ThreatQuotient

A Securonix Company

Criminal IP Operation

Version 1.1.0

June 01, 2026

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.

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	1.1.0
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.
- **Criminal IP Get Domain Reports** - performs a domain reports lookup against Criminal IP.

The integration is compatible with IP Address and FQDN indicator types.

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.

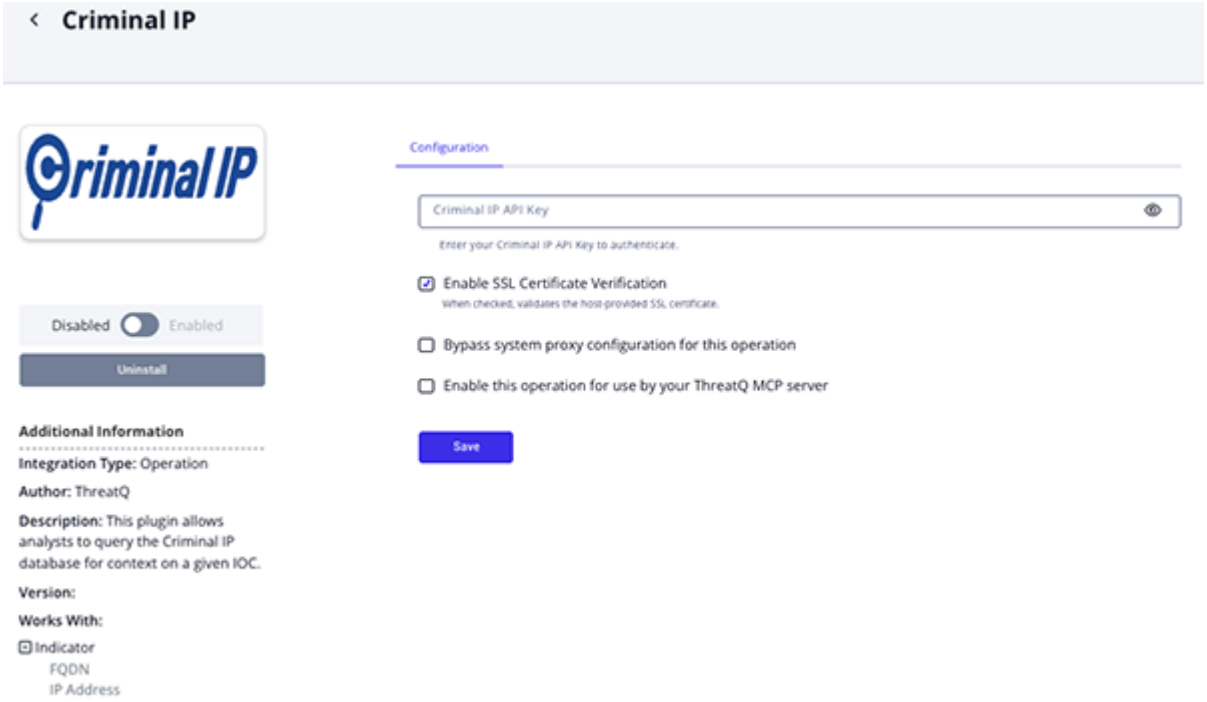
Configuration

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.
Enable SSL Certificate Verification	Enable this parameter if the operation should validate the host-provided SSL certificate.
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 actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Query IP	Performs an IP lookup against Criminal IP.	Indicators	IP Address
Get Domain Reports	Performs a domain reports lookup against Criminal IP.	Indicators	FQDN

