ThreatQuotient

A Securonix Company

Criminal IP Operation

Version 1.0.0

December 12, 2025

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.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.

Copyright © 2025 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: tq-support@securonix.com
Support Web: https://ts.securonix.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	>= 5.6.0
Support Tier	ThreatQ Supported

Introduction

The Criminal IP Operation for ThreatQ enhances analyst workflows by integrating rich contextual intelligence on internet-connected systems directly into the platform. Criminal IP provides detailed insights such as open ports, vulnerabilities, WHOIS data, and other network attributes that help identify malicious activity and strengthen the evaluation of indicators of compromise (IOCs).

The integration provides the following operation action:

- **Criminal IP Query IP** - queries Criminal IP for contextual information on IP addresses.

The integration is compatible with IP Address type indicators.

Prerequisites

The following is required to run the integration:

- A Criminal IP API 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 whl 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.

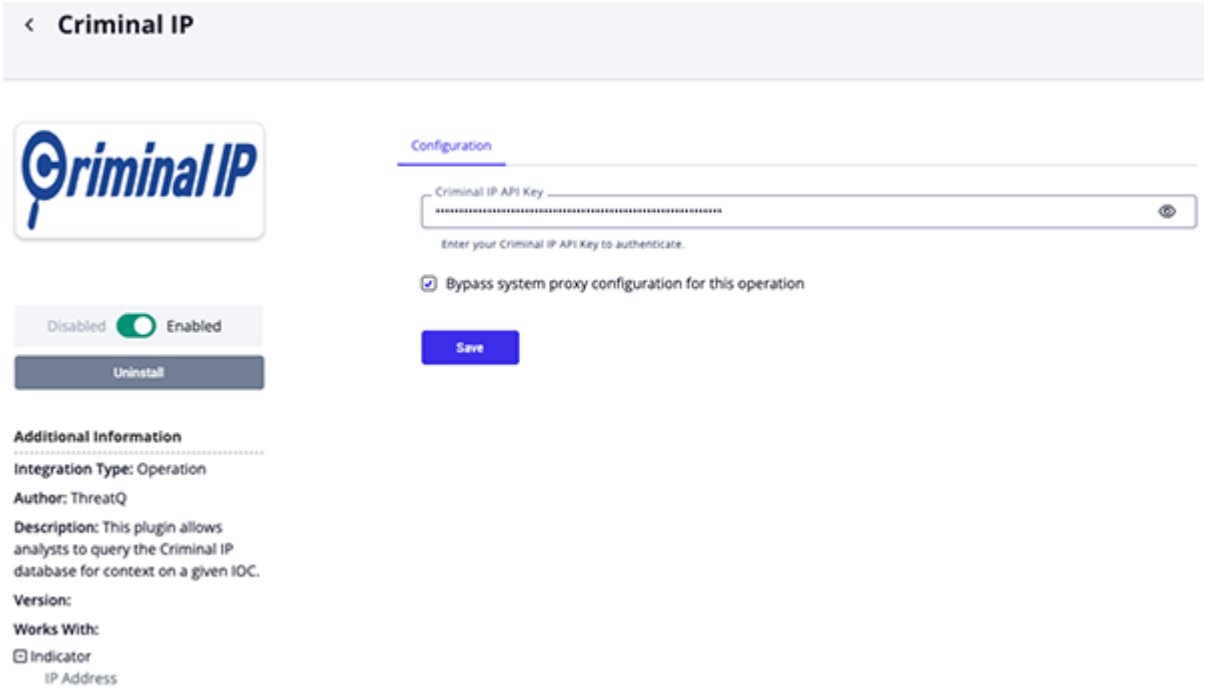
Configuration

> 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
API Key	Enter your Criminal IP API Key.
Bypass System Proxy Configuration for this Operation	Enable this parameter if the operation should not honor proxies 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 operation provides the following action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Query IP	Performs an IP lookup against Criminal IP.	Indicators	IP Address

