FORTINET Training Institute

FORTINET CERTIFIED SOLUTION SPECIALIST
Security Operations

Security Operations Analyst

SOC Automation

FortiAnalyzer 7.4

Last Modified: 21 January 2025

Lesson Overview

- Playbook Concepts
- Creating Playbooks
- Managing Playbooks
- Automation Stitches

Playbook Concepts

Objectives

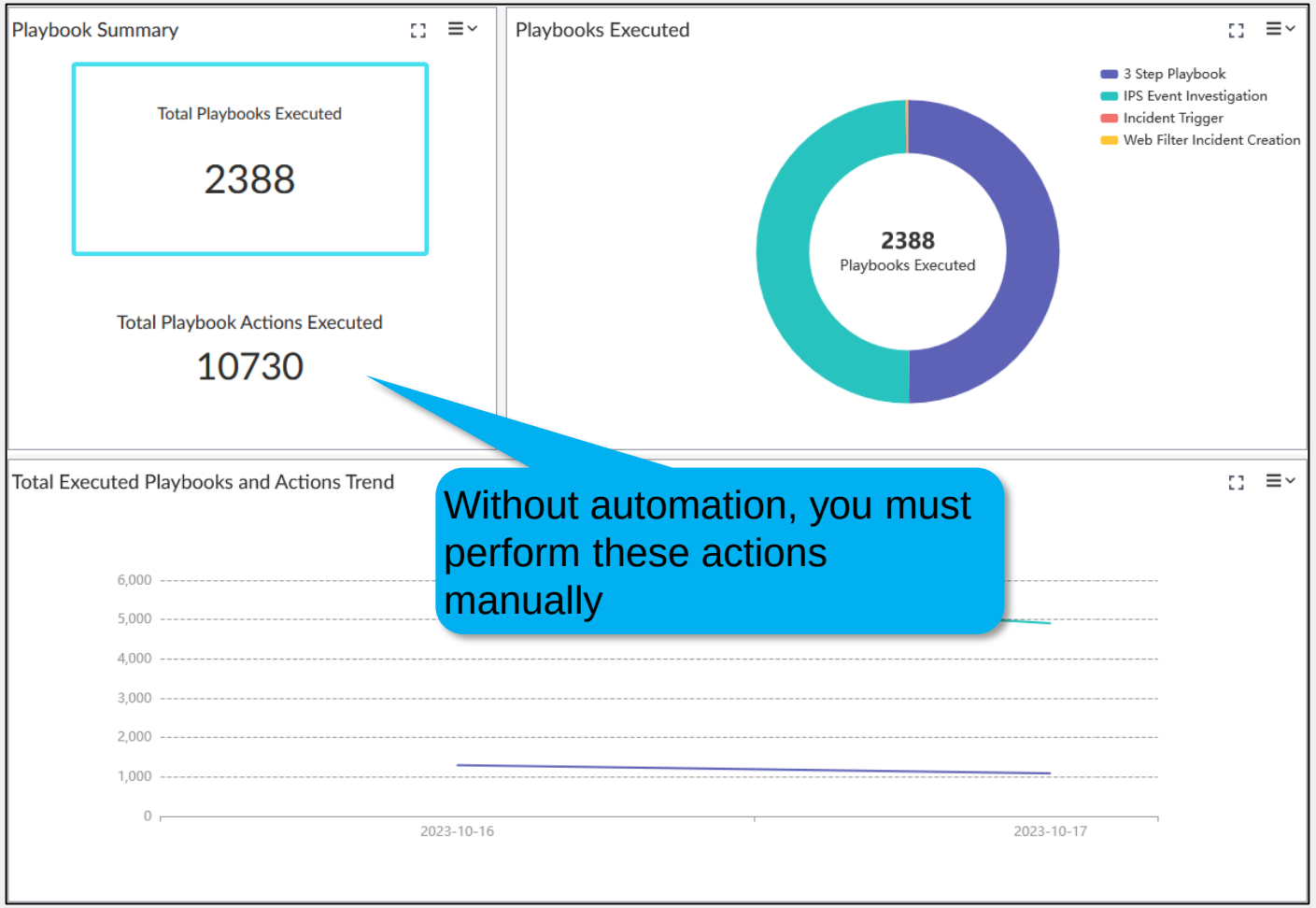
- Describe FortiAnalyzer automation capabilities
- Identify playbook components
- Describe trigger types and properties
- Describe playbook tasks

Why Automation?

- In general, the benefits of using automation include:
  - Improved productivity
  - Increased efficiency
  - Reduced costs
  - Fewer human errors

