

ThreatQuotient



GreyNoise Action Bundle Guide

Version 1.0.0

April 18, 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

Integration Details	5
Introduction	6
Prerequisites	7
Installation	8
Configuration	9
Action Functions	11
Find Similar IPs	12
RIOT	14
IP Quick Check	15
Enriched Data	16
Find Similar IPs	16
RIOT	16
IP Quick Check	17
Use Case Example	18
Known Issues / Limitations	19
Change Log	20

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	1.0.0
Compatible with ThreatQ Versions	>= 5.12.1
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/greynoise-action-bundle

Introduction

The GreyNoise Actions for ThreatQ enables analysts to use GreyNoise Enterprise for automated enrichment and investigations.

The action bundle provides the following actions:

- **GreyNoise - Find Similar IPs** - locates similar IPs to corresponding IPs from the selected data collection.
- **GreyNoise - RIOT** - check to see if IPs within a data collection are in GreyNoise's RIOT dataset (known good services).
- **GreyNoise - IP Quick Check** - performs a quick noise check on the IPs of the selected data collection.

The action is both compatible with and returns IP Address type indicators.



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

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing 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 action bundle zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the zip file using one of the following methods:
 - Drag and drop the zip file into the dialog box
 - Select **Click to Browse** to locate the zip 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 actions.

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	API Key for authentication with the IPInfo API
Similarity Score Threshold (<i>Find Similar IPs action only</i>)	Enter a value, between 0-100, that will serve as the minimum similarity score required to ingest a similar IP Address.
Feature Match Requirements (<i>Find Similar IPs action only</i>)	Enter a comma-separated list of features that need to be matched for a similar IP Address to be ingested. <div> This parameter is case-sensitive.</div>
Similar IP Status (<i>Find Similar IPs action only</i>)	Select the status of the similar IP Addresses ingested.

PARAMETER	DESCRIPTION
Relate Similar IPs to Original IP <i>(Find Similar IPs action only)</i>	Enable this option to relate the similar IPs to the original IP Address.
RIOT IP Status <i>(IP Quick Check and RIOT actions only)</i>	Select the status of the IP Addresses that are within the RIOT dataset.
Non-RIOT IP Status <i>(IP Quick Check and RIOT actions only)</i>	Select the status of the IP Addresses that are not within the RIOT dataset.
GreyNoise Context Filter	Select Attributes for the action to ingest. Options and default selections will differ based on the action selected.
Objects Per Run	Maximum number of Objects to Submit per workflow run.



Uninstall

Additional Information
 Integration Type: Action
 Version:
 Action ID: 20
 Accepted Data Types:

Configuration

🔑

GreyNoise API Key.

Context Filter
The pieces of Context to Ingest back into ThreatQ.

☒ RIOT
 ☒ Category
 ☒ Service Name
 ☒ Trust Level
 ☐ External Reference
 ☐ Last Updated

RIOT IP Status

▼

The status of the IPs that are within the RIOT dataset.

Non-RIOT IP Status

▼

The status of the IPs that are NOT within the RIOT dataset.

Objects Per Run

The max number of objects to send to this action, per run. This number should scale with your API rate limit.

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

GreyNoise Action Bundle Guide
Version 1.0.0

10

Action Functions

The action bundle provides the following actions:

FUNCTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
GreyNoise - Find Similar IPs	Find similar IPs to corresponding IPs from the selected data collection.	Indicator	IP Address
GreyNoise - RIOT	Check if IPs in a data collection are part of the GreyNoise RIOT database (known good services)	Indicator	IP Address
GreyNoise - IP Quick Check	Quickly checks if IPs in a data collection are noise or not (also checks RIOT)	Indicator	IP Address

Find Similar IPs

The Find Similar IPs action finds similar IPs to corresponding IPs from the selected data collection, allowing you to easily uncover actor infrastructure.

GET <https://api.greynoise.io/v3/similarity/ips/{{ value }}>

Sample Response:

```
{
  "ip": {
    "ip": "52.73.169.169",
    "actor": "CyberGreen",
    "classification": "benign",
    "first_seen": "2017-09-19",
    "last_seen": "2022-11-29",
    "asn": "AS14618",
    "city": "Ashburn",
    "country": "United States",
    "country_code": "US",
    "organization": "Amazon.com, Inc."
  },
  "similar_ips": [
    {
      "ip": "67.198.237.116",
      "score": 0.82805526,
      "features": [
        "os",
        "ports",
        "rdns",
        "spoofable_bool"
      ],
      "actor": "unknown",
      "classification": "unknown",
      "first_seen": "2022-09-21",
      "last_seen": "2022-10-13",
      "asn": "AS35908",
      "city": "Los Angeles",
      "country": "United States",
      "country_code": "US",
      "organization": "Krypt Technologies"
    },
    {
      "ip": "54.36.163.223",
      "score": 0.82805526,
      "features": [
        "os",
        "ports",
        "rdns",
        "spoofable_bool"
      ],
      "actor": "unknown",
      "classification": "unknown",
      "first_seen": "2021-07-05",
      "last_seen": "2022-10-19",
      "asn": "AS16276",

