ThreatQuotient

A Securonix Company



IPInfo Action

Version 1.1.0

November 16, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: 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**
IPInfo 12
Enriched Data **17**
Use Case Example **18**
Known Issues / Limitations **19**
Change Log **20**

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 © 2026 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: 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
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The IPInfo action submits a collection of supported indicators of compromise (IOC) to the IPInfo API in the form of individual HTTP Requests. IPInfo returns a response for each object containing any information it has about the IOC.

The integration can perform the following action:

- **IPInfo** - enriches IP Addresses with Location information such as Region, Coordinates, Country Code, and City.

The action is compatible with IP Address indicator types and returns enriched IP Addresses.



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

Prerequisites

The action requires the following:

- An IPInfo API Key.
- An active ThreatQ TRD Orchestrator (TDR) license.
- A data collection containing at IP Address indicator types.

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
IPInfo API Key	Your API Key for authentication with the IPInfo API
Objects Per Run	The Maximum number of objects to submit per workflow run. The max value for this parameter is 50,000.
IPInfo Context Filter	Select the attributes for ingestion. Options include: ◦ Location Coordinates (default) ◦ City (default) ◦ Country (default) ◦ Region (default) ◦ Hostname ◦ Is Anycast ◦ Postal Code

PARAMETER	DESCRIPTION
	◦ Timezone ◦ ASN ◦ AS Organization ◦ AS Domain ◦ Network ◦ AS Type ◦ Company Name ◦ Company Domain ◦ Company Type ◦ Is VPN ◦ Is Proxy ◦ Is TOR ◦ Is Relay ◦ Is Hosting ◦ Privacy Service ◦ Abuse Contact Address ◦ Abuse Contact Country Code ◦ Abuse Contact Email ◦ Abuse Contact Name ◦ Abuse Contact Network ◦ Abuse Contact Phone ◦ Hosted Domain Count ◦ Related Domains
Ingest ASNs As	Select what to ingest ASNs as in ThreatQ. Options include: ◦ **Indicators** *(default)* - in Indicators mode, select ASN in Context Filter to create an ASN indicator related to the original IP. Remove the leading AS prefix and surrounding whitespace: AS15169 becomes the string "15169". Selected AS Organization, AS Domain,

PARAMETER	DESCRIPTION
	Network, and AS Type fields are attached to that ASN indicator. Missing or invalid ASN values do not create indicators. ◦ **Attributes** - in attributes mode, selected ASN fields are stored as attributes on the original IP. The ASN attribute preserves the returned value, such as AS15169. No related ASN indicator is created.

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

Actions

The integration provides the following action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
IPInfo	Submits a ThreatQ data collection and queries the IPInfo API for context.	Indicator	IP Address

IPInfo

The IPInfo action submits a ThreatQ data collection and queries the IPInfo API for context. The vendor will returned enriched data of the collection submitted.

```
GET https://ipinfo.io/111.121.216.118?token={user-token}
```

The action uses the same endpoint for free-tier and enterprise tokens. Available response fields depend on the token's data access and the IP address. Selecting more context fields does not cause additional API calls.

Sample Response:

```
{
  "ip": "8.8.8.8",
  "city": "Mountain View",
  "region": "California",
  "country": "US",
  "loc": "37.4056,-122.0775",
  "org": "AS15169 Google LLC",
  "timezone": "America/Los_Angeles"
}
```

The default selections ingest Location coordinates, City, Country Code, and Region from this response. Timezone is also ingested if selected. The sample's org field has no mapping in this action; ASN context is read from the structured asn object when returned.