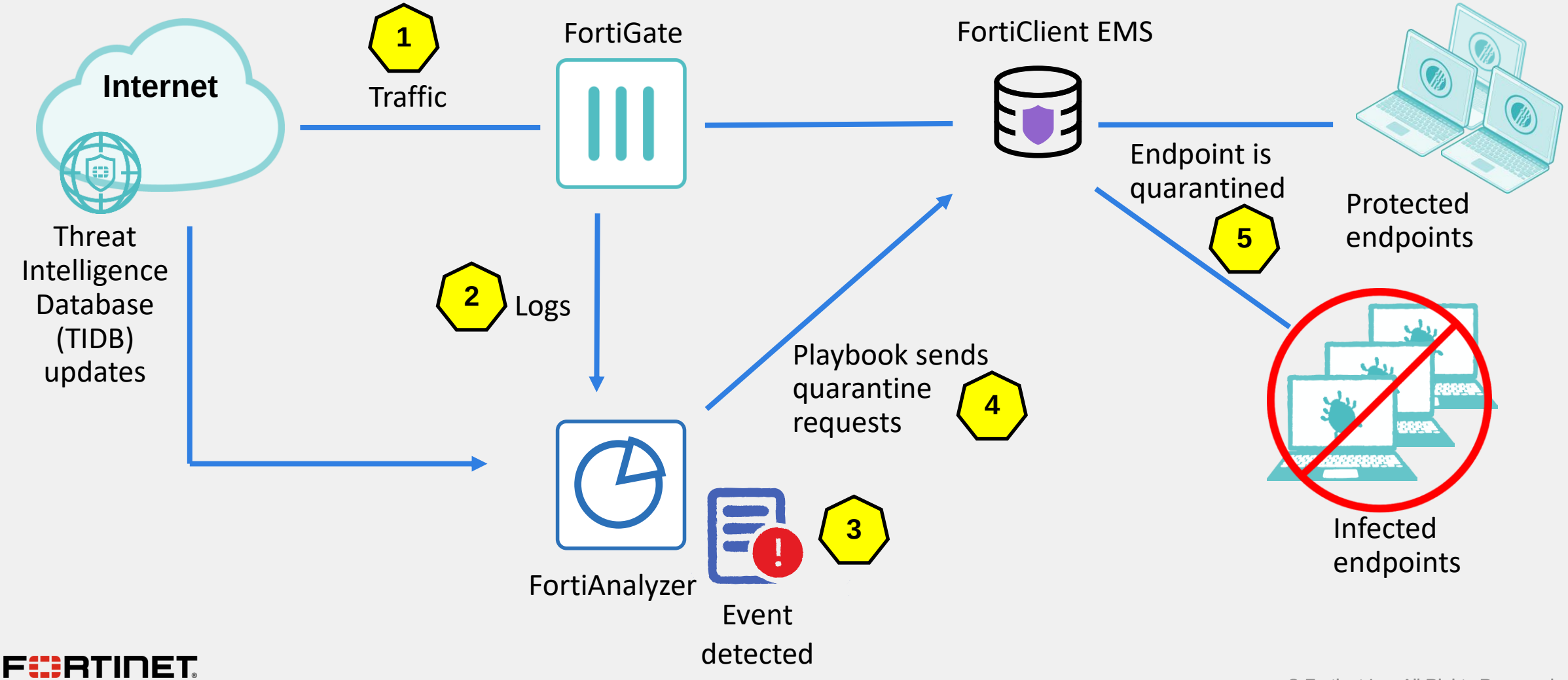
- In a SOC environment, the benefits of using playbooks results in:
  - Faster incident response time
  - Faster data analysis
  - Better use of analysts' time
  - Better compliance management
  - Consistent security posture

Fabric View > Automation > Summary



Without automation, you must perform these actions manually

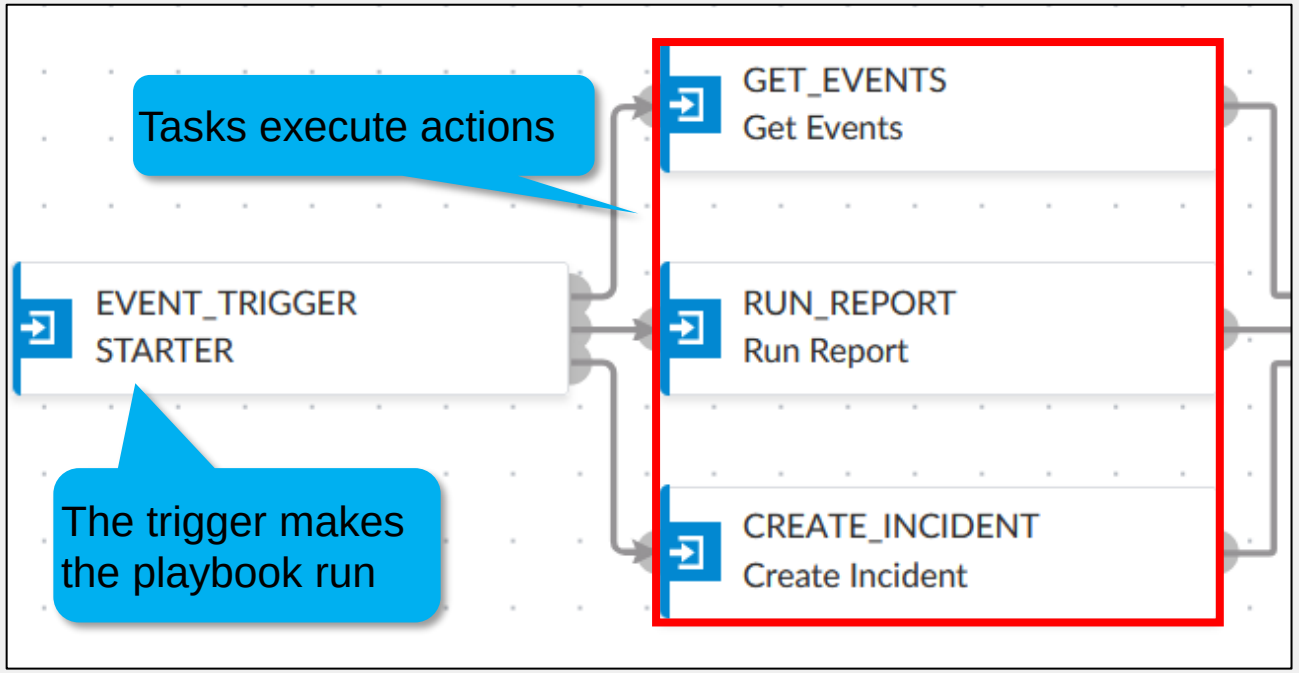
Automation With a Playbook



Playbook Components

- Playbooks are ADOM-specific
- Each playbook has only one trigger
  - Determines when a playbook executes
- Playbooks have one or more tasks
  - Actions that will take place
- The actions that can be performed by a task depends on the connector
  - Different devices (connectors) allow different actions
- Playbooks can be created from built-in templates or from scratch

