Validin Platform - User Guide

Version 0.4

Published on 2024-03-25

Prepared by Validin LLC

Table of Contents

Introduction

This document provides an overview of understanding and using Validin's Platform for triage and investigation, threat infrastructure tracking, proactive lookalike domain discovery, and surface area assessment.

Validin is a DNS and public infrastructure intelligence company, leading the way to world-class proactive data & insights. Validin thoroughly maps and indexes the public DNS space regularly to build a uniquely comprehensive mapping & history of global DNS state, as well as dozens of unique insights.

Overview

The Validin platform enables security teams, threat researchers, and threat hunters to search, discover, and explore connections between known and unknown infrastructure. Validin simplifies discovery and research through tooling and interfaces designed around security experts' needs and use cases.

By leveraging Validin's uniquely comprehensive data, we deliver:

- A single source for investigating domain and IP DNS state and history, certificates, reputation, and relationships to other domains and IPs
- Reduced investigation and response time during security incidents
- Discovery of unknown threats to you and your customers
- Seamless pivoting through dozens of domain, IP, hosting, and certificate features
- Proactive identification and monitoring of targeted threats

Purpose of the documentation

This documentation provides first-time users an overview of the Validin platform and guidance on how to leverage the platform to accomplish common workflows.

Scope and Limitations

This documentation covers all major features of the Validin platform. As such, it is intended for distribution to end users within your organization of Validin's web-based UI. Some features may not be available on your plan.

Documentation for system administration and developer guides are out of scope for this document.

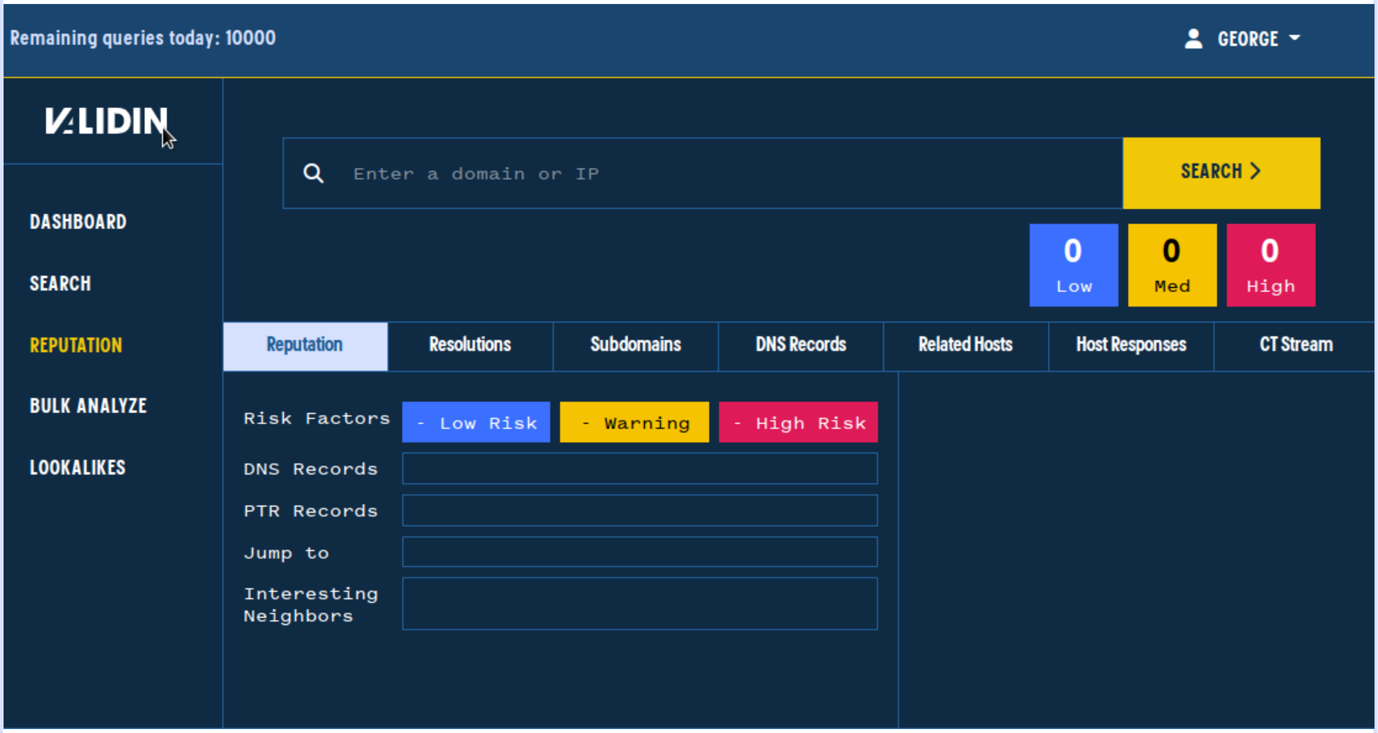
Using the Validin Platform

The Validin platform requires authentication for all core functionality. For help activating your account, please see Managing your account.

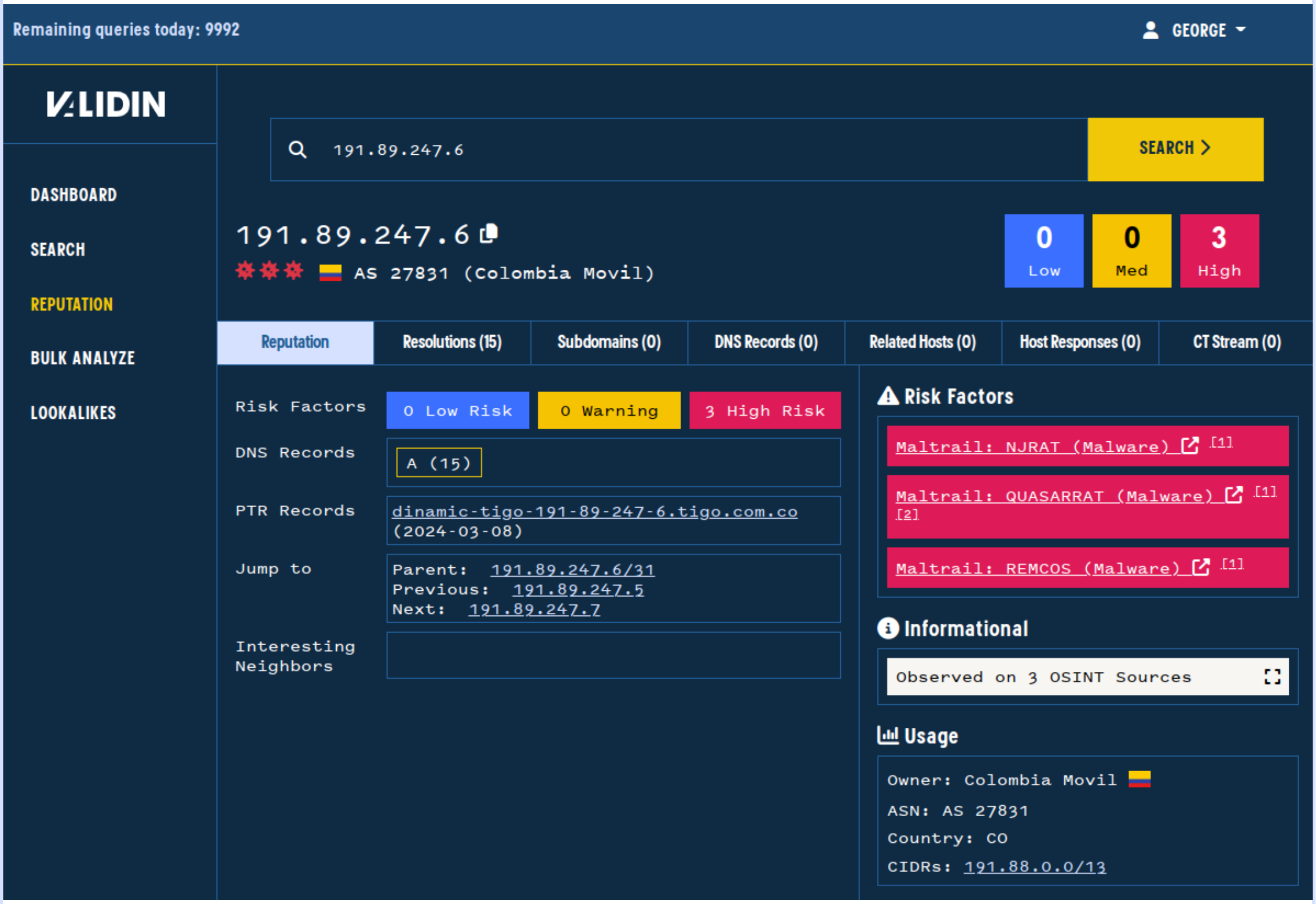
Important note: the examples used in the screenshots below may be malicious and might cause harm if visited directly. Please use caution!

“Reputation” - Domain and IP triage

Visit the “Reputation” page to quickly triage a single domain name, IP address, or CIDR (range of IPs) within the Validin platform. This page provides context about domain names and IP addresses from many data sources that Validin collects and curates. Enter the domain or IP/CIDR that you want to research, then click “Search” or press “enter” on your keyboard to begin the search.



