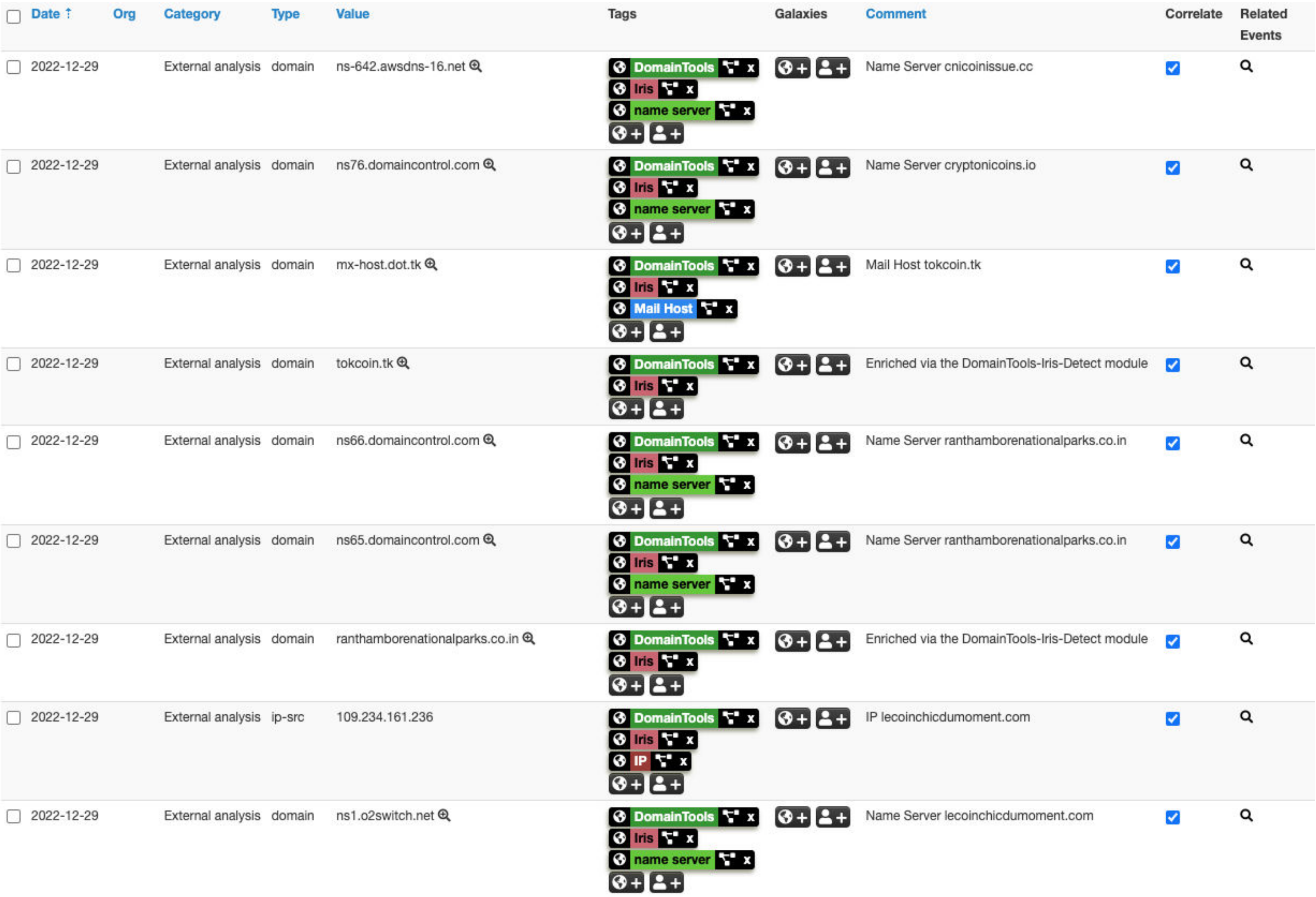
User Guide

DomainTools App for MISP

Version 2.0, April 2023

DomainTools



☐	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events
☐	2022-12-29		External analysis	domain	ns-642.awsdns-16.net	DomainTools Iris name server		Name Server cnicoinissue.cc	☑	🔍
☐	2022-12-29		External analysis	domain	ns76.domaincontrol.com	DomainTools Iris name server		Name Server cryptonicoins.io	☑	🔍
☐	2022-12-29		External analysis	domain	mx-host.dot.tk	DomainTools Iris Mail Host		Mail Host tokcoin.tk	☑	🔍
☐	2022-12-29		External analysis	domain	tokcoin.tk	DomainTools Iris		Enriched via the DomainTools-Iris-Detect module	☑	🔍
☐	2022-12-29		External analysis	domain	ns66.domaincontrol.com	DomainTools Iris name server		Name Server ranthamborenationalparks.co.in	☑	🔍
☐	2022-12-29		External analysis	domain	ns65.domaincontrol.com	DomainTools Iris name server		Name Server ranthamborenationalparks.co.in	☑	🔍
☐	2022-12-29		External analysis	domain	ranthamborenationalparks.co.in	DomainTools Iris		Enriched via the DomainTools-Iris-Detect module	☑	🔍
☐	2022-12-29		External analysis	ip-src	109.234.161.236	DomainTools Iris IP		IP lecoinchicdumoment.com	☑	🔍
☐	2022-12-29		External analysis	domain	ns1.o2switch.net	DomainTools Iris name server		Name Server lecoinchicdumoment.com	☑	🔍

Example showing data returned by the Iris Investigate and Iris Detect modules

Overview

The DomainTools MISP module 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 of MISP. It helps Threat Intelligence teams and Security Analysts uncover actor infrastructure and profile threats by leveraging DomainTools APIs. Analysts receive additional context on indicators by utilizing both the hover and expansion capabilities of MISP. This allows them to map connected infrastructure and surface historical domain information to better assess risk.

Customers who deploy the DomainTools MISP module benefit from:

- Greater context on domain names in MISP events with registration, infrastructure and SSL attributes.
- See essential domain attributes, including DomainTools Risk Score with component classifiers and potential pivots, directly in MISP popups on domain attributes.
- Pinpoint dedicated hosting, SSL certificate re-use, boutique hosting and shared identities with Guided Pivot counts in attribute comments.

- Quickly identify opportunities to map connected infrastructure with Guided Pivot tags in the MISP event attribute list
- Build a more complete view of the attacker's resources with Iris pivots on IP, nameserver, registrant email and more.
- Find correlated MISP events with shared attributes drawn from the extensive DomainTools Iris dataset
- Effortlessly import domains from the DomainTools Iris Investigate Platform into MISP for rapid sharing with teammates and industry peers
- *[**New in 2.0**]* Import newly discovered domains from Iris Detect to discover and monitor newly-created domains that imitate brands, company names, or an organization's supply chain. (Separate subscription required)
- *[**New in 2.0**]* Enrich up to 60 domains per minute using the Iris Enrich module to add DomainTools internet infrastructure intelligence to higher-volume sources. (Separate subscription required)

Features

DomainTools Iris Investigate (previously "DomainTools Iris")

- Designed for MISP tooltip or hover actions on domain names
- Provides risk scoring, domain age, hosting, Whois, MX and related infrastructure for a domain.
- Guided Pivot counts help investigators identify connected attributes to other domain infrastructure
- Requires Iris Investigate account provisioning

DomainTools Iris Enrich (new in 2.0)

- Optimized for high-volume domain enrichment, providing Risk scoring, Hosting, Whois, MX and related infrastructure information for a domain.
- Requires Iris Enrich account provisioning

DomainTools Iris Pivot

- Enriches domain attributes with nearly every available field from the Iris Investigate API.
- Includes complete Risk Score data, with component scores and evidence when available.
- Adds Guided Pivot counts to attribute comments.
- Tags attributes as potential Guided Pivots when connections are shared with fewer than 300 domains (this can be configured in the module attributes).
- Enables pivots on IPs, SSL hashes, nameserver hostnames, and registrant email addresses.
- Requires Iris Investigate account provisioning

DomainTools Iris Import

- Import domains from the Iris Investigate Pivot Engine directly to a MISP event
- Export an investigation from the Iris Investigate UI by copying the search hash (Menu -> Search -> Filters -> Export), importing a list of up to 5000 domains as indicators into MISP
- Requires Iris Investigate account provisioning

