



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

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://marketplace.threatconnect.com/>

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.

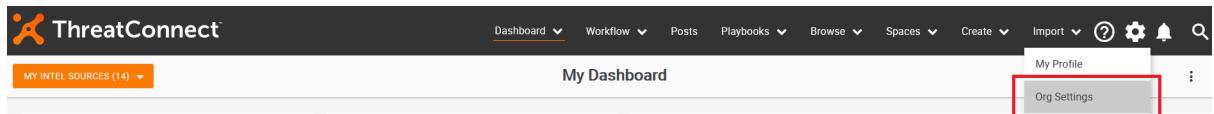
To install these Playbooks, go to the Playbooks tab within the ThreatConnect Platform. Select New > Import and locate the .pbx file you wish to add to your ThreatConnect Platform. Follow the on-screen instructions to complete the Playbook import.

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.

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

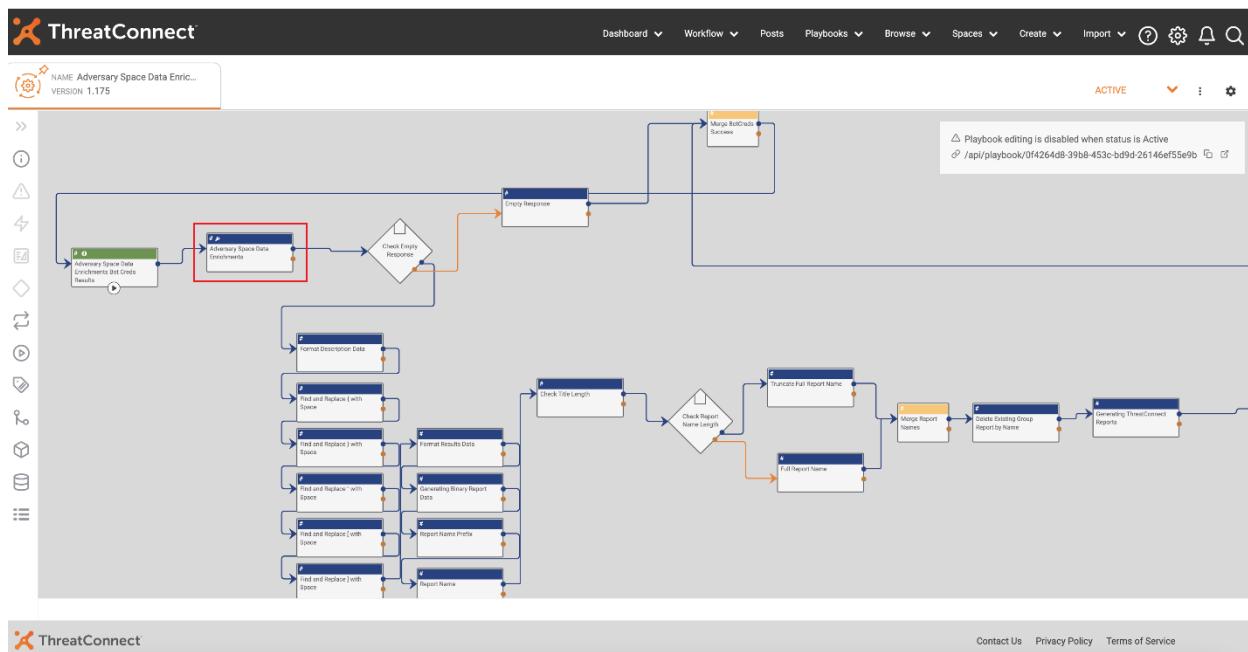
The image contains two screenshots. The top screenshot shows the 'Organization Settings' page for 'IPQualityScore'. It has tabs for Membership, Communities/Sources, Groups, Invitations, Variables (which is highlighted with a red box), Metrics, Settings, Apps, and Styling. A 'NEW VARIABLE' button is also 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 (showing 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

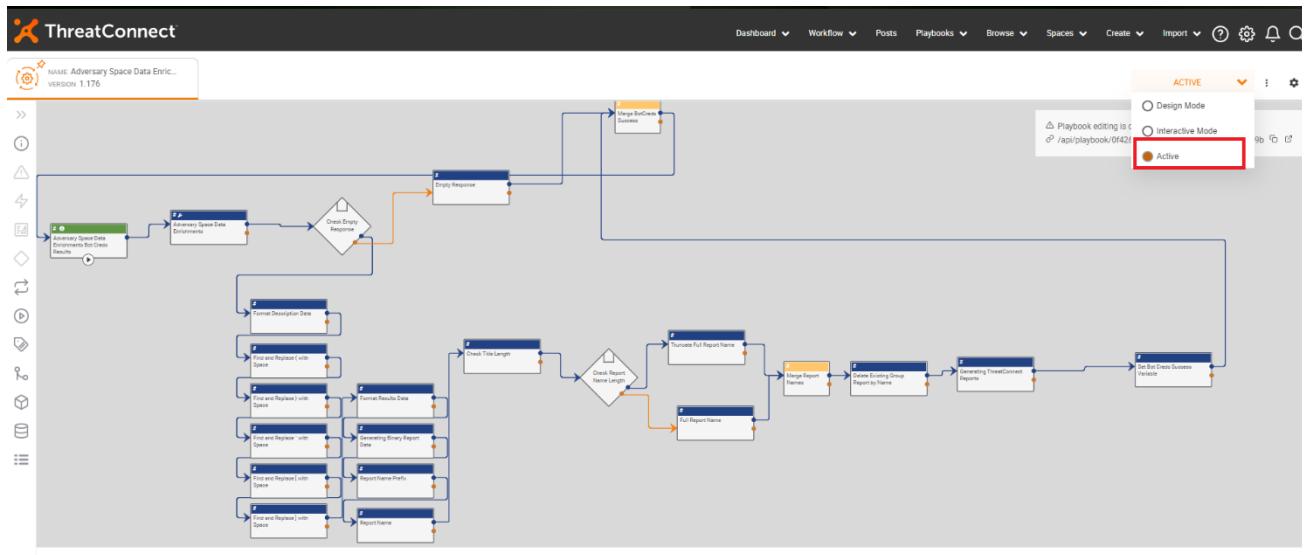
ThreatConnect – Adversary Space Data Enrichments App User Guide