After searching, you will see a page that looks like this:



191.89.247.6

191.89.247.6

AS 27831 (Colombia Movil)

Risk Factors: 0 Low Risk | 0 Warning | 3 High Risk

DNS Records: A (15)

PTR Records: dinamic-tigo-191-89-247-6.tigo.com.co (2024-03-08)

Jump to:
Parent: 191.89.247.6/31
Previous: 191.89.247.5
Next: 191.89.247.7

Interesting Neighbors

Risk Factors

Maltrail: NJRAT (Malware) [1]

Maltrail: QUASARRAT (Malware) [1] [2]

Maltrail: REMCOS (Malware) [1]

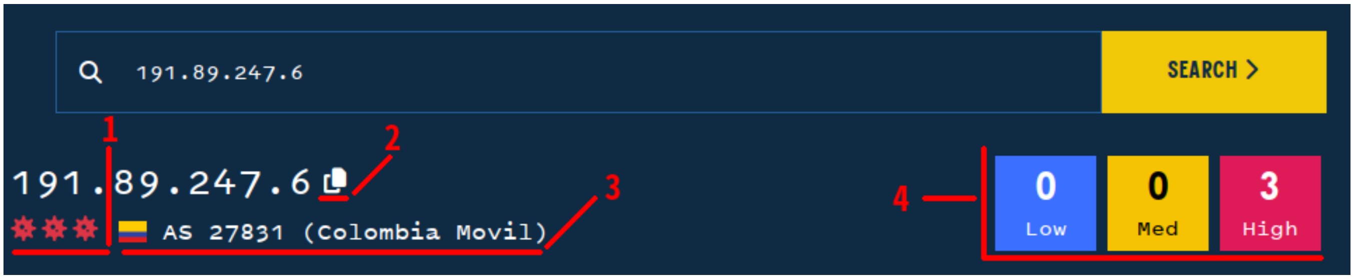
Informational

Observed on 3 OSINT Sources

Usage

Owner: Colombia Movil
ASN: AS 27831
Country: CO
CIDRs: 191.88.0.0/13

Validin provides a summary of the domain names or IP address that you search at the top:



191.89.247.6

191.89.247.6

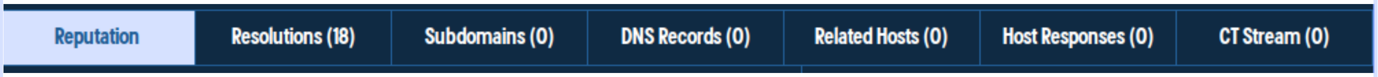
AS 27831 (Colombia Movil)

Description:

1. Notable attributes are highlighted here. Mouse over the icon to see the reason as a tool tip.
   a. A red “virus” symbol indicates that the IP or domain is on a named malware list.
   b. A red “bug” symbol indicates that the IP or domain is on a named “malicious” list.
   c. A yellow “triangle” symbol indicates that the domain or IP shows up on a “suspicious” list.
   d. A blue “flame” symbol indicates that the domain or IP shows up on a popularity list.
2. The defanged (exercise caution) indicator may be copied to your clipboard for rapid copy/paste to custom block lists or further research.

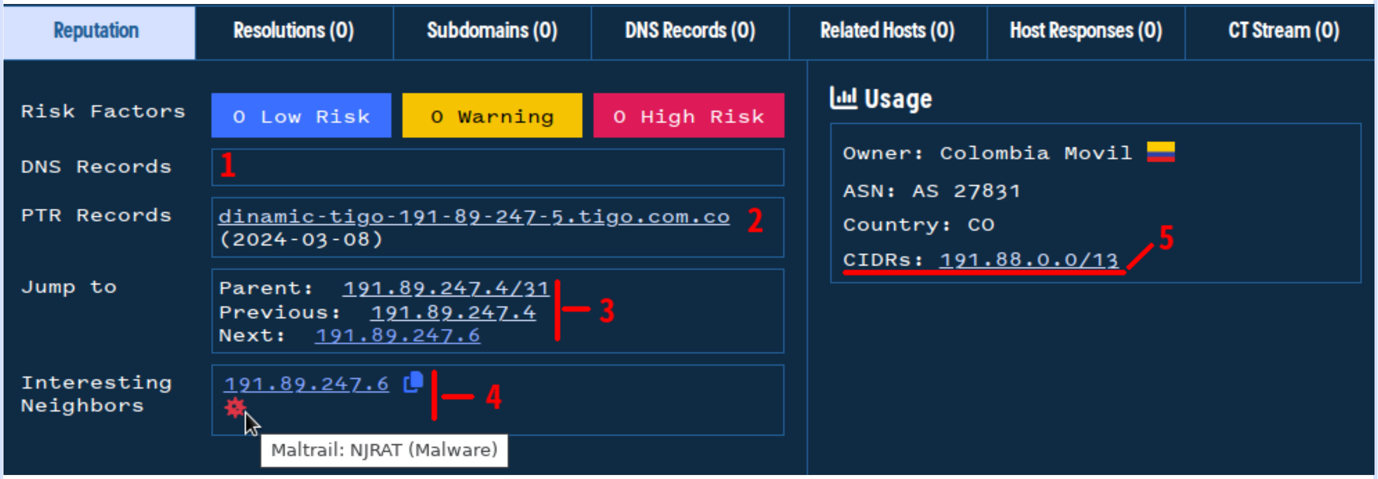
3. For IP addresses only: the parent Autonomous System (AS) number, country, and owner name is shown.
4. A summary of reputation risk factors are shown here.

The reputation page presents context about domain names and IP addresses within tabs, described below.



Reputation

The reputation tab shows a more detailed summary of the domain or IP being searched.



Risk Factors: 0 Low Risk | 0 Warning | 0 High Risk

DNS Records:

PTR Records: dinamic-tigo-191-89-247-5.tigo.com.co (2024-03-08)

Jump to:
Parent: 191.89.247.4/31
Previous: 191.89.247.4
Next: 191.89.247.6

Interesting Neighbors: 191.89.247.6

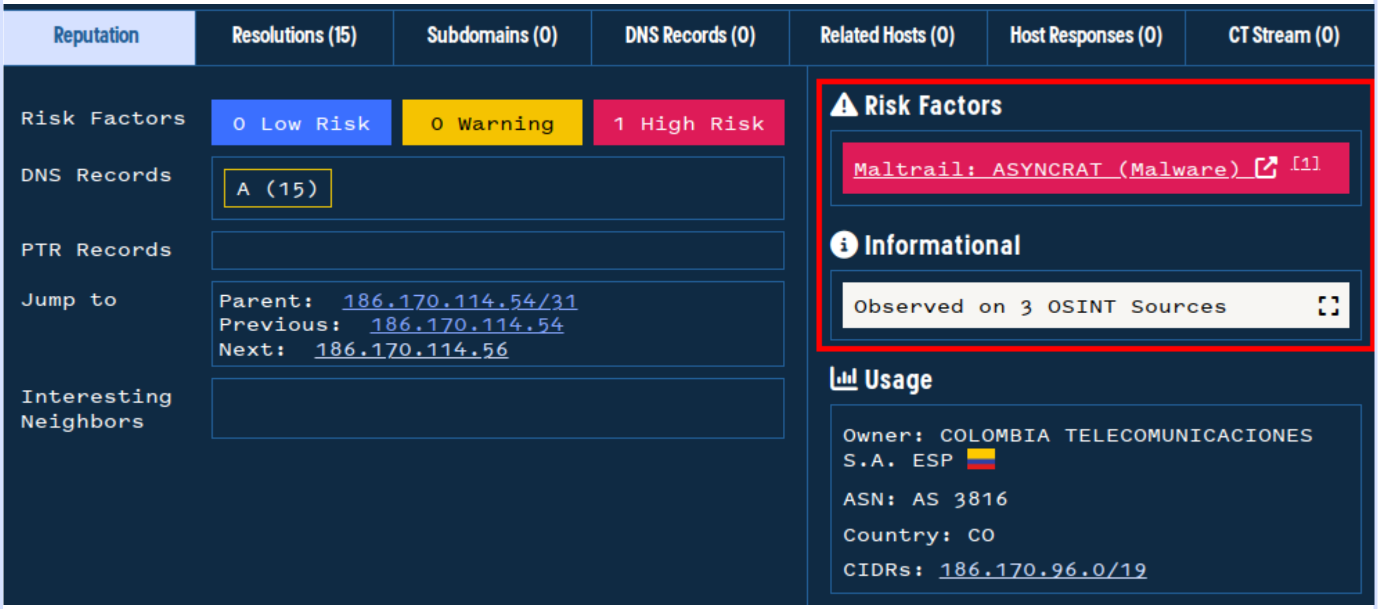
Maltrail: NJRAT (Malware)

Owner: Colombia Movil
ASN: AS 27831
Country: CO
CIDRs: 191.88.0.0/13

Description:

1. A summary of DNS record types and counts that have been associated with the domain or IP.
2. The PTR record for the IP (if any) or IPs that have the domain as the PTR record (if any).
3. Quick links to neighboring IPs and CIDRs (for IPs) and to labels at different depths (for domains).
4. For IPs and CIDRs: neighboring IPs that are interesting in some way, either through popularity or through being associated with known malicious activity. Mouse over the icon to see the reason as a tool tip.
5. For IPs and CIDRs, the parent CIDR is provided as a quick search link.

For domains and IPs with additional OSINT context, additional “Risk Factors” and “Informational” sections are added on the right side of the page.



Reputation | Resolutions (15) | Subdomains (0) | DNS Records (0) | Related Hosts (0) | Host Responses (0) | CT Stream (0)

Risk Factors: 0 Low Risk | 0 Warning | 1 High Risk

DNS Records: A (15)

PTR Records

Jump to:
Parent: 186.170.114.54/31
Previous: 186.170.114.54
Next: 186.170.114.56

Interesting Neighbors

Risk Factors

Maltrail: ASYNCRAT (Malware) [1]

Informational

Observed on 3 OSINT Sources

Usage

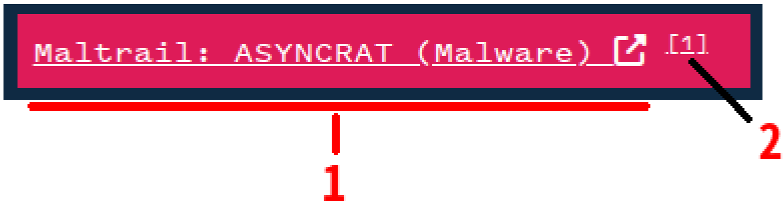
Owner: COLOMBIA TELECOMUNICACIONES S.A. ESP

ASN: AS 3816

Country: CO

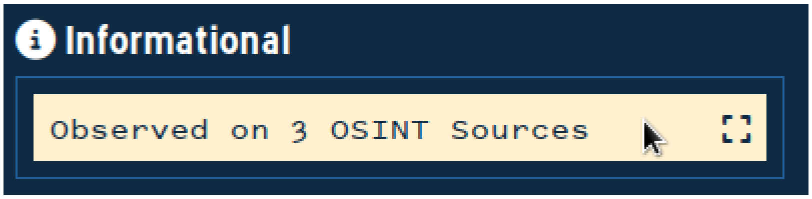
CIDRs: 186.170.96.0/19

Risk factors may be positive or negative. For risk factors associated with known, named malware families or malicious actors, the actor name, OSINT source (2), and OSINT indicator collection (1) are provided as direct, external links. These links provide context for analysts and researchers to continue investigation and remediation efforts.



