ThreatQuotient

Cisco Umbrella Action Bundle

Version 1.1.1

September 04, 2024

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	1.1.1
Compatible with ThreatQ Versions	>= 5.17.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Cisco Umbrella actions for ThreatQ enables analysts to use Cisco Umbrella's APIs for enrichment. Analysts will be able to enrich IOCs from their Threat Library with context from the Cisco Umbrella Investigate API, including but not limited to, the categorization, risk scores, hash samples, and WHOIS information.

The bundle provides the following actions:

- **Cisco Umbrella Investigate - Get Security Context** - fetches security context from Cisco Umbrella such as a domain's threat type and scores.
- **Cisco Umbrella Investigate - Get Risk Scores** - returns the risk score for a given domain.
- **Cisco Umbrella Investigate - Get Categorization** - fetches a domain's disposition as well as its security and content categories.
- **Cisco Umbrella Investigate - Get Samples** - retrieves related sample hashes for a given IOC, as well as some other contextual information.
- **Cisco Umbrella Investigate - Get WHOIS** - retrieves a domain's WHOIS records.
- **Cisco Umbrella Enforcement** - block or allow selected IOCs.

The action is compatible with the following system indicator types:

> Individual actions may only be compatible with a subset of these types.

- IP Address
- FQDN
- MD5
- SHA-1
- SHA-256
- URL

The action returns the following enriched indicator types:

> Individual actions may only return a subset of these types.

- IP Address
- FQDN
- MD5
- SHA-1
- SHA-256

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

Prerequisites

- A Cisco Umbrella Investigate License & API Key.
- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing the following indicator object types:
  - IP Address
  - FQDN
  - MD5
  - SHA-1
  - SHA-256
  - URL (Enforcement Action)

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.

All Actions

PARAMETER	DESCRIPTION
API Key	Enter your Umbrella Investigate API Key.
Objects Per Run	The number of objects to process per run of the workflow.

Get Categorization Parameters

PARAMETER	DESCRIPTION
API Key	Enter your Umbrella Investigate API Key.
Disposition Filter	Only ingest categorization for domains with the selected depositions. Options include: ◦ Unknown ◦ Benign (default) ◦ Malicious (default)
Attribution Filter	Select the pieces of context to ingest into ThreatQ when a record is found. Options include: ◦ Disposition (default) ◦ Content Category (default) ◦ Security Category (default)
Objects Per Run	The number of objects to process per run of the workflow.

Get Risk Scores Additional Parameters

PARAMETER	DESCRIPTION
API Key	Enter your Umbrella Investigate API Key.
Risk Score Threshold	Only ingest risk scores for domains with a risk score greater than or equal to this value.
Objects Per Run	The number of objects to process per run of the workflow.

Get Samples Parameters

PARAMETER	DESCRIPTION
API Key	Enter your Umbrella Investigate API Key.
Max Samples	Enter the maximum number of samples to return. The default value is **10**.
Sort Samples By	Select how you want to sort the samples. Options include: ◦ Score (default) ◦ Last Seen ◦ First Seen
Minimum Threat Score Threshold	Enter the minimum threat score threshold for samples to be ingested. The default value is **75**. You can set this to **0** to ingest all samples.
Hash Type Filter	Select the hash types you want to bring into ThreatQ when samples are found. Options include: ◦ MD5 (default) ◦ SHA-1 ◦ SHA-256
Attribution Filter	Select the pieces of context you want ingested into ThreatQ when a record is found. Options include: ◦ Threat Score (default) ◦ File Type (default) ◦ File Size (in bytes) ◦ Detection (per AV Engine)
Objects Per Run	The number of objects to process per run of the workflow.

Get Security Content Parameters

PARAMETER	DESCRIPTION
API Key	Enter your Umbrella Investigate API Key.
Only Ingest Records Found in Cisco Umbrella	Only ingest records found in Cisco Umbrella's database (i.e. found = true). If a record is not found, some scores are still populated such as DGA Score & Entropy. This option is enabled by default.
Only Ingest Records Associated with an Attack	Only ingest records that are associated with an attack (i.e. Emotet). This option is disabled by default.
Attribution Filter	Select the pieces of general context you want ingested into ThreatQ when a record is found. Options include: • Attack (default) • Threat Type (default) • Is Found • ASN Score • DGA Score • Entropy • Geodiversity Score • Page Rank • Perplexity • Popularity (default) • Prefix Score • RIP Score • Securerank • Flastflux (default)
Objects Per Run	The number of objects to process per run of the workflow.

