# Cisco Umbrella™ Investigate Spaces

## User Guide

**Software Version 1.0**

**September 8, 2020**

30006-02 EN Rev. A

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 | F: .703.229.4489
www.ThreatConnect.com

# Table of Contents

# OVERVIEW

The Cisco Umbrella Investigate Spaces app provides enrichment data from Cisco Umbrella Investigate in real time on Address, Email Address, and Host Indicators from within ThreatConnect®, allowing analysts to gain valuable insights from Cisco Umbrella Investigate without leaving ThreatConnect.

# DEPENDENCIES

## ThreatConnect Dependencies

- Installation of the **TCS - Cisco Umbrella Investigate 1.1** contextually aware Spaces app. See *Contextually Aware Spaces* for more information.

***NOTE: All ThreatConnect dependencies will be provided by default to subscribing ThreatConnect Cloud customers. Private Instance customers can enable these settings during configuration on the*** *Account Settings* ***screen within their Private Instance of ThreatConnect.***

## Cisco Umbrella Investigate Dependencies

- A Cisco Umbrella Investigate API (Application Programming Interface) token, which is provided via a subscription to the Cisco Umbrella API.

# CONFIGURATION PARAMETERS

## Parameter Definition

The parameters defined in Table 1 apply to the configuration parameters during the job-creation process.

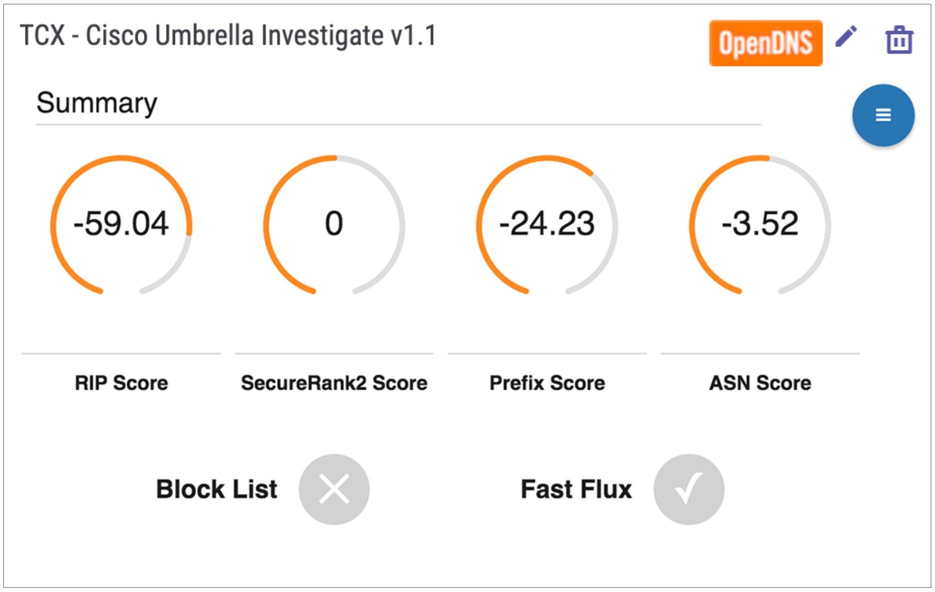
Table 1

| Name | Description |
|---|---|
| Logging level | This parameter, for support issues only, sets the logging level for debugging. Acceptable values are **debug**, **info**, **warning**, **error**, and **critical**. |
| Cisco Umbrella Investigate API Token | This parameter is the Cisco Umbrella Investigate API token used by the Data Enrichment Investigate feature. |
| Comma-separated list of tags applied to indicator on an add | This parameter is the comma-separated list of Tags to apply to any Indicator added using the app. |
| Confidence applied to indicator on an add (0-100) | This parameter is the Confidence Rating to apply to any Indicator added using the app. |
| Rating applied to indicator on an add (0-5) | This parameter is the Threat Rating to apply to any Indicator added using the app. |
| Automatically send Security Labels (comma separated values) | This parameter is the comma-separated list of Security Labels to apply to any Indicator added using the app. |

# CONTEXT OVERVIEW

This guide provides an overview of the Cisco Umbrella Investigate Spaces app for ThreatConnect. While it provides descriptions of Cisco Umbrella Investigate metrics, it is not the source of definitions of these metrics. The metrics can be changed by Cisco Umbrella at any time. For full details on Cisco Umbrella Investigate metrics, visit the Cisco Umbrella website: https://umbrella.cisco.com/products/threat-intelligence.

The user interface of the app displays a card with a **Summary** screen showing key metrics for the given Indicator type, as shown in Figure 1 for the Host Indicator context. Options for viewing additional detail-level elements are accessed by clicking the **Action** ≡ menu button in the upper right-hand corner of the card.



RIP Score: -59.04
SecureRank2 Score: 0
Prefix Score: -24.23
ASN Score: -3.52
Block List ✗
Fast Flux ✓

Figure 1

The app can be added to the **Details** screens of the following Indicator types under the **Spaces** tab:

- Address (IP address)
- Host
- Email Address

# Address Context

The Address context for the Cisco Umbrella Investigate Spaces app retrieves contextual data on the selected IP address from the Cisco Umbrella Investigate API. The **Action** ≡ menu button provides options for viewing the following screens:

- **Summary**
- **IP Resource Record**

## Summary

Figure 2 displays the **Summary** screen for the Address context.

