ThreatQuotient

GreyNoise Operation Guide

Version 1.0.0

January 28, 2021

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.

Contents

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions >= `4.0`

Introduction

The GreyNoise Operation for ThreatQuotient allows a ThreatQ user to query GreyNoise for any indicator context. If matches are found, related indicators will be returned, as well as any context.

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 operation 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 operation and will require user confirmation before proceeding.
6. You will still need to configure and then enable the operation.

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 **Operations** option from the *Type* 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 parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Token	Your GreyNoise API Token.

5. Click **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Query	Query GreyNoise for indicator context	Indicator	IP Address

Query

This action will query GreyNoise for any metadata, including reverse DNS, tags, geolocation, and scanned paths/ports.

```
GET https://api.greynoise.io/experimental/gnql
```

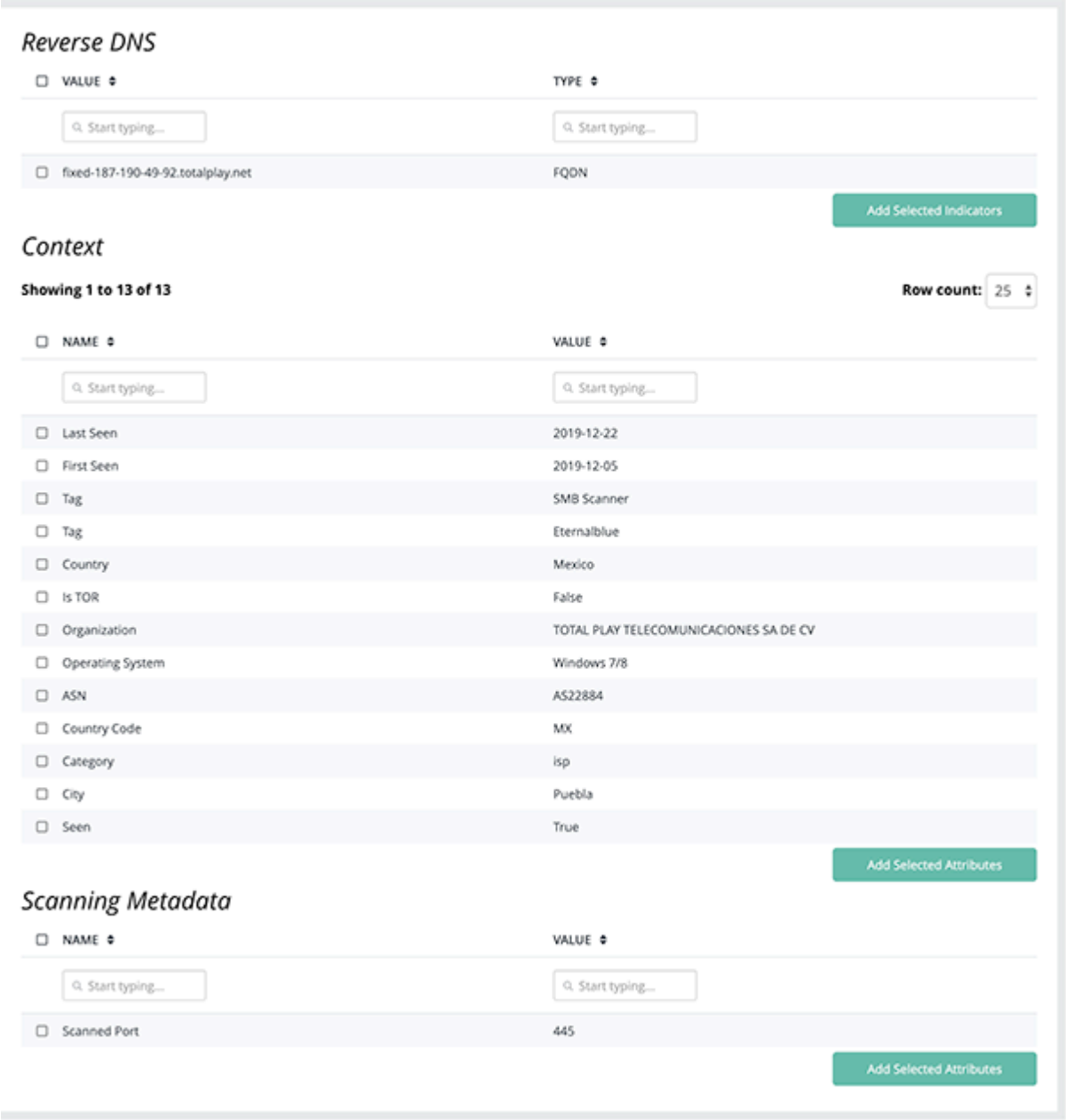
JSON response sample:


```
{
    "data": [
        {
            "first_seen": "2019-12-05",
            "actor": "unknown",
            "ip": "187.190.49.92",
            "seen": true,
            "last_seen": "2019-12-22",
            "classification": "malicious",
            "tags": [
                "SMB Scanner",
                "Eternalblue"
            ],
            "raw_data": {
                "ja3": [],
                "web": {},
                "scan": [
                    {
                        "port": 445,
                        "protocol": "TCP"
                    }
                ]
            },
            "metadata": {
                "category": "isp",
                "country_code": "MX",
                "tor": false,
                "os": "Windows 7/8",
                "organization": "TOTAL PLAY TELECOMUNICACIONES SA DE CV",
                "rdns": "fixed-187-190-49-92.totalplay.net",
                "asn": "AS22884",
                "city": "Puebla",
                "country": "Mexico"
            }
        }
    ],
    "message": "ok",
    "complete": true,
    "count": 1,
    "query": "187.190.49.92"
}
```

