ThreatQuotient

Cisco Umbrella Investigate Operation Guide

Version 2.0.0

November 29, 2022

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ⚠ ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	2.0.0
Compatible with ThreatQ Versions	>= 4.57.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/cisco-umbrella-investigate-operation

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.
- **Latest Malicious Domains** - retrieves a list of malicious domains related to a given IP Address.

The operation is compatible with the following indicator types:

- Email Address
- FQDN
- IP Address
- URL

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.

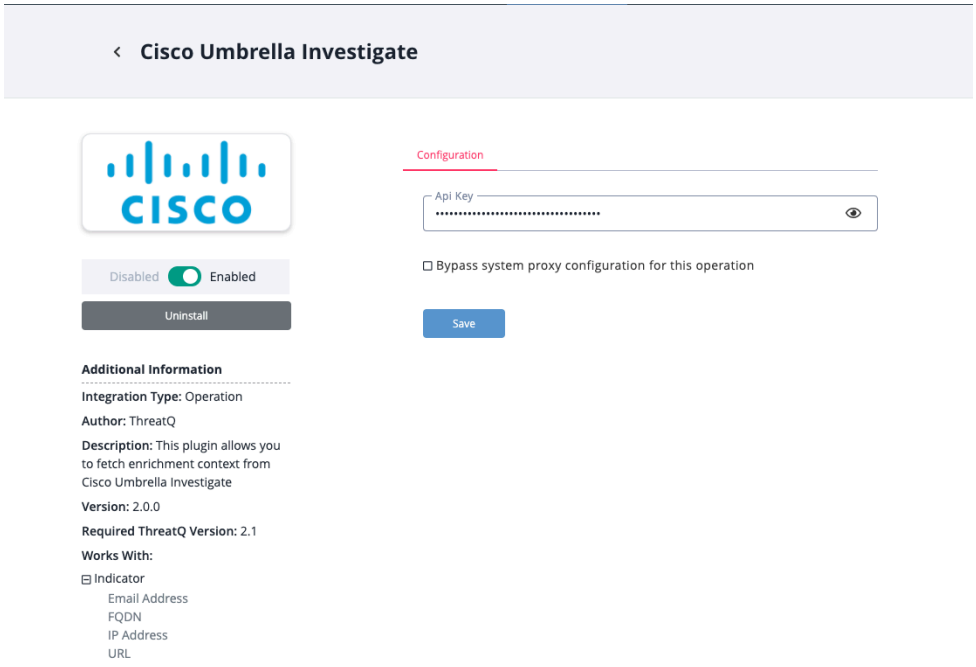
Configuration

> 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
API Key	Your Cisco Umbrella Investigate API Key.



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
Enrich	Enriches a domain with contextual or historical metadata.	Indicator	FQDN
Get Samples	Retrieves Cisco Threat Grid samples that are related to a given domain, IP, or URL.	Indicator	FQDN, IP Address, URL
Reverse WHOIS	Retrieves domains related to a given email address.	Indicator	Email Address
Get Associated Names	Retrieves domains related to a given IP Address.	Indicator	IP Address
Latest Malicious Domains	Retrieves a list of malicious domains related to a given IP Address.	Indicator	IP Address

