USER GUIDE v1.0.0

Farsight DNSDB Enrichment Integration Guide ThreatConnect Platform

Introduction

Farsight Security DNSDB® is the world's largest DNS intelligence database that provides a unique, fact-based, multifaceted view of the configuration of the global Internet infrastructure. DNSDB leverages the richness of Farsight's Security Information Exchange (SIE) data-sharing platform and is engineered and operated by leading DNS experts. Farsight collects Passive DNS data from its global sensor array. It then filters and verifies the DNS transactions before inserting them into the DNSDB, along with ICANN-sponsored zone file access download data. The end result is the highest-quality and most comprehensive DNS intelligence data service of its kind - with more than 100 billion DNS records since 2010.

This document outlines the process to install **Farsight DNSDB Enrichment** App provided by Farsight Security into the ThreatConnect Platform.

Farsight DNSDB Enrichment Playbook App enables ThreatConnect Platform users to perform On-Demand Enrichment of Passive DNS using the Farsight DNSDB Enrichment source.

1. Configuration

1.1. Requirement

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

- Access to ThreatConnect instance
- Access to execute ThreatConnect Playbooks
- Farsight DNSDB API Key provisioned by Farsight Security to authenticate requests to Farsight DNSDB API
- Farsight DNSDB Server API URL

- Farsight DNSDB Enrichment app installed in ThreatConnect Instance. (See **App Installation** section)
- Farsight DNSDB Playbook Templates installed in ThreatConnect Instance.
- Farsight DNSDB specific custom attributes imported in ThreatConnect Instance.

1.2. Farsight DNSDB Enrichment App Installation

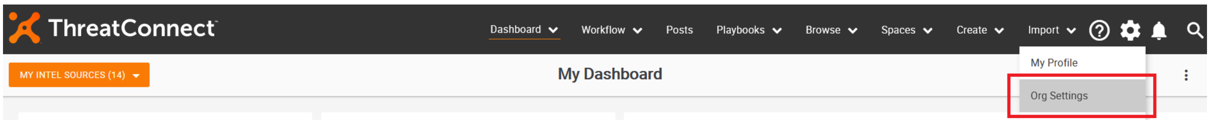
Farsight DNSDB Enrichment App for ThreatConnect is available on GitHub.
Download the App package with tcx extension and install it in your ThreatConnect instance. For installation instructions, refer to the "Install an App" in the ThreatConnect System Administration Guide. For more information, contact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

1.3. Farsight DNSDB Enrichment App Configuration

- Farsight DNSDB API Key - String
  - Farsight DNSDB API Key provisioned by Farsight Security.
- Farsight DNSDB Server - String
  - Farsight DNSDB Server API URL
- Max Pivots - Integer (Default value set to 10)
  - Limit the number of intermediate pivot queries used by playbooks.
- Results Limit - Integer (Default value set to 100)
  - Limit for the number of results returned via these lookup methods.
- Indicator - String
  - Host or Address Value.
- Farsight DNSDB Start Date - String
  - Farsight DNSDB Start Date Value in YYYY-MM-DD format.
- Farsight DNSDB End Date - String
  - Farsight DNSDB End Date Value in YYYY-MM-DD format.
- 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 Farsight DNSDB API, if set to True.

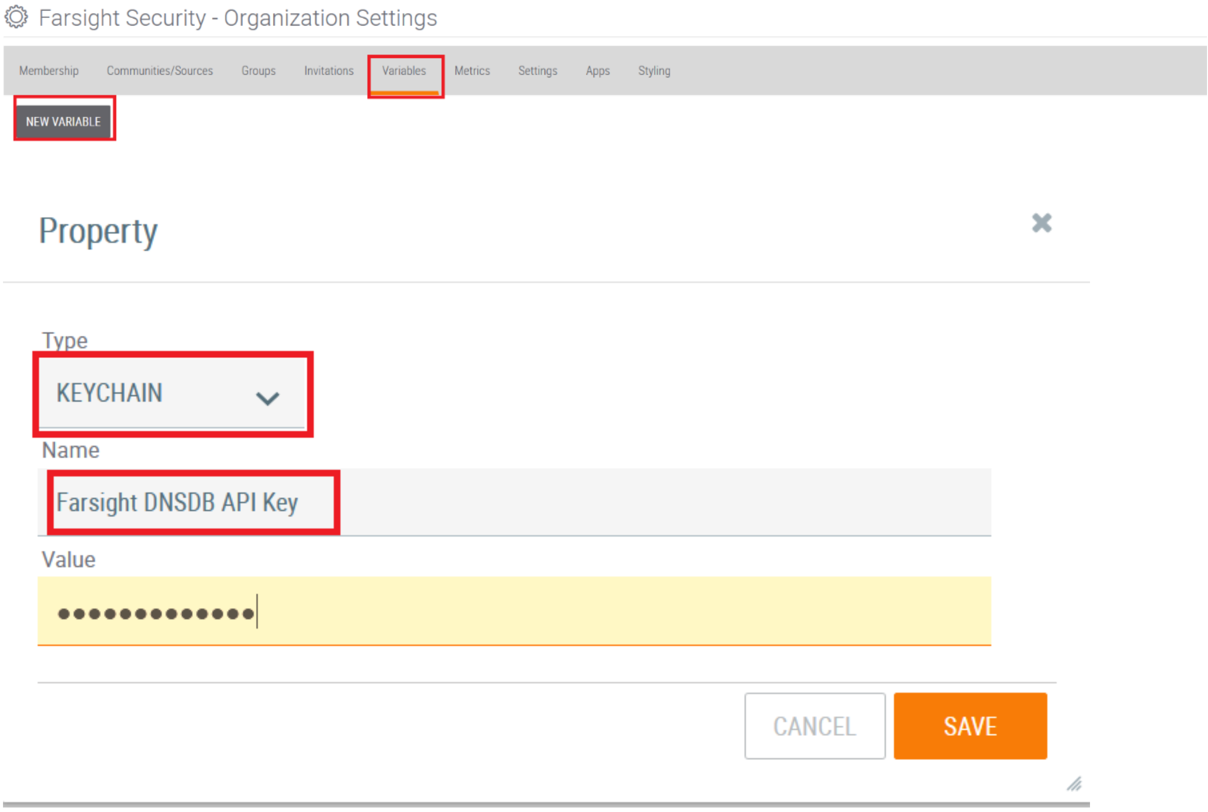
1.4. Farsight DNSDB API Key Variable

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



- Go to Variables
  1. Click on New Variable

2. Type = KEYCHAIN
3. Name = Farsight DNSDB API Key
4. Value = API Key provided by Farsight Security
5. Click on Save.



Type: KEYCHAIN

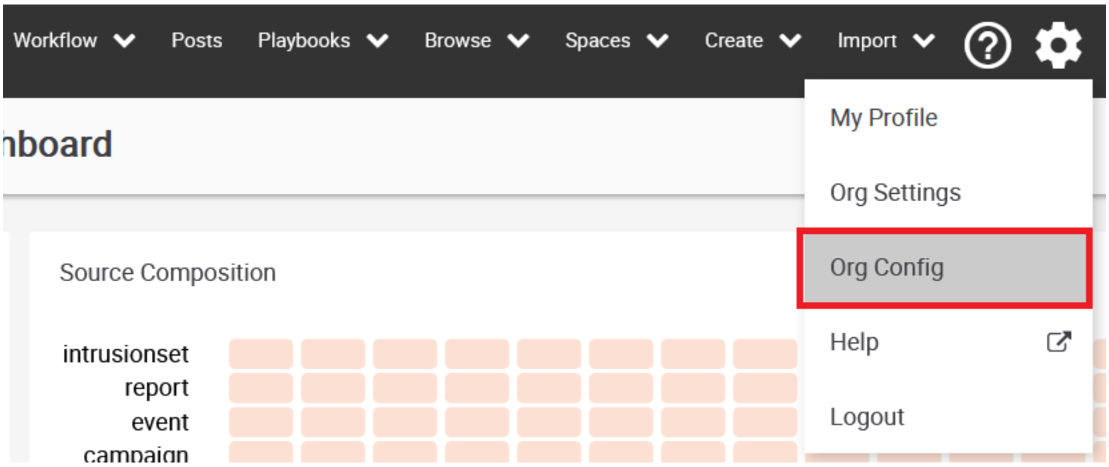
Name: Farsight DNSDB API Key

Value: ••••••••••••••

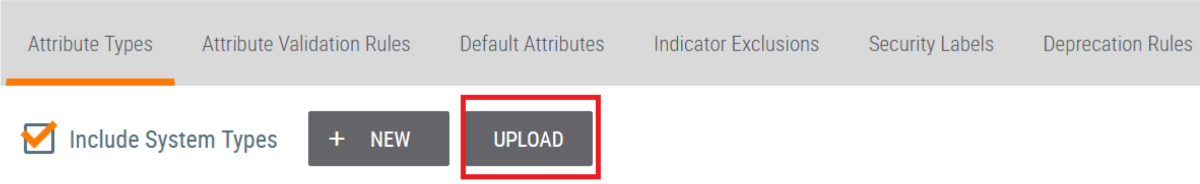
1.5. Adding Farsight DNSDB Attributes

You can find the Farsight_DNSDB_Attributes.json file available on GitHub, please download it.

