

ThreatQuotient

A Securonix Company



Criminal IP Action

Version 1.0.0

December 09, 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 3

Support 4

Integration Details..... 5

Introduction 6

Prerequisites 7

Installation..... 8

Configuration 9

Actions 12

 Criminal IP - Get Malicious Info..... 13

Enriched Data..... 18

Change Log 19

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
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Criminal IP Action enables analysts to enrich IP Address indicators with contextual intelligence sourced from the Criminal IP platform, which provides data such as open ports, vulnerabilities, and WHOIS information to help identify malicious activity.

The integration provides the following action:

- **Criminal IP - Get Malicious Info** - queries the Criminal IP API to enrich an IP Address with intelligence indicating whether the indicator is malicious, along with additional contextual data used to support the assessment of the IOC.

The integration is compatible with and returns enriched IP Address type indicators.



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

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A Criminal IP API Key.
- A ThreatQ data collection containing IP Address type indicators.

Installation

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
 - Drag and drop the zip file into the dialog box
 - Select **Click to Browse** to locate the zip file on your local machine



ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to [configure](#) the action.

Configuration



ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.



To configure the integration:

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



The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
API Key	Enter your Criminal IP API key to authenticate.
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.
Only Enrich Malicious IPs	Enable this parameter to only ingest enrichment information for IPs marked as malicious. This parameter is disabled by default.
Attribute Filter	<p>Select the pieces of context to ingest. Options include:</p> <ul style="list-style-type: none"> ◦ Is Malicious (<i>default</i>) ◦ Is VPN ◦ Can Remote Access (<i>default</i>) ◦ Category (<i>default</i>) ◦ Open Port ◦ IDS Classification ◦ IDS Message ◦ External Reference

PARAMETER	DESCRIPTION
	<ul style="list-style-type: none"> ◦ Category Detection Source
Ingest Related Vulnerabilities (CVEs)	<p>Enable this parameter to ingest CVEs related to the enriched IP. This parameter is enabled by default.</p>
Ingest CVEs As	<p>Select the entity type to ingest CVE IDs as in ThreatQ. Options include</p> <ul style="list-style-type: none"> ◦ Vulnerabilities ◦ Indicators <div>  This parameter is only accessible if the Ingest Related Vulnerabilities (CVEs) parameter is enabled. </div>
Vulnerability Attribute Filter	<p>Select the pieces of context to ingest with related vulnerabilities. Options include:</p> <ul style="list-style-type: none"> ◦ Affected Product (<i>default</i>) ◦ Affected Product Version ◦ Affected Vendor (<i>default</i>) ◦ CVSSv2 Vector ◦ CVSSv2 Score ◦ CVSSv3 Vector ◦ CVSSv3 Score ◦ CWE ID <div>  These are only applied if the Ingest Related Vulnerabilities (CVEs) parameter is enabled. </div>
Objects Per Run	<p>The number of objects to process per run of the workflow. The default value is 10000.</p>

< Criminal IP - Get Malicious Info



Uninstall

Additional Information

Integration Type: Action

Version:

Action ID: 8

Accepted Data Types:

- ☒ Indicators
 - IP Address

Configuration

Authentication

API Key

Enter your Criminal IP API key to authenticate.

- ☒ Enable SSL Certificate Verification

When checked, validates the host-provided SSL certificate.
- ☐ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

Enrichment Filtering

- ☐ Only Enrich Malicious IPs

Enable this to only ingest enrichment information for IPs marked as malicious.

Attribute Filter

Select the pieces of context to ingest into ThreatQ, from Criminal IP.

- ☒ Is Malicious
- ☐ Is VPN
- ☒ Can Remote Access
- ☒ Category
- ☐ Category Detection Source
- ☐ IDS Classification
- ☐ IDS Message
- ☐ External Reference
- ☐ Open Port
- ☒ Ingest Related Vulnerabilities (CVEs)

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

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Criminal IP - Get Malicious Info	Fetches contextual information factoring into a malicious evaluation, from the Criminal IP API	Indicator	IP Address

Criminal IP - Get Malicious Info

The Criminal IP - Get Malicious Info action queries the Criminal IP API to enrich an IP Address with intelligence indicating whether the indicator is malicious, along with additional contextual data used to support the assessment of the IOC.

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 action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.is_malicious	Indicator.Attribute	Is Malicious	N/A	true	User-configurable. Updatable
.is_vpn	Indicator.Attribute	Is VPN	N/A	false	User-configurable. Updatable
.can_remote_access	Indicator.Attribute	Can Remote Access	N/A	true	User-configurable. Updatable
.ip_category.data[].type	Indicator.Attribute	Category	N/A	attack (Low)	User-configurable.
.ip_category.data[].detection_source	Indicator.Attribute	Category Detection Source	N/A	C-TAS(igloosec)	User-configurable.
.current_opened_port.data[].port	Indicator.Attribute	Open Port	N/A	80	User-configurable.
.ids.data[].classification	Indicator.Attribute	IDS Classification	N/A	3coresec	User-configurable.
.ids.data[].message	Indicator.Attribute	IDS Message	N/A	ET CINS Active Threat Intelligence Poor Reputation IP UDP group 37	User-configurable.
.ids.data[].url	Indicator.Attribute	External Reference	N/A	N/A	N/A
.vulnerability.data[].cve_id	Indicator/vulnerability.Indicator	CVE	N/A	CVE-2023-11423	Ingested as an Indicator (CVE Type). User-configurable. It is configurable via Ingest CVEs As option.
.vulnerability.data[].cwe_ids[]	Indicator/vulnerability.Attribute	CWE ID	N/A	CWE-444	User-configurable. It is configurable via Ingest CVEs As option.
.vulnerability.data[].product_name	Indicator/vulnerability.Attribute	Affected Product	N/A	Apache	User-configurable. It is configurable via Ingest CVEs As option.
.vulnerability.data[].product_version	Indicator/vulnerability.Attribute	Affected Product Version	N/A	Apache v2.4.3	The value is concatenated (Product Name and Product Version) in UI. User-configurable. It is configurable via Ingest CVEs As option.
.vulnerability.data[].product_vendor	Indicator/vulnerability.Attribute	Affected Vendor	N/A	Apache	User-configurable. It is configurable via Ingest CVEs As option.
.vulnerability.data[].cvssv2_vector	Indicator/vulnerability.Attribute	CVSSv2 Vector	N/A	NETWORK	User-configurable. It is configurable via Ingest CVEs As option.
.vulnerability.data[].cvssv3_vector	Indicator/vulnerability.Attribute	CVSSv3 Vector	N/A	NETWORK	User-configurable. It is configurable via Ingest CVEs As option.
.vulnerability.data[].cvssv2_score	Indicator/vulnerability.Attribute	CVSSv2 Score	N/A	7.9	User-configurable. It is configurable via Ingest CVEs As option.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.vulnerability.data[].cvssv3_score	Indicator/vulnerability.Attribute	CVSSv3 Score	N/A	6.5	User-configurable. It is configurable via Ingest CVEs As option.

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.

METRIC	RESULT
Run Time	2 minutes
Indicators	225
Indicator Attributes	782

Change Log

- Version 1.0.0
 - Initial release