Query IP

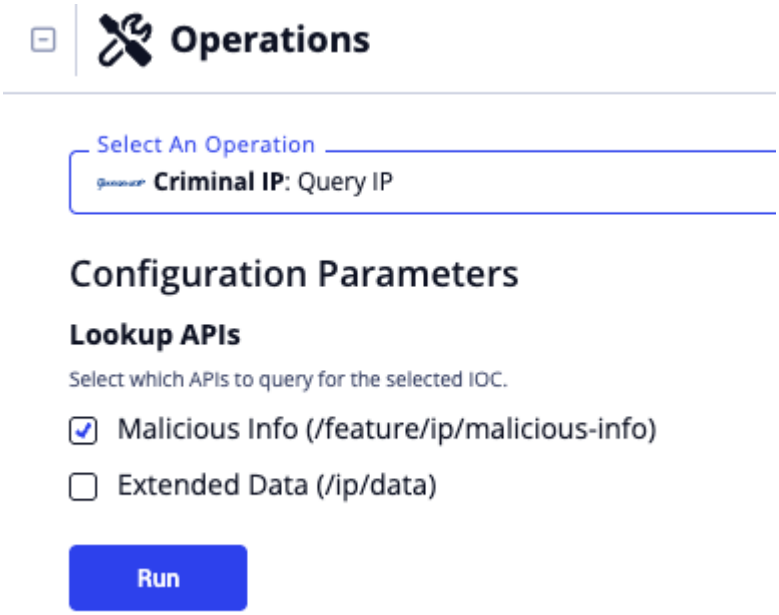
The Criminal IP - Query IP action performs a URL lookup against the Criminal IP API to see if a given URL is a known phishing indicator. The type of requests and selected APIs are set in operation's **Lookup APIs** run parameter that is accessible from an object's details page.

Run Configuration Option

> The following configuration option is set after selecting the action to run against an object and are not set from the operation's configuration screen.

The following configuration option is available for this operation action:

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 configuration option.

```
GET https://api.criminalip.io/v2/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	Indicator.attribute	Is Malicious	N/A	true	N/A
.is_vpn	Indicator.attribute	Is VPN	N/A	false	N/A
.can_remote_access	Indicator.attribute	Can Remote Accress	N/A	true	N/A
.ip_category.data[].type	Indicator.attribute	Category	N/A	attack (Low)	N/A
.ip_category.data[].detect_source	Indicator.attribute	Category Detection Source	N/A	C-TAS(igloosec)	N/A
.current_opened_port.data[].port	Indicator.attribute	Open Port	N/A	80	N/A
.ids.data[].classification	Indicator.attribute	IDS Classification	N/A	3coresec	N/A
.ids.data[].message	Indicator.attribute	IDS Message	N/A	ET CINS Active Threat Intelligence Poor Reputation IP UDP group 37	N/A
.ids.data[].url	Indicator.attribute	External Reference	N/A	N/A	N/A
.vulnerability.data[].cve_id	Indicator.value	CVE	N/A	CVE-2023-11423	N/A
.vulnerability.data[].cwe_ids[]	Related Indicator.attribute	CWE ID	N/A	CWE-444	Prefixed with CWE- from cwe_ids[].
.vulnerability.data[].product_name	Related Indicator.attribute	Affected Product	N/A	Apache	N/A
.vulnerability.data[].product_version	Related Indicator.attribute	Affected Product Version	N/A	9.3p1	N/A
.vulnerability.data[].product_vendor	Related Indicator.attribute	Affected Vendor	N/A	Apache	N/A
.vulnerability.data[].cvssv2_vector	Related Indicator.attribute	CVSSv2 Vector	N/A	NETWORK	N/A
.vulnerability.data[].cvssv3_vector	Related Indicator.attribute	CVSSv3 Vector	N/A	NETWORK	N/A
.vulnerability.data[].cvssv2_score	Related Indicator.attribute	CVSSv2 Score	N/A	7.9	Value should be > 0
.vulnerability.data[].cvssv3_score	Related Indicator.attribute	CVSSv3 Score	N/A	6.5	Value should be > 0

Extended Data

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

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

Sample Response (truncated):