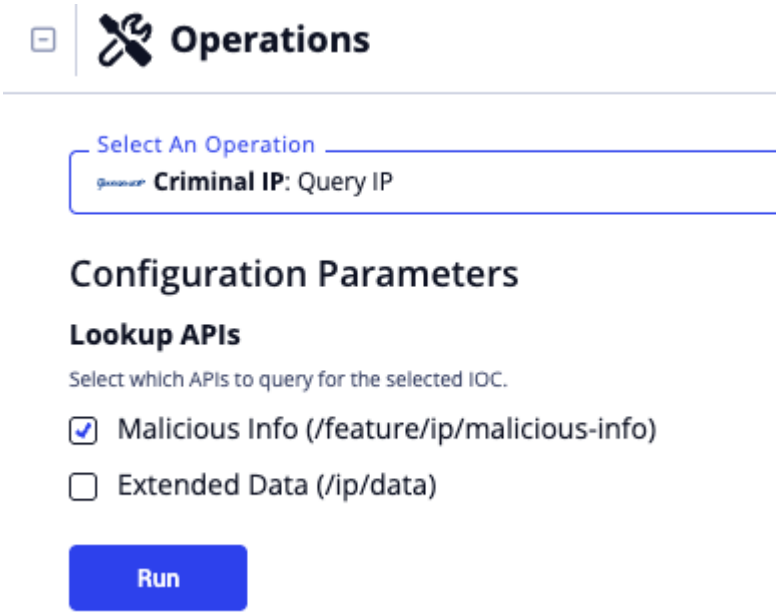
Query IP

The Criminal IP - Query IP action performs a URL lookup against the Criminal IP API to see if a given URL is a known phishing indicator. The type of requests and selected APIs are set in operation's **Lookup APIs** run parameter that is accessible from an object's details page.

Run Parameters

The following run parameter is available after selecting the operation's **Query IP** action for an object:

PARAMETER	DESCRIPTION
Lookup APIs	Select which APIs to query for the selected IOC. Options include: • Malicious Info (`/feature/ip/malicious-info`) • Extended Data (`/ip/data`)



Malicious Info

The following are the sample response and mapping tables if you have selected the **Malicious Info** option for the Lookup APIs run parameter.

```
GET https://api.criminalip.io/v1/feature/ip/malicious-info?ip={ip}
```

Sample Response:


```
{
  "status": 200,
  "ip": "45.148.10.81",
  "is_malicious": true,
  "is_vpn": false,
  "can_remote_access": true,
  "current_opened_port": {
    "count": 2,
    "data": [
      {
        "socket_type": "tcp",
        "port": 22,
        "protocol": "ssh",
        "product_name": "openssh",
        "product_version": "7.6p1",
        "has_vulnerability": false,
        "confirmed_time": "2023-03-19 13:14:46"
      },
      {
        "socket_type": "tcp",
        "port": 80,
        "protocol": "http",
        "product_name": "apache",
        "product_version": "2.4.29",
        "has_vulnerability": true,
        "confirmed_time": "2023-03-20 08:16:04"
      }
    ]
  },
  "remote_port": {
    "count": 1,
    "data": [
      {
        "socket_type": "tcp",
        "port": 22,
        "protocol": "ssh",
        "product_name": "openssh",
        "product_version": "7.6p1",
        "has_vulnerability": false,
        "confirmed_time": "2023-03-19 13:14:46"
      }
    ]
```

```
},
"vulnerability": {
  "count": 51,
  "data": [
    {
      "cve_id": "CVE-2023-25690",
      "cwe_ids": [444],
      "edb_ids": [],
      "ports": {
        "tcp": [80],
        "udp": []
      },
      "cvssv2_vector": "",
      "cvssv2_score": 0,
      "cvssv3_vector": "NETWORK",
      "cvssv3_score": 9.8,
      "product_name": "apache",
      "product_version": "2.4.29",
      "product_vendor": "apache"
    },
    {
      "cve_id": "CVE-2022-37436",
      "cwe_ids": [436, 113],
      "edb_ids": [],
      "ports": {
        "tcp": [80],
        "udp": []
      },
      "cvssv2_vector": "",
      "cvssv2_score": 0,
      "cvssv3_vector": "NETWORK",
      "cvssv3_score": 5.3,
      "product_name": "apache",
      "product_version": "2.4.29",
      "product_vendor": "apache"
    }
  ]
},
"ids": {
  "count": 2,
  "data": [
    {
      "classification": "3coresec",
      "url": "blacklist.3coresec.net/lists/et-open.txt",
      "message": "ET 3CORESec Poor Reputation IP UDP group 26",
      "source_system": "./snort-2.9.0 10182",
      "confirmed_time": "2022-11-28 21:26:39"
    },
    {
      "classification": "ciarmy",
```

```
        "url": "www.cinsscore.com",
        "message": "ET CINS Active Threat Intelligence Poor Reputation IP UDP
group 37",
        "source_system": "./snort-2.9.0 10272",
        "confirmed_time": "2023-03-20 07:39:51"
      }
    ]
  },
  "scanning_record": {
    "count": 20,
    "data": [
      {
        "log_date": "Wed, 17 Aug 2022 00:00:00 GMT",
        "dst_port": 80,
        "protocol_type": "tcp",
        "user_agent": "Go-http-client/1.1\r",
        "message": "[17/Aug/2022:07:01:43] GET http://example.com/ HTTP/1.1",
        "confirmed_time": "2022-08-17 00:00:00"
      },
      {
        "log_date": "Sun, 07 Aug 2022 00:00:00 GMT",
        "dst_port": 8090,
        "protocol_type": "tcp",
        "user_agent": "-\r",
        "message": "[07/Aug/2022:16:21:29] Phsa",
        "confirmed_time": "2022-08-07 00:00:00"
      }
    ]
  },
  "ip_category": {
    "count": 6,
    "data": [
      {
        "type": "attack (Low)",
        "detect_source": "C-TAS(igloosec)",
        "confirmed_time": "2022-09-23 17:05:39"
      },
      {
        "type": "bruteforce (fail2ban)",
        "detect_source": "",
        "confirmed_time": "2022-08-18 15:27:50"
      }
    ]
  }
}
```

