

# ThreatQuotient

A Securonix Company



## Cisco Umbrella Investigate Operation

**Version 3.0.0**

September 08, 2026

**ThreatQuotient**

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147

 **ThreatQ Supported**

### **Support**

Email: [tq-support@securonix.com](mailto:tq-support@securonix.com)

Web: <https://ts.securonix.com>

Phone: 703.574.9893

# Contents

|                                   |           |
|-----------------------------------|-----------|
| <b>Warning and Disclaimer</b>     | <b>3</b>  |
| <b>Support</b>                    | <b>4</b>  |
| <b>Integration Details</b>        | <b>5</b>  |
| <b>Introduction</b>               | <b>6</b>  |
| <b>Prerequisites</b>              | <b>7</b>  |
| <b>Installation</b>               | <b>8</b>  |
| <b>Configuration</b>              | <b>9</b>  |
| <b>Actions</b>                    | <b>10</b> |
| Enrich                            | 11        |
| Get Categorizations               | 11        |
| Get Risk Scores                   | 12        |
| Get Security Context              | 13        |
| Get WHOIS                         | 15        |
| Get Related Domains               | 16        |
| Get Domain History                | 17        |
| Run Configuration Options         | 18        |
| Get Samples                       | 19        |
| Reverse WHOIS                     | 21        |
| Get Associated Names              | 22        |
| <b>Known Issues / Limitations</b> | <b>23</b> |
| <b>Change Log</b>                 | <b>24</b> |

## 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:** [tq-support@securonix.com](mailto: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** 3.0.0

**Compatible with ThreatQ Versions**  $\geq 4.57.0$

**Support Tier** ThreatQ Supported

# Introduction

The Cisco Umbrella Investigate Operation for ThreatQuotient enables a user to enrich indicators in ThreatQ with context from Cisco Umbrella.

The operation provides the following actions:

- **Enrich** - enriches a domain with contextual or historical metadata.
- **Get Samples** - retrieves Cisco Threat Grid samples that are related to a given domain, IP, or URL.
- **Reverse WHOIS** - retrieves domains related to a given email address.
- **Get Associated Names** - retrieves domains related to a given IP Address.

The operation is compatible with the following indicator types:

- Email Address
- FQDN
- IP Address
- URL

# Prerequisites

The following is required to run the integration:

- A Cisco Umbrella API Client ID.
- A Cisco Umbrella API Client Secret.

# 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 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 parameter under the **Configuration** tab:

## PARAMETER

## DESCRIPTION

### Client ID

Enter your Cisco Umbrella API Client ID to authenticate.

### Client Secret

Enter your Cisco Umbrella API Client Secret to authenticate.

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        |
|--------------------------------------|-------------------------------------------------------------------------------------|-------------|-----------------------|
| <a href="#">Enrich</a>               | Enriches a domain with contextual or historical metadata.                           | Indicator   | FQDN                  |
| <a href="#">Get Samples</a>          | Retrieves Cisco Threat Grid samples that are related to a given domain, IP, or URL. | Indicator   | FQDN, IP Address, URL |
| <a href="#">Reverse WHOIS</a>        | Retrieves domains related to a given email address.                                 | Indicator   | Email Address         |
| <a href="#">Get Associated Names</a> | Retrieves domains related to a given IP Address.                                    | Indicator   | IP Address            |

## Enrich

The Enrich action retrieves one or more enrichment datasets for a domain from Cisco Umbrella Investigate v2.

### Get Categorizations

GET <https://api.umbrella.com/investigate/v2/domains/categorization/{domain}>

#### Sample Response:

```
{
  "facebook.com": {
    "status": 1,
    "security_categories": ["150"],
    "content_categories": ["Social Networking"]
  }
}
```

ThreatQ provides the following default mapping for this dataset:

| FEED DATA PATH           | THREATQ ENTITY      | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES          | NOTES                                       |
|--------------------------|---------------------|--------------------------------------|----------------|-------------------|---------------------------------------------|
| .*.security_categories[] | Indicator.Attribute | Security Category                    | N/A            | 150               | Same mapping as the previous implementation |
| .*.content_categories[]  | Indicator.Attribute | Content Category                     | N/A            | Social Networking | Same mapping as the previous implementation |

