



# 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	<a href="mailto:support@advintel.tech">support@advintel.tech</a>
----------------	--

## Version History

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

## Table of Contents

Support .....	1
Version History .....	1
1. Introduction.....	3
2. Configuration .....	4
2.1. Pre-Requisites.....	4
2.2. Adversary Space Data Enrichments App Installation.....	4
2.3. Adversary Space Data Enrichments App Configuration.....	4
3. Outputs.....	6
4. Adversary Space Data Enrichments Playbook .....	6
4.1. Adversary Space Data Enrichments Playbook Installation.....	6
4.2. Andariel API Key Variable Set Up.....	6
5. Running Adversary Space Data Enrichments Bot Creds Playbook.....	7
6. Running Adversary Space Data Enrichments Botnet Playbook .....	9
7. Running Adversary Space Data Enrichments Dark Web Playbook .....	11
8. Running Adversary Space Data Hunting Create Playbook .....	13
9. Running Adversary Space Data Hunting Status Playbook.....	15
10. Running Adversary Space Data Enrichments IOC Playbook.....	16
11. Playbooks.....	18
11.1 Running Adversary Space Data Enrichments Botnet Playbook for Indicator and Groups.....	19
11.2 Running Adversary Space Data Enrichments BotCreds Playbook for Indicator and Groups ...	22
11.3 Running Adversary Space Data Enrichments IOC Playbook for Indicator and Groups .....	25

### 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

<b>Output</b>	<b>TC Type</b>	<b>Description</b>
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.

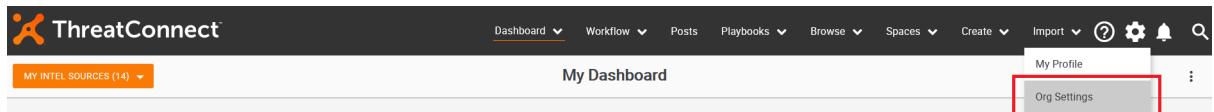
To install these Playbooks, go to the Playbooks tab within the ThreatConnect Platform. Select New > Import and locate the .pbx file you wish to add to your ThreatConnect Platform. Follow the on-screen instructions to complete the Playbook import.

### 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.

## ThreatConnect – Adversary Space Data Enrichments App User Guide

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



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

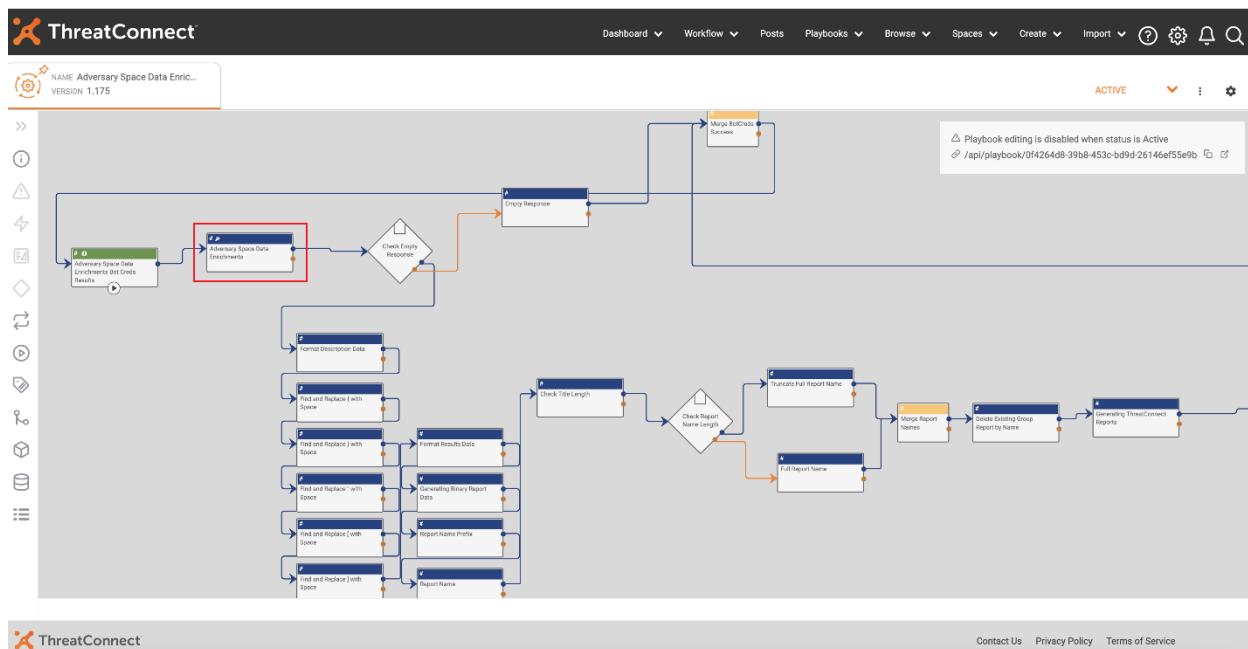
The image contains two screenshots. The top screenshot shows the 'Organization Settings' page for 'IPQualityScore'. It has tabs for Membership, Communities/Sources, Groups, Invitations, Variables (which is highlighted with a red box), Metrics, Settings, Apps, and Styling. A 'NEW VARIABLE' button is also highlighted with a red box. The bottom screenshot shows a 'Property' dialog box. It has fields for Type (set to KEYCHAIN), Name (set to 'Andariel API Key'), and Value (containing a masked API key). The 'SAVE' button at the bottom right is highlighted with a red box.

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

# ThreatConnect – Adversary Space Data Enrichments App User Guide



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

The screenshot shows the ThreatConnect 'Edit App' configuration page for the 'Adversary Space Data Enrichments' app. The configuration section is highlighted with a red box, and the 'Configure' tab is selected (also highlighted with a red box).

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

**Job Name:** Adversary Space Data Enrichments

**Search By:** Domain

**Domain:** example.com

**From Date:** (empty)

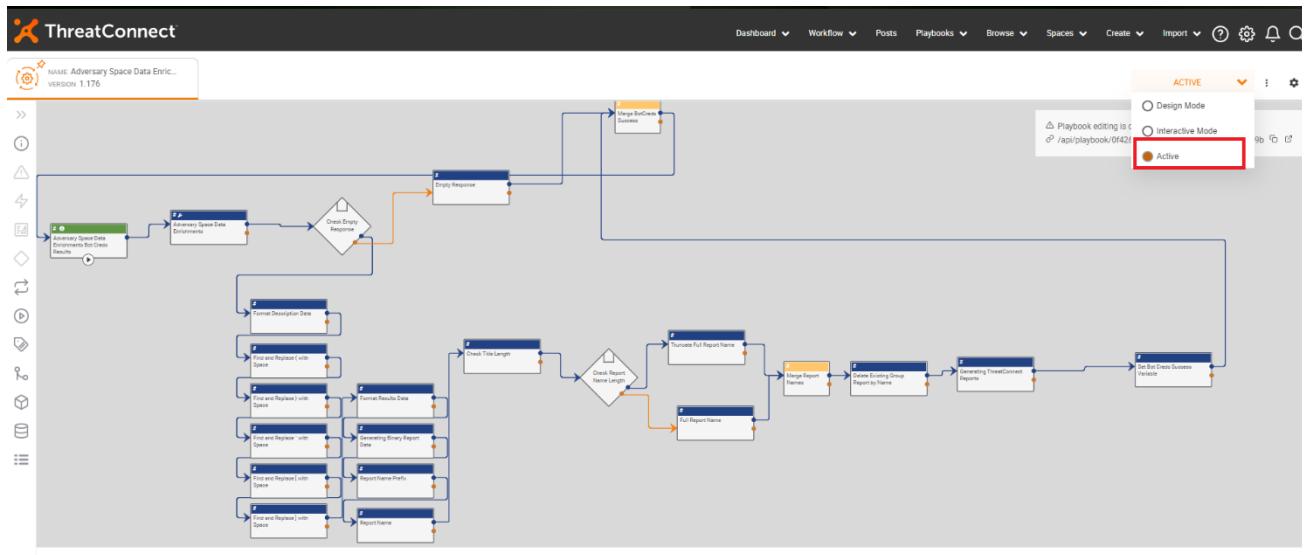
**To Date:** (empty)