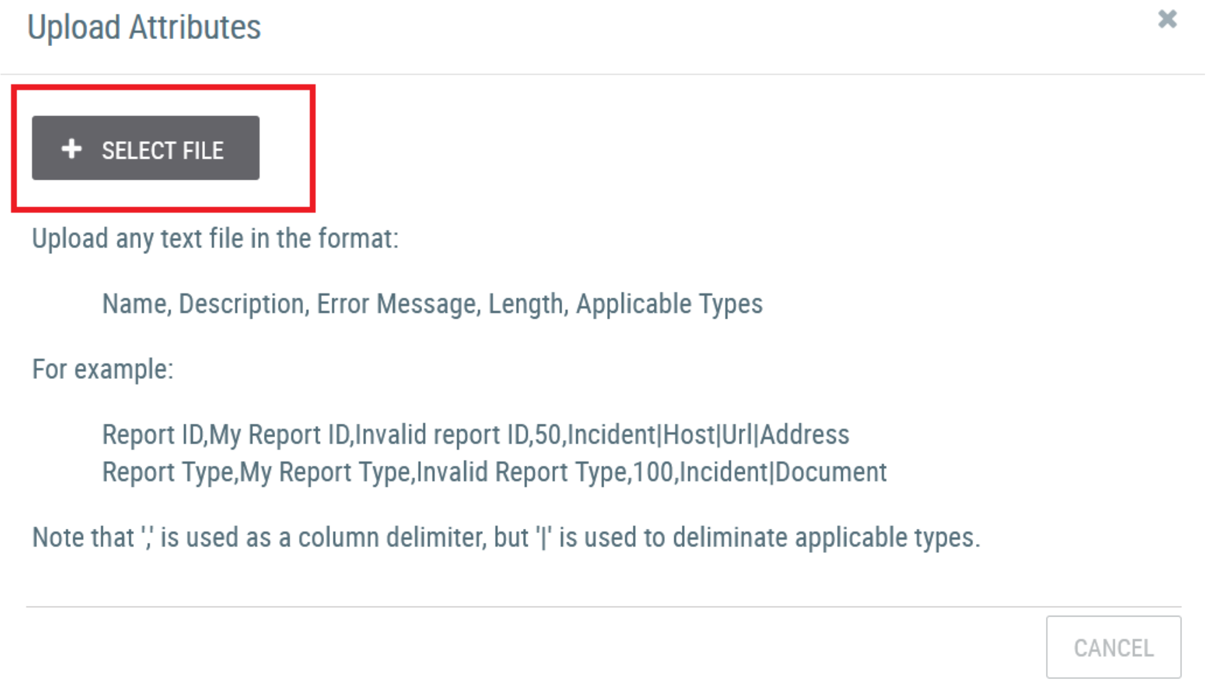
- **Step 1**: Click on the settings (gear icon) in the top right to get to your Org Config page.



- **Step 2**: Click on the Upload button.



- **Step 3**: Click on the Select File button and navigate to the Farsight_DNSDB_Attributes.json file, which was downloaded in the above step.



Upload any text file in the format:

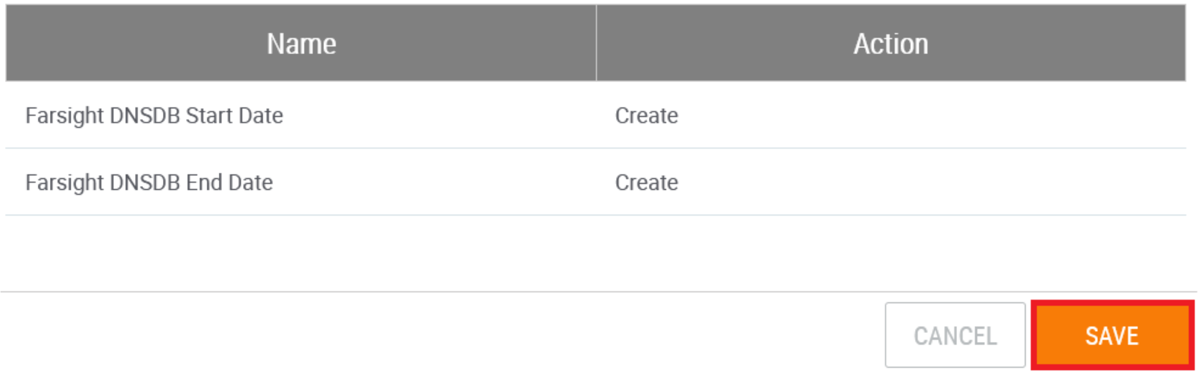
Name, Description, Error Message, Length, Applicable Types

For example:

```
Report ID,My Report ID,Invalid report ID,50,Incident|Host|Url|Address
Report Type,My Report Type,Invalid Report Type,100,Incident|Document
```

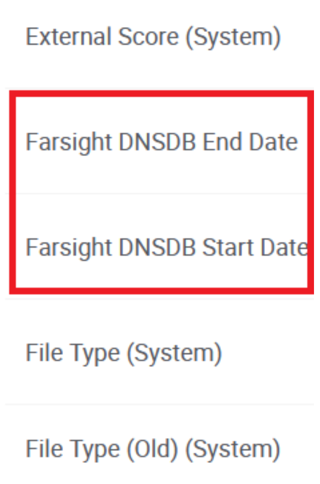
Note that ',' is used as a column delimiter, but '|' is used to deliminate applicable types.

- **Step 4**: Click on Save



Name	Action
Farsight DNSDB Start Date	Create
Farsight DNSDB End Date	Create

- **Step 5**: After saving Farsight DNSDB Start Date and Farsight DNSDB End Date custom attributes will be created as shown below.



External Score (System)

Farsight DNSDB End Date

Farsight DNSDB Start Date

File Type (System)

File Type (Old) (System)

2. Farsight DNSDB Playbook Templates

2.1. Farsight DNSDB Enrichment Playbook Templates Installation

Farsight DNSDB provides three Playbook Templates

- Farsight DNSDB Co-Located Host Playbook Template
  - **This use case describes the desire to easily identify Hosts that are co-located (based on Address) based on the input of a Host and a given point in time. The response would be a set of domains that also shared the same IP address as the originating domain name at the given point in time.**

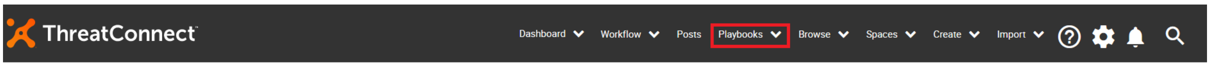
- Farsight DNSDB Historical Address Playbook Template
  - **This use case describes the desire to identify all Addresses used as DNS A records for a given Host based on a time window from a starting and stopping point in time**

- Farsight DNSDB Historical Host Playbook Template
  - **This use case describes the desire to identify all Hosts that resolved to a given Address based on a time window from a starting and stopping point in time.**

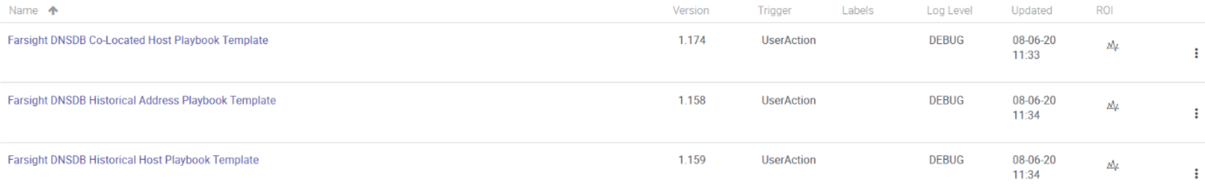
These Playbook Templates are available on GitHub. These templates provide a basic understanding on how to use the Farsight DNSDB Enrichment App in the playbooks.
To install these Playbook Templates, visit the Playbooks tab within the ThreatConnect Platform. Select New > Import and locate the PBX file you wish to add to your ThreatConnect Platform. Follow the on-screen instructions to complete the Playbook Template import.

