ThreatQuotient

GreyNoise Community Action Guide

Version 1.0.3

December 06, 2022

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.

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	1.0.3
Compatible with ThreatQ Versions	>= 5.6.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/greynoise-community-action

Introduction

The GreyNoise Community Action submits a collection of FQDN and IP Addresses to the GreyNoise Community API in individual HTTP Requests. GreyNoise returns a response for each object containing any information they have about the indicator. A sample response can be found within this file.

The action can perform the following function:

- **GreyNoise Community** - enriches IP Addresses with attributes describing the observed behavior of the IP Address.

The action is compatible with the following indicator type:

- IP Address

The action returns the following enriched indicator types:

- IP Address

> This action is intended for use with ThreatQ TRD Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

The action requires the following:

- A GreyNoise API key.
- An active ThreatQ TRD Orchestrator (TQO) license.
- A data collection containing the following indicator type:
  - IP Address

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 action file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action 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 action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to configure the action.

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 **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
GreyNoise API Key	Your API Key for authentication with the GreyNoise API.
Objects Per Run	The maximum number of objects to submit per workflow run. The max value for this parameter is 50,000.
GreyNoise Context Filter	Maximum number of objects to submit per workflow run. Options include: ◦ Classification ◦ Link ◦ Last Seen ◦ Name ◦ RIOT

PARAMETER	DESCRIPTION
	◦ Noise

5. Review any additional settings, make any changes if needed, and click on **Save**.

Action Functions

The action provides the following functions

FUNCTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
GreyNoise Community	Queries the GreyNoise Community API for context	Indicator	IP Address

GreyNoise Community

GET `https://api.greynoise.io/v3/community/{{IP Address}}`

Sample Response:

```
{
    "ip": "111.121.216.118",
    "noise": true,
    "riot": false,
    "classification": "malicious",
    "name": "unknown",
    "link": "https://viz.greynoise.io/ip/111.121.216.118",
    "last_seen": "2022-12-02",
    "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
.classification	Indicator.Attribute	Classification	N/A	benign	If enabled
.name	Indicator.Attribute	Name	N/A	ShadowServer	'unknown' is ignored
.noise	Indicator.Attribute	Noise	N/A	True	If enabled
.riot	Indicator.Attribute	Riot	N/A	True	If enabled
.last_seen	Indicator.Attribute	Last Seen	N/A	True	If enabled
.link	Indicator.Attribute	Link	N/A	https://viz.greynoise.io/ip/64.62.197.2	If enabled

Enriched Data

Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	1 Minute
Indicators	50
Indicator Attributes	230

Use Case Example

1. A Threat Analyst identifies a collection of IP Addresses they would like to enrich.
2. The Threat Analyst adds the GreyNoise Community Action to a Workflow
3. The Threat Analyst configures the action with the desired parameters, and enables the Workflow
4. The Workflow executes all Actions in the graph, including GreyNoise Community
5. The action returns the documented Attributes from the provider, and the Workflow ingests this data into the ThreatQ platform.

   Example Return Results:

   ◦ 99 Indicators
   ◦ 30 Indicator Attributes

Known Issues / Limitations

- The GreyNoise Community API is limited to 50 lookups per day.

Change Log

- **Version 1.0.3**
  - Initial release on the ThreatQ Marketplace.