

## Exercise 2: Configuring Playbooks

In this exercise, you will configure playbooks on FortiAnalyzer to generate incidents from the events that the data handlers created. You will also configure playbooks to add event data to those incidents.


### Configure Playbooks


You will configure and import playbooks that will trigger when the custom event handlers that you created in the previous exercise create events. These playbooks will generate incidents and you will configure these playbooks to add the data from the events to these incidents.


To configure the SMTP enumeration playbook


1. On the bastion host, in Chrome, log in to the FAZ-SiteB (10.200.4.238) GUI with the following credentials:
  - Username: admin
  - Password: Fortinet1!
2. Click **Fabric View > Automation > Playbook**.
3. Click **Create New**.
4. In the **Choose from Playbook Templates** step, select **New Playbook created from scratch**.


Choose from Playbook Templates


 **New Playbook created from scratch**  
Custom build playbook to get started


 **Attach Endpoint Vulnerability list to incident**  
Playbook to collect the list of endpoint vulnerabilities from logs and attach to incident.

 **Compromised Host Incident**  
Playbook to create incident on FortiAnalyzer for detected compromised hosts by IoC feature.

 **Critical Intrusion Incident**  
Playbook to create incident on FortiAnalyzer for detected critical intrusions by IPS

 **Enrich Incident with Process List**  
Playbook to get running processes on endpoint by EMS connector and attach to incident.


 **Enrich Incident with Software Inventory**  
Playbook to get software inventory from endpoint by EMS Connector and attach to incident.


 **Enrich Incident with Vulnerability List**  
Playbook to collect the list of endpoint vulnerabilities from logs and attach to incident.


5. In the **Add a Trigger to start the playbook** step, select **EVENT\_TRIGGER**.


! Add a Trigger to start the playbook

TRIGGERS

 EVENT\_TRIGGER

 INCIDENT\_TRIGGER

 ON\_SCHEDULE

 ON\_DEMAND

6. In the **EVENT\_TRIGGER** step, select **All of the following conditions**.
7. Click **Add Condition**.
8. Configure the following conditions:
  - **Basic Handler Name | Equal To | SOC SMTP Enumeration Data Handler**

EVENT\_TRIGGER

All of the following conditions

Basic Handler Name

Equal To

SOC SMTP Enumeration Data  
Handler

Add Condition Group

Add Condition

9. Click **Save**.
10. In the **Name** field, type SOC SMTP Enumeration Playbook.
11. In the **Description** field, type Playbook to generate incident and add event data for SMTP Enumeration events.

Edit Playbook

Name

SOC SMTP Enumeration Playbook

Description

Playbook to generate incident and add event data for SMTP Enumeration events

Enabled

EVENT\_TRIGGER

Select a Step

Empty area

12. On the **EVENT\_TRIGGER** step, drag one of the connectors to an empty area in the playbook editor.
- The **Connectors** window opens.

13. In the **Connectors** window, click **FortiAnalyzer**.

Connectors

FortiAnalyzer

FortiOS

EMS

FortiMail

14. In the **LOCALHOST** window, configure the following settings:

Field	Value
Name	Create SMTP Enumeration Incident
Connector	Local Connector
Action	Create Incident

15. In the **Endpoint ID** field, select **Playbook Starter**, and then click the **A** icon to change to text mode.

LOCALHOST

Name

Create SMTP Enumeration Incident

Description

Connector

Local Connector

This connector is auto-selected. You must click "OK" and save playbook to apply this selection.

Action

Create Incident

Endpoint ID ⓘ

Playbook Starter

epid

A

End User ID ⓘ

Playbook Starter

type

A

Endpoint ⓘ

Playbook Starter

from

A

16. In the **Endpoint ID** field, type `${trigger.id}`.
17. Configure the remaining settings by clicking the **A** icon, and then changing to text mode, where applicable:

Field	Value
End User ID	<code>\${trigger.type}</code>
Endpoint	<code>\${trigger.from}</code>
Category	Denial of Service (DoS)
Severity	High
Status	New
Description	<code>\${trigger.msg}</code>
MITRE Information	From Fixed Selection T1589 Gather Victim Identity Information
MITRE Tech ID	T1589.002 Email Addresses

LOCALHOST

Name

Create SMTP Enumeration Incident

Description

Connector

Local Connector

This connector is auto-selected. You must click "OK" and save playbook to apply this selection.

Action

Create Incident

Endpoint ID ⓘ

`${trigger.id}`

End User ID ⓘ

`${trigger.type}`

Endpoint ⓘ

`${trigger.from}`

Category

Denial of Service (DoS)

Severity

High

Status

New

Description

`${trigger.msg}`

MITRE Information ⓘ

From Fixed Selection

Q

T1589 Gather Victim Identity Information

T1589.002 Email Addresses

2 entries selected

18. Click **OK**.
19. On the **EVENT\_TRIGGER** step, drag another one of the connectors to an empty area in the playbook editor.