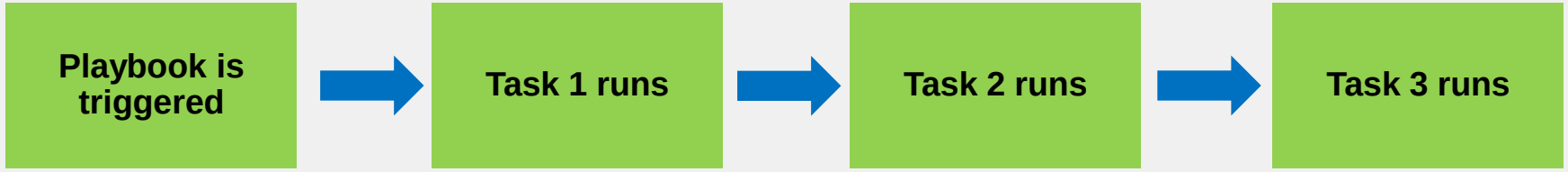
Playbook Designer



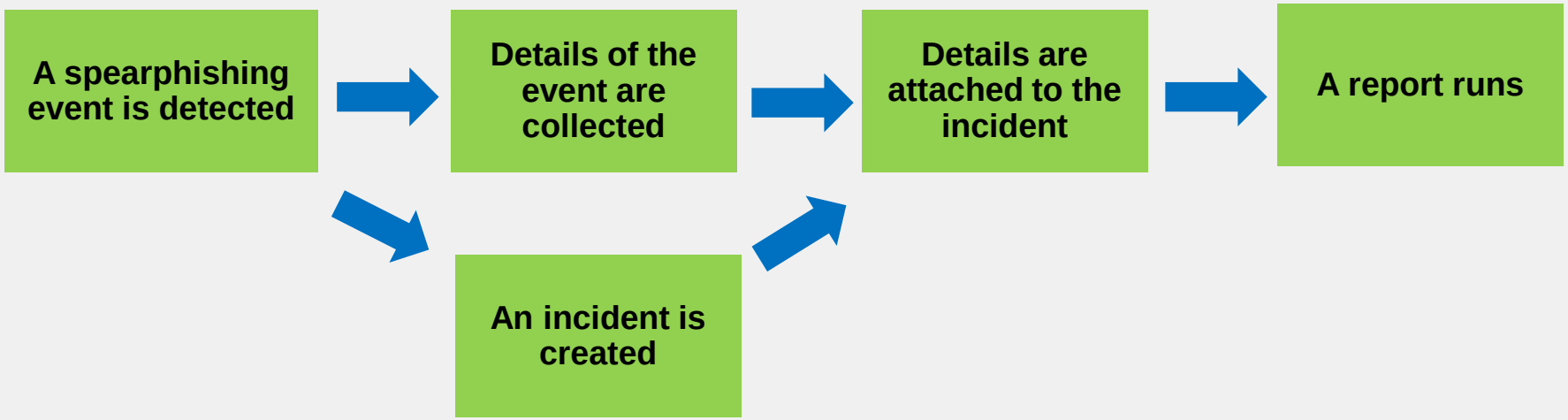
- Playbooks are created using an intuitive playbook designer
- Flow diagrams help you visualize the workflow

