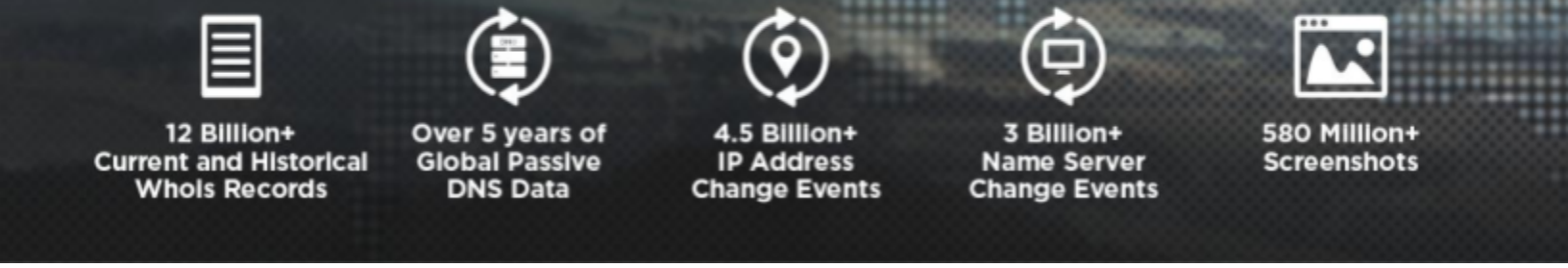
DOMAINTOOLS

DomainTools Resilient App User Guide

v1.1
Sep 2019



Overview

DomainTools Resilient App enables users to automate Incident Response processes by bringing in DomainTools intelligence data and analytics within the Resilient platform.

Our users can automate their Incident playbooks entirely or perform ad-hoc actions on domain-based Artifacts to gain in-line contextual intelligence.

The App leverages the Iris Investigate API to automate data enrichment inside of IBM Resilient.

Key Benefits

1. Automate incident handling to triage an incident by leveraging Resilient Rules and workflows to identify dangerous domain artifacts
2. Gain context by enriching domain artifacts on-demand with DomainTools Intelligence
3. Avoid context switching and preserve DomainTools enrichment data in a DataTable within an Incident
4. Automate incident handling by leveraging DomainTools Risk Score Analytics
5. Leverage DomainTools Iris Tags to identify malicious domain artifacts
6. Discover unknown infrastructures by automating connected infrastructure discovery using DomainTools Pivot Analytics

Deployment Guide

Pre-Requisites

- An active DomainTools Iris API key
- IBM Resilient >= v33.0.5112
- Python 2.7
- An Integrations Server running resilient-circuits >= v31.0.0
- The DomainTools Resilient App installed from App Exchange

Install Steps

1. Copy the fn_domaintools-1.*.*.zip to the Integrations server and SSH into it

2. Unzip the package

```
$ unzip fn_domaintools-1.x.x.zip
```

3. Install the package

```
$ pip install fn_domaintools-1.x.x.tar.gz
```

4. Export to server

```
$ resilient-circuits customize
```

5. Import the configurations into your app.config file:

```
$ resilient-circuits config -u
```

6. Open the config file, scroll to the bottom and add your DomainTools API keys

```
$ nano ~/.resilient/app.config
```

Config	Required	Description
dt_api_user_name	Yes	The DomainTools API username
dt_api_key	Yes	The DomainTools API Key

7. Save and Close the app.config file

8. Run resilient-circuits

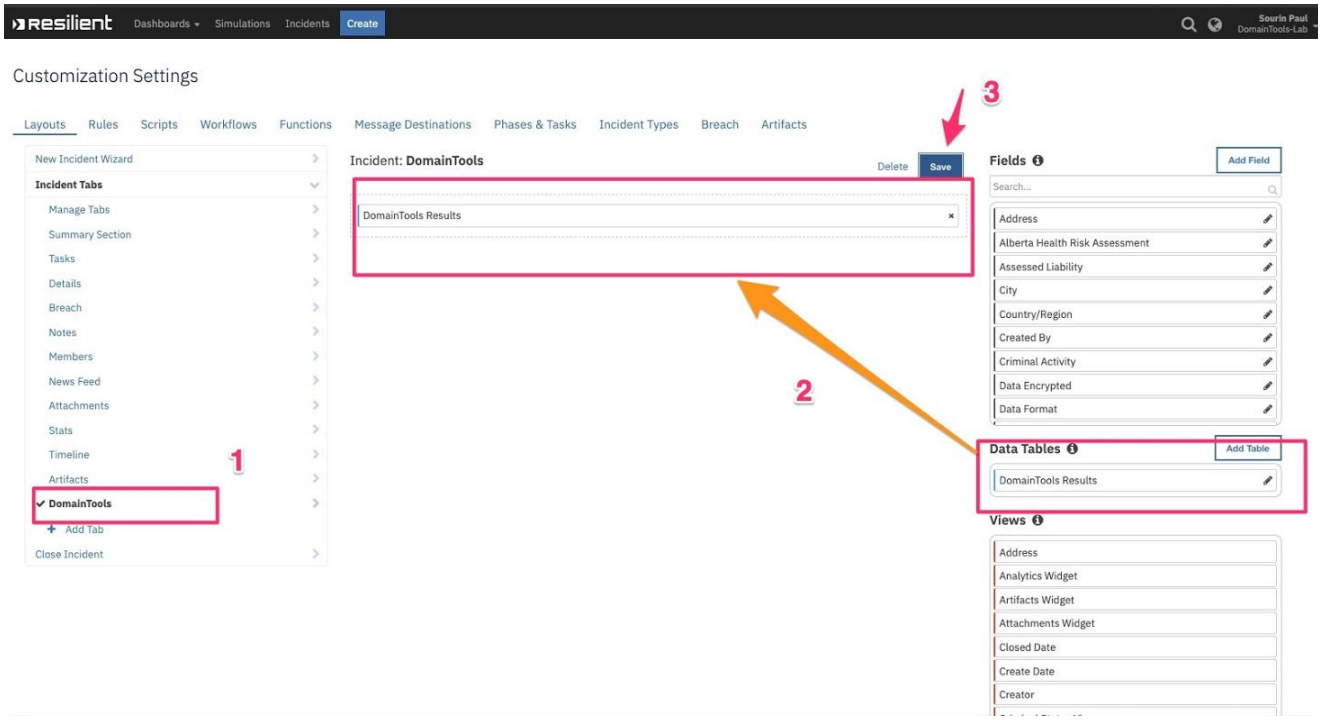
```
$ resilient-circuits run
```

9. Login to the Resilient Appliance. Go to Customization Settings > Layouts > Incident Tabs

   In order to persist/ view the enrichment data from DomainTools you can store the enrichment result inside a Resilient DataTable.

   1. Create a new Incident Tab named '**DomainTools**'.
   2. Then drag DomainTools Result from under *Data Tables column* to the middle of the page.
   3. Hit the Save button.