DomainTools Iris Detect (new in 2.0)

- Imports newly discovered and/or newly changed domains from DomainTools Iris Detect.
- Set up and manage monitored terms using the Iris Detect UI (https://iris.domaintools.com/detect/) then automatically import them into MISP using this module.
- Requires Iris Detect account provisioning

DomainTools Analyze

- This module is superseded by the Iris Investigate module but remains here for backward compatibility. Optimized for MISP hover actions, the Analyze capability provides Whois data, a Domain Risk Score and counts of connected domains to help give quick context on an indicator to inform an interesting pivot and map connected infrastructure.
- Leverages the following DomainTools endpoints: Parsed Whois, Domain Profile, Risk, Reverse IP, Reverse Whois

DomainTools Pivot

- This module is superseded by the Iris Pivot module, but remains here for backward compatibility. Optimized for enrichment actions, the Pivot capability provides additional context on indicators by automatically building out a list of connected infrastructure from the counts presented in the Analyze capability.
- The Pivot module will also expand email addresses to a list of other domains that share the same contact information, and expand IP addresses to the list of other domains pointed to the same IP.
- Leverages the following DomainTools endpoints: Parsed Whois, Domain Profile, Risk, Reverse IP, Reverse Whois

DomainTools Historic

- The Historic capability will act on Domains or URLs to find historical context by expanding domain names to lists of registrars, IPs and emails historically connected with that indicator
- Leverages the following DomainTools endpoints: Whois History, Hosting History, Domain Profile, Reverse IP, Reverse Whois, Parsed Whois, Whois

Quick Start Guide

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

Installation

MISP is an open source project maintained primarily by volunteers. It is not a product offered by a vendor, and the expectation is that people who install and operate it are comfortable working with the ambiguity and lack of support that comes with any open source project.

That same expectation applies to MISP modules - the customer or prospect must be comfortable following technical directions to get the modules installed and operational in their environment.

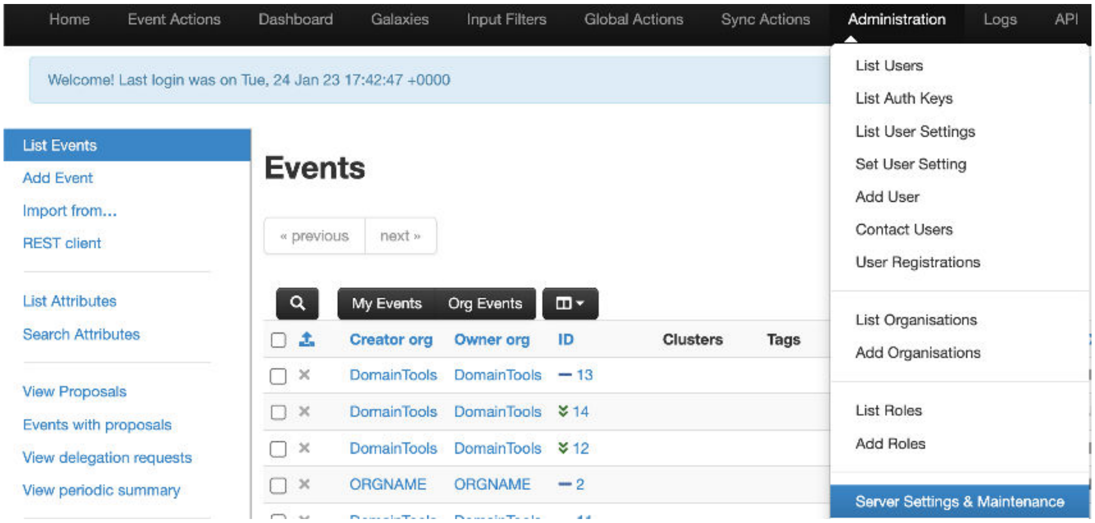
We provide instructions on how to install the modules on our GitHub page for the module code (scroll down for the contents of the README file). That is the best source of the instructions, because it will stay in sync with the code, and set the expectation of a technical user to get them installed and running properly.

Requirements

- MISP app
- Python 3.7 and up

Configuration

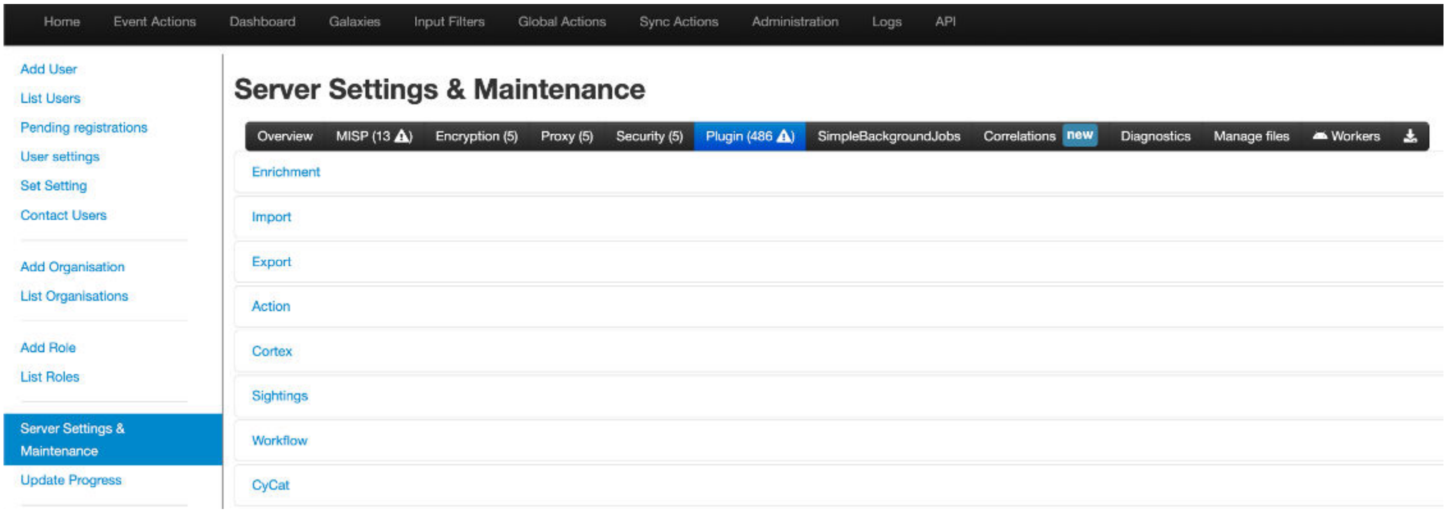
1. After the modules are installed and the module system in MISP is operational, log in as a MISP user with admin rights, point to the **Administration** menu, and select **Server Settings & Maintenance.**



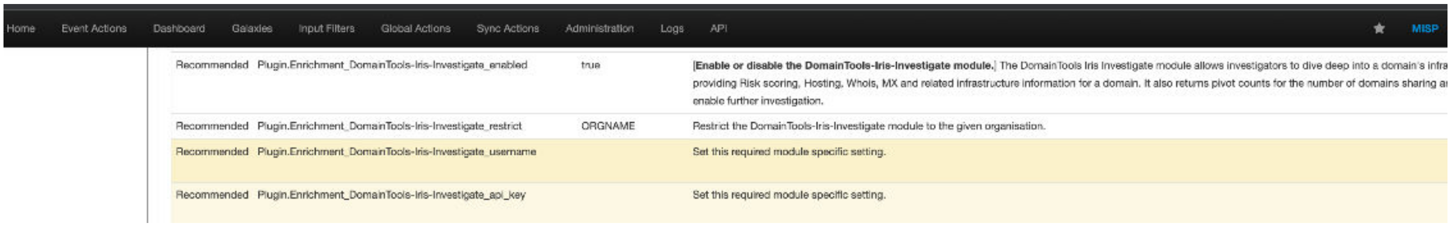
Welcome! Last login was on Tue, 24 Jan 23 17:42:47 +0000

		Creator org	Owner org	ID	Clusters	Tags
□	×	DomainTools	DomainTools	13		
□	×	DomainTools	DomainTools	14		
□	×	DomainTools	DomainTools	12		
□	×	ORGNAME	ORGNAME	2		

2. Click on the **Plugin** tab (modules are called "plugins" in some parts of MISP). Click to expand the **Enrichment** section for the Iris Investigate, Iris Enrich, Iris Pivot, Analyze, Pivot, and Historic DomainTools modules, or the **Import** section for the DomainTools Iris Import and DomainTools Iris Detect modules.