Maltrail: ASYNCRAT (Malware) [1]

Clicking on the "Observed on N OSINT Sources" box will open a slide-out from the right that will provide additional block lists, popularity lists, and other context to assist with indicator triage:

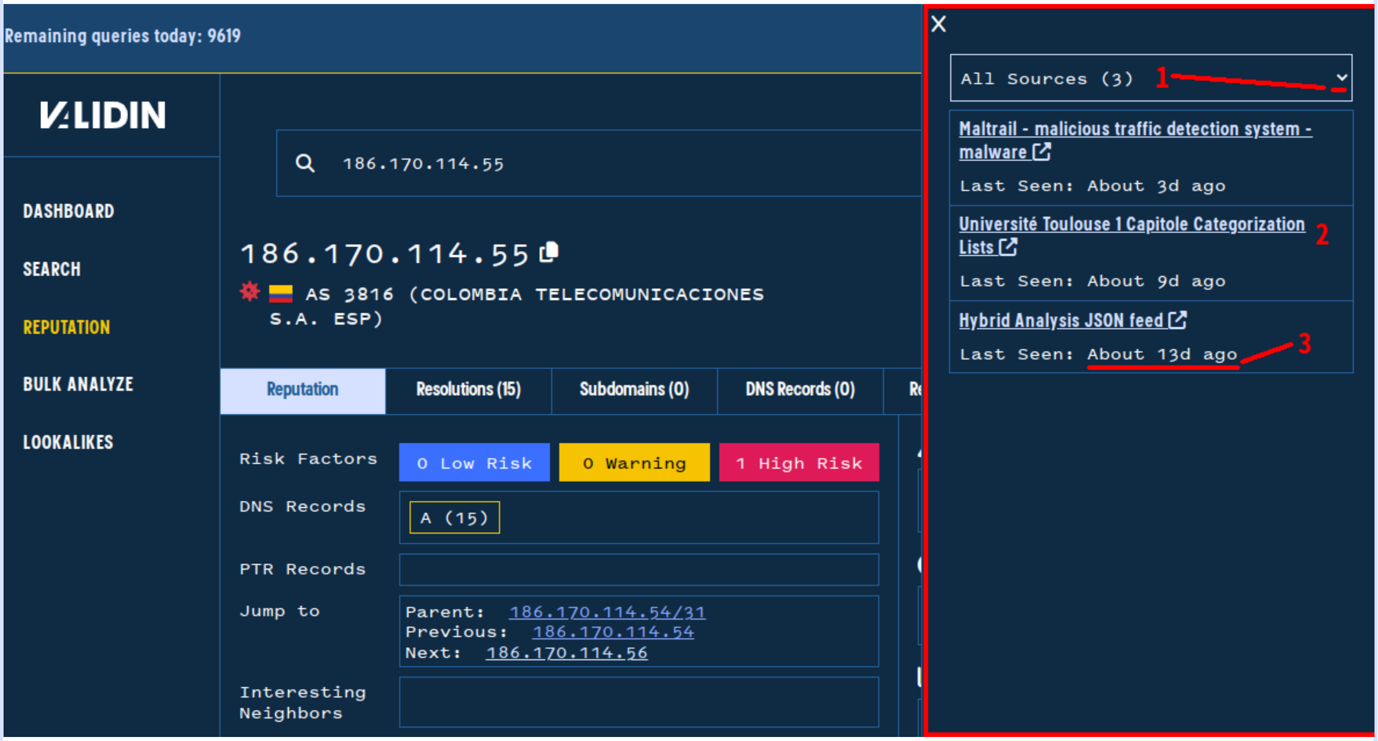


Informational

Observed on 3 OSINT Sources

The slide-out provides:

1. Filters for the type(s) of sources on which the indicators were observed.
2. Direct links to the OSINT sources.
3. The age of the sighting on the linked indicator list.



186.170.114.55

186.170.114.55

AS 3816 (COLOMBIA TELECOMUNICACIONES S.A. ESP)

Risk Factors	0 Low Risk · 0 Warning · 1 High Risk
DNS Records	A (15)
PTR Records	
Jump to	Parent: 186.170.114.54/31 Previous: 186.170.114.54 Next: 186.170.114.56
Interesting Neighbors	

All Sources (3)

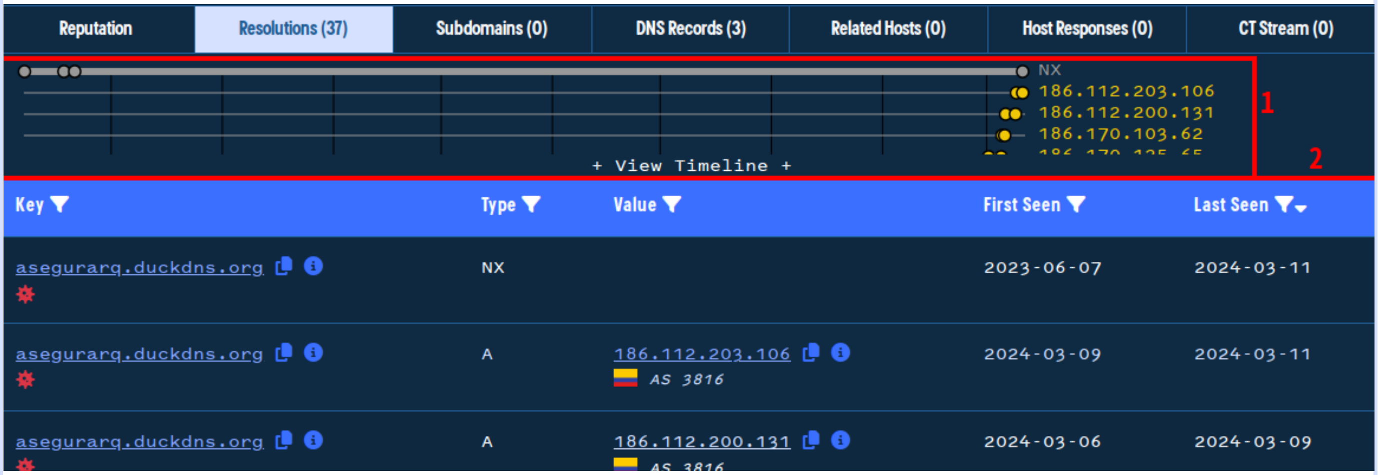
Maltrail - malicious traffic detection system - malware
Last Seen: About 3d ago

Université Toulouse 1 Capitole Categorization Lists
Last Seen: About 9d ago

Hybrid Analysis JSON feed
Last Seen: About 13d ago

Resolutions

The “Resolutions” tab shows A, AAAA, and NS records for a domain name, and A and AAAA answer histories (the domains that used the given IP as an answer) for IP addresses. For domain names, if any of the queries to A, AAAA, or NS returned NXDomain (“NX”) instead of “no answer,” the resolutions page will show “NX” history.

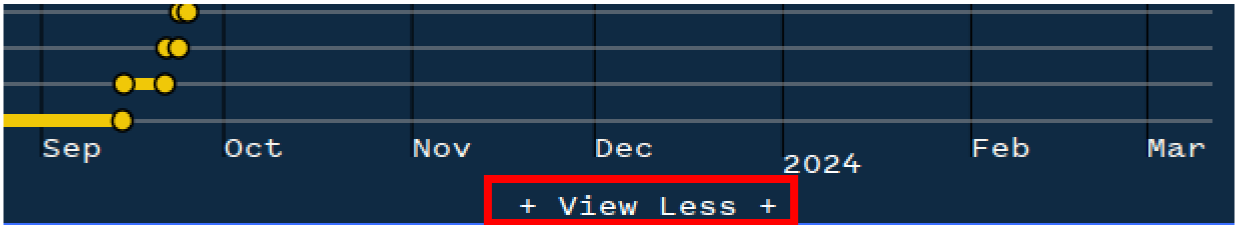


Key	Type	Value	First Seen	Last Seen
asegurarq.duckdns.org	NX		2023-06-07	2024-03-11
asegurarq.duckdns.org	A	186.112.203.106 AS 3816	2024-03-09	2024-03-11
asegurarq.duckdns.org	A	186.112.200.131 AS 3816	2024-03-06	2024-03-09

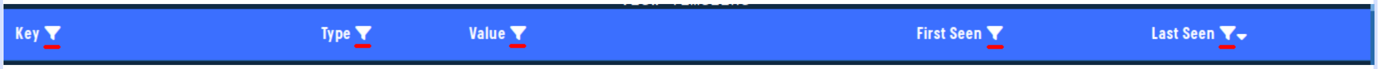
The “Resolutions” tab is divided into two sections:

1. A visual timeline view
2. A tabular view

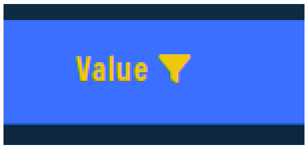
Expand and collapse the timeline view by clicking “View Timeline” and “View Less.”



Each header in the table may be sorted, and some may be additionally filtered, by clicking on the filter icon in a table header:

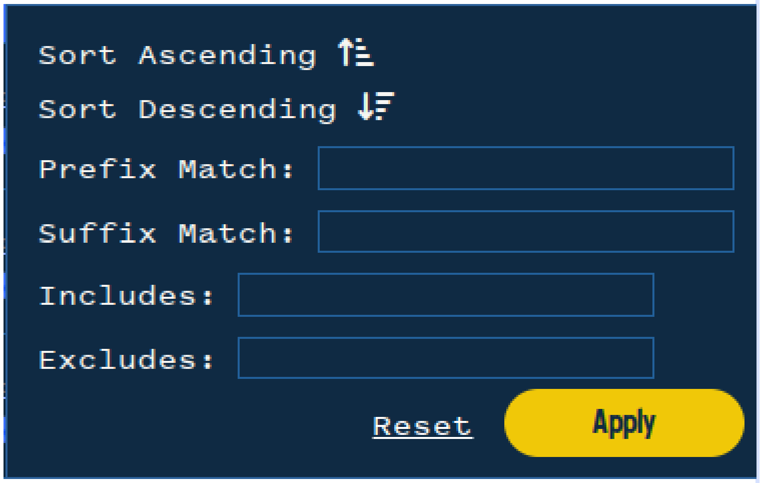


The up and down arrows indicate the sort direction. The table header and filter icons will turn yellow when there's an active search filter:



Keys and values support search by:

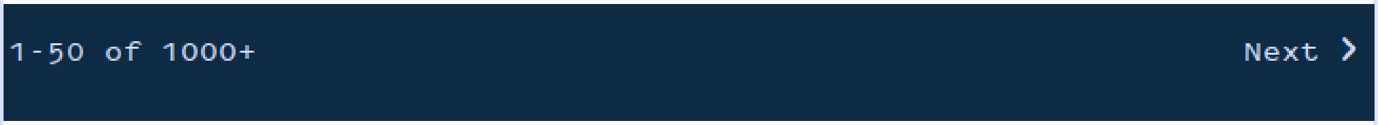
- Prefix Match (e.g., "goo" would match "google.com" but not "play.google.com")
- Suffix Match (e.g., "google" would match "via.google" but not "google.com")
- Includes: any part of the key/value text contains the search string
- Excludes: no part of the key/value text may contain the search string



Date filters have the ability to filter by first and last seen dates. The specific definitions are:

- ***Not Before***: Do not show any results that include any observations before this date.
- ***Not After***: Do not show any results that include any observations *after* this date.

