



Anomali ThreatStream – WhoisXMLAPI App User Guide

Version 1.0.0

Support

Account Service and Management Team Email	support@whoisxmlapi.com
Technical Service Team Email	service.desk@whoisxmlapi.com

Introduction

Access billions of domain and DNS records with our collection of APIs. Map and study all connections across domain names, current and historical resource owners, IP addresses, subdomains, NS and MX servers, and more.

WhoisXMLAPI has developed a Context-Based Enrichment Integration and Pivot-Based Enrichment Integration for the Anomali ThreatStream platform.

This document outlines the process to install the **WhoisXMLAPI** enrichment Integration into the Anomali ThreatStream Platform and provides details on how to efficiently use the integration to acquire detailed threat information from WhoisXMLAPI and Threat Intelligence Platform.

List of IOC's supported for enrichment.

IOC	WhoisXMLAPI	ThreatIntelligencePlatform
Domain	Yes	Yes
Email	Yes	No
IP	Yes	No

List of WhoisXMLAPI endpoints supported for context-based enrichment.

Entity Type	API Endpoint
Domain	WHOIS API
	WHOIS History API
	DNS Lookup API
	IP Geolocation API
	Reverse DNS API (SOA)
	Reverse DNS API (txt)
	Reverse DNS API (CNAME)
	Connected Domains API
	Subdomains Lookup API
	Domains & Subdomains Discovery API (Domains - Ends With)
	Domains & Subdomains Discovery API (Domains - Contains)
	Domains & Subdomains Discovery API (Subdomains - Contains)
	Website Categorization API
	Website Contacts API
	Reverse NS
	Reverse MX
	Brand Alert
Email	Email Verification API
	Reverse WHOIS API
	WHOIS API
	Registrant Alert API
IP	
	Reverse IP API
	IP Geolocation API
	IP Netblocks API

List of Threat Intelligence Platform API endpoints supported for context-based enrichment.

Entity Type	API Endpoint
Domain	Connected Domain
	SSL Certificate Chain API
	Domain Malware Check API
	Domain Infrastructure Analysis
	Domain Reputation API

List of WhoisXMLAPI endpoints supported for pivot-based enrichment.

Entity Type	API Endpoint
Domain	WHOIS API
	WHOIS History API
Email	WHOIS API
	Reverse WHOIS API

Configuration

To configure and activate the **WhoisXMLAPI** App Enrichment bundle for ThreatStream platform, follow the steps mentioned below:

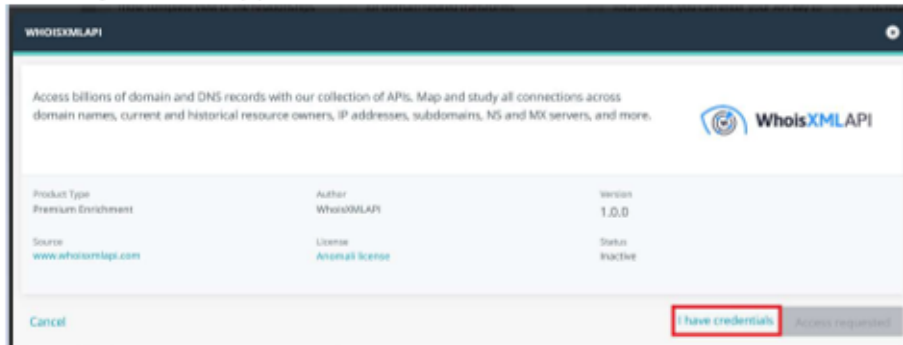
- Login into Anomali ThreatStream platform.
- Click on “APP STORE” button on the top menu-bar.



- All Integrations will be listed here. If you do not see WhoisXMLAPI Integration on the page, contact Support.

Within the **WhoisXMLAPI** integration application, click on the “Manage” button as shown below to configure **WhoisXMLAPI** App.

- A dialog box will appear as shown below, click on “I have credentials” button



- Insert your WhoisXMLAPI API key and Threat Intelligence Platform API Key in the API Key text-field. Finally, click on the Activate button to finish your configuration.

In case you have not obtained an API key from WhoisXMLAPI, contact “sales@whoisxmlapi.com” to get your API key.

WHOISXMLAPI

Access billions of domain and DNS records with our collection of APIs. Map and study all connections across domain names, current and historical resource owners, IP addresses, subdomains, NS and MX servers, and more.

Product Type: Premium Enrichment
Author: WhoisXMLAPI
Version: 1.0.0
Source: www.whoisxmlapi.com
License: Anonak license
Status: Inactive

Credentials

WhoisXMLAPI key
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Threat Intelligence Key
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Cancel **Activate**

At this point, the configuration for your **WhoisXMLAPI** Enrichment App is complete and is ready to be used. In case any error occurs, contact Support for further assistance.

WhoisXMLAPI	Threat Intelligence API	Message
Valid API key	Valid API key	Enrichment Activated
Valid API key	Invalid API key	Enrichment Activated only for WhoisXML API
Invalid API key	Valid API key	Enrichment Activated only for Threat Intelligence API
Invalid API key	Invalid API key	Failed to Activate enrichment WhoisXMLAPI

Activation is performed using the following API endpoints.

For WhoisXMLAPI Subdomains Lookup API endpoint with domain google.com is used.

For Threat Intel Platform API endpoint Domain Reputation with domain google.com is used.

Context-Based Enrichments

Context-based enrichments enable analysts to step through entire workflows on observable details pages, thus eliminating the need to jump between product screens. On the details page of an Observable (Domain, IP, Email) click on “WhoisXMLAPI” tab under the Enrichments sections (as shown below) to fetch the enrichment data for that Observable.

Domain Observable Context Enrichment

Categorization of different endpoints is achieved with different tabs.

