



DomainTools Iris Investigate for Cortex XSOAR

Version 1.1, August 2022



DomainTools

Table of Contents

Table of Contents	2
DomainTools App for Cortex XSOAR	3
Getting Started	4
App Deployment	4
Requirements	4
Setup & Configuration	4
DomainTools App Capabilities	7
Adhoc Investigations in 'War-Room'	7
Enrich a Domain:	7
Retrieve DomainTools Analytics:	8
Discover connected Infrastructure:	9
Automating using Playbooks	10
Auto Enrichment of Domains:	10
Automate Connected Infrastructure Discovery:	10
Custom Playbooks	12
Auto Enrichment of Indicators	12
Prerequisites	13
Automation Scripts:	13
Custom Indicator fields:	13
DomainTools Iris Investigate Tags	15
Prerequisites	15
Creating Tags in DomainTools Iris Investigate:	15
Automation Scripts:	15
Custom 'Tag' List:	16

DomainTools App for Cortex XSOAR

The screenshot shows the marketplace entry for the 'DomainTools Iris Investigate' app. At the top, it says 'Marketplace > DomainTools Iris Investigate'. Below this are navigation tabs: 'Details' (selected), 'Content', 'Dependencies', 'Version History', and 'Reviews'. The app title is 'DomainTools Iris Investigate' with version '1.1.5' and ID '3656716'. It has a 5-star rating and a 'Write a review' link. The description states: 'Facilitates automation of key infrastructure characterization and hunting portions of the incident response process. Organizations will have access to essential domain profile, web crawl, SSL, and infrastructure data from within Cortex XSOAR. Requires a DomainTools Iris Investigate API key.' Below the description are icons for '1 Integrations' and '1 Playbooks'. A paragraph explains: 'Together, DomainTools and Cortex XSOAR automate and orchestrate the incident response processes with essential domain profile, web crawl, SSL, and infrastructure data delivered by the DomainTools Iris Investigate API. SOCs can create custom, automated workflows to trigger Indicator of Compromise (IoC) investigations, block threats based on connected infrastructure, and identify potentially malicious incidents before weaponization.' Another paragraph says: 'With the DomainTools Iris App for Cortex XSOAR, the Iris dataset is available not only for ad-hoc War-Room investigations on specific incidents, but also for automated actions. Organizations will be able to fetch a complete Iris profile for a domain name including:' followed by a bulleted list of capabilities.

The Cortex XSOAR Iris Investigate App brings contextual DNS intelligence from DomainTools Iris to Cortex XSOAR. Security teams using Cortex 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 Investigate App, we enable the capabilities of Iris Investigate API within Cortex XSOAR and bringing forth a richer dataset and economize the enrichment process for our users. Cortex XSOAR users can leverage Cortex 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 Cortex XSOAR Incidents
- Triage with DomainTools Risk Score, Threat Profile Scores and other actionable Analytics
- Persist DomainTools Intelligence inside Cortex XSOAR
- Discover Connected Infrastructure for a malicious domain
- Automate triaging of DomainTools Iris Investigate Tags inside Cortex XSOAR
- Automate enrichment process using DomainTools playbooks
- Target threat hunting at key aspects of a domain name's registration profile

