



# Iris Detect

User Guide



DOMAINTOOLS®

## Introduction

Iris Detect protects against malicious domains impersonating your brands and domains so you can safeguard your organization, your customers and your trademarks. You can also defend against supply chain attacks where malicious domains impersonate either well-known technology vendors or even partners you work with on a regular basis. Iris Detect does this by discovering new domains appearing globally that mimic your brands. You can quickly see key information from DNS, Whois, screenshots and the DomainTools Risk Score to easily access the level of threat. Iris Detect also monitors domains over time so you can see how they evolve, and then lets you take action as needed.

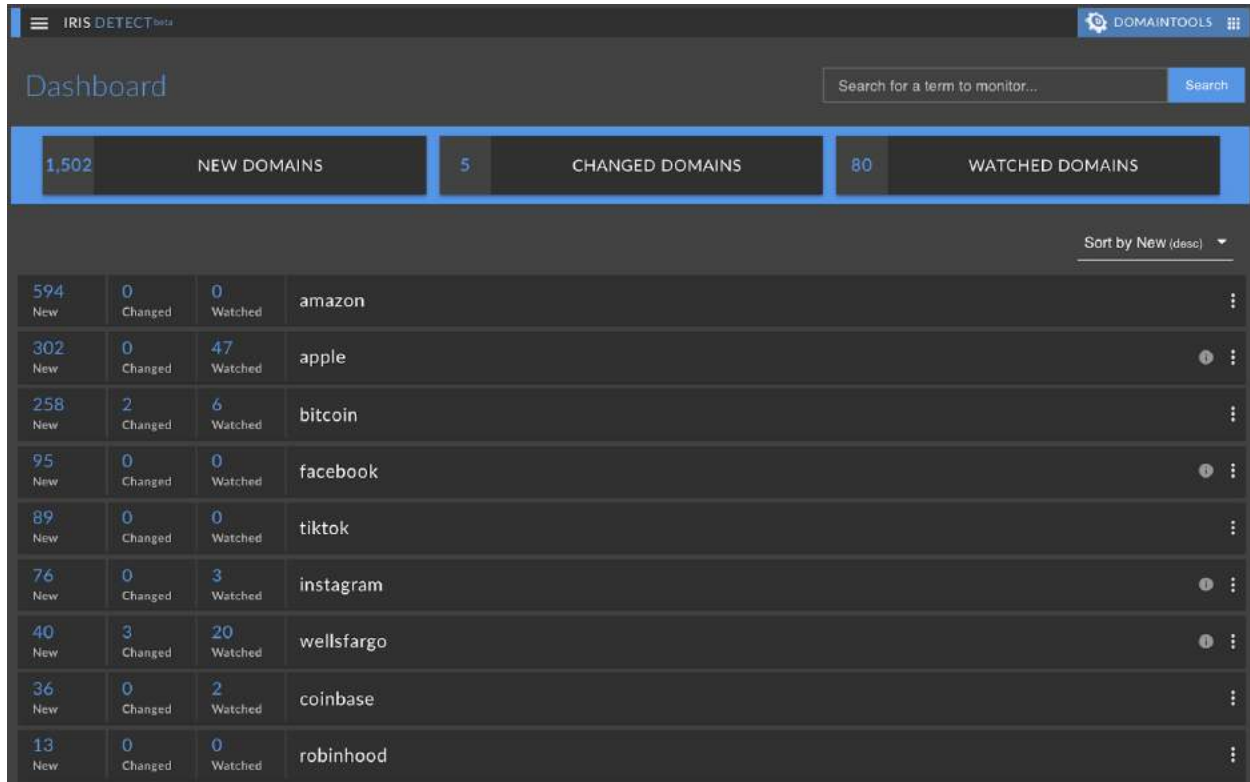
## Getting Started

<https://iris.domaintools.com/detect>

**Iris Detect requires an Enterprise account login on DomainTools**, and your account must include Iris Detect access. Additionally, user permissions control whether users can manage monitors, triage domains, or escalated domains. By default, users have read-only access to the application.