## Get Risk Scores

GET <https://api.umbrella.com/investigate/v2/domains/risk-score/{domain}>

### Sample Response:

```
{
  "risk_score": 6,
  "indicators": [
    {
      "indicator": "Geo Popularity Score",
      "indicator_id": "Geo Popularity Score",
      "normalized_score": 2,
      "score": -3.6108782
    }
  ]
}
```

ThreatQ provides the following default mapping for this dataset:

| FEED DATA PATH                 | THREATQ ENTITY      | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES             | NOTES                                                           |
|--------------------------------|---------------------|--------------------------------------|----------------|----------------------|-----------------------------------------------------------------|
| risk_score                     | Indicator.Attribute | Risk Score                           | N/A            | 6                    | Main risk score value                                           |
| .indicators[].indicator        | Indicator.Attribute | Scoring Indicator                    | N/A            | Geo Popularity Score | Used as the attribute name shown in the scoring breakdown table |
| .indicators[].normalized_score | Indicator.Attribute | Normalized Score                     | N/A            | 2                    | Displayed in the scoring breakdown table                        |
| .indicators[].score            | Indicator.Attribute | Raw Score                            | N/A            | -3.6108782           | Displayed in the scoring breakdown table                        |

## Get Security Context

GET <https://api.umbrella.com/investigate/v2/security/name/{domain}>

### Sample Response:

```
{
  "perplexity": 0.18786756104373362,
  "entropy": 1.9182958340544896,
  "dga_score": 38.301771886101335,
  "securerank2": -1.3135141095601992,
  "pagerank": 4.072185,
  "threat_type": "",
  "geodiversity_normalized": [
    ["BM", 0.18798495007664884]
  ]
}
```

ThreatQ provides the following default mapping for this dataset:

| FEED DATA PATH | THREATQ ENTITY      | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES            | NOTES                      |
|----------------|---------------------|--------------------------------------|----------------|---------------------|----------------------------|
| .dga_score     | Indicator.Attribute | DGA Score                            | N/A            | 38.301771886101335  | N/A                        |
| .perplexity    | Indicator.Attribute | Perplexity                           | N/A            | 0.18786756104373362 | N/A                        |
| .entropy       | Indicator.Attribute | Entropy                              | N/A            | 1.9182958340544896  | N/A                        |
| .securerank2   | Indicator.Attribute | Securerank                           | N/A            | -1.3135141095601992 | N/A                        |
| .pagerank      | Indicator.Attribute | Page Rank                            | N/A            | 4.072185            | N/A                        |
| .asn_score     | Indicator.Attribute | ASN Score                            | N/A            | -29.75810625887133  | N/A                        |
| .prefix_score  | Indicator.Attribute | Prefix Score                         | N/A            | -64.9070502788884   | N/A                        |
| .rip_score     | Indicator.Attribute | RIP Score                            | N/A            | -75.64720536038982  | N/A                        |
| .popularity    | Indicator.Attribute | Popularity                           | N/A            | 25.335450495507196  | N/A                        |
| .fastflux      | Indicator.Attribute | Fastflux                             | N/A            | false               | N/A                        |
| .attack        | Indicator.Attribute | Attack                               | N/A            | false               | N/A                        |
| .threat_type   | Indicator.Attribute | Threat Type                          | N/A            | benign              | Empty values are not added |

| FEED DATA PATH             | THREATQ ENTITY      | THREATQ OBJECT TYPE OR ATTRIBUTE KEY  | PUBLISHED DATE | EXAMPLES                    | NOTES                                        |
|----------------------------|---------------------|---------------------------------------|----------------|-----------------------------|----------------------------------------------|
| .geoscore                  | Indicator.Attribute | Geodiversity Score                    | N/A            | N/A                         | N/A                                          |
| .ks_test                   | Indicator.Attribute | Kolmogorov-Smirnov Geodiversity Score | N/A            | N/A                         | N/A                                          |
| .geodiversity_normalized[] | Indicator.Attribute | Country Code / Geodiversity Score     | N/A            | ['BM', 0.18798495007664884] | Rendered in the geodiversity breakdown table |

