USER GUIDE v1.0.0

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 and WhoIs endpoints using the HYAS Enrichment source

1. Configuration

1.1. Requirement

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

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

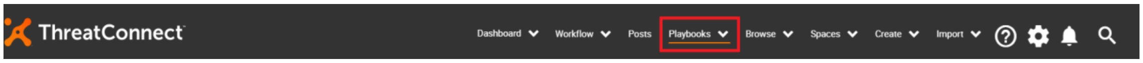
1.2. App Installation

HYAS 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.

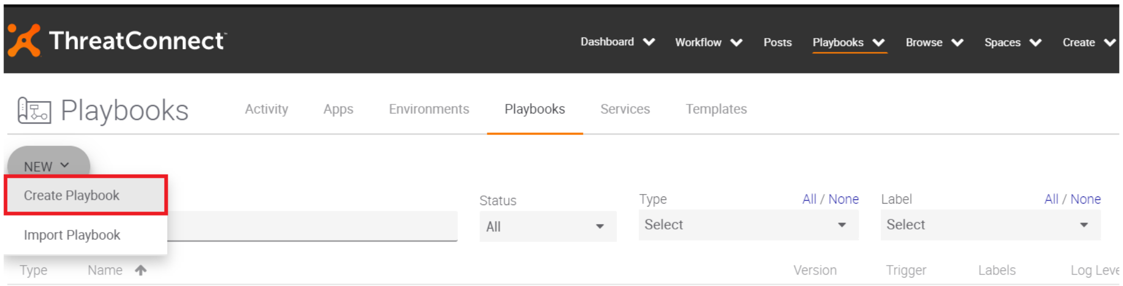
1.3. App Configuration

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

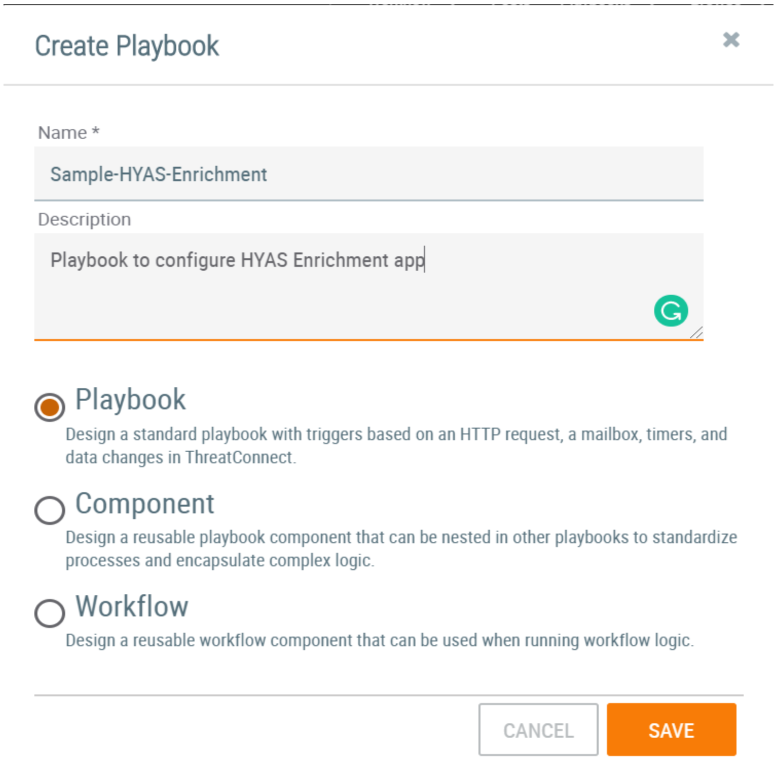
1. Click on **Playbooks** on the top menu-bar to go to the Playbooks page.