Enrich

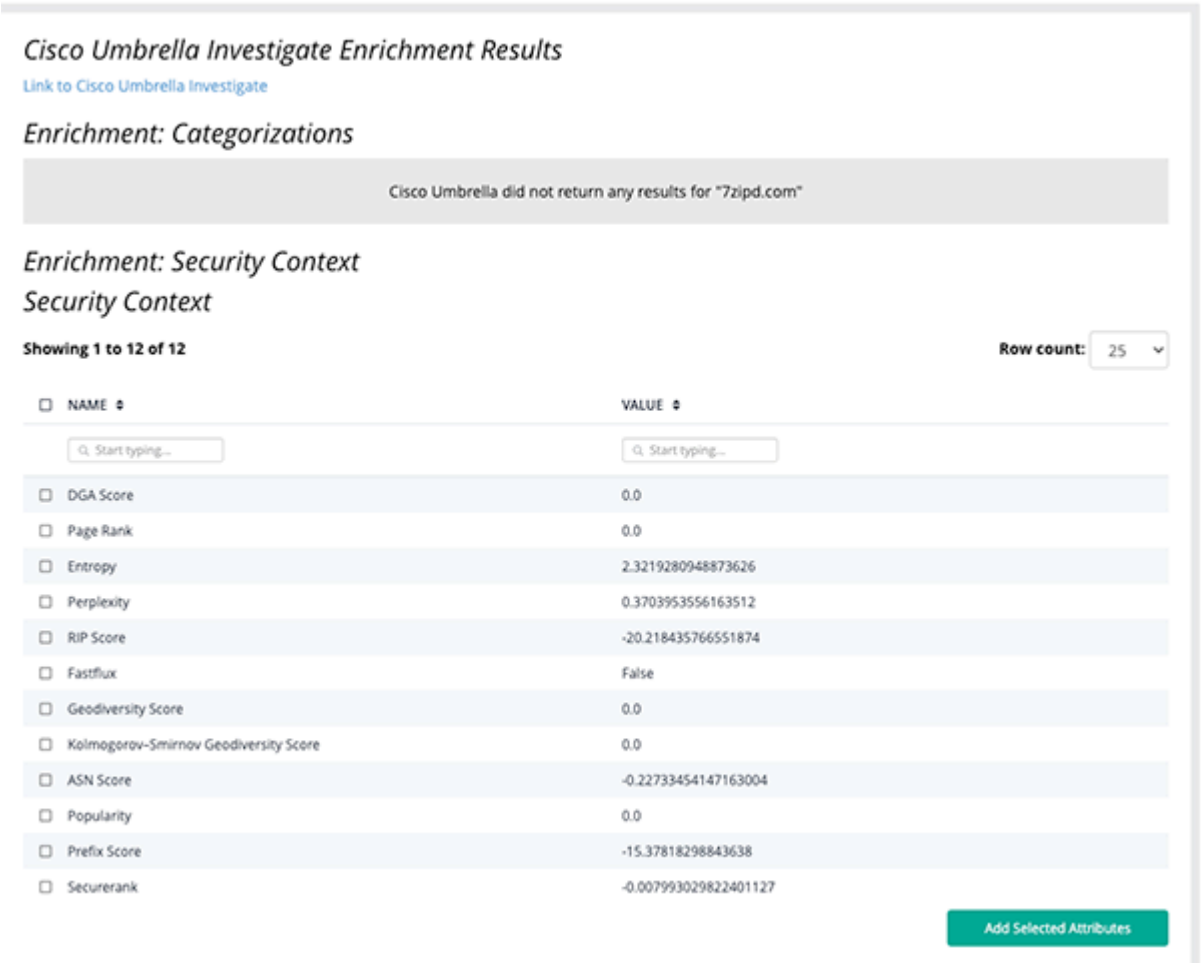
The Enrich action enriches a domain with contextual or historical metadata.

Action Parameters

The following configuration option is provided when using the action on an object:

PARAMETER	DESCRIPTION
Select Enrichment Options	Select one or more enrichment options (API Endpoints) to use to fetch metadata. Options include: • Get Risk Scores • Get Categorizations (default) • Get Security Context (default) • Get WHOIS (default) • Get Related Domains • Get Domain History

Enrich Example Result



Cisco Umbrella Investigate Enrichment Results

Link to Cisco Umbrella Investigate

Enrichment: Categorizations

Cisco Umbrella did not return any results for "7zipd.com"