2.2. Making sure the Playbook is set to active

- **Step1**: Go to the playbook menu in the top banner area to select the Farsight DNSDB playbook Templates.

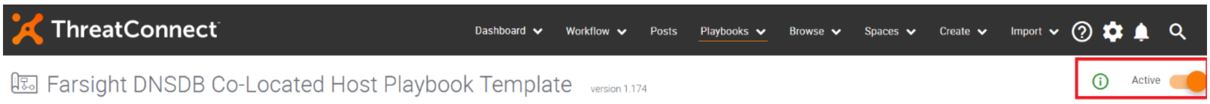


- **Step2**: Click and open each of the Farsight DNSDB playbook Templates.

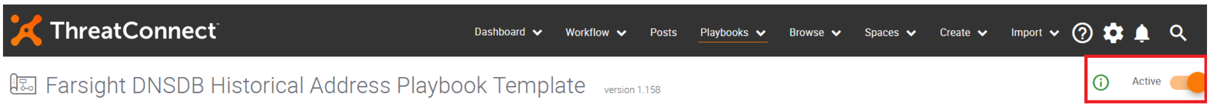


Name	Version	Trigger	Labels	Log Level	Updated	ROI
Farsight DNSDB Co-Located Host Playbook Template	1.174	UserAction		DEBUG	08-06-20 11:33	
Farsight DNSDB Historical Address Playbook Template	1.158	UserAction		DEBUG	08-06-20 11:34	
Farsight DNSDB Historical Host Playbook Template	1.159	UserAction		DEBUG	08-06-20 11:34	

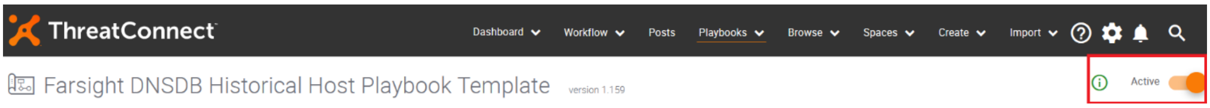
- **Step3**: Toggle the switch to mark the playbook as active.



Farsight DNSDB Co-Located Host Playbook Template version 1.174

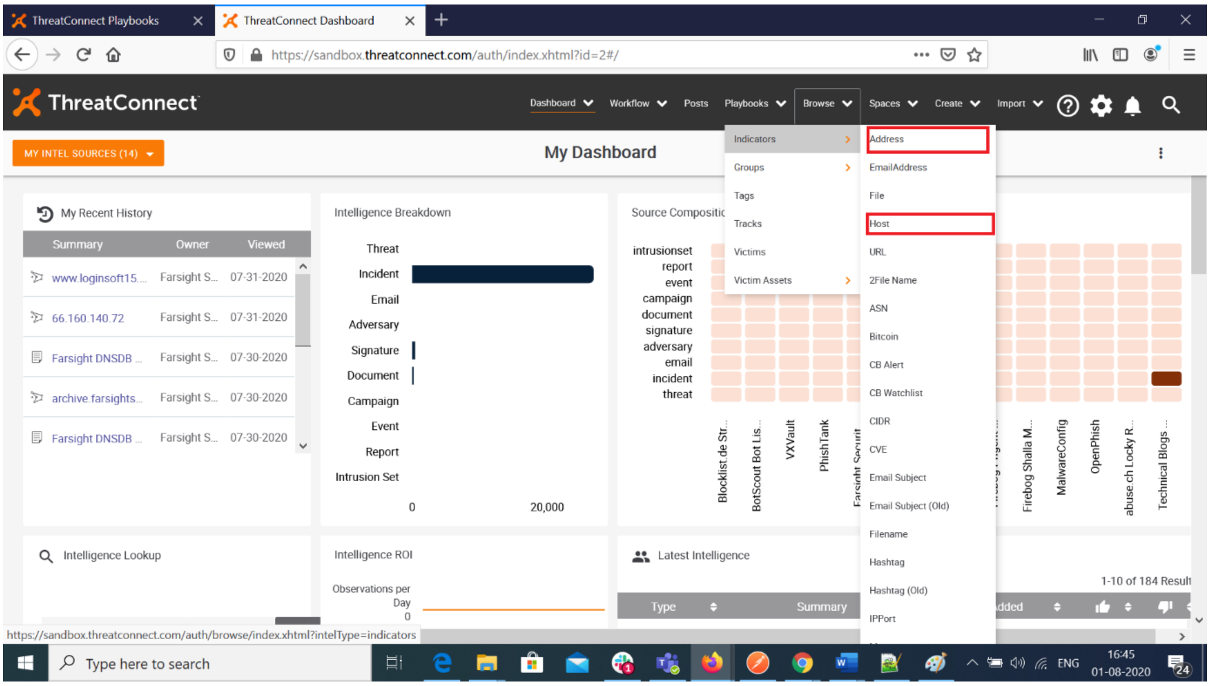


Farsight DNSDB Historical Address Playbook Template version 1.158

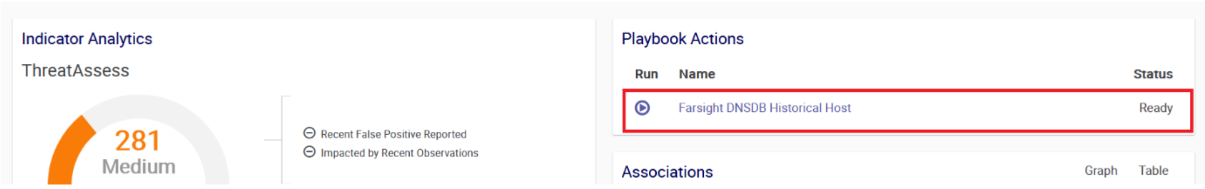


Farsight DNSDB Historical Host Playbook Template version 1.159

2.3. Browse to the existing Host/Address Indicators (or) Create a new Host/Indicator.

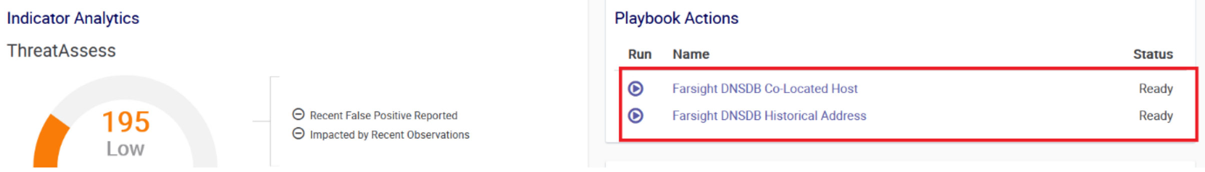


2.4. For Address Indicators, you will see the "Farsight DNSDB Historical Host" Playbook Action in the details page



Run	Name	Status
⊙	Farsight DNSDB Historical Host	Ready

2.5. For Host Indicators, you will see the "Farsight DNSDB Co-Located Host" and "Farsight DNSDB Historical Address" Playbook Actions in the details page


Indicator Analytics
ThreatAssess
195
Low
Recent False Positive Reported
Impacted by Recent Observations
Playbook Actions

Run	Name	Status
⊙	Farsight DNSDB Co-Located Host	Ready
⊙	Farsight DNSDB Historical Address	Ready

2.6. Provide the Farsight DNSDB Start Date, Farsight DNSDB End Date attributes to the indicator.

- Click on plus sign in the attributes section, then in the edit attribute page select Farsight DNSDB Start Date/ Farsight DNSDB End Date and provide values in YYYY-MM-DD format, and click on save.