## Dashboard

Iris Detect's Dashboard shows monitors already set up for your organization and lets you create new ones. Remember that **monitors are shared by all Detect users in your organization**. If you don't yet have any monitors yet, the Welcome page provides a search box for adding the first monitor. To learn more about adding monitors, see the section below on **Creating Monitors**. For each monitor, the dashboard shows the term that is being monitored plus statistics for the number of new domains, the number of watched domains, and the number of watched domains that have recently changed.



The dashboard displays the following statistics:

- 1,502 NEW DOMAINS
- 5 CHANGED DOMAINS
- 80 WATCHED DOMAINS

The table below shows the monitored terms and their associated statistics:

Term	New	Changed	Watched
amazon	594	0	0
apple	302	0	47
bitcoin	258	2	6
facebook	95	0	0
tiktok	89	0	0
instagram	76	0	3
wellsfargo	40	3	20
coinbase	36	0	2
robinhood	13	0	0

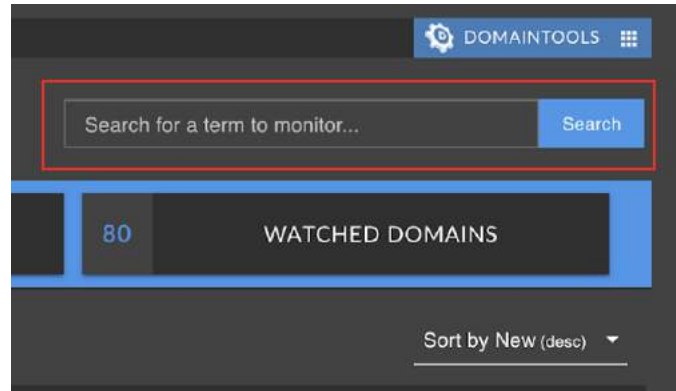
*Dashboard for Iris Detect*

To view the domains associated with the monitor, you can **click on the term or any of the statistics** to see a list of corresponding domains.

Monitor ordering on the dashboard can be controlled by the “**Sort by**” dropdown on the dashboard.

## Create Monitors

Use the **Search** box on the Dashboard to enter the term you want to monitor. The term represents the brand or domain you want to defend. Enter a single word in the text box - up to 63 characters that are either “a-z”, “0-9” or a dash “-”. Whitespace is not allowed.



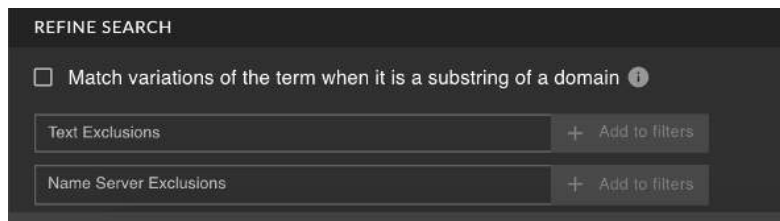
*Search box to start create monitor workflow*

If you're setting up a monitor for typosquatting against a domain, you only need to enter the "root" of the domain: Instead of `domaintools.com`, just enter "domaintools." Iris Detect will automatically find typosquat domains in any Top Level Domain (TLD) globally.

After entering the term for monitoring, Iris Detect shows all known active domains that match the term, including variations that might be used by typo-squatters. This list uses historical matches to provide insight on the quality and number of domains that will be discovered by the monitor once it is set up. The chart at the top of the page shows the number of historical matches for up to the last 30 days. The daily average indicates the number of domains that might be discovered in the future. Use these results to understand whether the monitor will produce an expected number of daily matches. **The chart can be hidden through the collapse icon** on the upper left corner of the chart.

## Refine Monitor Configuration

To optimize monitor configuration, select “Refine Results” from the lower-left of the results page.