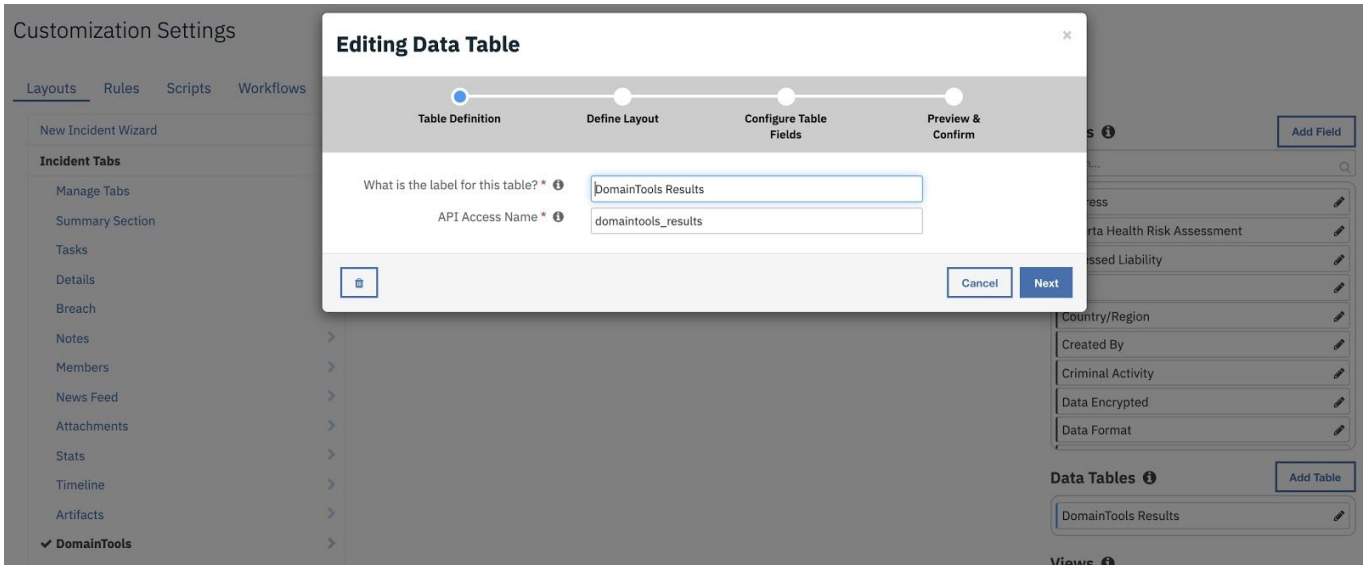
See screenshot below:



10. Verify Setup

The DomainTools App contains 5 Functions, 4 Workflows, 4 Rules and 1 Data Table that automates the functionalities within IBM Resilient. Login to the Resilient Appliance and verify the following setup exists in your Resilient instance:

DataTable

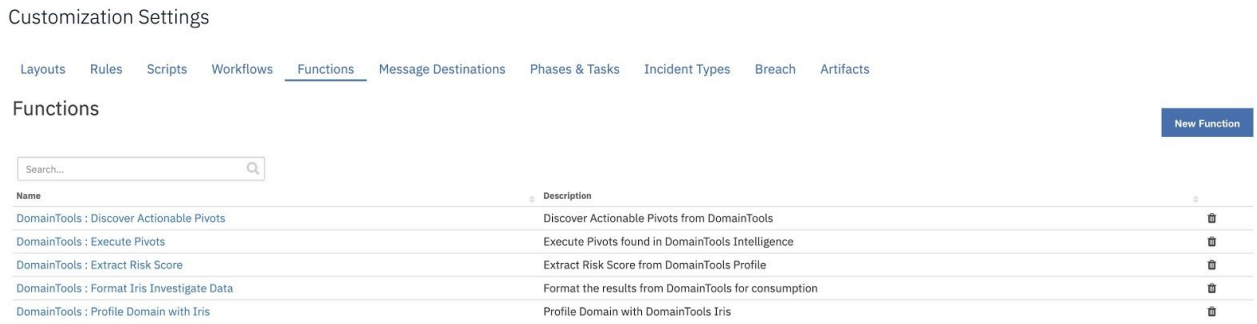


Artifacts

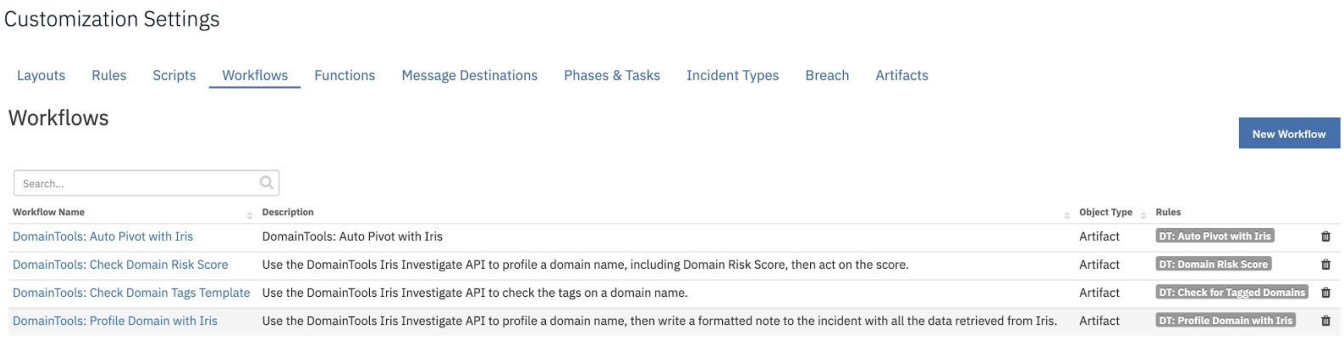
Ensure that DNS Name artifact exists in your environment. If not, create one.

