ThreatConnect – Adversary Space Data Enrichments App User Guide

Version 1.0.0

Support

For assistance with this App, to report a bug, or feature requests please contact us via the following.

Support Portal	support@advintel.tech

Version History

Date	Version	Description
06-02-2022	1.0.0	User Guide for the Adversary Space Data Enrichments App.

Table of Contents

1. Introduction

AdvIntel is a next-generation threat prevention and loss prevention company launched by a team of certified investigators, reverse engineers, and security experts. We offer state-of-the-art solutions to combat fraud, ransomware, and botnets by providing early-warning alerting, applied threat intelligence and long-term strategic services to the private sector and government organizations.

Our past experience in the governmental, legal, forensics, and corporate finance sectors allows us to develop the most actionable intelligence tailored to your needs and the needs of your clients.

Botnet API - This API is designed to conveniently preview and demonstrate information and indicators of compromise (IOCs) regarding workstations, machines, and networks that were infected or unlawfully accessed by threat actors.

Bot Creds API - This API is designed to quickly and conveniently access AdvIntel's Andariel botnet credential dataset containing only high-value botnet credentials:

Raw botnet high-value credentials (no low-tier collections) based on fqdn, user and URL the compromised machine accessed.

Dark Web Intelligence API - This API is designed to efficiently and conveniently preview and demonstrate selected information on threat-related content, and breach activity presented on the selected top-tier underground sites.

The API is designed to preview information from a selected customized base of Top-tier sources. These selected sources were chosen due to their highest level of threat credibility within the cybercrime hierarchy. Being the central nodes of the cybercrime network all across the world, these several communities accumulate the most dangerous and prolific cybercrime offers and discussions and host the most credited cybercrime auctions.

Information and intelligence which is accumulated and previewed via this API requests includes:

1. Structurally
    a. Elite underground forums (limited to 9 for high sound to noise ratio)
    b. Elite underground forums (limited to 19 for high sound to noise ratio)
2. Content-Based
    a. Auctions and breaches
    b. Dumps
    c. CVV
    d. Account Shops
    e. SSNs
3. Current Volume ~ 100,000 daily
4. Intelligence Highlights:
    a. Novel fraud schemes
    b. Ransomware updates

c. Malware offers
d. Exploit discussions
e. Targeted attack discovery

Hunting API - This API is designed to quickly and conveniently access AdvIntel's botnet and breach logs, as well as other sensitive records, which are otherwise not made available on the Andariel platform due to their sensitive nature.

This document helps you in configuring the **Adversary Space Data Enrichments** App provided by AdvIntel Andariel into the ThreatConnect Platform. The **Adversary Space Data Enrichments** App enables ThreatConnect Platform users to perform On-Demand Enrichment of IOC's using the AdvIntel Intelligence.

IOC API - Andariel Indicators of Compromise (IOC) API is designed for quick and convenient access to AdvIntel's Andariel Platform indicator searches across the Advanced Intelligence IOC dataset.

This section includes AdvIntel's technical reporting on the most urgent emerging malware threats and botnet collections, including the analysis created by our reverse engineering operations.

2. Configuration

2.1. Pre-Requisites

To configure the **Adversary Space Data Enrichments** App in your ThreatConnect Playbooks, the following requirements need to be fulfilled:

- Access to ThreatConnect instance
- Permission to execute ThreatConnect Playbooks
- Andariel API Key provisioned by AdvIntel to authenticate requests to Andariel API
- Adversary Space Data Enrichments App installed in ThreatConnect Instance
- Adversary Space Data Enrichments Playbooks and installed in ThreatConnect Instance

2.2. Adversary Space Data Enrichments App Installation

Adversary Space Data Enrichments App for ThreatConnect is available on ThreatConnect Marketplace at: https://go.threatconnect.market/browse/categories/data-enrichment. Download the App package with tcx extension and install it in your ThreatConnect instance. For installation instructions, refer to the "Install an App" in the ThreatConnect System Administration Guide. For more information, please contact your ThreatConnect Customer representatives.

2.3. Adversary Space Data Enrichments App Configuration

Adversary Space Data Enrichments App has the following configuration.

- Andariel API Key **-** String
  - ➢ API key provisioned by AdvIntel

- Enrichment Type – Dropdown
  - Dropdown containing “Botnet”, “Bot Creds”,” Dark Web”, “Hunting” and “IOC”
  - Depending on which enrichment type is chosen, different configurations will populate. A full list of configuration options is presented below

  Botnet Enrichment Type configuration options:
  - Botnet Query – String

  Bot Creds Enrichment Type configuration options:
  - Search By – Dropdown
    - Dropdown containing “Domain”, “Username”” and “URL”
  - Domain – String
    - This is visible when “Domain” is selected in Search By dropdown
  - Username – String
    - This is visible when “Username” is selected in Search By dropdown
  - URL – String
    - This is visible when “URL” is selected in Search By dropdown
  - From Date – String
  - To Date – String

  Dark Web Enrichment configuration options:
  - Dark Web Query – String

  Hunting Enrichment configuration options:
  - Task – Dropdown
    - Dropdown containing “Create” and “Status”
  - Hunting Query – String
    - This is visible when “Create” is selected in Task dropdown
  - Email Address – String
    - This is visible when “Create” is selected in Task dropdown
  - Task Id – String
    - This is visible when “Status” is selected in Task dropdown

  IOC Enrichment configuration options:
  - IOC Query – String
  -
- Fail on Error - Checkbox (default to True)
  - Fails the App when an error occurs, if set to True

- Fail on no results – Checkbox (default to False)
  - Fails the App when there are no results returned by the Andariel API, if set to True

3. Outputs

Output	TC Type	Description
adv.botnet.json.raw	String	Raw response object from Andariel API.
adv.botnet.results.data	String	Processed Response object
adv.botnet.results.count	String	Raw Number of records from Andariel API
adv.botcreds.json.raw	String	Raw response object from Andariel API.
adv.botcreds.results.data	String	Processed Response object
adv.botcreds.results.count	String	Raw Number of records from Andariel API
adv.darkweb.json.raw	String	Raw response object from Andariel API.
adv.darkweb.results.data	String	Processed Response object
adv.darkweb.results.count	String	Raw Number of records from Andariel API
adv.hunting.json.raw	String	Raw response object from Andariel API.
adv.hunting.results.data	String	Processed Response object
adv.ioc.json.raw	String	Raw response object from Andariel API.
adv.ioc.results.data	String	Processed Response object
adv.ioc.results.count	String	Raw Number of records from Andariel API

4. Adversary Space Data Enrichments Playbook

4.1. Adversary Space Data Enrichments Playbook Installation

This integration provides five Playbook as listed below:

a. Adversary Space Data Enrichments Bot Creds Playbook
b. Adversary Space Data Enrichments Botnet Playbook
c. Adversary Space Data Enrichments Dark Web Playbook
d. Adversary Space Data Enrichments Hunting Create Playbook
e. Adversary Space Data Enrichments Hunting Status Playbook
f. Adversary Space Data Enrichments IOC Playbook

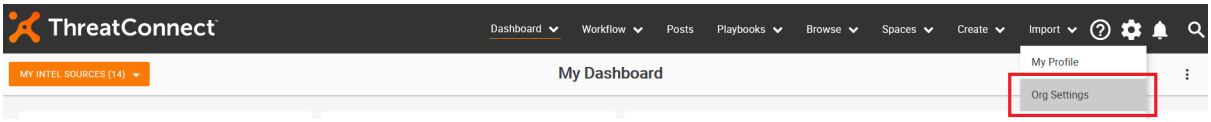
The above playbooks are available on GitHub. These playbooks provide a basic understanding on how to use the Adversary Space Enrichments Data App in the playbooks.

To install these Playbooks, go to 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 import.

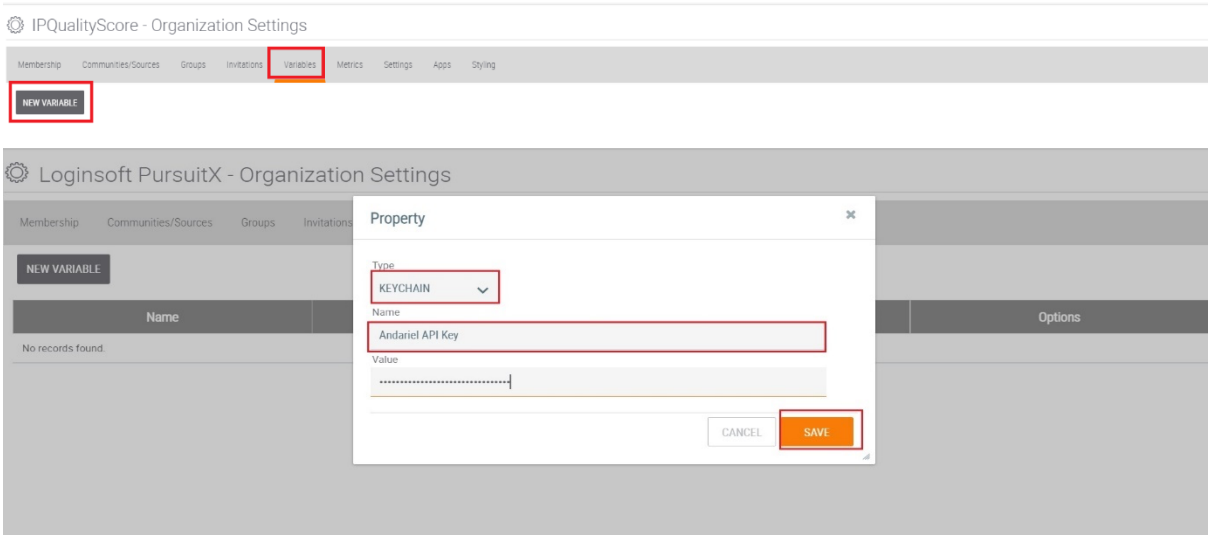
4.2. Andariel API Key Variable Set Up

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

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



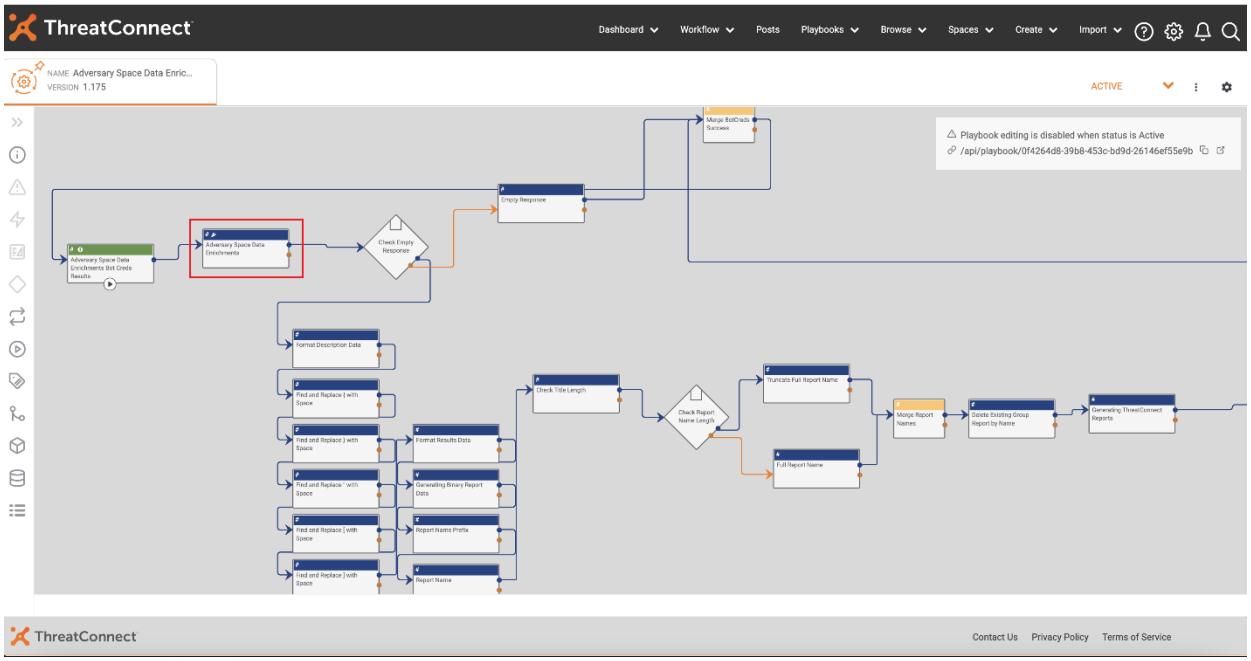
- Go to Variables.
    1. Click on New Variable
    2. Type = KEYCHAIN
    3. Name = Andariel API Key
    4. Value = Andariel API Key provided by AdvIntel
    5. Click on Save



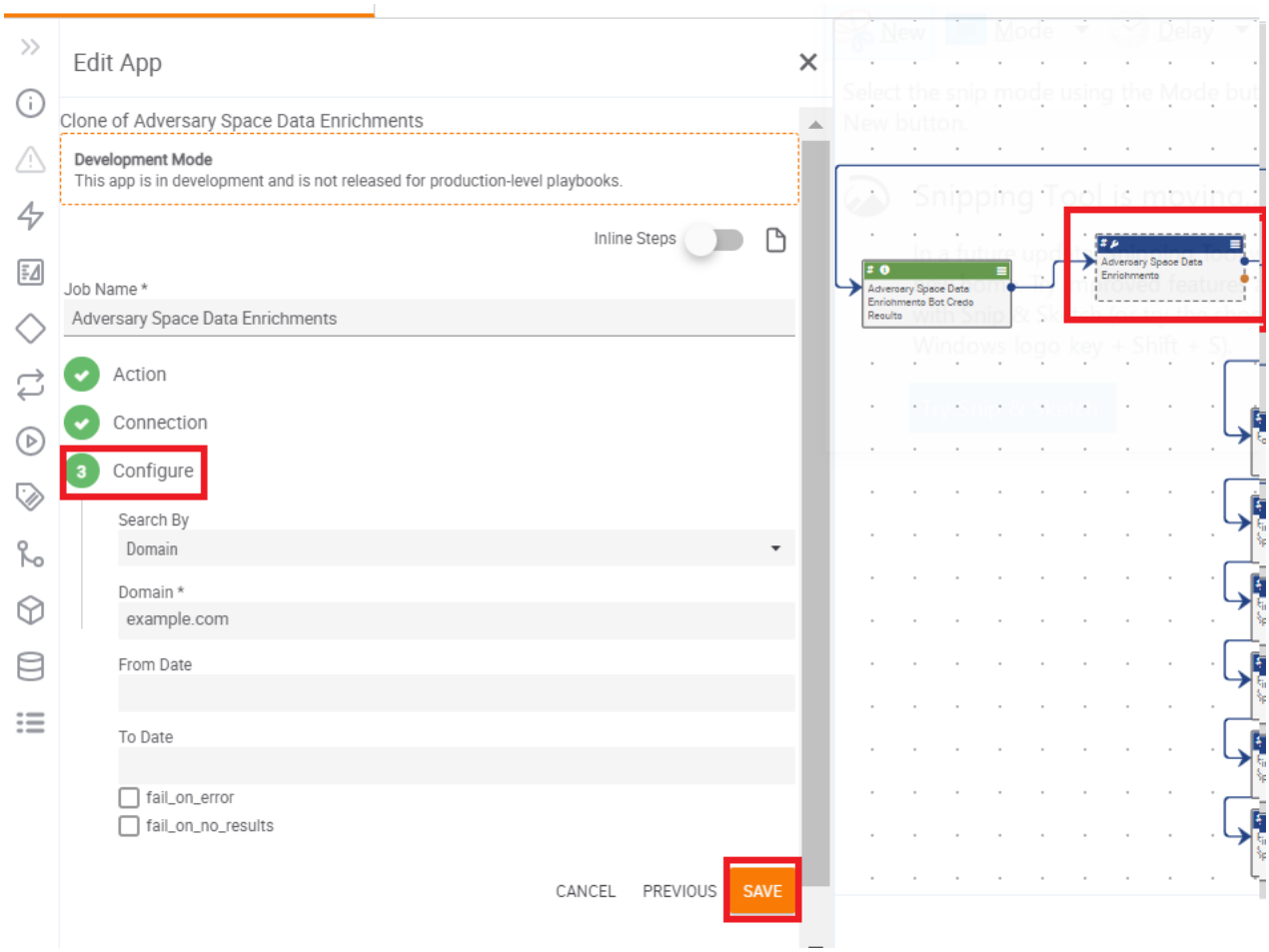
Let's go through following Playbooks:

5. Running Adversary Space Data Enrichments Bot Creds Playbook

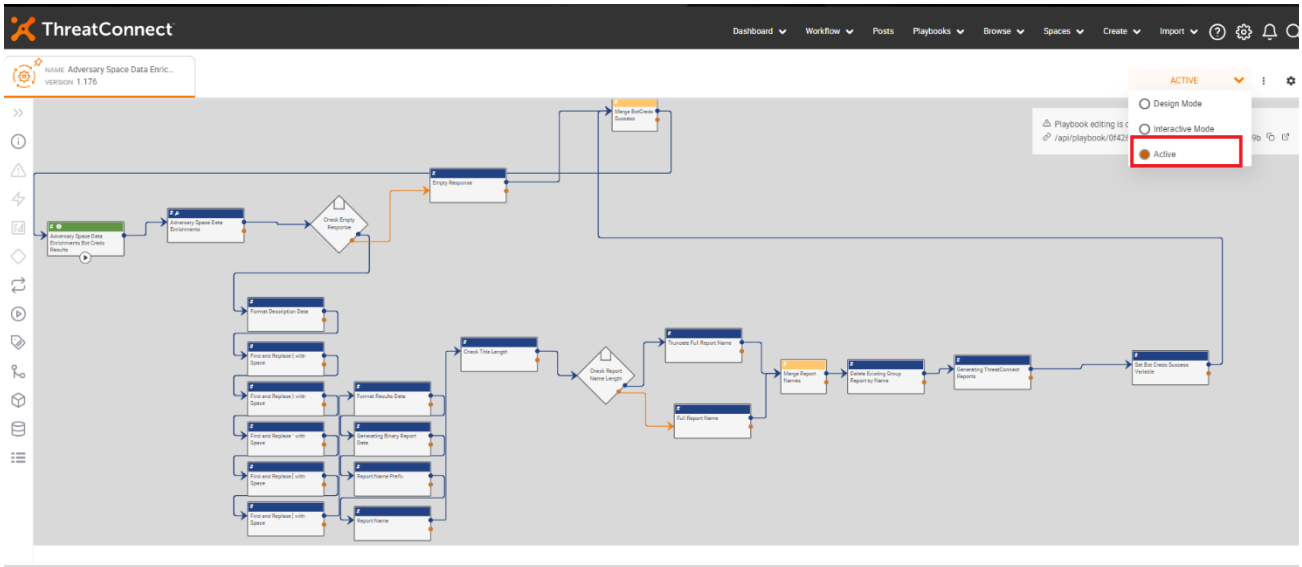
Step 1: Open the Adversary Space Data Enrichments Bot Creds Playbook, double click the App as shown below



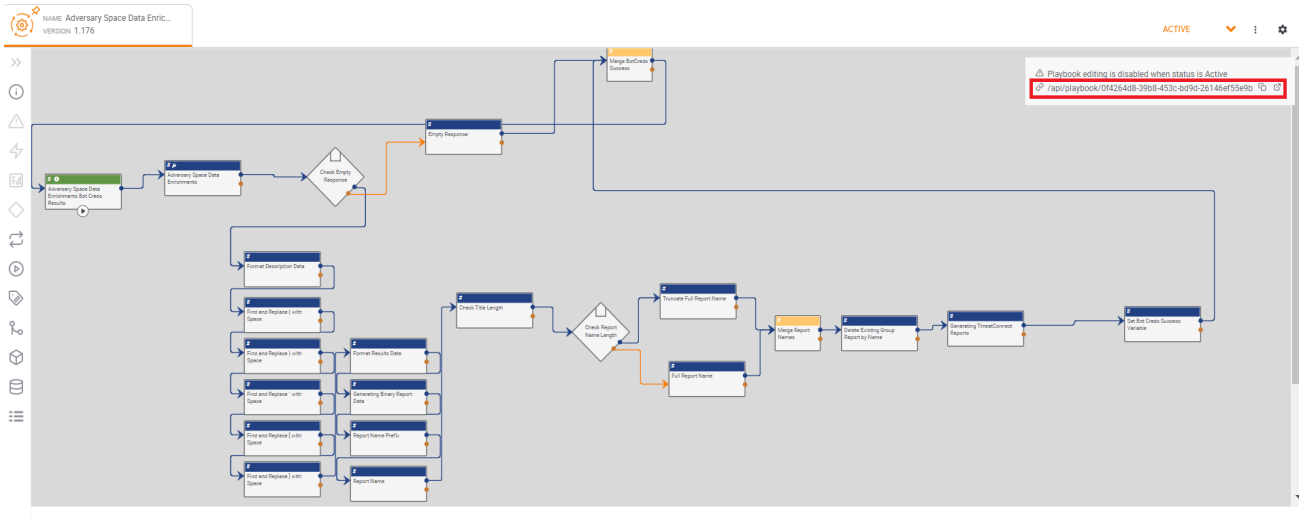
Step 2: Go to Configure section of the App and provide your desired values to search and click on Save as shown below.



Step 3: Activate the Playbook as shown below.

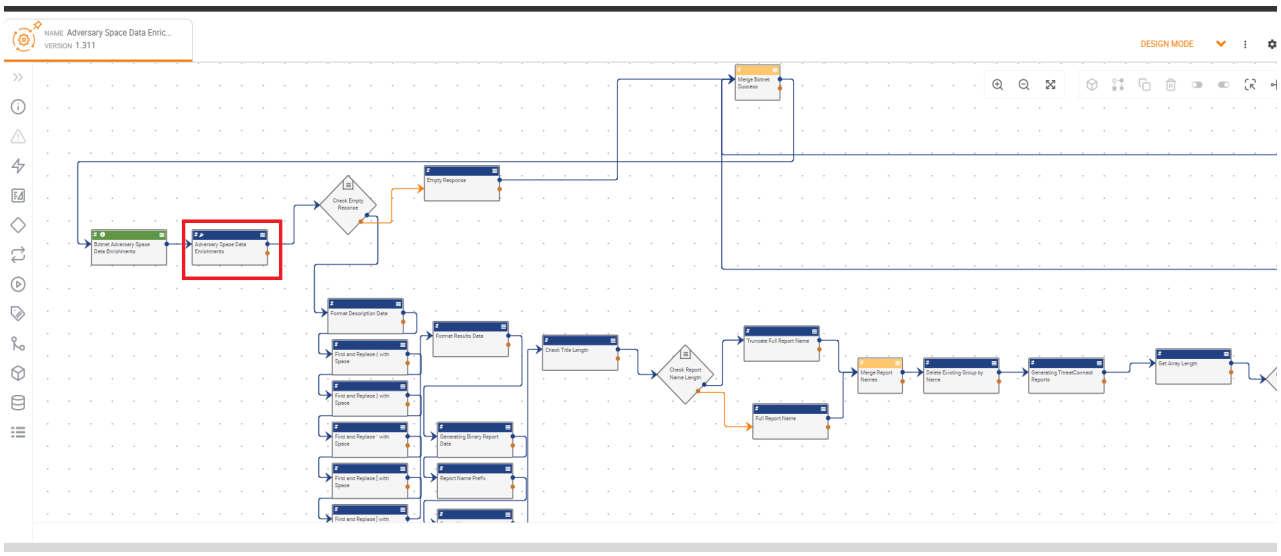


Step 4: Once the Playbook is activated, please click on the execute endpoint, this will fetch the results from Andariel API.

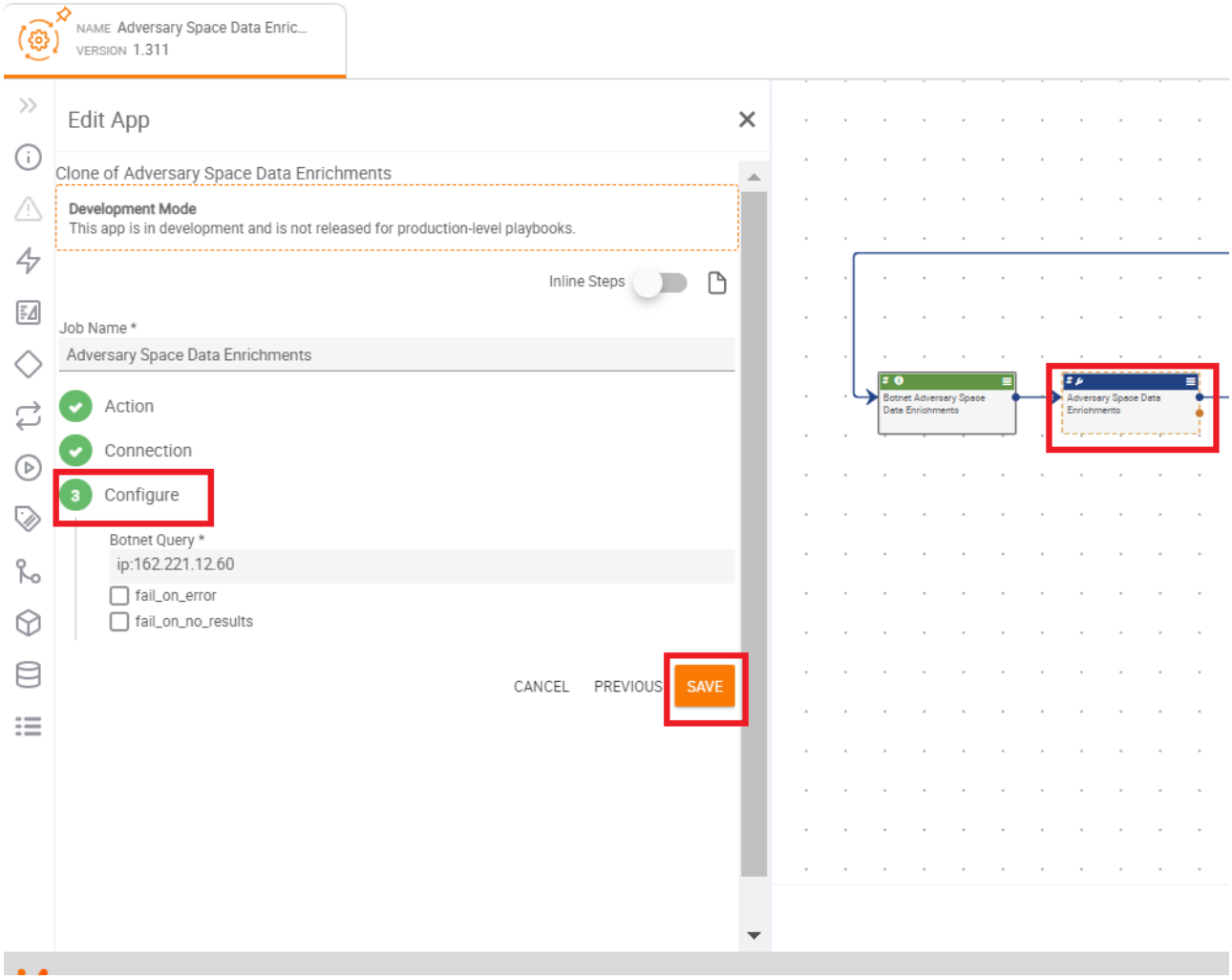


6. Running Adversary Space Data Enrichments Botnet Playbook

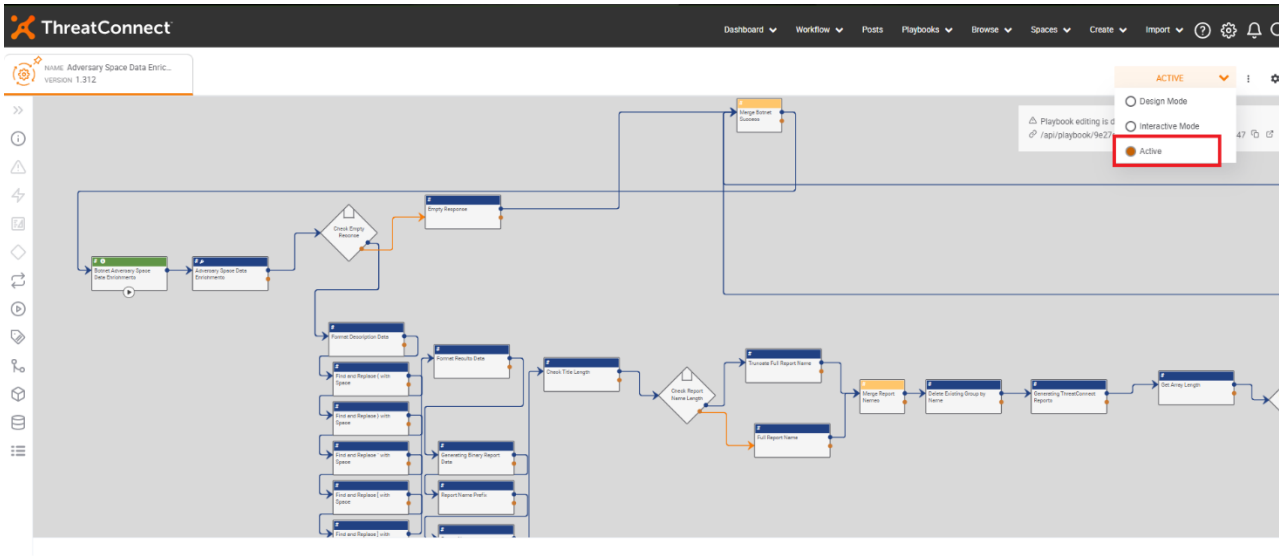
Step 1: Open the Adversary Space Data Enrichments Botnet Playbook, double click the App as shown below.



