DomainTools App for Splunk and Splunk ES

Version 4.4, March 2023
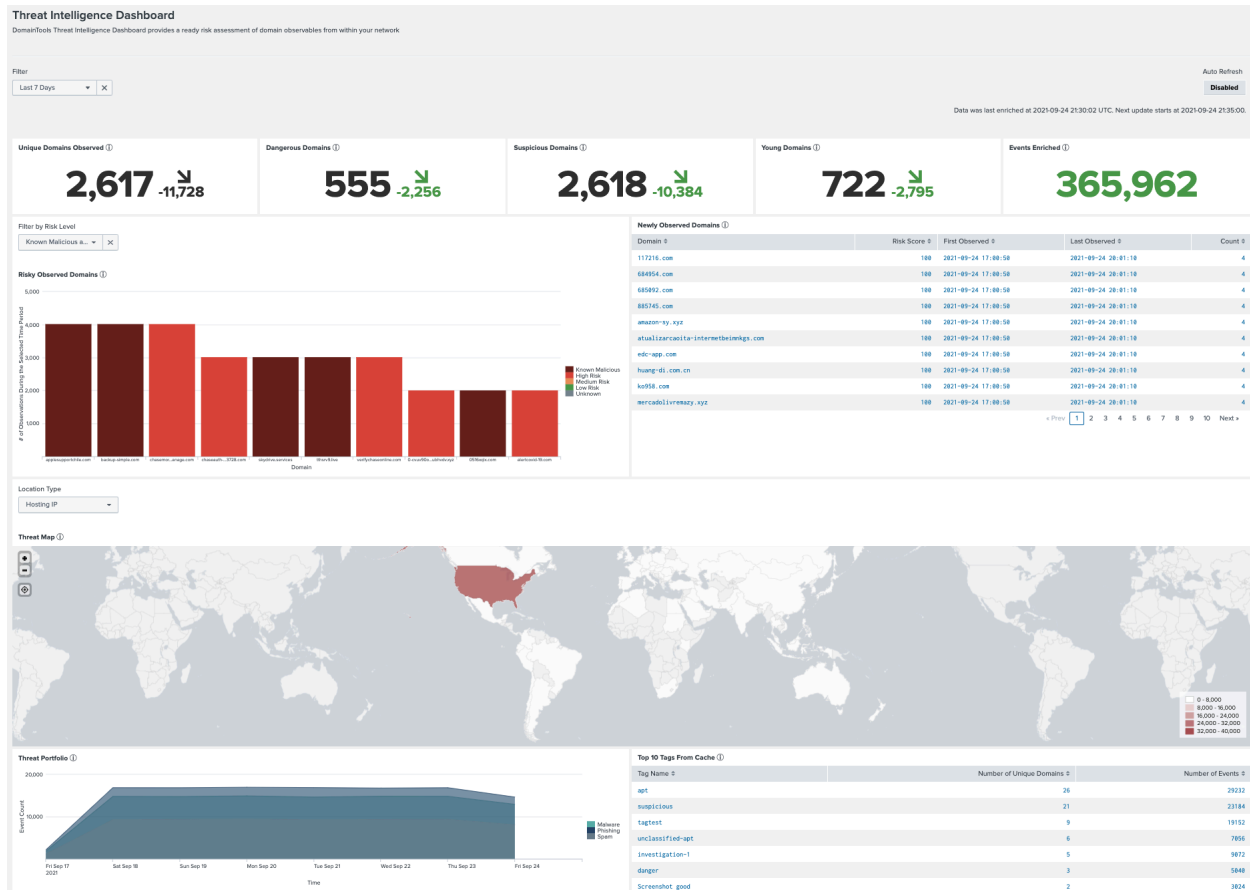
DomainTools

Threat Intelligence Dashboard
DomainTools Threat Intelligence Dashboard provides a ready risk assessment of domain observables from within your network

Filter
Last 7 Days

Auto Refresh
Disabled

Data was last enriched at 2021-09-24 21:30:02 UTC. Next update starts at 2021-09-24 21:35:00.

Unique Domains Observed	Dangerous Domains	Suspicious Domains	Young Domains	Events Enriched
2,617 -11,728	555 -2,256	2,618 -10,384	722 -2,795	365,962

Filter by Risk Level
Known Malicious a...

Risky Observed Domains

Known Malicious
High Risk
Medium Risk
Low Risk
Unknown

Newly Observed Domains

Domain	Risk Score	First Observed	Last Observed	Count
117216.com	100	2021-09-24 17:00:50	2021-09-24 20:01:10	4
684954.com	100	2021-09-24 17:00:50	2021-09-24 20:01:10	4
685692.com	100	2021-09-24 17:00:50	2021-09-24 20:01:10	4
885745.com	100	2021-09-24 17:00:50	2021-09-24 20:01:10	4
amazon-sy.xyz	100	2021-09-24 17:00:50	2021-09-24 20:01:10	4
atualizarcaoita-intermetbeimnkgs.com	100	2021-09-24 17:00:50	2021-09-24 20:01:10	4
edc-app.com	100	2021-09-24 17:00:50	2021-09-24 20:01:10	4
huang-di.com.cn	100	2021-09-24 17:00:50	2021-09-24 20:01:10	4
ko958.com	100	2021-09-24 17:00:50	2021-09-24 20:01:10	4
mercadolivremazy.xyz	100	2021-09-24 17:00:50	2021-09-24 20:01:10	4

‹ Prev 1 2 3 4 5 6 7 8 9 10 Next ›

Location Type
Hosting IP

Threat Map

0 - 8,000
8,000 - 16,000
16,000 - 24,000
24,000 - 32,000
32,000 - 40,000

Threat Portfolio

Malware
Phishing
Spam

Fri Sep 17 2021 Sat Sep 18 Sun Sep 19 Mon Sep 20 Tue Sep 21 Wed Sep 22 Thu Sep 23 Fri Sep 24
Time

Top 10 Tags From Cache

Tag Name	Number of Unique Domains	Number of Events
apt	26	29232
suspicious	21	23184
tagtest	9	19152
unclassified-apt	6	7056
investigation-1	5	9072
danger	3	5040
Screenshot_good	2	3024

DomainTools Threat Intelligence Dashboard

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's 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 4.4 is the General Availability (GA) release of our app for Splunk, Splunk Enterprise, and Splunk Cloud, focusing on updated dashboards that resolve HTML warnings and no longer requires older versions of jQuery. Please review the release notes to understand the key features and changes in this release.

4.4 Release Notes

New
- Added an inline Passive DNS lookup command, `dtdnsdbenrich`.
- All pages have been rebuilt using SimpleXML and React, resolving HTML dashboard warnings and removing dependencies on older versions of jQuery.

Deprecated
- Removed support for PhishEye (replaced by Iris Detect)
- Stopped replicating KV stores to indexers (an unused feature taking up space on indexers, but if you miss it, please let us know!)

Changes and Fixes
- The Iris Detect page has been separated into two pages: an Iris Detect Dashboard and Iris Detect Monitored Term setup page.
- Added an `inline_results` option to `dtirisenrich` to preserve previous fields, if desired.
- Resolved an issue that would cause Iris Detect domains to be imported into Splunk, regardless of whether or not a monitored term was enabled.
- Resolved an issue on Splunk 9 when Iris Detect domains would not be imported at all.
- Domains with parsing issues are logged (if Diagnostic Panel is enabled) and skipped, resolving a queue builder error in some environments.
- Improved in-app documentation and syntax highlighting on custom search commands.

Appendix B contains release notes for prior versions.

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`. See 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. If you are unsure who this is, if this is your first time setting up Splunk with DomainTools, please contact your Account Manager or Enterprise Support to 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?"** Please click the **"Enable"** button to enable the minimum set of saved searches that run the enrichment process.

Enable Additional Saved Searches

Go to **DT Settings → Configure Saved Searches** to enable any additional saved searches you may wish to utilize. See the Saved Search Names and Descriptions section 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 that is helpful for new users to understand. Additional information covering the app components: configuration files, stanzas and fields, KV store, macros, and saved searches, is contained in Appendix A.
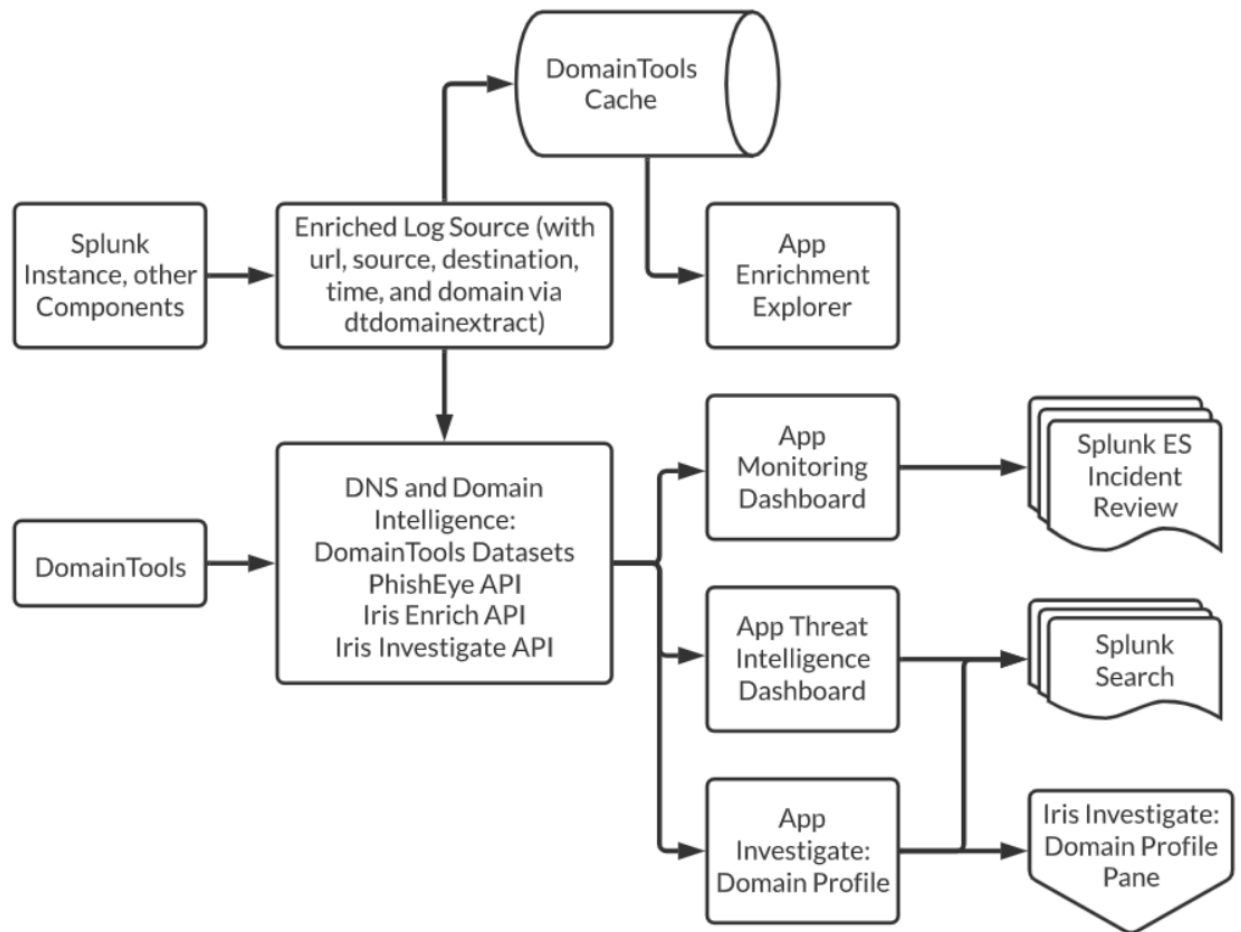
High-level topology of both Splunk and DomainTools resources