Getting Started

App Deployment

Requirements

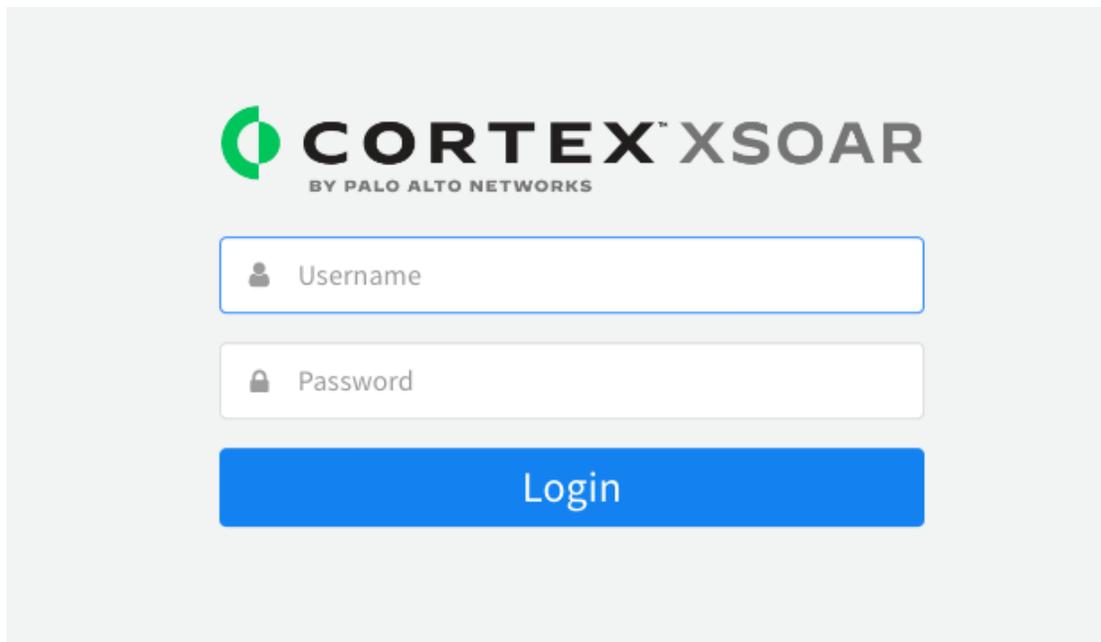
The following requirements and components need to be installed and activated prior to deployment:

- Cortex XSOAR Server - 4.5.0
- Cortex XSOAR Content version 19.11.0 (33434)
- Active DomainTools Iris Investigate API (username and key)

Setup & Configuration

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

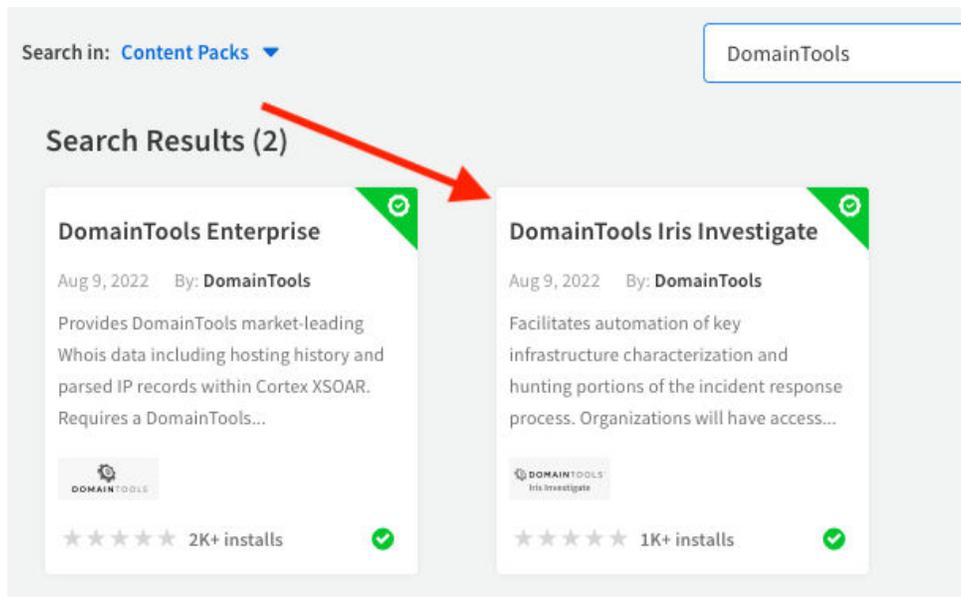
1. Login to your Cortex XSOAR platform with your username and password



The screenshot shows the Cortex XSOAR login page. At the top, there is the Cortex XSOAR logo, which consists of a green circular icon with a white 'C' shape inside, followed by the text 'CORTEX™ XSOAR' in a bold, sans-serif font, and 'BY PALO ALTO NETWORKS' in a smaller font below it. Below the logo, there are two input fields: the first is labeled 'Username' with a person icon, and the second is labeled 'Password' with a lock icon. Below these fields is a prominent blue button with the text 'Login' in white.

2. Search in the **Marketplace** for “DomainTools”.

You should be able to see the Iris Investigate App.



