



DomainTools App for Splunk and Splunk ES

Version 5, June 2024



DomainTools

- Overview..... 3
- What’s New..... 5
 - 5.0 Release Notes..... 5
- Quick Start Guide..... 6
 - App Installation..... 6
 - Configure the Base Search..... 6
 - Adding a DomainTools API Key..... 6
 - Enable Additional Saved Searches..... 6
 - Enrich, Investigate, and Alert..... 7
- Deployment Guide..... 7
 - Overview..... 7
 - Prerequisites..... 9
 - DomainTools App Bundle..... 9
 - API Keys..... 9
 - Firewall Rules..... 10
 - Splunk Credentials to Install App..... 10
 - Splunk Permissions to Operate App..... 10
 - Validating the App in Non-Production Environments..... 10
 - App Installation..... 10
 - Uninstalling Prior Versions..... 11
 - Splunk Cloud Deployment..... 11
 - On-Premise Installation..... 11
 - Installation Steps..... 12
 - Application Setup..... 14
 - Configuring Base Search Using the Pre-Configured Query..... 14
 - Configure Log Source..... 15
 - Managing API Connectivity..... 16
 - Configure Saved Searches..... 17
 - Further Configuration..... 18
 - Configuring the Base Search Using the Custom SPL..... 18
 - Pros and Cons Between Pre-Configured and Custom SPL for Base Search..... 19
 - Add Custom Fields for Notable Events..... 20
 - Enable Mass Enrichment..... 21
 - Enable Enrichment History..... 21
 - DomainTools Thresholds..... 21
 - Set Up Monitoring for Domains with Iris Tags..... 23
 - Adding Domains to the Allowlist..... 23

Configure Iris Detect.....	24
Configure DT Indexes.....	29
Key App Capabilities.....	29
Threat Intel Dashboard.....	29
Interacting With and Reading the Dashboard Panels.....	29
Reading the Splunk Timecharts.....	31
Extending DomainTools Commands Outside the App.....	31
Examples.....	33
Investigation Workflows.....	35
About Domain Profile.....	35
Domain Risk Scoring.....	36
Tags.....	36
Connected Infrastructure.....	36
Contact Information.....	37
Recent Events.....	37
Importing Domains from an Iris Investigation.....	38
Farsight DNSDB pDNS Searching.....	38
Investigate Domains Within Incident Review.....	40
Domain Monitoring Dashboard.....	40
Interacting With and Reading the Dashboard Panels.....	41
Historical Analysis of Enrichment Activity.....	43
Alerts for Splunk (without ES) with the dt_alerts Index.....	44
Troubleshooting & Known Issues.....	44
Enabling Logging.....	44
Checking the Status of Saved Searches.....	44
Appendix A: App Components.....	45
Table: Main Configuration Files, Stanzas, and Fields.....	45
Table: KV Store/Collection Names and Fields.....	51
Table: Key Macros for Enrichment.....	52
Table: Saved Search Names and Descriptions.....	54

Overview

The DomainTools App for Splunk provides direct access to DomainTools' industry-leading threat intelligence data, predictive risk scoring, and critical tactical attributes to gain situational awareness of malicious domains inside Splunk.

Customers who deploy the app in Splunk benefit from:

- A Threat Hunting Dashboard highlighting the risk profile of domains along with relevant activities from within your network to help drive threat hunting and incident response.
- Ability to surface network events related to the investigated domain from configured log sources for faster investigation.
- Guided Pivots (integrated in the Domain Profile page) that indicate data points of interest and import more domain indicators into Splunk when pivoting on that data point.
- Ad hoc investigation of domain indicators within Splunk, and seamless integration with [DomainTools Iris Investigate](#) to further your investigations.
- Investigate a domain's current and historical infrastructure with passive DNS using [Farsight DNSDB](#) Standard and Flexible search.
- Deeper investigation capabilities to discover, import, and further monitor potentially malicious domains using DomainTools investigation capabilities.
- Automated detection throughout the alerting lifecycle within Splunk, leveraging the power of DomainTools [Iris Investigate](#), [Farsight DNSDB](#), and [Iris Detect](#) in a single application context.
- Proactive monitoring of domain indicators and tags originating from DomainTools Iris Investigate and Iris Detect in a centralized location within Splunk.
- Simple user interface for easily managing a list of allowed domains to reduce false positives.
- At-a-glance operational dashboard keeps track of your API usage and allocation.

What's New

DomainTools App for Splunk 5.0 is the General Availability (GA) release of our app for Splunk, Splunk Enterprise, and Splunk Cloud.

5.0 Release Notes

New

- Send alerts sent to any SOAR platform with the new `dt_alerts` index
- New configurable *Risk Score Increase* alert from Iris Detect results.
- Log all domain enrichment values, and compare enrich values over time, using the new `dt_enrich_history` index.
- Track changes to Whois data with the `dtwhoishistory` custom search script
- Iris Investigate and Enrich API responses now include `website_title`, `first_seen` and `server_type`, as well as the SSL fields `ssl.alt_names`, `ssl.duration`, `ssl.common_name`, `ssl.issuer_common_name`, `ssl.not_after`, and `ssl.not_before`. These are available in the domain profile, enrichment explorer, and in Enrich and Investigate custom search commands.

Quick Start Guide

The following sections list the minimum steps to get started with Splunk in your environment. Links are provided to other areas in this document to help provide additional information or context if needed.

App Installation

The latest app is available on [Splunkbase](#). Please ensure the [prerequisites](#) are met. For Splunk Cloud deployments, [install the app](#) directly from Splunkbase. For on-prem distributed environments, deploy the DomainTools App to both indexer and search head cluster members using the standard process for [deploying apps and add-ons to clusters](#). See the [App Installation](#) section for more information.

Configure the Base Search

The base search is an SPL Query that allows users to define which log sources are to be monitored by the DomainTools App. It should output the required fields the DomainTools App uses to populate dashboards and enrich events. The app arrives with a pre-configured performance-optimized query. This query will work well in environments where data sources are Common Information Model (CIM) compliant.

To configure the base search, go to DT Settings → Configure Log Source. The required fields are: `url`, `src`, `dest`, `log_source`, `domain`, and `_time`. Consult [Configuring Base Search Using the Pre-Configured Query](#) for more information.

Adding a DomainTools API Key

Navigate to **DT Settings** → **API Keys** to enter your DomainTools API credentials. DomainTools API credentials are available from your organization's API administrator. Your Account Manager or DomainTools Enterprise Support (enterprisesupport@domaintools.com) can ensure your API key is appropriately provisioned.

Saving new API credentials will prompt you to enable default saved searches: "Would you like to enable the default set of Saved Searches?"

Enable Additional Saved Searches

Enable saved searches in **DT Settings** → **Configure Saved Searches**. Consult [Saved Search Names and Descriptions](#) for a description of the searches available.

Enrich, Investigate, and Alert

Once initial setup is completed, the DomainTools app will query the DomainTools Iris Enrich API with domains found in the configured base search. Please allow 10-15 minutes after configuration for the enrichment process to start populating the dashboards.

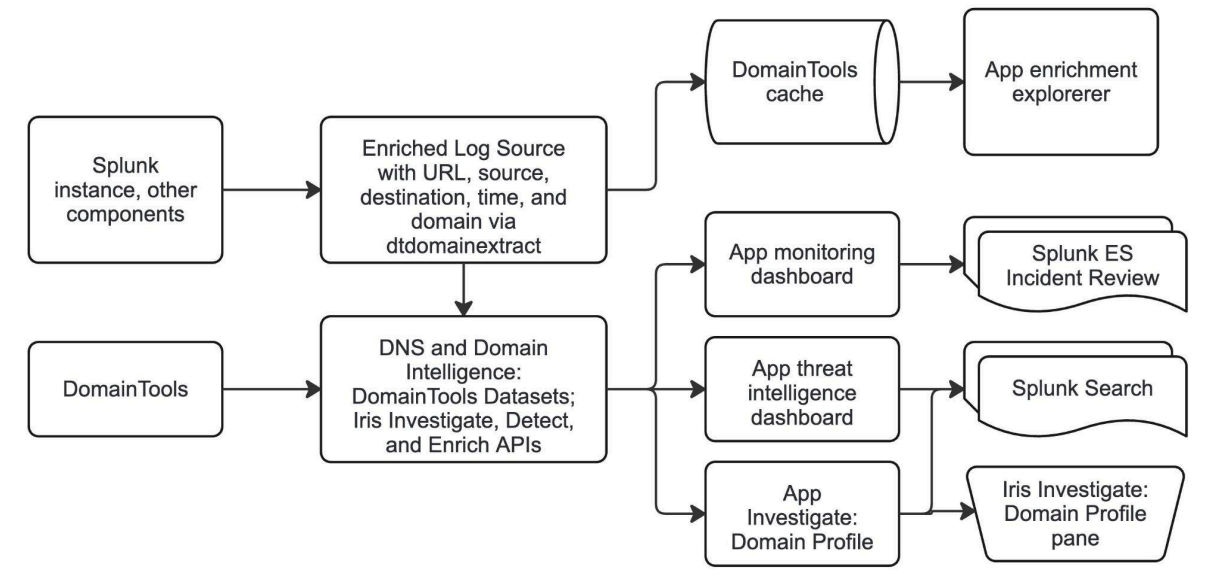
New events will be enriched every 5 minutes by default. The Threat Intelligence panel is a good starting place to see what the enrichment data looks like. See the [Key Capabilities](#) section for more information on monitoring, alerting, and using DomainTools data as part of other workflows.

If the Threat Intelligence Dashboard remains empty after the initial 10-15 minute wait period, you may wish to [enable logging](#), or see the [Troubleshooting & Known Issues](#) section for more information.

Deployment Guide

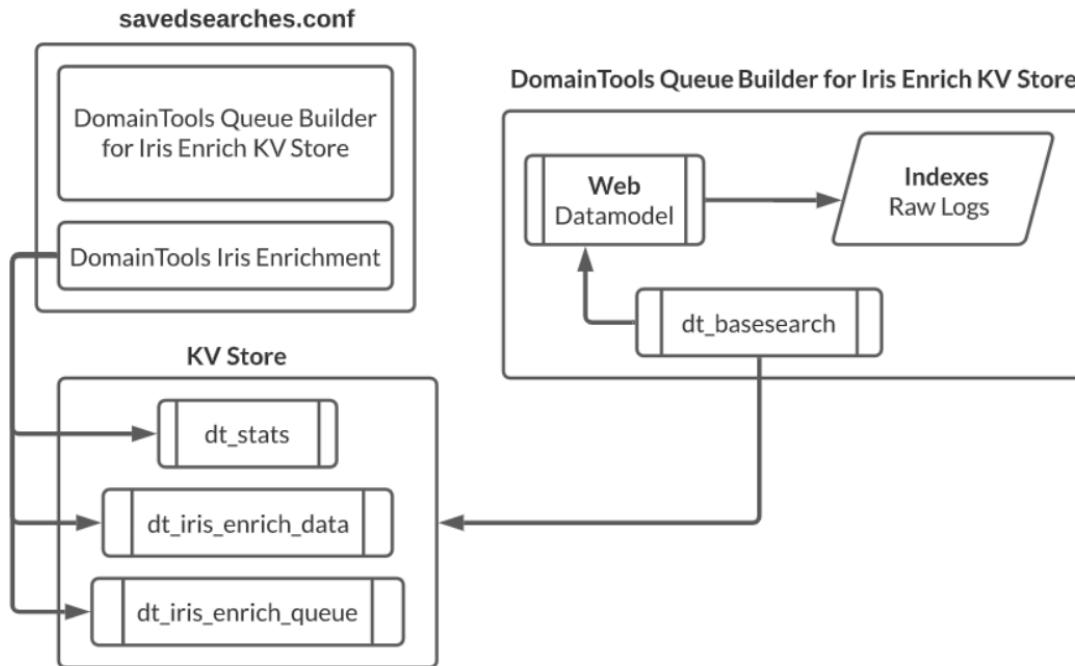
Overview

The following sections outline some background architecture and deployment information. [Appendix A](#) contains additional information on app components, including configuration files, stanzas and fields, KV store, macros, and saved searches.



High-level topology of both Splunk and DomainTools resources

The *Saved Searches* configuration file ([savedsearches.conf](#)) defines the processes for enrichment and the Queue Builder for the Iris Enrich KV store. In the Queue Builder process, raw logs in the Splunk Indexes are queried from the `web` data model as defined by the DomainTools base search configuration ([dt_basesearch](#)). This process includes checking to see if the domain already exists when comparing to existing Iris Enrich data, as that would indicate if the domain has already been enriched. If not, the new domain is queued for enrichment. Each domain is stored with the enriched data in the KV store.



Domain Enrichment Process between DomainTools and Splunk Indexes

Prerequisites

The DomainTools App works best with Splunk Enterprise Security (ES), which makes it easy for an analyst to set up alerts and triage new domain indicators. With Version 5 of the DomainTools App, users of Splunk (without Enterprise Security) can receive a wide range of customized alerts.

DomainTools App Bundle

The latest app is available on [Splunkbase](#).

API Keys

A DomainTools API username and API key is required to complete the app setup. DomainTools provides access to obtain API credentials by creating an account for the primary point of contact in your organization. If you wish to evaluate the app and need to obtain new API keys, contact us via email at enterprisesupport@domaintools.com. If you are an existing DomainTools customer, to ensure your DomainTools API key is appropriately provisioned, please contact your account manager.

For complete App functionality, your DomainTools API key should include access to the Iris Enrich API and Iris Investigate API. Limited app functionality is available for users without Iris Enrich API and Iris Investigate API access. Notably, management of Iris Investigate monitors, importing Iris Investigate and Detect terms, and ingesting Iris Investigate and Detect discoveries into Splunk will not be available.

Firewall Rules

Ensure you can reach <https://api.domaintools.com/> from the Splunk server. If required, update firewall rules to allow access to this endpoint for the app to be functional. If you are on a managed infrastructure and cannot connect to the DomainTools endpoint, please contact enterprisesupport@domaintools.com.

Splunk Credentials to Install App

A Splunk account with `admin` access is required to install and configure the app. After installation, most user functions should be available with less privileged accounts.

You may also need command-line access (e.g., SSH) to perform some deployment and diagnostics functions, especially if deploying in a clustered environment.

Splunk Permissions to Operate App

Ensure that the `list_storage_passwords` privilege is added to the user operating the app. The admin role may need to be used to access the password storage within Splunk.

