ThreatQuotient

GreyNoise Operation Guide

Version 1.1.0

May 30, 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.

Copyright © 2023 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.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.1.0
Compatible with ThreatQ Versions	>= 4.0.0
Support Tier	ThreatQ Supported

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.

The GreyNoise Operation provides the following action:

- **Query** - queries GreyNoise for any metadata, including reverse DNS, tags, geolocation, and scanned paths/ports.
- **Find Similar IPs** - queries GreyNoise to find similar IP Addresses.
- **Get Timeline** - queries GreyNoise to get an IP's recent timeline events.

The operation is compatible with the IP Address type 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 operation already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the operation 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.

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

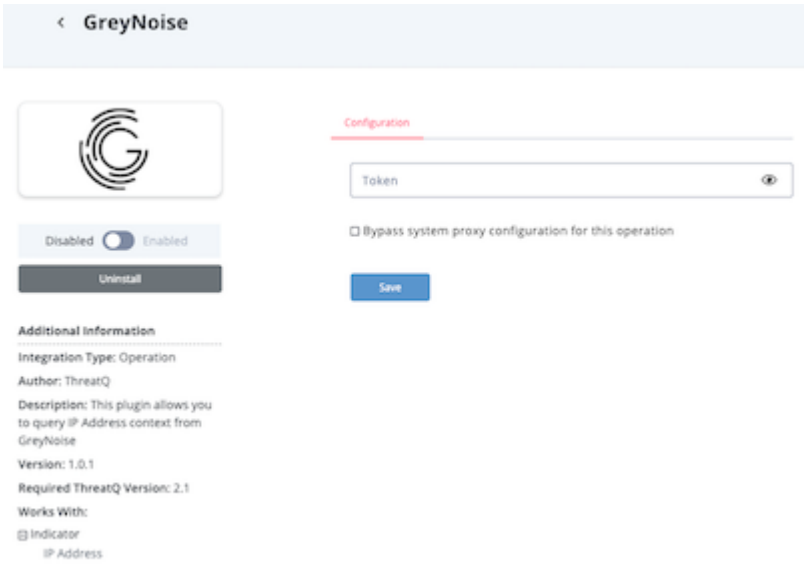
Configuration

> 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 **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Token	Your GreyNoise API Token.



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.

Actions

The operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Query	Query GreyNoise for indicator context.	Indicator	IP Address
Find Similar IPs	Query GreyNoise to find similar IP Addresses.	Indicator	IP Address
Get Timeline	Query GreyNoice to get an IP's recent timeline entries.	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`

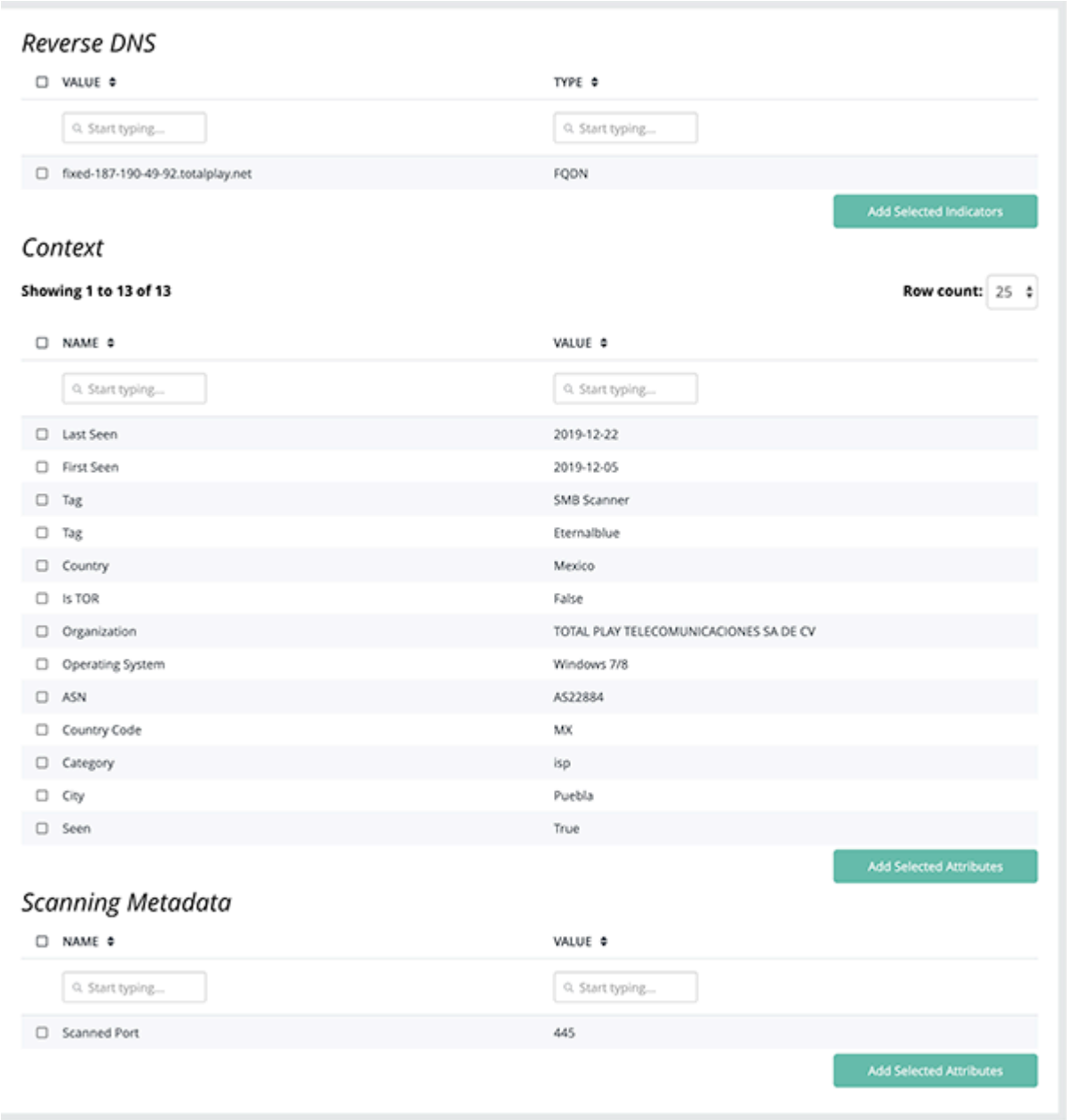
Sample Response:


```
{
    "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"
}
```

