ThreatQuotient

A Securonix Company

CCN CERT Reyes Operation

Version 1.0.0

July 22, 2025

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	1.0.0
Compatible with ThreatQ Versions	>= 5.21.0
Support Tier	ThreatQ Supported

Introduction

The CCN CERT Reyes operation enriches data in the ThreatQ platform that has been ingested from CCN CERT Reyes search endpoints.

The integration provides the following action:

- **Enrich** - submits the selected indicator for enrichment using the CCN CERT Reyes API.

The integration is with compatible with the following indicator types:

- FQDN
- IP Address
- URL

Prerequisites

The following is required to run the integration:

- Reyes Hostname
- Reyes API Key
- Reyes Client Certificate in PEM format
- Reyes Client Certificate Key

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.

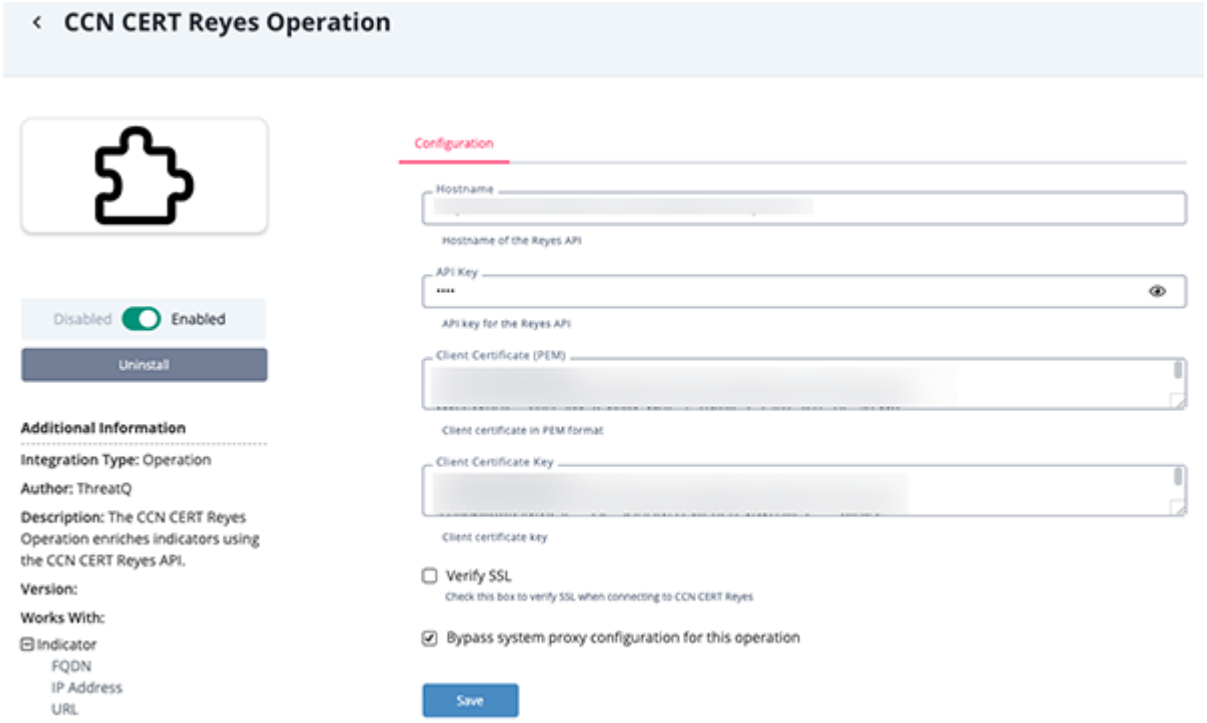
Configuration

> 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 parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Hostname	Enter the hostname for the Reyes API.
API Key	Enter your API Key.
Client Certificate (PEM)	Enter client certificate in **PEM** format.
Client Certificate Key	Enter the client certificate key.
Verify SSL	Enable this parameter if the operation should validate the host-provided SSL certificate.
Bypass system proxy configuration for this operation	Enable this parameter to bypass proxy settings set in the ThreatQ UI.



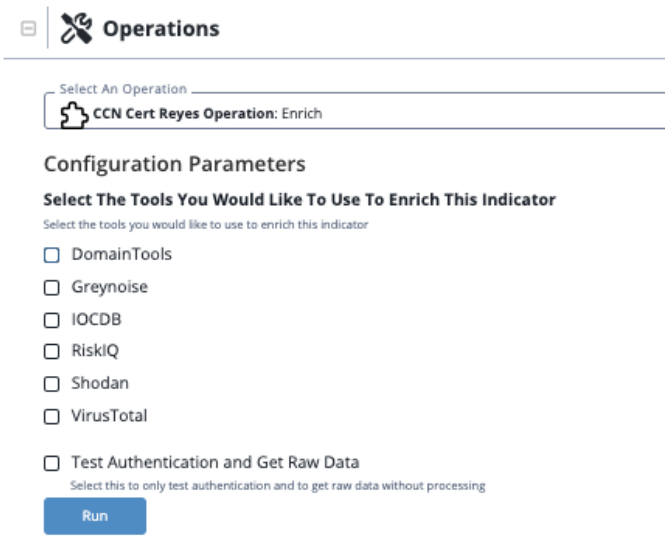
5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

The CCN CERT Reyes operation provides a single action, **Enrich**, which queries a user-selected tool for object enrichment. You will be prompted to select which tool to use after you have selected the operation for an object. In addition to selecting an enrichment tool, you can also enable the **Test Authentication and Get Raw Data** parameter to test the authentication and retrieve raw data without processing.

