# ThreatQuotient

**A Securonix Company**

## Infoblox OSINT CDF

**Version 1.0.0**

March 16, 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.

# 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** | >= 5.12.1 |
| **Support Tier** | ThreatQ Supported |

# Introduction

The Infoblox OSINT CDF enables analysts to automatically ingest open source threat intelligence from Infoblox's public GitHub repository into ThreatQ. The repository contains periodically updated CSV files with indicators of compromise associated with tracked campaigns and threat actors, allowing analysts to correlate this data with existing intelligence and support threat analysis.

The integration provides the following feed:

- **Infoblox OSINT Indicators** - retrieves domain indicators from the Infoblox Open Threat Intelligence GitHub repository.

This feed 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 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
6. Select the individual feeds to install, when prompted and click **Install**.

   > 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(s) 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.

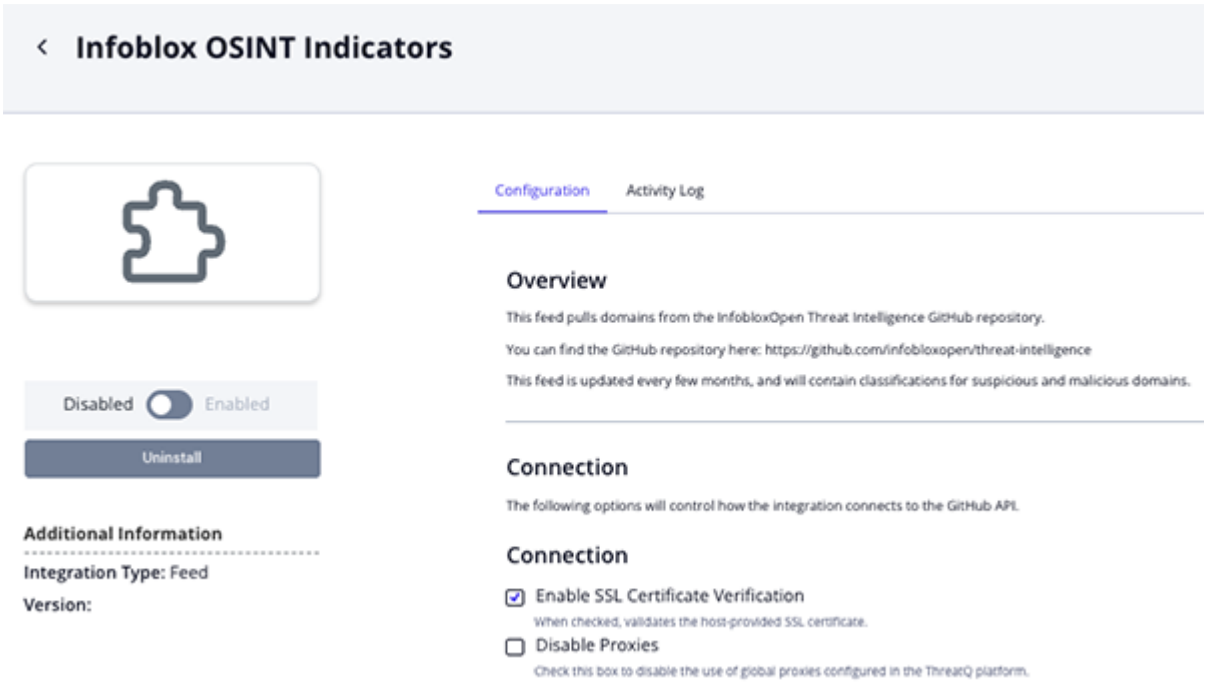
To configure the integration:

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 |
|---|---|
| **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

## Infoblox OSINT Indicators

The Infoblox OSINT Indicators feed ingests intelligence from the Infoblox OSINT API.

`GET https://raw.githubusercontent.com/infobloxopen/threat-intelligence/refs/heads/main/indicators/combined.csv`

### Sample Response:

```
type,indicator,classification,detected_date
domain,mssoftupdateserver.com,malicious,2025-09-11
domain,updatemssoft.com,malicious,2025-07-09
domain,domainzone123.com,malicious,2025-07-14
domain,nupdate0625.com,malicious,2025-06-19
domain,updatemsdnserver.com,malicious,2025-07-03
domain,msgdetox.com,malicious,2024-12-20
domain,knowableuniverse.com,malicious,2024-11-14
domain,infosystemsllc.com,malicious,2024-11-13
domain,betelgeuserigel.com,malicious,2024-11-02
domain,dns-routing.com,malicious,2025-05-03
domain,deidrerealestate.com,malicious,2025-05-03
domain,flow-distributor.com,malicious,2025-06-15
```

ThreatQuotient provides the following default mapping for this feed based on the column indexes of the csv file.

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| `0-type` | Indicator.Type | N/A | N/A | domain | Converted to the ThreatQ indicator type. |
| `1-indicator` | Indicator.Value | FQDN | `3-detected_date` | `baddomain[.]top` | N/A |
| `2-classification` | Indicator.Attribute | Classification | `3-detected_date` | `malicious` | N/A |
| `3-classification` | Indicator.Attribute | Detected At | `3-detected_date` | `2025-06-15` | 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** | 1 minute |
| **Indicators** | 202 |
| **Indicator Attributes** | 404 |

# Change Log

- **Version 1.0.0**
  - Initial release