Users within the DomainTools App must have read privileges to all the components of the app. If a user expects to add, update, or append values in any of the internal stores (ex. monitoring lists, or Iris Detect terms), their user profiles must include write privileges to the KV stores involved. For the list of KV stores and descriptions, please see the [App Components](#) Appendix.

Validating the App in Non-Production Environments

If you use a staging environment or development environment to test new Splunk apps, ensure the same data sources you plan to use in production are also available to the Splunk search heads in the test environment.

App Installation

The DomainTools App is designed to be installed on a search head or within a search head cluster. It has been tested with the recommended Splunk deployment model for apps in a clustered environment, including distributed configuration.

We encourage customers to follow Splunk guidelines to ensure a successful deployment. Please review the Splunk docs on app install and config in a clustered environment, including the page on [Distributed Search](#).

DomainTools provides support for apps deployed in this standard configuration model. Although it is possible to use an alternative method for deploying apps, such as a configuration management tool, those methods create scenarios that are unique to your environment. As such, DomainTools can provide only limited support for those deployments.

Uninstalling Prior Versions

If you are currently running a 3.x or 4.x version of the DomainTools app, we recommend uninstalling the older version first and performing a fresh installation when migrating to version 5.

For best results, use the Splunk web UI to uninstall any previous versions of the DomainTools App or TA (if using an older version). Use command-line access to completely remove any remaining DomainTools specific folders.

```
# from deployer
/opt/splunk/etc/apps/ $ rm -rf DomainTools-App-for-Splunk/
```

Splunk Cloud Deployment

The DomainTools app is vetted and available for Splunk Cloud. Please follow the instructions to [Install apps on your Splunk Cloud Platform deployment](#) to add or update it on your Splunk Cloud installation. The latest version of the DomainTools App can be found on [Splunkbase](#) (app ID 5226).

Once the app is installed, proceed to the [Application Setup](#) section.

Upgrade note for Splunk Cloud users: We have observed that users using the self-service app installation might run into issues installing the components of the app needed on indexers. The installation proceeds normally, but attempts to run `dtomainextract` return an error. This may be due to [Splunk self-service only installing apps on search heads](#). Please see the associated [known issue](#) and workarounds.

On-Premise Installation

For on-premise installation, first follow the instructions outlined here for Indexer Clusters: https://docs.splunk.com/Documentation/AddOns/released/Overview/Distributedinstall#Indexer_clusters

Installation Steps

1. Obtain the latest version of the DomainTools App from Splunkbase.
2. Identify the server with the deployer role.
3. Obtain admin and console access to the server, then ssh into the deployer server.
4. If performing a fresh Install, skip this step.
 - a. Remove the existing app bundle from the deployer.

```
# from deployer
```

```
/opt/splunk/etc/apps/ $ rm -rf DomainTools-App-for-Splunk/
```

5. scp tar file to deployer /tmp directory.

```
# from local
```

```
scp -i ~/.ssh/**.pem ./domaintools-App-for-splunk_xxx.tgz user@hostname:/tmp
```

6. Extract the app to the directory.

```
/tmp $ sudo tar -xvf domaintools-App-for-splunk_xxx.tgz -C /opt/splunk/etc/apps/  
$ sudo chown -R splunk:splunk /opt/splunk/etc/apps/DomainTools-App-for-Splunk/
```

7. Restart the app.

```
$ sudo /opt/splunk/bin/splunk restart
```

8. If performing a fresh Install, skip this step.
 - a. In the deployer, remove the app from /opt/splunk/etc/shcluster/apps

```
/opt/splunk/etc/shcluster/apps/ $ sudo rm -rf DomainTools-App-for-Splunk/
```

```
/opt/splunk/etc/shcluster/apps/ $ sudo cp -r  
/opt/splunk/etc/apps/DomainTools-App-for-Splunk/ ./
```

9. Ensure correct permissions are used.

```
$ sudo chown -R splunk:splunk
```

10. Then copy the new one from app/ dir

```
/opt/splunk/etc/shcluster/apps/DomainTools-App-for-Splunk/
```

11. Ensure to run the deploy command as a splunk user.

```
sudo su - splunk
```

12. Copy out the app to search clusters.

- a. The IP is the IP for one of the searchheads.
- b. Use admin credentials if it asks for them.
- c. Target is the private IP of any one of the search heads in the cluster.
- d. The admin password is the default (SPLUNK-<instanceid>) - instance-id of the deployer.

```
/opt/splunk/bin/splunk apply shcluster-bundle -target https://172.16.1.xxx:8089  
-auth <user>:<password>
```

13. Verify the app is deployed by SSH into one of the searchheads.

- a. Run a status check on the search head. See below for an example output.

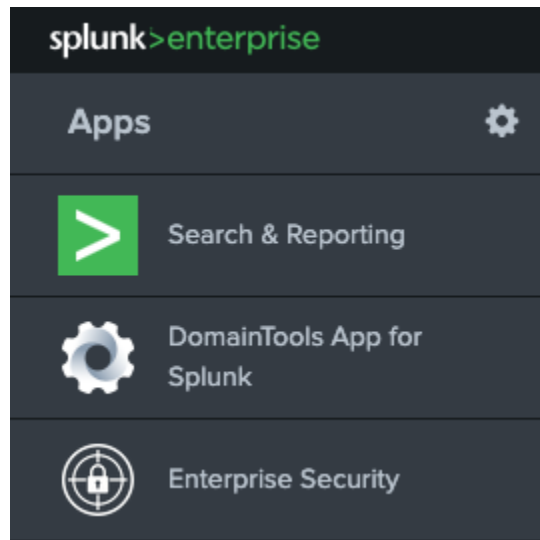
```
[splunk@ip-172-16-01-xxx ~]$ /opt/splunk/bin/splunk show shcluster-status  
Captain:
```

```
dynamic_captain : 1  
elected_captain : Wed Nov 20 15:56:03 2023  
id : D6327B1F-6898-477D-928E-xxx  
initialized_flag : 1  
label : ip-172-16-01-xxx  
mgmt_uri : https://hostname:8089  
min_peers_joined_flag : 1  
rolling_restart_flag : 0  
service_ready_flag : 1
```

Members:

```
ip-172-16-01-xxx  
  label : ip-172-16-01-xxx  
  mgmt_uri : https://hostname:8089  
  mgmt_uri_alias : https://172.16.1.xxx:8089  
  status : Up
```

14. Log in to your splunk instance and verify you can see the DomainTools app installed:



DomainTools App shown on a successful installation

Application Setup

This section covers the base items needed to get your DomainTools App for Splunk instance up and running.

Configuring Base Search Using the Pre-Configured Query

The app arrives with a pre-configured performance-optimized query. This query will work well in environments where data sources are Common Information Model (CIM) compliant.

First, identify relevant CIM-compliant data sources for ingestion. It may be data sources already configured to use web proxy events, for example. If your base search involves working with relevant data sources that are not CIM-compliant, please go to the [Configuring Base Search Using the Custom SPL](#) section.

To use the pre-configured query:

1. Go to DT Settings → Configure Log Source page.
2. Confirm the details of the pre-configured Splunk search query. The pre-configured base search made available in the app is:

The app natively supports logs with multivalued URLs contained in a single event entry, commonly seen in Proofpoint logs. Users who previously may have used `mvexpand url` to work around this issue can remove that command to have the URLs more accurately reported as a single event.

A regex-based `dtomainextract2` macro is available for high-throughput environments and can significantly increase performance of the URL-to-domain conversion with a slight trade-off in accuracy. Notably, some wildcard and exception TLDs (e.g. `*.np`, `!city.kawasaki.jp`) can be misidentified as a domain. Note that `mvexpand url` would still be needed with `dtomainextract2` in environments processing multivalued URLs. The updated base search would look like this:

```
tstats summariesonly=true count FROM datamodel=Web BY Web.url
Web.src Web.dest source _time | rename Web.url AS url | rename
Web.src AS src | rename Web.dest AS dest | rename source AS
log_source | mvexpand url | `dtomainextract2` | eval
domain=lower(domain) | fields url src dest log_source domain
_time
```

3. If needed, customize the preconfigured base search to ensure the required fields are available.
4. Select the Save button.
5. Select the Timeframe for the Base Search.

Base search requirements and recommendations:

- `domain` and `_time` are required output fields to operate the app.
- We recommend adding the optional fields `Source`, `Destination`, and `Log Source` in your base search. They provide additional contextual information on the events. The app will also not error out in the absence of these fields.

Performance considerations:

- The Web data model must have acceleration turned on.
- If acceleration is not turned on, yet data has been mapped to the CIM, you can modify the base search to use `summariesonly=false` with some potential degradation in performance.

If you already have the domains extracted out in the CIM, you can remove the `dtomainextract` function from your base search. This will further improve performance.

Configure Log Source

DomainTools extracts domain names from your data input sources that contain domain names - including proxy logs, DNS logs, SMTP server logs, and more.

To define a Base Search that is used across the app:

1. Go to **DT Settings** → **Configure Log Source**.
2. Add the Base Search. Please go to the following sections in this User Guide to read more:
 - a. [Configuring Base Search Using the Pre-Configured Query](#).
 - b. [Configuring Base Search Using the Custom SPL](#).

The app automatically validates the base search by retrieving events from your environment. It displays the following fields: **URL**, **Domain Name**, **_time**, and the optional fields **Source**, **Destination**, and **Log Source**. A successful run sample is below:

URL	Source	Destination	Log Source	Domain Name	_time
http://028Y4.KcFvVwH.9362388.com/	10.10.130.58	http://028Y4.KcFvVwH.9362388.com/	udp:5140	9362388.com	2020-09-25 13:00
http://04X8S.ZUJzJGJx.cleanindiagroup.in/	10.10.236.136	http://04X8S.ZUJzJGJx.cleanindiagroup.in/	udp:5140	cleanindiagroup.in	2020-09-25 13:00
http://070C1.gJsRKLgD.recordnotes.Live/	10.10.186.68	http://070C1.gJsRKLgD.recordnotes.Live/	udp:5140	recordnotes.Live	2020-09-25 13:00
http://0A7HA.rays.com/	10.10.227.8	http://0A7HA.rays.com/	udp:5140	rays.com	2020-09-25 13:00
http://0F073.nlgSEox0.9951026.cc/	10.10.177.119	http://0F073.nlgSEox0.9951026.cc/	udp:5140	9951026.cc	2020-09-25 13:00
http://0GKPG.MkRGGwZ.knull.info/	10.10.74.126	http://0GKPG.MkRGGwZ.knull.info/	udp:5140	knull.info	2020-09-25 13:00
http://0HQBM.FDaKsaIS.161555x.com/	10.10.253.26	http://0HQBM.FDaKsaIS.161555x.com/	udp:5140	161555x.com	2020-09-25 13:00
http://0KNJ7.IRebrBWX.jny68.com/	10.10.77.176	http://0KNJ7.IRebrBWX.jny68.com/	udp:5140	jny68.com	2020-09-25 13:00
http://0NN0M.akamai.agency/	10.10.128.97	http://0NN0M.akamai.agency/	udp:5140	akamai.agency	2020-09-25 13:00
http://0NYON.btzpgf.cn/	10.10.150.223	http://0NYON.btzpgf.cn/	udp:5140	btzpgf.cn	2020-09-25 13:00

An example of a successful base search test run. Note the parsed domain name

Managing API Connectivity

Adding and Testing API Connectivity

1. Navigate to **DT Settings** → **API Keys**.
2. Enter your DomainTools API Username and API Key
3. Optionally enter a Farsight API key, if enabled. It enables the Farsight Flexible and Standard pDNS search options, as well as the in-line DNSDB enrichment.
4. Click the Test Connection button to validate the connection(s).
5. Once validated, **Update** to save the settings. A successful test will show the API licenses associated with the API username along with additional information.

Adding Proxy Configuration

1. Configure proxy configuration and proxy credential support in the same API Key section.
2. Select **Enable Proxy**.
3. Add the **Proxy Server** and **Proxy Port**.
4. If required, select **Enable Proxy Authentication**, and add the proxy credentials on the Proxy Username and Proxy Password fields.

Adding SSL

1. Configure **SSL details** in the same API Key section.
2. Select **Enable Custom SSL Certificate** and add the path in the **Custom SSL Certificate Path** field.

API Keys

Allows you to manage your DomainTools API Key and validate connectivity with DomainTools, and optionally Farsight.

DomainTools API Credentials (Required)

DomainTools API Username:

DomainTools API Key:

Farsight API Credentials (Optional)

Farsight API Key:

<p>Proxy ⓘ</p> <p><input type="checkbox"/> Enable Proxy</p> <p>Proxy Server: <input type="text"/></p> <p>Proxy Port: <input type="text"/></p>	<p>Proxy Authentication</p> <p><input type="checkbox"/> Enable Proxy Authentication</p> <p>Proxy Username: <input type="text"/></p> <p>Proxy Password: <input type="password"/></p>
---	---

SSL

Enable Custom SSL Certificate

Custom SSL Certificate Path:

[Test Connection/View Account Information](#) [Update](#)

The API Key dashboard

Configure Saved Searches

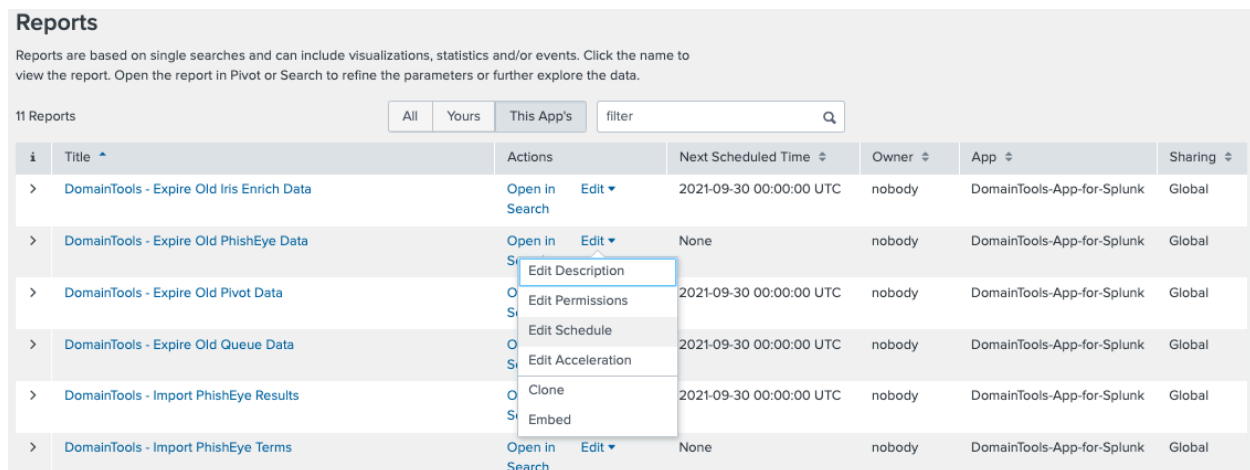
Saved Searches automate some operational tasks within Splunk. The full list of saved searches can be found in the [Saved Search Names and Descriptions](#) table in Appendix A.

