Doc Type

DomainTools App for Anomali

Version 1.0.6, 2024-04

DomainTools

Changelog

Version	Release Date	Summary
1.0.6	2024-03-18	- Updated pivot links with search directives - Added new Iris fields: server_type; website_title; ga4; gtm_codes; fb_codes; hotjar_codes; baidu_codes; yandex_codes; matomo_codes; statcounter_project_codes; statcounter_security_codes; issuer_common_name; common_name; not_after; not_before; alt_names - Added retry functionality to minimize the query rate limit error for “pivot all” action - Updated app metadata file and DomainTools logo - Improved error/exception handling; formatting issues; several bug fixes
1.0.4	2022-04-06	- Under-the-hood error handling fixes.
1.03	2021-08	- Under-the-hood upgrade of Python2 components to Python3.
1.02	2021-05	- Adds the ability to open a guided pivot directly on the DomainTools Iris platform. - Domain enrichment and pivoting will show results for the primary domain when a FQDN is presented. - Improved error handling when pivots return too many results to display. - Fixed support for additional entity types when pivoting on domains: name server, mail server, SSL certificate information, and registrant information.
1.01	2020-07	- Improved error handling when pivoting or enriching domains with empty create_date or risk_score values. - Improved error handling when pivoting or enriching domains with no results.

Contents

Introduction

The DomainTools Iris App for Anomali delivers a critical subset of DomainTools Iris data, including pivot enrichment, context enrichment for domains, and context enrichment for IPs, emails, and SSL certificates, directly inside the Anomali Threatstream platform to enable rapid in-context assessments of domain name observables and discovery of connected infrastructure.

Additional technical documentation on DomainTools products and features is available at www.domaintools.com/resources.

Getting Started

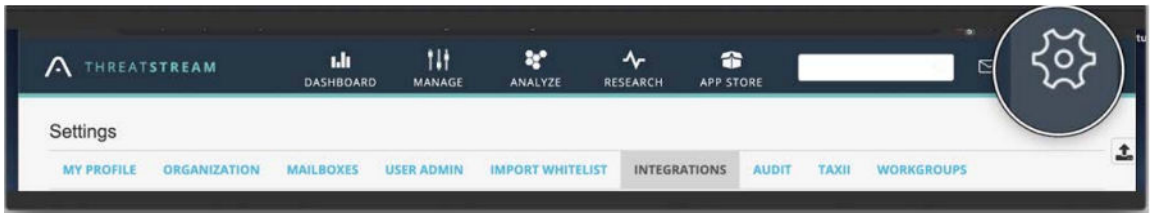
*Powered by the **DomainTools Iris Investigate API** - included with most enterprise subscriptions.*

To activate the enrichment, you will need a DomainTools API username and API key. Contact your DomainTools account manager if you need help obtaining access, or email enterprisesupport@domaintools.com.

NOTE: If you currently have API keys for the original DomainTools v1.0 Anomali integration, you may need to **obtain a new API key** or add more capabilities to your existing API key to use a newer version. Contact your DomainTools account manager for details on how to obtain access to the **Iris Investigate API**.

Once you have the API key, you need to activate the DomainTools Iris App inside Anomali. The steps are listed below:

1. Log in to your ThreatStream user interface.
2. In the top navigation bar, click the Settings icon and then Integrations.



3. Locate the box labeled **DomainTools Iris** and click Activate.
4. Enter your DomainTools API key and API username in the appropriate boxes, and click **Save**.

App Functionalities

Context-Based Enrichment

When enriching an Observable in Anomali Threatstream, the DomainTools App enriches the critical DomainTools dataset when the user opens up the Observable under Analyze - Observable tab.