Get WHOIS Parameters

PARAMETER	DESCRIPTION
API Key	Enter your Umbrella Investigate API Key.
Ingest Redacted Values	Enabling this will ingest values that are labeled as redacted. The default value is **False**.
Ingest Nameservers As...	Enabling this option will ingest nameservers as the selected type. Options include ◦ Do Not Ingest (default) ◦ Indicators (FQDN) ◦ Attributes (Nameserver) .
General Attribution Filter	Select the pieces of general context you want ingested into ThreatQ when a record is found. Options include: • Registrar Name (default) • Created At (default) • Status • Is Expired • Expires At
WHOIS Attribution Filter	Select the pieces of WHOIS context you want ingested into ThreatQ when a record is found. Options include: ◦ Admin Contact Name ◦ Admin Contact Email ◦ Admin Contact Organization ◦ Admin Contact City ◦ Admin Contact Country ◦ Admin Contact State ◦ Admin Contact Street ◦ Admin Contact Postal Code ◦ Admin Contact Telephone ◦ Technical Contact Name ◦ Technical Contact Email ◦ Technical Contact Organization ◦ Technical Contact City ◦ Technical Contact Country ◦ Technical Contact State ◦ Technical Contact Street

PARAMETER	DESCRIPTION
	◦ Registrant Name ◦ Registrant Email ◦ Registrant Organization ◦ Registrant City ◦ Registrant Country ◦ Registrant State ◦ Registrant Street ◦ Registrant Postal Code ◦ Registrant Telephone ◦ Technical Contact Postal Code ◦ Technical Contact Telephone ◦ Billing Contact Name ◦ Billing Contact Email ◦ Billing Contact Organization ◦ Billing Contact City ◦ Billing Contact Country ◦ Billing Contact State ◦ Billing Contact Street ◦ Billing Contact Postal Code ◦ Billing Contact Telephone
Objects Per Run	The number of objects to process per run of the workflow.

Enforcement Parameters

PARAMETER	DESCRIPTION
API Key	Enter your Umbrella Investigate API Key.
Key Secret	Enter your Umbrella Key Secret.
List Name	Enter the name of the list to add/remove IOCs to/from.
Action to Perform	Select the action to perform. Options include Allow and Block.
Objects Per Run	The number of objects to process per run of the workflow.
Verify SSL	When checked, validates the host-provided SSL certificate. This option is enabled by default.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.

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

Action

The following actions are included with the bundle:

FUNCTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Cisco Umbrella Investigate - Get Security Context	Get threat types or associated attacks for domains.	Indicator	FQDN
Cisco Umbrella Investigate - Get Risk Scores	Get the risk scores for domains.	Indicator	FQDN
Cisco Umbrella Investigate - Get Categorization	Get dispositions and content/ security categories for domains.	Indicator	FQDN
Cisco Umbrella Investigate - Get Samples	Get related samples (hashes) or sample information for a set of indicators.	Indicator	IP Address, FQDN, MD5, SHA-1, SHA-256
Cisco Umbrella Investigate - Get WHOIS	Get WHOIS records for domains.	Indicator	FQDN
Cisco Umbrella Enforcement	Allow or Block selected IOCs.	Indicator	IP Address, FQDN, URL,

Get Security Context

The Get Security Context action will fetch security context from Cisco Umbrella such as a domain's threat type and scores.

```
GET https://investigate.api.umbrella.com/security/name/{{ domain }}
```

Sample Response:


```
{
  "dga_score": 38.301771886101335,
  "perplexity": 0.4540313302593146,
  "entropy": 2.5216406363433186,
  "securerank2": -1.3135141095601992,
  "pagerank": 0.0262532,
  "asn_score": -29.75810625887133,
  "prefix_score": -64.9070502788884,
  "rip_score": -75.64720536038982,
  "popularity": 25.335450495507196,
  "fastflux": false,
  "geodiversity": [0.24074075, 0.018518519],
  "geodiversity_normalized": [0.3761535390278368, 0.0005015965168831449],
  "tld_geodiversity": [0],
  "geoscore": 0,
  "ks_test": 0,
  "attack": "WannaCry",
  "threat_type": "Ransomware",
  "found": true
}
```

ThreatQuotient provides the following default mapping for this action:

> All scores are rounded to 5 decimal places. All mapped fields are subject to user-configured filtering options

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.attack`	Indicator.Attribute	Attack	N/A	`WannaCry`	N/A
`.threat_type`	Indicator.Attribute	Threat Type	N/A	`Ransomware`	N/A
`.asn_score`	Indicator.Attribute	ASN Score	N/A	`-29.75810`	The attribute value is updated at ingestion
`.dga_score`	Indicator.Attribute	DGA Score	N/A	`38.30177`	The attribute value is updated at ingestion
`.entropy`	Indicator.Attribute	Entropy	N/A	`2.52164`	The attribute value is updated at ingestion
`.geoscore`	Indicator.Attribute	Geodiversity Score	N/A	`0`	The attribute value is updated at ingestion
`.pagerank`	Indicator.Attribute	Page Rank	N/A	`0.02625`	N/A
`.perplexity`	Indicator.Attribute	Perplexity	N/A	`0.45403`	The attribute value is updated at ingestion
`.popularity`	Indicator.Attribute	Popularity	N/A	`25.33545`	The attribute value is updated at ingestion
`.prefix_score`	Indicator.Attribute	Prefix Score	N/A	`-64.90705`	The attribute value is updated at ingestion
`.rip_score`	Indicator.Attribute	RIP Score	N/A	`-75.64720`	The attribute value is updated at ingestion
`.securerank2`	Indicator.Attribute	Securerank	N/A	`-1.31351`	N/A
`.fastflux`	Indicator.Attribute	Fastflux	N/A	`false`	N/A
`.found`	Indicator.Attribute	Is Found	N/A	`true`	N/A

Get Risk Scores

The Get Risk Scores action retrieves the risk score for a given domain.

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

Sample Response:


```
{
  "indicators": [
    {
      "indicator": "Geo Popularity Score",
      "indicator_id": "Geo Popularity Score",
      "normalized_score": 50,
      "score": 0
    },
    {
      "indicator": "Keyword Score",
      "indicator_id": "Keyword Score",
      "normalized_score": 15,
      "score": 0.15823231832454354
    },
    {
      "indicator": "Lexical",
      "indicator_id": "Lexical",
      "normalized_score": 13,
      "score": 0.136
    },
    {
      "indicator": "Popularity 1 Day",
      "indicator_id": "Popularity 1 Day",
      "normalized_score": null,
      "score": null
    },
    {
      "indicator": "Popularity 30 Day",
      "indicator_id": "Popularity 30 Day",
      "normalized_score": null,
      "score": null
    },
    {
      "indicator": "Popularity 7 Day",
      "indicator_id": "Popularity 7 Day",
      "normalized_score": null,
      "score": null
    },
    {
      "indicator": "Popularity 90 Day",
      "indicator_id": "Popularity 90 Day",
      "normalized_score": null,
```

```
      "score": null
    },
    {
      "indicator": "TLD Rank Score",
      "indicator_id": "TLD Rank Score",
      "normalized_score": 1,
      "score": 0.01983927366419238
    },
    {
      "indicator": "Umbrella Block Status",
      "indicator_id": "Umbrella Block Status",
      "normalized_score": 100,
      "score": true
    }
  ],
  "risk_score": 100
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.risk_score`	Indicator.Attribute	Risk Score	N/A	`100`	The attribute value is updated at ingestion.

Get Categorization

The Get Categorization action retrieves a domain's disposition as well as its security and content categories.

```
GET https://investigate.api.umbrella.com/domains/categorization/{{ domain }}
```

Sample Response:

```
{
  "esoskraadami.shop": {
    "status": -1,
    "security_categories": ["Malware"],
    "content_categories": ["Hacking"]
  }
}
```

ThreatQuotient provides the following default mapping for this action:

Feed data paths are based on the keys after selecting the domain name key.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.status`	Indicator.Attribute	Disposition	N/A	`Malicious`	Mapped from the integer value to a human-readable value. The attribute value is updated at ingestion
`.security_categories[]`	Indicator.Attribute	Security Category	N/A	`Malware`	N/A
`.content_categories[]`	Indicator.Attribute	Content Category	N/A	`Hacking`	N/A

Get Samples

The Get Samples action retrieves related sample hashes for a given IOC, as well as some other contextual information.

If the input IOC is a hash, the following endpoint is used:

```
GET https://investigate.api.umbrella.com/sample/{{ hash }}
```

If the input IOC is *not* a hash, the following endpoint is used:

```
GET https://investigate.api.umbrella.com/samples/{{ domain }}
```

Sample Response:


```
{
  "query": "google.com",
  "totalResults": 10,
  "moreDataAvailable": true,
  "limit": 10,
  "offset": 0,
  "samples": [
    {
      "sha256":
"e9d3470c37dada28d5a32fb53a243c5b20def35bb01abf8f5403182cc2b91fdd",
      "sha1": "de182fdcc3c0d473b90a0df0ad14c2074d1e7c50",
      "md5": "282f80e8a2cf9e0e0dd72093787d99c6",
      "magicType": "PE32 executable (GUI) Intel 80386, for MS Windows",
      "threatScore": 100,
      "size": 192512,
      "firstSeen": "1460108539000",
      "lastSeen": "1460108539000",
      "visible": true,
      "avresults": [
        {
          "signature": "Win.Trojan.Ramnit",
          "product": "ClamAV"
        },
        {
          "signature": "Win.Trojan.Parite",
          "product": "ClamAV"
        }
      ]
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

> All mapped fields are subject to user-configured filtering options.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.samples[].threatScore`	Indicator/Related Indicator.Attribute	Threat Score	`.samples[].firstSeen`	`100`	The attribute value is updated at ingestion
`.samples[].magicType`	Indicator/Related Indicator.Attribute	File Type	`.samples[].firstSeen`	`PE32 executable (GUI) Intel 80386, for MS Windows`	N/A
`.samples[].size`	Indicator/Related Indicator.Attribute	File Size	`.samples[].firstSeen`	`192512`	N/A
`.samples[].av results[].signature`	Indicator/Related Indicator.Attribute	Detection	`.samples[].firstSeen`	`Win.Trojan.Ramnit`	N/A
`.samples[].md5`	Related Indicator.Value	MD5	`.samples[].firstSeen`	`282f80e8a2cf9e0e0dd72093787d99c6`	N/A
`.samples[].sha1`	Related Indicator.Value	SHA-1	`.samples[].firstSeen`	`de182fdcc3c0d473b90a0df0ad14c2074d1e7c50`	N/A
`.samples[].sha256`	Related Indicator.Value	SHA-256	`.samples[].firstSeen`	`e9d3470c37dada28d5a32fb53a243c5b20def35bb01abf8f5403182cc2b91fdd`	N/A

Get WHOIS

The Get WHOIS action retrieves a domain's WHOIS records.