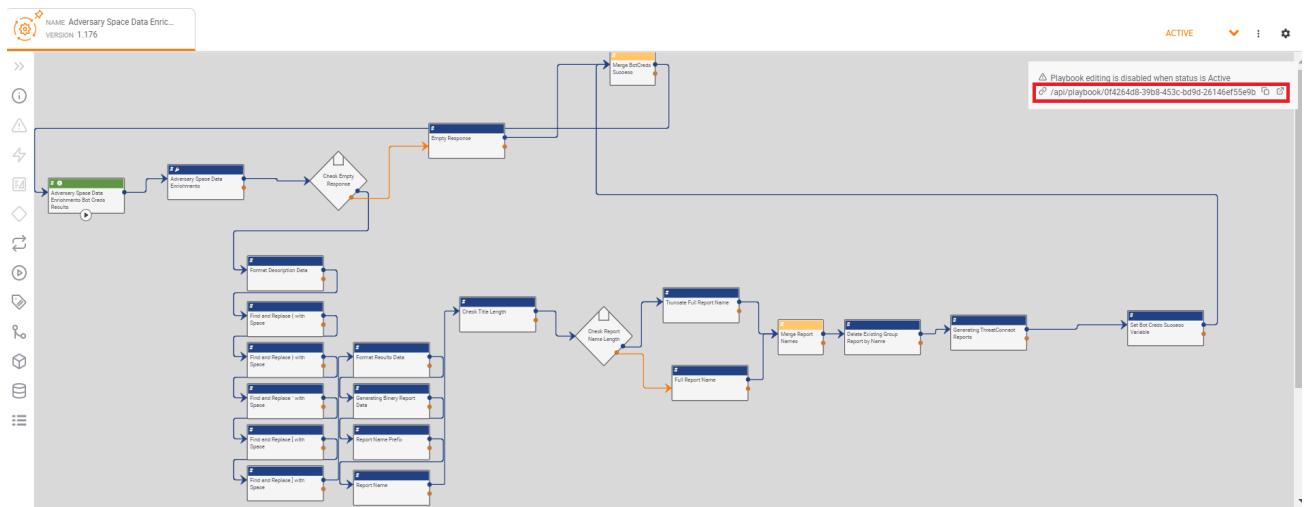
Step 2: Go to Configure section of the App and provide your desired values to search and click on Save as shown below.

The screenshot shows the 'Edit App' configuration page for a clone of the 'Adversary Space Data Enrichments' app. The 'Development Mode' warning is visible. The 'Configure' tab is selected and highlighted with a red box. The configuration fields include 'Job Name' set to 'Adversary Space Data Enrichments', 'Search By' set to 'Domain', 'Domain' set to 'example.com', and two optional checkboxes: 'fail_on_error' and 'fail_on_no_results'. At the bottom, there are 'CANCEL', 'PREVIOUS', and a large red 'SAVE' button.

Step 3: Activate the Playbook as shown below.



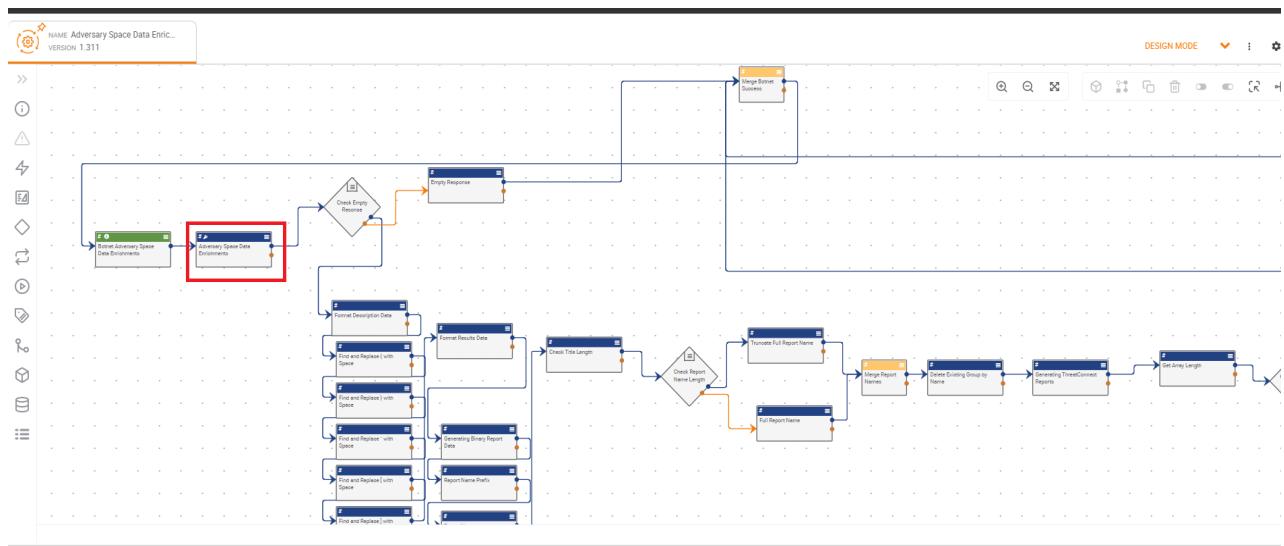
Step 4: Once the Playbook is activated, please click on the execute endpoint, this will fetch the results from Andariel API.



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

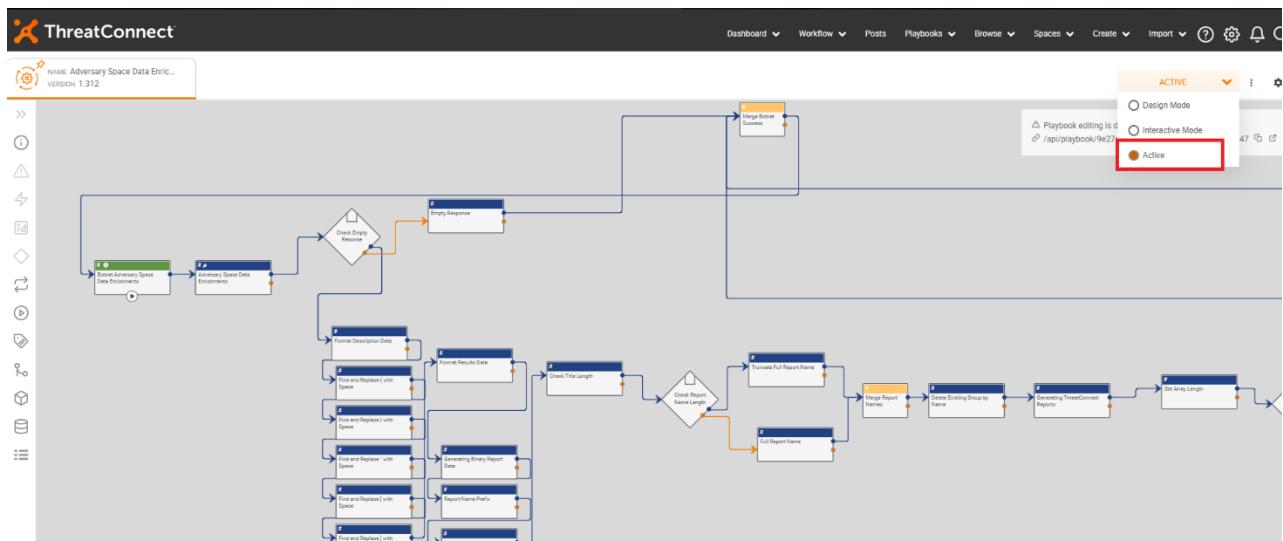


Step 2: Go to Configure section of the App and provide your desired values to search and click on Save as shown below.