Playbook Concepts

- A simple playbook execution sequence
  - Tasks run one after another



- Multiple tasks can be triggered
- Tasks can be sequential, or run in parallel



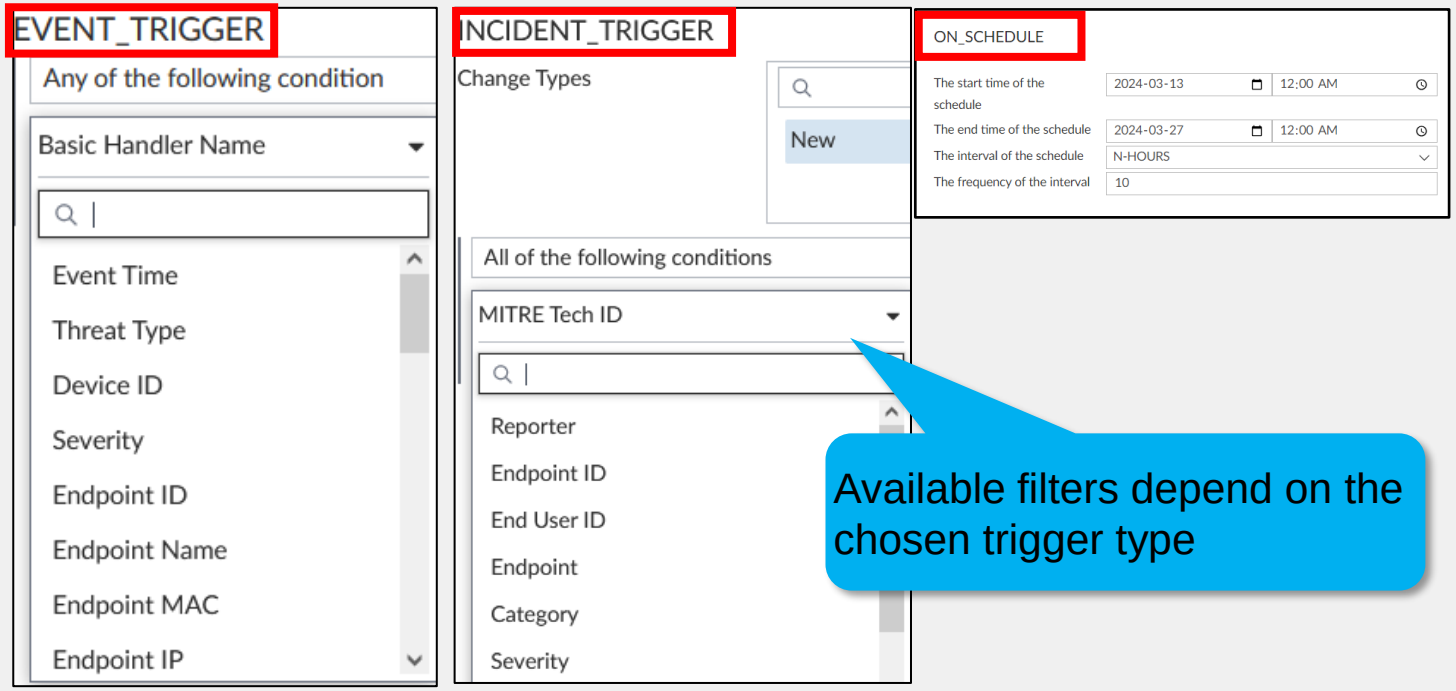
Triggers

Trigger type	Description
EVENT_TRIGGER	The playbook is run when an event is created that matches the configured filters When no filters are set, all events will trigger the playbook
INCIDENT_TRIGGER	The playbook is run when an incident is created that matches the configured filters When no filters are set, all incidents will trigger the playbook
ON_SCHEDULE	The playbook is run during the configured schedule You can define the start time, end time, interval type, and interval frequency for the schedule
ON_DEMAND	The playbook is run when it is manually started by an administrator

Triggers (Contd)

- Use more than one condition to limit playbook execution
- Apply logic to determine when and how conditions trigger events
  - Apply AND logic to enforce the rule that *all* conditions must match
  - Apply OR logic to enforce the rule that *any* conditions must match
- ON_SCHEDULE triggers parameters are all based on timeframes
- ON_DEMAND triggers have no extra configurable parameters

Fabric View > Automation > Summary



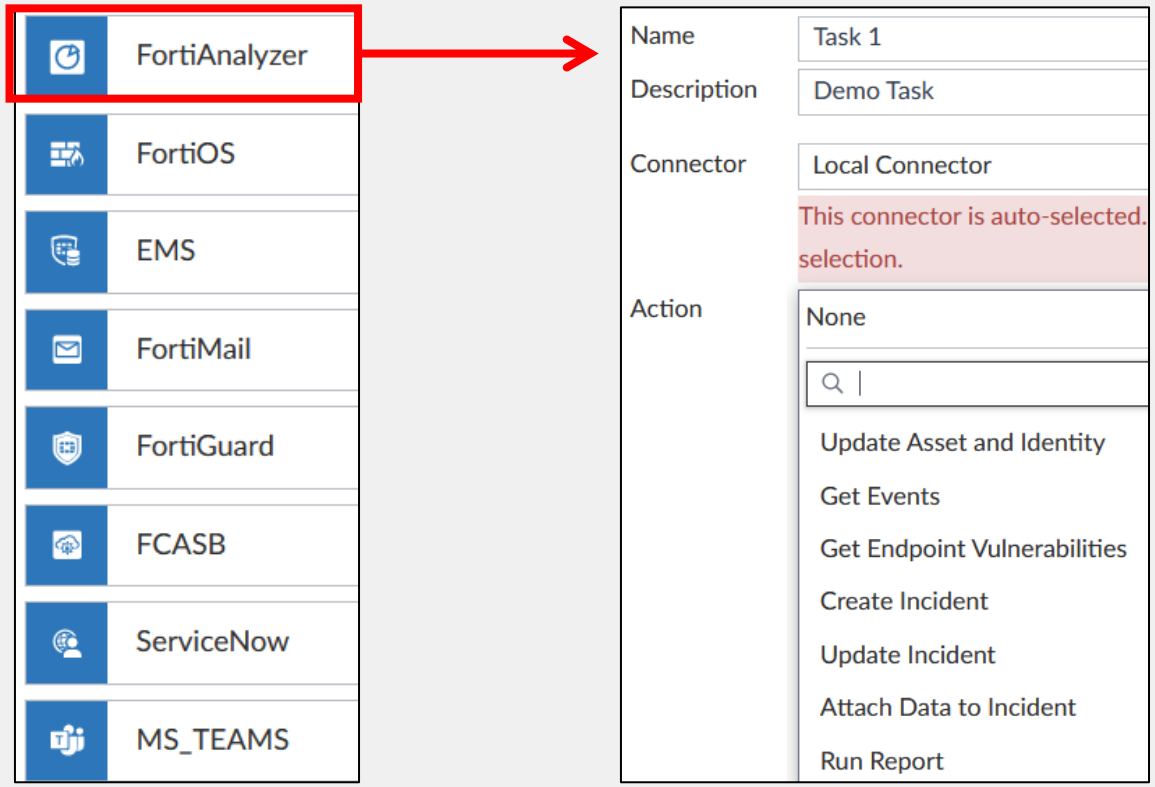
Available filters depend on the chosen trigger type