3. Scroll or search through the list of module settings to locate the DomainTools module you want to configure. You must double click a value in the table to begin editing it. At a minimum, each module must be enabled and have a **username** and **api_key** attribute populated. The **username** is the API username assigned to the customer's API account, and the **api_key** is the corresponding key for that API. Some modules have specific options that should work with default settings; their function is documented inline.



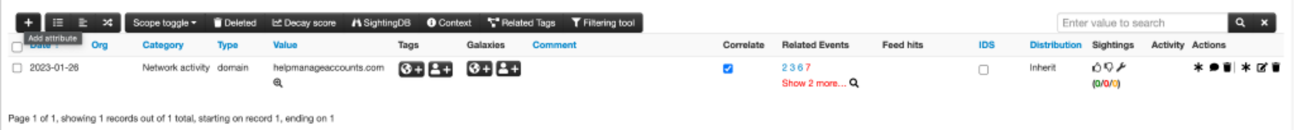
Recommended	Plugin.Enrichment_DomainTools-Iris-Investigate_enabled	true	**[Enable or disable the DomainTools-Iris-Investigate module.]** The DomainTools Iris Investigate module allows investigators to dive deep into a domain's infra providing Risk scoring, Hosting, Whois, MX and related infrastructure information for a domain. It also returns pivot counts for the number of domains sharing a enable further investigation.
Recommended	Plugin.Enrichment_DomainTools-Iris-Investigate_restrict	ORGNAME	Restrict the DomainTools-Iris-Investigate module to the given organisation.
Recommended	Plugin.Enrichment_DomainTools-Iris-Investigate_username		Set this required module specific setting.
Recommended	Plugin.Enrichment_DomainTools-Iris-Investigate_api_key		Set this required module specific setting.

Usage

MISP enrichment modules act on attributes of events - and those attributes must be of a specific type for the system to offer them for enrichment. These usage instructions focus on the Iris modules. The concepts are similar to the Enterprise modules.

- **Adding a domain attribute to MISP**

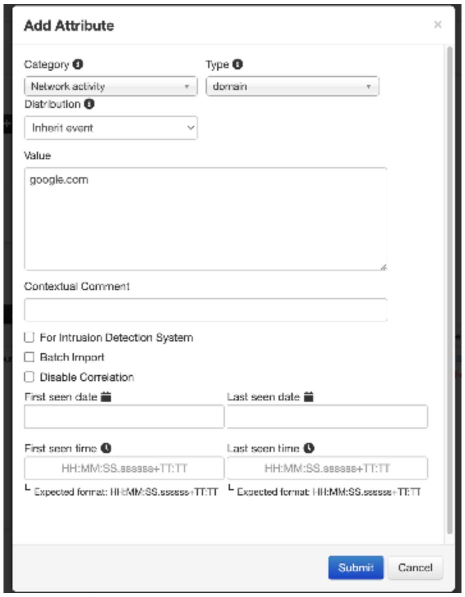
    1. Create an event in MISP with any default values.
    2. Scroll down to the attributes table and click the +.



Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2023-01-26		Network activity	domain	helpmanageaccounts.com				☑	2 3 6 7 Show 2 more...		□	Inherit	(0/0/0)		

Page 1 of 1, showing 1 records out of 1 total, starting on record 1, ending on 1

3. Specify the attribute type: under **Category** choose **Network activity**, then under **Type** choose **domain**.
4. Under **Value** enter an active domain name and click **Submit**.



Add Attribute

Category: Network activity

Type: domain

Distribution: Inherit event

Value: google.com

Contextual Comment

□ For Intrusion Detection System

□ Batch Import

□ Disable Correlation

First seen date

Last seen date

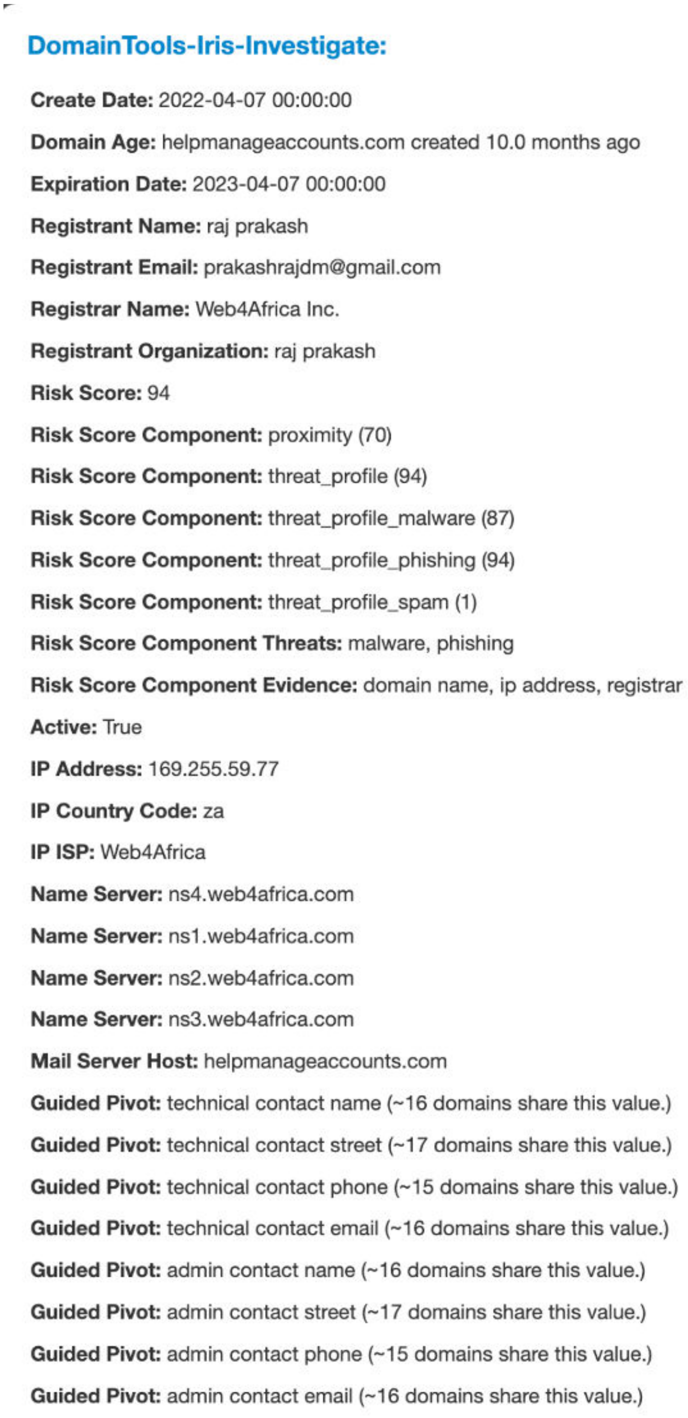
First seen time: HH:MM:SS.ssssss+TT:TT

Last seen time: HH:MM:SS.ssssss+TT:TT

Expected format: HH:MM:SS.ssssss+TT:TT

Expected format: HH:MM:SS.ssssss+TT:TT

- **Using the DomainTools-Iris-Investigate and DomainTools-Iris-Enrich modules**
    1. In the event detail page, locate a domain name in the list of attributes (the module only works on domain names).
    2. Find the magnifying glass icon next to the domain name and click it, or hover over the domain. The appearance will differ slightly but the content is the same.



DomainTools-Iris-Investigate:

Create Date: 2022-04-07 00:00:00

Domain Age: helpmanageaccounts.com created 10.0 months ago

Expiration Date: 2023-04-07 00:00:00

Registrant Name: raj prakash

Registrant Email: prakashrajdm@gmail.com

Registrar Name: Web4Africa Inc.

