ThreatQuotient

GreyNoise Action Bundle

Version 1.1.0

September 04, 2024

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	1.1.0
Compatible with ThreatQ Versions	>= 5.12.1
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The GreyNoise Action Bundle 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.
- **GreyNoise - CVE Enrichment** - enriches selected CVEs with GreyNoise data.
- **GreyNoise - IP Context** - enriches select IPs with GreyNoise's full contextual data.

The integration is both compatible with and returns IP Address type indicators. Additionally, the GreyNoise - CVE Enrichment action is also compatible and enriches CVE type indicators and vulnerabilities.

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:
  - All actions except the CVE Enrichment action - IP Address type indicators.
  - The GreyNoise CVE Enrichment action - CVE type indicators and Vulnerability objects

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
6. Select the actions to install, when prompted, and click on the **Install** button.

   > 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.

   The action(s) have been installed on your ThreatQ instance. You will still need to configure the action(s).

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:

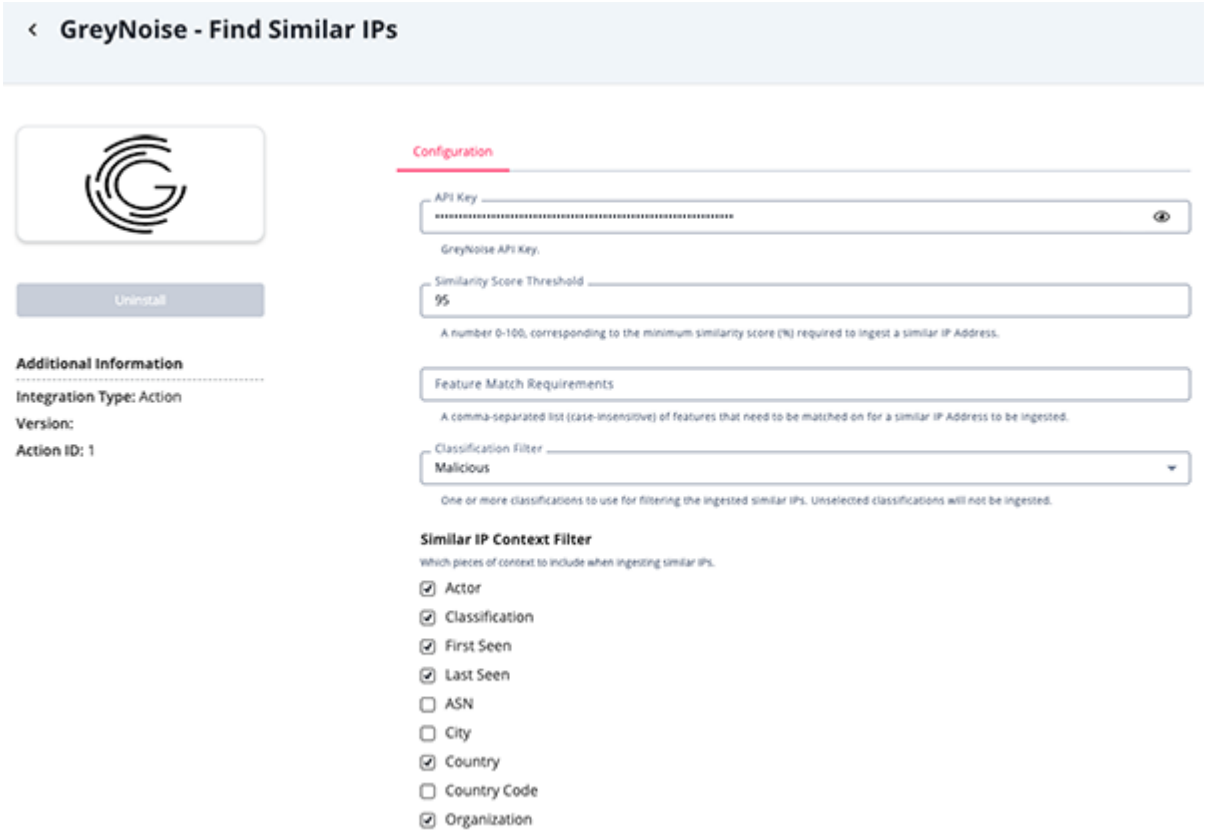
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> 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.

