



USER GUIDE v1.1.1

HYAS™ Insight Enrichment Integration Guide ThreatConnect Platform

Introduction

This document outlines the process to install HYAS Insight Enrichment App provided by HYAS into the ThreatConnect Platform.

HYAS Insight Enrichment Playbook App enables ThreatConnect Platform users to perform On-Demand Enrichment of Passive DNS, Dynamic DNS, Passive Hash, SSL Certificate, Device Geo (Mobile Geolocation), Sinkhole, and whoIs endpoints using the HYAS Insight Enrichment source

1. Configuration

1.1. Requirement

The following requirements must be met to use **HYAS Insight Enrichment** App in your ThreatConnect Playbooks:

- Access to ThreatConnect instance
- Access to execute ThreatConnect Playbooks
- HYAS Insight API Key provisioned by HYAS to authenticate requests to HYAS Insight
- HYAS Insight Enrichment app installed in ThreatConnect Instance. (See **App Installation** section)

1.2. App Installation

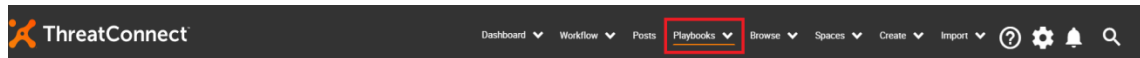
HYAS Insight Enrichment App for ThreatConnect is available on GitHub.

Download the App package with tcx extension and install it in your instance. For installation instructions, refer to the ThreatConnect System Administration Guide (Install an App). For more information, contact your ThreatConnect Customer Success representatives.

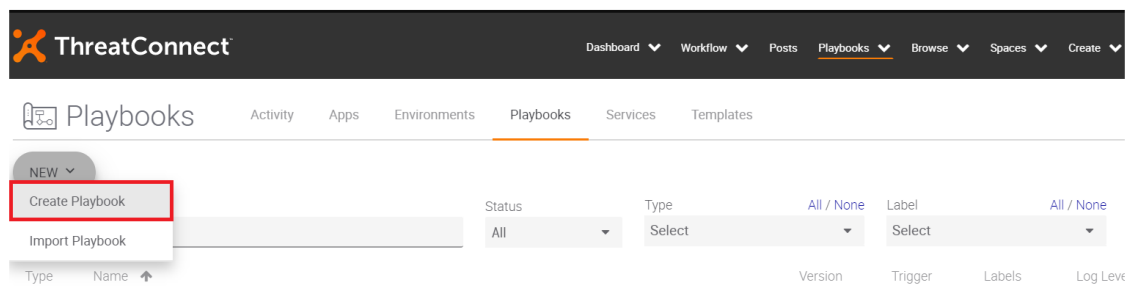
1.3. App Configuration

To demonstrate configuration of **HYAS Insight Enrichment** App in ThreatConnect Playbook editor, let us create a sample Playbook as below:

1. Click on **Playbooks** on the top menu-bar to go to the Playbooks page.



2. Hover the cursor over the **New** button on the left side of the page and click on **Create Playbook** from the drop-down menu



3. The **Create Playbook** dialog box will appear. Choose a suitable **Name** and **Description** for the sample Playbook and click **Save**. The page will then automatically redirect you to the Playbook editor.

Create Playbook



Name *

Sample-HYAS-Insight-Enrichment

Description

Playbook to configure HYAS Insight Enrichment app



☒ **Playbook**

Design a standard playbook with triggers based on an HTTP request, a mailbox, timers, and data changes in ThreatConnect.

☐ **Component**

Design a reusable playbook component that can be nested in other playbooks to standardize processes and encapsulate complex logic.

☐ **Workflow**

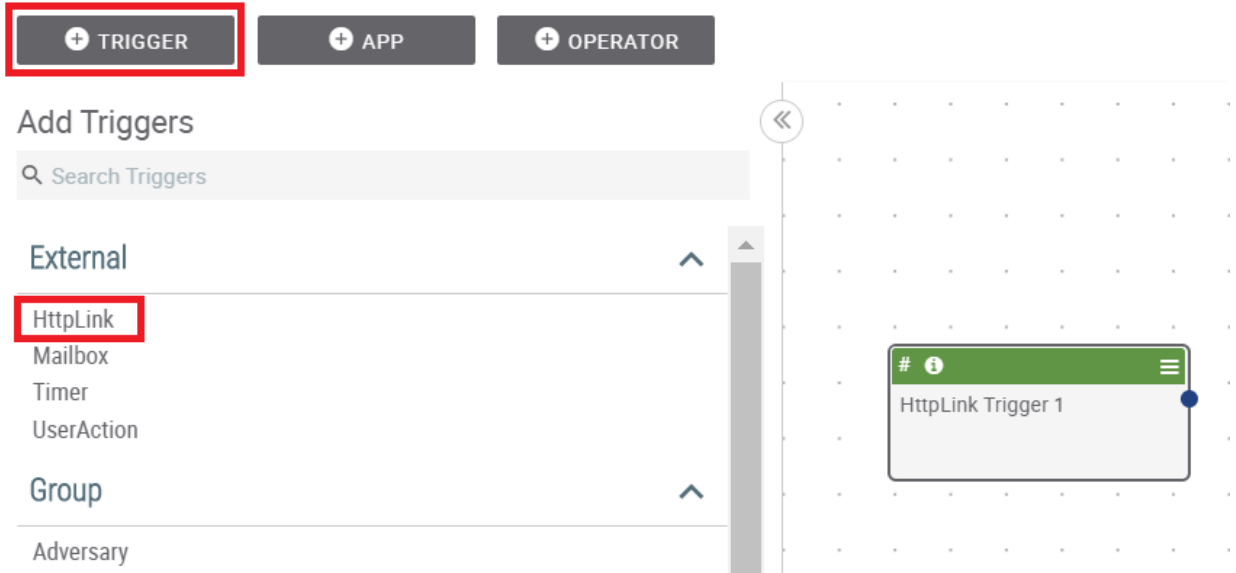
Design a reusable workflow component that can be used when running workflow logic.

CANCEL

SAVE

- To test the App, you can use a Trigger block to trigger the App to run. Click on + **TRIGGER** button and select **HttpLink**. This will provide you with an endpoint URL to signal the Playbook to run.

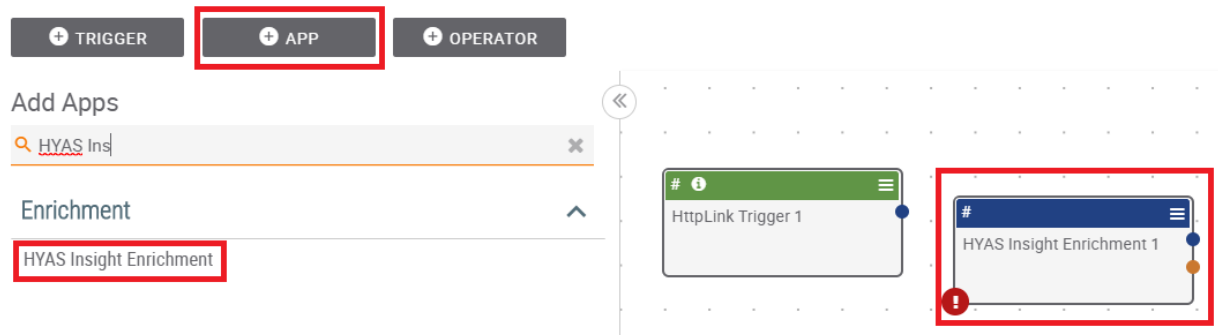
Sample-HYAS-Insight-Enrichment version 1.0



The screenshot shows the Playbook editor interface. At the top, there are three buttons: '+ TRIGGER' (highlighted with a red box), '+ APP', and '+ OPERATOR'. Below these is the 'Add Triggers' panel, which includes a search bar and a list of trigger categories: 'External' and 'Group'. Under 'External', 'HttpLink' is selected and highlighted with a red box. Other options in this category include 'Mailbox', 'Timer', and 'UserAction'. Under 'Group', 'Adversary' is listed. On the right side of the canvas, a 'HttpLink Trigger 1' block is added.

- In the Playbook editor page, click on + **APP** button to select the ThreatConnect app to be imported into the Playbook. Next search for "HYAS" to filter out all HYAS Apps in the ThreatConnect Platform and choose the **HYAS Insight Enrichment** App.

Sample-HYAS-Insight-Enrichment version 1.0



The screenshot shows the Playbook editor interface. At the top, there are three buttons: '+ TRIGGER', '+ APP' (highlighted with a red box), and '+ OPERATOR'. Below these is the 'Add Apps' panel, which includes a search bar with 'HYAS Ins' entered. Under the 'Enrichment' category, 'HYAS Insight Enrichment' is selected and highlighted with a red box. On the right side of the canvas, two blocks are added: 'HttpLink Trigger 1' and 'HYAS Insight Enrichment 1' (highlighted with a red box).

- Once you click on the App, it will appear in the Playbook editor as shown below. Connect the output of the trigger block to the app block as shown in the figure below. Double click on the App block to view the **Edit App** panel on the left side. The **HYAS Insight Enrichment** has three configuration steps. The **Action** step is used to select one of the Enrichment Type, Domain or Email or Phone Number or IP Address indicator can be selected.

Sample-HYAS-Insight-Enrichment version 1.0

+ TRIGGER **+ APP** **+ OPERATOR**

Edit App Display Notes ☐ ⚙ ⏪

HYAS Insight Enrichment

Job Name *
HYAS Insight Enrichment 1

1 Action

Enrichment Type *

Domain

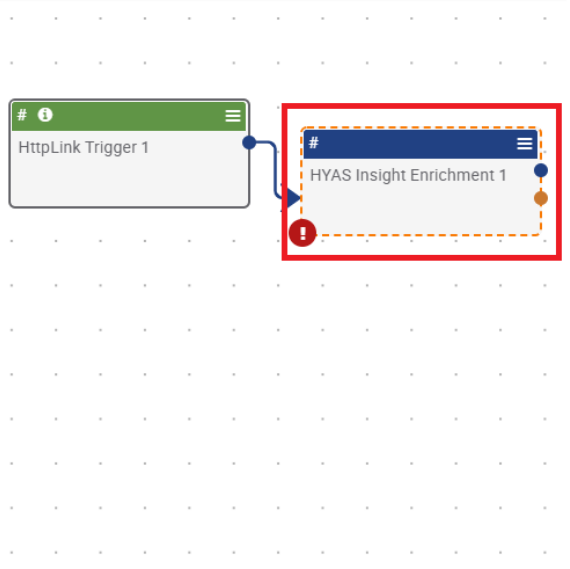
Domain

Email

Phone Number

IP Address

CANCEL NEXT



- Click on **Next** to see the second step **Connection**. In this step, enter the API key provided to you by HYAS in the **HYAS API Key** textbox.

Sample-HYAS-Insight-Enrichment version 1.0

+ TRIGGER + APP + OPERATOR

Edit App Display Notes

HYAS Insight Enrichment

Job Name *
HYAS Insight Enrichment 1

✓ Action

2 Connection

HYAS Insight Api Key *

3 Configure

CANCEL PREVIOUS NEXT

- The final step is, **Configure** is used for providing Domain or Email or Phone Number or IP Address as input. Please provide a valid Domain or Email or Phone Number or IP Address to get enrichment details. Click on **Save** to finish the App configuration settings. At this point, the **HYAS Insight Enrichment** App setup is complete and is ready to be used with other objects of the Playbook as required by the user.

+ TRIGGER
+ APP
+ OPERATOR

Edit App
Display Notes ☐
⚙️
⏪

HYAS Insight Enrichment

Job Name *

HYAS Insight Enrichment 1

✓ Action

✓ Connection

3 Configure

Domain *

www.abc.com

☐ Fail on no results

☒ Fail on error

CANCEL
PREVIOUS
SAVE

9. To run the Playbook, toggle the **Active** button on the top-right corner of the Playbook editor. A green exclamation symbol will appear on its left if all the Apps in the Playbook have been configured properly. Click on the green exclamation and it will show the endpoint URL that you need to hit to trigger the Playbook to run. Optionally, you can click on **Execute Endpoint** menu-item to do this automatically.