Domain Enrichment Process between DomainTools and Splunk Indexes
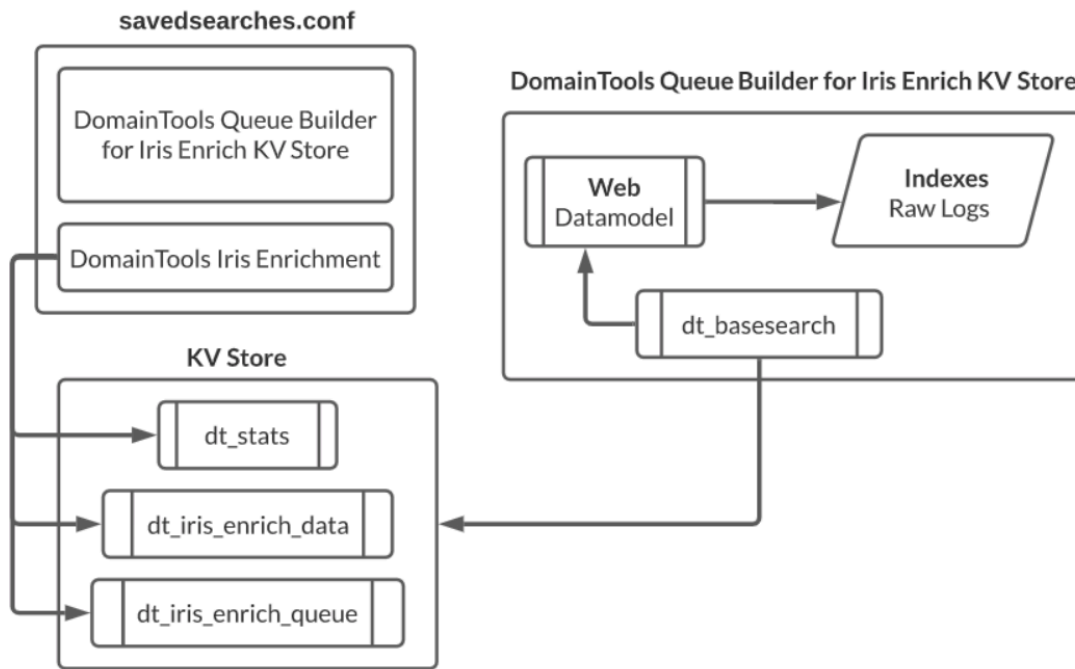
The *Saved Searches* configuration file (`savedsearches.conf`) defines the processes for enrichment and the Queue Builder for the Iris Enrich KV store. In the Queue Builder process, raw logs in the Splunk Indexes are queried from the `Web` data model as defined by the DomainTools base search configuration (`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.

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, but can function as a standalone monitoring platform without Splunk ES. Customers who have not yet deployed ES can still realize significant value from the DomainTools solution.

Versions 4.1.2 and above work best when installed on indexers, in addition to previous requirements, during deployment. Our Enterprise Support team can assist with workarounds if such a setup is not feasible for your environment.

DomainTools App Bundle

The latest app is available on Splunkbase.

API Keys

You will need a DomainTools API username and API key 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 sales@domaintools.com. If you are an existing DomainTools customer, to ensure your DomainTools API key is appropriately provisioned, please contact your account manager or Enterprise Support .

For complete App functionality, your DomainTools API key should include access to the following: Iris Enrich API, Iris Investigate API, and PhishEye API.

For app versions 4.3+, if your DomainTools API key is provisioned for Iris Detect, you can triage and monitor domains directly within Splunk. Additionally, if you have a Farsight DNSDB API key, you can now perform DNSDB pDNS lookups directly within the DomainTools App.

Limited app functionality is available for users with Iris Enrich API and Iris Investigate API access. Notably, management of PhishEye monitors, importing PhishEye & Iris Detect terms, and ingesting PhishEye & Iris Detect discoveries into Splunk will not be available.

Firewall Rule

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 reach out to us so we can help verify any additional IP allow-listing activities that may be needed.

> *If you are on a managed infrastructure and cannot connect to the DomainTools endpoint, please reach out to us so we can help verify any additional IP allow-listing activities that may be needed.*

Upgrading From Previous Versions

For most customers, Versions 4.x can be safely upgraded in-place. Customers using an older version should review the *Uninstalling Prior Versions* section in this User Guide. In all cases, please review the release notes of

respective versions to be aware of any breaking changes in your environment. You may also contact DomainTools Support for assistance with the app installation.

Upgrade note for Splunk Cloud users:
We have observed that users using self-service app installation sometimes run into issues installing the components of the app needed on indexers. The installation proceeds normally, but attempts to run `dtdomainextract` return an error. This may be due to Splunk's documentation indicating that self-service only installs apps on search heads. Please see the associated known issue and workarounds.

Upgrade note for users of v4.1.2 using a scpv2 workaround:

A fresh uninstall and reinstall would remove the workaround, but would also remove DomainTools-specific settings and enrichment data. To upgrade manually revert the scpv2 workaround follow these steps:

1. Remove the following stanza from local/commands.conf

```
[dtdomainextract]
type = python
filename = domain_extract_scp1.py
streaming = true
local = true
passauth = true
chunked = false
```

2. Deploy the configuration change to all Search Heads.

3. Restart Splunk.

Splunk Credentials to Install App

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

You may also need command-line access (like SSH access) 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 PhishEye/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 version of the DomainTools app, we recommend uninstalling the older version first and performing a fresh installation when migrating to version 4 and above.

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

`dtdomainextract` return an error. This may be due to Splunk's [documentation](#) indicating that self-service only installs 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 2019
    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:
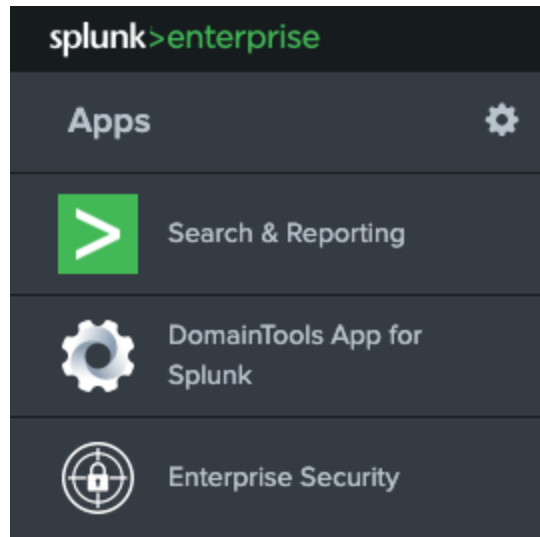
DomainTools App shown on a successful installation

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:

```
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 | dtdomainextract field_in=url field_out=domain | eval
domain=lower(domain) | fields url src dest log_source domain
_time
```

The app natively supports logs with multivalue URLs (as of v4.2) contained in a single event entry, commonly seen in Proofpoint logs. Users who previously may have used `mvexpand url` to workaround this issue can remove that command to have the urls more accurately reported as a single event.

Version 4.2 also introduced a regex-based `dtdomainextract2` macro available for high-throughput environments that 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 mis-identified as a domain. Note that `mvexpand url` would still be needed with `dtdomainextract2` in environments processing multivalue 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 | `dtdomainextract2` | 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 `dtdomainextract` 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*.
3. Select the **Save** button.

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:

Test Base Search

URL ⇕	Source ⇕	Destination ⇕	Log Source ⇕	Domain Name ⇕	_time ⇕
http://028Y4.KcfYvWwH.9362388.com/	10.10.130.58	http://028Y4.KcfYvWwH.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://07OC1.gJsRKLgD.recordvnotes.live/	10.10.186.68	http://07OC1.gJsRKLgD.recordvnotes.live/	udp:5140	recordvnotes.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://0FO73.nLgSEoxO.9951026.cc/	10.10.177.119	http://0FO73.nLgSEoxO.9951026.cc/	udp:5140	9951026.cc	2020-09-25 13:00
http://0GKPG.MkkRGGwZ.knull.info/	10.10.74.126	http://0GKPG.MkkRGGwZ.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.jnjy68.com/	10.10.77.176	http://0KNJ7.IRebrBWX.jnjy68.com/	udp:5140	jnjy68.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

The API Key dashboard

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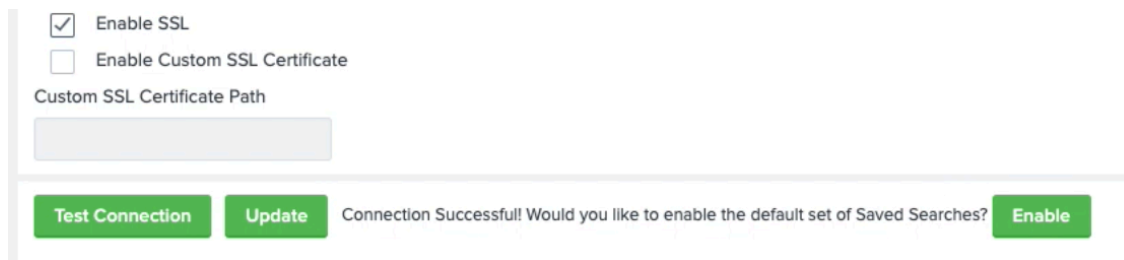
Adding SSL:
1. Configure SSL details in the same *API Key* section.
2. Select *Enable Custom SSL Certificate* and add the path in the *Custom SSL Certificate Path* field.

Configure Saved Searches

The app uses a series of Saved Searches to automate 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. Clicking enable will turn on the set of seven minimum required saved searches for the Core App functionality noted in the saved searches table.

Prompt on the API key page to enable the base set of Saved Searches

To enable PhishEye and Iris Detect capabilities or alerting in Splunk Enterprise Security, you will need to enable additional saved searches outlined in the table.

To manage 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.
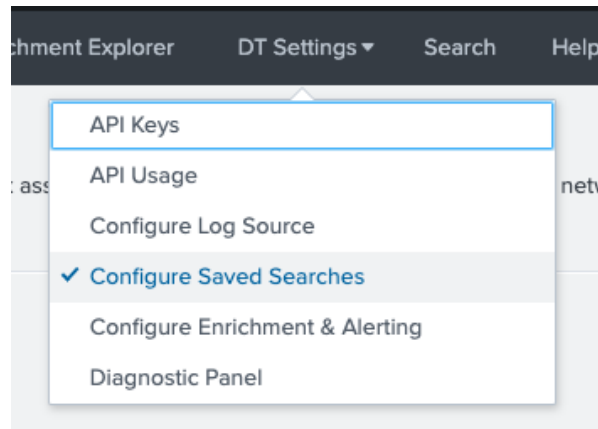
"Configure Saved Searches" menu item

Perform the following steps to enable a Saved Search:
1. Click on the *Edit* button
2. Select *Edit Schedule*:

"Edit Schedule" menu item

3. Check *Enable and Schedule*:

Enable and Schedule a report to activate the saved search.