Note that this article describes the newer and more full-featured Iris Investigate app, not the previous Enterprise app that interacts with our previous generation Research APIs

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

A screenshot of the 'DomainTools Iris' configuration form. The form has a title bar with 'DomainTools Iris' and icons for help and refresh. Below the title bar, there are four input fields, each with a red asterisk indicating a required field. The first field is 'API Username' with the value 'demisto_lab'. The second field is 'API Key' with a masked value '*****'. The third field is 'High-Risk Threshold' with the value '70'. The fourth field is 'Young Domain Timeframe (within Days)' with the value '7'.

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 Cortex 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 Cortex XSOAR.

5. Test to check connectivity with DomainTools by clicking 'Test' button

The screenshot shows the 'DomainTools Iris' configuration window. It contains the following fields and options:

- API Username:** demisto_lab
- API Key:** [Redacted]
- 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

A green box at the bottom of the configuration area displays the message: **✓ Success!**

At the bottom of the window, there are four buttons: **Delete**, **Test**, **Cancel**, and **Done**.

DomainTools App Capabilities

Adhoc Investigations in 'War-Room'

1. Enrich a Domain:

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) [C](#) [O](#) [V](#)
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': '08ent85ua4h879o777g041pls@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': '08ent85ua4h879o777g041pls@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': '08ent85ua4h879o777g041pls@domaindiscreet.com', 'count': 2} Name: {"value": "PERFECT PRIVACY, LLC", "count": 7427398} Phone: {"value": "19027492701", "count": 5326031}

2. Retrieve DomainTools Analytics:

a. Actionable Analytics from Iris Intelligence

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

New Entry

 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.](#)

b. 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.

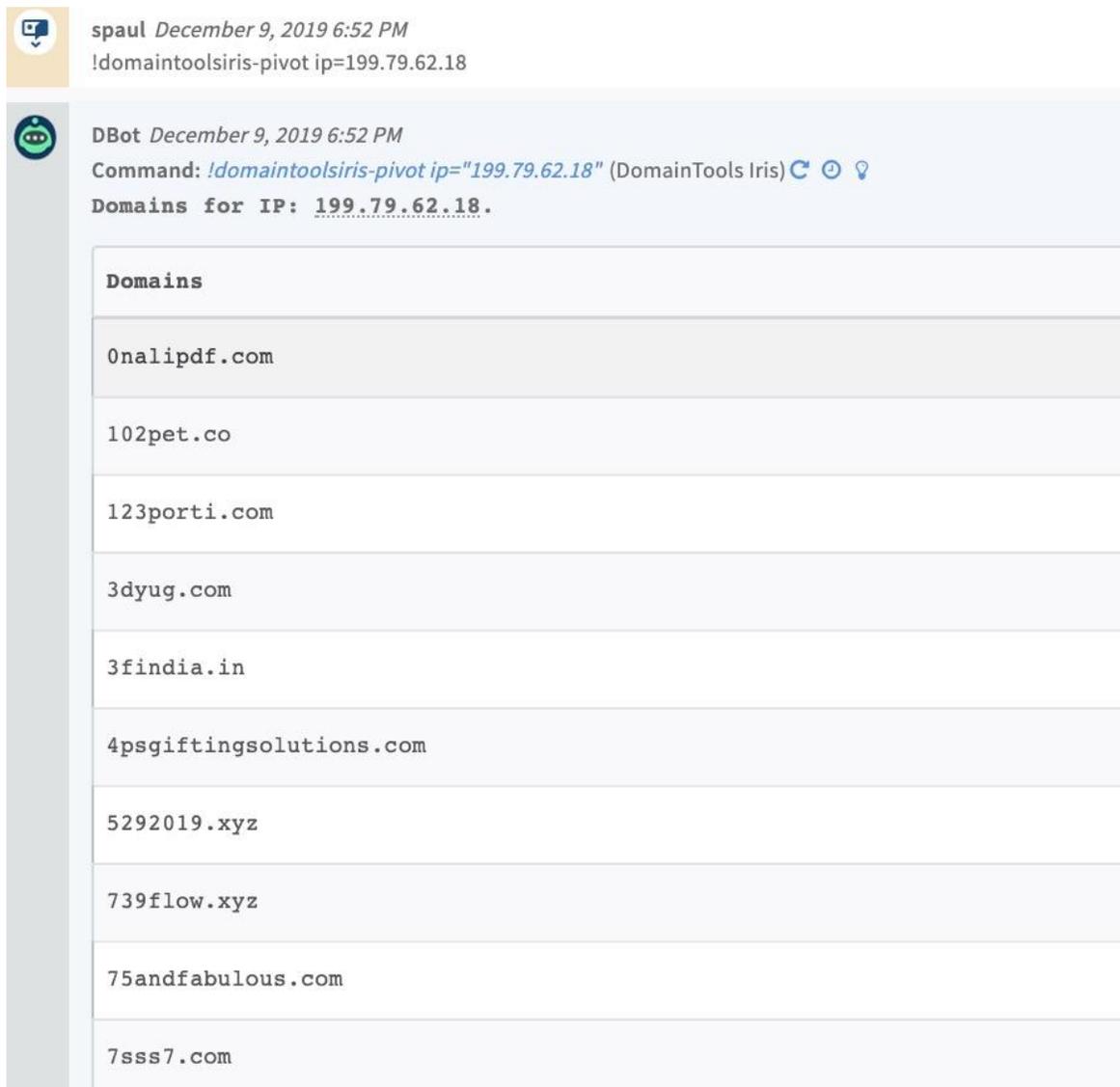
Overall Risk Score	100
Proximity Risk Score	100
Threat Profile Risk Score	87
Threat Profile Threats	phishing
Threat Profile Evidence	age, domain name, registration, infrastructure
Threat Profile Malware Risk Score	35
Threat Profile Phishing Risk Score	87
Threat Profile Spam Risk Score	3