**Configuration Options:**

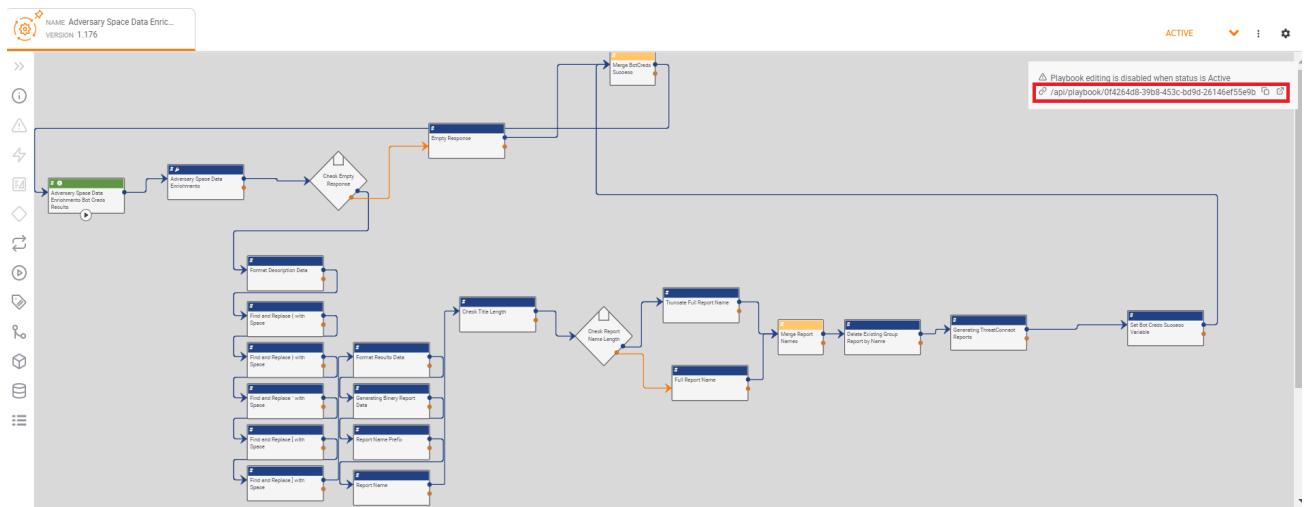
- fail\_on\_error
- fail\_on\_no\_results

**Buttons:** CANCEL, PREVIOUS, SAVE (highlighted with a red box).

**Step 3:** Activate the Playbook as shown below.



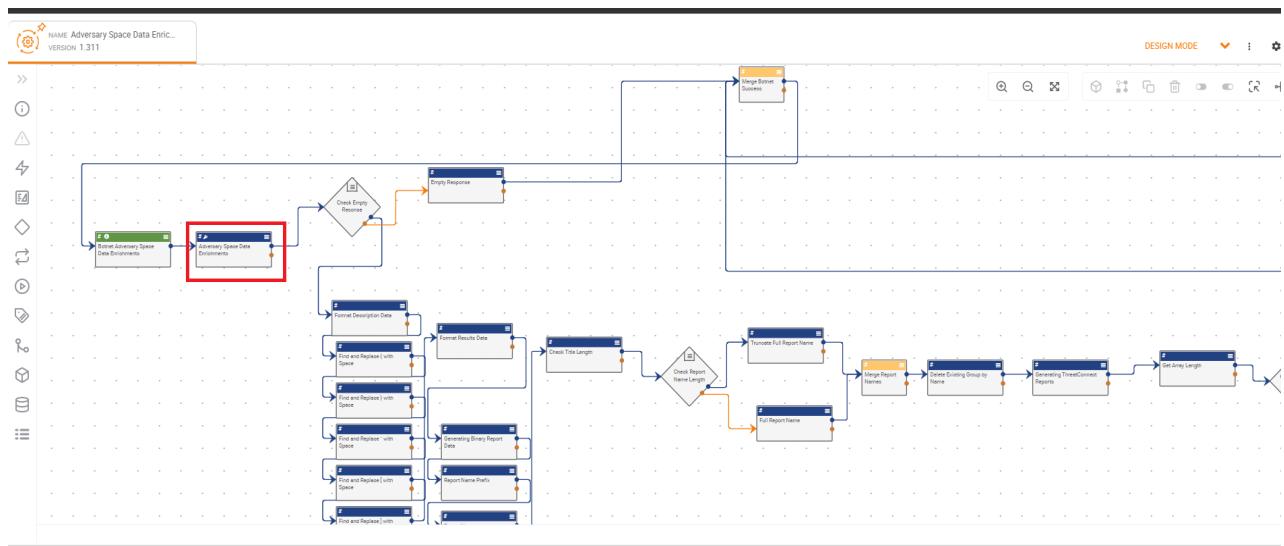
**Step 4:** Once the Playbook is activated, please click on the execute endpoint, this will fetch the results from Andariel API.



## 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.

## ThreatConnect – Adversary Space Data Enrichments App User Guide

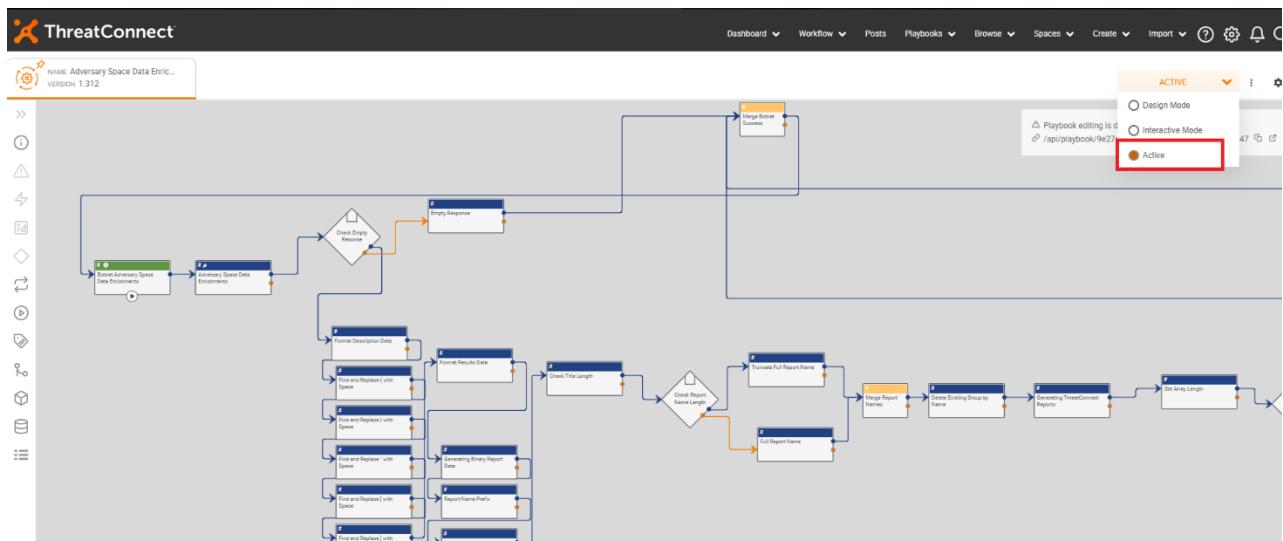


**Step 2:** Go to Configure section of the App and provide your desired values to search and click on Save as shown below.

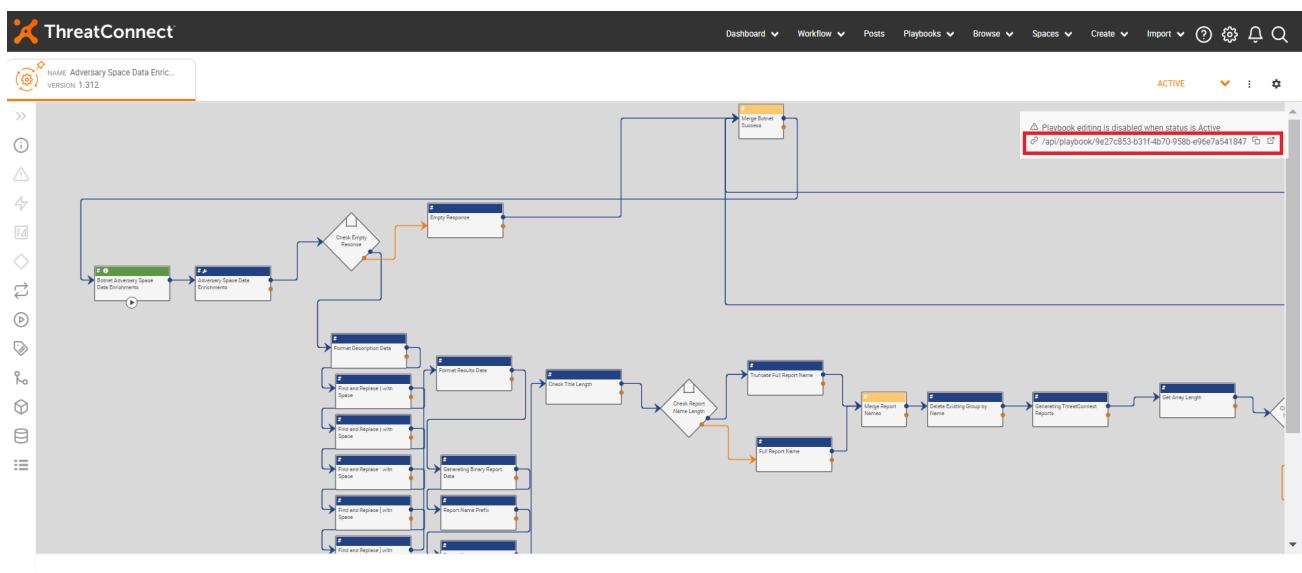
The screenshot shows the ThreatConnect app configuration dialog for 'Adversary Space Data Enrichments'. The 'Configure' tab is selected and highlighted with a green box. The 'SAVE' button at the bottom right is highlighted with a red box. The background shows the playbooks editor with the app's flowchart.

