User Guide

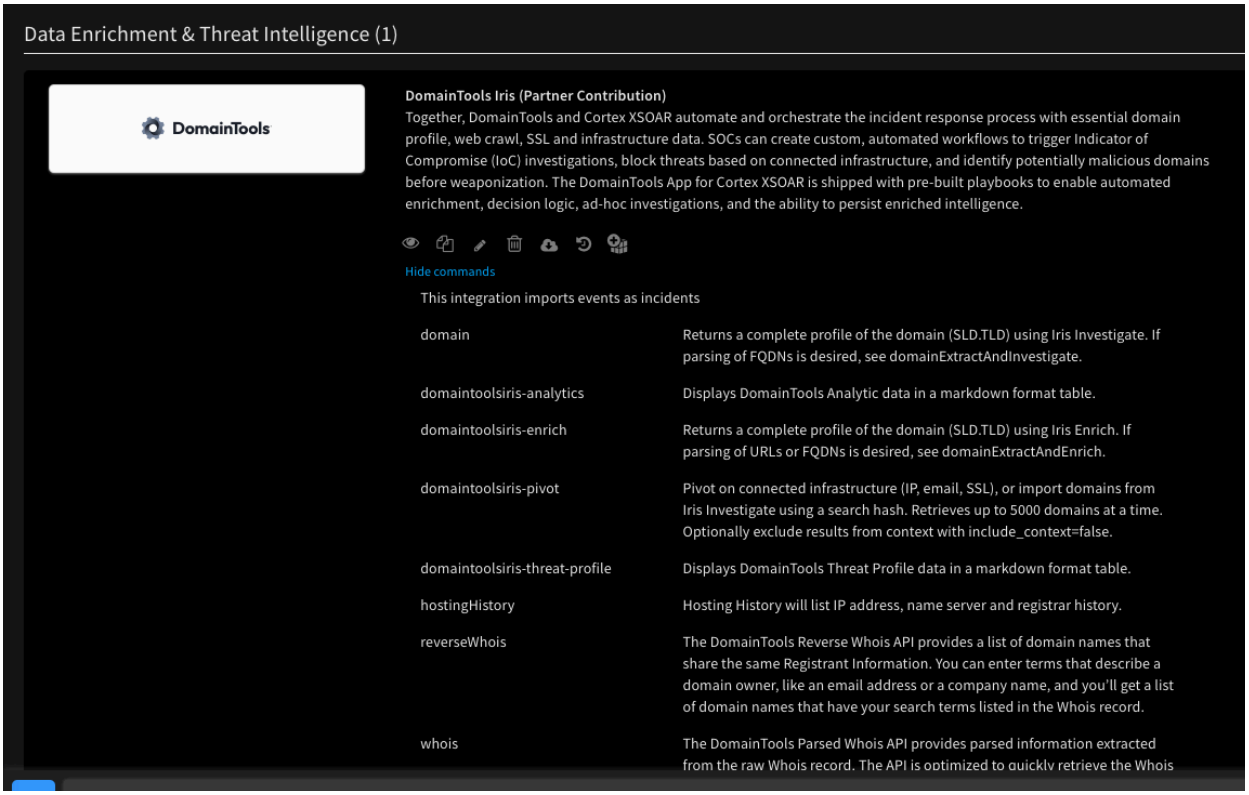
DomainTools Iris Investigate for Palo Alto XSOAR

Version 2.0, January 2024

DomainTools

Table of Contents

DomainTools App for Palo Alto XSOAR



Data Enrichment & Threat Intelligence (1)

DomainTools Iris (Partner Contribution)

Together, DomainTools and Cortex XSOAR automate and orchestrate the incident response process with essential domain profile, web crawl, SSL and infrastructure data. SOCs can create custom, automated workflows to trigger Indicator of Compromise (IoC) investigations, block threats based on connected infrastructure, and identify potentially malicious domains before weaponization. The DomainTools App for Cortex XSOAR is shipped with pre-built playbooks to enable automated enrichment, decision logic, ad-hoc investigations, and the ability to persist enriched intelligence.

This integration imports events as incidents

domain	Returns a complete profile of the domain (SLD.TLD) using Iris Investigate. If parsing of FQDNs is desired, see domainExtractAndInvestigate.
domaintoolsiris-analytics	Displays DomainTools Analytic data in a markdown format table.
domaintoolsiris-enrich	Returns a complete profile of the domain (SLD.TLD) using Iris Enrich. If parsing of URLs or FQDNs is desired, see domainExtractAndEnrich.
domaintoolsiris-pivot	Pivot on connected infrastructure (IP, email, SSL), or import domains from Iris Investigate using a search hash. Retrieves up to 5000 domains at a time. Optionally exclude results from context with include_context=false.
domaintoolsiris-threat-profile	Displays DomainTools Threat Profile data in a markdown format table.
hostingHistory	Hosting History will list IP address, name server and registrar history.
reverseWhois	The DomainTools Reverse Whois API provides a list of domain names that share the same Registrant Information. You can enter terms that describe a domain owner, like an email address or a company name, and you'll get a list of domain names that have your search terms listed in the Whois record.
whois	The DomainTools Parsed Whois API provides parsed information extracted from the raw Whois record. The API is optimized to quickly retrieve the Whois

The new Palo Alto XSOAR Iris App brings contextual DNS intelligence from DomainTools Iris to Palo Alto XSOAR. Security teams using Palo Alto XSOAR can leverage the App to automate the enrichment of malicious observables within incidents. Security analysts can now leverage DomainTools intelligence across all their response workflows and automate mundane tasks.

With this Iris App, we enable the capabilities of Iris Investigate API within Palo Alto XSOAR and bring forth a richer dataset and economize the enrichment process for our users. Users can leverage Palo Alto XSOAR's investigation and case management capabilities to investigate Domain observables with greater context and speed.

Key capabilities enabled by the app include:

- Adhoc investigations of Domain IOCs inside Palo Alto XSOAR Incidents
- Triage with DomainTools Risk Score, Threat Profile Scores and other actionable Analytics
- Persist DomainTools Intelligence inside Palo Alto XSOAR
- Discover Connected Infrastructure for a malicious domain
- Automate triaging of DomainTools Iris Tags inside Palo Alto XSOAR
- Automate enrichment process using DomainTools playbooks
- Target threat hunting at key aspects of a domain name’s registration profile

