

# ThreatQuotient

A Securonix Company



## GreyNoise CDF

**Version 1.6.1**

June 08, 2026

### ThreatQuotient

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147

 **ThreatQ Supported**

### Support

Email: [tq-support@securonix.com](mailto:tq-support@securonix.com)

Web: <https://ts.securonix.com>

Phone: 703.574.9893

# Contents

<b>Warning and Disclaimer</b> .....	<b>3</b>
<b>Support</b> .....	<b>4</b>
<b>Integration Details</b> .....	<b>5</b>
<b>Introduction</b> .....	<b>6</b>
<b>Installation</b> .....	<b>7</b>
<b>Configuration</b> .....	<b>8</b>
GreyNoise Configuration Parameters .....	8
GreyNoise Enrichment Configuration Parameters.....	11
<b>ThreatQ Mapping</b> .....	<b>13</b>
GreyNoise .....	13
GreyNoise Enrichment.....	13
Shared Response and Mapping .....	13
GreyNoise Malware Tags Mapping.....	18
GreyNoise Trust Level Mapping.....	19
<b>Average Feed Run</b> .....	<b>20</b>
GreyNoise .....	20
GreyNoise Enrichment.....	20
<b>Known Issues / Limitations</b> .....	<b>21</b>
<b>Change Log</b> .....	<b>22</b>

## 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](mailto: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** 1.6.1

**Compatible with ThreatQ Versions**  $\geq 5.6.0$

**Support Tier** ThreatQ Supported

# Introduction

GreyNoise collects, analyzes, and labels data on IPs that saturate security tools with noise. This unique perspective helps analysts waste less time on irrelevant or harmless activity, and spend more time focused on targeted and emerging threats.

The GreyNoise CDF provides the following feeds:


- **GreyNoise** - ingests new, malicious IP Addresses every day. Additionally, a GNQL query can be provided to narrow down the results.
- **GreyNoise Enrichment** - queries GreyNoise with IP Addresses from a Threat Collection and enriches those IP Addresses with the data that it ingests.

The following system object types are ingested by the integration:


- Indicators
  - Indicator Attributes
- Vulnerabilities

# 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
6. Select the 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.

7. The feeds 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).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

## GreyNoise Configuration Parameters

PARAMETER	DESCRIPTION
<b>API Token</b>	Your GreyNoise API Token.
<b>Enable SSL Certificate Verification</b>	Enable this parameter if the feed should validate the host-provided SSL certificate.
<b>Disable Proxies</b>	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
<b>Last Seen Time Range</b>	The date the device was most recently observed by GreyNoise. You can use the keyword <code>today</code> or <code>1d</code> to specify how many days to go back.
<b>GNQL Query</b>	ThreatQuotient highly recommends utilizing this parameter to narrow down the ingested dataset. The field allows you to specify query arguments other than <code>last_seen</code> field, which is the default. See the <a href="https://docs.greynoise.io/reference/gnqlv3query">https://docs.greynoise.io/reference/gnqlv3query</a> documentation for instructions on how to build a GNQL query.

PARAMETER	DESCRIPTION
<b>Items per Page</b>	<p>The number of items to return per page from the GreyNoise API.</p> <div data-bbox="548 384 1442 499" style="border: 1px solid #4a7ebb; border-radius: 10px; padding: 10px; margin-top: 10px;">  You should lower this value if you are encountering 400 errors when running the feed.                 </div>
<b>Attribute Filter</b>	<p>Select the pieces of context, attributes and tags, to ingest into the platform. Options include:</p> <ul style="list-style-type: none"> <li>◦ Tags (default)</li> <li>◦ Classification (default)</li> <li>◦ Malware Family (default)</li> <li>◦ Actor (default)</li> <li>◦ Category (default)</li> <li>◦ CVE (default)</li> <li>◦ Country</li> <li>◦ Country Code (default)</li> <li>◦ City</li> <li>◦ Destination Countries</li> <li>◦ Organization</li> <li>◦ Is TOR (default)</li> <li>◦ Is VPN (default)</li> <li>◦ Is Spoofable</li> <li>◦ Is Bot</li> <li>◦ VPN Service</li> <li>◦ Operating System</li> <li>◦ ASN</li> <li>◦ rDNS</li> <li>◦ Scanned Paths</li> <li>◦ Scanned Ports</li> </ul>
<b>Relationship Filter</b>	<p>Select the related IOC types to ingest into ThreatQ.</p> <div data-bbox="548 1535 1442 1650" style="border: 1px solid #4a7ebb; border-radius: 10px; padding: 10px; margin-top: 10px;">  At the time of this publication, the only option is CVE.                 </div>
<b>Ingest CVEs As</b>	<p>Select the entity type to ingest CVEs as in ThreatQ. Options include:</p> <ul style="list-style-type: none"> <li>◦ Indicators</li> </ul>