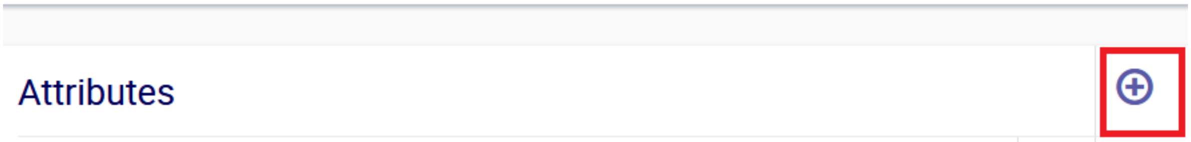
Important Points to be noted:

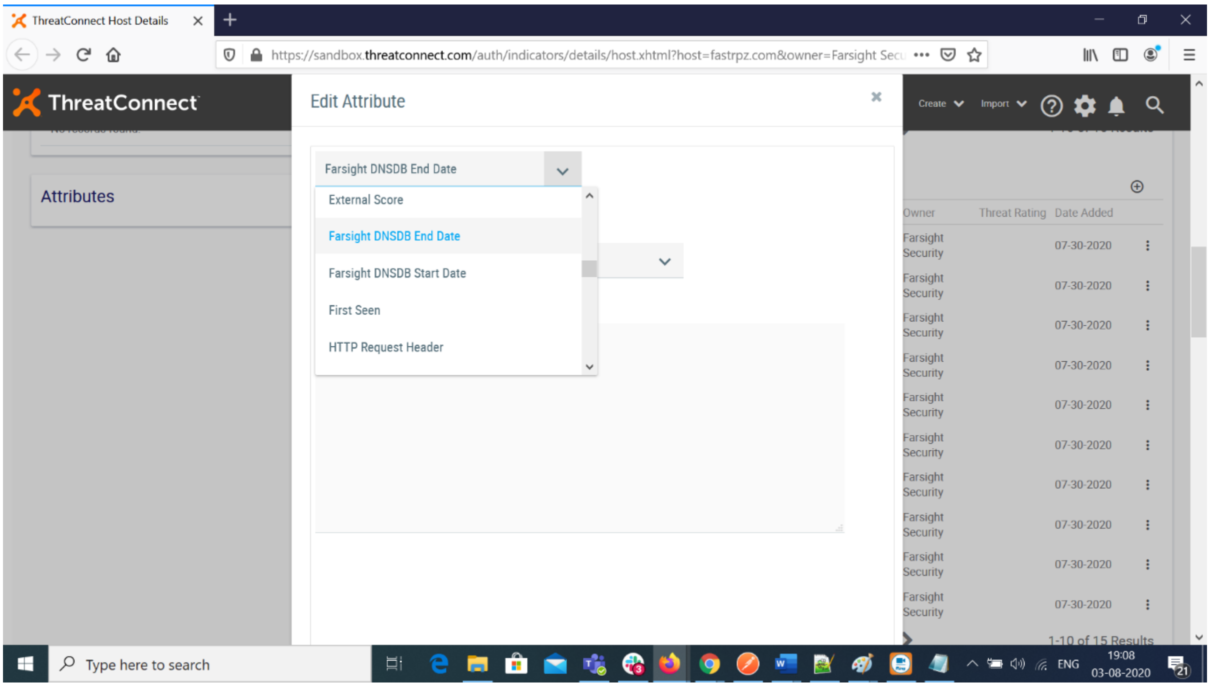
- **If multiple date values are provided for Farsight DNSDB Start Date or Farsight DNSDB End Date, the lookup will consider the first date value provided in the list.**

- **If only Farsight DNSDB Start Date is provided by the user, system would use this value and provide results that were last observed after the start date.**

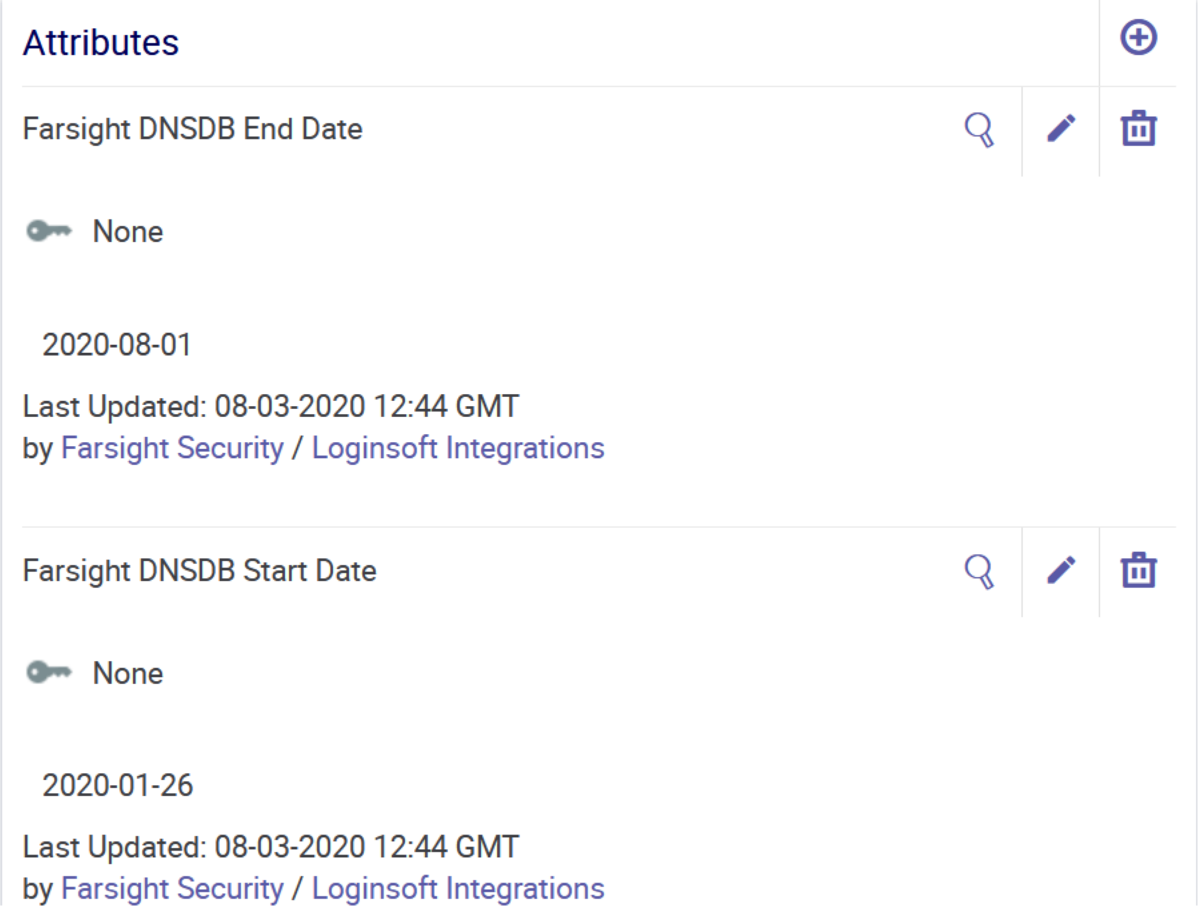
- **If only Farsight DNSDB End Date is provided by the user, system would use**
  - **Farsight DNSDB Start Date = Farsight DNSDB End Date – 90 days**

- **If Farsight DNSDB Start Date and Farsight DNSDB End Date are not provided by the user, system would use:**
  - **Farsight DNSDB Start Date = Todays Date – 90 days**
  - **Farsight DNSDB End Date = Today’s Date**





© 2020 Farsight Security. All Rights Reserved.



Attributes

Farsight DNSDB End Date

None

2020-08-01

Last Updated: 08-03-2020 12:44 GMT
by Farsight Security / Loginsoft Integrations

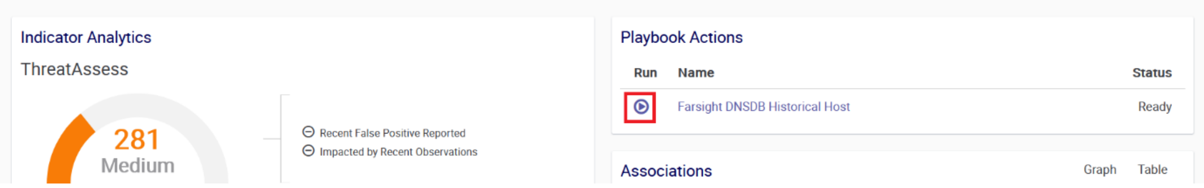
Farsight DNSDB Start Date

None

2020-01-26

Last Updated: 08-03-2020 12:44 GMT
by Farsight Security / Loginsoft Integrations

2.7. Run the desired playbook actions by clicking the play button.



Indicator Analytics

ThreatAssess

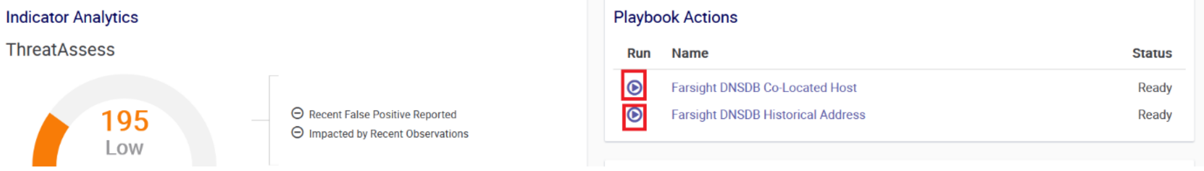
281
Medium

⊖ Recent False Positive Reported
⊖ Impacted by Recent Observations

Playbook Actions

Run	Name	Status
▶	Farsight DNSDB Historical Host	Ready

Associations



Indicator Analytics

ThreatAssess

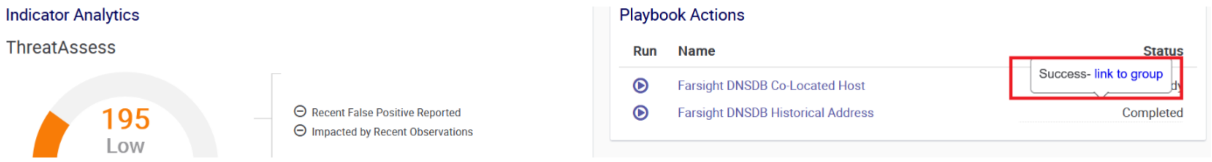
195
Low

⊖ Recent False Positive Reported
⊖ Impacted by Recent Observations

Playbook Actions

Run	Name	Status
▶	Farsight DNSDB Co-Located Host	Ready
▶	Farsight DNSDB Historical Address	Ready