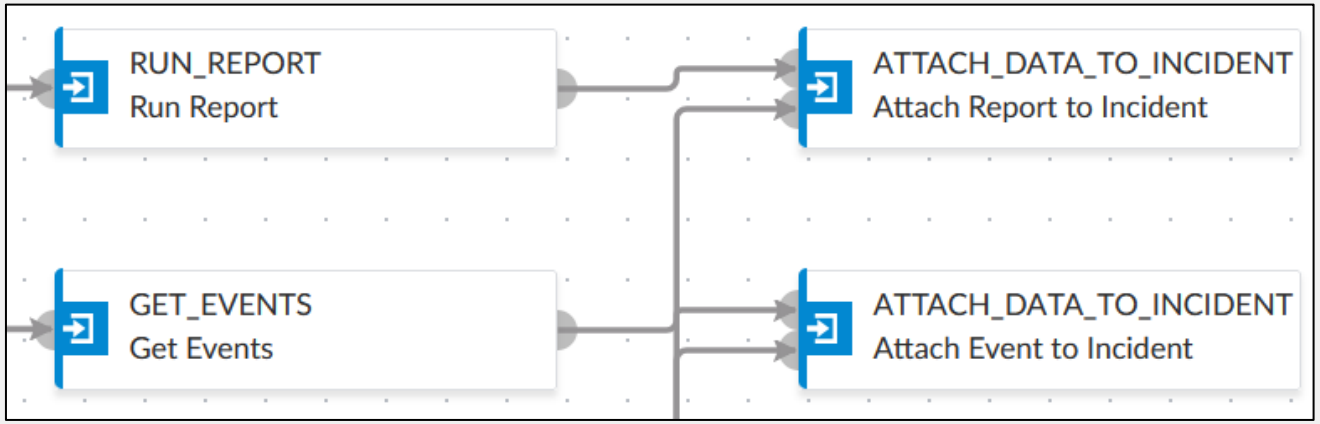
Example

Tasks

- Tasks are actions that are executed when the playbook runs
- Available actions depend on the connector
- Chain one task to another task to execute a sequence of actions
- The output of a task can be used as an input for the next task in the sequence

Fabric View > Automation > Playbook





Knowledge Check

1. Which trigger type must you use to manually run a playbook?
   A. Event_Trigger
   ✔ B. On_Demand

2. Which playbook element determines the available actions a task can perform?
   ✔ A. Connectors
   B. Trigger type

Lesson Progress

- ✓ Playbook Concepts
- Creating Playbooks
- Managing Playbooks
- Automation Stitches

Creating Playbooks

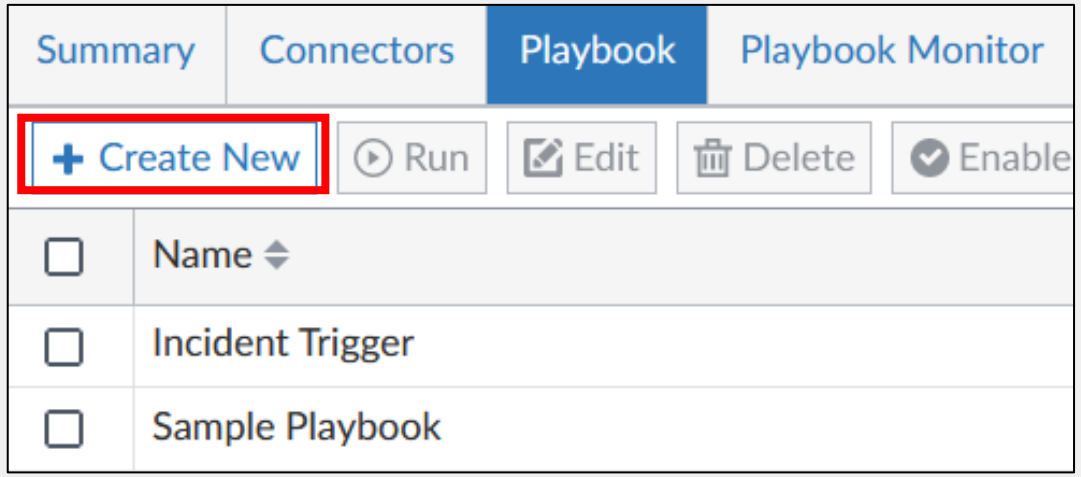
Objectives

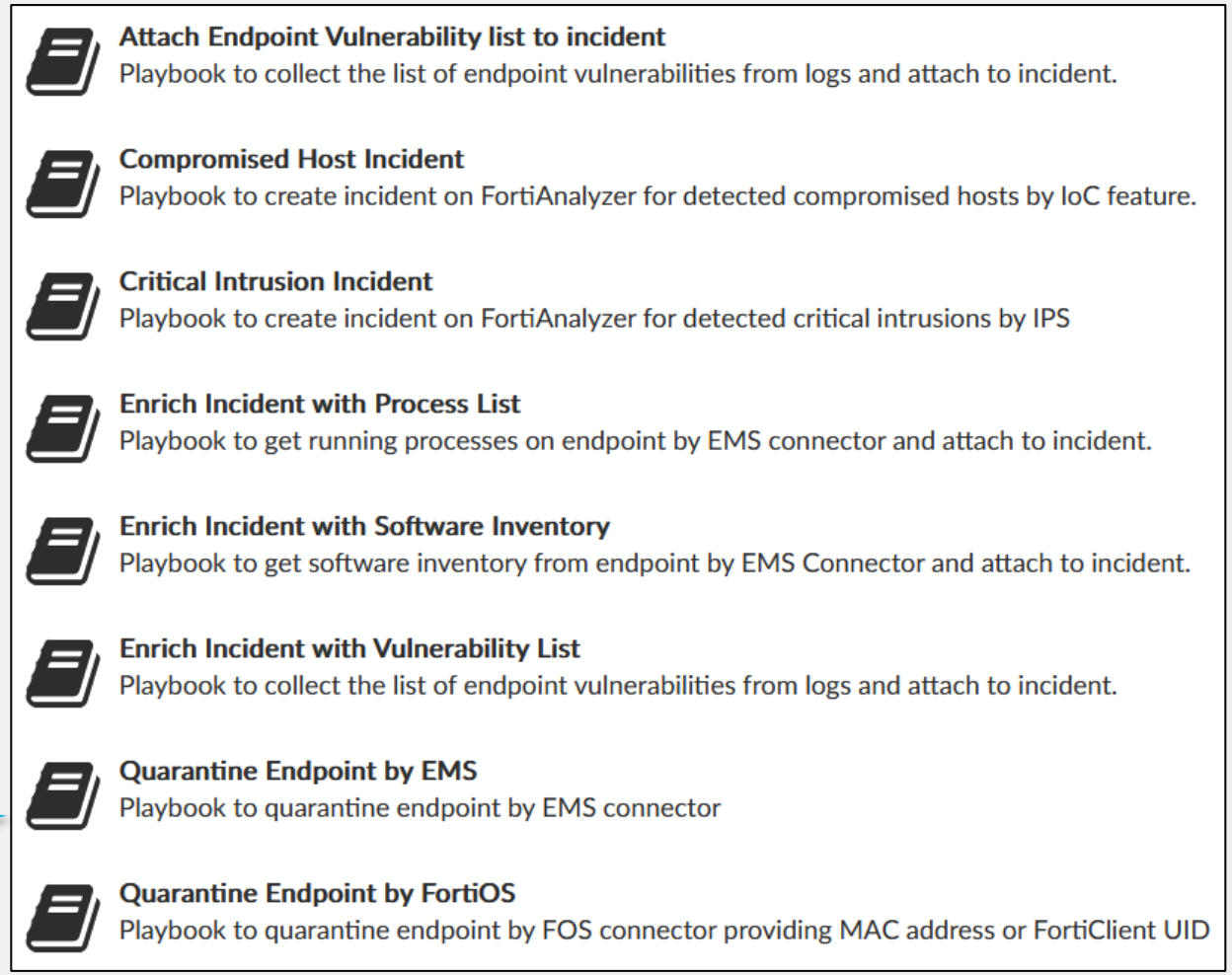
- Create new playbooks from a template
- Customize playbook settings
- Create new playbooks from scratch
- Use variables in tasks