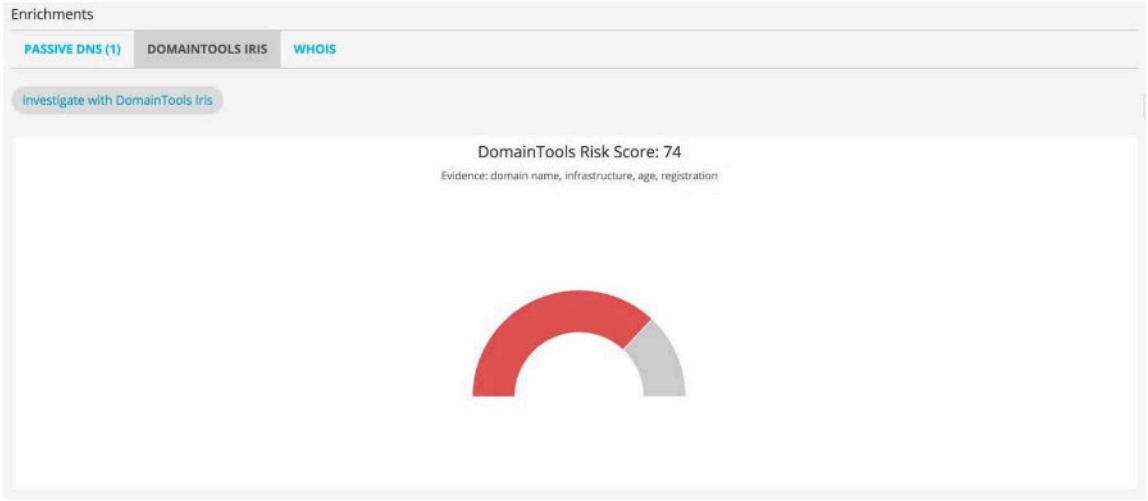
The App adds a **“DomainTools Iris” tab** to the set of context enrichment options for supported entity types. Some of the key intelligence is summarized below for your quick reference:

- Domain Risk Score with supporting evidence and component scores from machine learning classifiers & proximity-based risk algorithms.
- Domain profile attributes from the DomainTools Iris dataset, including identity, infrastructure, web crawl, and SSL details.
