HYAS™ Insight Enrichment Integration Guide ThreatConnect Platform

User Guide v2.0.0

Contents

1. Introduction

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, whoIs and C2 Attribution endpoints using the HYAS Insight Enrichment source.

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

2. HYAS Insight Enrichment App Configuration

2.1 HYAS Insight Enrichment App 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)

2.2 HYAS Insight Enrichment App Installation

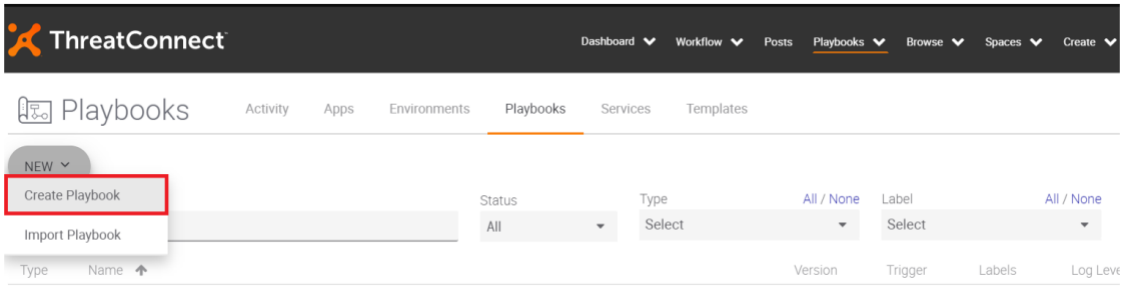
HYAS Insight Enrichment App for ThreatConnect is available on GitHub.
Download the App package with tcx extension and install it in your instance. For installation instructions, refer to the ThreatConnect System Administration Guide (Install an App). For more information, contact your ThreatConnect Customer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

2.3 HYAS Insight Enrichment App Configuration

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

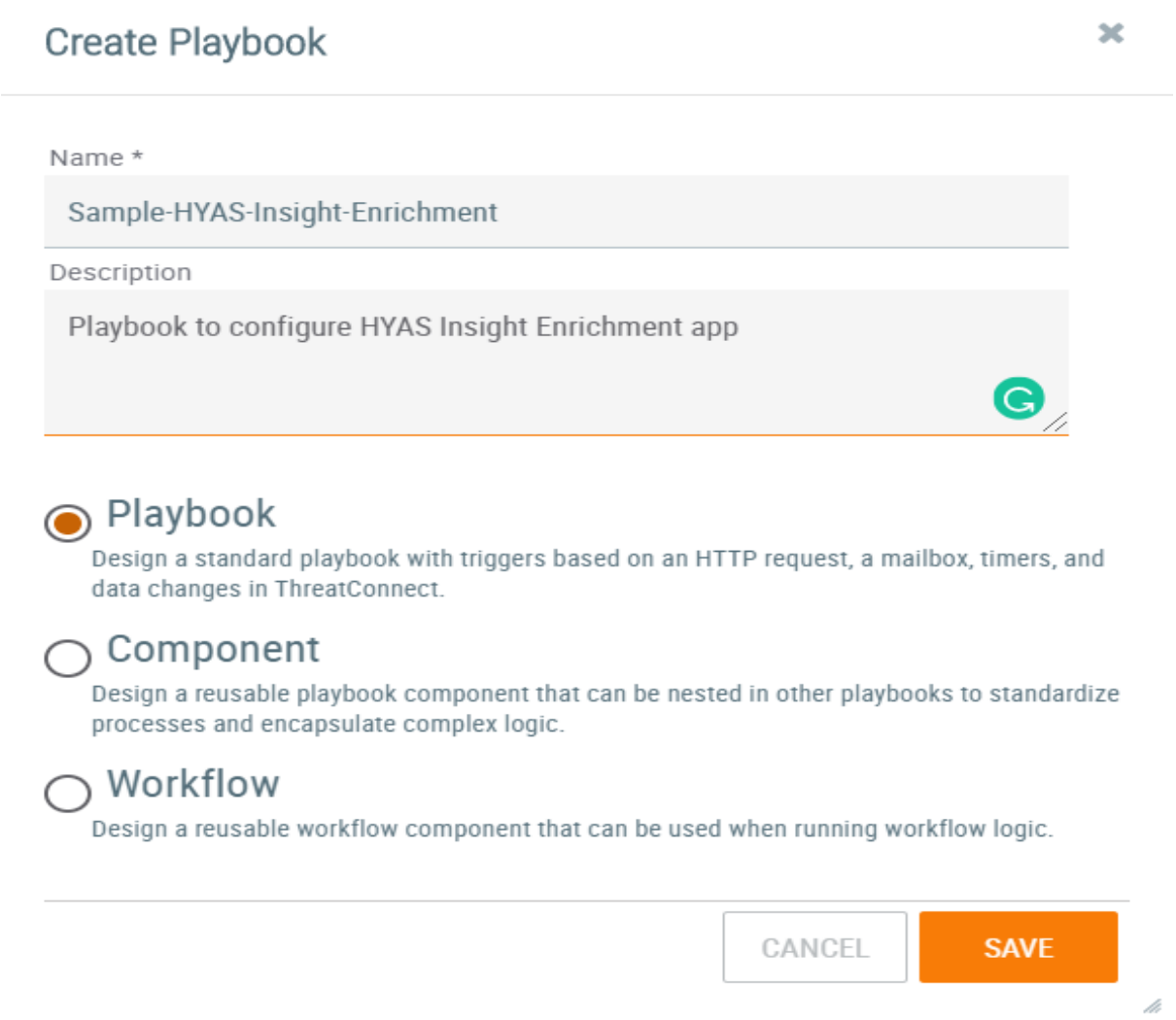
1. Click on **Playbooks** on the top menu-bar to go to the Playbooks page.

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.

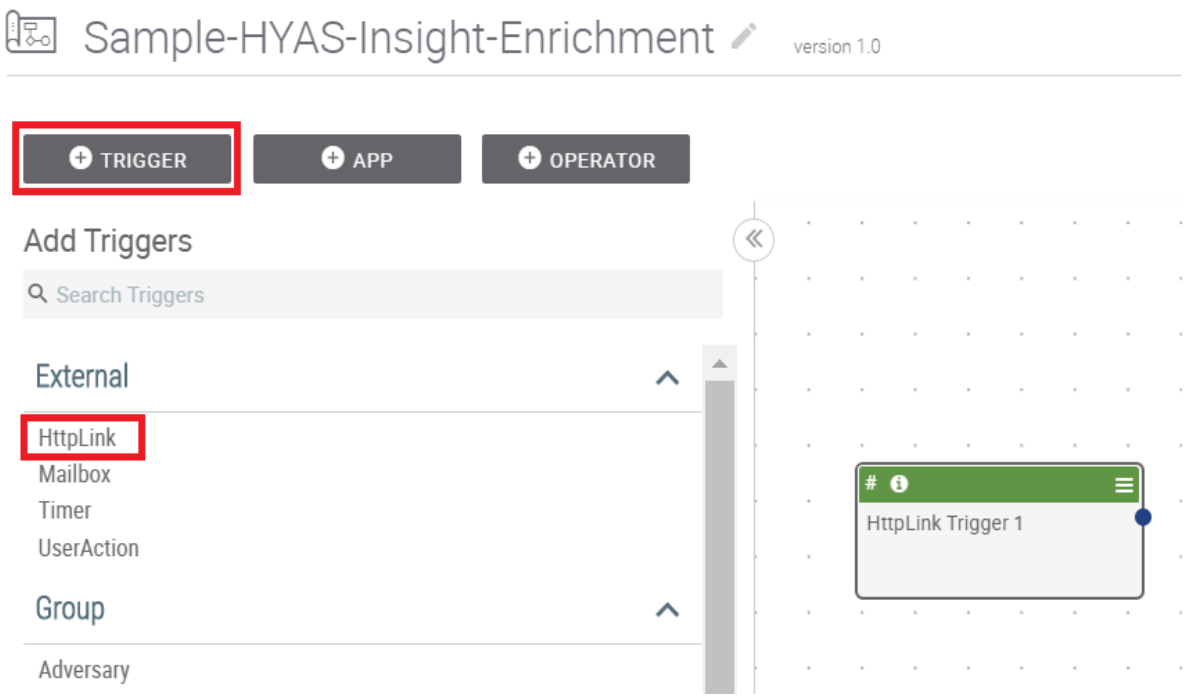


3. The **Create Playbook** dialog box will appear. Choose a suitable **Name** and **Description** for the sample Playbook and click **Save**. The page will then automatically redirect you to the Playbook

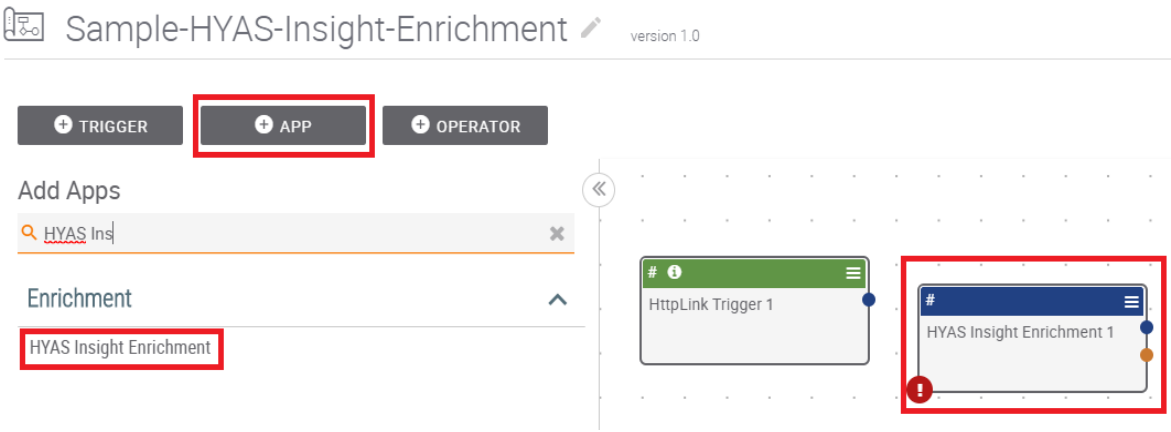
editor.



