User Guide

DomainTools App for Splunk SOAR

Version 1.5, May 2024

DomainTools

Contents

Getting Started

Connector Version: 1.5.0
Minimum Product Version: 6.1.1

This app supports investigative actions to profile domain names, get risk scores, and find connected domains that share the same Whois details, web hosting profiles, SSL certificates, and more on DomainTools Iris Investigate.

To learn more about DomainTools Iris Investigate, visit www.domaintools.com/products/platform/iris-investigate.

DomainTools Iris Investigate Monitoring Playbook Feature

This feature allows the user to schedule playbooks to run on a specified interval and run it on a specific container/event ID you provided on each row. Coupled with our reference playbooks, linked below, this can be a powerful tool to notify you of domain infrastructure changes, or when newly created domains match specific infrastructure you're monitoring.

See the individual playbooks for more information. This readme covers how to set up Iris Monitoring for those playbooks.

Configuration

This feature depends on the 1 asset configuration fields that are required when using this feature.

Name	Description	Default Value	Required
Splunk SOAR HTTPS port (default: 8443)	Splunk SOAR HTTP port if your instance uses one other than the default, 8443	8443	Yes

To configure this, you need to:

1. Go to Apps
2. Select DomainTools Iris Investigate
3. Select a configured asset or create one if you don't have any.
4. Go to Asset Settings
5. Look for the `Splunk SOAR HTTPS port (default: 8443)` field. By default it contains a value of `8443`.

Prerequisites

This feature uses a custom list named domaintools_scheduled_playbooks.
To generate the custom list, you need to:

1. Go to Apps
2. Select DomainTools Iris Investigate
3. Select a configured asset or create one
4. Go to Actions dropdown
5. Select configure scheduled playbooks action
6. Select Test Action.

Once these steps are complete, return to the custom list page and you will see the domaintools_scheduled_playbooks generated for you.

The values of this list have 6 columns and the header should not be altered. The last 3 columns are intentionally left blank and used by the playbook scheduler.

Sample `domaintools_scheduled_playbooks` table:

Repo / playbook_name	**event_id**	**Interval (mins)**	**last_run (server time)**	**last_run_status**	**Remarks**
local/DomainTools Monitor Domain Risk Score	<your_event_id>	1440			
local/DomainTools Monitor Domain Infrastructure	<your_event_id>	1440			
local/DomainTools Monitor Search Hash	<your_event_id>	1440			

In this example, we've specified to run three separate monitoring playbooks on daily schedules. Note that each scheduled lookup will consume Iris Investigate queries, depending how many domains or Iris search hashes are being monitored.

Monitoring/scheduling in the DomainTools Iris Investigate App

How to use this feature:

1. Under Apps > DomainTools Iris Investigate > Asset Settings > Ingest Settings > Label, specify or select a label to apply to objects from this source. Recommended: Use a custom label rather than using a predefined label such as events.
2. Specify a polling interval to check if playbooks need to be run. Note that this is separate from the playbook run interval specified in step 4. We recommend running every minute for the most accurate scheduling.

3. Under Custom Lists > domaintools_scheduled_playbooks input your desired playbook schedule following the example in the Configuration Section
   Ensure the label of the playbook and event_id you inputted shares the label that you selected in Step 1. The domaintools_scheduled_playbooks custom list should have been created when you updated or installed the DomainTools app, but if you don't see it, you can generate it by following the Prerequisites section of this page.
4. Go to `domaintools_scheduled_playbooks` custom list, Modify the table based on your desired values.Note: The interval column is used to specify the interval in minutes on which the playbook will run

Note: For the DomainTools reference playbooks, see our GitHub repository: https://github.com/DomainTools/playbooks/tree/main/Splunk%20SOAR.

Configuration Variables

The below configuration variables are required for this Connector to operate. These variables are specified when configuring a DomainTools Iris Investigate asset in SOAR.