Tool options, and the indicator types their support, are as follows:

TOOL	OBJECT TYPES	OBJECT SUBTYPES
DomainTools	Indicator	FQDN, IP Address
GreyNoise	Indicator	IP Address
Intel CTR	Indicator	IP Address
RiskIQ	Indicator	FQDN, IP Address
Shodan	Indicator	FQDN, IP Address
VirusTotal	Indicator	FQDN, IP Address, URL



Enrich - DomainTools

The DomainTools tool option for the Enrich action supports FQDN and IP Address type indicators.

FQDN

`GET {HOSTNAME}/apireyes/api/v4/search/tool/domain-tools?domain:infomanage28391.cfd`

Sample Response:


```
{
    "success": true,
    "data": {
        "infomanage28391.cfd": {
            "ip": [
                {
                    "value": "172.67.212.97",
                    "lastResolved": "2024-11-25T03:29:05.000Z"
                },
                {
                    "value": "104.21.61.171",
                    "lastResolved": "2024-11-25T03:29:05.000Z"
                }
            ],
            "whoIsDomainItem": {
                "auditUpdateDate": "2024-11-25T03:29:05.000Z",
                "createdDate": "2024-09-12T02:00:00.000Z",
                "dataObject": {
                    "createdDate": "2024-09-12",
                    "updatedDate": "2024-11-25T02:29:05.984000",
                    "expiresDate": "2025-09-12",
                    "registrant": {
                        "countryCode": "US",
                        "organization": "Global Domain Group Privacy Service",
                        "state": "California",
                        "name": ""
                    },
                    "registrantContact": {},
                    "technicalContact": {
                        "countryCode": "",
                        "city": "",
                        "organization": "",
                        "state": "",
                        "email": "please query the rdds service of the registrar of record identified in this output for information on how to contact the registrant, admin, or tech contact of the queried domain name.",
                        "name": ""
                    },
```

```
                    "domainName": "infomanage28391.cfd",
                    "nameServers": [
                        "ARIELLA.NS.CLOUDFLARE.COM",
                        "NOEL.NS.CLOUDFLARE.COM"
                    ],
                    "active": false,
                    "status": [
                        "addperiod",
                        "clienttransferprohibited",
                        "servertransferprohibited"
                    ],
                    "parseCode": 0,
                    "audit": {},
                    "registrarName": "Global Domain Group LLC",
                    "registryData": {
                        "parseCode": 0
                    },
                    "estimatedDomainAge": 0,
                    "ipLocation": "US",
                    "isp": "CloudFlare Inc.",
                    "ipAddress": "172.67.212.97",
                    "asn": "AS13335",
                    "billingContact": {},
                    "zoneContact": {},
                    "administrativeContact": {
                        "countryCode": "",
                        "city": "",
                        "state": "",
                        "email": "please query the rdds service of the
registrar of record identified in this output for information on how to contact
the registrant, admin, or tech contact of the queried domain name.",
                        "name": ""
                    }
                },
                "historyObject": []
            }
        }
    },
    "error": [
        null
    ]
}
```

ThreatQuotient provides the following default mapping for FQDN objects using the DomainTools tool based on `.data.<fqdn_value>.domain` entry.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.ip[].value	Related Indicator.Value	IP Address	N/A	172.67.212.97	N/A
.whoIsDomainItem.dataObject.registrant.organization	Attribute	Organization	N/A	Global Domain Group Privacy Service	N/A
.whoIsDomainItem.dataObject.registrant.countryCode	Attribute	Country	N/A	US	N/A
.whoIsDomainItem.dataObject.registrant.state	Attribute	State	N/A	California	N/A
.whoIsDomainItem.dataObject.registrant.city	Attribute	City	N/A	N/A	N/A
.whoIsDomainItem.dataObject.status[]	Attribute	Status	N/A	clienttransferprohibited	N/A
.whoIsDomainItem.dataObject.nameServers[]	Attribute	Name Server	N/A	ARIELLA.NS.CLOUDFLARE.COM	N/A

IP Address

`GET {HOSTNAME}/apireyes/api/v4/search/tool/domain-tools?ip:8.8.8.8`

Sample Response:


```
{
    "success": true,
    "data": {
        "8.8.8.8": {
            "whoIsIPItem": [
                {
                    "cidr": "8.8.8.0/24",
                    "auditUpdateDate": "2023-12-28T01:00:00.000Z",
                    "createdDate": "2023-12-28T01:00:00.000Z",
                    "dataObject": {
                        "abuseContact": {
                            "telephone": "16502530000",
                            "email": "network-abuse@google.com",
                            "name": "ABUSE"
                        },
                        "registrant": {
                            "countryCode": "US",
                            "city": "Mountain View",
                            "postalCode": "94043",
                            "street": "1600 Amphitheatre Parkway",
                            "organization": "Google LLC (GOGL)",
                            "state": "CA",
                            "name": "GOOGLE LLC"
                        },
                        "registrantContact": {},
                        "technicalContact": {
                            "telephone": "16502530000",
                            "email": "arin-contact@google.com",
                            "name": "GOOGLE LLC"
                        },
                        "nameServers": [],
                        "active": false,
                        "status": [
                            "Direct Allocation"
                        ],
                        "parseCode": 0,
                        "audit": {},
                        "registryData": {
                            "parseCode": 0
                        },
                        "estimatedDomainAge": 0,
                        "billingContact": {},
                        "zoneContact": {},
                        "administrativeContact": {
```

```
                            "telephone": "16502530000",
                            "email": "arin-contact@google.com",
                            "name": "GOOGLE LLC"
                        }
                    }
                }
            ]
        }
    },
    "error": [
        null
    ]
}
```