*Options refining monitor configuration from search page*

The first option is a checkbox to **enable matching variations of the term when it appears in a longer domain name**. For example, if the term were “domaintools,” enabling this feature would match the domain account-domaintools.com (where zeros replace the “o’s” in DomainTools.) This can produce high-quality results for longer terms or terms that are more specific. For shorter or more generic terms, the option can generate a large number of false positives. Compare the average number of daily matches both before and after plus view the historic domains for guidance on the quantity and quality of additional matches generated by using the option.

**Text Exclusions** will ignore domains that use specific words that would be considered “noisy” or false positives. For example, if you wanted to monitor for new domains related to the term “election”, the search results will include domains with the word “selection”. Adding “selection” as an exclusion will automatically hide domains that include that word. Multiple text exclusions can be added as needed to tune the monitor.

**Name Server Exclusions** can be used to hide domains that are being created by teams internally across your organization if they reference a known set of name servers. A domain is only excluded if all the name servers it uses are included in the exclusion list. You can use wildcards - for instance “\*.domaintools.com” will prevent the need to enter “ns1.domaintools.com”, ns2.domaintools.com”, etc.

As you refine the monitor, the total number of matching known domains changes - this can help you understand a general ratio of domains that might be excluded going forward compared to if the refinement was not included.

If you see existing domains that you would like to monitor with Iris Detect, you can do that once the monitor has been saved. See Previous Domains (below) for more details.

Once you add a monitor, it will appear on the Dashboard. Initially, there will be no domains associated with the monitor. Iris Detect will start to discover new domains and show them as New for the monitor. It will also provide a view of Previous Domains after a few minutes of background indexing completes.

## Edit and Delete Monitors

Monitors can be **edited from the menu to the far-right of the term**. You can adjust the refinements, adding or removing exclusions or changing the setting for including domains that include variations of the name as a

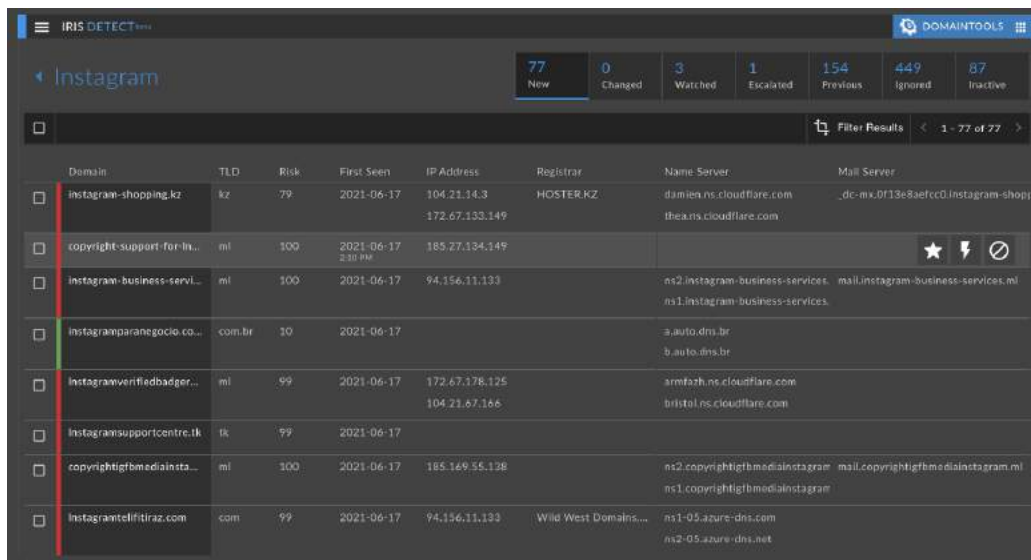
substring. Editing a monitor will adjust the New and Previous domains for a monitor, but it will not impact domains already selected to be Watched.