4. Click **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 at this time. IPs sent to the enrich API 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. Please see 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
> ```

Performance considerations:
- 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.

Configuring Base Search in Search Head Environments
- There is a known issue concerning Search Head environments affecting version 4.1 of the app. Please see the Issue Tracker in the *Troubleshooting and Known Issues* section.
- In later versions, most search head issues arise from an incorrect or incomplete installation of the app on the search head. Full removal and reinstallation are recommended when feasible.

Table: 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	1. No post-install customization or configuration required, other than the API username and key initial	1. Requires CIM compliant data sources that use the Web data model with hostnames in the *Web.url* field.

	app setup.	2. DomainTools Threat Hunting Dashboard will be empty if the base search can't find domains.
	2. Finds domain names in every CIM-compliant data source from the Web data model.	3. Must have acceleration turned on for the Web data model.
	3. Fast for most environments.	
Custom SPL	1. Does not require your data source to be CIM compliant.	1. May cause performance problems if the search is not manually optimized.
	2. Can be optimized to your environment and data sources.	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 *Notable Events*, which are events generated by DomainTools detection rules.

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:

Table: Enrichment Field Name and Label

Enrichment Field Name	Label
dt_num_of_times_enriched	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. If you wish to customize the Enrichment Settings:
1. Go to **DT Settings → Configure Enrichment & Alerting**.
2. Once any of the following settings are changed, select the **Save** button.

Enrichment and Alerting
- Select the **Queue Wait Time**.
  - Queue Wait Time is how often the app enriches Domain information. Default is 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.
- Configure the **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.

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.
  - *Threat Profile Score Threshold* (default value of 90)
    - If desired, a different threshold can be set for DomainTools ML-based scores than proximity scores. Threat Profile encompasses Phishing, Spam, and Malware indicators.
  - *Proximity Score Threshold* (default value of 75)
    - If desired, a different threshold can be set for DomainTools proximity score, which examines how closely connected a domain is to other known-bad domains.
- *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 (only for Splunk Enterprise Security)
This functionality only applies to customers with access to Splunk Enterprise Security. To generate notable events and enable alerts:

1. Select the *Create Notable Event* checkbox under the *Alert Settings* section.
2. Select or deselect relevant *Alert Rule Configurations* criteria under the *DomainTools Domain Monitoring* section. **Note that the *DomainTools Blocklisted Domains* section has been removed in the 4.1.1 release.**
   a. When multiple criteria are selected, they narrow down the alert generation rule. In other words, they form a logical 'AND' narrowing.
      i. Only Monitor Domains in the DomainTools Monitoring list (default) - an alert will only fire against domains that have been added to the [monitoring list]().
      ii. Exceeds Domains Risk Score Threshold - Only alert if the domain exceeds the risk threshold defined above.
      iii. Exceeds Domain Threat Profile Score Threshold - Only alert if the domain exceeds the threat profile threshold defined above.
      iv. Ignore Iris Detect Domains in DomainTools Monitoring list - ignores anything in the monitoring list where the Source equals "Iris Detect".
      v. Ignore PhishEye Domains in DomainTools Monitoring list - ignores anything in the monitoring list where the Source equals "PhishEye".
      vi. 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.
      vii. Select the **Urgency Tag** to associate with the Notable Event - applies the specified urgency level within Splunk Enterprise Security's Incident Review panel.
   b. Monitor young domains - creates a notable event whenever a young domain (lower than the young domain threshold) is observed.
      i. Optionally this can be restricted to new domains on the [monitoring list](). This is useful in conjunction with PhishEye monitors that can keep track of newly registered domains.
      ii. Similarly, select the separate **Urgency Tag** to associate with the "young domains" Notable Event - applies the specified urgency level within Splunk Enterprise Security's Incident Review panel.

Since version 4.2, investigate a domain directly from the Enterprise Security *Incident Review*. See [Investigate Domains Within Incident Review](#) for more information.

Set Up Monitoring for Domains

You can monitor domains by adding them manually in the app. You can also leverage PhishEye capabilities if you have access to the PhishEye API.

Manage Monitored Domains
A centralized Monitoring List which allows you to monitor domains manually or leveraging DomainTools Iris Detect and PhishEye capabilities.

Domain Name ⇕	Last Updated Date Time ⇕	Last Updated By ⇕	Added Date Time ▲	Added By ⇕	Source ⇕	Action ⇕
office365.services	2023-03-29T16:17:11.846Z	admin	2023-03-29T16:17:11.846Z	admin	admin	Remove
int-chase.com	2023-03-29T16:17:25.258Z	admin	2023-03-29T16:17:25.258Z	admin	admin	Remove
pepsicog.com	2023-03-29T16:17:43.046Z	admin	2023-03-29T16:17:43.046Z	admin	admin	Remove
ccbkint.com	2023-03-29T16:17:52.394Z	admin	2023-03-29T16:17:52.394Z	admin	admin	Remove
amazon-account-security-support.com	2023-03-29T16:18:04.684Z	admin	2023-03-29T16:18:04.684Z	admin	admin	Remove
applecokr.com	2023-03-29T16:18:17.186Z	admin	2023-03-29T16:18:17.186Z	admin	admin	Remove
citibanking.com	2023-03-29T16:18:25.476Z	admin	2023-03-29T16:18:25.476Z	admin	admin	Remove
anaeon.icu	2023-03-29T16:18:45.342Z	admin	2023-03-29T16:18:45.342Z	admin	admin	Remove
1manager-reactivation-commbank.com	2023-03-29T16:19:38.227Z	admin	2023-03-29T16:19:38.227Z	admin	admin	Remove
3dsecured-wellsfargo.tk	2023-03-29T16:19:51.593Z	admin	2023-03-29T16:19:51.593Z	admin	admin	Remove

‹ Prev 1 2 Next ›

Domain Monitoring page

To configure and change your centralized *Monitoring List*:

1. Go to the *Manage Monitored Domains* page via **Monitoring → Manage Monitored Domains**.
2. In the *Add to Monitoring* section, add the domain (like example.com).
   a. Multiple domains are separated with a comma (like example.com,domaintools.com).
3. Select the Source:
   a. *Current User* that is attributed to the Splunk account adding the domain.
   b. *PhishEye*, to leverage the PhishEye API. An API license is required.
   c. *Custom*, which is added as a customized field.
4. Select the **Add** button to submit.
   a. Subsequently to remove, use the **Remove** or **Remove Selected** options.
5. Confirm that the domain is in the *Monitoring List.*

Enterprise Security users can create notable events when a monitored domain is observed in the logs under **DT Settings → Configure Enrichment & Alerting**:

Example setup to create a high-urgency notable event when a domain in the Monitoring List is observed in the logs

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.

The Manage Monitored Tags page with examples of Tags being monitored

To monitor for Iris-tagged domains in Splunk:
1. Go to the *Manage Monitored Tags* page via **Monitoring → Manage Monitored Tags**.
2. Add the Tag(s) to be added to the proactive monitoring list.
3. Select the **Add** button.

Once tags are added, domains that share the same tag in Iris are monitored in Splunk. The *Tags List* offers the following fields:
- *Tag Being Monitored* - Name of the Tag.
- *Last Updated Date Time* - When the Tag was updated.
- *Last Updated By* - The Splunk username that updated the Tag.
- *Added Date Time* - When the Tag was added.
- *Added By* - The Splunk username that added the Tag.

- *Action* - Option to remove the Tag from Splunk only.

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.

Screenshot of the Manage Allowlist page

To add or remove domains in the Allowlist:
1. Go to **Monitoring** → **Manage Allowlist**
2. Use the pull-down to select the desired behavior for domains in the allowlist:
   a. *Exclude from alerts and dashboards (default)*
      i. Domains in the allowlist won't be counted towards dashboard visuals, or alerts, if configured
   b. *Exclude from alerts*
      i. Domains won't be alerted on (applies to users of Splunk Enterprise Security only), but will still appear in dashboard visuals
   c. *Exclude from dashboards*
      i. Domains won't appear in dashboard visuals but will still appear in alerts (applies to users of Splunk Enterprise Security only)
   d. *Exclude from all enrichment*
      i. Fully ignores the domain in all enrichment, alerts, and visuals
   e. *Do Nothing*
      i. Allowlist is informational-only. Domains remain enriched, alerted upon, and appear in dashboard visuals. This setting can be helpful for temporary use when debugging.
3. Add the SLD.TLD format of domain (such as example.com or example[.]com), or list of domains separated by a comma (such as domaintools.com,example.com).
4. Click the **Add** button and confirm the selection.
5. Use the **Remove** button or **Remove Selected** options to individually remove domains.

Successfully added domains will show in the *Allowlist* along with:

- *Domain Name*
- *Last Updated Date Time*
- *Last Updated By*
- *Added Date Time*
- *Added By*
- *Action*

Configure Iris Detect

Iris Detect is a new product launched by DomainTools in 2022 to discover and monitor lookalike domains. Iris Detect integration was added to the DomainTools App for Splunk as of version 4.3. Note that it replaces the PhishEye product that was removed from the Splunk app with version 4.4. It provides a superset of the functionality of PhishEye with new domain infrastructure collected and processed within minutes.

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. Under the API Keys page (**DT Settings → API Keys**), click on **Test Connection**. You should see a set of iris-detect-*APIs listed:

"Test Connection" results showing the full set of Iris Detect APIs enabled

The minimum set of Iris Detect APIs needed on the Splunk account (in addition to `iris-enrich` and `iris-investigate` used for base product functionality) are:

- `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 Browse.

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**).

Iris Detect Monitored Terms

This page shows all of the Iris Detect monitored terms on your account. You can set up and configure monitored terms at https://iris.domaintools.com/detect/ then click the "Refresh Now" button to update this page. New and changed domains matching those terms will be ingested for monitoring and alerting within the DomainTools Splunk App. You can monitor the results for the enabled terms on the "Iris Detect" page.