Getting Started

Requirements

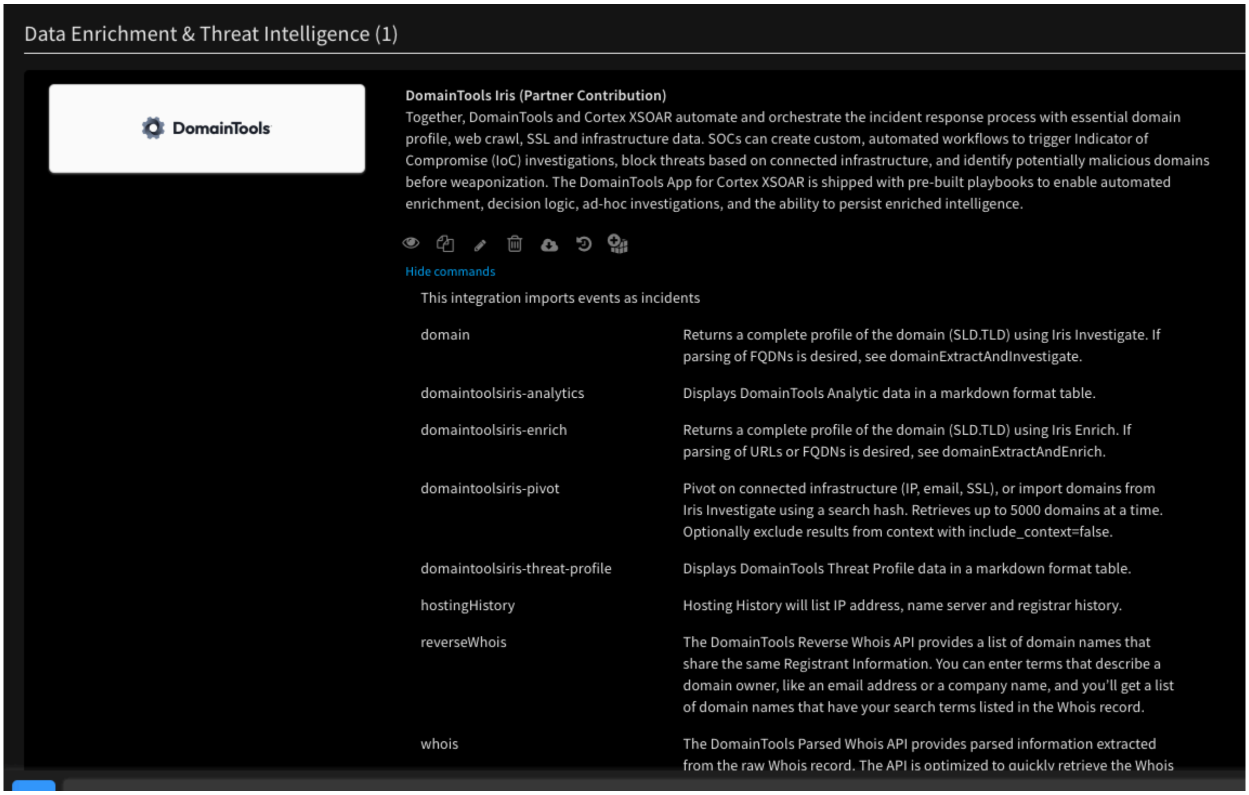
The following requirements and components need to be installed and activated prior to deployment:

- Palo Alto XSOAR Server - 6.6.0
- Palo Alto XSOAR Content version 1.32.44 (6877054)
- Active DomainTools Iris Investigate API (username and key)

Setup & Configuration

To install and configure the DomainTools App in Palo Alto XSOAR, follow the steps below:

1. Login to your Palo Alto XSOAR platform with your username and password
2. Select **Settings -> Integrations -> Servers & Services** menu options. Type "DomainTools" in the search integration text box. You should be able to see the new Iris App.



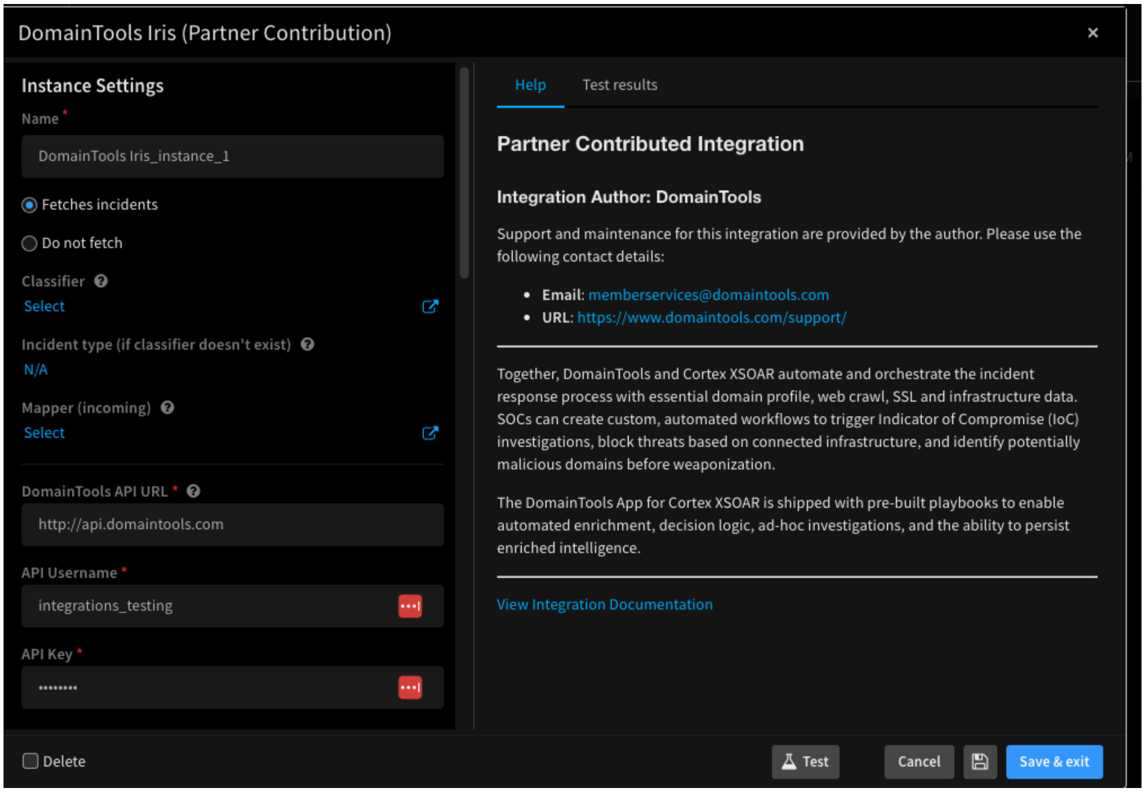
DomainTools Iris (Partner Contribution)

Together, DomainTools and Cortex XSOAR automate and orchestrate the incident response process with essential domain profile, web crawl, SSL and infrastructure data. SOCs can create custom, automated workflows to trigger Indicator of Compromise (IoC) investigations, block threats based on connected infrastructure, and identify potentially malicious domains before weaponization. The DomainTools App for Cortex XSOAR is shipped with pre-built playbooks to enable automated enrichment, decision logic, ad-hoc investigations, and the ability to persist enriched intelligence.

This integration imports events as incidents

domain	Returns a complete profile of the domain (SLD.TLD) using Iris Investigate. If parsing of FQDNs is desired, see domainExtractAndInvestigate.
domaintoolsiris-analytics	Displays DomainTools Analytic data in a markdown format table.
domaintoolsiris-enrich	Returns a complete profile of the domain (SLD.TLD) using Iris Enrich. If parsing of URLs or FQDNs is desired, see domainExtractAndEnrich.
domaintoolsiris-pivot	Pivot on connected infrastructure (IP, email, SSL), or import domains from Iris Investigate using a search hash. Retrieves up to 5000 domains at a time. Optionally exclude results from context with include_context=false.
domaintoolsiris-threat-profile	Displays DomainTools Threat Profile data in a markdown format table.
hostingHistory	Hosting History will list IP address, name server and registrar history.
reverseWhois	The DomainTools Reverse Whois API provides a list of domain names that share the same Registrant Information. You can enter terms that describe a domain owner, like an email address or a company name, and you'll get a list of domain names that have your search terms listed in the Whois record.
whois	The DomainTools Parsed Whois API provides parsed information extracted from the raw Whois record. The API is optimized to quickly retrieve the Whois

3. Select **Add Instance** to configure the DomainTools instance.
4. Enter configuration parameters described below:



Instance Settings

Name *
DomainTools Iris_instance_1

● Fetches incidents
○ Do not fetch

Classifier
Select

Incident type (if classifier doesn't exist)
N/A

Mapper (incoming)
Select

DomainTools API URL *
http://api.domaintools.com

API Username *
integrations_testing

API Key *
••••••••

□ Delete

Partner Contributed Integration

Integration Author: DomainTools

Support and maintenance for this integration are provided by the author. Please use the following contact details:

- **Email:** memberservices@domaintools.com
- **URL:** https://www.domaintools.com/support/

Together, DomainTools and Cortex XSOAR automate and orchestrate the incident response process with essential domain profile, web crawl, SSL and infrastructure data. SOCs can create custom, automated workflows to trigger Indicator of Compromise (IoC) investigations, block threats based on connected infrastructure, and identify potentially malicious domains before weaponization.