ThreatQuotient provides the following default mapping for this run request:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.is_malicious`	Attribute	Is Malicious	N/A	`true`	N/A
`.is_vpn`	Attribute	Is VPN	N/A	`false`	N/A
`.can_remote_access`	Attribute	Can Remote Accress	N/A	`true`	N/A
`.ip_category.data[].type`	Attribute	Category	N/A	`attack (Low)`	N/A
`.ip_category.data[].detect_source`	Attribute	Category Detection Source	N/A	`C-TAS(igloosec)`	N/A
`.current_opened_port.data[].port`	Attribute	Open Port	N/A	`80`	N/A
`.ids.data[].classification`	Attribute	IDS Classification	N/A	`3coresec`	N/A
`.ids.data[].message`	Attribute	IDS Message	N/A	`ET CINS Active Threat Intelligence Poor Reputation IP UDP group 37`	N/A
`.ids.data[].url`	Attribute	External Reference	N/A	N/A	N/A
`.vulnerability.data[].cve_id`	Indicator	CVE	N/A	`CVE-2023-11423`	N/A
`.vulnerability.data[].cwe_ids[]`	Attribute	CWE ID	N/A	`CWE-444`	Prefixed with `CWE-` from `cwe_ids[]`.
`.vulnerability.data[].product_name`	Attribute	Affected Product	N/A	`Apache`	N/A
`.vulnerability.data[].product_vendor`	Attribute	Affected Vendor	N/A	`Apache`	N/A
`.vulnerability.data[].cvssv2_vector`	Attribute	CVSSv2 Vector	N/A	`NETWORK`	N/A
`.vulnerability.data[].cvssv3_vector`	Attribute	CVSSv3 Vector	N/A	`NETWORK`	N/A
`.vulnerability.data[].cvssv2_score`	Attribute	CVSSv2 Score	N/A	`7.9`	N/A
`.vulnerability.data[].cvssv3_score`	Attribute	CVSSv3 Score	N/A	`6.5`	N/A

Extended Data

The following are the sample response and mapping tables if you have selected the **Extend Data** option for the Lookup APIs run parameter.