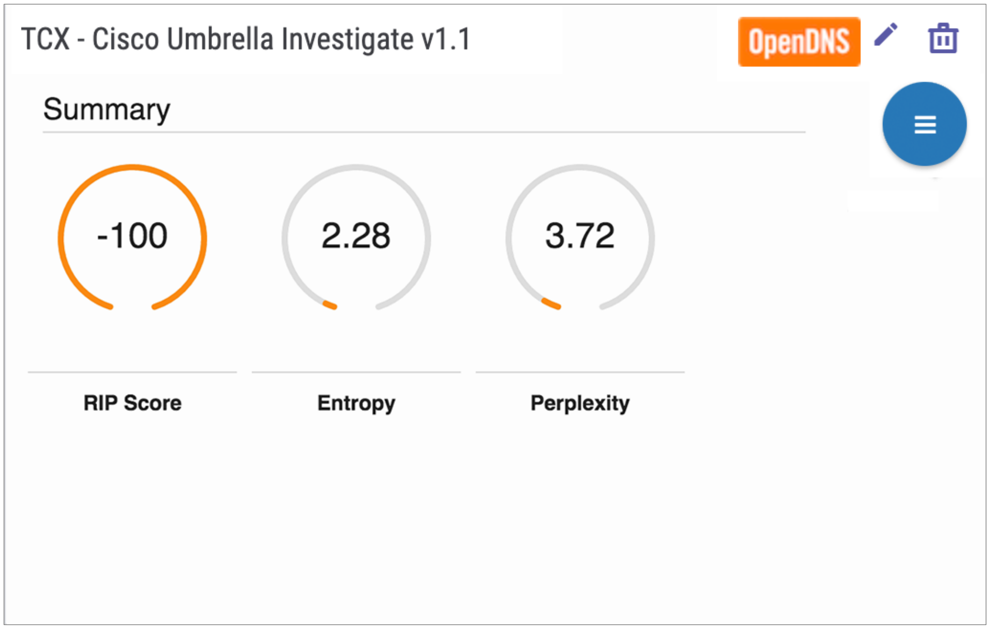


Figure 2

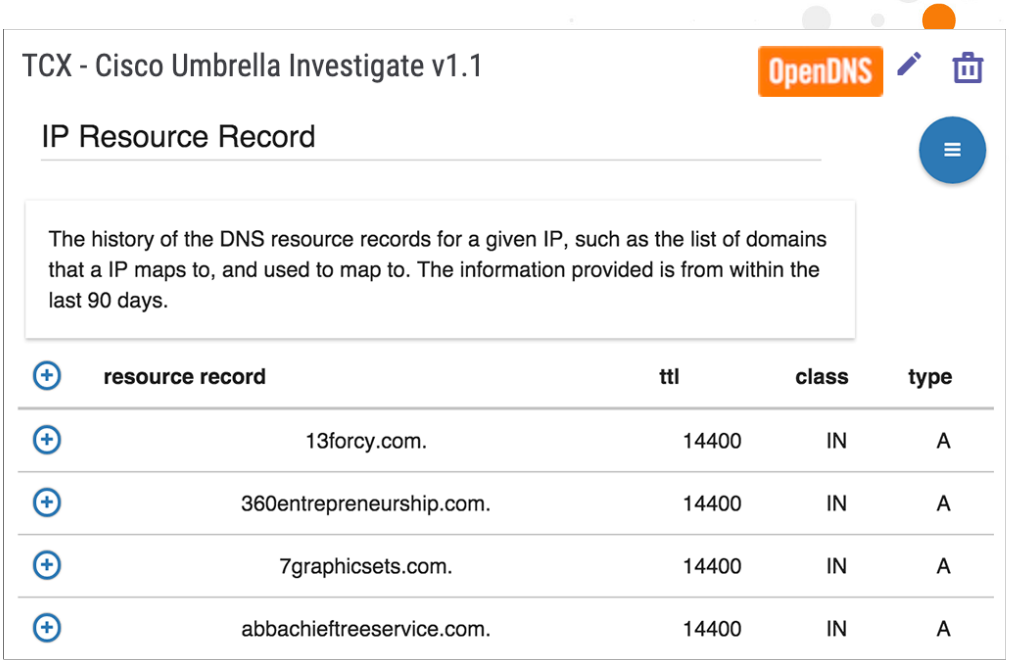
The **Summary** screen displays three key scores provided by Cisco Umbrella Investigate for an IP Address, as described in Table 2.

Table 2

| Score | Description |
|---|---|
| RIP Score | The RIP Score ranks domains given their IP addresses and the reputation score of these IP addresses. This score ranges from -100 (very suspicious) to 0. |
| Entropy | The Entropy score establishes the number of bits required to encode a domain name, as a score. This score is used in conjunction with the DGA (Domain Generation Algorithm) score (see Table 5) and Perplexity (see the next row in this table). |
| Perplexity | Perplexity grades the likeliness of a name to be algorithmically generated based on the mathematical concept of perplexity, on a scale from 0 to 100. This score is used in conjunction with the DGA score. (See Table 5.) |

## IP Resource Record

The **IP Resource Record** (Figure 3) represents the history of the Domain Name System (DNS) resource records for a given IP address, such as the list of domains to which the IP address maps and the domains to which it used to map. The information provided is from the last 90 days.