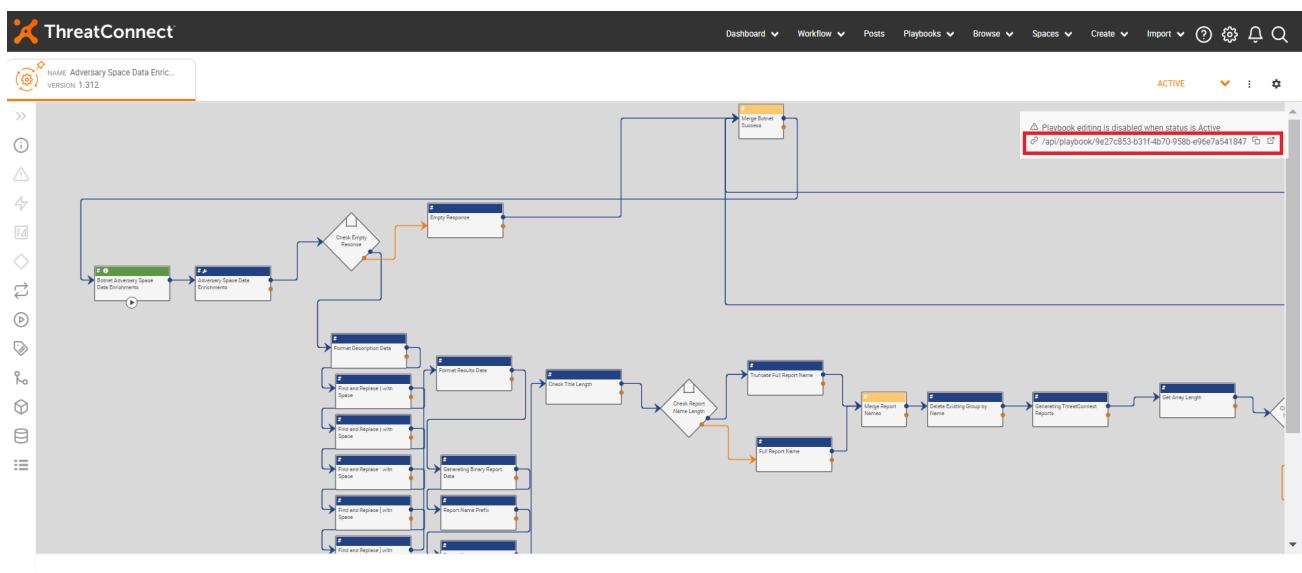
The screenshot shows the ThreatConnect app configuration dialog for 'Adversary Space Data Enrichments'. The 'Configure' tab is selected and highlighted with a green box. The 'SAVE' button at the bottom right is highlighted with a red box. The background shows the main playbooks editor interface.

ThreatConnect – Adversary Space Data Enrichments App User Guide

Step 3: Activate the Playbook as shown below.



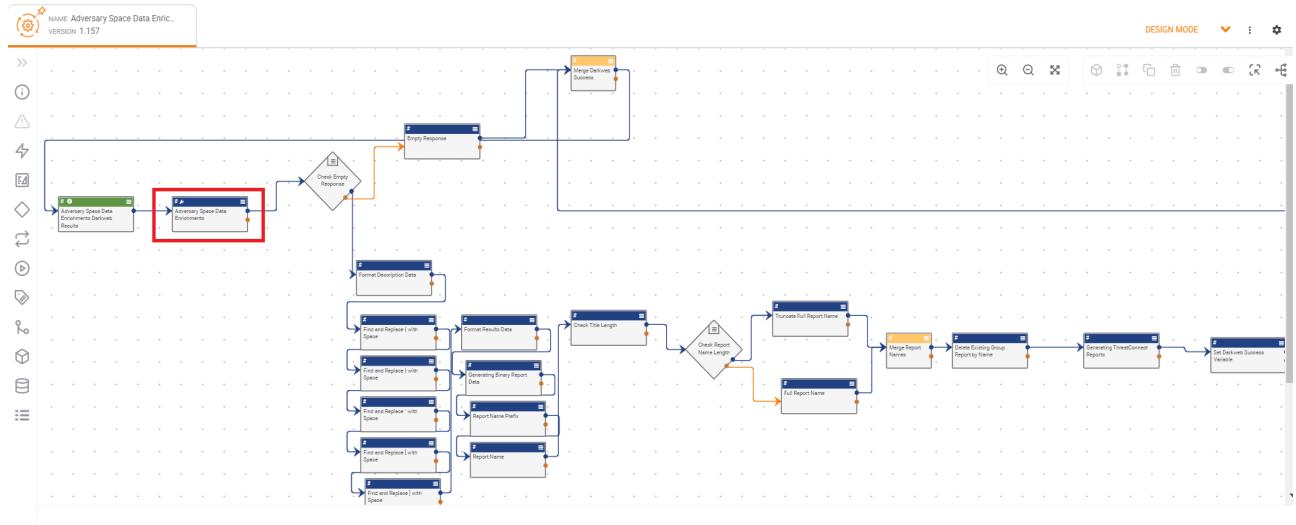
Step 4: Once the Playbook is activated, please click on the execute endpoint, this will fetch the results from Andariel API.



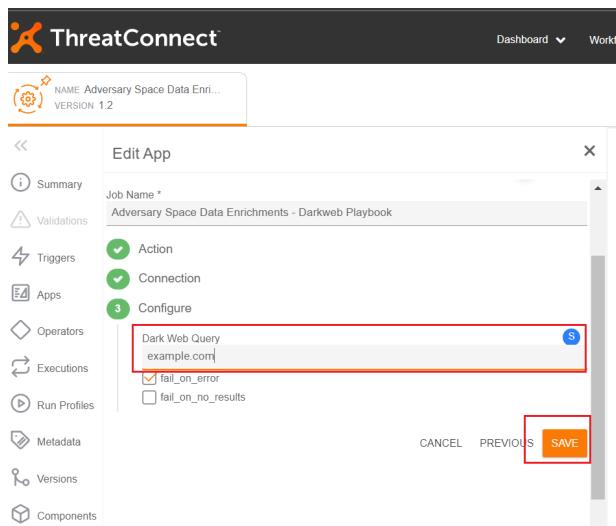
7. Running Adversary Space Data Enrichments Dark Web Playbook

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

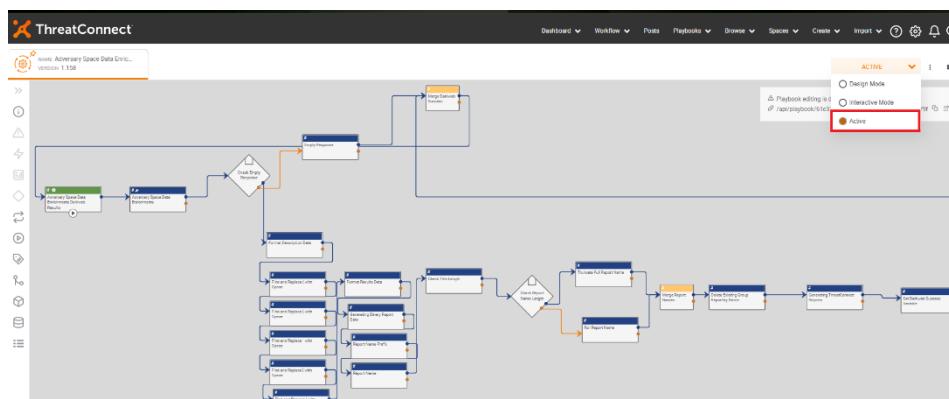
ThreatConnect – Adversary Space Data Enrichments App User Guide