## Get WHOIS

GET <https://api.umbrella.com/investigate/v2/whois/{domain}>

### Sample Response:

```
{
  "registrarName": "MarkMonitor, Inc.",
  "nameServers": ["a28-64.akam.net", "a3-64.akam.net"],
  "emails": ["dns-admin@google.com"],
  "created": "1987-05-14",
  "status": ["clientDeleteProhibited clientTransferProhibited"]
}
```

ThreatQ provides the following default mapping for this dataset:

| FEED DATA PATH | THREATQ ENTITY          | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES               | NOTES                       |
|----------------|-------------------------|--------------------------------------|----------------|------------------------|-----------------------------|
| .registrarName | Indicator.Attribute     | Registrar Name                       | N/A            | MarkMonitor, Inc.      | N/A                         |
| .nameServers[] | Related Indicator.Value | FQDN                                 | N/A            | a28-64.akam.net        | Added as related indicators |
| .emails[]      | Related Indicator.Value | Email Address                        | N/A            | dns-admin@google.com   | Added as related indicators |
| .created       | Indicator.Attribute     | Created At                           | N/A            | 1987-05-14             | N/A                         |
| .updated       | Indicator.Attribute     | Updated At                           | N/A            | 2025-09-09             | N/A                         |
| .expires       | Indicator.Attribute     | Expires At                           | N/A            | 2028-05-15             | N/A                         |
| .whoisServers  | Indicator.Attribute     | WHOIS Server                         | N/A            | whois.markmonitor.com  | N/A                         |
| .status[]      | Indicator.Attribute     | Status                               | N/A            | clientDeleteProhibited | N/A                         |

## Get Related Domains

GET <https://api.umbrella.com/investigate/v2/links/name/{domain}>

### Sample Response:

```
{
  "tb1": [
    ["app.hightoucherp.com.", 247]
  ],
  "found": true
}
```

ThreatQ provides the following default mapping for this dataset:

| FEED DATA PATH | THREATQ ENTITY          | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES              | NOTES                                       |
|----------------|-------------------------|--------------------------------------|----------------|-----------------------|---------------------------------------------|
| .tb1[][0]      | Related Indicator.Value | FQDN                                 | N/A            | app.hightoucherp.com. | Same mapping as the previous implementation |
| .tb1[][1]      | Indicator.Attribute     | Score (resolutions/minute)           | N/A            | 247                   | Displayed in the related domains table      |

## Get Domain History

GET <https://api.umbrella.com/investigate/v2/pdns/name/{domain}>

### Sample Response:

```
{
  "records": [
    {
      "minTtl": 1,
      "maxTtl": 86400,
      "firstSeenISO": "2014-06-23T19:03Z",
      "lastSeenISO": "2026-08-25T12:14Z",
      "name": "cisco.com",
      "type": "MX",
      "rr": "rcdn-mx-01.cisco.com.",
      "securityCategories": [],
      "contentCategories": ["Software/Technology", "Computers and
Internet"]
    }
  ]
}
```

ThreatQ provides the following default mapping for this dataset:

| FEED DATA PATH                  | THREATQ ENTITY          | THREATQ OBJECT TYPE OR ATTRIBUTE KEY      | PUBLISHED DATE         | EXAMPLES            | NOTES                                                         |
|---------------------------------|-------------------------|-------------------------------------------|------------------------|---------------------|---------------------------------------------------------------|
| .records[].rr                   | Related Indicator.Value | Indicator type depends on .records[].type | .records[].lastSeenISO | 72.163.4.185        | Added as a related indicator in the passive DNS history table |
| .records[].type                 | Indicator.Attribute     | Type                                      | N/A                    | A, AAAA, MX, NS     | Displayed in the passive DNS history table                    |
| .records[].minTtl               | Indicator.Attribute     | Min TTL                                   | N/A                    | 1                   | Displayed in the passive DNS history table                    |
| .records[].maxTtl               | Indicator.Attribute     | Max TTL                                   | N/A                    | 86400               | Displayed in the passive DNS history table                    |
| .records[].firstSeenISO         | Indicator.Attribute     | First Seen                                | N/A                    | 2014-06-23T19:03Z   | Displayed in the passive DNS history table                    |
| .records[].lastSeenISO          | Indicator.Attribute     | Last Seen                                 | N/A                    | 2026-08-25T12:14Z   | Displayed in the passive DNS history table                    |
| .records[].securityCategories[] | Indicator.Attribute     | Security Categories                       | N/A                    | Malware             | Displayed in the passive DNS history table                    |
| .records[].contentCategories[]  | Indicator.Attribute     | Content Categories                        | N/A                    | Software/Technology | Displayed in the passive DNS history table                    |

## Run Configuration Options



These configuration options are 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 provided when using the action on an object:

| PARAMETER                        | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select Enrichment Options</b> | <p>Select one or more enrichment options (API Endpoints) to use to fetch metadata. Options include:</p> <ul style="list-style-type: none"> <li>• Get Risk Scores</li> <li>• Get Categorizations (default)</li> <li>• Get Security Context (default)</li> <li>• Get WHOIS (default)</li> <li>• Get Related Domains</li> <li>• Get Domain History</li> </ul> |

## Get Samples

The Get Samples action fetches Cisco Threat Grid samples that are related to a given domain, IP, or URL.

GET <https://api.umbrella.com/investigate/v2/samples/{indicator}>

### Sample Response:

```
{
  "query": "example.com",
  "totalResults": 1,
  "moreDataAvailable": false,
  "samples": [
    {
      "sha256":
"0d477ed687d9f7424d2d28b66717bad4c0d21db8433752c9c51b032d04066af1",
      "sha1": "5a299e5bcf4b947e9e3aee9925ed068dd8809f9f",
      "md5": "d22dc224cc7f11bf35137ed753078d62",
      "magicType": "PE32 executable (GUI) Intel 80386, for MS
Windows",
      "threatScore": 95,
      "size": 10752,
      "firstSeen": 1785802695000,
      "lastSeen": 1786677026000,
      "avresults": [
        {
          "signature": "Gen:Variant.Worm.Phorpiex.153",
          "product": "ALYac"
        }
      ]
    }
  ]
}
```

ThreatQ provides the following default mapping for this operation action:

| FEED DATA PATH    | THREATQ ENTITY          | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES                                                         | NOTES |
|-------------------|-------------------------|--------------------------------------|----------------|------------------------------------------------------------------|-------|
| .samples[].sha256 | Related Indicator.Value | SHA-256                              | N/A            | 0d477ed687d9f7424d2d28b66717bad4c0d21db8433752c9c51b032d04066af1 | N/A   |
| .samples[].sha1   | Related Indicator.Value | SHA-1                                | N/A            | 5a299e5bcf4b947e9e3aee9925ed068dd8809f9f                         | N/A   |

| FEED DATA PATH                   | THREATQ ENTITY          | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES                                          | NOTES                                                                    |
|----------------------------------|-------------------------|--------------------------------------|----------------|---------------------------------------------------|--------------------------------------------------------------------------|
| .samples[].md5                   | Related Indicator.Value | MD5                                  | N/A            | d22dc224cc7f11bf35137ed753078d62                  | N/A                                                                      |
| .samples[].magicType             | Indicator.Attribute     | File Type                            | N/A            | PE32 executable (GUI) Intel 80386, for MS Windows | N/A                                                                      |
| .samples[].threatScore           | Indicator.Attribute     | Threat Score                         | N/A            | 95                                                | N/A                                                                      |
| .samples[].size                  | Indicator.Attribute     | File Size                            | N/A            | 10752                                             | N/A                                                                      |
| .samples[].firstSeen             | Indicator.Attribute     | First Seen                           | N/A            | 1785802695000                                     | Converted from epoch milliseconds                                        |
| .samples[].lastSeen              | Indicator.Attribute     | Last Seen                            | N/A            | 1786677026000                                     | Converted from epoch milliseconds                                        |
| .samples[].avresults[].signature | Indicator.Attribute     | Signature Detection                  | N/A            | Gen:Variant.Worm.Phoxiex.153                      | product is displayed in the table but not stored as a separate attribute |

## Reverse WHOIS

The Reverse WHOIS action fetches domains related to a given email address.