`GET https://api.criminalip.io/v1/ip/data?ip={ip}&full=true`

Sample Response:


```
{
  "ip": "45.148.10.81",
  "tags": {
    "is_vpn": false,
    "is_cloud": false,
    "is_tor": false,
    "is_proxy": false,
    "is_hosting": false,
    "is_mobile": false,
    "is_darkweb": false,
    "is_scanner": false,
    "is_snort": true
  },
  "score": {
    "inbound": 5,
    "outbound": 5
  },
  "user_search_count": 4,
  "protected_ip": {
    "count": 0,
    "data": []
  },
  "domain": {
    "count": 0,
    "data": []
  },
  "whois": {
    "count": 1,
    "data": [
      {
        "as_name": "Pptechnology Limited",
        "as_no": 48090,
        "city": "Amsterdam",
        "org_name": "DMZHOST",
        "postal_code": "1012",
        "longitude": 4.8883,
        "latitude": 52.3716,
        "org_country_code": "nl",
        "confirmed_time": "2023-03-20 00:00:00"
      }
    ]
  },
```

```
  "hostname": {
    "count": 0,
    "data": []
  },
  "ids": {
    "count": 2,
    "data": [
      {
        "classification": "3coresec",
        "url": "blacklist.3coresec.net/lists/et-open.txt",
        "message": "ET 3CORESec Poor Reputation IP UDP group 26",
        "source_system": "./snort-2.9.0 10182",
        "confirmed_time": "2022-11-28 21:26:39"
      },
      {
        "classification": "ciarmy",
        "url": "www.cinsscore.com",
        "message": "ET CINS Active Threat Intelligence Poor Reputation IP UDP
group 37",
        "source_system": "./snort-2.9.0 10272",
        "confirmed_time": "2023-03-20 07:39:51"
      }
    ]
  },
  "vpn": {
    "count": 0,
    "data": []
  },
  "webcam": {
    "count": 0,
    "data": []
  },
  "honeypot": {
    "count": 0,
    "data": []
  },
  "ip_category": {
    "count": 6,
    "data": [
      {
        "detect_source": "",
        "type": "malware",
        "confirmed_time": "2022-05-17 15:03:17"
      },
      {
        "detect_source": "",
        "type": "reputation (ban_list)",
        "confirmed_time": "2022-08-30 15:06:01"
      }
    ]
```

```
  },
  "port": {
    "count": 26,
    "data": [
      {
        "app_name": "Apache",
        "banner": "HTTP/1.1\nStatus: 200 OK\nDate: Mon, 20 Mar 2023 00:12:53
GMT\nEtag: 9-5e4e3d3111d8f\nContent Length: 9\nContent Type: text/html\nServer:
Apache/2.4.29 (Ubuntu)\n\neu server",
        "app_version": "2.4.29",
        "open_port_no": 80,
        "port_status": "open",
        "protocol": "HTTP",
        "socket": "tcp",
        "dns_names": null,
        "sdn_common_name": null,
        "jarm_hash": null,
        "ssl_info_raw": null,
        "technologies": [],
        "is_vulnerability": true,
        "confirmed_time": "2023-03-20 08:16:04"
      },
      {
        "app_name": "OpenSSH",
        "banner": "SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7\nKey:
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAt5VdEM/
Dhd3Gi5zKjqDjyp6DrxINwLgOP24x9q3ETEdyz60cRDP8B08JEYormTaZLdZjl5mVos8iwR3bgEVus=
\nAlgorithm: ecdsa-sha2-nistp256\nFingerprint:
7a1d147e6fc8412e736687b3dafd5021daf307b48ba6495bde99511fc06e8baf\n\nKex
Algorithms:\n\tcurve25519-sha256\n\tcurve25519-sha256@libssh.org\n\tecdh-sha2-
nistp256\n\tecdh-sha2-nistp384\n\tecdh-sha2-nistp521\n\tdiffie-hellman-group-
exchange-sha256\n\tdiffie-hellman-group16-sha512\n\tdiffie-hellman-group18-
sha512\n\tdiffie-hellman-group14-sha256\n\tdiffie-hellman-group14-
sha1\n\nServer Host Key Algorithms:\n\tssh-rsa\n\trsa-sha2-512\n\trsa-
sha2-256\n\tecdsa-sha2-nistp256\n\tssh-ed25519\n\nEncryption Algorithms:
\n\tchacha20-poly1305@openssh.com\n\taes128-ctr\n\taes192-ctr\n\taes256-
ctr\n\taes128-gcm@openssh.com\n\taes256-gcm@openssh.com\n\nMac Algorithms:
\n\tumac-64-etm@openssh.com\n\tumac-128-etm@openssh.com\n\thmac-sha2-256-
etm@openssh.com\n\thmac-sha2-512-etm@openssh.com\n\thmac-sha1-
etm@openssh.com\n\tumac-64@openssh.com\n\tumac-128@openssh.com\n\thmac-
sha2-256\n\thmac-sha2-512\n\thmac-sha1\n\nCompression Algorithms:
\n\tnone\n\tzlib@openssh.com",
        "app_version": "7.6p1",
        "open_port_no": 22,
        "port_status": "open",
        "protocol": "SSH",
        "socket": "tcp",
        "dns_names": null,
        "sdn_common_name": null,
        "jarm_hash": null,
```

```
        "ssl_info_raw": null,
        "technologies": [],