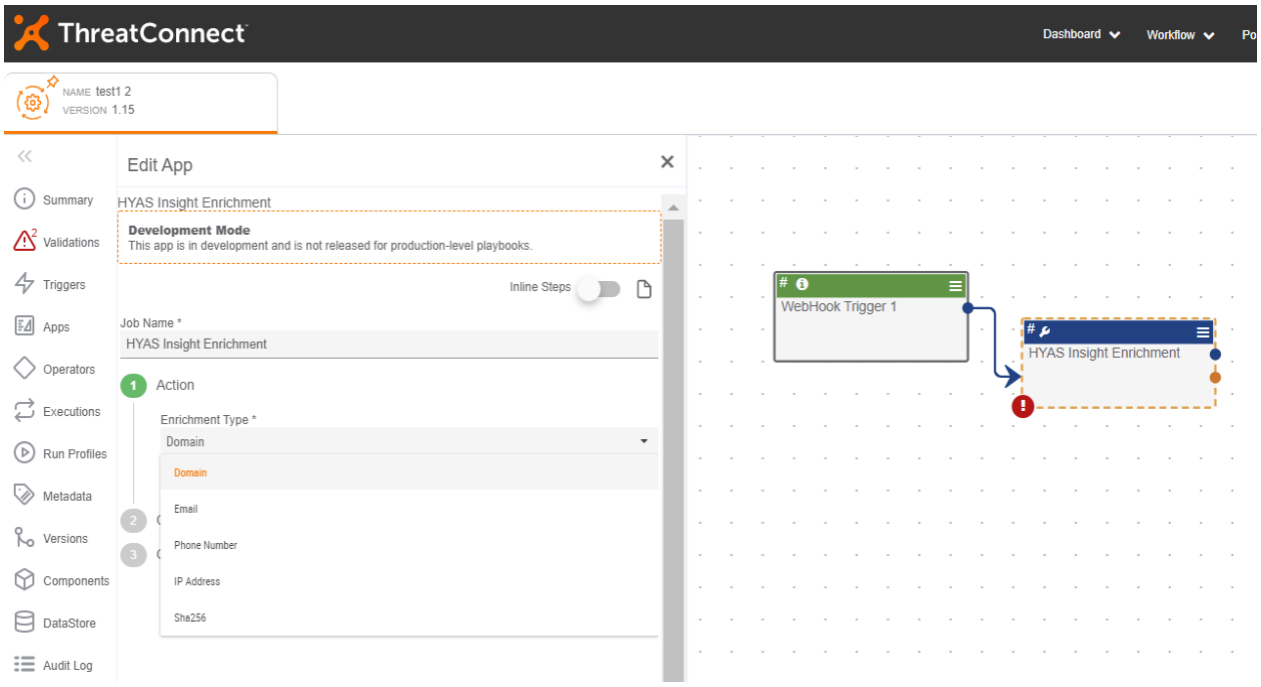
4. To test the App, you can use a Trigger block to trigger the App to run. Click on + **TRIGGER** button and select **HttpLink**. This will provide you with an endpoint URL to signal the Playbook to run.



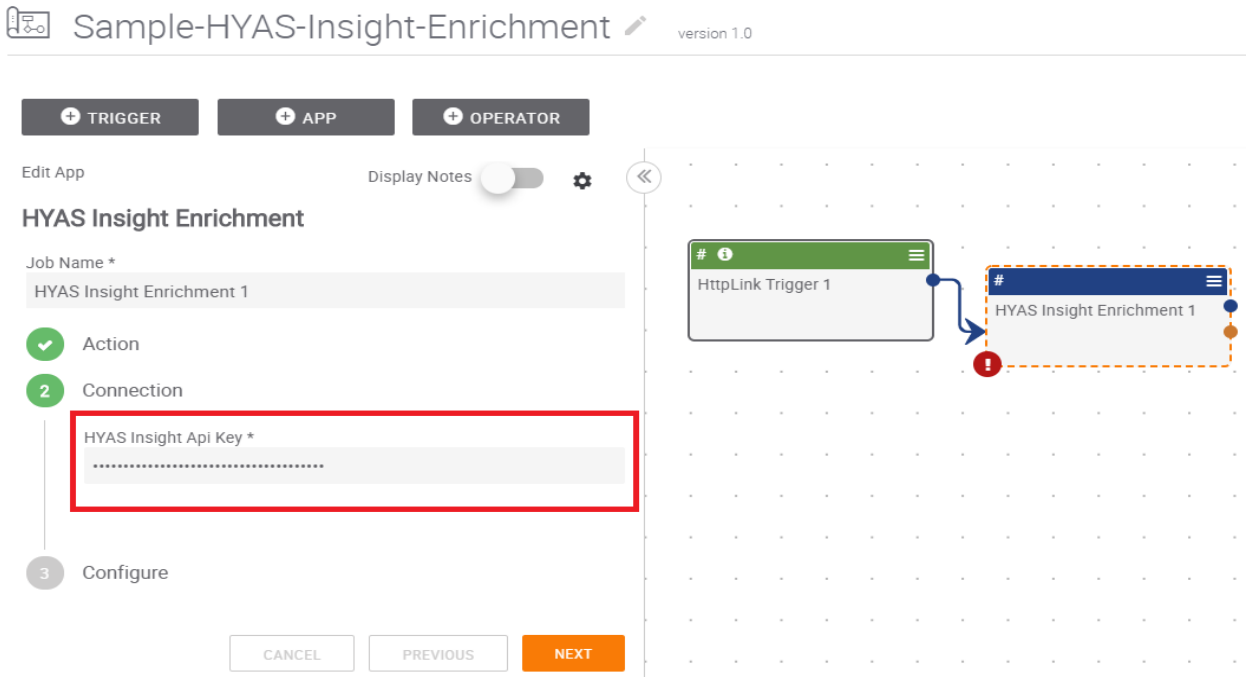
5. In the Playbook editor page, click on + **APP** button to select the ThreatConnect app to be imported into the Playbook. Next search for **"HYAS"** to filter out all HYAS Apps in the ThreatConnect Platform and choose the **HYAS Insight Enrichment** App.



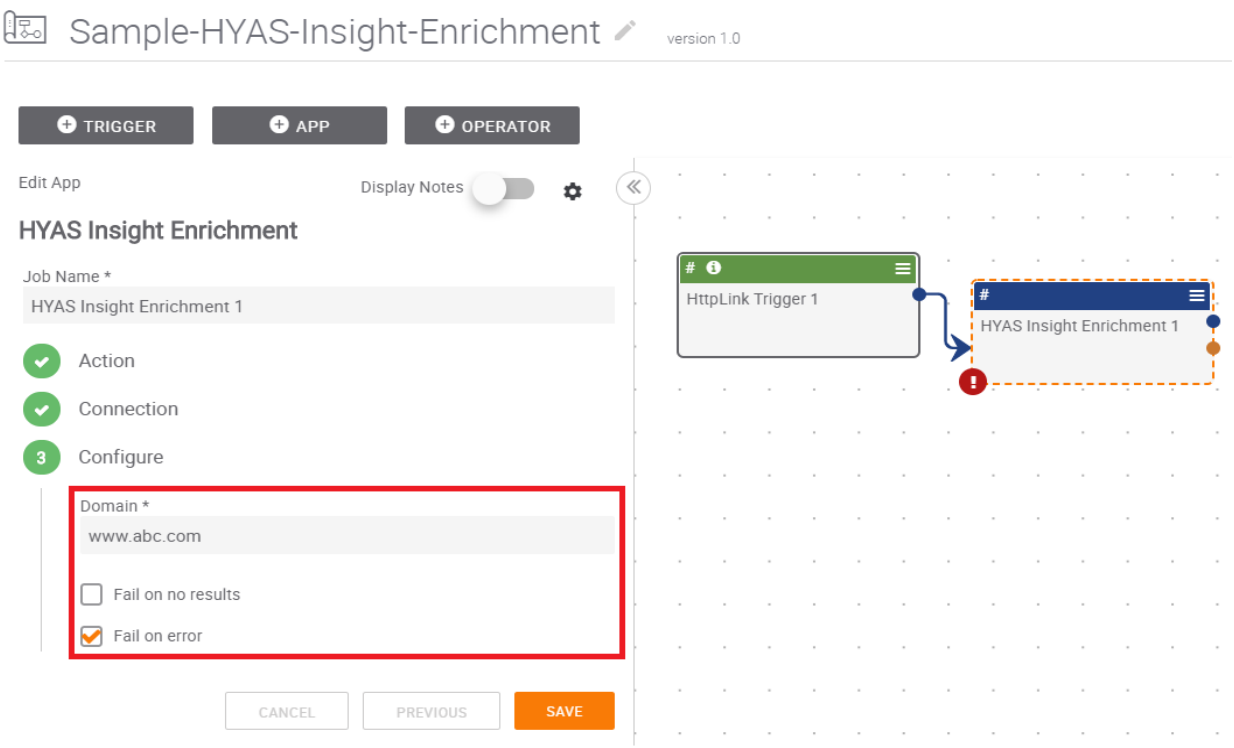
6. Once you click on the App, it will appear in the Playbook editor as shown below. Connect the output of the trigger block to the app block as shown in the figure below. Double click on the App block to view the **Edit App** panel on the left side. The **HYAS Insight Enrichment** has three configuration steps. The **Action** step is used to select one of the Enrichment Type, Domain or Email or Phone Number or IP Address or SHA256 indicator can be selected.



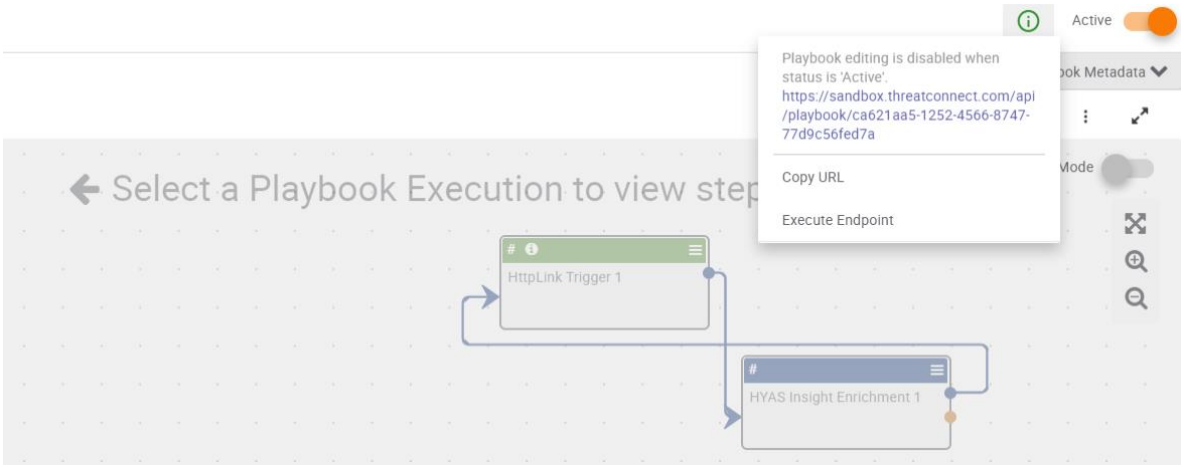
7. Click on **Next** to see the second step **Connection.** In this step, enter the API key provided to you by HYAS in the **HYAS API Key** textbox.