DomainTools Message Queue

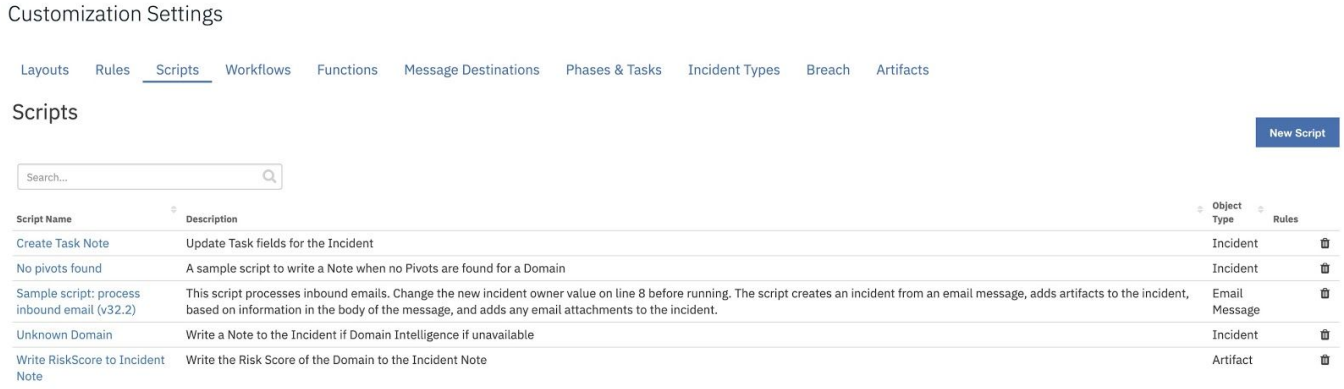
Functions



Workflows



Scripts

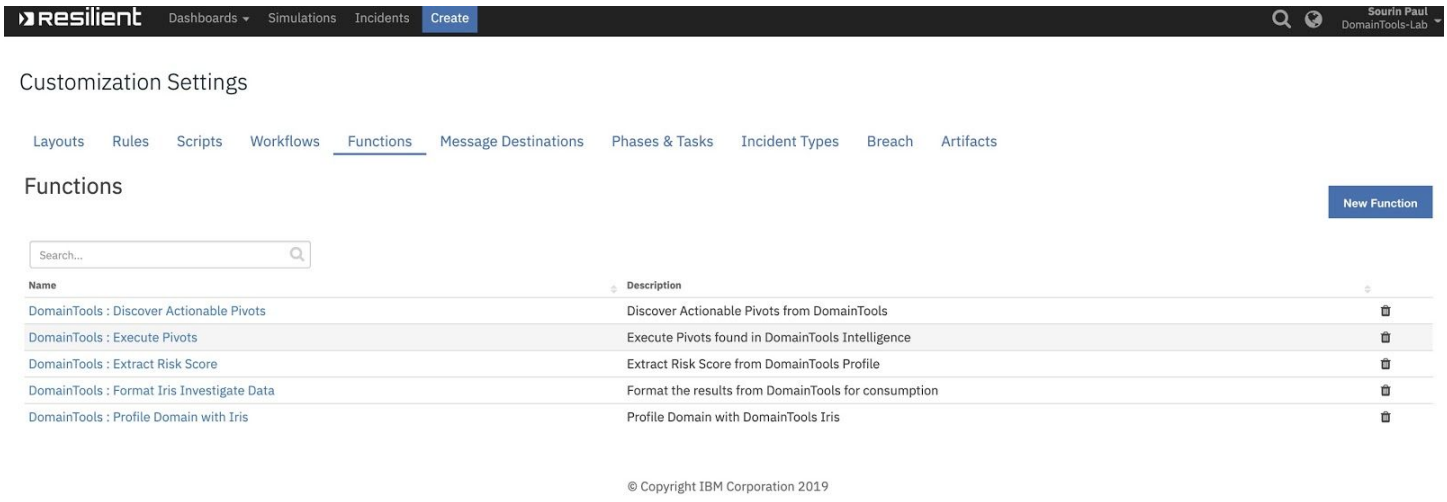


Customizing DomainTools App

App Config Settings:

```
[fn_domaintools]
dt_api_user_name=<API Username>
dt_api_key=<API Key>
```

Functions:



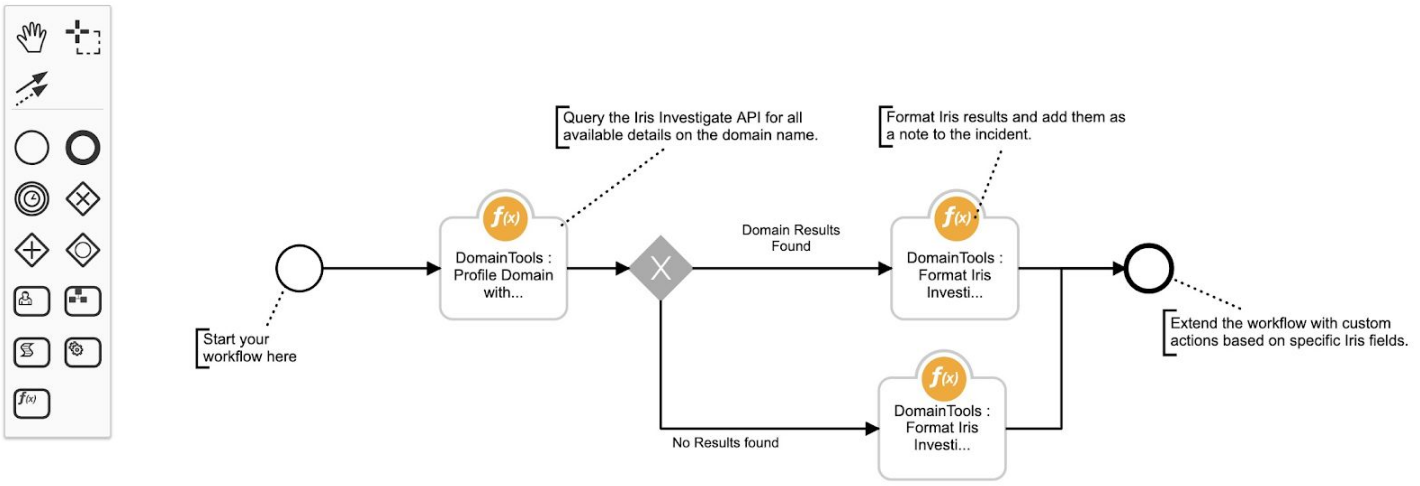
DomainTools : Profile Domain with Iris

Description:

This Function uses Iris Investigate API with domain as a parameter to retrieve all domain intelligence data inside Resilient.

Referenced Workflow:

Example of the function being invoked from a workflow



Inputs:

Input Name	Type	Required	Description
dt_domain_name	String	Yes	Domain Artifact of Type 'DNS Name'

Outputs:

Output Name	Type	Required	Description
dt_iris_data	JSON String	No	JSON String of DomainTools Iris Resultset

Pre-process Script:

```
inputs.dt_domain_name = artifact.value
```

Post-process Script:

```
incident.addNote('Performed DomainTools Iris profile of
{0}'.format(results['domain']))
```

```
incident.properties.domaintoolsdata = True
```

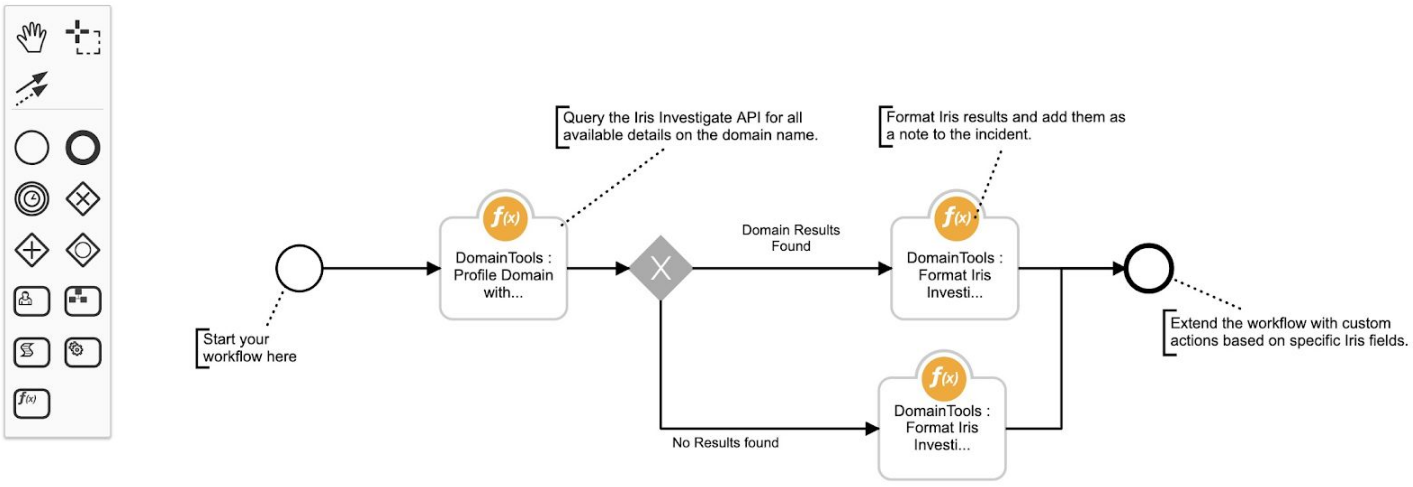
DomainTools : Format Iris Investigate Data

Description:

Format the results from Iris Investigate API query for downstream consumption and processing. It also includes the steps to write the data into DomainTools DataTable inside Resilient using post-processing scripts.