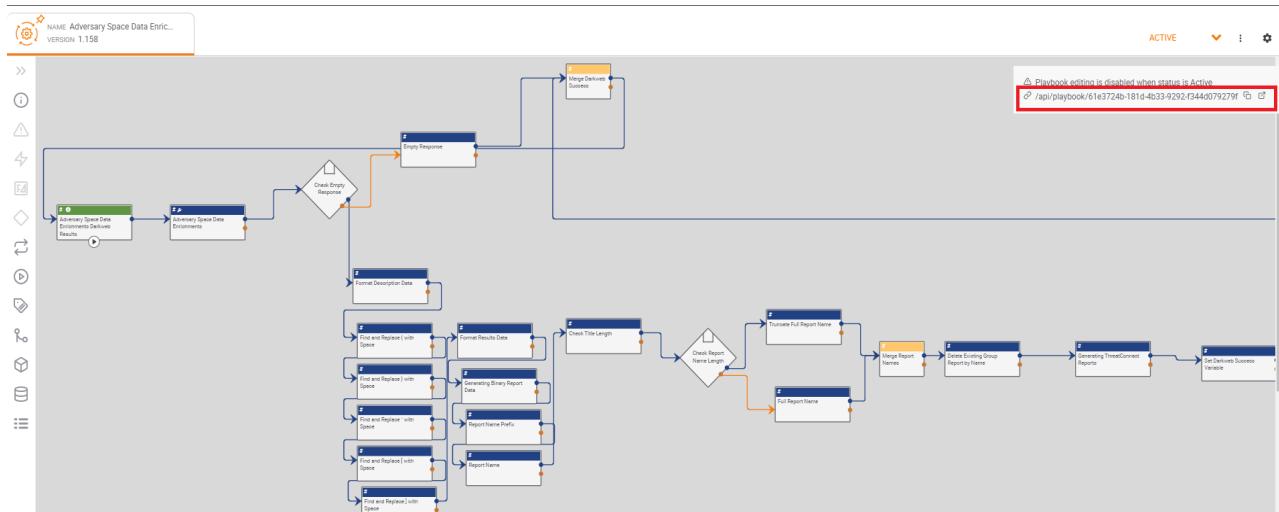
Step 2: Go to Configure section of the App and provide your desired values to search and click on Save as shown below.



Step 3: Activate the Playbook as shown below.

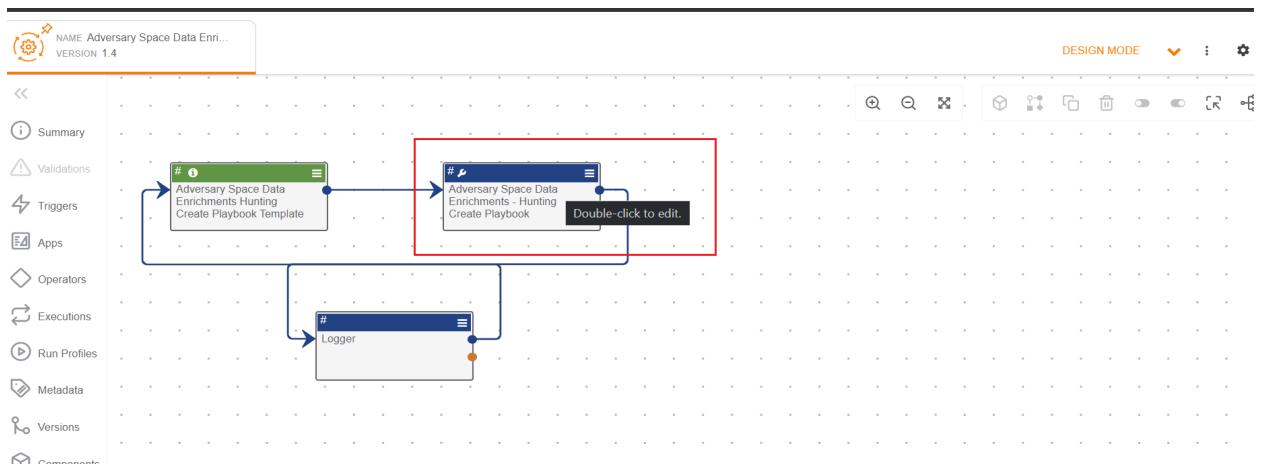


Step 4: Once the Playbook is activated, please click on the execute endpoint, this will fetch the results from Andariel API.



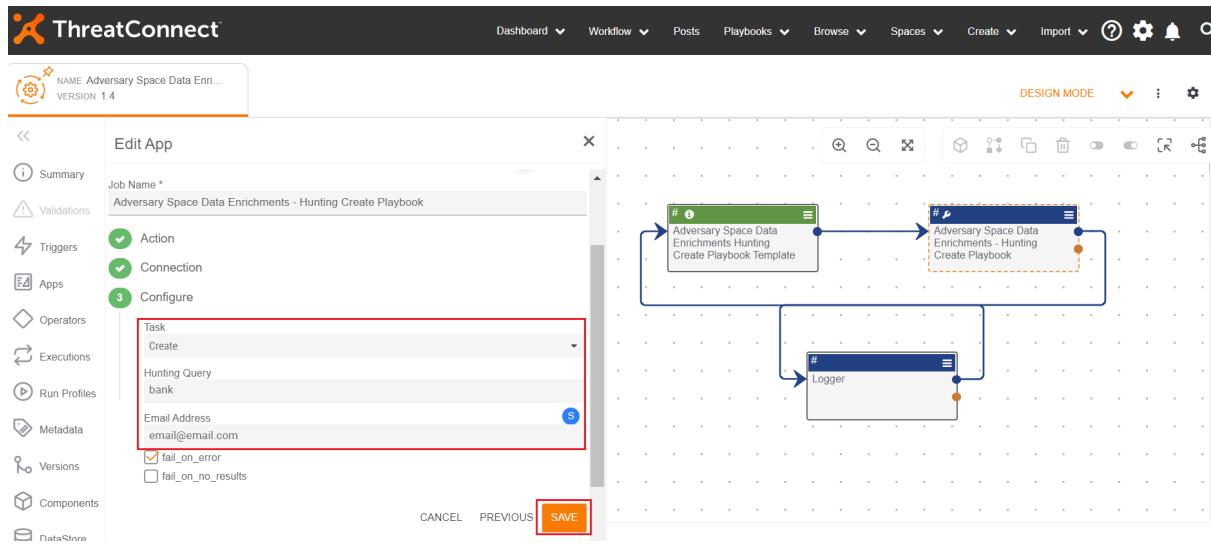
8. Running Adversary Space Data Hunting Create Playbook

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

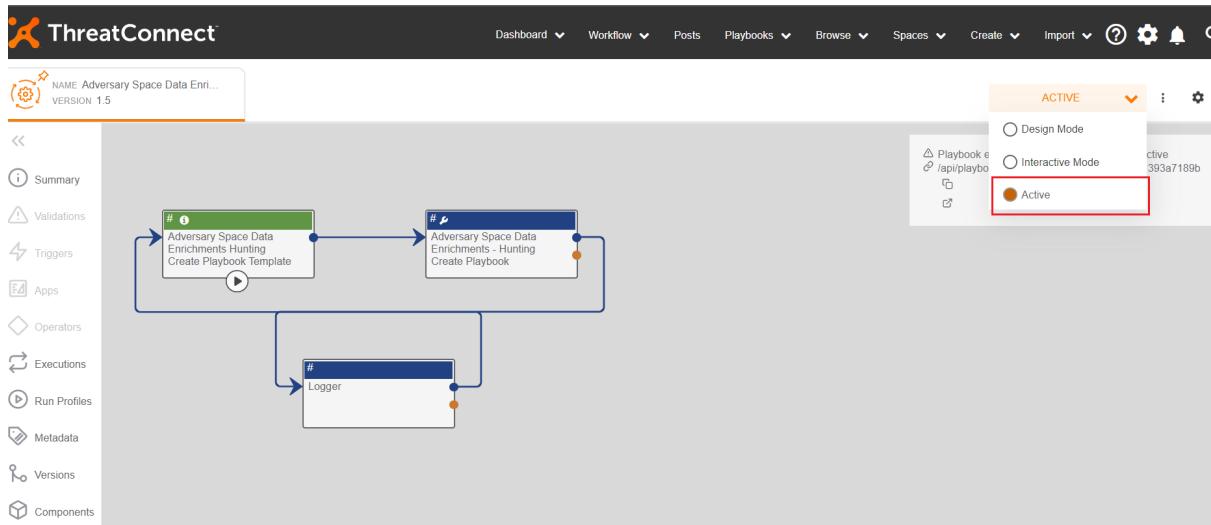


Step 2: Go to Configure section of the App and provide your desired values to search and click on Save as shown below.