ⓘ
Active ☒

Playbook editing is disabled when status is 'Active'.
<https://sandbox.threatconnect.com/api/playbook/ca621aa5-1252-4566-8747-77d9c56fed7a>

Copy URL
Execute Endpoint

← Select a Playbook Execution to view steps

2. Outputs

Output	TC Type	Description
hy.passivedns.json.raw	String	Raw response object from HYAS Insight API
hy.passivedns.json.raw.count	String	Raw Number of records from HYAS Insight API
hy.whois.currentemail	StringArray	Array containing emails
hy.whois.currentAlias	StringArray	Array containing Alias names
hy.whois.currentPhoneNumber	StringArray	Array containing phone numbers
hy.whois.currentRegistrar	String	String value of Registrar
hy.whois.current.json.raw	String	Raw Response object returned from the HYAS Insight API
hy.whois.current.json.raw.count	String	Raw Number of records from HYAS Insight API
hy.whois.historic.results.data	StringArray	Array Containing the historic Whois information for the domain
hy.whois.historic.json.raw	String	Raw Response object returned from the HYAS Insight API
hy.whois.historic.json.raw.count	String	Raw Number of records from HYAS Insight API
hy.dynamicdns.json.raw	String	Raw Response object returned from the HYAS Insight API
hy.dynamicdns.json.raw.count	String	Raw Number of records from HYAS Insight API
hy.devicegeo.json.raw	String	Raw Response object returned from the HYAS Insight API
hy.devicegeo.raw.count	String	Raw Number of records from HYAS Insight API
hy.passivehash.json.raw	String	Raw Response object returned from the HYAS Insight API

hy.passivehash.raw.count	String	Raw Number of records from HYAS Insight API
hy.sslcertificate.json.raw	String	Raw Response object returned from the HYAS Insight API
hy.sslcertificate.raw.count	String	Raw Number of records from HYAS Insight API
hy.sinkhole.json.raw	String	Raw Response object returned from the HYAS Insight API
hy.sinkhole.json.raw.count	String	Raw Number of records from HYAS Insight API
hy.enrichment_type	String	The Selected Enrichment type by the User for debugging purposes

hy.passivedns.json.raw, this output variable contains the array of objects containing the passive dns information of the domain. Each object will be JSON. Data can be extracted from JSON objects using JMESPath App

Attribute Name	Attribute Description
count	The passive DNS count
cert_name	The certificate name for passive DNS record
domain	The domain of the passive DNS information requested
first_seen	The first time this domain was seen
ip_geo_cityname	The city name for the domain's IP address
ip_geo_countryIsoCode	The country ISO code for the domain's IP address
ip_geo_countryName	The country name for the domain's IP address
ip_geo_locationLatitude	The location latitude for the domain's IP address
ip_geo_locationLongitude	The location longitude for the domain's IP address
ip_geo_postalCode	The postal code for the domain's IP address
ip_ipaddress	The IP address for the domain
ip_isp_autonomousSystemNumber	The Autonomous System Number(ASN) for the domain's ISP
ip_isp_autonomousSystemOrganization	The Autonomous System Organization for the domain's ISP
ip_isp_ipaddress	The IP Address for the domain's ISP
ip_isp_isp	The ISP of the domain
ip_isp_organization	The ISP organization of the domain
ipv4	The ipv4 address of the passive DNS record
ipv6	The ipv6 address of the passive DNS record
sha1	The sha1 sum of the passive DNS record
last_seen	The last time this domain was seen

hy.whois.historic.results, this output variable contains the array of objects containing the historic Whois information of the domain, each object contains the following attributes in key value pairs. Each object will be in JSON. Data can be extracted from JSON objects using JMESPath App

Note: Few attributes such as email, alias and phone will have array of values.

E.g.:- "email": [["abusecomplaints@markmonitor.com"](mailto:abusecomplaints@markmonitor.com),["dns-admin@google.com"](mailto:dns-admin@google.com)]

Attribute Name	Attribute Description
email	Historic Email associated with Domain
Alias	Historic name associated with the domain
Phone	Historic Phone Number associated with Domain
Registrar	Historic domain registrar

hy.whois.current.json.raw, this output variable contains the array of objects containing the Whois Current data, each object will be in JSON, data can be extracted from JSON objects using JMESPath App.

Attribute Name	Attribute Description
abuse_emails	Abuse contact address
address	Address Information
city	The city of the registrant
country	The country of the registrant
data	Data Information
datetime	Date Time Information
domain	The domain of the registrant
domain_2tld	The second-level domain of the registrant
domain_created_datetime	The date and time when the Whois record was created
domain_expires_datetime	The date and time when the Whois record expires
domain_updated_datetime	The date and time when the Whois record was last updated

email	Email Information
idn_name	The international domain name
meta_data	Metadata Information
name	The contact name (registrant contact, administrative contact, technical contact, or abuse contact)
nameserver	The nameserver domain
organization	Organization Information
phone	The phone number of the registrant in e164 format
registrar	The domain registrar
state	The state where domain was registered
whois_hash	Hash Information
whois_id	Id Information
whois_nameserver.domain	Nameserver's Domain Information
whois_nameserver.domain_2tld	Nameserver's Domain_2tld Information
whois_nameserver.whois_related_nameserver_id	Nameserver's Id Information
whois_pii.address	Personal Identity Address Information
whois_pii.city	Personal Identity City Information
whois_pii.data	Personal Identity Data Information
whois_pii.email	Personal Identity Email Information
whois_pii.geo_country_alpha_2	Personal Identity Country Information
whois_pii.name	Personal Identity Name Information
whois_pii.organization	Personal Identity Organization Information
whois_pii.phone_e164	Personal Identity Phone_e164 Information
whois_pii.state	Personal Identity State Information
whois_pii.whois_related_pii_id	Personal Identity Id Information
whois_pii.whois_related_type	Personal Identity Related Information
source	Source Information
total_count	Total Count Information

hy.whois.historic.json.raw, this output variable contains the array of objects containing the Whois Historic data, each object will be in JSON, data can be extracted from JSON objects using JMESPath App

Attribute Name	Attribute Description
address	Address Information
city	The city of the registrant
country	The country of the registrant
data	Data Information
datetime	Date Time Information
domain	The domain of the registrant
domain_2tld	The second-level domain of the registrant
domain_created_datetime	The date and time when the Whois record was created
domain_expires_datetime	The date and time when the Whois record expires
domain_updated_datetime	The date and time when the Whois record was last updated
email	The email of the registrant
idn_name	The international domain name
meta_data	Metadata Information
name	The contact name (registrant contact, administrative contact, technical contact, or abuse contact)
nameserver	The nameserver domain
phone.phone	The phone number of the registrant in e164 format
phone.phone_info.carrier	Phone Number carrier Information
phone.phone_info.country	Country Information
phone.phone_info.geo	Phone Geolocation Information
privacy_protection	Privacy Protection Information

registrar	The domain registrar
whois_hash	Hash Information
whois_id	Id Information

hy.dynamicdns.json.raw, this output variable contains the array of objects containing the Dynamic DNS data, each object will be in JSON, data can be extracted from JSON objects using JMESPath App

Attribute Name	Attribute Description
a_record	The A record for the domain
account	The account holder name
created	The date which the domain was created
created_ip	The IP address of the account holder
domain	The domain associated with the Dynamic DNS information
domain_creator_ip	The IP address of the domain creator
email	The email address connected to the domain

hy.passivehash.json.raw, this output variable contains the array of objects containing the Passive Hash data, each object will be in JSON, data can be extracted from JSON objects using JMESPath App

Attribute Name	Attribute Description
domain	The domain of the passive hash information requested
md5_count	MD5 hash count

hy.devicegeo.json.raw, this output variable contains the array of objects containing the Device Geo data, each object will be in JSON, data can be extracted from JSON objects using JMESPath App

Attribute Name	Attribute Description
datetime	A date-time string in RFC 3339 format
device_geo_id	Geolocation ID

device_user_agent	The user agent string for the device
geo_country_alpha_2	The ISO 3316 alpha-2 code for the country associated with the latitude/longitude reported
geo_horizontal_accuracy	Geolocation accuracy Information
ipv4	The ipv4 address assigned to the device. A device may have either or ipv4 and ipv6
ipv6	The ipv6 address assigned to the device. A device may have either or ipv4 and ipv6
latitude	Units are degrees on the WGS 84 spheroid
longitude	Units are degrees on the WGS 84 spheroid
wifi_bssid	The BSSID (MAC address) of the WIFI router that the device communicated through
wifi_ssid	The SSID (name) of the WIFI network that the device communicated through

hy.sslcertificate.json.raw, this output variable contains the array of objects containing the SSL Certificate data, each object will be in JSON, data can be extracted from JSON objects using JMESPath App

Attribute Name	Attribute Description
related_count	The number of IP addresses connected to this certificate
ssl_version	SSL Version Information
subject_commonName	The subject name that the certificate was issued to
subject_countryName	The country the certificate was issued to
subject_localityName	The city where the subject company is legally located
subject_organizationName	The organization name that received the certificate
subject_organizationalUnitName	The organization unit name that received the certificate
subject_stateOrProvinceName	The state or province name where the subject company is located
timestamp	Time Stamp Information
ssl_certs.ip	The IP address associated with certificate
ssl_certs.ssl_cert.cert_key	The certificate key (sha1)
ssl_certs.ssl_cert.expire_date	The expiry date of the certificate
ssl_certs.ssl_cert.issue_date	The issue date of the certificate

ssl_certs.ssl_cert.issuer_commonName	The common name that the certificate was issued from
ssl_certs.ssl_cert.issuer_countryName	The country the certificate was issued from
ssl_certs.ssl_cert.issuer_localityName	The city where the issuer company is legally located
ssl_certs.ssl_cert.issuer_organizationName	The organization name that issued the certificate
ssl_certs.ssl_cert.issuer_organizationalUnitName	The organization unit name that issued the certificate
ssl_certs.ssl_cert.issuer_stateOrProvinceName	The state or province where the issuer company is legally located
ssl_certs.ssl_cert.md5	SSL certificate MD5 Hash
ssl_certs.ssl_cert.serial_number	SSL certificate Serial Number
ssl_certs.ssl_cert.sha1	SSL certificate SHA1 Hash
ssl_certs.ssl_cert.sha_256	SSL certificate SHA 256 Hash
ssl_certs.ssl_cert.sig_algo	SSL certificate signing algorithm
ssl_certs.ssl_cert.signature	SSL certificate signature

hy.sinkhole.json.raw, this output variable contains the array of objects containing Sinkhole data, each object will be in JSON, data can be extracted from JSON objects using JMESPath App

Attribute Name	Attribute Description
count	The sinkhole counts
country_name	The country of the IP
data_port	The data port
datetime	The first seen date of the sinkhole
ipv4	The ipv4 of the sinkhole
last_seen	The last seen date of the sinkhole
organization_name	The ISP organization for the IP
sink_source	The ipv4 of the sink source

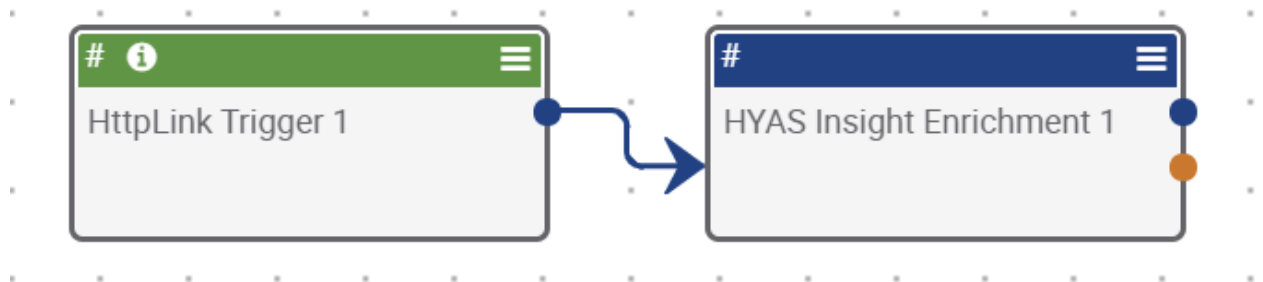
3. Sample Playbook Example

You can find the sample Playbook example “HYAS Insight Enrichment Playbook Example” available on GitHub. This example provides a basic understanding on how to use the HYAS Insight Enrichment App in the playbooks.

To install this Playbook Example, visit the Playbooks tab within the ThreatConnect Platform. Select New > Import and locate the PBX file you wish to add to your system. Follow the on-screen instructions to complete the import.