Registrant Organization: raj prakash

Risk Score: 94

Risk Score Component: proximity (70)

Risk Score Component: threat_profile (94)

Risk Score Component: threat_profile_malware (87)

Risk Score Component: threat_profile_phishing (94)

Risk Score Component: threat_profile_spam (1)

Risk Score Component Threats: malware, phishing

Risk Score Component Evidence: domain name, ip address, registrar

Active: True

IP Address: 169.255.59.77

IP Country Code: za

IP ISP: Web4Africa

Name Server: ns4.web4africa.com

Name Server: ns1.web4africa.com

Name Server: ns2.web4africa.com

Name Server: ns3.web4africa.com

Mail Server Host: helpmanageaccounts.com

Guided Pivot: technical contact name (~16 domains share this value.)

Guided Pivot: technical contact street (~17 domains share this value.)

Guided Pivot: technical contact phone (~15 domains share this value.)

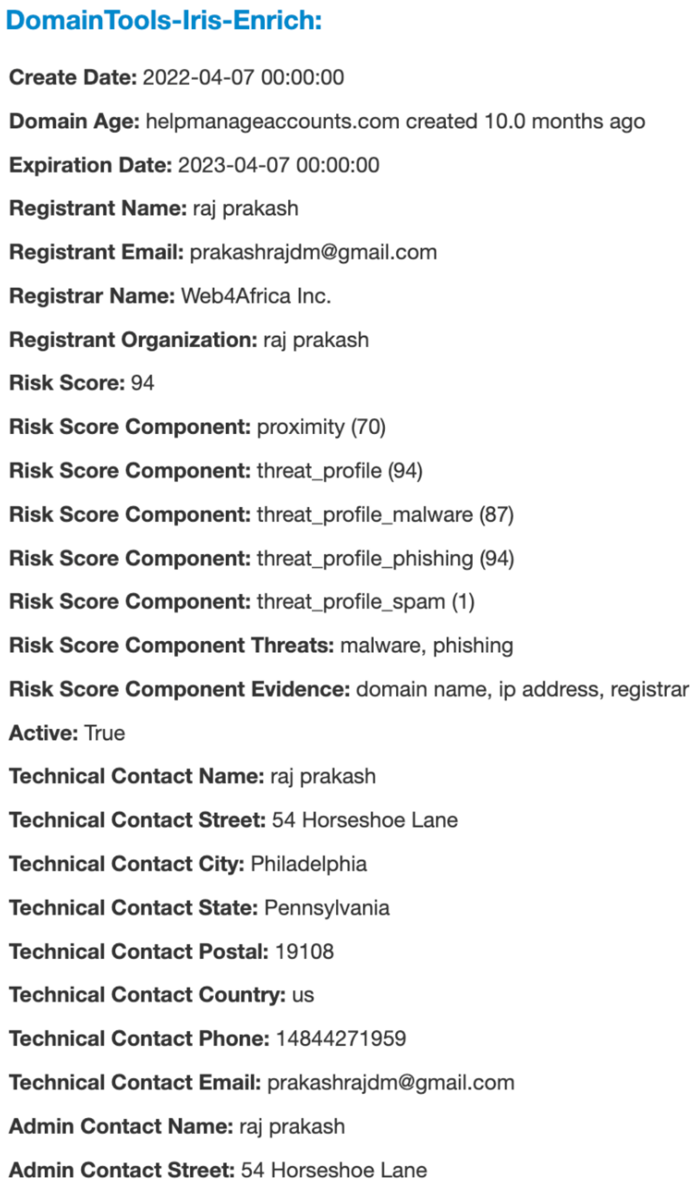
Guided Pivot: technical contact email (~16 domains share this value.)

Guided Pivot: admin contact name (~16 domains share this value.)

Guided Pivot: admin contact street (~17 domains share this value.)

Guided Pivot: admin contact phone (~15 domains share this value.)

Guided Pivot: admin contact email (~16 domains share this value.)



DomainTools-Iris-Enrich:

Create Date: 2022-04-07 00:00:00

Domain Age: helpmanageaccounts.com created 10.0 months ago

Expiration Date: 2023-04-07 00:00:00

Registrant Name: raj prakash

Registrant Email: prakashrajdm@gmail.com

Registrar Name: Web4Africa Inc.

Registrant Organization: raj prakash

Risk Score: 94

Risk Score Component: proximity (70)

Risk Score Component: threat_profile (94)

Risk Score Component: threat_profile_malware (87)

Risk Score Component: threat_profile_phishing (94)

Risk Score Component: threat_profile_spam (1)

Risk Score Component Threats: malware, phishing

Risk Score Component Evidence: domain name, ip address, registrar

Active: True

Technical Contact Name: raj prakash

Technical Contact Street: 54 Horseshoe Lane

Technical Contact City: Philadelphia

Technical Contact State: Pennsylvania

Technical Contact Postal: 19108

Technical Contact Country: us

Technical Contact Phone: 14844271959

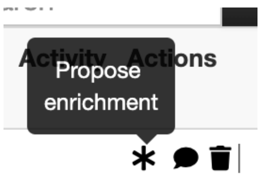
Technical Contact Email: prakashrajdm@gmail.com

Admin Contact Name: raj prakash

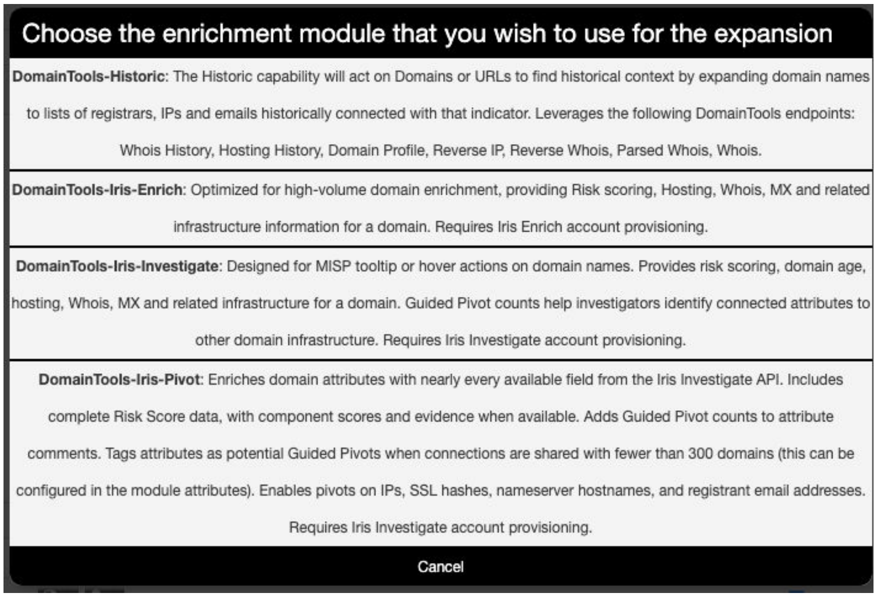
Admin Contact Street: 54 Horseshoe Lane

3. Attributes will appear from all configured enrichment modules that are enabled in MISP.
4. When available, the DomainTools-Iris-Investigate and DomainTools-Iris-Enrich tooltip will show the most important data on the domain name, including age, identity, IP country, risk score components, and any attributes with Guided Pivot counts (for Investigate) and value (for Enrich).

- **Using the DomainTools-Iris-Pivot module**
    1. Locate an attribute of a supported type in the list of event attributes.
        a. Domain names are the easiest starting point and are recommended for testing.
        b. IP addresses, hostnames (assumed to be name servers), email addresses, and SSL hashes also work, but they must be of specific types.
    2. Find the last asterisks or star at the far right of the row for that attribute and click it.



3. A list of available enrichment modules appears, including the Iris-Pivot and DomainTools-Iris-Analyze modules. Select the DomainTools-Iris-Pivot module.



