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

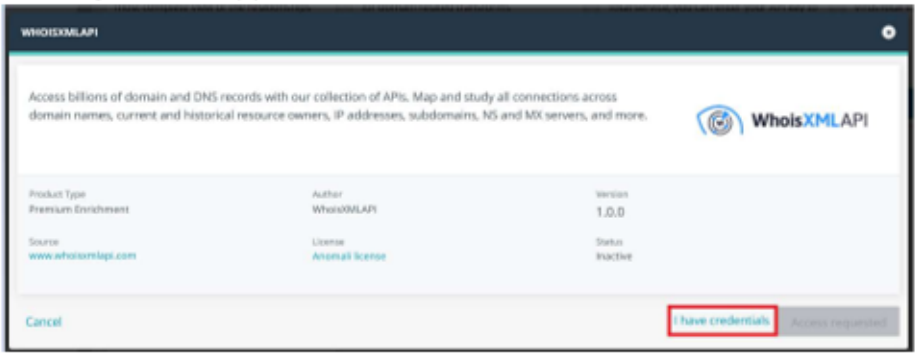
To configure and activate the **WhoisXMLAPI** App Enrichment bundle for ThreatStream platform, follow the steps mentioned below:

- 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.

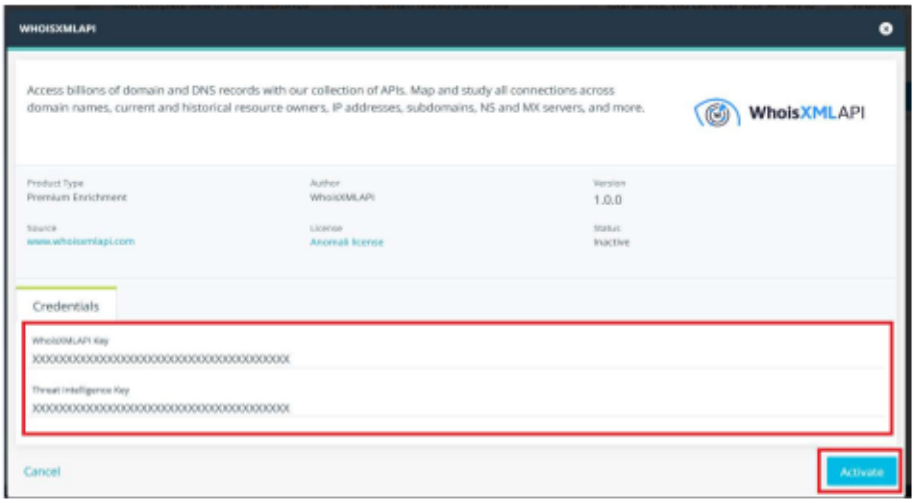
  Within the **WhoisXMLAPI** integration application, click on the “Manage” button as shown below to configure **WhoisXMLAPI** App.

- 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.



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.

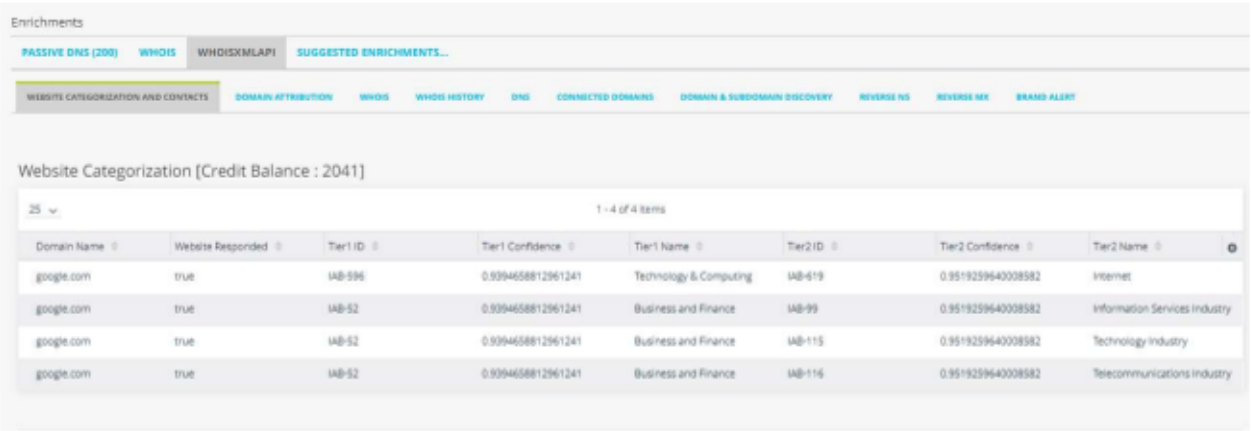
When user selects **Website Categorization and Contacts Tab** will be able to perform enrichment for domain with Website Categorization and Website Contacts endpoints

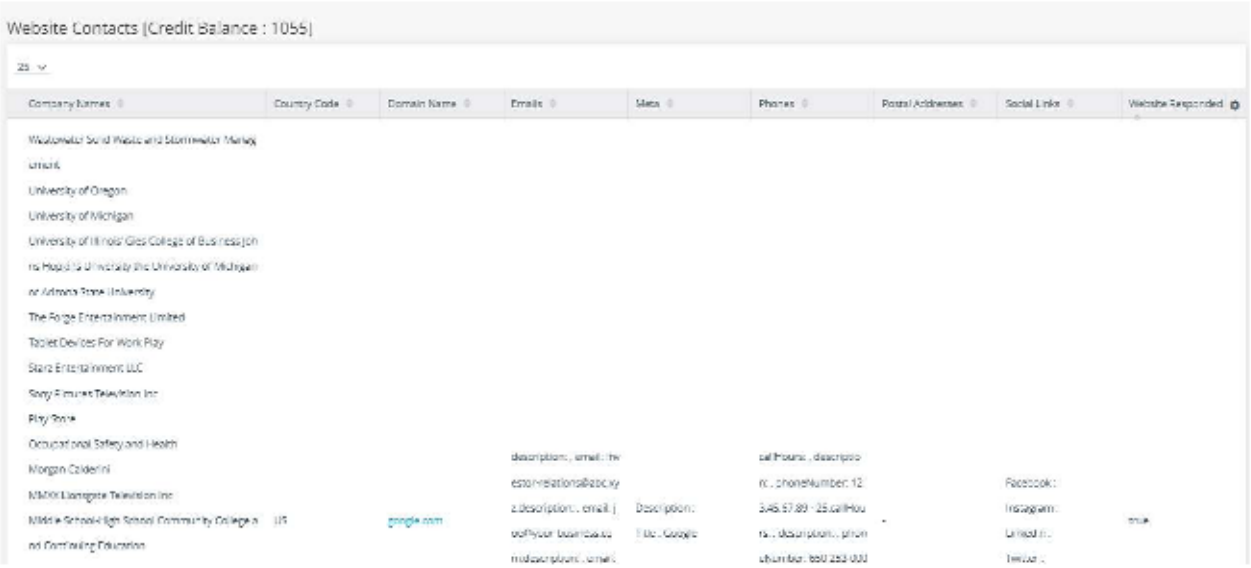
Credit balance is extracted from WhoisXML website [My products | WhoisXML API]

