ThreatQuotient

A Securonix Company

Scamalytics Action

Version 1.0.0

October 28, 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.

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	>= 5.12.1
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

Scamalytics provides fraud detection services to organizations by analyzing IP addresses and user behavior. The Scamalytics fraud risk API assesses the reputation of IP addresses, identifies proxy usage, and provides a fraud risk score. Additionally, Scamalytics uses shared blacklists and machine learning to detect high-risk users, particularly in industries like banking, payments, and dating services, helping businesses protect their customers and revenue from fraudulent activities.

The Scamalytics Action for ThreatQ allows users to automatically bulk lookup IP addresses, against Scamalytics's API. The action will fetch geolocation, proxy attributes, risk scores, and other information for each IP address, ingesting the results into ThreatQ.

The integration provides the following actions:

- **Scamalytics - Enrich IPs** - performs IP lookups against Scamalytics to fetch contextual information about how fraudulent an IP address may be.

The integration is compatible with the following object types:

- Indicators (IP Address)

The integration enriched the following object types:

- Indicators (IP Address, ASN)

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 data collection containing the following indicator objects:
  - IP Address
- A Scamalytics 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 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.

Scamalytics - Enrich IPs Parameters

PARAMETER	DESCRIPTION
API Region / Node	Select the region based on the region you selected when signing up for Scamalytics. • USA • Europe
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.
Username	Enter your Scamalytics username associated with your API Token.
API Token	Enter your Scamalytics API Token.

PARAMETER	DESCRIPTION
Selected Scamalytics Context	Select the primary context you would like to ingest with each enriched IP address (if available). This is useful for filtering out data you don't want to ingest, so your team can focus on the most relevant information to your organization. • Is Live • Scamalytics Score (Risk Score) (default) • Scamalytics Risk (Risk) (default) • Scamalytics Link • ISP (Premium Required) • ISP Score (default) • ISP Risk (default) • Organization (Premium Required) • Is VPN • Is Data Center • Is Apple iCloud Private Relay • Is Amazon AWS • Is Google
Re-map Scamalytics Risk Score	Scamalytics provides a risk score from 0-100 as well as their own normalized risk score. This option allows you to re-map the Scamalytics risk score to a custom normalized risk value.
Custom Risk Score Normalization Mapping	A mapping to normalize the numeric risk score values to the scorable attribute, "Normalized Risk". You may enter any number of mappings here. Shows when the **Re-map Scamalytics Risk Score** field is checked. • 0,25,Low | 26,50,Medium | 51,75,High | 76,100,Critical
Re-map Scamalytics ISP Score	Scamalytics provides an ISP score from 0-100 as well as their own normalized ISP score. This option allows you to re-map the Scamalytics ISP score to a custom normalized ISP value.
Custom ISP Score Normalization Mapping	A mapping to normalize the numeric ISP score values to the scorable attribute, "Normalized ISP". You may enter any number of mappings here. Shows when the **Re-map Scamalytics Risk Score** field is checked. • 0,25,Low | 26,50,Medium | 51,75,High | 76,100,Critical

PARAMETER	DESCRIPTION
Only Ingest True Flags	Scamalytics provides a handful of flags that indicate whether an IP address is associated with a specific type of activity (e.g., VPN, Data Center, Apple iCloud Private Relay, etc.). This option allows you to only ingest the flags as attributes if they are true. If this is disabled, all flags will be ingested regardless of their value. Be careful, enabling this after ingesting True values is risky, as it will permanently prevent those attributes from ever becoming False.
Selected External Datasources	Select the external datasources you would like to ingest context from. Different data sources may have overlapping context. • DB IP (Premium Required) • IP2Proxy (Premium Required) • IP2Proxy Lite • `MaxMind GeoLite2` • IPInfo • FireHOL • IPsum • X4BNet • Google • Amazon AWS • Apple iCloud Private Relay
Base DB IP Context	Select the specific context you would like to ingest from the DB IP datasource. Certain fields may not be available for all IP addresses. Shows when **DB IP** is selected in the **Selected External Datasources** field. • Country • Country Code • State • District • City • Postal Code • Geolocation
IP2Proxy Context	Select the specific context you would like to ingest from the IP2Proxy datasource. Shows when **IP2Proxy** is selected in the **Selected External Datasources** field. • Proxy Type