Variable	Required	Type	Description
username	required	string	User Name
key	required	password	API Key
proxy	optional	boolean	Use Proxy
proxy_auth	optional	boolean	Use Proxy Authentication
proxy_server	optional	string	Proxy Server
proxy_username	optional	string	Proxy Username
proxy_port	optional	numeric	Proxy Port
proxy_password	optional	password	Proxy Password
custom_ssl_certificate	optional	boolean	Use Custom SSL Certificate
ssl	optional	boolean	Use SSL

Variable	Required	Type	Description
custom_ssl_certificate_path	optional	string	Custom SSL Certificate Path
http_port	optional	string	Splunk SOAR HTTPS port (default: 8443)

Supported Actions

The following actions are supported, and are detailed in sections below:

- Test Connectivity - Validate the asset configuration for connectivity.
- Domain Reputation - Evaluates the risk of a given domain.
- Pivot Action - Find domains connected by any supported Iris Investigate search parameter.
- Reverse Domain - Extract IPs from a single domain response for further pivoting.
- Reverse IP - Find domains with web hosting IP, NS IP or MX IP.
- Load Hash - Load or monitor Iris Investigate search results by Iris Investigate export hash.
- Reverse Email - Find domains with email in Whois, DNS SOA or SSL certificate.
- Lookup Domain - Get all Iris Investigate data for a domain using the Iris Investigate API endpoint (required).
- Enrich Domain - Get all Iris Investigate data for a domain except counts using the high volume Iris Enrich API endpoint (if provisioned).
- Configure Scheduled Playbooks - Run on initial setup to configure the optional monitoring playbooks. This action creates a custom list to manage the playbook scheduling and run status.
- On Poll - Execute scheduled playbooks based on the set interval(mins) in 'domaintools_scheduled_playbooks' custom list. Smaller intervals will result in more accurate schedules.

Action: 'Test Connectivity'

Validate the asset configuration for connectivity.

Type: test
Read only: True

Action Parameters

No parameters are required for this action.

Action Output

No Output

Action: 'Domain Reputation'

Evaluates the risk of a given domain.

Type: Investigate
Read only: True

Action Parameters

Parameter	Required	Description	Type	Contains
domain	required	Domain or comma-separated list of domains to query	string	url domain

Action Output

Data Path	Type	Contains	Example Values
action_result.parameter.domain	string	url domain	
action_result.data	string		
action_result.status	string		success failed
action_result.message	string		
action_result.summary.domain_risk	numeric		

Data Path	Type	Contains	Example Values
action_result.summary.zerolisted	boolean		True False
action_result.summary.proximity	numeric		
action_result.summary.threat_profile	numeric		
action_result.summary.threat_profile_malware	numeric		
action_result.summary.threat_profile_phishing	numeric		
action_result.summary.threat_profile_spam	numeric		
summary.total_objects	numeric		1
summary.total_objects_successful	numeric		1

Action: 'Pivot Action'

Find domains connected by any supported Iris Investigate search parameter.

Type: Investigate
Read only: True

Action Parameters

Parameter	Required	Description	Type	Contains
query_value	required	Value to query	string	url domain ip email
pivot_type	required	Field to pivot on	string	
status	optional	Return domains of this registration type	string	
data_updated_after	optional	Iris Investigate records that were updated on or	string	

Parameter	Required	Description	Type	Contains
		after midnight on this date, in YYYY-MM-DD format or relative options ('today', 'yesterday')		
tld	optional	Limit results to only include domains in a specific top-level domain (i.e. “tld=com” or “tld=ru”)	string	
create_date	optional	Only include domains created on a specific date, in YYYY-MM-DD format or relative options ('today', 'yesterday')	string	
create_date_within	optional	Only include domains with a whois create date within the specified number of days (e.g. specifying '1' would indicate within the past day)	string	
first_seen_within	optional	Only include domains with a current lifecycle first observed within the specified number of seconds (e.g. specifying '86400' would indicate within the past day)	string	
first_seen_since	optional	Only include domains with a current lifecycle first observed since a specified datetime. (Example: 2023-04-10T00:00:00+00:00)	string	

Parameter	Required	Description	Type	Contains
expiration_date	optional	Only include domains expiring on a specific date, in YYYY-MM-DD format or relative options ('today', 'yesterday')	string	

Action Output

Data Path	Type	Contains	Example Values
action_result.parameter.create_date	string		
action_result.parameter.create_date_within	string		
action_result.parameter.data_updated_after	string		
action_result.parameter.first_seen_within	string		
action_result.parameter.first_seen_since	string		
action_result.parameter.expiration_date	string		
action_result.data.*.first_seen.count	numeric		
action_result.data.*.first_seen.value	string		
action_result.data.*.server_type.count	numeric		
action_result.data.*.server_type.value	string		
action_result.data.*.website_title.count	numeric		
action_result.data.*.website_title.value	string		