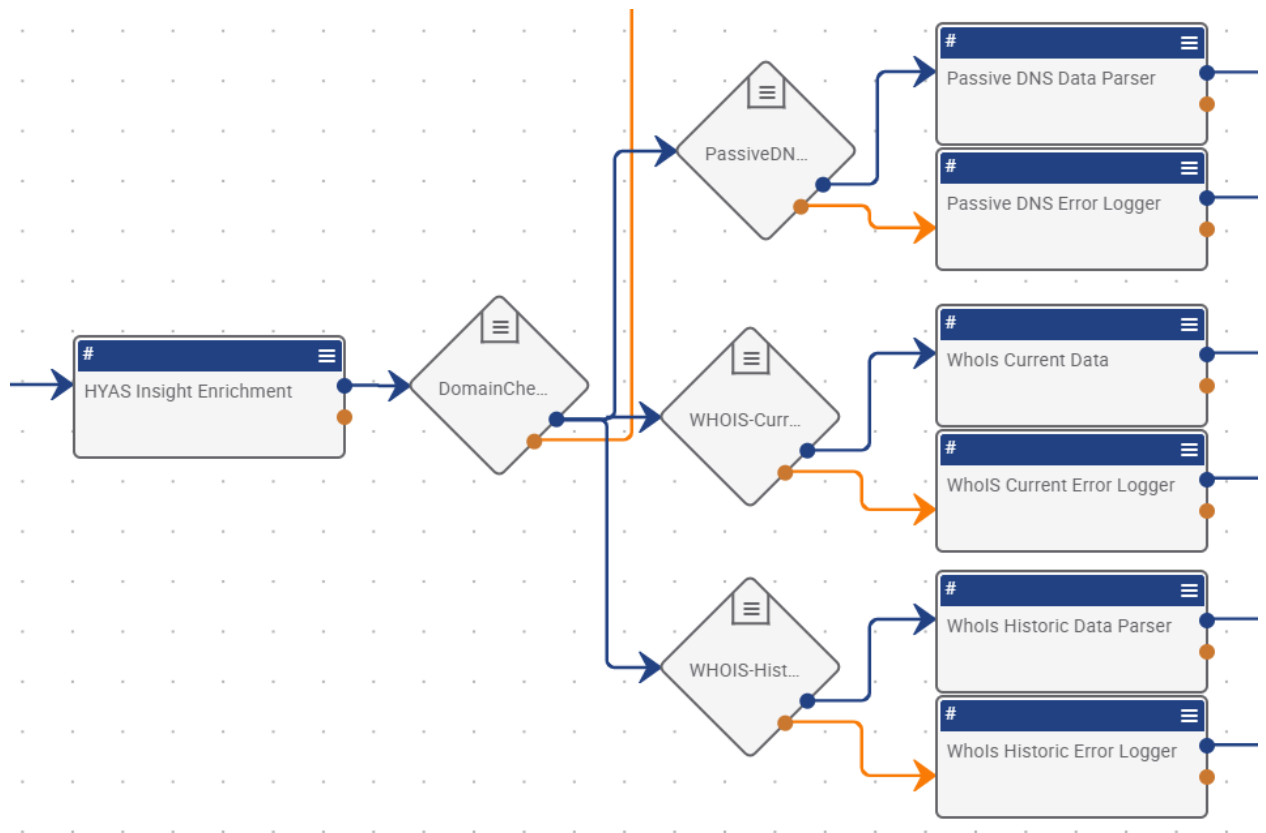
Steps Explained Below:

1. Use the ‘HttpLink Trigger’ and configure the ‘HYAS Insight Enrichment’ App from the Trigger and App section, respectively.

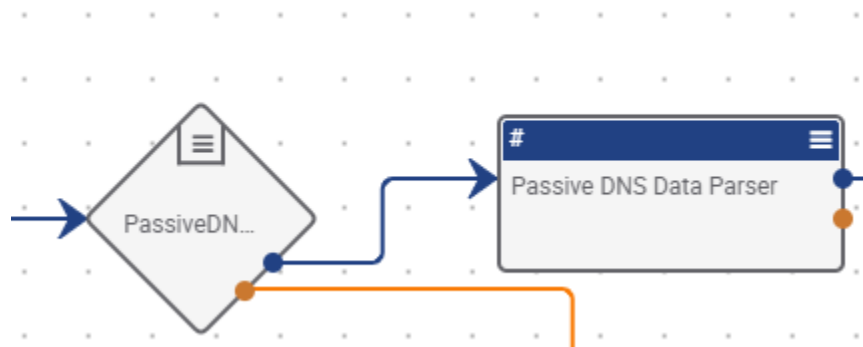


Domain Enrichment Flow:

- Check if the Enrichment type selected is “Domain”.
- Check if PassiveDNS records are greater than “0”.
- Check if whoIs Current records are greater than “0”.
- Check if whoIs Historic records are greater than “0”.



2. Defining the desired attributes needed from the Passive DNS data using the 'JMESPATH' Utility App which is 'Passive DNS Data Parser'.



+ TRIGGER

+ APP

+ OPERATOR

Edit App

Display Notes ☐

JMESPath

Job Name *

Passive DNS Data Parser

JSON Data *

#hy.passivedns.json.raw ✕

JMESPath String Expressions

Key	Value	
		+

☒ Strip Quotes from String Output

JMES Path StringArray Expressions

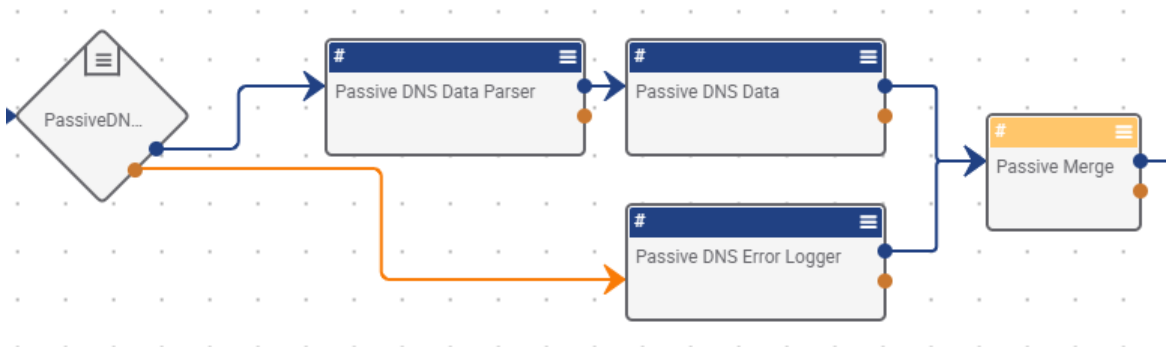
Key	Value	
		+

Key	Value	
parsed_data	[].[ipv4,first_seen,last_seen,ip.geo.city_name,ip.geo.country_name]	

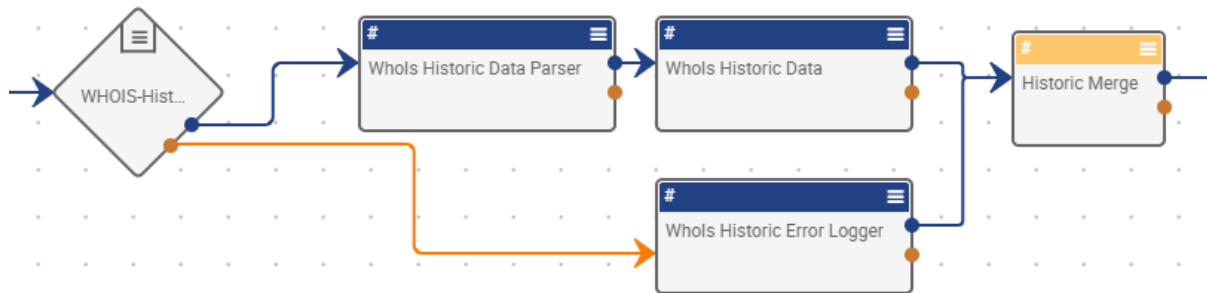
CANCEL

SAVE

- If the number of records of 'Passive DNS Data' is greater than zero
 - The Playbook will have the success path (which represents as a blue arrow path) and logs the Passive DNS data in a 'logger' App named as 'Passive DNS Data'.
 - If no records are returned from the 'Passive DNS Data', it will have the failed path (orange arrow) and logs the error in 'Passive DNS Error Logger'
 - Both success and failed Logger outputs are merged in the 'Merge' operator named as 'Passive Merge'.

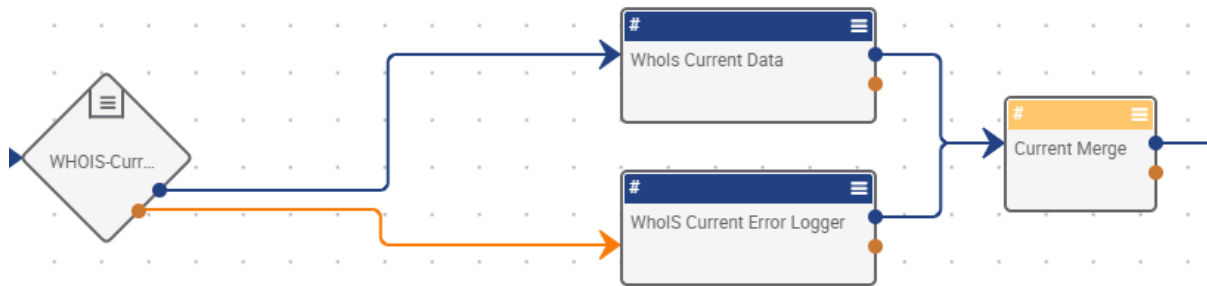


4. 'whols Historic Data' flow is configured as below:



5. If the number of records of 'Whols Historic Data' is greater than zero
- The Playbook should the success path (which represents as a blue arrow path) and logs the Whols Historic Data' in a 'logger' App named as 'Whols Historic Data'.
 - If no records are returned from the 'Whols Historic Data", it will have the failed path (orange arrow) and logs the error in 'Whols Historic Error Logger'
 - Both success and failed Logger outputs are merged in the 'Merge' operator named as 'Historic Merge'.

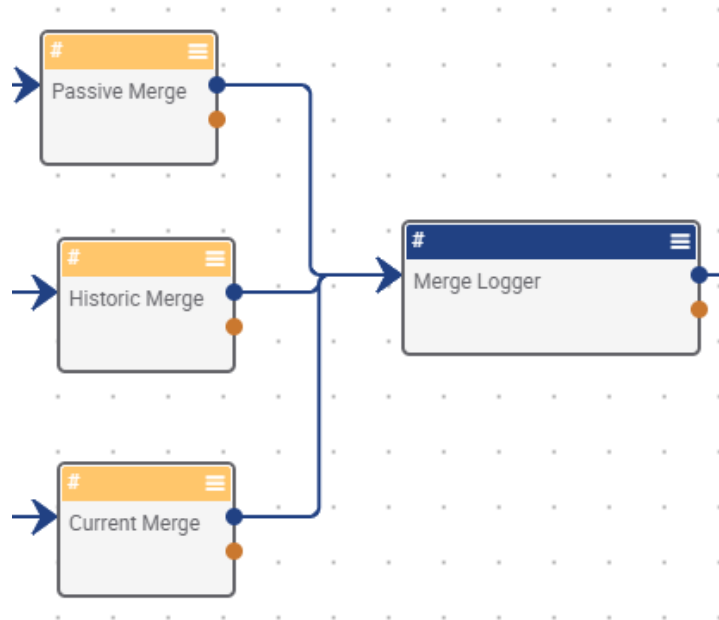
6. 'whols Current Data' flow is configured as below:



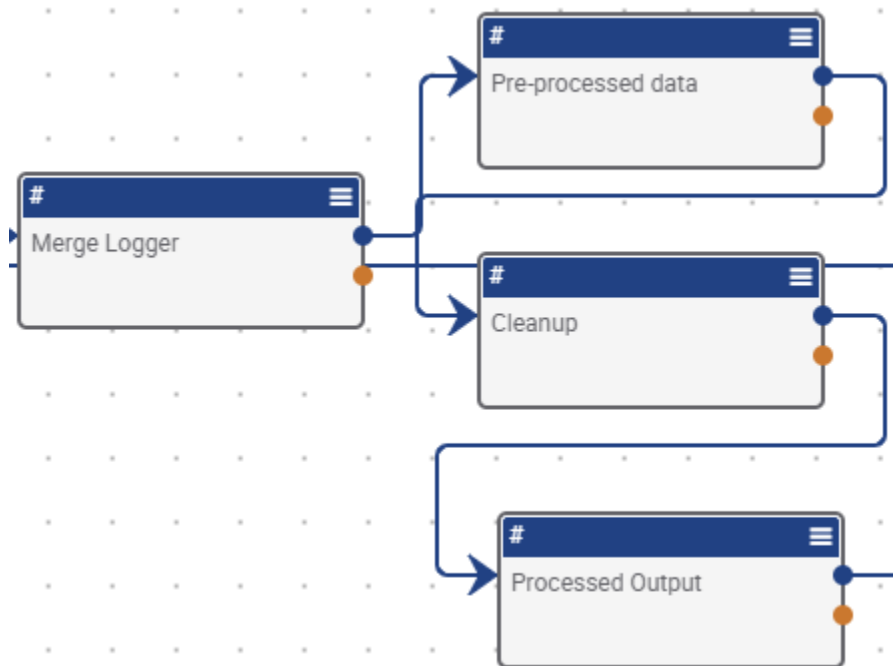
7. If the number of records of 'Whols Current Data' is greater than zero

- The Playbook should the success path (which represents as a blue arrow path) and logs the 'Whols Current Data' in a 'logger' App named as 'Whols Current Data'.
- If no records are returned from the 'Whols Current Data', it will have the failed path (orange arrow) and logs the error in 'Whols Current Error Logger'
- Both success and failed Logger outputs are merged in the 'Merge' operator named as 'Current Merge'.