PARAMETER	DESCRIPTION
IP2Proxy Lite Context	Select the specific context you would like to ingest from the IP2Proxy Lite datasource. Shows when **IP2Proxy Lite** is selected in the **Selected External Datasources** field. • ASN • AS Organization • Proxy Type • Blacklist Type • Proxy Provider • Country Code • Country • District • City
MaxMind GeoLite2 Context	Select the specific context you would like to ingest from the MaxMind GeoLite2 datasource. Shows when **MaxMind GeoLite2** is selected in the **Selected External Datasources** field. • ASN • AS Organization • Country Code • Country • State • City • District • Metro Code • Postal Code • Geolocation
IPInfo Context	Select the specific context you would like to ingest from the IPInfo datasource. Shows when **IPInfo** is selected in the **Selected External Datasources** field. • ASN • AS Organization • IP Range From • IP Range To • Country • Country Code • Continent • Continent Code

PARAMETER	DESCRIPTION
FireHOL Context	Select the specific context you would like to ingest from the FireHOL datasource. Shows when **FireHOL** is selected in the **Selected External Datasources** field. • Is Proxy
IPsum Context	Select the specific context you would like to ingest from the IPsum datasource. Shows when **IPsum** is selected in the **Selected External Datasources** field. • Blacklist Count
X4BNet Context	Select the specific context you would like to ingest from the X4BNet datasource. Shows when **X4BNet** is selected in the **Selected External Datasources** field. • Is TOR • Is Spambot • Is Opera Mini Bot • Is Semrush Bot
Google Context	Select the specific context you would like to ingest from the Google datasource. Shows when **Google** is selected in the **Selected External Datasources** field. • Is Google Bot • Is Special Crawler • Is User Triggered Fetcher
Amazon AWS Context	Select the specific context you would like to ingest from the Amazon AWS datasource. Shows when **Amazon AWS** is selected in the **Selected External Datasources** field. • Amazon AWS Region • Amazon AWS Service
Apple iCloud Private Relay Context	Select the specific context you would like to ingest from the Apple iCloud Private Relay datasource. Shows when **Apple iCloud Private Relay** is selected in the **Selected External Datasources** field. • Country Code • City

PARAMETER	DESCRIPTION
Stop Processing When Remaining Credits Drop Below	The number of credits remaining in your Scamalytics account before the workflow will stop processing. Set this to 0 to use all available credits.
Objects Per Run	The number of objects to process per run of the workflow.

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
Scamalytics - Erich IPs	Performs a bulk lookup of IPs against Scamalytics	Indicators	IP Address

Action

The Scamalytics - Erich IPs action enriches IP addresses in your Threat Library by performing lookups against Scamalytics's fraud risk API. The action fetches contextual information about how fraudulent an IP address may be, including geolocation, proxy attributes, risk scores, and other relevant data. The results are then ingested into ThreatQ as enriched indicators.

```
GET https://api11.scamalytics.com/v3/{{ username }}?key={{ api_token }}
&ip={{ ip_address }}
```