TCX - Cisco Umbrella Investigate v1.1

IP Resource Record

The history of the DNS resource records for a given IP, such as the list of domains that a IP maps to, and used to map to. The information provided is from within the last 90 days.

| ⊕ | resource record | ttl | class | type |
|---|---|---|---|---|
| ⊕ | 13forcy.com. | 14400 | IN | A |
| ⊕ | 360entrepreneurship.com. | 14400 | IN | A |
| ⊕ | 7graphicsets.com. | 14400 | IN | A |
| ⊕ | abbachieftreeservice.com. | 14400 | IN | A |

Figure 3

***NOTE: IP Resource Record mappings can be directly added to ThreatConnect by clicking on the Add ⊕ button. See the "ADDING INDICATORS" section for more details.***

## Host Context

The Host context for the Cisco Umbrella Investigate Spaces app retrieves contextual data on the selected domain name from the Cisco Umbrella Investigate API. The **Action** ≡ menu button provides options for viewing the following screens:

- Summary
- Categories
- Co-occurrences
- Links
- Security
- Tagging
- Domain Resource Record
- Whois - Domain

### Summary

Figure 4 displays the **Summary** screen for the Host context.

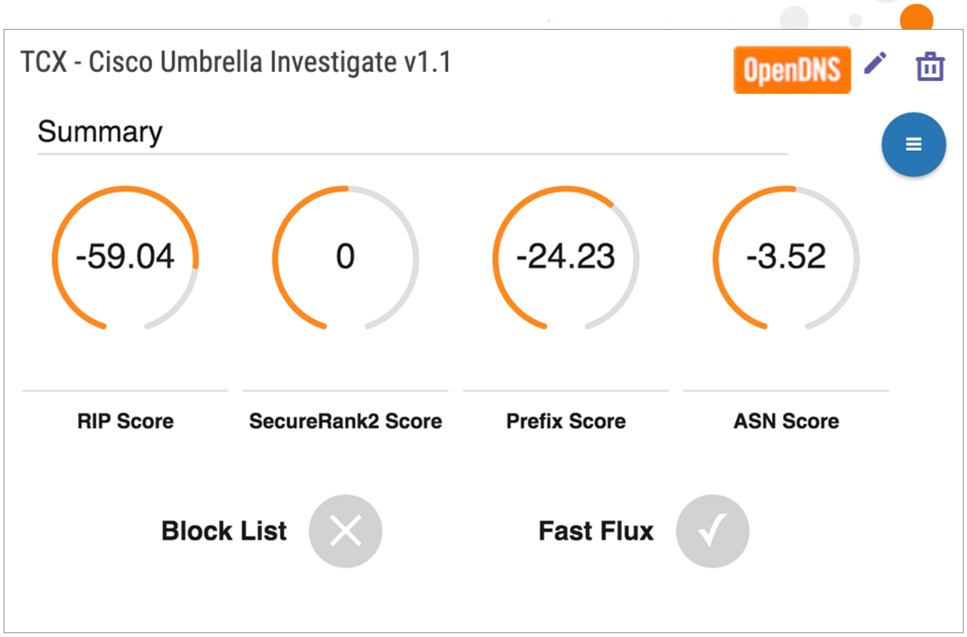


Figure 4

The **Summary** screen displays key metrics that provide a snapshot of Cisco Umbrella Investigate scores and flags for the selected Host, as described in Table 3.