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-Enrichment

Description

Playbook to configure HYAS Enrichment app

● Playbook

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

○ Component

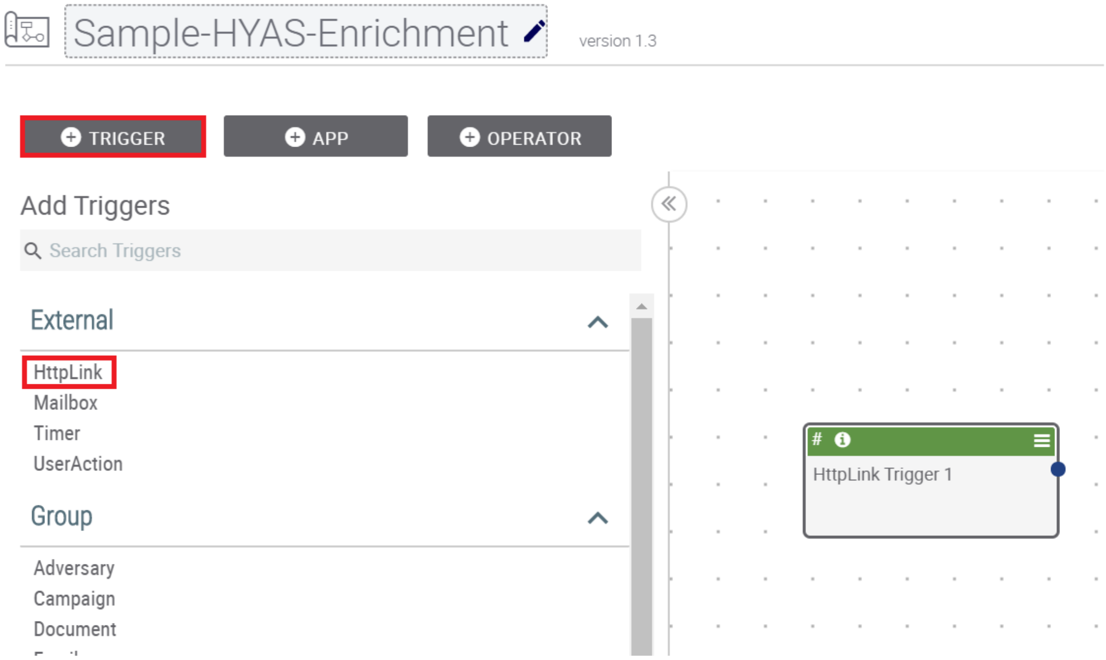
Design a reusable playbook component that can be nested in other playbooks to standardize processes and encapsulate complex logic.

○ Workflow

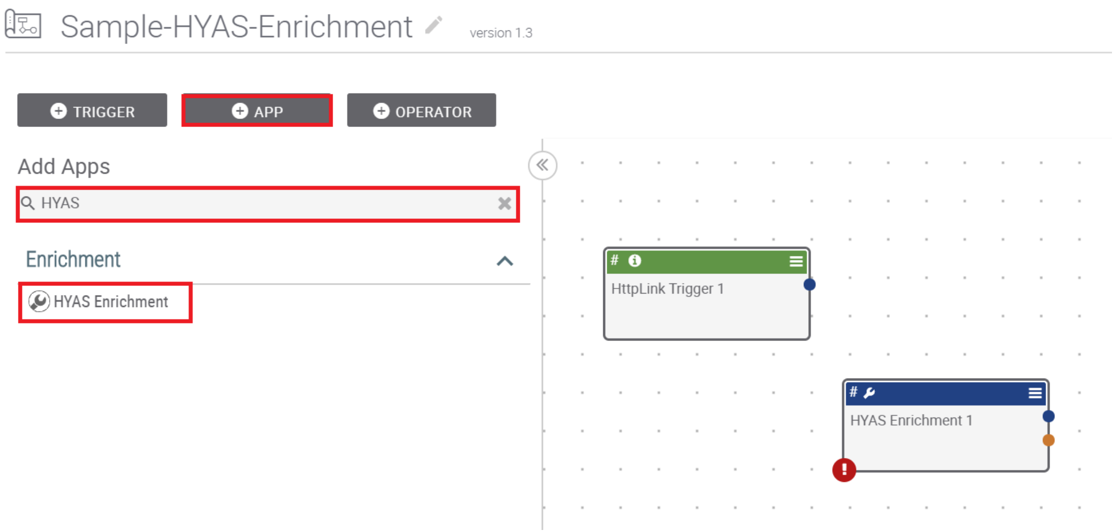
Design a reusable workflow component that can be used when running workflow logic.

CANCEL SAVE

4. In order 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.



5. 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 of HYAS Apps in the ThreatConnect Platform and choose the **HYAS Enrichment** App.