Enrichment: Security Context

Security Context

Showing 1 to 12 of 12 **Row count:** 25

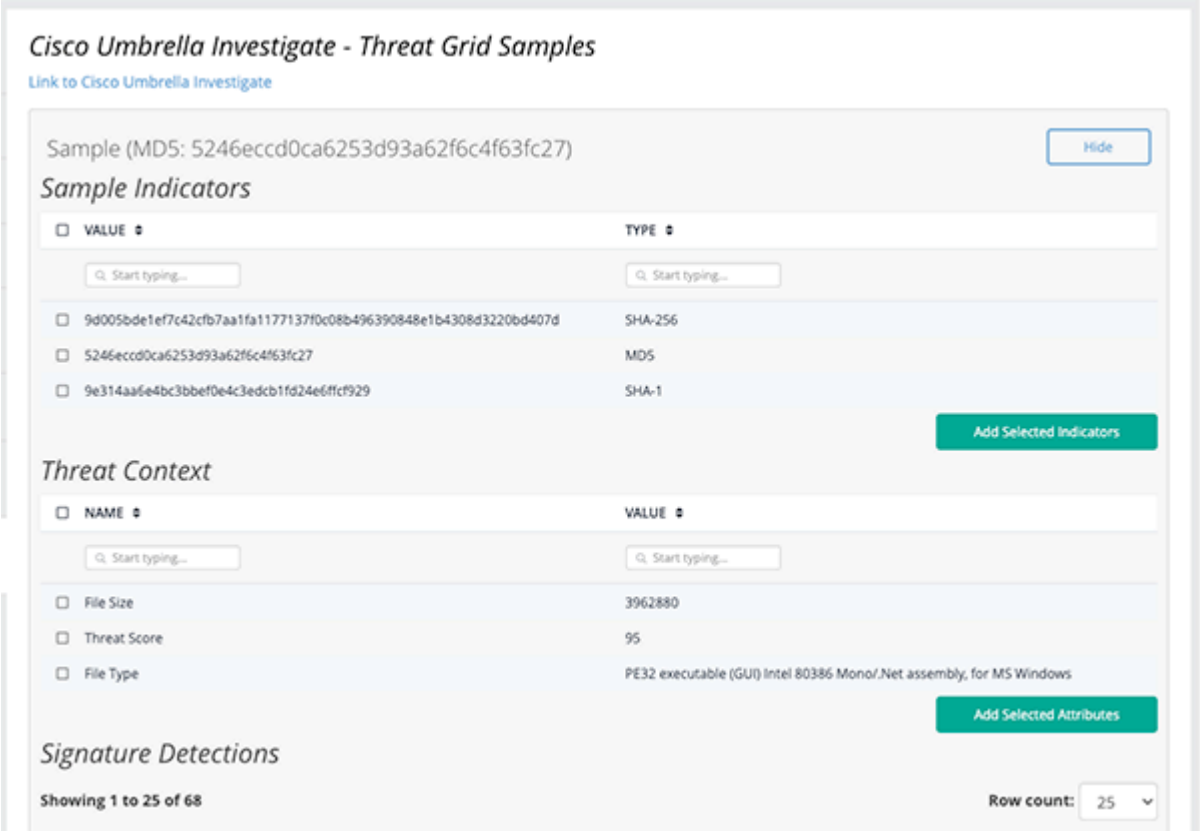
NAME	VALUE
DGA Score	0.0
Page Rank	0.0
Entropy	2.3219280948873626
Perplexity	0.3703953556163512
RIP Score	-20.218435766551874
Fastflux	False
Geodiversity Score	0.0
Kolmogorov-Smirnov Geodiversity Score	0.0
ASN Score	-0.22733454147163004
Popularity	0.0
Prefix Score	-15.37818298843638
Securerank	-0.007993029822401127