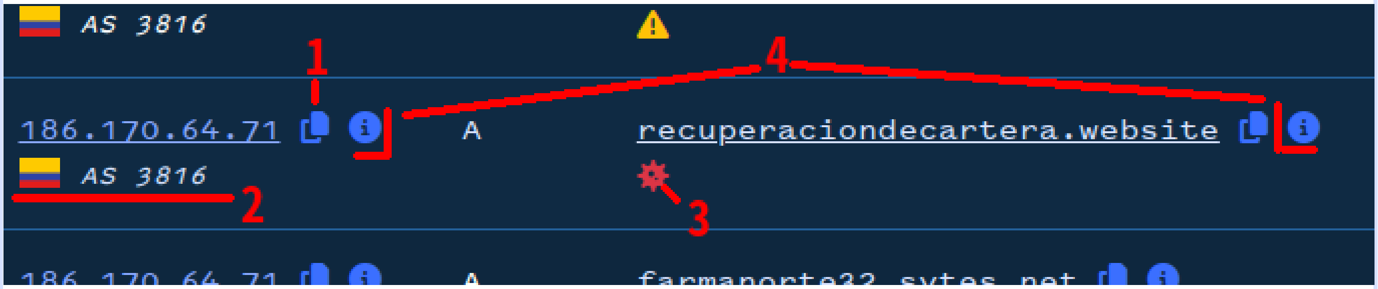
Page controls are at the bottom of the table:



Within the table view, you can:

1. Copy **defanged** (exercise caution) indicators
2. View the country flag and AS number for a given IP
3. View notable attributes about the domain or IP key or value (e.g., malicious or popular)

4. View quick context about popularity or maliciousness, view AS information, and open slide-outs that contain additional context.



AS 3816

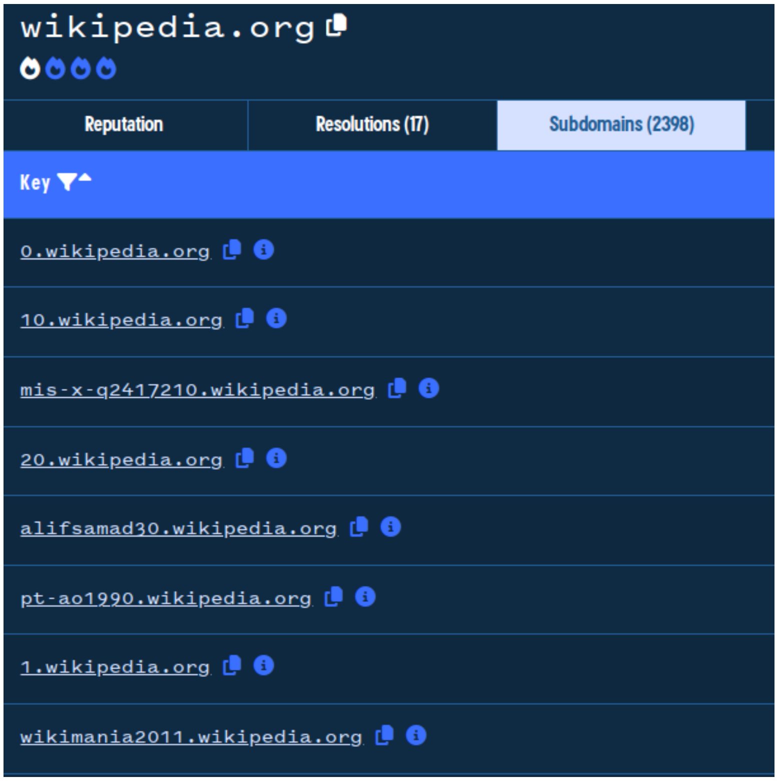
186.170.64.71 A recuperaciondecartera.website

AS 3816

186.170.64.71 A farmanorte32.sytes.net

You can also click any indicator that appears as a link on the page. Clicking that indicator will initiate a pivot/search for details about that indicator.

Subdomains



wikipedia.org

0.wikipedia.org

10.wikipedia.org

mis-x-q2417210.wikipedia.org

20.wikipedia.org

alifsamad30.wikipedia.org

pt-ao1990.wikipedia.org

1.wikipedia.org

wikimania2011.wikipedia.org

The subdomains tab enumerates all subdomains tracked by Validin for a domain at any depth except for ETLD (effective top-level domain). Note that a domain does not need to resolve, or to have ever resolved, for Validin to track it.

Subdomains may be filtered by prefix match, suffix match, “contains” or “excludes.”

DNS Records

The “DNS Records” tab shows the SOA, TXT, MX, SRV, HTTPS, CAA, and CNAME record history for a domain. Each of these records has at least one reverse-indexed field to enable searching for other domains that use the same full or partial answer. If the given domain or IP is an answer for the search key, those associations will be displayed in this tab as well.

Related Hosts

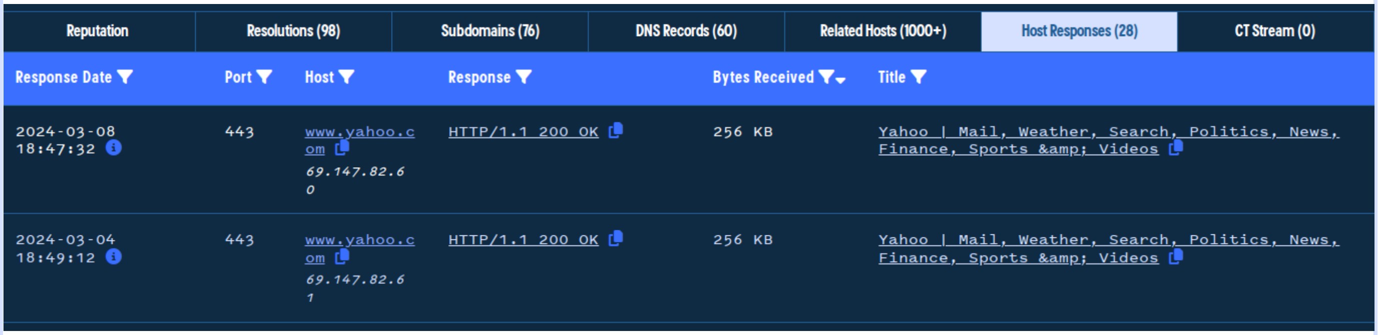
The “Related Hosts” tab shows domains and IPs that are associated with each other through non-DNS means:

- HTTP headers
- HTTPS certificates
- JavaScript links

- CSS links
- Link tags
- Iframes

Host Responses

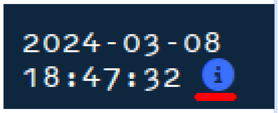
Validin periodically queries the home page (“/”) of every domain name in our database that resolves to an IPv4 and records the answer. Additionally, Validin periodically attempts HTTP and HTTPS requests to every routable IPv4 address and records the responses of successful connections. These answers are shown in the “Host Responses” tab.



Response Date	Port	Host	Response	Bytes Received	Title
2024-03-08 18:47:32	443	www.yahoo.com 69.147.82.60	HTTP/1.1 200 OK	256 KB	Yahoo | Mail, Weather, Search, Politics, News, Finance, Sports &amp; Videos
2024-03-04 18:49:12	443	www.yahoo.com 69.147.82.61	HTTP/1.1 200 OK	256 KB	Yahoo | Mail, Weather, Search, Politics, News, Finance, Sports &amp; Videos

The host responses summarize:

- The exact time of the response
- The port used to make the connection
- The host header and IP address to which the response was made
- The HTTP response line
- The number of bytes processed from the server
- The title tag parsed from the HTML, if any


2024-03-08 18:47:32

Clicking on the “info” button by the response date will open a slideout with additional details about the response:

- Response banner - the entire HTTP header/response
- Certificate details (HTTPS requests only), including:
  - Fingerprint
  - Issuer
  - Valid dates
  - Certificate domains
- HTTP External links from HTML content, including:
  - Links from <meta> tags
  - Links from <link> tags
  - Links from <script> tags
  - Links from <a> tags
  - Links from <iframe> tags
- Meta tags extracted from the HTML

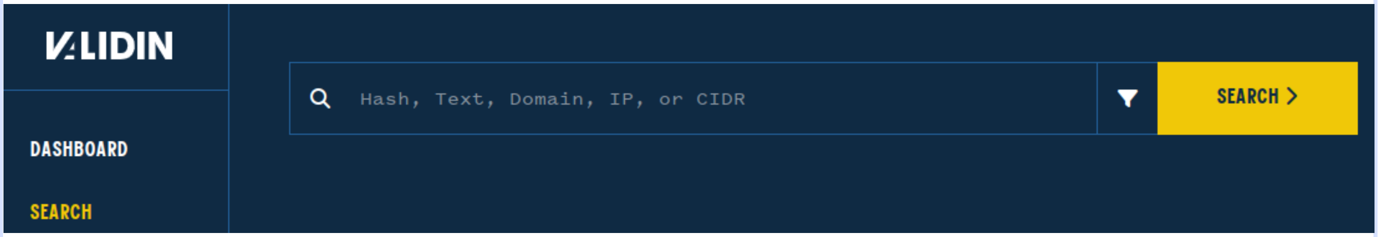
Any pivotable fields in these responses will show up as links. Clicking the link will find any other domains or IPs that had the same feature value (e.g., certificate fingerprint) in one of its responses.

CT Stream

The “CT Stream” tab shows certificates observed in the Certificate Transparency Pre-cert log. Clicking on the fingerprint ID of the certificate opens a slide-out that summarizes key certificate features, like other domains in the certificate, valid dates, and the issuer.

“Search” - Advanced name and feature searching

The “Search” page enables more precise, focused search capabilities by providing the ability to filter and search for non-domain and non-IP values that can be used to discover relationships between domains and IPs.