        "is_vulnerability": false,
        "confirmed_time": "2023-03-19 13:14:46"
      }
    ]
  },
  "vulnerability": {
    "count": 51,
    "data": [
      {
        "cve_id": "CVE-2023-25690",
        "cve_description": "Some mod_proxy configurations on Apache HTTP Server
versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.
Configurations are affected when mod_proxy is enabled along with some form of
RewriteRule or ProxyPassMatch in which a non-specific pattern matches some
portion of the user-supplied request-target (URL) data and is then re-inserted
into the proxied request-target using variable substitution. For example,
something like: RewriteEngine on RewriteRule '^/here/(.*)' 'http://
example.com:8080/elsewhere?$1'; [P] ProxyPassReverse /here/ http://
example.com:8080/ Request splitting/smuggling could result in bypass of access
controls in the proxy server, proxying unintended URLs to existing origin
servers, and cache poisoning. Users are recommended to update to at least
version 2.4.56 of Apache HTTP Server.",
        "cvssv2_vector": "",
        "cvssv2_score": 0,
        "cvssv3_vector": "NETWORK",
        "cvssv3_score": 9.8,
        "list_cwe": [
          {
            "cve_id": "CVE-2023-25690",
            "cwe_id": 444,
            "cwe_name": "Inconsistent Interpretation of HTTP Requests ('HTTP
Request/Response Smuggling')",
            "cwe_description": "The product acts as an intermediary HTTP
agent\n         (such as a proxy or firewall) in the data flow between two\n
entities such as a client and server, but it does not\n         interpret
malformed HTTP requests or responses in ways that\n         are consistent with
how the messages will be processed by\n         those entities that are at the
ultimate destination."
          }
        ],
        "list_edb": [],
        "app_name": "Apache",
        "app_version": "2.4.29",
        "open_port_no_list": {
          "TCP": [80],
          "UDP": []
        },
        "have_more_ports": false,
```

```
        "open_port_no": [
          {
            "port": 80,
            "socket": "tcp"
          }
        ],
        "list_child": [],
        "vendor": "apache",
        "type": "a",
        "is_vuln": "True",
        "target_hw": "",
        "target_sw": "",
        "update": "",
        "edition": ""
      },
      {
        "cve_id": "CVE-2022-37436",
        "cve_description": "Prior to Apache HTTP Server 2.4.55, a malicious
backend can cause the response headers to be truncated early, resulting in some
headers being incorporated into the response body. If the later headers have
any security purpose, they will not be interpreted by the client.",
        "cvssv2_vector": "",
        "cvssv2_score": 0,
        "cvssv3_vector": "NETWORK",
        "cvssv3_score": 5.3,
        "list_cwe": [
          {
            "cve_id": "CVE-2022-37436",
            "cwe_id": 113,
            "cwe_name": "Improper Neutralization of CRLF Sequences in HTTP
Headers ('HTTP Request/Response Splitting')",
            "cwe_description": "The product receives data from an HTTP agent/
component (e.g., web server, proxy, browser, etc.), but it does not neutralize
or incorrectly neutralizes CR and LF characters before the data is included in
outgoing HTTP headers."
          },
          {
            "cve_id": "CVE-2022-37436",
            "cwe_id": 436,
            "cwe_name": "Interpretation Conflict",
            "cwe_description": "Product A handles inputs or steps differently
than Product B, which causes A to perform incorrect actions based on its
perception of B's state."
          }
        ],
        "list_edb": [],
        "app_name": "Apache",
        "app_version": "2.4.29",
        "open_port_no_list": {
          "TCP": [80],
```

```
          "UDP": []
        },
        "have_more_ports": false,
        "open_port_no": [
          {
            "port": 80,
            "socket": "tcp"
          }
        ],
        "list_child": [],
        "vendor": "apache",
        "type": "a",
        "is_vuln": "True",
        "target_hw": "",
        "target_sw": "",
        "update": "",
        "edition": ""
      }
    ]
  },
  "mobile": {
    "count": 0,
    "data": []
  },
  "status": 200
}
```