Upon clicking Test Connection after entering your API key above, if the "Queue Builder for Iris Enrich KV Store" saved search is disabled, you will be prompted to enable the default set of saved searches. Selecting enable will turn on the set of seven minimum required saved searches for the Core App functionality noted in the saved searches [table](#).

To enable Iris Investigate and Detect capabilities or alerting in Splunk Enterprise Security, you will need to enable additional saved searches outlined in the [table](#).

To manage saved searches, select the **DT Settings** menu in the app, and select **Configure Saved Searches** to load the list of saved searches used by the DomainTools app.

To enable a Saved Search, select **Edit**, and select **Edit Schedule**.



Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

11 Reports

i	Title ^	Actions	Next Scheduled Time ↕	Owner ↕	App ↕	Sharing ↕
>	DomainTools - Expire Old Iris Enrich Data	Open in Search Edit ▼	2021-09-30 00:00:00 UTC	nobody	DomainTools-App-for-Splunk	Global
>	DomainTools - Expire Old PhishEye Data	Open in Search Edit ▼	None	nobody	DomainTools-App-for-Splunk	Global
>	DomainTools - Expire Old Pivot Data	Open in Search Edit ▼ Edit Description Edit Permissions Edit Schedule Edit Acceleration	2021-09-30 00:00:00 UTC	nobody	DomainTools-App-for-Splunk	Global
>	DomainTools - Expire Old Queue Data	Open in Search Edit ▼	2021-09-30 00:00:00 UTC	nobody	DomainTools-App-for-Splunk	Global
>	DomainTools - Import PhishEye Results	Open in Search Edit ▼ Clone Embed	2021-09-30 00:00:00 UTC	nobody	DomainTools-App-for-Splunk	Global
>	DomainTools - Import PhishEye Terms	Open in Search Edit ▼	None	nobody	DomainTools-App-for-Splunk	Global

Confirm the schedule, and enable the Saved Search by selecting **Save**.

Further Configuration

The above sections describe the minimum steps required to get started. The following sections go into additional detail to help configure the application to provide the most value in your environment.

Configuring the Base Search Using the Custom SPL

Configuring Base Search using your own custom Search Processing Language query (SPL) may be necessary if data is not yet CIM compliant, or input data sources are from ingested data from several different sources.

First, identify relevant data sources for ingestion. It may contain URLs or hostnames, in addition to domain names. IP addresses are not supported for processing with this app.

The DomainTools solution provides data on domain names, not IPs, subdomains, or full URLs. IPs sent to the Iris APIs will not return useful data and consume rate-limited resources. Querying a URL will result in inconsistent results. The default base search converts URLs to apex domains for the enrichment.

To configure using custom SPL:

1. Craft the Splunk search query that efficiently finds events from your preferred data source(s).
 - a. It is not necessary (or effective) to write regular expressions or other parsing rules to extract domains in logs filled with hostnames or URLs or de-duplicate logs. This task is handled by DomainTools queue builder search jobs.
 - b. We recommend using `tstats`. It is also used in the pre-configured base search for optimization.
 - i. If the default `tstats` base search is not used, there is a known issue in clustered SH environments for both Splunk 7.x and Splunk 8.x; consult the [Workaround and Known Issue](#) section.
2. Add the query as the base search via DT Settings → Configure Log Source page.
3. Add the query in the Base Search input field.
4. Click the Save button.

Your custom SPL must meet these criteria:

- If your custom search does not begin `tstats` you must add `search` to ensure proper functionality once it is merged into the DomainTools scheduled searches.
- Must not start with a pipe `|` character.
- Ensure the result contains a field named `domain` or use `rename` function.
- The search must efficiently return results from the last 10 minutes of events. Ideally in a few seconds, but no longer than two or three minutes.

Example:

```
search index=mycustomindex | rename url AS domain
```

The query should be performant in your environment. At a minimum, the query should return ten minutes of events in no more than two minutes of search execution time, with minimal impact on your search head or search head cluster.

Pros and Cons Between Pre-Configured and Custom SPL for Base Search

Ensure to select the correct base search method for your environment before proceeding with the installation. The following table lists the tradeoffs between the two methods.

Base Search	Pros	Cons
Pre-Configured	<ol style="list-style-type: none"> 1. No post-install customization or configuration required, other than the API username and key initial app setup. 2. Finds domain names in every CIM-compliant data source from the Web data model. 3. Fast for most environments. 	<ol style="list-style-type: none"> 1. Requires CIM compliant data sources that use the Web data model with hostnames in the Web.url field. 2. DomainTools Threat Hunting Dashboard will be empty if the base search can't find domains. 3. Must have acceleration turned on for the Web data model.
Custom SPL	<ol style="list-style-type: none"> 1. Does not require your data source to be CIM compliant. 2. Can be optimized to your environment and data sources. 	<ol style="list-style-type: none"> 1. May cause performance problems if the search is not manually optimized. 2. May require additional tuning after installation, making this option unsuitable for rigorous change management cycles. 3. Must return the hostname or domain name in a field explicitly named domain.

Add Custom Fields for Notable Events

This section only applies to Splunk Enterprise Security (ES) *Notable Events*, which are events generated by DomainTools detection rules. Users of Splunk (without ES) can generate notifications with the `dt_alerts` index.

To ensure that Notable Events provide context for triaging, we have extended some of the key enrichment fields already available from DomainTools into Splunk Enterprise Security.

Add the following fields and labels during the initial setup within your Enterprise Security module:

Enrichment Field Name	Label
<code>dt_num_of_times_enriched</code>	Enrichment Count

dt_looyn_date	Last Seen
log_source	Log Source
dt_age	Domain Age
en_threat_profile_type	DomainTools Threat Profile
dt_is_active	Domain Status
en_risk_score	Risk Score
domain	Domain

Once created, the notable events will automatically display these fields. There is no programmatic way to provision these fields during app deployment. For detailed steps to add custom fields, please refer to this [Splunk documentation](#).

Enable Mass Enrichment

We recommend leaving the current settings as a default. Visit **DT Settings** → **Configure Enrichment and Alerting** to change these settings.

The **Queue Wait Time** is how often the app enriches Domain information, and defaults to 5 minutes.. Decreasing the frequency can be helpful to reduce API usage or if the enrichment is taking longer than 5 minutes to run on a higher volume Splunk cluster.

The **Cache Settings** is the cache DomainTools maintains to reduce API query usage. Disable or reduce the cache retention times (for example, when monitoring volatile domains) in **Cache Settings**:

- DomainTools maintains a cache to reduce API query usage. A user may wish to disable or reduce the cache retention period times when monitoring volatile domains.
- **Enable Cache** - Enabled by default to optimize API consumption. Disable the cache to monitor for changes < 1 day old. (CAUTION: this can result in high API consumption)
- Add the **Cache Retention Period** - Sets how long domain enrichment should live in the cache before being re-queried. 30 days is the default.

Enable Enrichment History

The DomainTools App supports enrichment history with the custom `dt_enrich_history` index. This index stores all enrich values for all domains. When a domain is re-enriched, this index records the new values. The

index can be used to compare changes in values across whois info, IPs, SSL fields, risk scores, and other indicators. Indexes including `dt_enrich_history` can be created and configured in [Configure DT Indexes](#).

DomainTools Thresholds

This section defines thresholds used in creating dashboard KPIs and alerts (if enabled) throughout the app.

- Risk Score Threshold (default value of 75) - DomainTools Risk Score used when defining a "suspicious" domain in dashboard KPIs and creating alerts (if enabled) throughout the app. See the [Domain Risk Scoring](#) section for more information on DomainTools Risk Score.
- Young Domain Age (default value of 7 days)
 - Newly registered domains are often an indicator of interest. Specify the age threshold in days for a domain to be included in dashboards and optionally alerting.
- Guided Pivot Threshold (default value of 500)
 - When a small set of domains share an attribute (e.g. registrar), that can often be pivoted on in order to find other similar domains of interest. DomainTools tracks how many domains share each attribute and can highlight it for further investigation when the number of domains is beneath the set threshold.
- High Risk Threshold (default value of 90)
 - Used by the Risky Observed Domains graph on the [Threat Intelligence Dashboard](#). This sets the minimum DomainTools Risk Score threshold for flagging a domain as High Risk for this graph. Higher risk scores indicate riskier domains.
- Medium Risk Threshold (default value of 70)
 - Used by the Risky Observed Domains graph on the [Threat Intelligence Dashboard](#). This sets the minimum DomainTools Risk Score threshold for flagging a domain as Medium Risk for this graph. Higher risk scores indicate riskier domains.

Alert Settings for Splunk Enterprise Security (ES)

To generate notable events and enable alerts with Splunk Enterprise Security:

1. Select the **Create Notable Event** checkbox under the **Alert Settings** section.
2. Select or deselect relevant alert criteria in the **Monitor Domains**, **Monitor Young Domain**, **Monitor Risk Score Increase**, and **Iris Detect** panels. When multiple criteria are selected, they narrow down the alert generation rule. In other words, they form a logical 'AND' narrowing.
 - a. **Only Monitor Domains in the DomainTools Monitoring list (default)**: an alert will only fire against domains that have been added to the [monitoring list](#).
 - b. **Exceeds Domains Risk Score Threshold**: Only alert if the domain exceeds the risk threshold defined above.

- c. **Exceeds Domain Threat Profile Score Threshold:** Only alert if the domain exceeds the threat profile threshold defined above.
 - d. **Ignore Iris Detect Domains in DomainTools Monitoring list:** ignores anything in the monitoring list where the Source equals "Iris Detect".
 - e. **Monitor DomainTools Iris Tags in Tag Monitoring List:** The app will monitor any domains that are tagged in DomainTools Iris investigation platform. Selecting this option will alert you when new domains are observed in your environment that match any Iris tags that have been specified on the Monitoring Tags page.
 - f. **Select the Urgency Tag to associate with the Notable Event:** applies the specified urgency level within Splunk Enterprise Security's Incident Review panel.
3. **Monitor young domains** - creates a notable event whenever a young domain (lower than the young domain threshold) is observed. Optionally restricted to new domains on the [monitoring list](#). This is useful in conjunction with Iris Investigate monitors that can keep track of newly registered domains. Similarly, select the separate **Urgency Tag** to associate with the "young domains" Notable Event will apply the specified urgency level within Splunk Enterprise Security's Incident Review panel.

Alert Settings in Splunk (without Enterprise Security)

Alerting is supported in Splunk (without Enterprise Security) with indexes. Consult the [Create DT Indexes](#) section for more information.

Set Up Monitoring for Domains with Iris Tags

If you use the [Iris investigation platform](#) for domain investigations, you can monitor for domains that are associated with tags your team has applied within Iris, optionally alerting when a tagged domain is observed in Splunk.

Manage Monitored Tags

The App will monitor any domains that are tagged in DomainTools Iris investigation platform. You can add those Iris tags in this list for monitoring within Splunk.

Add Tags ⓘ Remove Tags

Saved Successfully!

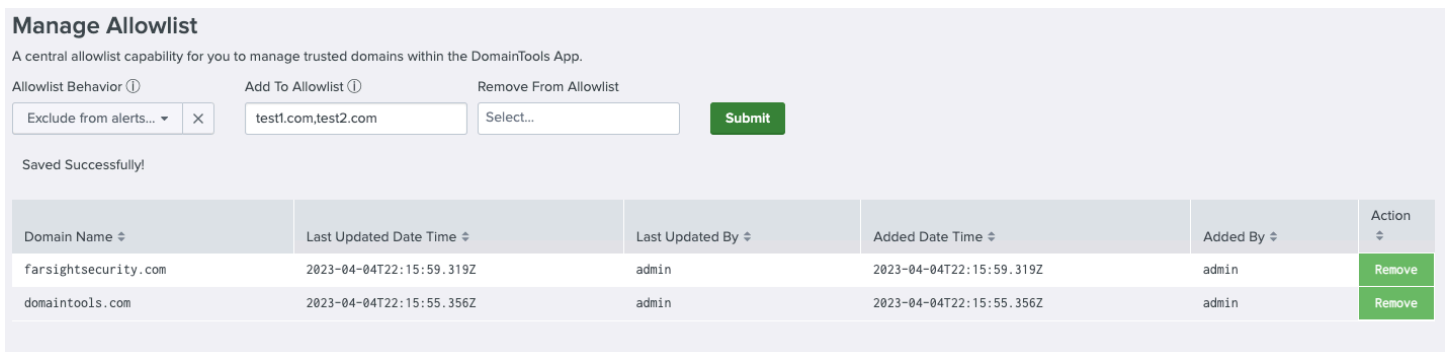
Tag Being Monitored ⇅	Last Updated Date Time ⇅	Last Updated By ⇅	Added Date Time ⇅	Added By ⇅	Action ⇅
suspicious	2023-04-04T22:14:36.726Z	admin	2023-04-04T22:14:36.726Z	admin	<input type="button" value="Remove"/>
delivery	2023-04-04T22:14:33.770Z	admin	2023-04-04T22:14:33.770Z	admin	<input type="button" value="Remove"/>
c2c	2023-04-04T22:14:31.147Z	admin	2023-04-04T22:14:31.147Z	admin	<input type="button" value="Remove"/>

The Manage Monitored Tags page with examples of Tags being monitored

To monitor for Iris-tagged domains in Splunk, visit **Monitoring** → **Manage Monitored Tags** to add tags to be added to the proactive monitoring list. Once tags are added, domains that share the same tag in Iris are monitored in Splunk.

Adding Domains to the Allowlist

Add your list of trusted domains, within your security operations workflow, to help reduce noise and false positives when creating alerts based on domain monitoring.



Manage Allowlist
A central allowlist capability for you to manage trusted domains within the DomainTools App.