- The Status for the playbook Action will change to Completed when done, mouse over to check the status, for successful results, you will see a link to the results group.
- The names of the Report Groups for the respective actions will be as follows
  - Farsight Results-CoLocated-Host-<DateTime>
  - Farsight Results-Historical-Address-< DateTime >
  - Farsight Results-Historical-Host-< DateTime >



Indicator Analytics

ThreatAssess

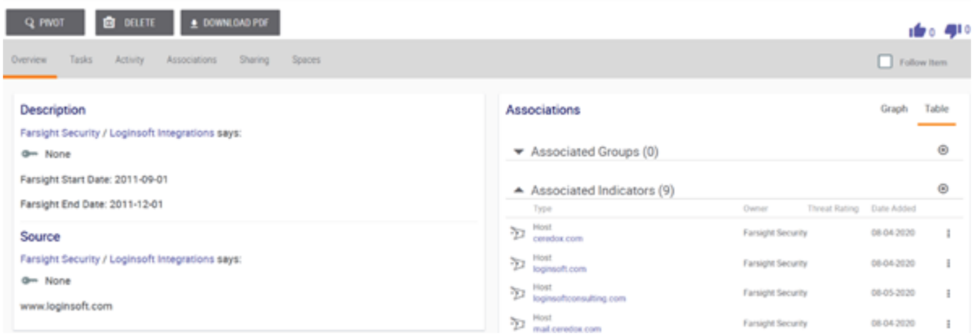
195 Low

⊖ Recent False Positive Reported
⊖ Impacted by Recent Observations

Playbook Actions

Run	Name	Status
⊙	Farsight DNSDB Co-Located Host	Success- link to group
⊙	Farsight DNSDB Historical Address	Completed

- Click on the "link to group", it will take you to the results group



Description

Farsight Security / Loginsoft Integrations says:

None

Farsight Start Date: 2011-09-01

Farsight End Date: 2011-12-01

Source

Farsight Security / Loginsoft Integrations says:

None

www.loginsoft.com

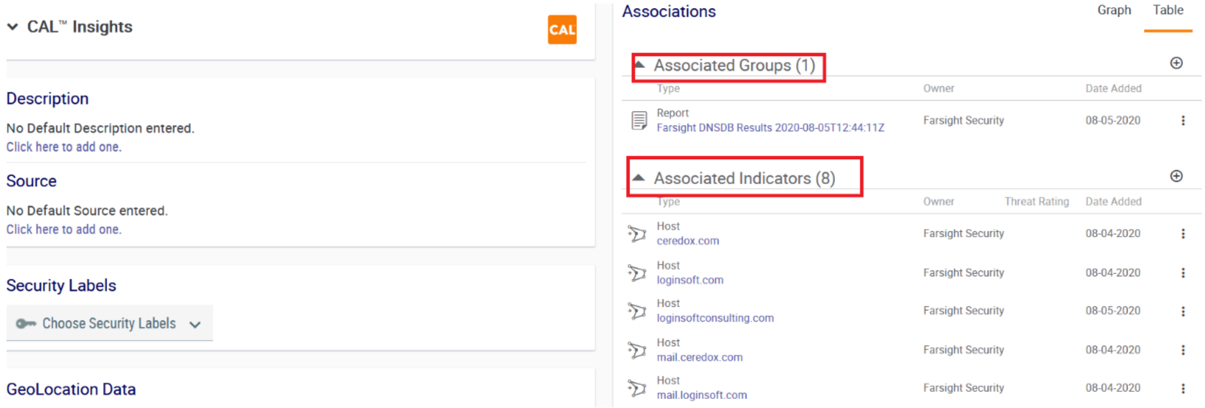
Associations

Associated Groups (0)

Associated Indicators (9)

Type	Owner	Threat Rating	Date Added
Host ceredox.com	Farsight Security		08-04-2020
Host loginsoft.com	Farsight Security		08-04-2020
Host loginsoftconsulting.com	Farsight Security		08-05-2020
Host mail.ceredox.com	Farsight Security		08-04-2020

- Refresh the Indicator page, you will see the newly created Report group under "Associated Groups" and newly created Indicators under "Associated Indicators"



CAL™ Insights

Description

No Default Description entered.
Click here to add one.

Source

No Default Source entered.
Click here to add one.

Security Labels

GeoLocation Data

Associations

Associated Groups (1)

Type	Owner	Date Added
Report Farsight DNSDB Results 2020-08-05T12:44:11Z	Farsight Security	08-05-2020

Associated Indicators (8)

Type	Owner	Threat Rating	Date Added
Host ceredox.com	Farsight Security		08-04-2020
Host loginsoft.com	Farsight Security		08-04-2020
Host loginsoftconsulting.com	Farsight Security		08-05-2020
Host mail.ceredox.com	Farsight Security		08-04-2020
Host mail.loginsoft.com	Farsight Security		08-04-2020

3. Outputs

Output	TC Type	Description
fs.co_located.rrset.json.raw	StringArray	Farsight DNSDB API response containing RRsets data in JSON format
fs.co_located.rrset.json.raw.count	String	Number of RRSets records in the response from Farsight DNSDB API
fs.co_located.rdata.json.raw	StringArray	Farsight DNSDB API response containing RData records in JSON format
fs.co_located.rdata.json.raw.count	String	Number of RData records in the response from Farsight DNSDB API
fs.co_located.rrset.results.data	StringArray	Processed response object of RRSets from Farsight DNSDB API
fs.co_located.rdata.results.data	StringArray	Processed response object of RData record values from Farsight DNSDB API
fs.historical_address.rrset.json.raw	StringArray	Farsight DNSDB API response containing RRsets data in JSON format
fs.historical_address.rrset.json.raw.count	String	Number of RRSets records in the response from Farsight DNSDB API
fs.historical_address.rrset.results.data	StringArray	Processed response object of RData record values from Farsight DNSDB API
fs.historical_host.rdata.json.raw	StringArray	Farsight DNSDB API response containing RData records in JSON format
fs.historical_host.rdata.json.raw.count	String	Number of RData records in the response from Farsight DNSDB API
fs.historical_host.rdata.results.data	StringArray	Processed response object of RData record values from Farsight DNSDB API
fs.start_date	String	Start Date Input used for this lookup
fs.end_date	String	End Date Input used for this lookup

fs.co_located.rrset.json.raw & fs.historical_address.rrset.json.raw, These output variables contain an array of objects containing the RRSets data in JSON format. Data can be extracted from JSON objects using JMESPath built in ThreatConnect App.

Attribute Name	Attribute Description
rrname	The owner name of the RRset in DNS presentation format
rrtype	The resource record type of the RRset, either using the standard DNS type mnemonic, or an RFC 3597 generic type
rdata	An array of one or more Rdata values
bailiwick	The "bailiwick" metadata value
count	The number of times the RRset was observed via passive DNS replication
time_first	UNIX epoch timestamps with second granularity indicating the first time the RRset was observed via passive DNS replication
time_last	UNIX epoch timestamps with second granularity indicating the last time the RRset was observed via passive DNS replication
zone_time_first	UNIX epoch timestamps with second granularity indicating the first time the RRset was observed via zone file import
zone_time_last	UNIX epoch timestamps with second granularity indicating the last time the RRset was observed via zone file import

fs.co_located.rdata.json.raw & fs.historical_host.rdata.json.raw, These output variables contain an array of objects containing the RData data in JSON format. Data can be extracted from JSON objects using JMESPath built in ThreatConnect App.