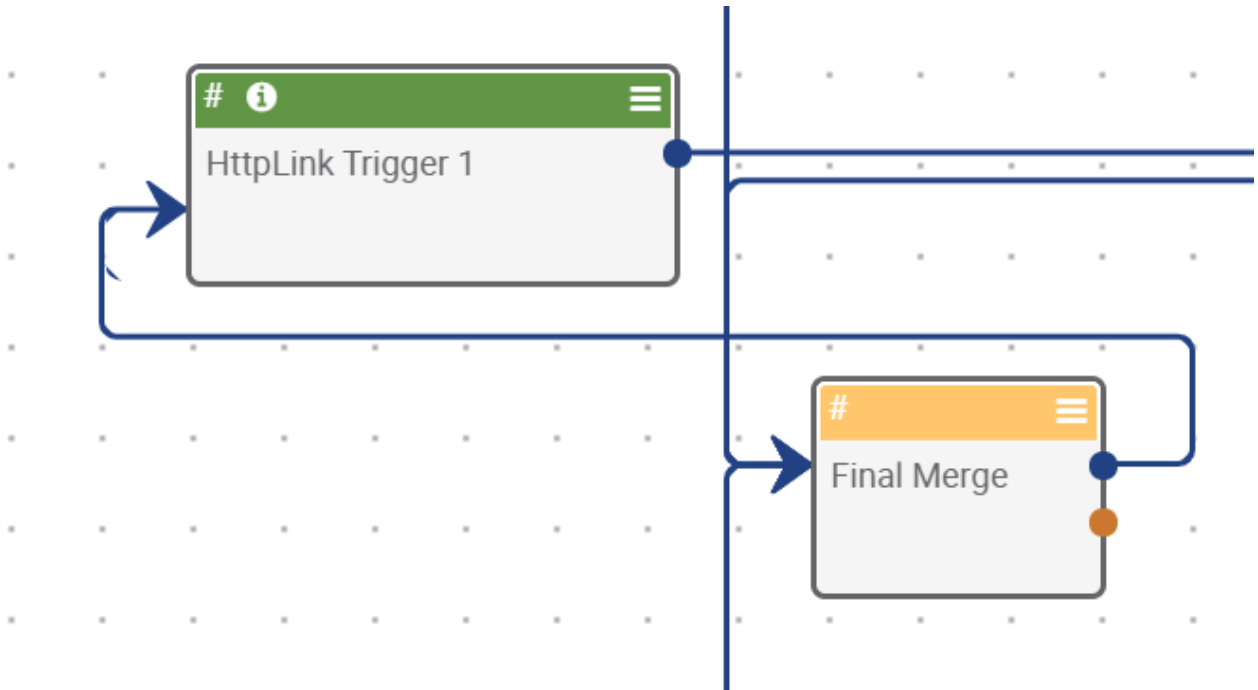
8. The Merge data from all the three endpoints (PassiveDNS/WhoIS Historic/Whois Current) is logged into Logger App named as 'Merge Logger' as below:



9. For beautification of the data, we have used the “Find and Replace” Apps named as Pre-processed data, Clean-up and Processed output, to format the output from merge logger.

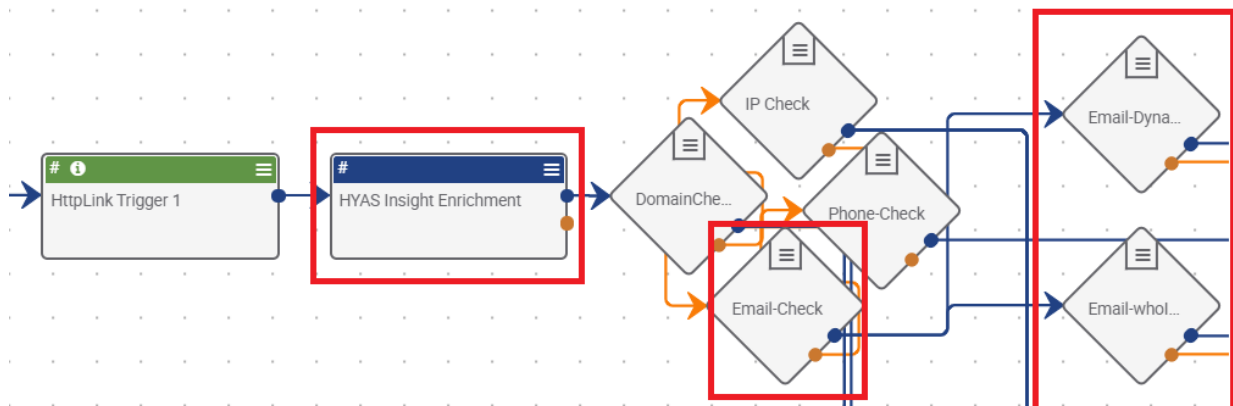


10. The Domain Enrichment output from the Merge operator named as “Final Merge” is given to ‘HttpLink Trigger’. The output can be visible, which is displayed in the body, after activating the Playbook and executing the Endpoint.

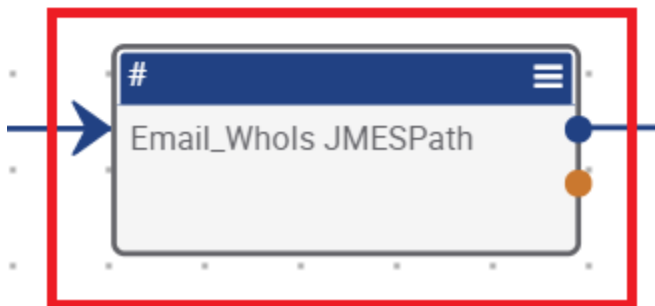
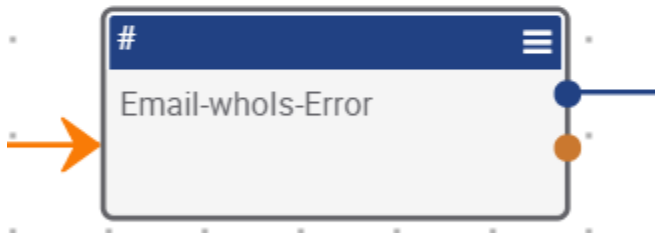
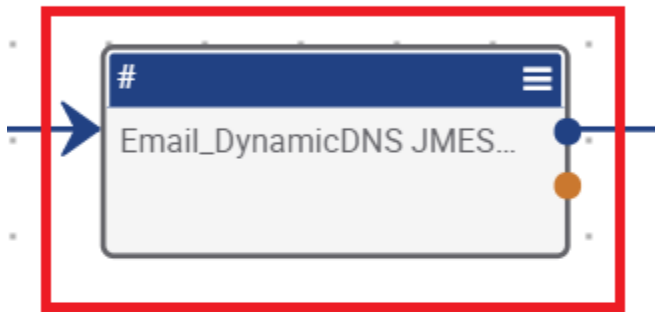
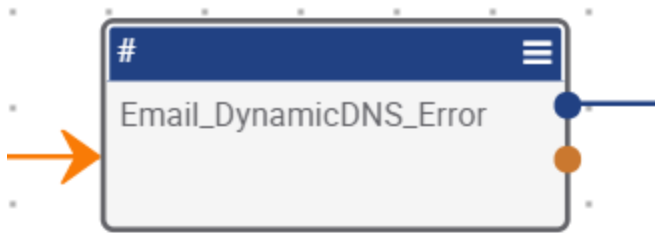


Email Enrichment Flow:

- Check if the Enrichment type selected is “Email”.
- Check if Dynamic DNS records are greater than “0”.
- Check if whois Historic records are greater than “0”.



1. Defining the desired attributes needed from the Dynamic DNS and WhoIs data using the 'JMESPATH' Utility App which are 'Email_DynamicDNS JMESPath' and 'Email_WhoIs JMESPath' respectively.



+ TRIGGER

+ APP

+ OPERATOR

Edit App

Display Notes ☐

JMESPath

Job Name *

Email_DynamicDNS JMESPath

JSON Data *

#hy.dynamicdns.json.raw *

JMESPath String Expressions

Key Value +

Key	Value	
Email_DynamicDNS _Data	[. [a_record,account,created,created_ip,domain,email]	

☒ Strip Quotes from String Output

JMES Path StringArray Expressions

Key Value +

CANCEL

SAVE

+ TRIGGER

+ APP

+ OPERATOR

Edit App

Display Notes



JMESPath

Job Name *

Email_Whols JMESPath

JSON Data *

#hy.whois.historic.json.raw ✕

JMESPath String Expressions

Key

Value



Key	Value	
Email_whols_Data	[.domain,phone[].phone_info.carrier,phone[].phone_info.country,phone[].phone_info.geo, registrar]	