**PARAMETER**

**DESCRIPTION**

- Vulnerabilities

< **GreyNoise**



Disabled  Enabled

Run Integration

Uninstall

**Additional Information**

Integration Type: Feed

Version:

Configuration **Activity Log**

**Authentication and Connection**

API Key

Enter an API Key to authenticate with the GreyNoise API.

**Enable SSL Certificate Verification**

When checked, validates the host provided SSL certificate.

**Disable Proxies**

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

**Ingestion Options**

Last Seen Time Range

The date the device was most recently observed by GreyNoise (YY-MM-DD)

GNQL Query

This query allows you to specifies additional query arguments. Using this field is required in order to limit the amount of data that is ingested.

Items Per Page

The number of items to return per page from the GreyNoise API. If you are running into 400 errors, try lowering this number.

## GreyNoise Enrichment Configuration Parameters

PARAMETER	DESCRIPTION
<b>API Token</b>	Your GreyNoise API Token.
<b>Enable SSL Certificate Verification</b>	Enable this parameter if the feed should validate the host-provided SSL certificate.
<b>Disable Proxies</b>	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
<b>Data Collection Hash</b>	<p>The hash of the Data Collection to be enriched. This hash can be found in your Threat Library after loading the Data Collection. The hash will be in the browser's URL.</p> <p><b>Example:</b> <code>https://&lt;instance&gt;/threat-library#38d08c87b6e81a37a8591444f8c5dba5</code></p>
<b>Attribute Filter</b>	<p>Select the pieces of context, attributes and tags, to ingest into the platform. Options include:</p> <ul style="list-style-type: none"> <li>◦ Tags (default)</li> <li>◦ Classification (default)</li> <li>◦ Malware Family (default)</li> <li>◦ Actor (default)</li> <li>◦ Category (default)</li> <li>◦ CVE (default)</li> <li>◦ Country</li> <li>◦ Country Code (default)</li> <li>◦ City</li> <li>◦ Is TOR (default)</li> <li>◦ Is VPN (default)</li> <li>◦ Is Spoofable</li> <li>◦ Is Bot</li> <li>◦ VPN Service</li> <li>◦ Operating System</li> <li>◦ ASN</li> <li>◦ rDNS</li> <li>◦ Scanned Paths</li> <li>◦ Scanned Ports</li> </ul>

**PARAMETER**

**DESCRIPTION**

- Destination Countries
- Organization

**Relationship Filter**

Select the related IOC types to ingest into ThreatQ.



At the time of this publication, the only option is CVE.

**Ingest CVEs As**

Select the entity type to ingest CVEs as in ThreatQ. Options include:

- Indicators
- Vulnerabilities

**< GreyNoise Enrichment**



Disabled  Enabled

**Additional Information**

Integration Type: Feed  
Version:

Configuration Activity Log

**Authentication and Connection**

API Key

Enter an API Key to authenticate with the GreyNoise API.

- Enable SSL Certificate Verification  
When checked, validates the host-provided SSL certificate.
- Disable Proxies  
If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

**Request Options**

Data Collection Hash

The hash of the Data Collection to be enriched. This hash can be found in your Threat Library after loading the Data Collection.

**Ingestion Options**

**Attribute Filter**

Select the pieces of context (Attributes & Tags) to bring into ThreatQ.