Allowlist Behavior ⓘ Add To Allowlist ⓘ Remove From Allowlist

Exclude from alerts... ✕ test1.com,test2.com Select... **Submit**

Saved Successfully!

Domain Name ⇅	Last Updated Date Time ⇅	Last Updated By ⇅	Added Date Time ⇅	Added By ⇅	Action ⇅
farsightsecurity.com	2023-04-04T22:15:59.319Z	admin	2023-04-04T22:15:59.319Z	admin	Remove
domaintools.com	2023-04-04T22:15:55.356Z	admin	2023-04-04T22:15:55.356Z	admin	Remove

Screenshot of the Manage Allowlist page

To add or remove domains in the Allowlist, visit **Monitoring** → **Manage Allowlist** and select the allowlist behavior:

1. **Exclude from alerts and dashboards** (default): Domains in the allowlist won't be counted towards dashboard visuals, or alerts, if configured
2. **Exclude from alerts**: Domains won't be alerted on (applies to users of Splunk Enterprise Security only), but will still appear in dashboard visuals
3. **Exclude from dashboards**: Domains won't appear in dashboard visuals but will still appear in alerts (applies to users of Splunk Enterprise Security only).
4. **Exclude from all enrichment**: Fully ignores the domain in all enrichment, alerts, and visuals
5. **Do Nothing**: Allowlist is informational-only. Domains remain enriched, alerted upon, and appear in dashboard visuals. This setting can be helpful for temporary use when debugging.

Successfully added domains will show in the Allowlist along with Domain Name, Last Updated Date Time, Last Updated By, Added Date Time, Added By, and Action.

Configure Iris Detect

The Iris Detect Splunk integration allows you to triage new domains matching Iris Detect Monitors within Splunk, and synchronize the Iris Detect Watch List with the Splunk Monitoring list to watch for new domain activity within your environment.

To configure Iris Detect within Splunk, first ensure your API key is provisioned for Iris Detect. Visit **DT Settings** → **API Keys**, select **Test Connection**, and it will list **Iris Detect APIs**.

The DomainTools App requires the following APIs for base product functionality:

- `iris-enrich`
- `iris-investigate`
- `iris-detect-monitors`: required for read-only access to the configured monitored Iris Detect terms within Splunk.
- `iris-detect-new-domains`: required for read-only access to the new domains matching monitored terms within Splunk.
- `iris-detect-watched-domains`: read-only access required to access the list of domains marked as “watched” in Iris Detect and pull updates to that list. Optionally, synchronize those domains with the Splunk Monitoring List.

Optionally enable:

- `iris-detect-manage-watchlist-domains`: useful for triaging domains, adding to the Iris Detect Watchlist to track changes to domain infrastructure over time.
- `iris-detect-escalate-domains`: used to enable additions to the blocklist and submissions to Google Safe Browsing.

Iris Detect functionality will work without the optional permissions but a user will receive an error if they attempt to watch, block, escalate or ignore a domain within the Iris Detect Results panel.

To configure Iris Detect monitors on the Iris Detect page (**Monitoring** → **Iris Detect**), first make sure that the `DomainTools - Import Iris Detect Monitors` and `DomainTools - Import Iris Detect Results` saved searches are enabled (**DT Settings** → **Configure Saved Searches**).

An Iris Detect Monitored Term (also referred to as “terms”) refers to the series of characters being searched against new domain observations. A term is the basis for an Iris Detect Monitor. In the screenshot above, the monitored term is “bank”. It is frequently used as a company or brand name. Adding and editing monitors can currently only be done within the [Iris Detect UI](#).

Import new Iris Detect Monitored Terms

Refresh the list of monitored terms in one of two ways:

1. Select the **Refresh Now** button on the **Iris Detect Monitored Terms** page to import any new terms.
2. Under **DT Settings** → **Configured Saved Searches** assign an update frequency on the **DomainTools - Import Iris Detect Monitors** saved search to sync daily or weekly.

Reading the Iris Detect Monitored Terms Table

In the **Monitoring** → **Iris Detect Monitored Terms** pane:

- **Term:** The term itself as it appears in Iris Detect. Adding and editing monitored terms can currently only be done within the [Iris Detect UI](#).
- **Monitor Last Updated In Splunk:** The date as to when the monitor was refreshed, either manually or via the Daily or Weekly detections. Click “Refresh Now” to force a manual refresh.
- **Ingest Daily Detections in Splunk:** Select the term(s) to ingest Iris Detect-monitored domains into Splunk so they show up on the **Monitoring** → **Iris Detect** Dashboard page.

Import new Iris Detect Results

The Iris Detect Dashboard contains the list of new or changed domains matching the enabled monitored terms. The Iris Detect API allows up to hourly synchronization.

Synchronize Iris Detect results in one of two ways:

1. Select the Refresh Iris Detect Results button on the Iris Detect Dashboard to manually import new domains.
2. Under **DT Settings** → **Configured Saved Searches** assign an update frequency on the **DomainTools - Import Iris Detect Results**. The default schedule is every 2 hours. Note that the DomainTools Iris Detect API is limited to an hourly refresh frequency.

Reading the Iris Detect Results

The **Monitored Term** filter at the top of the page displays the results for all monitors or a selected monitor. The **Time Range Filter** filters for updates within a specified time period. The **Type filter** tab at the top of the results page allows you to select between **New domains** matching the enabled search terms, or **Watched domains** (domains that have been added to your account’s Iris Detect Watch List) matching the selected terms, or the list of Ignored domains in case of erroneously triaging a domain to the wrong queue.

Time Range: Last 1 Day | Monitored Term: All | Type: New | Automatic Sync: Disabled

Sync Splunk Monitoring List and Iris Detect Watch List | Refresh Iris Detect Results

Domain	Act	Monitored Term	TLD	Country Code	ISP	Risk Score	Risk Score Status	First Seen	Last Updated	Registrar Name	IP Address	Name Server	Mail Server
eastwestbankportal.com	⚙️	bank	com			5	provisional	2023-03-29 16:40:07	2023-03-29 16:41:25				
expresspowerbanks.de	⚙️	bank	de	de gb	1&1 IONOS SE Rackspace Ltd.	13	provisional	2023-03-29 16:36:18	2023-03-29 16:36:18		217.160.0.104 78.136.60.248	ns1081.ui-dns.de ns1020.ui-dns.com ns1028.ui-dns.org ns1099.ui-dns.biz	mx00.kundenserver.de mx01.kundenserver.de
bank588.cn	⚙️	bank	cn	hk	Alicloud-hk	7	provisional	2023-03-29 16:36:06	2023-03-29 16:36:06	阿里云计算有限公司 (万网)	47.91.170.222	dns4.hichina.com dns3.hichina.com	
isbankasi-turkiye.com	⚙️	bank	com			96	provisional	2023-03-29 16:33:40	2023-03-29 16:34:54				
testbankf1.com	⚙️	bank	com	us	Confluence Networks Inc			2023-03-29 16:33:31	2023-03-29 16:31:31	NETWORK SOLUTIONS, LLC	208.91.197.132	ns1.pendingrenewaldeletion.com ns2.pendingrenewaldeletion.com	mail.b-io.co
marketbank.com.br	⚙️	bank	com.br			39	provisional	2023-03-29 16:30:20	2023-03-29 16:34:14			a.auto.dns.br b.auto.dns.br	

< Prev 1 2 3 4 5 ... 21 Next >

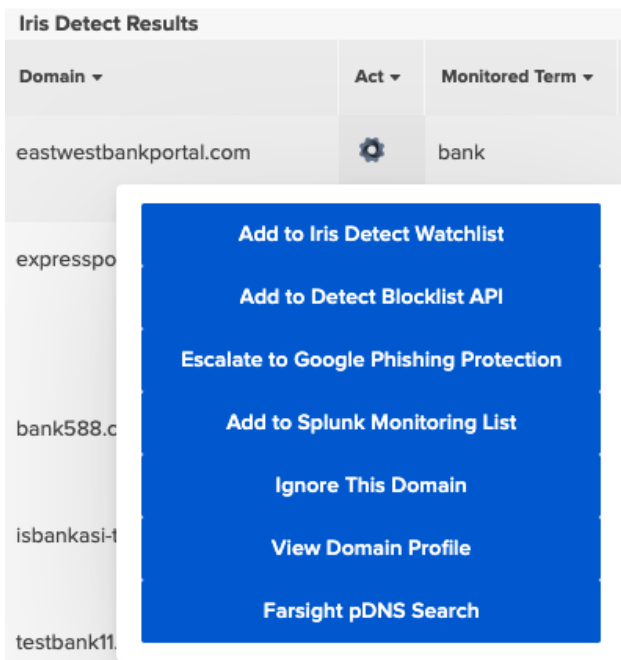
Example showing the Iris Detect Results pane

When new domains are discovered for the Enabled Monitors Terms, they are added in the results table with these fields. Click on a field heading to sort:

- **Domain:** The full domain name including TLD.
- **TLD:** The top-level domain for the selected domain.
- **Country Code:** The country code where the domain is registered.
- **ISP:** the Internet Service Provider associated with the IP address used by the domain.
- **Registrar Name:** The name of the registrar.
- **Risk Score:** The DomainTools Risk Score. See the [Domain Risk Scoring](#) section for more information on Risk Score.
- **Risk Score Status:** The risk score status indicates whether the scoring is provisional or full. Newly discovered domains will have only initial proximity or phishing scores and the score is designated as provisional. After 24-36 hours, a full risk score is calculated and adds malware and spam scoring values. At that point, the score becomes “full”.
- **First Seen/Lifecycle First Seen:** the date and time that DomainTools learned that a domain is likely active (or reactivated after going inactive).
- **Last Updated:** The date Iris Detect last observed any changes to the DNS or Whois attributes associated with the domain.
- **IP Address:** The numerical address that the domain name resolves to.
- **Name Server:** The server that translates a domain name into its numerical IP address.
- **Mail Server:** The server that handles emails sent to the domain.

The **Act Column** in **Iris Detect Results** helps triage discovered domains with the following actions:

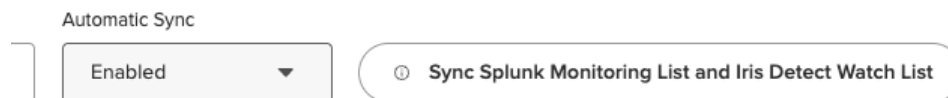
- **Add to the Iris Detect Watchlist:** Adds the listed domain to the Iris Detect Watchlist, which provides alerts on changes to these domains if hosting infrastructure or webpage changes are seen. This gives you the ability to track evolving threat campaigns, classify, and identify which domains are most likely to do harm. Such domains are candidates for escalation. The Iris Detect Watchlist can optionally be synchronized with the Splunk Monitoring list.
- **Add to the Detect Blocklist API:** Marks the domain for blocking. Useful for internal network defense infrastructure. The blocking designation is transmitted through the [Iris Detect APIs](#).
- **Escalate to Google Phishing Protection:** 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 Safari and Firefox.
- **Add to the Splunk Monitoring List:** Adds the listed domain to the [Monitored Domains List](#) within the DomainTools Splunk App. This can enable detection and alerting if the domain is seen within your monitored log sources.
- **Ignore This Domain:** If a domain is obviously a false positive, Ignoring the domain removes it from the “new” list on the next refresh. Watched Domains can be ignored if they are no longer of interest for change tracking.
- **View Domain Profile:** Load the [Domain Profile](#) page within Splunk, pulling up the Iris Investigate results for the listed domain.
- **Farsight pDNS Search:** Run a Farsight pDNS Standard Search (if provisioned) in DNSDB for RRNames containing the listed domain. This is useful for finding any active subdomains as well as seeing the dates when a domain has been active based on DNS traffic observed on Farsight’s Security Information Exchange (SIE).



See the [Iris Detect User Guide](#) for more information.

Alerting on Iris Detect Monitors

The DomainTools App for Splunk supports additional monitoring and alerting against domains in the Monitoring List. See [Set Up Monitoring for Domains](#) for more information. Synchronize the Iris Detect Watch List with the Monitored Domains List under **Monitoring Managed Monitored Domains:**



Synchronize the Splunk Monitoring with the Iris Detect Watch List either automatically or on a one-time basis to enable further enrichment and alerting

Selecting the option for Automatic Sync will add and remove **watched domains on an automatic schedule** based on the **Sync Iris Detect Watchlist** saved search. The default schedule is every day. **Sync Splunk Monitoring List and Iris Detect Watch List** will perform the sync on a one-time basis.

This option is also available under the **Monitoring** → **Manage Monitored Domains** page, where **Sync with Iris Detect Monitoring List** means that Automatic Sync will be enabled (both pages mirror the same setting).

Consult the [Set up Monitoring](#) section for more details and to set up alerting against monitored domains.

Configure DT Indexes

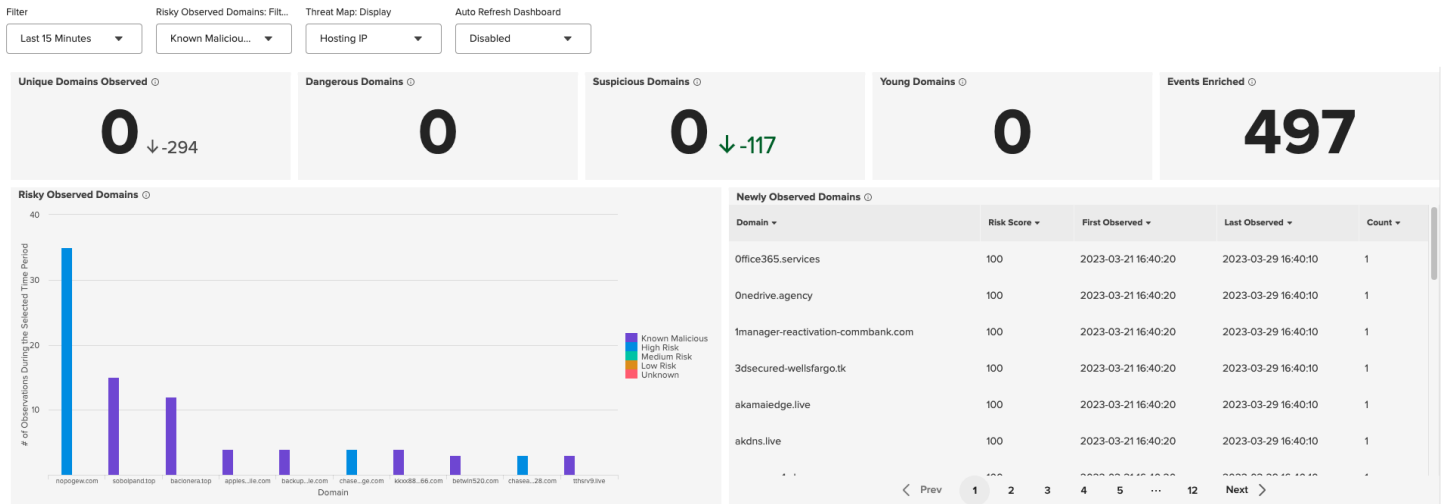
Both the **dt_alerts** and **dt_enrich_history** are built from Splunk indexes, and must be created. To create a Splunk index, consult the Splunk documentation on [Creating Event Indexes](#).