Monitors can be deleted as well but remember that deleting a monitor will remove the monitor and the corresponding domains for all users in your group.

## View New Domains

From the Dashboard, select the **New** count for a monitor to see newly discovered domains that need analysis. The top-level New Domains count can also be selected to see results across all monitors.

Domains appear in a table format by default - a convenient layout for quickly scanning across a large number of rows.

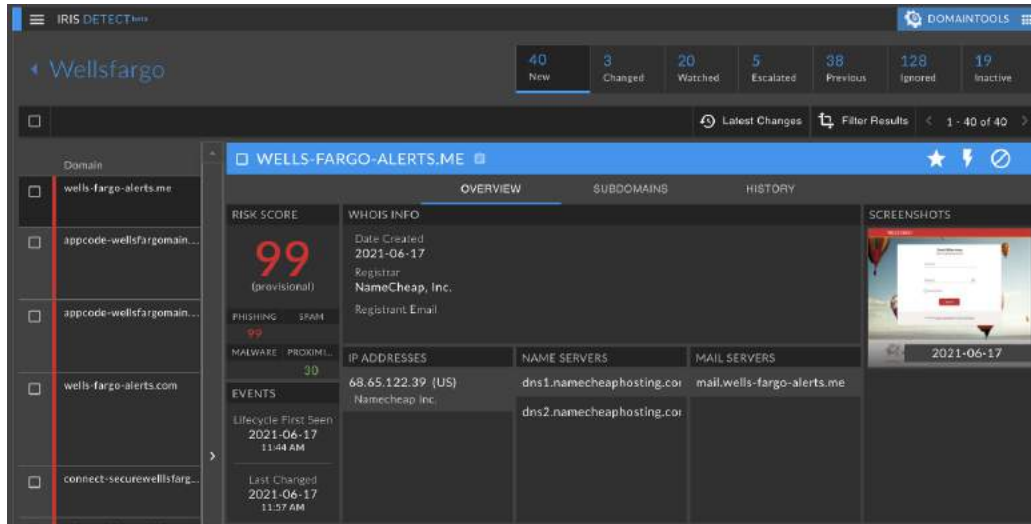


Domain	TLD	Risk	First Seen	IP Address	Registrar	Name Server	Mail Server
instagram-shopping.kz	kz	79	2021-06-17	104.21.14.3 172.67.133.149	HOSTER.KZ	damien.ns.cloudflare.com thea.ns.cloudflare.com	_dc.mx.0f13e8aefcc0.instagram-shop...
copyright-support-for-hi...	ml	100	2021-06-17 2:30 PM	185.27.134.149			
instagram-business-servi...	ml	100	2021-06-17	94.156.11.133		ns2.instagram-business-services. ns1.instagram-business-services.	mail.instagram-business-services.ml
instagramparanegocio.co...	com.br	10	2021-06-17			a.auto.dns.br b.auto.dns.br	
instagramverifiedbadger...	ml	99	2021-06-17	172.67.178.125 104.21.67.166		armfzrh.ns.cloudflare.com bristol.ns.cloudflare.com	
instagramsupportcentre.tk	tk	99	2021-06-17				
copyrightigfbmediainsta...	ml	100	2021-06-17	185.169.55.128		ns2.copyrightigfbmediainstagram ns1.copyrightigfbmediainstagram	mail.copyrightigfbmediainstagram.ml
instagramtellfitiraz.com	com	99	2021-06-17	94.156.11.133	Wild West Domains...	ns1-05.azure-dns.com ns2-05.azure-dns.net	

*Table-view of domain lists*

To see more detail for a domain, **selecting a domain's row** will switch the layout to card format, with more room to show additional information about a domain. Attributes displayed in card view include:

- IP address(es), plus the country code and ISP
- Name server hostname(s)
- MX server hostname(s)
- Create date from the Whois record
- Registrar
- Registrant email
- Risk score
- Screenshots
- Subdomains