ThreatQuotient provides the following default mapping for IP Address objects using the Domaintools tool option *based on* `.data.<ip_address_value>` entry.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.whoIsIPItem[].cidr	Attribute	CIDR	N/A	8.8.8.0/24	N/A
.whoIsIPItem[].dataObject.registrant.organization	Attribute	Organization	N/A	Google LLC (GOGL)	N/A
.whoIsIPItem[].dataObject.registrant.countryCode	Attribute	Country	N/A	US	N/A
.whoIsIPItem[].dataObject.registrant.state	Attribute	State	N/A	CA	N/A
.whoIsIPItem[].dataObject.registrant.city	Attribute	City	N/A	Mountain View	N/A
.whoIsIPItem[].dataObject.status[]	Attribute	Status	N/A	Direct Allocation	N/A
.whoIsIPItem[].dataObject.nameServers[]	Attribute	Name Server	N/A	N/A	N/A

Enrich - GreyNoise

The GreyNoise tool option for the Enrich action supports IP Address type indicators.

IP Address

`GET {HOSTNAME}/apireyes/api/v4/search/tool/greynoise?ip:8.8.8.8`

Sample Response:


```
{
    "success": true,
    "data": {
        "8.8.8.8": {
            "noise": [],
            "riot": [
                {
                    "ip": "8.8.8.8",
                    "category": "public_dns",
                    "description": "Google's global domain name system (DNS)
resolution service.",
                    "explanation": "Public DNS services are used as
alternatives to ISP's name servers. You may see devices on your network
communicating with Google Public DNS over port 53/TCP or 53/UDP to resolve DNS
lookups.",
                    "lastUpdated": "2024-11-25T13:11:02.000Z",
                    "name": "8.8.8.8",
                    "reference": "https://developers.google.com/speed/public-
dns/docs/isp#alternative",
                    "riot": true,
                    "trustLevel": "1"
                }
            ]
        }
    },
    "error": [
        null
    ]
}
```

ThreatQuotient provides the following default mapping for IP Address object types using the GreyNoise tool based on `.data.<ip_address_value>` entry.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.riot[].category	Attribute	Category	N/A	public_dns	N/A
.riot[].description	Attribute	Description	N/A	Google's global domain name system (DNS) resolution service	N/A
.riot[].explanation	Attribute	Explanation	N/A	Public DNS services are used as alternatives to ISP's name servers...	N/A
.riot[].lastUpdated	Attribute	Last Updated	N/A	2024-11-25T13:11:02.000Z	N/A
.riot[].reference	Attribute	Reference	N/A	https://developers.google.com/speed/public-dns/docs/isp#alternative	N/A
.riot[].riot	Attribute	Riot	N/A	True	N/A
.riot[].trustLevel	Attribute	Trust Level	N/A	1	N/A
.riot[].description	Indicator Description	N/A	N/A	Google's global domain name system (DNS) resolution service	Concatenated with the other fields.
.riot[].explanation	Indicator Description	N/A	N/A	Public DNS services are used as alternatives to ISP's name servers...	Concatenated with the other fields.
.noise[].classification	Attribute	Classification	N/A	public_dns	N/A
.noise[].first_seen	Attribute	First Seen	N/A	2024-11-25T13:11:02.000Z	N/A
.noise[].last_seen	Attribute	Last Seen	N/A	2024-11-25T13:11:02.000Z	N/A
.noise[].actor	Attribute	Actor	N/A	Bad Actor	N/A
.noise[].bot	Attribute	Bot	N/A	Gemini	N/A
.noise[].cve[]	Indicator	CVE	N/A	CVE-2020-9484	N/A
.noise[].metadata.asn	Attribute	ASN	N/A	AS20473	N/A
.noise[].metadata.city	Attribute	City	N/A	Los Angeles	N/A
.noise[].metadata.country_code	Attribute	Country	N/A	US	N/A
.noise[].metadata.organization	Attribute	Organization	N/A	The Constant Company, LLC	N/A
.noise[].metadata.category	Attribute	Category	N/A	hosting	N/A
.noise[].metadata.tor	Attribute	TOR	N/A	False	N/A
.noise[].metadata.rdns	Attribute	rDNS	N/A	45.63.52.184.vultrusercontent.com	N/A
.noise[].metadata.os	Attribute	Operating System	N/A	Linux	N/A
.noise[].metadata.sensor_hits	Attribute	Sensor Hits	N/A	1	N/A
.noise[].metadata.sensor_count	Attribute	Sensor Count	N/A	5	N/A
.noise[].metadata.destination_country_codes	Attribute	Destination Country	N/A	CA	N/A
.noise[].vpn_service	Attribute	VPN Service	N/A	Cisco	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.noise[].raw_data.scan[].port	Attribute	Port	N/A	22	N/A
.noise[].raw_data.scan[].protocol	Attribute	Protocol	N/A	TCP	N/A
.noise[].raw_data.web.paths[]	Attribute	Web Path	N/A	/favicon.ico	N/A
.noise[].raw_data.web.useragents[]	Attribute	User Agent	N/A	Mozilla/5.0 (compatible; Baiduspider/2.0; +http...	N/A

Enrich - Intel CTR

The Intel CTR tool option for the Enrich action supports IP Address indicator types.