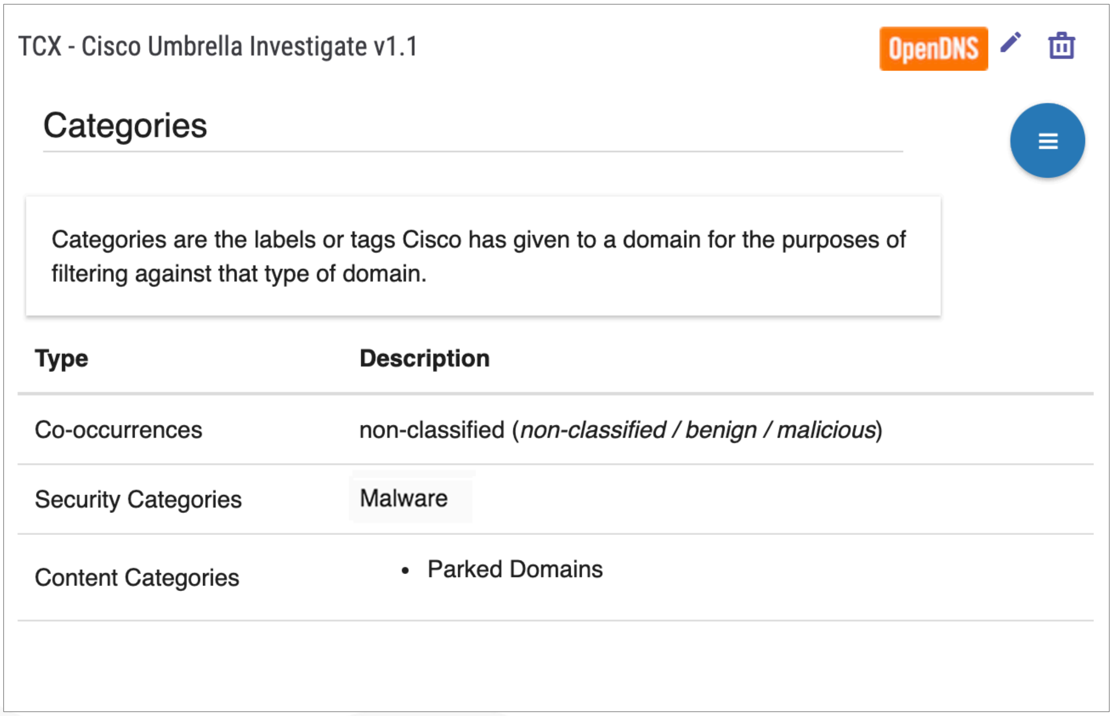
Table 3

| Score | Description |
|---|---|
| RIP Score | The RIP Score ranks domains given their IP addresses and the reputation score of these IP addresses. This score ranges from -100 (very suspicious) to 0. |
| SecureRank2 Score | The SecureRank2 Score rates the suspiciousness of a domain, based on the lookup behavior of client IP addresses for the domain. This score is defined to identify hostnames requested by known infected clients, but never requested by clean clients, assuming these domains are more likely to be bad. This score ranges from -100 (suspicious) to 100 (benign). |

|  |  |
|---|---|
| Prefix Score | The Prefix Score ranks domains given their IP prefixes (an IP prefix is the first three octets in an IP address) and the reputation score of these prefixes. This score ranges from -100 (very suspicious) to 0. |
| ASN Score | The ASN Score is a reputation score that ranges from -100 (very suspicious) to 0. |
| Block List | This flag signals whether a Host is on the block list (✓) or not (X). |
| FastFlux | This flag signals whether a Host is a candidate to be a fast flux domain (✓) or not (X). |

## Categories

Categories are the labels or tags Cisco Umbrella Investigate has given to a domain for the purpose of filtering against that type of domain. Figure 5 displays the **Categories** screen.



Categories

Categories are the labels or tags Cisco has given to a domain for the purposes of filtering against that type of domain.

| Type | Description |
|---|---|
| Co-occurrences | non-classified (*non-classified / benign / malicious*) |
| Security Categories | Malware |
| Content Categories | • Parked Domains |

Figure 5

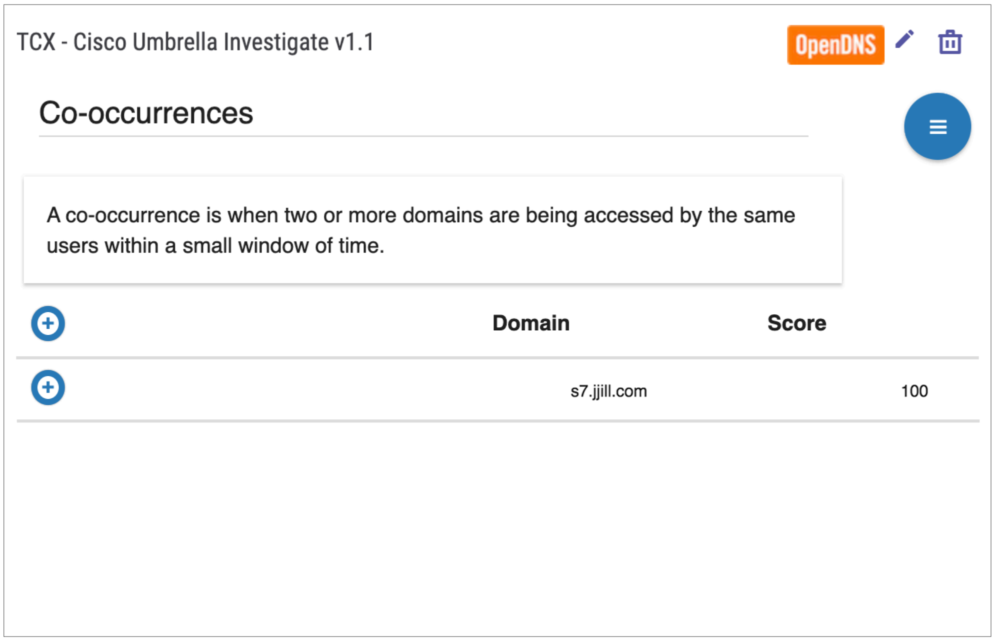
Table 4 describes the Category types.

Table 4

| Type | Description |
|---|---|
| Co-occurrences | A Co-occurrence is when two or more domains are being accessed by the same users within a small window of time. |
| Security Categories | Security category tag (or no match found) |
| Content Categories | Content category tag (or no match found) |

## Co-occurrences

A Co-occurrence is when two or more domains are being accessed by the same users within a small window of time. Figure 6 displays the **Co-occurrences** screen.



A co-occurrence is when two or more domains are being accessed by the same users within a small window of time.