Data Path	Type	Contains	Example Values
action_result.parameter.pivot_type	string		
action_result.parameter.query_value	string	url domain ip email	
action_result.parameter.status	string		
action_result.parameter.tld	string		
action_result.data.*.domain	string	domain	
action_result.data.*.domain_risk.risk_score	numeric		
action_result.data.*.domain_risk.risk_score_string	string		
action_result.status	string		success failed
action_result.message	string		
action_result.summary	string		
summary.total_objects	numeric		1
summary.total_objects_successful	numeric		1

Action: 'Reverse Domain'

Extract IPs from a single domain response for further pivoting.

Type: Investigate
Read only: True

Action Parameters

Parameter	Required	Description	Type	Contains

domain	required	Domain or comma-separated list of domains to query	string	`url` `domain`

Action Output

Data Path	Type	Contains	Example Values
action_result.parameter.domain	string	url domain	
action_result.data	string		
action_result.data.*.first_seen.count	numeric		
action_result.data.*.first_seen.value	string		
action_result.data.*.server_type.count	numeric		
action_result.data.*.server_type.value	string		
action_result.data.*.website_title.count	numeric		
action_result.data.*.website_title.value	string		
action_result.status	string		success failed
action_result.message	string		
action_result.summary.ip_list.*.count	numeric		
action_result.summary.ip_list.*.count_string	string		
action_result.summary.ip_list.*.ip	string	ip	
action_result.summary.ip_list.*.type	string		
summary.total_objects	numeric		1
summary.total_objects_successful	numeric		1

Action: 'Reverse IP'

Find domains with web hosting IP, NS IP or MX IP.

Type: Investigate
Read only: True

Action Parameters

Parameter	Required	Description	Type	Contains
ip	required	IP address to query	string	ip
status	optional	Return domains of this registration type	string	
data_updated_after	optional	Iris Investigate records that were updated on or after midnight on this date, in YYYY-MM-DD format or relative options ('today', 'yesterday')	string	
tld	optional	Limit results to only include domains in a specific top-level domain (i.e. “tld=com” or “tld=ru”)	string	
create_date	optional	Only include domains created on a specific date, in YYYY-MM-DD format or relative options ('today', 'yesterday')	string	
create_date_within	optional	Only include domains with a whois create date within the specified number of days (e.g. specifying '1'	string	

Parameter	Required	Description	Type	Contains
		would indicate within the past day)		
first_seen_within	optional	Only include domains with a current lifecycle first observed within the specified number of seconds (e.g. specifying '86400' would indicate within the past day)	string	
first_seen_since	optional	Only include domains with a current lifecycle first observed since a specified datetime. (Example: 2023-04-10T00:00:00 +00:00)	string	
expiration_date	optional	Only include domains expiring on a specific date, in YYYY-MM-DD format or relative options ('today', 'yesterday')	string	

Action Output

Data Path	Type	Contains	Example Values
action_result.parameter.create_date	string		
action_result.parameter.create_date_within	string		
action_result.parameter.data_updated_after	string		
action_result.parameter.expiration_date	string		
action_result.parameter.first_seen_within	string		
action_result.parameter.first_seen_since	string		

Data Path	Type	Contains	Example Values
action_result.parameter.ip	string	ip	
action_result.parameter.status	string		
action_result.parameter.tld	string		
action_result.data.*.domain	string	domain	
action_result.data.*.domain_risk.risk_score	numeric		
action_result.data.*.domain_risk.risk_score_string	string		
action_result.status	string		success failed
action_result.message	string		
action_result.summary	string		
summary.total_objects	numeric		1
summary.total_objects_successful	numeric		1

Action: 'Load Hash'

Load or monitor Iris Investigate search results by Iris Investigate export hash.