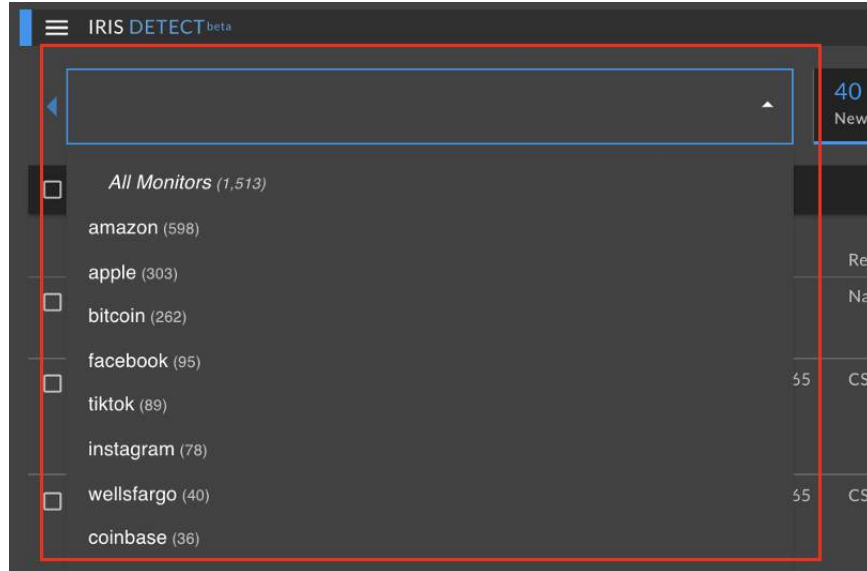
*Card-view of domains*

A key attribute of domains in Iris Detect is the **Lifecycle First Seen**, in some places shortened to just First Seen. This is the date and time that DomainTools learned that a domain is likely active. As domains can be active, then inactive for a while, and then active again, this field shows when a domain became active in its most recent lifecycle. By default, new domains are ordered by Lifecycle First Seen so domains are effectively listed by their age, with the newest listed first.

Another important attribute is the **Last Changed**, the date and time a field tracked in Detect was changed. See \_\_\_ for more details on viewing changes for domains.

To switch between different domains lists for a monitor, **select the count** for Changed, Watched, Escalated, etc. and the Watchlist will be filtered accordingly.

To quickly jump to the Watchlist for a different monitor, **select the monitor name**, see a list of your other monitors, and choose the other you wish to see.