Enrichments			
PASSIVE DNS (200)	WHOIS	WHOISXMLAPI	SUGGESTED ENRICHMENTS...
WEBSITE CATEGORIZATION AND CONTACTS	DOMAIN ATTRIBUTION	WHOIS	WHOIS HISTORY
	DNS	CONNECTED DOMAINS	DOMAIN & SUBDOMAIN DISCOVERY
	REVERSE NS	REVERSE MX	BRAND ALERT

When user selects **Website Categorization and Contacts Tab** will be able to perform enrichment for domain with Website Categorization and Website Contacts endpoints

Credit balance is extracted from WhoisXML website [My products | WhoisXML API](#)

****Credit Balance is applicable for all the WhoisXML API endpoints.**

Website Categorization and Contacts
Website Categorization
Website Contacts

Same is shown in the screenshots below.

Enrichments							
PASSIVE DNS (200)	WHOIS	WHOISXMLAPI	SUGGESTED ENRICHMENTS...				
WEBSITE CATEGORIZATION AND CONTACTS	DOMAIN ATTRIBUTION	WHOIS	WHOIS HISTORY	DNS	CONNECTED DOMAINS	DOMAIN & SUBDOMAIN DISCOVERY	REVERSE NS
							REVERSE MX
							BRAND ALERT

Website Categorization (Credit Balance : 2041)							
25	1 - 4 of 4 items						
Domain Name	Website Responded	Tier1 ID	Tier1 Confidence	Tier1 Name	Tier2 ID	Tier2 Confidence	Tier2 Name
google.com	true	IAB-596	0.994658812961241	Technology & Computing	IAB-619	0.9519259640008582	Internet
google.com	true	IAB-52	0.994658812961241	Business and Finance	IAB-99	0.9519259640008582	Information Services Industry
google.com	true	IAB-52	0.994658812961241	Business and Finance	IAB-115	0.9519259640008582	Technology Industry
google.com	true	IAB-52	0.994658812961241	Business and Finance	IAB-116	0.9519259640008582	Telecommunications Industry

Website Contacts (Credit Balance : 1055)								
25								
Company Names	Country Code	Domain Name	Emails	Meta	Phones	Postal Addresses	Social Links	Website Responded
Widomato Solid Plastic and Stormwater Manag Urmark University of Oregon University of Michigan University of Illinois-Gies College of Business (on The Hospital University (The University of Michigan The Arizona State University The Forge Entertainment Limited Tablet Devices For Work Play Starz Entertainment LLC Sony Financial Television Inc Play Store Occupational Safety and Health Morgan Calderini M3X10 Longene Television Inc Middle School High School Community College a and Continuing Education		google.com	description: , email: the estore@relations@ebcok description: , email: j coffey@business.co mailto:coffey@business.co	description: , email: the estore@relations@ebcok description: , email: j coffey@business.co mailto:coffey@business.co	phone: , descrip phone: , phoneNumber: 12 345.57.89 - 25 call Hou phone: , description: , phon number: 650.453.000		Facebook: Instagram: LinkedIn: Twitter:	true

When user selects **Domain Attribution Tab** will be able to perform enrichment for domain with Domain Infrastructure Analysis, Domain Reputation, Domain Malware Check, SSL Certification Chain and SSL Configuration Analysis endpoints.

Domain Attribution
Domain Infrastructure Analysis
Domain Reputation
Domain Malware Check
SSL Certification Chain
SSL Configuration Analysis

Same is shown in the screen shots below.

Enrichments

PASSIVE DNS (208) WHOIS WHOISXMLAPI SUGGESTED ENRICHMENTS...

WEBSITE CATEGORIZATION AND CONTACTS DOMAIN ATTRIBUTION WHOIS WHOIS HISTORY DNS CONNECTED DOMAINS DOMAIN & SUBDOMAIN DISCOVERY REVERSE NS REVERSE MX BRAND ALERT

Domain Infrastructure Analysis

25 1 - 11 of 11 items

Domain Name	Resource Type	IPv4	Geolocation	Subnetwork
google.com	web	142.250.72.174	City: Los Angeles Country: US Latitude: 34.05223 Longitude: -118.24368 Postalcode: 90001 Region: California Timezone: -08:00	Name: GOOGLE Ipaddressrange: 142.250.72.0 - 142.250.72.255 S Country: US Lastupdatedate: 2012-05-24T00:00:00Z
www.google.com	www:web	142.250.72.228	City: Los Angeles Country: US Latitude: 34.05223 Longitude: -118.24368 Postalcode: 90001 Region: California Timezone: -08:00	Name: GOOGLE Ipaddressrange: 142.250.72.0 - 142.250.72.255 S Country: US Lastupdatedate: 2012-05-24T00:00:00Z

Domain Reputation

25 1 - 2 of 2 items

Mode	Reputation Score	Tool	Tool Code	Warning
bot	90/11	WHOIS Domain check	95	warningDescription: Owner details are publicly a...
bot	90/11	SSL vulnerabilities	88	warningDescription: HTTP Strict Transport Secur...

Domain Malware Check

25

safeScore	warningDetails
100	

Enrichments

PASSIVE DNS (200) WHOIS WHOISXMLAPI SUGGESTED ENRICHMENTS...