Key App Capabilities

Threat Intel Dashboard

The Threat Intelligence Dashboard is designed to help organizations gain quick situational awareness of the risk presented by domain names on their network. The dashboard also helps guide teams to effectively leverage DomainTools data in their SOC workflows, with drill-downs that expose the underlying events.

Keep the dashboard and current with the latest information open on an always-on tab or dedicated display, turning on the Auto Refresh. Panels will refresh individually at 5-minute intervals.



The Threat Intelligence Dashboard with Unique Domains Observed, Dangerous Domains, Suspicious Domains, Young Domains, Events Enriched, Risky Domains and Newly Observed Domains panels

Interacting With and Reading the Dashboard Panels

The Threat Profile dashboard panels provide insights based on Splunk Timecharts (consult [Reading the Splunk Time Charts](#) for more information).

- **Unique Domains Observed:** Number of unique domains observed in your network currently being monitored within the DomainTools cache for the selected time period, compared to the previous time period.
- **Dangerous Domains:** Uses a combination of the suspicious Risk Score threshold being exceeded, threat profile threshold being exceeded, and domain age being younger than the set threshold to determine a domain's likelihood to be dangerous. Thresholds can be configured on the Enrichment & Alerting settings page. The displayed value indicates the number of domains observed in the selected time period compared to the previous time period.
- **Suspicious Domains:** Number of Domains with a DomainTools risk score higher than the configured Suspicious Risk Score threshold on the Enrichment & Alerting settings page. The displayed value indicates the number of domains observed in the selected time period compared to the previous time period.
- **Young Domains:** Number of Domains observed which were recently created, based on the number of days set on the Enrichment & Alerting settings page. The displayed value indicates the number of domains observed in the selected time period compared to the previous time period.
- **Events Enriched:** Displays the total number of Events associated with Domains enriched by DomainTools during the selected time period.

The following panels provide additional information either as a graph or paginated results:

- **Risky Observed Domains**
 - See the [Domain Risk Scoring](#) section for more information on Risk Score.
 - Risk Scores are classified by default as either 100 (Known Malicious), 90-99 (High), 70-89 (Medium), or 69 and below (Low).
 - Risk score thresholds may be configured under DT Settings → Configure Enrichment & Alerting, Risky Observed Domains Threshold Settings.
 - Click on a data point to view the underlying events.
 - Filtering by Risk level: All would show the default view used in earlier versions of the application.
- **Newly Observed Domains**
 - The paginated results show newly observed domains, risk score, the time and date that it has been first and last observed, and the number of events associated with that domain observed during the selected time period.
- **Threat Map**
 - Maps the number of suspicious domains observed during the selected time period, based on the GeoLocation of their Hosting IPs or Registrant Country (use the pull-down to select). The Risk Score threshold for a suspicious event is configurable on the Enrichment & Alerting settings page.
- **Threat Portfolio**
 - Plots the number of events associated with domains broken out by Threat Profile category over the selected time range. Click on a category in the legend to display the associated events from the filtered time period. See the [Domain Risk Scoring](#) section for more details.
- **Top 10 Tags from Cache**
 - Lists the top Iris Investigate Tags in use and the number of associated domains observed with that tag in the selected time period.

Interacting with the Dashboards

To drill down on the metric, click on each panel. This will show the total instances of all domain detections within the time filter applied to the dashboard. Results can also be filtered over a specified period of time. Hover over each panel to Open in Search, Export, go Fullscreen, or Refresh.

Interacting with the Threat Map

Hover over each country to find the unique domain count with a geo-located IP associated with that country. It is possible to reset to the original position and zoom.

Reading the Splunk Timecharts

The indicators on the top of the Threat Intelligence Dashboard and Monitoring Dashboard utilize Splunk's "Single Value Visualization" feature to provide a trending context to some of the dashboard metrics. The value displayed matches the filter time (e.g. "Last 15 Minutes") selected, compared to the previous filter time (e.g. previous 15 minutes). These are "bins" in Splunk nomenclature. Regardless of whether the trend is up or down, a green indicator represents a relatively desirable trend (fewer Suspicious Domains, for instance), while a red indicator represents a relatively undesirable trend.

Extending DomainTools Commands Outside the App

You can use the packaged commands (in Iris Investigate or Iris Enrich) from the DomainTools app to enrich domains and URLs within custom Splunk searches. Appendix A lists all the commands available with the DomainTools application. The more frequently-used commands are defined below:

Command	Description	Example(s)
<code>dtdomainextract</code>	Extracts a domain out of a URL field, based on the <code>tlextract</code> library. Note that the DomainTools APIs expect a domain name as an input. Passing subdomains or URLs to the APIs will result in inconsistent data enrichment, so we recommend using <code>dtdomainextract</code> command or the <code>dtdomainextract2</code> macro	<pre> dtdomainextract field_in=url field_out=domain</pre>
<code>dtirisenrich</code>	An eventing command that queries Iris Enrich against up to 100 comma-separated domains at a time. The Iris Enrich API endpoint is optimized for fast volumes and high-volume lookups. Add <code>inline_results</code> to keep event data inline	<pre> makeresults eval domain="domaintools.com" dtirisenrich domain=domain inline_results=true</pre>
<code>dtirisinvestigate</code>	A generating command that queries Iris Investigate against up to 100 comma-separated domains at a time, or pivot on a domain-related attribute to further your investigation. The Iris Investigate API is ideally suited for investigation and orchestration use cases at human scale	<pre> dtirisinvestigate domain="domaintools.com" dtirisinvestigate pivot_type="ip" pivot_value="199.30.228.112"</pre>
<code>dtformatinvestigate</code>	Formats the JSON returned by an Iris Investigate query into a row with component names. Use the output	<pre> dtirisinvestigate domain="domaintools.com" dtformatinvestigate</pre>

	parameter to specify the section of the response to format	output=risk <code>table risk_score type</code>
<code>dtDNSDB</code>	Queries DNSDB for Passive DNS information against a given IP, Domain, Hostname, or Subnet.	<code>dtDNSDB target=198.51.100.1 type="rdata"</code>
<code>dtDNSDBflex</code>	Performs a DNSDB Passive DNS Flexible Search.	<code>dtDNSDBflex query_type=rdata match_type=regex query="^domaintools\.com\.\$"</code>
<code>dtDNSDBlimit</code>	Returns the dnsdb api query limit, number of queries remaining, as well as the time the remaining queries will reset.	<code>dtDNSDBlimit</code>
<code>dtDNSDBenrich</code>	Enrich the Splunk events returned by a given SPL_QUERY with Passive DNS information reported by Farsight DNSDB, part of DomainTools.	... <code>dtDNSDBenrich field_in=domain field_type=domain lookup_type=rrset</code>
<code>dtWhoisHistory</code>	Performs a whoishistory search on a given domain using the Whois History API endpoint.	Parameters: mode: "list", "check_existence", "count" sort: "date_desc", "date_asc"

Examples

The following are a few example SPL commands that leverage DomainTools data for reference:

1. Enrich 300 events from the main index:

```
index=main
| dtDomainExtract field_in=url field_out=domain
| table url domain
| dedup domain
| head 300
```



```
| dtirisenrich domain=domain
```

The `dtirisenrich` command will batch API requests into groups of 100. The `head 300` filter in the example limits the example search to three API queries in case this is copy/pasted directly. It should be able to handle as many domains as you want to input if you want to remove that filter.

Use `| makeresults | eval domain="domaintools.com"` instead of pulling events if you have a set list of domains to enrich.

2. Use Iris Investigate for a domain

```
| dtirisinvestigate domain=domaintools.com
```

3. Use `pivot_type` with an ip address:

```
| dtirisinvestigate pivot_type="ip" pivot_value="199.30.228.112"
```

4. Look through the DomainTools cache to see when a URL was first and last observed on your network:

```
| lookup dt_stats _key AS domain OUTPUT dt_fooyntimestamp AS first_observed,  
dt_looyntimestamp AS last_observed
```

Or to provide full context against a datasource and format the date strings:

```
| tstats summariesonly=true count FROM datamodel=Web BY _time Web.url Web.src  
Web.dest source  
| rename Web.url AS url | rename Web.src AS src | rename Web.dest AS dest | rename  
source AS log_source  
| dtdomainextract field_in=url field_out=domain  
| eval domain=lower(domain)  
| fields url src dest log_source domain _time  
| table _time domain url  
| lookup dt_stats _key AS domain OUTPUT dt_fooyntimestamp AS first_observed,  
dt_looyntimestamp AS last_observed  
| eval first_observed=strftime(first_observed, "%Y-%m-%d %H:%M:%S"),  
last_observed=strftime(last_observed, "%Y-%m-%d %H:%M:%S")
```

5. View the latest Domains, URLs and risk scores from the DomainTools cache:

```
| lookup dt_iris_enrich_data en_domain_name AS domain OUTPUT en_risk_score AS "risk score"
```

Again, with more context against a data source:

```
| tstats summariesonly=true count FROM datamodel=Web BY _time Web.url Web.src Web.dest source  
| rename Web.url AS url | rename Web.src AS src | rename Web.dest AS dest |  
rename source AS log_source  
| dtomainextract field_in=url field_out=domain | eval domain=lower(domain) |  
fields url src dest log_source domain _time | table _time domain url  
| lookup dt_iris_enrich_data en_domain_name AS domain OUTPUT en_risk_score AS "risk score"
```

6. Show domains associated with an IP using DNSDB:

```
... | dtdnsdbenrich field_in=dest_ip field_type=ip max_count=5
```

7. Find recent subdomains under a domain using DNSDB and format the returned unix date fields to be human-readable:

```
... | dtdnsdbenrich field_in=domain field_type=domain lookup_type=rrset rrtype=A  
include_subdomains=true time_first_after=1593070040  
| eval dnsdb_time_first=strftime(dnsdb_time_first, "%Y-%m-%d %H:%M:%S"),  
dnsdb_time_last=strftime(dnsdb_time_last, "%Y-%m-%d %H:%M:%S")
```

8. Enrich 30 events from the main index with Iris Enrich and DNSDB Passive DNS information:

```
index=main  
| dtomainextract field_in=url field_out=domain  
| table url domain  
| dedup domain  
| head 30  
| dtirisenrich domain=domain  
| dtdnsdbenrich field_in=en_domain_name field_type=domain max_count=5
```

Investigation Workflows

About Domain Profile

The **Domain Profile** page provides a search function for ad hoc lookups of a single domain. The results provide a single pane of glass view of the domain, a contextual panel, tags, connected infrastructure information, contact details, and related events. Hover over the tooltips about the panel sections and click on the data points to interact. Use these results for further investigations in DomainTools.

Tip: Users can import lists of domains of interest into Splunk. All domains are imported along with their DomainTools Risk Profile for convenient triaging and subsequent monitoring. See the [Importing Domains from an Iris Investigation](#) section for more information.

To access and interact with the Domain Profile, visit **Investigate** → **Domain Profile** and add the domain in SLD.TLD format.

Domain: ×
SLD.TLD format. Press Return to search

Recent Events Time: ▼

[Remove From Monitoring List](#) [Remove From Allowlist](#)

[Open in Iris Investigate](#)
[Farsight pDNS Standard Search](#)

Risk Score 97	Domain helpmanageaccounts.com	Age (Days) 813 Days	Domain Status Inactive
--------------------------------	--	--------------------------------------	---

Threat Profile Scoring

Phishing 97	Malware 85	Spam 3	Proximity 65
------------------------------	-----------------------------	-------------------------	-------------------------------

Threat Profile Reason malware, phishing	Threat Evidence domain name, name server, registrar
--	--

Domain Profile of an example high Risk Score domain

Domain Risk Scoring

DomainTools Risk Score ranges from 0 to 100 and predicts how likely a domain is to be malicious. A higher value indicates greater confidence. The score comes from two distinct types of algorithms: Proximity, or proximity to known maliciousness, examines how closely connected a domain is to other known-bad domains. A Proximity score of 100 indicates the domain is on an industry blacklist. Threat Profile leverages machine learning to model how closely the domain resembles others used for spam, phishing or malware, to predict intention. The strongest signal from either of those algorithms becomes the overall Risk Score.

The Threat Profile Reason indicates the type(s) of threats predicted for a domain, while the Threat Evidence section exposes the strongest indicators that were used in predictive classification. Read more information about Threat Profile on our [blog](#) and [technical brief](#).

Tags

The tags associated with the domain. Consult the [Set Up Monitoring for Domains with Iris Tags](#) section for more information.

Connected Infrastructure

Connected Infrastructure information (such as Mail Servers, IP addresses, SPF information, Name Servers, SSL information, Registrar/Registry) are obtained from DomainTools datasets.

Guided Pivoting and Discovery

Ad hoc investigations with guided pivots will surface potential investigation points.

Hover over the gray gear icon wheel to show the number of connected domains. If the gray icon is clickable, a blue **Pivot** button appears. Select this button to import the list of domains associated with this data point.