ThreatQuotient 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 Output



Find Similar IPs

The Find Similar IPs action will query GreyNoise for similar IPs to the top-level IP Address. The results will display the similarity score as well as attribution contributing to the similarity score.

```
GET https://api.greynoise.io/v3/similarity/ips/{ip}
```

Sample Response:


```
{
    "ip": {
        "ip": "182.138.158.171",
        "actor": "unknown",
        "classification": "malicious",
        "first_seen": "2017-10-13",
        "last_seen": "2023-05-22",
        "asn": "AS4134",
        "city": "Shenzhen",
        "country": "China",
        "country_code": "CN",
        "organization": "CHINANET-BACKBONE"
    },
    "similar_ips": [
        {
            "ip": "122.96.28.15",
            "score": 0.93768877,
            "features": [
                "ja3_fp",
                "mass_scan_bool",
                "os",
                "ports",
                "web_paths"
            ],
            "actor": "unknown",
            "classification": "malicious",
            "first_seen": "2017-10-18",
            "last_seen": "2023-05-24",
            "asn": "AS4837",
            "city": "Shenzhen",
            "country": "China",
            "country_code": "CN",
            "organization": "CHINA UNICOM China169 Backbone"
        }
    ],
    "total": 2575}
```

ThreatQ provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.ip.first_seen	Indicator.Attribute	First Seen	N/A	2017-10-13	N/A
.ip.actor	Indicator.Attribute	Actor	N/A	unknown	N/A
.ip.last_seen	Indicator.Attribute	Last Seen	N/A	2023-05-22	N/A
.ip.classification	Indicator.Attribute	Classification	N/A	malicious	N/A
.ip.country_code	Indicator.Attribute	Country Code	N/A	CN	N/A
.ip.organization	Indicator.Attribute	Organization	N/A	CHINANET-BACKBONE	N/A
.ip.asn	Indicator.Attribute	ASN	N/A	AS4134	AS is stripped so it's just the number
.ip.city	Indicator.Attribute	City	N/A	Shenzhen	N/A
.ip.country	Indicator.Attribute	Country	N/A	China	N/A
.similar_ips[].ip	Indicator.Value	IP Address	N/A	122.96.28.15	N/A
.similar_ips[].first_seen	Indicator.Attribute	First Seen	N/A	2017-10-18	N/A
.similar_ips[].actor	Indicator.Attribute	Actor	N/A	unknown	N/A
.similar_ips[].classification	Indicator.Attribute	Classification	N/A	malicious	N/A
.similar_ips[].organization	Indicator.Attribute	Organization	N/A	CHINA UNICOM China169 Backbone	N/A
.similar_ips[].asn	Indicator.Attribute	ASN	N/A	AS4837	AS is stripped so it's just the number
.similar_ips[].city	Indicator.Attribute	City	N/A	CN	N/A
.similar_ips[].country	Indicator.Attribute	Country	N/A	China	N/A

Get Timeline

The Get Timeline action queries GreyNoise to get an IP's most recently timeline of events.

`GET https://api.greynoise.io/v3/noise/ips/{ip}/daily-summary`

JSON response sample:


```
{
  "activity": [
    {
      "timestamp": "2023-04-16T00:00:00Z",
      "country": "China",
      "country_code": "CN",
      "asn": "AS4134",
      "region": "Sichuan",
      "city": "Chengdu",
      "category": "isp",
      "rdns": "",
      "organization": "CHINANET-BACKBONE",
      "vpn": false,
      "vpn_service": "",
      "tor": false,
      "spoofable": true,
      "destinations": [
        {
          "country": "",
          "country_code": ""
        },
        {
          "country": "China",
          "country_code": "CN"
        }
      ],
      "protocols": [
        {
          "transport_protocol": "TCP",
          "port": 1701
        },
        {
          "transport_protocol": "TCP",
          "port": 993
        }
      ],
      "classification": "malicious",
      "tags": [
        {
          "name": "SSH Bruteforcer",
          "description": "IP addresses with this tag have been observed attempting to bruteforce SSH server
credentials.",
          "category": "worm",
          "intention": "malicious"
        },
        {
          "name": "Web Crawler",
          "description": "IP addresses with this tag have been seen crawling HTTP(S) servers around the Internet.",
```

```
          "category": "activity",
          "intention": "unknown"
        }
      ],
      "ja3_fingerprints": [
        "89be98bbd4f065fe510fca4893cf8d9b"
      ],
      "hassh_fingerprints": [],
      "http_paths": [],
      "http_user_agents": []
    }
  ],
  "metadata": {
    "start_time": "2023-04-16T00:00:00Z",
    "end_time": "2023-04-17T17:31:55.610977383Z",
    "ip": "182.138.158.171",
    "limit": 100,
    "next_cursor": ""
  }
}
```

Change Log

- **Version 1.1.0**
  - Added two new actions: **Find Similar IPs** and **Get Timeline**.
- **Version 1.0.1**
  - Fixed an issue where users received a timeout error when using a system proxy.
- **Version 1.0.0**
  - Initial release