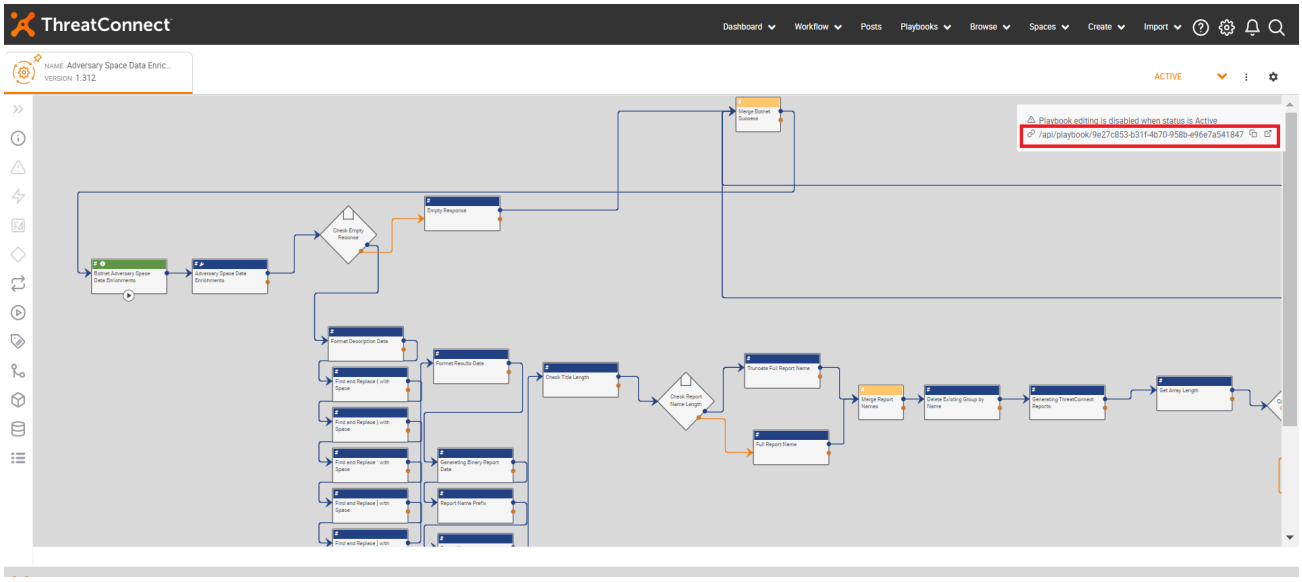
Step 2: Go to Configure section of the App and provide your desired values to search and click on Save as shown below.



Step 3: Activate the Playbook as shown below.

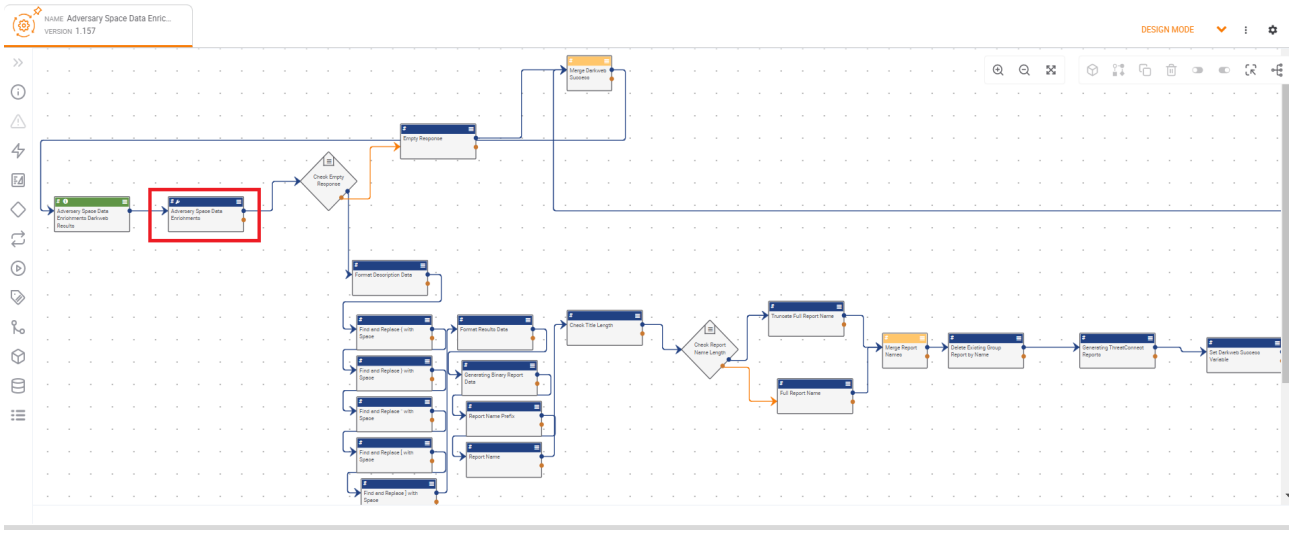


Step 4: Once the Playbook is activated, please click on the execute endpoint, this will fetch the results from Andariel API.

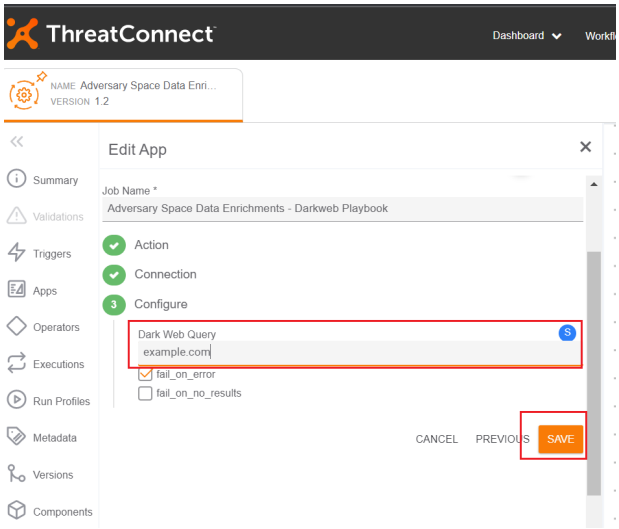


7. Running Adversary Space Data Enrichments Dark Web Playbook

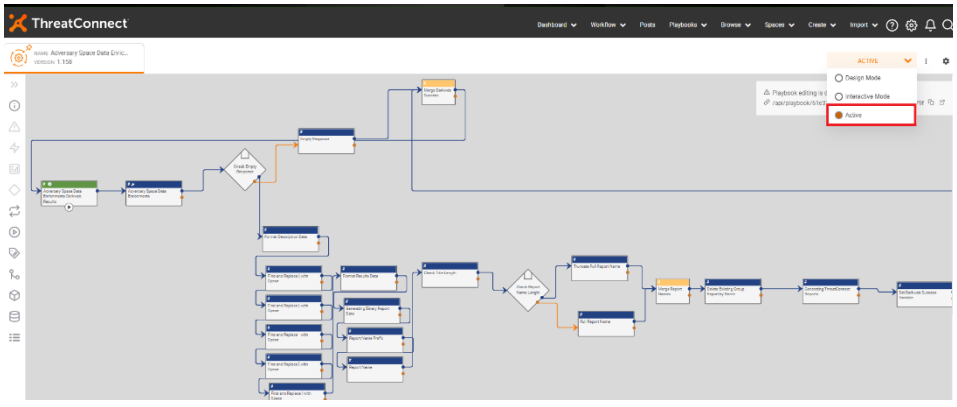
Step 1: Open the Adversary Space Data Enrichments Dark Web Playbook, double click the App as shown below.



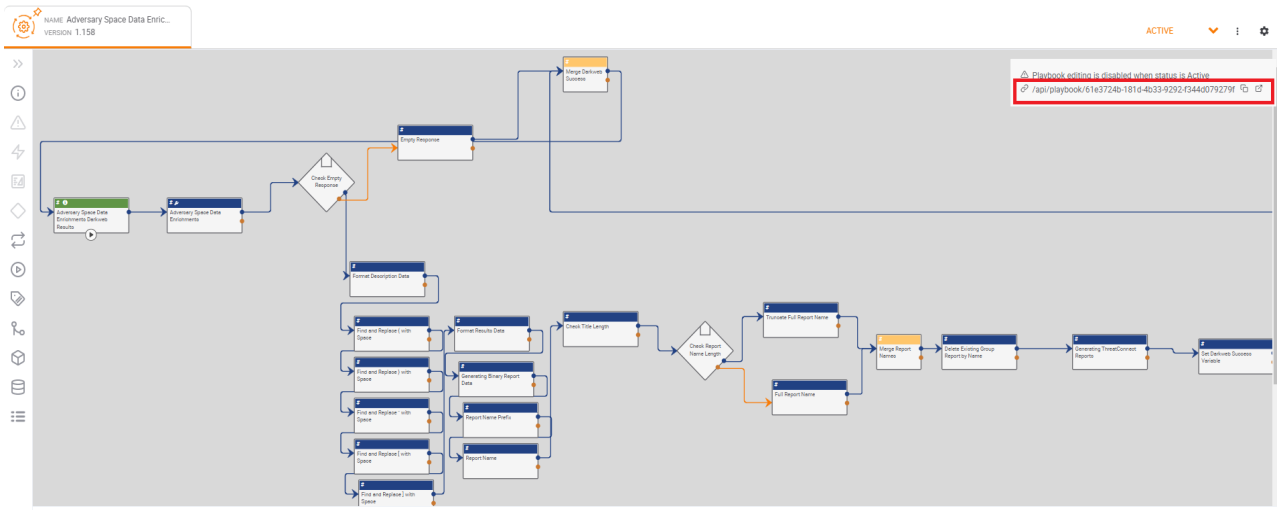
Step 2: Go to Configure section of the App and provide your desired values to search and click on Save as shown below.



Step 3: Activate the Playbook as shown below.

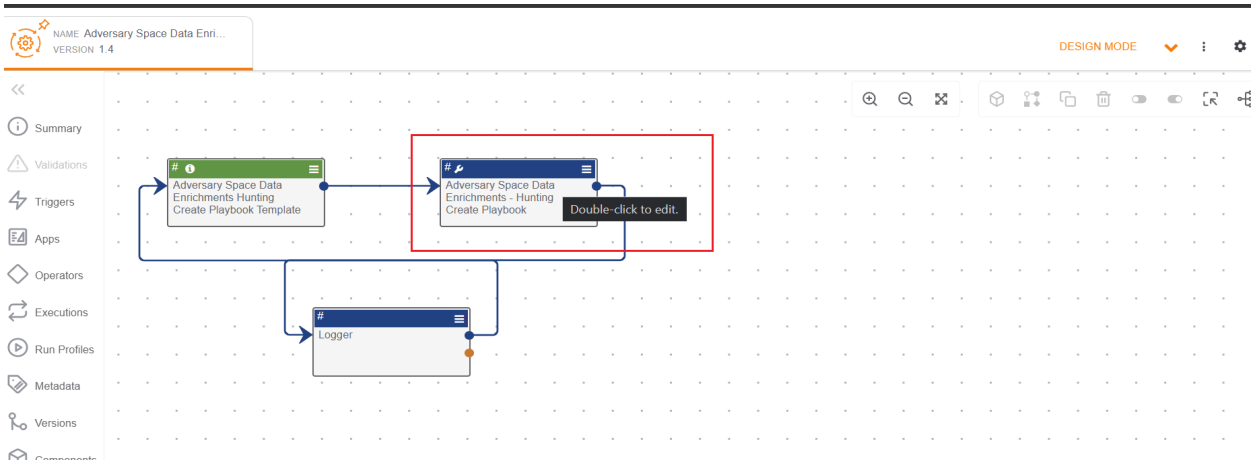


Step 4: Once the Playbook is activated, please click on the execute endpoint, this will fetch the results from Andariel API.

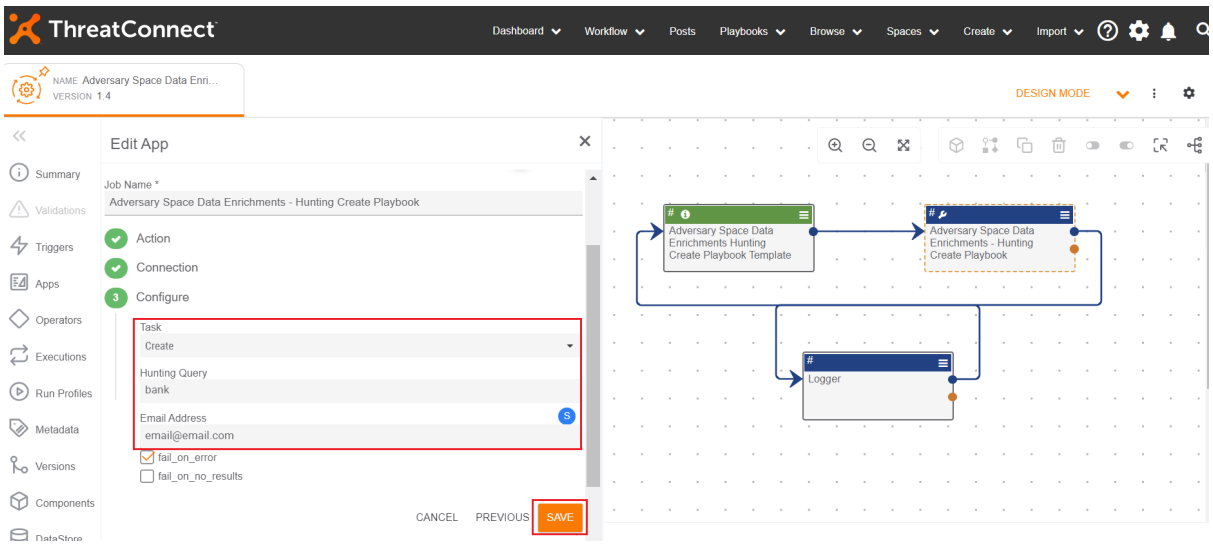


8. Running Adversary Space Data Hunting Create Playbook

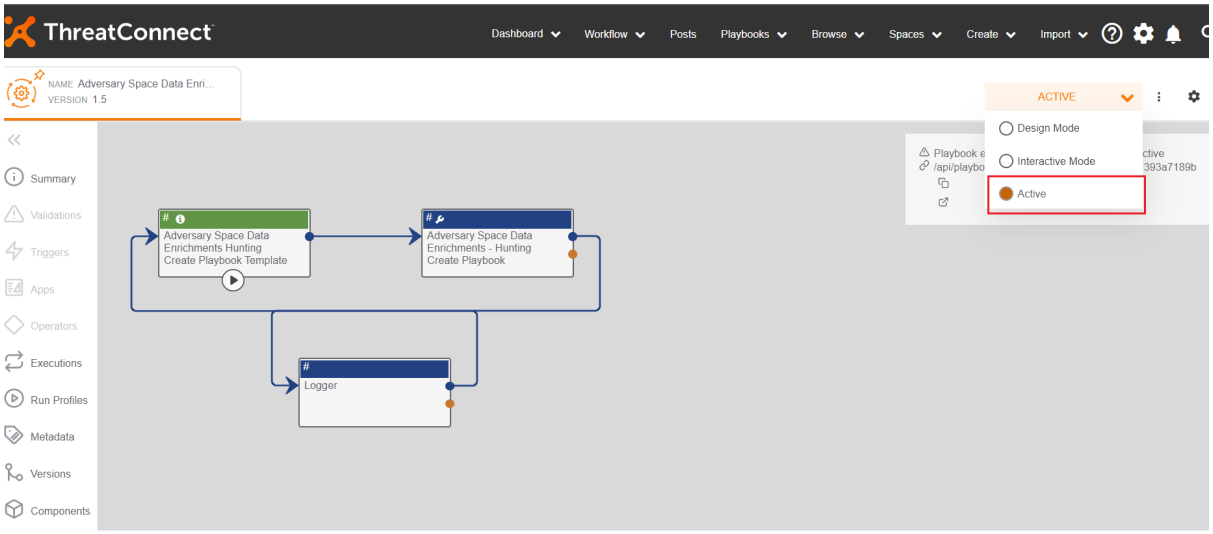
Step 1: Open the Adversary Space Data Enrichments Hunting Create Playbook, double click the App as shown below.