Connected Infrastructure

Domain	Host	Priority
helpmanageaccounts.com	helpmanageaccounts.com	0

Number of Connected Domains: 333

Pivot

169.255.59.77

Example of a Guided Pivot over an IP address, as indicated by the blue text

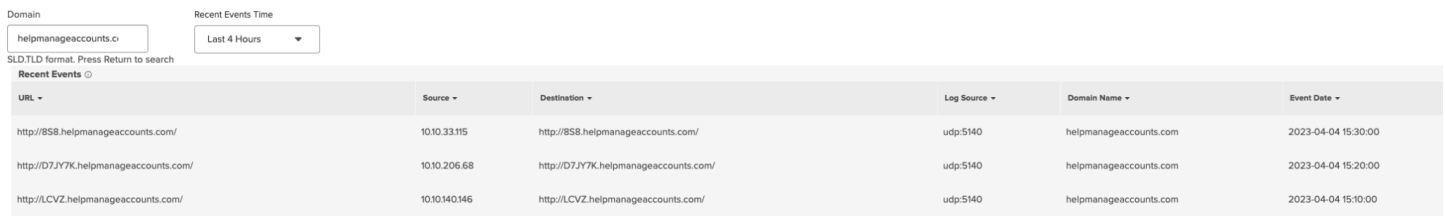
In cases where the connected domains are larger than the Guided Pivot threshold configured, the gray gear icon is not made into a guided pivot and is not clickable. The Guided Pivot threshold is configurable under **DT Settings** → **Configure Enrichment & Alerting**.

Contact Information

The contact information (Admin, Technical, Billing and Registrant) are gleaned from the DomainTools Whois dataset and surfaced on the Splunk app.

Recent Events

While investigating a domain, users can see any related and recent events from their configured log sources across different timeframes.



URL	Source	Destination	Log Source	Domain Name	Event Date
http://BSB.helpmanageaccounts.com/	10.10.33.115	http://BSB.helpmanageaccounts.com/	udp:5140	helpmanageaccounts.com	2023-04-04 15:30:00
http://D7JY7K.helpmanageaccounts.com/	10.10.206.68	http://D7JY7K.helpmanageaccounts.com/	udp:5140	helpmanageaccounts.com	2023-04-04 15:20:00
http://LCVZ.helpmanageaccounts.com/	10.10.140.146	http://LCVZ.helpmanageaccounts.com/	udp:5140	helpmanageaccounts.com	2023-04-04 15:10:00

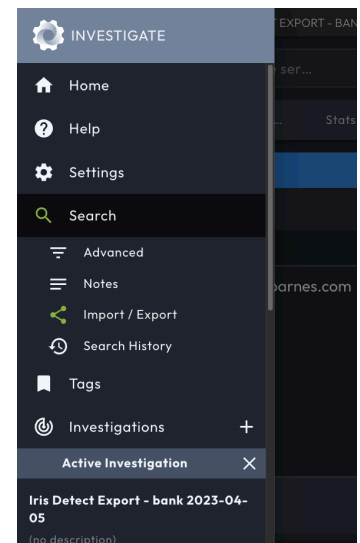
Example of Recent Events associated with a high Risk Score domain

Domain intelligence from such investigations is automatically added to the cache for future references.

Importing Domains from an Iris Investigation

Import the list of domains from Iris into Splunk using the Export and Import functionalities.

1. In the Iris Investigation platform, go to the **Navigation Menu (3 lines)** → **under Search** → **select Import/Export**.
2. The subsequent dialog contains the **Search Hash** to export.
3. From the DomainTools Splunk App, go to **Investigate** → **Import** from Iris Investigate, and paste the copied Search Hash in the input field.
4. After submitting, if the Search Hash has no results in the Iris Pivot Engine, there are no domains to import and Splunk will show the message "No results found". The imported domains will be shown as below:



Domain ↕	Risk Score ↕	Proximity ↕	Threat Profile ↕	Threat Profile Malware ↕	Threat Profile Phishing ↕	Threat Profile Spam ↕	Create Date ↕	Monitor ↕	Allowlist ↕
apexlottopromotion.org	76	76	52	21	35	52	2016-07-31	Enabled	Disabled
asfca-en.com	29	76	29	24	29	1	2016-10-04	Disabled	Disabled
barclayscreditdept.com	68	35	68	54	68	60	2017-02-09	Disabled	Disabled
bf-afdb.com	91	91	88	72	88	13	2019-06-23	Disabled	Disabled

Imported domains from an Iris Investigate and related data

Farsight DNSDB pDNS Searching

Investigate current and historical domain infrastructure with Passive DNS (pDNS) using Farsight's DNSDB Standard or Flexible search (API Key Required). Please contact enterprisesupport@domaintools.com for provisioning.

DNSDB is a database that stores and indexes both the passive DNS data available via DomainTools Security Information Exchange (SIE), as well as the authoritative DNS data that various zone operators make available.

Enter your Farsight DNSDB API key on the [API Keys](#) page.

[Farsight pDNS Standard Search](#) (found under the **Investigate** menu) is a powerful search tool used to uncover related infrastructure against a specific Domain or IP.

Farsight pDNS Standard Search

Farsight DNSDB Documentation

Time Range: All time | Resource Record Type (RRType): Any | OR Add Custom RRType: ANY | IP or Domain Name: farsightsecurity.com [Submit] Hide Filters

DNSDB RDATA Results

Time First	Time Last	RRName	RRType	RData	Zone Time First	Zone Time Last	rdata_tok	Count
09/24/13 17:49:33	09/25/13 20:42:14	207.4.20.149.in-addr.fs1.io.	PTR	farsightsecurity.com.	N/A	N/A	set	7
07/01/13 03:53:50	07/30/13 21:41:15	7.0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.5.6.0.0.1.0.0.0.8.f.4.0.1.0.0.2.ip6.arpa.	PTR	farsightsecurity.com.	N/A	N/A	set	3
09/25/13 20:36:43	10/08/13 20:23:45	81.64-26.140.160.66.in-addr.arpa.	PTR	farsightsecurity.com.	N/A	N/A	set	11
07/15/13 21:07:52	07/17/13 14:39:57	207.192-26.4.20.149.in-addr.arpa.	PTR	farsightsecurity.com.	N/A	N/A	set	4

DNSDB RRSET Results

Zone Time First	Zone Time Last	RRName	RRType	bailliwick	RData	Time First	Time Last	rrset_tok	Count
08/05/20 22:51:16	06/03/22 22:58:25	farsightsecurity.com.	NS	com.	ns5.dnsmadeeasy.com. ns6.dnsmadeeasy.com. ns7.dnsmadeeasy.com.	N/A	N/A	set	360
06/30/13 16:21:41	07/18/13 16:22:47	farsightsecuritytv.com.	NS	com.	ns.lah1.vix.com.	N/A	N/A	set	19

Input parameters are as follows:

- **Time Range**: the time range that should be queried for DNS observations.
- **Resource Record Type (RRType)**: Optionally specify which Record Resource Type (RRType) to search for. RRtype declares the type of mapping that a Resource Record Set establishes. ANY will match all RRTypes except DNSSEC RRTypes and is the default. ANY-DNSSEC will match only the DNSSEC RRTypes. Or enter a custom RRtype in the following text field.

- **IP or Domain Name:** Specify an IP (IPv4/IPv6), CIDR netblock, hostname (FQDN), or domain to search for. Left- or right-side wildcards are supported. Internationalized Domain Names (IDNs) will be automatically converted to Punycode.

[Farsight pDNS Flexible Search](#) (found under the **Investigate menu**) extends the Farsight DNSDB API with additional search capabilities. It provides more powerful searching capabilities (e.g. wildcards, regular expressions) than Standard Search, but the results will not be as complete as those from Standard Search.

Farsight pDNS Flexible Search Edit Export ...

[Flexible Search Documentation](#)

Select a time range: Query: Query type: Match type: Resource Record Type (RRType): Submit Hide Filters

rdata	rrtype	raw_rdata
0 5222 jabber.domaintools.com.	SRV	00000000146606A616262657208646F6061696E746F6F6C7303636F6D00
0 5269 jabber.domaintools.com.	SRV	000000001495066A616262657208646F6061696E746F6F6C7303636F6D00
0 mail.domaintools.co.uk.	MX	000046D61696C0B646F6D61696E746F6F6C7302636F92756B00
0 mail.domaintools.top.	MX	000046D61696C0B646F6D61696E746F6F6C7303746F7000
0 mail.adomaintools.com.	MX	000046D61696C0B61646F6D61696E746F6F6C7303636F6D00
0 mail.domaintoolplus.com.	MX	000046D61696C0F646F6D61696E746F6F6C73706C757303636F6D00

Input parameters are as follows:

- **Time Range:** the time range that should be queried for DNS observations.
- **Query:** Flexible Searches support strings and patterns. This field will use the selected Syntax under "Match type". For an expanded explanation please visit the [user guide](#).
- **Query Type:** Specifies which field of the DNS resource record to search. RDATA is the record data value or the "right hand side" of a DNS resource record set. Its content can be IP address(es), domain names, or other content (such as text), depending on the RRtype. An RRname is the owner name of the RRset, or the "left hand side" of a DNS resource record set. It will always be a domain name.
- **Match Type:** Which Flexible Search syntax to use. Regex is more common and represents the egrep-like Farsight Compatible Regular Expression ("FCRE") syntax, and Globbing is simpler wildcard pattern matching. See the [user guide](#) for examples.
- **Resource Record Type (RRType):** Optionally specify which Resource Record Type (RRType) to search for. RRtype declares the type of mapping that a Resource Record Set establishes. ANY will match all RRTypes except DNSSEC RRTypes and is the default. ANY-DNSSEC will match only the DNSSEC RRTypes.

Investigate Domains Within Incident Review

Description:
int-chase.com with Risk Score of 71 visited 30 times

Additional Fields

Additional Fields	Value
Domain	int-chase.com
Domain Age	898
Domain Status	Inactive
Last Seen	2023-03-29
Enrichment Count	25
Risk Score	71
DomainTools Threat Profile	spam
Log Source	udp:5140
Severity	high
URL	http://24D8.int-chase.com/ http://25QP.int-chase.com/ http://3M9S.int-chase.com/ http://3V77.int-chase.com/

Action

- Edit Tags
- DomainTools DNSDB: int-chase.com
- DomainTools Domain Profile: int-chase.com
- DomainTools Iris: int-chase.com

Related Investigations:
Currently not investigated.

Correlation Search:
DomainTools - DomainTools Domain Monitoring - Rule [🔗](#)

History:
[View all review activity for this Notable Event 🔗](#)

Contributing Events:
[Matching Events 🔗](#)

Adaptive Responses: [🔍](#)

Response	Mode	Time	User	Status
Notable	saved	2023-03-29T20:30:05+0000	nobody	✓ success

[View Adaptive Response Invocations 🔗](#)

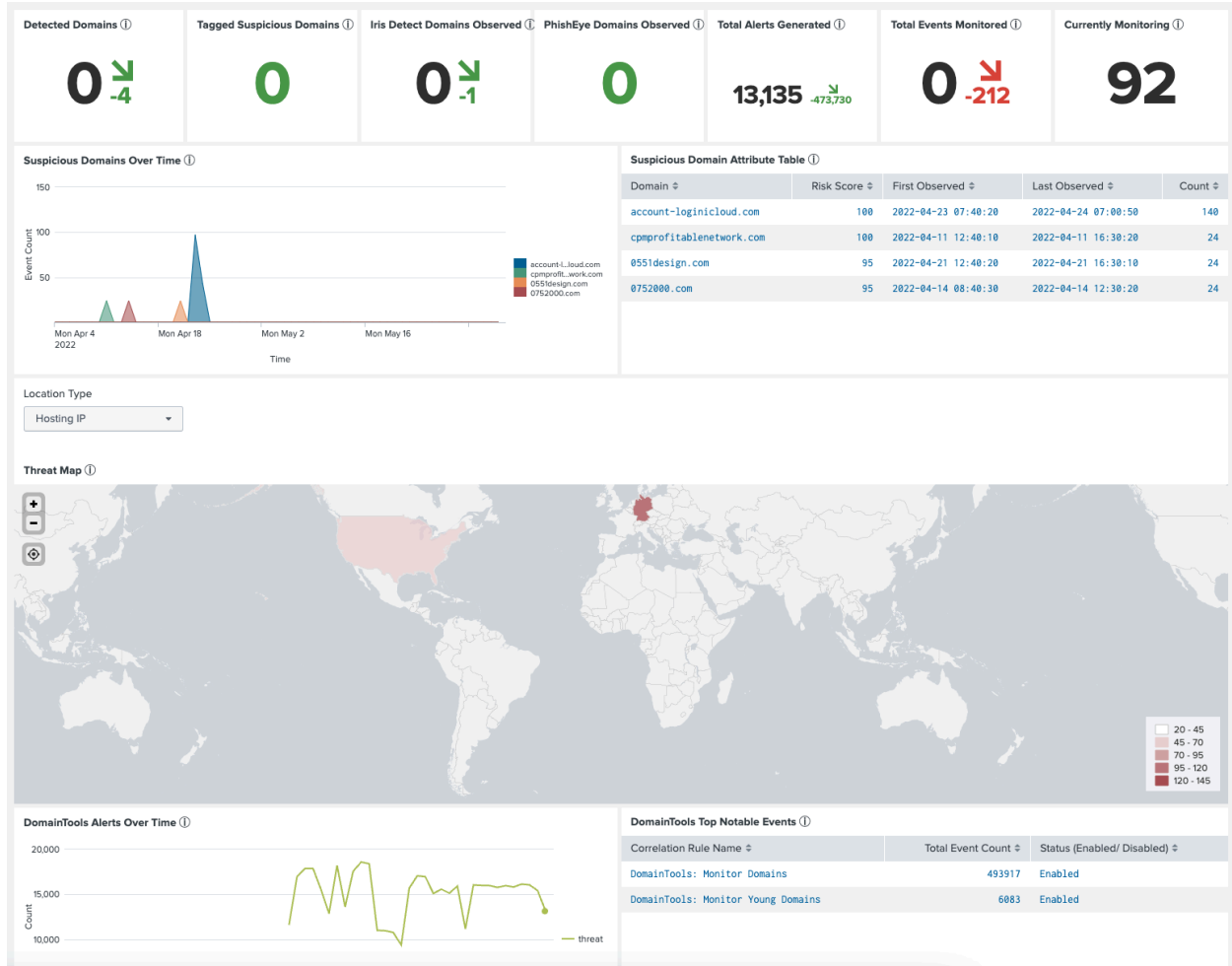
Next Steps:

Expanded Incident Review panel showing the available investigation options for a domain or URL

Investigate any domain or URL listed in an Incident Review event with a couple clicks. (Note that URLs are shortened to a domain lookup). Expand the arrow on the incident review event, and next to a domain or URL, expand the arrow under **Action**.

Domain Monitoring Dashboard

The **Domain Monitoring dashboard**, available from the **Monitoring menu**, enables the monitoring of suspicious domains within Splunk. The dashboard highlights monitoring KPIs for comprehensive reporting.