Attribute Name	Attribute Description
rrname	The owner name of the resource record in DNS presentation format
rrtype	The resource record type of the resource record, either using the standard DNS type mnemonic, or an RFC 3597 generic type
rdata	The record data value

count	The number of times the resource record was observed via passive DNS replication
time_first	UNIX epoch timestamps with second granularity indicating the first time the resource record was observed via passive DNS replication
time_last	UNIX epoch timestamps with second granularity indicating the last time the resource record was observed via passive DNS replication
zone_time_first	UNIX epoch timestamps with second granularity indicating the first time the resource record was observed via zone file import
zone_time_last	UNIX epoch timestamps with second granularity indicating the last time the resource record was observed via zone file import

fs.co_located.rrset.results.data & fs.historical_address.rrset.results.data, These output variables contain the same data as `fs.co_located.rrset.json.raw`, ‘fs.historical_address.rrset.json.raw’ output variables except all the timestamps are human readable (RFC3339 compliant) format. Data can be extracted from JSON objects using JMESPath built in ThreatConnect App.

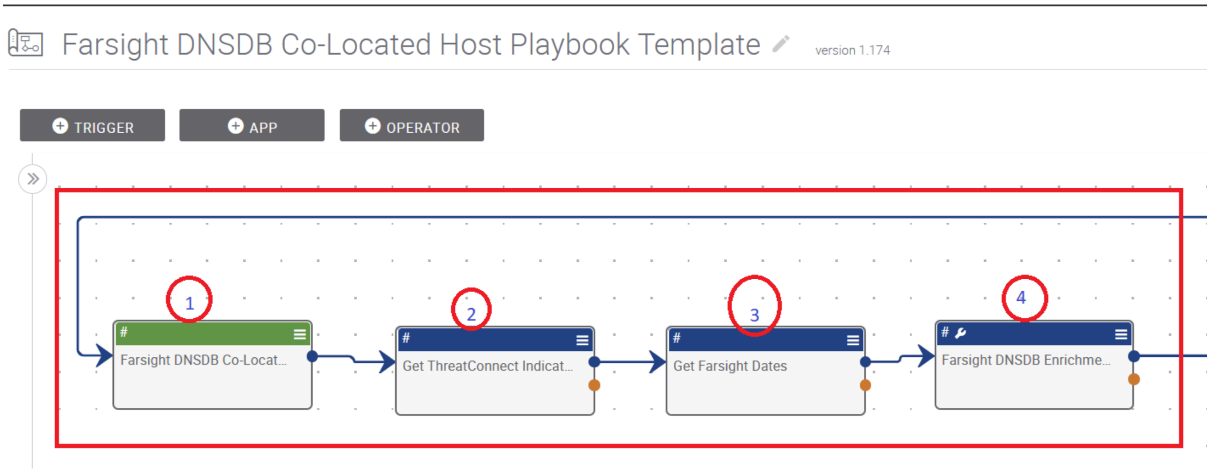
Attribute Name	**Attribute Description**
rrname	The owner name of the RRset in DNS presentation format
rrtype	The resource record type of the RRset, either using the standard DNS type mnemonic, or an RFC 3597 generic type
rdata	An array of one or more Rdata values
bailiwick	The "bailiwick" metadata value
count	The number of times the RRset was observed via passive DNS replication
time_first	Human readable (RFC3339 compliant) timestamps with second granularity indicating the first time the RRset was observed via passive DNS replication
time_last	Human readable (RFC3339 compliant) timestamps with second granularity indicating the last time the RRset was observed via passive DNS replication
zone_time_first	Human readable (RFC3339 compliant) timestamps with second granularity indicating the first time the RRset was observed via zone file import
zone_time_last	Human readable (RFC3339 compliant) timestamps with second granularity indicating the last time the RRset was observed via zone file import

fs.co_located.rdata.results.raw & fs.historical_host.rdata.results.raw, These output variables contain the same data as `fs.co_located.rdata.json.raw`,'fs.historical_host.rdata.json.raw' output variables except all the timestamps are human readable (RFC3339 compliant) format. Data can be extracted from JSON objects using JMESPath built in ThreatConnect App.

Attribute Name	Attribute Description
rrname	The owner name of the resource record in DNS presentation format
rrtype	The resource record type of the resource record, either using the standard DNS type mnemonic, or an RFC 3597 generic type
rdata	The record data value
count	The number of times the resource record was observed via passive DNS replication
time_first	Human readable (RFC3339 compliant) timestamps with second granularity indicating the first time the resource record was observed via passive DNS replication
time_last	Human readable (RFC3339 compliant) timestamps with second granularity indicating the last time the resource record was observed via passive DNS replication
zone_time_first	Human readable (RFC3339 compliant) timestamps with second granularity indicating the first time the resource record was observed via zone file import
zone_time_last	Human readable (RFC3339 compliant) timestamps with second granularity indicating the last time the resource record was observed via zone file import

4. APENDIX

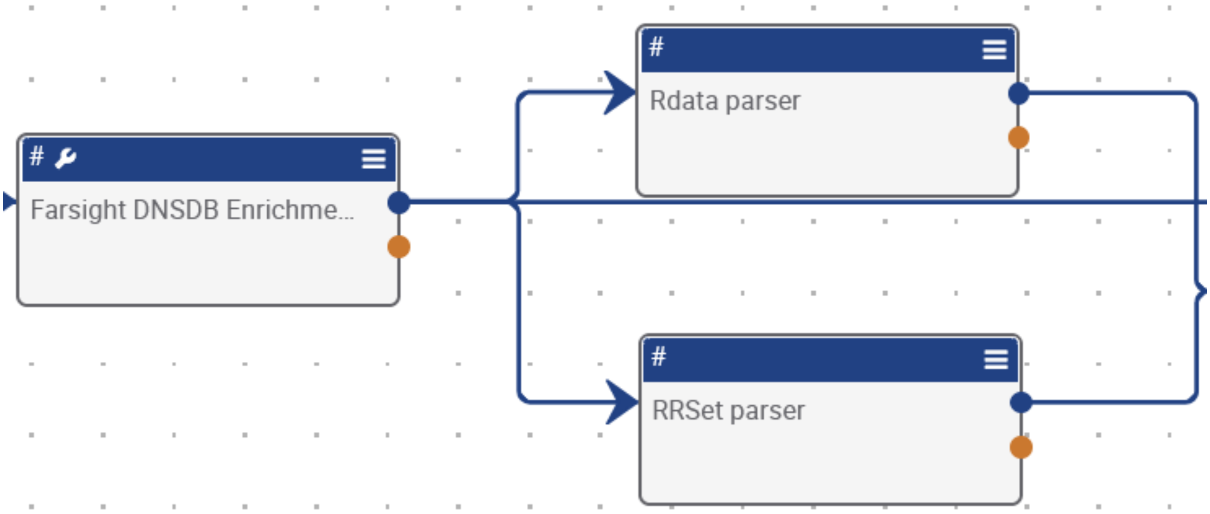
4.1. Farsight Co-Located Host Playbook Template


Farsight DNSDB Co-Located Host Playbook Template
version 1.174
TRIGGER
APP
OPERATOR
1
2
3
4
Farsight DNSDB Co-Locat...
Get ThreatConnect Indicat...
Get Farsight Dates
Farsight DNSDB Enrichme...

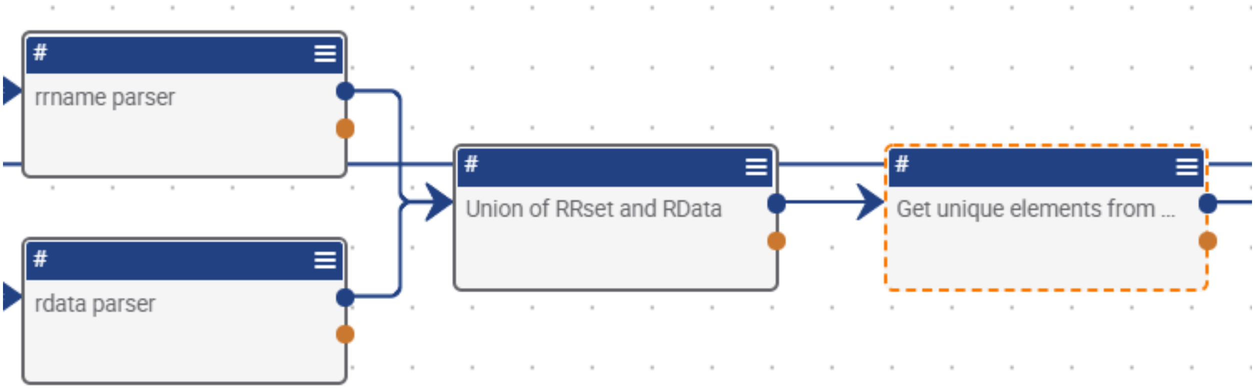
The above flow would be same for all the three playbook templates,

- First step is Trigger
- Second Step is to get the Indicator Details
- Third Step to get Farsight DNSDB Start and End Dates
- Fourth Step is Configuring the App.