Refresh Monitored Terms ⓘ

| Never ▾ | ✕ | **Submit** |

Refresh Now

Iris Detect Monitored Terms ⓘ

Term ⇕	Monitor Creation Date ⇕	Created By ⇕	Monitor Last Updated In Splunk ⇕	Ingest Daily Detections in Splunk ⇕
bank	2022-05-02 21:29:26	admin@domaintools.com	2023-03-29 16:40:11	Enabled

The Iris Detect Monitored Terms page

Monitoring for Daily or Weekly Monitored Terms

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.
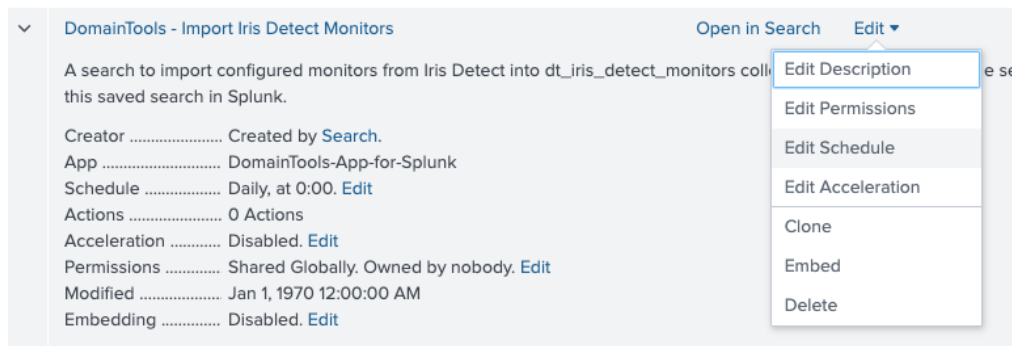
Set a schedule to automatically sync the Iris Detect monitored terms list inside splunk with those set up in the Iris Detect UI

Reading the Iris Detect Monitored Terms Table

- **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.

Once you have at least one monitor enabled, you view the results under the *Iris Detect Dashboard* page the next time the data is refreshed.

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.

Manually refresh the Iris Detect Results from the Iris Detect Dashboard

Reading the Iris Detect Results

Use the *Monitored Term* filter at the top of the page to view the results for all monitors or a selected monitor. Use the *Time Range Filter* to filter 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.

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.
- *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* - Sometimes called "Lifecycle First Seen", this is 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.

Additionally, there are actions available to help triage discovered domains:
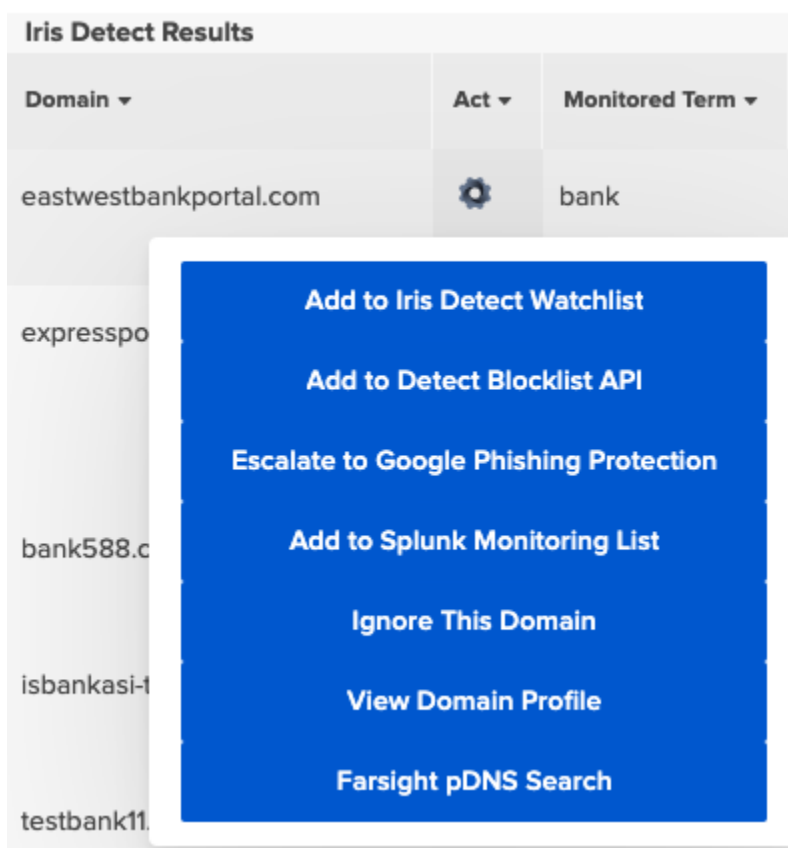
Actions available within the Iris Detect Results table

The available actions are (listed top to bottom):
- *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. You can synchronize the Iris Detect Watch List with the Monitored Domains List under **Monitoring → Managed Monitored Domains**:

Automatic Sync

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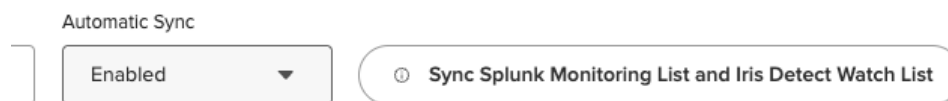
Synchronize the Splunk Monitoring with the Iris Detect Watch List either automatically or on a one-time basis to enable further enrichment and alerting

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. Pressing the "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:
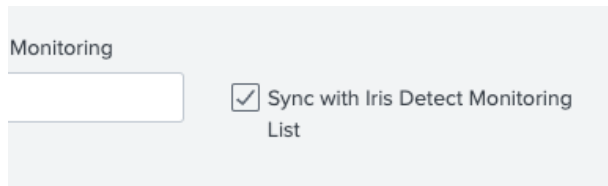
Available option to synchronize the Iris Detect Watchlist and Splunk Monitoring list

Clicking that checkbox is the same as selecting Automatic Sync to enabled. Both pages mirror the same setting.

See the *Set up Monitoring* section for more details and to set up alerting against monitored domains.

Configure PhishEye Detection (removed in v4.4+)

PhishEye remains supported within the DomainTools App for Splunk versions 4.1-4.3, but we encourage all users to migrate workflows to Iris Detect (supported from v4.3+).

Manage your PhishEye monitors, import terms, or ingest discoveries into Splunk in order to leverage PhishEye detection capabilities.

1. Go to **Monitoring** → **PhishEye** to access the section.
2. Add the PhishEye API.

The PhishEye monitoring page

Monitoring for Daily or Weekly Detections

Under the *Refresh Monitors* section:

1. Change the frequency to *Never*, *Daily* or *Weekly* to refresh the terms from DomainTools PhishEye.
2. Select the **Save** button to confirm.

Import new PhishEye Terms Manually

Under the *Refresh Monitors* section:
3. Select the **Refresh Now** button to import any new terms.
4. Alternatively, set up a *Daily* or *Weekly* frequency.

Reading the PhishEye Terms Table

- **Term** - The term itself as it appears on PhishEye.
- **Term Last Updated On** - The date as to when the term was refreshed, either manually or via the Daily or Weekly detections.
- **Ingest Daily Detections in Splunk** - Select the term(s) to ingest PhishEye-monitored domains into Splunk.

Reading the PhishEye Results

PhishEye results can be manually fetched for that same day or automatically checked if monitoring is enabled. If results already exist for that day, then the table will reload the data.

Select the drop down to view the results for all monitored terms or a selected term. When new domains are discovered for the Enabled Terms, they are added in the results with these fields:
- *Domain* - The full domain name including TLD.
- *Risk Score* - The DomainTools Risk Score.
- *Created Date* - The domain creation date.
- *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.
- *Registrar Name* - The registrant name. From Whois, so data may not be available.
- *Registrar Email* - The registrant email. From Whois, so data may not be available.
- *Monitor Domain* - Adds the domain to your [Monitoring List](#).

Example showing the PhishEye Results pane and option to enable monitoring

Manually Adding PhishEye Domains

The Monitoring Page supports manually adding domains and tagging them with the PhishEye source. To manually add individual domains, go to the *Manage Monitored Domains* page via **Monitoring→ Manage Monitored Domains**.

1. In the *Add to Monitoring* section, add a domain or comma-separated list of up to 100 domains in the SLD.TLD format, such as example.com or example[.]com.
2. Select *PhishEye* as a source.
3. Select *Add*, and confirm that the domain is shown in the *Monitoring List* table.

See the *Set up Monitoring* section for more details.

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.

New as of version 4.2: 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.
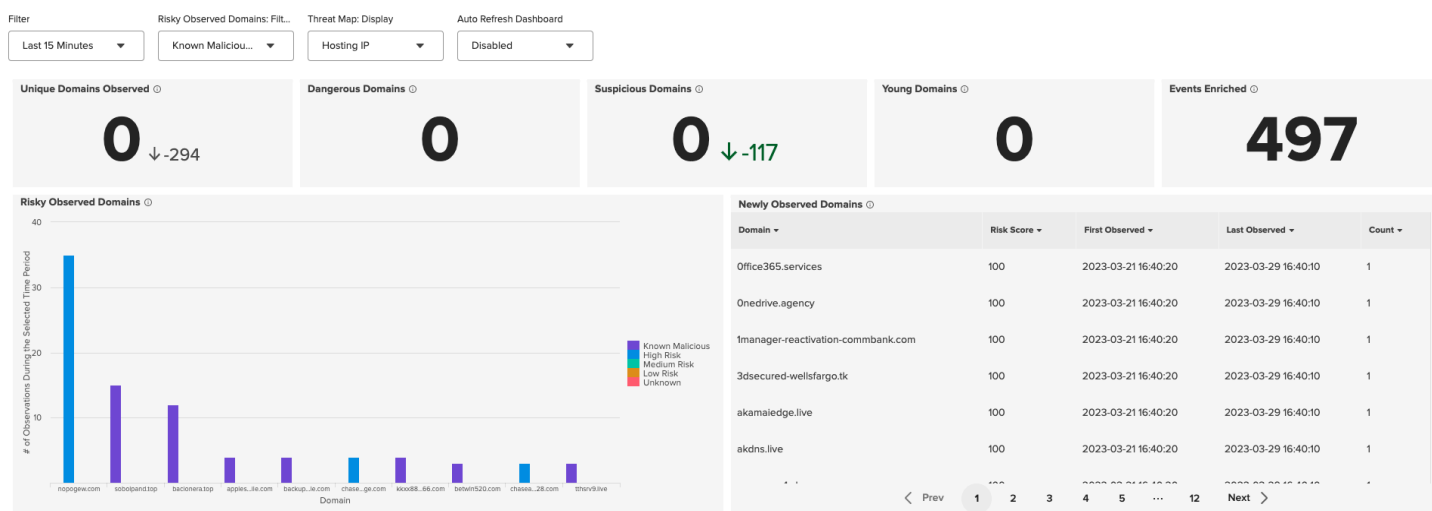
The Threat Intelligence Dashboard with Unique Domains Observed, Dangerous Domains, Suspicious Domains, Young Domains, Events Enriched, Risky Domains and Newly Observed Domains panels

Interacting With and Reading the Dashboard Panels

The Threat Profile dashboard panels provide insights based on Splunk Timecharts (see 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*
  - As of version 4.2+, this panel replaces the *Active Domains* panel. It graphs the number of events associated with domains observed in your network during the selected time period by DomainTools Risk Score levels. 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 select these options:
- *Open in Search* - Displays all the time buckets and respective sub-totals.
- *Inspect* - Open the Search job inspector window.
- *Refresh* - Fetch new results and update the panel.
- Clicking on the results opens a new search in order to drill down on further information.

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.