IP Address

`GET {HOSTNAME}/apireyes/api/v4/search/tool/intel-ctr?ip:8.8.8.8`

Sample Response:


```
            "event": [
                {
                    "settings": [
                        {
                            "value": "Slaved",
                            "key": "group"
                        },
                        {
                            "value": "65535",
                            "key": "buffer_size"
                        },
                        {
                            "value": "10485760",
                            "key": "max_packet_size"
                        },
                        {
                            "value": "c5fa0484-6841-42e6-8369-d6417bb6aa7f",
                            "key": "mutex"
                        },
                        {
                            "value": "8.8.8.8",
                            "key": "primary_dns_server"
                        },
                        {
                            "value": "8.8.4.4",
                            "key": "backup_dns_server"
                        }
                    ],
                    "urls": [
                        "tcp://report-reed.gl.at.ply.gg:25786"
                    ],
                    "encryption": [
                        {
                            "algorithm": "DES",
                            "key": "722018788c294897",
                            "context": "COMMUNICATION"
                        }
                    ],
```

```
                    "md5": "3511c9d5fa66610826129d4a821e61ed",
                    "sha1": "818afbdad6b64629f5404ba43f14fcbd7ab6d32c",
                    "sha256":
"91627cffcf4dc45431a510d1bc96e50bedd34c7d20fca36823b611c17f311505",
                    "fileType": "PEEXE_x86",
                    "fileSize": 3740891,
                    "threatType": "malware",
                    "threatFamily": "nanocore",
                    "firstSeen": "2023-11-25T17:04:53.000Z",
                    "lastSeen": "2023-11-25T17:04:53.000Z"
                },
                ...
            ]
```

ThreatQuotient provides the following default mapping for IP Address objects for the Intel CTR tool based on `.data.<ip_address_value>.event[]` entry.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.md5	Related Indicator.Value	MD5	N/A	3511c9d5fa66610826129d4a821e61ed	N/A
.sha1	Related Indicator.Value	SHA-1	N/A	818afbdad6b64629f5404ba43f14fcbd7ab6d32c	N/A
.sha256	Related Indicator.Value	SHA-256	N/A	91627cffcf4dc45431a510d1bc96e50bedd34c7d20fca36823b611c17f311505	N/A
.urls[]	Related Indicator.Value	IP Address or FQDN	N/A	report-reed.gl.at.ply.gg	The Scheme and Port Attributes will be extracted
.threatFamily	Related Malware.Value	Malware	N/A	Nanocore	If threatType == "malware"
.urls[]	Indicator.Attribute	Scheme	N/A	tcp	For IP Address/FQDN indicators
.urls[]	Indicator.Attribute	Port	N/A	25786	For IP Address/FQDN indicators
.fileType	Indicator.Attribute	File Type	N/A	PEEXE_x86	For MD5/SHA-1/ SHA-256 indicators
.fileSize	Indicator.Attribute	File Size	N/A	3740891	For MD5/SHA-1/ SHA-256 indicators

Enrich - RiskIQ

The RiskIQ tool option for the Enrich action supports FQDN, IP Address, and URL type indicators.

FQDN

`GET {HOSTNAME}/apireyes/api/v4/search/tool/riskiq?domain:ariella.ns.cloudflare.com`

Sample Response:


```
{
  "data": {
    "ariella.ns.cloudflare.com": {
      "dns": [
        {
          "firstSeen": "2024-09-12T09:13:12.000Z",
          "lastSeen": "2024-09-12T14:25:56.000Z",
          "recordType": "SOA",
          "value": "ariella.ns.cloudflare.com"
        },
        {
          "firstSeen": "2024-09-12T09:09:43.000Z",
          "lastSeen": "2024-09-15T21:08:55.000Z",
          "recordType": "NS",
          "value": "ariella.ns.cloudflare.com."
        }
      ],
      "ip": [
        {
          "firstSeen": "2024-09-12T09:12:29.000Z",
          "lastSeen": "2024-09-15T21:08:55.000Z",
          "recordType": "A",
          "value": "172.67.212.97"
        },
        {
          "firstSeen": "2024-09-12T09:12:29.000Z",
          "lastSeen": "2024-09-15T21:08:55.000Z",
          "recordType": "A",
          "value": "104.21.61.171"
        },
        {
          "firstSeen": "2024-09-13T02:25:27.000Z",
          "lastSeen": "2024-09-13T11:16:06.000Z",
          "recordType": "AAAA",
          "value": "2a06:98c1:3121::c"
        }
      ]
    }
  },
  "error": [
    null
  ],
  "success": true
}
```


ThreatQuotient provides the following default mapping for FQDN object types for the RiskIQ tool based on `.data.<fqdn_value>` entry.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.ip[].value	Related Indicator	IP Address/IPv6	N/A	104.21.61.171	Indicator type based on "recordType"