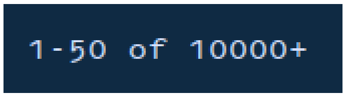
Search Filters

Validin supports the following search filters:

- Category (e.g., “A”, “AAAA”)
- IPv4 answer filter
- IPv6 answer filter
- Domain answer filter
- Time range filter

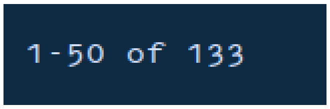
Answer filters apply to the “values” of the answers from the search query and can greatly reduce the time and effort required to filter results by substantially narrowing the scope of answers returned.

As an example, consider the domain “ns-cloud-a1.googledomains.com”. This domain is a very popular name server (NS) value, so even with a result limit of 10,000, we cannot retrieve all of the results.



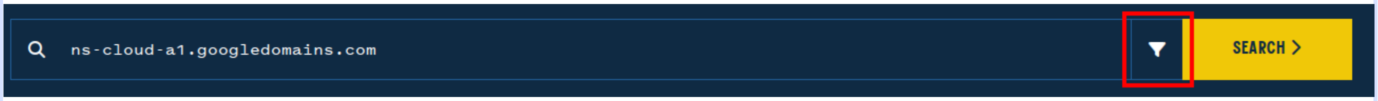
1-50 of 10000+

However, if we’re interested in a particular domain that ends with “.click” and use a domain answer filter for the TLD “click”, we’re able to get a much more manageable result set:



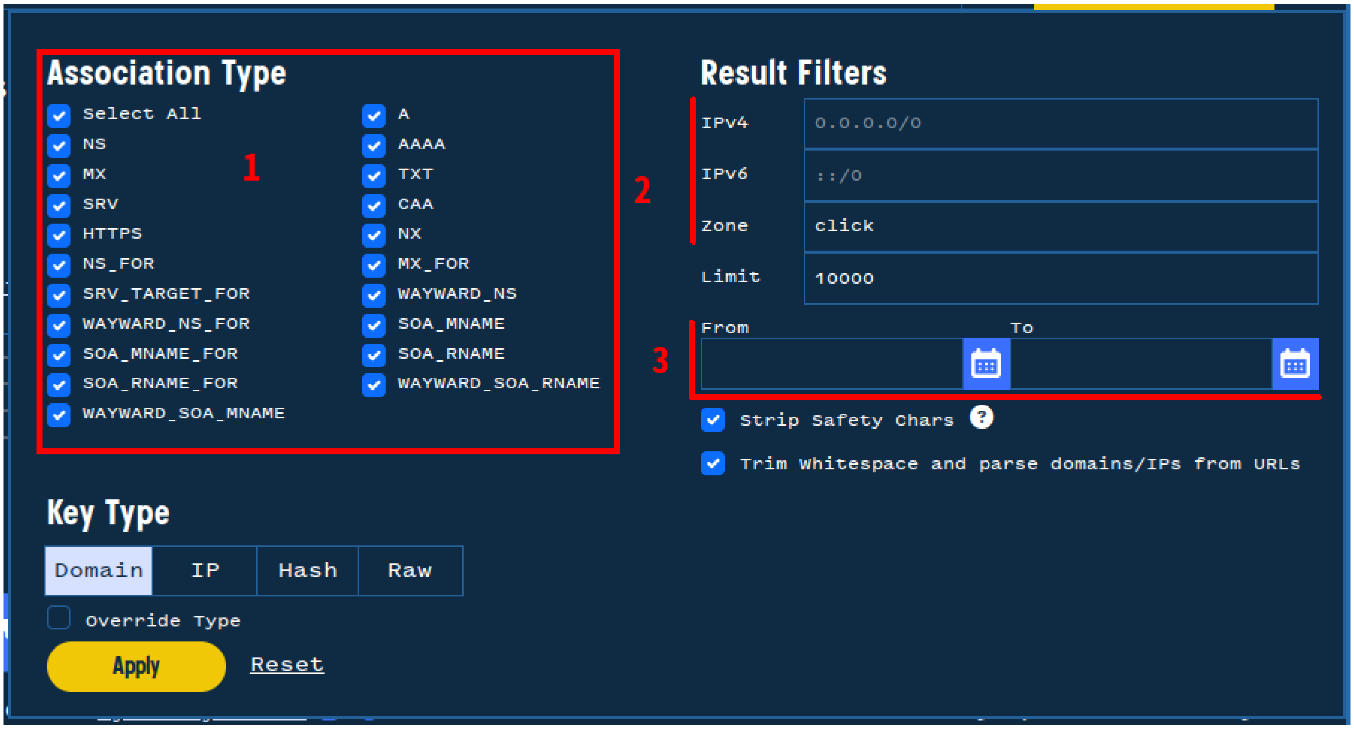
1-50 of 133

To set a filter, click on the “Filter” icon in between the search box and the “Search >” button on the advanced Search page:



ns-cloud-a1.googledomains.com

This will open a drop-down box with the filter options:



Association Type

☑ Select All	☑ A
☑ NS	☑ AAAA
☑ MX	☑ TXT
☑ SRV	☑ CAA
☑ HTTPS	☑ NX
☑ NS_FOR	☑ MX_FOR
☑ SRV_TARGET_FOR	☑ WAYWARD_NS
☑ WAYWARD_NS_FOR	☑ SOA_MNAME
☑ SOA_MNAME_FOR	☑ SOA_RNAME
☑ SOA_RNAME_FOR	☑ WAYWARD_SOA_RNAME
☑ WAYWARD_SOA_MNAME	

Result Filters

IPv4	0.0.0.0/0
IPv6	::/0
Zone	click
Limit	10000

From To

☑ Strip Safety Chars ?

☑ Trim Whitespace and parse domains/IPs from URLs

Key Type

Domain | IP | Hash | Raw

□ Override Type

The options include:

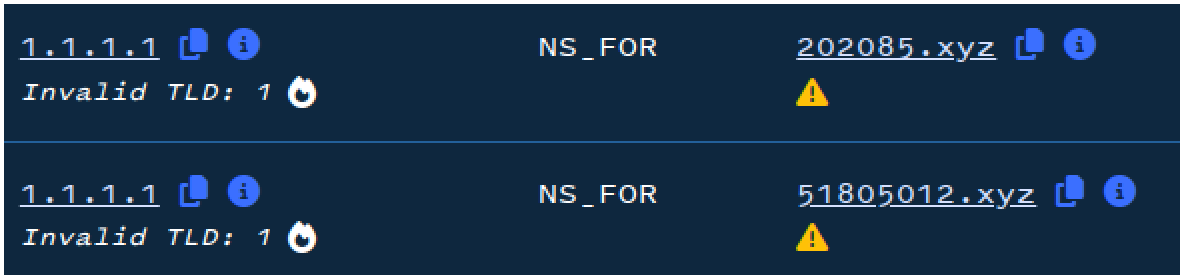
1. Association type filters (to limit to only associations of a specified type)
2. Answer filters
3. Date filters

Type the IPv4, IPv6, Zone (domain), and time window filters to limit your results, then click “Apply” to apply them.

Advanced Options

The drop-down filter box has several settings that are not commonly used:

- Override Type: this enables you to treat certain search keys as something different than they appear. The most common use case is to treat an IP address like a domain. For example, searching for “1.1.1.1” will default to finding associations for which “1.1.1.1” is an IP address, like an A record. However, overriding the type as a “Domain” will search for an answers where DNS answer is treated like a domain, like a Name Server (NS) answer:



1.1.1.1 *Invalid TLD: 1*	NS_FOR	202085.xyz ⚠
1.1.1.1 *Invalid TLD: 1*	NS_FOR	51805012.xyz ⚠

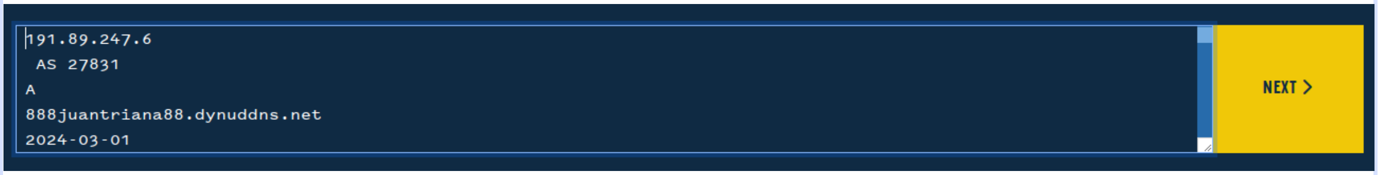
- Strip Safety Chars: when checked (the default), you can past full-defanged IPs and domains (e.g., “google\.com” or “8[.]8[.]8[.]8”) into the search field, and Validin will parse the key and search for the intended value. However, there may be times when you intend to search for the verbatim string, typically as a “Raw” value. To do this, uncheck “Strip Safety Chars” and type/paste your value into the search field.
- Trim whitespace and parse domains/IPs from URLs: Validin will parse domain names and IP addresses out of URLs pasted into the search bar by default. Validin will also trim whitespace. To search for the whitespace deliberately, uncheck “Trim Whitespace” first.

Bulk Analyze

The “Bulk Analyze” workflow is designed to help researchers quickly identify patterns between large sets of indicators.