WEBSITE CATEGORIZATION AND CONTACTS DOMAIN ATTRIBUTION WHOIS WHOIS HISTORY DNS CONNECTED DOMAINS DOMAIN & SUBDOMAIN DISCOVERY REVERSE NS REVERSE MX BRAND ALERT

WHOIS [Credit Balance : 1384]

25

Whois Data

Registrant : (organization: "Google LLC", street: "CA", country: "UNITED STATES", countryCode: "US"),
 AdministrativeContact : (organization: "Google LLC", street: "CA", country: "UNITED STATES", countryCode: "US"),
 TechnicalContact : (organization: "Google LLC", street: "CA", country: "UNITED STATES", countryCode: "US"),
 Nameservers : (ns1.google.com,ns2.google.com,ns3.google.com,ns4.google.com), hostName : (ns1.google.com,ns2.google.com,ns3.google.com,ns4.google.com), ip : (),
 Status : [clientUpdateProhibited,clientTransferProhibited,clientDeleteProhibited,serverUpdateProhibited,serverTransferProhibited,serverDeleteProhibited],
 Period : 2015,
 Audit : (CreatedDate: "2023-01-11 07:01:01 UTC", UpdatedDate: "2023-01-11 07:01:01 UTC"),
 CreatedDateNormalized : 1997-02-15 07:00:00 UTC,
 UpdatedDateNormalized : 2019-09-09 15:39:04 UTC,
 ExpireDateNormalized : 2028-09-14 04:00:00 UTC,
 RegistrarName : MarkMonitor, Inc.,
 RegistrarAsn : 792,
 ContactEmail : abusecomplaints@markmonitor.com,
 DomainName : .com.

When user selects **WHOIS History Tab** will be able to perform enrichment for WHOIS History endpoint

WHOIS History
WHOIS History

Same is shown in the screen shots below.

Enrichments

PASSIVE DNS (200) WHOIS WHOISXMLAPI SUGGESTED ENRICHMENTS...

WEBSITE CATEGORIZATION AND CONTACTS DOMAIN ATTRIBUTION WHOIS WHOIS HISTORY DNS CONNECTED DOMAINS DOMAIN & SUBDOMAIN DISCOVERY REVERSE NS REVERSE MX BRAND ALERT

WHOIS History [Credit Balance : 2143]

25 1 - 16 of 16 items

Whois History Data

CreatedDate : 1997-09-15 04:00:00 UTC,
 UpdatedDate : 2019-09-09 15:39:04 UTC,
 ExpireDate : 2028-09-14 04:00:00 UTC,
 Audit : (CreatedDate: "2023-01-11 07:00:57+00:00", UpdatedDate: "2023-01-11 07:00:57+00:00"),
 Nameservers : [NS1.GOOGLE.COM, NS2.GOOGLE.COM, NS3.GOOGLE.COM, NS4.GOOGLE.COM],
 WhoisServer : whois.markmonitor.com,
 RegistrarName : MarkMonitor, Inc.,
 Status : [clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited],
 RegistrantContact : (name: None, organization: "Google LLC", street: "", city: None, state: "CA", postalCode: None, country: "UNITED STATES", email: None, telephone: None, telephoneExt: None, fax: None, faxExt: None),
 AdministrativeContact : (name: None, organization: "Google LLC", street: "", city: None, state: "CA", postalCode: None, country: "UNITED STATES", email: None, telephone: None, telephoneExt: None, fax: None, faxExt: None),
 TechnicalContact : (name: None, organization: "Google LLC", street: "", city: None, state: "CA", postalCode: None, country: "UNITED STATES", email: None, telephone: None, telephoneExt: None, fax: None, faxExt: None),
 BillingContact : (name: None, organization: None, street: "", city: None, state: None, postalCode: None, country: None, email: None, telephone: None, telephoneExt: None, fax: None, faxExt: None),
 ZoneContact : (name: None, organization: None, street: "", city: None, state: None, postalCode: None, country: None, email: None, telephone: None, telephoneExt: None, fax: None, faxExt: None).

When the user selects **DNS Tab** will be able to perform enrichment for DNS Lookup, IP Geolocation, Reverse DNS SOA, Reverse DNS TXT and Reverse DNS CNAME endpoints.

DNS
DNS Lookup

IP Geolocation
Reverse DNS API (SOA)
Reverse DNS API (txt)
Reverse DNS API (CNAME)

Same is shown in the screen shots below.

Enrichments

PASSIVE DNS (200)

WHOIS

WHOISXMLAPI

SUGGESTED ENRICHMENTS...

WEBSITE CATEGORIZATION AND CONTACTS

DOMAIN ATTRIBUTION

WHOIS

WHOIS HISTORY

DNS

CONNECTED DOMAINS

DOMAIN & SUBDOMAIN DISCOVERY

REVERSE NS

REVERSE MX

BRAND ALERT

DNS Lookup [Credit Balance : 1491]

25

1 - 25 of 21 items

Type	Dns Type	Name	TTL	R Rset Type
16	TXT	google.com.	3600	16
16	TXT	google.com.	3600	16
16	TXT	google.com.	3600	16
16	TXT	google.com.	3600	16
16	TXT	google.com.	3600	16
16	TXT	google.com.	3600	16
16	TXT	google.com.	3600	16
16	TXT	google.com.	3600	16
16	TXT	google.com.	3600	16
16	TXT	google.com.	3600	16
16	TXT	google.com.	3600	16

IP Geolocation [Credit Balance : 782]

25

IP	Location	ISP	Connection Type
2507/2502400/2522.2000	Country : US Region : California City : Los Angeles Lat : 34.05225 Lng : -118.24368 Postcode : 90001 Timezone : -08:00 Geonameid : 5285247	Google LLC	

Enrichments

PASSIVE DNS (200)

WHOIS

WHOISXMLAPI

SUGGESTED ENRICHMENTS...