Referenced Workflow:

Example of the function being invoked from a workflow



Inputs:

Input Name	Type	Required	Description
incident_id	Number	Yes	Resilient Incident ID
dt_format_options	LOV	Yes	LOV includes - Analytics, Identity, Registration, Hosting
dt_format_type	LOV	Yes	Default to 'JSON'
dt_iris_data_in	JSON String	Yes	JSON string containing Iris

			resultset

Pre-processing Script:

```
inputs.incident_id = incident.id
inputs.dt_iris_data_in = workflow.properties.dt_iris_data['dt_iris_data']
```

Post-processing Script:

```
dt_row = incident.addRow("domaintools_results")
dt_row['domain_name'] = results["Domain Name"]

dt_row['retrieval_date'] = results["Retrieval Date"]
dt_row['age'] = results["Age"]
dt_row['overall_risk_score'] = results["Overall Risk Score"]
dt_row['proximity_risk_score'] = results["Proximity Risk Score"]
dt_row['threat_profile_risk_score'] = results["Threat Profile Risk Score"]

dt_row['website_response_code'] = results["Website Response Code"]

dt_row['ip_country_code'] = results["IP Country Code"]
dt_row['alexa'] = results["Alexa"]

dt_row['registrant_name'] = results["Registrant Name"]
dt_row['registrant_org'] = results["Registrant Org"]
dt_row['registrant_contact'] = results["Registrant Contact"]
dt_row['soa_email'] = results["SOA Email"]
dt_row['ssl_certificate_email'] = results["SSL Certificate Email"]
dt_row['admin_contact'] = results["Admin Contact"]
dt_row['technical_contact'] = results["Technical Contact"]
dt_row['billing_contact'] = results["Billing Contact"]
dt_row['email_domains'] = results["Email Domains"]
dt_row['additional_whois_emails'] = results["Additional Whois Emails"]

dt_row['domain_registrar'] = results["Domain Registrar"]
dt_row['registrar_status'] = results["Registrar Status"]
dt_row['domain_status'] = results["Domain Status"]
dt_row['created_date'] = results["Create Date"]
dt_row['expiration_date'] = results["Expiration Date"]

dt_row['ip_addresses'] = results["IP Addresses"]
dt_row['mail_servers'] = results["Mail Servers"]
dt_row['spf_record'] = results["SPF Record"]
```

```
dt_row['name_servers'] = results["Name Servers"]
dt_row['ssl_certificate'] = results["SSL Certificate"]
dt_row['redirects_to'] = results["Redirects To"]
dt_row['google_adsense_tracking_code'] = results["Google Adsense Tracking Code"]
dt_row['google_analytics_tracking_code'] = results["Google Analytics Tracking Code"]

incident.addNote('Added {0} to DomainTools Table'.format(results["Domain Name"]))
```

If no domain intelligence is available for a domain artifact, the following alternative script is executed:

```
incident.addNote('Domain Not Found')
```

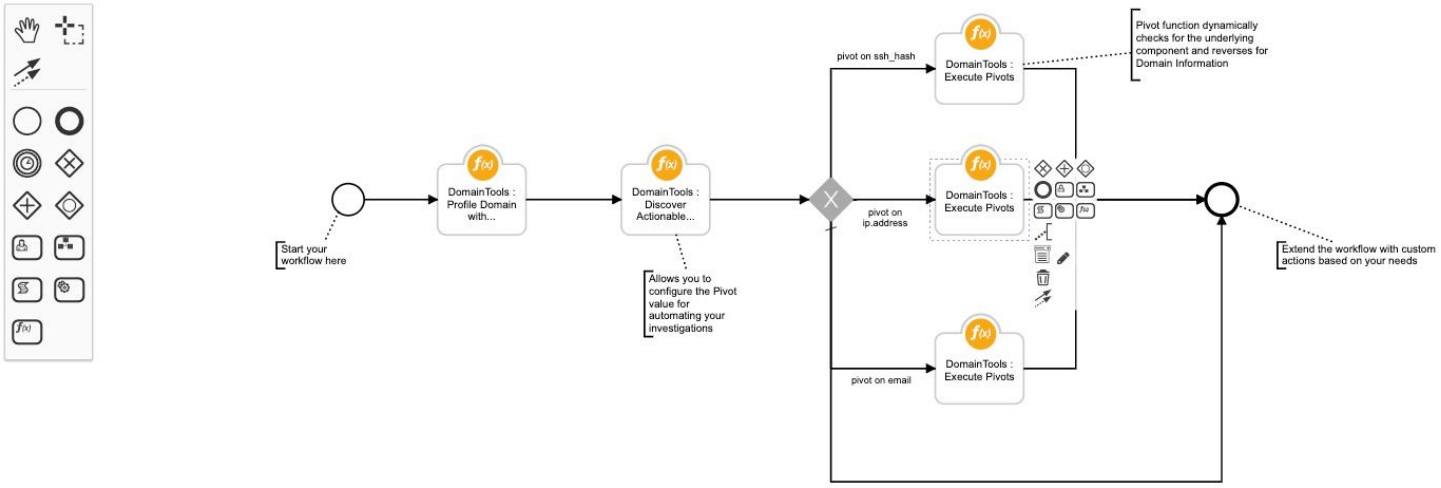
DomainTools : Discover Actionable Pivots

Description:

The function helps discover all available Pivot (Discovery points) for a specific Domain Artifact based on a configurable Guided Pivot value

Referenced Workflow:

Example of the function being invoked from a workflow



Inputs:

Input Name	Type	Required	Description
dt_iris_data_in	JSON String	No	JSON String of DomainTools Iris Resultset
dt_pivot_count	Number	Yes	Default set to '300' Defines the threshold value for DomainTools Guided Pivot, an analytics that helps discover connected infrastructure

Outputs:

Output Name	Type	Required	Description
dt_pivot_data	Number	Yes	List of all available Pivots for that Domain

Pre-processing Script:

```
inputs.dt_iris_data_in = workflow.properties.dt_iris_data['dt_iris_data']
```