Sample-HYAS-Enrichment version 1.3

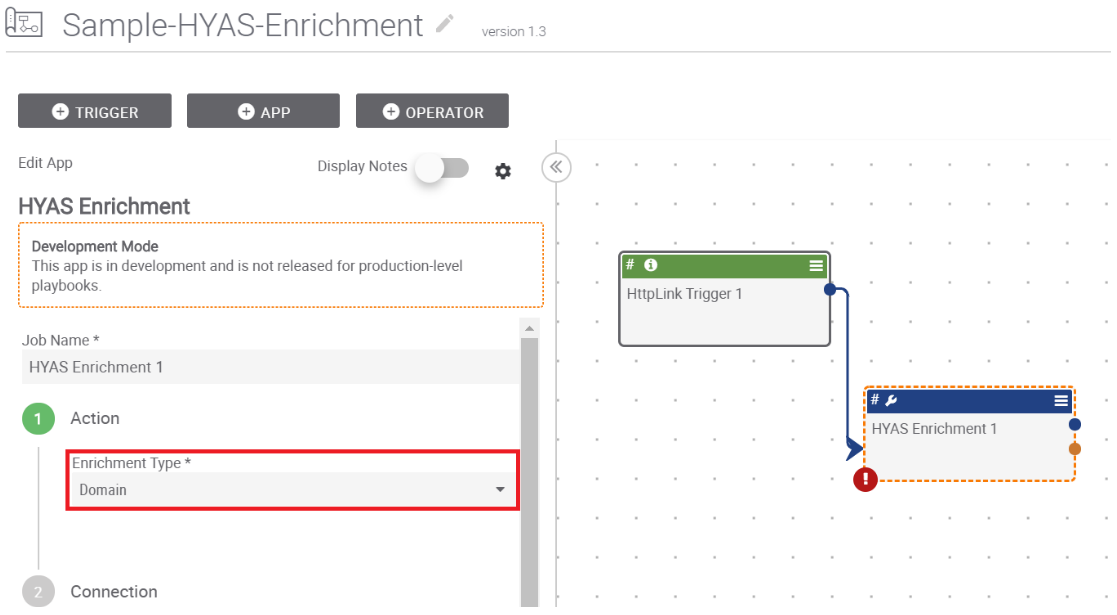
Add Apps

HYAS

Enrichment

HYAS Enrichment

6. 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 Enrichment** has three configuration steps. The **Action** step is used to select one of the HYAS Enrichment Type, Domain is default indicator selected.



Sample-HYAS-Enrichment version 1.3

Edit App

Display Notes

HYAS Enrichment

Development Mode
This app is in development and is not released for production-level playbooks.

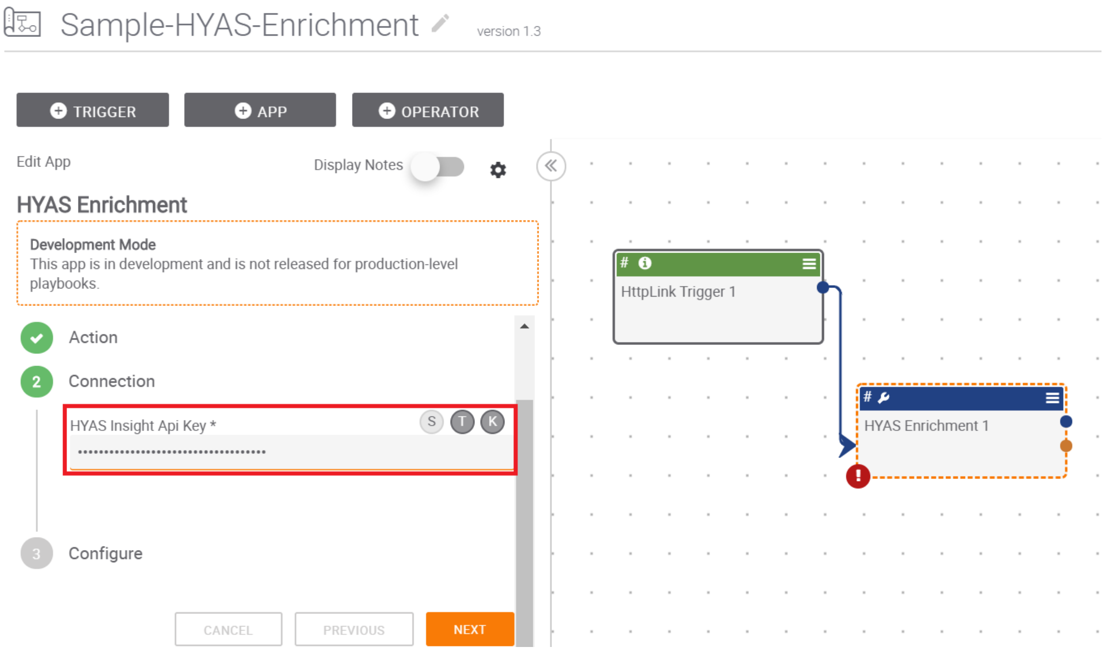
Job Name *
HYAS Enrichment 1

1 Action

Enrichment Type *
Domain

2 Connection

7. 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** text-box.