The DomainTools App for Cortex XSOAR is shipped with pre-built playbooks to enable automated enrichment, decision logic, ad-hoc investigations, and the ability to persist enriched intelligence.

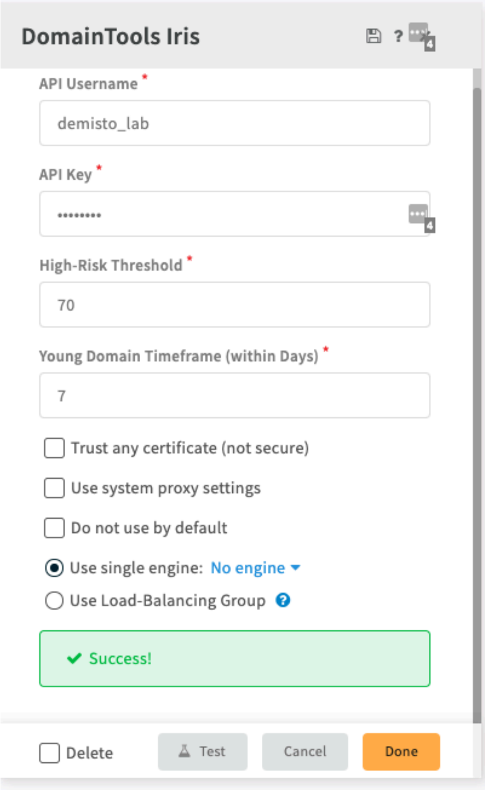
View Integration Documentation

Parameter Name	Required	Description
API Username	Yes	● Authentication Key to connect to DomainTools. It will be used for making API calls.
API Key	Yes	● API Secret to connect to DomainTools. It will be used for making API calls.
High-Risk Threshold	Yes	● A configurable threshold for DomainTools Risk Score that will be used to flag Risky Domains within your Palo Alto XSOAR Instance. ● Defaulted to 70.
Young Domain Timeframe	Yes	● A configurable threshold (in days) used to calculate if a domain is considered as a 'young domain' within Palo Alto XSOAR.
Guided Pivot Threshold	Yes	● A configurable
Fetch Incidents	Yes	● This field determines if we will enable the fetching of

Parameter Name	Required	Description
		incidents. (Monitoring of Iris Hash and Iris tag)
Classifier	No	● This field determines the Classifier to be used when incidents are fetched/created. It classifies the incident which type it will go to. ● You may choose: *DomainTools_Iris_Classifier* ● **Note**: If 'Fetches incident' is enabled, this field is required.
Incident Type	No	● This field determines what type of incident will be created. ● It should be default to "N/A" as we have 2 types of Incidents. The **Classifiers** will be used to handle this.
Mapper	No	● This field determines the Mapper to be used when incidents are fetched/created. It maps the result with a given key to the created incident. ● Currently maps the `domain` key from Iris result to **Additional Indicators** incident field. ● You may choose: **DomainTools_Iris_Mapper** ● **Note**: If 'Fetches incident' is enabled, this field is required.
Enabled on Monitoring Domains by Iris Hash	No	● This option determines what method will be used. ● Options are **Import Indicators Only** and **Create Incident and Import Indicators** . ● Defaults to **Import Indicators Only.** ● **Note**: If 'Fetches incident' is enabled, this field is required.
DomainTools Iris Investigate Search Hash	No	● **Note**: If 'Fetches incident' is enabled, this field is required.
Enabled on Monitoring Domains by Iris Tags		● This option determines what method will be used. ● Options are **Import Indicators Only** and **Create Incident and Import Indicators**. ● Defaults to **Import Indicators Only.** ● **Note**: If 'Fetches incident' is enabled, this field is required.
DomainTools Iris Tags	No	● This field contains the Iris Tags we want to monitor. ● It creates incident or/and create an indicator for each new domains found based on the ● **Note**: If 'Fetches incident' is enabled, this field is required.
Maximum	No	● This field determines the maximum incidents to fetch.

Parameter Name	Required	Description
Incidents to Fetch		- Defaults to 2. - One (1) for each possible feed type iris search hash and iris tags.
Incidents Fetch Interval	No	- This field determines the interval to fetch incidents (fetch results from Iris Investigate API with the given iris hash and iris tags.) - **Note**: If 'Fetches incident' is enabled, this field is required.

5. Test connectivity with DomainTools by clicking the 'Test' button and look for the **Success!** indicator.



DomainTools Iris

API Username *

demisto_lab

API Key *

••••••••

High-Risk Threshold *

70

Young Domain Timeframe (within Days) *

7

□ Trust any certificate (not secure)

□ Use system proxy settings

□ Do not use by default

● Use single engine: No engine

○ Use Load-Balancing Group

✓ Success!