Domain Monitoring Dashboard

Interacting With and Reading the Dashboard Panels

Hover for the tooltips about the panel sections and select the data points to interact. Use these results for further investigations in DomainTools, or to triage and analyze the results in ES Incident Review by selecting the Alerts Generated panel.

Keep the dashboard and current with the latest information open on an always-on tab or dedicated display, turning on the Auto Refresh. Panels will refresh individually at 5-minute intervals.

Details on the individual panels are below:

- Detected Domains:** Shows the number of domains detected within your network that are in the Monitored Domains List (configurable under Monitoring → Manage Monitored Domains). This includes any domains in the Allowlist. The displayed value indicates the number of domains observed in the selected time period compared to the previous time period.

- **Tagged Suspicious Domains:** Suspicious Domains with an Iris Investigate Tag that are being monitored in the DomainTools Tags List, excluding any in the Allowlist. Tags, the Risk Score threshold is configurable under **DT Settings** → **Configure Enrichment & Alerting**. The Monitored Tags and Allowlists are configurable under the **Monitoring menu**. Tags can be added to domains within the DomainTools [Iris Investigate UI](#). The displayed value indicates the number of domains observed in the selected time period compared to the previous time period.
- **Iris Detect Domains Observed:** Domains Discovered by DomainTools Iris Detect and observed in your network events. This includes any domains in the Allowlist. Add and configure Monitors in [Iris Detect](#), then select how Splunk uses them using the **Monitoring** → **Iris Detect** page. The displayed value indicates the number of domains observed in the selected time period compared to the previous time period.
- **Iris Investigate Domains Observed:** Domains discovered by DomainTools Iris Investigate and observed in your network events. This includes any domains in the Allowlist. The displayed value indicates the number of domains observed in the selected time period compared to the previous time period.
- **Total Alerts Generated:** Shows the number of alerts that were triggered within the selected time period, compared to the previous. Alerts are created based on rules set on the **DT Settings** → **Configure Enrichment & Alerting** page and can be triaged within Splunk Enterprise Security Incident Review or by clicking on the number displayed.
- **Total Events Monitored:** Shows the number of events associated with the domains detected within your network that are in the DomainTools Monitoring List (configurable under **Monitoring** → **Manage Monitored Domains**). This includes any domains in the Allowlist. The displayed value indicates the number of events observed in the selected time period compared to the previous time period.
- **Currently Monitoring:** Total number of Domains currently being monitored. This panel is not impacted by the dashboard time filter. Add domain monitors via **Monitoring** → **Manage Monitored Domains**.
- **Suspicious Domains over Time:** Shows a timeline of the suspicious domains observed over the filtered time period. Suspicious domains have a Risk Score at or above the suspicious Risk Threshold defined in the Enrichment & Alerting settings page .
- **Suspicious Domains Attribute Table:** Lists the domains observed with a Risk Score at or above the Risk Threshold defined in the **DT Settings** → **Configure Enrichment & Alerting** page.
- **Threat Map:** Plots the number of unique domains based on their GeoLocation, Hosting IPs and Registrant Country associated with Detected Domains in your cache.
- **DomainTools Alerts over Time:** Shows a timeline of the unique alerts observed over the filtered time period. Alerts are created based on rules set on the **DT Settings** → **Configure Enrichment & Alerting** page.
- **DomainTools Top Notable Events:** Displays the activity and status of DomainTools alerting rules within your environment. These can be configured on the **DT Settings** → **Configure Enrichment & Alerting** page.

Historical Analysis of Enrichment Activity

The Enrichment Explorer section available from the main menu provides a user-facing front of the DomainTools enrichment dataset or cache. This allows the user to browse and search from the enrichment cache based on filters.

The screenshot shows the DomainTools KV Store Explorer interface. At the top, there are several filter fields: Domain (empty), Age Less Than (days) (20), Last Enriched (Last 4 Hours), Risk Score Greater Than (90), Threat Type (No Filter), Show Monitored Domains Only (checkbox), and Display (radio buttons for Summary and All Fields). A green Submit button is on the right. Below the filters is a table titled "DomainTools KV Store Explorer (14)". The table has columns for Domain Name, Age, Active Status, Overall Risk Score, Last Enriched DateTime, Proximity Score, Threat Type, Threat Profile Malware, Threat Profile Phishing, Threat Profile Spam, Monitor, and Allowlist. The table contains 6 rows of data.

Domain Name	Age	Active Status	Overall Risk Score	Last Enriched DateTime	Proximity Score	Threat Type	Threat Profile Malware	Threat Profile Phishing	Threat Profile Spam	Monitor	Allowlist
2524874.com	17	Active	100	09-29-2021 13:10:03	100		97	98	99	Enabled	Disabled
2658616.top	3	Active	94	09-29-2021 13:10:03	45		91	94	44	Disabled	Disabled
496841.com	16	Active	97	09-29-2021 13:10:03	27		97	86	76	Disabled	Enabled
565393.com	14	Active	96	09-29-2021 13:10:03	21		87	95	96	Disabled	Disabled
7847538.com	10	Active	96	09-29-2021 13:10:03	48		94	96	89	Disabled	Disabled
88745v1.top	11	Active	95	09-29-2021 13:10:03	35		95	95	73	Disabled	Disabled

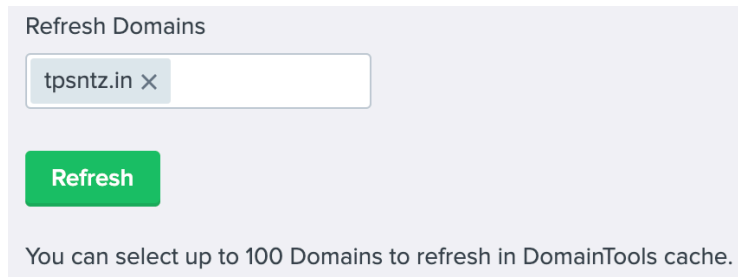
DomainTools Enrichment Explorer to research domains from your network that are currently in the DomainTools cache.

Filter by the following attributes:

- **Domain:** Use SLD.TLD like example.com or example[.]com. Allows a comma-separated list of up to 100 domains.
- **Domain Age:** By domain age, in days.
- **Risk Score:** Any value from 1 to 99.
- **Threat Type:** Defined as Any, None, Malware, Phishing or Spam.
- **Show Domains from Monitoring List only.**

Selecting the **Monitor** field to add or remove a domain from your monitoring list. Clicking on the "Allowlist" button will add or remove a domain from your allow list.

If the information for a domain observable appears to be dated (i.e., enrichment date from the past, or a set of domains from an Iris Investigate Search Hash import), the user can explicitly refresh their KV store with the latest Domain Intelligence, or reduce the Cache Retention Period under **DT Settings** → **Configure Enrichment & Alerting**.



The Refresh Domains option at the bottom of the Enrichment Explorer page

Alerts for Splunk (without ES) with the dt_alerts Index

The `dt_alerts` index enables alerting in Splunk (without Enterprise Security). [Create the dt_alerts index](#), and utilize it in the Search Page.

Troubleshooting & Known Issues

Enabling Logging

Logging is disabled by default. To enable logging to help with diagnostics, go to **DT Settings** → **Diagnostic Panel** and select **Enable Diagnostic Panel**. Allow a few minutes for logs to populate, then refresh the page.

Checking the Status of Saved Searches

Having one or more required saved searches disabled is a common customer issue that could manifest itself as incomplete app functionality.

To check on the status of saved searches:

1. Select the **DT Settings menu** within the app.
2. Select **Configure Saved Searches** to load the list of saved searches used by the DomainTools app

Compare the scheduled time on the resulting set of reports against the table of [Saved Search Names and Descriptions in Appendix A](#) to ensure the required core app saved searches, as well as the additional ones if required for Iris Investigate or Alerting in Splunk Enterprise Security are enabled.

11 Reports							
		All	Yours	This App's	filter	Q	
i	Title ^	Actions		Next Scheduled Time ↕	Owner ↕	App ↕	Sharing ↕
>	DomainTools - Expire Old Iris Enrich Data	Open in Search	Edit ▾	2021-09-30 00:00:00 UTC	nobody	DomainTools-App-for-Splunk	Global
>	DomainTools - Expire Old PhishEye Data	Open in Search	Edit ▾	2021-09-30 00:00:00 UTC	nobody	DomainTools-App-for-Splunk	Global
>	DomainTools - Expire Old Pivot Data	Open in Search	Edit ▾	2021-09-30 00:00:00 UTC	nobody	DomainTools-App-for-Splunk	Global
>	DomainTools - Expire Old Queue Data	Open in Search	Edit ▾	2021-09-30 00:00:00 UTC	nobody	DomainTools-App-for-Splunk	Global
>	DomainTools - Import PhishEye Results	Open in Search	Edit ▾	2021-09-30 00:00:00 UTC	nobody	DomainTools-App-for-Splunk	Global
>	DomainTools - Import PhishEye Terms	Open in Search	Edit ▾	2021-09-30 00:00:00 UTC	nobody	DomainTools-App-for-Splunk	Global
>	DomainTools - Iris Enrich Monitored Domains	Open in Search	Edit ▾	2021-09-30 00:00:00 UTC	nobody	DomainTools-App-for-Splunk	Global
>	DomainTools - Iris Enrich Monitored Domains Live	Open in Search	Edit ▾	None	nobody	DomainTools-App-for-Splunk	Global
>	DomainTools - Iris Enrichment	Open in Search	Edit ▾	2021-09-29 19:45:00 UTC	nobody	DomainTools-App-for-Splunk	Global
>	DomainTools - Queue Builder for Iris Enrich KV Store	Open in Search	Edit ▾	2021-09-29 19:46:00 UTC	nobody	DomainTools-App-for-Splunk	Global
>	DomainTools - Summary - Timechart count by domain with latest time	Open in Search	Edit ▾	2021-09-29 20:05:00 UTC	nobody	DomainTools-App-for-Splunk	Global

Configure Saved Searches page showing a single report disabled

Appendix A: App Components

The Splunk app is provisioned with the following main components.

Table: Main Configuration Files, Stanzas, and Fields

These configuration files are relevant to utilizing the app and DomainTools datasets.

Note: The configuration files are relevant for this version only. The configuration files, stanzas and fields will be different in other versions.

Conf File	Stanza Tag	Fields	Description
app.conf	package	id	Add details for the Splunk App.
	install	is_configured	
	ui	is_visible, label	
	launcher	author, description, version	

Conf File	Stanza Tag	Fields	Description
commands.conf	dtaccountinfo	chunked, filename	These are helper commands for the app. The most commonly used ones outside the app are described in greater detail in Extending DomainTools Commands Outside the App , as well as the in-app documentation.
	dtimportirisdetectmonitors	chunked, filename	
	dtimportirisdetectresults	chunked, filename	
	dtirisdetectescalate	chunked, filename	
	dtirisdetectchangestate	chunked, filename	
	dtsyncirisdetectwatchlist	chunked, filename	
	dtirisinvestigate	chunked, filename	
	dtirisenrich	chunked, filename	
	dtformatenrich	chunked, filename	
	dtformatinvestigate	chunked, filename	
	dtexpirecache	chunked, filename	
	dtdomainextract	type, filename, streaming, local, passauth, chunked	The template to modify the DomainTools domainextract function to use Splunk SDK SCP1, should the latest SDK face throughput issues.
	dtDNSDB	filename, retainevents, supports_multivalues, streaming, overrides_timeorder, passauth	Queries DNSDB for Passive DNS information against a given IP, Domain, Hostname, or Subnet.
dtDNSDBflex	filename, retainevents, supports_multivalues, streaming, overrides_timeorder, passauth	Performs a DNSDB Passive DNS Flexible Search.	
dtDNSDBenrich	chunked, filename	Enrich the Splunk events returned by a given SPL_QUERY with Passive DNS information reported by Farsight DNSDB, part of DomainTools.	

Conf File	Stanza Tag	Fields	Description
	validateip	filename, retainevents, supports_multivalues, streaming, overrides_timeorder	
	dtdnsdblimit	filename, retainevents, supports_multivalues, streaming, overrides_timeorder, passauth	Returns the dnsdb api query limit, number of queries remaining, as well as the time the remaining queries will reset.
	flushcache	filename, retainevents, supports_multivalues, streaming, overrides_timeorder, passauth	
searchbnf.conf	dtaccountinfo-command	syntax, shortdesc, usage, comment1, example1	The syntax (shorter name), description and if the usage is public.
	dtirisinvestigate-command	syntax, shortdesc, usage, comment1, example1, comment2, example2, related	
	dtirisdetectmonitors-command	syntax, shortdesc, usage, comment1, example1	
	dtyncirisdetectwatchlist-command	syntax, shortdesc, usage, comment1, example1	
	dtirisenrich-command	syntax, shortdesc, usage, comment1, example1, comment2, example2, related	
	dtformatinvestigate-command	syntax, shortdesc, usage, comment1, example1, related	
	dtformatenrich-command	syntax, shortdesc, usage	

Conf File	Stanza Tag	Fields	Description
	dtomainextract-command	syntax, shortdesc, usage, comment1, example1, comment2, example2	
	dtexpirecache-command	syntax, shortdesc, usage, comment1, example1	
	dtDNSdb-command	syntax, description, shortdesc, example1, example2, example3, usage	
	dtDNSdbflex-command	syntax, shortdesc, example1, example2, example3, usage	
	dtDNSdbenrich-command	syntax, description, shortdesc, example1, example2, example3, usage	
	dtDNSdblimit-command	syntax, description, shortdesc, example1, usage	
server.conf	shclustering	conf_replication_includ e.domaintools	Default value is set to true.
transforms.conf	dt_iris_enrich_queue	external_type, collection, fields_list, case_sensitive_match	These are KV store fields. Please see the table in this section KV Store/Collection Name with Descriptions and Fields for the array of fields_list for each stanza.
	dt_iris_enrich_data	external_type, collection, fields_list, case_sensitive_match	
	dt_stats	external_type, collection, fields_list, case_sensitive_match	
	dt_allowlist	external_type, collection, fields_list	

Conf File	Stanza Tag	Fields	Description
	dt_monitoring_list	external_type, collection, fields_list	
	dt_tags_list	external_type, collection, fields_list	
	dt_iris_detect_monitors	external_type, collection, fields_list	
	dt_iris_detect_results	external_type, collection, fields_list	
	dt_iris_investigate	external_type, collection, fields_list	
	dt_public_suffix_list	filename, match_type, max_matches	
domaintools.conf	domaintools	proxy_enabled	Use a proxy when connecting to the DomainTools API. To enable, set to 1.
		proxy_server	The proxy server address to use.
		proxy_port	The proxy server port to use.
		ssl_enabled	Use SSL when connecting to the DomainTools API. To enable, set to 1.
		custom_certificate_enabled	Use a custom SSL certificate for the SSL connection. To enable set to 1.
		custom_certificate_path	The path to the custom SSL certificate.
		guided_pivot_threshold	The Guided Pivot Threshold on the Domain Profile page. Set a lower value to narrow investigations. 500 is the default and recommended value.

