ThreatQuotient

A Securonix Company

NSFOCUS CDF

Version 1.0.0

April 13, 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 NSFOCUS CDF integration enables the automated ingestion of NSFOCUS Threat Intelligence (NTI) into the ThreatQ platform, providing analysts with timely and actionable insight into emerging cyber threats. Leveraging a global sensor network with strong visibility into North Asia, NSFOCUS delivers high-quality indicators of compromise, including IP addresses, domains, URLs, and file hashes. Each indicator is enriched with contextual metadata such as confidence, threat level, threat type, and category, allowing organizations to enhance threat analysis, accelerate response efforts, and strengthen proactive defense capabilities.

The integration provides the following feed:

- **NSFOCUS Threat Intelligence IOCs** - ingests NSFOCUS Threat Intelligence IOCs, such as domains, IP Addresses, and URLs into ThreatQ.

The integration ingests indicator type objects into the ThreatQ platform.

Prerequisites

The integration requires the following:

- An NSFOCUS NTI API Key.

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:

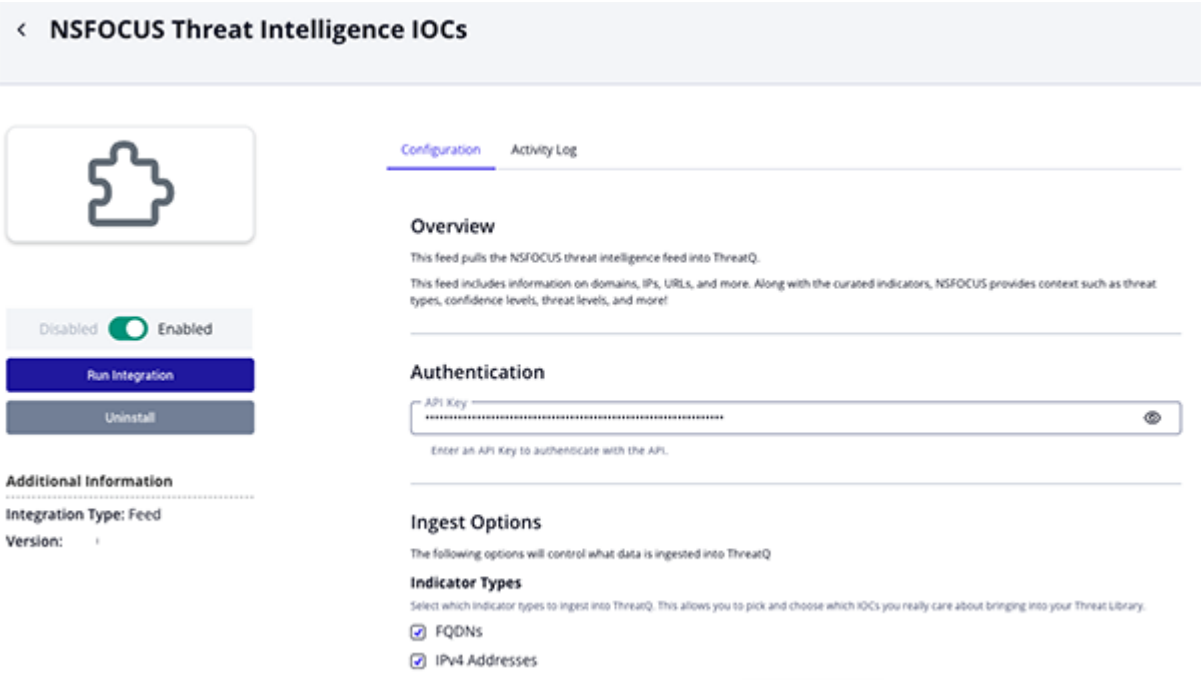
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   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
API Key	Enter your NSFOCUS NTI API Key.
Indicator Types	Select which indicator types to ingest into ThreatQ. Options include: ◦ FQDNs *(default)* ◦ IP Addresses *(default)* ◦ IPv6 Addresses ◦ URLs *(default)* ◦ MD5 Hashes *(default)* ◦ SHA-1 Hashes *(default)* ◦ SHA-256 Hashes *(default)*
Confidence Threshold	Specify a numeric value between 0 and 100 to define the minimum confidence score required for indicator ingestion. The majority of indicators in this feed have a confidence score of 90 or higher. The default value is 90.
Context Filter	Select the context to ingest into ThreatQ, along with each indicator. Options include:

PARAMETER	DESCRIPTION
	◦ Tags *(default)* ◦ Confidence Score *(default)* ◦ Threat Score *(default)* ◦ Threat Type *(default)* ◦ Threat Subtype *(default)* ◦ Category *(default)* ◦ Revoked ◦ Credit Level ◦ Valid Until Some pieces of context may not be available for all indicators.
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

NSFOCUS Threat Intelligence IOCs

The NSFOCUS Threat Intelligence IOCs feed ingests intelligence from the NSFOCUS API.

```
GET https://nti.nsfocusglobal.com/api/v2/download/feed/
```

Sample Response:


```
{"count": 381607, "title": "ioc-updated", "default": {"created_by":
"nsfocus"}, "created": "2025-11-13T04:04:20.080Z", "spec_version":
"2.0", "created_by": "nsfocus", "version": "20251113.0001", "type":
"igroup", "id": "0d1502266914e84403101", "previous": "20251112.0001"}
{"valid_until": "2025-11-18T23:59:00Z", "confidence": 100,
"act_types": [0], "revoked": false, "tags": [{"tag_values":
["inbound"], "tag_type": "direction"}], "credit_level": 5, "pattern":
"[ipv4-addr:value = '218.67.12.167']", "modified":
"2025-11-11T02:55:16.000Z", "created_by": "nsfocus", "observables":
[{"type": "ipv4-addr", "value": "218.67.12.167"}], "threat_types":
[5], "threat_level": 5, "type": "indicator", "id":
"0c9010276912341d030f1", "categories": ["ip"]}
{"valid_until": "2025-11-17T23:59:00Z", "confidence": 100,
"act_types": [0], "revoked": false, "tags": [{"tag_values":
["inbound"], "tag_type": "direction"}], "credit_level": 5, "pattern":
"[ipv4-addr:value = '182.35.212.220']", "modified":
"2025-11-10T10:18:54.000Z", "created_by": "nsfocus", "observables":
[{"type": "ipv4-addr", "value": "182.35.212.220"}], "threat_types":
[5], "threat_level": 5, "type": "indicator", "id":
"0c90101369114b60030f1", "categories": ["ip"]}
{"valid_until": "2026-02-09T23:59:00Z", "confidence": 100,
"act_types": [0], "revoked": false, "tags": [{"tag_values":
["inbound"], "tag_type": "direction"}], "credit_level": 5, "pattern":
"[ipv4-addr:value = '36.221.39.220']", "modified":
"2025-11-11T17:20:19.000Z", "created_by": "nsfocus", "observables":
[{"type": "ipv4-addr", "value": "36.221.39.220"}], "threat_types":
[50302], "threat_level": 5, "type": "indicator", "id":
"0c90104968e3102b030f1", "categories": ["ip"]}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.pattern	Indicator.Value	FQDN, IP Address, URL, MD5, SHA-1, SHA-256	N/A	218.67.12.167	N/A
.threat_types[]	Indicator.Attribute	Threat Type	N/A	Malware	Converted from ID to friendly name
.threat_types[]	Indicator.Attribute	Threat Subtype	N/A	Trojan	Subtype is calculated from the threat type IDs
.categories[]	Indicator.Attribute	Category	N/A	N/A	Basic categories are ignored, i.e. ip, domain, etc.
.threat_level	Indicator.Attribute	Threat Score	N/A	5	N/A
.confidence	Indicator.Attribute	Confidence Score	N/A	100	N/A
.revoked	Indicator.Attribute	Revoked	N/A	false	N/A
.valid_until	Indicator.Attribute	Valid Until	N/A	2026-02-09T23:59:00Z	N/A
.credit_level	Indicator.Attribute	Credit Level	N/A	5	N/A
.tags[]	Indicator.Attribute	.tags[].tag_type	N/A	inbound	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	42 minutes
Indicators	42,511
Indicator Attributes	331,307

Known Issues / Limitations

- This feed fetches the `incremental` feed from NSFOCUS NTI. This is due to the volume of the full feed being extremely large. For more information and the full list regarding the threat type and subtype, refer to the NSFOCUS API docs.

Change Log

- **Version 1.0.0**
  - Initial release