Sample Response:


```
{
  "scamalytics": {
    "status": "ok",
    "mode": "live",
    "ip": "66.220.149.25",
    "scamalytics_score": 0,
    "scamalytics_risk": "low",
    "scamalytics_url": "https://scamalytics.com/ip/66.220.149.25",
    "scamalytics_isp": "Facebook, Inc.",
    "scamalytics_org": "Facebook, Inc.",
    "scamalytics_isp_score": 0,
    "scamalytics_isp_risk": "low",
    "scamalytics_proxy": {
      "is_datacenter": true,
      "is_vpn": true,
      "is_apple_icloud_private_relay": true,
      "is_amazon_aws": true,
      "is_google": true
    },
    "is_blacklisted_external": true,
    "credits": {
      "used": 95,
      "remaining": 11905,
      "last_sync_timestamp_utc": "2024-03-27 12:13:03",
      "seconds_elapsed_since_last_sync": 31,
```

```
    "note": "Credits used and remaining are approximate values."
  },
  "exec": "6.99 ms"
},
"external_datasources": {
  "dbip": {
    "ip_country_code": "US",
    "ip_state_name": "Virginia",
    "ip_district_name": "Loudoun",
    "ip_city": "Sterling",
    "ip_postcode": "20163",
    "ip_geolocation": "39.0067,-77.4291",
    "ip_country_name": "United States",
    "isp_name": "Facebook, Inc.",
    "org_name": "Facebook, Inc.",
    "connection_type": "",
    "history_monthly": {
      "09-2023": {
        "isp_name": "Facebook, Inc.",
        "org_name": "Facebook, Inc."
      },
      "10-2023": {
        "isp_name": "Facebook, Inc.",
        "org_name": "Facebook, Inc."
      },
      "11-2023": {
        "isp_name": "Facebook, Inc.",
        "org_name": "Facebook, Inc."
      },
      "datasource_name": "db-ip.com",
      "license_info": "info@scamalytics.com"
    }
  },
  "ip2proxy": {
    "proxy_type": "SES",
    "datasource_name": "ip2proxy.com",
    "license_info": "info@scamalytics.com"
  },
  "ip2proxy_lite": {
    "asn": "32934",
    "as_name": "FACEBOOK",
    "proxy_type": "SES",
    "proxy_last_seen": 30,
    "usage_type": "COM",
    "ip_blacklisted": true,
    "ip_blacklist_type": "BOTNET",
    "ip_provider": "NordVPN",
    "ip_country_code": "US",
    "ip_country_name": "United States",
    "ip_district_name": "",
```

```
    "ip_city": "Prineville",
    "isp_name": "Facebook, Inc.",
    "domain": "facebook.com",
    "datasource_name": "https://lite.ip2location.com/ip2proxy-lite",
    "license_info": "https://creativecommons.org/licenses/by-sa/4.0"
  },
  "maxmind_geolite2": {
    "asn": "32934",
    "as_name": "FACEBOOK",
    "ip_geoname_id": "5746901",
    "ip_location_accuracy_km": "20",
    "ip_country_code": "US",
    "ip_state_name": "Oregon",
    "ip_district_name": "",
    "ip_city": "Prineville",
    "ip_metro_code": "821",
    "ip_postcode": "97754",
    "ip_geolocation": "44.3041,-120.8364",
    "ip_country_name": "United States",
    "ip_time_zone": "America/Los_Angeles",
    "datasource_name": "maxmind.com and geonames.org",
    "license_info": "https://creativecommons.org/licenses/by-sa/4.0"
  },
  "ipinfo": {
    "asn": "32934",
    "ip_range_from": "66.220.144.248",
    "ip_range_to": "66.220.155.127",
    "as_name": "Facebook, Inc.",
    "as_domain": "facebook.com",
    "ip_country_code": "US",
    "ip_country_name": "United States",
    "ip_continent_code": "NA",
    "ip_continent_name": "North America",
    "datasource_name": "ipinfo.io",
    "license_info": "https://creativecommons.org/licenses/by-sa/4.0"
  },
  "firehol": {
    "ip_blacklisted_30": false,
    "ip_blacklisted_1day": false,
    "is_proxy": false,
    "last_updated_timestamp_utc": "2024-03-27 12:13:03",
    "datasource_name": "https://iplists.firehol.org/",
    "license_info": "GPL v2"
  },
  "ipsum": {
    "ip_blacklisted": true,
    "num_blacklists": 7,