Strip Quotes from String Output

JMES Path StringArray Expressions

Key

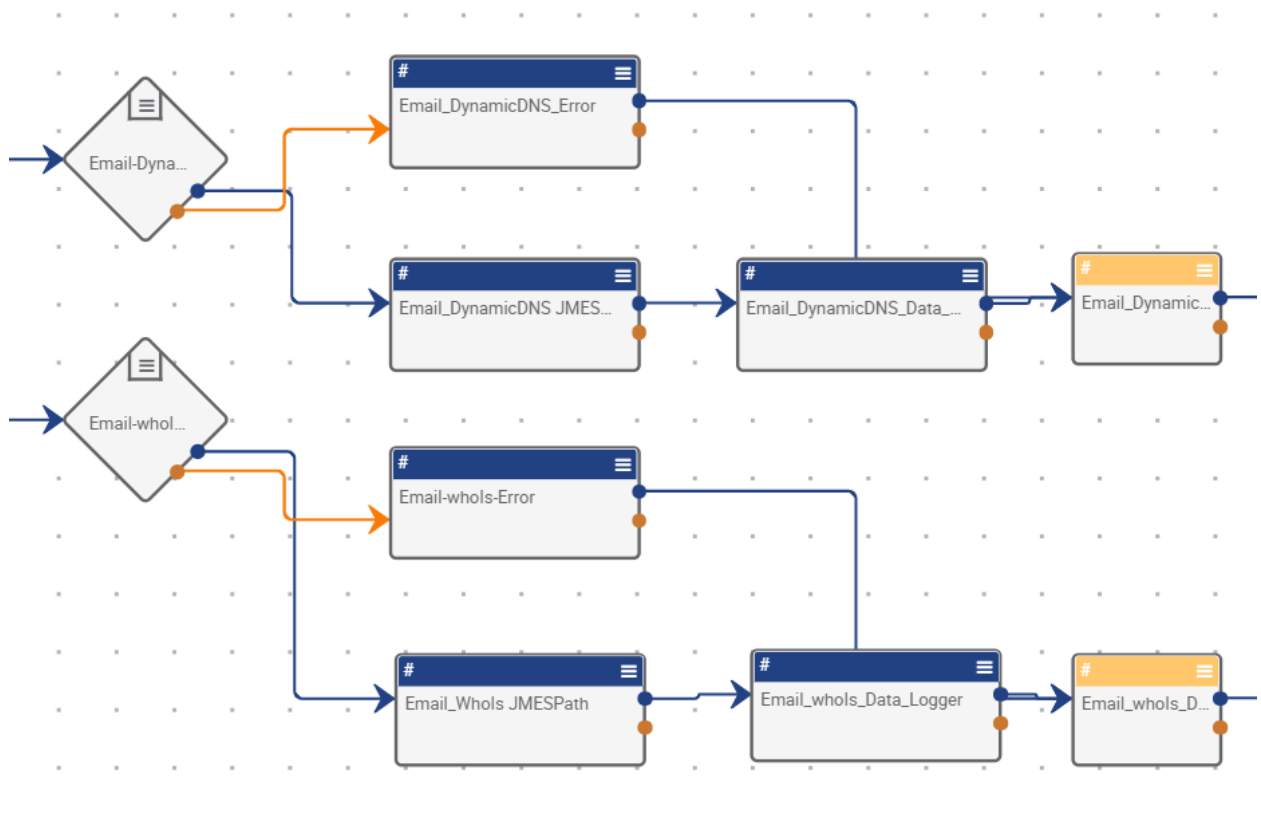
Value



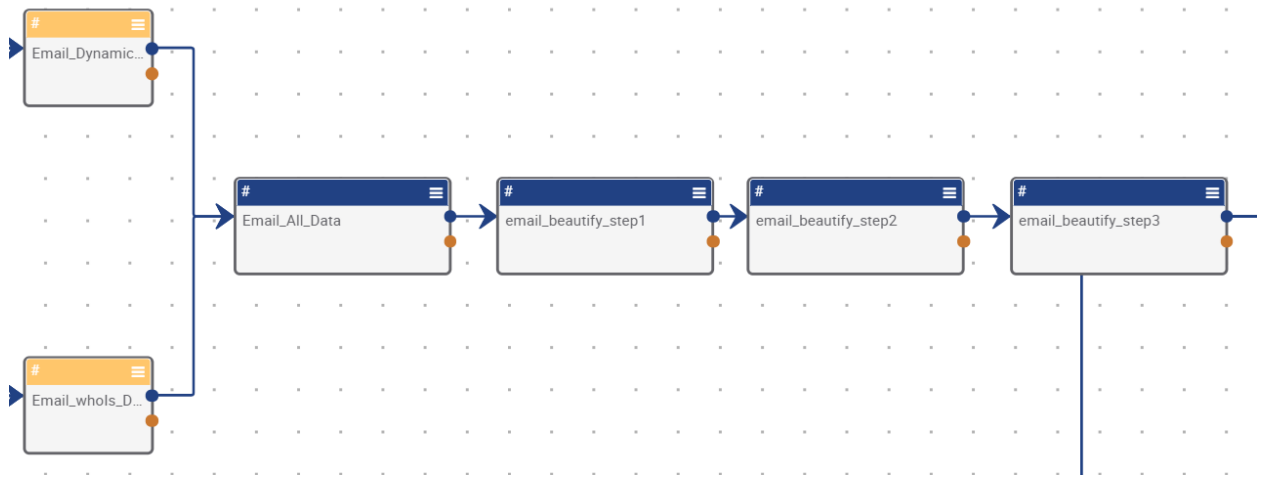
CANCEL

SAVE

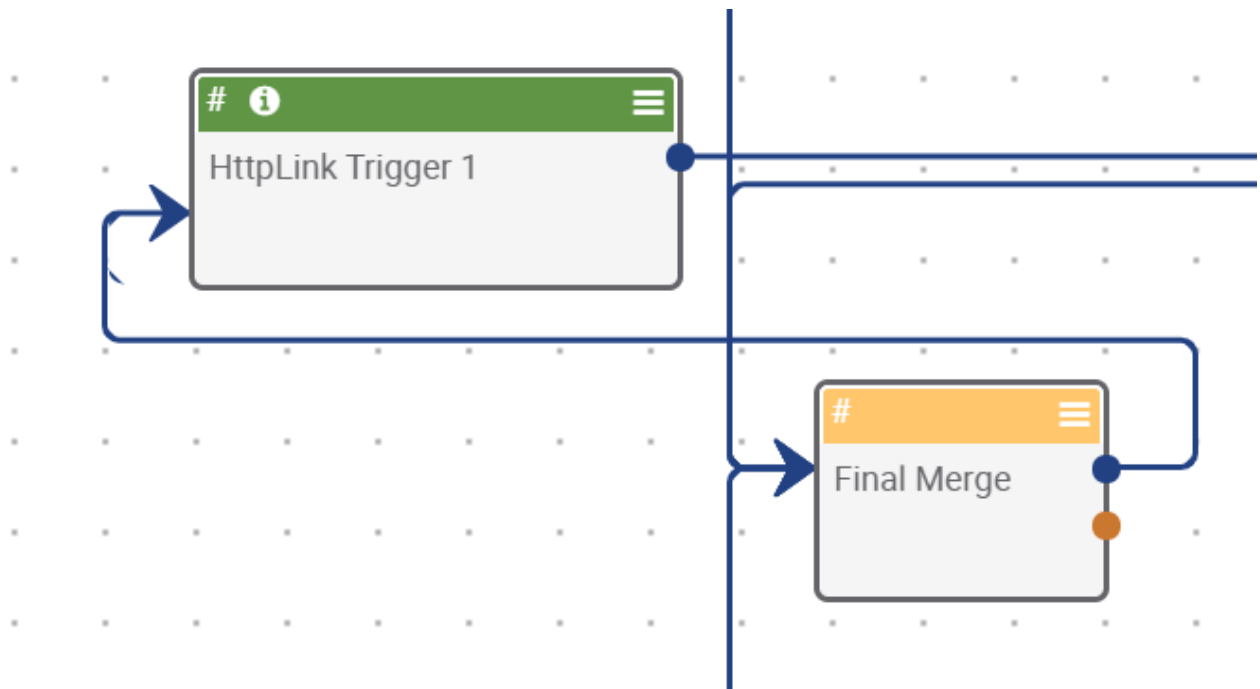
2. If the number of records of 'Dynamic DNS Data' is greater than zero
 - The Playbook will have the success path (which represents as a blue arrow path) and logs the Dynamic DNS data in a 'logger' App named 'Email_DynamicDNS_Data_Logger'.
 - If no records are returned from the 'Dynamic DNS Data' data, it will have the failed path (orange arrow) and logs the error in in 'Email_DynamicDNS_Error' Logger App
 - Both success and failed Logger outputs are merged in the 'Merge' operator 'Email_DynamicDns_Data_Merger' as shown below.
3. If the number of records of 'whols Historic Data' is greater than zero
 - The Playbook will have the success path (which represents as a blue arrow path) and logs the Dynamic DNS data in a 'logger' App named 'Email_whols_Data_Logger'.
 - If no records are returned from the 'Dynamic DNS Data' data, it will have the failed path (orange arrow) and logs the error in in 'Email_whols_Error' Logger App
 - Both success and failed Logger outputs are merged in the 'Merge' operator 'Email_whols_Data_Merger' as shown below.



4. The Merge data from all the two endpoints (Dynamic DNS/whols Historic) is logged into Logger App named as 'Email_ALL_Data' as shown below.
5. For beautification of the data, we have used the "Find and Replace" Apps named as email_beautify_step1, email_beautify_step2 and email_beautify_step3, to format the output from merge logger as shown below.

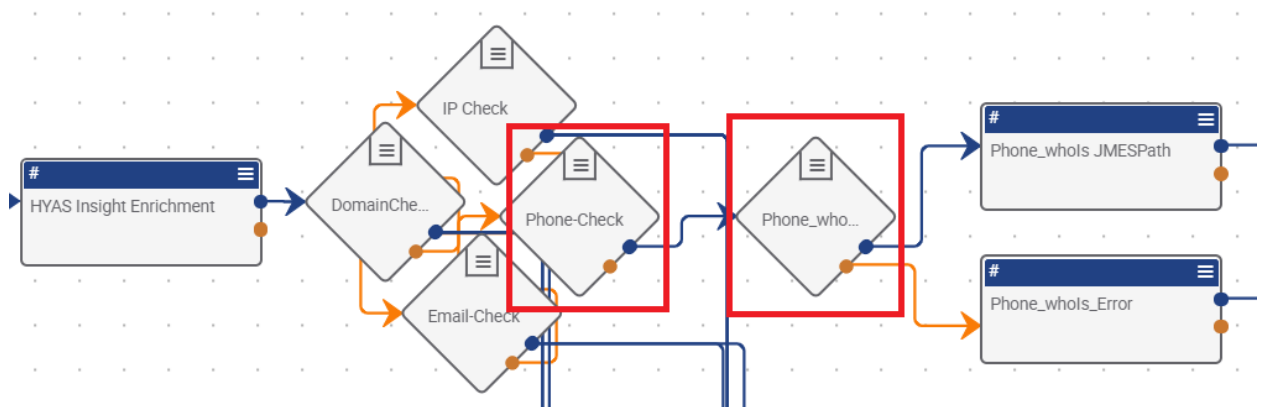


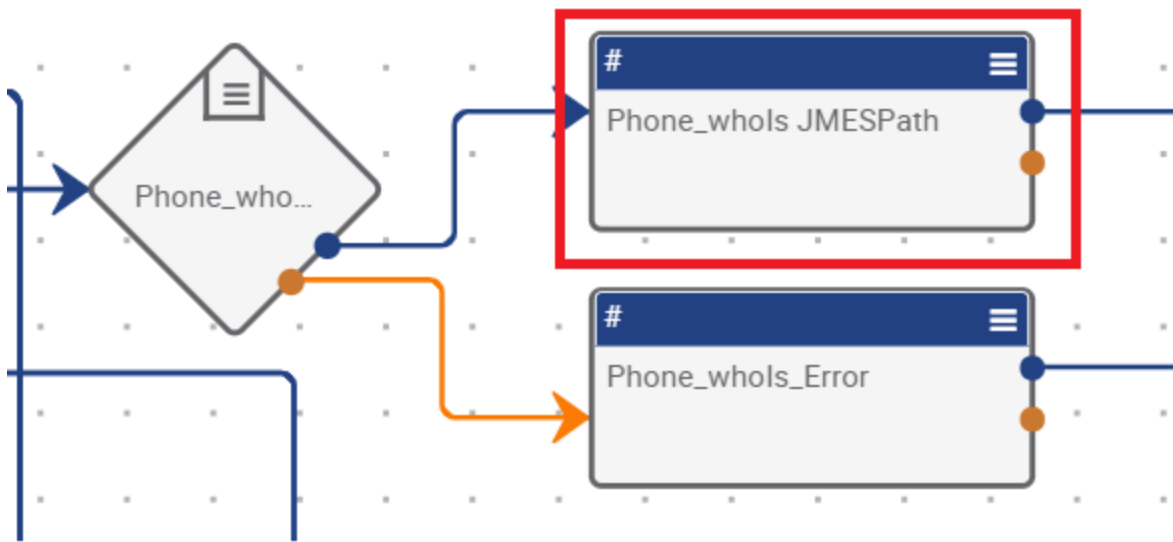
6. The Email Enrichment output from the Merge operator named as "Final Merge" is given to 'HttpLink Trigger'. The output can be visible, which is displayed in the body, after activating the Playbook and executing the Endpoint.



Phone Number Enrichment Flow:

- Check if the Enrichment type selected is “Phone Number”.
 - Check if whols Historic records are greater than “0”.
1. Defining the desired attributes needed from the Whols data using the ‘JMESPATH’ Utility App
‘Phone_whols JMESPath’ as shown below:





+ TRIGGER

+ APP

+ OPERATOR

Edit App

Display Notes ☐



JMESPath

Job Name *


Phone_whols JMESPath


JSON Data *

#hy.whois.historic.json.raw ✕

JMESPath String Expressions

Key	Value
-----	-------




Key	Value	
Phone_whols_Data	[. [domain,phone[].phone_info.carrier,phone[].phone_info.country,phone[].phone_info.geo, registrar]	