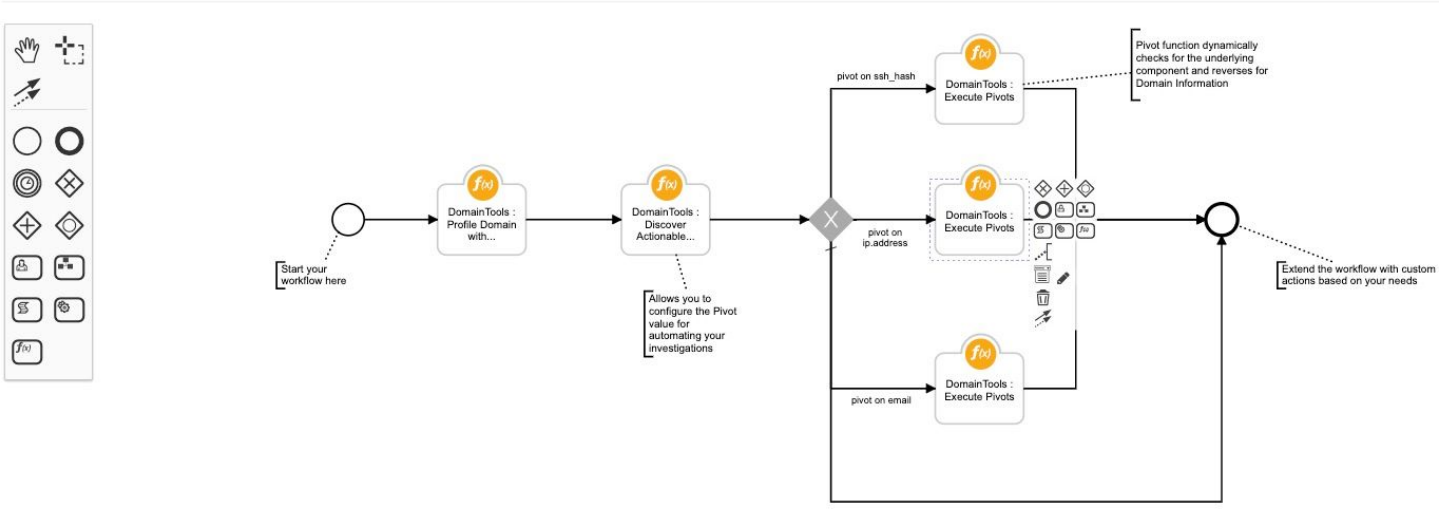
DomainTools : Execute Pivots

Description:

The Execute Pivots function, takes the pivot_data resultset from 'Discover Actional Pivots' function as an input and then performs a reverse look up to identify any associated Domains. This enables user to discover connected infrastructures associated with the domains.

Referenced Workflow:

Example of the function being invoked from a workflow



Inputs:

Input Name	Type	Required	Description
dt_pivot_value	String	Yes	The specific JSON attribute containing the domain attribute field
dt_pivot_type	LOV	Yes	List of values can be one of the following: ip, email, email_domain, nameserver_hsot, nameserver_domain,

			nameserver_ip, registrar, registrant, registrant_orf, mailserver_hsot, mailserver_domain, mailserver_ip, redirect_domain, ssl_dhash, ssl_subject, ssl_email, ssl_org, google_analytics, adsense
dt_data_updated_after	Date	No	Date Updated After parameter to further filter the lookup
dt_created_date	Date	No	Created Date parameter to further filter the lookup

Post-processing Script:

```
incident.addNote('New Domains discovered from SSL Hash - Iris Pivot Function')
for k, domain in enumerate(results['pivots']):
        incident.addNote('DNS Name, {0}, pivot from Iris'.format(domain))
```

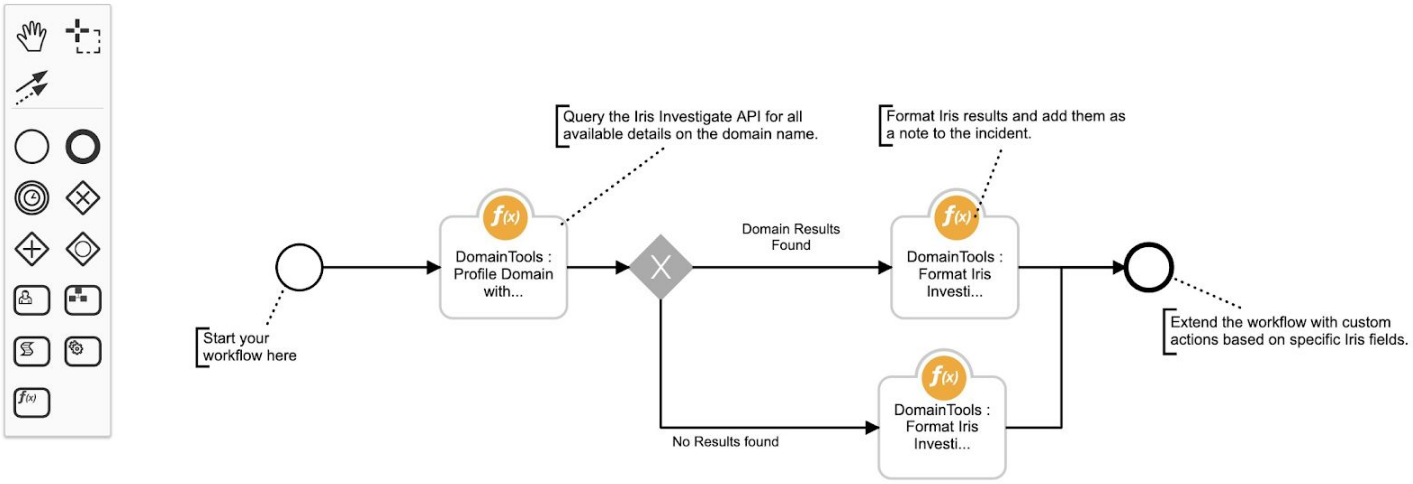
In the above templated workflow, we pivot on ssl_hash, ip_address and email fields to demonstrate an example. You can further extend the workflow to pivot on any of the 19 attributes listed under dt_pivot_type below.

DomainTools App Functionalities

The DomainTools App delivers these functionalities via a set of pre-packaged Resilient Functions and Workflows. Detailed below are steps to execute the workflows in your instance, once the app is configured. Users can and should further customize these workflows to meet their organization's incident response processes.

Domain Enrichment for Artifacts

This workflow allows the ability for Resilient users to perform ad-hoc enrichment of Domain Artifacts in an Incident with core DomainTools Iris data. The integration brings in Iris data for a domain, including Whois, DomainTools Analytics like Risk Score, Threat Profiles, and artifacts associated with the domain like SSL, ASN info, etc.



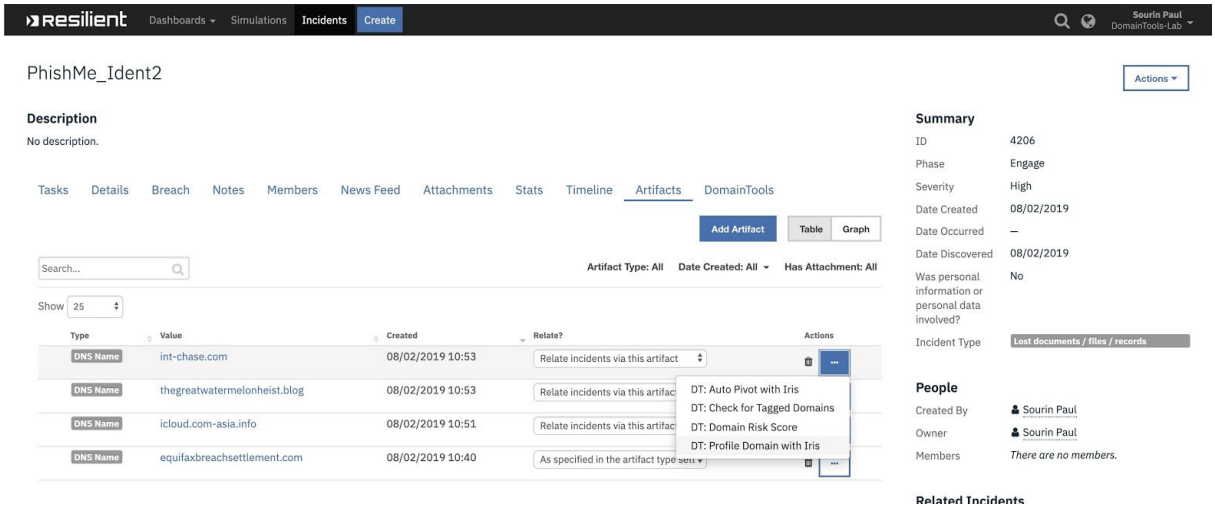
Workflow Name: DomainTools: Profile Domain with Iris