    "last_updated_timestamp_utc": "2024-03-27 12:13:03",
    "datasource_name": "https://github.com/stamparm/ipsum",
    "license_info": "https://unlicense.org/"
```

```
  },
  "spamhaus_drop": {
    "ip_blacklisted": true,
    "last_updated_timestamp_utc": "2024-03-27 12:13:03",
    "datasource_name": "https://www.spamhaus.org/drop",
    "license_info": "https://www.spamhaus.org/drop/terms/"
  },
  "x4bnet": {
    "is_vpn": true,
    "is_datacenter": true,
    "is_tor": false,
    "is_blacklisted_spambot": false,
    "is_bot_operamini": false,
    "is_bot_semrush": true,
    "last_updated_timestamp_utc": "2024-03-27 12:13:03",
    "datasource_name": "https://github.com/X4BNet/",
    "license_info": "https://www.gnu.org/licenses/agpl-3.0.en.html"
  },
  "google": {
    "is_google_general": false,
    "is_googlebot": false,
    "is_special_crawler": false,
    "is_user_triggered_fetcher": false,
    "last_updated_timestamp_utc": "2024-12-10 12:00:03",
    "datasource_name": "https://developers.google.com/"
  },
  "amazon_aws": {
    "data": [
      {
        "ip_prefix": "3.5.140.0/22",
        "region": "ap-northeast-2",
        "service": "EC2",
        "network_border_group": "ap-northeast-2"
      }
    ],
    "last_updated_timestamp_utc": "2024-12-10 13:00:16",
    "datasource_name": "https://docs.aws.amazon.com/"
  },
  "apple_icloud_private_relay": {
    "data": [
      {
        "ip_prefix": "172.224.224.0/27",
        "country_code": "GB",
        "state_code": "GB-EN",
        "city": "London"
      }
    ],
    "last_updated_timestamp_utc": "2024-12-10 13:00:16",
    "datasource_name": "https://developer.apple.com/"
  }
```

```
  }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.scamalytics.scamalytics_score`	Attribute	Risk Score	N/A	`10`	User-configurable. Updatable
`.scamalytics.scamalytics_score`	Attribute	Normalized Risk	N/A	`Indeterminate`	User-configurable. Updatable. Based on user-mapping
`.scamalytics.scamalytics_risk`	Attribute	Risk	N/A	`Low`	User-configurable. Updatable
`.scamalytics.scamalytics_isp_score`	Attribute	ISP Risk Score	N/A	`10`	User-configurable. Updatable
`.scamalytics.scamalytics_isp_score`	Attribute	Normalized ISP Risk	N/A	`Low`	User-configurable. Updatable. Based on user-mapping
`.scamalytics.scamalytics_isp_risk`	Attribute	ISP Risk	N/A	`Low`	User-configurable. Updatable.
`.scamalytics.mode`	Attribute	Is Live	N/A	`True`	User-configurable. Updatable. True if value is live, otherwise False
`.scamalytics.scamalytics_url`	Attribute	Scamalytics Link	N/A	`https://scamalytics.com/ip/<IP_ADDRESS>`	User-configurable
`.scamalytics.scamalytics_isp`	Attribute	ISP	N/A	`Facebook, Inc.`	User-configurable
`.scamalytics.scamalytics_org`	Attribute	Organization	N/A	`Facebook, Inc.`	User-configurable
`.scamalytics.scamalytics_proxy.is_vpn`	Attribute	Is VPN	N/A	`True`	User-configurable. Updatable
`.scamalytics.scamalytics_proxy.is_datacenter`	Attribute	Is Data Center	N/A	`False`	User-configurable. Updatable
`.scamalytics.scamalytics_proxy.is_apple_icloud_private_relay`	Attribute	Is Apple iCloud Private Relay	N/A	`False`	User-configurable. Updatable
`.scamalytics.scamalytics_proxy.is_amazon_aws`	Attribute	Is Amazon AWS	N/A	`False`	User-configurable. Updatable
`.scamalytics.scamalytics_proxy.is_google`	Attribute	Is Google	N/A	`False`	User-configurable. Updatable
`.external_datasources.dbip.ip_country_name`	Attribute	Country	N/A	`United States`	User-configurable. If `DB IP (Premium Required)` datasource enabled.
`.external_datasources.dbip.ip_country_code`	Attribute	Country Code	N/A	`US`	User-configurable. If `DB IP (Premium Required)` datasource enabled.
`.external_datasources.dbip.ip_state_name`	Attribute	State	N/A	`Virginia`	User-configurable. If `DB IP (Premium Required)` datasource enabled.