Find Similar IPs Parameters

PARAMETER	DESCRIPTION
GreyNoise API Key	API Key for authentication with the IPInfo API
Similarity Score Threshold	Enter a value, between 0-100, that will serve as the minimum similarity score required to ingest a similar IP Address.
Feature Match Requirements	Enter a comma-separated list of features that need to be matched for a similar IP Address to be ingested. ⚠ This parameter is **case-sensitive**.
Classification Filter	Select one or more classifications to use for filtering the ingested similar IPs. Options include: ◦ Malicious ◦ Unknown ◦ Benign

PARAMETER	DESCRIPTION
	 Unselected classifications will not be ingested.
Similar IP Context Filter	Select the context to include when ingesting similar IPs. Options include: ◦ Actor ◦ Classification ◦ First Seen ◦ Last Seen ◦ ASN ◦ City ◦ Country ◦ Country Code ◦ Organization
Similar IP Status	Select the status of the similar IP Addresses ingested. Options include: ◦ Indirect ◦ Review ◦ Active ◦ Whitelisted
Relate Similar IPs to Original IP	Enable this option to relate the similar IPs to the original IP Address.
Objects Per Run	Maximum number of Objects to Submit per workflow run.
Disable Proxies	Enable this option to have the action ignore proxies settings set in the ThreatQ UI.
Enable SSL Verification	Enable this option to verify the provider's SSL certificate.