□ Delete

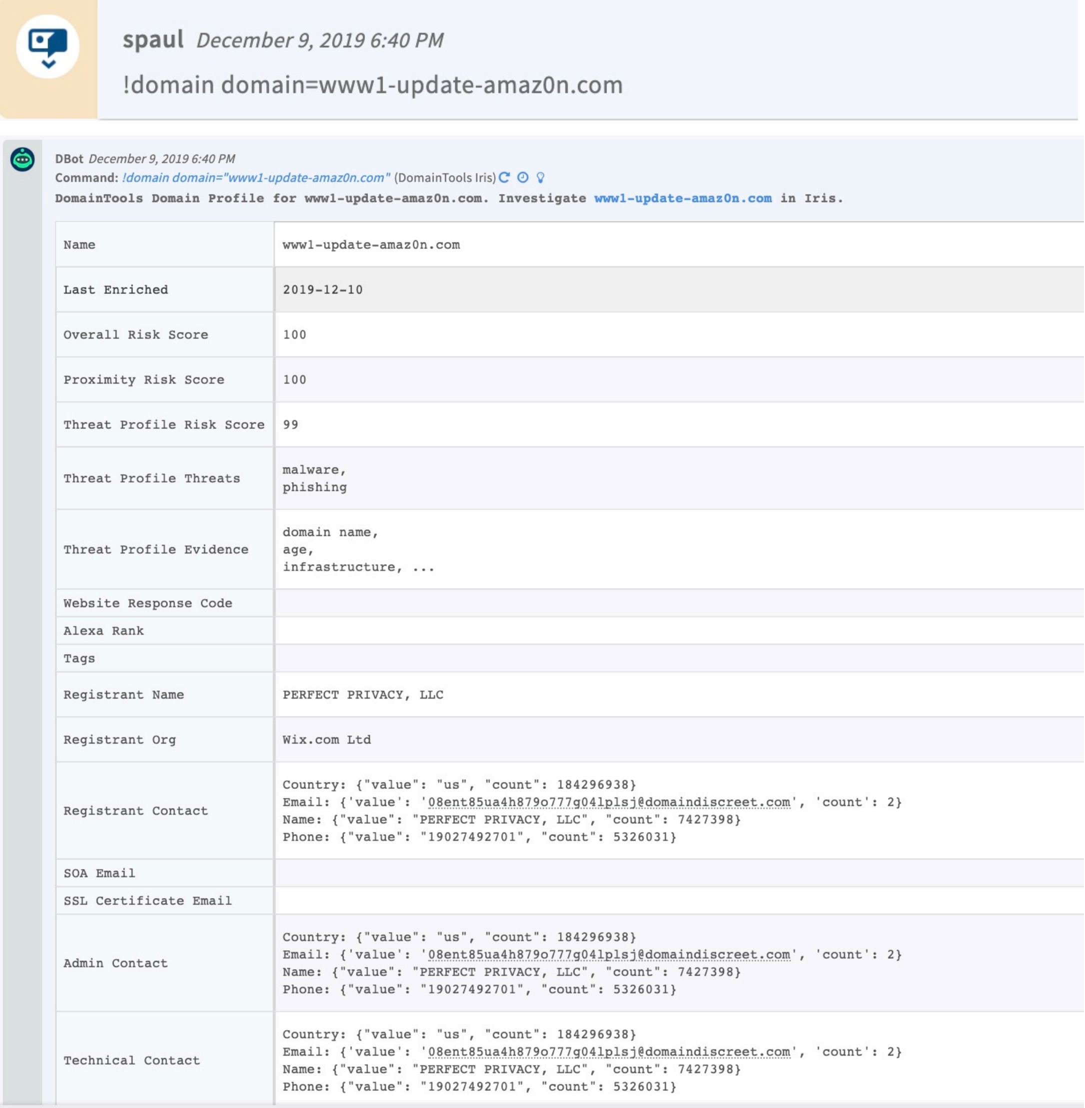
DomainTools App Capabilities

Ad Hoc Investigations in "War-Room"

Enrich a Domain

Enriches domain-related data from the Iris dataset, including domain risk scores, Whois, IP, active DNS, website, and SSL data. Enables rapid enrichment of proxy and DNS logs, enhancing the ability to detect and respond to threats in real-time. Customers can identify malicious domains and assess their risk levels efficiently.

Query DomainTools for DNS intelligence for a specific Indicator:



spaul *December 9, 2019 6:40 PM*

!domain domain=www1-update-amaz0n.com

DBot *December 9, 2019 6:40 PM*

Command: *!domain domain="www1-update-amaz0n.com"* (DomainTools Iris)

DomainTools Domain Profile for www1-update-amaz0n.com. Investigate www1-update-amaz0n.com in Iris.

Name	www1-update-amaz0n.com
Last Enriched	2019-12-10
Overall Risk Score	100
Proximity Risk Score	100
Threat Profile Risk Score	99
Threat Profile Threats	malware, phishing
Threat Profile Evidence	domain name, age, infrastructure, ...
Website Response Code	
Alexa Rank	
Tags	
Registrant Name	PERFECT PRIVACY, LLC
Registrant Org	Wix.com Ltd

Registrant Contact	Country: {"value": "us", "count": 184296938}
	Email: {'value': '08ent85ua4h879o777g04lplsj@domaindiscreet.com', 'count': 2}
	Name: {"value": "PERFECT PRIVACY, LLC", "count": 7427398}
	Phone: {"value": "19027492701", "count": 5326031}

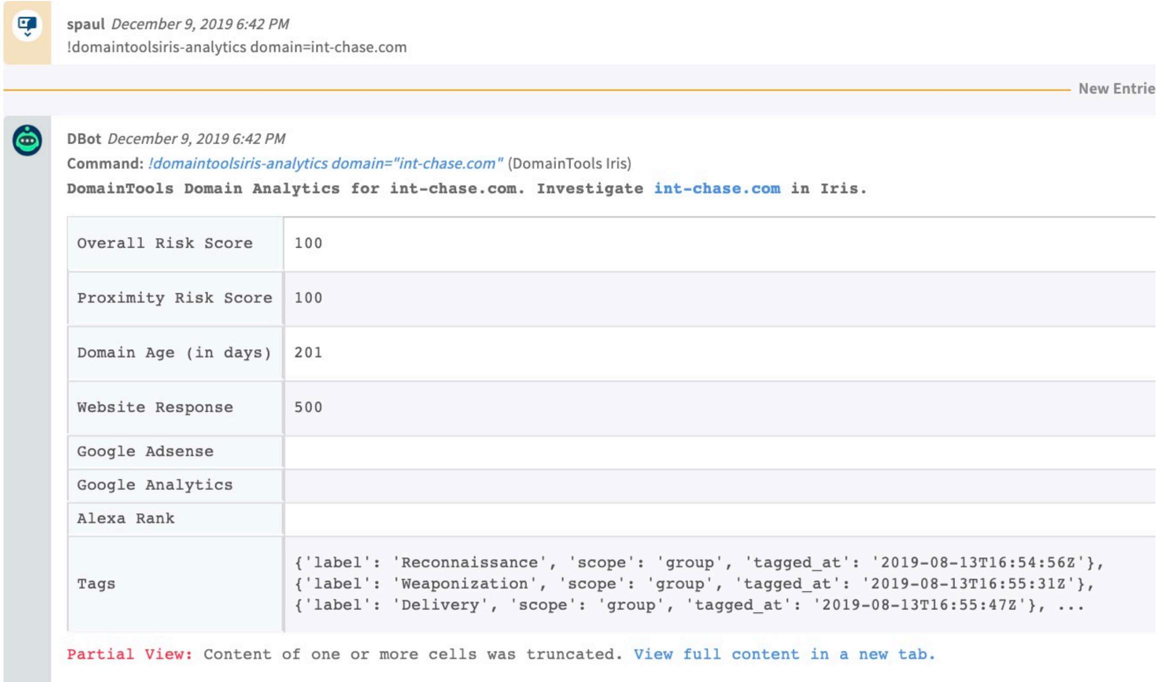
SOA Email	
SSL Certificate Email	

Admin Contact	Country: {"value": "us", "count": 184296938}
	Email: {'value': '08ent85ua4h879o777g04lplsj@domaindiscreet.com', 'count': 2}
	Name: {"value": "PERFECT PRIVACY, LLC", "count": 7427398}
	Phone: {"value": "19027492701", "count": 5326031}

Technical Contact	Country: {"value": "us", "count": 184296938}
	Email: {'value': '08ent85ua4h879o777g04lplsj@domaindiscreet.com', 'count': 2}
	Name: {"value": "PERFECT PRIVACY, LLC", "count": 7427398}
	Phone: {"value": "19027492701", "count": 5326031}