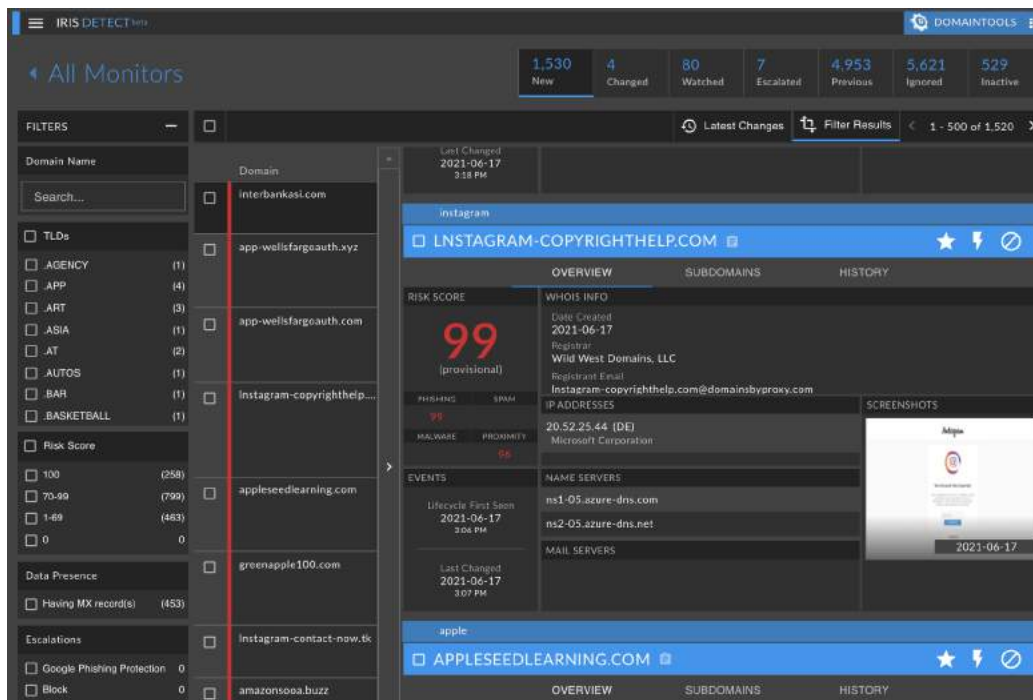


Switch monitors via drop-down

To view new domains across all monitors in a single view, select “All Monitors” from either the dropdown list of monitors, or select an all-monitor statistic from the Dashboard.

## Filter Domains

From any domain list for a monitor, open the filter pane to target specific sets of domains.



Domain filtering



The sort order can be changed from first seen to the date last changed, or the list can be ordered by risk. Use the Sort options at the bottom of the filter pane to change the list order.

## Watched Domains

**Watched** domains are those that have been manually selected to be Watched, either from New or Previous. There is no limit on the number of domains that can be watched. By default, they are ordered by most recently changed. Watched domains appear under Changed when a DNS or Whois attribute changes. Domains can be added to the Watchlist one at a time by selecting the 'star' icon on the right of the domain card. They can also be added in bulk by selecting the checkbox for multiple domains and choosing "Add to Watchlist" from the Action drop-down. Watched domains can be **Ignored** if they are no longer of interest for change tracking.

## Changed Domains

Domains that are Watched are tracked for changes to their DNS, Whois information and when the domain is identified as active or inactive. When these fields change, the Last Changed field updates to show when the most recent change happened for one of the tracked fields.

Changed domains are ordered by Date Last Changed, with the most recently changed listed first. By default, Changed shows only domains that have changed in the last 24 hours. This can be easily updated by selecting the upper-left menu, Settings, General, and selecting the Changed Domain Timeframe option.

## Latest Changes

To easily see which fields most recently changed, select the Latest Changes control. The most recently changed field will be highlighted along with other fields changed within 24 hours of the most recent change. This lets you quickly scan for changes in domains across your list. Mousing over a highlighted field will show the date and time the field changed.

*Latest Changes with mouse-over showing date/time of change*

## Domain History

For a more comprehensive view of changes to a domain over time, select History for a domain. This shows changes to the following fields:

- Status - when a domain was discovered as active, and when it was determined to be inactive
- IP Address
- Nameserver
- MX Host in DNS
- Whois Date Created
- Registrar
- Registrant email

IRIS DETECT beta

Tiktok

5,294 New | 2 Changed | 49 Watched | 0 Escalated | 9,897 Previous | 3 Ignored | 3 Inactive

Latest Changes | Filter Results | 1 - 2 of 2

last changed 2021-10-08

TOKTOKBET.COM.BR WATCHED

OVERVIEW		SUBDOMAINS		HISTORY	
Date	Field	Previous Value		New Value	
2021-09-30 12:36 PM	IP Address	191.252.51.57 (BR) Locaweb Servi Os De Internet S/a		186.202.157.79 (BR) Locaweb Servi Os De Internet S/a	
2021-09-29 10:00 PM	Name Server	a.auto.dns.br b.auto.dns.br		ns1.locaweb.com.br ns2.locaweb.com.br ns3.locaweb.com.br	
2021-09-29 9:59 PM	Mail Server	(empty)		mx.core.locaweb.com.br mx.b.locaweb.com.br mx.a.locaweb.com.br mx.jk.locaweb.com.br	
2021-09-29 9:59 PM	IP Address	(empty)		191.252.51.57 (BR) Locaweb Servi Os De Internet S/a	
2021-09-12 9:49 AM	Registrar	(empty)		(empty)	
2021-09-12 9:49 AM	Date Created	(empty)		2017-04-06	

### Domain History

To focus on one or more specific types of changes, use the filter control next to the Field header in the history table.