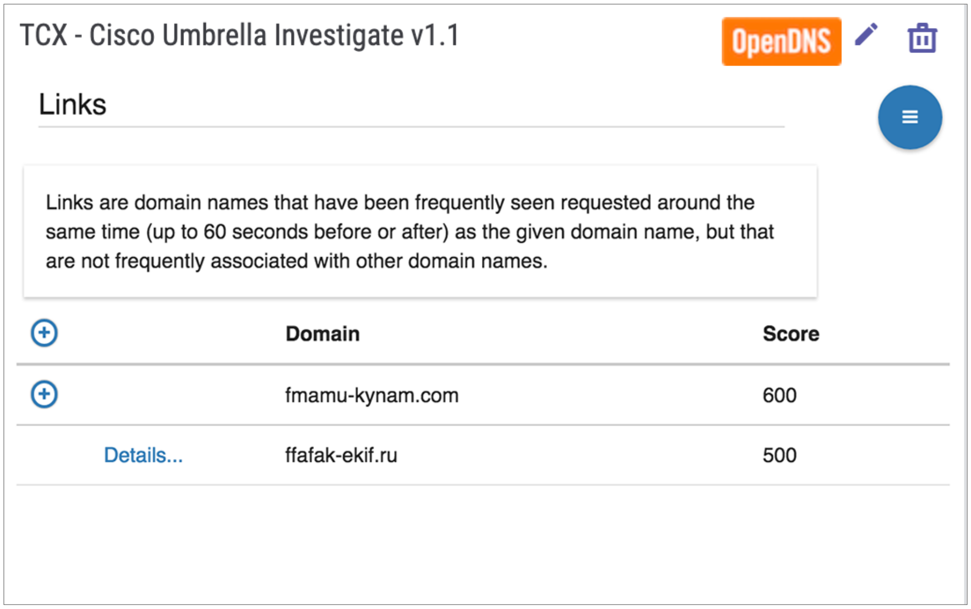
| | Domain | Score |
|---|---|---|
| ⊕ | s7.jjill.com | 100 |

Figure 6

***NOTE: Domain co-occurrences can be directly added to ThreatConnect by clicking on the Add ⊕ button. See the "ADDING INDICATORS" section for more details.***

## Links

Links are domain names that are frequently requested around the same time (up to 60 seconds before or after) as the given domain name, but that are not frequently associated with other domain names. Figure 7 displays the **Links** screen, with one domain already added to ThreatConnect (hyperlinked with **Details…**).



TCX - Cisco Umbrella Investigate v1.1

Links

Links are domain names that have been frequently seen requested around the same time (up to 60 seconds before or after) as the given domain name, but that are not frequently associated with other domain names.

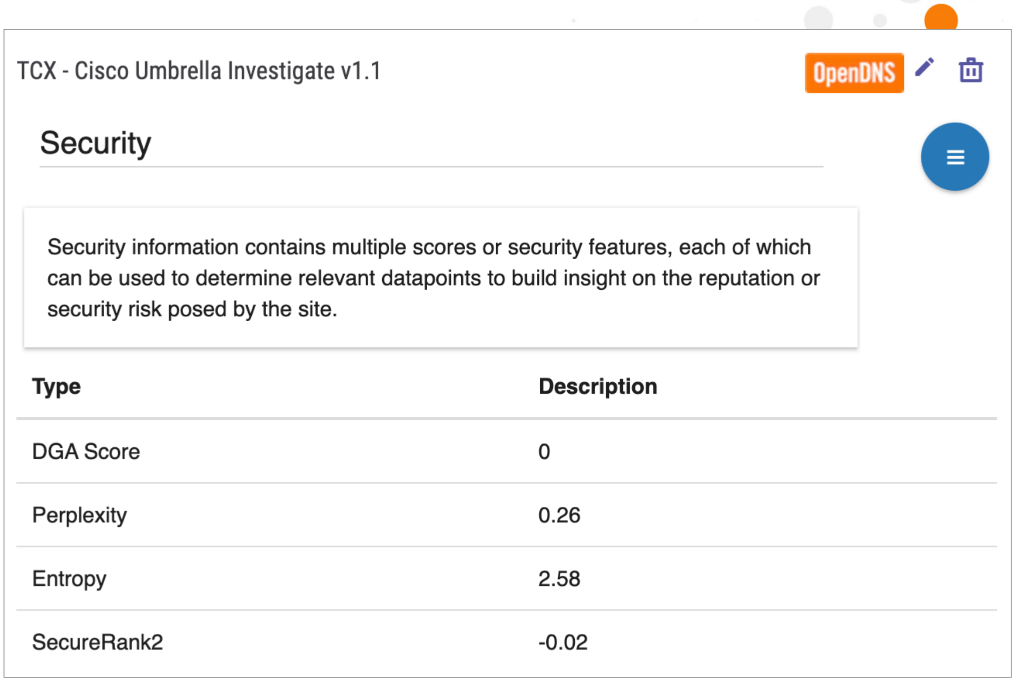
| ⊕ | Domain | Score |
|---|---|---|
| ⊕ | fmamu-kynam.com | 600 |
| Details... | ffafak-ekif.ru | 500 |

Figure 7

***NOTE: Domain links can be directly added to ThreatConnect by clicking on the*** *Add* ⊕ ***button. Using the configured parameter definitions, the domain name will be created as a Host in the current owner. To add all domains in the list, click on the*** *Add* ⊕ ***button in the table header.***

## Security

The **Security** screen (Figure 8) displays multiple scores or security features, each of which can be used to determine relevant data points to build insight on the reputation or security risk posed by the site.



TCX - Cisco Umbrella Investigate v1.1

Security

Security information contains multiple scores or security features, each of which can be used to determine relevant datapoints to build insight on the reputation or security risk posed by the site.

| Type | Description |
|---|---|
| DGA Score | 0 |
| Perplexity | 0.26 |
| Entropy | 2.58 |
| SecureRank2 | -0.02 |

Figure 8

Table 5 contains a description of each metric.

