ThreatQuotient

A Securonix Company

IPsum CDF

Version 1.0.0

August 17, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.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.

Copyright © 2026 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.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: tq-support@securonix.com
Support Web: https://ts.securonix.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	>= 5.29.0
Support Tier	ThreatQ Supported

Introduction

The IPsum CDF integration enables ThreatQ to automatically ingest suspicious and malicious IP addresses from the IPsum threat intelligence repository, which aggregates data from more than 30 publicly available sources. The integration periodically imports IP addresses and their associated blacklist occurrence counts into ThreatQ as Indicators and Indicator Attributes, providing analysts with consolidated IP reputation intelligence.

The integration provides the following feed:

- **IPsum** - retrieves IPsum blacklist data from GitHub and ingests it into ThreatQ.

The integration ingests IP Address type indicators and indicator attributes.

Prerequisites

The following is not required but recommended for running the integration:

- GitHub API Token (Recommended) - a GitHub personal access token is recommended to authenticate requests to the GitHub API.

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 yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration yaml file using one of the following methods:
    - Drag and drop the file into the dialog box
    - Select **Click to Browse** to locate the 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 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
GitHub API Token	Enter your GitHub personal access token to authenticate requests to the GitHub API. *(Recommended)*
Minimum Blacklist Count	Enter the minimum number of blacklist occurrences required for an IP address to be ingested into ThreatQ. The specified value is inclusive. *(default: 5)*
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.

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

IPsum

The IPsum feed periodically retrieves blacklist data from the IPsum GitHub repository and ingests the associated IP addresses into ThreatQ as Indicator objects.

```
GET https://github.com/stamparm/ipsum/blob/master/levels/
{{level_value}}.txt
```

The following text data is a sample of the files found in the levels directory of the IPsum GitHub repository. Each level (1-8) corresponds to the number of blacklist occurrences:

```
14.103.165.154
218.92.0.233
218.92.0.236
218.92.0.237
45.148.10.203
46.19.143.66
94.159.104.177
154.213.187.182
183.6.76.2
195.178.110.34
218.92.0.111
218.92.0.114
218.92.0.198
218.92.0.216
218.92.0.217
218.92.0.218
218.92.0.219
218.92.0.220
218.92.0.223
218.92.0.225
218.92.0.226
218.92.0.227
218.92.0.228
218.92.0.229
218.92.0.230
218.92.0.231
218.92.0.232
218.92.0.235
```

Sample Response:


```
[
  {
    "sha": "75fafbceeec34c3577275b8a96b0d9f7ede9f392",
    "commit": {
      "author": {
        "name": "Miroslav Stampar",
        "email": "miroslav.stampar@gmail.com",
        "date": "2026-08-12T01:04:25Z"
      },
      "committer": {
        "name": "Miroslav Stampar",
        "email": "miroslav.stampar@gmail.com",
        "date": "2026-08-12T01:04:25Z"
      },
      "message": "Automatic update"
    },
    "files": [
      {
        "filename": "levels/5.txt",
        "status": "added",
        "raw_url": "https://github.com/stamparm/ipsum/raw/
75fafbceeec34c3577275b8a96b0d9f7ede9f392/levels/5.txt"
      },
      {
        "filename": "levels/6.txt",
        "status": "added",
        "raw_url": "https://github.com/stamparm/ipsum/raw/
75fafbceeec34c3577275b8a96b0d9f7ede9f392/levels/6.txt"
      },
      {
        "filename": "levels/7.txt",
        "status": "added",
        "raw_url": "https://github.com/stamparm/ipsum/raw/
75fafbceeec34c3577275b8a96b0d9f7ede9f392/levels/7.txt"
      },
      {
        "filename": "levels/8.txt",
        "status": "added",
        "raw_url": "https://github.com/stamparm/ipsum/raw/
75fafbceeec34c3577275b8a96b0d9f7ede9f392/levels/8.txt"
      }
```

```
    ]
  }
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
data[].data	Indicator.Value	IP Address	Uses the Created At date	37.44.238.68	N/A
data[].total_blacklists	Indicator.Attribute	Blacklist Count	N/A	5	Updatable

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	1 minute
Indicators	850
Indicator Attributes	1,100

Change Log

- **Version 1.0.0**
  - Initial release