8. 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.



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.



3. 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.c2attribution.json.raw	String	Raw Response object returned from the HYAS Insight API
hy.c2attribution.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""","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

.

hy.c2attribution.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

actor_ipv4	The actor, c2 or referrer ip
c2_domain	The c2 or email domain
c2_ip	The c2_ip of c2_attribution
c2_url	The c2_url of c2_attribution
datetime	The first seen date of the c2_attribution
email	The email connected to the c2 panel
email_domain	The email_doman of the c2_attribution
referrer_domain	The referrer_domain of c2_attribution
referrer_ipv4	The referrer_ipv4 of c2_attribution
referrer_url	The referrer_url of the c2_attribution
sha256	The sha256 malware hash

4. HYAS Insight Playbook Templates

4.1 HYAS Insight Enrichment Playbook Templates Installation

HYAS provides four Playbook Templates:

- **HYAS Insight IP Address Enrichment Playbook Template**
  - This Playbook provides PassiveDNS, DynamicDNS, C2 Attribution, Device Geo, PassiveHash, SSL Certificate and SinkHole Information for the provided IP Address.
- **HYAS Insight Email Address Enrichment Playbook Template**
  - This Playbook provides DynamicDNS, C2 Attribution and WhoIs Information for the provided Email Address.
- **HYAS Insight Host Enrichment Playbook Template**
  - This use case describes the desire to identify all Hosts that resolved to a given Address based on a time window from a starting and stopping point in time.
- **HYAS Insight SHA256 Enrichment Playbook Template**
  - This Playbook provides C2 Attribution Information for the provided Sha256 File Hashes.

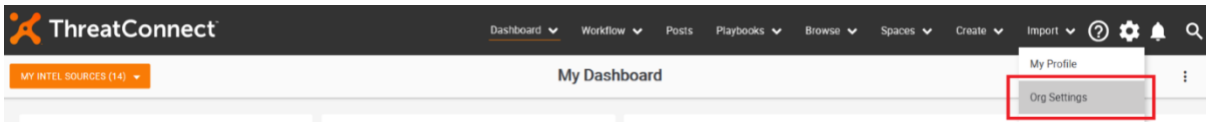
These Playbook Templates are available on GitHub. These templates provide a basic understanding on how to use the Enrichment App in the playbooks.

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

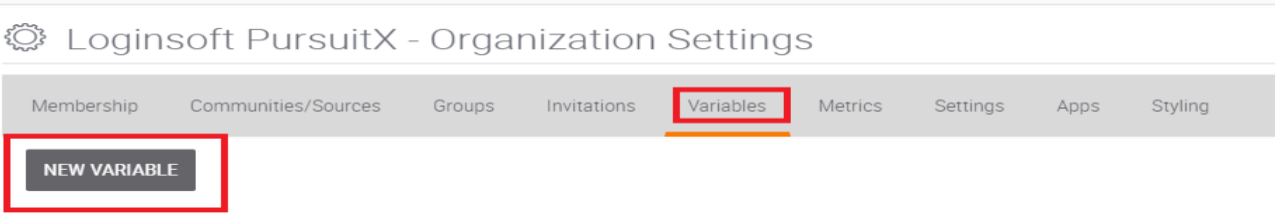
4.2 HYAS Insight API Key Variable Set Up

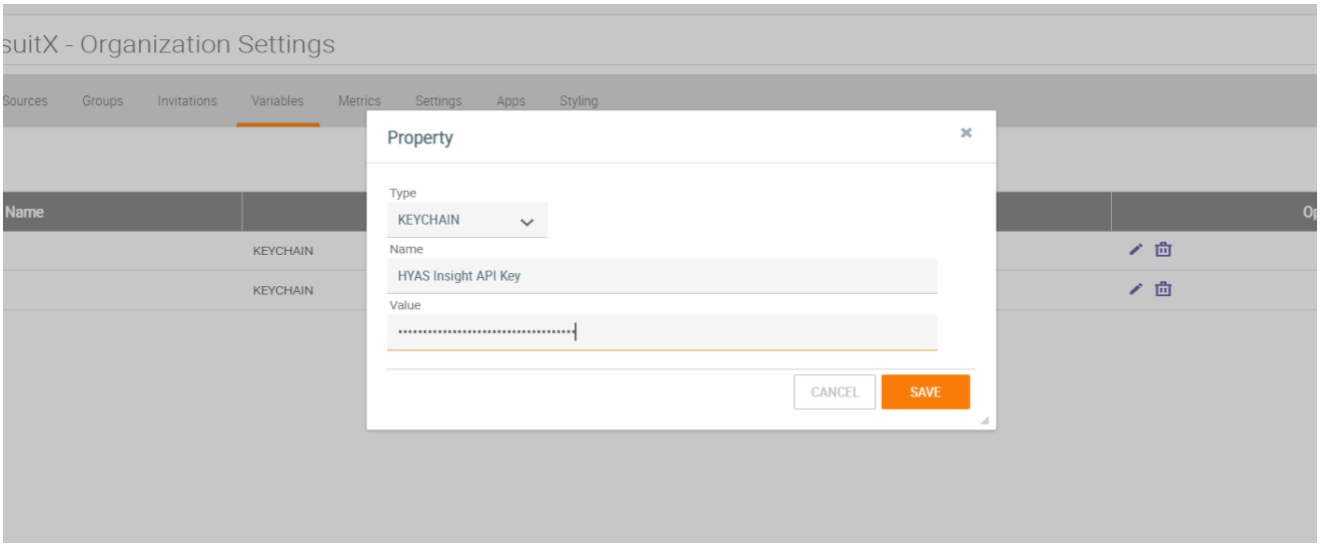
Note: This step is required, otherwise Playbook Templates will not work as expected. If you want to skip this step, you need to provide HYAS API Key in each of the Playbook Templates.

- Click on the settings (gear icon) in the top right corner in the ThreatConnect platform to select Org Settings → Variables.



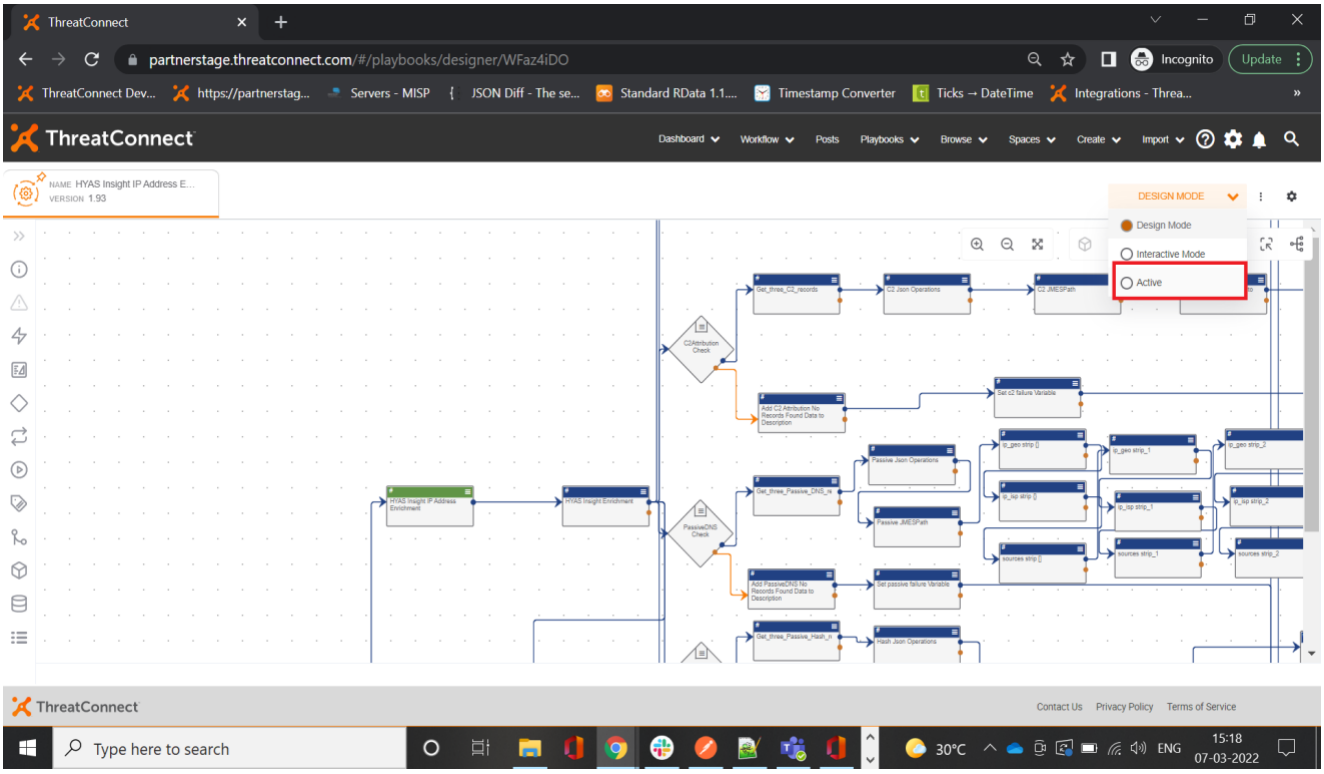
- Go to Variables.
  1. Click on New Variable
  2. Type = KEYCHAIN
  3. Name = HYAS Insight API Key
  4. Value = HYAS Insight API Key provided by HYAS
  5. Click on Save