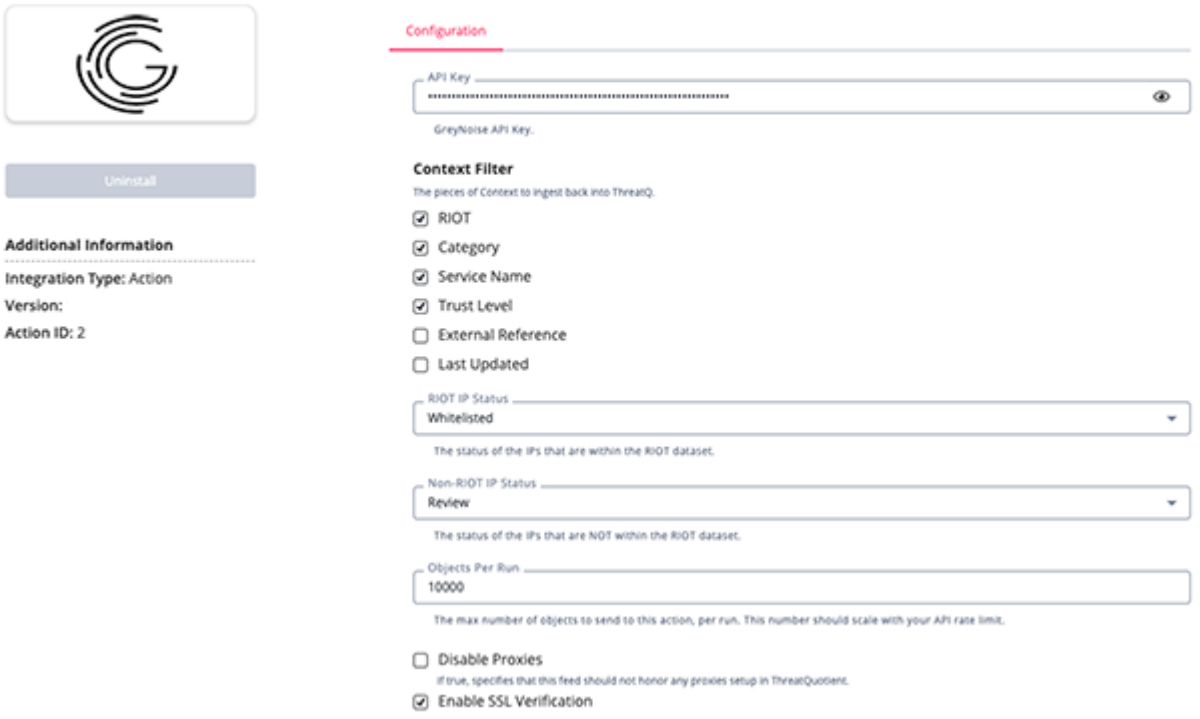


RIOT Parameters

PARAMETER	DESCRIPTION
GreyNoise API Key	API Key for authentication with the IPInfo API
Context Filter	Select the pieces of Context to ingest back into ThreatQ. Options include: ◦ RIOT ◦ Category ◦ Service Name ◦ Trust Level ◦ External Reference ◦ Last Updated
RIOT IP Status	Select the status of the IP Addresses that are within the RIOT dataset. Options include: ◦ Whitelisted ◦ Review

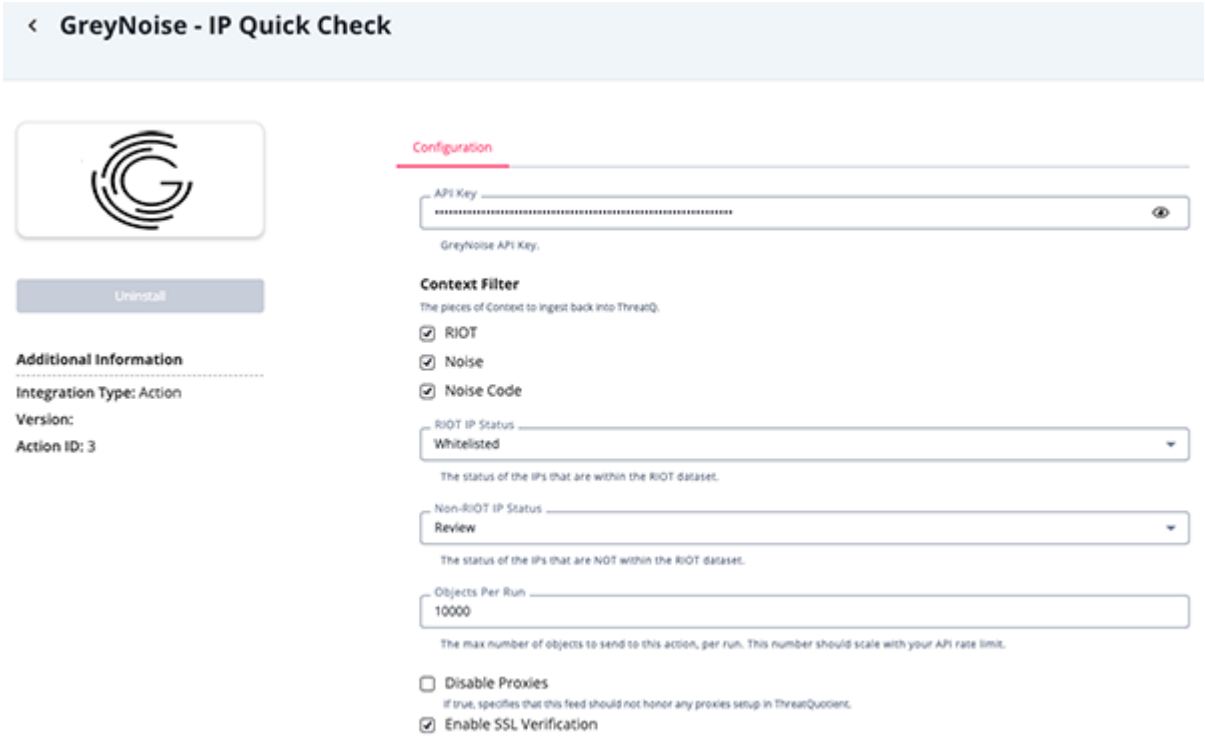
PARAMETER	DESCRIPTION
	◦ Active
Non-RIOT IP Status	Select the status of the IP Addresses that are not within the RIOT dataset. Options include: ◦ Whitelisted ◦ Review ◦ Active
Objects Per Run	Maximum number of Objects to Submit per workflow run.
Disable Proxies	Enable this option to have the action ignore proxies settings set in the ThreatQ UI.
Enable SSL Verification	Enable this option to verify the provider's SSL certificate.