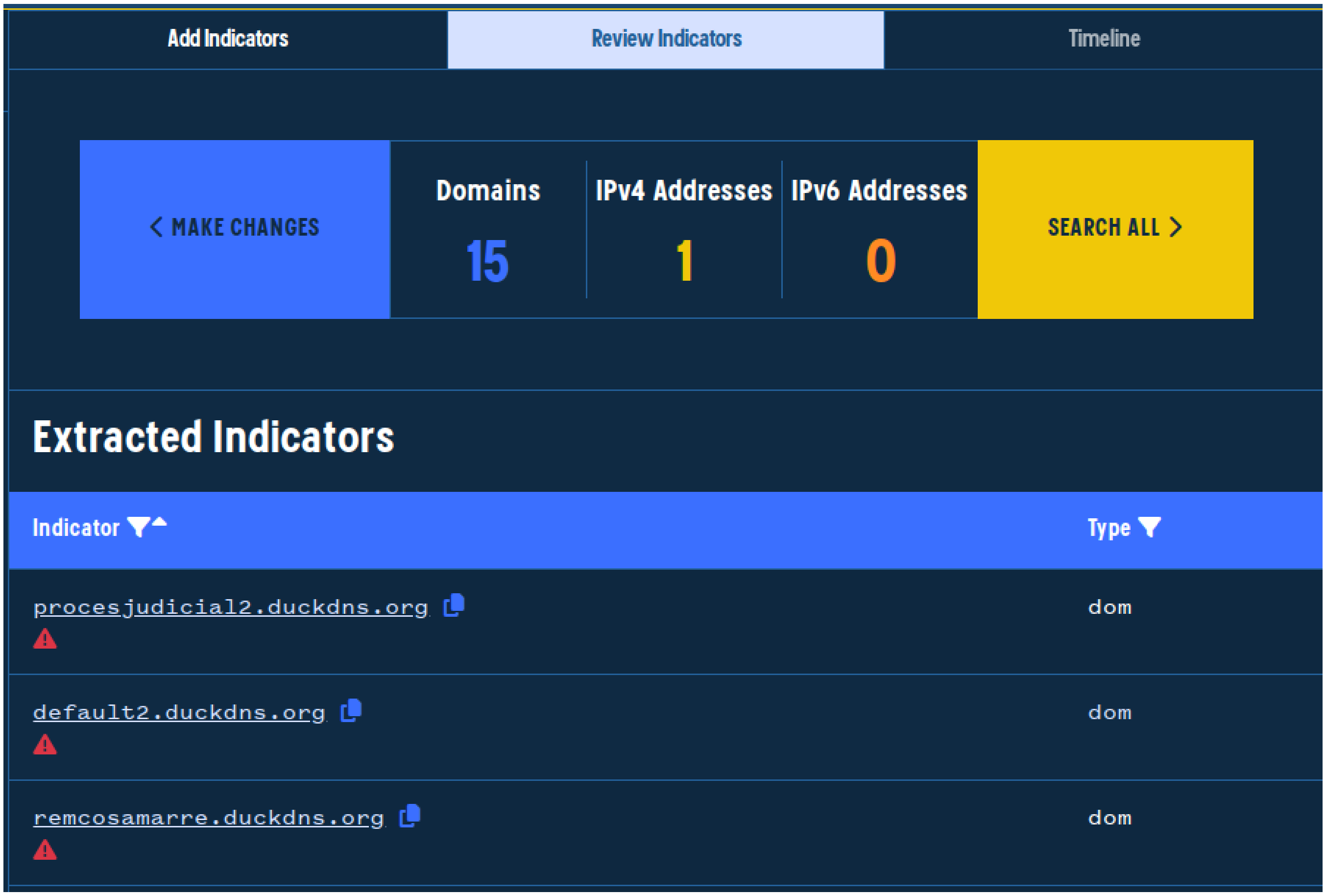
To begin the workflow, visit the “Bulk Analyze” page, type or copy/paste indicators into the search box, then click “Next.”

> Note: Validin will parse defanged and unstructured content out of indicators. The workflow is designed to make it very easy to copy/paste from reports and other sources.



```
191.89.247.6
 AS 27831
A
888juantriana88.dynuddns.net
2024-03-01
```

Validin will parse the indicators you provided, determine the type, then show you details about any known malware families or popularity associated with the indicators.

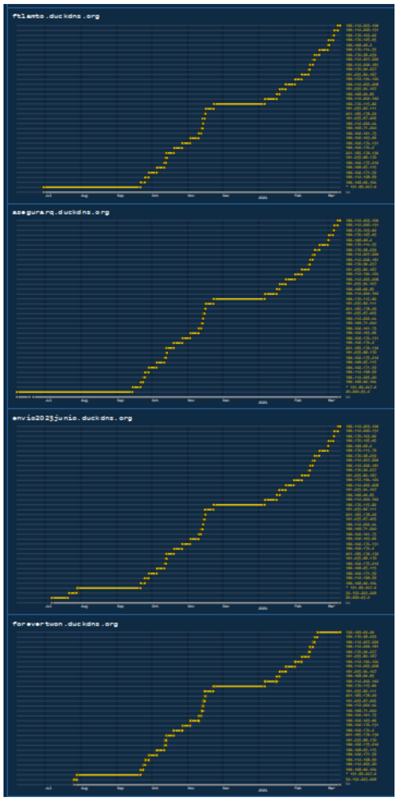


Domains	IPv4 Addresses	IPv6 Addresses
15	1	0

Extracted Indicators

Indicator	Type
procesjudicial2.duckdns.org	dom
default2.duckdns.org	dom
remcosamarre.duckdns.org	dom

To make changes, click the blue "Make Changes" button and continue editing the indicators in the text box.



Once you are satisfied, click the yellow "Search All" button to begin finding DNS history for every indicator in your input set. The results are displayed as a timeline, which allows researchers and analysts to rapidly identify patterns of behavior across large sets of indicators visually.

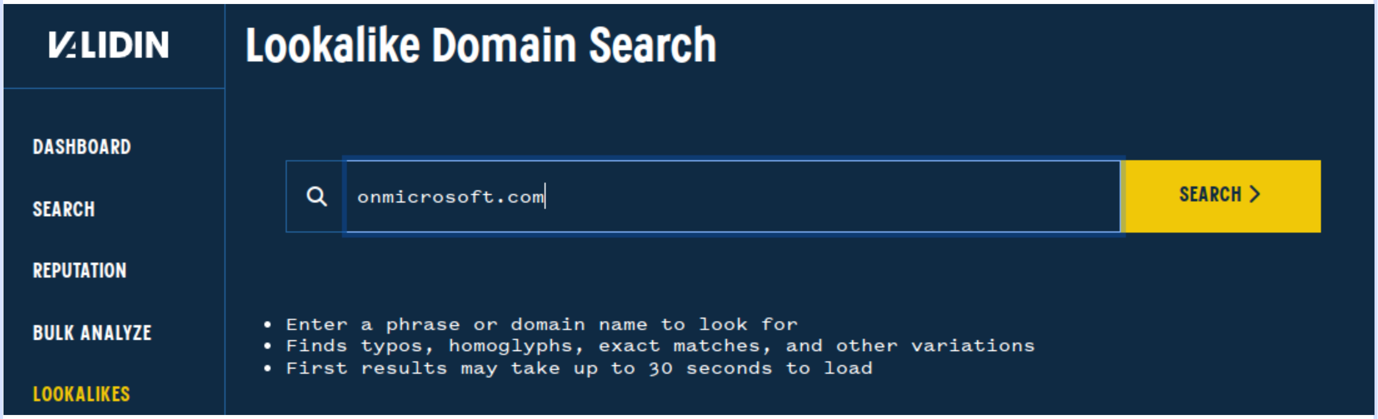
Associations that are part of your original will be prefixed with an asterisk ("*"). Indicators not in your original set will not contain an asterisk.

You may copy/paste answers and add them back to your initial indicator set to begin the process with additional indicators.

Lookalikes

The Validin platform enables "fuzzy searching" across the entire domain set known to Validin (~3.9 billion as of March 1, 2024).

To search for lookalike domains, visit the “Lookalikes” page in the platform, then type a domain name, company name, or brand to search, then click “Search.” The Validin platform will look for typos, homoglyphs, subdomain matches, and many other variations that we’ve observed.

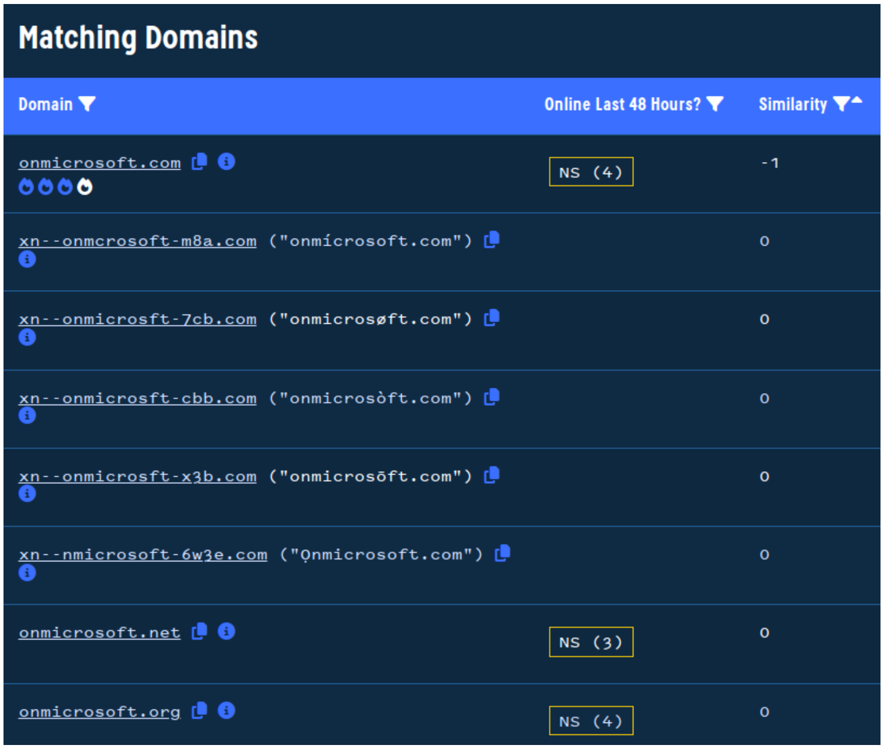


Lookalike Domain Search

onmicrosoft.com

- Enter a phrase or domain name to look for
- Finds typos, homoglyphs, exact matches, and other variations
- First results may take up to 30 seconds to load

The search may take up to 30 seconds to complete. Once finished, Validin will display the matching domain, a summary of active resolving infrastructure, and a score describing the similarity to the queried domain (0 means “very close match,” and higher numbers are a further edit distance match).