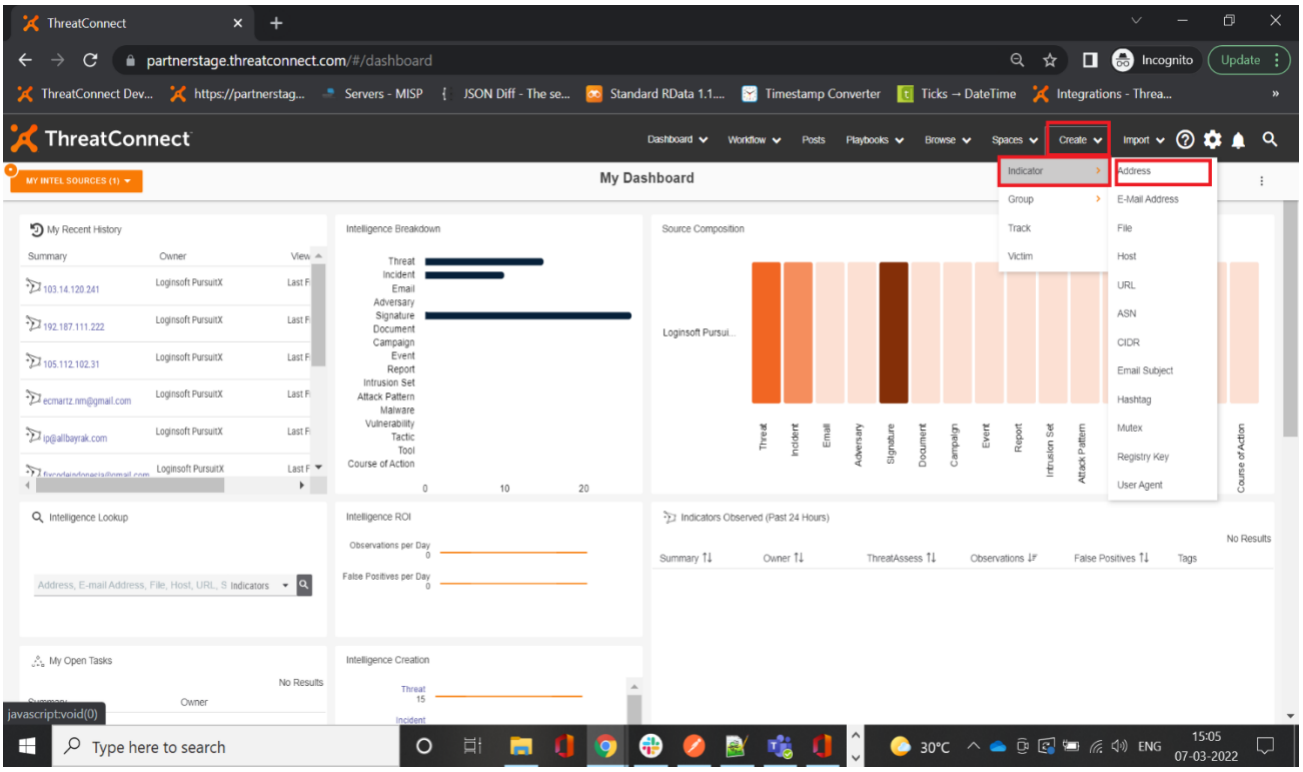


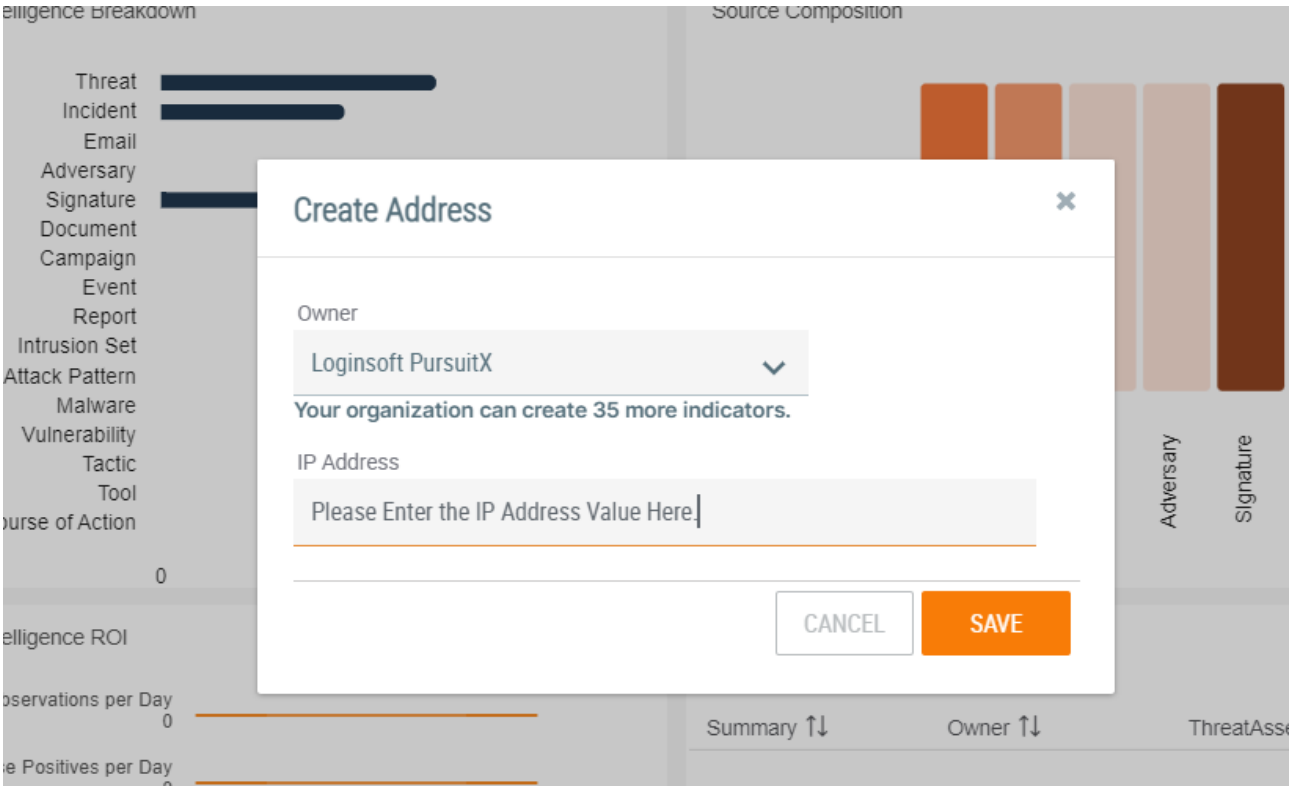
5. Running HYAS Insight IP Address Enrichment Playbook Template

Step 1: Go to the playbooks and select and open the HYAS Insight IP Address Enrichment Playbook Templates. Please activate the playbook as shown below.

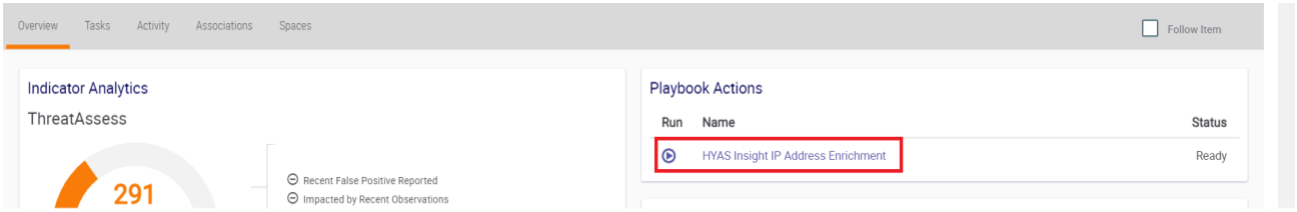


Step 2: Browse the existing IP Address Indicators (or) Create a new IP Address Indicator.



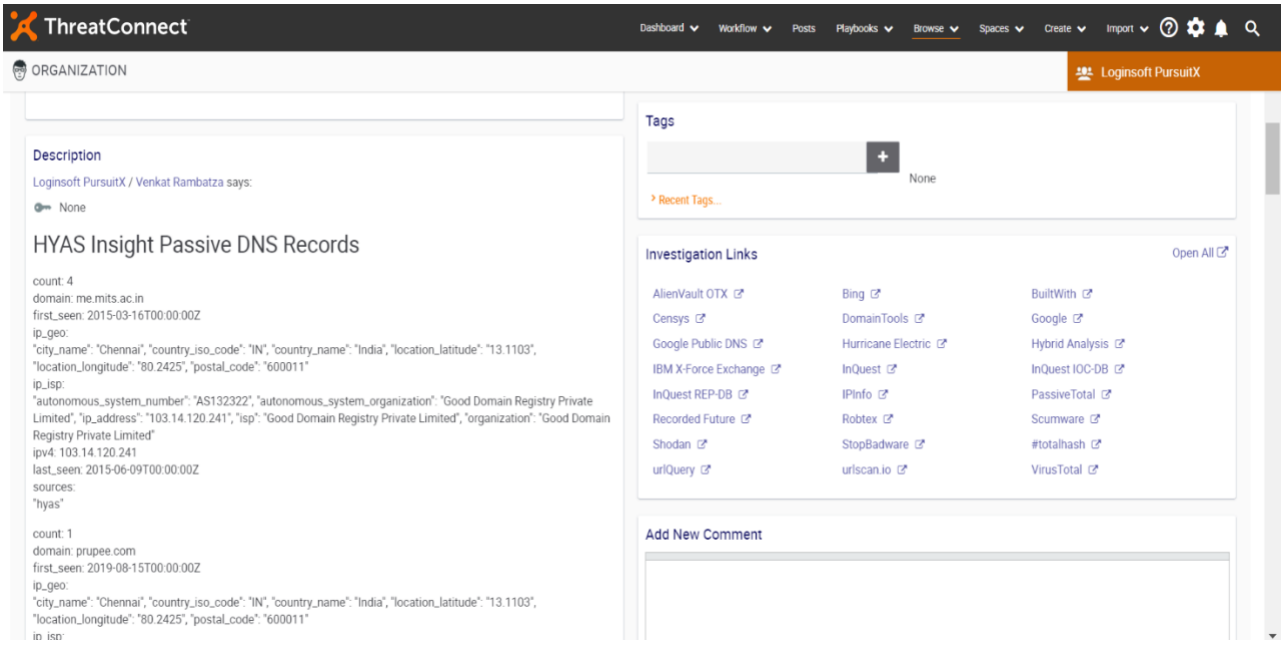


Step 3: For Address Indicators, you will see the "HYAS Insight IP Address Enrichment" Playbook Action in the details page. Click on play button to run the playbook.