**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.

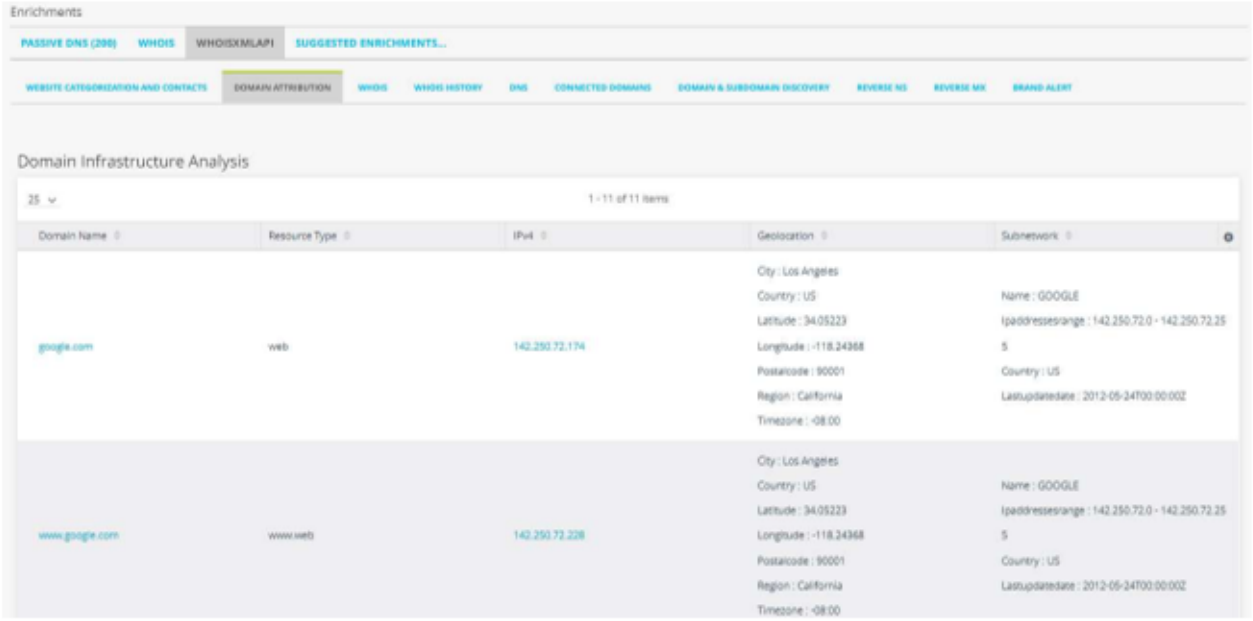


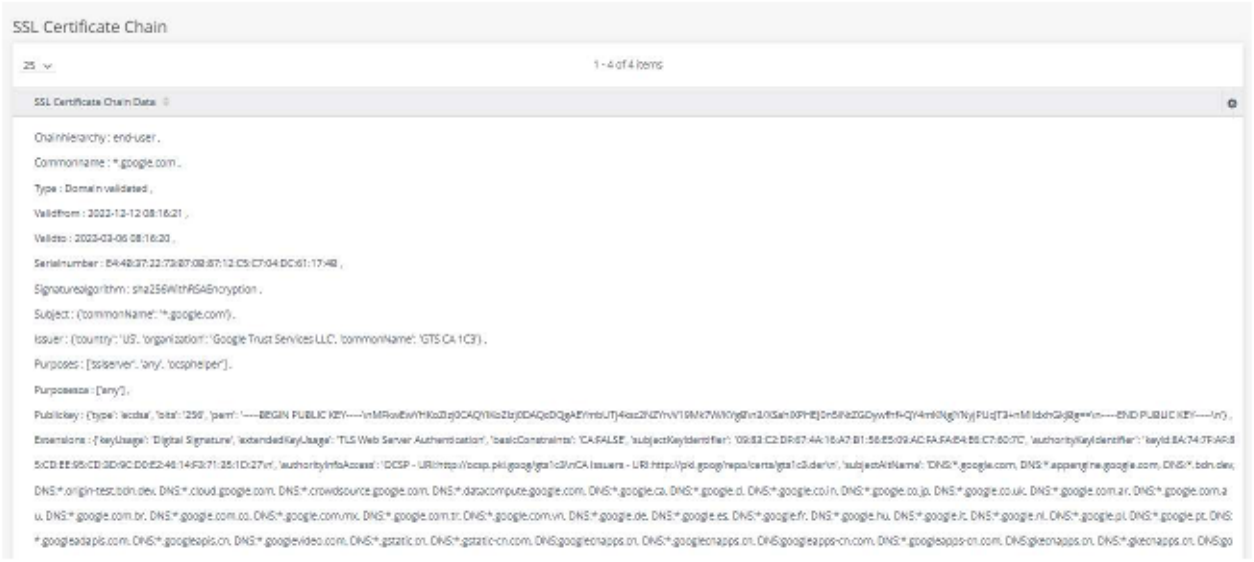


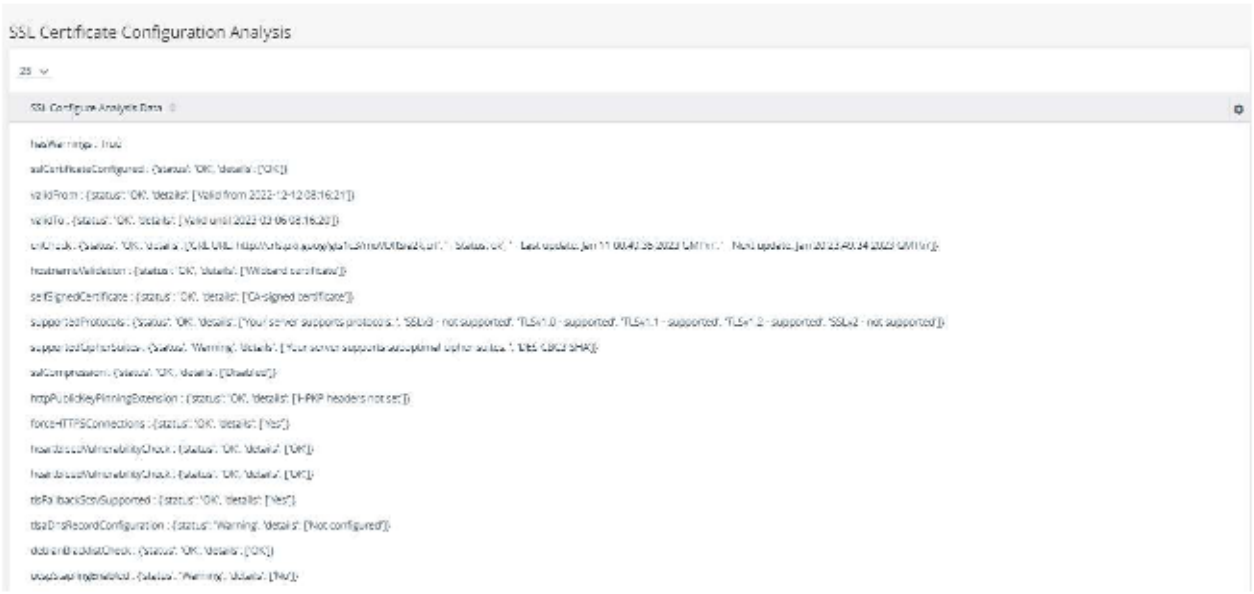
When user selects **Domain Attribution Tab** will be able to perform enrichment for domain with Domain Infrastructure Analysis, Domain Reputation, Domain Malware Check, SSL Certification Chain and SSL Configuration Analysis endpoints.

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

Same is shown in the screen shots below.



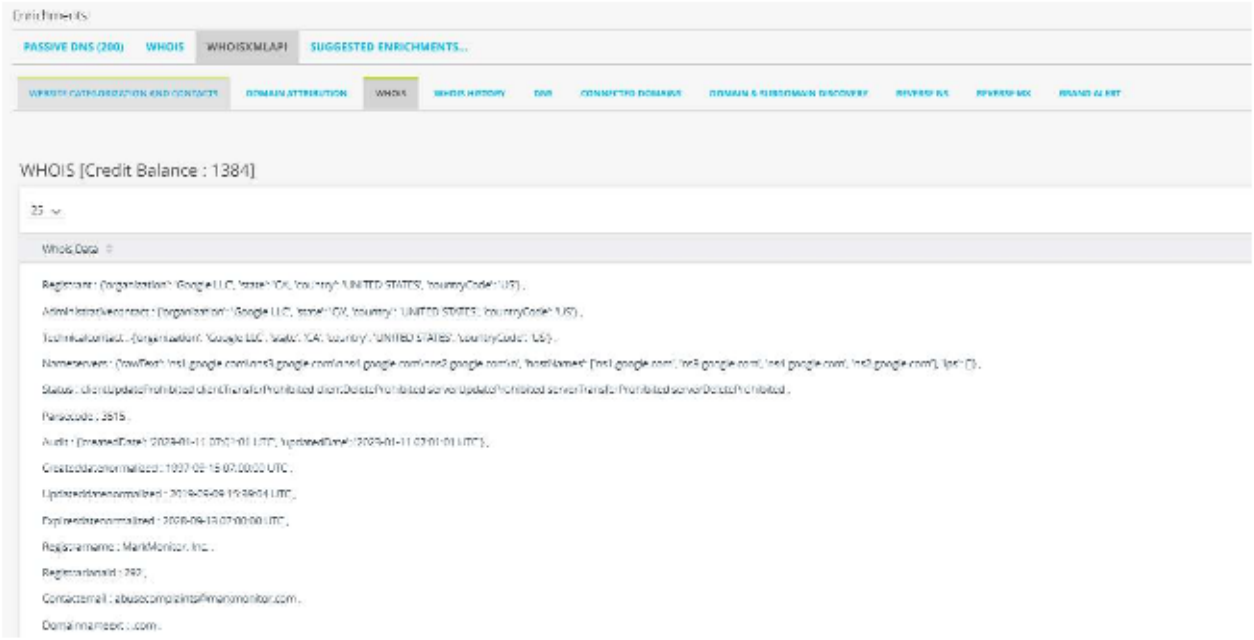




When user selects **WHOIS Tab** will be able to perform enrichment for WHOIS endpoint