3. Discover connected Infrastructure:

Cortex 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:



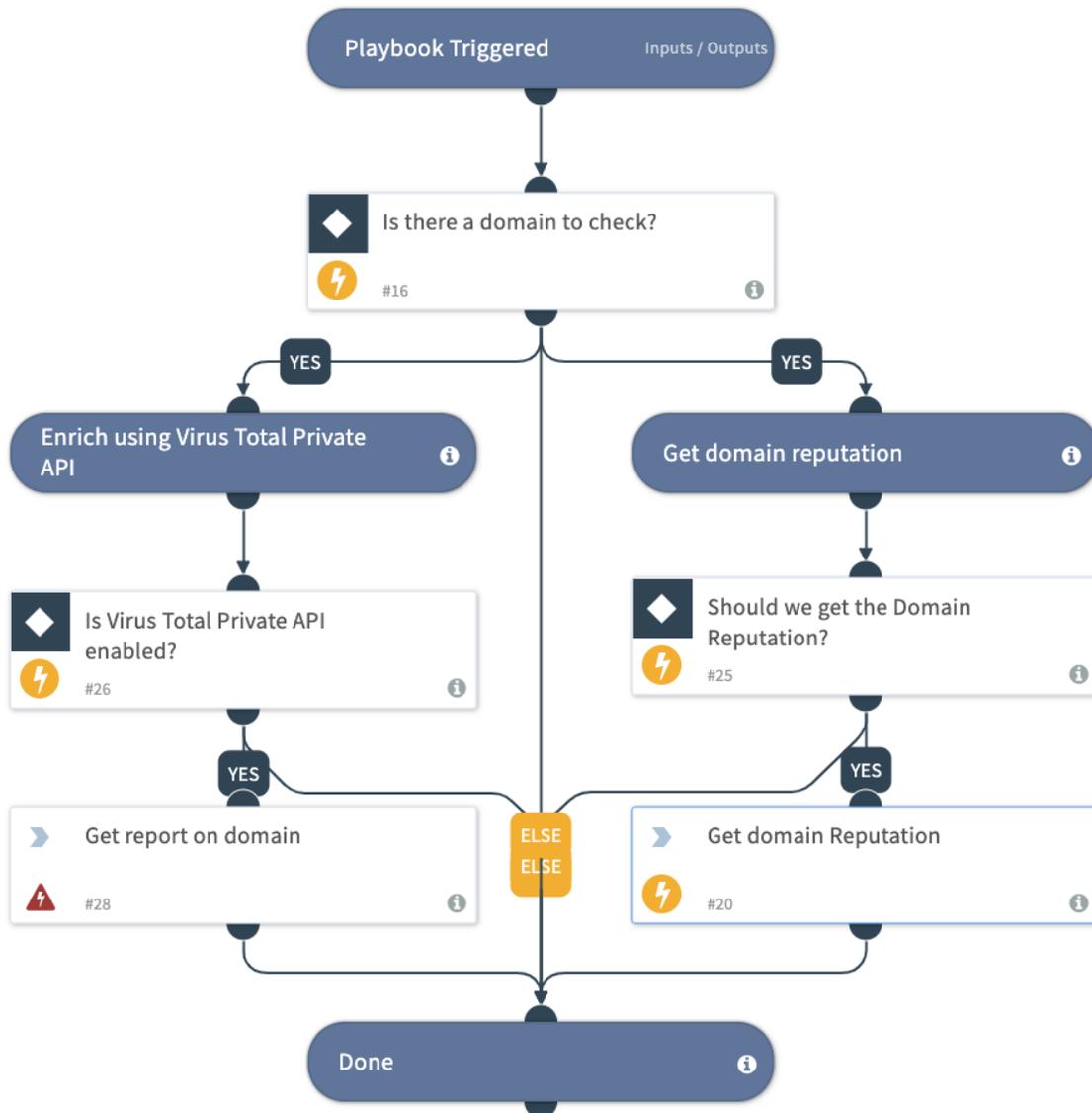
The screenshot shows a chat window with two messages. The first message is from 'spaul' at 6:52 PM on December 9, 2019, containing the command '!domaintoolsiris-pivot ip=199.79.62.18'. The second message is from 'DBot' at the same time, showing the command '!domaintoolsiris-pivot ip="199.79.62.18"' and its output: 'Domains for IP: 199.79.62.18.'. Below the command is a table listing ten domains.