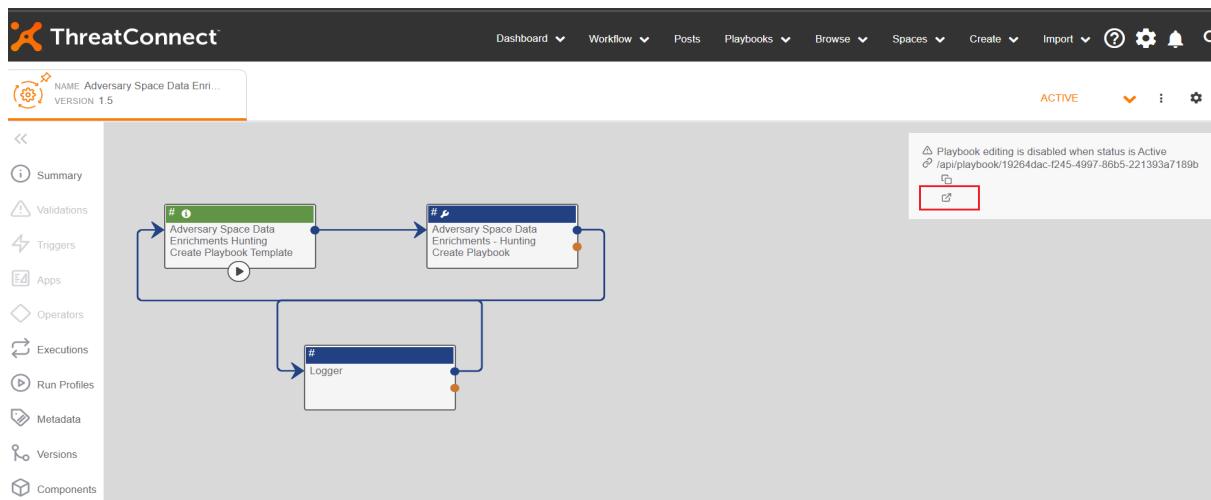
ThreatConnect – Adversary Space Data Enrichments App User Guide



Step 3: Activate the Playbook as shown below.

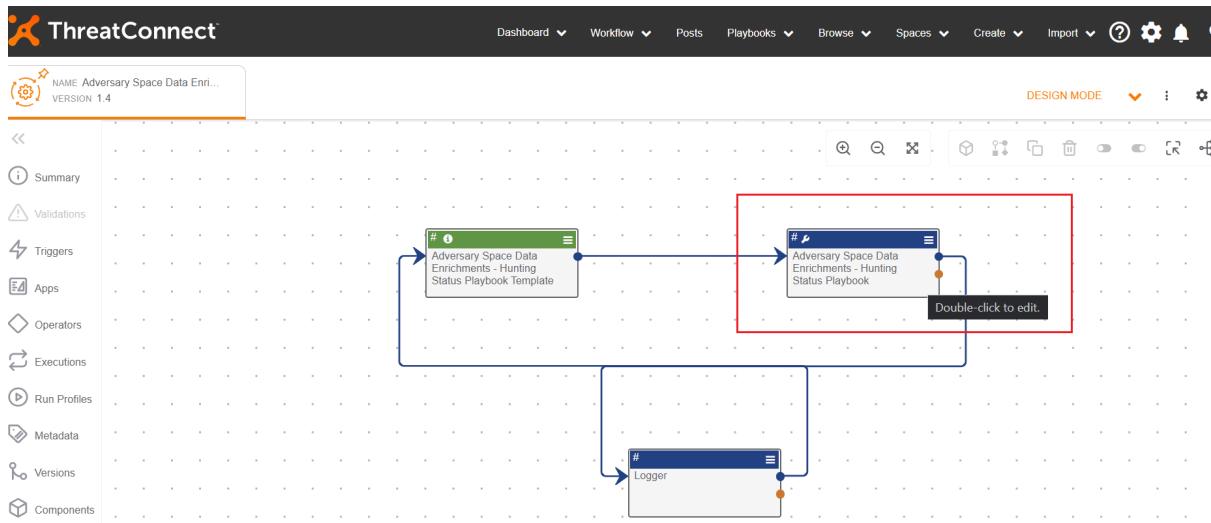


Step 4: Once the Playbook is activated, please click on the execute endpoint, this will fetch the results from Andariel API.