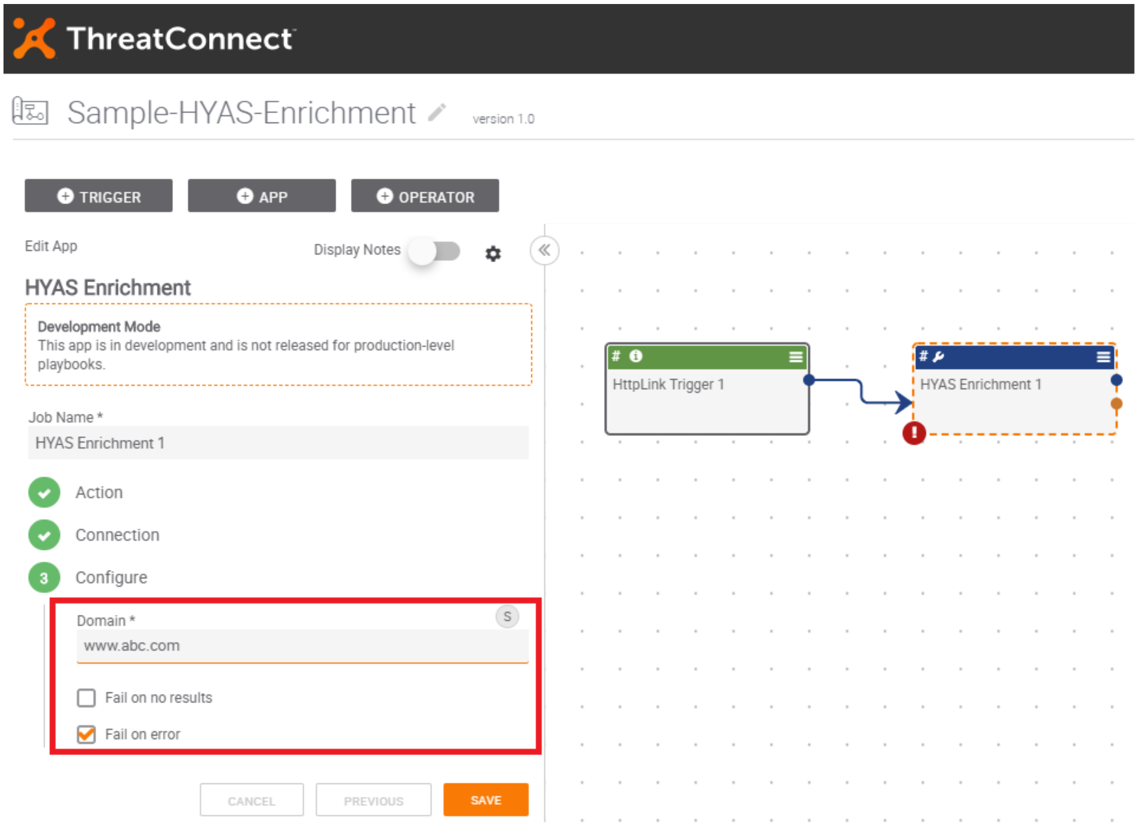


HYAS Enrichment

Development Mode
This app is in development and is not released for production-level playbooks.

HYAS Insight Api Key *
••••••••••••••••••••••••••••••••••••

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



ThreatConnect

Sample-HYAS-Enrichment version 1.0

Edit App

HYAS Enrichment

Development Mode
This app is in development and is not released for production-level playbooks.

Job Name *
HYAS Enrichment 1

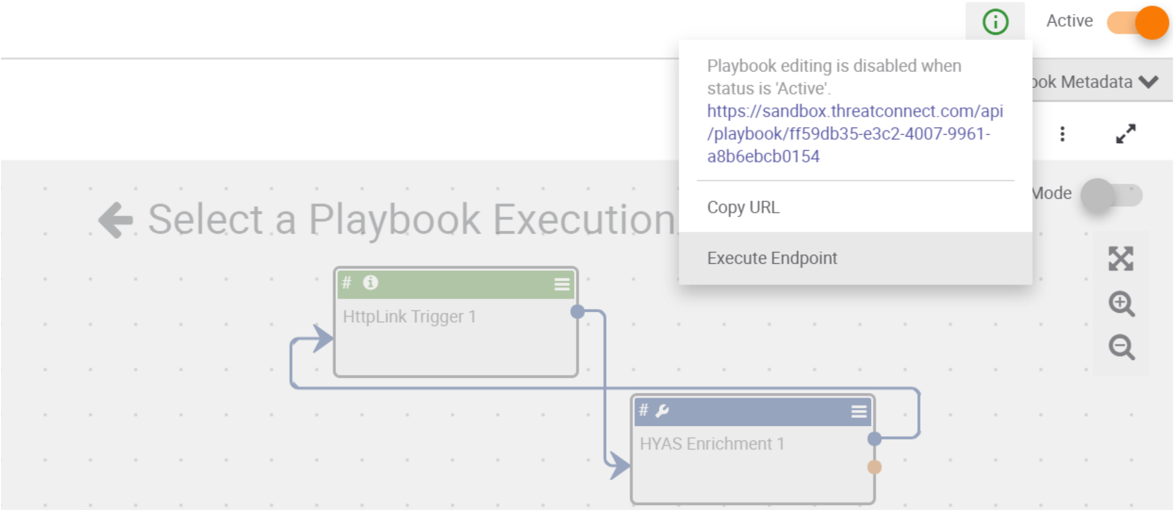
✓ Action
✓ Connection
3 Configure

Domain *
www.abc.com

☐ Fail on no results

☑ Fail on error

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 in order to trigger the Playbook to run. Optionally, you can click on **Execute Endpoint** menu-item to do this automatically.



Playbook editing is disabled when status is 'Active'.
https://sandbox.threatconnect.com/api/playbook/ff59db35-e3c2-4007-9961-a8b6ebcb0154

2. Outputs

Output	TC Type	Description
hy.passivedns.json.raw	String	Raw response object from HYAS Insight API for debugging purposes
hy.passivedns.json.raw.count	String	Raw Number of records from HYAS Insight API for debugging purposes
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 for debugging purposes
hy.whois.current.json.raw.count	String	Raw Number of records from HYAS Insight API for debugging purposes
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 for debugging purposes
hy.whois.historic.json.raw.count	String	Raw Number of records from HYAS Insight API 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”",”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

.