Type: Investigate
Read only: True

Action Parameters

Parameter	Required	Description	Type	Contains

search_hash	required	Paste the "Current Search Export" string (Advanced -> Import/Export Search) from Iris Investigate in this field to import up to 5000 domains	string	

Action Output

Data Path	Type	Contains	Example Values
action_result.parameter.search_hash	string		
action_result.data.*.domain	string	domain	
action_result.data.*.domain_risk.risk_score	numeric		
action_result.data.*.domain_risk.risk_score_string	string		
action_result.status	string		success failed
action_result.message	string		
action_result.summary	string		
summary.total_objects	numeric		1
summary.total_objects_successful	numeric		1

Action: 'Reverse Email'

Find domains with email in Whois, DNS SOA or SSL certificate

Type: Investigate
Read only: True

Action Parameters

Parameter	Required	Description	Type	Contains
email	required	Email query	string	email
status	optional	Return domains of this registration type	string	
data_updated_after	optional	Iris Investigate records that were updated on or after midnight on this date, in YYYY-MM-DD format or relative options ('today', 'yesterday')	string	
tld	optional	Limit results to only include domains in a specific top-level domain (i.e. “tld=com” or “tld=ru”)	string	
create_date	optional	Only include domains created on a specific date, in YYYY-MM-DD format or relative options ('today', 'yesterday')	string	
create_date_within	optional	Only include domains with a whois create date within the specified number of days (e.g. specifying '1' would indicate within the past day)	string	
first_seen_within	optional	Only include domains with a current lifecycle first observed within the specified number of seconds (e.g. specifying '86400' would indicate within the past day)	string	

Parameter	Required	Description	Type	Contains
first_seen_since	optional	Only include domains with a current lifecycle first observed since a specified datetime. (Example: 2023-04-10T00:00:00+00:00)	string	
expiration_date	optional	Only include domains expiring on a specific date, in YYYY-MM-DD format or relative options ('today', 'yesterday')	string	

Action Output

Data Path	Type	Contains	Example Values
action_result.parameter.create_date	string		
action_result.parameter.create_date_within	string		
action_result.parameter.data_updated_after	string		
action_result.parameter.email	string	email	
action_result.parameter.expiration_date	string		
action_result.parameter.first_seen_within	string		
action_result.parameter.first_seen_since	string		
action_result.parameter.status	string		
action_result.parameter.tld	string		
action_result.data.*.domain	string	domain	
action_result.data.*.domain_risk.risk_score	numeric		

Data Path	Type	Contains	Example Values
action_result.data.*.domain_risk.risk_score_string	string		
action_result.data.*.first_seen.count	numeric		
action_result.data.*.first_seen.value	string		
action_result.data.*.server_type.count	numeric		
action_result.data.*.server_type.value	string		
action_result.data.*.website_title.count	numeric		
action_result.data.*.website_title.value	string		
action_result.status	string		success failed
action_result.message	string		
action_result.summary	string		
summary.total_objects	numeric		1
summary.total_objects_successful	numeric		1

Action: 'Lookup Domain'

Get all Iris Investigate data for a domain using the Iris Investigate API endpoint (required).

Type: Investigate
Read only: True

Action Parameters

Parameter	Required	Description	Type	Contains
domain	required	Domain or comma-separated list of	string	url domain

Parameter	Required	Description	Typ e	Contains
		domains to query using the Iris Investigate API		

Action Output

Data Path	Type	Contains	Example Values
action_result.status	string		failed success
action_result.parameter.domain	string	url domain	
action_result.data.*.additional_whois_email.*.count	numeric		
action_result.data.*.additional_whois_email.*.value	string		
action_result.data.*.admin_contact.city.count	numeric		
action_result.data.*.admin_contact.city.value	string		
action_result.data.*.admin_contact.country.count	numeric		
action_result.data.*.admin_contact.country.value	string		
action_result.data.*.admin_contact.fax.count	numeric		
action_result.data.*.admin_contact.fax.value	string		
action_result.data.*.admin_contact.name.count	numeric		
action_result.data.*.admin_contact.name.value	string		
action_result.data.*.admin_contact.org.count	numeric		
action_result.data.*.admin_contact.org.value	string		
action_result.data.*.admin_contact.phone.count	numeric		
action_result.data.*.admin_contact.phone.value	string		
action_result.data.*.admin_contact.postal.count	numeric		