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

Automating using Playbooks

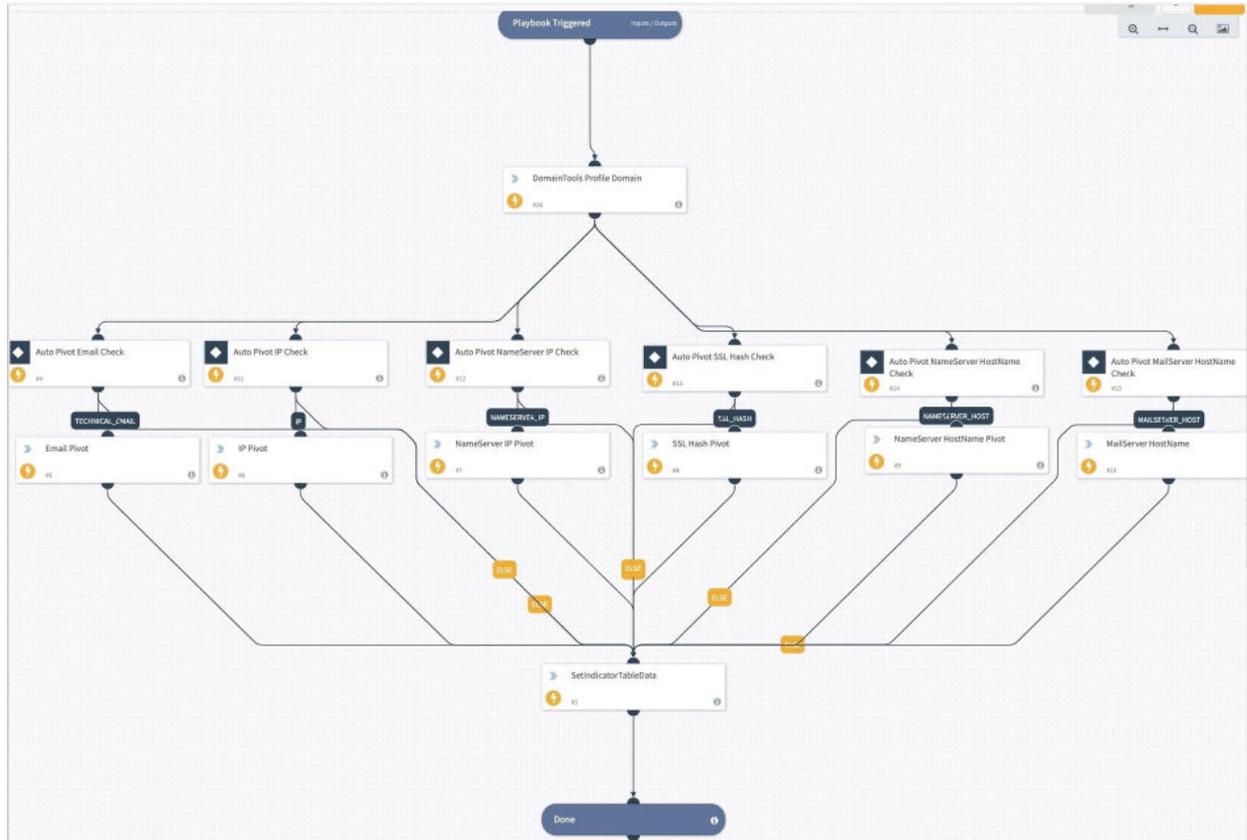
Auto Enrichment of Domains:

Our enrichment is integrated with Cortex XSOAR '!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

In addition to the automation available within Cortex XSOAR content (app), we continue to build additional content that our users may benefit from. One can download these automation scripts/content directly from [DomainTools Cortex XSOAR repository in Github](#).

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

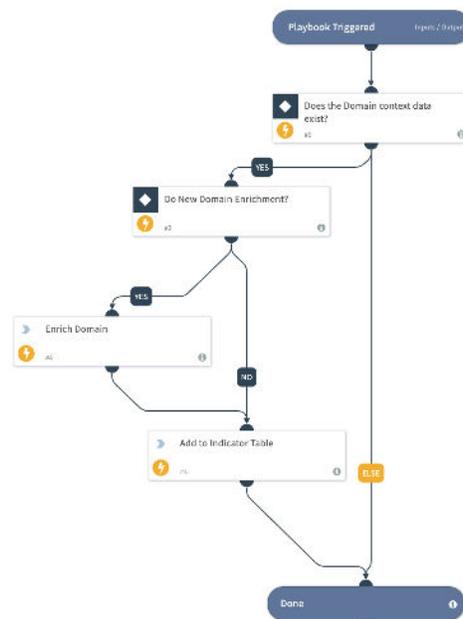
We hope to keep the documentation updated with future additions to GitHub. Below is what is available at the time of generating this guide.

Auto Enrichment of Indicators

Although Cortex 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 Cortex XSOAR Indicator Table

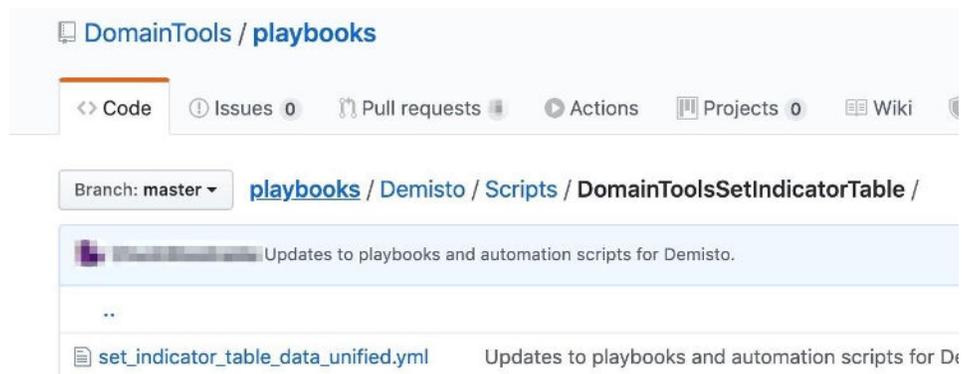
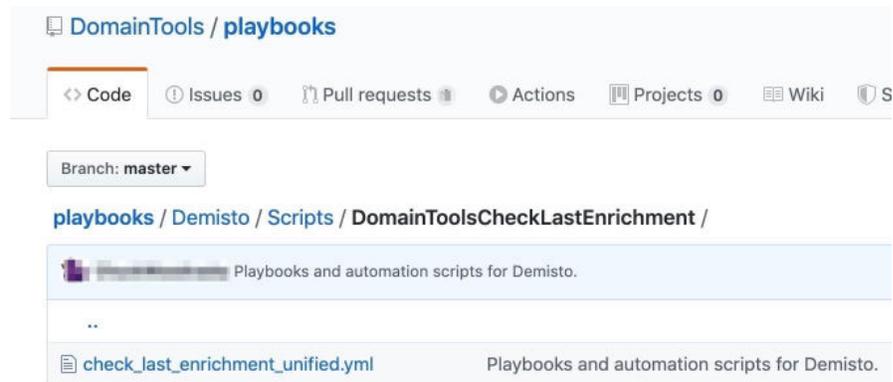