20. On the **Connectors** page, click **FortiAnalyzer**.
21. On the **LOCALHOST** page, configure the following settings:

Field	Value
Name	Get_Events
Connector	Local Connector
Action	Get Events
Time Range	Last N Minutes   1
Filter	Match All Conditions

22. Click + to add a condition.
23. In the **Field** column, select **Basic Handler Name**.
24. In the **Match Criteria** column, select ==.
25. In the **Value** column, type SOC SMTP Enumeration Data Handler.

LOCALHOST ✕

Name

Get\_Events

Description

Connector

Local Connector

This connector is auto-selected. You must click "OK" and save playbook to apply this selection.

Action

Get Events

Time Range

Last N Minutes

1

Filter

Match All Conditions

Match Any Condition

Field	Match Criteria	Value	Action
Basic Handler Name	==	SOC SMTP Enumeration Data Handler	<span>✕</span> <span>+</span>

26. Click **OK**.
27. On the **Create\_SMTP\_Enumeration\_Incident** step, drag one of the connectors to an empty area in the playbook editor.
28. On the **Connectors** page, select **FortiAnalyzer**.
29. On the **LOCALHOST** page, configure the following settings:

Field	Value
Name	Attach_Data_To_Incident
Connector	Local Connector
Action	Attach Data to Incident
Incident ID	Create_SMTP_Enumeration_Incident   incident_id
Attachment	Do not modify the values in this field.

LOCALHOST ✕

Name

Attach\_Data\_To\_Incident

Description

Connector

Local Connector

This connector is auto-selected. You must click "OK" and save playbook to apply this selection.

Action

Attach Data to Incident

Incident ID ?

Create\_SMTP\_Enumeration\_Incident  
(placeholder\_a457faa9\_e9ed\_4758\_bbc0\_

incident\_id

A

Attachment ?

Click to select

Click to select

A

30. Click **OK**.
31. On the **Get\_Events** step, drag one of the connectors to the **Attach\_Data\_To\_Incident** step.
32. Edit the **Attach\_Data\_To\_Incident** step.
33. In the **Attachment** field, in the first drop-down list, select **Get\_Events**, and then in the second drop-down list, select **events**.