IP Address

```
GET {HOSTNAME}/apireyes/api/v4/search/tool/riskiq?ip:8.8.8.8
```

Sample Response:


```
{
    "domain": [
        {
            "firstSeen": "2023-09-12T15:29:20.000Z",
            "lastSeen": "2024-11-24T16:28:51.000Z",
            "recordType": "A",
            "resolution": true,
            "value":
"0efd02432153657373696f6e206b696c6c65643a204e6f20726561736f6e206.76976656e00.o.
gov-by.net"
        },
        {
            "firstSeen": "2023-09-21T13:17:31.000Z",
            "lastSeen": "2024-11-24T16:47:18.000Z",
            "recordType": "A",
            "resolution": true,
            "value":
"c4f602432153657373696f6e206b696c6c65643a204e6f20726561736f6e206.76976656e00.o.
gov-by.net"
        }
    ],
    "hash": [
        {
            "collectionDate": "2024-11-25T01:00:00.000Z",
            "name":
"e6a9fff8367bd276e28ab5f1130de8b745b3a629412fd3b8a6338e17926e0457",
            "sampleDate": "2024-11-25T01:00:00.000Z",
            "sha256":
"e6a9fff8367bd276e28ab5f1130de8b745b3a629412fd3b8a6338e17926e0457"
        },
        {
            "collectionDate": "2024-11-25T01:00:00.000Z",
            "name":
"e08eb6c5f0f7bca97ce64c85549a2a837e2c46c5bcfdd91542b661ade21f0e3b",
            "sampleDate": "2024-11-25T01:00:00.000Z",
            "sha256":
"e08eb6c5f0f7bca97ce64c85549a2a837e2c46c5bcfdd91542b661ade21f0e3b"
        }
    ],
    "url": [
        {
            "source": "developers.google.com",
            "tags": [
                "search-engine",
```

```
                "google"
            ],
            "value": "https://developers.google.com/speed/public-dns"
        },
        {
            "source": "live.paloaltonetworks.com",
            "tags": [
                "search-engine",
                "paloaltonetworks"
            ],
            "value": "https://live.paloaltonetworks.com/t5/general-topics/
application-match-sophos-live-protection-to-8-8-8-8/td-p/229518"
        },
        {
            "source": "www.reddit.com",
            "tags": [
                "search-engine",
                "reddit"
            ],
            "value": "https://www.reddit.com/r/techsupport/comments/10xnkgn/
should_i_change_my_dns_to_8888/"
        }
    ]
}
```


ThreatQuotient provides the following default mapping for IP Address object types for the RiskIQ tool based on `.data.<ip_address_value>` entry.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.hash[].sha256	Related Indicator.Value	SHA-256	N/A	e6a9fff8367bd276e28ab5f1130de8b745b3a629412f3b8a6338e17926e0457	N/A
.hash[].sha1	Related Indicator.Value	SHA-1	N/A	N/A	N/A
.hash[].md5	Related Indicator.Value	MD5	N/A	N/A	N/A
.domain[].value	Related Indicator.Value	FQDN	N/A	maclifttruck.ao	N/A
.url[].value	Indicator.Attribute	Reference	N/A	https://developers.google.com/speed/public-dns	N/A

Enrich - Shodan

The Shodan tool option for the Enrich action supports FQDN and IP Address type indicators.

FQDN

```
GET {HOSTNAME}/apireyes/api/v4/search/tool/shodan?domain:infomanage28391.cfd
```

Sample Response:


```
{
    "success": true,
    "data": {
        "infomanage28391.cfd": {}
    },
    "error": [
        null
    ]
}
```


ThreatQuotient provides the following default mapping for FQDN object for the Shodan tool option based on `.data.<fqdn_value>` entry.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.subdomain[].value	Attribute	Subdomain	N/A	N/A	N/A

IP Address

```
GET {HOSTNAME}/apireyes/api/v4/search/tool/shodan?ip:8.8.8.8
```

Sample Response:


```
{
    "success": true,
    "data": {
        "8.8.8.8": {
            "subdomain": [
                {
                    "value": "dns.google",
                    "subdomain": true
                }
            ]
        }
    },
    "error": [
        null
    ]
}
```

ThreatQuotient provides the following default mapping for IP Address objects for the Shodan tool based on `.data.<ip_address_value>` entry.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.subdomain[].value	Attribute	Subdomain	N/A	dns.google	N/A

Enrich - VirusTotal

The VirusTotal tool option supports FDQN, IP Address, and URL type indicators.

FQDN

`GET {HOSTNAME}/apireyes/api/v4/search/tool/virus-total?domain:infomanage28391.cfd`