WEBSITE CATEGORIZATION AND CONTACTS

DOMAIN ATTRIBUTION

WHOIS

WHOIS HISTORY

DNS

CONNECTED DOMAINS

DOMAIN & SUBDOMAIN DISCOVERY

REVERSE DNS

REVERSE MX

BRAND ALERT

Connected Domains

25

Domains

01selfw7ur.com

08jhe3a8g.com

0s8a3g1q.com

123uss.liv

2ja6kulmty.com

4a69p1fz.com

5f8q378n.com

5manul0mz.com

67a0mug3l.com

6l8q307.com

Subdomains Lookup [Credit Balance : 2118]

25

1 - 25 of 10,000 items

Domain	First Seen	Last Seen
18e1anducapriwefga.google.com	04 Jan 2019 16:40:34	14 Jun 2020 20:41:48
4lnt6.chemu.google.com	04 Jan 2019 16:10:43	14 Jun 2020 22:22:43
an50aepm1.google.com	04 Jan 2019 16:21:29	14 Jun 2020 19:38:50
an1-safefrowsing.google.com	04 Jan 2019 16:19:30	14 Jun 2020 20:02:14
2q9s3-feedproxy.ghs.google.com	04 Jan 2019 14:11:06	14 Jun 2020 16:33:53
6wrtm1.google.com	04 Jan 2019 15:46:22	14 Jun 2020 20:44:48
144pwr-feedproxy.ghs.google.com	04 Jan 2019 13:55:00	14 Jun 2020 19:17:15
13j8h0-feedproxy.ghs.google.com	04 Jan 2019 13:59:51	14 Jun 2020 19:08:24
136jyn-feedproxy.ghs.google.com	04 Jan 2019 13:49:33	14 Jun 2020 19:14:54
hwty0-feedproxy.ghs.google.com	04 Jan 2019 19:51:00	14 Jun 2020 21:28:50
wphn12-hisucap.google.com	05 Jan 2021 08:07:02	05 Jan 2021 08:08:02
salatocm1v.scp.google.com	16 Sep 2020 20:16:04	12 Jan 2021 00:08:09

When user selects **Domains & Subdomains Discovery** Tab will be able to perform enrichment for Domains & Subdomains Discovery (Domains - Ends With), Domains & Subdomains Discovery (Domains - Contains) and Domains & Subdomains Discovery (Subdomains - Contains) endpoints.

Domains & Subdomains Discovery
Domains & Subdomains Discovery (Domains - Ends With)
Domains & Subdomains Discovery (Domains - Contains)
Domains & Subdomains Discovery (Subdomains - Contains)

Same is shown in the screen shots below.

Enrichments

PASSIVE DNS (208) WHOIS WHOISXMLAPI SUGGESTED ENRICHMENTS...

WEBSITE CATEGORIZATION AND CONTACTS DOMAIN ATTRIBUTION WHOIS WHOIS HISTORY DNS CONNECTED DOMAINS DOMAIN & SUBDOMAIN DISCOVERY REVERSE NS REVERSE MX BRAND ALERT

Domains Subdomains Discovery (Domains - Ends With) [Credit Balance : 2107]

25 ▾

Domains ⌵

- flashgoogle.com
- perfigoogle.com
- mail.gujargoogle.com
- webmail.gujargoogle.com
- oqongoogle.com
- w3dgtarsolution.seoongoogle.com
- supermaricolor-color-printer.corp.google.com
- ww16.kanygoogle.com
- www.elgerbults.nlgoogle.com
- ppelmmimgoogle.com

Domains Subdomains Discovery (Domains - Contains) [Credit Balance : 2096]

25 ▾

Domains ⌵

- xrn-ocf-mra06nca.com
- 1f21vug.feedproxy.ghs.google.com
- 16df1va.feedproxy.ghs.google.com
- 122rp1a.feedproxy.ghs.google.com
- 13v6rge.feedproxy.ghs.google.com
- 138y7gu.feedproxy.ghs.google.com
- 1daiinqw.feedproxy.ghs.google.com
- 1ew46o8.feedproxy.ghs.google.com
- 1es2bmd.feedproxy.ghs.google.com
- 1a2dkj5.feedproxy.ghs.google.com
- 1a2ghte.feedproxy.ghs.google.com
- abxpwo.feedproxy.ghs.google.com

Domains Subdomains Discovery (Subdomains - Contains) [Credit Balance : 2085]

25 ▾

Domains ⌵

- google.com.58rnox.com
- google.com.90ac729de208f5.site
- google.com.533hu.com
- google.com.76rnox.com
- google.com.hax0r.us
- google.com.ar.com
- google.com.6hu08.com
- google.com.6hu36.com
- google.com.6hu79.com
- google.com.bitfiya.com
- google.com.310hu.com

When user selects **Reverse NS** Tab will be able to perform enrichment for Reverse NS endpoint

Reverse NS
Reverse NS

Same is shown in the screen shots below.

Enrichments		
PASSIVE DNS (200)	WHOIS	WHOISXMLAPI
SUGGESTED ENRICHMENTS...		
WEBSITE CATEGORIZATION AND CONTACTS	DOMAIN ATTRIBUTION	WHOIS
WHOIS HISTORY	DNS	CONNECTED DOMAINS
DOMAIN & SUBDOMAIN DISCOVERY	REVERSE NS	REVERSE MX
BRAND ALERT		
Reverse NS [Credit Balance : 2080]		
25	1 - 25 of 35 items	
Name	First Seen	Last Visit
artrake.com	19 Nov 2021 00:00:00	19 Nov 2022 00:00:00
azmaicompany.net	19 Nov 2021 00:00:00	21 Dec 2022 00:00:00
cyblenetwork	06 Jun 2022 00:00:00	16 Dec 2022 00:00:00
cybleshop	16 Jul 2022 00:00:00	16 Dec 2022 00:00:00
cyblestore	12 Jul 2022 00:00:00	15 Dec 2022 00:00:00
devdynamonline	04 Dec 2022 00:00:00	04 Dec 2022 00:00:00
huan.br	18 Nov 2021 00:00:00	02 Dec 2022 00:00:00

When user selects **Reverse MX** tab will be able to perform enrichment for Reverse MX endpoint

Reverse MX
Reverse MX

Same is shown in the screen shots below.