Steps to invoke the workflow:

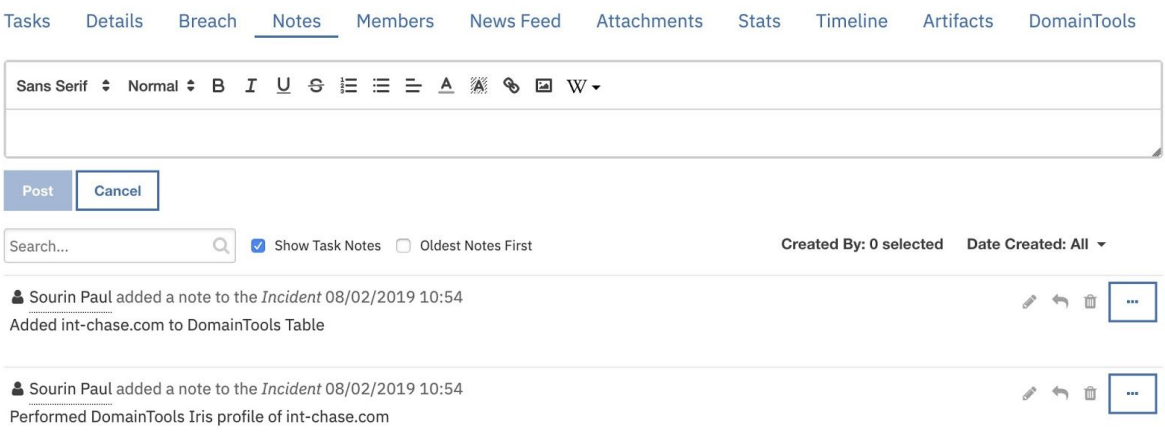
1. From IBM Resilient interface, select an incident to investigate
2. Select the **Artifacts** Tab to view the artifacts associated with the incident
3. If an Artifact of Type **DNS Name** does NOT exist, one can add a new Artifact to the incident

> *Refer to IBM Resilient Documentation for details about how to use the Incident Interface.*

4. Click the Hamburger menu for the Artifact and select the workflow ''**DT: Profile Domain with Iris**"



5. Check the Notes section to see the results of the enrichment



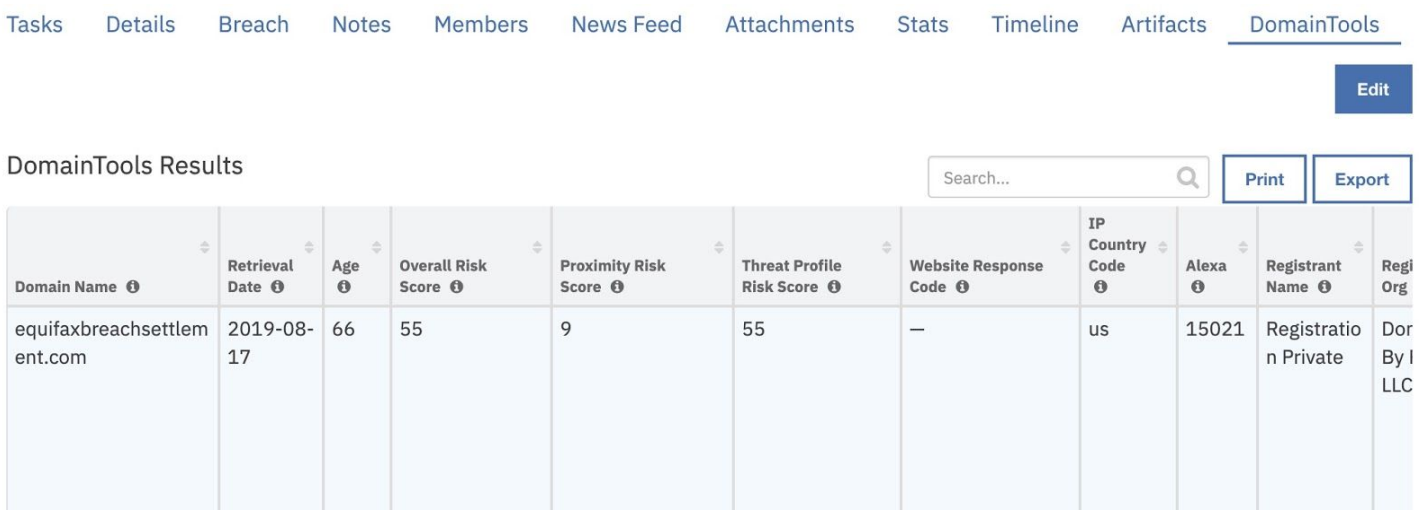
Persist Enrichment data in DataTable

This functionality provides an ability to persist the enrichment data in Data Tables inside an Incident. Users can review the enrichment data over the life of the incident and co-relate multiple domain Artifacts that share common straits.

The DomainTools table also provides a way to review the complete DomainTools intelligence conveniently across all Artifacts for that incident.

Steps to access DomainTools tab

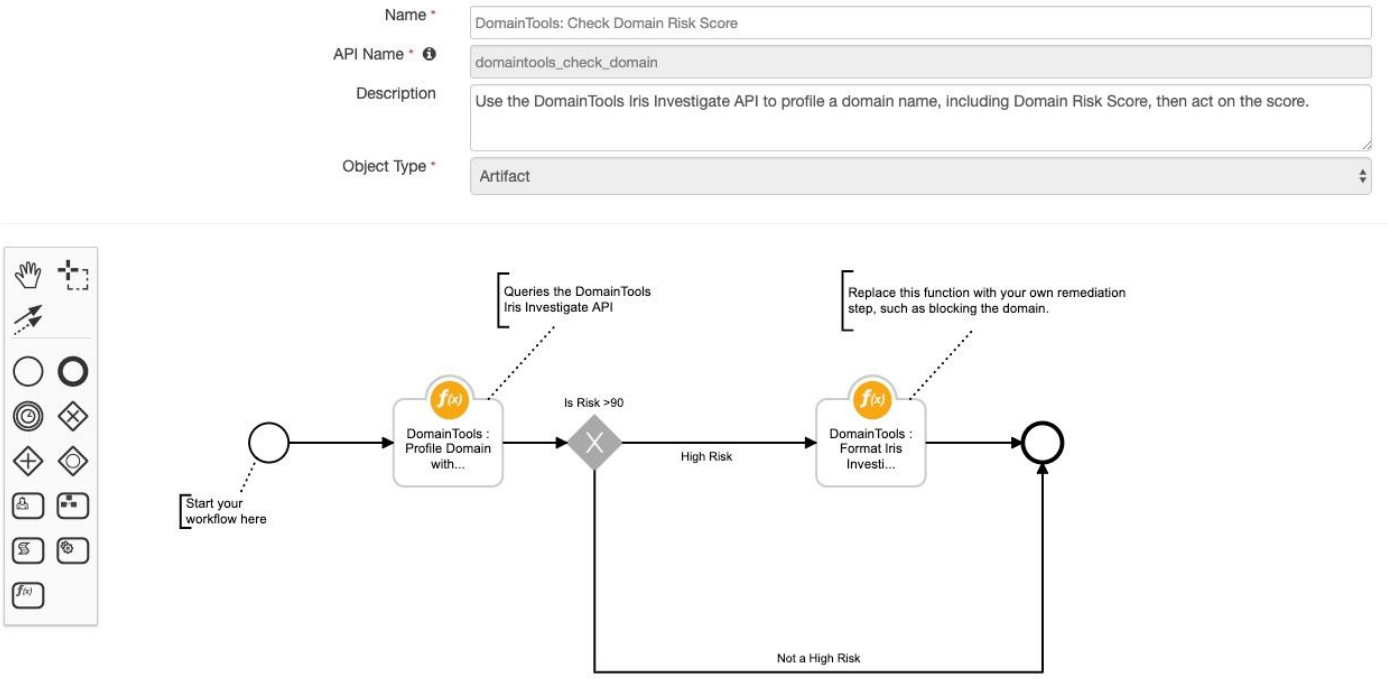
1. Follow the steps detailed above to enrich a particular Artifact using '**DT: Profile Domain with Iris'**
2. Select the DomainTools tab, to view the Domain intelligence for an Artifact