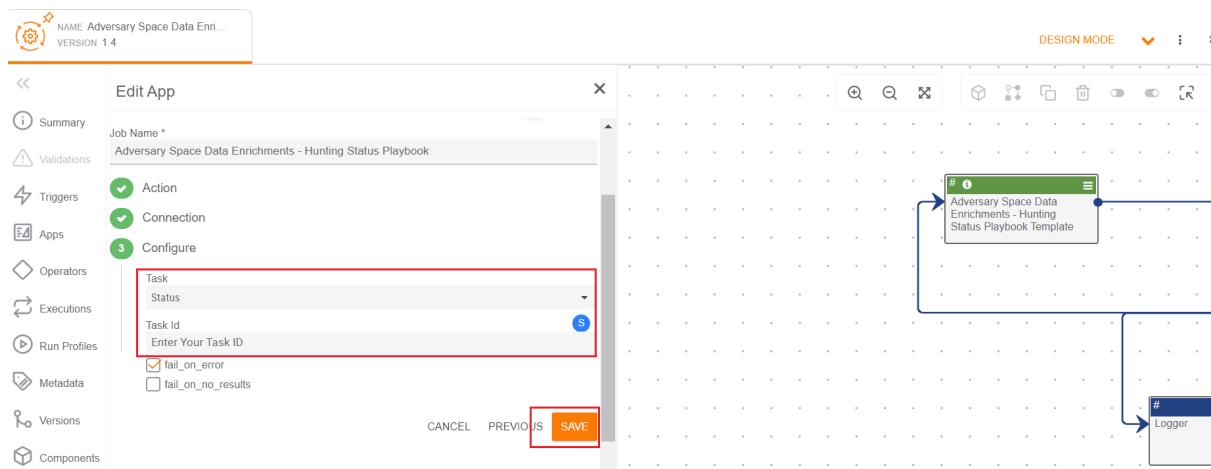


9. Running Adversary Space Data Hunting Status Playbook

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

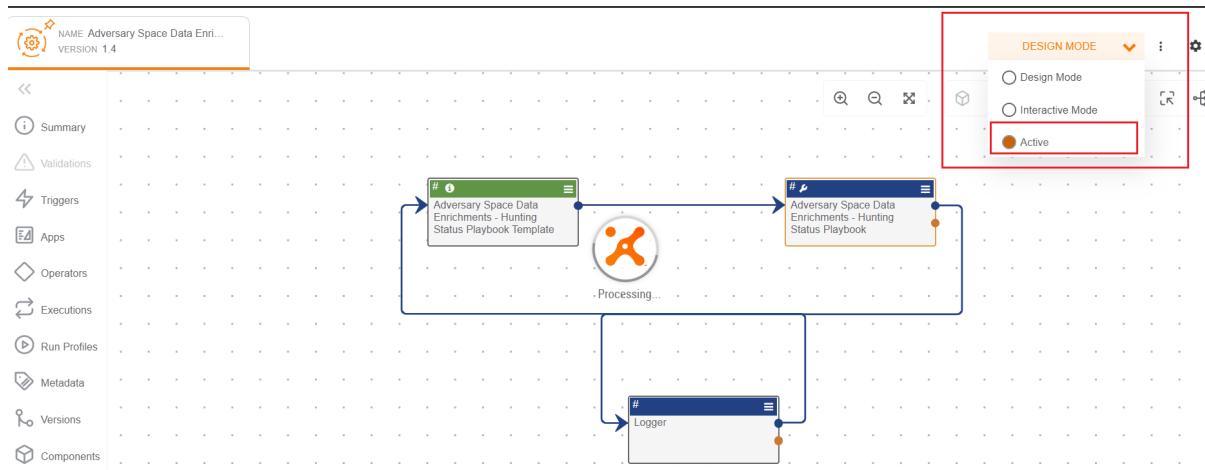


Step 2: Go to Configure section of the App and provide your desired values to search and click on Save as shown below.

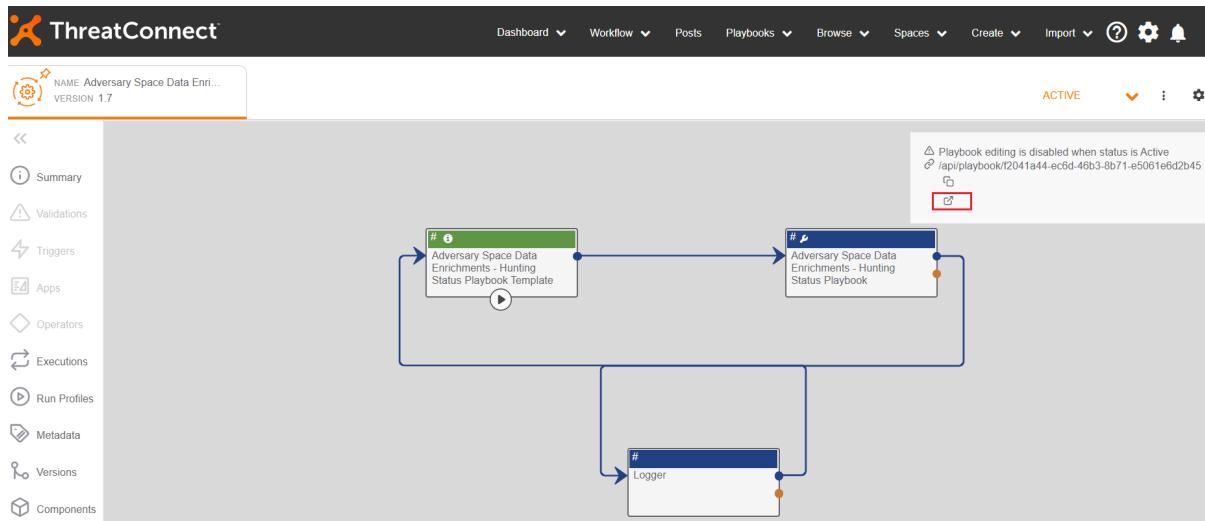


Step 3: Activate the Playbook as shown below.

ThreatConnect – Adversary Space Data Enrichments App User Guide



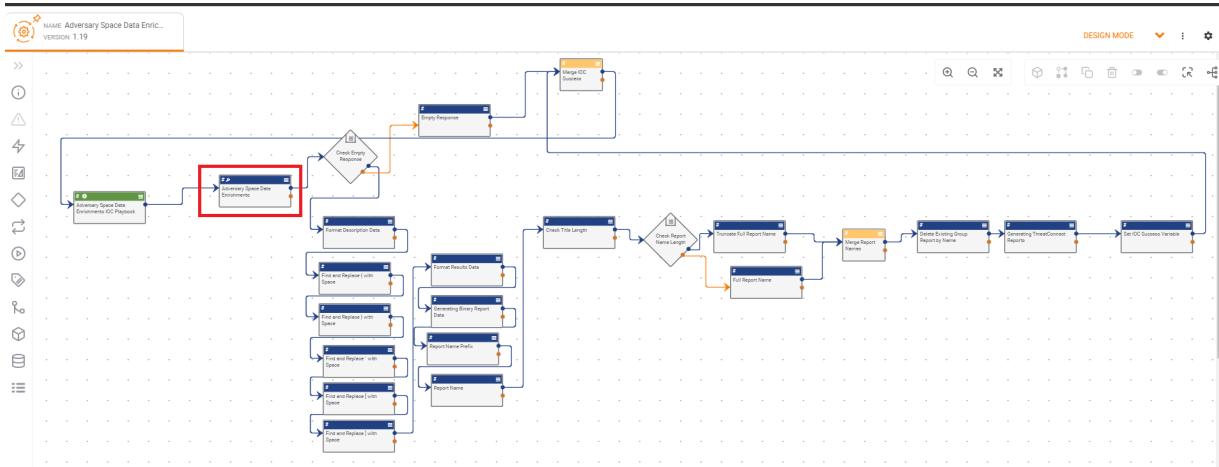
Step 4: Once the Playbook is activated, please click on the execute endpoint, this will fetch the results from Andariel API.