The dashboard panels use the *timechart* command to provide the aforementioned trends for:
- Threat Intelligence Dashboard
  - *Unique Domains Observed*
  - *Dangerous Domains*
  - *Suspicious Domains*
  - *Young Domains*
- Monitoring Dashboard
  - *Detected Domains*
  - *Tagged Suspicious Domains*
  - *PhishEye Domains Observed*
  - *Total Alerts Generated*
  - *Total Events Monitored*
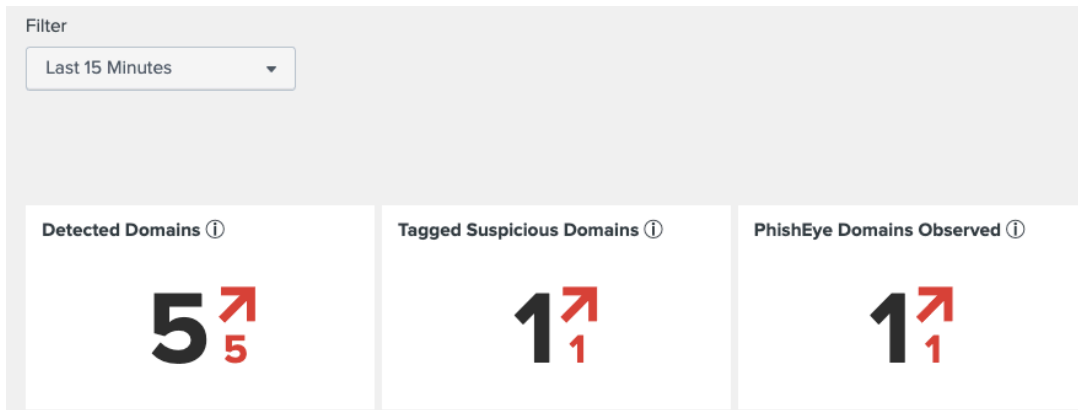
Example of 'Detected Domains' panel with a time filter of 15 minutes applied to the Monitoring Dashboard

In the above *Detected Domains* panel:
- The black '5' reflects the number of domains detected in the latest time-bucket, 15 minutes in this case.
- The red '5' reflects the increase in the number of domains observed since the last time-bucket, 15 minutes.
- The upward arrow icon indicates an increase in trend.
- The red color indicates that the increase represents a less desirable 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. A few of the more frequently-used commands are defined below:

Command	Description	Example(s)

`dtdomainextract`	Extracts a domain out of a URL field, based on the tldextract 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 dtdomainextract command or the dtdomainextract2 macro	`| dtdomainextract`
		`field_in=url`
		`field_out=domain`

`dtirisenrich`	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. [**New**] in 4.4 add inline_results to keep event data inline	`| makeresults	eval` `domain="domaintools.com" |` `dtirisenrich domain=domain` `inline_results=true`

`dtirisinvestigate`	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	`| dtirisinvestigate domain="domaintools.com"`
		
		`| dtirisinvestigate pivot_type="ip" pivot_value="199.30.228.112"`

`dtformatinvestigate`	Formats the JSON returned by an Iris Investigate query into a row with component names. Use the `output` parameter to specify the section of the response to format	`| dtirisinvestigate domain="domaintools.com" | dtformatinvestigate output=risk | table risk_score type`
`dtdnsdb`	Queries DNSDB for Passive DNS information against a given IP, Domain, Hostname, or Subnet.	`| dtdnsdb target=198.51.100.1 type="rdata"`
`dtdnsdbflex`	Performs a DNSDB Passive DNS Flexible Search.	`| dtdnsdbflex query_type=rdata match_type=regex query="^domaintools\.com\.$"`
`dtdnsdblimit`	Returns the dnsdb api query limit, number of queries remaining, as well as the time the remaining queries will reset.	`| dtdnsdblimit`
`dtdnsdbenrich`	Enrich the Splunk events returned by a given SPL_QUERY with Passive DNS information reported by Farsight DNSDB, part of DomainTools.	`… | dtdnsdbenrich field_in=domain field_type=domain lookup_type=rrset`

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.

You can 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_fooyn_timestamp AS first_observed,
dt_looyn_timestamp 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_fooyn_timestamp AS first_observed,
dt_looyn_timestamp 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 | 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_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
| dtdomainextract 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:

1. Go to **Investigate** → **Domain Profile**.
2. Add the domain in SLD.TLD format (example.com or example[.]com).

a. Lookup for *subdomains* is not currently supported.
3. Click **Submit**.

Domain Profile of an example high Risk Score domain

The Domain Profile options are:
1. *Add to or Remove from Monitoring List*
2. *Add to or Remove from Allowlist*
3. *Open in Iris Investigate* - this will open a new window with the *Iris Inspect* pane for an in-depth investigation into the domain.
    a. Additional investigation features include: *Domain Profile*, *Screenshot History*, *Whois History*, *Hosting History* and *SSL Profile*. See the [Iris User Guide](#) for more information
4. *Farsight pDNS Standard Search* - this will open a new window with a passiveDNS search for the queried domain. Note that a separate DNSDB API key is required and should be entered on the API Keys page

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 blocklist. *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. See the *Set Up Monitoring for Domains with Iris Tags* section for more information.

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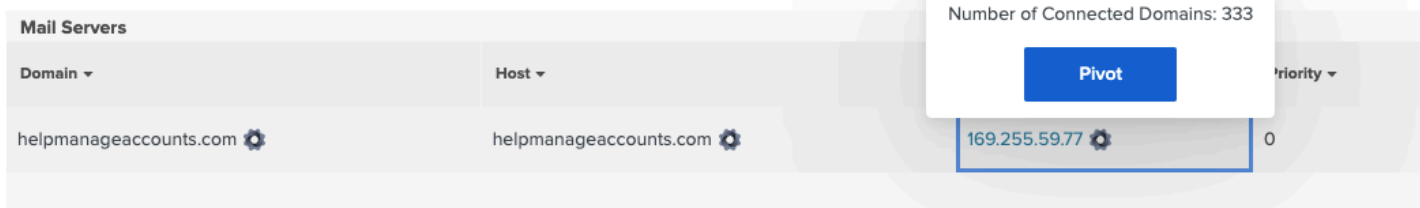
Connected Infrastructure information (such as Mail Servers, IP addresses, SPF information, Name Servers, SSL information, Registrar/Registry) are gleaned from DomainTools datasets.

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.

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.

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**.
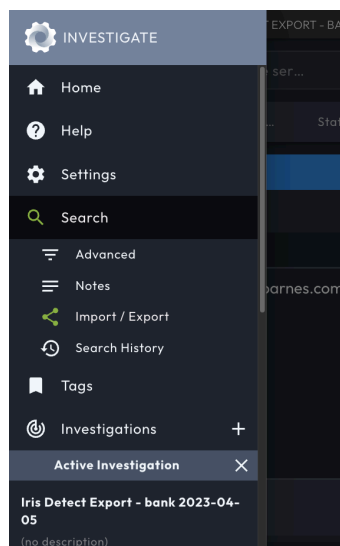
Iris Investigate UI menu location of the Import/Export item

2. The subsequent dialog contains the Search Hash to export. Click the copy icon next to the *Current Search Export* section:
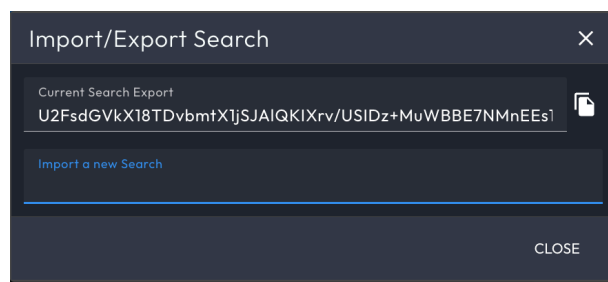
Example search hash to export from the Iris Investigate UI

3. Back in the DomainTools Splunk App, go to **Investigate** → select **Import from Iris Investigate**.
4. Paste the copied *Search Hash* in the input field.
5. Click the **Submit** button. 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

Domains are imported with the following fields:
- *Domain*
- *Risk Score*
- *Proximity*
- *Threat Profile*
- *Threat Profile Malware*
- *Threat Profile Phishing*
- *Threat Profile Spam*
- *Create Date*
- *Monitor*
- *Allowlist*

Farsight DNSDB pDNS Searching

(introduced in version 4.3) Investigate current and historical domain infrastructure with Passive DNS (pDNS) using Farsight's DNSDB Standard or Flexible search (API Key Required). Please contact sales@domaintools.com for provisioning.

DNSDB is a database that stores and indexes both the passive DNS data available via Farsight Security's Security Information Exchange 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. The full documentation is maintained here.

Farsight pDNS Standard Search
Farsight DNSDB Documentation

Time Range		Resource Record Type (RRType) ⓘ	OR Add Custom RRTYPE	IP or Domain Name ⓘ		
All time	▾	Any ▾	ANY	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.fsi.io.	PTR	⧉ farsightsecurity.com.	N/A	N/A	set	7
07/01/13 03:53:50	07/30/13 21:41:15	⧉ 7.0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.6.6.0.0.1.0.0.0.8.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 ⇕	bailiwick ⇕	RData ⇕	Time First ⇕	Time Last ⇕	rrset_tok ⇕	Count ⇕
08/05/20 22:51:16	06/03/22 22:50:25	⧉ 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	⧉ farsightsecurity.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 much more powerful searching capabilities (e.g. wildcards, regular expressions) than Standard Search, but the results will not be as "full" as the results from Standard Search. Documentation for flexible searching is maintained [here](#).

Farsight pDNS Flexible Search
Flexible Search Documentation

Select a time range		Query ⓘ	Query type ⓘ	Match type ⓘ	Resource Record Type (RRType) ⓘ		
All time	▾	domaintools	RDATA (Right-Hand) ▾	Regex ▾	Any ▾	Submit	Hide Filters

rdata ⇕	rrtype ⇕	raw_rdata ⇕
0 0 5222 jabber.domaintools.com.	SRV	00000001465066A61626265720B646F6D61696E746F6F6C7303636F6D00
0 0 5269 jabber.domaintools.com.	SRV	00000001495066A61626265720B646F6D61696E746F6F6C7303636F6D00
0 mail.domaintools.co.uk.	MX	0000046D61696C0B646F6D61696E746F6F6C7302636F6F82756B00
0 mail.domaintools.top.	MX	0000046D61696C0B646F6D61696E746F6F6C7303746F7000
0 mail.adomaintools.com.	MX	0000046D61696C0C61646F6D61696E746F6F6C7303636F6D00
0 mail.domaintoolsplus.com.	MX	0000046D61696C0F646F6D61696E746F6F6C73706C757303636F6D00

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 Example:
  - Bank
  - north.*bank

  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

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

Splunk Enterprise Security customers using the DomainTools app can investigate any domain or URL listed in an Incident Review event with a couple clicks. (Note that URLs are shortened to a domain lookup).

1. Expand the arrow on the incident review event.
2. Next to a domain or URL, expand the arrow under *Action* .
3. View the domaintools domain profile within Splunk, or on the Iris platform.
4. View Passive DNS traffic to the domain in DNSDB.