Retrieve DomainTools Analytics

Actionable Analytics from Iris



spaul *December 9, 2019 6:42 PM*
!domaintoolsiris-analytics domain=int-chase.com

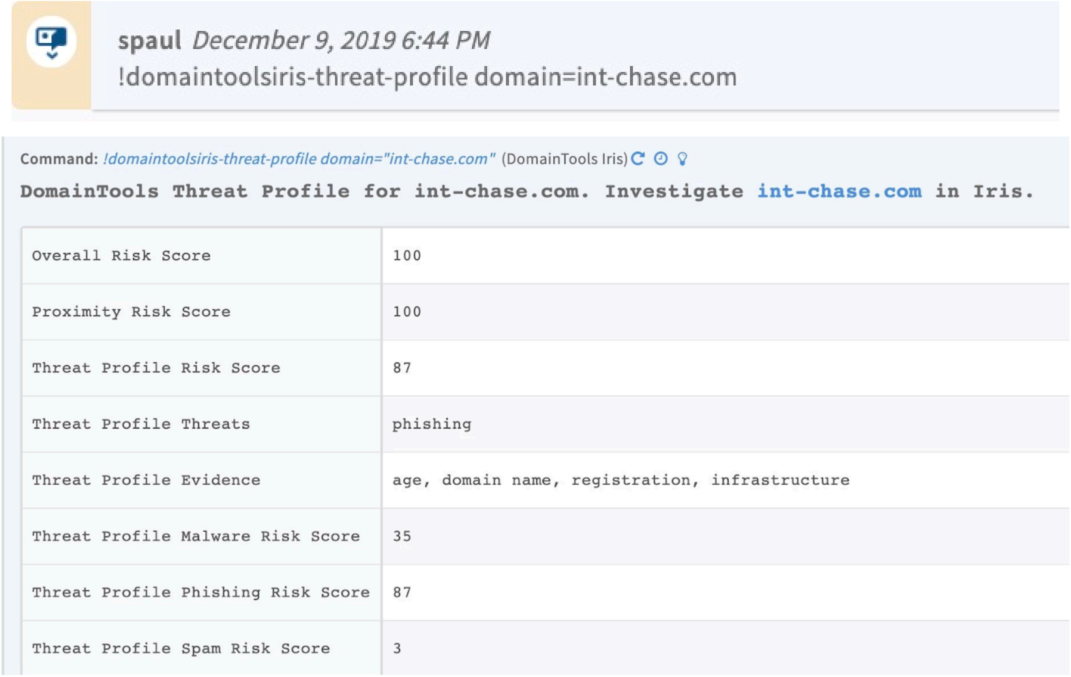
DBot *December 9, 2019 6:42 PM*
Command: *!domaintoolsiris-analytics domain="int-chase.com"* (DomainTools Iris)

DomainTools Domain Analytics for int-chase.com. Investigate int-chase.com in Iris.

Overall Risk Score	100
Proximity Risk Score	100
Domain Age (in days)	201
Website Response	500
Google Adsense	
Google Analytics	
Alexa Rank	
Tags	{'label': 'Reconnaissance', 'scope': 'group', 'tagged_at': '2019-08-13T16:54:56Z'}, {'label': 'Weaponization', 'scope': 'group', 'tagged_at': '2019-08-13T16:55:31Z'}, {'label': 'Delivery', 'scope': 'group', 'tagged_at': '2019-08-13T16:55:47Z'}, ...

Partial View: Content of one or more cells was truncated. View full content in a new tab.

Risk Scores, Threat Profiles, and Evidence



spaul *December 9, 2019 6:44 PM*
!domaintoolsiris-threat-profile domain=int-chase.com

Command: *!domaintoolsiris-threat-profile domain="int-chase.com"* (DomainTools Iris)

DomainTools Threat Profile for int-chase.com. Investigate int-chase.com in Iris.

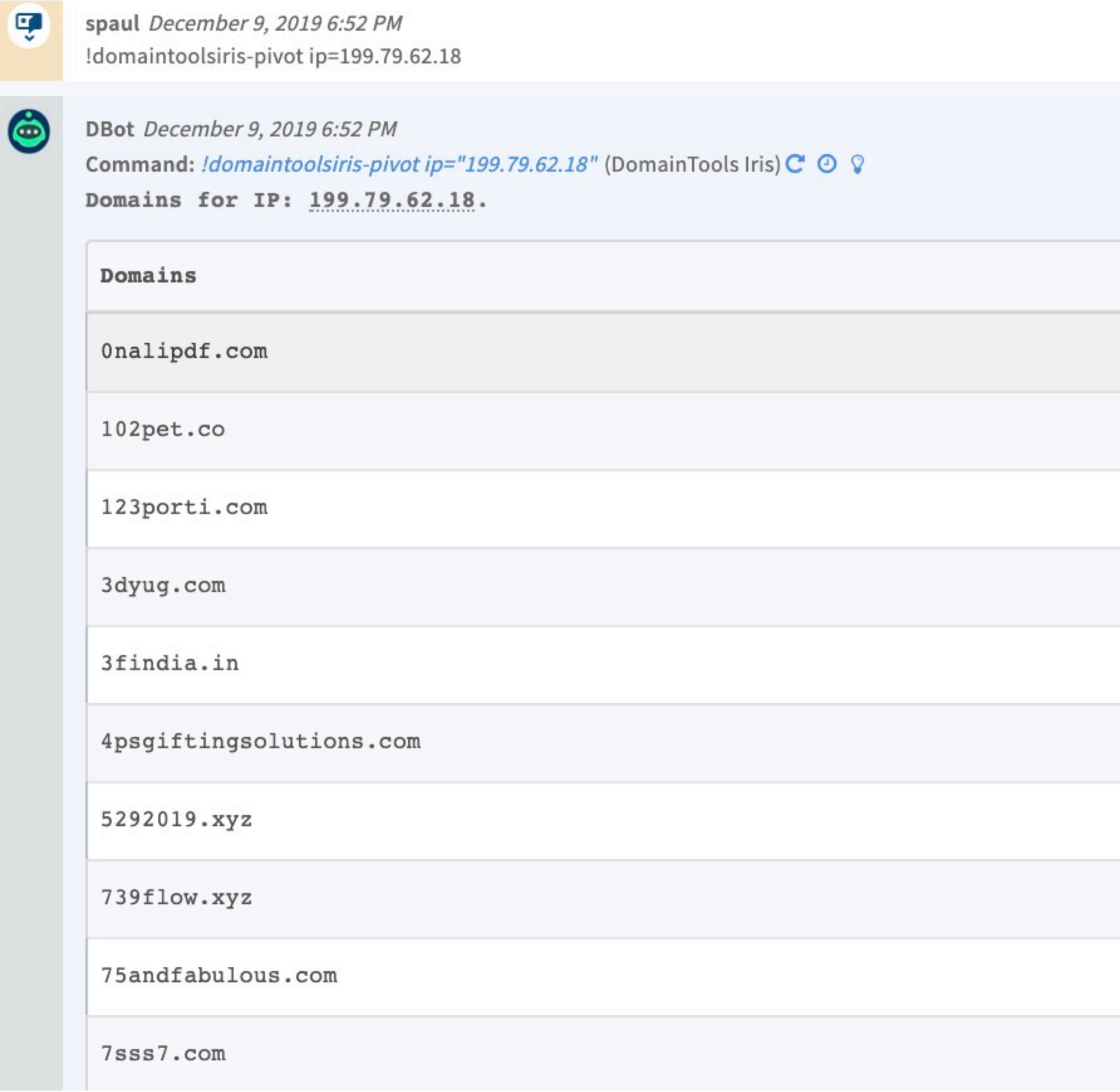
Overall Risk Score	100
Proximity Risk Score	100
Threat Profile Risk Score	87
Threat Profile Threats	phishing
Threat Profile Evidence	age, domain name, registration, infrastructure
Threat Profile Malware Risk Score	35
Threat Profile Phishing Risk Score	87
Threat Profile Spam Risk Score	3

Discover Connected Infrastructure

Palo Alto XSOAR users can pivot on any of the below DomainTools attributes to discover potentially malicious infrastructure associated with the DNS artifact:

- IP
- Email
- Mailserver_Host
- Nameserver_Host
- Nameserver_IP
- SSL Hash

Below is one example of pivoting on the Hosting IP address:



spaul *December 9, 2019 6:52 PM*
!domaintoolsiris-pivot ip=199.79.62.18

DBot *December 9, 2019 6:52 PM*
Command: *!domaintoolsiris-pivot ip="199.79.62.18"* (DomainTools Iris)