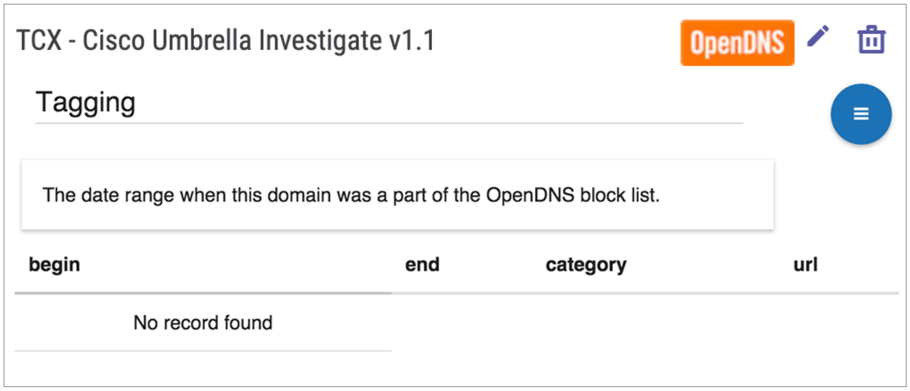
Table 5

| Score | Description |
|---|---|
| DGA Score | The Domain Generation Algorithm (DGA) score is generated based on the likeliness of the domain name being generated by an algorithm rather than a human. This algorithm is designed to identify domains that have been created using an automated randomization strategy, which is a common evasion technique in malware kits or botnets. This score ranges from -100 (suspicious) to 0 (benign). |
| Perplexity | The Perplexity score grades the likeliness of a name to be algorithmically generated based on the mathematical concept of perplexity, on a scale from 0 to 100. This score is used in conjunction with the DGA score. |
| Entropy | The Entropy score establishes the number of bits required to encode the domain name, as a score. This score is to be used in conjunction with the DGA Score and the Perplexity score. |

| | |
|---|---|
| SecureRank2 | The SecureRank2 Score rates the suspiciousness of a domain, based on the lookup behavior of client IP addresses for the domain. This score is designed to identify hostnames requested by known infected clients, but never requested by clean clients, assuming these domains are more likely to be bad. Scores returned range from -100 (suspicious) to 100 (benign). |
| PageRank™ | The PageRank Score ranks popularity according to Google™'s PageRank algorithm. |
| ASN Score | The ASN Score is a reputation score that ranges from -100 (very suspicious) to 0. |
| Prefix Score | The Prefix Score ranks domains given their IP prefixes (an IP prefix is the first three octets in an IP address) and the reputation score of these prefixes. This score ranges from -100 (very suspicious) to 0. |
| RIP Score | The RIP Score ranks domains given their IP addresses and the reputation score of these IP addresses. This score ranges from -100 (very suspicious) to 0. |
| FastFlux | This flag signals whether a domain is a candidate to be a fast flux domain (**true**) or not (**false**). |
| Popularity | The Popularity score tracks the number of unique client IPs visiting a site relative to all the requests to all sites. It is a score of how many different client/unique IPs go to a domain compared with other domains. |
| Attack | The Attack feature obtains the name of any known attacks associated with the domain. If it returns a blank, then there is no known threat associated with the domain. |
| Threat Type | The Threat Type feature obtains the type of a known attack, such as botnet or APT, associated with a domain. If it returns a blank, then there is no known threat associated with the domain. |

# Tagging

The **Tagging** screen (Figure 9) displays the date range for when a domain was a part of the Cisco Umbrella block list.



TCX - Cisco Umbrella Investigate v1.1

Tagging

The date range when this domain was a part of the OpenDNS block list.

| begin | end | category | url |
|---|---|---|---|
| No record found | | | |

Figure 9

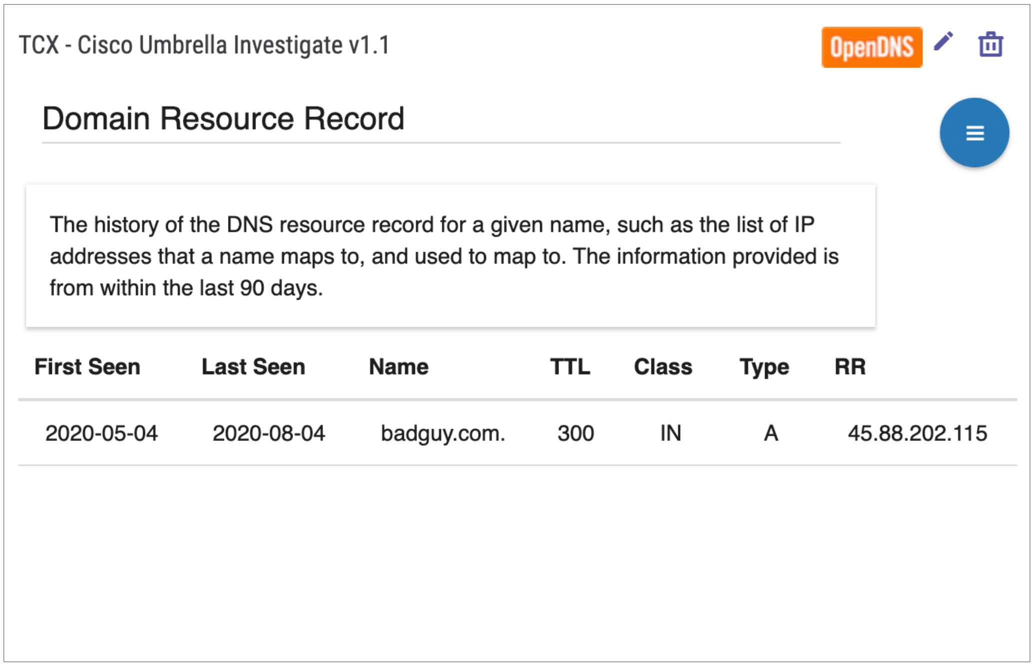
Table 6 provides a description for each information field provided in the **Tagging** screen.