## ThreatConnect – Adversary Space Data Enrichments App User Guide

**Step 3:** Activate the Playbook as shown below.



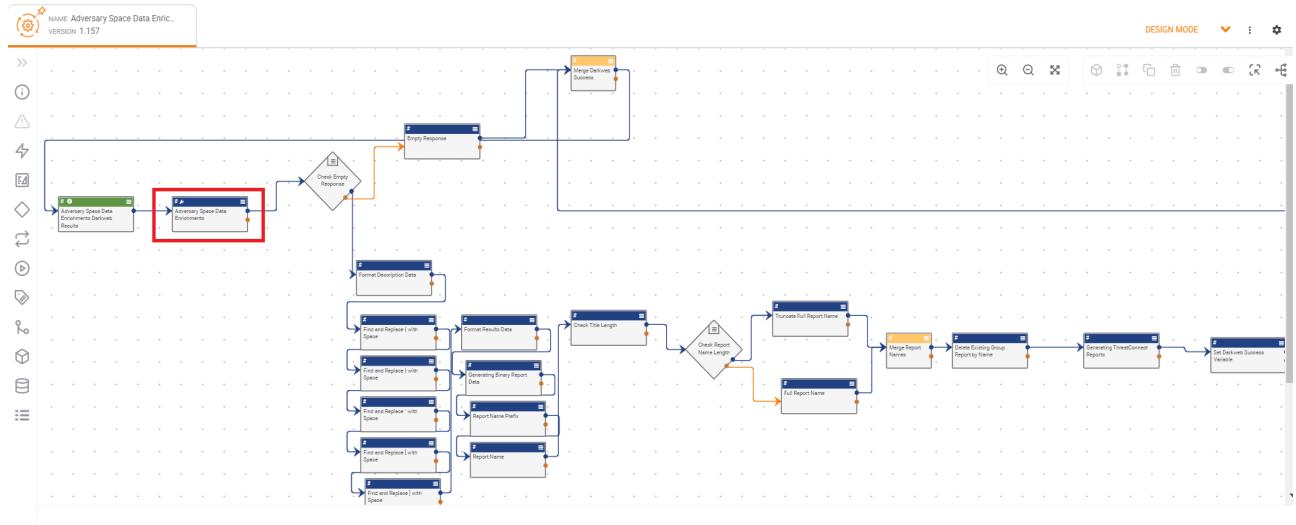
**Step 4:** Once the Playbook is activated, please click on the execute endpoint, this will fetch the results from Andariel API.



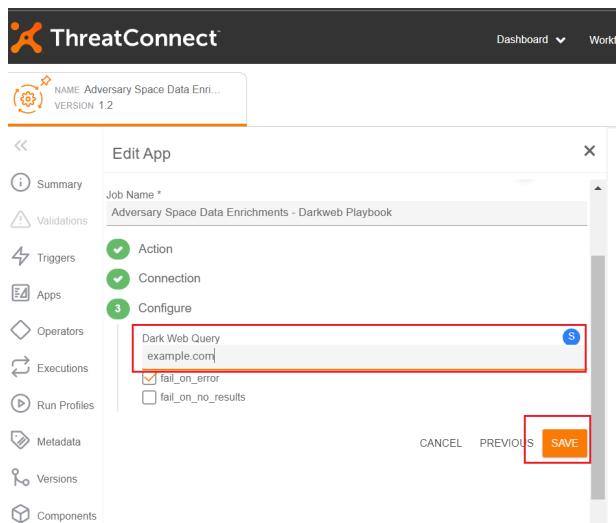
## 7. Running Adversary Space Data Enrichments Dark Web Playbook

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

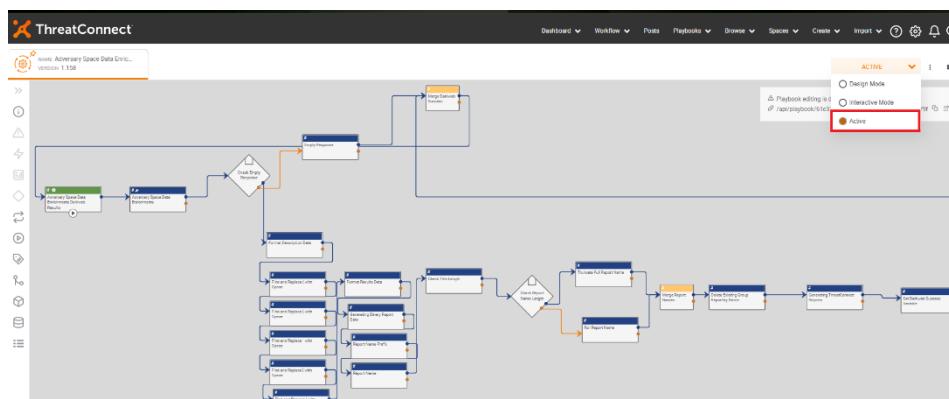
## ThreatConnect – Adversary Space Data Enrichments App User Guide



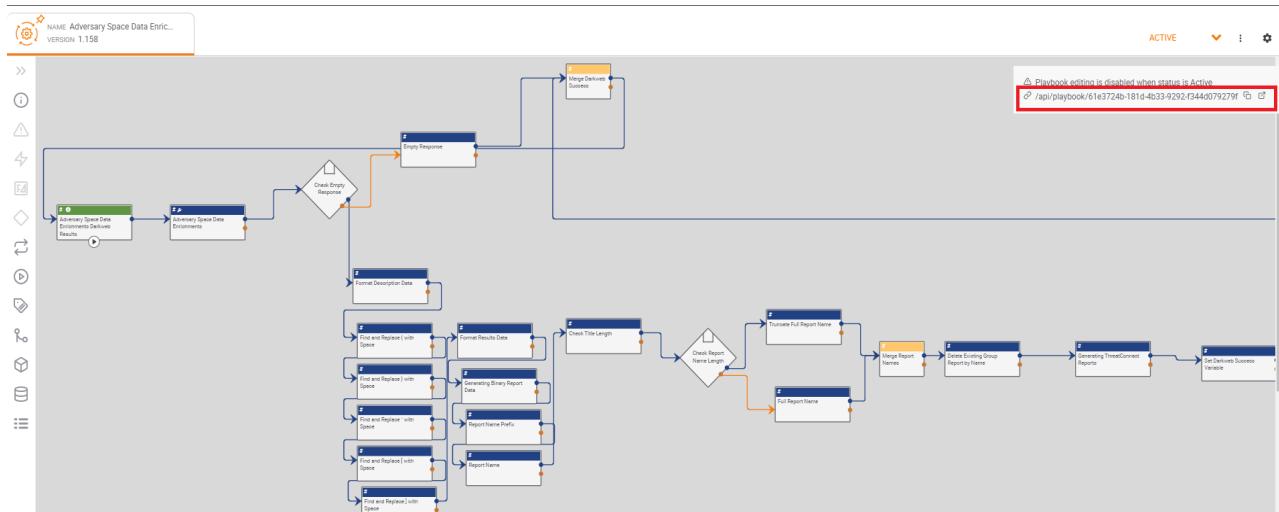
**Step 2:** Go to Configure section of the App and provide your desired values to search and click on Save as shown below.