Add Selected Attributes

Get Samples

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

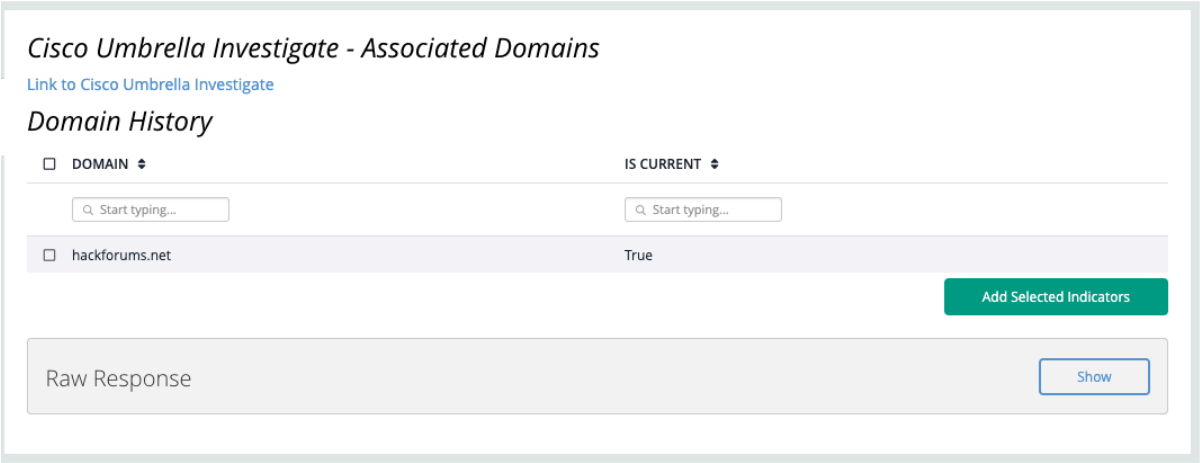
Get Samples Example Result



Reverse WHOIS

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

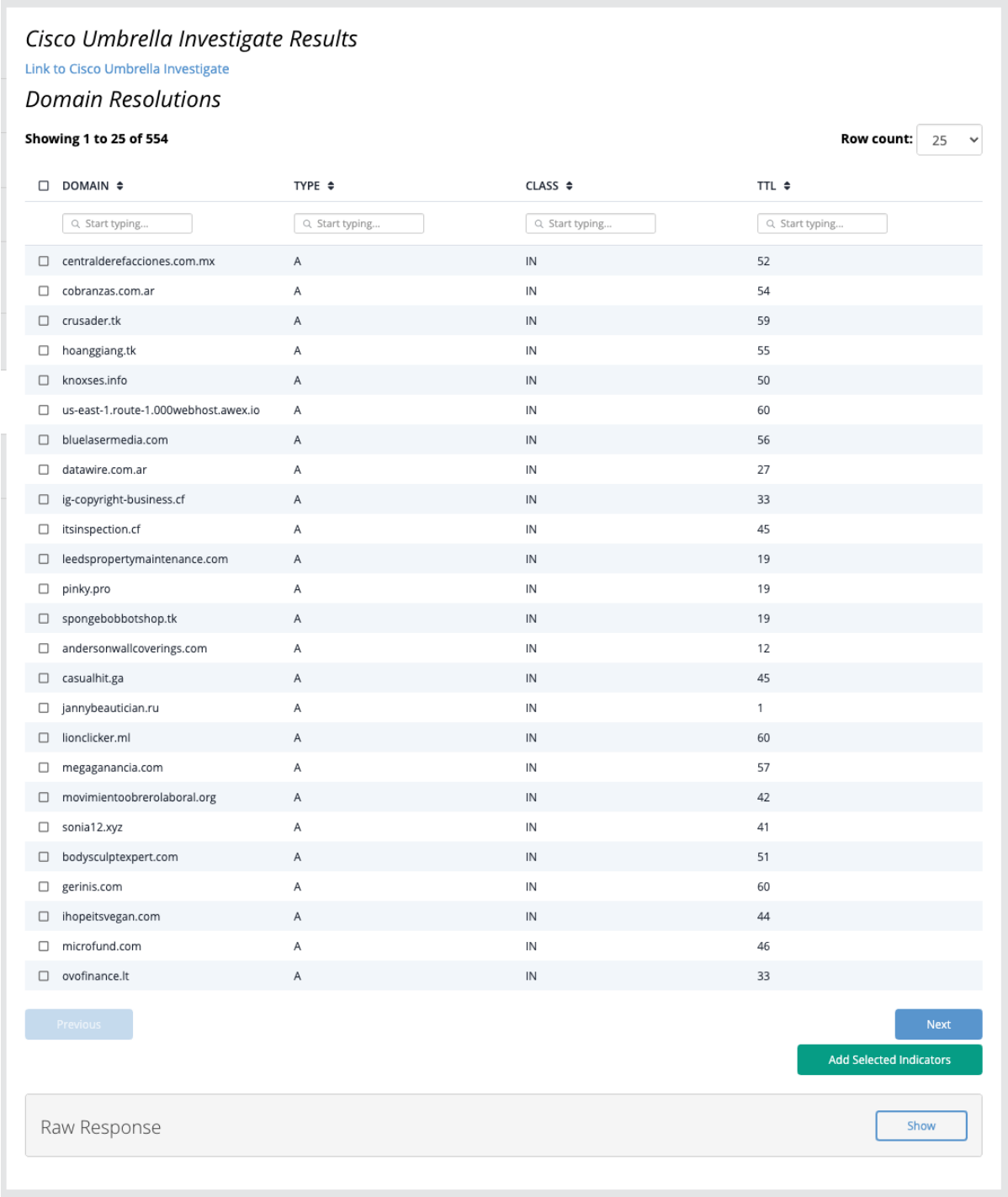
Reverse WHOIS Example Result



Get Associated Names

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

Get Associated Names Example Result



Cisco Umbrella Investigate Results

Link to Cisco Umbrella Investigate

Domain Resolutions

Showing 1 to 25 of 554 **Row count:** 25

DOMAIN	TYPE	CLASS	TTL
centralderefacciones.com.mx	A	IN	52
cobranzas.com.ar	A	IN	54
crusader.tk	A	IN	59
hoanggiang.tk	A	IN	55
knoxses.info	A	IN	50
us-east-1.route-1.000webhost.awex.io	A	IN	60
bluelasermedia.com	A	IN	56
datawire.com.ar	A	IN	27
ig-copyright-business.cf	A	IN	33
itsinspection.cf	A	IN	45
leedspropertymaintenance.com	A	IN	19
pinky.pro	A	IN	19
spongebobbotshop.tk	A	IN	19
andersonwallcoverings.com	A	IN	12
casualhit.ga	A	IN	45
jannybeautician.ru	A	IN	1
lionclicker.ml	A	IN	60
megaganancia.com	A	IN	57
movimientoobrerolaboral.org	A	IN	42
sonia12.xyz	A	IN	41
bodysculptexpert.com	A	IN	51
gerinis.com	A	IN	60
ihopeitsvegan.com	A	IN	44
microfund.com	A	IN	46
ovofinance.lt	A	IN	33