Matching Domains

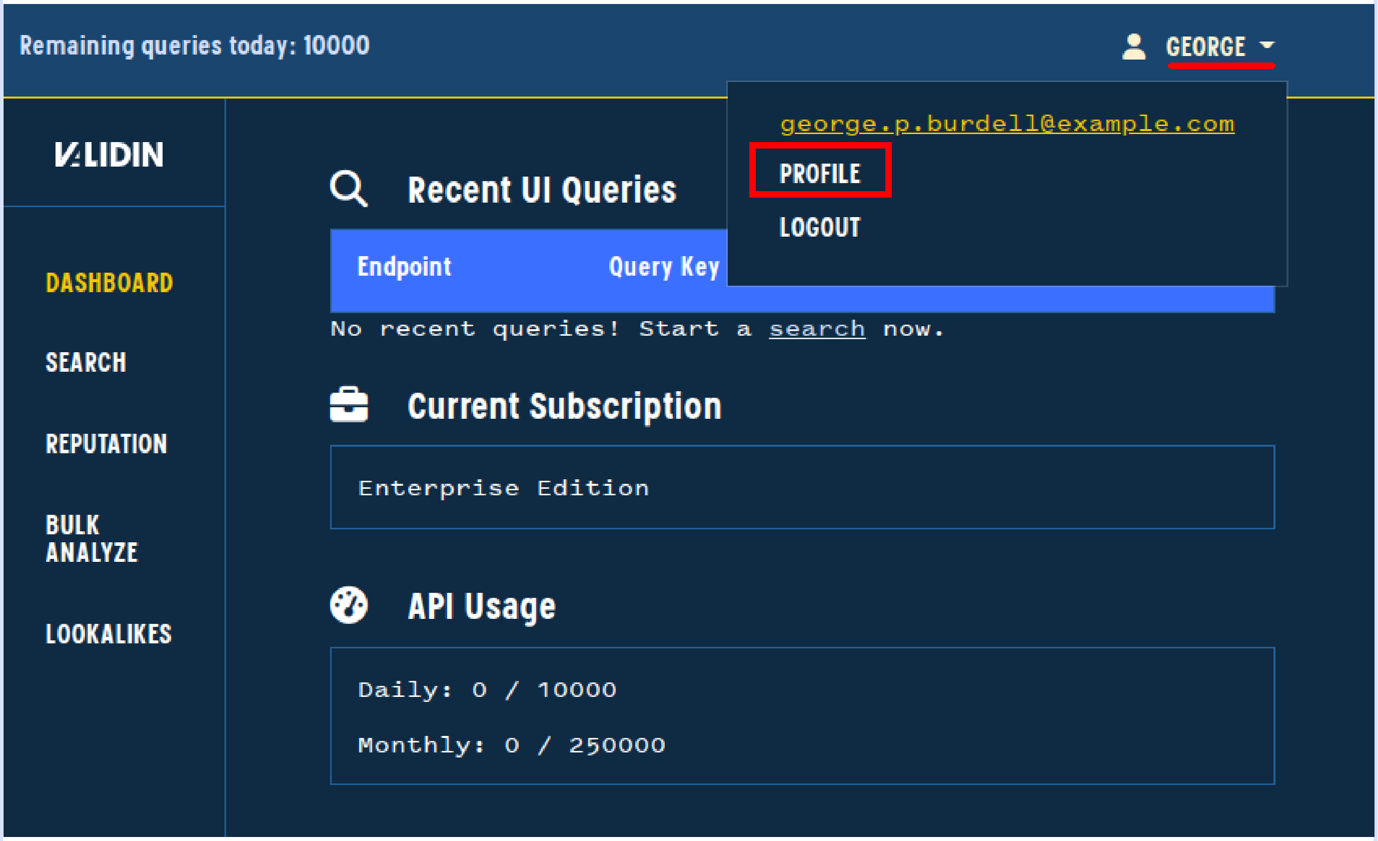
Domain	Online Last 48 Hours?	Similarity
onmicrosoft.com	NS (4)	-1
xn--onmcrosoft-m8a.com ("onmícrosoft.com")		0
xn--onmicrosft-7cb.com ("onmicrosøft.com")		0
xn--onmicrosft-cbb.com ("onmicrosòft.com")		0
xn--onmicrosft-x3b.com ("onmicrosōft.com")		0
xn--nmicrosoft-6w3e.com ("Ọnmicrosoft.com")		0
onmicrosoft.net	NS (3)	0
onmicrosoft.org	NS (4)	0

Managing your account

This section describes account management actions available on the Validin platform.

Changing your password

You may change your password at any time by visiting your profile:



Remaining queries today: 10000

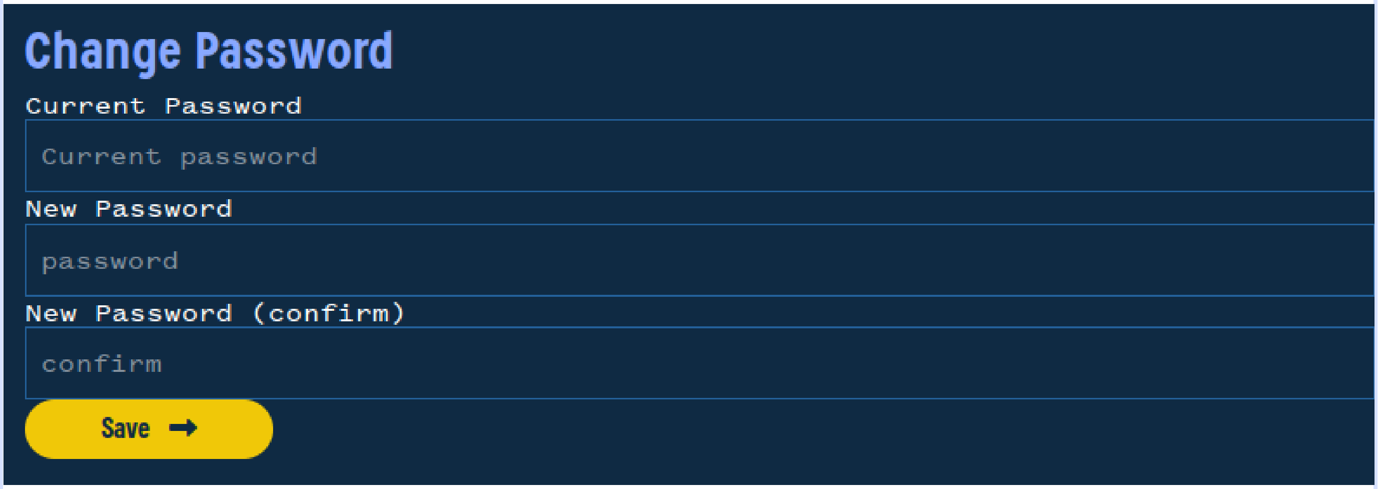
No recent queries! Start a search now.

Enterprise Edition

Daily: 0 / 10000

Monthly: 0 / 250000

Scroll down to “Change Password,” then enter your current password and your new password twice (to confirm).



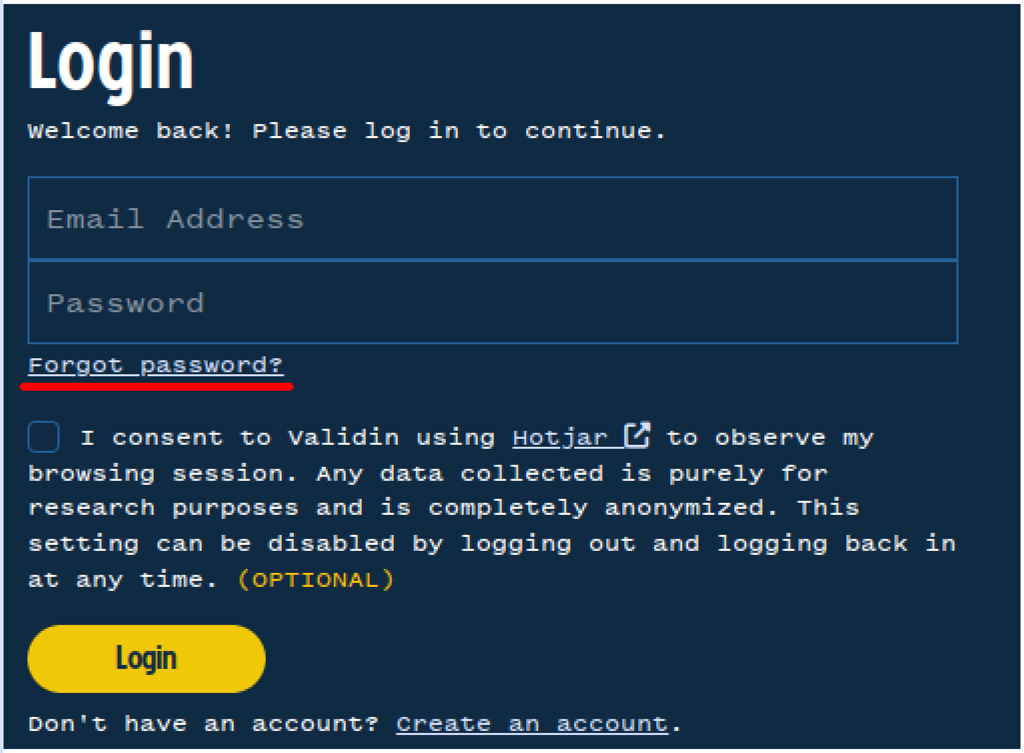
Current Password: Current password

New Password: password

New Password (confirm): confirm

Resetting a forgotten password

If you’ve forgotten your password, you can retrieve your password via self-service password reset by first visiting the login screen and clicking “Forgot password?”



Login

Welcome back! Please log in to continue.

Email Address

Password

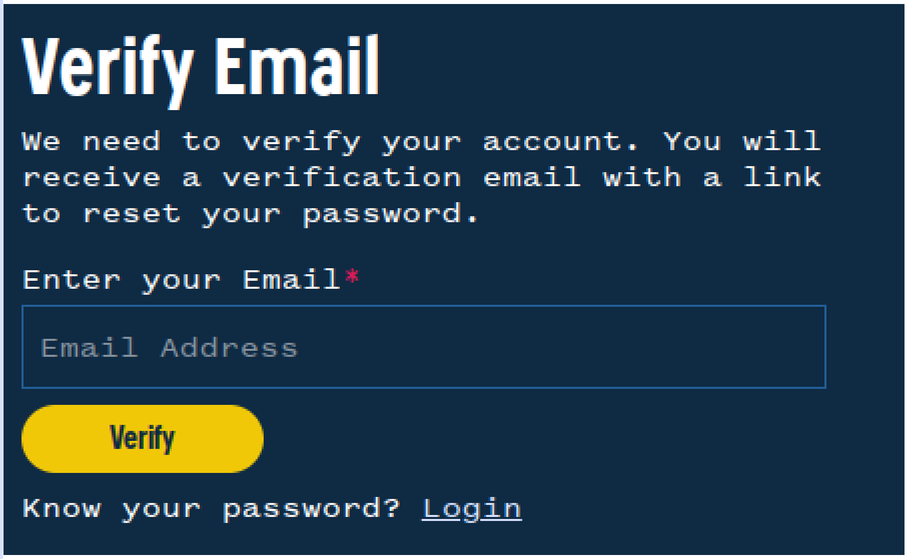
Forgot password?

□ I consent to Validin using Hotjar to observe my browsing session. Any data collected is purely for research purposes and is completely anonymized. This setting can be disabled by logging out and logging back in at any time. (OPTIONAL)

Login

Don't have an account? Create an account.

On the next screen, enter the email address associated with your account:



Verify Email

We need to verify your account. You will receive a verification email with a link to reset your password.