Prerequisites

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



Custom Indicator fields:

The playbook leverages the following custom fields in the Indicator table to store the domain intelligence inside Cortex 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

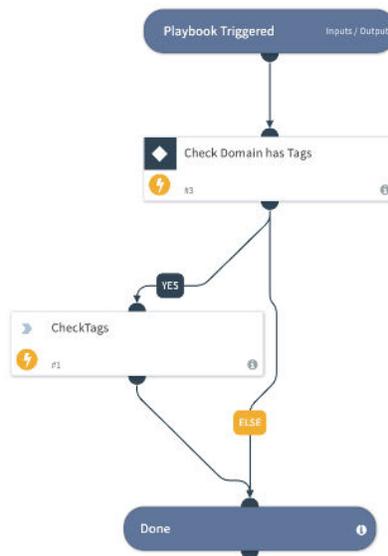
<input type="checkbox"/>	Field Name	Type	Mandatory	System ↓
<input type="checkbox"/>	additionalWhoisEmails	abc Short text	No	No
<input type="checkbox"/>	domainAge	abc Short text	No	No
<input type="checkbox"/>	emailDomains	abc Short text	No	No
<input type="checkbox"/>	ipAddresses	abc Short text	No	No
<input type="checkbox"/>	mailServers	abc Short text	No	No
<input type="checkbox"/>	nameServers	abc Short text	No	No
<input type="checkbox"/>	soaEmail	abc Short text	No	No
<input type="checkbox"/>	spfRecord	abc Short text	No	No
<input type="checkbox"/>	sslCertificate	abc Short text	No	No

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



Prerequisites

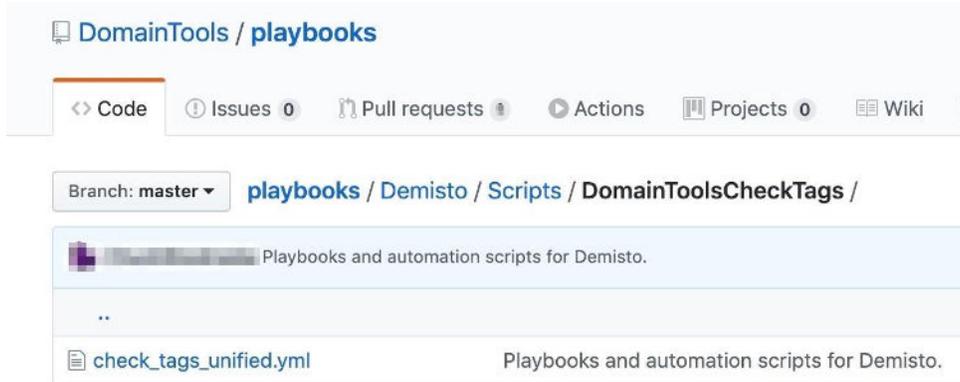
Creating Tags in DomainTools Iris Investigate:

To leverage this feature Cortex XSOAR Users must be using the Tagging capabilities from DomainTools Iris Investigate platform. Once a Domain is 'Tagged' in Iris, the tags become available for consumption within Cortex XSOAR. Please refer to 'Tagging Domains' in [DomainTools Iris Investigate 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



Custom 'Tag' List:

Cortex XSOAR users can store the list of tags inside Cortex 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