Attach\_Data\_To\_Incident

Name

Attach\_Data\_To\_Incident

Description

Connector

Local Connector

Action

Attach Data to Incident

Incident ID

Create\_SMTp\_Enumeration\_Incident  
(placeholder\_a457faa9\_e9ed\_4758\_bbc0\_

incident\_id

A

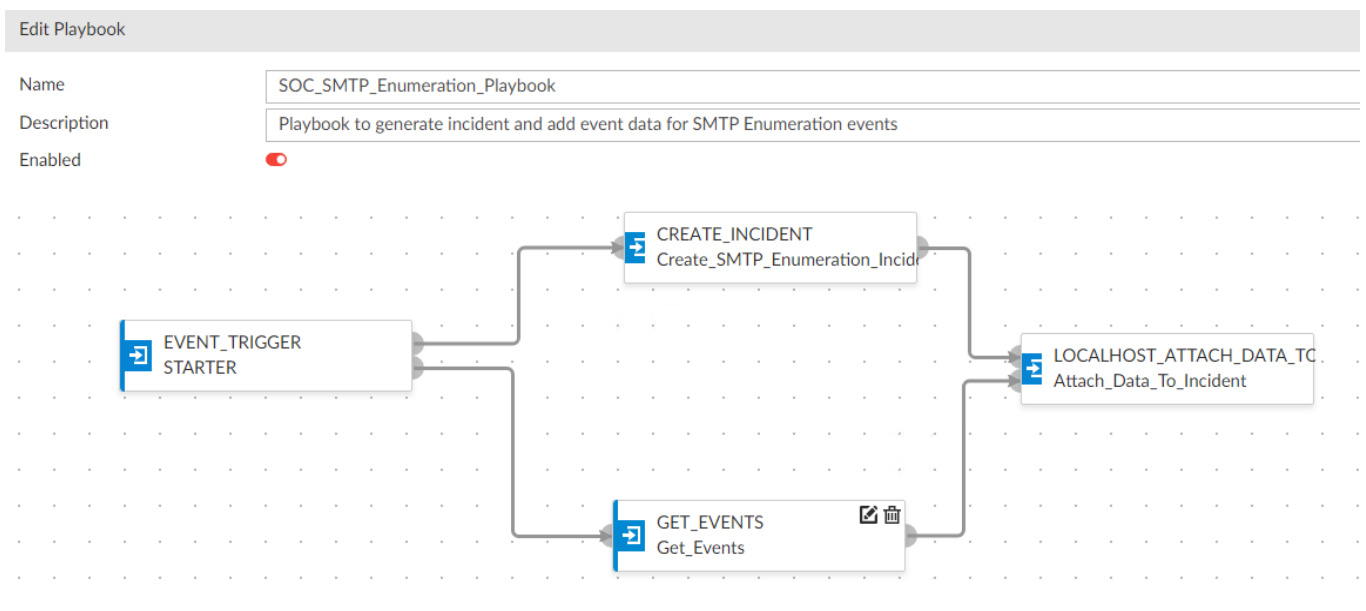
Attachment

Get\_Events  
(placeholder\_c886d808\_2207\_4b91\_b06e

events

A

34. Click **OK**.
35. Confirm that the playbook connectors follow the flow in the following image:



36. Click **Save Playbook**.

### To import a playbook for a spearphishing attack

1. Continuing on the FAZ-SiteB GUI, click **Fabric View > Automation > Playbook**.
2. Click **More > Import**.
3. Click **Add Files**.
4. Navigate to **Desktop > Resources > Modules > SOC FAZ Analyst > Playbooks**.
5. Select the **Spear\_Phishing\_Attachment\_Playbook.json** file.
6. Click **Open**.

Add files by drag & drop here or [Add Files](#)

File

Spear\_Phishing\_Attachment\_Playbook.json



File Type

txt

7. Click **OK**.

8. Select **Spear\_Phishing\_Attachment\_Playbook**.

9. Click **Edit**.

10. Edit the **EVENT\_TRIGGER** step.

11. Configure the following **EVENT\_TRIGGER** step conditions:

- **Basic Handler Name | Equal To | Spearphishing Handler**

EVENT\_TRIGGER

All of the following conditions

Basic Handler Name

Equal To

Spearphishing Handler



Add Condition Group

Add Condition

12. Click **Save**.

13. Edit the **Get\_Events** step.

14. In the **Value** field, type Spearphishing Handler.

Get\_Events

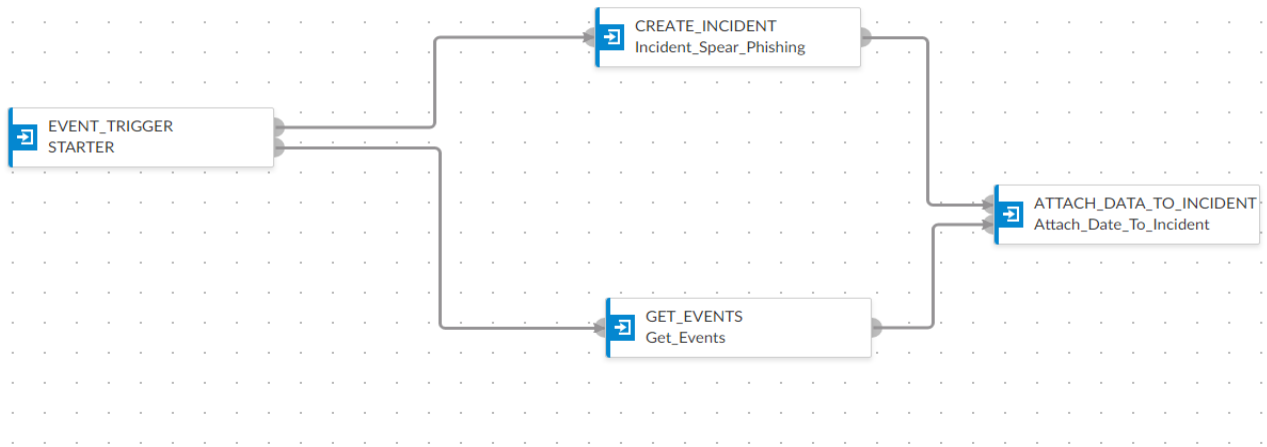


Name	Get_Events										
Description											
Connector	Local Connector										
Action	Get Events										
Time Range	Last N Minutes	1									
Filter	<div> <div>Match All Conditions</div> <div>Match Any Condition</div> </div> <table border="1"> <thead> <tr> <th>Field</th> <th>Match Criteria</th> <th>Value</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>Basic Handler Name</td> <td>==</td> <td>Spearphishing Handler</td> <td> <div>×</div> <div>+</div> </td> </tr> </tbody> </table>			Field	Match Criteria	Value	Action	Basic Handler Name	==	Spearphishing Handler	<div>×</div> <div>+</div>
Field	Match Criteria	Value	Action								
Basic Handler Name	==	Spearphishing Handler	<div>×</div> <div>+</div>								

15. Click **OK**.

16. Click **Save Playbook**.

Name	Spear_Phishing_Attachment_Playbook
Description	Custom build playbook to get started
Enabled	<input checked="" type="checkbox"/>



Save Playbook	Cancel
---------------	--------

## LAB-4 > Configuring Playbooks