GreyNoise - RIOT



IP Quick Check Parameters

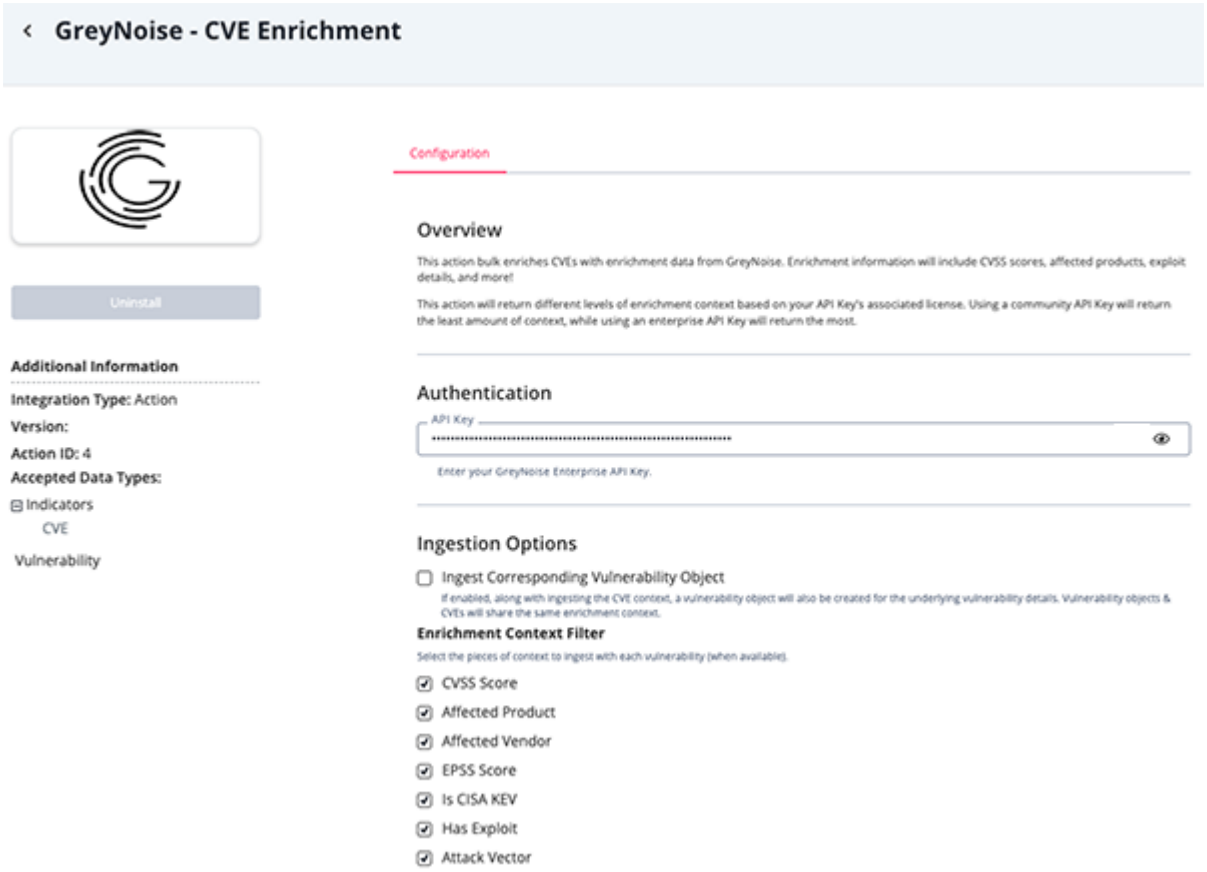
PARAMETER	DESCRIPTION
GreyNoise API Key	API Key for authentication with the IPInfo API
Context Filter	Select the pieces of Context to ingest back into ThreatQ. Options include: ◦ RIOT ◦ Noise ◦ Noise Code
RIOT IP Status	Select the status of the IP Addresses that are within the RIOT dataset. Options include: ◦ Whitelisted ◦ Review ◦ Active
Non-RIOT IP Status	Select the status of the IP Addresses that are not within the RIOT dataset. Options include: ◦ Whitelisted ◦ Review ◦ Active
Objects Per Run	Maximum number of Objects to Submit per workflow run.
Disable Proxies	Enable this option to have the action ignore proxies settings set in the ThreatQ UI.
Enable SSL Verification	Enable this option to verify the provider's SSL certificate.