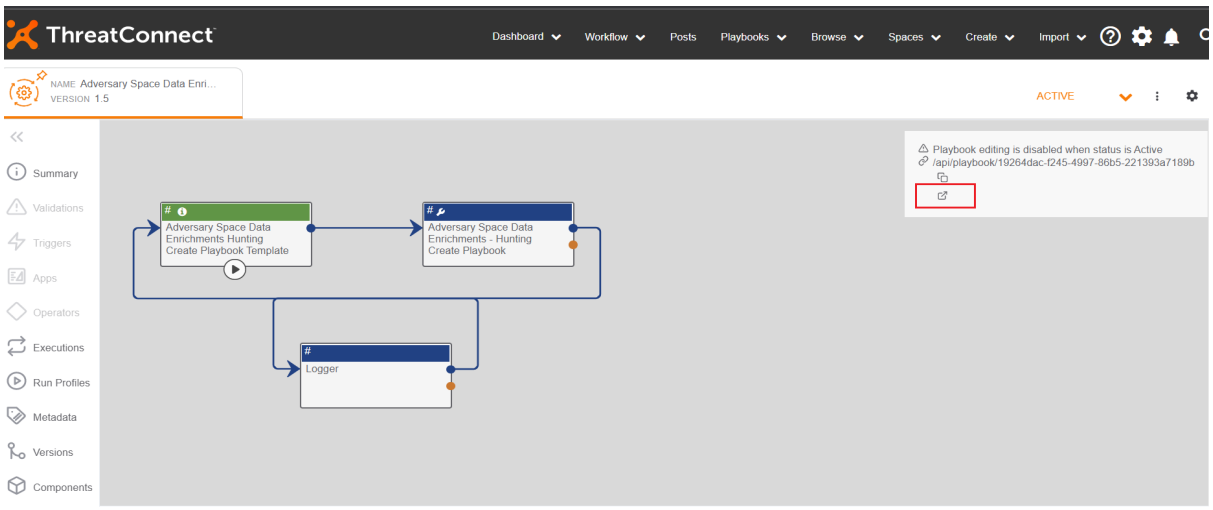
Step 2: Go to Configure section of the App and provide your desired values to search and click on Save as shown below.



Step 3: Activate the Playbook as shown below.

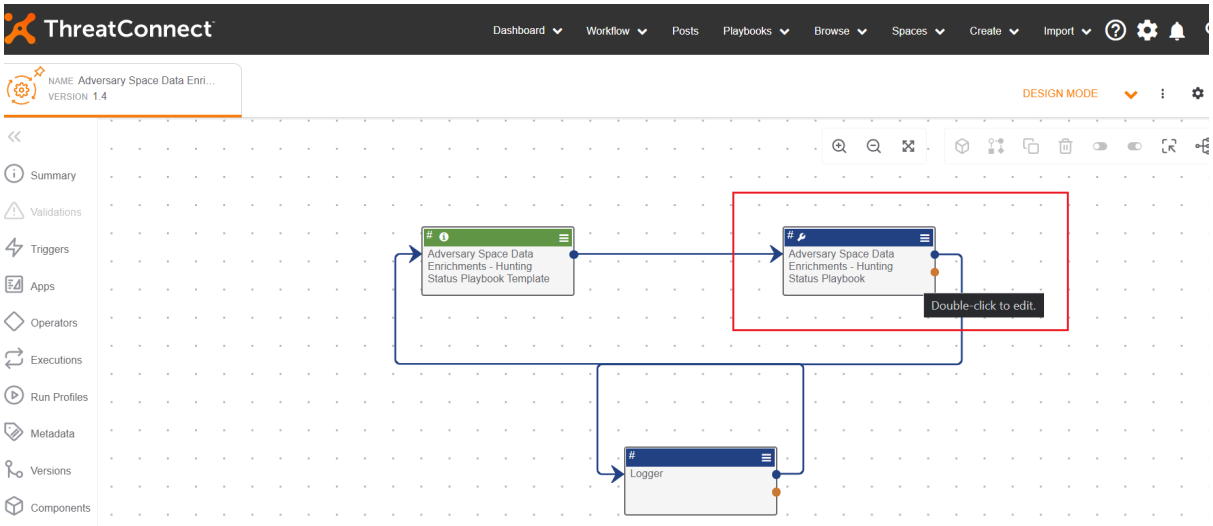


Step 4: Once the Playbook is activated, please click on the execute endpoint, this will fetch the results from Andariel API.

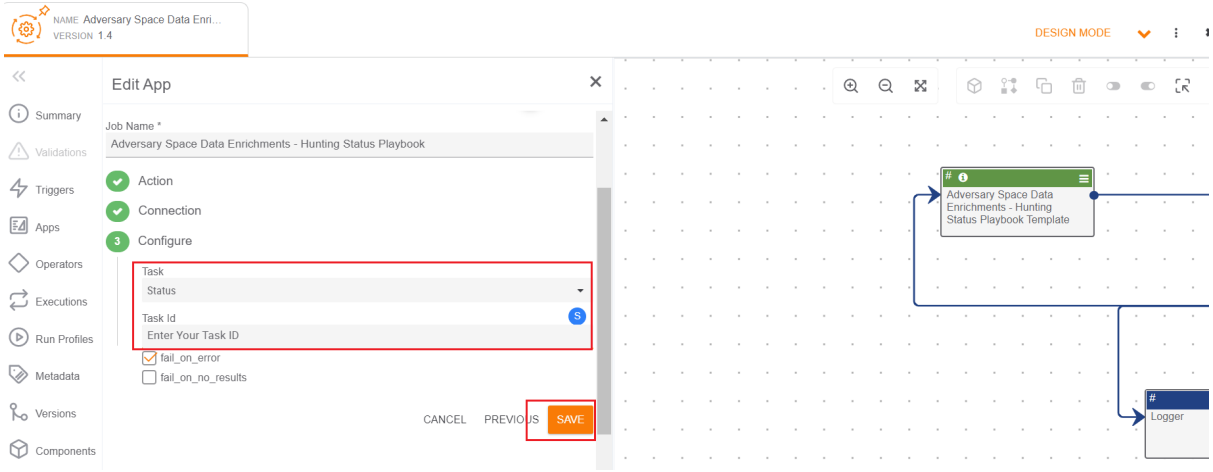


9. Running Adversary Space Data Hunting Status Playbook

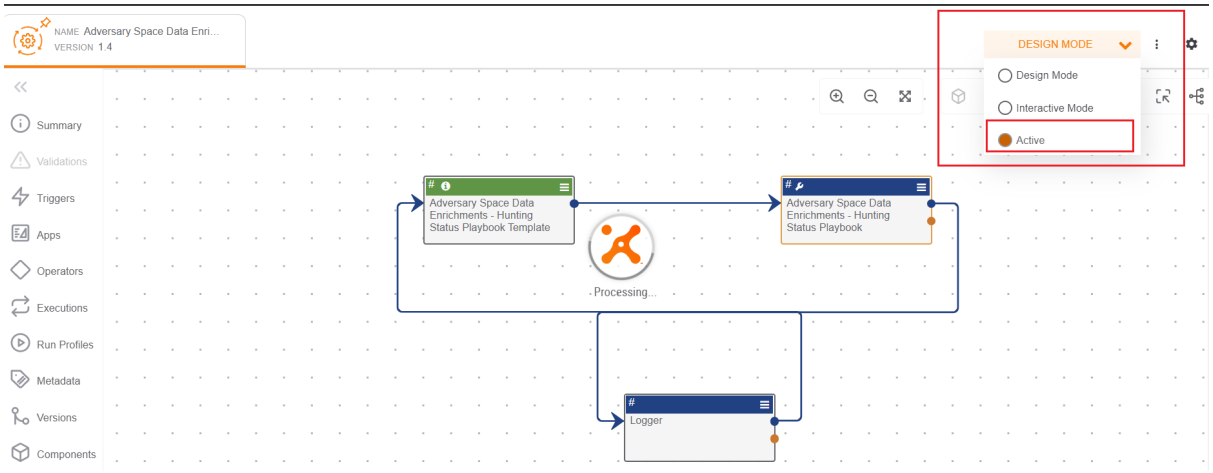
Step 1: Open the Adversary Space Data Enrichments Hunting Status Playbook, double click the App as shown below



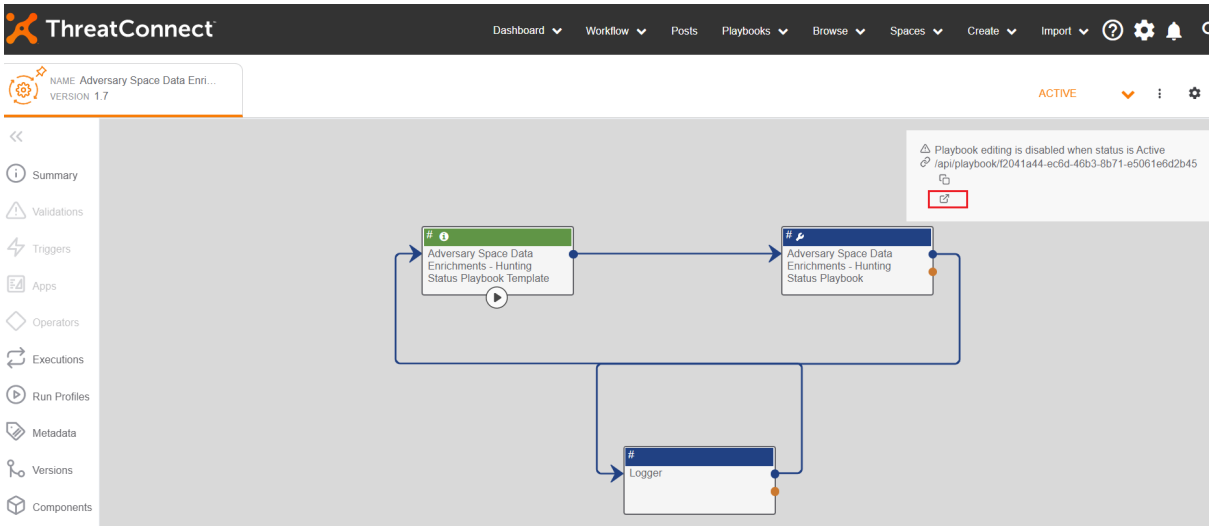
Step 2: Go to Configure section of the App and provide your desired values to search and click on Save as shown below.



Step 3: Activate the Playbook as shown below.

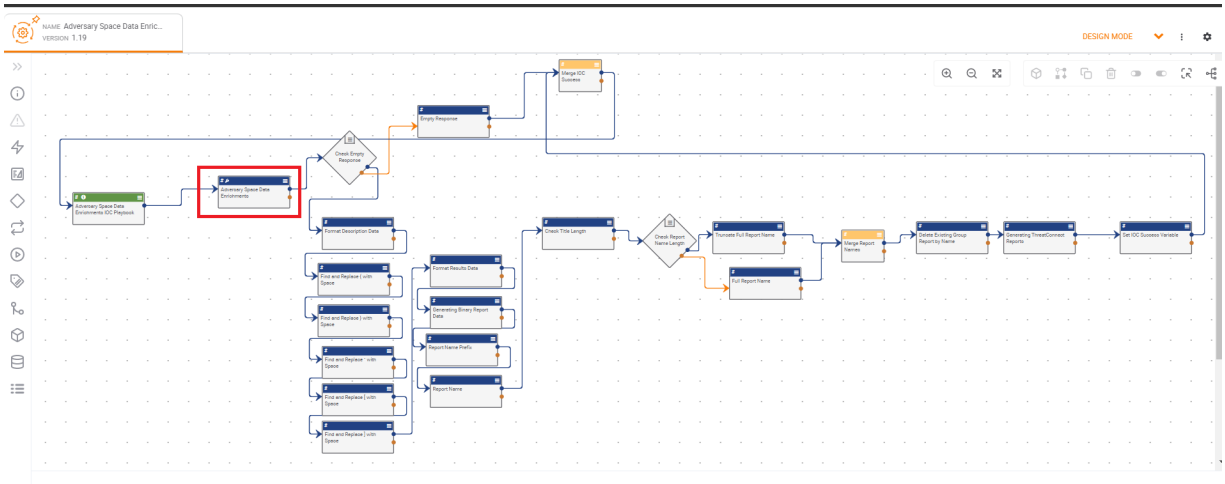


Step 4: Once the Playbook is activated, please click on the execute endpoint, this will fetch the results from Andariel API.