Data Path	Type	Contains	Example Values
action_result.data.*.admin_contact.postal.value	string		
action_result.data.*.admin_contact.state.count	numeric		
action_result.data.*.admin_contact.state.value	string		
action_result.data.*.admin_contact.street.count	numeric		
action_result.data.*.admin_contact.street.value	string		
action_result.data.*.adsense.count	numeric		
action_result.data.*.adsense.value	string		
action_result.data.*.alexa	numeric		
action_result.data.*.billing_contact.city.count	numeric		
action_result.data.*.billing_contact.city.value	string		
action_result.data.*.billing_contact.country.count	numeric		
action_result.data.*.billing_contact.country.value	string		
action_result.data.*.billing_contact.fax.count	numeric		
action_result.data.*.billing_contact.fax.value	string		
action_result.data.*.billing_contact.name.count	numeric		
action_result.data.*.billing_contact.name.value	string		
action_result.data.*.billing_contact.org.count	numeric		
action_result.data.*.billing_contact.org.value	string		
action_result.data.*.billing_contact.phone.count	numeric		
action_result.data.*.billing_contact.phone.value	string		
action_result.data.*.billing_contact.postal.count	numeric		
action_result.data.*.billing_contact.postal.value	string		
action_result.data.*.billing_contact.state.count	numeric		

Data Path	Type	Contains	Example Values
action_result.data.*.billing_contact.state.value	string		
action_result.data.*.billing_contact.street.count	numeric		
action_result.data.*.billing_contact.street.value	string		
action_result.data.*.create_date.count	numeric		
action_result.data.*.create_date.value	string		
action_result.data.*.domain_risk.risk_score	numeric		
action_result.data.*.email_domain.*.count	numeric		
action_result.data.*.email_domain.*.value	string		
action_result.data.*.expiration_date.count	numeric		
action_result.data.*.expiration_date.value	string		
action_result.data.*.first_seen.count	numeric		
action_result.data.*.first_seen.value	string		
action_result.data.*.google_analytics.count	numeric		
action_result.data.*.google_analytics.value	string		
action_result.data.*.ip.*.address.count	numeric		
action_result.data.*.ip.*.address.value	string		
action_result.data.*.ip.*.asn.*.count	numeric		
action_result.data.*.ip.*.asn.*.value	string		
action_result.data.*.ip.*.country_code.count	numeric		
action_result.data.*.ip.*.country_code.value	string		
action_result.data.*.ip.*.isp.count	numeric		
action_result.data.*.ip.*.isp.value	string		
action_result.data.*.mx.*.domain.count	numeric		

Data Path	Type	Contains	Example Values
action_result.data.*.mx.*.domain.value	string		
action_result.data.*.mx.*.host.count	numeric		
action_result.data.*.mx.*.host.value	string		
action_result.data.*.mx.*.ip.*.count	numeric		
action_result.data.*.mx.*.ip.*.value	string		
action_result.data.*.name_server.*.domain.count	numeric		
action_result.data.*.name_server.*.domain.value	string		
action_result.data.*.name_server.*.host.count	numeric		
action_result.data.*.name_server.*.host.value	string		
action_result.data.*.name_server.*.ip.*.count	numeric		
action_result.data.*.name_server.*.ip.*.value	string		
action_result.data.*.redirect.count	numeric		
action_result.data.*.redirect.value	string		
action_result.data.*.redirect_domain.count	numeric		
action_result.data.*.redirect_domain.value	string		
action_result.data.*.registrant_contact.city.count	numeric		
action_result.data.*.registrant_contact.city.value	string		
action_result.data.*.registrant_contact.country.count	numeric		
action_result.data.*.registrant_contact.country.value	string		
action_result.data.*.registrant_contact.email.*.value	string		
action_result.data.*.registrant_contact.email.*.count	numeric		
action_result.data.*.registrant_contact.fax.count	numeric		
action_result.data.*.registrant_contact.fax.value	string		

Data Path	Type	Contains	Example Values
action_result.data.*.registrant_contact.name.count	numeric		
action_result.data.*.registrant_contact.name.value	string		
action_result.data.*.registrant_contact.org.count	numeric		
action_result.data.*.registrant_contact.org.value	string		
action_result.data.*.registrant_contact.phone.count	numeric		
action_result.data.*.registrant_contact.phone.value	string		
action_result.data.*.registrant_contact.postal.count	numeric		
action_result.data.*.registrant_contact.postal.value	string		
action_result.data.*.registrant_contact.state.count	numeric		
action_result.data.*.registrant_contact.state.value	string		
action_result.data.*.registrant_contact.street.count	numeric		
action_result.data.*.registrant_contact.street.value	string		
action_result.data.*.registrant_name.count	numeric		
action_result.data.*.registrant_name.value	string		
action_result.data.*.registrant_org.count	numeric		
action_result.data.*.registrant_org.value	string		
action_result.data.*.registrar.count	numeric		
action_result.data.*.registrar.value	string		
action_result.data.*.server_type.count	numeric		
action_result.data.*.server_type.value	string		
action_result.data.*.soa_email.*.count	numeric		
action_result.data.*.soa_email.*.value	string		
action_result.data.*.ssl_info.*.alt_names.*.count	numeric		