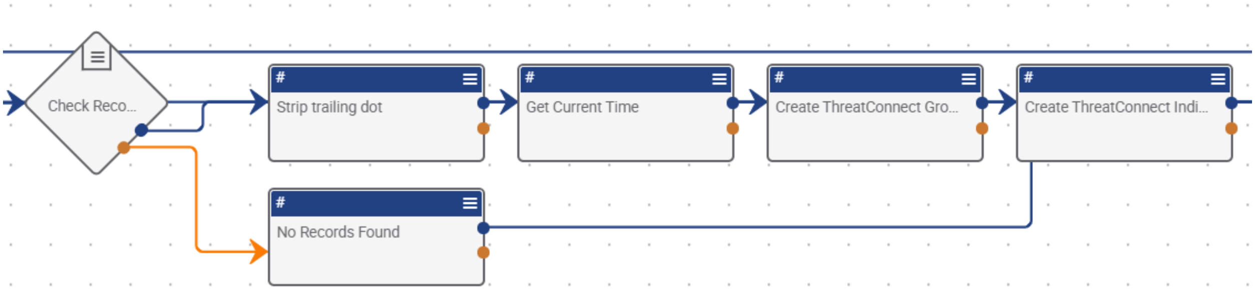
1. The Apps ‘RRSet parser' and ‘Rdata parser' are used to parse rrset and rdata json objects



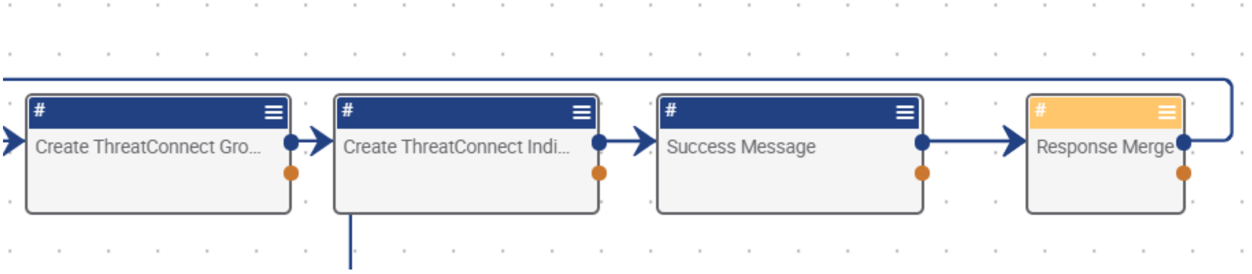
2. The following are two Array Operations named as 'Union of RRset and RData' and 'Get unique elements from parsed data' are used for merging the RRset and RData information and get unique results:



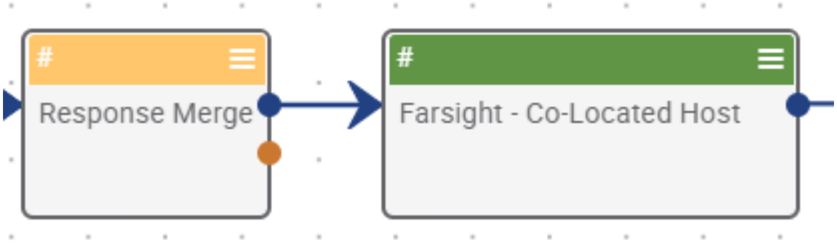
3. The below flow checks whether the results are returned, if yes create the Indicators and Report Group or else log as no results found.



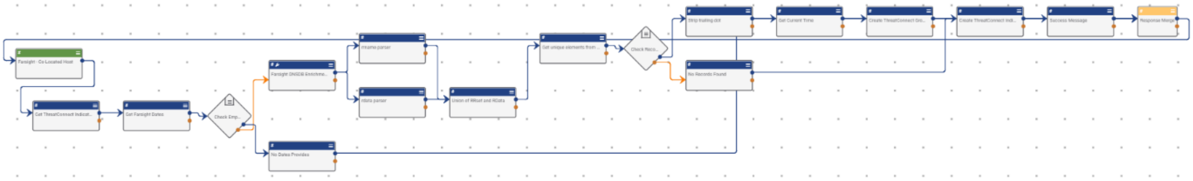
4. The 'Response Merge' App takes all success and failure failures and sends the appropriate message to User Action Trigger, It will Show the either Success message or Error message on the Host/Address details page.



5. Then the merged messages are passed to the trigger as below.

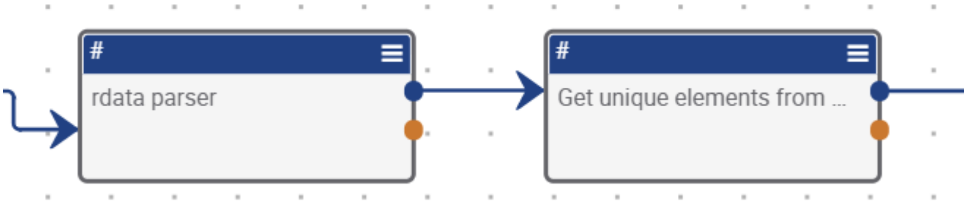


6. Final Playbook will look like as below:

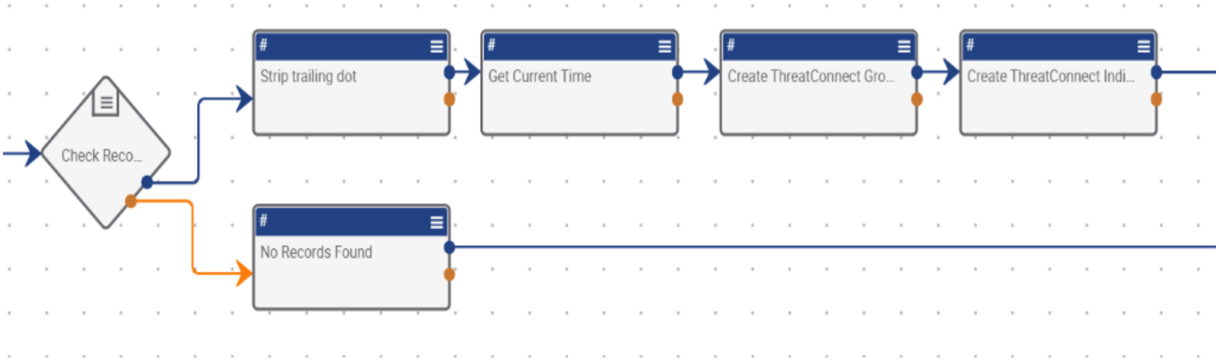


4.2. Farsight Historical Address Playbook Template

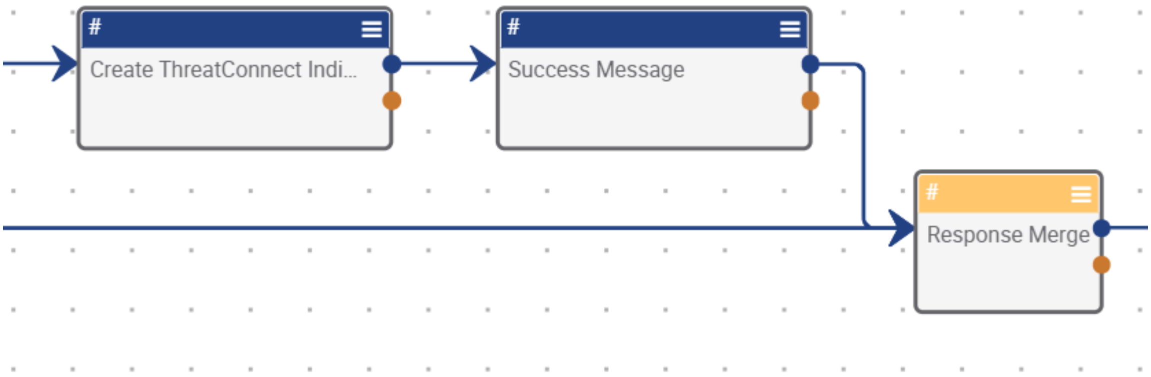
1. Extracted rdata values from the Farsight DNSDB Enrichment App using JMESPath app and passed the results to the Array Operations app to get only the unique elements.