Sample Response: Enterprise Data

```
{
  "ip": "8.8.8.8",
  "hostname": "dns.google",
  "anycast": true,
  "city": "Mountain View",
  "region": "California",
  "country": "US",
  "loc": "37.4056,-122.0775",
  "postal": "94043",
  "timezone": "America/Los_Angeles",
  "asn": {
    "asn": "AS15169",
    "name": "Google LLC",
    "domain": "google.com",
    "route": "8.8.8.0/24",
    "type": "hosting"
  },
  "company": {
    "name": "Google LLC",
    "domain": "google.com",
    "type": "hosting"
  },
  "privacy": {
    "vpn": false,
    "proxy": false,
    "tor": false,
    "relay": false,
    "hosting": true,
    "service": ""
  },
  "abuse": {
    "address": "US, CA, Mountain View, 1600 Amphitheatre Parkway,
94043",
    "country": "US",
    "email": "network-abuse@google.com",
    "name": "Abuse",
    "network": "8.8.8.0/24",
    "phone": "+1-650-253-0000"
  },
  "domains": {
    "ip": "8.8.8.8",
    "total": 9791,
    "domains": [
```

```
      "musicool.cn",
      "kagou.vip",
      "nmgk2.com",
      "91xiazai.com",
      "bits-hyderabad.ac.in"
    ]
  }
}
```

ThreatQuotient provides the following mapping for this action. Attribute and related-indicator sources are **IPinfo**. The original IP retains its existing first source when available, falling back to IPinfo if no source is supplied. The API response contains no publication timestamp, so Published Date is **N/A**.

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.ip	Indicator.Value	IP Address	N/A	8.8.8.8	Matching check: the response IP must equal the requested indicator value. The original indicator value comes from the workflow input.
.city	Indicator.Attribute	City	N/A	Mountain View	Selected by default in Context Filter.
.country	Indicator.Attribute	Country Code	N/A	US	Selected by default in Context Filter.
.region	Indicator.Attribute	Region	N/A	California	Selected by default in Context Filter.
.loc	Indicator.Attribute	Location coordinates	N/A	37.4056,-122.0775	Selected by default in Context Filter. Preserve the latitude/longitude pair as one value.
.hostname	Indicator.Attribute	Hostname	N/A	dns.google	Ingested when its Context Filter option is selected and the field is present.
.anycast	Indicator.Attribute	Is Anycast	N/A	true	When selected; store the boolean as a string.
.postal	Indicator.Attribute	Postal Code	N/A	94043	When selected; preserve as a string.
.timezone	Indicator.Attribute	Timezone	N/A	America/Los_Angeles	Ingested when its Context Filter option is selected and the field is present.
.asn.asn	Related Indicator.Value	ASN	N/A	15169	Requires ASN in Context Filter and Ingest ASNs As = Indicators (default). Remove the leading AS prefix from AS15169, trim whitespace, and retain the numeric portion as a string. Relate the ASN indicator to the original IP.
.asn.asn	Indicator.Attribute	ASN	N/A	AS15169	Requires ASN in Context Filter and Ingest ASNs As = Attributes. Store on the original IP; do not create an ASN indicator.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.asn.name	Indicator.Attribute / Related Indicator.Attribute	AS Organization	N/A	Google LLC	Requires the matching Context Filter option. Stored on the original IP in Attributes mode, or the related ASN in Indicators mode; creating the ASN also requires ASN to be selected.
.asn.domain	Indicator.Attribute / Related Indicator.Attribute	AS Domain	N/A	google.com	Requires the matching Context Filter option. Stored on the original IP in Attributes mode, or the related ASN in Indicators mode; creating the ASN also requires ASN to be selected.
.asn.route	Indicator.Attribute / Related Indicator.Attribute	Network	N/A	8.8.8.0/24	Requires the matching Context Filter option. Stored on the original IP in Attributes mode, or the related ASN in Indicators mode; creating the ASN also requires ASN to be selected. Preserve the CIDR value.
.asn.type	Indicator.Attribute / Related Indicator.Attribute	AS Type	N/A	hosting	Requires the matching Context Filter option. Stored on the original IP in Attributes mode, or the related ASN in Indicators mode; creating the ASN also requires ASN to be selected.
.company.name	Indicator.Attribute	Company Name	N/A	Google LLC	Ingested when its Context Filter option is selected and the field is present.
.company.domain	Indicator.Attribute	Company Domain	N/A	google.com	Ingested when its Context Filter option is selected and the field is present.
.company.type	Indicator.Attribute	Company Type	N/A	hosting	Ingested when its Context Filter option is selected and the field is present.
.privacy.vpn	Indicator.Attribute	Is VPN	N/A	false	When selected; retain both true and false values as strings.
.privacy.proxy	Indicator.Attribute	Is Proxy	N/A	false	When selected; retain both true and false values as strings.
.privacy.tor	Indicator.Attribute	Is TOR	N/A	false	When selected; retain both true and false values as strings.
.privacy.relay	Indicator.Attribute	Is Relay	N/A	false	When selected; retain both true and false values as strings.
.privacy.hosting	Indicator.Attribute	Is Hosting	N/A	true	When selected; retain both true and false values as strings.
.privacy.service	Indicator.Attribute	Privacy Service	N/A	Empty string in sample	When selected; skip when empty or null.
.abuse.address	Indicator.Attribute	Abuse Contact Address	N/A	US, CA, Mountain View, 1600 Amphitheatre Parkway, 94043	When selected; preserve the complete address as one value.
.abuse.country	Indicator.Attribute	Abuse Contact Country Code	N/A	US	Ingested when its Context Filter option is selected and the field is present.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.abuse.email	Indicator.Attribute	Abuse Contact Email	N/A	network-abuse@google.com	Ingested when its Context Filter option is selected and the field is present.
.abuse.name	Indicator.Attribute	Abuse Contact Name	N/A	Abuse	Ingested when its Context Filter option is selected and the field is present.
.abuse.network	Indicator.Attribute	Abuse Contact Network	N/A	8.8.8.0/24	Ingested when its Context Filter option is selected and the field is present.
.abuse.phone	Indicator.Attribute	Abuse Contact Phone	N/A	+1-650-253-0000	When selected; preserve as a string.
.domains.ip	Indicator.Value	IP Address	N/A	8.8.8.8	When present, must match the original IP before domain context is used. A mismatch skips Hosted Domain Count and Related Domains. No duplicate IP is created.
.domains.total	Indicator.Attribute	Hosted Domain Count	N/A	9791	When selected; this can exceed the number of domains included in the response. Retain zero when returned.
.domains.domains[]	Related Indicator.Value	FQDN	N/A	musicool.cn, kagou.vip, nmgk2.com, 91xiazai.com, bits-hyderabad.ac.in	When selected; requires Related Domains in Context Filter. Create one indicator per distinct nonempty domain and relate it to the original IP. Trim whitespace, lowercase names, and remove trailing dots.