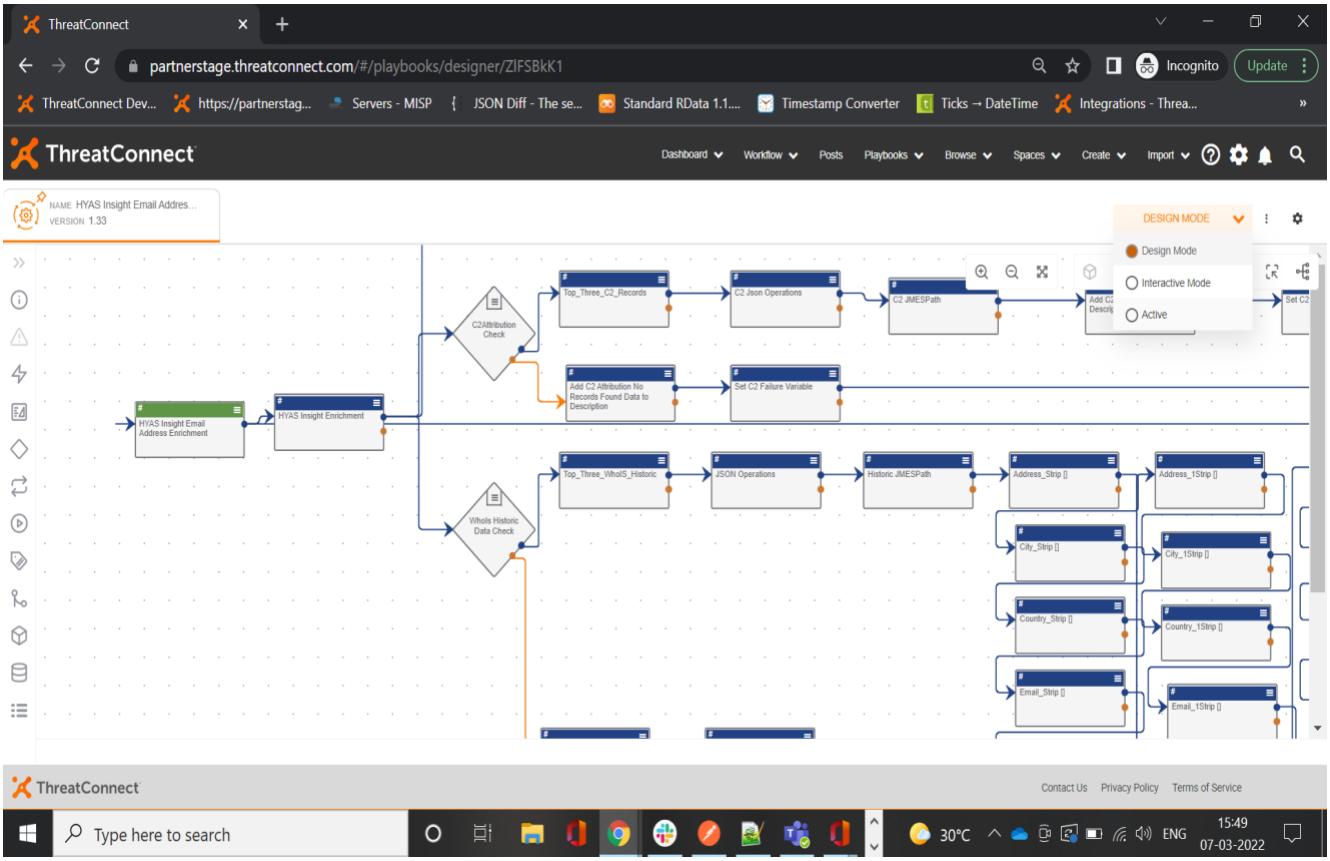
Step 4: Once the playbook is completed, please refresh the page, the enrichment data from HYAS Insight for the IP Address will be added to the description attribute.

Example:

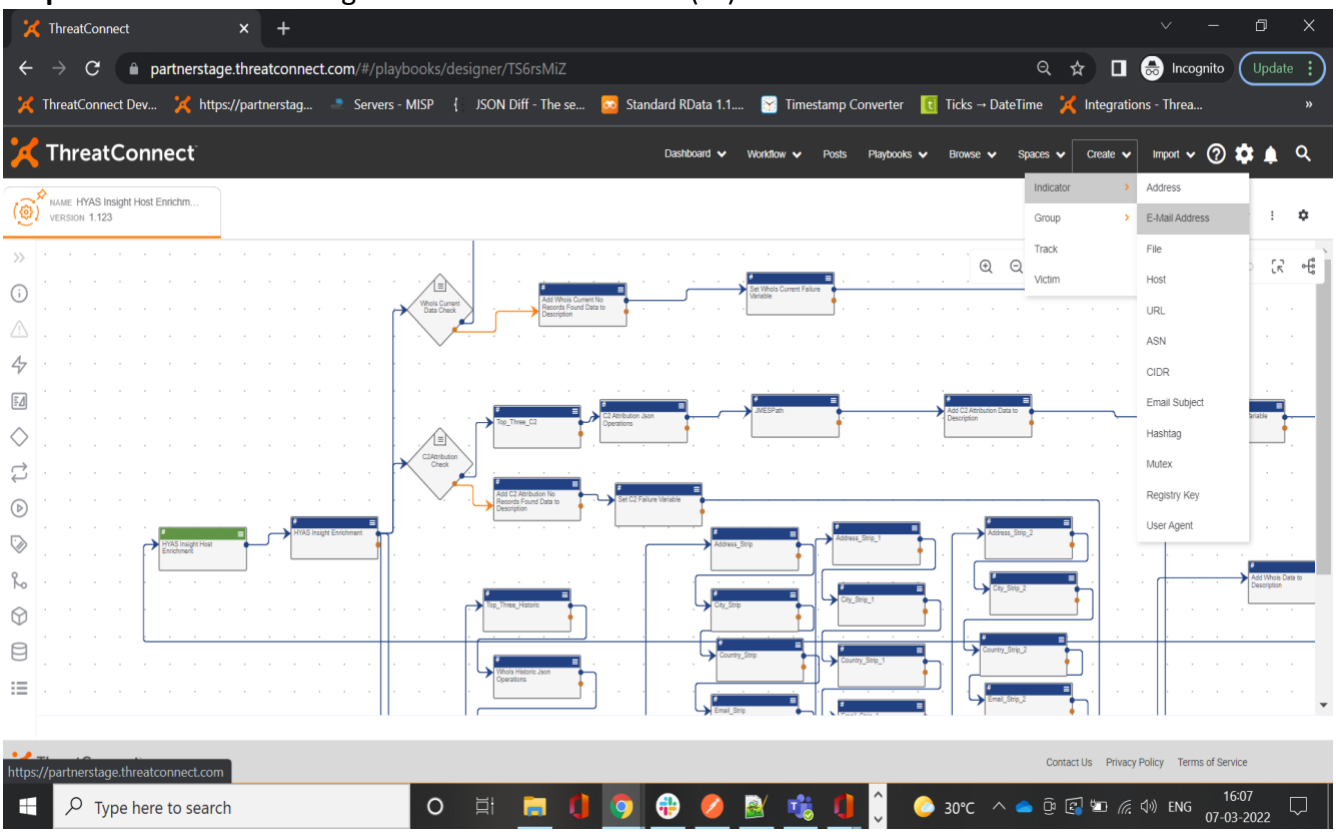


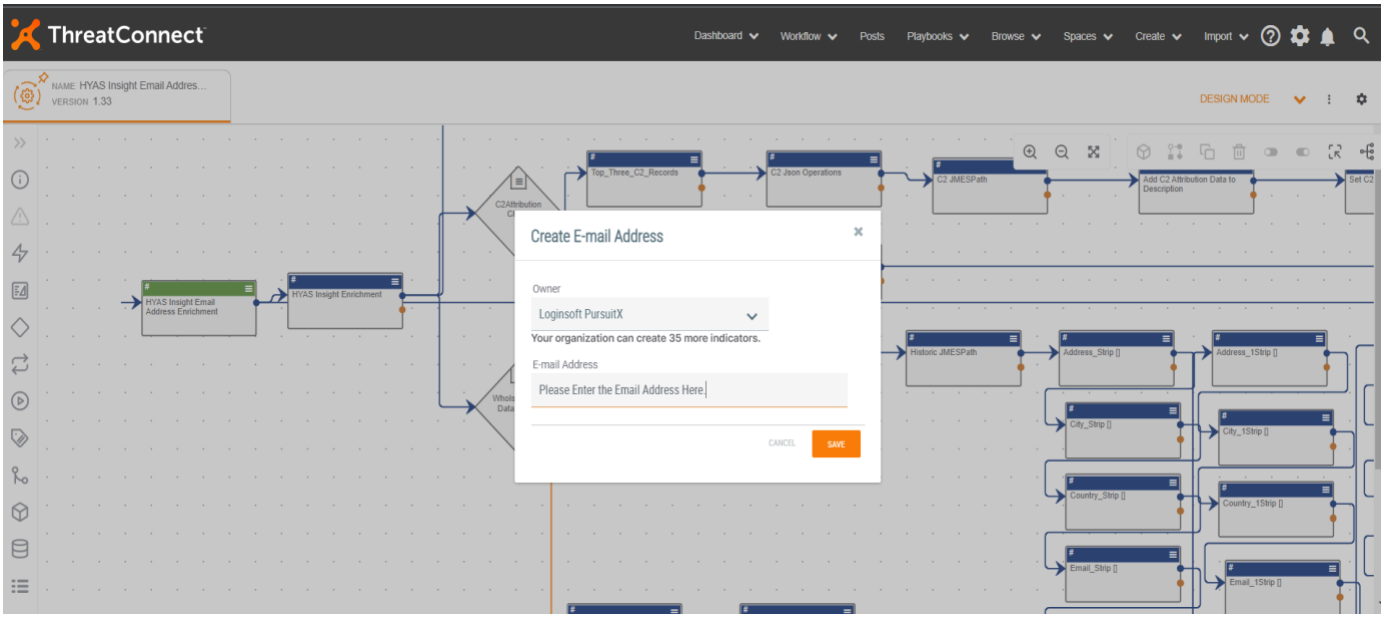
6. Running HYAS Insight Email Address Enrichment Playbook Template

Step 1: Go to the playbooks and select and open the HYAS Insight Email Address Enrichment Playbook Templates. Please activate the playbook as shown below.