GET <https://api.umbrella.com/investigate/v2/whois/emails/{email}>

### Sample Response:

```
{
  "admin@example.net": {
    "domains": [
      {
        "domain": "0emm.com",
        "current": true
      }
    ],
    "totalResults": 1,
    "offset": 0,
    "moreDataAvailable": false,
    "limit": 500,
    "sortField": "domain"
  }
}
```

ThreatQ provides the following default mapping for this operation action:

| FEED DATA PATH       | THREATQ ENTITY          | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES                                 |
|----------------------|-------------------------|--------------------------------------|----------------|----------|---------------------------------------|
| .*.domains[].domain  | Related Indicator.Value | FQDN                                 | N/A            | 0emm.com | Added as related indicators           |
| .*.domains[].current | Indicator.Attribute     | Is Current                           | N/A            | true     | Displayed in the domain history table |

## Get Associated Names

The Get Associated Names action fetches domains related to a given IP Address.

GET <https://api.umbrella.com/investigate/v2/pdns/ip/{ip}>

### Sample Response:

```
{
  "records": [
    {
      "minTtl": 0,
      "maxTtl": 0,
      "firstSeenISO": "2022-05-11T13:07Z",
      "lastSeenISO": "2022-10-25T12:27Z",
      "name": "04.pong.sasci.net.",
      "type": "A",
      "rr": "208.67.222.222",
      "securityCategories": ["Malware"],
      "contentCategories": ["Software/Technology"]
    }
  ]
}
```

ThreatQ provides the following default mapping for this operation action:

| FEED DATA PATH                  | THREATQ ENTITY          | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES            | NOTES                                                       |
|---------------------------------|-------------------------|--------------------------------------|----------------|---------------------|-------------------------------------------------------------|
| .records[].name                 | Related Indicator.Value | FQDN                                 | N/A            | 04.pong.sasci.net.  | Added as related indicators in the domain resolutions table |
| .records[].type                 | Indicator.Attribute     | Type                                 | N/A            | A                   | Displayed in the domain resolutions table                   |
| .records[].minTtl               | Indicator.Attribute     | Min TTL                              | N/A            | 0                   | Displayed in the domain resolutions table                   |
| .records[].maxTtl               | Indicator.Attribute     | Max TTL                              | N/A            | 0                   | Displayed in the domain resolutions table                   |
| .records[].firstSeenISO         | Indicator.Attribute     | First Seen                           | N/A            | 2022-05-11T13:07Z   | Displayed in the domain resolutions table                   |
| .records[].lastSeenISO          | Indicator.Attribute     | Last Seen                            | N/A            | 2022-10-25T12:27Z   | Displayed in the domain resolutions table                   |
| .records[].securityCategories[] | Indicator.Attribute     | Security Categories                  | N/A            | Malware             | Displayed in the domain resolutions table                   |
| .records[].contentCategories[]  | Indicator.Attribute     | Content Categories                   | N/A            | Software/Technology | Displayed in the domain resolutions table                   |

## Known Issues / Limitations

- **Passive DNS Metadata:** Passive DNS metadata displayed in the **Get Associated Names** and **Domain History** tables is intended for display purposes only. Related indicators are added without creating ThreatQ attributes from empty or unavailable metadata values.

---

# Change Log

- **Version 3.0.0**
  - Migrated authentication to use Cisco Umbrella Investigate v2 client credentials.
  - Updated supported API endpoints to use the Cisco Umbrella Investigate v2 base URL.
  - Enhanced passive DNS processing for associated names and domain history.
  - Removed the **Latest Malicious Domains** action as Cisco Umbrella Investigate v2 does not provide a direct replacement.
- **Version 2.0.0**
  - Initial release