☒ Strip Quotes from String Output

JMES Path StringArray Expressions

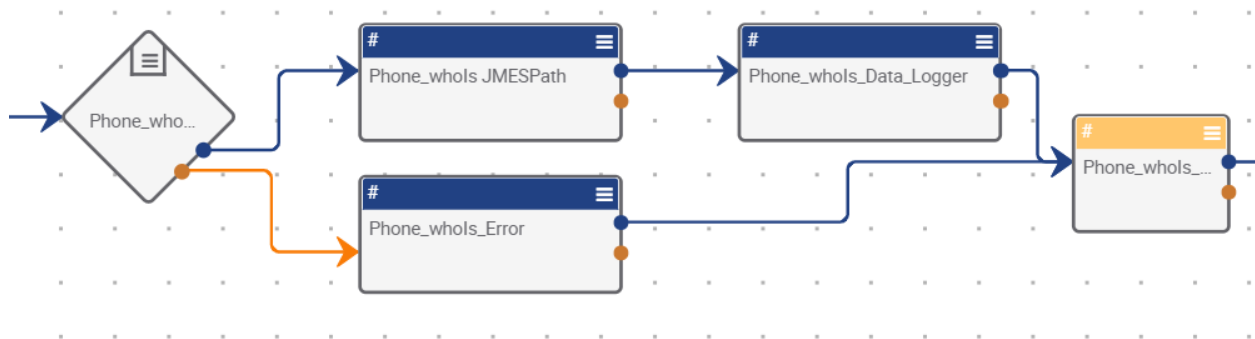
Key	Value
-----	-------



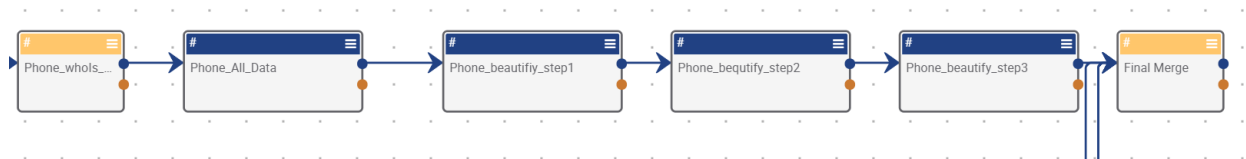
CANCEL

SAVE

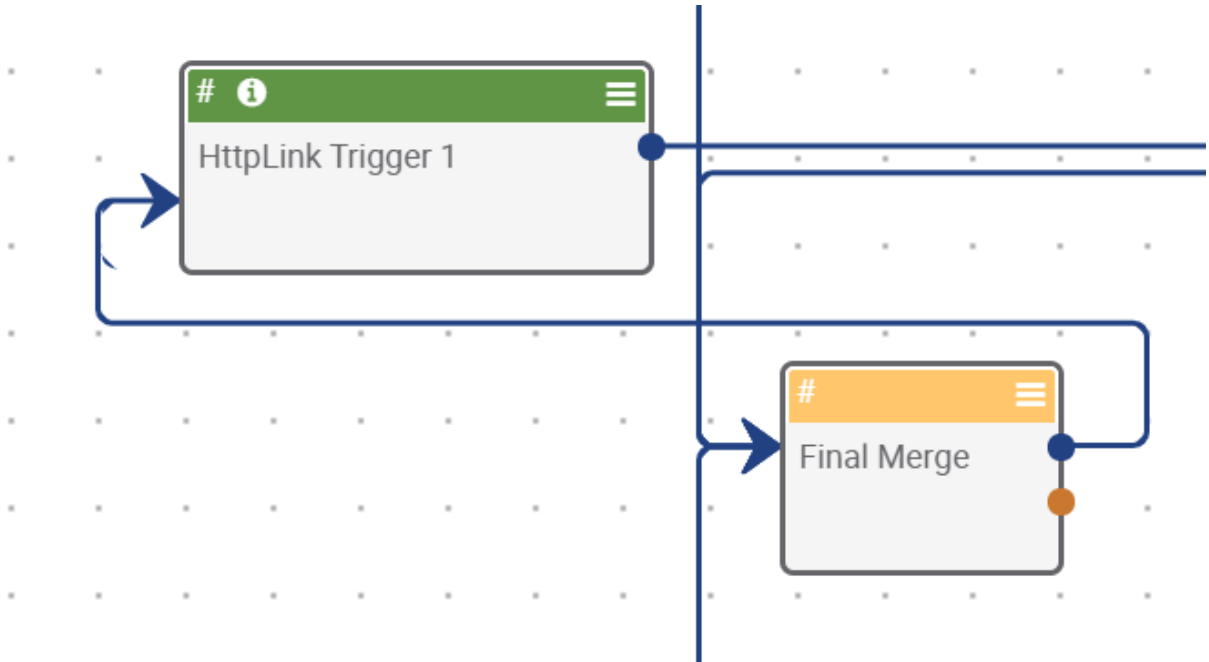
2. If the number of records of 'Whols Data' is greater than zero
 - The Playbook will have the success path (which represents as a blue arrow path) and logs the whols Historic data in a logger App 'Phone_whols_Data_Logger'
 - If no records are returned from the 'whols Historic Data', it will have the failed path (orange arrow) and logs the error in logger App 'Phone_whols_Error'
 - The Merge data from whols Historic Data is logged into Logger App named as 'Phone_whols_Data_Merger' as shown below.



3. The merged output is being logged in one single place as 'Phone_All_Data' Logger Utility App.
4. For beautification of the data, we have used the "Find and Replace" Apps named as Phone_beautify_step1, Phone_beautify_step2 and Phone_beautify_step3, to format the output from merge logger as shown below.

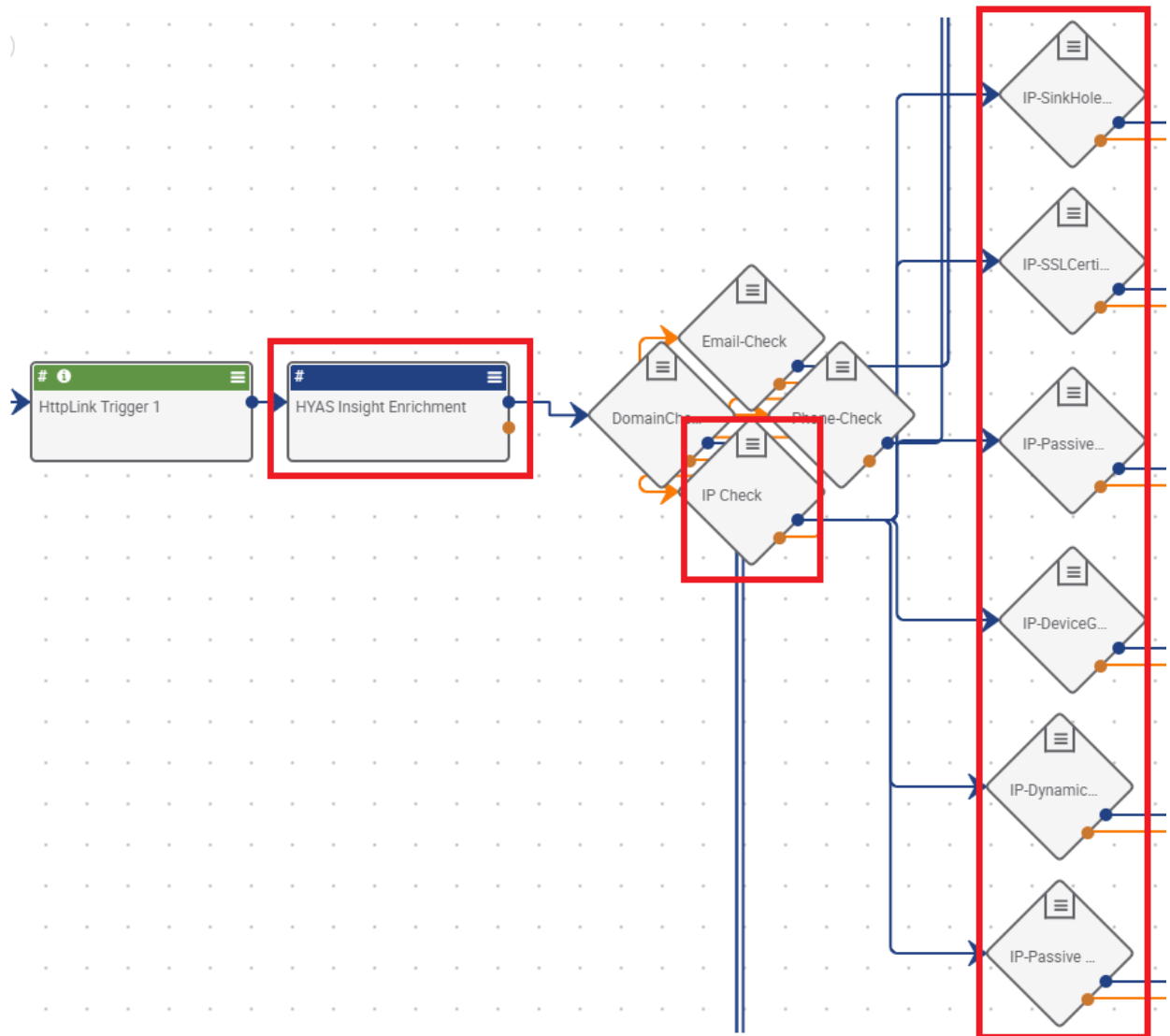


5. The Phone Number Enrichment output from the Merge operator named as "Final Merge" is given to 'HttpLink Trigger'. The output can be visible, which is displayed in the body, after activating the Playbook and executing the Endpoint.

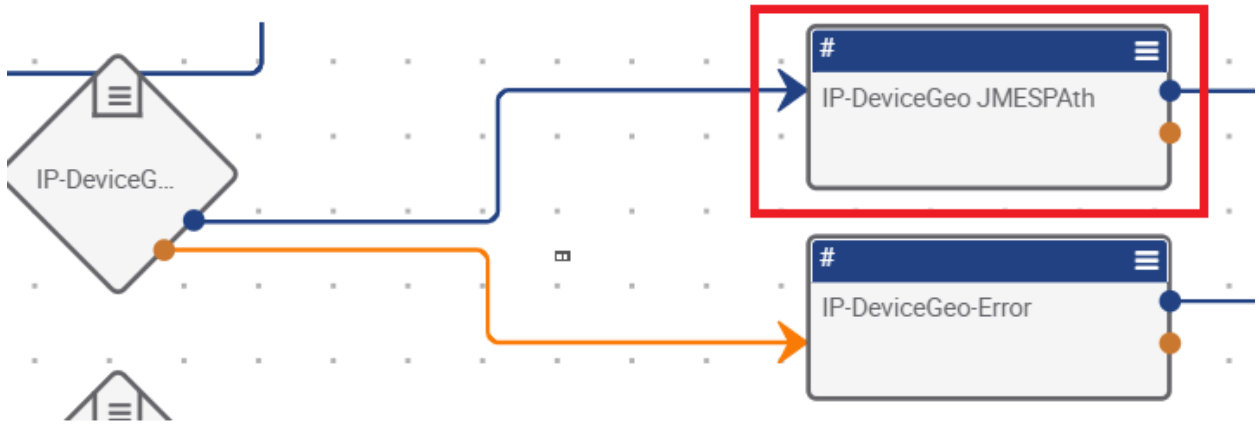


IP Address Enrichment Flow:

- Check if the Enrichment type selected is "IP Address".
- Check if Sinkhole records are greater than "0".
- Check if SSL_Certificate records are greater than "0".
- Check if Passive Hash records are greater than "0".
- Check if Device Geo records are greater than "0".
- Check if Dynamic DNS records are greater than "0".
- Check if Passive DNS records are greater than "0".



1. Defining the desired attributes needed from the 'device_geo' data using the 'JMESPATH' Utility App 'IP-DeviceGeo JMESPath'.



+ TRIGGER

+ APP

+ OPERATOR

Edit App

Display Notes ☐



JMESPath

Job Name *

IP-DeviceGeo JMESPath

JSON Data *

#hy.devicegeo.json.raw ✕

JMESPath String Expressions

Key	Value

+

Key	Value	
IP_DeviceGeo_Data	[].[datetime,device_geo_id,latitude,longitude]	

☒ Strip Quotes from String Output

JMES Path StringArray Expressions

Key	Value

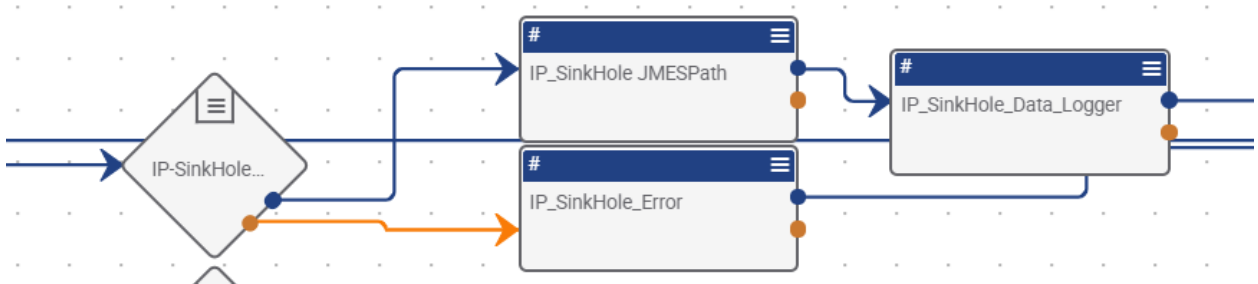
+

CANCEL

SAVE

- If the number of records of Device Geo Data is greater than zero
 - The Playbook will have the success path (which represents as a blue arrow path) and logs the Device Geo data in a Logger Utility App 'IP_DeviceGeo_Data_Logger'.
 - If no records are returned from the 'Device Geo Data', it will have the failed path (orange arrow) and logs the error in 'Device Geo Error Logger'.
 - Both success and failed Logger outputs are merged in the 'Merge' operator named as 'IP_DeviceGeo_Merge'.

3. Defining the desired attributes needed from the 'sinkhole' data using the 'JMESPATH' Utility App 'IP_SinkHole JMESPath'.



+ TRIGGER

+ APP

+ OPERATOR

Edit App

Display Notes ☐

JMESPath

Job Name *

IP_SinkHole JMESPath

JSON Data *

#hy.sinkhole.json.raw ✕

JMESPath String Expressions

Key Value +

Key	Value	
IP_SinkHole_Data	[. [country_name,datetime,last_seen,organization_name,sink_source]	

☒ Strip Quotes from String Output

JMES Path StringArray Expressions

Key Value +

CANCEL

SAVE

4. If the number of records of Sinkhole Data is greater than zero
 - The Playbook will have the success path (which represents as a blue arrow path) and logs the Sinkhole data in a Logger Utility App 'IP_SinkHole_Data_Logger'.
 - If no records are returned from the 'Sinkhole Data', it will have the failed path (orange arrow) and logs the error in 'IP_SinkHole_Error' Logger Utility App.
 - Both success and failed Logger outputs are merged in the 'Merge' operator named as 'IP_SinkHole_Data_Merger'.
5. Defining the desired attributes needed from the 'ssl_certificate' data using the 'JMESPATH' Utility App 'IP-SSL_Certificate JMESPath'.