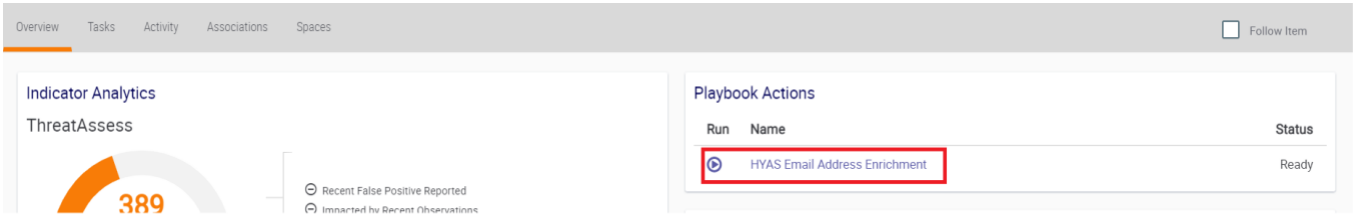


Step 2: Browse the existing Email Address Indicators (or) Create a new Email Address Indicator.



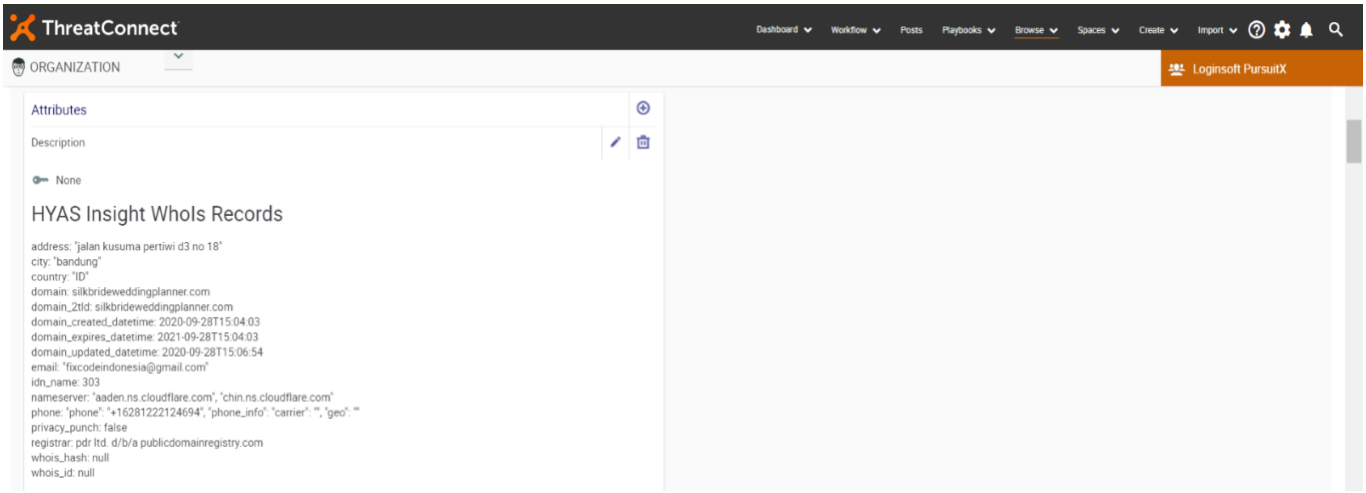


Step 3: For Address Indicators, you will see the "HYAS Insight Email Address Enrichment" Playbook Action in the details page. Click on play button to run the playbook.



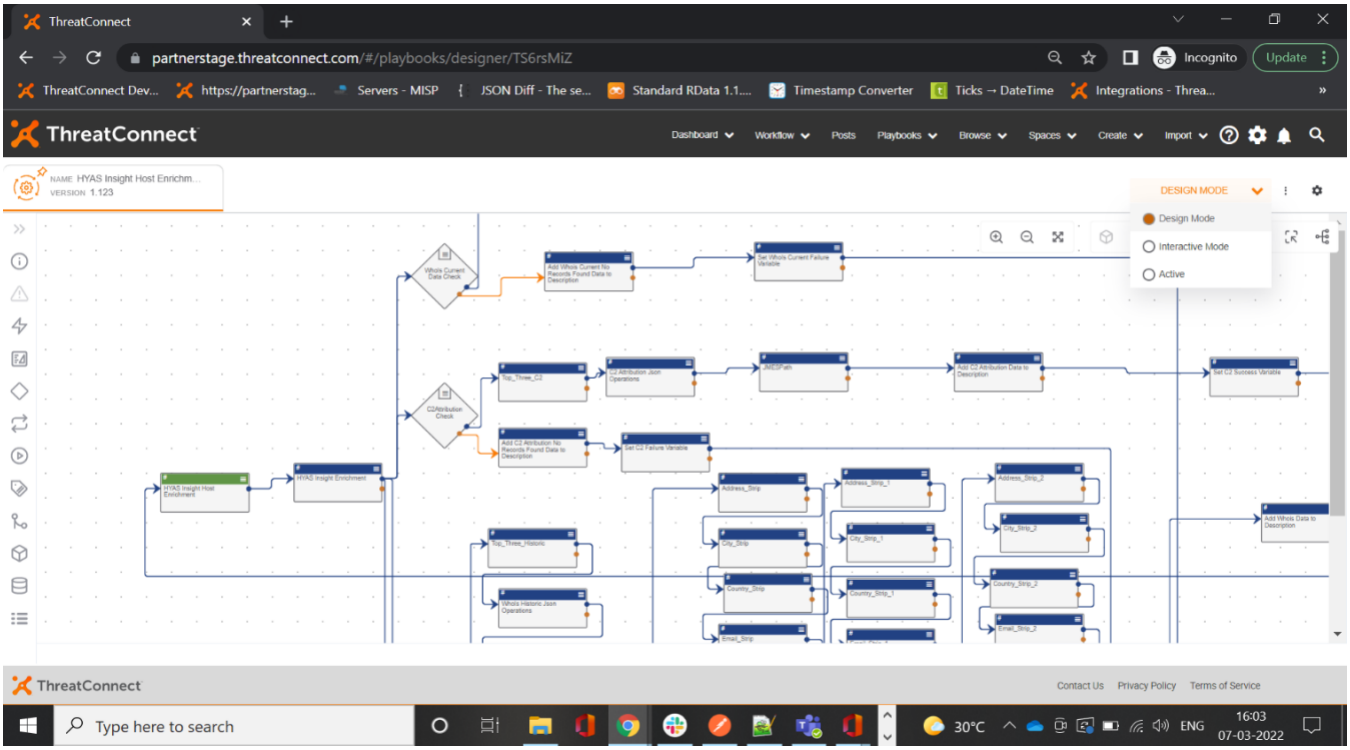
Step 4: Once the playbook is completed, please refresh the page, the enrichment data from HYAS Insight for the Email Address will be added to the description attribute.

Example:

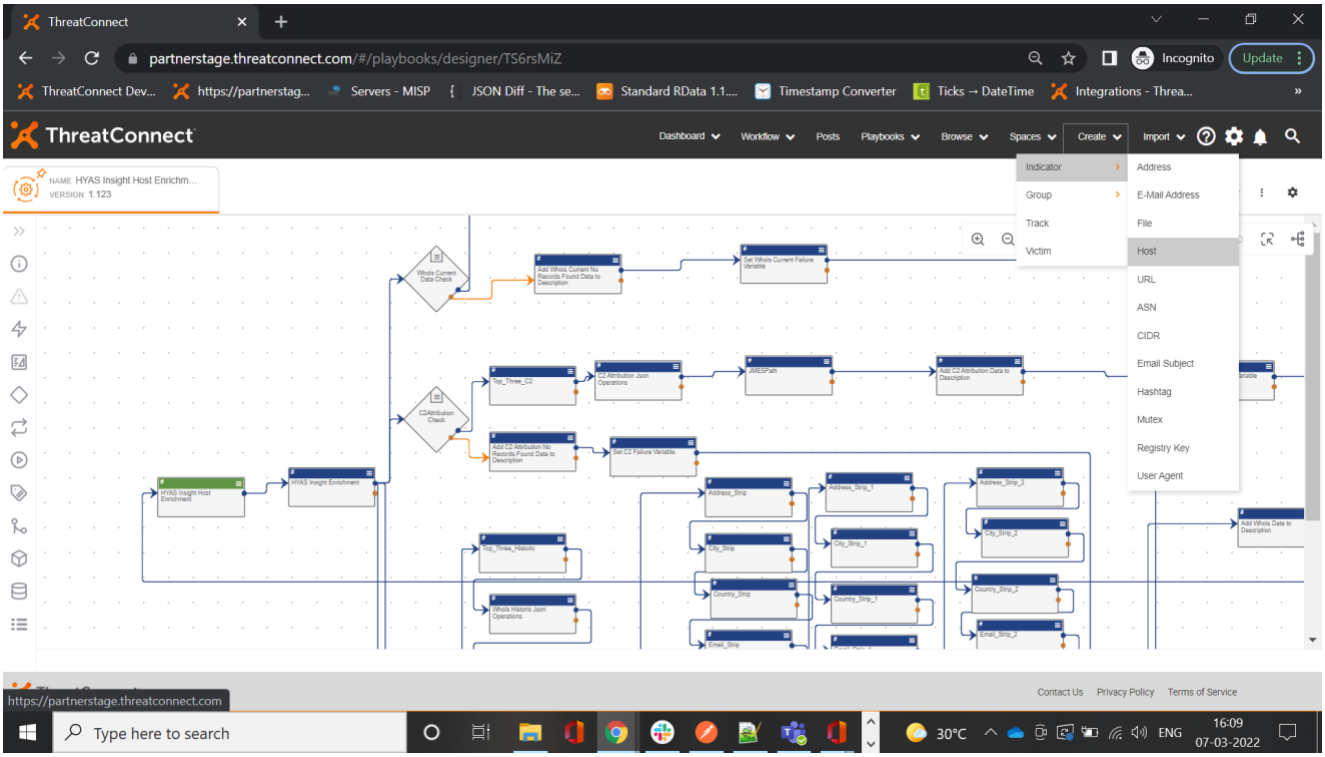


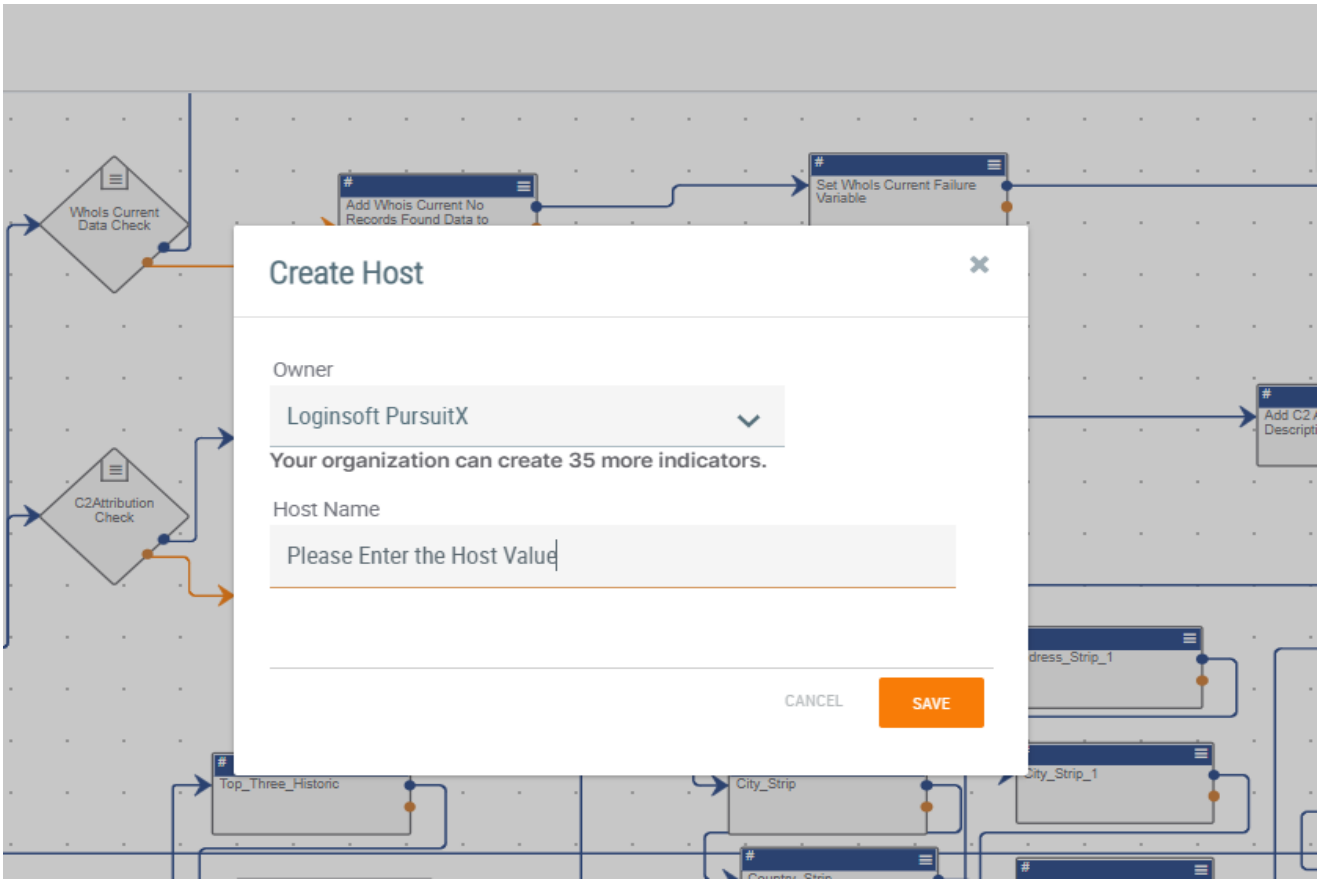
7. Running HYAS Insight Host Enrichment Playbook Template

Step 1: Go to the playbooks and select and open the HYAS Insight Host Enrichment Playbook Templates. Please activate the playbook as shown below.

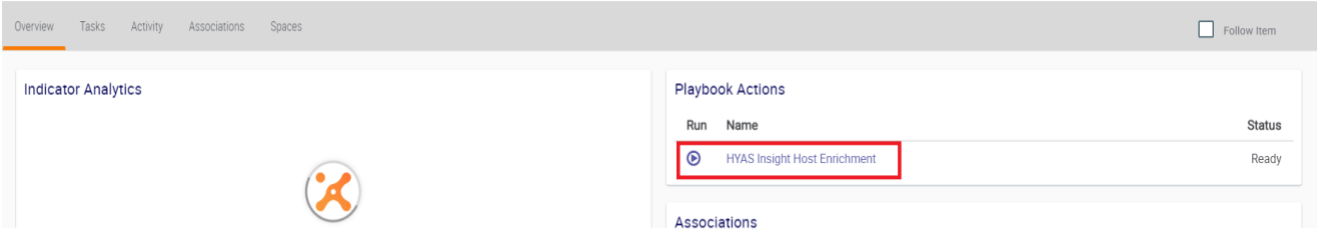


Step 2: Browse the existing Host Indicators (or) Create a new Host Indicator.



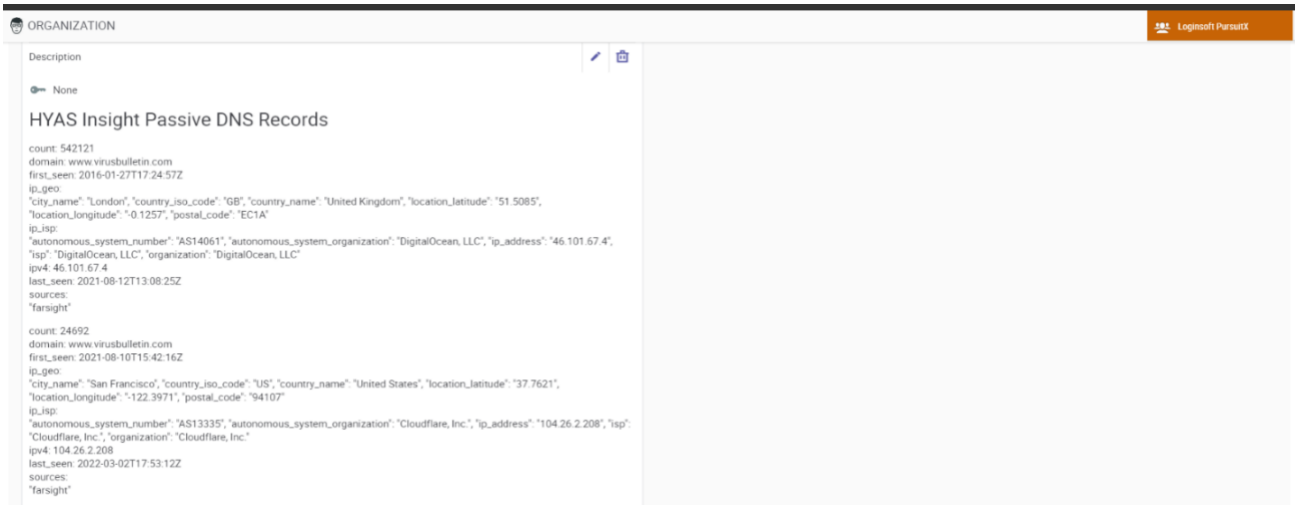


Step 3: For Address Indicators, you will see the "HYAS Insight Host Enrichment" Playbook Action in the details page. Click on play button to run the playbook.



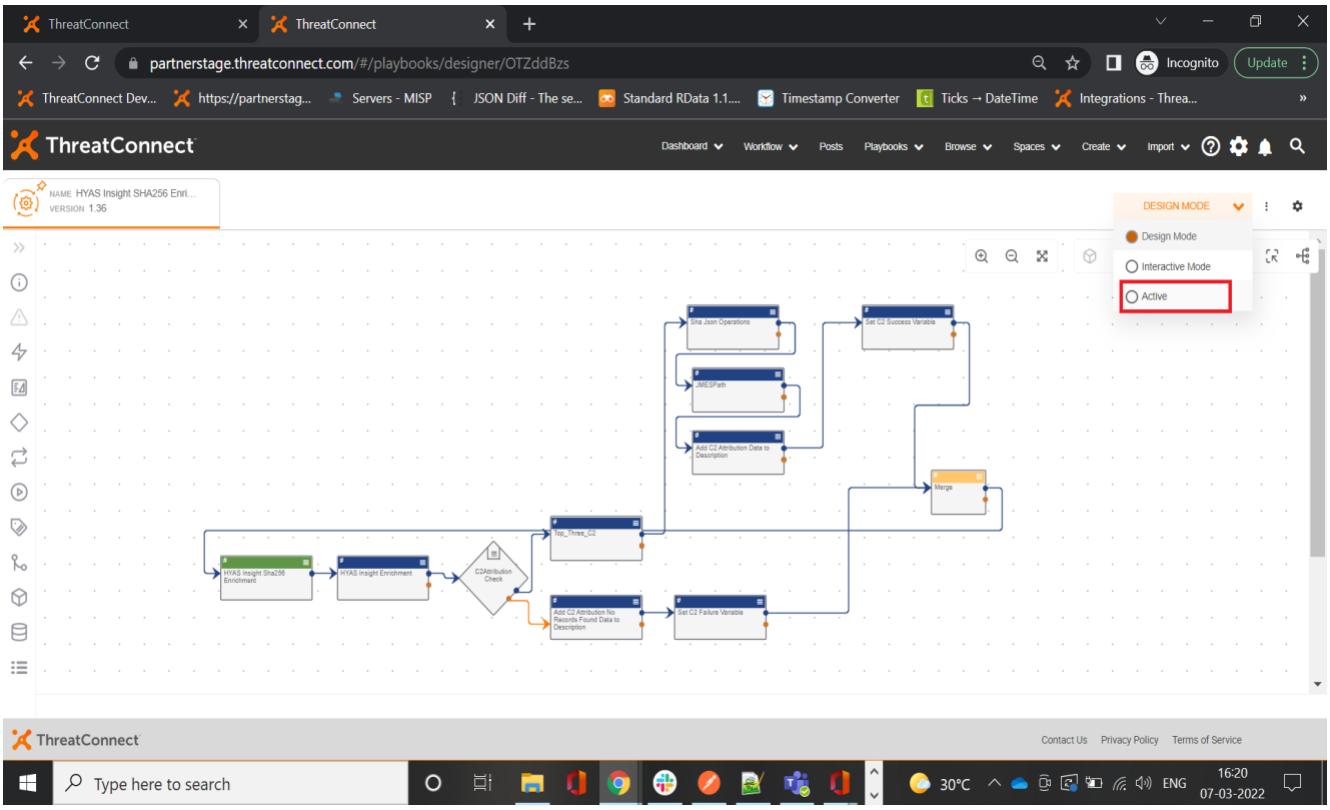
Step 4: Once the playbook is completed, please refresh the page, the enrichment data from HYAS Insight for the Host will be added to the description attribute.