- Tags
- Classification

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

## GreyNoise

The GreyNoise feed ingests new, malicious IP Addresses every day. Additionally, a GNQL query can be provided to narrow down the results.

```
GET https://api.greynoise.io/v3/gnql/metadata
```

### Sample Parameters:

```
{
  "query": "last_seen:1d AND classification:malicious AND
destination_country:Iceland"
}
```

## GreyNoise Enrichment

The GreyNoise Enrichment feed enriches IP Addresses from a given Threat Collection with information from GreyNoise.

```
POST https://api.greynoise.io/v3/ip
```

### Sample Body:

```
{
  "ips": [
    "1.1.1.1"
  ]
}
```

## Shared Response and Mapping

The following sample response and mapping table can be used for both feeds.

### Sample Response:

```
{
  "data": [
    {
      "business_service_intelligence": {
        "category": "public_dns",
        "description": "Cloudflare, Inc. is an American web
```

```

infrastructure and website security company.",
  "explanation": "Public DNS services are used as alternatives
to ISP name servers for DNS lookups.",
  "found": true,
  "last_updated": "2025-12-05T09:11:03Z",
  "name": "Cloudflare Public DNS",
  "reference": "https://one.one.one.one",
  "trust_level": "1"
},
"internet_scanner_intelligence": {
  "actor": "APT9",
  "bot": false,
  "classification": "malicious",
  "cves": [
    "CVE-2020-1234",
    "CVE-2021-2345"
  ],
  "first_seen": "2025-12-01",
  "found": false,
  "metadata": {
    "asn": "AS3462",
    "category": "isp",
    "organization": "Data Communication Business Group",
    "os": "Windows 7/8",
    "rdns": "crawl-66-249-79-17.googlebot.com",
    "source_city": "Milan",
    "source_country": "Italy",
    "source_country_code": "IT",
    "destination_countries": [
      "Germany"
    ],
    "destination_country_codes": [
      "DE"
    ]
  },
  "raw_data": {
    "http": {
      "path": [
        "/bootstrap/3.3.6/css/bootstrap.min.css"
      ]
    },
    "scan": [
      {

```

```

        "port": 80,
        "protocol": "TCP"
    }
]
},
"spooftable": true,
"tags": [
    {
        "id": "0adee501-f8d5-4287-96cf-0c7f47e4e2b3",
        "slug": "apple-ios-lockdownnd-scanner",
        "name": "Apple iOS Lockdownnd Crawler",
        "description": "Observed attempting to discover legacy
Apple iOS devices with lockdownnd service.",
        "category": "activity",
        "intention": "suspicious",
        "references": [
            "https://www.theiphonewiki.com/wiki/
Usbmux#lockdownnd_protocol"
        ],
        "created": "2021-09-03",
        "updated_at": "2025-12-09T17:05:28.043568Z"
    },
    {
        "id": "0adee501-f8d5-4287-96cf-0c7f47e4e2b4",
        "slug": "emotet",
        "name": "Emotet",
        "description": "Observed attempting to send phishing
attacks.",
        "category": "activity",
        "intention": "suspicious",
        "created": "2021-09-03",
        "updated_at": "2025-12-09T17:05:28.043568Z"
    }
],
"tor": false,
"vpn": false,
"vpn_service": "Cisco"
},
"ip": "1.1.1.1"
}