+
TRIGGER

+
APP

+
OPERATOR

Edit App
Display Notes

JMESPath

Job Name *

IP-SSL_Certificate JMESPath

JSON Data *

#hy.sslcertificate.json.raw

JMESPath String Expressions

Key	Value	
IP_SSL_Certificate_Data	ssl_certs[. [ip,ssl_cert.cert_key,ssl_cert.expire_date,ssl_cert.i ssue_date,ssl_cert.issuer_organizationName]	

☒ Strip Quotes from String Output

JMES Path StringArray Expressions

Key	Value	
-----	-------	--

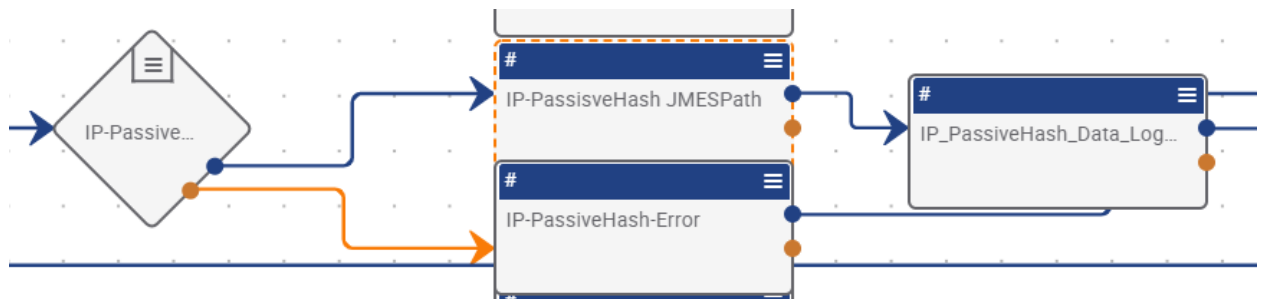
CANCEL

SAVE

6. If the number of records of ssl_certificate Data is greater than zero

- The Playbook will have the success path (which represents as a blue arrow path) and logs the ssl_certificate data in a Logger Utility App 'IP_SSL-Certificate_Data_Logger'.
- If no records are returned from the 'ssl_certificate Data', it will have the failed path (orange arrow) and logs the error in 'IP-SSL_Certificate-Error' Logger Utility App.
- Both success and failed Logger outputs are merged in the 'Merge' operator named as 'IP_SSL-Certificate_Merger'.

7. Defining the desired attributes needed from the 'passivehash' data using the 'JMESPATH' Utility App 'IP-PassiveHash JMESPath'.



+ TRIGGER

+ APP

+ OPERATOR

Edit App

Display Notes ☐



JMESPath

Job Name *

IP-PassiveHash JMESPath

JSON Data *

#hy.passivehash.json.raw ✕

JMESPath String Expressions

Key

Value



Key	Value	
IP_PassiveHash_Data	[][domain,md5_count]	

☒ Strip Quotes from String Output

JMES Path StringArray Expressions

Key

Value

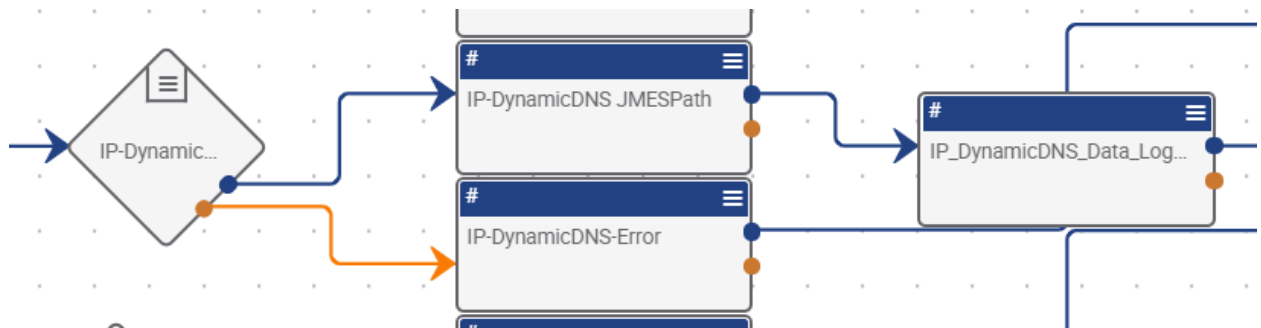


CANCEL

SAVE

8. If the number of records of passive hash Data is greater than zero
- The Playbook will have the success path (which represents as a blue arrow path) and logs the passive hash data in a Logger Utility App 'IP_PassiveHash_Data_Logger'.
 - If no records are returned from the 'passive hash Data', it will have the failed path (orange arrow) and logs the error in 'IP-PassiveHash-Error' Logger Utility App.
 - Both success and failed Logger outputs are merged in the 'Merge' operator named as 'IP_PassiveHash_Merge'.

9. Defining the desired attributes needed from the 'DynamicDNS' data using the 'JMESPATH' Utility App 'IP-DynamicDNS JMESPath'.



+ TRIGGER

+ APP

+ OPERATOR

Edit App

Display Notes ☐

JMESPath

Job Name *

IP-DynamicDNS JMESPath


JSON Data *

#hy.passivedns.json.raw ✕

JMESPath String Expressions

Key	Value

+

Key	Value	
IP_DynamicDNS_Data	[. [a_record,account,created,created_ip,domain,email]	

☒ Strip Quotes from String Output

JMES Path StringArray Expressions

Key	Value

+

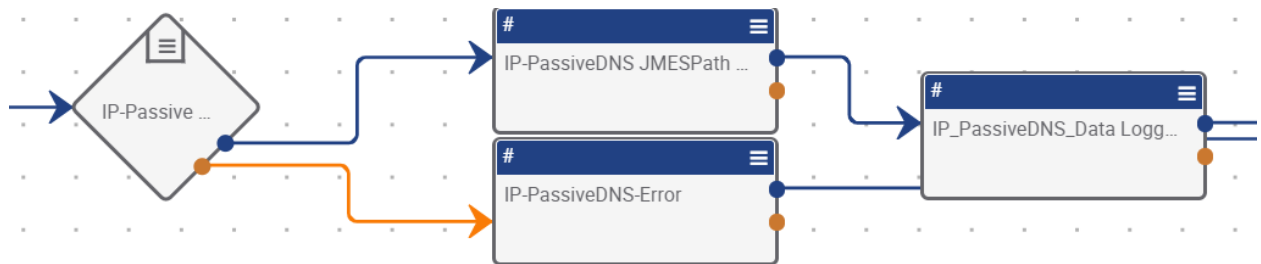
CANCEL

SAVE

10. If the number of records of DynamicDNS Data is greater than zero

- The Playbook will have the success path (which represents as a blue arrow path) and logs the DynamicDNS data in a Logger Utility App 'IP_DynamicDNS_Data_Logger'.
- If no records are returned from the 'DynamicDNS Data', it will have the failed path (orange arrow) and logs the error in 'IP-DynamicDNS-Error' Logger Utility App.
- Both success and failed Logger outputs are merged in the 'Merge' operator named as 'IP_DynamicDNS_Merger'.

11. Defining the desired attributes needed from the 'PassiveDNS' data using the 'JMESPATH' Utility App 'IP-PassiveDNS JMESPath'.



+ TRIGGER

+ APP

+ OPERATOR

Edit App

Display Notes ☐

JMESPath

Job Name *

IP-PassiveDNS JMESPath Data

JSON Data *

#hy.passivedns.json.raw *

JMESPath String Expressions

Key	Value

+

Key	Value	
IP_PassiveDNS_Data	[.ipv4,first_seen,last_seen,ip.geo.city_name,ip.geo.country_name]	