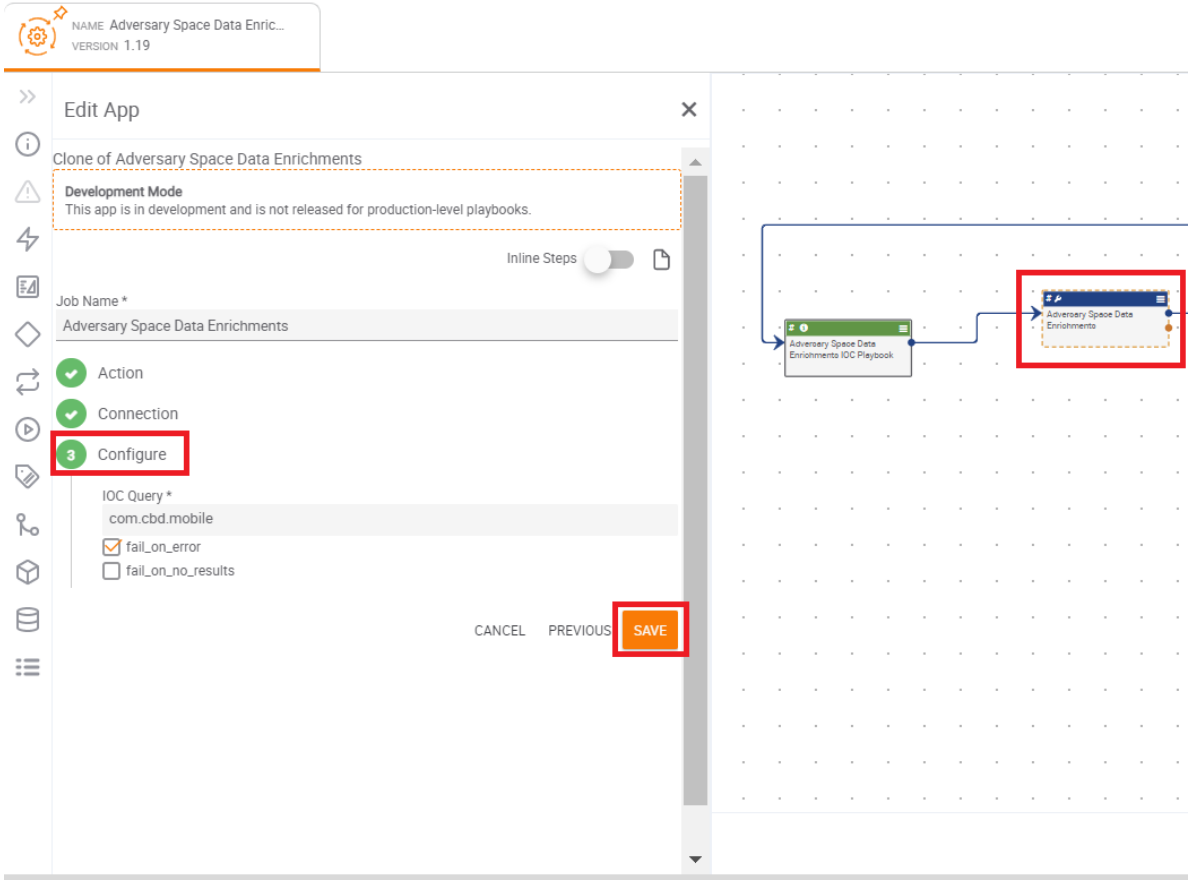


10. Running Adversary Space Data Enrichments IOC Playbook

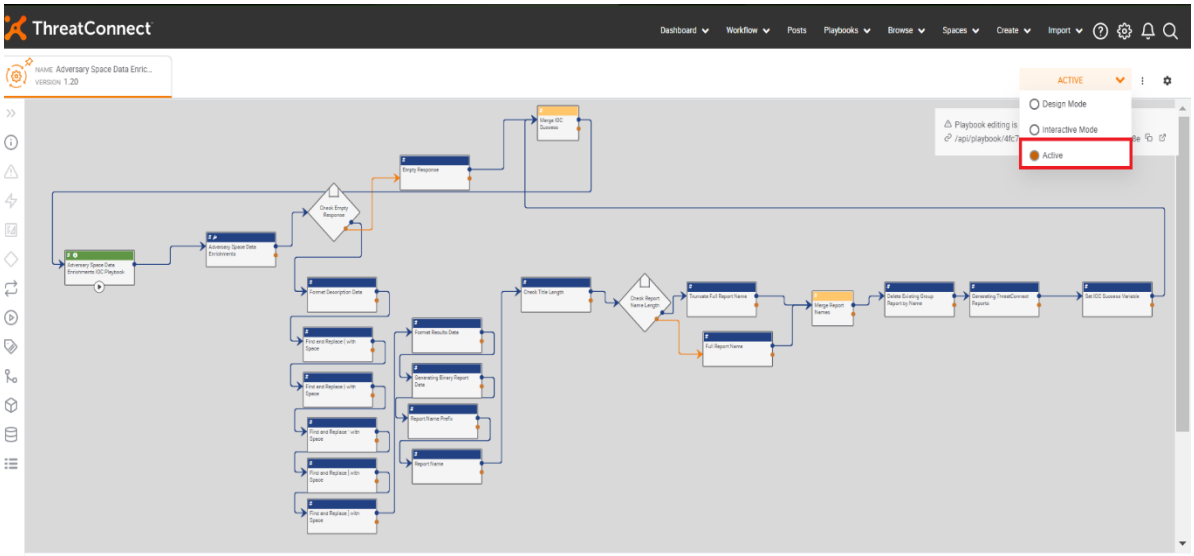
Step 1: Open the Adversary Space Data Enrichments IOC Playbook, double click the App as shown below.



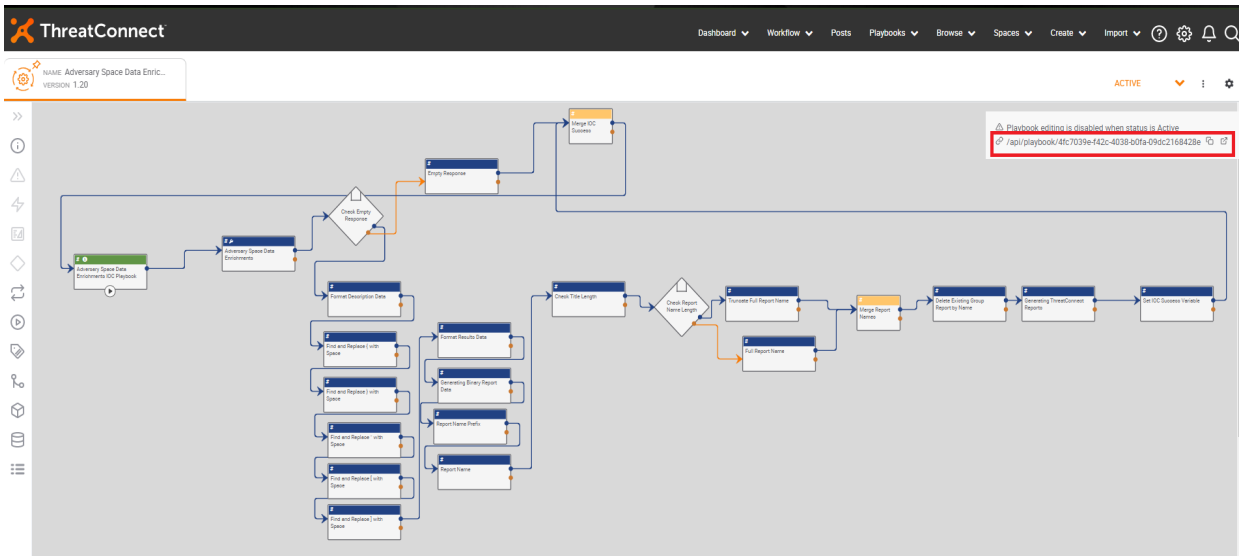
Step 2: Go to Configure section of the App and provide your desired values to search and click on Save as shown below.



Step 3: Activate the Playbook as shown below.



Step 4: Once the Playbook is activated, please click on the execute endpoint, this will fetch the results from Andariel API.



11. Playbooks

Let's go through the following playbooks:

11.1. Running Adversary Space Data Enrichments Botnet Playbook for Indicator and Groups

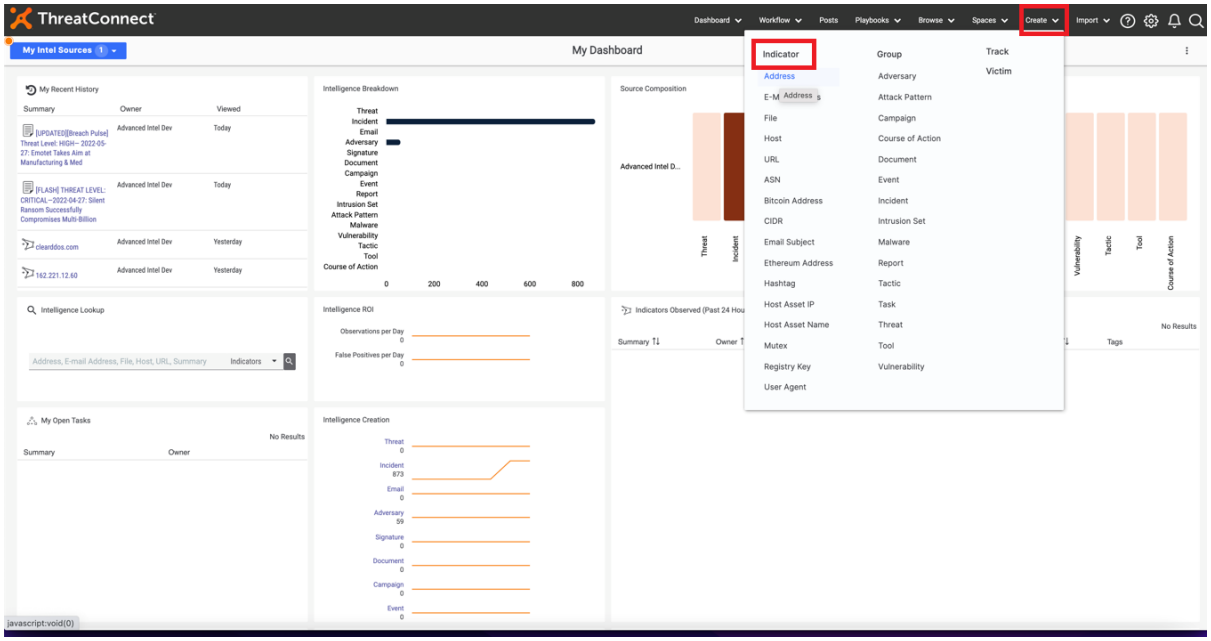
11.2. Running Adversary Space Data Enrichments BotCreds Playbook for Indicator and Groups

11.3. Running Adversary Space Data Enrichments IOC Playbook for Indicator and Groups

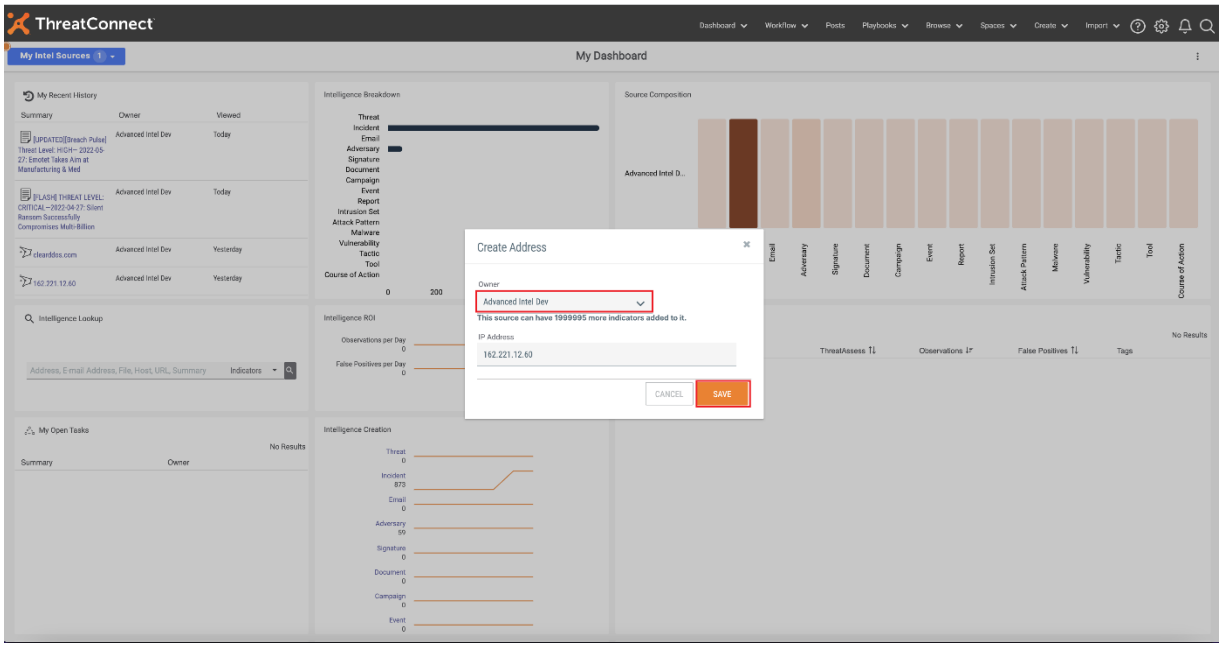
11.1 Running Adversary Space Data Enrichments Botnet Playbook for Indicator and Groups

Step 1: Make Sure the Playbook is set to active.

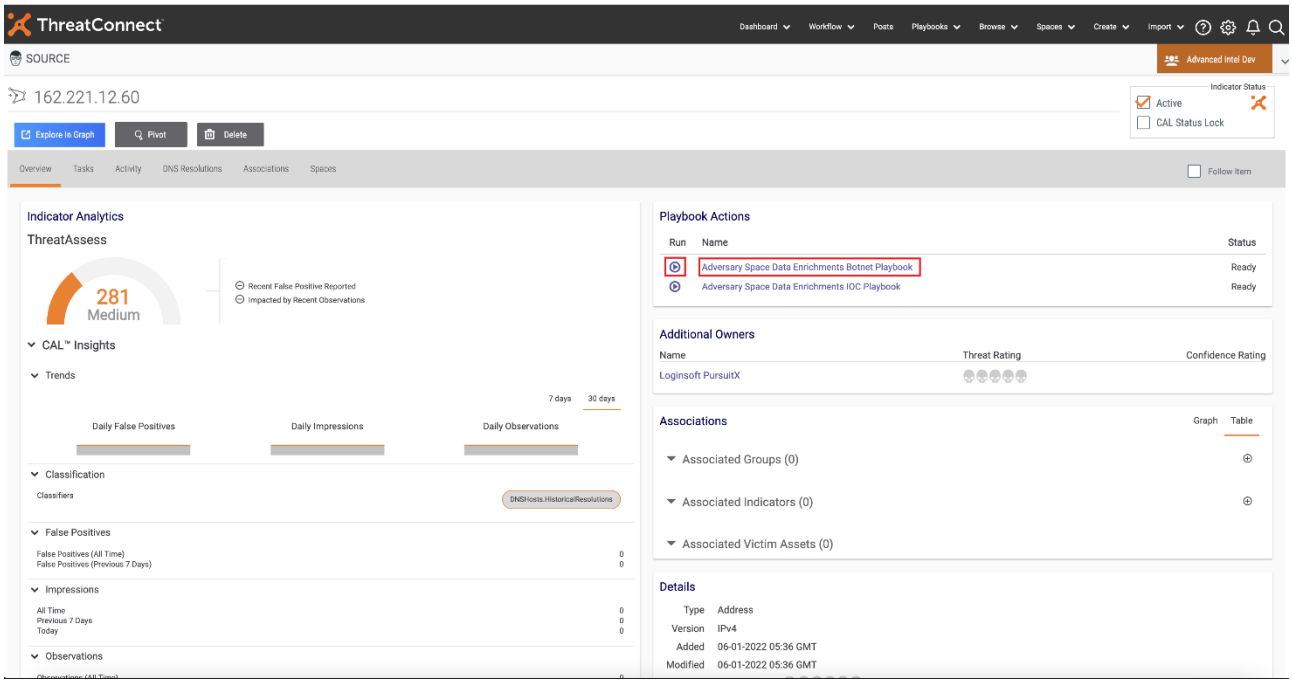
Step 2: Browse to the existing Address/Host/URL/ASN/Adversary/Malware Indicators/Groups (or) Create a new Address/Host/URL/ASN/Adversary/Malware Indicators/Groups.