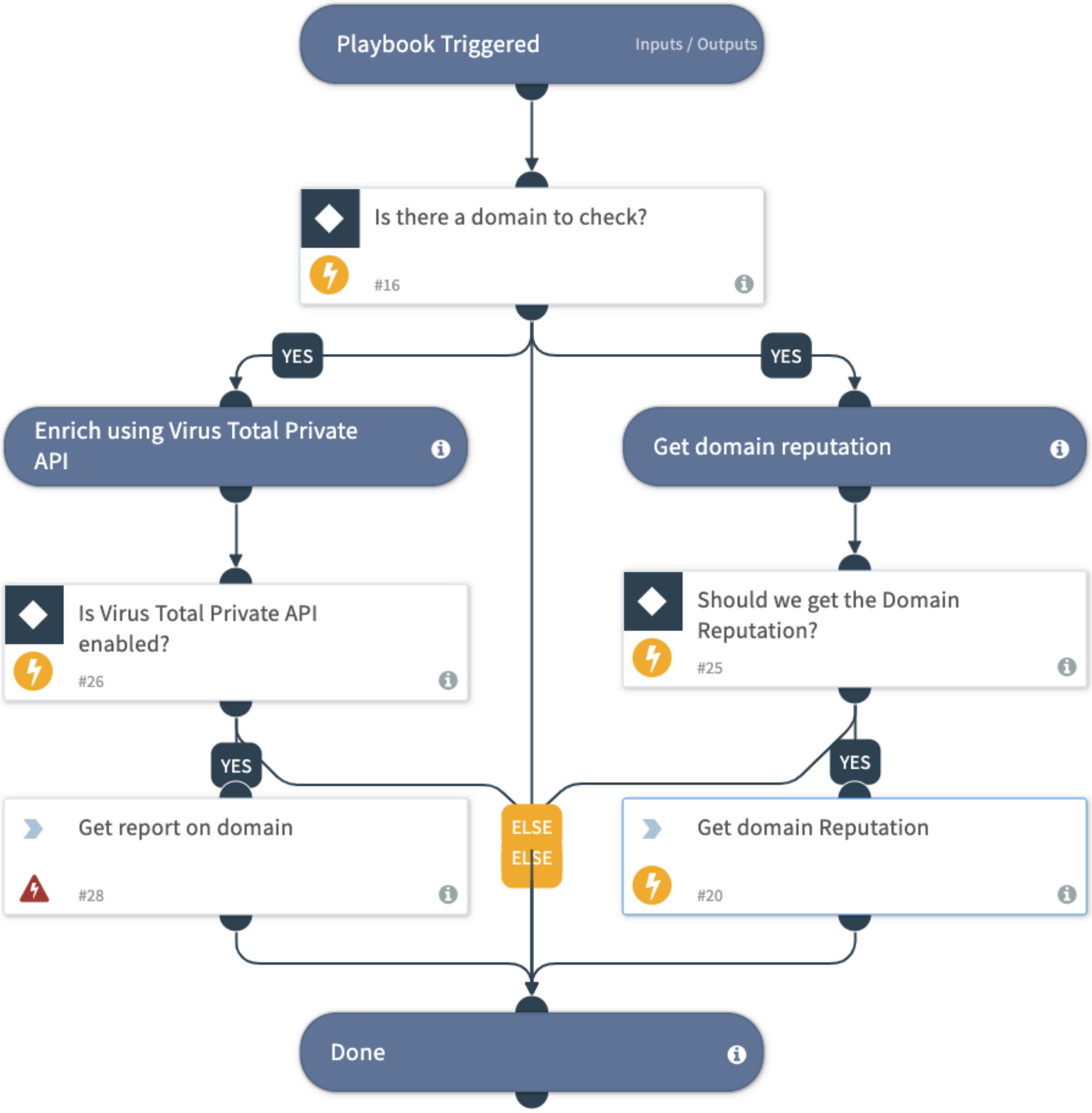
```
Domains for IP: 199.79.62.18.
```

Domains
0nalipdf.com
102pet.co
123porti.com
3dyug.com
3findia.in
4psgiftingsolutions.com
5292019.xyz
739flow.xyz
75andfabulous.com
7sss7.com

Automating using Playbooks

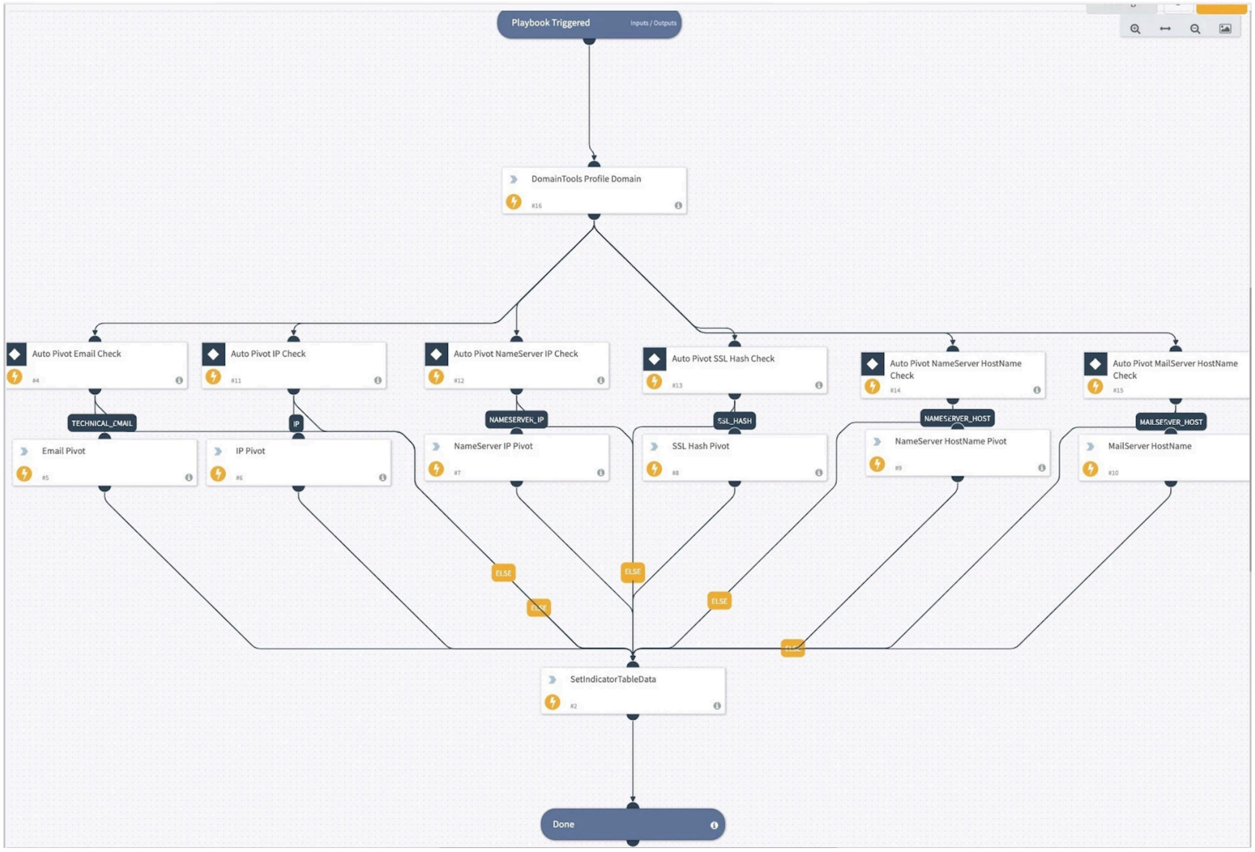
Auto Enrichment of Domains

Our enrichment is integrated with Palo Alto XSOAR's '!domain' command and hence can be triggered with any of the out-of-the-box' playbooks as such:



Automate Connected Infrastructure Discovery

The below playbook automates the pivoting command for all 6 functions that a user can execute manually in the 'war room' (see above). The playbook leverages the 'guided-pivot' threshold value to discover any qualified infrastructure that may be connected with the Indicator.



