ThreatQuotient

GreyNoise CDF User Guide

Version 1.5.0

August 08, 2023

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

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: 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	1.5.0
Compatible with ThreatQ Versions	>= 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 feed:

- **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

    > 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 *(GreyNoise Feed Only)*	ThreatQuotient highly recommends utilizing this parameter to narrow down the ingested dataset. The field allows you to specify query arguments other than `last_seen` 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.
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:** https:// /threat-library**#38d08c87b6e81a37a8591444f8c5dba5**

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 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"
}
```

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	N/A	`data[].first_seen`	CRAZY PANDA	If this is 'unknown', it will be ignored
`.data[].tags[]`	Indicator.Tags	N/A	N/A	Eternalblue	The data path is a list of tags
`.data[].classification`	Indicator.Attribute	Classification	`data[].first_seen`	malicious	For this feed, this will always be 'malicious'
`.data[].cve[]`	Indicator.Attribute	N/A	`data[].first_seen`	N/A	N/A
`.data[].metadata.rdns`	Indicator.Attribute	FQDN	`data[].first_seen`	114-25-66-87.dynamic-ip.hinet.net	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.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
`.data[].metadata.tor`	Indicator.Attribute	Is Tor	`data[].first_seen`	true/false	This is converted to a yes/no
`.data[].metadata.os`	Indicator.Attribute	Operating System	`data[].first_seen`	Windows 7/8	N/A
`.data[].metadata.category`	Indicator.Attribute	Category	`data[].first_seen`	isp	N/A
`.data[].raw_data.web.paths[]`	Indicator.Attribute	Scanned Path	`data[].first_seen`	/bootstrap/3.3.6/css/bootstrap.min.css	N/A
`.data[].bot`	Indicator.Attribute	Is Bot	`data[].first_seen`	Yes	Boolean -> Yes/No
`.data[].vpn`	Indicator.Attribute	Is VPN	`data[].first_seen`	Yes	Boolean -> Yes/No
`.data[].spoofable`	Indicator.Attribute	Is Spoofable	`data[].first_seen`	Yes	Boolean -> Yes/No
`.data[].vpn_service`	Indicator.Attribute	VPN Service	`data[].first_seen`	Express VPN	N/A
`.data[].name`	Indicator.Attribute	Name	`data[].first_seen`	Google Public DNS	N/A

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

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

Change Log

- **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