Choose the enrichment module that you wish to use for the expansion

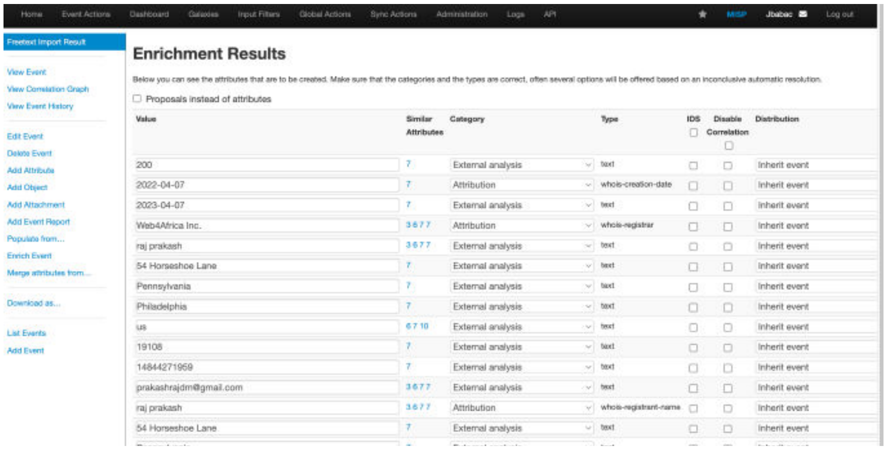
DomainTools-Historic: The Historic capability will act on Domains or URLs to find historical context by expanding domain names to lists of registrars, IPs and emails historically connected with that indicator. Leverages the following DomainTools endpoints: Whois History, Hosting History, Domain Profile, Reverse IP, Reverse Whois, Parsed Whois, Whois.

DomainTools-Iris-Enrich: Optimized for high-volume domain enrichment, providing Risk scoring, Hosting, Whois, MX and related infrastructure information for a domain. Requires Iris Enrich account provisioning.

DomainTools-Iris-Investigate: Designed for MISP tooltip or hover actions on domain names. Provides risk scoring, domain age, hosting, Whois, MX and related infrastructure for a domain. Guided Pivot counts help investigators identify connected attributes to other domain infrastructure. Requires Iris Investigate account provisioning.

DomainTools-Iris-Pivot: Enriches domain attributes with nearly every available field from the Iris Investigate API. Includes complete Risk Score data, with component scores and evidence when available. Adds Guided Pivot counts to attribute comments. Tags attributes as potential Guided Pivots when connections are shared with fewer than 300 domains (this can be configured in the module attributes). Enables pivots on IPs, SSL hashes, nameserver hostnames, and registrant email addresses. Requires Iris Investigate account provisioning.

4. For domain attributes, the DomainTools-Iris-Pivot enrich module queries the Iris Investigate API endpoint and populates a table of attributes with data returned from Iris.
    a. The simplest path is to click the **Submit Attributes** button at the bottom left corner of the page to add all the attributes to the event.
    b. Experienced users may want to clean extra attributes out of the list that they might not need - click the X at the far right of the page to remove an attribute before it is added to the event.
    c. Some attributes, like risk score, depend on the comment field to provide context
    d. Other attributes, like IP addresses, use the comment field to show the Guided Pivot count ("GP: 10,383") for that attribute
    e. The **similar attributes** column is part of a powerful MISP capability that correlates events together. It shows other events that share the same attribute, which for risk numbers is mostly meaningless, but can be highly relevant for IP addresses or other more unique identifiers.



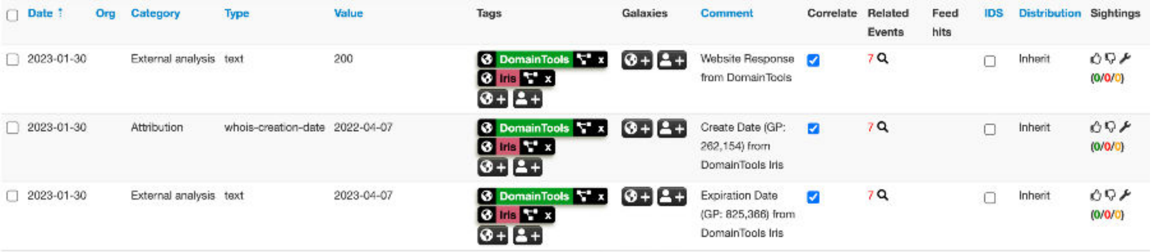
Enrichment Results

Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered based on an inconclusive automatic resolution.

□ Proposals instead of attributes

Value	Similar Attributes	Category	Type	IDS □	Disable Correlation □	Distribution
200	7	External analysis	text	□	□	Inherit event
2022-04-07	7	Attribution	whois-creation-date	□	□	Inherit event
2023-04-07	7	External analysis	text	□	□	Inherit event
Web4Africa Inc.	3 6 7 7	Attribution	whois-registrar	□	□	Inherit event
raj prakash	3 6 7 7	External analysis	text	□	□	Inherit event
54 Horseshoe Lane	7	External analysis	text	□	□	Inherit event
Pennsylvania	7	External analysis	text	□	□	Inherit event
Philadelphia	7	External analysis	text	□	□	Inherit event
us	6 7 10	External analysis	text	□	□	Inherit event
19108	7	External analysis	text	□	□	Inherit event
14844271959	7	External analysis	text	□	□	Inherit event
prakashrajdm@gmail.com	3 6 7 7	External analysis	text	□	□	Inherit event
raj prakash	3 6 7 7	Attribution	whois-registrant-name	□	□	Inherit event
54 Horseshoe Lane	7	External analysis	text	□	□	Inherit event

5. After the attributes are added to the event, they appear in the attribute table with similar columns as the module results.
    a. The comments are still visible, offering access to the Guided Pivot counts after the **GP:** prefix.
    b. GP: counts in comments can be useful to distinguish between shared and dedicated hosting IPs.
    c. Tags are added automatically to attributes returned by the DomainTools modules.
    d. Attributes that would make good pivots are also labeled with the **Guided Pivot** tag. This is added to any attribute returned by a domain pivot that has less than 300 domains shared by it. The threshold is configurable in the plugin settings.
    e. The latest version of MISP adds the ability to filter the event attribute list - this can be used to quickly find Guided Pivot attributes in a large table.



□	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings
□	2023-01-30		External analysis	text	200	DomainTools Iris		Website Response from DomainTools	☑	7		□	Inherit	(0/0/0)
□	2023-01-30		Attribution	whois-creation-date	2022-04-07	DomainTools Iris		Create Date (GP: 262,154) from DomainTools Iris	☑	7		□	Inherit	(0/0/0)
□	2023-01-30		External analysis	text	2023-04-07	DomainTools Iris		Expiration Date (GP: 825,366) from DomainTools Iris	☑	7		□	Inherit	(0/0/0)

6. The DomainTools-Iris-Pivot module can also find related domains that share the same attribute by pivoting on a few supported Iris fields.
    a. Only a subset of Iris pivots are available, primarily because MISP does not have enough distinct types to represent all the types of data we return from Iris, and it does not provide any other way to select which type of a pivot you want to perform.

```
MISP Type                Iris Pivot
==========================================
ip-src, ip-dest          ip
whois-registrant-email   email
email-dst, email-src     email
hostname                 nameserver_host
whois-registrar          registrar
whois-registrant-name    registrant
x509-fingerprint-sha1    ssl_hash
```

b. To perform a pivot on one of these types of attributes, find it in the list of event attributes, and click the same far-right asterisk as in step 2 above.

c. Choose the DomainTools-Iris-Pivot module.

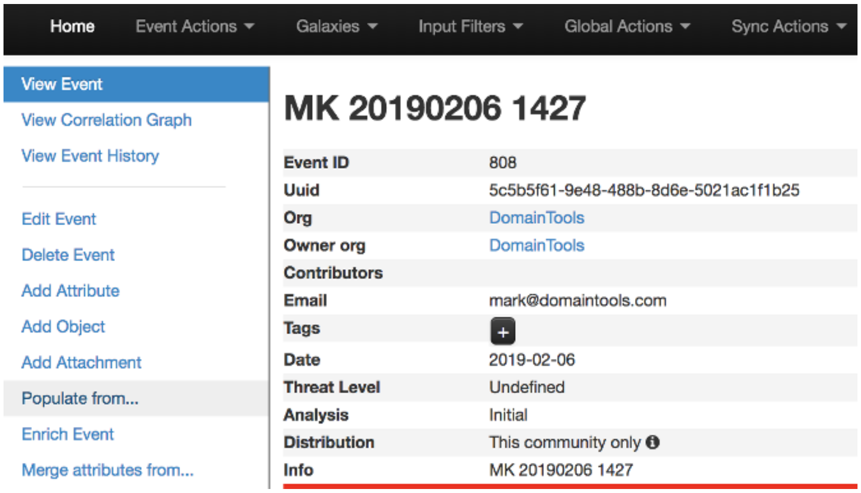
d. MISP will query the Iris Investigate API and return a list of domain names.

e. Click the **Submit Attributes** button at the bottom right corner to the page to add the attributes to the event.

