

ThreatQuotient



GreyNoise CDF Guide

Version 1.0.1

December 07, 2021

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

Support 4

Versioning..... 5

Introduction 6

Installation..... 7

Configuration 8

ThreatQ Mapping 10

 GreyNoise (Feed)..... 10

Average Feed Run..... 12

Known Issues / Limitations 13

Change Log..... 14

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 © 2021 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.

Versioning

- Current integration version: 1.0.1
- Compatible with ThreatQ versions \geq 4.15.0

Introduction

The GreyNoise CDF integration for ThreatQ allows a user to ingest malicious IP addresses from the GreyNoise API.

The CDF provides the following endpoint:

- **GreyNoise** - ingests indicators from the GreyNoise API.

The following system object type is ingested by the integration:

- Adversaries
- Indicators

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: <ul style="list-style-type: none">• Malicious (default)• Benign• Unknown
Additional GNQL Query	Specify an extension to the default query of <code>last_seen:today AND classification:malicious</code> . ThreatQuotient highly recommends utilizing this parameter to narrow down the ingested dataset. See the http://docs.greynoise.io/#gnql-query documentation for instructions on how to build a GNQL query.

Configuration

Activity Log

API Key



Your GreyNoise API Key

Classifications


Classifications

☒ Malicious

☐ Benign

☐ Unknown

Additional GNQL Query



This query allows you to specify an extension to the default query of 'last_seen:today AND classification:malicious'. Using this field is greatly advised.

How frequent should we pull information from this feed?

Every Day

▼

Set indicator status to...

Active

▼

☒ Send a notification when this feed encounters issues.

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)

This feed will ingest indicators from the GreyNoise API

GET <https://api.greynoise.io/v2/experimental/gnq1>

```
{
  "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": "unknown",
      "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"
      },
      "raw_data": {
        "scan": [
          {
            "port": 445,
            "protocol": "TCP"
          }
        ],
        "web": {},
        "ja3": []
      }
    }
  ]
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
data[]	Object	Indicator	N/A	N/A
data[].ip	Object Value	Indicator	114.25.66.87	N/A
data[].first_seen	Published At	Indicator	2019-07-28	N/A
data[].metadata.rdns	Object Value	Related Indicator	114-25-66-87.dynamic-ip.hinet.net	This will always be an FQDN
data[].actor	Object Name	Related Adversary	CRAZY PANDA	If this is 'unknown', it will be ignored
data[].classification	Attribute	Classification	malicious	For this feed, this will always be 'malicious'
data[].tags[]	Attribute	Tag	Eternalblue	The data path is a list of tags
data[].metadata.country	Attribute	Country	Taiwan, Province of China	N/A
data[].metadata.country_code	Attribute	Country Code	TW	N/A
data[].metadata.city	Attribute	City	Nankang	N/A
data[].metadata.organization	Attribute	Organization	Data Communication Business Group	N/A
data[].metadata.asn	Attribute	ASN	AS3462	N/A
data[].metadata.tor	Attribute	Is Tor	true/false	This is converted to a yes/no
data[].metadata.os	Attribute	Operating System	Windows 7/8	N/A
data[].metadata.category	Attribute	Category	isp	N/A
data[].raw_data.web.paths[]	Attribute	Scanned Path	/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

Known Issues / Limitations

- The GreyNoise feed has no historical feature due to the sheer amount of indicators from the feed. The feed only will pull 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 1.0.1**
 - Limited the number of ingested paths attributes to 9000 to improve integration performance.
- **Version 1.0.0**
 - Initial Release