WHOIS
WHOIS

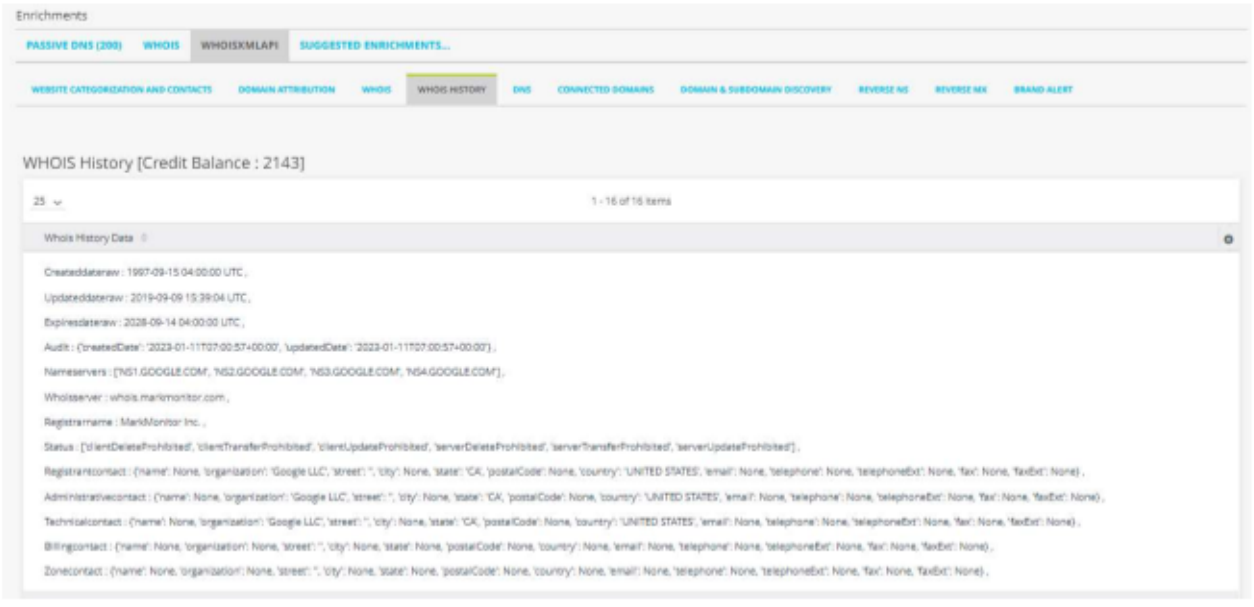
Same is shown in the screen shots below.



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.

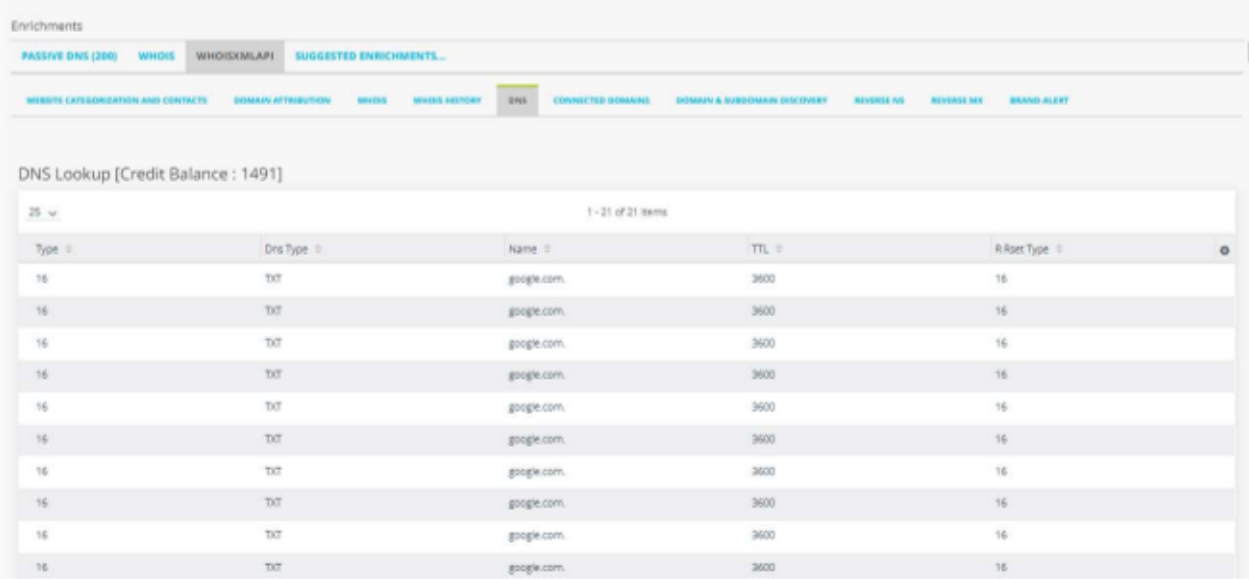


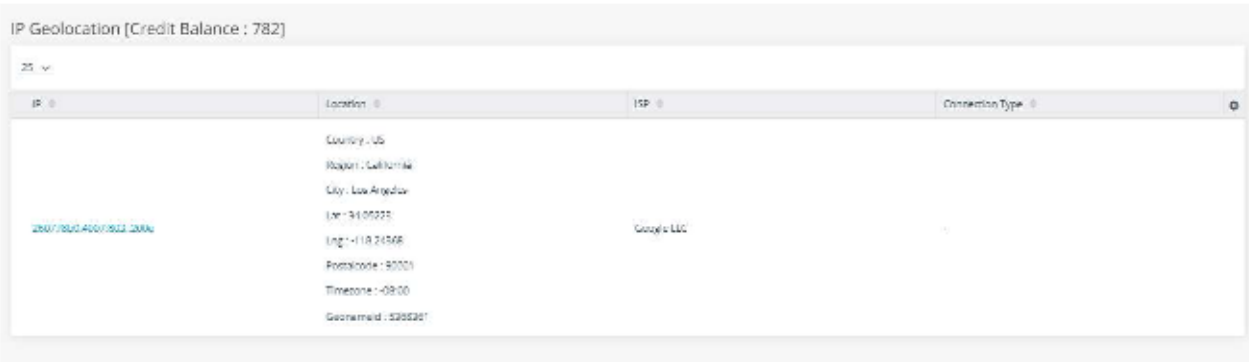
When the user selects **DNS Tab** will be able to perform enrichment for DNS Lookup, IP Geolocation, Reverse DNS SOA, Reverse DNS TXT and Reverse DNS CNAME endpoints.