```

```
]
}
```

ThreatQuotient provides the following default mapping for both feeds based on fields within each of the `.data[]`:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.ip</code>	Indicator.Value	IP Address	<code>.first_seen</code>	1.1.1.1	N/A
<code>.business_service_intelligence.explanation</code>	Indicator.Description	N/A	N/A	Public DNS services are used as alternatives ...	N/A
<code>.business_service_intelligence.description</code>	Indicator.Description	N/A	N/A	Cloudflare, Inc. is an American web infrastructure ...	N/A
<code>.internet_scanner_intelligence.tags[].name</code>	Indicator.Tags	N/A	N/A	Apple iOS Lockdownd Crawler	User-configurable.
<code>.internet_scanner_intelligence.actor</code>	Indicator.Attribute	Actor	<code>.first_seen</code>	APT9	User-configurable. If this is 'unknown', it will be ignored.
<code>.internet_scanner_intelligence.classification</code>	Indicator.Attribute	Classification	<code>.first_seen</code>	malicious	User-configurable.
<code>.internet_scanner_intelligence.metadata.rdns</code>	Indicator.Attribute	rDNS	<code>.first_seen</code>	crawl-66-249-79-17.googlebot.com	User-configurable
<code>.internet_scanner_intelligence.metadata.source_country</code>	Indicator.Attribute	Source Country	<code>.first_seen</code>	Italy	User-configurable
<code>.internet_scanner_intelligence.metadata.source_country_code</code>	Indicator.Attribute	Country Code	<code>.first_seen</code>	IT	User-configurable
<code>.internet_scanner_intelligence.metadata.source_city</code>	Indicator.Attribute	Source City	<code>.first_seen</code>	Milan	User-configurable
<code>.internet_scanner_intelligence.metadata.destination_countries[]</code>	Indicator.Attribute	Destination Country	<code>.first_seen</code>	Germany	User-configurable
<code>.internet_scanner_intelligence.metadata.destination_country_codes[]</code>	Indicator.Attribute	Destination Country Code	<code>.first_seen</code>	DE	User-configurable
<code>.internet_scanner_intelligence.metadata.organization</code>	Indicator.Attribute	Organization	<code>.first_seen</code>	Data Communication Business Group	User-configurable
<code>.internet_scanner_intelligence.metadata.asn</code>	Indicator.Attribute	ASN	<code>.first_seen</code>	AS3462	User-configurable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.internet_scanner_intelligence.tor	Indicator.Attribute	Is Tor	.first_seen	False	User-configurable. This is converted to string. Updatable.
.internet_scanner_intelligence.metadata.os	Indicator.Attribute	Operating System	.first_seen	Windows 7/8	User-configurable
.internet_scanner_intelligence.metadata.category	Indicator.Attribute	Category	.first_seen	isp	User-configurable
.internet_scanner_intelligence.raw_data.http.path[]	Indicator.Attribute	Scanned Path	.first_seen	/bootstrap/3.3.6/css/bootstrap.min.css	User-configurable. Only populated when the response includes raw_data.
.internet_scanner_intelligence.raw_data.scan[].port	Indicator.Attribute	Scanned Port	.first_seen	80	User-configurable. Only populated when the response includes raw_data.
.internet_scanner_intelligence.bot	Indicator.Attribute	Is Bot	.first_seen	False	User-configurable. This is converted to string. Updatable.
.internet_scanner_intelligence.vpn	Indicator.Attribute	Is VPN	.first_seen	False	User-configurable. This is converted to string. Updatable.
.internet_scanner_intelligence.spoofable	Indicator.Attribute	Is Spoofable	.first_seen	True	User-configurable. This is converted to string. Updatable
.internet_scanner_intelligence.vpn_service	Indicator.Attribute	VPN Service	.first_seen	Cisco	User-configurable
.internet_scanner_intelligence.tags[]	Indicator.Attribute	Malware Family	.first_seen	Emotet	User-configurable. If the value is present in the table below Greynoise Malware Tags Mapping
.business_service_intelligence.name	Indicator.Attribute	Name	.first_seen	Google Public DNS	N/A
.business_service_intelligence.trust_level	Indicator.Attribute	Trust Level	.first_seen	Trustworthy	Mapped according to Greynoise Trust Mapping
.business_service_intelligence.reference	Indicator.Attribute	Reference	.first_seen	https://one.one.one.one	N/A
.internet_scanner_intelligence.cves[]	Related Indicator.Vulnerability	CVE/Vulnerability	.first_seen	CVE-2020-1234	User-configurable. Ingested according to Ingest CVEs As.

## GreyNoise Malware Tags Mapping

The following is how GreyNoise malware tags are mapped as attribute values in ThreatQ.