Enrichments		
PASSIVE DNS (200)	WHOIS	WHOISXMLAPI
SUGGESTED ENRICHMENTS...		
WEBSITE CATEGORIZATION AND CONTACTS	DOMAIN ATTRIBUTION	WHOIS
WHOIS HISTORY	DNS	CONNECTED DOMAINS
DOMAIN & SUBDOMAIN DISCOVERY	REVERSE NS	REVERSE MX
BRAND ALERT		
Reverse MX [Credit Balance : 2075]		
25	1 - 25 of 300 items	
Name	First Seen	Last Visit
121do.com	19 Nov 2021 00:00:00	10 Jan 2023 00:00:00
150svasss.com.br	08 Jun 2022 00:00:00	08 Jan 2023 00:00:00
38k.co.jp	27 May 2022 00:00:00	18 Nov 2022 00:00:00
40engenbaria.com.br	16 Jun 2022 00:00:00	18 Dec 2022 00:00:00
4messages.net	01 May 2022 00:00:00	21 Dec 2022 00:00:00
85videos.com	15 Jun 2022 00:00:00	11 Jan 2023 00:00:00
wibewinq.br	30 Sep 2022 00:00:00	31 Dec 2022 00:00:00

When user selects **Brand Alert Tab** will be able to perform enrichment for Brand Alert endpoint

Brand Alert
Brand Alert

Same is shown in the screen shots below.

Enrichments		
PASSIVE DNS (200)	WHOIS	WHOISXMLAPI
SUGGESTED ENRICHMENTS...		
WEBSITE CATEGORIZATION AND CONTEXTS		
DOMAIN ATTRIBUTION		
WHOIS		
WHOIS HISTORY		
DNS		
CONNECTED DOMAINS		
DOMAIN & SUBDOMAIN DISCOVERY		
REVERSE MX		
REVERSE MX		
BRAND ALERT		
Brand Alert [Credit Balance : 2065]		
25	1 - 25 of 100 items	
Domain Name	Date	Action
positionmemogoogle.com	2023-01-10	added
almetagoogle.com	2023-01-10	added
googlephonenum.com	2023-01-10	added
googlelunten.ch	2023-01-10	dropped
googleic518.cn	2023-01-10	discovered
googleadvertising.uk	2023-01-10	added
google-3g.com	2023-01-10	dropped

IP Observable Context Enrichment

Categorization of different endpoints is achieved with different tabs.

Enrichments			
PASSIVE DNS (2)	WHOIS	WHOISXMLAPI	SUGGESTED ENRICHMENTS...
CONNECTED INFRASTRUCTURE			
IP GEOLOCATION			
IP NETBLOCKS WHOIS			

When user selects **Connected Infrastructure Tab** will be able to perform enrichment for Reverse IP endpoint

Connected Infrastructure
Reverse IP

Same is shown in the screen shots below.

Enrichments			
PASSIVE DNS (2)	WHOIS	WHOISXMLAPI	SUGGESTED ENRICHMENTS...
CONNECTED INFRASTRUCTURE	IP GEOLOCATION	IP NETBLOCKS WHOIS	
Reverse IP			
25	1 - 8 of 8 items		
Domain	Rev. Taken	Last Valid	
01-team.mingyong-groups.com	18 Jan 2021 00:00:00	29 Nov 2022 00:00:00	
521wells.com	12 Nov 2021 00:00:00	10 Jun 2023 00:00:00	
c3c.digital	15 Feb 2020 00:00:00	21 Nov 2022 00:00:00	
ivickents.com	17 Oct 2019 00:00:00	30 Dec 2022 00:00:00	
lovepoems.work	19 Aug 2022 00:00:00	07 Jan 2023 00:00:00	
mbcsp.com	28 Jul 2021 00:00:00	01 Jan 2023 00:00:00	
prismelionas.kontora.com.akadns.net	05 Oct 2019 00:00:00	28 Dec 2022 00:00:00	
vip.206689.top	04 Jun 2022 00:00:00	01 Jan 2023 00:00:00	

When user selects **IP Geolocation Tab** will be able to perform enrichment for IP Geolocation endpoint

IP Geolocation
IP Geolocation

Same is shown in the screen shots below.

Enrichments

PASSIVE DNS (2)

WHOIS

WHOISXMLAPI

SUGGESTED ENRICHMENTS...

CONNECTED INFRASTRUCTURE

IP GEOLOCATION

IP NETBLOCKS WHOIS

IP Geolocation [Credit Balance : 781]

25

IP	Location	ISP	Connection Type	Domains	AS
1.2.4.5	Country : CN Region : Beijing Shi City : Chedagou Lat : 39.94696 Lng : 116.29472 Postalcode : Timezone : +08:00 Geonameid : 1899239	China Internet Network Information Cen ter	-	lovepoems.work prismelionas.kontora.com.akadns.net vip.206689.top c3c.digital 521wells.com	Asn : 24409 Name : CHN-CRITICAL-IP Route : 1.2.4.0/24 Domain : Type :

When user selects **IP Netblocks WHOIS Tab** will be able to perform enrichment for IP Netblocks endpoint

IP Netblocks WHOIS
IP Netblocks

Same is shown in the screen shots below.

Enrichments

PASSIVE DNS (2)

WHOIS

WHOISXMLAPI

SUGGESTED ENRICHMENTS...

CONNECTED INFRASTRUCTURE

IP GEOLOCATION

IP NETBLOCKS WHOIS

IP Netblocks [Credit Balance : 993]

25

1 - 5 of 5 items

IPNetblocks Data

```

{
  "netnum": "1.2.4.0 - 1.2.4.255",
  "netnumRtst": "28147058862072",
  "netnumLstst": "281470698952927",
  "asn": {
    "asn": "24409",
    "name": "CHNIC-CRITICAL-AP",
    "type": "I",
    "route": "1.2.4.0/24",
    "domain": ""
  },
  "netname": "CHNIC-CRITICAL-CN",
  "nethandle": "",
  "description": ["China Network Information Center", "No 4, Zhongguancun No.4 South Street, Haidian District, Beijing", "P.O.Box No 6 Branch-box of No 349 Mailbox, Beijing"],
  "modified": "2021-08-16T01:30:45Z",
  "country": "CN",
  "city": "",
  "address": []
}

```

Email Observable Context Enrichment

Categorization of different endpoints is achieved with different tabs.