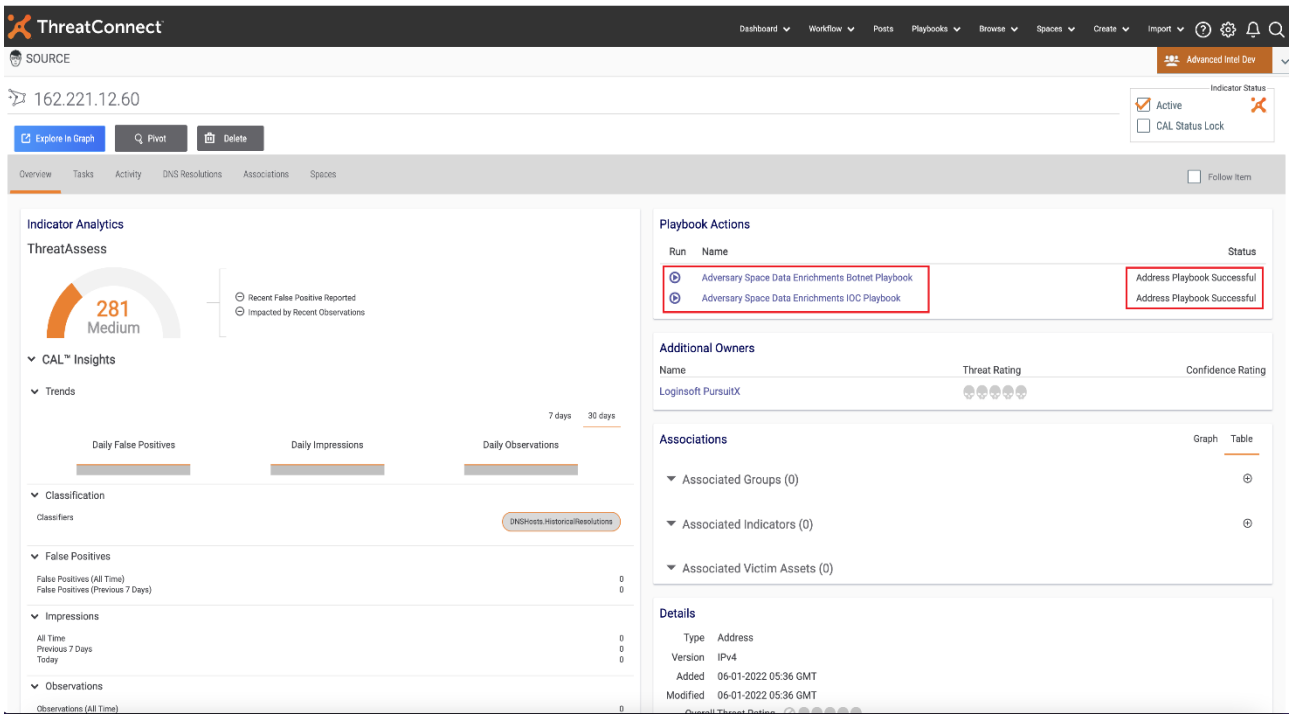


Please enter Address and Save

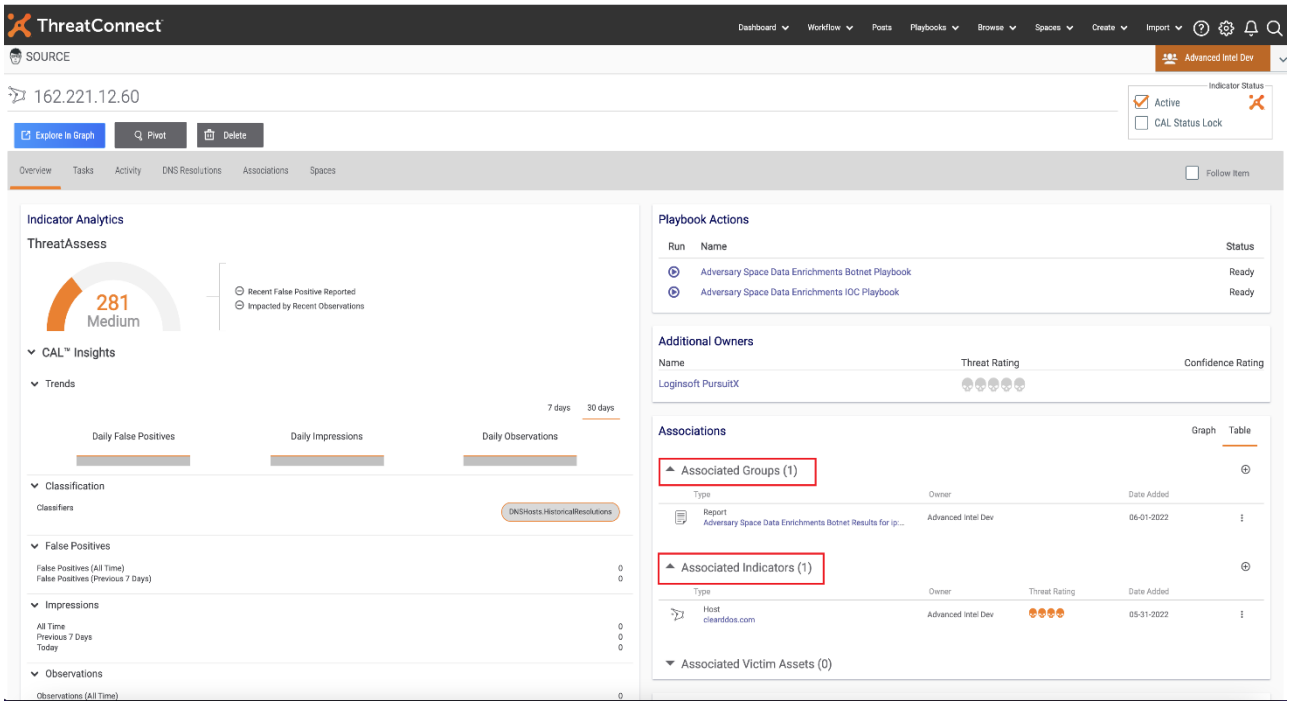


Now, run the required Playbook

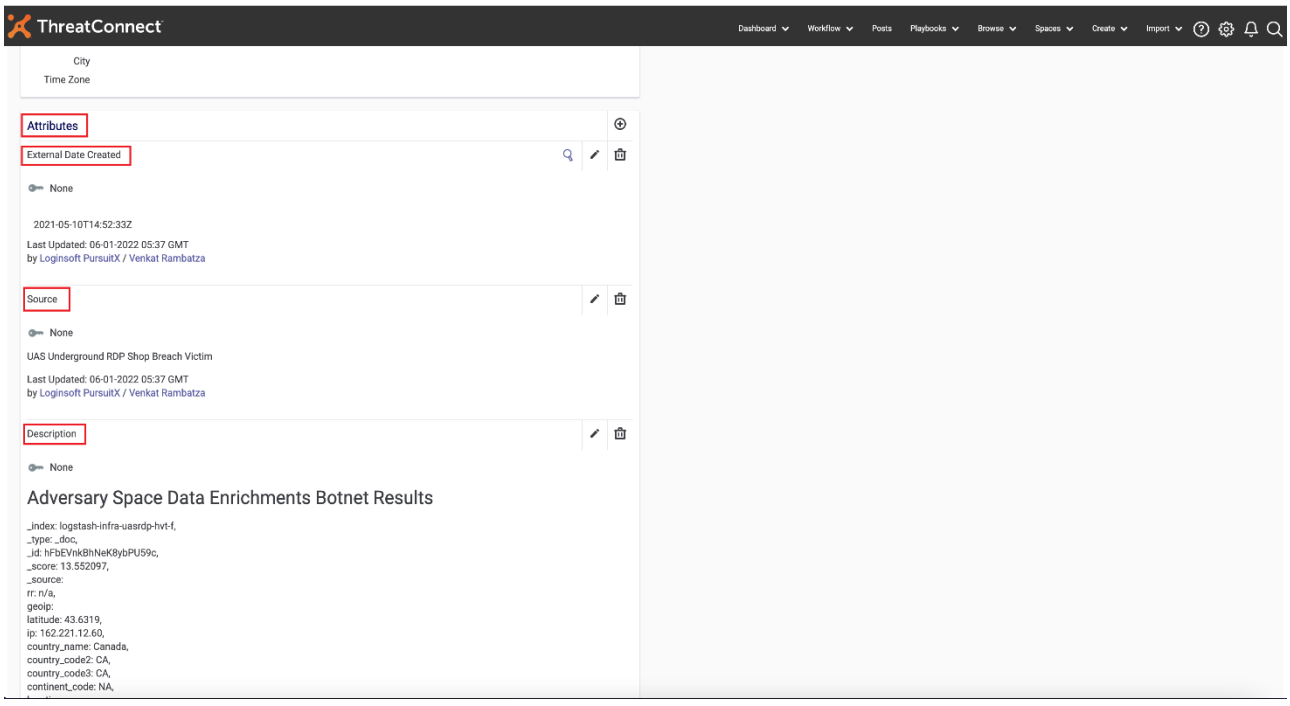




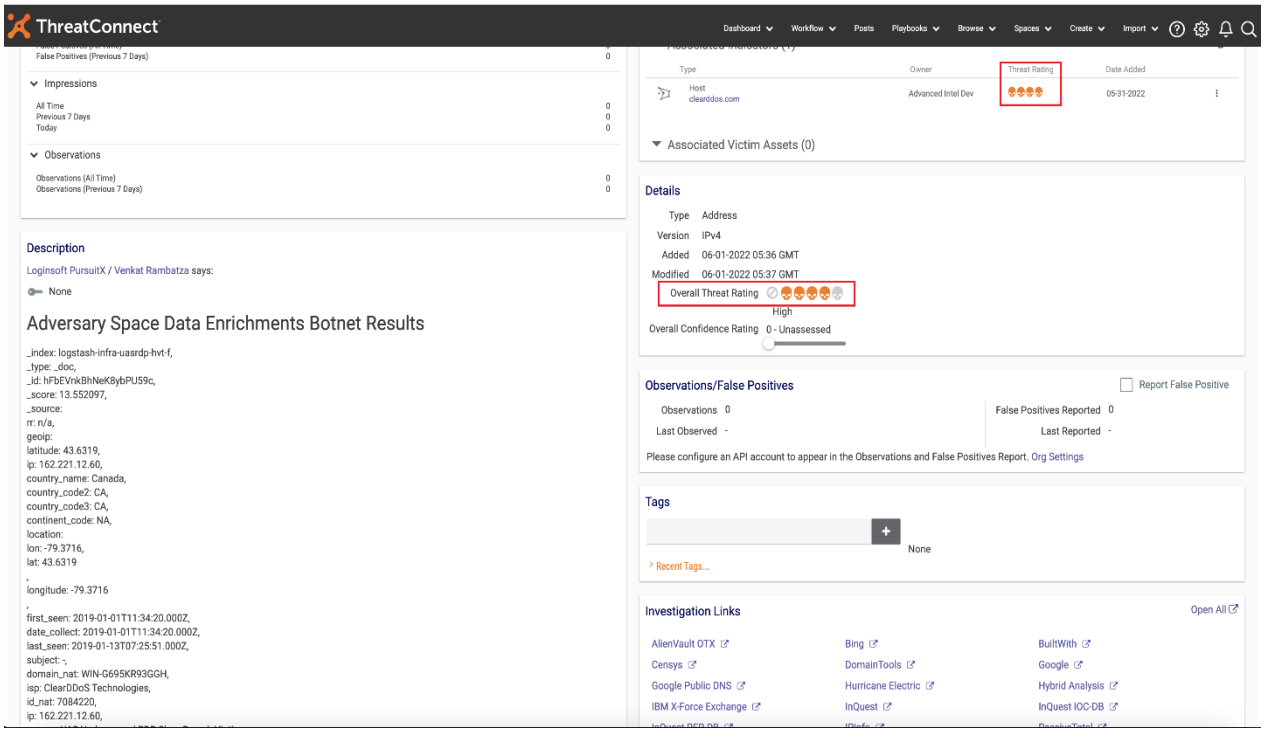
After successful completion of Playbook, need to refresh the page to get the required Attributes, Rating, Associations and Report.



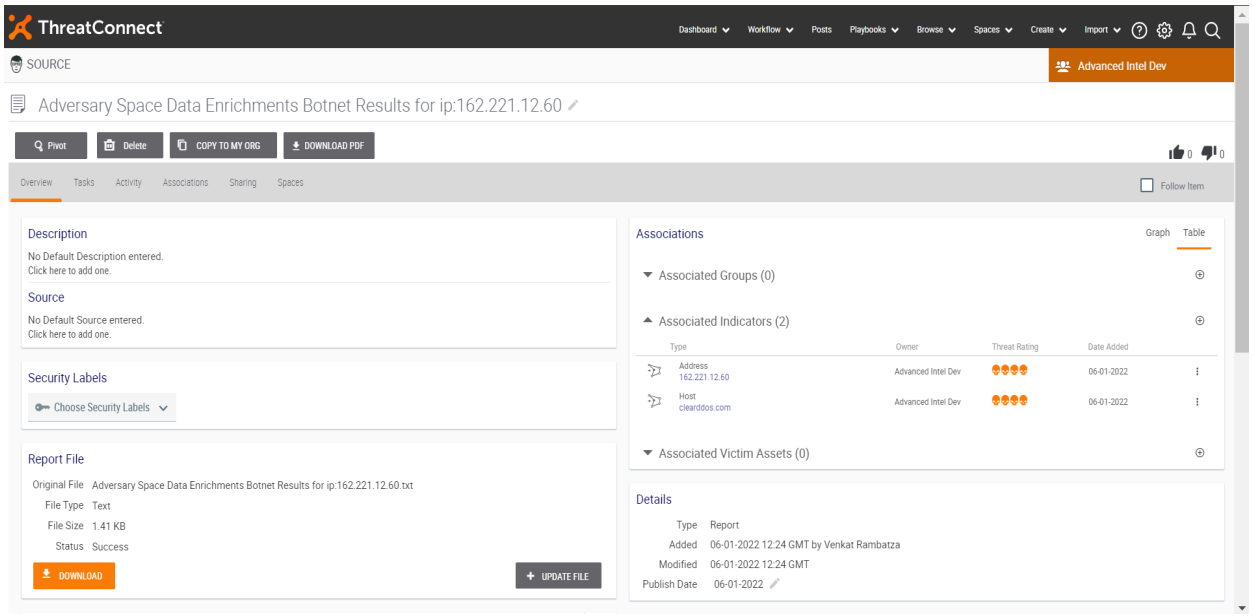
Here you can find the Attributes



You can find the overall threat rating as mentioned in below image.