ThreatQuotient provides the following default mapping for this run request:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.tags.is_vpn	Attribute	Is VPN	N/A	true	N/A
.tags.is_cloud	Attribute	Is Cloud	N/A	false	N/A
.tags.is_tor	Attribute	Is TOR	N/A	false	N/A
.tags.is_proxy	Attribute	Is Proxy	N/A	false	N/A
.tags.is_hosting	Attribute	Is Hosting	N/A	false	N/A
.tags.is_mobile	Attribute	Is Mobile	N/A	false	N/A
.tags.is_darkweb	Attribute	Is Dark Web	N/A	false	N/A
.tags.is_scanner	Attribute	Is Scanner	N/A	false	N/A
.tags.is_snort	Attribute	Is Snort	N/A	true	N/A
.score.inbound	Attribute	Inbound Score	N/A	5	N/A
.score.outbound	Attribute	Outbound Score	N/A	5	N/A
.vpn.data[].vpn_name	Attribute	VPN Name	N/A	NordVPN	N/A
.vpn.data[].vpn_source_url	Attribute	VPN Source URL	N/A	N/A	N/A
.honeypot.data[].detect_reason	Attribute	Honeypot Detect Reason	N/A	N/A	N/A
.honeypot.data[].scan_object	Attribute	Honeypot Scan Object	N/A	N/A	N/A
.honeypot.data[].protocol_type	Attribute	Honeypot Protocol Type	N/A	N/A	N/A
.honeypot.data[].dst_port	Attribute	Honeypot Destination Port	N/A	N/A	N/A
.ip_category.data[].type	Attribute	Category	N/A	attack (Low)	N/A
.ip_category.data[].detect_source	Attribute	Category Detection Source	N/A	C-TAS(igloosec)	N/A
.whois.data[].as_name	Attribute	AS Name	N/A	Pptechnology Limited	N/A
.whois.data[].as_no	Attribute	ASN	N/A	48090	N/A
.whois.data[].city	Attribute	City	N/A	Amsterdam	N/A
.whois.data[].org_name	Attribute	Organization	N/A	DMZHOST	N/A
.whois.data[].postal_code	Attribute	Postal Code	N/A	1012	N/A
.whois.data[].longitude	Attribute	Longitude	N/A	4.8883	N/A
.whois.data[].latitude	Attribute	Latitude	N/A	52.3716	N/A
.whois.data[].org_country_code	Attribute	Country Code	N/A	nl	N/A
.vulnerability.data[].cve_id	Indicator	CVE	N/A	N/A	N/A
.vulnerability.data[].cve_description	Attribute	CVE Description	N/A	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.vulnerability.data[].cvssv2_vector`	Attribute	`CVSSv2 Vector`	N/A	N/A	N/A
`.vulnerability.data[].cvssv2_score`	Attribute	`CVSSv2 Score`	N/A	N/A	N/A
`.vulnerability.data[].cvssv3_vector`	Attribute	`CVSSv3 Vector`	N/A	N/A	N/A
`.vulnerability.data[].cvssv3_score`	Attribute	`CVSSv3 Score`	N/A	N/A	N/A
`.vulnerability.data[].list_cwe[].cwe_id`	Attribute	`CWE ID`	N/A	N/A	Prefixed with `CWE-` (e.g. `CWE-444`).
`.vulnerability.data[].list_cwe[].cwe_name`	Attribute	`CWE Name`	N/A	N/A	N/A
`.vulnerability.data[].app_name`	Attribute	`Vulnerable Application`	N/A	`Apache`	N/A
`.ids.data[].classification`	Attribute	IDS Classification	N/A	`3coresec`	N/A
`.ids.data[].message`	Attribute	IDS Message	N/A	`ET CINS Active Threat Intelligence Poor Reputation IP UDP group 37`	N/A
`.ids.data[].url`	Attribute	External Reference	N/A	N/A	N/A

Change Log

- **Version 1.0.0**
  - Initial release