Domain Monitoring Dashboard

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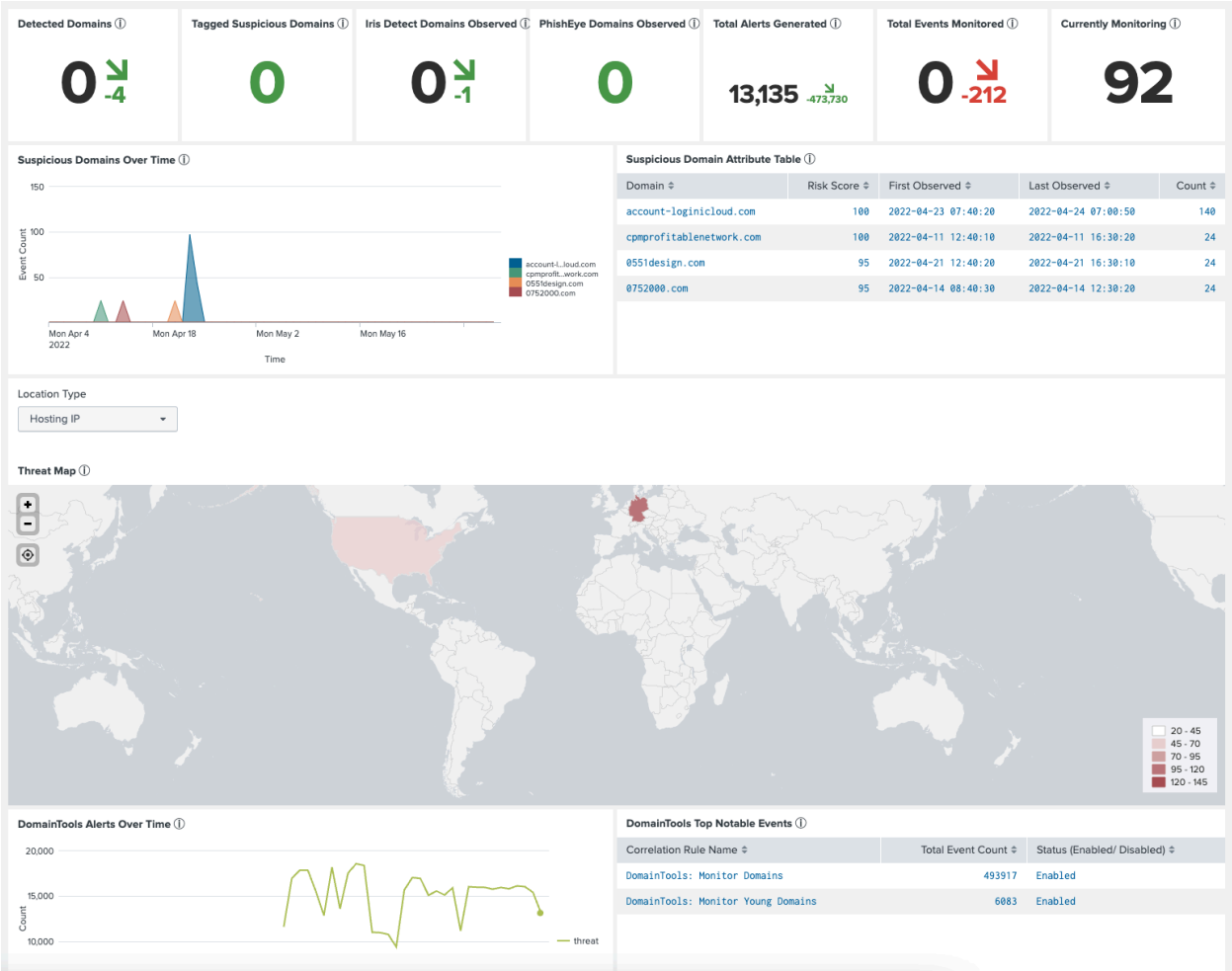
Domain Monitoring Dashboard

Interacting With and Reading the Dashboard Panels

Hover for the tooltips about the panel sections and click on 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 clicking on the Alerts Generated panel.

Since version 4.2, 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.
- [versions 4.3+] *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.
- *PhishEye Domains Observed* - Domains discovered by DomainTools PhishEye 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.

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.

Clicking on 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.

Tip: If the intelligence 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

Troubleshooting & Known Issues

Enabling Logging

Since version 4.2, logging is disabled by default. To enable logging to help with diagnostics, go to **DT Settings** → **Diagnostic Panel** and click **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
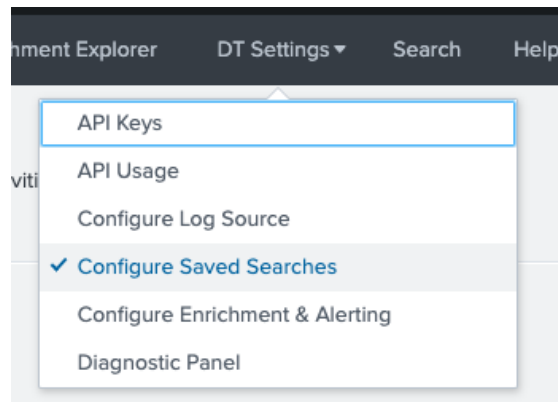
Compare the scheduled time on the resulting set of reports against the table of Saved Search Names and Descriptions in Appendix A to ensure the required core app saved searches, as well as the additional ones if required for PhishEye or Alerting in Splunk Enterprise Security are enabled.

Configure Saved Searches page showing a single report disabled.

Issue Tracker

DomainTools will continue to monitor the feasibility of these known issues and make adjustments as needed to accommodate various Splunk deployment scenarios/environments.

For reproducible issues, we have included the Bug ID for your convenience. We will address these Bugs in subsequent product releases.

The list below contains all known issues and each contains a workaround or resolution step as appropriate

ID	Issue Overview	Bug ID
1	Base Search configuration fails with `dtdomainextract` error on v4.0 or v4.1	ID-724
2	Event parsing fails with the error "*Failed to send message to external search command, see search.log*".	n/a
3	Entering proxy authentication in the app configuration page. (Fixed in v4.1.3)	ID-678
4	*"Invalid key in stanza"* warning displayed under Splunk 7	n/a
5	"Error in 'dtdomainextract' command" on Splunk Cloud installations (Fixed in v4.3)	ID-1370
6	Recent events appear to be "missing" from the Threat Intelligence or Monitoring Dashboards	n/a
7	All dashboard panels are stuck "Loading Results…"	INT-236
8	Capitalized URLs or special characters in the domain can cause saved searches to fail	INT-1803
9	A custom JavaScript error caused an issue loading your dashboard	ID-1793

Issue Details

Base Search configuration fails with 'dtdomainextract' error on version v4.0 or v4.1

This issue has been addressed in the 4.1.1 release, and the workaround is no longer needed for up-to-date installations.

While configuring the base search in version 4.1, the app throws the below exception:

```
Error in 'dtdomainextract' command: External search command exited unexpectedly with
non-zero error code 1..
```

```
index=main
| table _time url source src
| dtdomainextract field_in=url field_out=domain
| eval domain=lower(domain)
| eval dest=url, log_source=source
| fields url src dest log_source domain _time
| dedup domain
| stats latest(_time) as looyn, earliest(_time) as fooyn by domain
```

⚠️ 3 errors occurred while the search was executing. Therefore, search results might be incomplete. Hide errors.

- [idx-i-03249474244d186f3.domaintools.splunkcloud.com] Streamed search execute failed because: Error in 'dtdomainextract' command: External search command exited unexpectedly with non-zero error code 1..
- [idx-i-090b6a5120ebb1799.domaintools.splunkcloud.com] Streamed search execute failed because: Error in 'dtdomainextract' command: External search command exited unexpectedly with non-zero error code 1..
- [idx-i-0f89f9180cfe43b04.domaintools.splunkcloud.com] Streamed search execute failed because: Error in 'dtdomainextract' command: External search command exited unexpectedly with non-zero error code 1..

Screenshot of error messages thrown for the base search configuration fail issue.

Environments & Scenarios Observed

In cluster environments, and when solely using a streaming command without any non-streaming commands before using `dtdomainextract` command in the base search.

Reasoning

The `dtdomainextract` is a streaming command and by default, it attempts to run in the indexer. Using |*localop* will force `dtdomainextract` to run in the search head.

Workaround

Add '| *localop*' command to the base search to force *dtdomainextract* command to run locally on the search head.

> Example:
> ```
> index=main
> | table _time url source src
> | localop
> | dtdomainextract field_in=url field_out=domain
> ```

Event parsing fails with the error "Failed to send message to external search command, see search.log."

This issue has been addressed in the 4.1.3 release, and the workaround is no longer needed for up-to-date installations.

User may see this error in one of the below forms:

1. While parsing events in the UI:

    ```
    Error in 'dtdomainextract' command: Failed to send message to external search
    command, see search.log.
    ```

```
The search job has failed due to an error. You may be able to view the job in
the Job Inspector.
```


Screenshot of error messages thrown for the event parsing fail issue.

2. In the `search.log`:

```
ERROR ChunkedExternProcessor - Failure writing result chunk, buffer full.
External process possibly failed to read its stdin.
```

Reasoning:

There is a known [bug](#) in Splunk's new SCPv2 protocol causing any custom search commands using it to fail when processing large amounts of events.

A fix has been published by Splunk, which is reflected in the 4.1.3 update.

The resolution below will enable the `dtdomainextract` custom search command to use the SCPv1 version of our domain extract script.

Resolution:

1. Upgrade to 4.1.3 or above

Entering proxy authentication in the app configuration page

This issue has been addressed in the 4.1.1 release, and the workaround is no longer needed for up-to-date installations.

If you need to authenticate to the proxy server in version 4.1, there aren't explicit fields in the UI to capture this information.

Screenshot of API Key management page

Workaround:
You may enter the credentials in the *Proxy Server* input box and test connectivity.

```
https://username:password@172.16.1.1
```

Resolution:
1. Upgrade to a version 4.1.1 or above

"Invalid key in stanza" warning displayed under Splunk 7

If you elect to install the app on a Splunk 7 indexer cluster, it may report warnings about an invalid stanza key (python.version). This key is used in Splunk 8 to define the default python version, but ignored in Splunk 7. You may ignore these warnings.

"Error in 'dtdomainextract' command" on Splunk Cloud installations

We have received sporadic reports about an "Error in 'dtdomainextract' command..." issue on Splunk Cloud installations. The specific language of the error varies, but the overall theme is that the `dtdomainextract` custom search command fails when running on the indexer. The most straightforward way to confirm the

problem is with the indexer is by adding the `| localop` command before `dtdomainextract` to force the action to occur on the search head.

Reasoning:

The DomainTools app did not get fully installed on the indexer. Note that for users using self-service app installation, Splunk's [documentation suggests](#) the apps only get installed on the search heads, so you may be missing or running outdated libraries on the indexers.