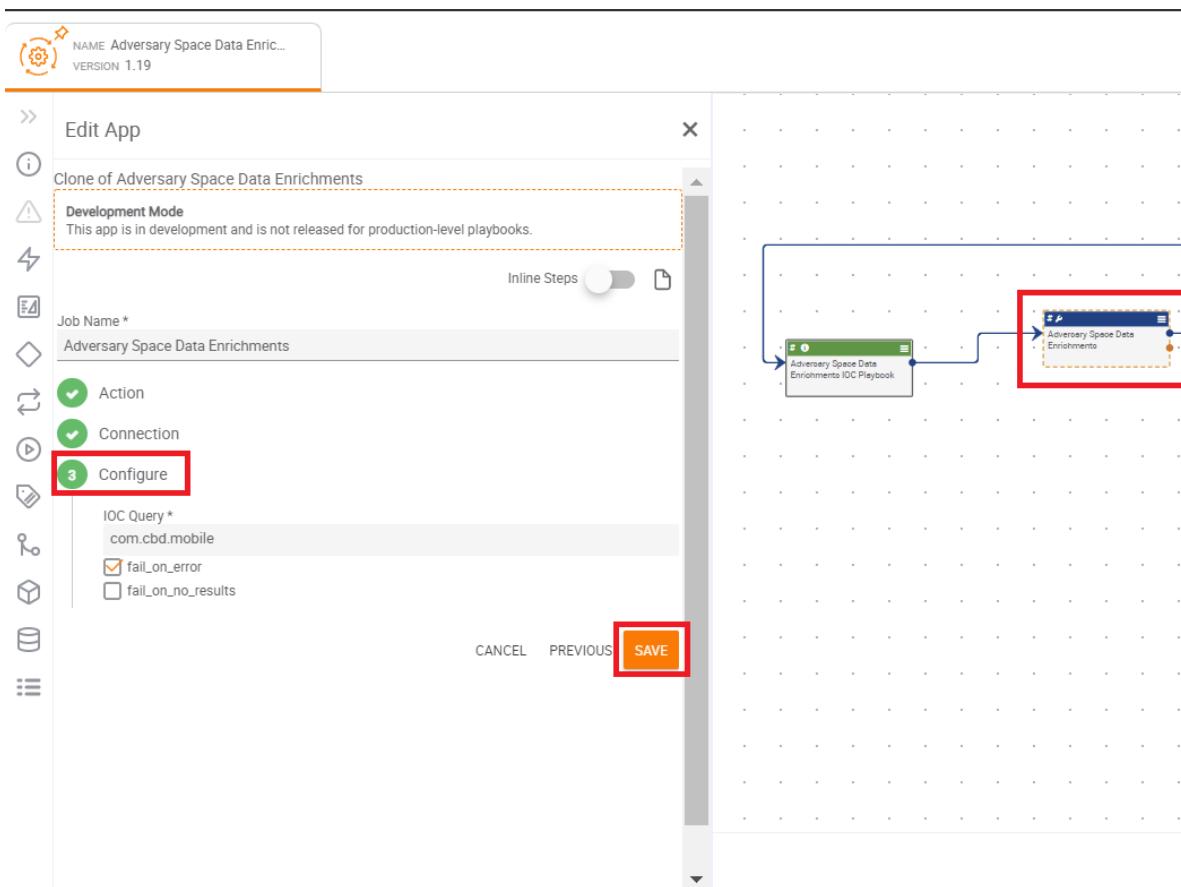
10. Running Adversary Space Data Enrichments IOC Playbook

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

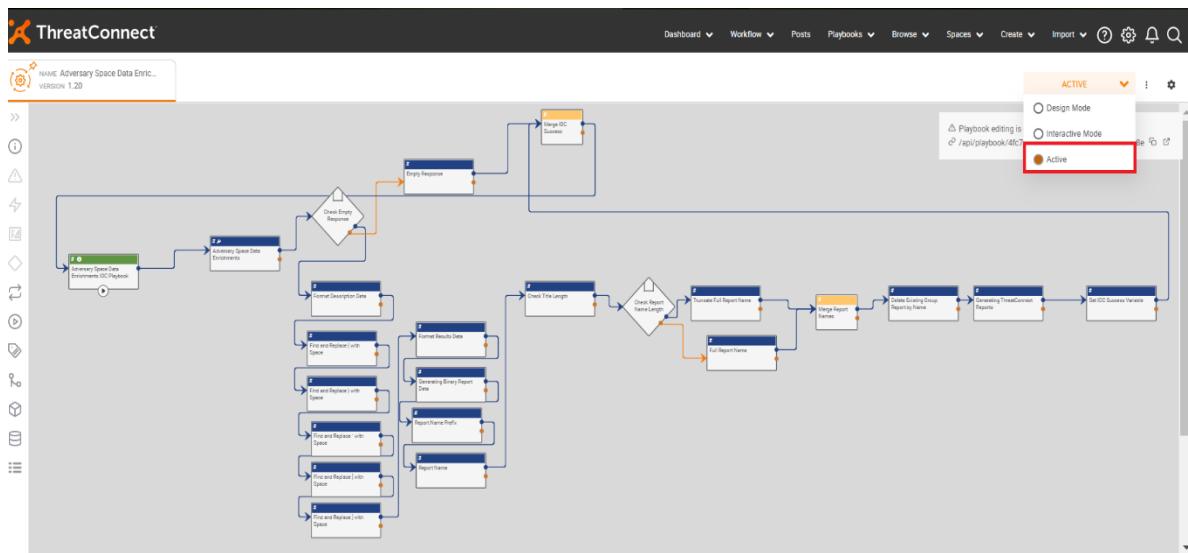


Step 2: Go to Configure section of the App and provide your desired values to search and click on Save as shown below.

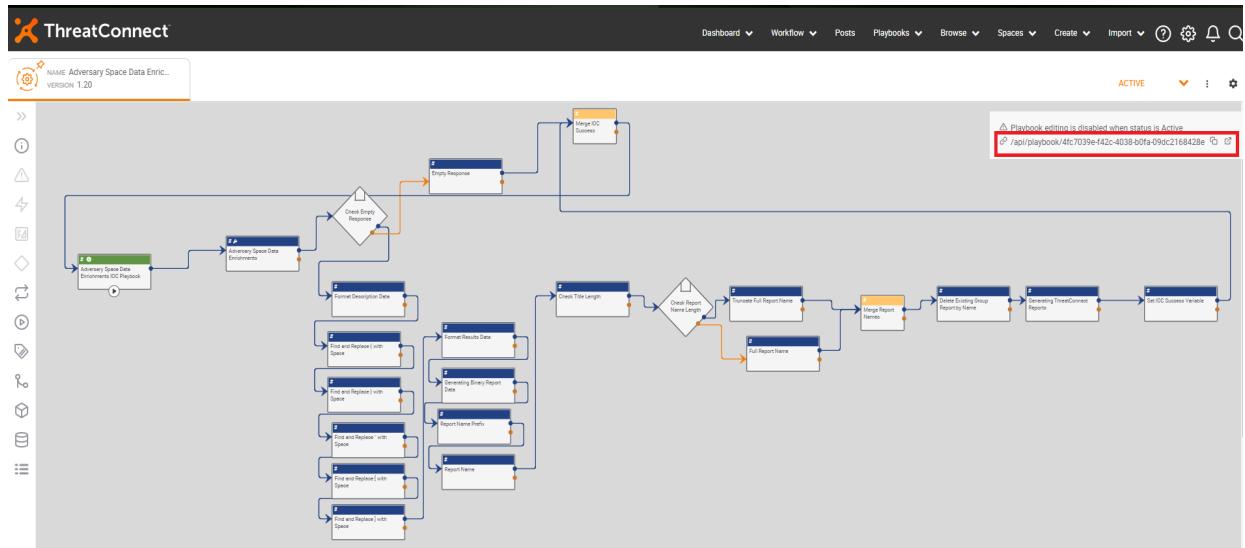


Step 3: Activate the Playbook as shown below.

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. To the right, there is a grid of items categorized under 'Address'. The items listed are: Address, Attack Pattern, File, Campaign, Host, Course of Action, URL, Document, ASN, Event, Bitcoin Address, Incident, CIDR, Intrusion Set, Email Subject, Malware, Ethereum Address, Report, Hashtag, Tactic, Host Asset IP, Task, Host Asset Name, Threat, Mutex, Tool, Registry Key, Vulnerability, and User Agent. Below the grid, it says 'No Results' and 'Tags'.