Enrichments

WHOIS

WHOISXMLAPI

SUGGESTED ENRICHMENTS...

EMAIL VERIFICATION

WHOIS API

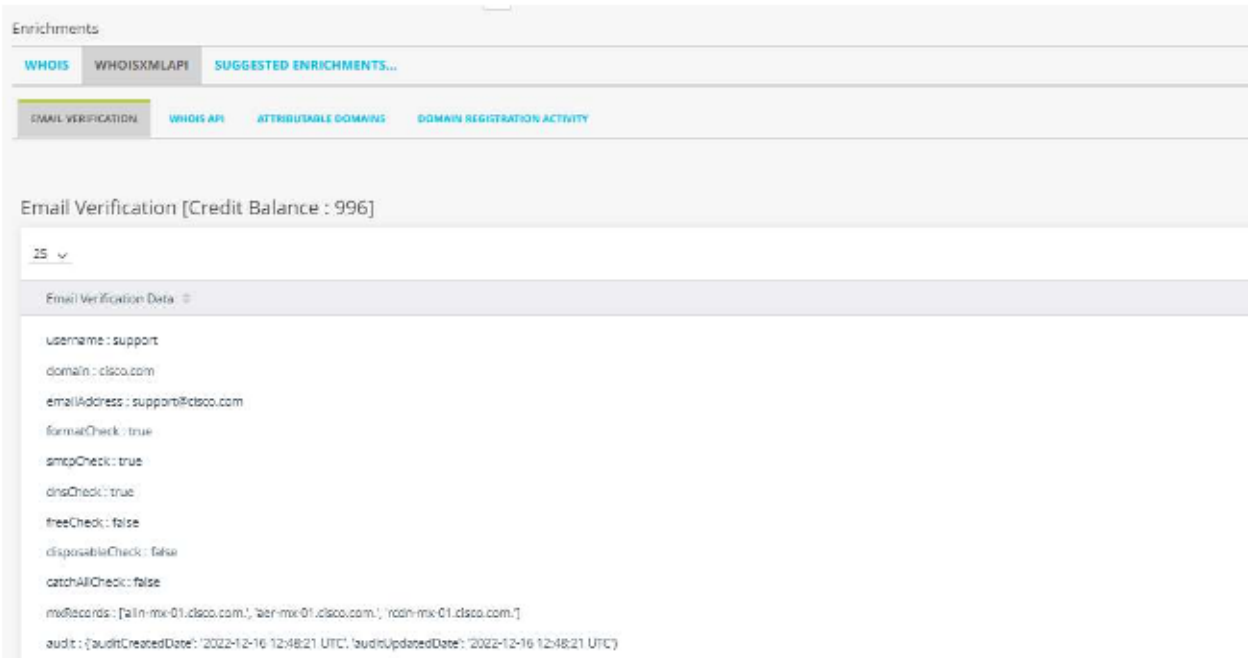
ATTRIBUTABLE DOMAINS

DOMAIN REGISTRATION ACTIVITY

When user selects **Email Verification Tab** will be able to perform enrichment for Email Verification endpoint

Email Verification
Email Verification

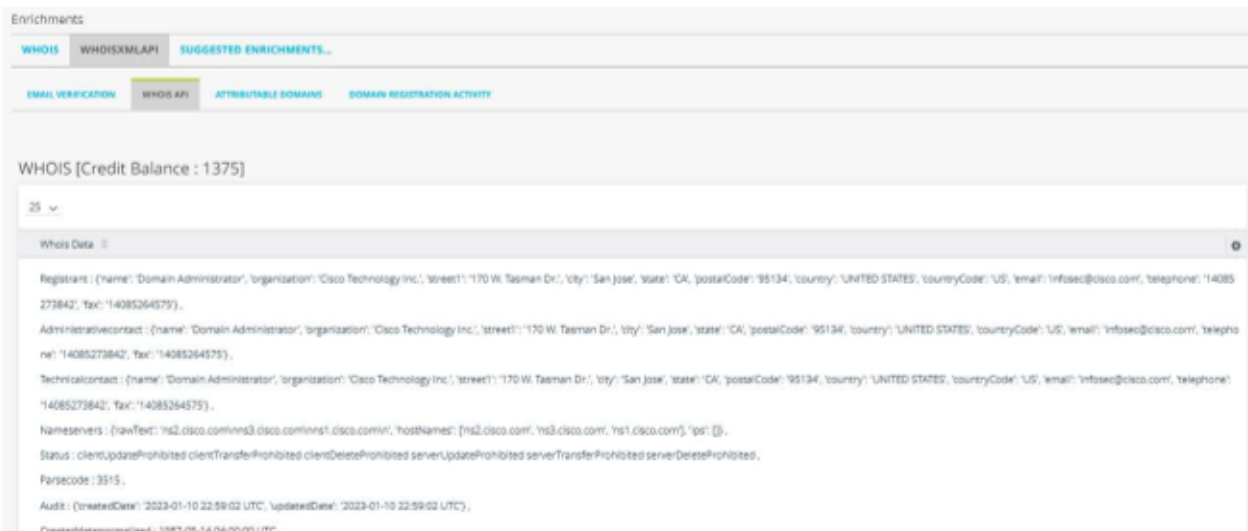
Same is shown in the screen shots below.