**Step 3:** Activate the Playbook as shown below.

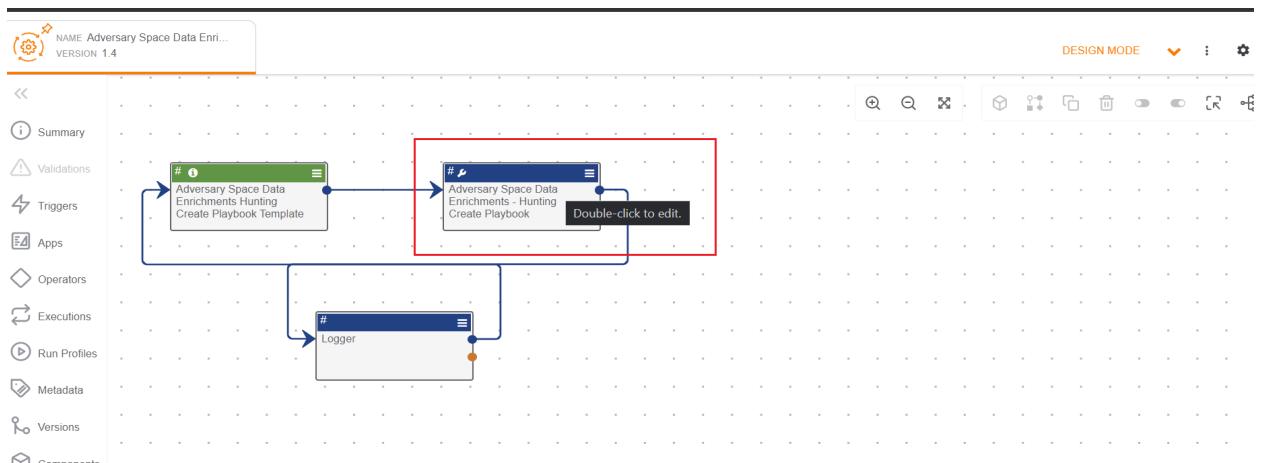


**Step 4:** Once the Playbook is activated, please click on the execute endpoint, this will fetch the results from Andariel API.



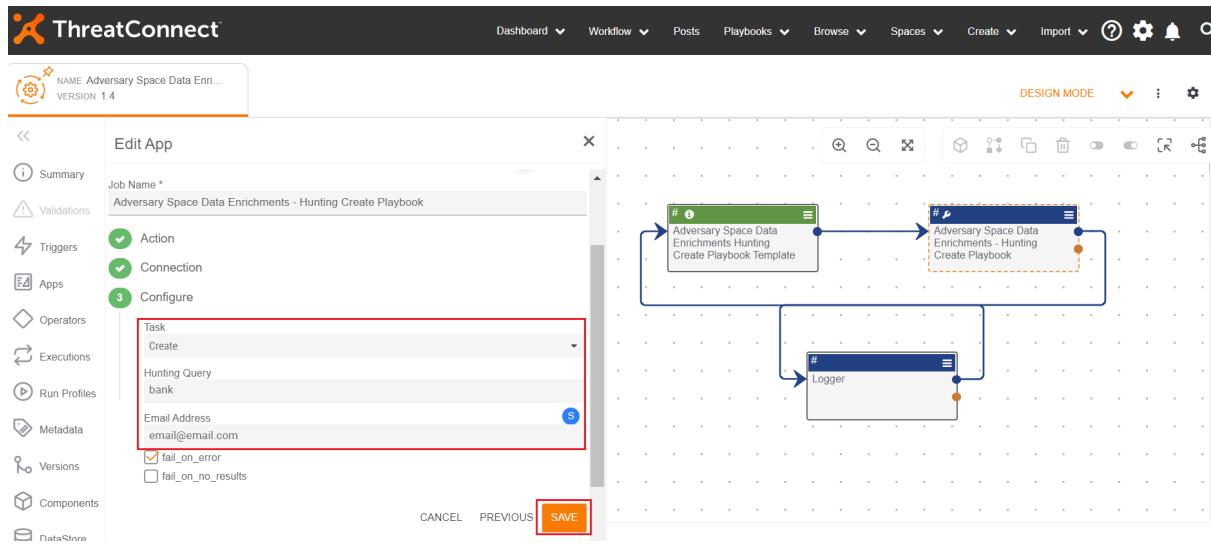
## 8. Running Adversary Space Data Hunting Create Playbook

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

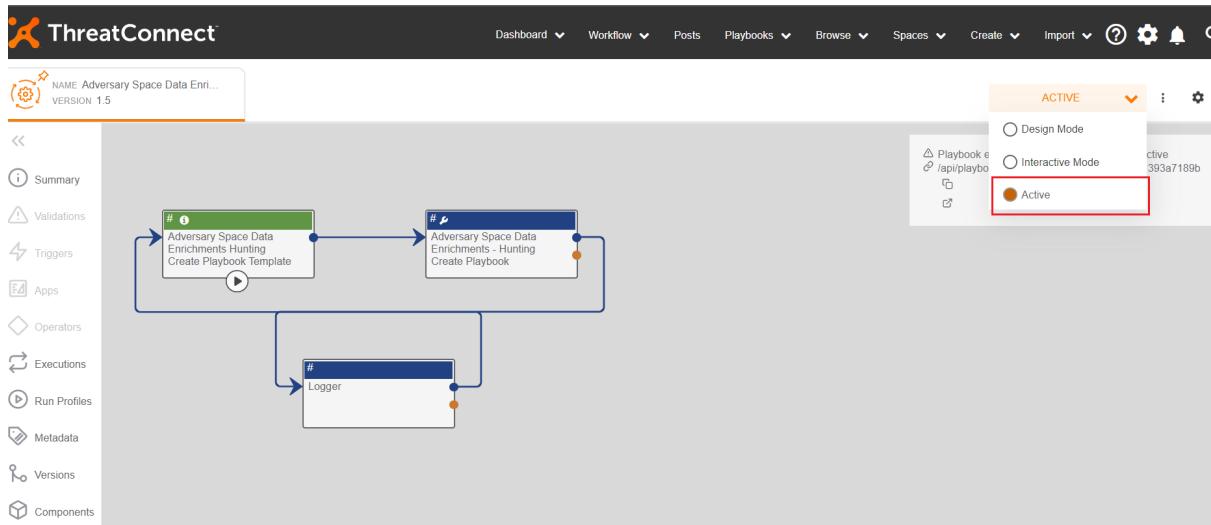


**Step 2:** Go to Configure section of the App and provide your desired values to search and click on Save as shown below.

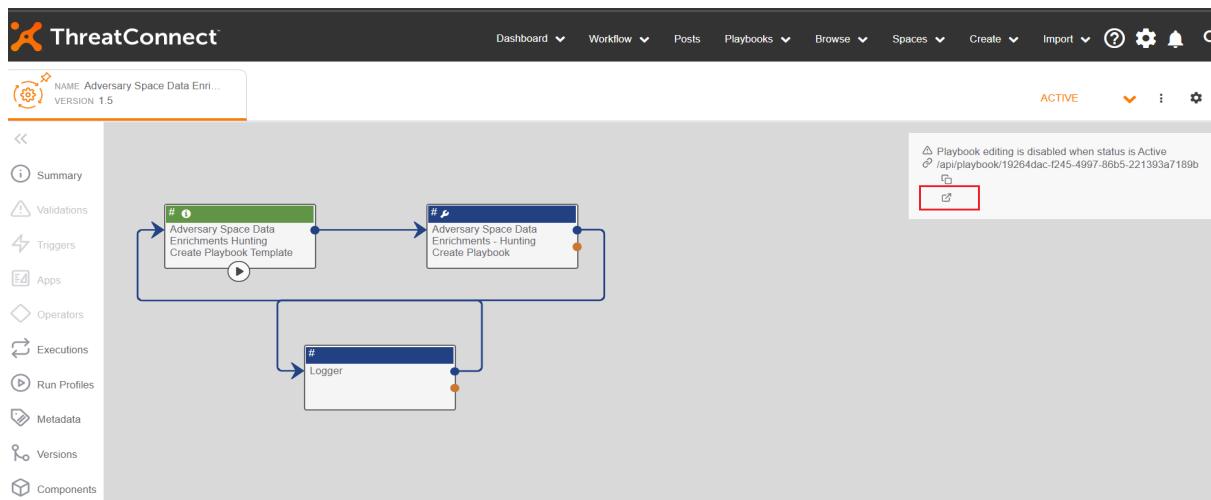
## ThreatConnect – Adversary Space Data Enrichments App User Guide