Please enter Address and Save

The screenshot shows the ThreatConnect interface with the 'Create Address' dialog box open. The 'Owner' dropdown is set to 'Advanced Intel Dev' and is highlighted with a red box. The dialog also contains fields for 'IP Address' (162.221.12.60) and 'Cancel' and 'Save' buttons. The background dashboard 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)	Adversary 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. On the left, the 'Indicator Analytics' section displays a 'ThreatAssess' card with a '281 Medium' rating and a 'Recent False Positive Reported' link. Below it are sections for 'CAL™ Insights', 'Trends', 'Classification', 'False Positives', 'Impressions', and 'Observations'. On the right, the 'Playbook Actions' section lists two playbooks: 'Adversary Space Data Enrichments Botnet Playbook' and 'Adversary Space Data Enrichments IOC Playbook', both marked as 'Ready'. The 'Associations' section shows 'Associated Groups (1)', 'Associated Indicators (1)', and 'Associated Victim Assets (0)'. A navigation bar at the top includes links for Dashboard, Workflow, Posts, Playbooks, Browse, Spaces, Create, Import, Help, Settings, and Logout.

Here you can find the Attributes

The screenshot shows the 'Attributes' tab of a specific item's details page. It includes fields for 'External Date Created' (2021-05-10T14:52:33Z), 'Source' (UAS Underground RDP Shop Breach Victim), and 'Description' (Adversary Space Data Enrichments Botnet Results). The 'Description' field contains a JSON snippet of logstash data:

```
_index: logstash-infra-usardp-hvt-f,
_type: _doc,
_id: ffbEvnkBhNeK8ybPU59c,
_score: 13.552097,
_source:
rr: n/a,
geopl:
lat: -43.6919,
ip: 162.221.12.69,
country_name: Canada,
country_code2: CA,
country_code3: CA,
continent_code: NA,
```

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

ThreatConnect – Adversary Space Data Enrichments App User Guide

The screenshot shows the ThreatConnect interface with the following details:

- Left Panel:** Shows "False Positives (Previous 7 Days)" with 0 results. Under "Impressions", "All Time" has 0, "Previous 7 Days" has 0, and "Today" has 0. Under "Observations", "Observations (All Time)" has 0 and "Observations (Previous 7 Days)" has 0.
- Top Bar:** Includes links for Dashboard, Workflow, Posts, Playbooks, Browse, Spaces, Create, Import, and various search/filter icons.
- Main Content Area:**
 - Associated Indicators (1):** One indicator is listed: "Host clearddos.com" owned by "Advanced Intel Dev" with a threat rating of 4.5/5.0, added on 05-31-2022.
 - Associated Victim Assets (0):** No assets are listed.
 - Details:** Shows the indicator's type as Address, version as IPv4, and various timestamps. It includes a "Overall Threat Rating" of 4.5/5.0 (High) and an "Overall Confidence Rating" of 0 - Unassessed.
 - Observations/False Positives:** Observations count is 0, Last Observed is -, and False Positives Reported is 0. A link to "Report False Positive" is available.
 - Tags:** No tags are assigned.
 - Investigation Links:** A list of external investigation tools: AlienVault OTX, Bing, BuiltWith, Censys, DomainTools, Google, Google Public DNS, Hurricane Electric, Hybrid Analysis, IBM X-Force Exchange, InQuest, InQuest IOC-DB, and PassiveTotal.

Now you can Download the Report

The screenshot shows the ThreatConnect interface with the following details:

- Top Bar:** Includes links for Dashboard, Workflow, Posts, Playbooks, Browse, Spaces, Create, Import, and various search/filter icons. The owner is listed as "Advanced Intel Dev".
- Left Panel:**
 - SOURCE:** "Adversary Space Data Enrichments Botnet Results for ip:162.221.12.60" is selected.
 - Actions:** Buttons for "Pivot", "Delete", "COPY TO MY ORG", and "DOWNLOAD PDF".
 - Overview:** The "Associations" tab is selected. Other tabs include Tasks, Activity, Associations, Sharing, and Spaces.
 - Description:** No default description is entered. Click here to add one.
 - Source:** No default source is entered. Click here to add one.
 - Security Labels:** "Choose Security Labels" dropdown.
 - 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. Buttons: "DOWNLOAD" and "+ UPDATE FILE".
- Right Panel:**
 - Associations:**
 - Associated Groups (0):** No groups are listed.
 - Associated Indicators (2):** Two indicators are listed: "Address 162.221.12.60" and "Host clearddos.com", both owned by "Advanced Intel Dev" with a threat rating of 4.5/5.0, added on 06-01-2022.
 - Associated Victim Assets (0):** No assets are listed.
 - Details:** Shows the report type as Report, added on 06-01-2022 at 12:24 GMT by Venkat Rambatza, modified on 06-01-2022 at 12:24 GMT, and published on 06-01-2022.

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'. In the main area, there's a search bar with filters and a table of indicators. A red box highlights the 'Create' dropdown menu in the top right corner.

Indicator	Group	Track
Address	Adversary	Victim
E-Mail Address	Attack Pattern	
File	Campaign	
Host	Course of Action	
URL	Document	
ASN	Event	
Bitcoin Address	Incident	
CIDR	Intrusion Set	
Email Subject	Malware	
Ethereum Address	Report	
Hashtag	Tactic	
Host Asset IP	Task	
Host Asset Name	Threat	
Mutex	Tool	
Registry Key	Vulnerability	
User Agent		

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'. The 'SAVE' button is 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 '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 displays various threat intelligence sections like 'Indicator Analytics', 'ThreatAssess', and 'CAL™ Insights'. On the right side, the 'Playbook Actions' section is open, showing three available playbooks: 'Adversary Space Data Enrichments Botnet Playbook' (selected and highlighted with a red border), 'Adversary Space Data Enrichments Bot Creds Playbook', and 'Adversary Space Data Enrichments IOC Playbook'. The status for the selected playbook is 'Ready'.

This screenshot is similar to the one above but shows the outcome of running the 'Botnet Playbook'. The 'Status' column for the playbook now shows 'Ready' with a green checkmark and the message 'Host Playbook Successful' in red. The rest of the interface remains the same, displaying the 'zigg.nl' source details and various threat intelligence sections.

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

This screenshot shows the ThreatConnect interface after the 'Botnet Playbook' has been run successfully. The 'Status' column for the playbook now shows 'Ready' with a green checkmark and the message 'Host Playbook Successful' in red. The 'Associations' section on the right shows a new entry: 'Associated Groups (1)' with a single item. The 'Details' section shows the host information: Type: Host, Added: 09-01-2022 11:56 GMT, Modified: 09-01-2022 11:57 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 title 'Adversary Space Data Enrichments Bot Creds Results'. The 'Tags' section is highlighted with a red box, showing a 'Recent Tag...' button. Other sections like 'Description', 'Associations', and 'Details' are also visible.

Here you are enabled to download report

The screenshot shows the ThreatConnect interface with the title 'Adversary Space Data Enrichments Bot Creds Results for ziggo.nl'. The 'Report File' section is highlighted with a red box, showing a 'Download' button. Other sections like 'Description', 'Associations', and 'Details' are also visible.

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 unchecked), and a 'Follow Item' button.

Indicator Analytics section:

- ThreatAssess:** A gauge showing a score of 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) <input checked="" type="checkbox"/>	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 unchecked), 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) <input checked="" type="checkbox"/>	Adversary 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
 - 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:**

