ThreatQuotient

GreyNoise Community Operation Guide

Version 1.1.0

July 12, 2022

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

Not Actively Supported

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 **Not Actively Supported**.

Integrations, apps, and add-ons designated as **Not Actively Supported** are not supported by ThreatQuotient's Customer Support team.

While you can report issues to ThreatQ's Customer Support team regarding the integration/app/add-on, you are solely responsible for ensuring proper functionality and version compatibility of Not Supported designations with the applicable ThreatQuotient software.

If unresolvable functional or compatibility issues are encountered, you may be required to uninstall the integration/app/add-on from your ThreatQuotient environment in order for ThreatQuotient to fulfill support obligations.

> ⚠ For ThreatQuotient Hosted instance customers, the Service Level Commitment and Service Level Credit in the ThreatQuotient Service Level Schedule will not apply to issues caused by Not Actively Supported integrations/apps/add-ons.

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	Not Actively Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/greynoise-community-operation

Introduction

The GreyNoise Community operation provides you with the ability to query info about an IP address from GreyNoise's Community API.

The operation is compatible with IP Address-type indicators and provides the following action:

- **Query** - queries for info about an IP address from GreyNoise's Community API.

See the Actions chapter for more information on this action.

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 **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 Key	A GreyNoise API Key that will allow a high rate limit.

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 GreyNoise Community operation provides the following action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Query	Queries for info about an IP address from GreyNoise's Community API.	Indicator	IP Address

Query

The Query action queries for info on a specific IP address. The data returned is a flat JSON object as demonstrated in the sample response below.

```
<GET> https://api.greynoise.io/v3/community/<IP ADDRESS>
```

Sample Response:

```
{
  "ip": "8.8.8.8",
  "noise": false,
  "riot": true,
  "classification": "benign",
  "name": "Google Public DNS",
  "link": "https://viz.greynoise.io/riot/8.8.8.8",
  "last_seen": "2021-05-13",
  "message": "Success"
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
noise	Indicator.Attribute	Noise	N/A	False	N/A
riot	Indicator.Attribute	RIOT	N/A	True	Stands for Rule It Out
classification	Indicator.Attribute	Classification	N/A	benign	N/A
name	Indicator.Attribute	Name	N/A	Google Public DNS	N/A
link	Indicator.Attribute	Link	N/A	https://viz.greynoise.io/riot/8.8.8.8	N/A
last_seen	Indicator.Attribute	Last Seen	N/A	2021-05-13	N/A

Change Log

- **Version 1.1.0**
  - Added **API Key** parameter to the configuration section.
- **Version 1.0.0**
  - Initial release