Workarounds:

There are a few ways to work around the issue:
1) Open a ticket for Splunk support, asking them to fully install the app on the indexer. Our support team is available to help work with them. Contact us at enterprisesupport@domaintools.com
2) Force the data summarization to occur on the search head instead of the indexers by adding the `| localop` command to your base search under **DT Settings** → **Configure** → **Log Source**. This has a performance trade-off and may not be suitable for high-volume environments. Even if performance does not allow this to be an ongoing solution, this is a good way to confirm the issue is with the indexer installation.
3) Fully remove and reinstall the app, following the instructions in the [App Installation](#) section.

Resolution:

Unfortunately, the best option here is to work with Splunk support and ask their team to perform the upgrade manually, to version 4.3 or above. Version 4.3 adds the **distsearch.conf** file to force the required packages to distribute to the indexing tier.

Recent events appear to be missing from the Threat Intelligence or Monitoring Dashboards

When viewing the Threat Intelligence or Monitoring Dashboards on a 5 Minute, 15 Minute, or 2 Hour view, some events appear to be reflected in the dashboard display that don't appear on the 4 hour, daily, or multi-day views.
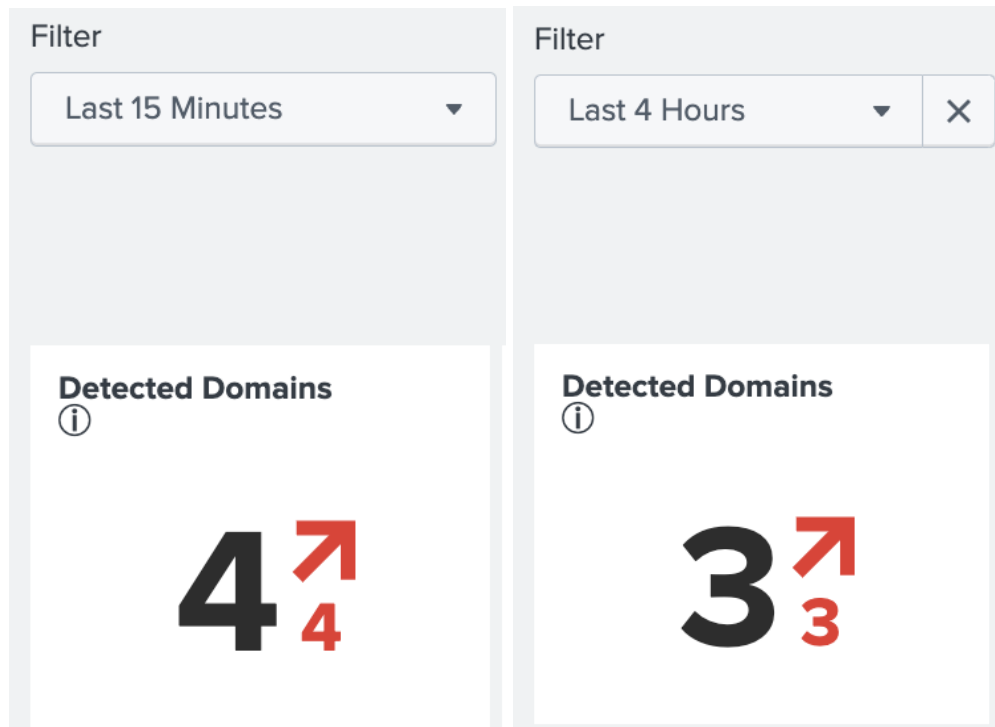
Example screenshots showing the lower "Detected Domains" count despite the larger time window filter.

Reasoning:

The Threat Intelligence and Monitoring Dashboard time charts use summary data to speed loading when viewing data at a 4-hour time period or above. Those summary statistics are triggered by the "DomainTools - Summary - Timechart count by domain with latest time" saved search that runs hourly by default. Due to this scheduling design, it's possible that an event can appear in a 15-minute or 2-hour view that doesn't (yet) appear in the 4-hour view until the scheduled saved search takes place.

Workaround:

Use the shorter time windows if more recent data is desired. Utilize the "Auto Refresh" feature in v4.2 or above to help keep tabs on the latest data.

Dashboard panels are stuck "Loading Results..."

Depending on the Splunk version, either dashboard panels are stuck on "Loading Results...", or entire pages of the app refusee to load, stuck at "Loading..."

Reasoning:

Splunk has deprecated HTML dashboards and older versions of jQuery. The DomainTools App for Splunk is heavily dependent on both up through version 4.3. Older versions can work around this through easing security restrictions, but version 4.4 resolves the issue.

Workaround:

Unrestrict **Unsupported Hotlinked Imports** (*Server settings* > *Internal Library Settings* > *Unsupported Hotlink Imports*), and on version 9.0+ also unrestrict *jQuery Libraries older than 3.5*.
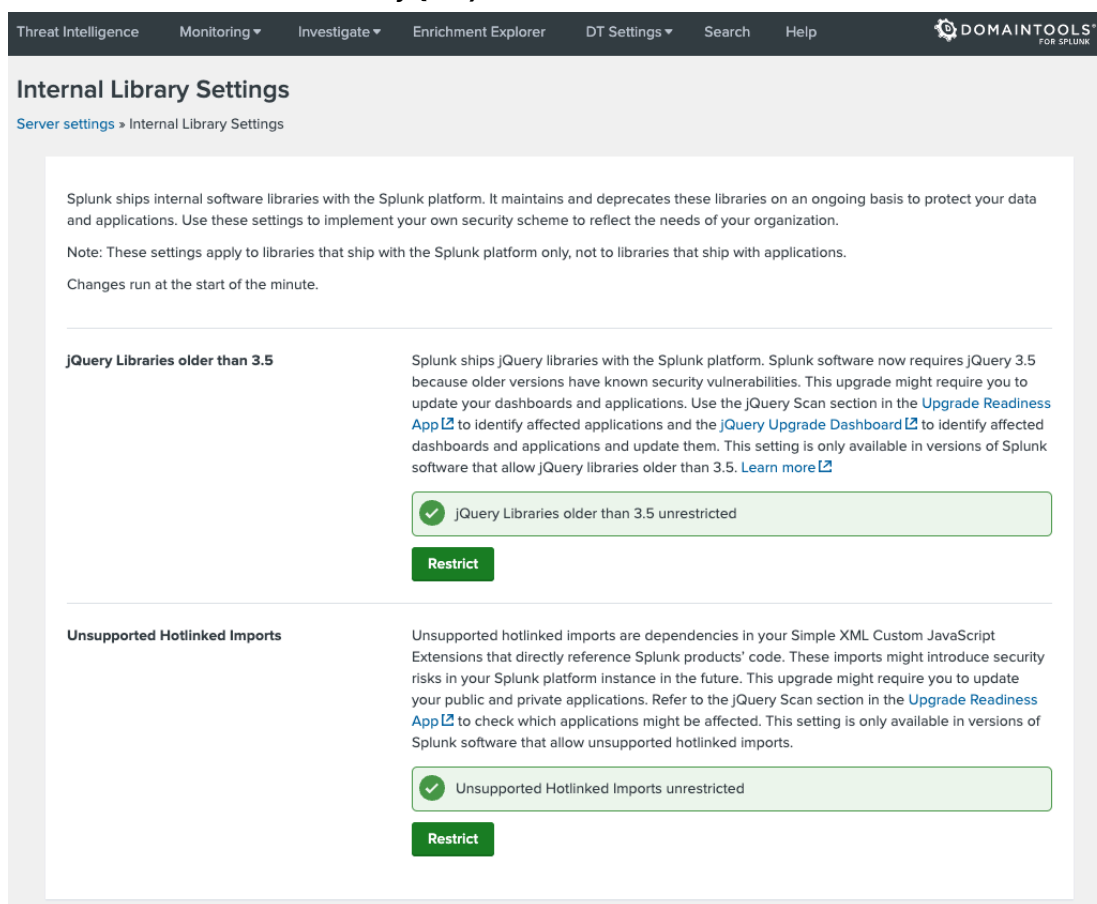
Recommended Splunk library settings as a short-term workaround

Solution:

Upgrade to version 4.4 or above. Version 4.4 of the app represents a complete rewrite of the frontend of the app in order to resolve this issue and no longer require the workaround above.

Capitalized URLs or special characters in the domain can cause saved searches to fail

In versions up through 4.3.1 of the DomainTools for Splunk app version, some capitalized letters in the URL or special characters in the domain can cause saved searches to fail with an error similar to the following:

```
The following error(s) and caution(s) occurred while the search ran. Therefore, search
results might be incomplete.

Found no results to append to collection 'dt_iris_enrich_data'.
InvalidCodepoint at "/app/splunk/lib/python3.7/site-packages/idna/core.py"...
```

In version 4.4.0 of the app, those same URLs are caught but logged as errors in the logs. up through 4.3.1 of the DomainTools for Splunk app version, some capitalized letters in the URL or

Reasoning:
While we make every effort to address the variety of logged URLs and domains that can show up in a monitoring environment, sometimes edge cases slip through our testing. Newer versions of our app will continue to improve parsing. In the interim, please see the Workaround section for a few options.

Workarounds:
A few workarounds are available to help mitigate these issues.

1. In case the errors are caused by URL capitalization, [modify your base search](#) to move the `| eval domain=lower(domain)` clause as close to the end of the base search as feasible, for example:

    ```
    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 | dtdomainextract field_in=url field_out=domain | eval
    domain=lower(domain) | fields url src dest log_source domain
    _time
    ```

    After making this change, you will need to clear the enrich_queue to remove the error-causing entries. Run:

    ```
    | outputlookup dt_iris_enrich_queue
    ```

2. If using version 4.2 or higher, replace dtdomainextract with the dtdomainextract2 macro. See [configuring Base Search](#) above for an example and the trade-offs. After making this change, you will need to clear the enrich_queue to remove the error-causing entries. Run:

    ```
    | outputlookup dt_iris_enrich_queue
    ```

Solution:
A fix will be available in a forthcoming release.

(Version 4.4+) A custom JavaScript error caused an issue loading your dashboard

After an upgrade to the DomainTools App for Splunk version 4.4+, when loading pages in the app, an error is displayed "A custom JavaScript error caused an issue loading your dashboard. Please see the developer console for more details". The page may or may not load fully.

Reasoning:
All the dashboards were rewritten from HTML to React and SimpleXML in version 4.4. The user's browser may have older versions of some Javascript libraries cached.

Workaround:
Clear the browser's cache and hard reload each affected page. In Chrome, press F12 to open the developer console, right-click on the browser's Reload button and select "Empty Cache & Hard Reload". In Firefox, open the developer toolbox, scroll down to advanced settings, then check the option to "Disable Cache (when toolbox is open)" and refresh the page. Similar settings for other browsers can be found on their respective help pages. It is important to clear *all* content via a "hard" refresh, since javascript files will often persist through lesser options.

Solution:
A forthcoming release will better address browser caching issues.

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	
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. `chunked` is used to indicate the search command supports Splnuk's "chunked" custom protocol, used by all of these stanzas `filename` Indicates the location of the Python .py filenames for these commands.
	dtimportphisheyeterms **(removed in 4.4.0)**	chunked, filename	
	dtimportphisheyeresults **(removed in 4.4.0)**	chunked, filename	
	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	

Conf File	Stanza Tag	Fields	Description
	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.
	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`.
	dtphisheyeterms-command **(removed in 4.4.0)**	syntax, shortdesc, usage	
	dtirisinvestigate-command	syntax, shortdesc, usage, comment1, example1, comment2, example2, related	

Conf File	Stanza Tag	Fields	Description
	dtirisdetectmonitors-command	syntax, shortdesc, usage, comment1, example1	
	dtsyncirisdetectwatchlist-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	
	dtdomainextract-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_include. 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.