Data Path	Type	Contains	Example Values
action_result.data.*.ssl_info.*.alt_names.*.value	string		
action_result.data.*.ssl_info.*.common_name.count	numeric		
action_result.data.*.ssl_info.*.common_name.value	string		
action_result.data.*.ssl_info.*.duration.count	numeric		
action_result.data.*.ssl_info.*.duration.value	string		
action_result.data.*.ssl_info.*.email.*.count	numeric		
action_result.data.*.ssl_info.*.email.*.value	string		
action_result.data.*.ssl_info.*.hash.count	numeric		
action_result.data.*.ssl_info.*.hash.value	string		
action_result.data.*.ssl_info.*.issuer_common_name.count	numeric		
action_result.data.*.ssl_info.*.issuer_common_name.value	string		
action_result.data.*.ssl_info.*.not_after.count	numeric		
action_result.data.*.ssl_info.*.not_after.value	string		
action_result.data.*.ssl_info.*.not_before.count	numeric		
action_result.data.*.ssl_info.*.not_before.value	string		
action_result.data.*.ssl_info.*.organization.count	numeric		
action_result.data.*.ssl_info.*.organization.value	string		
action_result.data.*.ssl_info.*.subject.count	numeric		
action_result.data.*.ssl_info.*.subject.value	string		
action_result.data.*.tags.*.label	string		
action_result.data.*.tags.*.scope	string		
action_result.data.*.tags.*.tagged_at	string		

Data Path	Type	Contains	Example Values
action_result.data.*.technical_contact.city.count	numeric		
action_result.data.*.technical_contact.city.value	string		
action_result.data.*.technical_contact.country.count	numeric		
action_result.data.*.technical_contact.country.value	string		
action_result.data.*.technical_contact.fax.count	numeric		
action_result.data.*.technical_contact.fax.value	string		
action_result.data.*.technical_contact.name.count	numeric		
action_result.data.*.technical_contact.name.value	string		
action_result.data.*.technical_contact.org.count	numeric		
action_result.data.*.technical_contact.org.value	string		
action_result.data.*.technical_contact.phone.count	numeric		
action_result.data.*.technical_contact.phone.value	string		
action_result.data.*.technical_contact.postal.count	numeric		
action_result.data.*.technical_contact.postal.value	string		
action_result.data.*.technical_contact.state.count	numeric		
action_result.data.*.technical_contact.state.value	string		
action_result.data.*.technical_contact.street.count	numeric		
action_result.data.*.technical_contact.street.value	string		
action_result.data.*.tld	string		
action_result.summary	string		
action_result.data.*.website_title.count	numeric		
action_result.data.*.website_title.value	string		
action_result.status	string		success failed

Data Path	Type	Contains	Example Values
action_result.message	string		
summary.total_objects	numeric		1
summary.total_objects_successful	numeric		1

Action: 'Enrich Domain'

Get all Iris Investigate data for a domain except counts using the high volume Iris Enrich API endpoint (if provisioned).

Type: Investigate
Read only: True

Action Parameters

Parameter	Required	Description	Type	Contains
domain	required	Domain or comma-separated list of domains to query using the Iris Enrich API (if provisioned)	string	url domain

Action Output

Data Path	Type	Contains	Example Values
action_result.status	string		failed success
action_result.parameter.domain	string	url domain	
action_result.data.*.additional_whois_email.*.value	string		

action_result.data.*.admin_contact.city.value	string		
action_result.data.*.admin_contact.country.value	string		
action_result.data.*.admin_contact.fax.value	string		
action_result.data.*.admin_contact.name.value	string		
action_result.data.*.admin_contact.org.value	string		
action_result.data.*.admin_contact.phone.value	string		
action_result.data.*.admin_contact.postal.value	string		
action_result.data.*.admin_contact.state.value	string		
action_result.data.*.admin_contact.street.value	string		
action_result.data.*.adsense.value	string		
action_result.data.*.alexa	numeric		
action_result.data.*.billing_contact.city.value	string		
action_result.data.*.billing_contact.country.value	string		
action_result.data.*.billing_contact.fax.value	string		
action_result.data.*.billing_contact.name.value	string		
action_result.data.*.billing_contact.org.value	string		
action_result.data.*.billing_contact.phone.value	string		
action_result.data.*.billing_contact.postal.value	string		
action_result.data.*.billing_contact.state.value	string		
action_result.data.*.billing_contact.street.value	string		
action_result.data.*.create_date.value	string		
action_result.data.*.domain_risk.risk_score	numeric		
action_result.data.*.email_domain.*.value	string		
action_result.data.*.expiration_date.value	string		
action_result.data.*.first_seen.value	string		