Creating Playbooks From a Template

- FortiAnalyzer includes several playbook templates
- You can customize the playbooks created from these templates to fit your needs

Fabric View > Automation > Playbook

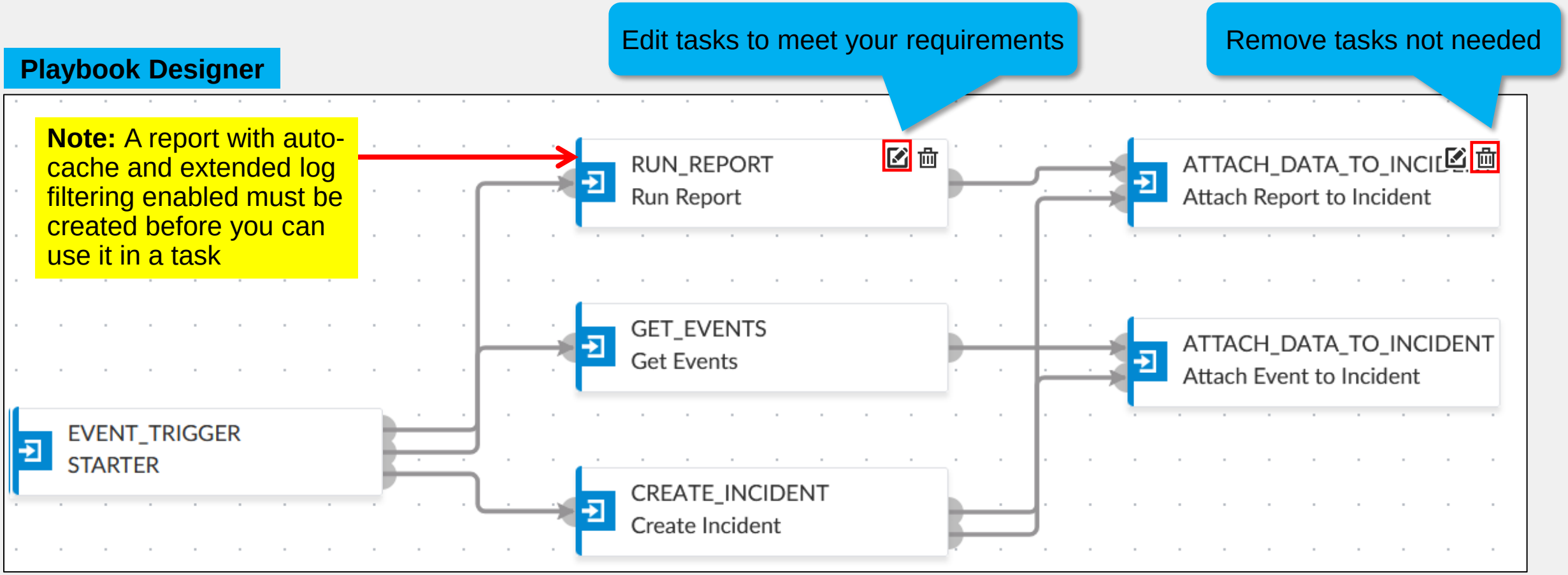




Explore the available templates before creating a playbook from scratch since they cover many common scenarios (not all templates are shown)

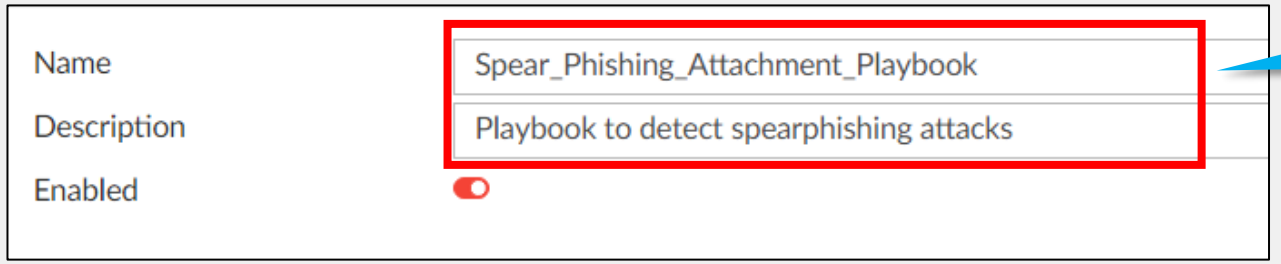
Customizing Playbook Settings

- A new playbook created from a template is preloaded with all required components
- You can remove or customize tasks to meet your needs