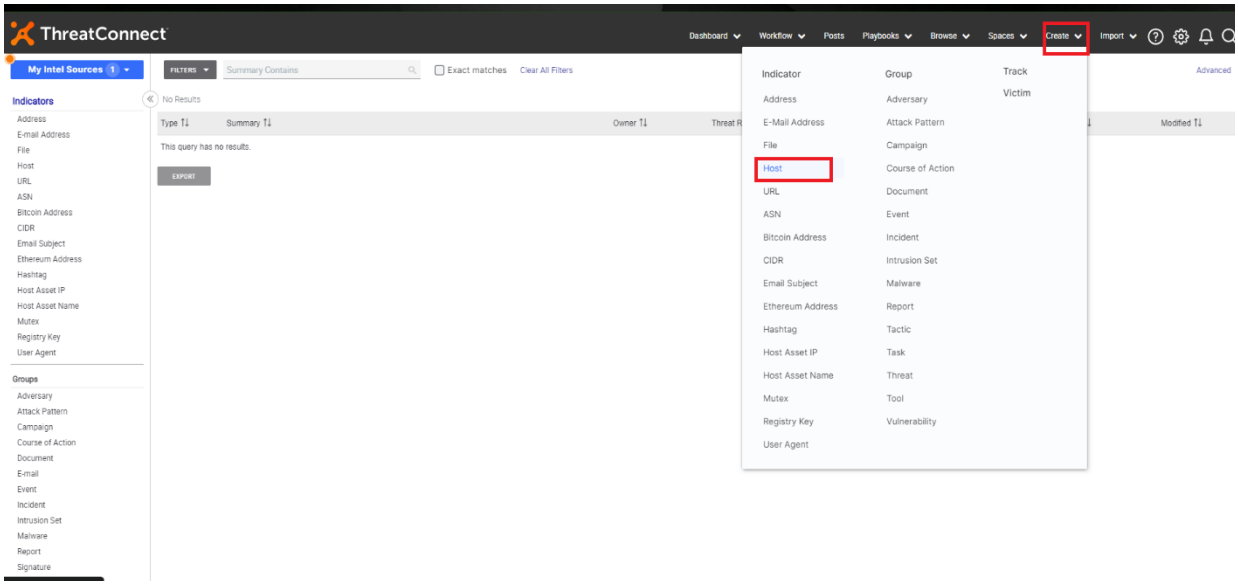
Now you can Download the Report



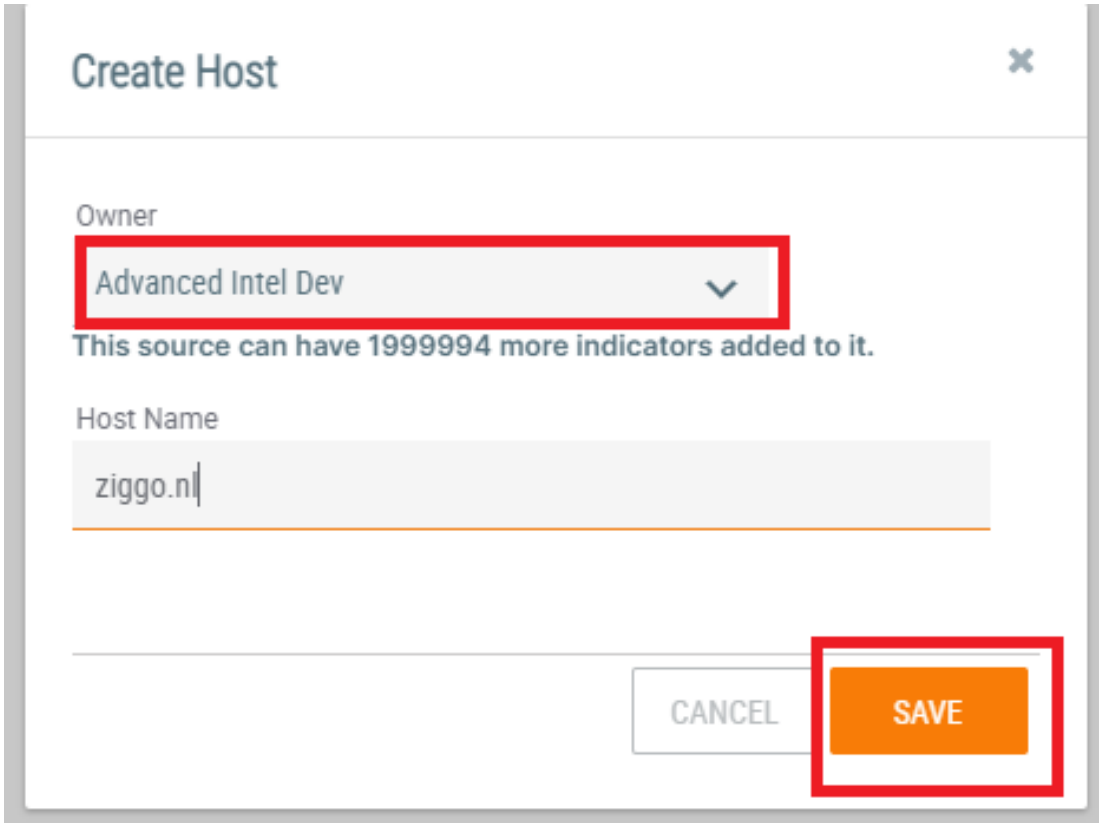
11.2 Running Adversary Space Data Enrichments BotCreds Playbook for Indicator and Groups

Step 1: Make Sure the Playbook is set to active.

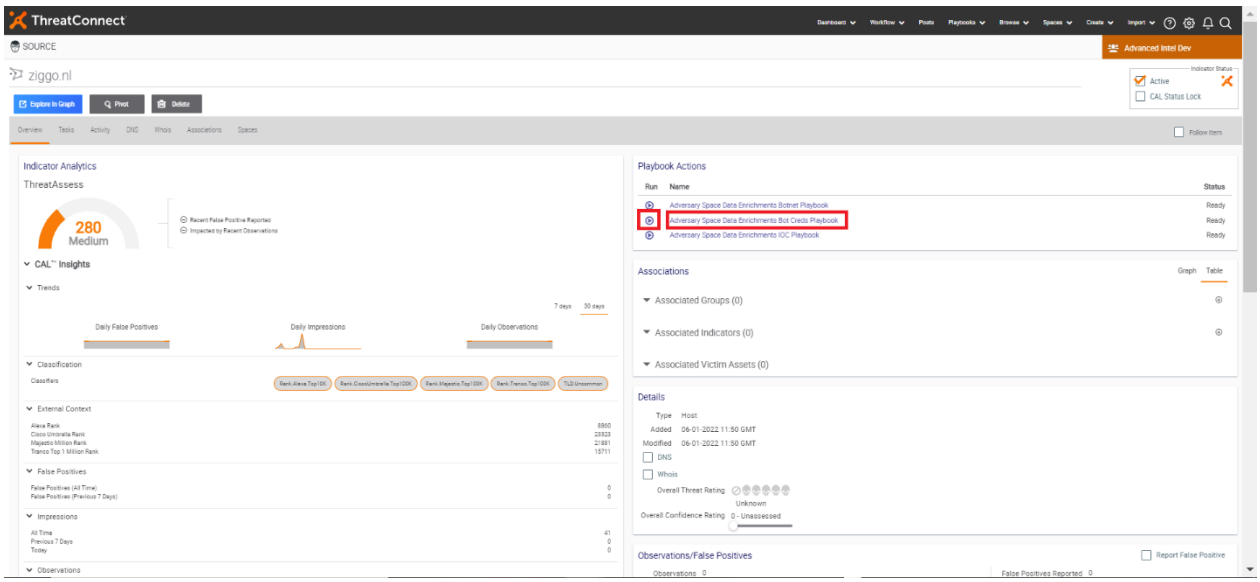
Step 2: Browse to the existing Host/Email Address/URL Indicators (or) Create a new Host/Email Address/URL Indicators.

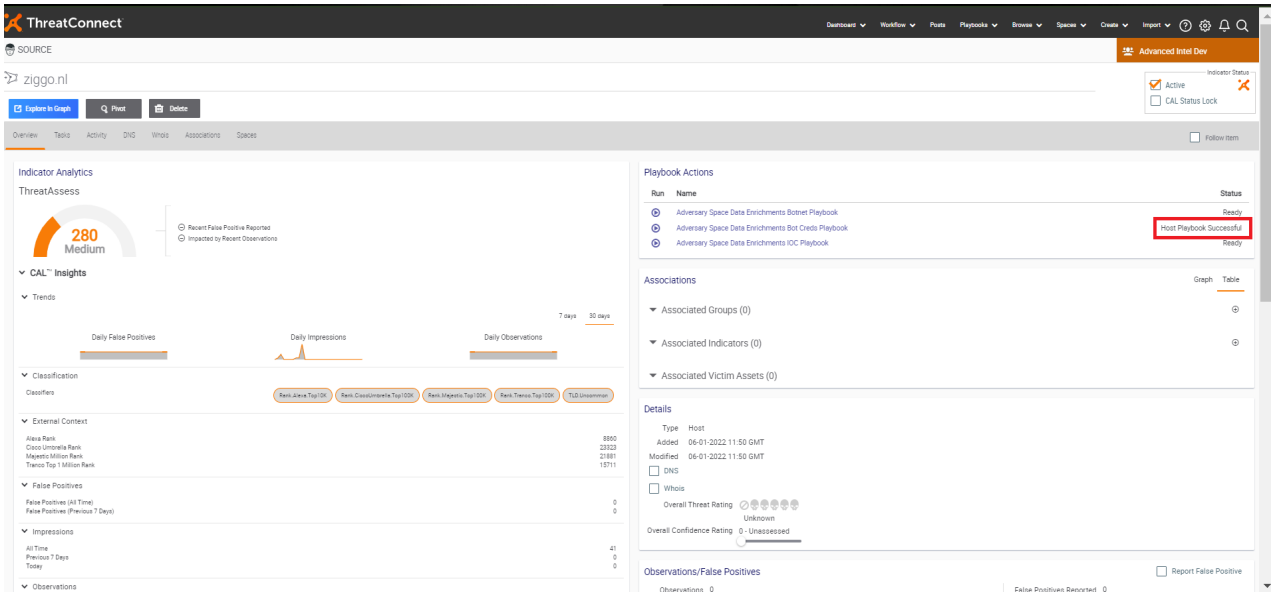


Please enter host address and Save

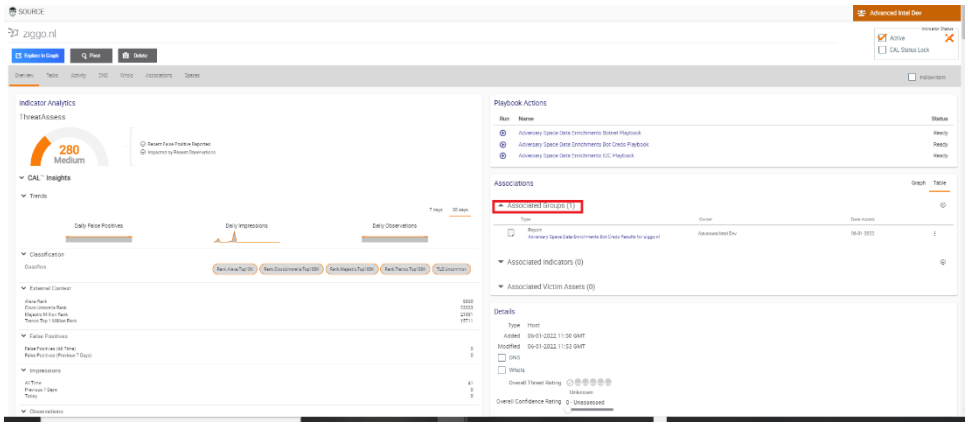


Now, run the required Playbook

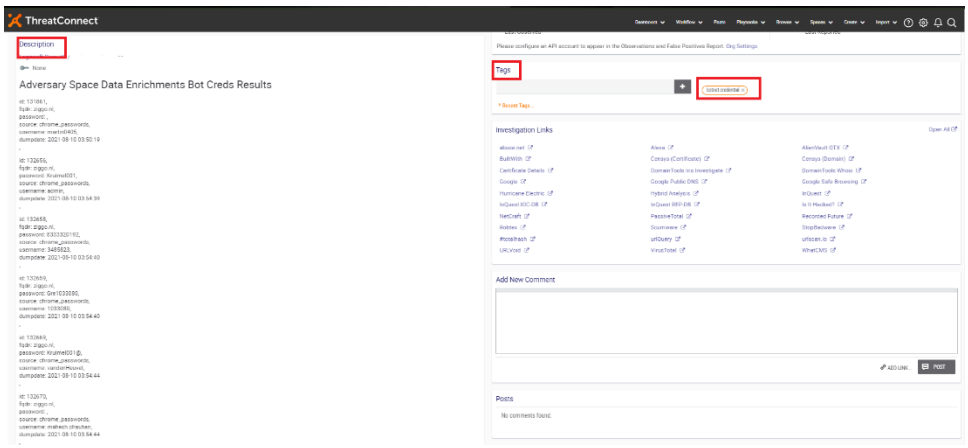




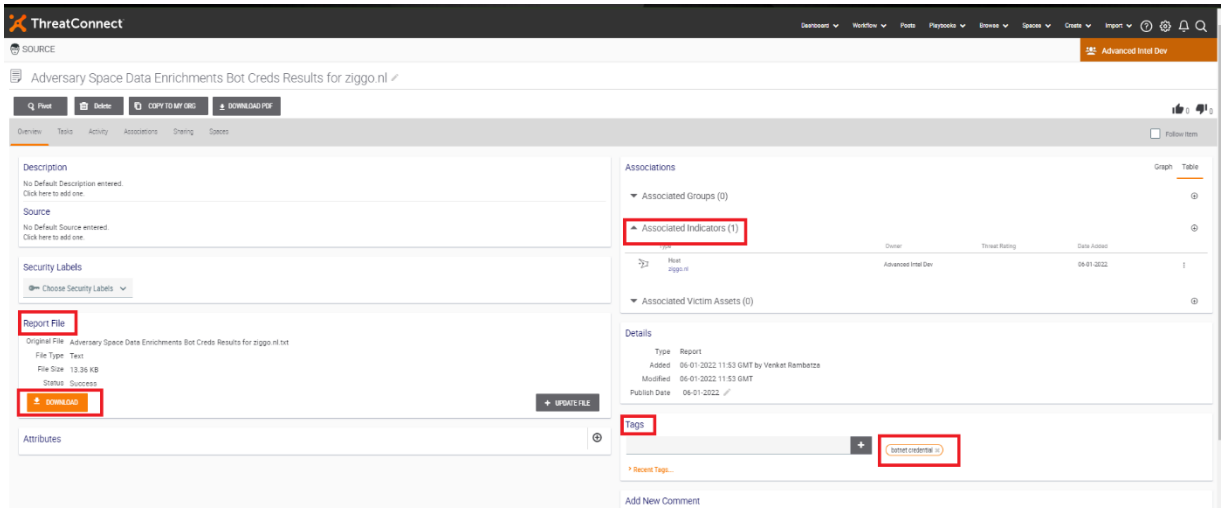
After successful of Playbook, refresh the page and get the required Attributes, Associations and Report.