ThreatQ provides the following default mapping for this Action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].first_seen	Indicator.Attribute	First Seen	N/A	2019-12-05	N/A
.data[].actor	Indicator.Attribute	Adversary	N/A	unknown	N/A
.data[].seen	Indicator.Attribute	Seen	N/A	True	N/A
.data[].last_seen	Indicator.Attribute	Last Seen	N/A	2019-12-22	N/A
.data[].classification	Indicator.Attribute	Classification	N/A	malicious	N/A
.data[].tags[]	Indicator.Attribute	Tag	N/A	Eternalblue	N/A
.data[].raw_data.scan.port	Indicator.Attribute	Scanned Port	N/A	445	N/A
.data[].raw_data.web.paths	Indicator.Attribute	Scanned Path	N/A	/home	N/A
.data[].metadata.category	Indicator.Attribute	Category	N/A	isp	N/A
.data[].metadata.country_code	Indicator.Attribute	Country Code	N/A	MX	N/A
.data[].metadata.tor	Indicator.Attribute	Is TOR	N/A	False	N/A
.data[].metadata.os	Indicator.Attribute	Operating System	N/A	Windows 7/8	N/A
.data[].metadata.organization	Indicator.Attribute	Organization	N/A	TOTAL PLAY TELECOMUNICACIONES SA DE CV	N/A
.data[].metadata.rdns	Indicator	FQDN	N/A	fixed-187-190-49-92.totalplay.net	N/A
.data[].metadata.asn	Indicator.Attribute	ASN	N/A	AS22884	N/A
.data[].metadata.city	Indicator.Attribute	City	N/A	Puebla	N/A
.data[].metadata.country	Indicator.Attribute	Country	N/A	Mexico	N/A

Example


Reverse DNS
VALUE
TYPE
Start typing...
Start typing...
fixed-187-190-49-92.totalplay.net
FQDN
Add Selected Indicators
Context
Showing 1 to 13 of 13
Row count: 25
NAME
VALUE
Start typing...
Start typing...
Last Seen
2019-12-22
First Seen
2019-12-05
Tag
SMB Scanner
Tag
Eternalblue
Country
Mexico
Is TOR
False
Organization
TOTAL PLAY TELECOMUNICACIONES SA DE CV
Operating System
Windows 7/8
ASN
AS22884
Country Code
MX
Category
isp
City
Puebla
Seen
True
Add Selected Attributes
Scanning Metadata
NAME
VALUE
Start typing...
Start typing...
Scanned Port
445
Add Selected Attributes

Change Log

- **Version 1.0.0**
  - Initial release