`.external_datasources.dbip.ip_district_name`	Attribute	District	N/A	`Loudoun`	User-configurable. If `DB IP (Premium Required)` datasource enabled.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.external_datasources.dbip.ip_city	Attribute	City	N/A	Sterling	User-configurable. If DB IP (Premium Required) datasource enabled.
.external_datasources.dbip.ip_postcode	Attribute	Postal Code	N/A	20163	User-configurable. If DB IP (Premium Required) datasource enabled.
.external_datasources.dbip.ip_geolocation	Attribute	Geolocation	N/A	39.0067,-77.4291	User-configurable. If DB IP (Premium Required) datasource enabled.
.external_datasources.ip2proxy.proxy_type	Attribute	Proxy Type	N/A	SES	User-configurable. If IP2Proxy (Premium Required) datasource enabled.
.external_datasources.ip2proxy_lite.proxy_type	Attribute	Proxy Type	N/A	SES	User-configurable. If IP2Proxy Lite datasource enabled.
.external_datasources.ip2proxy_lite.blacklist_type	Attribute	Blacklist Type	N/A	BOTNET	User-configurable. If IP2Proxy Lite datasource enabled.
.external_datasources.ip2proxy_lite.proxy_provider	Attribute	Proxy Provider	N/A	N/A	User-configurable. If IP2Proxy Lite datasource enabled.
.external_datasources.ip2proxy_lite.ip_country_code	Attribute	Country Code	N/A	US	User-configurable. If IP2Proxy Lite datasource enabled.
.external_datasources.ip2proxy_lite.ip_country_name	Attribute	Country	N/A	United States	User-configurable. If IP2Proxy Lite datasource enabled.
.external_datasources.ip2proxy_lite.ip_district_name	Attribute	District	N/A	N/A	User-configurable. If IP2Proxy Lite datasource enabled.
.external_datasources.ip2proxy_lite.ip_city	Attribute	City	N/A	Prineville	User-configurable. If IP2Proxy Lite datasource enabled.
.external_datasources.maxmind_geolite2.ip_country_code	Attribute	Country Code	N/A	US	User-configurable. If MaxMind GeoLite2 datasource enabled.
.external_datasources.maxmind_geolite2.ip_country_name	Attribute	Country	N/A	United States	User-configurable. If MaxMind GeoLite2 datasource enabled.
.external_datasources.maxmind_geolite2.ip_state_name	Attribute	State	N/A	N/A	User-configurable. If MaxMind GeoLite2 datasource enabled.
.external_datasources.maxmind_geolite2.ip_district_name	Attribute	District	N/A	N/A	User-configurable. If MaxMind GeoLite2 datasource enabled.
.external_datasources.maxmind_geolite2.ip_city	Attribute	City	N/A	Prineville	User-configurable. If MaxMind GeoLite2 datasource enabled.
.external_datasources.maxmind_geolite2.ip_metro_code	Attribute	Metro Code	N/A	821	User-configurable. If MaxMind GeoLite2 datasource enabled.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.external_datasources.maxmind_geolite2.ip_postcode`	Attribute	Postal Code	N/A	`97754`	User-configurable. If `MaxMind GeoLite2` datasource enabled.
`.external_datasources.maxmind_geolite2.ip_geolocation`	Attribute	Geolocation	N/A	`44.3041,-120.8364`	User-configurable. If `MaxMind GeoLite2` datasource enabled.
`.external_datasources.ipinfo.ip_range_from`	Attribute	IP Range From	N/A	`66.220.144.248`	User-configurable. If `IPInfo` datasource enabled.
`.external_datasources.ipinfo.ip_range_to`	Attribute	IP Range To	N/A	`66.220.144.255`	User-configurable. If `IPInfo` datasource enabled.
`.external_datasources.ipinfo.ip_country_name`	Attribute	Country	N/A	`United States`	User-configurable. If `IPInfo` datasource enabled.
`.external_datasources.ipinfo.ip_country_code`	Attribute	Country Code	N/A	`US`	User-configurable. If `IPInfo` datasource enabled.
`.external_datasources.ipinfo.ip_continent_code`	Attribute	Continent Code	N/A	`NA`	User-configurable. If `IPInfo` datasource enabled.