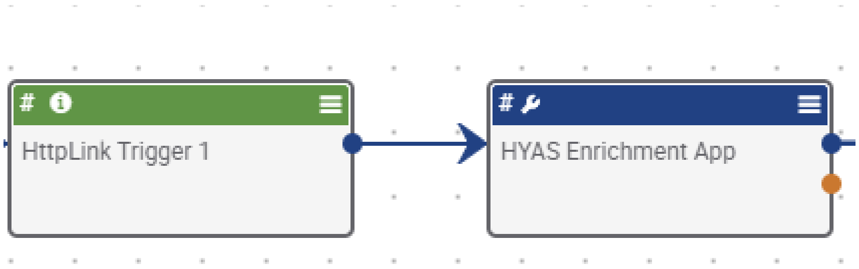
3. Sample Playbook Example

You can find the sample Playbook example “HYAS Enrichment Playbook Template” available on GitHub.

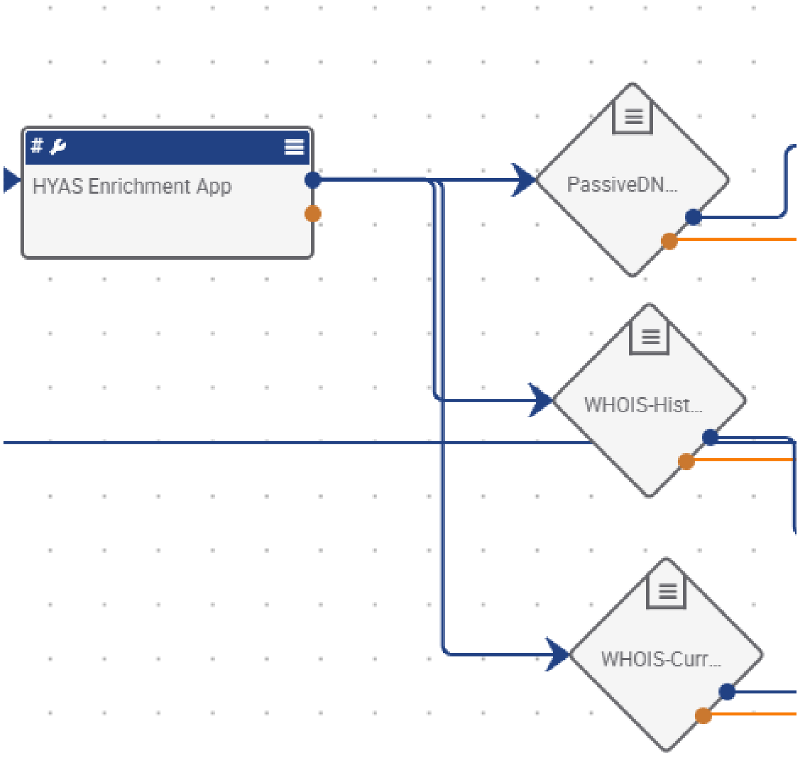
To install this Playbook Example, visit the Playbooks tab within the ThreatConnect Platform. Select New > Import and locate the PBX file you wish to add to your system. Follow the on-screen instructions to complete the import.

Steps Explained Below:

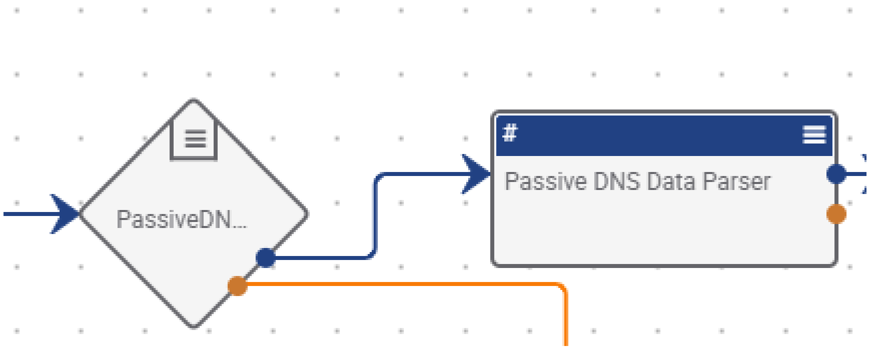
1. Use the ‘Httplink Trigger’ and configure the ‘HYAS Enrichment’ App from the Trigger and APP section respectively.

