User Guide

Iris Detect

May 2024

DomainTools

Contents

Introduction **3**
Get Started **3**
User Access 4
The Dashboard **4**
Add and Edit Monitors **4**
Domain Groups **5**
Monitor Dashboard **6**
Domain Information 6
Domain Actions 8
Add to Watchlist 8
Escalate 9
Ignore 9
Export (Bulk Update) 9
Iris Investigate 9
File Download 9
Highlight Latest Changes 10
Filter Domains 10
Sort Domains 10
Iris Detect API Integration **11**
Monitor IDs and Domain IDs 11
Settings **11**
Changed Domains Timeframe 11
Email Alert Configuration 12

Introduction

Iris Detect is an Internet infrastructure detection, monitoring, and enforcement tool. It rapidly discovers malicious domains that are engaged in brand impersonation, risk-scores them within minutes, and supports your automation of detection, escalation, and enforcement actions. Read more about Iris Detect and the Iris Platform on our Products Page.

Use the Iris Detect web interface to create, edit, and observe monitors. Monitors are lists of domains updated in near real-time, based on your search terms and our fuzzy matching techniques.

For each monitor, the web interface provides a range of information for each domain, such as its Risk Score, DNS, Whois, and web-related data. Monitors also point to matching domains that are newly discovered, recently changed, recently reactivated, or that were flagged or ignored by a user in your organization.

Use the Iris Detect API to search and filter within all or individual monitors, and to watchlist or escalate domains (here is its API Reference). Test your API queries with the OpenAPI Specification on SwaggerHub. Use the API to automate detection, escalation, and enforcement.

Get Started

Log in at https://iris.domaintools.com/detect. Iris Detect requires the following:

- An Enterprise Account with DomainTools, which is accessible at https://account.domaintools.com/my-account/
- Provisioned access for Iris Detect
- The ability to interact with the web interface and, if required, the REST API

Contact enterprisesupport@domaintools.com for assistance.

User Access

Your organization's administrators provision users with the following access tiers:

User Role	Access Type
Viewer	Read
Add to Watched	Add domain to watched
Escalate and Ignore (requires Add to Watched)	Escalate and ignore domains
Editor	Read Add to watched Escalate and ignore domains Edit Delete

The Dashboard

The Iris Detect web interface opens to the dashboard.

The Dashboard displays the monitor list, as well as links to domains with new, changed, or watched status (see Domain Groups, below).

Add and Edit Monitors

Adding and editing monitors is limited to users with editor access.

To add a monitor, begin by entering the keyword to monitor, such as a portion of its name, in the search bar. and Iris Detect will load the **Search and Evaluate** page.

Select **Refine Results** to see the options available to enhance the monitor's effectiveness.

Enabling **Match Variations** will include domains where variations of the term are substrings within matched domains. For example, the monitored term `domaintools` will match the domains `domaintools.com` and `account-domaint00ls.com`. Without

Match Variations enabled, the `domaintools` search would match `domaintools.com`, but not `account-domaint00ls.com`.

This is not recommended for terms of 6 characters or less, as it can create many false positives. The search results will update to indicate how your refinements impact the results.

Text Exclusions allow you to remove domains from the results that have a specific string within the domain name. For example, the monitor term "election" will include domains containing the word "selection". Adding "selection" as an exclusion will not include domains with this string. Using text exclusions can reduce false positives in the results.

Name Server Exclusions will exclude a domain, but only when all of the domain's nameservers are added. Exclusions can remove local infrastructure from the results. Wildcards (*) are accepted: for example, `*.domaintools.com` will catch `ns1.domaintools.com` and `ns2.domaintools.com`.

Select **Add Monitor** to save your monitor to your organization's dashboard, where it will be accessible to all other users in your organization.

To edit a monitor, select the Overflow Menu (three vertical dots) on the right side of the Monitor's row. Select **edit** to load the monitor's search criteria, and save.

Domain Groups

The Iris Detect web interface organizes domains into lists depending on whether they have been newly active, previously active, or are being watched for changes by your group.

From Monitor Dashboard, clicking on a monitor will navigate to the monitor's individual dashboard where all the organized lists are located in the top right.

From the Dashboard, select buttons on the navigation panel to view all New, Changed, or Watched domains. Counts for the individual monitor's main 3 lists are also available.

At the top of the group's dashboard there are counts for the main 3 lists for all monitors combined. Counts for the individual monitor's main 3 lists are also available.

Using the Iris Detect API, return domains from the specific lists as needed.

Domain Category	Description
New	New Domains are domains that have been newly detected by passive DNS in their current lifecycle. This list is populated as domains are discovered in near real-time.
Watched	Adding a domain to the monitor's watchlist will trigger DomainTools to watch for any infrastructure changes made to the domain. When a change occurs to the domain's infrastructure, it will move into the Changed list.
Changed	When a domain that is being watched experiences a change to its infrastructure it is moved into the changed list. Changed domains have experienced an infrastructure change in the last 3 days by default. Adjust the Changed Domains Timeframe in Settings.
Inactive	Domains being watched that have not been observed in DNS in the last 10 days.
Previous	Domains fitting the monitor's criteria that were active prior to creating the monitor.
Escalated	
Ignored	

Monitor Dashboard

Select a Monitor in the Dashboard to view more information about that monitor.