Conf File	Stanza Tag	Fields	Description
	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	
	dt_monitoring_list	external_type, collection, fields_list	
	dt_tags_list	external_type, collection, fields_list	
	dt_phisheye_terms (**removed in 4.4.0**)	external_type, collection, fields_list	
	dt_phisheye_results (**removed in 4.4.0**)	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	Needed for macro dtdomainextract2
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.

Conf File	Stanza Tag	Fields	Description
		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.
		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

KV Store/ Collection Name	Fields
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_fooyn_timestamp, dt_looyn_timestamp, 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
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_phisheye_terms (**removed in 4.4.0**)	_key, term, discover_new_domains, dt_updated
dt_phisheye_results (**removed in 4.4.0**)	_key, dt_term, dt_alert_date, dt_domain, dt_riskScore, dt_createdDate, dt_ip_address_1, dt_ip_address_2, dt_ip_raw, dt_nameServer_1, dt_nameServer_2, dt_nameServer_raw, dt_registrarName, dt_registrantEmail, dt_monitor_flag, dt_imported
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

KV Store/ Collection Name	Fields
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.
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.

Macro Field Name	Default Value	Description
dtdomainextract2	rex field=url "(.*:\/\/)?(?P<temp_domain>[^:#\/?]+)" \ | 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")	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.
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. Splunk ES only.
dt_only_monitored_domains_in_notable_events	1 (enabled)	Enrichment alert setting for notable events. Splunk ES only.
dt_use_risk_threshold_in_notable_events	0 (false)	Enrichment alert setting for notable events. Splunk ES only.
dt_use_threatprofile_threshold_in_notable_events	0 (false)	Enrichment alert setting for notable events. Splunk ES only.
dt_ignore_phisheye_in_notable_events	0 (false)	Enrichment alert setting for notable events. Splunk ES only.
dt_ignore_iris_detect_in_notable_events	0 (false)	Enrichment alert setting for notable events. Splunk ES only.

Macro Field Name	Default Value	Description
dt_monitor_tags_in_notable_events	0 (false)	Enrichment alert setting for notable events. Splunk ES only.
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

Saved Search Name		Type	Description of the Saved Search	Required (Yes, No, Optional)	App Functionalities
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. You can 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
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

Saved Search Name		Type	Description of the Saved Search	Required (Yes, No, Optional)	App Functionalities
DomainTools - Import PhishEye Terms (**removed in 4.4.0)**		Reports	A search to import configured terms from PhishEye into `dt_phisheye_terms` collection. The frequency of the search can be configured in the app. Customers using PhishEye functionalities in the app must enable this saved search in Splunk. The UI will default to the Refresh Monitors frequency to "Never" by default. Changing the selection in UI will change the frequency in .conf, but will NOT enable the search. You'll still need to enable the search through reports. Default cron_schedule = 0 0 * * *	Optional (Required for PhishEye)	PhishEye
DomainTools - Import PhishEye Results (**removed in 4.4.0)**		Reports	A search to import newly discovered domains from PhishEye for terms enabled in the app. Customers using PhishEye functionalities in the app must enable this saved search in Splunk. Default cron_schedule = 0 */12 * * *	Optional (Required for PhishEye)	PhishEye
DomainTools - Expire Old PhishEye Data (**removed in 4.4.0)**		Reports	A search to remove PhishEye domains that were imported more than 14 days ago. Customers using PhishEye functionalities in the app must enable this saved search in Splunk. Default cron_schedule = 0 0 * * *	Optional (Required for PhishEye)	PhishEye

| 75

Saved Search Name		Type	Description of the Saved Search	Required (Yes, No, Optional)	App Functionalities
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

Saved Search Name		Type	Description of the Saved Search	Required (Yes, No, Optional)	App Functionaliti es
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
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

Saved Search Name		Type	Description of the Saved Search	Required (Yes, No, Optional)	App Functionalities
DomainTools - DomainTools Blocklisted Domains - Rule (**removed in 4.1.1**)		Alerts	A saved search to create events based on the criteria selected in DomainTools App → DT Settings → Configure Enrichment & Alerting. This functionality was removed in the 4.1.1 release. In 4.1.1, *DomainTools Domain Monitoring - Rule* must be enabled to support this use case, and will alert on Critical domains with a Proximity score of 100, given that • The Exceeds a Domain Risk Score threshold is checked, and • The Risk Score Threshold is set at 100 or below. 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.

Appendix B: Revision History

Release notes for prior 4.x versions of the DomainTools App for Splunk are maintained here for reference.

4.3.1 Release Notes

New

- Manage previously-ignored Iris Detect Monitor alerts within Splunk (API Functionality Required)
- Checks for invalid domains, skipping and logging them (if enabled) during enrichment

Changes and Fixes

- Fixes support for proxy usage broken in 4.3
- Fixes a parsing error on the DNSDB Flexible Search page when using regexes
- Fixes a display issue for the Risk Score panel on the Domain Profile page
- Updated DomainTools branding

Note: This version relies on HTML dashboards and un-restricting older jQuery libraries. An updated version to address these issues is forthcoming.

4.3 Release Notes

New

- Triage new domains matching Iris Detect Monitors within Splunk (API Functionality Required)
- Synchronize the Iris Detect Watch List with the Splunk Monitoring list to watch for new domain activity within your environment
- Investigate current and historical domain infrastructure with Passive DNS (pDNS) using Farsight's DNSDB Standard or Flexible search (API Key Required)

Changes and Fixes

- Removed Python 2 support due to updated dependent libraries
- Added a distributed search configuration to address occasional issues when updating in Splunk Cloud
- Slightly lowered the default risk score thresholds used in the *Enrichment Settings* page. This does *not* override any user-specified thresholds when doing an in-place upgrade
- Simplified the DT Settings Menu. Moved Monitoring-specific settings under a new *Monitoring* menu
- Replaced HTML dashboards with single page apps to maintain Splunk Cloud compatibility
- Updated to jQuery v3.6
- Minor fixes and UI polishing

4.2.1 Release Notes

Fix

- Adds a trigger stanza in app.conf to avoid unnecessary "restart required" messages

4.2 Release Notes

New

- Power an always-on SOC display with auto-refreshing *Threat Profile* and *Monitoring* dashboard panels.
- Simplify your triage process, investigating domains flagged in Enterprise Security *Incident Review* within the DomainTools app *Domain Profile* page.
- Improve app performance using a new regex-based *dtdomainextract2* macro.
- Expedite your workflow, adding domains to monitoring or allow-lists directly from DomainTools *Enrichment Explorer*.
- Natively enrich logs containing multivalue URLs (most commonly encountered with Proofpoint).

Changes and Fixes

- To improve performance, logging has been disabled by default. It can be re-enabled in the Diagnostic Panel
- Allows for "Informational"-level urgency tags when creating *Notable Events* in Enterprise Security
- Expanded configuration levels for allow-list actions
- *Active Domains* panel on the Threat Intelligence Dashboard has been replaced by *Risky Observed Domains*
- *Threat Portfolio* and *Domain Alerts Over Time* timelines show the number of events instead of domains. Click on the legend entry to show all matching events of a given type during the filtered time period
- Threat profile panels preserve the search time frame in the Splunk query for a more consistent experience
- Search *Enrichment Explorer* and *Domain Profile,* or add to the *Allowlist* or *Monitoring List* using escaped domains (e.g. example[.]com)
- Removed sparklines on dashboard panels
- Improved in-app documentation and user guide

4.1.3 Release Notes

Changes and Fixes

- Resolves Splunk Cloud compatibility issues related to installation on indexers during deployment

- Eliminates the need for localop installation workaround on Splunk Cloud
- Resolves an error when using the *Events Enriched* drill-down
- Resolves an error when trying to run a Queue Builder search with over ~500K events
- Eliminates the need for scpv2 workaround (see <u>upgrade notes</u>)

4.1.2 Release Notes

Changes and Fixes

- Resolves Splunk Cloud compatibility issues
- App defaults to Python 3 in 8.0; if customers are using 7.x, the default remains Python 2

4.1.1 Release Notes

New

- Ability to add proxy authentication via the App UI
- Workflow action to investigate IOC in DomainTools Iris platform
- Support for streaming command in Base Search definition
- A new field in the Enrichment Explorer - 'Observed in Logs' to convey if a domain was seen in your logs

Changes and Fixes

- Resolves inconsistencies with importing DomainTools IOCs via search hash
- Resolves inconsistencies with last enrichment time for investigated domains via Domain Profile
- Resolves inconsistencies with detecting certain tags from the Tag Monitoring list
- Resolves inconsistencies with Threat Portfolio drill-down from the dashboard
- Resolves inconsistencies and error handling with drill down elements in Monitoring and Threat Intelligence dashboards, in instances where there was no data
- Resolves inconsistencies with Risk Score presentation for scores of 100. Domains associated with Critical risk (a risk score of 100) will now consistently display "Proximity" as the risk profile. As such, the *DomainTools Blocklisted Domains - Rule* has been removed. This functionality will now be included as part of the *DomainTools Domain Monitoring - Rule*. When enabled, notable events will now be triggered for domains with a Proximity score of 100 when the Risk Score threshold is 100 or below
- Updated the cron schedule to run every 24 hours for cleaning up pivot information cache table
- Changed time picker options on the Log Source configuration page to 1, 5, and 10 min. The default is set to 10 mins
- Miscellaneous descriptive changes to better articulate functionalities throughout the app

4.1 Release Notes

Pre-requisites
- Access to Iris Enrich and Iris Investigate APIs are required.
- Access to PhishEye API is optional but recommended for full app functionality.
- Access to Account Information API, which is implicitly provisioned with your DomainTools api account.

New
- App Diagnostic Dashboard to provide visibility into audit activities of the app.
- API Usage Dashboard to provide visibility into query API consumption.
- A native Allowlisting ability to suppress monitoring of trusted domains.
- Introducing Investigation of Domain IOCs leveraging DomainTools Guided Pivot analytics.
- Ability to import IOCs from DomainTools using Iris export hash.
- Ability to discover connected domain IOCs for proactive monitoring.
- Richer domain context for notable events generated by DomainTools detection rules.
- Re-architected app with full support for recent Splunk SDK supporting Splunk 8.0 and Python 3. environments.
- Support for configuring proxies and custom SSL certs within the app UI.

Changes
- Redesigned ThreatIntel Dashboard with optimized searches.
- Redesigned Monitoring Dashboard for centralized monitoring.
- Redefined workflow to ingest PhishEye IOCs into Splunk.
- Redesigned Dashboard for ad hoc domain lookup.

Deprecated Functionalities *(From older versions)*
- Brand monitor functionality.
- Alexa 1M filtering.
- Support removed for DomainTools Classic APIs.