- Guided Pivot counts for each attribute to identity dedicated infrastructure, novel identities, and potential research pathways.
- An outbound link to the DomainTools Iris Investigation Platform to perform deeper analysis, with the domain name context preserved in the link to streamline the investigation process.

Enrichment for Domain Observables

For a Domain observable, the **DomainTools Iris** tab brings in the following context enrichment real-time:

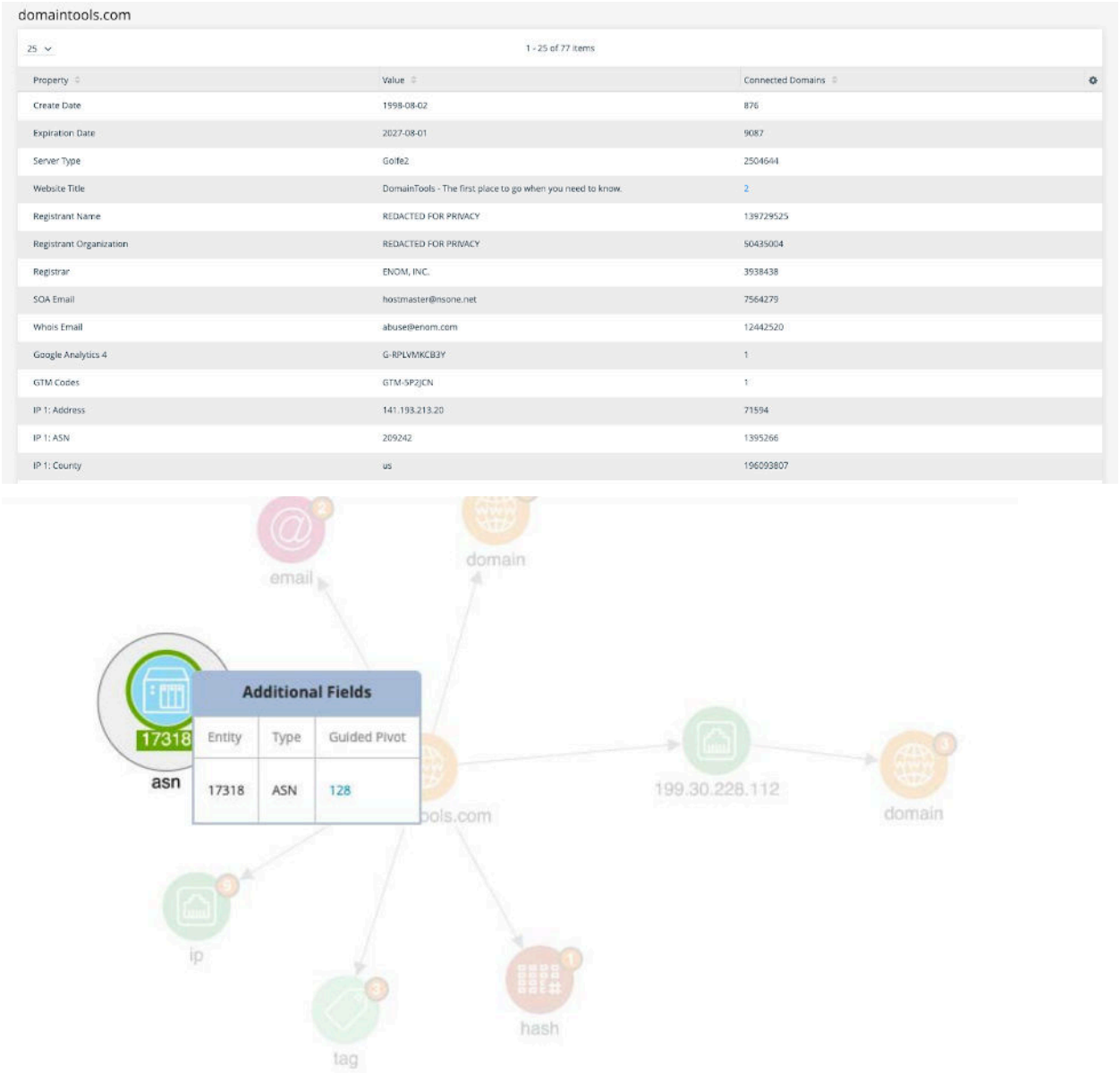
- *Domain Risk Score* with supporting evidence