When user selects **WHOIS API Tab** will be able to perform enrichment for WHOIS endpoint

WHOIS API
WHOIS

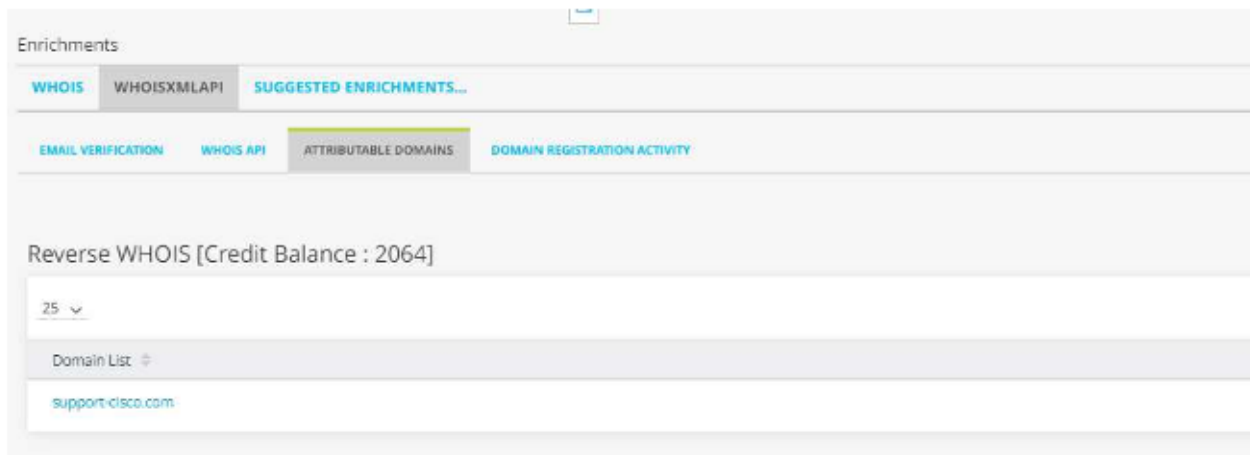
Same is shown in the screen shots below.



When user selects **Attributable Domains Tab** will be able to perform enrichment for Reverse WHOIS endpoint

Attributable Domains
Reverse WHOIS

Same is shown in the screen shots below.



When user selects **Domain Registration Activity Tab** will be able to perform enrichment for Registrant Alert endpoint

Domain Registration Activity
Registrant Alert

Same is shown in the screen shots below.

****with sample mail id not data available**



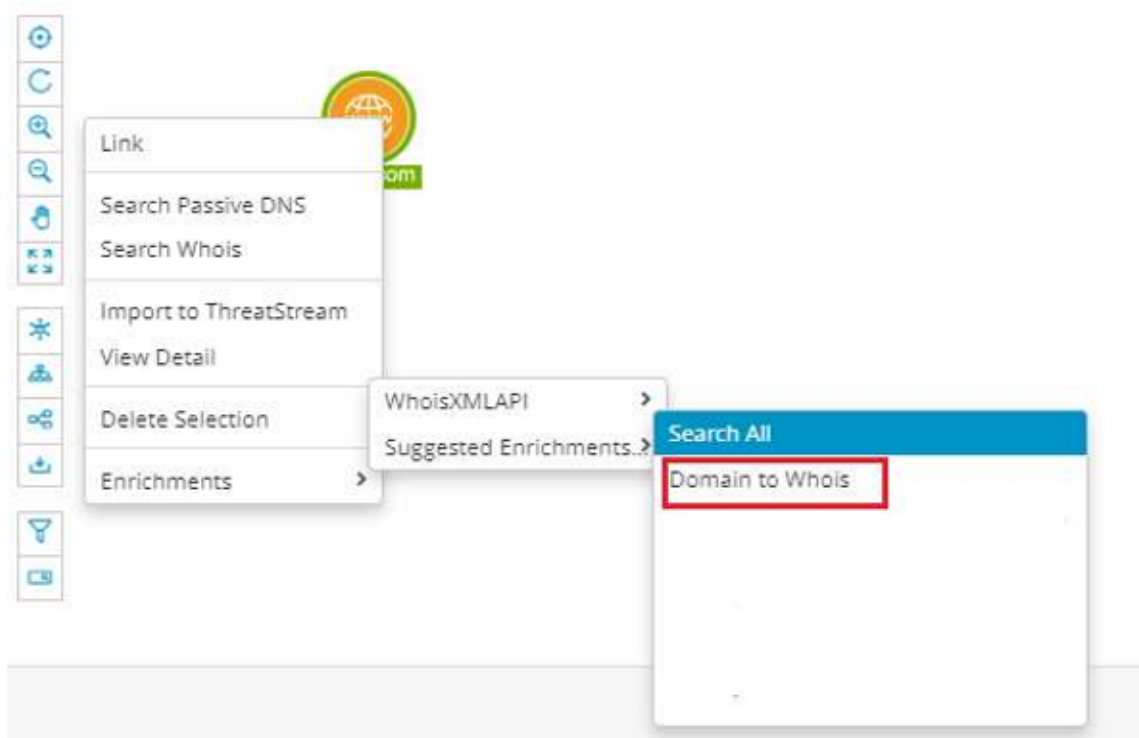
Pivot-Based Enrichments

Pivot-based enrichments expand the breadth of data that analysts can use to build out graphical relationships during threat research on the pivoting tool on the Investigations user interface within ThreatStream.

Domain to Whois

When user selects **Domain to Whois Enrichment**, will be able to see the Whois Endpoints Contact Email, Name Server, Registrar Name, Organization Name and Telephone.