Domain Information

The following Domain information is displayed for each listed domain:

Domain Information category	Description
TLD (Top-Level Domain)	The Top Level Domain, or domain suffix.
Domain Risk Score	DomainTools' proprietary risk calculation. Consult the Iris Investigate User Guide, and the Domain Risk Score Technical Brief to learn more.
First Seen / Lifecycle First Seen	The date/time that DomainTools first observed the current life cycle of the domain in DNS. This may differ from the create date if the domain went through a period of inactivity before becoming active again.
IP Address	The Internet Protocol address(es) associated with the domain.
Registrar	The Domain Name Registrar that maintains the domain's current registration cycle.
Name Server(s)	Name servers associated with the domain.
Mail Server(s)	Mail servers associated with the domain.

View full domain information in Iris Investigate with the Export Menu. A subset of this information is available from the API.

Select a domain and open the domain in a card view with additional information:

Domain Info Panel	Description
Phishing	The predicted likelihood that a domain was registered with malicious, phishing-related intent, determined with machine learning. Consult the Iris Investigate User Guide, and the Domain Risk Score Technical Brief to learn more.
Malware	The predicted likelihood that a domain was registered with malicious, malware-related intent, determined with machine learning. Consult the Iris Investigate User Guide, and the Domain Risk Score Technical Brief to

	learn more.
Spam	The predicted likelihood that a domain was registered with malicious, spam-related intent, determined with machine learning. Consult the Iris Investigate User Guide, and the Domain Risk Score Technical Brief to learn more.
Proximity	The likelihood that a domain is part of an attack, determined by analyzing how closely it is connected to known-bad domains. Consult the Iris Investigate User Guide, and the Domain Risk Score Technical Brief to learn more.
Screenshot (most recent)	The most recent screenshot of the web page associated with the domain. Hover on the screenshot to display the date/time of capture.
Subdomains	A live and non-persistent list of subdomains, if any, observed with passive DNS. Not returned with Detect API queries.
Domain Change History	A sequential list of changes made to the domain's infrastructure, organized by data point. Tracked data points include: Emails, IP address, Mail server, Name server, Web content (i.e., screenshot), Other WHOIS data.

Domain Actions

Add to Watchlist

Once the domain is added to the monitor's watchlist, DomainTools will track the domain for infrastructure changes: hosting IP, MX (mail) records, NS (Name Server) records, registrar, registrant email, create date, and screenshot. If there are any changes made, the domain will also be shown in the Changed Domains list.

Mouseover the domain row to make action icons appear on the right side of the row. Select the star-shaped icon and Iris Detect will add the domain to your organization's shared watchlist. Access the watchlist for individual monitors or all monitors in both the web interface and the API. Consult the Export (Bulk Update) section below for more information on bulk updates.

Escalate

Mouseover the domain row to make action icons appear on the right side of the row. Select the lightning-shaped icon and choose to either:

- Submit to the Google Safe Browsing team for them to perform their own review of the domain. If Google deems the domain to be malicious it will be blocked in their Chrome browser. Safari and Firefox will also take actions to block the domain in accordance with Google's decision.
- Mark the domain as blocked in Iris Detect. Selecting Block will flag that domain for blocking. Then, if you choose to use the Detect API, you'd be able to programmatically make decisions on domains with the value "block" for the "tag" attribute.

Ignore

Mouseover the domain row to make action icons appear on the right side of the row. Mark the domain as ignored. Track ignored domains for each monitor in the Monitor Dashboard. Use the Iris Detect API to retrieve and act on ignored domains in your own infrastructure.

Export (Bulk Update)

From the Monitor Dashboard, select one or more domains, and the bar will populate with `Export` and `Update` menus.

Iris Investigate

Select `Iris Investigate` to open the selected domains as a new investigation in Iris Investigate.

Access Iris Investigate from the DomainTools panel on the right side of the web interface.

File Download

Select CSV or `STIX 2.0` to download the file in either format.

Highlight Latest Changes

Highlighting latest changes helps track changes over time, and alert to new 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.

By clicking on a domain in the list you will open up the card view.

A `Latest Changes` link appears at the top; select it to highlight the latest infrastructure changes for the domains. A solid blue box and right arrow for new values; a dashed blue box and left arrow for removed values; a solid blue box with left and right arrows for new screenshots.

For a more detailed history of infrastructure changes, visit the `History` tab in the card view.

Filter Domains

Select the `Filter Results` in the bar, and select filters on the column that appears to the left. These categories are explained in the Domain Information section, above. Filter by:

- Domain name
- Domain ID (described in the Iris Detect API section, below)
- Top-Level Domains (TLDs)
- Risk Score ranges
- MX records presence
- Escalations

Sort Domains

Select the Filter Results button in the navigation pane, and navigate to the bottom of the column that appears to the left. These categories are explained in the Domain Information section, above. Sort by the following categories:

- Risk Score
- First seen
- Last changed

Iris Detect API Integration

This section provides a short overview of the Iris Detect API endpoints. For a complete description of the API with usage examples, consult the API Reference or OpenAPI Specification.

An API key and password or HMAC authentication is required to access the Iris Detect API. Consult the Iris Detect API Reference for more information on login requirements.

Monitor IDs and Domain IDs

Iris Detect assigns a unique ID to each Monitor and domain. Use these IDs to denote Monitors or domains when interacting with the API. The API responds with full Monitor and domain names.

Each monitor can also display its API ID to help set up integration with Iris Detect API endpoints. To retrieve results from all monitors, stay within the 1/hour rate limit by querying all domains, rather than individual monitors. The API ID can be enabled in Settings.

Consult the Iris Detect API Reference or the OpenAPI Specification on SwaggerHub for more information.

Settings

Load the settings menu from the Product Menu on the side of the web interface.

Changed Domains Timeframe

Under **General**, edit the **Changed Domains Timeframe** to control the scope of the domains listed as changed.

Email Alert Configuration

Under **Alert Configuration**, set email updates for discovered domains. Set the frequency, level of detail, and other options.