Note: Domain history began tracking changes for domains in October 2021, it does not include historic changes from before then.

## Take Action on Domains

Analyzing and triaging newly discovered domains is an activity that should be done regularly, so New domains only shows recently discovered domains. Triage options include:

- **Add to Watchlist:** Adding a domain to the Watchlist removes it from New and allows tracking of when domains most recently changed in DNS or Whois. Watched domains will have screenshots captured daily so you see how the webpage evolves over time.
- **Ignore:** If a domain is obviously a false positive, Ignoring the domain removes it from New and places it under Ignored. The decision can always be reversed and the domain can be moved from Ignored to Watched instead.
- **Escalate:** Two escalation activities are supported as shown below. Escalating a New domain will also add it to be Watched for changed.
  - Domains can be sent to **Google's Phishing Protection team**. If Google agrees the domain is malicious, it will be blocked in Chrome browsers globally. This list is also picked up by Apple for their Safari browser and Firefox.

- Domains can be **marked for Blocking** if they are to be blocked in internal network defense infrastructure. The blocking designation is transmitted through the Detect APIs. Integration with the APIs can automate the process of blocking domains.

To take action on a single domain, **select the corresponding icon** (for Watch, Escalate, Ignore) on the right side of the row (in table view) or card (in card view). To triage multiple domains, use the checkboxes and then the Update menu that appears whenever one or more domains are checked.

## Export Domains

You can open domains in Iris Investigate to see even more detail about the domains and how they might relate to other domains. First, check the domains, then use the **Export** menu that appears whenever one or more domains are checked.

You can also download domains for use outside of the product, either in CSV or STIX 2.0 file format.

## Escalated Domains

**Escalated** is a single way to keep track of all the domains that have been Escalated and are active. When viewing escalated domains in card view, hover over the Escalated sticker to see who escalated the domain, what type of escalation was done, and when this happened.

## Previous Domains

When setting up a new monitor, Iris Detect shows domains that were already active and matched the monitoring criteria. Those domains can be manually added to a monitor's Watchlist after the monitor has been added.

To work with Previous domains, open a monitor, then select the Previous count to view a list of the domains. The list is capped at the most recent 10,000 domains if the monitor has a large number of matching domains. You can add Previous domains to Watched either one at a time, or in multiples via the checkboxes and the Update drop-down menu.

## Ignored Domains

**Ignored Domains** shows domains that have been ignored. In card view, hover over the Ignored sticker to see who ignored the domain and when. Ignored domains can be added back to the Watchlist.

## Inactive Domains

**Inactive Domains** shows domains that were Watched and then became inactive. If one of these domains becomes active again, it will appear as New.

*For domains that became inactive from October 2021 onwards, the date/time the domain became inactive can be seen from Domain History.*

## Email Alerts

From Settings > Alert Configuration, set up alerts for new domains to be emailed either daily or four times daily. First, add email addresses that will receive alerts. Note that a maximum of 127 domains are listed for each monitor, if a monitor has more than this, use the Detect website to see full results.

Choose the detailed format for emails that include a list of new domains for your monitors or the summary format for just statistics on new domains for each monitor. Use the checkbox to include changed domains as well as new.

**Frequency** lets you receive emails either once a day or four times daily - each option will include new domains just for that reporting period. You can choose to receive alerts even if there are no new results if you want to use the emails to confirm there are no new matches.

## Theme

From Settings > Theme, choose either bright or dark mode as your preferred styling when using Iris Detect.