- **Using the DomainTools-Iris-Import module**

  The DomainTools Iris Import module helps tell an integrated story with the Iris Investigate UI and the MISP project, and it supports the MISP mission of sharing indicators with peers. The module leverages the Iris search hash and the Iris Investigate API to bring in all the domain names found by a given Iris Investigate search. This makes it possible to import any list of Iris domains that the Iris Pivot Engine can find, including historical matches and other criteria not yet supported by the standard Iris Investigate API.

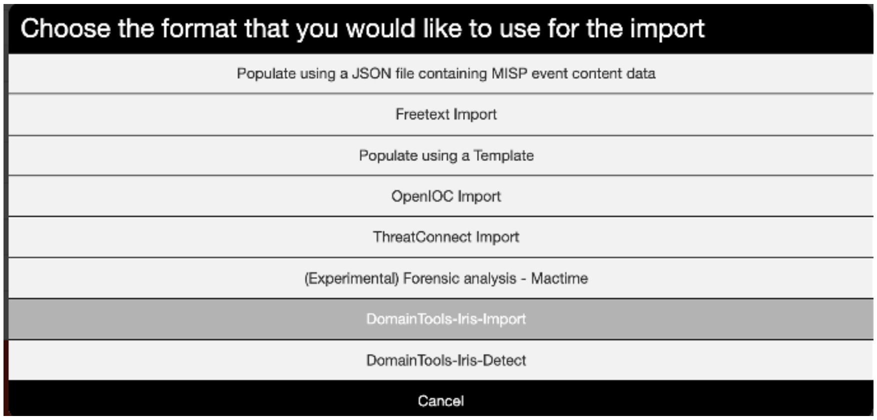
  1. Create an event in MISP, or open an existing event.
  2. Locate the "Populate From..." option on the left sidebar of the event.



MK 20190206 1427

Event ID	808
Uuid	5c5b5f61-9e48-488b-8d6e-5021ac1f1b25
Org	DomainTools
Owner org	DomainTools
Contributors	
Email	mark@domaintools.com
Tags	+
Date	2019-02-06
Threat Level	Undefined
Analysis	Initial
Distribution	This community only
Info	MK 20190206 1427

  3. Choose the "DomainTools-Iris-Import" module from the list of available import modules.



Choose the format that you would like to use for the import

Populate using a JSON file containing MISP event content data

Freetext Import

Populate using a Template

OpenIOC Import

ThreatConnect Import

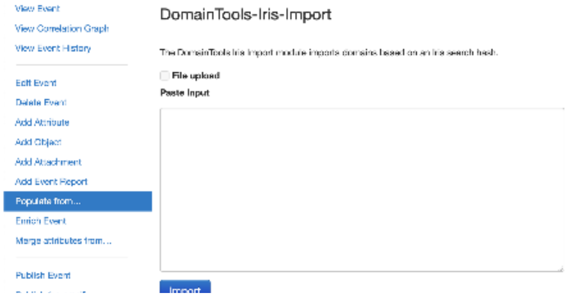
(Experimental) Forensic analysis - Mactime

DomainTools-Iris-Import

DomainTools-Iris-Detect

Cancel

4. The MISP import window will appear with a large empty text area.



DomainTools-Iris-Import

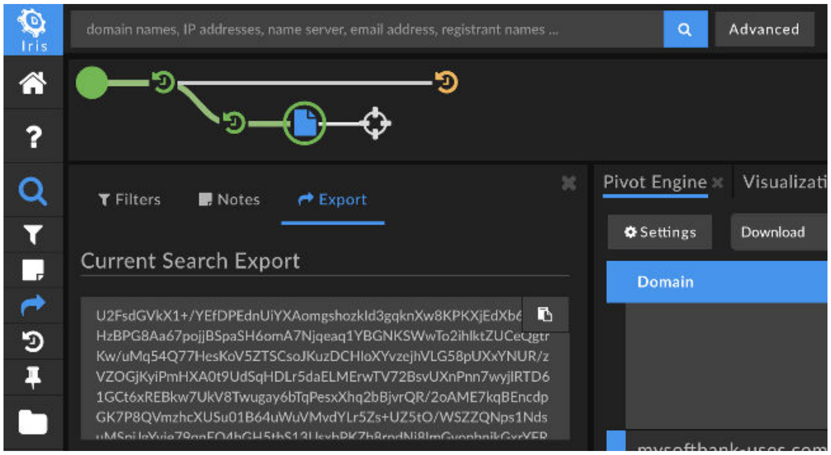
The DomainTools Iris Import module imports domains based on an Iris search hash.

□ File upload

Paste Input

Import

5. In the Iris Investigate Platform, click the **Advanced** button next to the search, then click **Export**, and copy the "Current Search Export" to your clipboard.

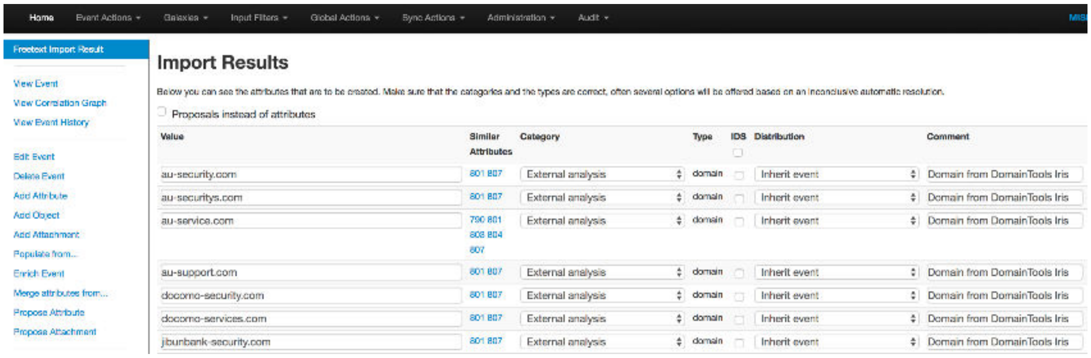


Iris
domain names, IP addresses, name server, email address, registrant names ...
Advanced
Filters
Notes
Export
Pivot Engine
Visualizati
Settings
Download
Domain

Current Search Export

U2FsdGVkX1+/YEfDPEdnUiYXAomgshozkld3gqknXw8KPKXjEdXb6
HzBPG8Aa67pojjBSpaSH6omA7Njqeaq1YBGNKSWwTo2ihlktZUCeQgtr
Kw/uMq54Q77HesKoV5ZTSCsoJKuzDCHloXYvzejhVLG58pUXxYNUR/z
VZOGjKyiPmHXA0t9UdSqHDLr5daELMErwTV72BsvUXnPnn7wyjlRTD6
1GCt6xREBkw7UkV8Twugay6bTqPesxXhq2bBjvrQR/2oAME7kqBEncdp
GK7P8QVmzhcXUSu01B64uWuVMvdYLr5Zs+UZ5tO/WSZZQNps1Nds

6. Paste the search export into the MISP Import and click **Import**. Domain names that match the exported Iris search will appear in MISP as attributes for review, just like a pivot search result on a non-domain attribute.