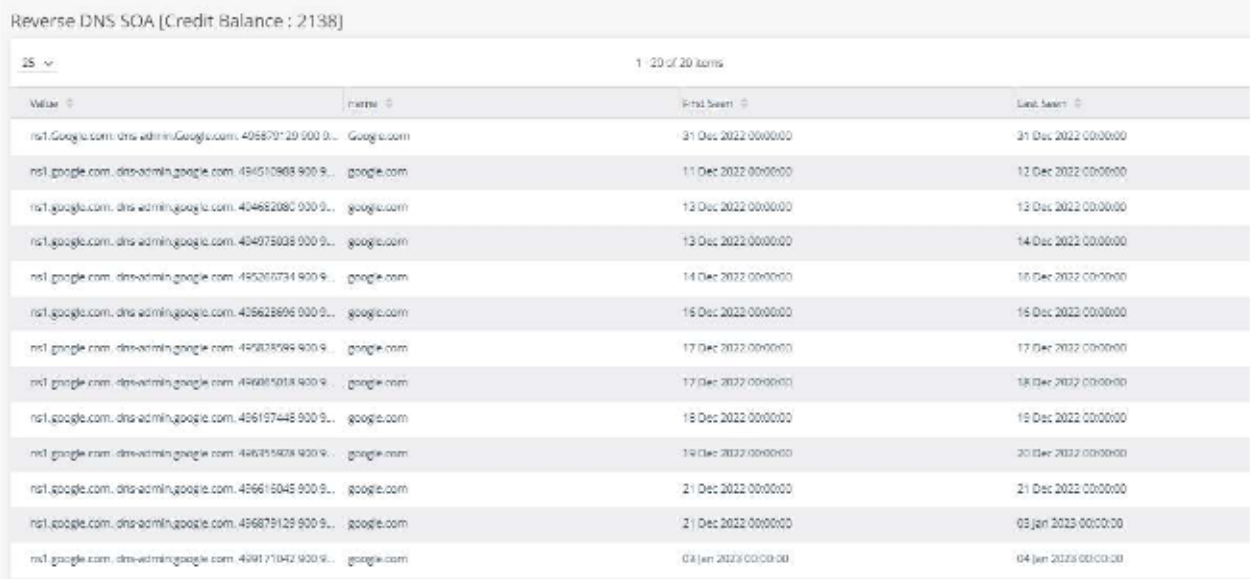
DNS
DNS Lookup

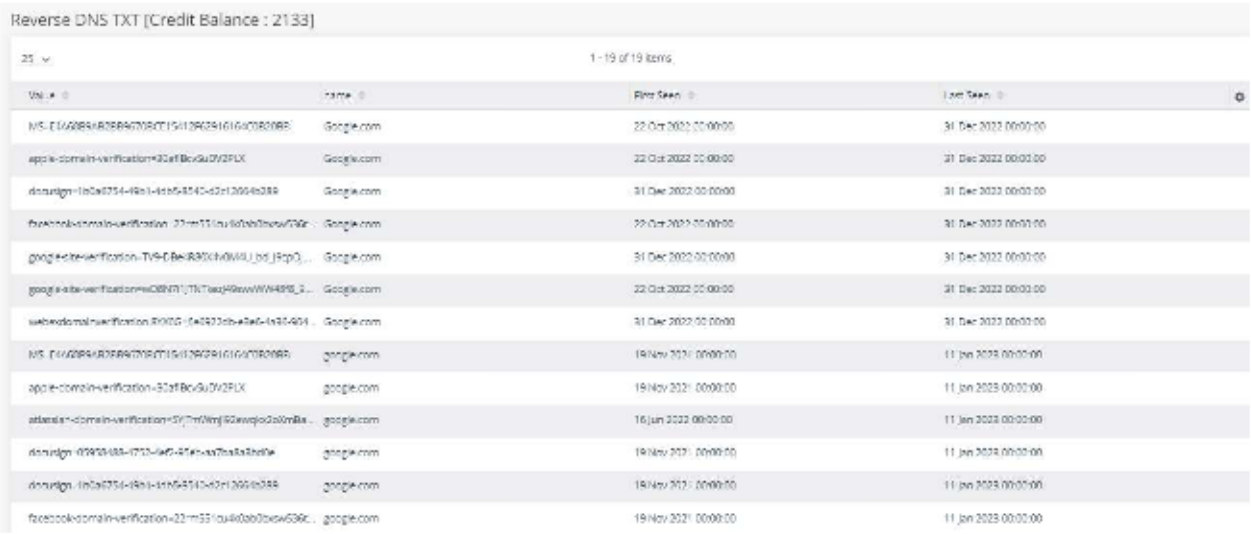
IP Geolocation
Reverse DNS API (SOA)
Reverse DNS API (txt)
Reverse DNS API (CNAME)

Same is shown in the screen shots below.





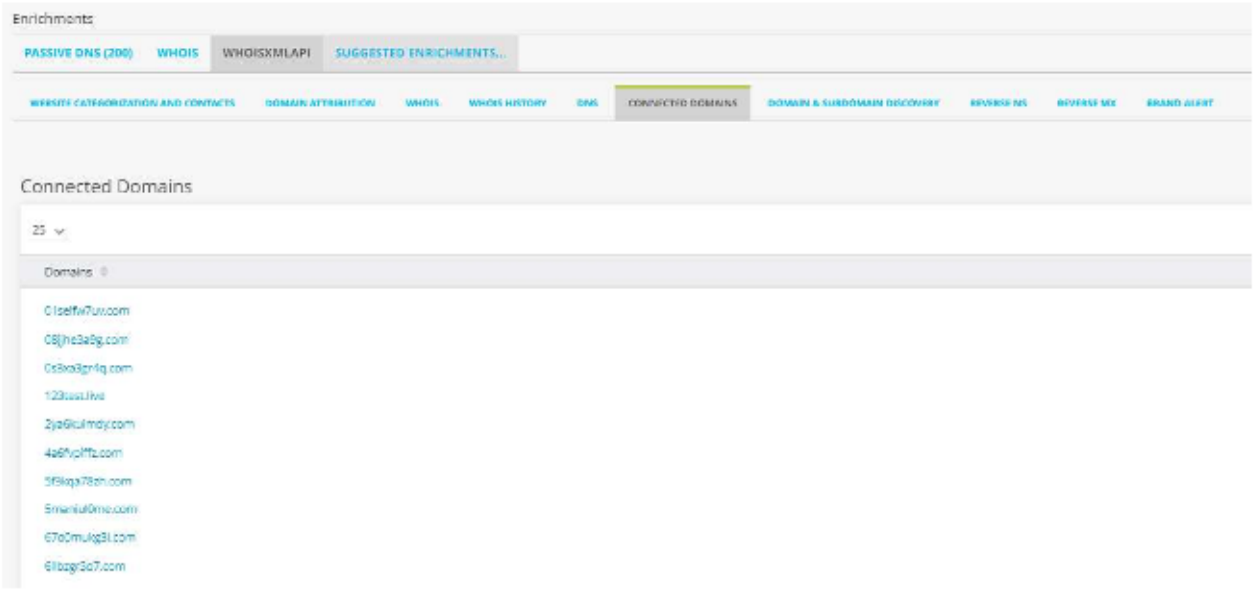


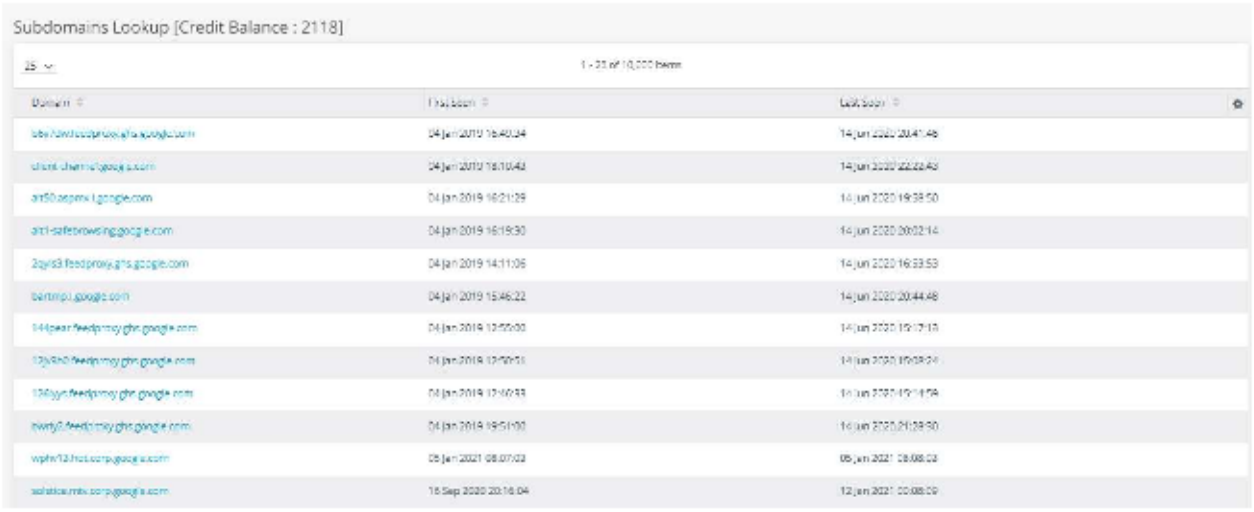


When the user selects **Connected Domains Tab** will be able to perform enrichment for Connected Domains and Subdomains Lookup endpoints.

Connected Domains
Connected Domains
Subdomains Lookup

Same is shown in the screen shots below.