CVE Enrichment Parameters

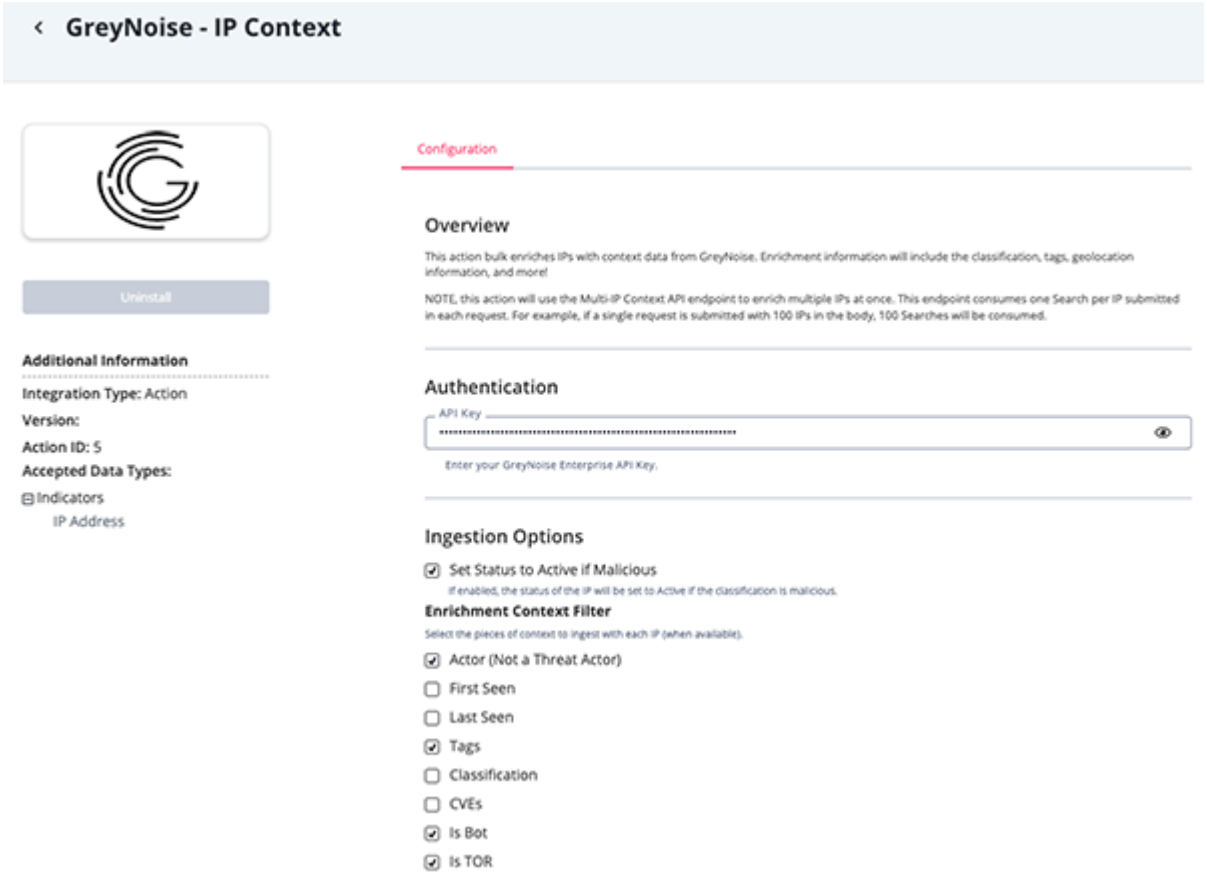
PARAMETER	DESCRIPTION
GreyNoise API Key	API Key for authentication with the IPInfo API
Ingest Corresponding Vulnerability Object	If enabled, along with ingesting the CVE context, a vulnerability object will also be created for the underlying vulnerability details. Vulnerability objects & CVEs will share the same enrichment context. If it's not enabled, `Vulnerability Name` attribute is created for the CVE.
Enrichment Context Filter	Select the pieces of context to ingest with each vulnerability (when available). Options include: ◦ CVSS Score (default) ◦ Affected Product (default) ◦ Is CISA KEV (default) ◦ Has Exploit (default) ◦ Attack Vector (default)