Workflow to Identify High-Risk Domains

A pre-built workflow that pivots on DomainTools Risk Score to evaluate if a particular domain is Risky or Not. The workflow template also provides a way to configure the Risk Threshold (90 by default), which can be further customized based on your organization's processes.

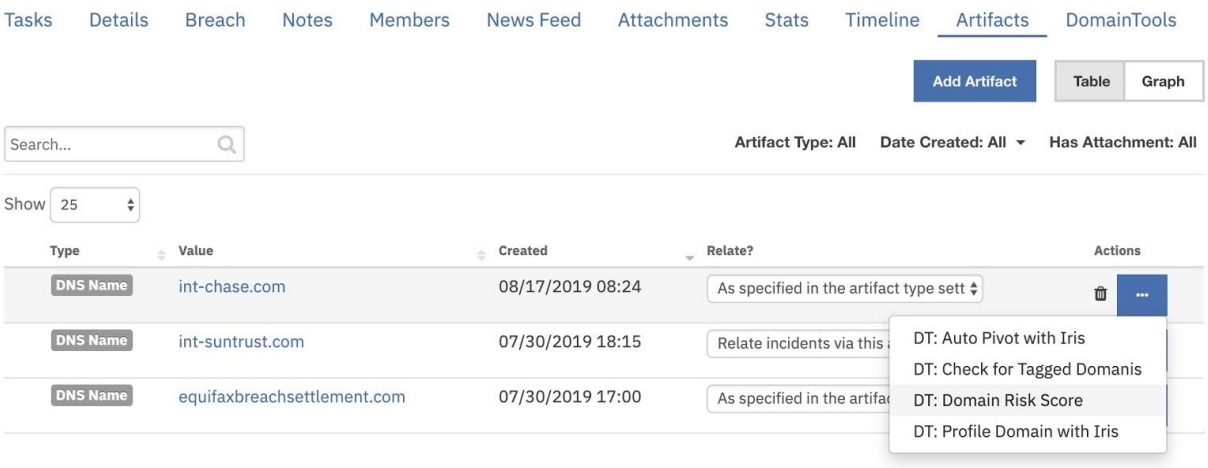
If an Artifact is deemed Risky, the workflow will append a Note to the Incident record noting the Risk Score and Domain Artifact.



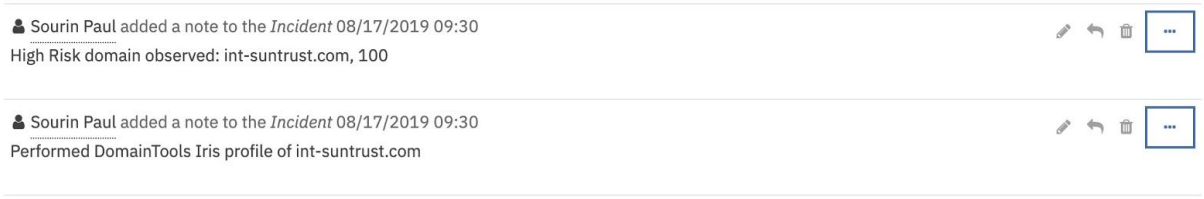
Workflow Name: DomainTools: Check Domain Risk Score

Steps to invoke the workflow:

1. Follow the steps detailed above to locate an Artifact of type DNS Name
2. Click the Hamburger menu for the Artifact and select the workflow ''**DT: Domain Risk Score**"



3. Check the Notes section to see the results of the enrichment

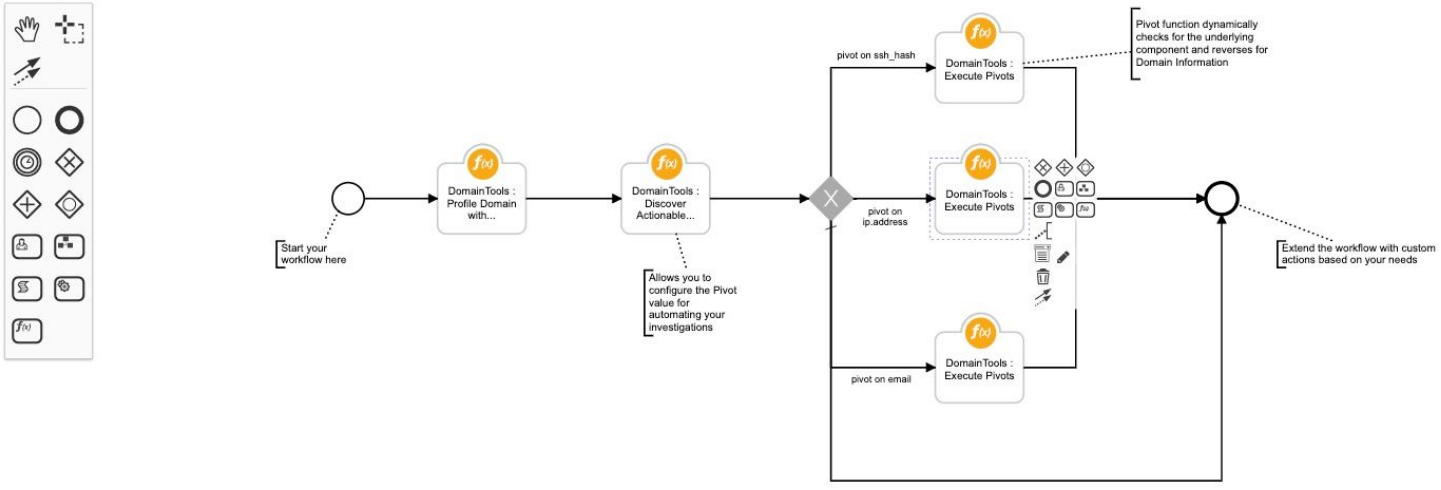


Workflow to Discover Malicious Infrastructure

This workflow shows how DomainTools Guided Pivots can be leveraged within an Investigation. The workflow template also allows users to configure a threshold for the connected pivots (default value is set to 300 domains) based on their organization's security posture.