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	100
Indicator Attributes	400

Use Case Example

1. A Threat Analyst identifies a collection of IP Addresses they would like to enrich.
2. The Threat Analyst adds the IPInfo Action to a Workflow
3. The Threat Analyst configures the action with the desired parameters, and enables the Workflow
4. The Workflow executes all Actions in the graph, including IPInfo
5. The action returns the documented Attributes from the provider, and the Workflow ingests this data into the ThreatQ platform.

Known Issues / Limitations

- The IPInfo Free plan is limited to 50k lookups per month. Refer to your IPInfo account details for rate limit information.

Change Log

- **Version 1.1.0**
  - Added optional mappings for hostname, anycast status, postal code, timezone, ASN, company, privacy, abuse contact, hosted domain count, and related domains.
  - Added **Ingest ASNs As** to choose whether related ASNs are ingested as indicators or added as attributes to the original IP.
  - Added Context Filter configuration selections and guidance about enterprise token requirements. The four existing location defaults are unchanged.
  - Added support for single-object and list responses, with handling for missing or null fields while retaining valid false and zero values.
- **Version 1.0.3**
  - Updated the **Country** display label to **Country Code** in the integration mappings and **IPInfo Context Filter** configuration parameter options for improved clarity and consistency.
- **Version 1.0.2**
  - Initial release to the ThreatQ Marketplace.