```

```

    "city": "Redbridge",
    "country": "United Kingdom",
    "country_code": "GB",
    "organization": "OVH SAS"
  }
],
"total": 68
}

```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.similar_ips[].ip	Indicator.Value	IP Address	N/A	67.198.237.116	N/A
.similar_ips[].first_seen	Indicator.Attribute	First Seen	N/A	2022-09-21	N/A
.similar_ips[].actor	Indicator.Attribute	Actor	N/A	unknown	N/A
.similar_ips[].last_seen	Indicator.Attribute	Last Seen	N/A	2022-10-13	N/A
.similar_ips[].classification	Indicator.Attribute	Classification	N/A	unknown	N/A
.similar_ips[].organization	Indicator.Attribute	Organization	N/A	Krypt Technologies	N/A
.similar_ips[].asn	Indicator.Attribute	ASN	N/A	35908	AS is stripped so it's just the number
.similar_ips[].city	Indicator.Attribute	City	N/A	Los Angeles	N/A
.similar_ips[].country	Indicator.Attribute	Country	N/A	United States	N/A
.similar_ips[].country_code	Indicator.Attribute	Country Code	N/A	US	N/A

RIOT

The RIOT action checks IPs to see if they are within GreyNoise's RIOT dataset (a known benign service) and retrieves context information from GreyNoise to be ingested.

GET `https://api.greynoise.io/v2/riot/{{ value }}`

Sample Response:

```
{
  "ip": "1.1.1.1",
  "riot": true,
  "category": "public_dns",
  "name": "Cloudflare Public DNS",
  "description": "Cloudflare, Inc. is an American web infrastructure and website security company, providing content delivery network (CDN) services, distributed denial of service (DDoS) mitigation, Internet security, and distributed domain name system (DNS) services. This is their public DNS offering.",
  "explanation": "Public DNS services are used as alternatives to ISP's name servers. You may see devices on your network communicating with Cloudflare Public DNS over port 53/TCP or 53/UDP to resolve DNS lookups.",
  "last_updated": "2023-01-12T17:11:04Z",
  "reference": "https://one.one.one.one",
  "trust_level": "1"
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.ip	Indicator.Value	IP Address	N/A	1.1.1.1	N/A
.riot	Indicator.Attribute	RIOT	N/A	true	N/A
.category	Indicator.Attribute	Category	N/A	public_dns	N/A
.name	Indicator.Attribute	Service Name	N/A	Cloudflare Public DNS	N/A
.last_updated	Indicator.Attribute	Last Updated	N/A	2023-01-12T17:11:04Z	N/A
.reference	Indicator.Attribute	External Reference	N/A	https://one.one.one.one	N/A
.trust_level	Indicator.Attribute	Trust Level	N/A	1	N/A

IP Quick Check

This action checks IPs to see if they are within GreyNoise's RIOT dataset (a known benign service).

GET `https://api.greynoise.io/v2/noise/quick/{{ value }}`

Sample Response:

```
{
  "ip": "12.199.79.244",
  "noise": true,
  "riot": false,
  "code": "0x01"
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.ip	Indicator.Value	IP Address	N/A	12.199.79.244	N/A
.riot	Indicator.Attribute	RIOT	N/A	true	N/A
.noise	Indicator.Attribute	Noise	N/A	true	N/A
.code	Indicator.Attribute	Noise Code	N/A	0x01 - The IP has been observed by the GreyNoise sensor network	N/A

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.

Find Similar IPs

METRIC	RESULT
Run Time	1 minute
Indicators	395
Indicator Attributes	1,397

RIOT

METRIC	RESULT
Run Time	1 minute
Indicators	25
Indicator Attributes	121

IP Quick Check

METRIC	RESULT
Run Time	1 minute
Indicators	25
Indicator Attributes	73

Use Case Example

- **Find Similar IPs** - you have a list of known IPs from a bad actor, and want to find similar IPs to uncover previously unknown actor infrastructure to proactively prevent future attacks.
- **RIOT** - you have a list of IPs and are unsure if they are malicious or benign. You would use the RIOT endpoint to see if any of the IPs are known good (benign).
- **IP Quick Check** - you have a list of IPs and want to see if any of them have been observed scanning or attacking devices on the internet.

Known Issues / Limitations

- A maximum of 100 similar indicators can be brought back per IOC in your data collection.

Change Log

- Version 1.0.0
 - Initial release