`GET https://investigate.api.umbrella.com/whois/{{ domain }}`

Sample Response:


```
{
  "administrativeContactFax": null,
  "whoisServers": "whois.corporatedomains.com",
  "addresses": ["1355 market street"],
  "administrativeContactName": "Domain Admin",
  "zoneContactEmail": null,
  "billingContactFax": null,
  "administrativeContactTelephoneExt": null,
  "administrativeContactEmail": "domains@twitter.com",
  "technicalContactEmail": "domains-tech@twitter.com",
  "technicalContactFax": "14152220922",
  "nameServers": [
    "a.r06.twtrdns.net",
    "b.r06.twtrdns.net",
    "c.r06.twtrdns.net",
    "d.r06.twtrdns.net",
    "d01-01.ns.twtrdns.net",
    "d01-02.ns.twtrdns.net",
    "ns3.p34.dynect.net",
    "ns4.p34.dynect.net"
  ],
  "zoneContactName": null,
  "billingContactPostalCode": null,
  "zoneContactFax": null,
  "registrantTelephoneExt": null,
  "zoneContactFaxExt": null,
  "technicalContactTelephoneExt": null,
  "billingContactCity": null,
  "zoneContactStreet": [],
  "created": "2000-01-21",
  "administrativeContactCity": "San Francisco",
  "registrantName": "Twitter, Inc.",
  "zoneContactCity": null,
  "domainName": "twitter.com",
  "zoneContactPostalCode": null,
  "administrativeContactFaxExt": null,
  "technicalContactCountry": "UNITED STATES",
  "registrarIANAID": "299",
  "updated": "2023-01-17",
  "administrativeContactStreet": ["1355 market street"],
  "billingContactEmail": null,
  "status": [
```

```
    "clientTransferProhibited serverDeleteProhibited serverTransferProhibited
serverUpdateProhibited"
  ],
  "registrantCity": "San Francisco",
  "billingContactCountry": null,
  "expires": "2024-01-21",
  "technicalContactStreet": ["1355 market street"],
  "registrantOrganization": "Twitter, Inc.",
  "billingContactStreet": [],
  "registrarName": "CSC CORPORATE DOMAINS, INC.",
  "registrantPostalCode": "94103",
  "zoneContactTelephone": null,
  "registrantEmail": "domains@twitter.com",
  "technicalContactFaxExt": null,
  "technicalContactOrganization": "Twitter, Inc.",
  "emails": ["domains-tech@twitter.com", "domains@twitter.com"],
  "registrantStreet": ["1355 market street"],
  "technicalContactTelephone": "14152229670",
  "technicalContactState": "CA",
  "technicalContactCity": "San Francisco",
  "registrantFax": "14152220922",
  "registrantCountry": "UNITED STATES",
  "billingContactFaxExt": null,
  "timestamp": null,
  "zoneContactOrganization": null,
  "administrativeContactCountry": "UNITED STATES",
  "billingContactName": null,
  "registrantState": "CA",
  "registrantTelephone": "14152229670",
  "administrativeContactState": "CA",
  "registrantFaxExt": null,
  "technicalContactPostalCode": "94103",
  "zoneContactTelephoneExt": null,
  "administrativeContactOrganization": "Twitter, Inc.",
  "billingContactTelephone": null,
  "billingContactTelephoneExt": null,
  "zoneContactState": null,
  "administrativeContactTelephone": "14152229670",
  "billingContactOrganization": null,
  "technicalContactName": "Tech Admin",
  "administrativeContactPostalCode": "94103",
  "zoneContactCountry": null,
  "billingContactState": null,
  "auditUpdatedDate": "2023-01-20 12:03:17 UTC",
  "recordExpired": false,
  "timeOfLatestRealtimeCheck": 1674270179742,
  "hasRawText": true
}
```

ThreatQuotient provides the following default mapping for this action:

> All mapped fields are subject to user-configured filtering options

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.nameServers[]`	Related Indicator.Value	FQDN	N/A	`a.r06.twtrdns.netz`	If nameservers are ingested as Indicators
`.nameServers[]`	Indicator.Attribute	Nameserver	N/A	`a.r06.twtrdns.net`	If nameservers are ingested as Attributes
`.registrarName`	Indicator.Attribute	Registrar Name	N/A	`CSC CORPORATE DOMAINS, INC.`	N/A
`.created`	Indicator.Attribute	Created At	N/A	`2000-01-21`	N/A
`.status`	Indicator.Attribute	Status	N/A	`clientTransferProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited`	N/A
`.recordExpired`	Indicator.Attribute	Is Expired	N/A	`false`	N/A
`.expires`	Indicator.Attribute	Expires At	N/A	`2024-01-21`	N/A
`.administrativeContactName`	Indicator.Attribute	Admin Contact Name	N/A	`Domain Admin`	N/A
`.administrativeContactOrganization`	Indicator.Attribute	Admin Contact Organization	N/A	`Twitter, Inc.`	N/A
`.administrativeContactEmail`	Indicator.Attribute	Admin Contact Email	N/A	`domains@twitter.com`	N/A
`.administrativeContactCity`	Indicator.Attribute	Admin Contact City	N/A	`San Francisco`	N/A
`.administrativeContactState`	Indicator.Attribute	Admin Contact State	N/A	`CA`	N/A
`.administrativeContactCountry`	Indicator.Attribute	Admin Contact Country	N/A	`UNITED STATES`	N/A
`.administrativeContactPostalCode`	Indicator.Attribute	Admin Contact Postal Code	N/A	`94103`	N/A
`.administrativeContactStreet`	Indicator.Attribute	Admin Contact Street	N/A	`1355 market street`	N/A
`.administrativeContactTelephone`	Indicator.Attribute	Admin Contact Telephone	N/A	`14152229670`	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.registrantName`	Indicator.Attribute	Registrant Name	N/A	`Twitter, Inc.`	N/A
`.registrantOrganization`	Indicator.Attribute	Registrant Organization	N/A	`Twitter, Inc.`	N/A
`.registrantEmail`	Indicator.Attribute	Registrant Email	N/A	`domains@twitter.com`	N/A
`.registrantCity`	Indicator.Attribute	Registrant City	N/A	`San Francisco`	N/A
`.registrantState`	Indicator.Attribute	Registrant State	N/A	`CA`	N/A
`.registrantCountry`	Indicator.Attribute	Registrant Country	N/A	`UNITED STATES`	N/A
`.registrantPostalCode`	Indicator.Attribute	Registrant Postal Code	N/A	`94103`	N/A
`.registrantStreet`	Indicator.Attribute	Registrant Street	N/A	`1355 market street`	N/A
`.registrantTelephone`	Indicator.Attribute	Registrant Telephone	N/A	`14152229670`	N/A
`.technicalContactName`	Indicator.Attribute	Technical Contact Name	N/A	`Tech Admin`	N/A
`.technicalContactOrganization`	Indicator.Attribute	Technical Contact Organization	N/A	`Twitter, Inc.`	N/A
`.technicalContactEmail`	Indicator.Attribute	Technical Contact Email	N/A	`domains-tech@twitter.com`	N/A
`.technicalContactCity`	Indicator.Attribute	Technical Contact City	N/A	`San Francisco`	N/A
`.technicalContactState`	Indicator.Attribute	Technical Contact State	N/A	`CA`	N/A
`.technicalContactCountry`	Indicator.Attribute	Technical Contact Country	N/A	`UNITED STATES`	N/A
`.technicalContactPostalCode`	Indicator.Attribute	Technical Contact Postal Code	N/A	`94103`	N/A
`.technicalContactStreet`	Indicator.Attribute	Technical Contact Street	N/A	`1355 market street`	N/A
`.technicalContactTelephone`	Indicator.Attribute	Technical Contact Telephone	N/A	`14152229670`	N/A
`.billingContactName`	Indicator.Attribute	Billing Contact Name	N/A	`Billing Admin`	N/A
`.billingContactOrganization`	Indicator.Attribute	Billing Contact Organization	N/A	`Twitter, Inc.`	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.billingContactEmail`	Indicator.Attribute	Billing Contact Email	N/A	N/A	N/A
`.billingContactCity`	Indicator.Attribute	Billing Contact City	N/A	`San Francisco`	N/A
`.billingContactState`	Indicator.Attribute	Billing Contact State	N/A	`CA`	N/A
`.billingContactCountry`	Indicator.Attribute	Billing Contact Country	N/A	`UNITED STATES`	N/A
`.billingContactPostalCode`	Indicator.Attribute	Billing Contact Postal Code	N/A	`94103`	N/A
`.billingContactStreet`	Indicator.Attribute	Billing Contact Street	N/A	`1355 market street`	N/A
`.billingContactTelephone`	Indicator.Attribute	Billing Contact Telephone	N/A	`14152229670`	N/A

Enforcement

The Cisco Umbrella Enforcement action submits indicators to be allowed or blocked.

`POST https://api.umbrella.com/policies/v2/destinationlists/{list_id}/destinations`

Sample Response:

```
[
    {
        "destination": "something-something.com"
    }
]
```

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.

Get Security Context

METRIC	RESULT
Run Time	2 minutes
Indicators	395
Indicator Attributes	1,265

Get Risk Scores

METRIC	RESULT
Run Time	1 minute
Indicators	25
Indicator Attributes	22

Get Categorization

METRIC	RESULT
Run Time	1 minute
Indicators	25
Indicator Attributes	54

Get Samples

METRIC	RESULT
Run Time	2 minutes
Indicators	52
Indicator Attributes	191

Get WHOIS

METRIC	RESULT
Run Time	3 minutes
Indicators	52
Indicator Attributes	524

Known Issues / Limitations

- Rate Limits may effect the ability to enrich large sets of IOCs, depending on your Cisco Umbrella Investigate license tier.
  - More information can be found here: https://developer.cisco.com/docs/cloud-security/#!investigate-getting-started/rate-limits
  - Each action implements a 0.6 second delay between each request to partially mitigate this.

    > It is highly advised that you check your license tier and adjust the `Objects Per Run` user configuration field for each action accordingly.

- Only domains and URLs are accepted for block lists.
- Only URLs, Domains, and IP Addresses are accepted for allow lists.

Change Log

- **Version 1.1.1**
  - The **Cisco Umbrella Investigate - Block/Allow IOC** action has been renamed to **Cisco Umbrella Enforcement**.
- **Version 1.1.0**
  - Added a new action: Cisco Umbrella Block/Allow IOC.
- **Version 1.0.0**
  - Initial release