ThreatQuotient

IPInfo Action Guide

Version 1.0.2

December 06, 2022

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	1.0.2
Compatible with ThreatQ Versions	>= 5.6.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/ipinfo-action

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 action can perform the following function:

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

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

This action is intended for use with ThreatQ TRD 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 (TQO) 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 file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action 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 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

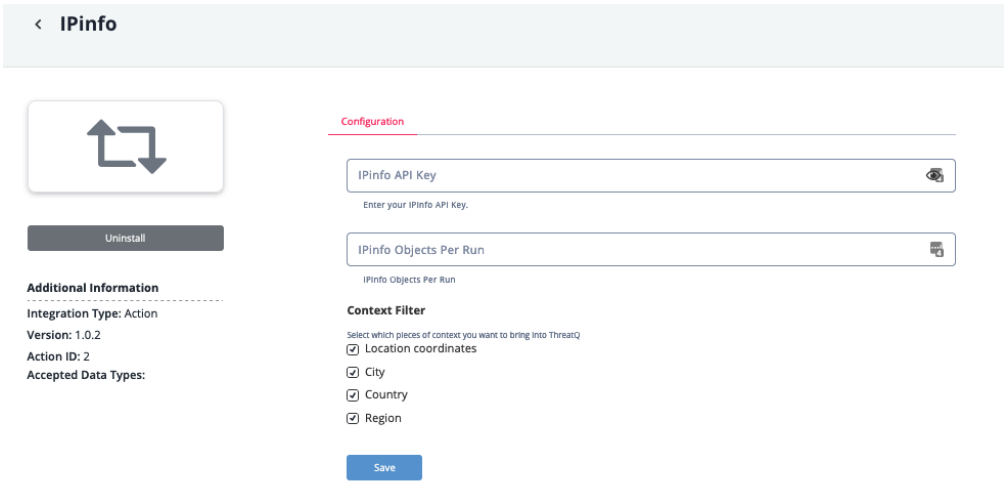
> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

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)



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

Action Functions

The action provides the following function:

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

IPInfo

The IPInfo function 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}
```

Sample Response:

```
{
    "ip": "111.121.216.118",
    "city": "Guiyang",
    "region": "Guizhou",
    "country": "CN",
    "loc": "26.5833,106.7167",
    "org": "AS4134 CHINANET-BACKBONE",
    "timezone": "Asia/Shanghai"
}
```

ThreatQuotient provides the following default mapping for this function:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.region`	Indicator.Attribute	Region	N/A	Guizhou	If enabled
`.city`	Indicator.Attribute	City	N/A	Guiyang	If enabled
`.country`	Indicator.Attribute	Country	N/A	CN	If enabled
`.loc`	Indicator.Attribute	Location Coordinates	N/A	26.5833,106.7167	If enabled

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 1.0.2**
  - Initial release to the ThreatQ Marketplace.