Import Results

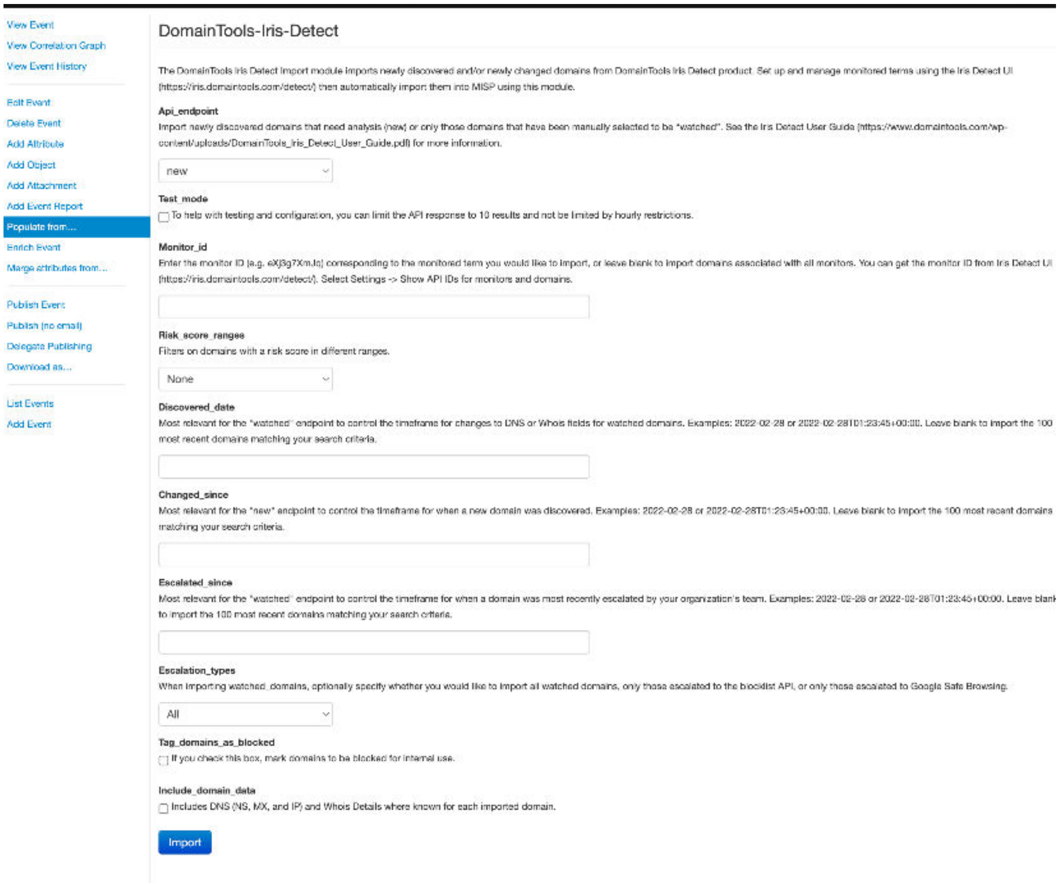
Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered based on an inconclusive automatic resolution.

□ Proposals instead of attributes

Value	Similar Attributes	Category	Type	IDS □	Distribution	Comment
au-security.com	801 807	External analysis	domain	□	Inherit event	Domain from DomainTools Iris
au-securitys.com	801 807	External analysis	domain	□	Inherit event	Domain from DomainTools Iris
au-service.com	790 801 808 804 807	External analysis	domain	□	Inherit event	Domain from DomainTools Iris
au-support.com	801 807	External analysis	domain	□	Inherit event	Domain from DomainTools Iris
docomo-security.com	801 807	External analysis	domain	□	Inherit event	Domain from DomainTools Iris
docomo-services.com	801 807	External analysis	domain	□	Inherit event	Domain from DomainTools Iris
jibunbank-security.com	801 807	External analysis	domain	□	Inherit event	Domain from DomainTools Iris

7. Scroll to the bottom and click **Submit Attributes** to add the domains to the MISP event.

- **Using the DomainTools-Iris-Detect module**
  The DomainTools Iris Detect Import module imports newly discovered and/or newly changed domains from the DomainTools Iris Detect product. Set up and manage monitored terms using the [Iris Detect UI](https://iris.domaintools.com/detect/) then automatically import them into MISP using this module.
  1. Follow the Steps 1-3 of the DomainTools-Iris-Import usage but choose DomainTools-Iris-Detect in step 3.
  2. Fill-in the data and click **Import**. Follow carefully the instructions per input field.



DomainTools-Iris-Detect

The DomainTools Iris Detect Import module imports newly discovered and/or newly changed domains from DomainTools Iris Detect product. Set up and manage monitored terms using the Iris Detect UI (https://iris.domaintools.com/detect/) then automatically import them into MISP using this module.

Api_endpoint
Import newly discovered domains that need analysis (new) or only those domains that have been manually selected to be "watched". See the Iris Detect User Guide (https://www.domaintools.com/wp-content/uploads/DomainTools_Iris_Detect_User_Guide.pdf) for more information.

new

Test_mode
□ To help with testing and configuration, you can limit the API response to 10 results and not be limited by hourly restrictions.

Monitor_id
Enter the monitor ID (e.g. eXj3g7Xm.Iq) corresponding to the monitored term you would like to import, or leave blank to import domains associated with all monitors. You can get the monitor ID from Iris Detect UI (https://iris.domaintools.com/detect/). Select Settings -> Show API IDs for monitors and domains.

Risk_score_ranges
Filters on domains with a risk score in different ranges.

None

Discovered_date
Most relevant for the "watched" endpoint to control the timeframe for changes to DNS or Whois fields for watched domains. Examples: 2022-02-28 or 2022-02-28T01:23:45+00:00. Leave blank to import the 100 most recent domains matching your search criteria.

Changed_since
Most relevant for the "new" endpoint to control the timeframe for when a new domain was discovered. Examples: 2022-02-28 or 2022-02-28T01:23:45+00:00. Leave blank to import the 100 most recent domains matching your search criteria.

Escalated_since
Most relevant for the "watched" endpoint to control the timeframe for when a domain was most recently escalated by your organization's team. Examples: 2022-02-28 or 2022-02-28T01:23:45+00:00. Leave blank to import the 100 most recent domains matching your search criteria.

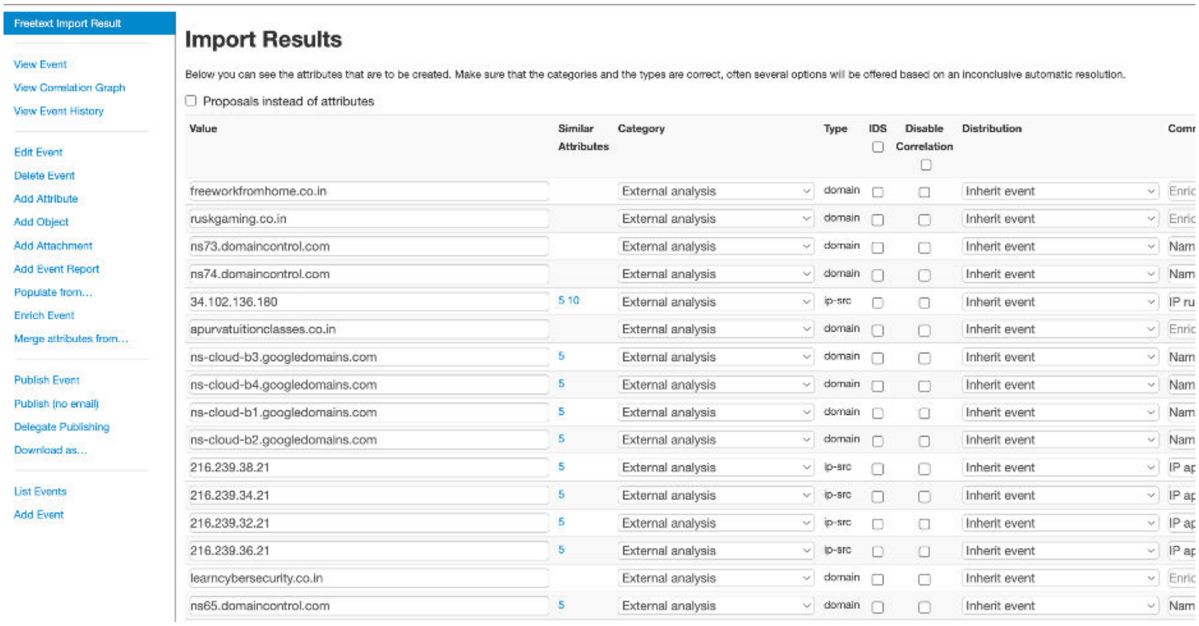
Escalation_types
When importing watched_domains, optionally specify whether you would like to import all watched domains, only those escalated to the blocklist API, or only those escalated to Google Safe Browsing.

All

Tag_domains_as_blocked
□ If you check this box, mark domains to be blocked for internal use.

Include_domain_data
□ Includes DNS (NS, MX, and IP) and Whois Details where known for each imported domain.