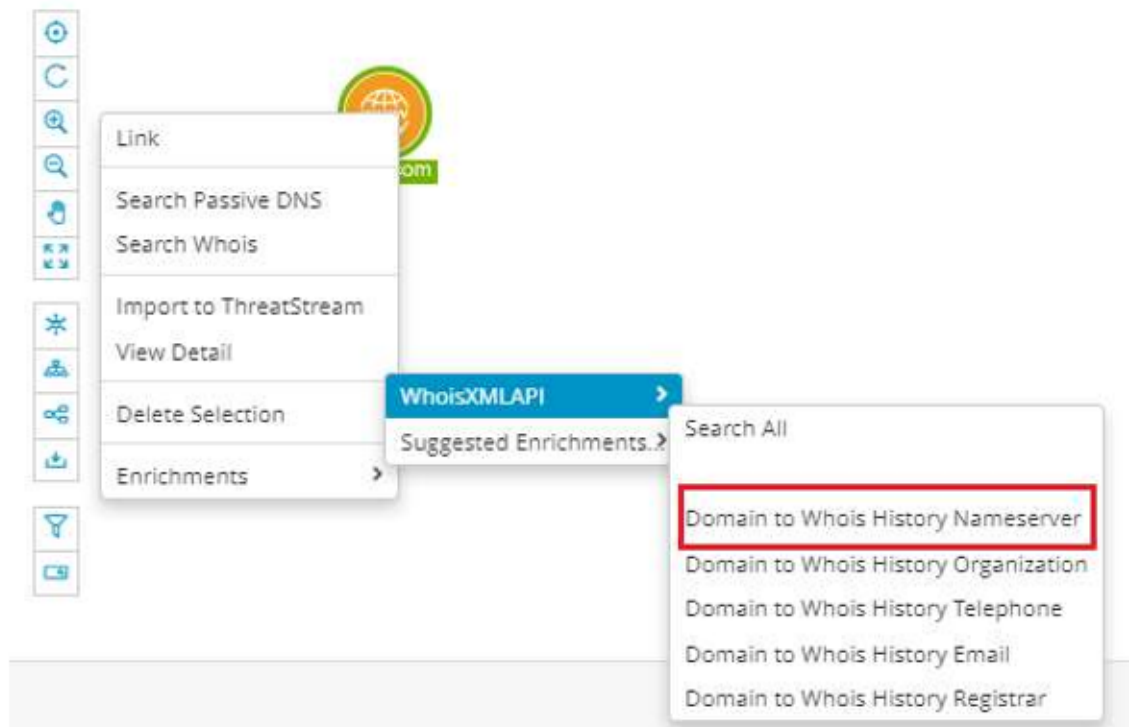
Contact Email
Name Server
Registrar Name
Organization Name
Telephone



Domain to Whois History

When user selects **Domain to Whois History Enrichment** will be able to perform enrichment for Whois History endpoints Name Server, Registrar Name, Organization Name and Telephone

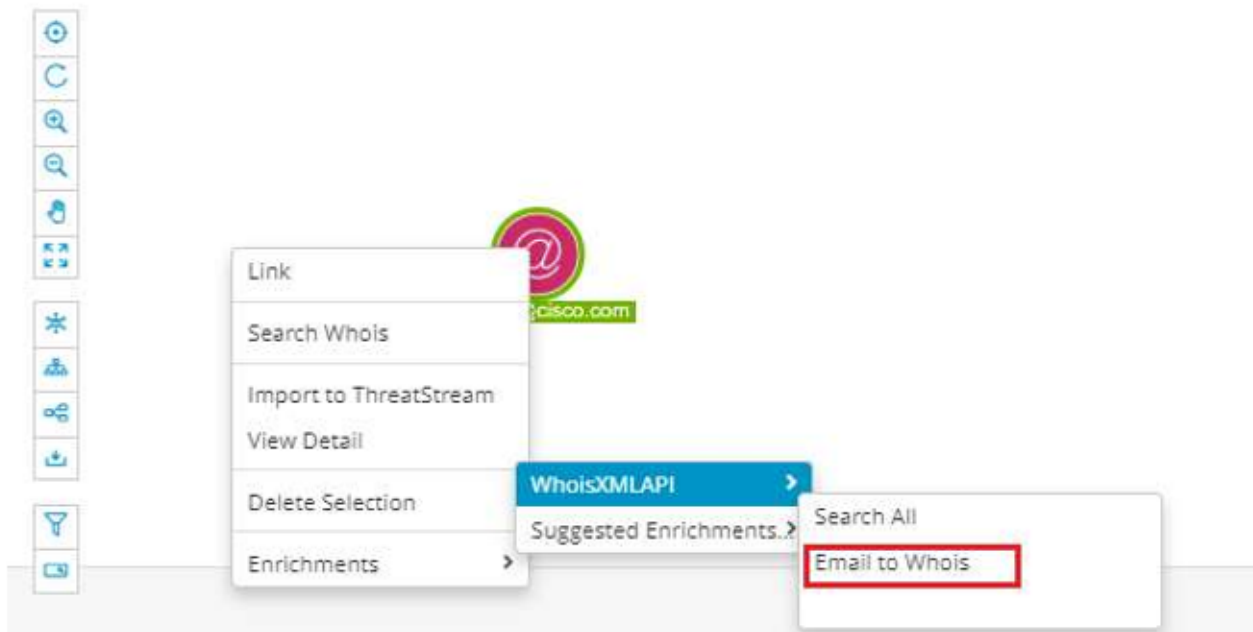
Email
Name Server
Registrar Name
Organization Name
Telephone



Email to Whois

When user selects **Email to Whois Enrichment** will be able to perform enrichment for Email to Whois endpoints Domain Name, Name Server, Registrar Name, Organization Name and Telephone.

Domain Name
Name Server
Registrar Name
Organization name
Telephone



Email to Reverse Whois Domain

When user selects **Email to Reverse Whois Enrichment** will be able to perform enrichment for Reverse Whois endpoint