Custom Playbooks

Getting Started with Custom Playbooks

In addition to the automation available within Palo Alto XSOAR, DomainTools continues to build additional content for XSOAR users. You can download our automation scripts directly from the DomainTools Palo Alto XSOAR repository in Github. We plan to update our GitHub repository with new playbooks in the future. Our current offering is as follows.

Customizing Error Handling

XSOAR playbooks will halt on errors by default. Currently, some DomainTools playbooks may generate errors (such as when fed unregistered domains) that want to skip over.

You can modify a playbook's error handling via its **On Error** tab in **Task Details** in several ways:

- Specify a permitted number of retries and the time between retries
- Set the task to continue through an error
- Set the task to take an error path

Palo Alto documents customized error handling in this YouTube video.

Checking Prerequisites

Before you upload these custom playbooks, please review the **Prerequisites** section for each. It identifies any additional configurations and dependencies associated with these playbooks.

Playbook: DomainTools Auto Pivots

This playbook fetches the Iris Investigate profile of a domain and automatically identifies related infrastructure artifacts based on DomainTools Guided Pivot values.

- **Automated Investigations**: It streamlines the investigative process by automatically identifying connected infrastructure, saving analysts time and reducing human error.
- **Comprehensive Understanding**: Customers gain a more complete understanding of threats by uncovering associated infrastructure, enabling better threat assessment.
- **Proactive Threat Detection**: By automating pivot lookups, it assists in the early detection of threats associated with a specific domain.

Playbook: DomainTools Check Domain Risk Score By Iris Tags

This playbook periodically checks domains for risk based on Iris Investigate tags. Users can define a list of tags to monitor, and the playbook will add new high-risk domains as indicators on associated incidents.

- **Proactive Risk Management**: Customers can proactively monitor domains associated with specific tags, enabling early risk detection and mitigation.
- **Automation**: The playbook automates the process of tracking and alerting on domain risk, reducing manual effort and ensuring timely responses.
- **Incident Enrichment**: It enriches incidents with high-risk domain indicators, providing context for incident responders and aiding in swift decision-making.

Playbook: DomainTools Check New Domains by Iris Hash Playbook

This playbook assists in monitoring new domains based on predefined infrastructure criteria, such as registrar, DNS, SSL certs, etc. It uses Iris Investigate data to identify newly registered domains.

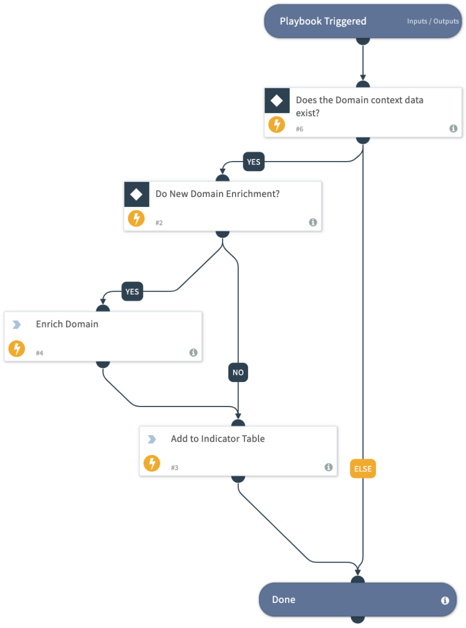
- **Timely Threat Detection**: Customers can detect new domains associated with specific infrastructure parameters, allowing them to identify potential threats in their early stages.
- **Customizable Monitoring**: Users can define specific criteria for monitoring, tailoring the playbook to their organization's unique threat landscape.
- **Integration with Iris Investigate**: It leverages DomainTools' data to enhance monitoring capabilities, ensuring comprehensive threat visibility.

Playbook: Auto Enrichment of Indicators

Although Palo Alto XSOAR users can leverage the enrichment capability out-of-the-box, we wanted to further extend their ability to optimize the auto-enrichment process.

The **DomainTools_Domain_Auto_Enrichment** playbook provides you with the following functionalities:

- Checks if enrichment data is recent if so skips redundant enrichment of the domain
- Performs Domain Enrichment
- Stores key Enrichment Intelligence in Palo Alto XSOAR Indicator Table

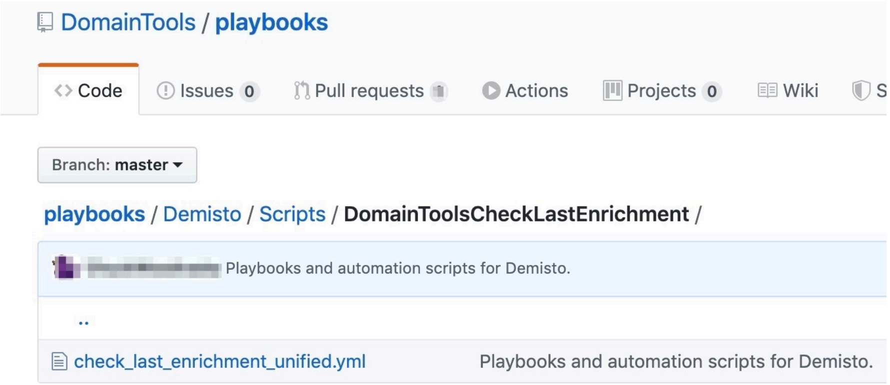


Prerequisites

Automation Scripts

The playbook uses the following automation scripts to deliver these functionalities. Both of these are available for the download in the same repository above (under Scripts' folder):

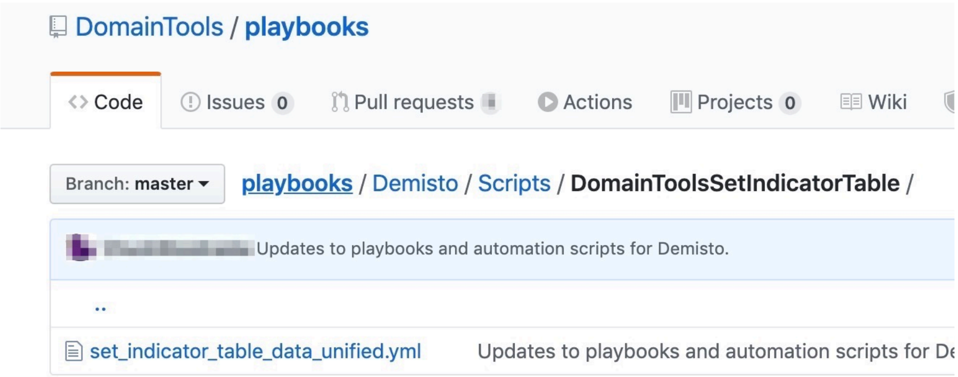
- DomainToolsCheckLastEnrichment
- DomainToolsSetIndicatorTable



playbooks / Demisto / Scripts / DomainToolsCheckLastEnrichment /

[redacted] Playbooks and automation scripts for Demisto.

check_last_enrichment_unified.yml Playbooks and automation scripts for Demisto.



playbooks / Demisto / Scripts / DomainToolsSetIndicatorTable /

[redacted] Updates to playbooks and automation scripts for Demisto.

