ThreatQuotient

GreyNoise Feed Implementation Guide

Version 1.0.0

Monday, March 9, 2020

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

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.

Last Updated: Monday, March 9, 2020

Contents

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions >= `4.15.0`

Introduction

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

Installation

Perform the following steps to install the feeds:

The same steps can be used to upgrade the feed to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the **GreyNoise** feed file.
3. Navigate to your ThreatQ instance.
4. Click on the **Settings** icon and select **Incoming feeds**.
5. Click on the **Add New Feed** button.
6. Upload the feeds file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the feed 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.

The feed will be added to the **Commercial** tab for Incoming Feeds. 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 feed-related credentials.

To configure the feed:

1. Click on the **Settings** icon and select **Incoming Feeds**.
2. Locate the feed under the **Commercial** tab.
3. Click on the **Feed Settings** link for the feed.
4. Under the **Connection** tab, enter the following configuration parameters:

Parameter	Description
API Token	Your GreyNoise API Token.
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 in order to narrow down the ingested dataset. A document detailing how to build a GNQL query can be found here: http://docs.greynoise.io/#gnql-query.

5. Click on **Save Changes**.
6. Click on the toggle switch to the left of the feed name to enable the feed.

ThreatQ Mapping

GreyNoise (Feed)

This feed will ingest 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": "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
data[]	Object	Indicator	N/A
data[].ip	Object Value	Indicator	114.25.66.87
data[].first_seen	Published At	Indicator	2019-07-28
data[].metadata.rdns	Object Value	Related Indicator	114-25-66-87.dynamic-ip.hinet.net
data[].actor	Object Name	Related Adversary	CRAZY PANDA
data[].classification	Attribute	Classification	malicious
data[].tags[]	Attribute	Tag	Eternalblue
data[].metadata.country	Attribute	Country	Taiwan, Province of China
data[].metadata.country_code	Attribute	Country Code	TW
data[].metadata.city	Attribute	City	Nankang
data[].metadata.organization	Attribute	Organization	Data Communication Business Group
data[].metadata.asn	Attribute	ASN	AS3462
data[].metadata.tor	Attribute	Is Tor	true/false

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples
data[].metadata.os	Attribute	Operating System	Windows 7/8
data[].metadata.category	Attribute	Category	isp
data[].raw_data.web.paths[]	Attribute	Scanned Path	/bootstrap/3.3.6/css/bootstrap.min.css

Known Issues/Limitations

- This 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.
    - Here is a document detailing how to build a GNQL query: http://-docs.greynoise.io/#gnql-query.
    - This query will be appended to the base query of, 'last_seen:today AND classification:malicious'