**Step 3:** Activate the Playbook as shown below.

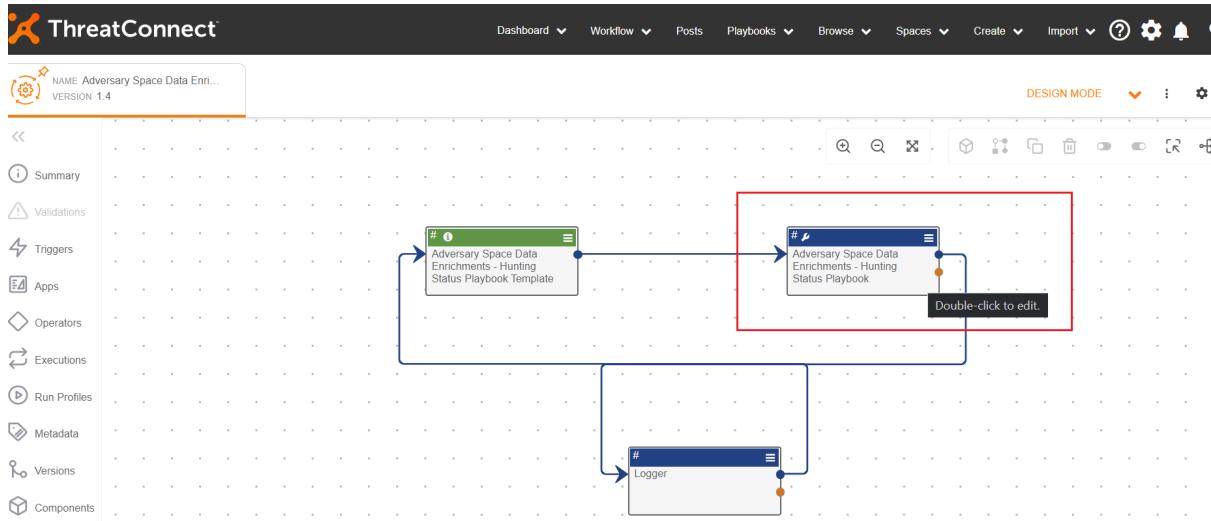


**Step 4:** Once the Playbook is activated, please click on the execute endpoint, this will fetch the results from Andariel API.

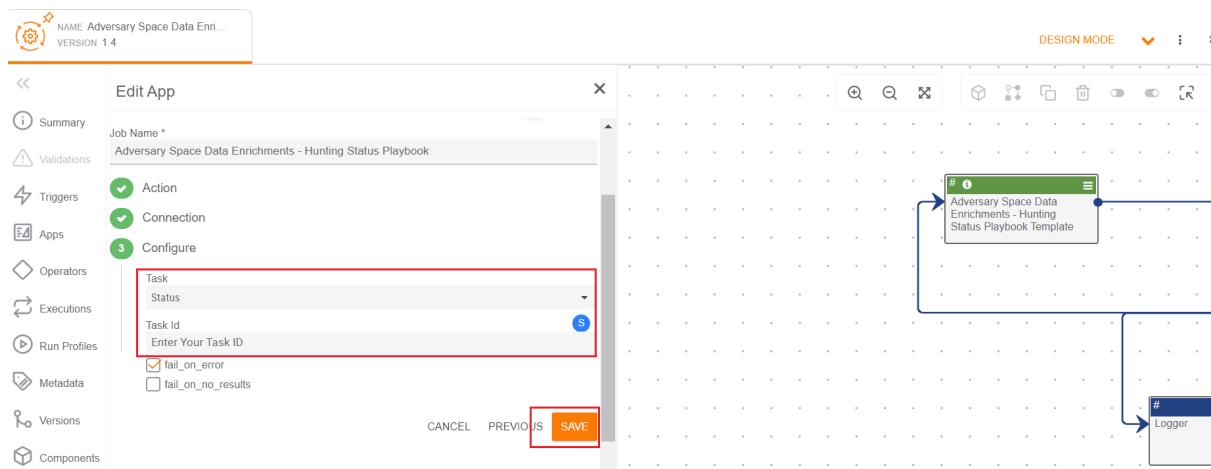


### 9. Running Adversary Space Data Hunting Status Playbook

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

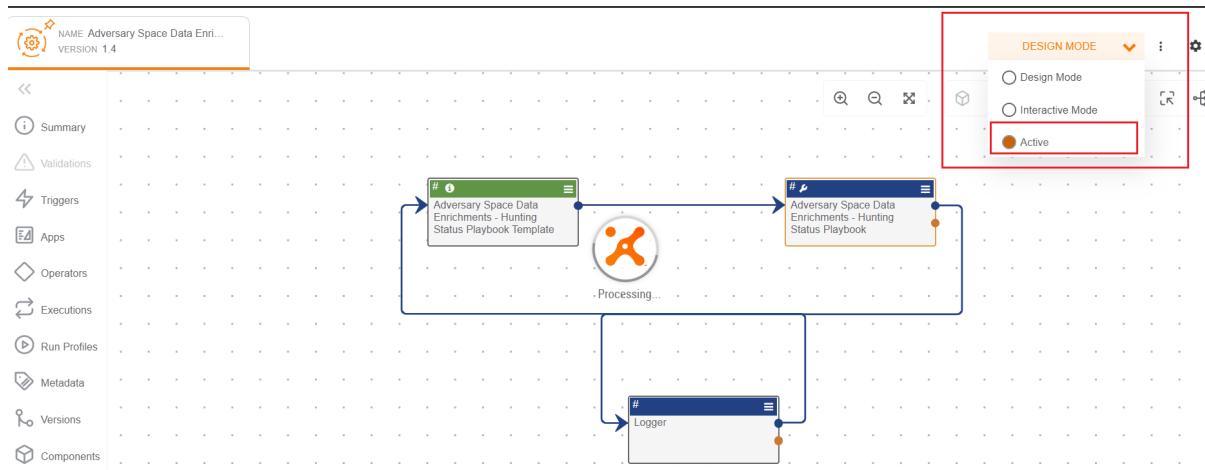


**Step 2:** Go to Configure section of the App and provide your desired values to search and click on Save as shown below.

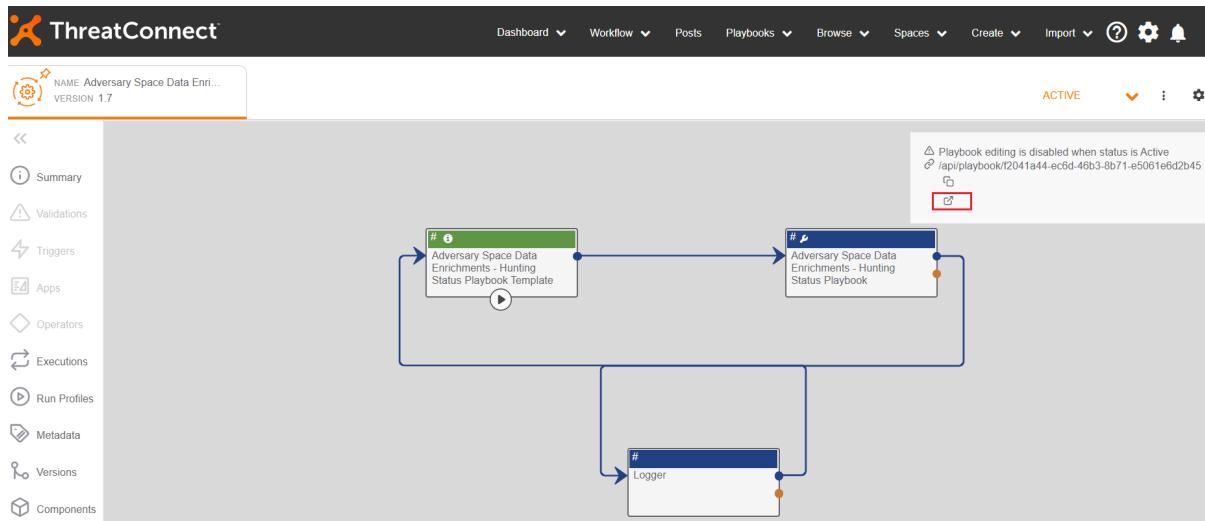


**Step 3:** Activate the Playbook as shown below.

## ThreatConnect – Adversary Space Data Enrichments App User Guide



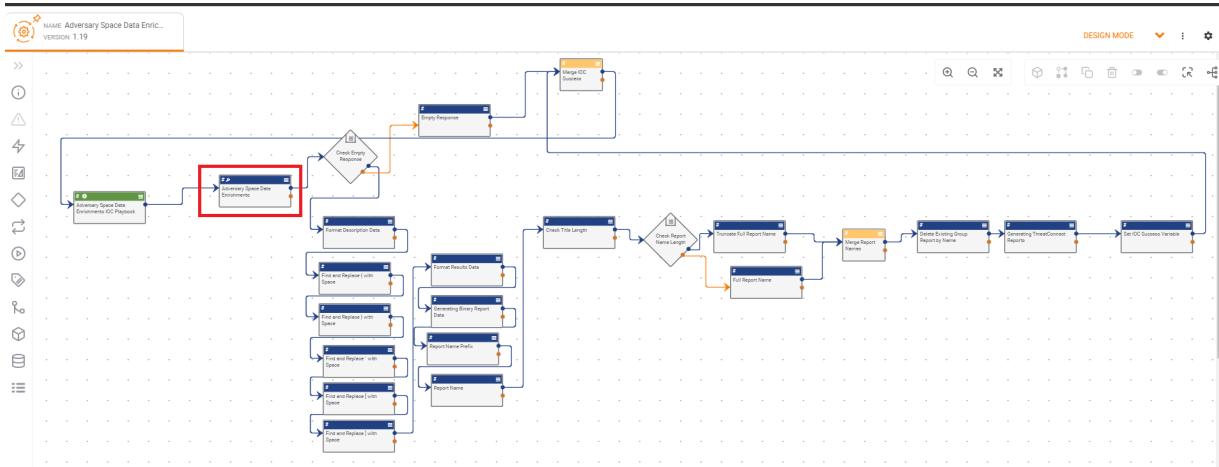
**Step 4:** Once the Playbook is activated, please click on the execute endpoint, this will fetch the results from Andariel API.