Here you can find the Attributes and tag (botnet credentials)



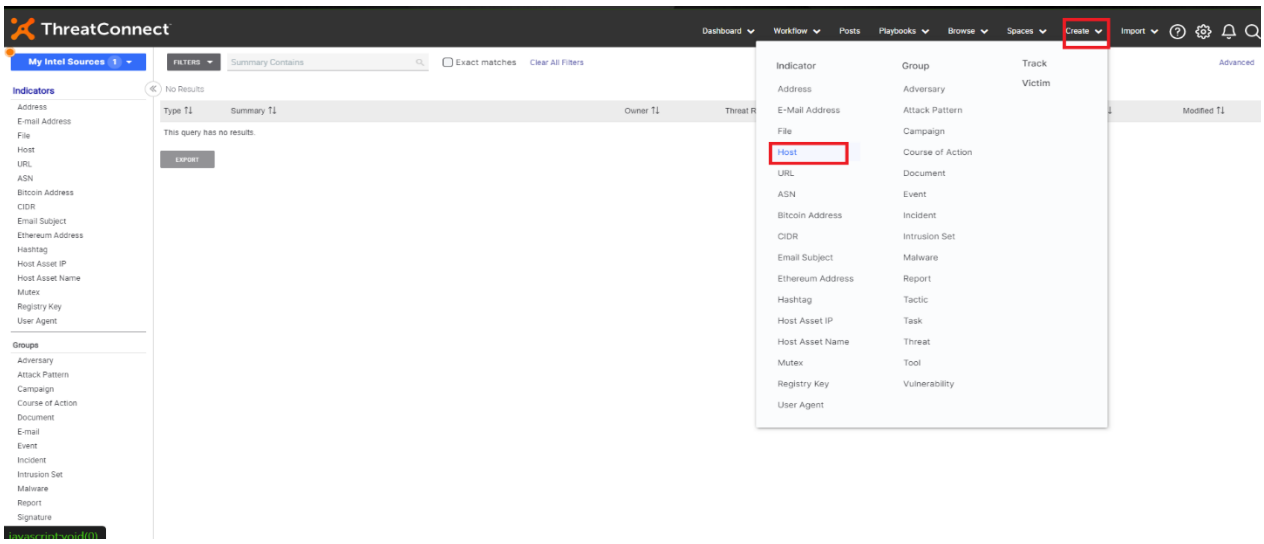
Here you are enabled to download report



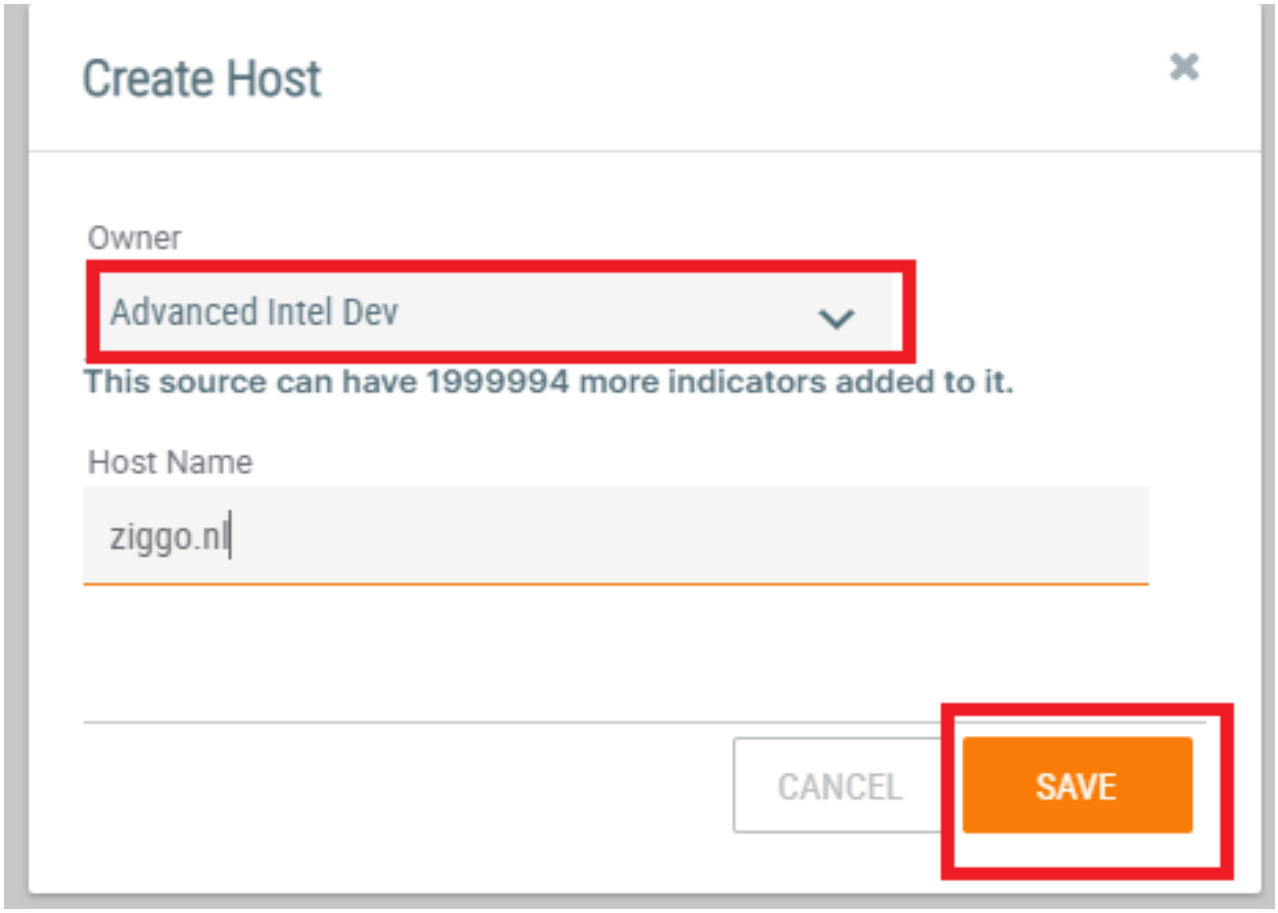
11.3 Running Adversary Space Data Enrichments IOC Playbook for Indicator and Groups

Step 1: Make Sure the Playbook is set to active.

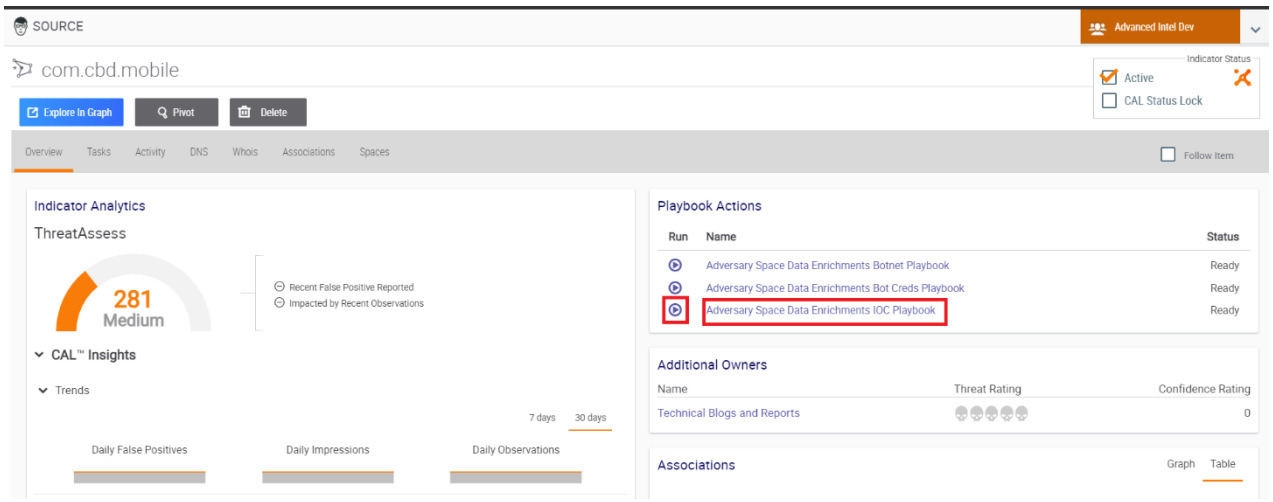
Step 2: Browse to the existing Address/Host/URL/File Indicators (or) Create a new Address/Host/URL/File Indicators.

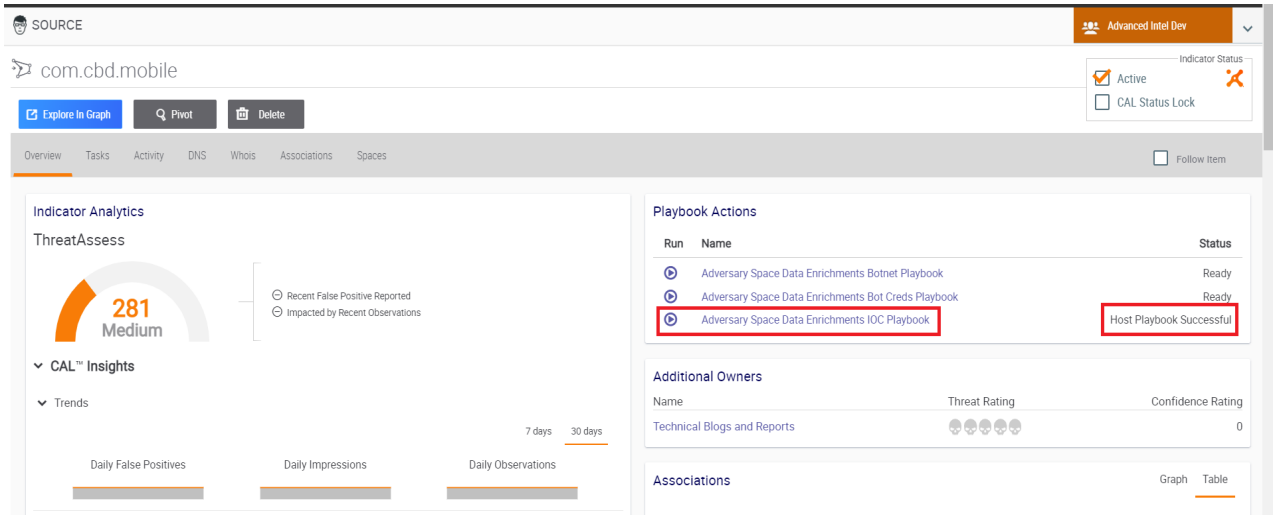


Please enter the host address and save

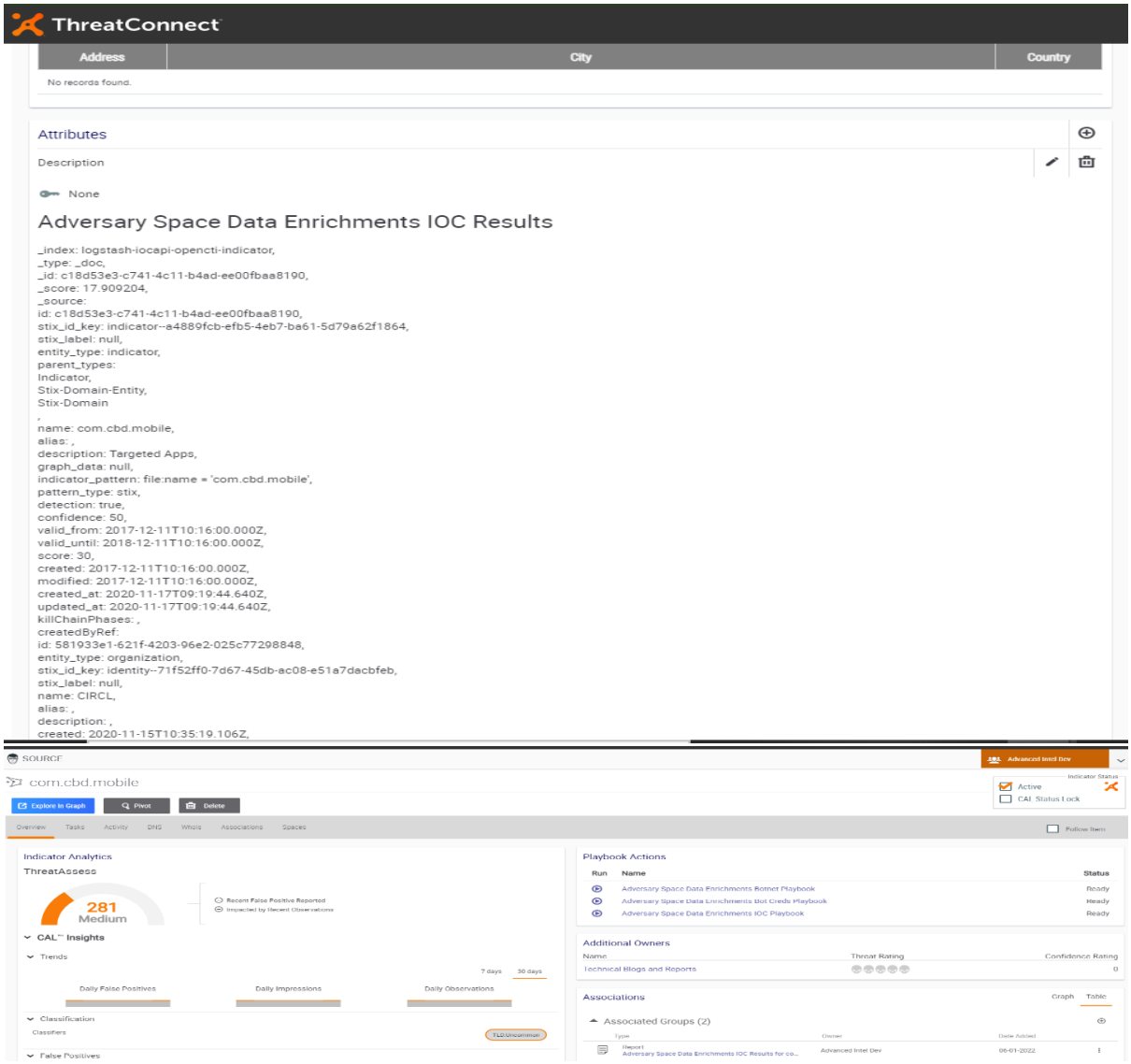


Now, run the required playbook.





After successful of Playbook, refresh the page and get the required Attributes, Associations and Report.



Now you can download report