Previous Next

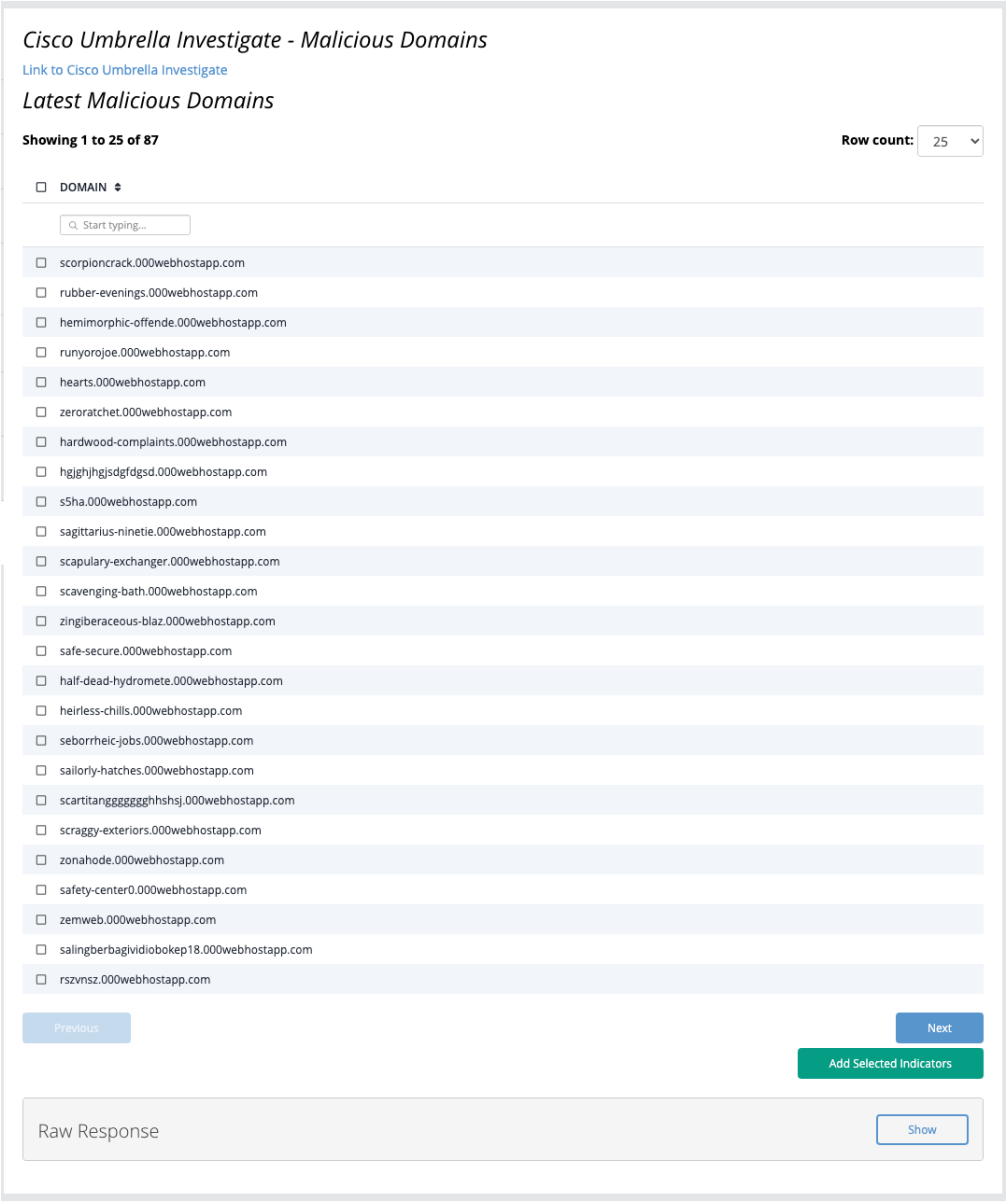
Add Selected Indicators

Raw Response Show

Latest Malicious Domains

The Latest Malicious Domains action fetches a list of malicious domains related to a given IP Address.

Latest Malicious Domains Example Result



Change Log

- **Version 2.0.0**
  - Initial release