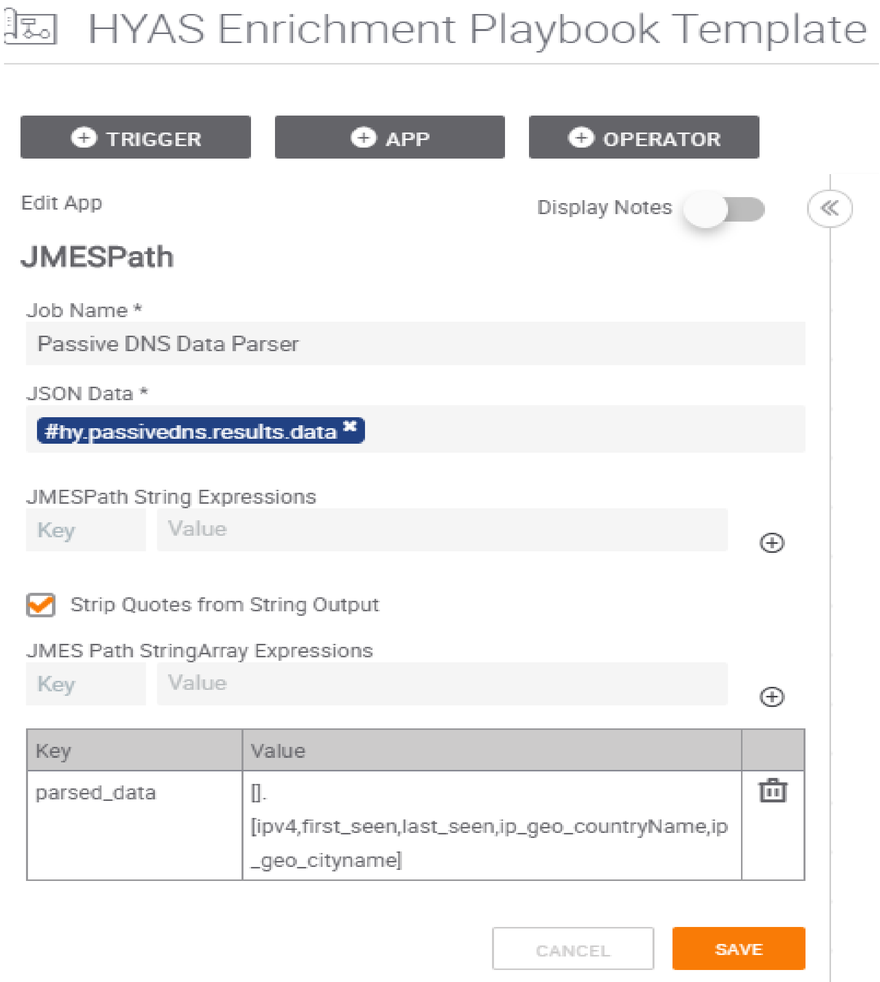


2. Check for the records present in the Passive DNS and WhoIs (Historic/Current) endpoints in the below step:



3. Selection of specific attributes form the Passive DNS endpoint using the ‘JMESPATH’ App which is named as ‘Passive DNS Data Parser' here.





HYAS Enrichment Playbook Template

Edit App

Display Notes

JMESPath

Job Name *
Passive DNS Data Parser

JSON Data *
#hy.passivedns.results.data

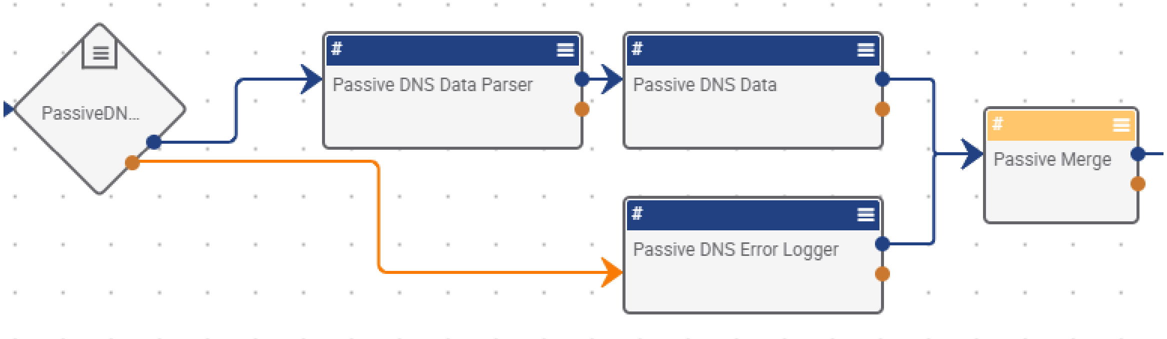
JMESPath String Expressions
Key Value

☑ Strip Quotes from String Output

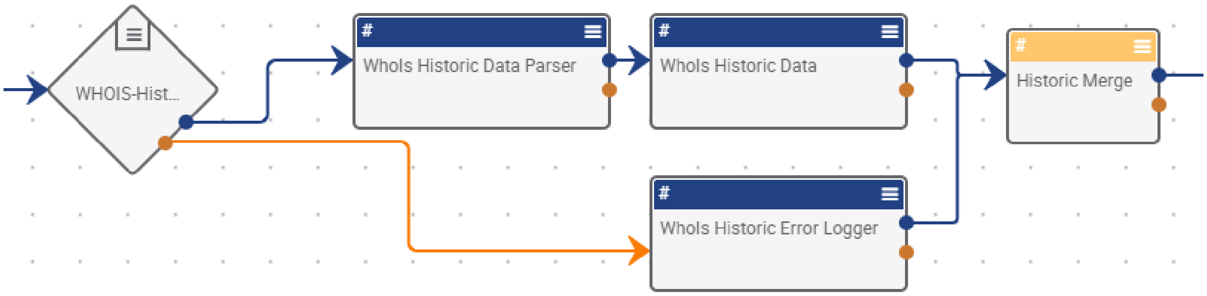
JMES Path StringArray Expressions
Key Value