☒ Strip Quotes from String Output

JMES Path StringArray Expressions

Key	Value

+

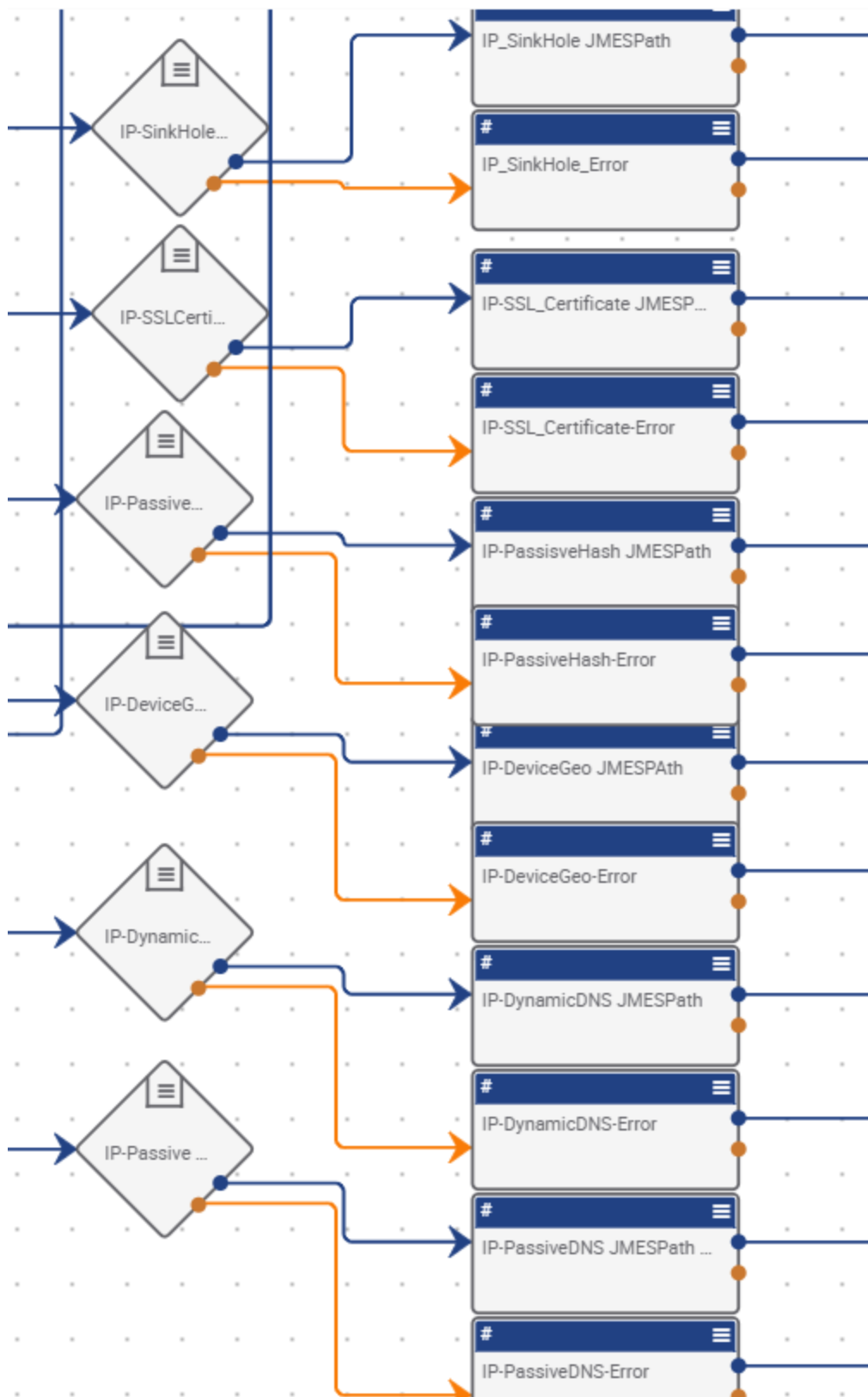
CANCEL

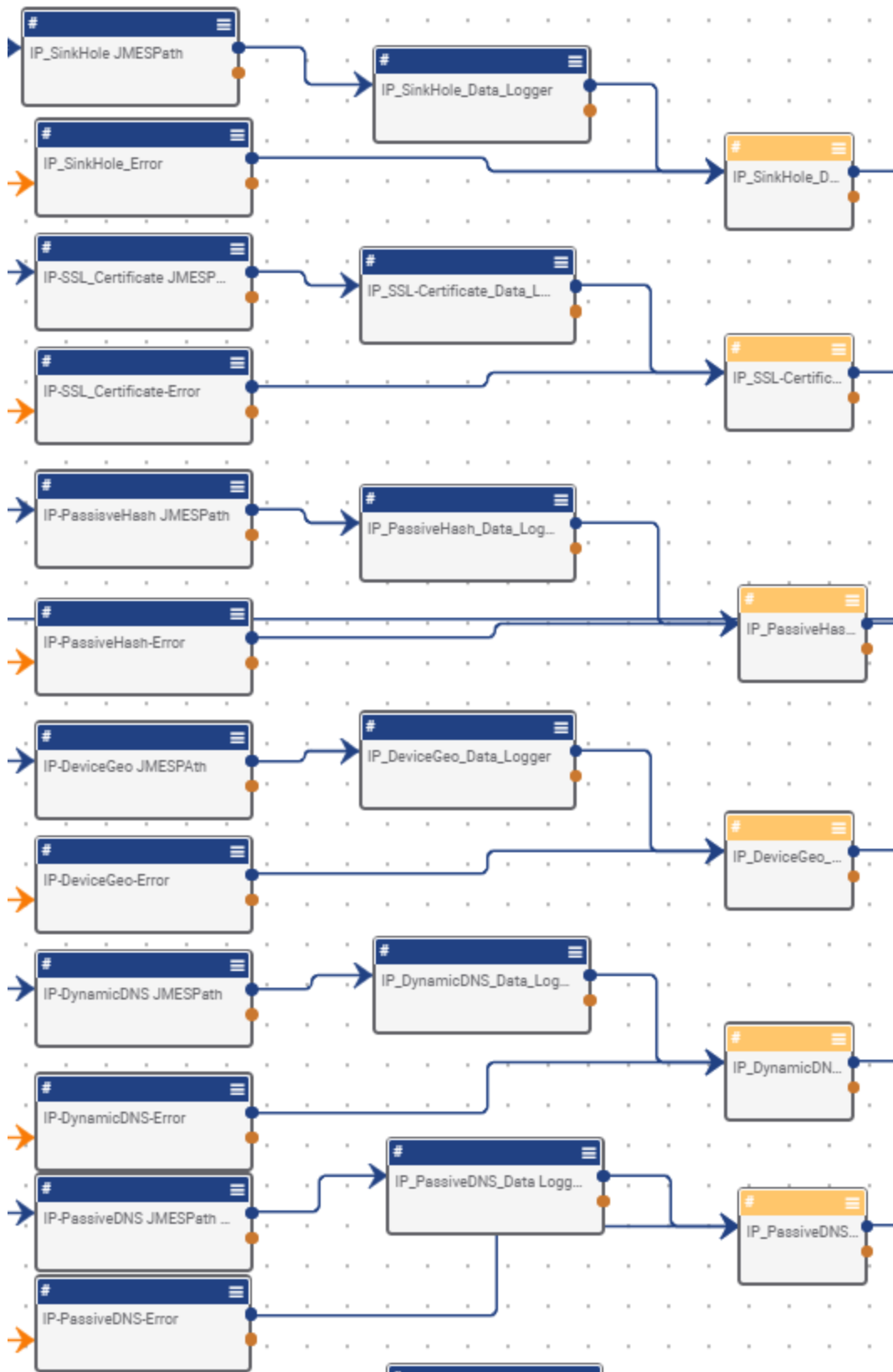
SAVE

12. If the number of records of PassiveDNS Data is greater than zero

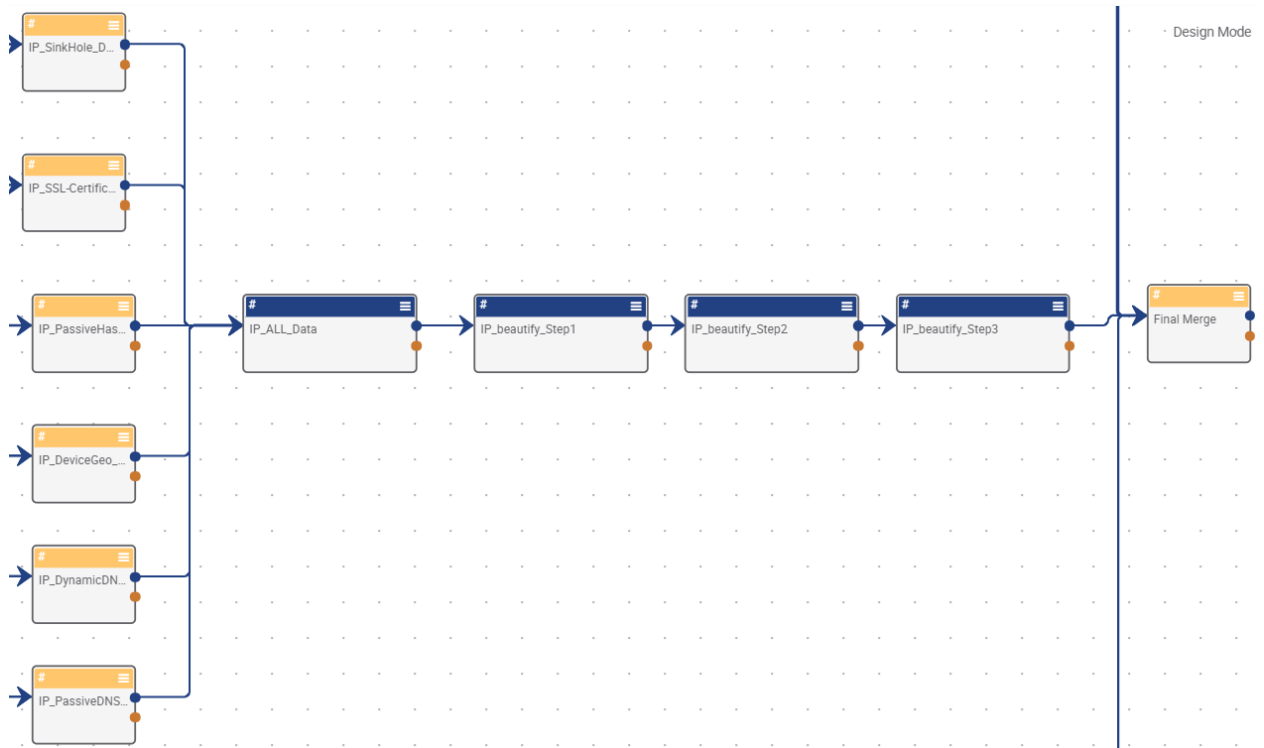
- The Playbook will have the success path (which represents as a blue arrow path) and logs the PassiveDNS data in a Logger Utility App 'IP_PassiveDNS_Data Logger'.
- If no records are returned from the 'PassiveDNS Data', it will have the failed path (orange arrow) and logs the error in 'IP-PassiveDNS-Error' Logger Utility App.
- Both success and failed Logger outputs are merged in the 'Merge' operator named as 'IP_PassiveDNS_Merge'.

13. The final structure of the IP Address Enrichment is shown below:



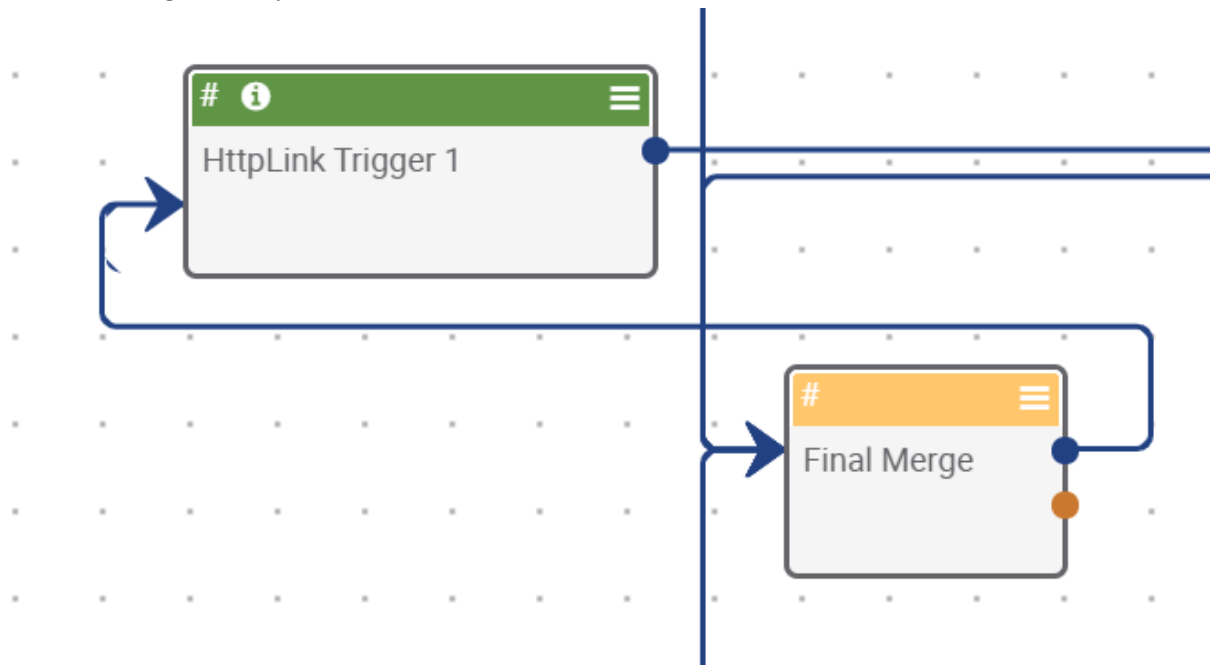


14. The merged output is being logged in one single place as 'IP_ALL_Data' Logger Utility App and make some beautification by using 'Find and Replace' Utility App names as 'IP_beautify_Step1', 'IP_beautify_Step2' and 'IP_beautify_Step3' to format the output from merge logger as shown below.

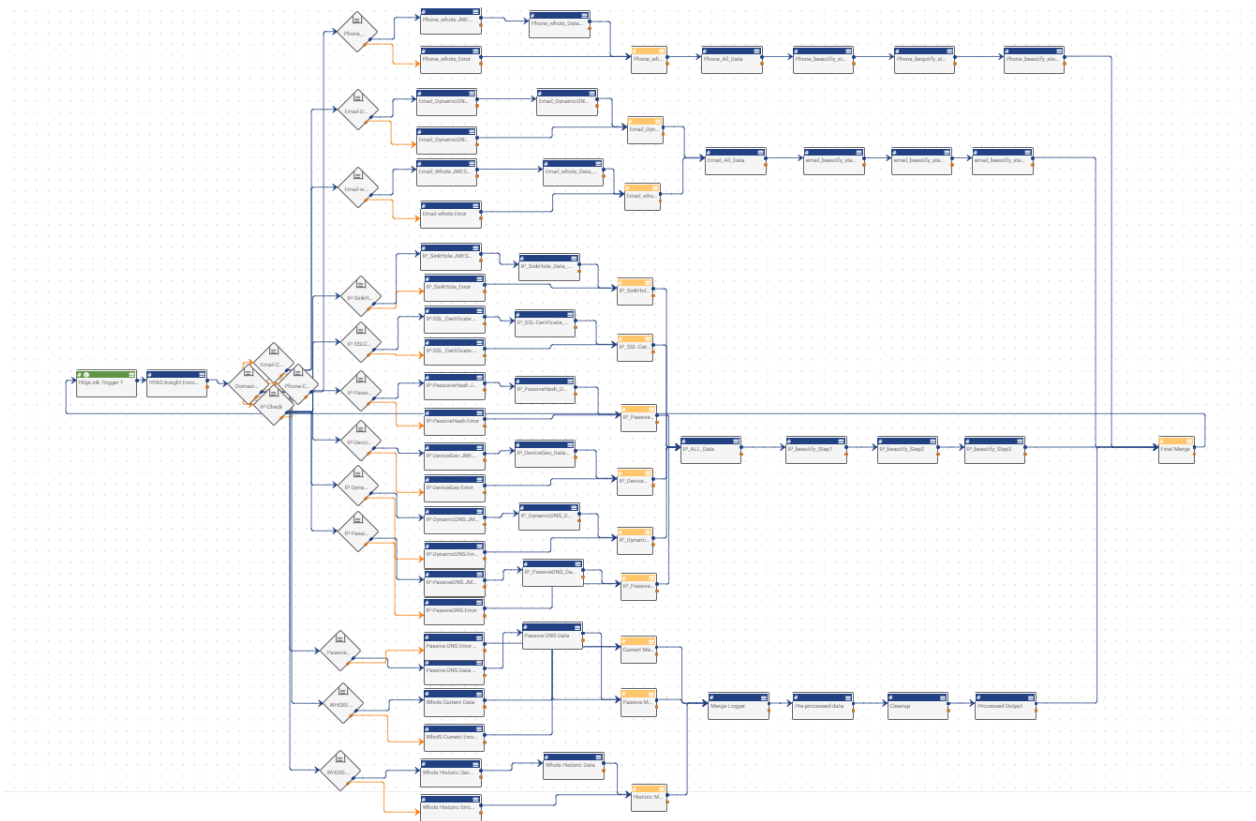


15. The IP Enrichment output from the Merge operator named as "Final Merge" is given to 'HttpLink Trigger'. The output can be visible, which is displayed in the body, after activating the Playbook

and executing the Endpoint.



At last the playbook will look as below:



4. Support

For assistance with this App, to report a bug, or feature requests please contact us via the webpage <https://www.hyas.com/contact> or via email at support@hyas.com.