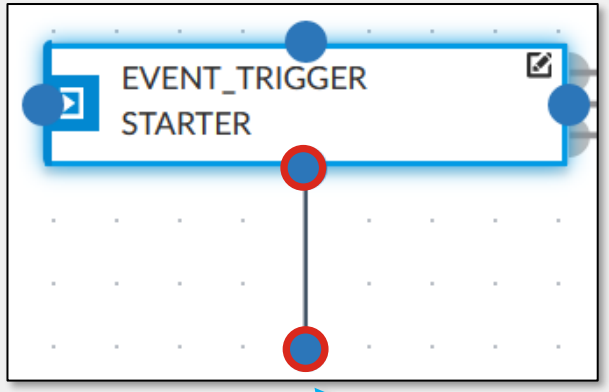


Customizing Playbook Settings (Contd)

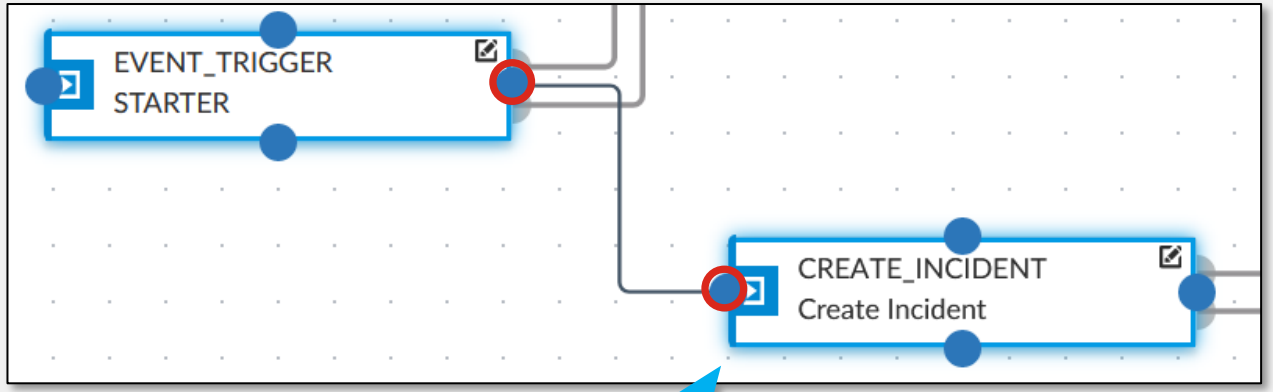
Fabric View > Automation > Playbook



Customize the playbook name and description



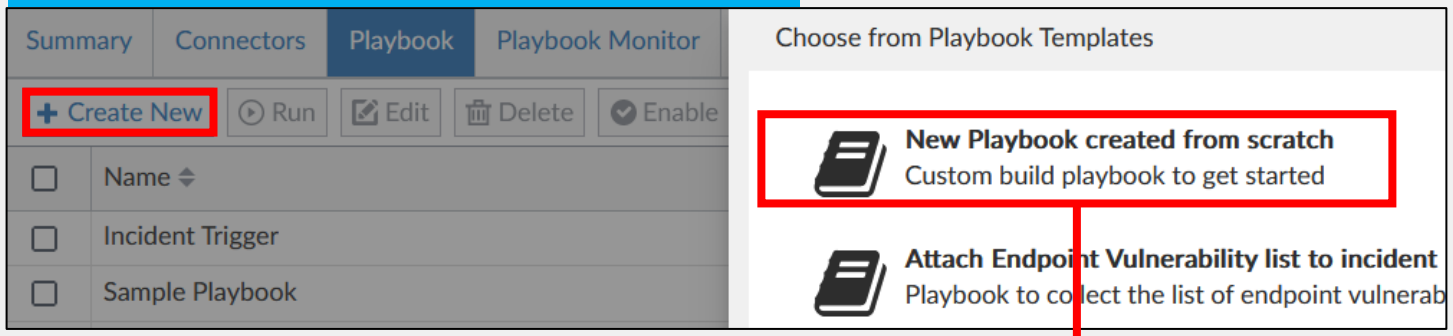
Click and drag a connector tab to an empty space to add new tasks