Sample Response:


```
{
    "data": {
        "infomanage28391.cfd": {
            "domain": {
                "categories": [
                    {
                        "name": "alphaMountain.ai",
                        "value": "Phishing (alphaMountain.ai)"
                    }
                ],
                "comments": [
                    {
                        "count": 1,
                        "date": 1726220951000,
                        "tags": [
                            "phishing"
                        ],
                        "text": "#phishing",
                        "vote": {
                            "abuse": 0,
                            "negative": 0,
                            "positive": 0
                        }
                    }
                ],
                "creationDate": 1726099200000,
                "jarm":
"27d3ed3ed0003ed1dc42d43d00041d6183ff1bfae51ebd88d70384363d525c",
                "lastAnalysisDate": 1728890916000,
                "lastAnalysisResults": [
                    {
                        "category": "harmless",
                        "engineName": "Acronis",
                        "method": "blacklist",
                        "result": "clean"
                    },
                    {
                        "category": "undetected",
```

```
                "engineName": "0xSI_f33d",
                "method": "blacklist",
                "result": "unrated"
            },
            {
                "category": "harmless",
                "engineName": "Abusix",
                "method": "blacklist",
                "result": "clean"
            },
            {
                "category": "harmless",
                "engineName": "ADMINUSLabs",
                "method": "blacklist",
                "result": "clean"
            },
            {
                "category": "undetected",
                "engineName": "Axur",
                "method": "blacklist",
                "result": "unrated"
            }
        ],
        "lastAnalysisStats": {
            "harmless": 52,
            "malicious": 11,
            "positives": 11,
            "suspicious": 1,
            "timeout": 0,
            "total": 94,
            "undetected": 30
        },
        "lastDnsRecords": [
            {
                "ttl": 21600,
                "type": "NS",
                "value": "ariella.ns.cloudflare.com"
            },
            {
                "ttl": 300,
                "type": "A",
                "value": "172.67.212.97"
            },
            {
                "ttl": 21600,
                "type": "NS",
                "value": "noel.ns.cloudflare.com"
            },
            {
                "ttl": 300,
```

```
                    "type": "AAAA",
                    "value": "2606:4700:3031::6815:3dab"
                },
                {
                    "expire": 604800,
                    "rname": "dns.cloudflare.com",
                    "ttl": 1800,
                    "type": "SOA",
                    "value": "ariella.ns.cloudflare.com"
                },
                {
                    "ttl": 300,
                    "type": "AAAA",
                    "value": "2606:4700:3035::ac43:d461"
                },
                {
                    "ttl": 300,
                    "type": "A",
                    "value": "104.21.61.171"
                }
            ],
            "lastDnsRecordsDate": 1726416860000,
            "lastUpdateDate": 1726099200000,
            "popularityRanks": [],
            "positives": 11,
            "reputation": -58,
            "subdomain": false,
            "total": 94,
            "totalVotes": {
                "harmless": 0,
                "malicious": 1
            },
            "whois": "Create date: 2024-09-12 00:00:00\nDomain name:
infomanage28391.cfd\nDomain registrar id: 3956\nDomain registrar url: https://
www.globaldomaingroup.com\nExpiry date: 2025-09-12 00:00:00\nName server 1:
noel.ns.cloudflare.com\nName server 2: ariella.ns.cloudflare.com\nQuery time:
2024-09-13 12:49:34\nRegistrant company: c0dbd0252fd47a8b\nRegistrant country:
United States\nRegistrant email: f651612a2f356ad3s@\nRegistrant state:
77ab92f1911d7c5f\nUpdate date: 2024-09-12 00:00:00",
            "whoisDate": 1757635200000
        }
    }
},
"error": [
    {
        "message": "Peticiones agotadas, por favor pÃ³ngase en contacto con
reyes@ccn-cert.cni.es",
        "nameApp": "virustotal",
        "type": "WARN"
    }
```

```
    ],
    "success": true
}
```

ThreatQuotient provides the following default mapping for this action based on `.data.<fqdn_value>.domain` entry.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.categories[].value	Attribute	Category	N/A	Phishing (alphaMountain.ai)	N/A
.reputation	Attribute	Reputation	N/A	-58	N/A
.positives	Attribute	Positive Count	N/A	11	N/A
.lastAnalysisStats.harmless	Attribute	Harmless Count	N/A	52	N/A
.lastAnalysisStats.malicious	Attribute	Malicious Count	N/A	11	N/A
.lastAnalysisStats.undetected	Attribute	Undetected Count	N/A	30	N/A
.lastAnalysisStats.suspicious	Attribute	Suspicious Count	N/A	1	N/A
.lastDnsRecords.value	Attribute	Name Server	N/A	noel.ns.cloudflare.com	if `.lastDnsRecords.type` == "NS"
.lastDnsRecords.value	Attribute	Start of Authority	N/A	ariella.ns.cloudflare.com	if `.lastDnsRecords.type` == "SOA"
.lastDnsRecords.value	Related Indicator.Value	IP Address	N/A	172.67.212.97	if `.lastDnsRecords.type` == "A"
.lastDnsRecords.value	Related Indicator.Value	IPv6 Address	N/A	2606:4700:3031::6815:3dab	if `.lastDnsRecords.type` == "AAAA"

IP Address

```
GET {HOSTNAME}/apireyes/api/v4/search/tool/virus-total?ip:8:8:8:8
```