  3. Scroll to the bottom and click "Submit Attributes" to add the domains to the MISP event.



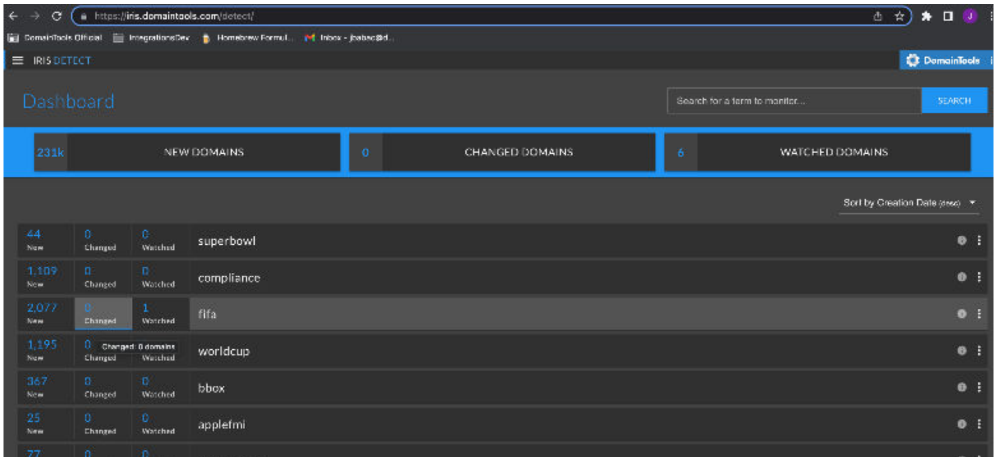
Import Results

Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered based on an inconclusive automatic resolution.

☐ Proposals instead of attributes

Value	Similar Attributes	Category	Type	IDS ☐	Disable Correlation ☐	Distribution	Comr
freeworkfromhome.co.in		External analysis	domain	☐	☐	Inherit event	Enric
ruskgaming.co.in		External analysis	domain	☐	☐	Inherit event	Enric
ns73.domaincontrol.com		External analysis	domain	☐	☐	Inherit event	Nam
ns74.domaincontrol.com		External analysis	domain	☐	☐	Inherit event	Nam
34.102.136.180	5 10	External analysis	ip-src	☐	☐	Inherit event	IP ru
apurvatuitionclasses.co.in		External analysis	domain	☐	☐	Inherit event	Enric
ns-cloud-b3.googledomains.com	5	External analysis	domain	☐	☐	Inherit event	Nam
ns-cloud-b4.googledomains.com	5	External analysis	domain	☐	☐	Inherit event	Nam
ns-cloud-b1.googledomains.com	5	External analysis	domain	☐	☐	Inherit event	Nam
ns-cloud-b2.googledomains.com	5	External analysis	domain	☐	☐	Inherit event	Nam
216.239.38.21	5	External analysis	ip-src	☐	☐	Inherit event	IP ap
216.239.34.21	5	External analysis	ip-src	☐	☐	Inherit event	IP ap
216.239.32.21	5	External analysis	ip-src	☐	☐	Inherit event	IP ap
216.239.36.21	5	External analysis	ip-src	☐	☐	Inherit event	IP ap
learncybersecurity.co.in		External analysis	domain	☐	☐	Inherit event	Enric
ns65.domaincontrol.com	5	External analysis	domain	☐	☐	Inherit event	Nam

- **Getting monitor IDs via API response or the Iris Detect UI**
    1. View Iris Detect's dashboard via https://iris.domaintools.com/detect/. It shows monitors already set up for your organization and lets you create new ones. Remember that monitors are shared by all Detect users in your organization.

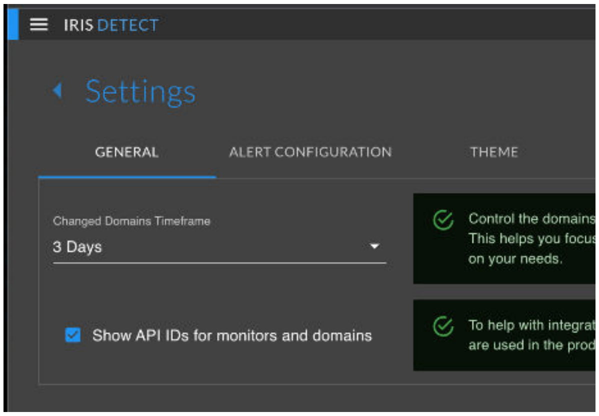


Dashboard

231k	NEW DOMAINS	
0	CHANGED DOMAINS	
6	WATCHED DOMAINS	

New	Changed	Watched	
44	0	0	superbowl
1,109	0	0	compliance
2,077	0	1	fifa
1,195	0		worldcup
367	0	0	bbox
25	0	0	applefmi
77	0	0	

    2. Select **Settings** and tick **Show API IDs for monitors and domains.**



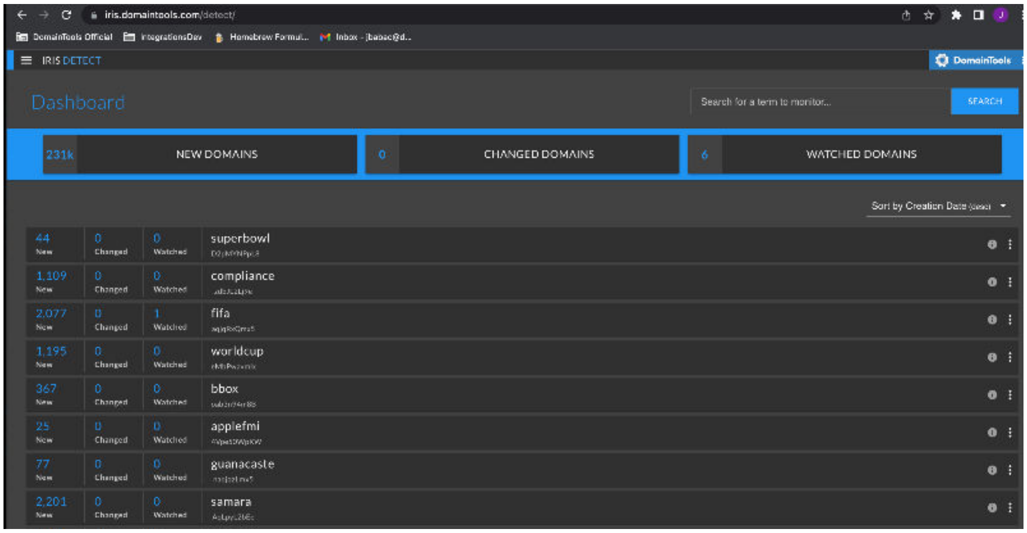
Changed Domains Timeframe: 3 Days

☑ Show API IDs for monitors and domains

Control the domains
This helps you focus
on your needs.

To help with integrat
are used in the prod

3. Go back to **Dashboard** and you can see the monitor ID below the monitor name.



44 New	0 Changed	0 Watched	superbowl [illegible]
1,109 New	0 Changed	0 Watched	compliance [illegible]
2,077 New	0 Changed	1 Watched	fifa [illegible]
1,195 New	0 Changed	0 Watched	worldcup [illegible]
367 New	0 Changed	0 Watched	bbox [illegible]
25 New	0 Changed	0 Watched	applefmi [illegible]
77 New	0 Changed	0 Watched	guanacaste [illegible]
2,201 New	0 Changed	0 Watched	samara [illegible]

Changelog

2.0 Release Notes

New

- Added DomainTools-Iris-Detect module. Populate lookalike domains from the Iris Detect product into a MISP event for investigation and triaging (separate provisioning required).
- Added DomainTools-Iris-Enrich module. Enrich up to 60 domains per minute via the Iris Enrich endpoint (separate provisioning required).

Changes and Fixes

- Renamed DomainTools-Iris-Analyze to DomainTools-Iris-Investigate for disambiguation
- Removed the deprecated "reputation" endpoint in legacy modules DomainTools-Analyze and DomainTools-Pivot. Use the Risk, Enrich or Investigate endpoints instead.
- Improved risk score presentation.

- Improved Guided Pivot details in DomainTools-Iris-Investigate
- Fixed handling of empty results.
- Replaced Alexa with DomainTools Rank (popularity_rank).
- Added additional fields in DomainTools-Iris-Investigate
- Fixed invalid search_hash issue for Iris-Import .

Troubleshooting & Known Issues

No known issues as of March 2023. Please reach out to enterprisesupport@domaintools.com with any questions or feedback.