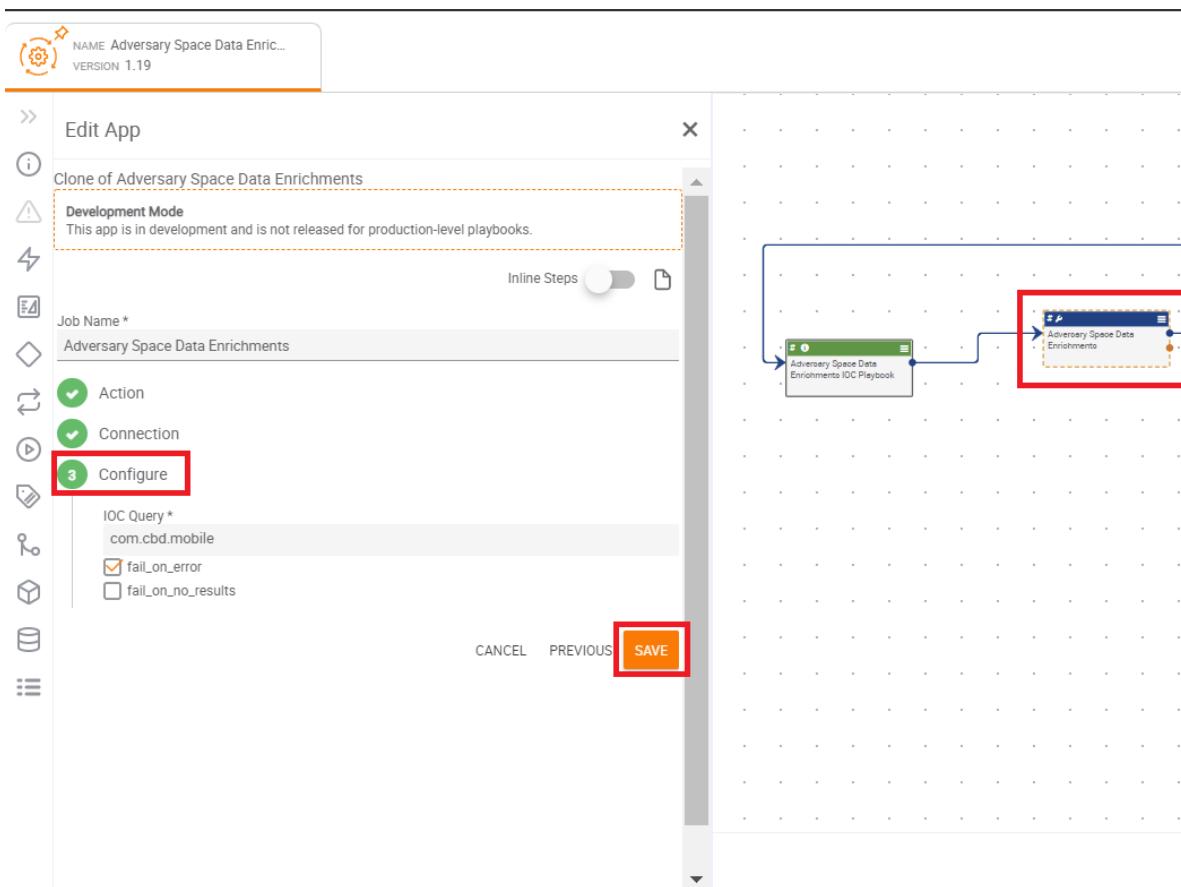
## 10. Running Adversary Space Data Enrichments IOC Playbook

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

## ThreatConnect – Adversary Space Data Enrichments App User Guide

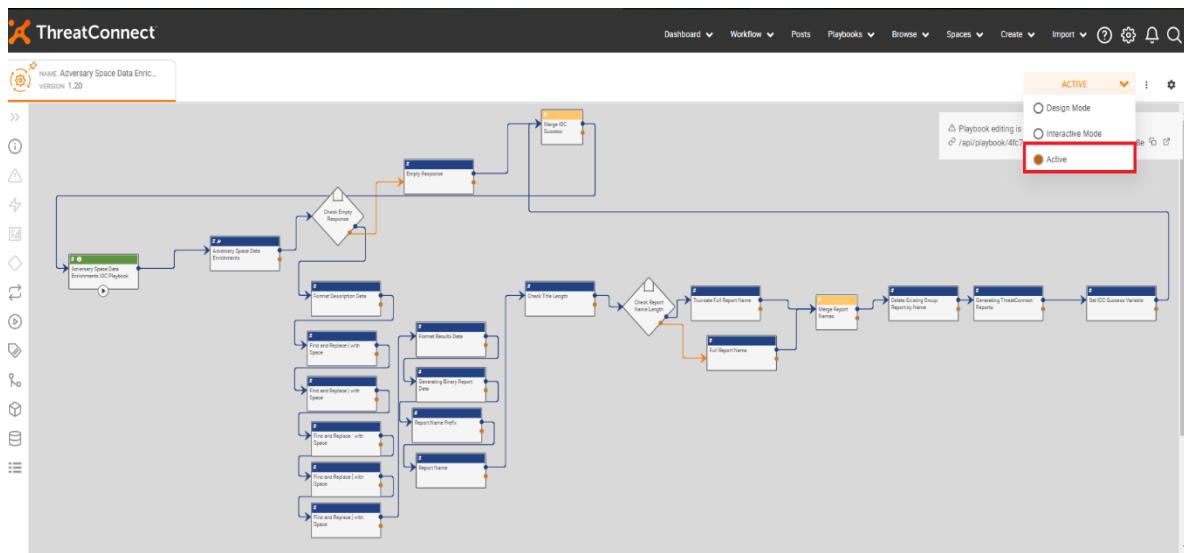


**Step 2:** Go to Configure section of the App and provide your desired values to search and click on Save as shown below.

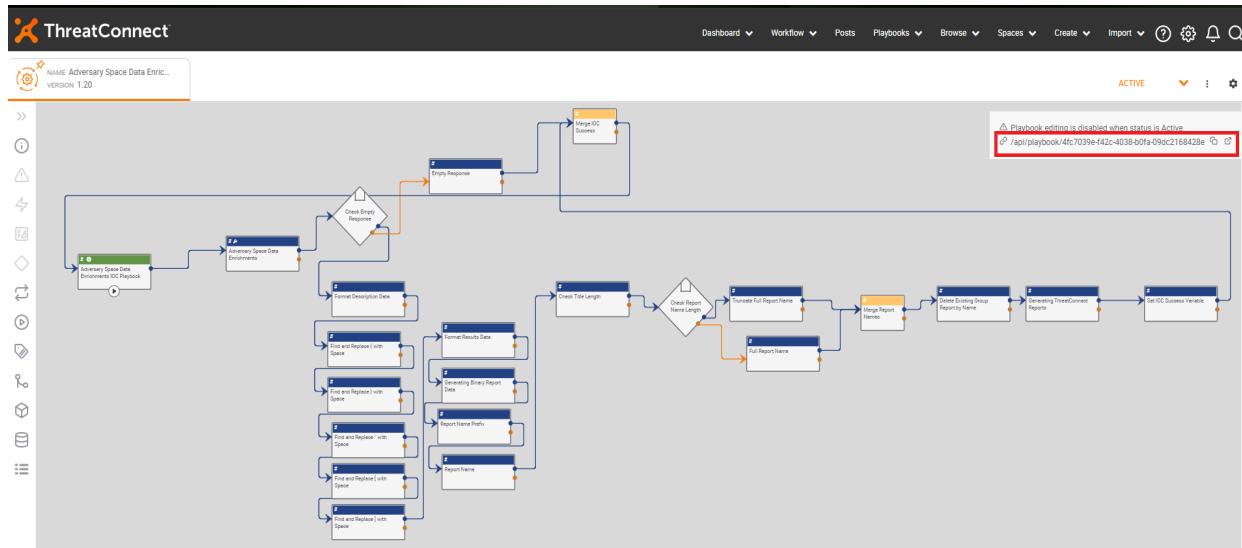


**Step 3:** Activate the Playbook as shown below.

## ThreatConnect – Adversary Space Data Enrichments App User Guide



**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

## ThreatConnect – Adversary Space Data Enrichments App User Guide

### 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.

The screenshot shows the ThreatConnect interface with the 'Create' menu open. The 'Indicator' option is highlighted with a red box. Other options like 'Address', 'Group', 'Track', and 'Victim' are also visible in the dropdown menu. The main dashboard area shows various intelligence breakdowns and source compositions.