- *Threat component scores* from DomainTools machine learning classifiers & proximity-based risk algorithms.

- *Domain attributes* from the DomainTools Iris dataset, including identity, infrastructure, web crawl, and SSL details

- *Guided Pivot counts* for each attribute to identity dedicated infrastructure, novel identities, and potential research pathways; pictured here in the **Enrichments** tab, and in an investigation:

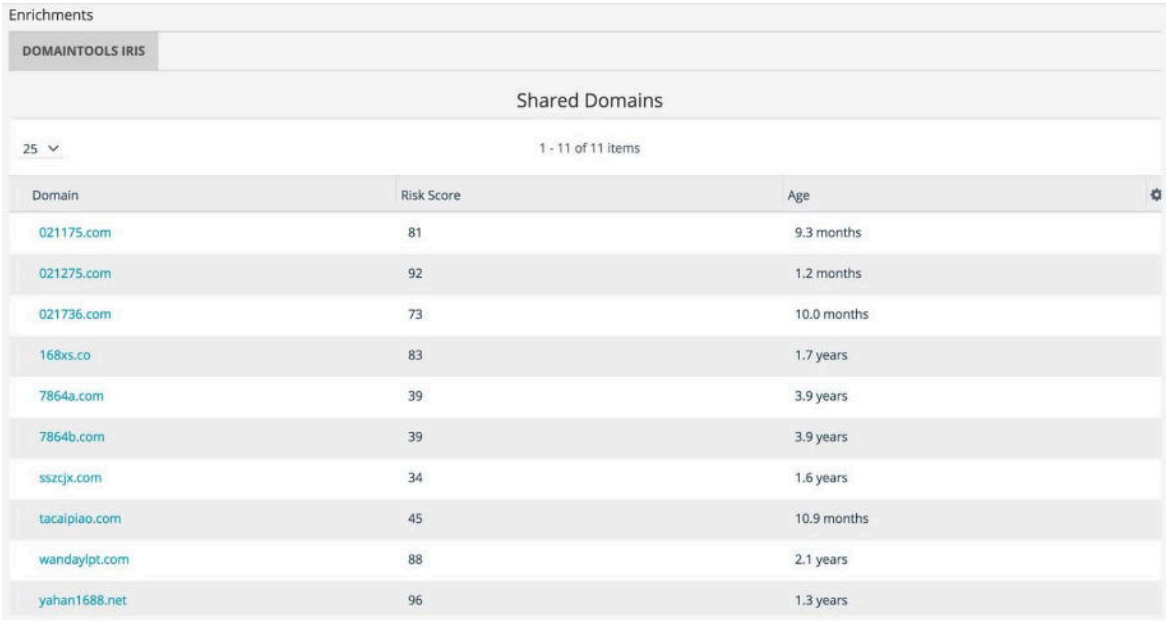


- Guided Pivots within the Enrichments tab
- Guided pivots within an investigation
- *An outbound link to DomainTools Iris Research Platform* enables deeper analysis, with context preserved in the link to streamline the investigation process

Enrichment for IPs, Emails, and SSL

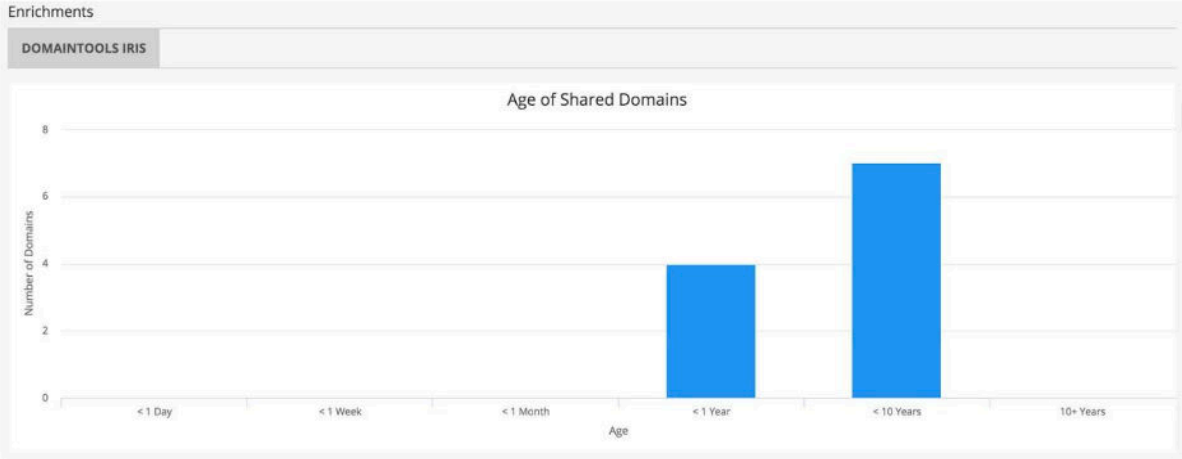
Sourced from the Iris Investigate API, a list of connected domains, the domain Risk Score, and the domain age distribution will be displayed for the same observable value.

- E.g., List of the domains associated with the observable, their Risk Scores, and domain ages:



- E.g., analytic showing the Risk Score Distribution across the set of domains associated with the observable:

- E.g., Analytic showing the Domain Age distribution across the set of domains associated with the observable



Pivot Enrichment

The DomainTools Iris App for Anomali leverages Anomali's built-in graph utility capability to assist in researching connected infrastructure associated with an Indicator.

To get started, add an entity of the supported type (see below) and right-click on the node. You will see a **DomainTools Iris** menu with options to pivot and obtain additional details or domains from the Iris Investigate API.

In the example below, an analyst is able to pivot on an IP associated with a known Observable to discover additional malicious domains within Anomali. The analyst can conveniently import the results of such investigations for sustaining monitoring.

Supported Attributes in Pivot Enrichment

Observable Attribute	**Pivot Types**	**Expected Results *(if available)***
Domain	Pivot Domain	• Web hosting ASN • Name server and Mail-server • IP addresses - Web host • Nameserver • Mail server hostnames (as a URL) • Registrant name (as a tag) • Registrar name (as a tag) • Email addresses • Whois, SOA, or SSL • SSL certificate hash (as a hash)
IP	Pivot NS IP Pivot MX IP Pivot DNS IP	Domain entities that share the IP address
Email	Pivot Email	Domain entities that share the email address
Hash	Pivot SSL Hash	Domain entities that share the SSL hash
URL	Pivot Name Server Host Pivot Mail Server Host	Domain entities that share the hostname