The workflow automates the ability to lookup associated IPs, SSL hashes, and registrant email addresses and if available can reverse on these artifacts to retrieve domains associated with them. If a user wishes to pivot on additional attributes of a domain, he can further extend the workflow to add additional decision steps and conveniently accomplish that.

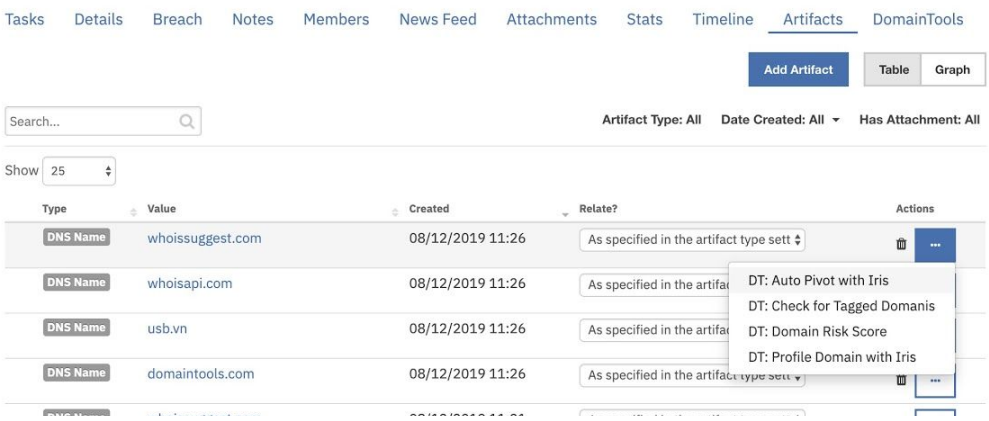
The default action on this workflow adds findings on the Incident Note, but users can conveniently add their custom workflow or downstream systems to extend these further.



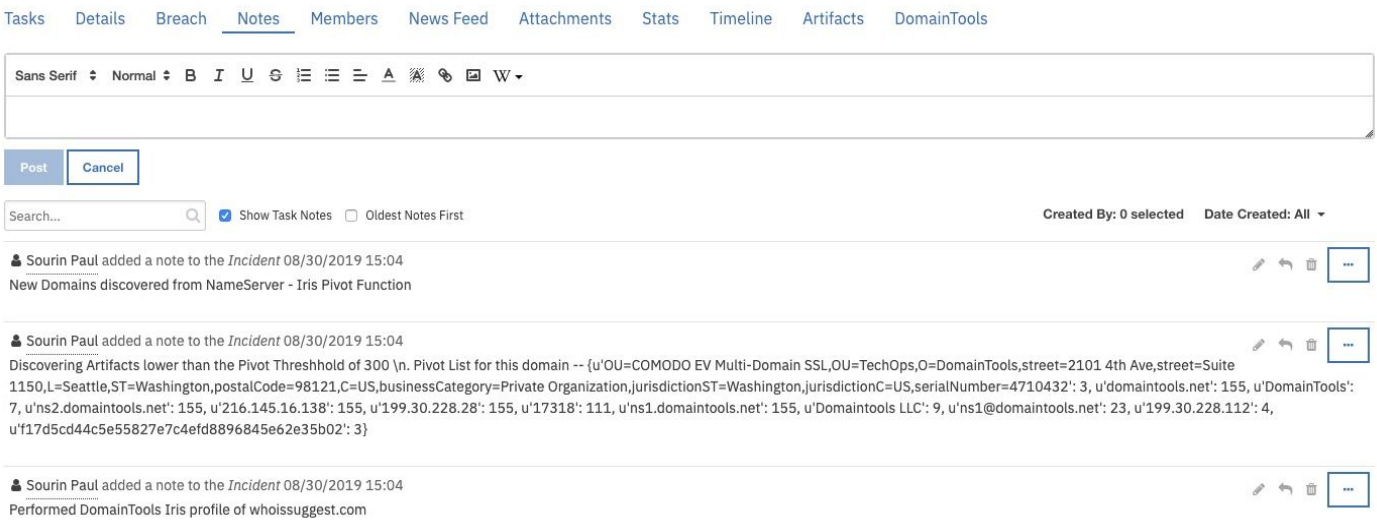
Workflow Name: DomainTools: Auto Pivot with Iris

Steps to invoke the workflow:

1. Follow the steps detailed above to locate an Artifact of type DNS Name
2. Click the Hamburger menu for the Artifact and select the workflow ''**DT: Auto Pivot with Iris**"

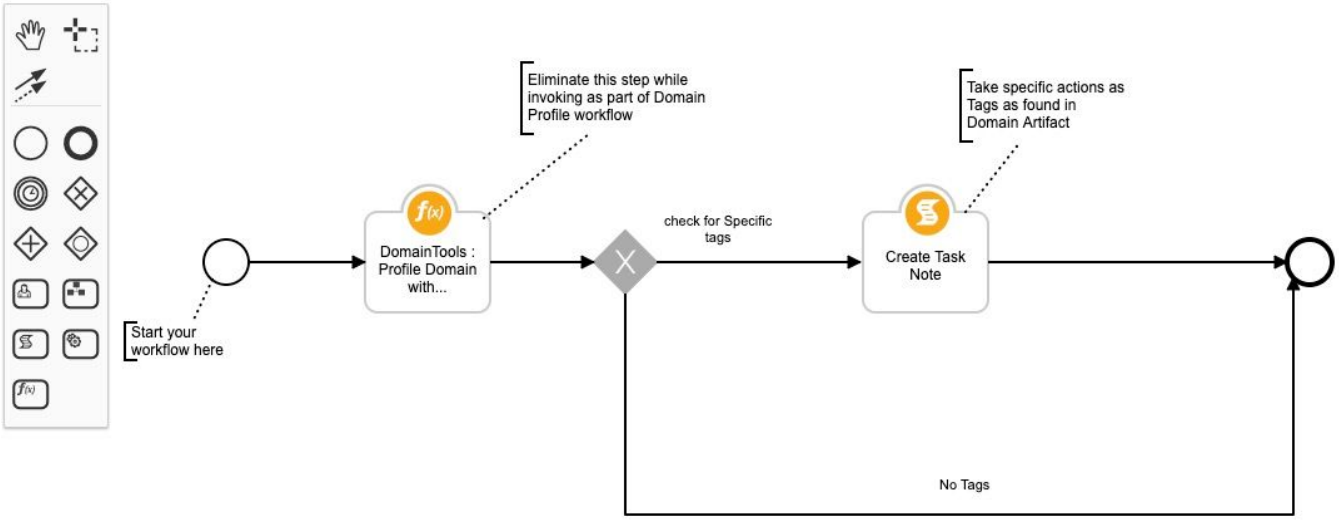


3. Check the Notes section to see the results of the enrichment



Workflow to Pivot on Tagged Domains

This workflow template allows to automatically detect if a domain Artifact has been tagged by the Threat Investigation resource inside of Iris with a specific tag. And based on the Tag value, allows the incident response team to take adaptive response.



Users can further customize this workflow to process a list of tags and take different actions based on different tags. Please refer to the IBM Resilient workflow guide to customize the scripts/ actions according to your needs.

Workflow Name: DomainTools: Check Domain Tags Template

Steps to invoke the workflow:

4. Follow the steps detailed above to locate an Artifact of type DNS Name
5. Click the Hamburger menu for the Artifact and select the workflow ''**DT: Check for Tagged-Domains**"
6. Check the Notes section to see the results of the enrichment