Sample Response:


```
{
    "success": true,
    "data": {
        "8.8.8.8": {
            "ip": {
                "asOwner": "GOOGLE",
                "asn": 15169,
                "continent": "NA",
                "country": "US",
                "jarm":
"29d3fd00029d29d00042d43d00041d598ac0c1012db967bb1ad0ff2491b3ae",
                "lastAnalysisDate": 1732534880000,
                "lastAnalysisResults": [
                    {
                        "engineName": "Acronis",
                        "category": "harmless",
                        "method": "blacklist",
                        "result": "clean"
                    },
                    {
                        "engineName": "0xSI_f33d",
                        "category": "undetected",
                        "method": "blacklist",
                        "result": "unrated"
                    },
                    {
                        "engineName": "Abusix",
                        "category": "harmless",
                        "method": "blacklist",
                        "result": "clean"
                    },
                    {
                        "engineName": "ADMINUSLabs",
                        "category": "harmless",
                        "method": "blacklist",
                        "result": "clean"
                    }
                ],
                "lastAnalysisStats": {
                    "harmless": 63,
                    "malicious": 0,
                    "suspicious": 0,
                    "undetected": 31,
                    "timeout": 0,
```

```
                    "positives": 0,
                    "total": 94
                },
                "network": "8.8.8.0/24",
                "regionalInternetRegistry": "ARIN",
                "reputation": 540,
                "tags": [],
                "totalVotes": {
                    "harmless": 212,
                    "malicious": 36
                },
                "whois": "NetRange: 8.8.8.0 - 8.8.8.255\nCIDR:
8.8.8.0/24\nNetName: GOGL\nNetHandle: NET-8-8-8-0-2\nParent: NET8
(NET-8-0-0-0-0)\nNetType: Direct Allocation\nOriginAS: \nOrganization: Google
LLC (GOGL)\nRegDate: 2023-12-28\nUpdated: 2023-12-28\nRef: https://
rdap.arin.net/registry/ip/8.8.8.0\nOrgName: Google LLC\nOrgId: GOGL\nAddress:
1600 Amphitheatre Parkway\nCity: Mountain View\nStateProv: CA\nPostalCode:
94043\nCountry: US\nRegDate: 2000-03-30\nUpdated: 2019-10-31\nComment: Please
note that the recommended way to file abuse complaints are located in the
following links. \nComment: \nComment: To report abuse and illegal activity:
https://www.google.com/contact/\nComment: \nComment: For legal requests:
http://support.google.com/legal \nComment: \nComment: Regards, \nComment: The
Google Team\nRef: https://rdap.arin.net/registry/entity/GOGL\nOrgAbuseHandle:
ABUSE5250-ARIN\nOrgAbuseName: Abuse\nOrgAbusePhone: +1-650-253-0000
\nOrgAbuseEmail: network-abuse@google.com\nOrgAbuseRef: https://rdap.arin.net/
registry/entity/ABUSE5250-ARIN\nOrgTechHandle: ZG39-ARIN\nOrgTechName: Google
LLC\nOrgTechPhone: +1-650-253-0000 \nOrgTechEmail: arin-
contact@google.com\nOrgTechRef: https://rdap.arin.net/registry/entity/ZG39-
ARIN\n",
                "whoisDate": 1731367316000,
                "positives": 0,
                "total": 94,
                "comments": [
                    {
                        "count": 92,
                        "date": 1728659511000,
                        "text": "This indicator was mentioned in a report.
\n\n\uD83D\uDD0E Title: Cyberespionage the Gamaredon way: Analysis of toolset
used to spy on Ukraine in 2022 and 2023\n\uD83D\uDCD1 Reference: https://web-
assets.esetstatic.com/wls/en/papers/white-papers/cyberespionage-gamaredon-
way.pdf\n\uD83D\uDCC6 Report Publish Date: 2024-09-26\n\uD83C\uDFF7 Reference
ID: #21abb39ec (https://www.virustotal.com/gui/search/21abb39ec/comments for
report's related indicators)\n",
                        "vote": {
                            "positive": 0,
                            "negative": 0,
                            "abuse": 0
                        },
                        "tags": [
                            "21abb39ec"
```

```
                    ]
                },
                {
                    "count": 92,
                    "date": 1728319925000,
                    "text": "What a beautiful IP",
                    "vote": {
                        "positive": 0,
                        "negative": 0,
                        "abuse": 0
                    },
                    "tags": []
                }
            ]
        },
        "urls": [
            {
                "value": "http://mozilla1.com/",
                "positives": 2,
                "total": 96,
                "scanDate": 1732543395000,
                "url": "http://mozilla1.com/"
            },
            {
                "value": "https://www.usevchala.cfd/",
                "positives": 1,
                "total": 96,
                "scanDate": 1732535294000,
                "url": "https://www.usevchala.cfd/"
            },
            {
                "value": "https://www.tryvchala.cfd/",
                "positives": 1,
                "total": 96,
                "scanDate": 1732534027000,
                "url": "https://www.tryvchala.cfd/"
            }
        ],
        "relatedSamples": [
            {
                "sha256":
"fb47468a2cd3953c7131431991afcc6a2703f14640520102eea0a685a7e8d6de",
                "sampleDate": 1732444650000,
                "positives": 0,
                "total": 62,
                "dateCommunicatingSamples": 1732444650000,
                "firstSubmissionDate": 1726865917,
                "lastModificationDate": 1732546083000,
                "downloadable": true,
                "lastAnalysisDate": 1732444650000
```

```
                },
                {
                    "sha256":
"fb2d9f058c2010c57f86a05ae33d282f33e3825290c66b8b120cd177416c6bdf",
                    "sampleDate": 1732107089000,
                    "positives": 0,
                    "total": 63,
                    "dateCommunicatingSamples": 1732107089000,
                    "firstSubmissionDate": 1730720182,
                    "lastModificationDate": 1732545035000,
                    "downloadable": true,
                    "lastAnalysisDate": 1732107089000
                },
                {
                    "sha256":
"f29f1818f5952bcf2e6381afb06c830be7053c7c285f8e371f0dce0c99f5165f",
                    "sampleDate": 1715792008000,
                    "positives": 0,
                    "total": 64,
                    "dateCommunicatingSamples": 1715792008000,
                    "firstSubmissionDate": 1715792008,
                    "lastModificationDate": 1728435612000,
                    "downloadable": true,
                    "lastAnalysisDate": 1715792008000
                }
            ],
            "ipResolutions": [
                {
                    "value": "sugar998.top",
                    "lastResolved": 1732545965000,
                    "positives": 0,
                    "total": 94,
                    "hostName": "sugar998.top",
                    "resolver": "Georgia Institute of Technology",
                    "date": 1732545965000,
                    "name": "sugar998.top",
                    "resolution": true
                },
                {
                    "value": "hurguven.win",
                    "lastResolved": 1732545953000,
                    "positives": 0,
                    "total": 94,
                    "hostName": "hurguven.win",
                    "resolver": "Georgia Institute of Technology",
                    "date": 1732545953000,
                    "name": "hurguven.win",
                    "resolution": true
                },
                {
```

```
                    "value": "frontlinesassessment.com",
                    "lastResolved": 1732545951000,
                    "positives": 0,
                    "total": 94,
                    "hostName": "frontlinesassessment.com",
                    "resolver": "Georgia Institute of Technology",
                    "date": 1732545951000,
                    "name": "frontlinesassessment.com",
                    "resolution": true
                }
            ]
        }
    },
    "error": [
        null
    ]
}
```