Please enter Address and Save

The screenshot shows the ThreatConnect interface with a 'Create Address' dialog box open over the dashboard. The dialog box has fields for 'Owner' (set to 'Advanced Intel Dev') and 'IP Address' (set to '162.221.12.60'). There are 'CANCEL' and 'SAVE' buttons at the bottom. The main dashboard area shows various intelligence breakdowns and source compositions.

Now, run the required Playbook

# ThreatConnect – Adversary Space Data Enrichments App User Guide

**Indicator Analytics**

**ThreatAssess**

**CAL™ Insights**

**Trends**

Daily False Positives, Daily Impressions, Daily Observations

**Classification**

**False Positives**

False Positives (All Time), False Positives (Previous 7 Days)

**Impressions**

All Time, Previous 7 Days, Today

**Observations**

Observations (All Time)

**Playbook Actions**

Run	Name	Status
(R)	Adversary Space Data Enrichments Botnet Playbook	Ready
(R)	Adversary Space Data Enrichments IOC Playbook	Ready

**Additional Owners**

Name	Threat Rating	Confidence Rating
Loginsoft PursuitX	5	5

**Associations**

- Associated Groups (0)
- Associated Indicators (0)
- Associated Victim Assets (0)

**Details**

Type	Address
Version	IPv4
Added	06-01-2022 05:36 GMT
Modified	06-01-2022 05:36 GMT

**Indicator Analytics**

**ThreatAssess**

**CAL™ Insights**

**Trends**

Daily False Positives, Daily Impressions, Daily Observations

**Classification**

**False Positives**

False Positives (All Time), False Positives (Previous 7 Days)

**Impressions**

All Time, Previous 7 Days, Today

**Observations**

Observations (All Time)

**Playbook Actions**

Run	Name	Status
(R)	Adversary Space Data Enrichments Botnet Playbook	Address Playbook Successful
(R)	Adversory Space Data Enrichments IOC Playbook	Address Playbook Successful

**Additional Owners**

Name	Threat Rating	Confidence Rating
Loginsoft PursuitX	5	5

**Associations**

- Associated Groups (0)
- Associated Indicators (0)
- Associated Victim Assets (0)

**Details**

Type	Address
Version	IPv4
Added	06-01-2022 05:36 GMT
Modified	06-01-2022 05:36 GMT

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

# ThreatConnect – Adversary Space Data Enrichments App User Guide

The screenshot shows the ThreatConnect interface with the Adversary Space Data Enrichments App selected. The left sidebar has sections like Indicator Analytics, ThreatAssess, CAL™ Insights, Trends, Classification, False Positives, Impressions, and Observations. The main content area includes Playbook Actions (Adversary Space Data Enrichments Botnet Playbook, Adversary Space Data Enrichments IOC Playbook), Additional Owners (Loginsoft PursuitX), and Associations (Associated Groups, Associated Indicators). A summary bar at the top right shows '281 Medium' and various status indicators.

Here you can find the Attributes

The screenshot shows the ThreatConnect interface with the Adversary Space Data Enrichments App selected. The left sidebar has sections like City, Time Zone, and Attributes. The main content area displays the Attributes section, showing fields for Attributes, External Date Created, Source, and Description, along with their respective values and creation details.

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

## ThreatConnect – Adversary Space Data Enrichments App User Guide

**Description**

Loginsoft PursuitX / Venkat Rambatza says:

None

**Adversary Space Data Enrichments Botnet Results**

```
_index: logstash-infra-uasrdp-hvt-f,
_type: doc,
_id: hfBfEvkBhNeK8ybPU59c,
_score: 13.552097,
_source:
rr: n/a,
geopl:
latitude: 43.6319,
ip: 162.221.12.60,
country_name: Canada,
country_code2: CA,
country_code3: CA,
continent_code: NA,
location:
lon: -79.3716,
lat: 43.6319
longitude: -79.3716
first_seen: 2019-01-01T11:34:20.000Z,
date_collect: 2019-01-01T11:34:20.000Z,
last_seen: 2019-01-13T07:25:51.000Z,
subject: ,
domain_nat: WIN-G695KR93GGH,
isp: ClearDDoS Technologies,
id_nat: 7084220,
ip: 162.221.12.60,
```

**Associated Indicators (1)**

Type	Owner	Threat Rating	Date Added
Host	Advanced Intel Dev	High	05-31-2022

**Associated Victim Assets (0)**

**Details**

Type: Address  
Version: IPv4  
Added: 06-01-2022 05:36 GMT  
Modified: 06-01-2022 05:37 GMT  
Overall Threat Rating: High  
Overall Confidence Rating: 0 - Unassessed

**Observations/False Positives**

Observations: 0  
Last Observed: -  
Report False Positive:

Please configure an API account to appear in the Observations and False Positives Report. Org Settings

**Tags**

None

**Recent Tags...**

**Investigation Links**

Open All

AlienVault OTX	Bing	BuiltWith
Censys	DomainTools	Google
Google Public DNS	Hurricane Electric	Hybrid Analysis
IBM X-Force Exchange	InQuest	InQuest IOC-DB
InQuest PDF API	Intelsat	Intelsat Total

Now you can Download the Report

**SOURCE**

**Adversary Space Data Enrichments Botnet Results for ip:162.221.12.60**

**Actions**

- Pivot
- Delete
- COPY TO MY ORG
- DOWNLOAD PDF

**Overview**

**Associations**

**Associated Groups (0)**

**Associated Indicators (2)**

Type	Owner	Threat Rating	Date Added
Address	Advanced Intel Dev	High	06-01-2022
Host	Advanced Intel Dev	High	06-01-2022

**Associated Victim Assets (0)**

**Details**

Type: Report  
Added: 06-01-2022 12:24 GMT by Venkat Rambatza  
Modified: 06-01-2022 12:24 GMT  
Publish Date: 06-01-2022

**Report File**

Original File: Adversary Space Data Enrichments Botnet Results for ip:162.221.12.60.txt  
File Type: Text  
File Size: 1.41 KB  
Status: Success

**Actions**

- DOWNLOAD
- UPDATE FILE

## 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.

## ThreatConnect – Adversary Space Data Enrichments App User Guide

The screenshot shows the ThreatConnect interface. On the left, there's a sidebar with sections for 'Indicators' and 'Groups'. The 'Indicators' section lists various types like Address, E-mail Address, File, Host, URL, ASN, etc. The 'Groups' section lists types like Adversary, Attack Pattern, Campaign, etc. In the center, there's a search bar with filters and a table of indicators. A red box highlights the 'Create' dropdown menu at the top right. The table has columns for 'Indicator', 'Group', 'Track', and 'Victim'. One row in the table is highlighted with a red box and labeled 'Host'.

Please enter host address and Save

The screenshot shows a 'Create Host' dialog box. It has fields for 'Owner' (set to 'Advanced Intel Dev'), 'Host Name' (set to 'ziggo.nl'), and two buttons at the bottom: 'CANCEL' and 'SAVE'. A red box highlights the 'SAVE' button.

Now, run the required Playbook

# ThreatConnect – Adversary Space Data Enrichments App User Guide

The screenshot shows the ThreatConnect interface for the 'zigg.nl' source. In the top right corner, there is an 'Advanced Intel Dev' section with checkboxes for 'Active' and 'CAL Status Lock'. Below it, a 'Follow item' checkbox is present. The main content area includes sections for 'Indicator Analytics' (ThreatAssess), 'CAL™ Insights' (with a score of 280 Medium), 'Trends' (Daily False Positives, Daily Impressions, Daily Observations), 'Classification' (Classifiers: BenignTop100, BenignCommodityTop1000, BenignMalwareTop100, BenignTrendsTop1000, TLDUnknown), 'External Context' (Alexa Rank, Cross Universe Rank, Malware Million Rank, Trend Top 1 Million Rank), 'False Positives' (All Time, Previous 7 Days, Today), 'Impressions' (All Time, Previous 7 Days, Today), and 'Observations' (All Time, Previous 7 Days, Today). On the right side, the 'Playbook Actions' section shows three runs: 'Adversary Space Data Enrichments Botnet Playbook' (selected and highlighted with a red box), 'Adversary Space Data Enrichments Bot Creds Playbook' (highlighted with a red box), and 'Adversary Space Data Enrichments IOC Playbook'. The 'Associations' section lists 'Associated Groups (0)', 'Associated Indicators (0)', and 'Associated Victim Assets (0)'. The 'Details' section provides host information: Type: Host, Added: 06-01-2022 11:50 GMT, Modified: 06-01-2022 11:50 GMT, DNS: [unchecked], Whois: [unchecked], Overall Threat Rating: Unknown, Overall Confidence Rating: 0 - Unassessed. The 'Observations/False Positives' section shows 0 observations and 0 false positives reported.