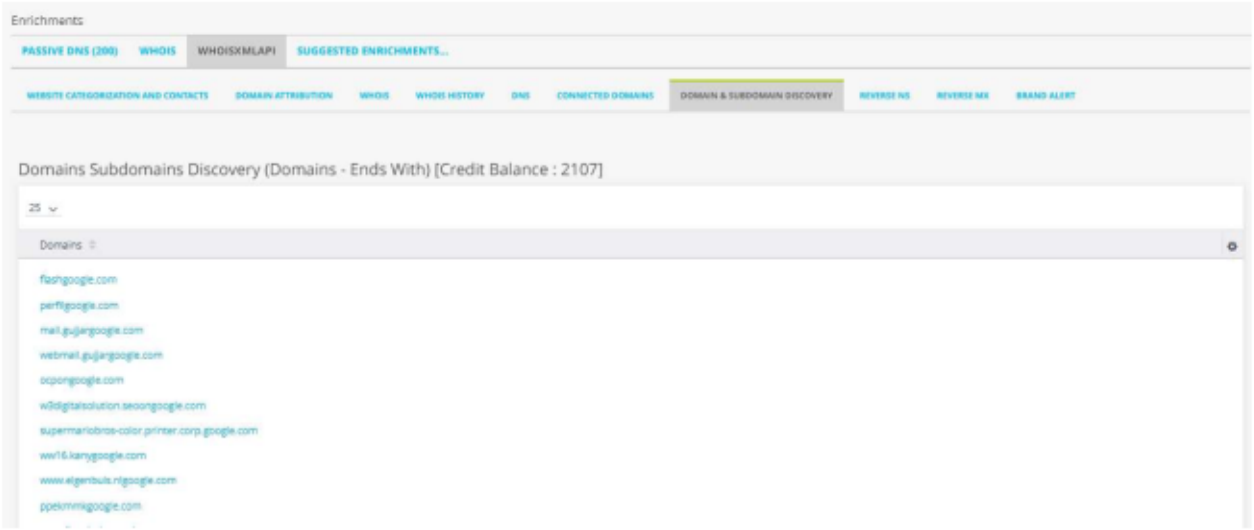




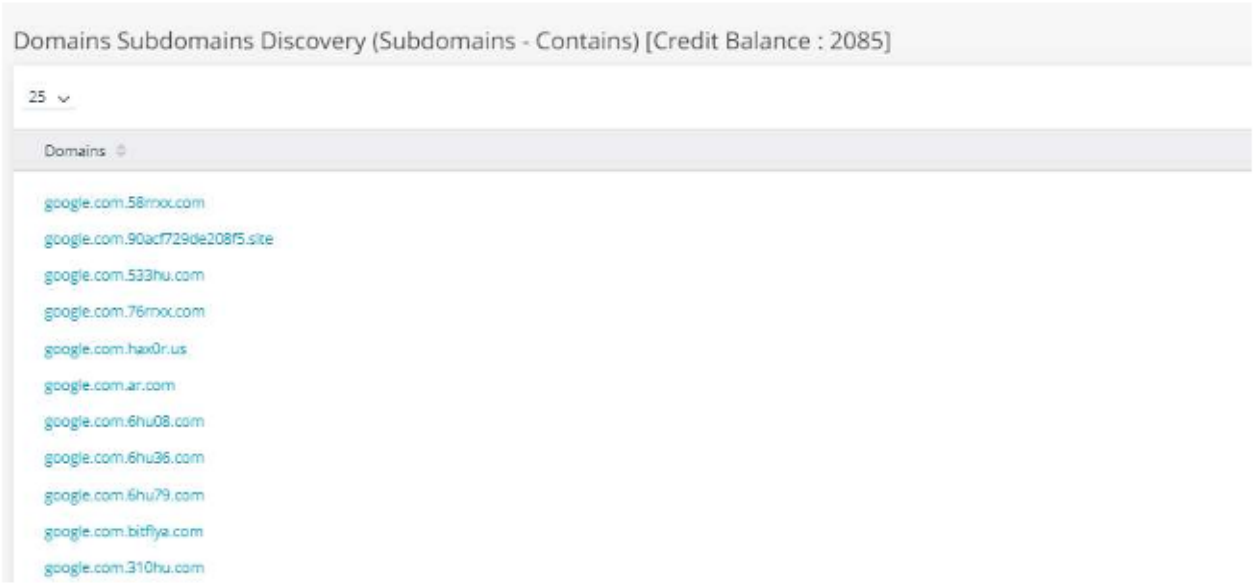
When user selects **Domains & Subdomains Discovery Tab** will be able to perform enrichment for Domains & Subdomains Discovery (Domains - Ends With), Domains & Subdomains Discovery (Domains - Contains) and Domains & Subdomains Discovery (Subdomains - Contains) endpoints.

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 (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
Domains Subdomains Discovery (Domains - Ends With) [Credit Balance : 2107]
25
Domains
flashgoogle.com
perflgoogle.com
mail.gujargoogle.com
webmail.gujargoogle.com
ocpongoogle.com
w3digitalsolution.seoongoogle.com
supermariobros-color.printer.corp.google.com
ww16.kanygoogle.com
www.elgenbuls.ntgoogle.com
ppeimmigoogle.com

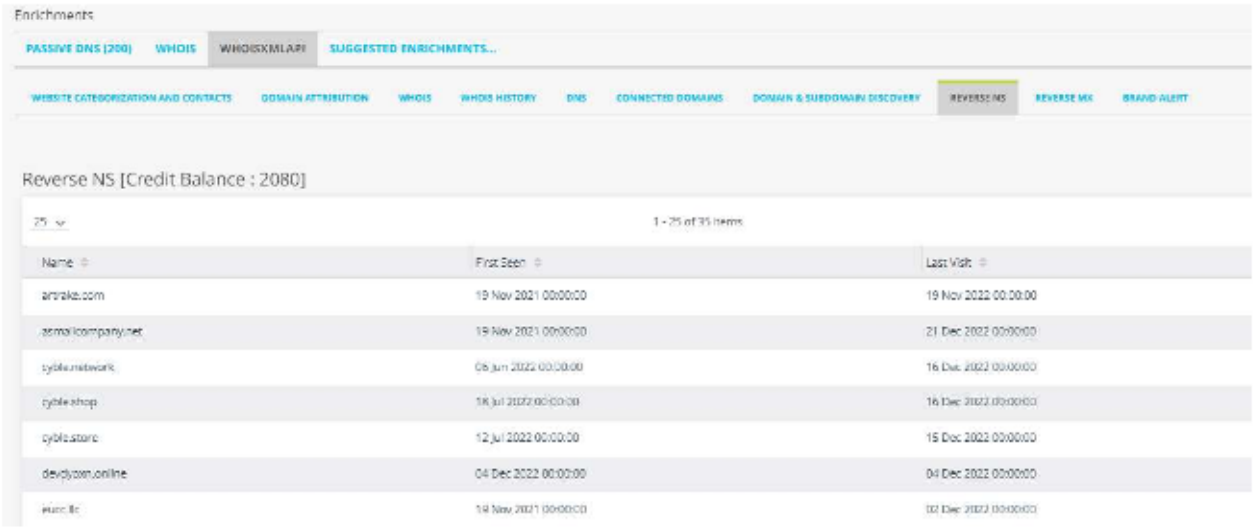

Domains Subdomains Discovery (Domains - Contains) [Credit Balance : 2096]
25
Domains
xn--ocl-mra06nca.com
1f21vug.feedproxy.ghs.google.com
16df1va.feedproxy.ghs.google.com
122rp1o.feedproxy.ghs.google.com
13v6rge.feedproxy.ghs.google.com
138y7gu.feedproxy.ghs.google.com
1dainqw.feedproxy.ghs.google.com
1ew46o8.feedproxy.ghs.google.com
1es3bmd.feedproxy.ghs.google.com
1d2dkj6.feedproxy.ghs.google.com
1d2ghte.feedproxy.ghs.google.com
abxpwio.feedproxy.ghs.google.com


Domains Subdomains Discovery (Subdomains - Contains) [Credit Balance : 2085]
25
Domains
google.com.58rnxx.com
google.com.90acf729de208f5.site
google.com.533hu.com
google.com.76rnxx.com
google.com.hax0r.us
google.com.ar.com
google.com.6hu08.com
google.com.6hu36.com
google.com.6hu79.com
google.com.bitflya.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

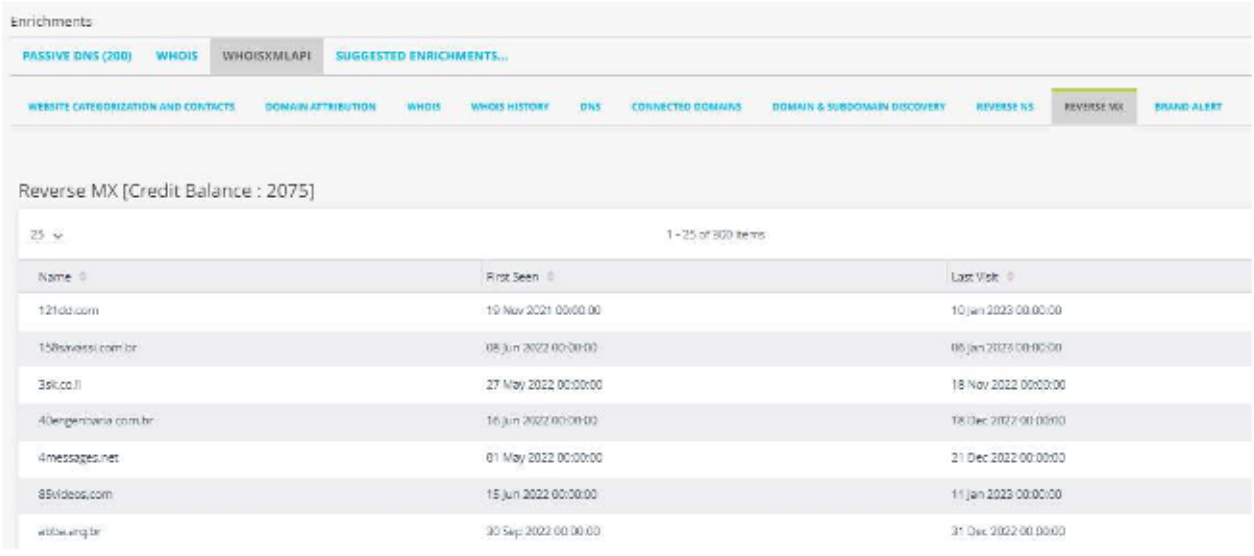
Same is shown in the screen shots below.