PARAMETER	DESCRIPTION
	◦ Affected Vendor (default) ◦ EPSS Score (default)
Objects Per Run	Maximum number of Objects to Submit per workflow run.
Disable Proxies	Enable this option to have the action ignore proxies settings set in the ThreatQ UI.
Enable SSL Verification	Enable this option to verify the provider's SSL certificate.



IP Context Parameters

PARAMETER	DESCRIPTION
GreyNoise API Key	API Key for authentication with the IPInfo API
Set Status to Active If Malicious	Enter a value, between 0-100, that will serve as the minimum similarity score required to ingest a similar IP Address.
Enrichment Context Filter	Select the pieces of context to ingest with each vulnerability (when available). Options include: ◦ Actor (Not a Threat Actor) ◦ First Seen ◦ Last Seen ◦ Tags ◦ Classification ◦ CVEs ◦ Is Bot ◦ Is TOR ◦ Is VPN ◦ VPN Service ◦ ASN ◦ City ◦ Country ◦ Country Code ◦ Region ◦ Organization ◦ Category ◦ Operating System ◦ Destination Country ◦ Destination Country Code ◦ Source Country ◦ Source Country Code ◦ RDNS
Objects Per Run	Maximum number of Objects to Submit per workflow run.
Disable Proxies	Enable this option to have the action ignore proxies settings set in the ThreatQ UI.
Enable SSL Verification	Enable this option to verify the provider's SSL certificate.



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

Actions

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
GreyNoise - CVE Enrichment	Enriches CVEs with GreyNoise data	Indicator, Vulnerability	Indicator - CVE
GreyNoise - IP Context	Enriches IPs with GreyNoise's full contextual data	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

The GreyNoise - IP Quick Check 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

CVE Enrichment

The GreyNoise - CVE Enrichment action performs CVE ID lookups to enrich CVEs with GreyNoise data.