action_result.data.*.google_analytics.value	string		
action_result.data.*.ip.*.address.value	string		
action_result.data.*.ip.*.asn.*.value	string		
action_result.data.*.ip.*.country_code.value	string		
action_result.data.*.ip.*.isp.value	string		
action_result.data.*.mx.*.domain.value	string		
action_result.data.*.mx.*.host.value	string		
action_result.data.*.mx.*.ip.*.value	string		
action_result.data.*.name_server.*.domain.value	string		
action_result.data.*.name_server.*.host.value	string		
action_result.data.*.name_server.*.ip.*.value	string		
action_result.data.*.redirect.value	string		
action_result.data.*.redirect_domain.value	string		
action_result.data.*.registrant_contact.city.value	string		
action_result.data.*.registrant_contact.country.value	string		
action_result.data.*.registrant_contact.email.*.value	string		
action_result.data.*.registrant_contact.fax.value	string		
action_result.data.*.registrant_contact.name.value	string		
action_result.data.*.registrant_contact.org.value	string		
action_result.data.*.registrant_contact.phone.value	string		
action_result.data.*.registrant_contact.postal.value	string		
action_result.data.*.registrant_contact.state.value	string		
action_result.data.*.registrant_contact.street.value	string		
action_result.data.*.registrant_name.value	string		

action_result.data.*.registrant_org.value	string		
action_result.data.*.registrar.value	string		
action_result.data.*.server_type.value	string		
action_result.data.*.soa_email.*.value	string		
action_result.data.*.ssl_info.*.alt_names.*.value	string		
action_result.data.*.ssl_info.*.common_name.value	string		
action_result.data.*.ssl_info.*.duration.value	string		
action_result.data.*.ssl_info.*.email.*.value	string		
action_result.data.*.ssl_info.*.hash.value	string		
action_result.data.*.ssl_info.*.issuer_common_name.value	string		
action_result.data.*.ssl_info.*.not_after.value	string		
action_result.data.*.ssl_info.*.not_before.value	string		
action_result.data.*.ssl_info.*.organization.value	string		
action_result.data.*.ssl_info.*.subject.value	string		
action_result.data.*.tags.*.label	string		
action_result.data.*.tags.*.scope	string		
action_result.data.*.tags.*.tagged_at	string		
action_result.data.*.technical_contact.city.value	string		
action_result.data.*.technical_contact.country.value	string		
action_result.data.*.technical_contact.fax.value	string		
action_result.data.*.technical_contact.name.value	string		
action_result.data.*.technical_contact.org.value	string		
action_result.data.*.technical_contact.phone.value	string		
action_result.data.*.technical_contact.postal.value	string		

action_result.data.*.technical_contact.state.value	string		
action_result.data.*.technical_contact.street.value	string		
action_result.data.*.tld	string		
action_result.data.*.website_title.value	string		
action_result.summary	string		
action_result.message	string		
summary.total_objects	numeric		1
summary.total_objects_successful	numeric		1

Action: 'Configure Scheduled Playbooks'

Run on initial setup to configure the optional monitoring playbooks. This action creates a custom list to manage the playbook scheduling and run status.

Type: Investigate
Read only: True

Action Parameters

No parameters are required for this action.

Action Output

Data Path	Type	Contains	Example Values
action_result.status	string		failed success
action_result.data.*	string		
action_result.summary	string		
action_result.message	string		
summary.total_objects	numeric		1

summary.total_objects_successful	numeric		1

Action: 'On Poll'

Execute scheduled playbooks based on the set interval (mins) in domaintools_scheduled_playbooks custom list. Smaller intervals will result in more accurate schedules.

Type: ingest
Read only: True

Action Parameters

No parameters are required for this action

Action Output

No Output