Key	Value	
parsed_data	[].[ipv4,first_seen,last_seen,ip_geo_countryName,ip_geo_cityname]	

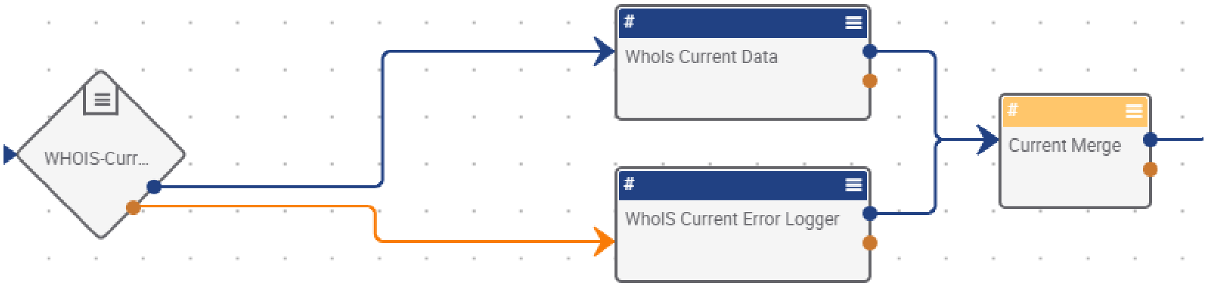
4. If the number of records of ‘Passive DNS Data' is greater than zero, then this Playbook should follow success path (which represents as a blue arrow path) and logs the data in a ‘logger’ App named ‘Passive DNS Data', else it will follow the failed output path (orange arrow) and logs the error in ‘Passive DNS Error Logger’and both Logger outputs are merged in the ‘Merge' operator name here as ‘Passive Merge'.



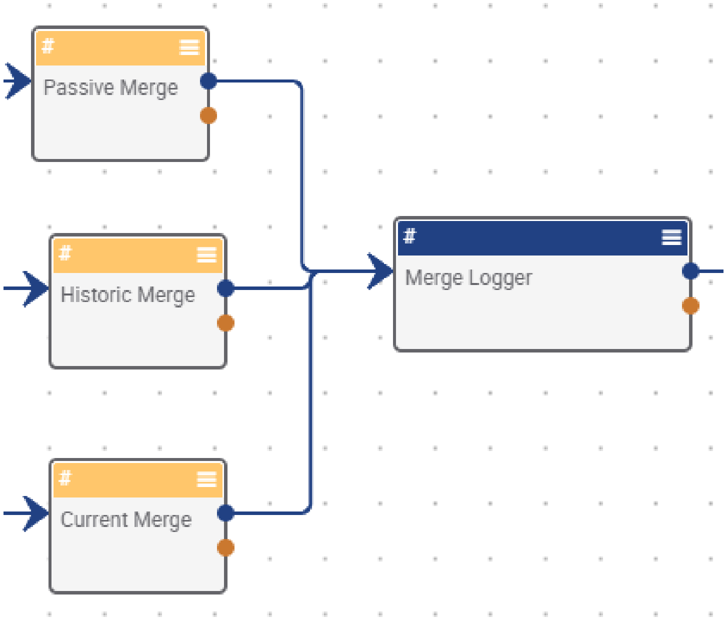
5. In the same way mentioned in the step number 3 & 4, ‘WhoIS Historic Data' is configured as below:



6. If the number of records of ‘WhoIs Current Data' is greater than zero , then this Playbook should follow success path (which represents as a blue arrow path) and logs the data in a ‘logger’ App named ‘WhoIs Current Data', else it will follow the failed output path (orange arrow) and logs the error in ‘WhoIs Current Error Logger’and both Logger outputs are merged in the ‘Merge' operator name here as ‘Current Merge'.