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

Reverse MX
Reverse MX

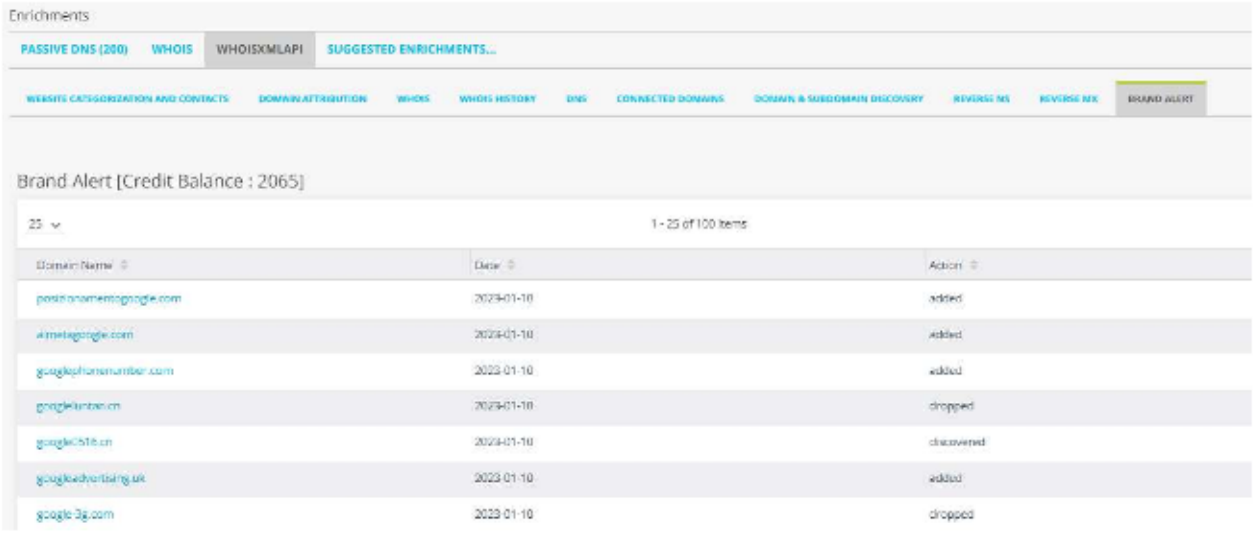
Same is shown in the screen shots below.



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.



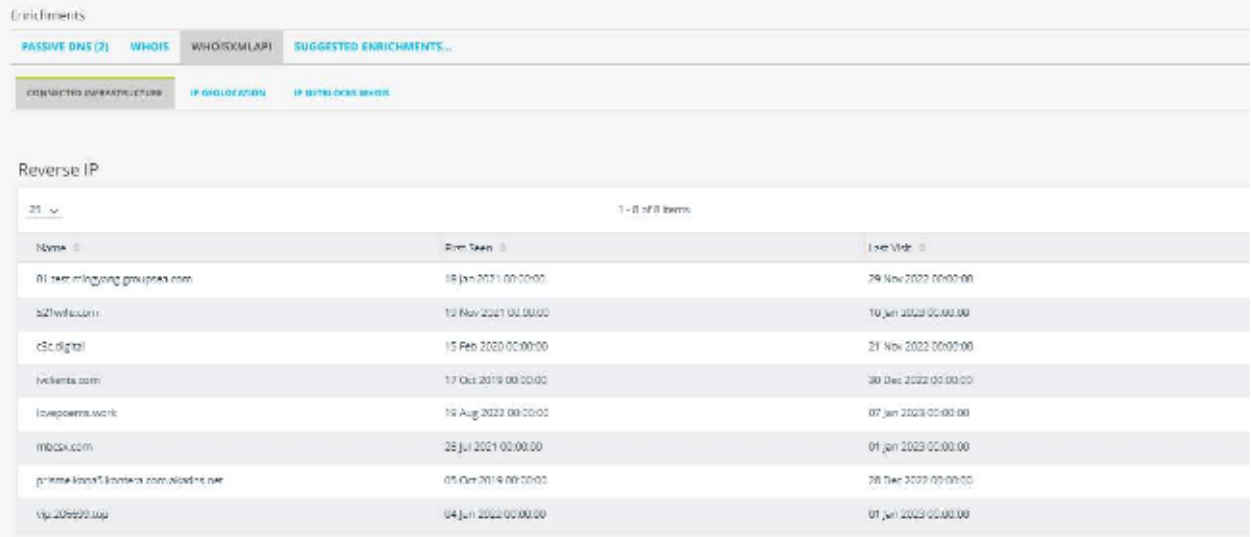
IP Observable Context Enrichment

Categorization of different endpoints is achieved with different tabs.

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

Connected Infrastructure
Reverse IP

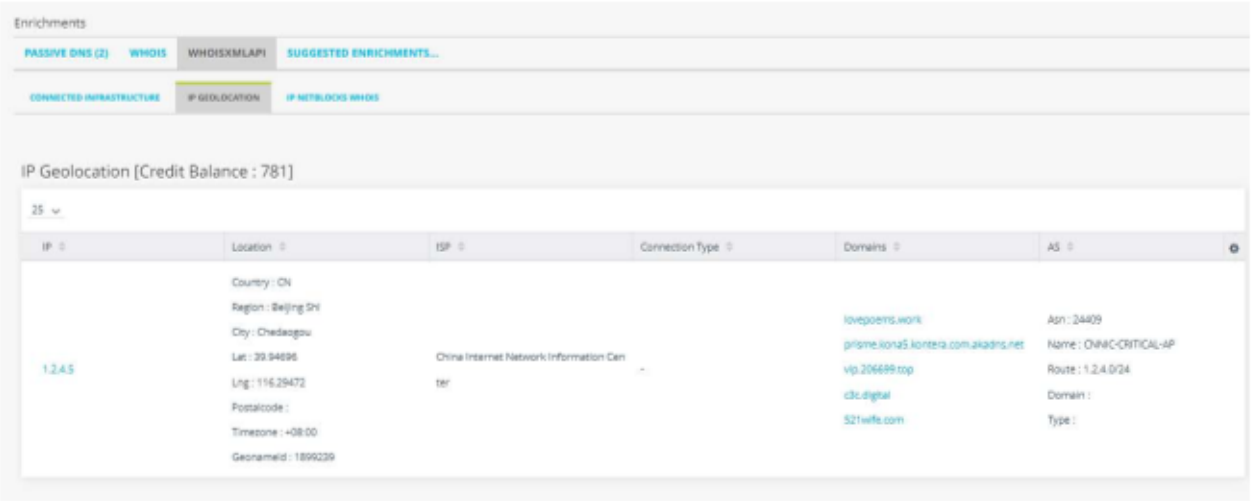
Same is shown in the screen shots below.