..

set_indicator_table_data_unified.yml Updates to playbooks and automation scripts for De

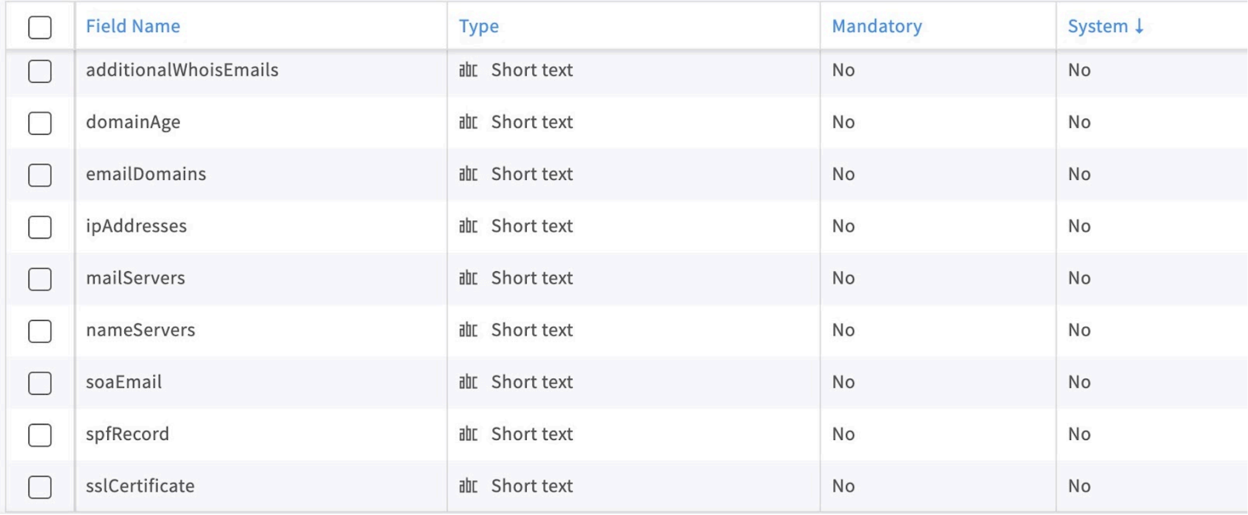
Custom Indicator fields

The playbook leverages the following custom fields in the Indicator table to store the domain intelligence inside Palo Alto XSOAR. These fields must be created prior to executing the playbook:

1. Select **Settings ->Advanced -> Fields** menu options
2. Select Indicator from the dropdown list, shown below
3. Add New Fields per the table below:

Field Name	Field Type	Mandatory
additionalWhoisEmails	Short text	No
domainAge	Short text	No
emailDomains	Short text	No
ipAddresses	Short text	No
mailServers	Short text	No
nameServers	Short text	No
soaEmail	Short text	No
spfRecord	Short text	No
sslCertificate	Short text	No

4. The following list of fields will appear under Indicator table, once fields are created successfully



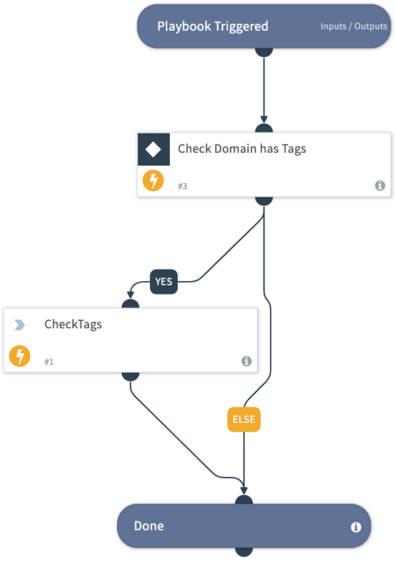
□	Field Name	Type	Mandatory	System ↓
□	additionalWhoisEmails	Short text	No	No
□	domainAge	Short text	No	No
□	emailDomains	Short text	No	No
□	ipAddresses	Short text	No	No
□	mailServers	Short text	No	No
□	nameServers	Short text	No	No
□	soaEmail	Short text	No	No
□	spfRecord	Short text	No	No
□	sslCertificate	Short text	No	No

Playbook: DomainTools Iris Tags

The DomainTools_Iris_Tags playbook helps users flag any domains that have already been flagged in the DomainTools Iris investigation platform. This helps various cross-functional teams within the SOC to collaborate during an investigation.

The **DomainTools_Iris_Tags** playbook provides you with the following functionalities:

- Allows Palo Alto XSOAR users to configure a list of 'Iris tags' they want to monitor inside Palo Alto XSOAR
- Automate checking for any Indicators that match one of the tags
- Escalates the Incident Severity to 'High'



Prerequisites

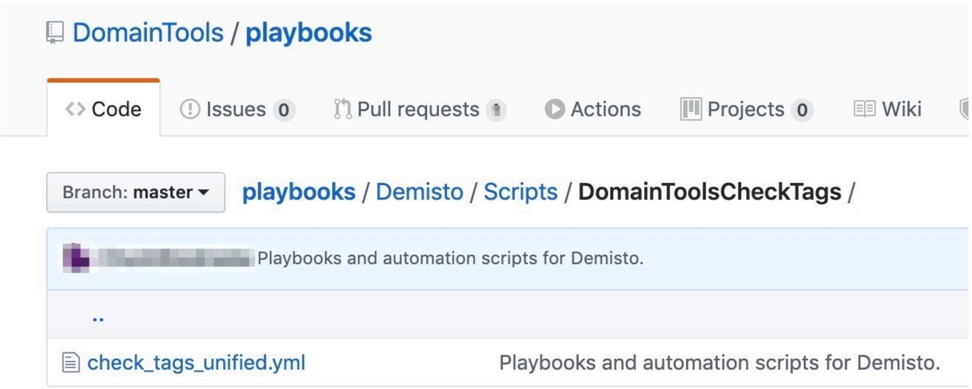
Creating Tags in DomainTools Iris

To leverage this feature Palo Alto XSOAR Users must be using the Tagging capabilities from DomainTools Iris Investigation platform. Once a Domain is 'Tagged' in Iris, the tags become available for consumption within Palo Alto XSOAR. Please refer to 'Tagging Domains' in DomainTools Iris user guide for further reference.

Automation Scripts

The playbook uses the below automation script to deliver these functionalities. This script is also available for the download in the same repository under 'Scripts' folder (see above):

- DomainToolsCheckTags



playbooks / Demisto / Scripts / DomainToolsCheckTags /

[redacted] Playbooks and automation scripts for Demisto.

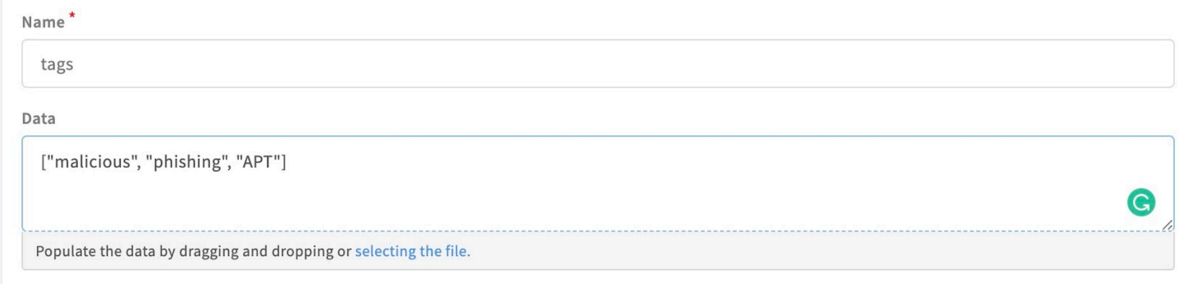
..

check_tags_unified.yml Playbooks and automation scripts for Demisto.

Custom 'Tag' List

Palo Alto XSOAR users can store the list of tags inside Palo Alto XSOAR following the below steps:

1. Select **Select Settings ->Advanced -> Lists -> New List** menu options
2. Set values:
    a. Name: 'tags'
    b. Data: <Your list of tags comma delimited>
3. The list will appear similar to the below setup in our lab environment



Name *

tags

Data

["malicious", "phishing", "APT"]

Populate the data by dragging and dropping or selecting the file.