limitations

- While this feed offers domains that are related to tracking services, it does not mean that all domains are malicious and should be blocked. You should always review the domains before blocking them. Services such as `Google` or `Microsoft` track users, but their domains shouldn't be blocked as they are widely used. The integration includes a configuration parameter field, **Ignore Entities**, where you can select which services you'd like to ignore. The field is pre-populated with a list of services that are commonly used or non-malicious. You can add more services to that list if you wish to ignore domains from other services. See the following URL for a complete list of services: https://github.com/disconnectme/disconnect-tracking-protection/blob/master/descriptions.md.

Change Log

- **Version 1.0.0**
  - Initial release