ThreatQuotient provides the following default mapping for IP Address objects for the VirusTotal tool based on `.data.<ip_address_value>` entry.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.ip.asOwner	Attribute	AS Owner	N/A	GOOGLE	N/A
.ip.asn	Attribute	ASN	N/A	15169	N/A
.ip.country	Attribute	Country	N/A	US	N/A
.ip.lastAnalysisStats.harmless	Attribute	Harmless Count	N/A	63	N/A
.ip.lastAnalysisStats.malicious	Attribute	Malicious Count	N/A	0	N/A
.ip.lastAnalysisStats.undetected	Attribute	Undetected Count	N/A	31	N/A
.ip.lastAnalysisStats.suspicious	Attribute	Suspicious Count	N/A	0	N/A
.ip.reputation	Attribute	Reputation	N/A	540	N/A
.urls[].value	Related Indicator.Value	URL	N/A	http://mozilla1.com/	N/A
.urls[].positives	Related Indicator.Attribute	Positive Count	N/A	2	N/A
.urls[].total	Related Indicator.Attribute	Total	N/A	96	N/A
.urls[].scanDate	Related Indicator.Attribute	Scan Date	N/A	2024-11-25 01:03:15 UTC	%Y-%m-%d %H:%M:%S %Z
.relatedSamples[].sha256	Related Indicator.Value	SHA-256	N/A	fb47468a2cd3953c7131431991afcc6a2703f14640520102eea0a685a7e8d6de	N/A
.relatedSamples[].positives	Related Indicator.Attribute	Positive Count	N/A	0	N/A
.relatedSamples[].total	Related Indicator.Attribute	Total	N/A	62	N/A
.relatedSamples[].sampleDate	Related Indicator.Attribute	Sample Date	N/A	2024-11-25 01:03:15 UTC	%Y-%m-%d %H:%M:%S %Z
.ipResolutions[].value	Related Indicator.Value	FQDN	N/A	sugar998.top	N/A
.ipResolutions[].positives	Related Indicator.Attribute	Positive Count	N/A	0	N/A
.ipResolutions[].total	Related Indicator.Attribute	Total Count	N/A	94	N/A
.ipResolutions[].resolver	Related Indicator.Attribute	Resolver	N/A	Georgia Institute of Technology	N/A
.ipResolutions[].lastResolved	Related Indicator.Attribute	Last Resolved	N/A	2024-11-25 01:03:15 UTC	%Y-%m-%d %H:%M:%S %Z

URL

`GET {HOSTNAME}/apireyes/api/v4/search/tool/virus-total?url:http://216.173.64.63:4646/update.cmd`

Sample Response:


```
{
    "success": true,
    "data": {
        "http://216.173.64.63:4646/update.cmd": {
            "url": {
                "value": "http://216.173.64.63:4646/update.cmd",
                "tags": ["ip", "ns-port"],
                "positives": 1,
                "total": 96,
                "scanDate": 1726230047000,
                "url": "http://216.173.64.63:4646/update.cmd",
                "title": "",
                "lastAnalysisDate": 1726230047000,
                "lastHttpResponseCode": 200,
                "lastHttpResponseCodeLength": 168,
                "lastHttpResponseContentSha256":
"45d28ec6422ca94e4d9290b1d0d5ae1c355f728aa41083a561ec1e0a64a243ea",
                "lastSubmissionDate": 1726230047000,
                "reputation": -58,
                "lastAnalysisResults": [
                    {
                        "engineName": "Artists Against 419",
                        "category": "harmless",
                        "method": "blacklist",
                        "result": "clean"
                    },
                    {
                        "engineName": "Acronis",
                        "category": "harmless",
                        "method": "blacklist",
                        "result": "clean"
                    },
                    {
                        "engineName": "Abusix",
                        "category": "harmless",
                        "method": "blacklist",
                        "result": "clean"
                    }
                ],
                "totalVotes": {
                    "harmless": 0,
                    "malicious": 1
                },
```

```
                "lastAnalisysStats": {
                    "harmless": 67,
                    "malicious": 1,
                    "suspicious": 0,
                    "undetected": 28,
                    "timeout": 0,
                    "positives": 1,
                    "total": 96
                },
                "comments": [
                    {
                        "count": 1,
                        "date": 1726230105000,
                        "text": "#XWorm\nhttps://x.com/karol_paciorek/status/
1834532649236349137",
                        "vote": {
                            "positive": 0,
                            "negative": 0,
                            "abuse": 0
                        },
                        "tags": [
                            "xworm"
                        ]
                    }
                ]
            }
        }
    },
    "error": [null]
}
```

ThreatQuotient provides the following default mapping for URL objects for the VirusTotal tool based on `.data.<url_value>.url` entry.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.lastAnalysisStats.harmless	Attribute	Harmless Count	N/A	67	N/A
.lastAnalysisStats.malicious	Attribute	Malicious Count	N/A	1	N/A
.lastAnalysisStats.undetected	Attribute	Undetected Count	N/A	28	N/A
.lastAnalysisStats.suspicious	Attribute	Suspicious Count	N/A	0	N/A
.reputation	Attribute	Reputation	N/A	-58	N/A
.positives	Attribute	Positive Count	N/A	1	N/A
.lastHttpResponseContentSha256	Related Indicator.Value	SHA-256	N/A	45d28ec6422ca94e4d9290b1d0d5ae1c355f728aa41083a561ec1e0a64a243ea	N/A

Change Log

- **Version 1.0.0**
  - Initial release