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

IP Geolocation
IP Geolocation

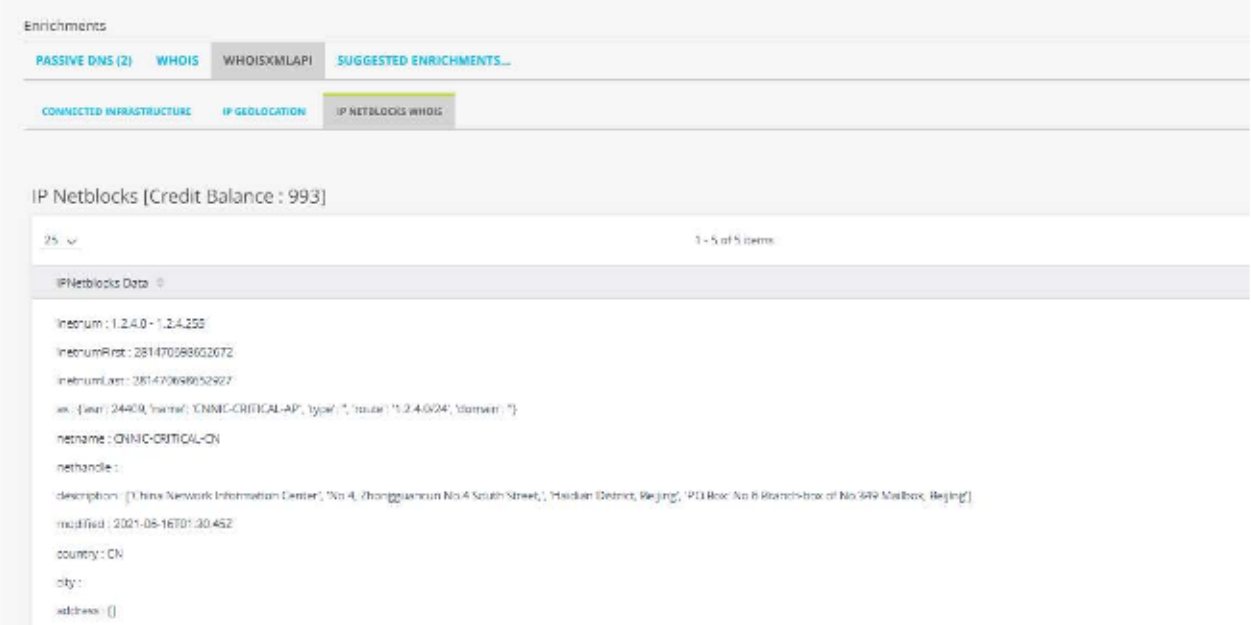
Same is shown in the screen shots below.



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.



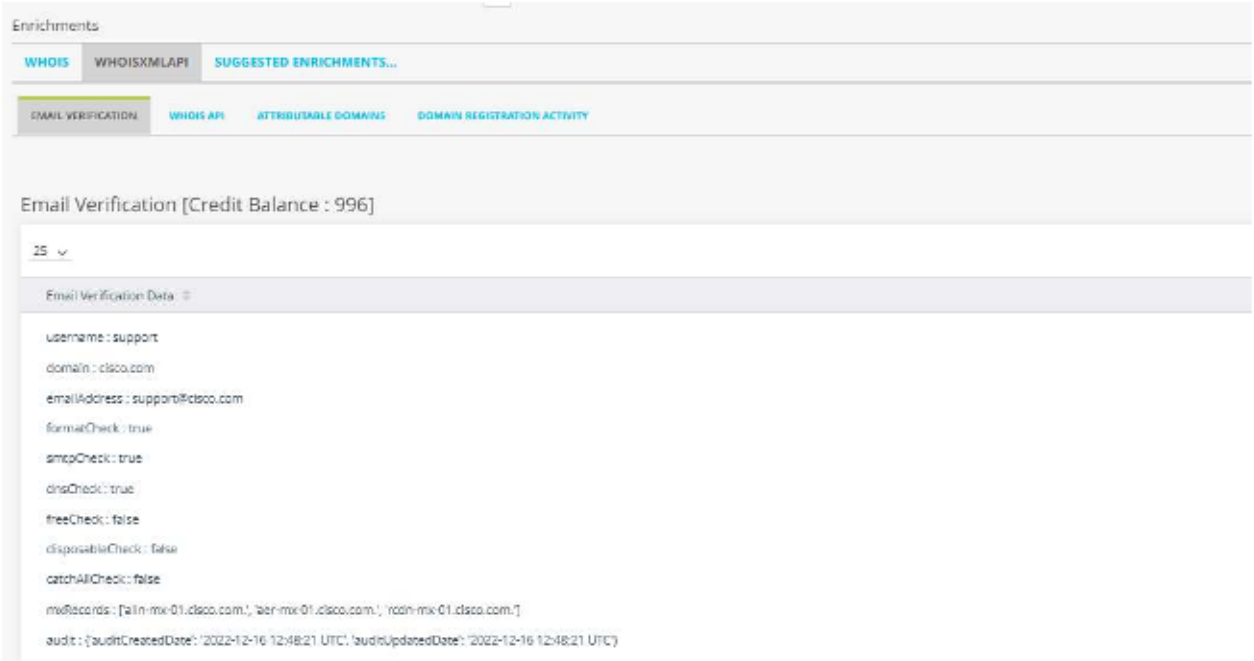
Email Observable Context Enrichment

Categorization of different endpoints is achieved with different tabs.

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

Email Verification
Email Verification

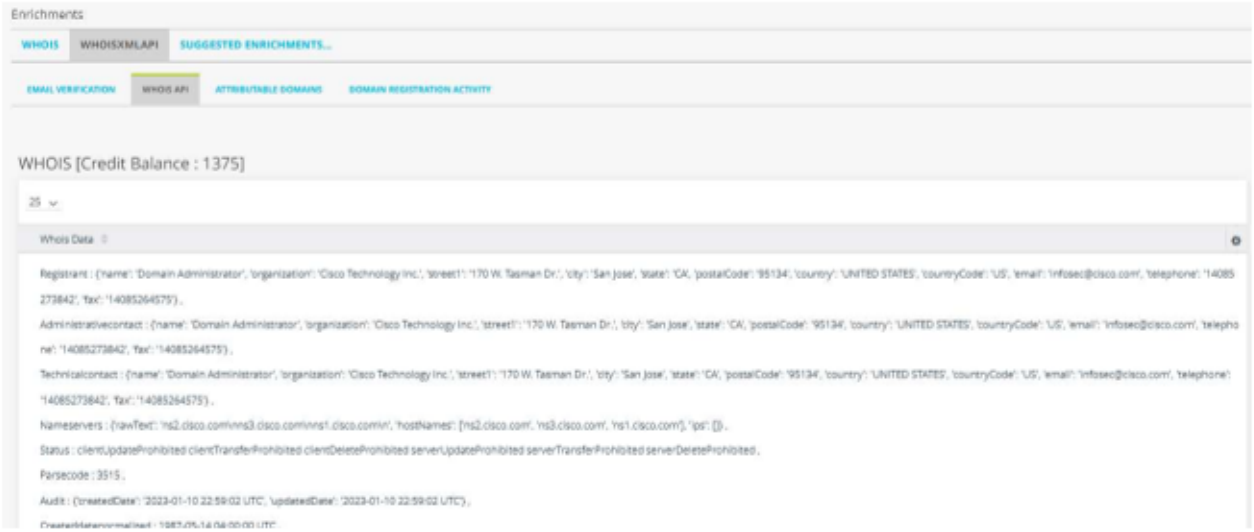
Same is shown in the screen shots below.



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

WHOIS API
WHOIS

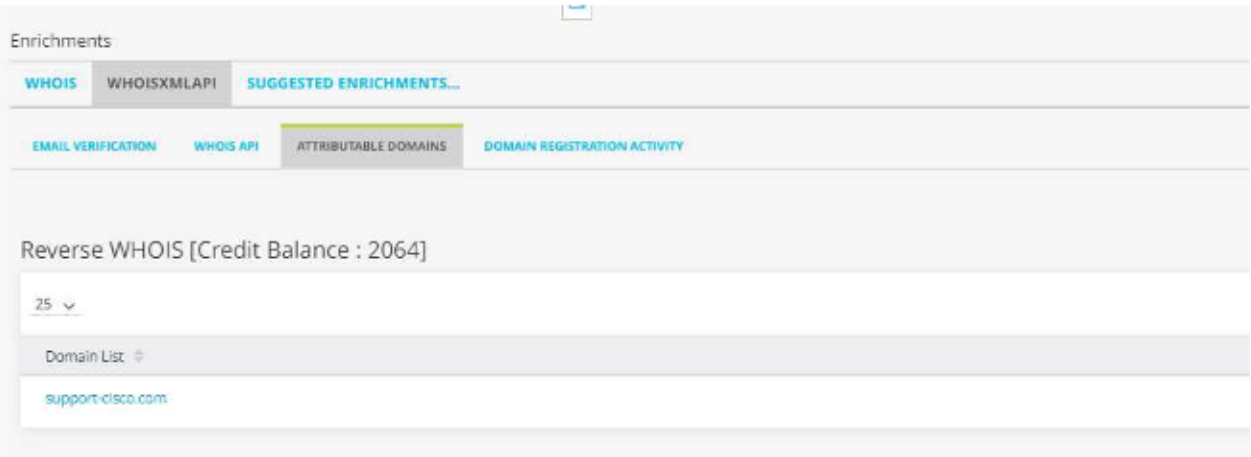
Same is shown in the screen shots below.