<b>GREYNOISE MALWARE TAG</b>	<b>THREATQ ATTRIBUTE VALUE</b>
emotet	Emotet
trickbot	TrickBot
mirai	Mirai
looks like conficker	Conficker
d3c3mb3r botnet	D3C3MB3R Bot
looks like eternalblue	EternalBlue
zmeu worm	ZmEu
e6 group	E6
zte router worm	ZTE Router Worm
ssh bruteforcer	SSH Bruteforcer
androxgh0st	Androxgh0st
zyxel router worm	Zyxel Router Worm


---

## GreyNoise Trust Level Mapping

The following is how GreyNoise trust levels are mapped as attribute values in ThreatQ.

<b>GREYNOISE TRUST LEVEL</b>	<b>THREATQ ATTRIBUTE VALUE</b>
1	Trustworthy
2	Somewhat Trustworthy

# 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.

## GreyNoise

METRIC	RESULT
Run Time	1 minute
Indicators	8,591
Indicator Attributes	469,101
Vulnerabilities	134

## GreyNoise Enrichment

METRIC	RESULT
Run Time	1 minute
Indicators	6
Indicator Attributes	1,310
Vulnerabilities	5

## Known Issues / Limitations

- The current implementation of GreyNoise feed will not prevent the timeout errors from occurring, but it will minimize them. Also, should the error occur, the integration will still ingest the information it has received up to that point. Users should include as many limiting search parameters as they can in order to prevent any timeout errors they might encounter from the Greynoise API.

---

# Change Log

- **Version 1.6.1**
  - Updated the GreyNoise feed to utilize the **GNQL Metadata API endpoint**, reducing response payload sizes and improving memory efficiency during feed processing.
- **Version 1.6.0**
  - Updated both feeds, **GreyNoise** and **GreyNoise Enrichment**, to utilize GreyNoise v3 api endpoints.
  - Added the following new configuration parameters for both feeds:
    - **Enable SSL Certificate Verification** - determine if the feed should validate the host-provided SSL certificate.
    - **Disable Proxies** - determine if the feed should honor proxies set in the ThreatQ UI.
    - **Relationship Filter** - select the related IOC types to ingest into ThreatQ.
    - **Ingest CVEs As** - Select the entity type to ingest CVEs as in ThreatQ.
  - Updated the minimum ThreatQ version to 5.6.0.
- **Version 1.5.3**
  - Resolved an issue where users would encounter a `Error creating objects from threat data error` with the **GreyNoise** feed when `first_seen` contained an empty string.
- **Version 1.5.2**
  - Added the ability to ingest the `Destination Country` attribute.
- **Version 1.5.1**
  - Added the GreyNoise feed back into the integration.
  - The **user agent** has been updated to be unique for each feed.
- **Version 1.5.0**
  - Added configuration field, **Attribute Filter**, that allows you to select which context is ingested into the ThreatQ platform.
  - Resolved an issue where certain attributes would only be ingested if the **vpn** attribute existed.

- 
- Lowered the default limit parameter to prevent hitting pagination scroll ID timeouts. The parameter is now configurable from the configuration page: **Items per Page**.
  - Updated the minimum ThreatQ version to 4.58.0.
  - Fixed typo for the rDNS attribute (was RDSN)
  - Removed GreyNoise feed due to GreNoise limitations regarding large data ingestion
  - **Version 1.4.0**
    - Improved integration performance by saving CVE, Malware, RDNS, and ASN as attributes.
    - Removed the **Ingest CVEs** parameter from the configuration page.
  - **Version 1.3.0**
    - Fixed a filter error with the GreyNoise Enrichment feed that would occur when GreyNoise did not return any enrichment data.
    - Added a manual run option for the GreyNoise Enrichment feed.
  - **Version 1.2.0**
    - Added new GreyNoise Enrichment feed.
    - Add new user configuration fields for GreyNoise feed.
  - **Version 1.1.0**
    - Added new user field.
    - Added published date to all attributes.
    - Added tags.
  - **Version 1.0.1**
    - Limited the number of ingested `paths` attributes to 9000 to improve integration performance.
  - **Version 1.0.0**
    - Initial Release