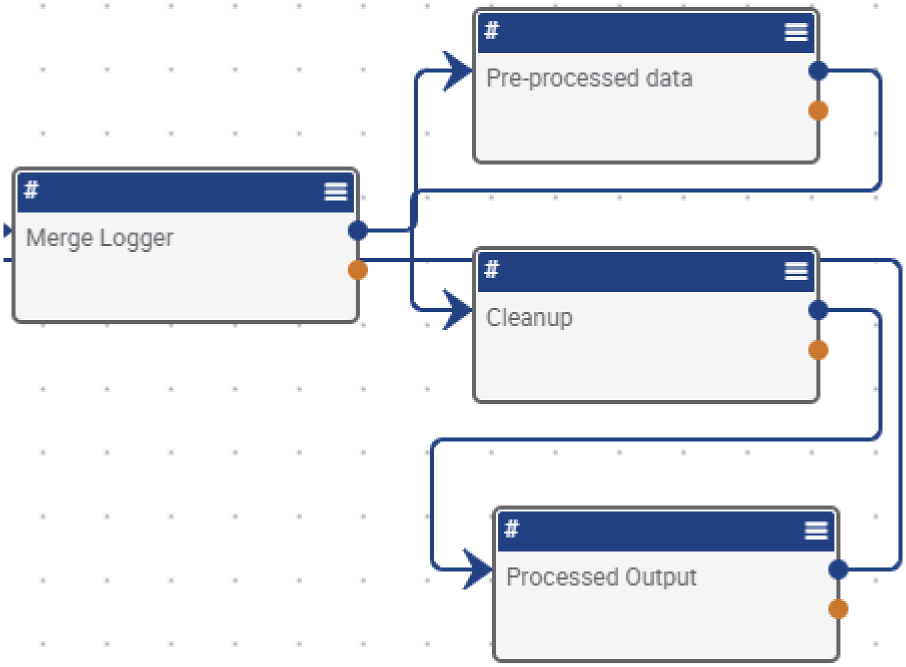


7. The Merge data from all the three endpoints (PassiveDNS/WhoIS Historic/WhoIs Current) is logged into Logger App named as ‘Merge Logger' as below:

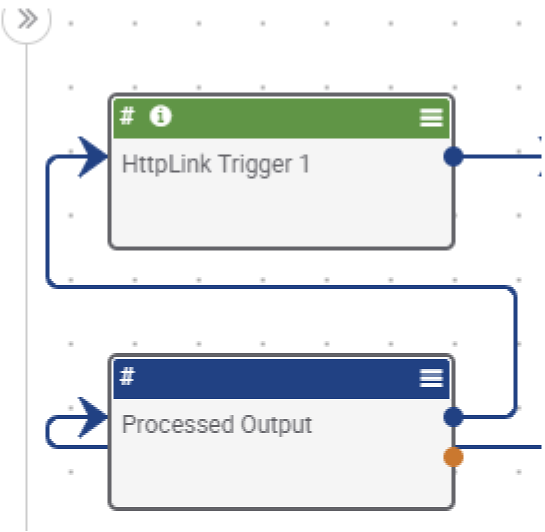


8. Used the “Find and Replace” Apps named as Pre-processed data, Clean-up and Processed output, to format the output from merge logger.

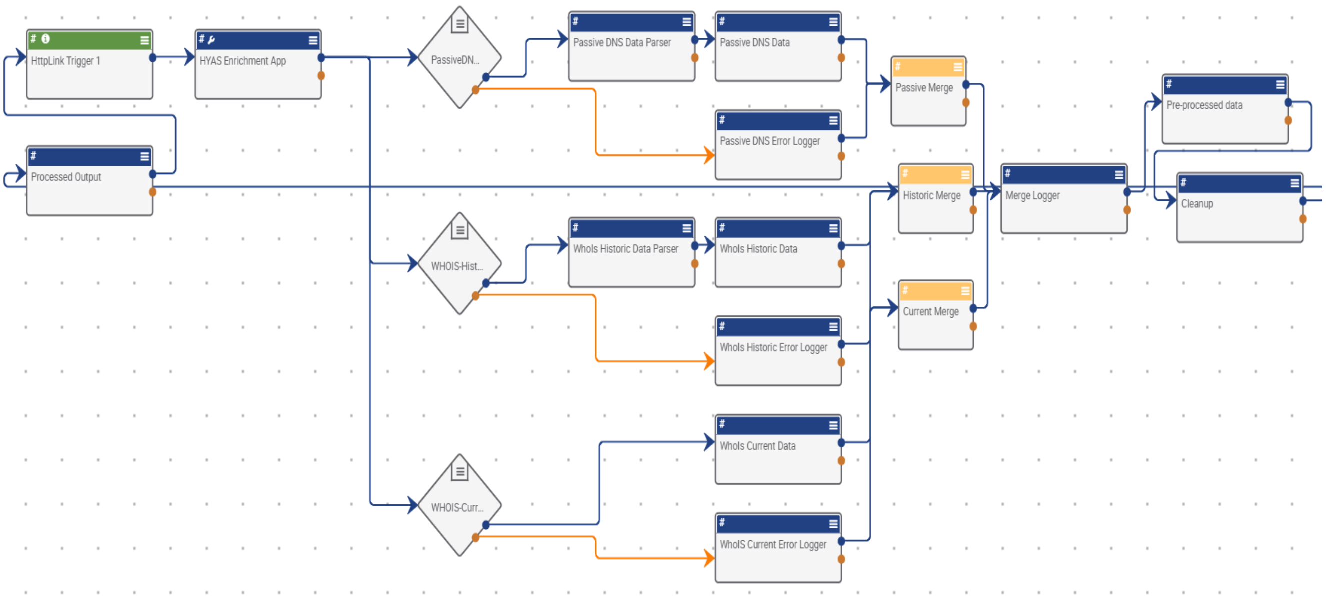
Note: A user can modify and format the output according to the business needs.



9. The output from the “Find and Replace” App named as Processed output is given to ‘HttpLink Trigger'. The output can be visible, which is displayed in the body, after activating the Playbook and executing the Endpoint.



10. The Playbook template looks as below:



4. Support

For assistance with this App, to report a bug, or feature requests please contact us at https://www.hyas.com/contact