`.external_datasources.ipinfo.ip_continent_name`	Attribute	Continent Name	N/A	`North America`	User-configurable. If `IPInfo` datasource enabled.
`.external_datasources.firehol.is_proxy`	Attribute	Is Proxy	N/A	`False`	User-configurable. Updatable. If `FireHOL` datasource enabled.
`.external_datasources.ipsum.num_blacklists`	Attribute	Blacklist Count	N/A	`7`	User-configurable. Updatable. If `IPsum` datasource enabled.
`.external_datasources.x4bnet.is_tor`	Attribute	Is TOR	N/A	`False`	User-configurable. Updatable. If `X4BNet` datasource enabled.
`.external_datasources.x4bnet.is_blacklisted_spambot`	Attribute	Is Spambot	N/A	`False`	User-configurable. Updatable. If `X4BNet` datasource enabled.
`.external_datasources.x4bnet.is_bot_operamini`	Attribute	Is Opera Mini Bot	N/A	`False`	User-configurable. Updatable. If `X4BNet` datasource enabled.
`.external_datasources.x4bnet.is_bot_semrush`	Attribute	Is Semrush Bot	N/A	`True`	User-configurable. Updatable. If `X4BNet` datasource enabled.
`.external_datasources.google.is_googlebot`	Attribute	Is Google Bot	N/A	`False`	User-configurable. Updatable. If `Google` datasource enabled.
`.external_datasources.google.is_special_crawler`	Attribute	Is Special Crawler	N/A	`False`	User-configurable. Updatable. If `Google` datasource enabled.
`.external_datasources.google.is_user_triggered_fetcher`	Attribute	Is User Triggered Fetcher	N/A	`False`	User-configurable. Updatable. If `Google` datasource enabled.
`.external_datasources.amazon_aws.data[].region`	Attribute	AWS Region	N/A	`us-west-2`	User-configurable. If `Amazon AWS` datasource enabled.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.external_datasources.amazon_aws.data[].service`	Attribute	AWS Service	N/A	`EC2`	User-configurable. If `Amazon AWS` datasource enabled.
`.external_datasources.apple_icloud_private_relay.data[].country_code`	Attribute	Country Code	N/A	`GB`	User-configurable. If `Apple iCloud Private Relay` datasource enabled.
`.external_datasources.apple_icloud_private_relay.data[].city`	Attribute	City	N/A	`London`	User-configurable. If `Apple iCloud Private Relay` datasource enabled.
`.external_datasources.ip2proxy_lite.as_name`	Attribute	AS Organization	N/A	`Facebook, Inc.`	User-configurable. If `IP2Proxy Lite` datasource enabled.
`.external_datasources.maxmind_geolite2.as_name`	Attribute	AS Organization	N/A	`Facebook, Inc.`	User-configurable. If `MaxMind GeoLite2` datasource enabled.
`.external_datasources.ipinfo.as_name`	Attribute	AS Organization	N/A	`Facebook, Inc.`	User-configurable. If `IPInfo` datasource enabled.
`.external_datasources.ip2proxy_lite.asn`	Related Indicator Value	ASN	N/A	`32934`	User-configurable. If `IP2Proxy Lite` datasource enabled.
`.external_datasources.maxmind_geolite2.asn`	Related Indicator Value	ASN	N/A	`32934`	User-configurable. If `MaxMind GeoLite2` datasource enabled.
`.external_datasources.ipinfo.asn`	Related Indicator Value	ASN	N/A	`32934`	User-configurable. If `IPInfo` datasource 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.

Scamalytics Enrich-IPs

METRIC	RESULT
Run Time	2 minutes
Indicators	279
Indicator Attributes	5,109

Use Case Example

I have a list of IP Addresses and want to figure out the likelihood of any of them being used for fraudulent activity. I can use this action to enrich each IP with Scamalytics data, including risk scores, proxy information, ISP information, and additional context from various aggregated external data sources.

Known Issues / Limitations

- Be aware of your API rate limits and configure the `Objects Per Run` setting accordingly.
- If True values have already been ingested, activating `Only Ingest True` Flags will stop those attributes from ever becoming `False`.

Change Log

- **Version 1.0.0**
  - Initial release