This screenshot is identical to the one above, but the 'Adversary Space Data Enrichments Botnet Playbook' run now has a status of 'Ready' with a green checkmark, and the 'Host Playbook Successful' status is highlighted with a red box in the 'Playbook Actions' section. The rest of the interface remains the same, including the 'Indicator Analytics', 'CAL™ Insights', 'Trends', 'Classification', 'External Context', 'False Positives', 'Impressions', 'Observations', 'Associations', and 'Details' sections.

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

The screenshot shows the ThreatConnect interface after the playbook has been successfully run. The 'Playbook Actions' section now shows the 'Host Playbook Successful' status. The 'Associations' section displays 'Associated groups (1)' with a single entry: 'Adversary Space Data Enrichments Botnet Playbook' (Type: Host, Owner: ThreatConnectBot, Associated By: ThreatConnectBot, Date Accessed: 06-01-2022). The 'Details' section also reflects the successful run, showing Type: Host, Added: 06-01-2022 11:50 GMT, Modified: 06-01-2022 11:51 GMT, DNS: [unchecked], Whois: [unchecked], Overall Threat Rating: Unknown, Overall Confidence Rating: 0 - Unassessed.

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

## ThreatConnect – Adversary Space Data Enrichments App User Guide

The screenshot shows the ThreatConnect interface with the following details:

- Description:** None
- Tags:** botnet credential (highlighted with a red box)
- Investigation Links:** A list of various investigation sources including AbuseCh, Bleeping, Censys, Google, Hybris, Maltego, MaxMind, Osint, OsintHub, Shodan, ThreatMiner, ThreatIntel, VirusShare, Whois, and WhoisCMS.
- Add New Comment:** A text input field for adding a comment.
- Posts:** No comments found.

Here you are enabled to download report

The screenshot shows the ThreatConnect interface for the 'Adversary Space Data Enrichments Bot Creds Results for ziggo.nl' entry. Key sections include:

- Description:** No Default Description entered. Click here to add one.
- Source:** No Default Source entered. Click here to add one.
- Security Labels:** Choose Security Labels.
- Report File:** Original File: Adversary Space Data Enrichments Bot Creds Results for ziggo.nl.txt, File Type: Text, File Size: 13.36 KB, Status: Success. Includes a red box around the 'DOWNLOAD' button.
- Associations:**
  - Associated Groups (0)
  - Associated Indicators (1):
    - Host: ziggo.nl (highlighted with a red box)
  - Associated Victim Assets (0)
- Details:** Type: Report, Created: 06-01-2022 11:53 GMT by Venker Rambatta, Modified: 06-01-2022 11:53 GMT, Published Date: 06-01-2022 ✓.
- Tags:** A list of tags including botnet credential (highlighted with a red box).
- Add New Comment:** A text input field for adding a comment.

### 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.

## ThreatConnect – Adversary Space Data Enrichments App User Guide

The screenshot shows the ThreatConnect interface with the 'Create' dropdown menu open. The 'Host' option is highlighted with a red box. The menu lists various indicator types such as Address, E-mail Address, File, URL, ASN, CIDR, Email Subject, Ethereum Address, Hashtag, Host Asset IP, Host Asset Name, Mutex, Registry Key, User Agent, Group, Adversary, Attack Pattern, Campaign, Course of Action, Document, Event, Incident, Intrusion Set, Malware, Report, and Signature.

Please enter the host address and save

The 'Create Host' dialog box is shown. The 'Owner' field is set to 'Advanced Intel Dev' (highlighted with a red box). The 'Host Name' field contains 'ziggo.nl'. At the bottom right are 'CANCEL' and 'SAVE' buttons, with 'SAVE' highlighted with a red box.

Now, run the required playbook.

# ThreatConnect – Adversary Space Data Enrichments App User Guide

The screenshot shows the ThreatConnect interface for the 'com.cbd.mobile' source. The top navigation bar includes 'SOURCE', 'Advanced Intel Dev', 'Indicator Status' (Active checked, CAL Status Lock uncheckable), and a 'Follow Item' button.

**Indicator Analytics** section:

- ThreatAssess:** A gauge showing 281 Medium.
- CAL™ Insights:** Recent False Positive Reported and Impacted by Recent Observations.
- Trends:** Daily False Positives, Daily Impressions, Daily Observations (7 days, 30 days).

**Playbook Actions** section:

Run	Name	Status
①	Adversary Space Data Enrichments Botnet Playbook	Ready
②	Adversary Space Data Enrichments Bot Creds Playbook	Ready
③	Adversary Space Data Enrichments IOC Playbook	Ready

The screenshot shows the ThreatConnect interface for the 'com.cbd.mobile' source. The top navigation bar includes 'SOURCE', 'Advanced Intel Dev', 'Indicator Status' (Active checked, CAL Status Lock uncheckable), and a 'Follow Item' button.

**Playbook Actions** section:

Run	Name	Status
①	Adversary Space Data Enrichments Botnet Playbook	Ready
②	Adversary Space Data Enrichments Bot Creds Playbook	Ready
③	Adversory Space Data Enrichments IOC Playbook	Host Playbook Successful

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

# ThreatConnect – Adversary Space Data Enrichments App User Guide

The screenshot shows the ThreatConnect interface with the following details:

- Address:** No records found.
- City:** No records found.
- Country:** No records found.
- Attributes:**
  - Description: None
- Adversary Space Data Enrichments IOC Results:**

```
_index: logstash-icapi-opencb-indicator,
_type: _doc,
_id: c18d53e3-c741-4c11-b4ad-ee00fbaa8190,
_score: 17.909204,
_source:
id: c18d53e3-c741-4c11-b4ad-ee00fbaa8190,
stix_id_key: indicator-a4889fcf-efb5-4eb7-ba61-5d79a62f1864,
stix_label: null,
entity_type: indicator,
parent_types:
Indicator,
Stix-Domain-Entity,
Stix-Domain
,
name: com.cbd.mobile,
alias: ,
description: Targeted Apps,
graph_data: null,
indicator_pattern: file.name = 'com.cbd.mobile',
pattern_type: stix,
detected: true,
confidence: 50,
value: from: 2017-12-11T10:16:00.000Z,
valid_until: 2018-12-11T10:16:00.000Z,
score: 30,
created: 2017-12-11T10:16:00.000Z,
modified: 2017-12-11T10:16:00.000Z,
created_at: 2020-11-17T09:19:44.640Z,
updated_at: 2020-11-17T09:19:44.640Z,
killChainPhases: ,
createdByRef:
id: 581933e1-621f-4203-96e2-025c77298848,
entity_type: organization,
stix_id_key: identity-71f52ff0-7d67-45db-ac08-e51a7decbfeb,
stix_label: null,
name: CIRCL,
alias: ,
description: ,
created: 2020-11-15T10:35:19.106Z,
```
- SOURCE:** com.cbd.mobile
- Indicator Analytics:**
  - ThreatAssess:** 281 Medium
  - CAL™ Insights:**
  - Trends:** Daily False Positives, Daily Impressions, Daily Observations
  - Classification:** Classifies
  - False Positives:**
- Playbook Actions:**

Run Name	Status
Adversary Space Data Enrichments Botnet Playbook	Ready
Adversary Space Data Enrichments Bot Grids Playbook	Ready
Adversary Space Data Enrichments IOC Playbook	Ready
- Additional Owners:** Technical Blogs and Reports
- Associations:**
  - Associated Groups (2):** Report, Adversary Space Data Enrichments IOC Results for com.cbd.mobile, Advanced Intel Dev

Now you can download report

The screenshot shows the ThreatConnect interface with the following details:

- SOURCE:** Adversary Space Data Enrichments IOC Results for com.cbd.mobile
- Report File:**
  - Original File: Adversary Space Data Enrichments IOC Results for com.cbd.mobile.txt
  - Type: Text
  - File Size: 7.01 KB
  - Status: Success
- Download Button:** DOWNLOAD
- Associations:**
  - Associated Indicators (1):** Host com.cbd.mobile (Owner: Advanced Intel Dev, Date Added: 06-01-2022)
  - Associated Victim Assets (0):**
- Details:**

Type	Report
Added	06-01-2022 12:09 GMT by Venkat Rambatza
Modified	06-01-2022 12:09 GMT
Publish Date	06-01-2022
- Tags:**