`GET https://api.greynoise.io/v1/cve/{{ cve_id }}`

Sample Response:


```
{
  "id": "CVE-2024-23897",
  "details": {
    "vulnerability_name": "Jenkins Command Line Interface (CLI) Path Traversal
Vulnerability",
    "vulnerability_description": "Jenkins 2.441 and earlier, LTS 2.426.2 and
earlier does not disable a feature of its CLI command parser that replaces an
'@' character followed by a file path in an argument with the file's contents,
allowing unauthenticated attackers to read arbitrary files on the Jenkins
controller file system.",
    "cve_cvss_score": 9.8,
    "product": "Jenkins Command Line Interface (CLI)",
    "vendor": "Jenkins",
    "published_to_nist_nvd": true
  },
  "timeline": {
    "cve_published_date": "2024-01-24T18:15:09Z",
    "cve_last_updated_date": "2024-05-14T15:01:24Z",
    "first_known_published_date": "2024-01-30T00:00:00Z",
    "cisa_kev_date_added": "2024-08-19T00:00:00Z"
  },
  "exploitation_details": {
    "attack_vector": "NETWORK",
    "exploit_found": true,
    "exploitation_registered_in_kev": true,
    "epss_score": 0.97225
  },
  "exploitation_stats": {
    "number_of_available_exploits": 48,
    "number_of_threat_actors_exploiting_vulnerability": 2,
    "number_of_botnets_exploiting_vulnerability": 0
  },
  "exploitation_activity": {
    "activity_seen": false,
    "benign_ip_count_1d": 0,
    "benign_ip_count_10d": 0,
    "benign_ip_count_30d": 0,
    "threat_ip_count_1d": 0,
    "threat_ip_count_10d": 0,
    "threat_ip_count_30d": 0
  }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.details.vulnerability_name`	Vulnerability Value	N/A	`.timeline.cve_published_date`	`Jenkins Command Line Interface (CLI) Path Traversal Vulnerability`	User-configurable;
`.details.vulnerability_name`	Indicator Attribute	`Vulnerability Name`	`.timeline.cve_published_date`	`Jenkins Command Line Interface (CLI) Path Traversal Vulnerability`	If `Ingest Corresponding Vulnerability Object` is unchecked;
`exploited`	Indicator/ Vulnerability TAG	N/A	`.timeline.cve_published_date`	`exploited`	If `.exploitation_details.exploitation_registered_in_kev` or `.exploitation_details.exploit_found` is True
`.details.cve_cvss_score`	Indicator/ Vulnerability Attribute	`CVSS Score`	`.timeline.cve_published_date`	`9.8`	Updatable; User-configurable;
`.details.product`	Indicator/ Vulnerability Attribute	`Affected Product`	`.timeline.cve_published_date`	`Jenkins Command Line Interface (CLI)`	User-configurable;
`.details.vendor`	Indicator/ Vulnerability Attribute	`Affected Vendor`	`.timeline.cve_published_date`	`Jenkins`	User-configurable;
`.exploitation_details.attack_vector`	Indicator/ Vulnerability Attribute	`Attack Vector`	`.timeline.cve_published_date`	`NETWORK`	User-configurable;
`.exploitation_details.exploit_found`	Indicator/ Vulnerability Attribute	`Has Exploit`	`.timeline.cve_published_date`	`true`	Updatable; User-configurable;
`.exploitation_details.exploitation_registered_in_kev`	Indicator/ Vulnerability Attribute	`Is CISA KEV`	`.timeline.cve_published_date`	`true`	Updatable; User-configurable;
`.exploitation_details.epss_score`	Indicator/ Vulnerability Attribute	`EPSS Score`	`.timeline.cve_published_date`	`0.97225`	Updatable; User-configurable;
`.timeline.*`, `.exploitation_stats.*`, `.exploitation_activity.*`	Indicator/ Vulnerability Description	N/A	N/A	N/A	Various fields concatenated to build description HTML

IP Context

The GreyNoise - IP Context action enriches IPs with GreyNoise's full contextual data such as geolocation information and classification.

`POST https://api.greynoise.io/v2/noise/multi/context`

Sample Response:


```
{
  "data": [
    {
      "actor": "unknown",
      "bot": false,
      "classification": "malicious",
      "cve": [],
      "first_seen": "2024-08-19",
      "ip": "45.63.52.184",
      "last_seen": "2024-08-19",
      "metadata": {
        "asn": "AS20473",
        "category": "hosting",
        "city": "Los Angeles",
        "country": "United States",
        "country_code": "US",
        "destination_countries": ["Canada"],
        "destination_country_codes": ["CA"],
        "organization": "The Constant Company, LLC",
        "os": "",
        "rdns": "45.63.52.184.vultrusercontent.com",
        "region": "California",
        "sensor_count": 1,
        "sensor_hits": 5,
        "source_country": "United States",
        "source_country_code": "US",
        "tor": false
      },
      "published_at": "2024-08-19 00:00:00+00:00",
      "raw_data": {
        "hassh": [],
        "ja3": [],
        "scan": [
          {
            "port": 983,
            "protocol": "TCP"
          }
        ],
        "web": {}
      },
      "seen": true,
```