Example:

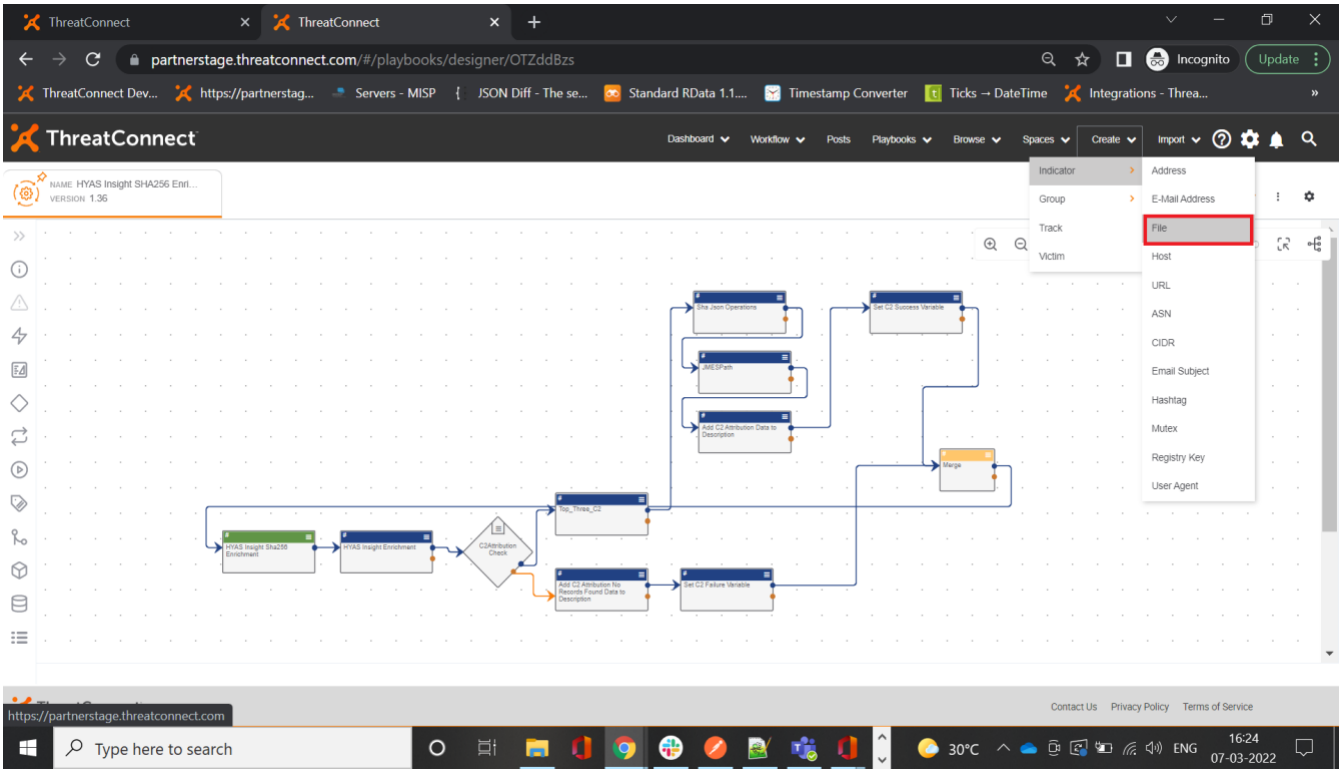


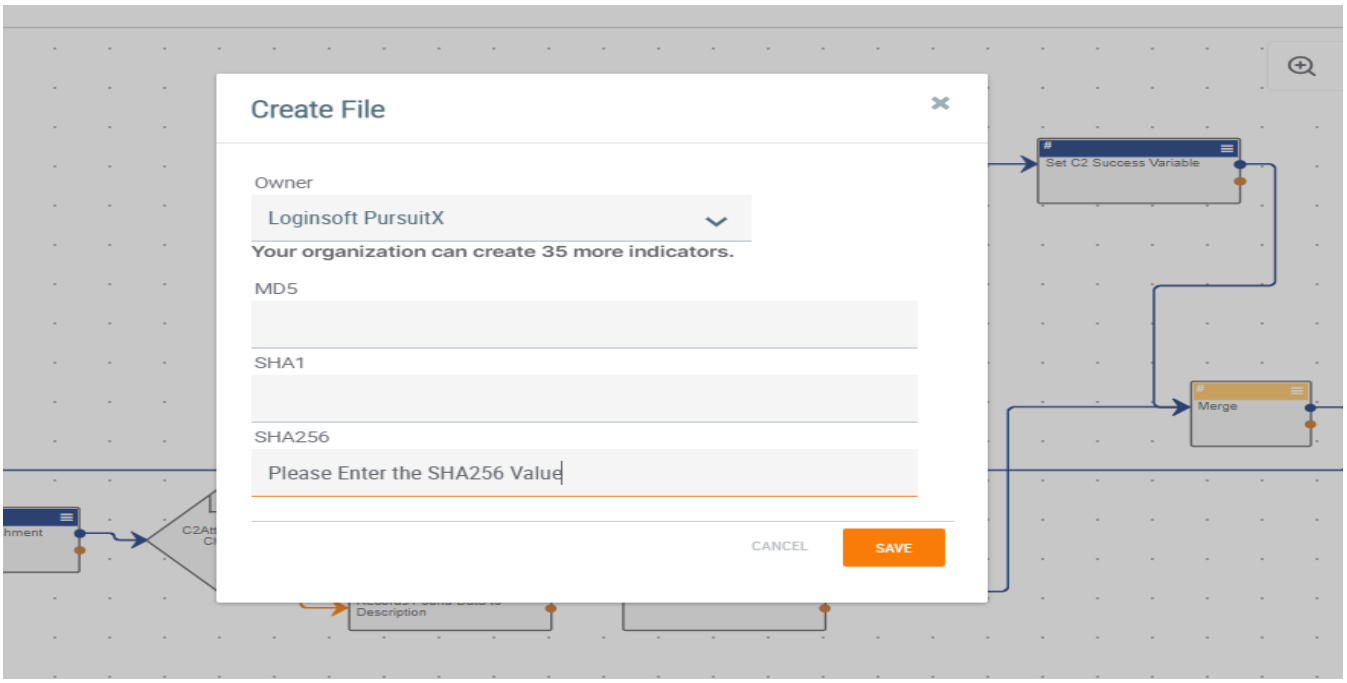
8. Running HYAS Insight SHA256 Enrichment Playbook Template

Step 1: Go to the playbooks and select and open the HYAS Insight SHA256 Enrichment Playbook Templates. Please activate the playbook as shown below.

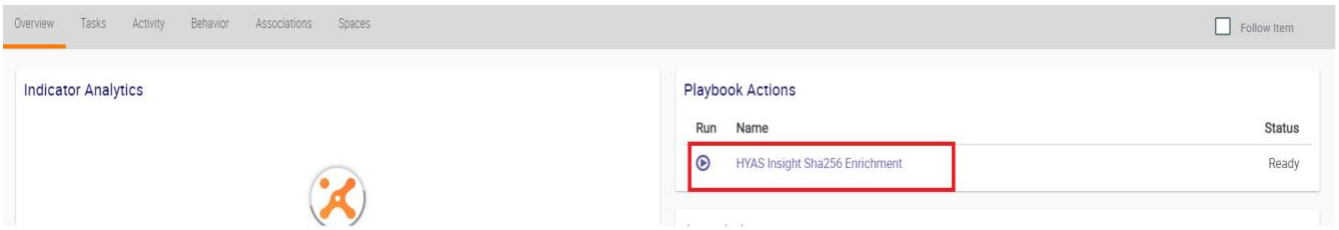


Step 2: Browse the existing File Indicators (or) Create a new File Indicator.



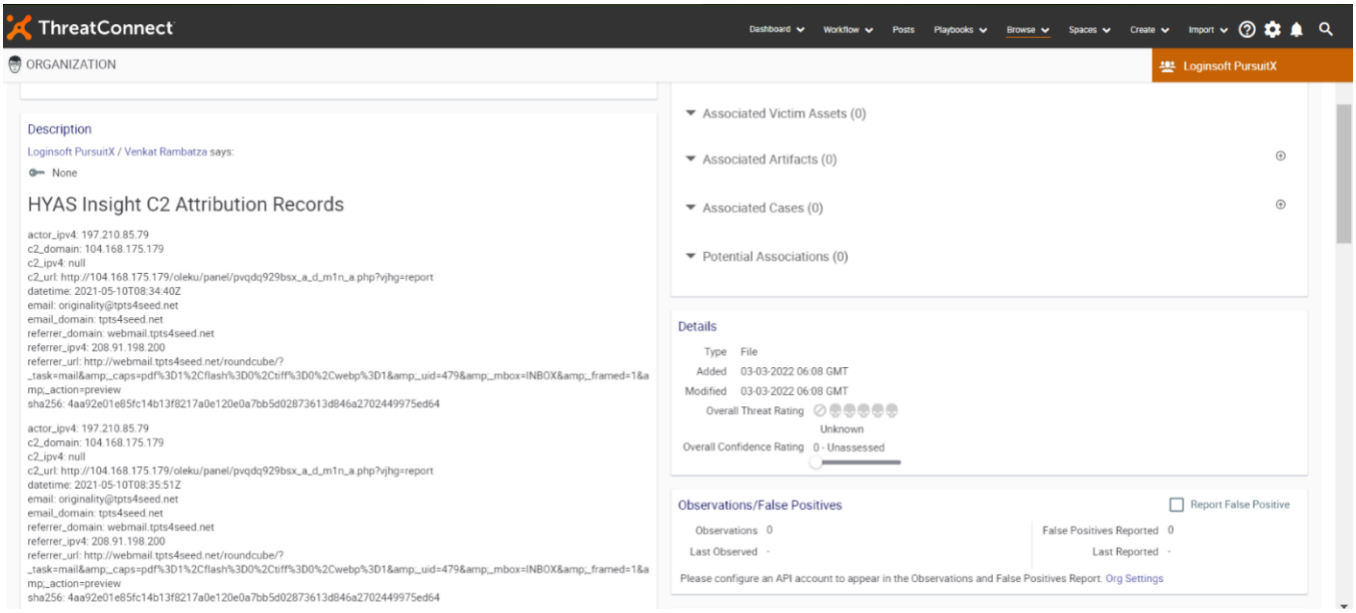


Step 3: For Address Indicators, you will see the "HYAS Insight SHA256 Enrichment" Playbook Action in the details page. Click on play button to run the playbook.



Step 4: Once the playbook is completed, please refresh the page, the enrichment data from HYAS Insight for the SHA256 will be added to the description attribute.

Example:



9. 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.