Table 6

| Type | Description |
|---|---|
| begin/end | This field is the date range for which a domain has been on the block list. |
| category | This field is a domain tag, such as **malware** or **phishing**, identifying the security category of a domain. |
| url | This field, if available or possible, lists a specific URL hosting malicious content. |

## Domain Resource Record

The **Domain Resource Record** screen (Figure 10) displays the history of the DNS resource record for a given name, such as the list of IP addresses to which a name maps and to which it used to map. The information provided is from the last 90 days.



Domain Resource Record

The history of the DNS resource record for a given name, such as the list of IP addresses that a name maps to, and used to map to. The information provided is from within the last 90 days.

| First Seen | Last Seen | Name | TTL | Class | Type | RR |
|---|---|---|---|---|---|---|
| 2020-05-04 | 2020-08-04 | badguy.com. | 300 | IN | A | 45.88.202.115 |

Figure 10

Table 7 displays the information included in the **Domain Resource Record** screen.

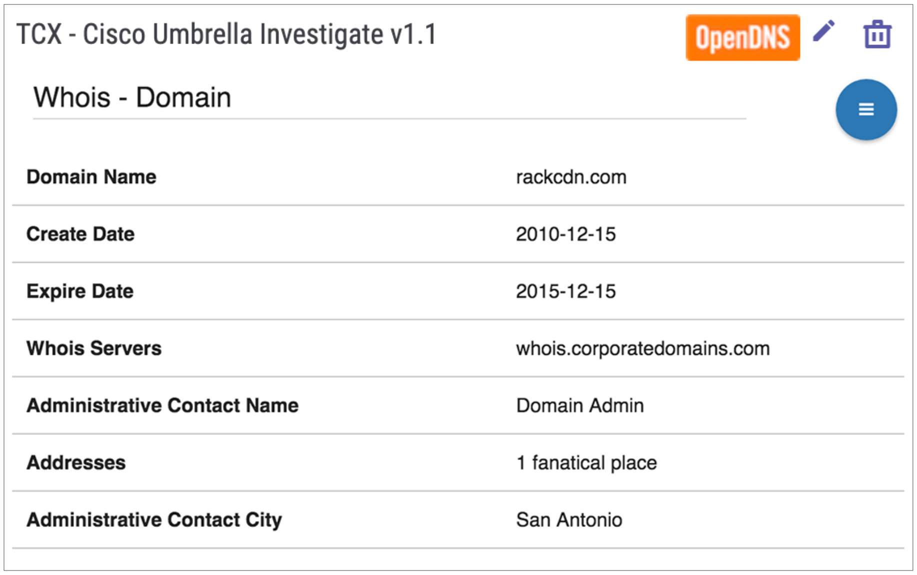
Table 7

| Type | Description |
|---|---|
| First Seen | This field is the date when a domain was first seen on the Cisco Umbrella Investigate database. |
| Last Seen | This field is the date when a domain was last seen on the Cisco Umbrella Investigate database. |
| Name | This field is the name of a domain. |
| TTL | This field is the time-to-live for a record. |

| | |
|---|---|
| Class | This field is the DNS class type. |
| Type | This field is the query type. |
| RR | This field is the resource record IP address for a domain. |

### Whois - Domain

The **Whois - Domain** screen (Figure 11) displays Whois information for the Host. Since there are no standards for Whois information, the information returned can vary.



Whois - Domain

| | |
|---|---|
| **Domain Name** | rackcdn.com |
| **Create Date** | 2010-12-15 |
| **Expire Date** | 2015-12-15 |
| **Whois Servers** | whois.corporatedomains.com |
| **Administrative Contact Name** | Domain Admin |
| **Addresses** | 1 fanatical place |
| **Administrative Contact City** | San Antonio |

Figure 11

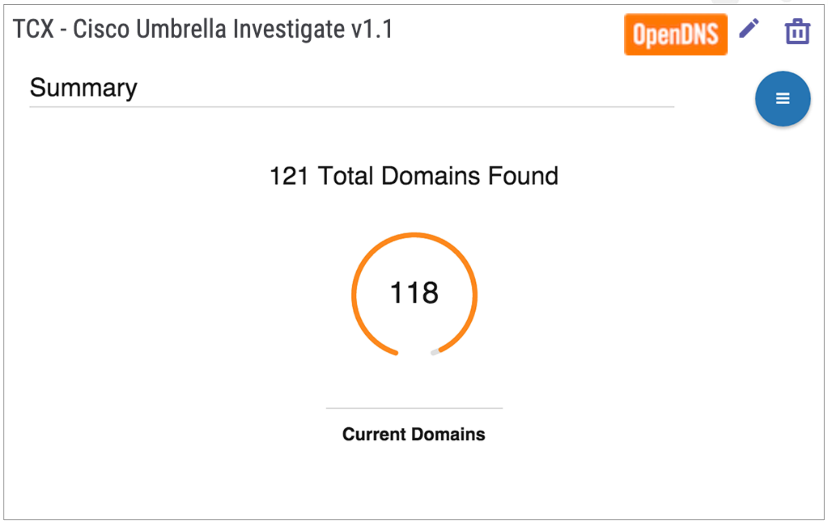
## Email Address Context

The Email Address context for the Cisco Umbrella Investigate Spaces app retrieves contextual data on a selected email address from the Cisco Umbrella Investigate API. The **Action** ≡ menu button provides options for viewing the following screens:

- **Summary**
- **Whois - Email**

### Summary

Figure 12 displays the **Summary** screen for the Email Address context.