```
      "spoofable": true,
      "tags": [],
      "vpn": false,
      "vpn_service": ""
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.actor	Attribute	Actor	.first_seen	Alpha Strike Labs	User-configurable; Not a threat actor
.bot	Attribute	Is Bot	.first_seen	false	Updatable; User-configurable;
.classification	Attribute	Classification	.first_seen	malicious	Updatable; User-configurable;
.cve[]	Indicator.Value, Vulnerability.Value	CVE	.first_seen	false	User-configurable; Ingested entitiy depends on user configuration
.first_seen	Attribute	First Seen	.first_seen	2024-08-15	User-configurable;
.last_seen	Attribute	Last Seen	.first_seen	2024-08-19	Updatable; User-configurable;
.tags[]	Tag	N/A	N/A	Mirai	User-configurable;
.vpn	Attribute	Is VPN	.first_seen	false	Updatable; User-configurable;
.vpn_service	Attribute	VPN Service	.first_seen	N/A	User-configurable;
.metadata.asn	Attribute	ASN	.first_seen	AS123456	User-configurable;
.metadata.rdns	Attribute	RDNS	.first_seen	45.63.52.184.vultrusercontent.com	User-configurable;
.metadata.category	Attribute	Category	.first_seen	Hosting	User-configurable;
.metadata.city	Attribute	City	.first_seen	New York	User-configurable;
.metadata.country	Attribute	Country	.first_seen	United States	User-configurable;
.metadata.country_code	Attribute	Country Code	.first_seen	US	User-configurable;
.metadata.destination_countries[]	Attribute	Destination Country	.first_seen	Russia	User-configurable;
.metadata.destination_country_codes[]	Attribute	Destination Country Code	.first_seen	RU	User-configurable;

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.metadata.organization`	Attribute	`Organization`	`.first_seen`	`Podaon SIA`	User-configurable;
`.metadata.os`	Attribute	`Operating System`	`.first_seen`	N/A	User-configurable;
`.metadata.region`	Attribute	`Region`	`.first_seen`	`North Holland`	User-configurable;
`.metadata.source_country`	Attribute	`Source Country`	`.first_seen`	`Netherlands`	User-configurable;
`.metadata.source_country_code`	Attribute	`Source Country Code`	`.first_seen`	`NL`	User-configurable;
`.metadata.tor`	Attribute	`Is TOR`	`.first_seen`	`true`	Updatable; User-configurable;
`.raw_data.scan.port`, `.raw_data.scan.protocol`, `raw_data.web.paths`	Description	N/A	`.first_seen`	N/A	Value created with multiple response data

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

CVE Enrichment

METRIC	RESULT
Run Time	1 minute
Indicators	5
Indicator Attributes	35
Vulnerabilities	4
Vulnerability Attributes	29

IP Context

METRIC	RESULT
Run Time	1 minute
Indicators	9
Indicator Attributes	163

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).
- I**P 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.
- **CVE Enrichment** - you have a list of CVEs and want to enrich them with additional context from GreyNoise to better understand the risk associated with each CVE.
- **IP Context** - you have a list of IPs and want to enrich them with additional context from GreyNoise to better understand whether or not they are just noise or are actually malicious.

Known Issues / Limitations

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

Change Log

- **Version 1.1.0**
  - Added two new actions: **GreyNoise CVE Enrichment** and **GreyNoise IP Context**.
  - Added the follow configuration options to all actions:
    - **Disable Proxies** - enable this option to have the action ignore proxy settings set in the ThreatQ UI.
    - **Enable SSL Verification** - enable this option to verify the provider's SSL certificate.
- **Version 1.0.0**
  - Initial release