```
{
  "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,
  "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"
    }]
  },
  "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"
    }]
  },
  "ip_category": {
    "count": 6,
    "data": [{
      "type": "malware",
      "confirmed_time": "2022-05-17 15:03:17"
    }, {
      "type": "reputation (ban_list)",
      "confirmed_time": "2022-08-30 15:06:01"
    }]
  },
  "port": {
    "count": 26,
    "data": [{
      "app_name": "Apache",
      "app_version": "2.4.29",
      "open_port_no": 80,
      "protocol": "HTTP",
      "socket": "tcp",
      "is_vulnerability": true,
      "banner": "HTTP/1.1 Status: 200 OK ... Server: Apache/2.4.29
(Ubuntu)",
      "confirmed_time": "2023-03-20 08:16:04"
    }, {
      "app_name": "OpenSSH",
      "app_version": "7.6p1",
      "open_port_no": 22,
      "protocol": "SSH",
      "socket": "tcp",
      "banner": "SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7 ...",
      "confirmed_time": "2023-03-19 13:14:46"
    }]
  },
  "vulnerability": {
    "count": 51,
```

```
    "data": [{
      "cve_id": "CVE-2023-25690",
      "cvssv3_score": 9.8,
      "app_name": "Apache",
      "app_version": "2.4.29",
      "vendor": "apache",
      "cwe_name": "HTTP Request/Response Smuggling"
    }, {
      "cve_id": "CVE-2022-37436",
      "cvssv3_score": 5.3,
      "app_name": "Apache",
      "app_version": "2.4.29",
      "vendor": "apache",
      "cwe_name": "HTTP Request/Response Splitting"
    }]
  },
  "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

Get Domain Reports

The Get Domain Reports operation action performs a domain reports lookup against the Criminal IP API for FQDN indicators.

```
GET https://api.criminalip.io/v1/domain/reports?query={domain}
offset=0
```

Sample Response


```
{
  "status": 200,
  "message": "api success",
  "data": {
    "count": 4082,
    "reports": [
      {
        "connected_ip_cnt": 1,
        "country_code": [""],
        "issue": ["list_of_countries", "mail_server",
"diff_domain_favicon"],
        "jarm":
"27d40d40d00040d1dc42d43d00041d6183ff1bfae51ebd88d70384363d525c",
        "reg_dtime": "2026-05-18 10:04:38",
        "scan_id": "55765539",
        "score": "Safe",
        "technologies": [
          {
            "logo_url": "https://cip-live-image.s3.us-
west-1.amazonaws.com/tech/CloudFlare.svg",
            "tech_name": "Cloudflare"
          }
        ],
        "title": "Example Domain",
        "url": "https://example.com"
      }
    ]
  }
}
```

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
.data.count	Indicator.attribute	Report Count	N/A	4082	N/A
.data.reports[].url	Indicator.value	URL or FQDN	N/A	https://example.com	URLs are added as URL indicators.
.data.reports[].score	Related Indicator.attribute	Criminal IP Score	N/A	Safe	N/A
.data.reports[].title	Related Indicator.attribute	Title	N/A	Example Domain	N/A
.data.reports[].scan_id	Related Indicator.attribute	Criminal IP Scan ID	N/A	55765539	N/A
.data.reports[].reg_dtime	Related Indicator.attribute	Criminal IP Report Time	N/A	2026-05-18 10:04:38	N/A
.data.reports[].connected_ip_cnt	Related Indicator.attribute	Connected IP Count	N/A	1	N/A
.data.reports[].country_code[]	Related Indicator.attribute	Country Codes	N/A	us	Empty values are ignored.
.data.reports[].issue[]	Related Indicator.attribute	Criminal IP Issues	N/A	mail_server	N/A
.data.reports[].technologies[].tech_name	Related Indicator.attribute	Technologies	N/A	Cloudflare	N/A
.data.reports[].jarm	Related Indicator.attribute	JARM	N/A	27d40d40d00040d1dc42d43d00041d6183ff1bfae51ebd88d70384363d525c	N/A

Change Log

- **Version 1.1.0**
  - Updated the **IP Malicious Info** lookup to use the Criminal IP `/v2/feature/ip/malicious-info` endpoint.
  - Added the **Get Domain Reports** action for FQDN indicators using the `/v1/domain/reports` endpoint.
  - Added a new configuration parameter to enable SSL certificate verification for Criminal IP API requests.
- **Version 1.0.0**
  - Initial release