TCX - Cisco Umbrella Investigate v1.1

Summary

121 Total Domains Found

118

Current Domains

Figure 12

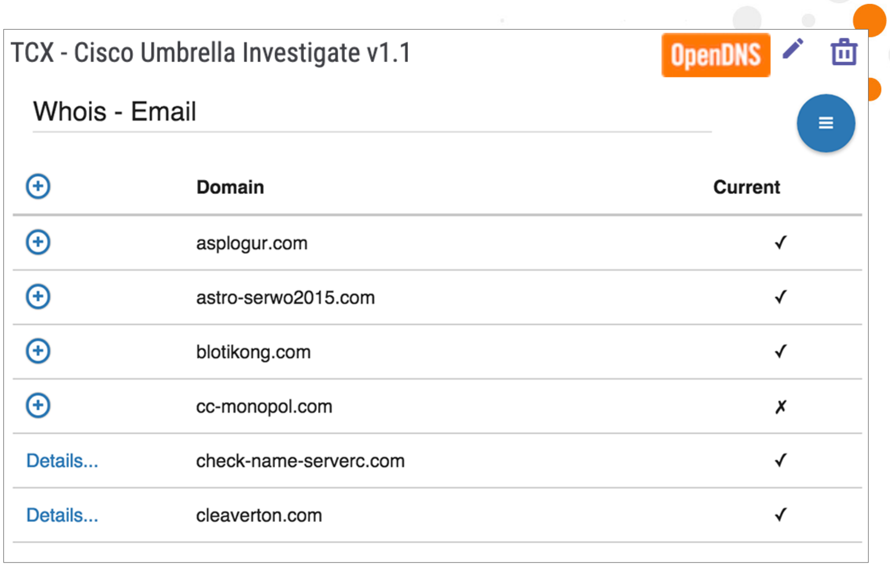
The **Summary** screen displays two key metrics provided by Cisco Umbrella Investigate for an Email Address, as summarized in Table 8.

Table 8

| Type | Description |
|---|---|
| Total Domains Found | This metric is the total number of domains registered by the Email Address (maximum: 500). |
| Current Domains | This flag designates whether a domain is currently registered by the Email Address. |

## Whois - Email

The **Whois - Email** screen (Figure 13) displays the first 500 domains (capped by Cisco Umbrella Investigate) registered by the Email Address.



TCX - Cisco Umbrella Investigate v1.1

Whois - Email

| ⊕ | Domain | Current |
|---|---|---|
| ⊕ | asplogur.com | ✓ |
| ⊕ | astro-serwo2015.com | ✓ |
| ⊕ | blotikong.com | ✓ |
| ⊕ | cc-monopol.com | ✗ |
| Details... | check-name-serverc.com | ✓ |
| Details... | cleaverton.com | ✓ |

Figure 13

***NOTE: Domain links can be directly added to ThreatConnect as Indicators by clicking on the Add ⊕ button. Indicators that have already been added will display a Details... link instead of a Add ⊕ button. See the "ADDING INDICATORS" section for more details.***

Table 9 defines the information displayed by the **Whois - Email** screen.

Table 9

| Type | Description |
|---|---|
| Domain | This field is the domain name registered by the Email Address. |
| Current | This flag designates whether the given domain is currently registered by the Email Address (✓) or not (X). |

## ADDING INDICATORS

Indicators displayed in the Cisco Umbrella Investigate Spaces app can provide valuable insight for an analyst. The app allows Indicators to be added to the current owner by clicking on an **Add** ⊕ button, either to the left of a single Indicator to add only that Indicator or in the header row to add all new Indicators in the table.

When an Indicator is added to the current owner, the app uses the parameters provided in Table 10, as excerpted from the "Parameter Definition" section. These parameters automate the task of adding Indicators with Tags, a Threat Rating, and a Confidence Rating. Once the Indicator is added, the button will change to a **Details…** link, along with a success message. Clicking on the link will display the Indicator's **Details** screen, where further updates can be performed if desired.

Table 10

| Type | Description |
|---|---|
| Comma-separated list of tags applied to indicator on an add | This parameter is a comma-separated list of Tags to apply to any Indicator added using the app. |
| Confidence applied to indicator on an add (0-100%) | This parameter is the Confidence Rating to apply to any Indicator added using the app. |
| Rating applied to indicator on an add (0-5 skulls) | This parameter is the Threat Rating to apply to any Indicator added using the app. |

On subsequent page loads for the added Indicators, the app will recognize if the Indicator exists in the current owner and display a **Details…** hyperlink in place of the **Add** button. The hyperlink indicates that the Indicator exists, and clicking on it will display its **Details** screen.