Conf File	Stanza Tag	Fields	Description
		bulk_enrichment_batch_size	Number of domains batched in an API call. Set the value from 1 to 100.
		optimize_enrichment_searches	This setting enables quicker correlation of cached data of known domains from the Enrichment table. Requires additional disk space. Disabling will reduce disk space consumption but will slow down searches. Set 1 to enable.
		populate_scores	Checks for whether or not to use the Risk Score over lower tiered scores. Turned off (set to 0) by default.
		logging_on	Toggles whether or not to write logs to file.
macros.conf	See the table in this section Key Macros for Enrichment .		
savedsearches.conf	See the table in this section Saved Search Names and Descriptions .		
collections.conf	See the table in this section KV Store/Collection Name with Descriptions and Fields .		
distsearch.conf	replicationWhitelist	domainextract	Path to domainextract custom search command to be copied to indexers
		lib	Path to python libs to be copied to indexers
workflow_actions.conf		dt_iris_lookup	Lookup domain using Iris Investigate
		dt_domain_profile	Lookup domain using Domain Profile
		dt_dnsdb	Lookup passive dns using Farsight pDNS Standard Search

Table: KV Store/Collection Names and Fields

KV Store/ Collection Name	Fields
dt_iris_enrich_queue	_key, domain, queued, observed
dt_iris_enrich_data	_key, _raw, dt_queued, dt_retrieved, dt_observed, en_domain_name, en_is_active, en_adsense_code, en_google_analytics_code, en_alexa_ranking, en_domain_create_date, en_domain_updated_timestamp, en_domain_expiration_date, en_tld, en_website_response_code, en_redirect_url, en_registrant_name, en_registrant_org, en_registrar, en_spf_info, en_additional_whois_email, en_additional_soa_email, en_additional_ssl_raw, en_ssl_info_1_hash, en_ssl_info_1_organization, en_ssl_email, en_ssl_info_1_subject, en_risk_score, en_proximity_score, en_threat_profile_type, en_threat_profile_malware, en_threat_profile_phishing, en_threat_profile_spam, en_threat_profile_evidence, en_additional_name_servers_raw, en_name_server_1_domain, en_name_server_1_host, en_name_server_1_ip, en_name_server_2_domain, en_name_server_2_host, en_name_server_2_ip, en_additional_mx_raw, en_mx_1_domain, en_mx_1_host, en_mx_1_priority, en_mx_1_ip, en_additional_ips_raw, en_ip_1_address, en_ip_1_country_code, en_ip_1_isp, en_ip_1_asn, en_ip_2_address, en_ip_2_country_code, en_ip_2_isp, en_ip_2_asn, en_admin_contact_city, en_admin_contact_country, en_admin_contact_fax, en_admin_contact_name, en_admin_contact_org, en_admin_contact_phone, en_admin_contact_postal, en_admin_contact_state, en_admin_contact_street, en_admin_contact_email, en_billing_contact_city, en_billing_contact_country, en_billing_contact_fax, en_billing_contact_name, en_billing_contact_org, en_billing_contact_phone, en_billing_contact_postal, en_billing_contact_state, en_billing_contact_street, en_billing_contact_email, en_technical_contact_city, en_technical_contact_country, en_technical_contact_fax, en_technical_contact_name, en_technical_contact_org, en_technical_contact_phone, en_technical_contact_postal, en_technical_contact_state, en_technical_contact_street, en_technical_contact_email, en_registrant_contact_city, en_registrant_contact_country, en_registrant_contact_fax, en_registrant_contact_name, en_registrant_contact_org, en_registrant_contact_phone, en_registrant_contact_postal, en_registrant_contact_state, en_registrant_contact_street, en_registrant_contact_email, en_tag, en_tag_raw
dt_stats	_key, dt_last_enriched_datetime, dt_num_of_times_enriched, dt_num_of_AdhocLookups, dt_fooyntimestamp, dt_looyntimestamp, en_attribute_name, en_attribute_type, en_risk_score
dt_allowlist	_key, en_attribute_type, _dt_updated, _dt_updated_by, _dt_created, _dt_created_by

KV Store/ Collection Name	Fields
dt_monitoring_list	_key, en_attribute_type, _dt_updated, _dt_updated_by, _dt_created, _dt_created_by, _dt_source
dt_tags_list	_key, en_attribute_type, _dt_updated, _dt_updated_by, _dt_created, _dt_created_by
dt_iris_detect_monitors	_key, monitor_id, term, state, match_substring_variations, nameserver_exclusions, text_exclusions, created_date, updated_date, status, created_by, discover_new_domains, dt_updated
dt_iris_detect_results	_key, dt_domain, dt_state, dt_status, dt_discovered_date, dt_escalations, dt_risk_score, dt_risk_status, dt_mx_exists, dt_tld, dt_domains_id, dt_monitor_ids, dt_create_date, dt_ip_address_1, dt_ip_address_2, dt_ip_raw, dt_nameServer_1, dt_nameServer_2, dt_nameServer_raw, dt_mailServer_1, dt_mailServer_2, dt_mailServer_raw, dt_registrar, dt_registrant_contact_email, dt_proximity_score, dt_threat_profile_malware, dt_threat_profile_phishing, dt_threat_profile_spam, dt_threat_profile_evidence, dt_monitor_flag, dt_imported
dt_iris_investigate	_key, dt_pivot_type, dt_pivot_value, dt_investigate_raw, _dt_created
dt_rrset_kvstore	
dt_rdata_kvstore	

Table: Key Macros for Enrichment

Macro Field Name	Default Value	Description
dt_basesearch		The value that is defined is the base search. Data is pulled directly from the datamodel. We use this search to search for and queue up domains for the app and certain features such as the dashboards.
enable_cache	1 (enabled)	Enrichment setting to determine caching of enriched data. DomainTools will always enrich every domain in the queue. When turned off (set to 0) an API call will be made for every domain.
dt_cache_retention_period	30 (in days)	Enrichment setting. Set the value to how many days back before removing older data from the enrichment kvstore. There is also a saved search that will remove records that are over 30 days old.

Macro Field Name	Default Value	Description
dt_proximity_score_threshold	65	Enrichment setting. Set the threshold throughout the app when filtering based on the Proximity score.
dt_threat_profile_score_threshold	85	Enrichment setting. Set the threshold throughout the app when filtering based on the Threat Profile score.
dt_high_risk_threshold	90	Enrichment setting. Set the threshold throughout the app.
dt_medium_risk_threshold	70	Enrichment setting. Set the threshold throughout the app.
dt_refresh_interval	15 (in minutes)	The refresh interval.
dtdomainextract2	<pre> rex field=url "(.*:VV)?(?P<temp_domain>[^\:#V?]+)" \ lookup dt_public_suffix_list wildcard_tld AS temp_domain OUTPUT tld AS tld \ where match(temp_domain, "(.*[.@])?([\p{L}\w-]+[.]" tld."\$") \ eval domain = replace(temp_domain, "(.*[.@])?([\p{L}\w-]+[.]" tld."\$)", "\2") </pre>	Alternative to dtdomainextract that does regex-based matching for TLDs. It is higher performance for high-throughput environments, with a small accuracy trade-off. Notably, some multi-level tlds (e.g. edu.np) can be mis-identified as a domain.
dt_risk_score_threshold	75	Enrichment setting. Set the threshold throughout the app when filtering based on the Risk Score.
dt_young_domain_age	7 (in days)	Enrichment setting. The number of days the app considers a domain to be young.
dt_include_allowlisted_domains	0 (false)	Allowlist setting. Set to 1 (enabled) to exclude showing domains in the allowlist in our dashboards.
dt_include_monitoring_list_domains	0 (false)	Setting to include monitoring list domains.

Macro Field Name	Default Value	Description
dt_enrich_to_stats_lookup		A partial search that is used by the saved searches that update the enriched data KV Store.
dt_include_allowlisted_domains_in_notable_events	0 (false)	Enrichment alert setting for notable events.
dt_only_monitored_domains_in_notable_events	1 (enabled)	Enrichment alert setting for notable events.
dt_use_risk_threshold_in_notable_events	0 (false)	Enrichment alert setting for notable events.
dt_use_threatprofile_threshold_in_notable_events	0 (false)	Enrichment alert setting for notable events.
dt_ignore_iris_detect_in_notable_events	0 (false)	Enrichment alert setting for notable events.
dt_monitor_tags_in_notable_events	0 (false)	Enrichment alert setting for notable events.
dt_notable_events		Search for notable events provided by the DomainTools App for Splunk ES.
dt_rename_base_fields		Renames the base search fields. For example, rename src to Source, dest as Destination, log_source as Log Source and domain as Domain Name.
dt_rename_iris_fields		
unknown_domain_retry	1 (enabled)	Retry enrichment of domains that are unknown to DomainTools.
unknown_domain_retry_time	60 (in minutes)	Number of minutes to wait before trying to re-enrich a domain.
toEpoch(1)	if(isnull(round(relative_time(time(), "\$reltime\$"))), "\$reltime\$", round(relative_time(time(), "\$reltime\$")))	Changes timestamp to epoch.

Table: Saved Search Names and Descriptions

The following is a complete list of Saved Searches, descriptions, and supported functionalities.

Saved Search Name	Type	Description of the Saved Search	Required (Yes, No, Optional)	App Functionalities
DomainTools - Queue Builder for Iris Enrich KV Store	Reports	A search to extract domains from raw events based on your configured base search and store them in the dt_iris_enrich_queue KV store for enrichment. Default cron_schedule = */2 * * * *	Yes*	Core App
DomainTools - Expire Old Queue Data	Reports	A search to remove domains from the dt_iris_enrich_queue collection that are over a day old. Default cron_schedule = 0 0 * * *	Yes	Core App
DomainTools - Iris Enrichment	Reports	A search to enrich domains found in dt_iris_enrich_queue, and store results in dt_iris_enrich_data collection. By default, the search is scheduled to run every 5 minutes and pulls data over the past 30 minutes. Customize this frequency in the app. Default cron_schedule = */5 * * * *	Yes*	Core App
DomainTools - Expire Old Iris Enrich Data	Reports	A search to remove enrichment data from the dt_iris_enrich_data collection based on the cache retention settings configured in the app. Default cron_schedule = 0 0 * * *	Yes	Core App
DomainTools - Iris Enrich Monitored Domains	Reports	A search to refresh enrichment data for monitored domains based on the frequency configured in the app. Default cron_schedule = 0 0 * * *	Yes	Core App
DomainTools - Summary - Timechart count by domain with latest time	Reports	A search to summarize events from the base search whenever the selected time window is greater than 2 hours in any of our dashboards. Default cron_schedule = */5 * * * *	Yes**	Core App
DomainTools - Expire Old Investigate Data	Reports	A search to remove investigative results older than 24 hours. Default cron_schedule = 0 0 * * *	Yes	Core App

Saved Search Name	Type	Description of the Saved Search	Required (Yes, No, Optional)	App Functionalities
DomainTools - Iris Enrich Monitored Domains Live	Reports	A search to refresh enrichment data for monitored domains, whenever it is seen on your network. Default cron_schedule = 5 * * * *	No (DomainTools app will manage this automatically)	Core App
DomainTools - Import Iris Detect Monitors	Reports	A search to import newly discovered and watched domains from Iris Detect monitors in the app. Customers using Iris Detect functionalities in the app must enable this saved search in Splunk. Default cron_schedule = 0 0 * * *	Optional (Required for Iris Detect)	Iris Detect
DomainTools - Import Iris Detect Results	Reports	A search to import newly discovered domains from Iris Detect for monitors enabled in the app. Customers using Iris Detect functionalities in the app must enable this saved search in Splunk. Default cron_schedule = 45 */2 * * *	Optional (Required for Iris Detect)	Iris Detect
DomainTools - Sync Iris Detect Watchlist	Reports	A search to automatically sync Iris Detect Watchlist with DomainTools Monitoring List inside of Splunk. Default cron_schedule = 0 0 * * *	Optional (Required for Iris Detect)	Iris Detect
DomainTools - Expire Old Iris Detect Data	Reports	A search to remove Iris Detect domains that were imported more than 14 days ago. Customers using Iris Detect functionalities in the app must enable this saved search in Splunk. Default cron_schedule = 0 0 * * *	Optional (Required for Iris Detect)	Iris Detect
DomainTools - DomainTools Domain Monitoring - Rule	Alerts	A saved search to create events based on the criteria selected in DomainTools App → DT Settings → Configure Enrichment & Alerting. Customers wanting to create Notable Events within Enterprise Security must either enable this saved search or enable the correlation search inside Splunk ES. Default cron_schedule = */30 * * * *	Optional (Required for Enterprise Security)	Alerting in Splunk Enterprise Security

Saved Search Name	Type	Description of the Saved Search	Required (Yes, No, Optional)	App Functionalities
DomainTools - DomainTools Young Domains - Rule	Alerts	A saved search to create events based on the criteria selected in DomainTools App → DT Settings → Configure Enrichment & Alerting. Customers wanting to create Notable Events within Enterprise Security must either enable this saved search or enable the correlation search inside Splunk ES. Default cron_schedule = */30 * * * *	Optional (Required for Enterprise Security)	Alerting in Splunk Enterprise Security

*The app will function with "DomainTools - Queue Builder for Iris Enrich KV Store" and "DomainTools - Iris Enrichment" disabled, but won't automatically enrich events. Some customers choose to disable these when building their own enrichment pipelines, using the DomainTools app for ad hoc search or monitoring only.

**The app will function with "DomainTools - Summary - Timechart count by domain with latest time" disabled, but dashboard views 4 hours or above will fail to show any data. These larger time frames rely on the summary data generated by this saved search. In some customer environments, this may be an acceptable tradeoff for performance considerations.