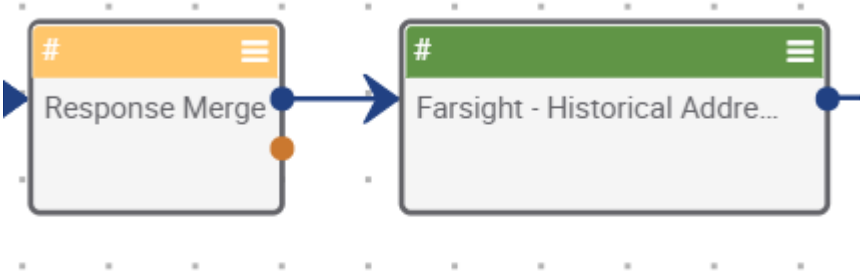
2. The below flow checks whether the results are returned, if yes create the Indicators and Report Group or else log as no results found.



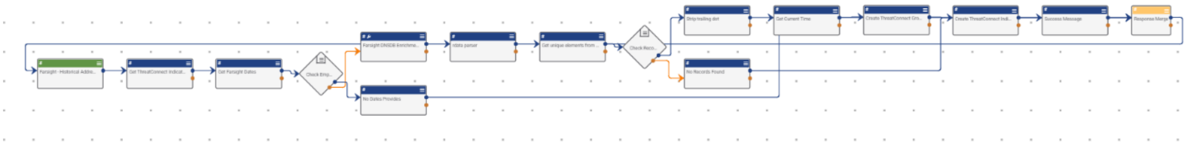
3. After Creating the indicators successfully, the success message is created and merged with all the response messages.



4. Then the merged messages are passed to the trigger.

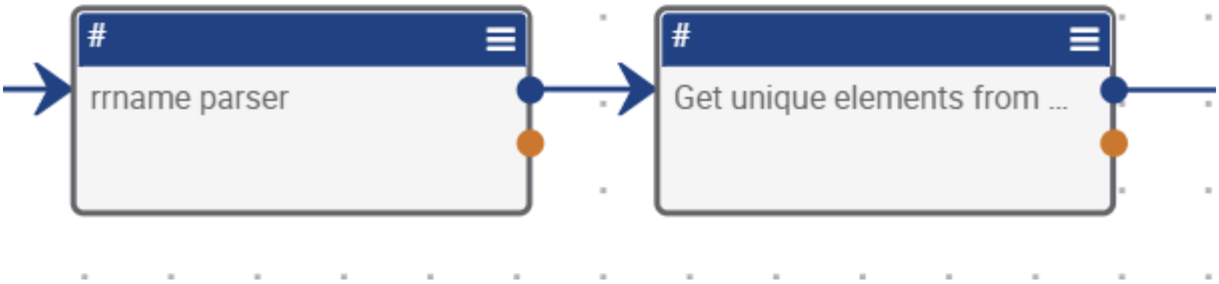


5. In the end the playbook looks as following image.

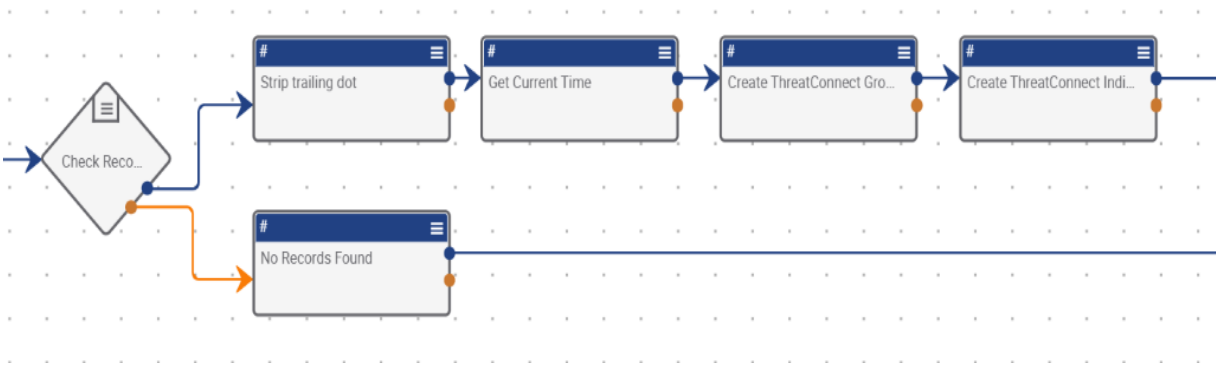

Farsight - Historical Addre...
Get ThreatConnect Indicat...
Get Farsight Dates
Check Emp...
Farsight DNSDB Enrichme...
rdata parser
Get unique elements from ...
No Dates Provides
Check Reco...
Strip trailing dot
Get Current Time
Create ThreatConnect Gro...
Create ThreatConnect Indi...
Success Message
Response Merge
No Records Found

4.3. Farsight Historical Host Playbook Template

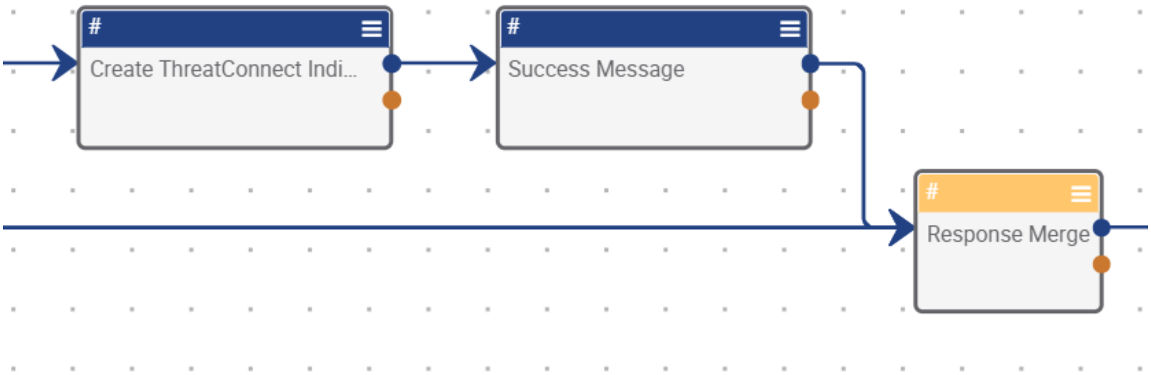
1. Extracted rrname values from the Farsight DNSDB Enrichment App using JMESPath app and passed the results to the Array Operations app to get only the unique elements.



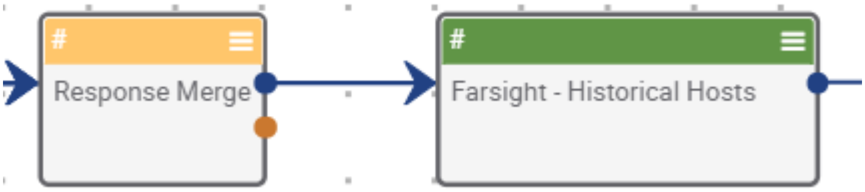
2. The below flow checks whether the results are returned, if yes create the Indicators and Report Group or else log as no results found.



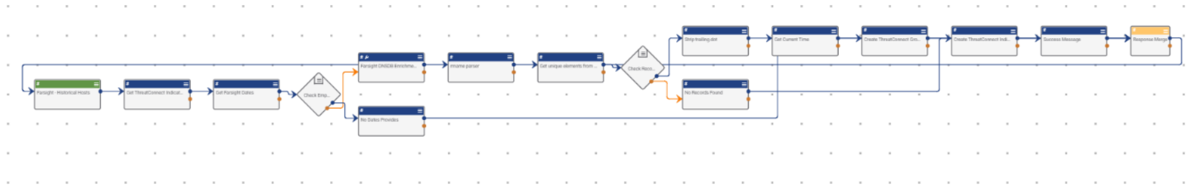
3. After Creating the indicators successfully, the success message is created and merged with all the response messages.



4. Then the merged messages are passed to the trigger.



5. In the end the playbook looks as following image.


Farsight - Historical Hosts
Get ThreatConnect Indicat...
Get Farsight Dates
Check Emp...
Farsight DNSDB Enrichme...
No Dates Provides
rrname parser
Get unique elements from ...
Check Reco...
Strip trailing dot
No Records Found
Get Current Time
Create ThreatConnect Gro...
Create ThreatConnect Indi...
Success Message
Response Merge