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

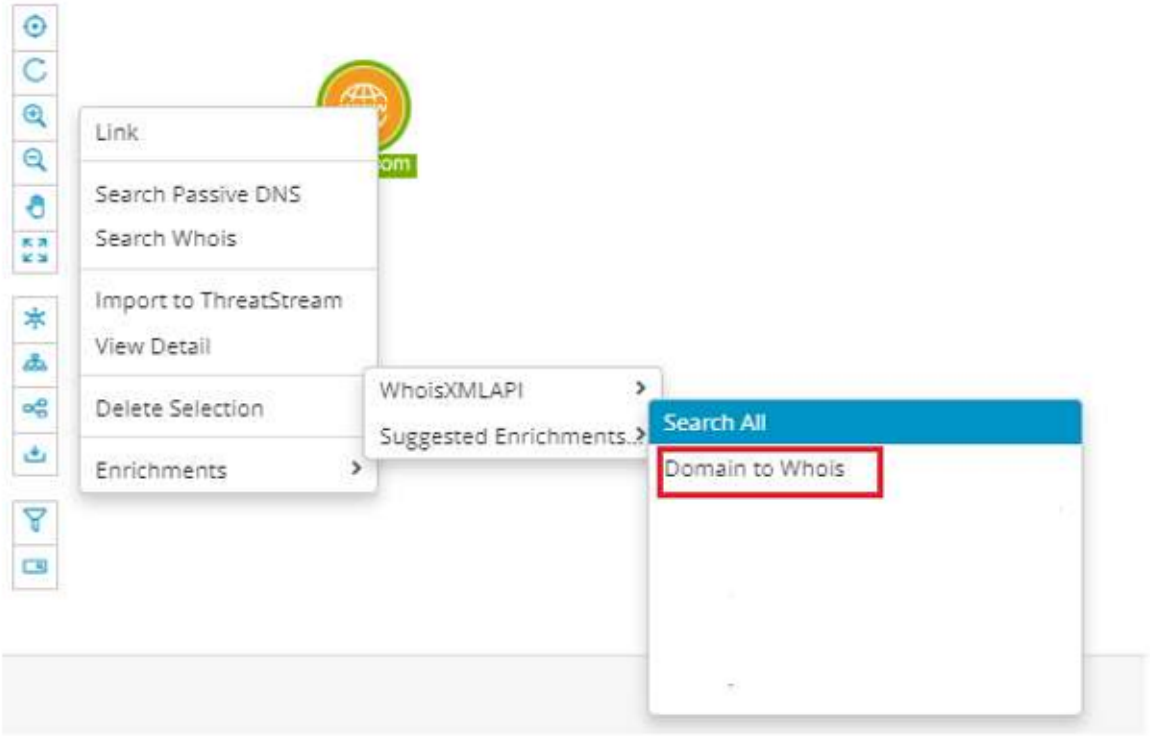
Pivot-Based Enrichments

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.

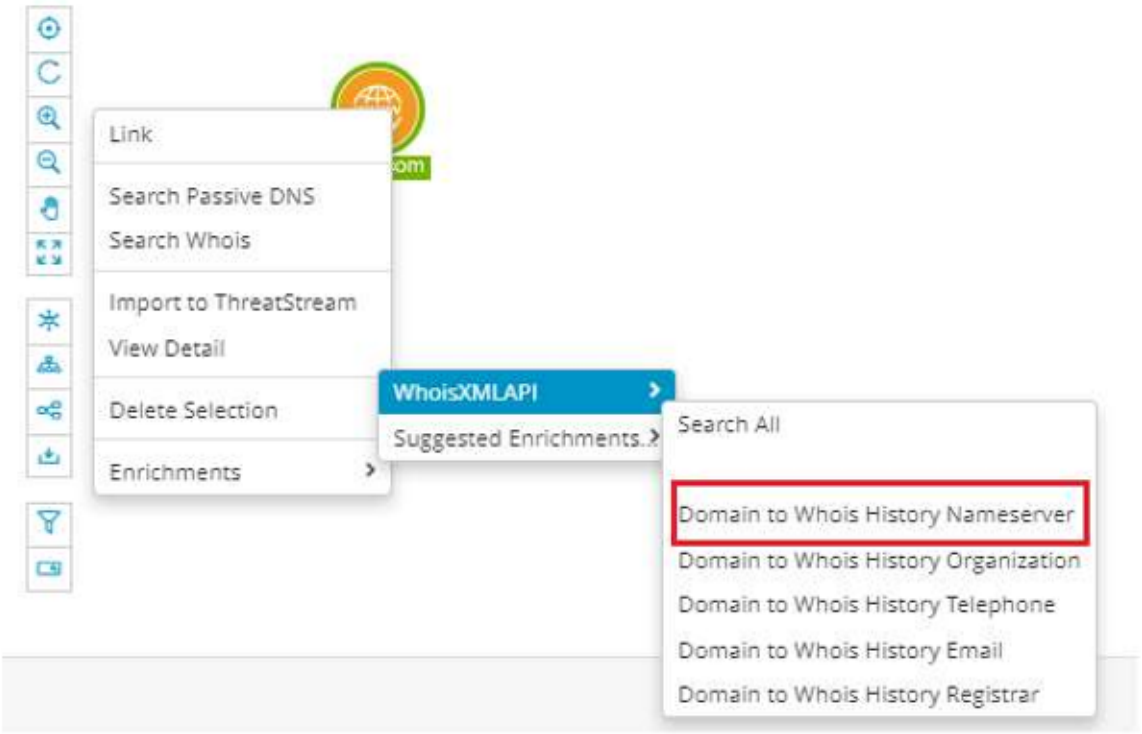
Contact Email
Name Server
Registrar Name
Organization Name
Telephone



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

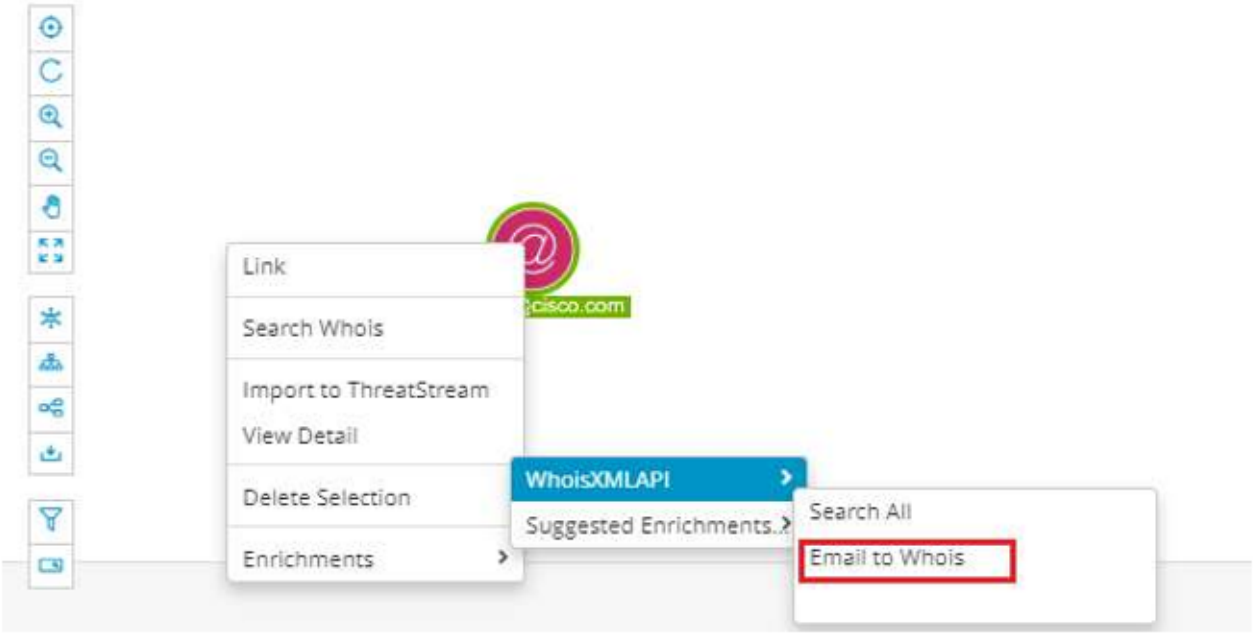
Email
Name Server
Registrar Name
Organization Name
Telephone



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