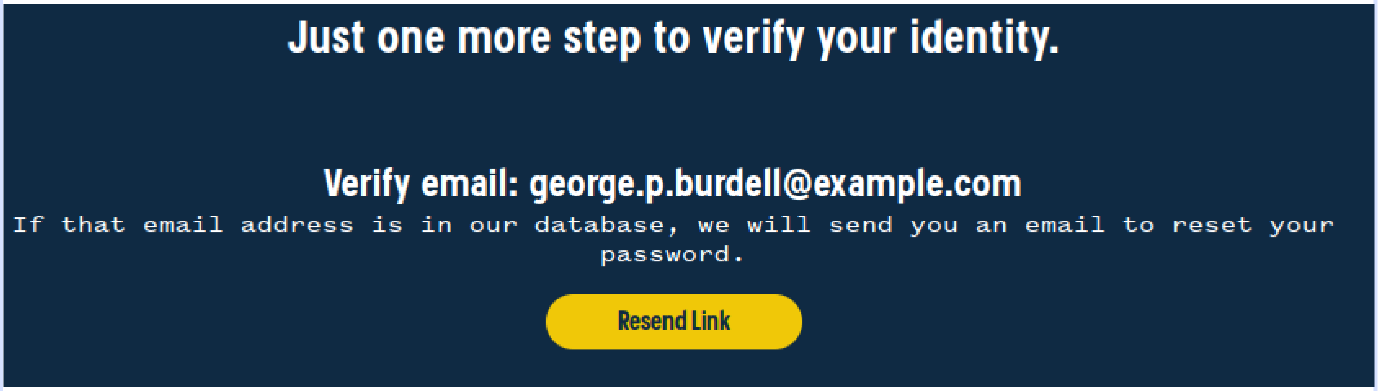
Enter your Email*

Email Address

Verify

Know your password? Login

Then hit "Verify." Validin will send you an email to confirm that you are the owner of the account associated with that email address:



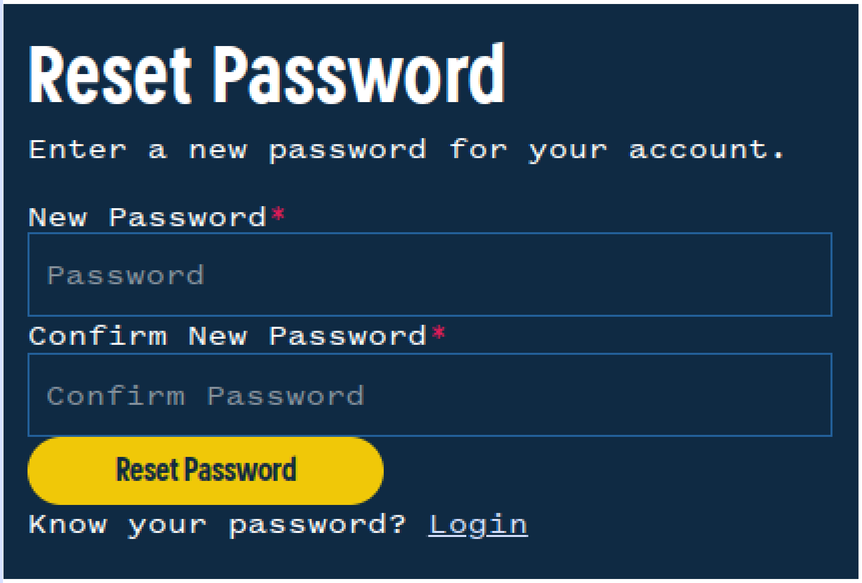
Just one more step to verify your identity.

Verify email: george.p.burdell@example.com

If that email address is in our database, we will send you an email to reset your password.

Resend Link

Once you receive the password reset email, click the link and enter your new password:



Reset Password

Enter a new password for your account.

New Password*

Password

Confirm New Password*

Confirm Password

Reset Password

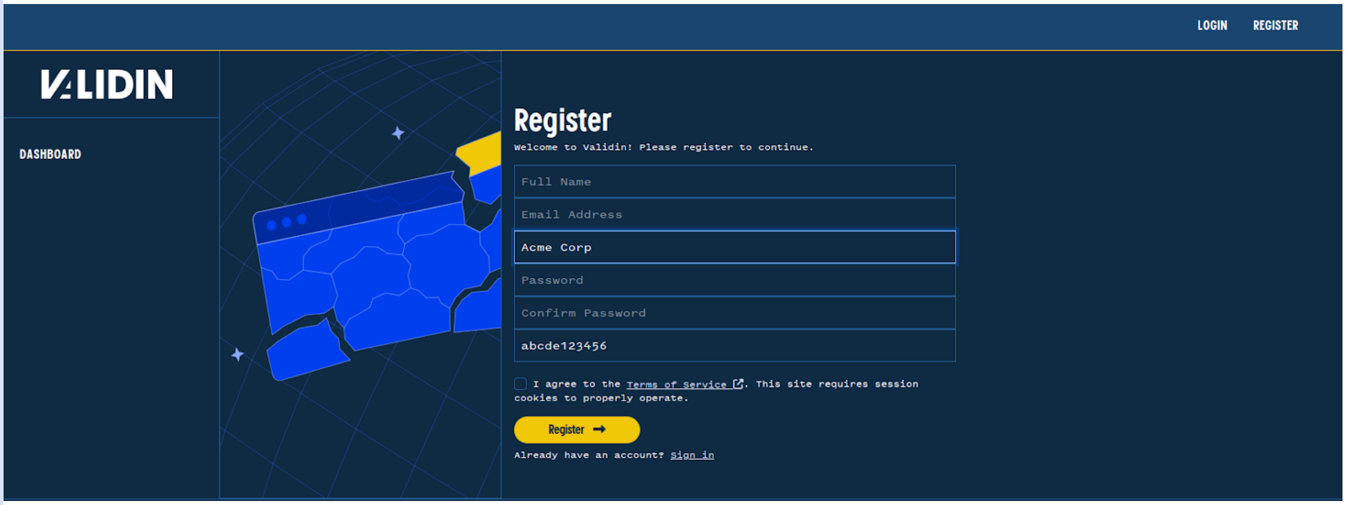
Know your password? Login

After resetting your password, you will be able to login normally with the new password.

Creating your Enterprise account

The Validin platform supports individual accounts with pooled, company-wide query quotas. Each person using the Validin platform should do some from their own account; account credentials should not be shared.

You will receive an account creation link from one of your company's administrators. The account creation link will prompt you to provide your name, email address, and password. Your name, email address, and company name may already be pre-filled. You must also read and understand the Terms of Service. The latest version of the Terms of Service are on the Validin platform website.



LOGIN REGISTER

VALIDIN

DASHBOARD

Register

Welcome to Validin! Please register to continue.

Full Name

Email Address

Acme Corp

Password

Confirm Password

abcde123456

□ I agree to the Terms of Service. This site requires session cookies to properly operate.

Register →

Already have an account? Sign in

After successfully creating your account, you will receive an activation email from Validin. Use this link to complete the account setup process.

Frequently Asked Questions

Data Sources

What data does Validin collect?

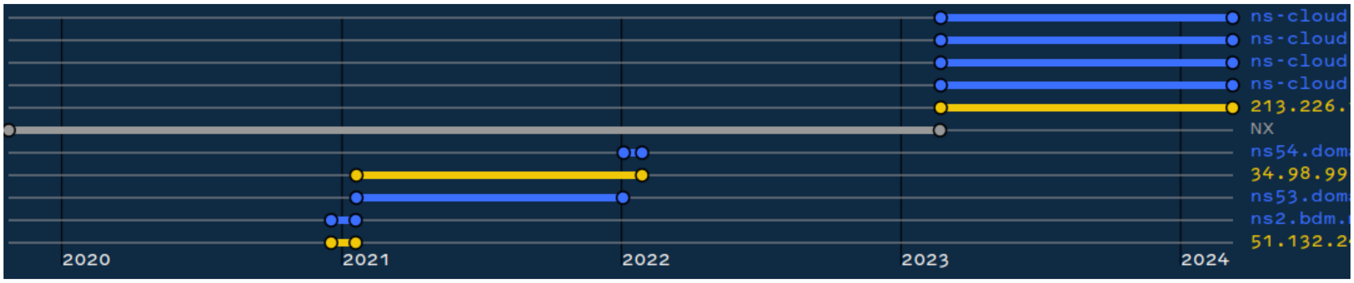
Validin collects the following types of data:

- DNS
- HTTP response headers and metadata
- Certificates from CT logs

Additionally, Validin monitors hundreds of popularity, block, and reputation lists for changes and appearances.

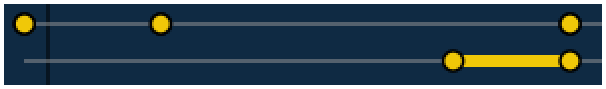
Results

Why does NX sometimes overlap with other results?



Some DNS servers will respond with NXDOMAIN for labels that exist, but for which there are no records for the requested type. This is most common with AAAA (IPv6) records, but can happen with any record type. Validin requests A, AAAA, and NS records for each domain we track on at least a daily basis, so if we see NX for one query, but an answer for another, we'll record both answers and display them when asked.

When do you display contiguous lines in your timelines vs. individual points?



Validin will combine data points into a single line if the time between consecutive measurements with the same value is less than 2 days.

Times appear to be aligned to 6-hour windows. Why?

We record DNS and banner answers with second granularity. However, to reduce storage space in our databases, we bucketize answers into 6-hour windows.

How often do you make DNS queries?
We make DNS queries throughout the day.

Where do you get your data?
We collect DNS and banner data in-house with custom crawling and scanning tooling and infrastructure. We use forward DNS with in-house closed recursive resolvers. By design, we do NOT monitor traffic from individuals and have no ability to see who is querying what at any level.

How do you determine what to query?
We query every name in our database at least daily. However, there are some names we drop from our database from time-to-time. For example, we only query the subdomains of some popular domains that are wildcarded (e.g., blogspot.com) when we see them explicitly referenced on a popularity or public block list.

Where do you get new names for forward DNS?
We discover new names from hundreds of independent and derivative sources, including popularity lists, zone files, DNS answers, and custom crawling results. We don’t have a reliance on any particular source for domain name discovery. We supplement this discovery process with educated guesses about other domains that might exist (for example, if google.<TLD> exists on many TLD zone files that we have access to, we’ll also periodically check if it exists on TLDs that do not give us zone file access).

Support and Contact

Mailing address:

Validin LLC
Atlanta Tech Village
3423 Piedmont Road NE
Atlanta, GA 30305

Email: support@validin.com
Website: www.validin.com