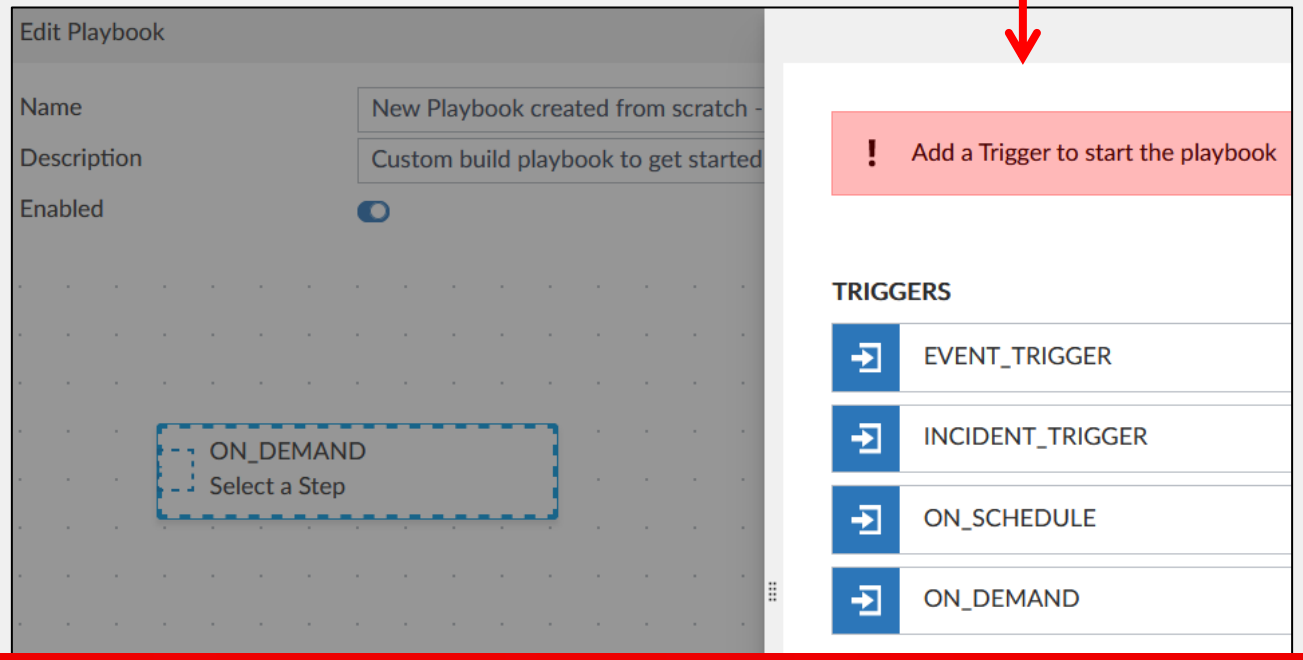


Click and drag a connector tab to another task to connect them

Creating a New Playbook From Scratch

Fabric View > Automation > Playbook





FortiAnalyzer needs a few minutes to parse a newly created playbook

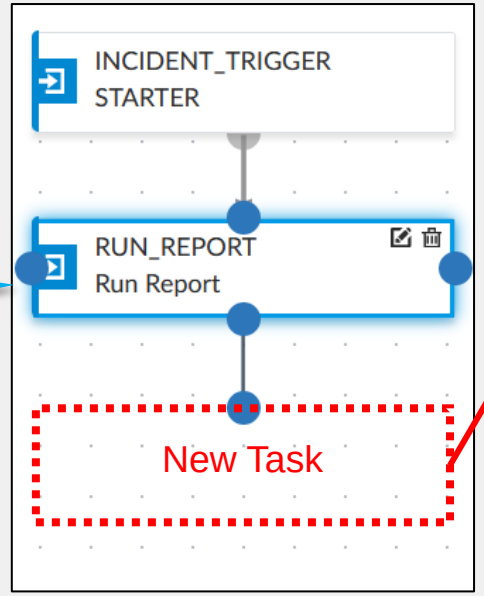
Server error: FAZ is parsing the recent created playbook: 301f8fc9-7831. Please wait for about 5 minutes.

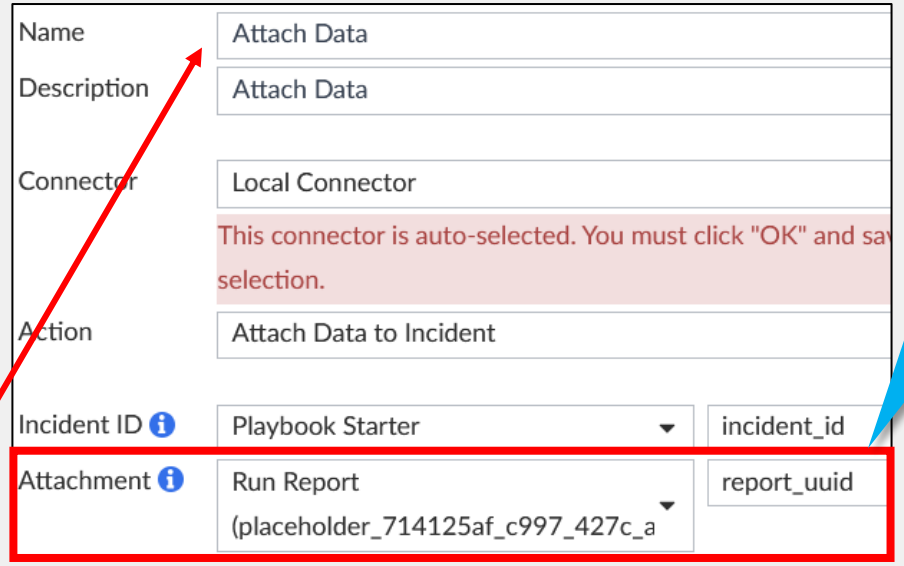
Variables

- You can use output variables and trigger variables in playbook tasks
- Output variables: Output of previous task is the input of current task
  - Format: `${task_id.output}`
  - Previous task ID *required*
- Trigger variables: Use some of the information from the trigger to filter the action in the task
  - Format: `${trigger.variable}`

Fabric View > Automation > Playbook

Second task generates a report





The new task uses an output variable. On the left is the report task ID, and on the right is the output of the report task (the actual report)

Knowledge Check

1. Which type of variable takes the output of a preceding task as the input of a current task?
   A. Trigger variable
   ✓ B. Output variable

Lesson Progress

- ✓ Playbook Concepts
- ✓ Creating Playbooks
- Managing Playbooks
- Automation Stitches

Lesson Progress

- ✓ Playbook Concepts
- ✓ Creating Playbooks
- ✓ Managing Playbooks
- Automation Stitches

Managing Playbooks

Objectives

- Monitor playbooks
- Export and import playbooks
- Review the mock threat report

Monitoring Playbooks

- To see the playbook execution logs, click **Details** and then **View Log**

This playbook has three tasks: One task is successful but the other two failed

Fabric View > Automation > Playbook Monitor

Playbook	Trigger	Start Time	End Time	Status	Details
Spear_Phishing_Attachment_Playbook	event(20240313100(	2024-03-13 06:31:00-0700	2024-03-13 06:31:06-0700	failed(Scheduled:0/Running:0/Success:1/Failed:2)	

Fabric View > Automation > Playbook Monitor

Refresh | View Raw Log | Search...

	Task ID	Task	Start Time	End Time	Status
☐	placeholder_4c03461e_adea_4970_8029_3abcb	Attach_Date_To_Incident	2024-03-13 06:31:05-0700	2024-03-13 06:31:05-0700	upstream_failed
☑	placeholder_00f4d7f1_fac5_4354_a60a_3127a6	Incident_Spear_Phishing	2024-03-13 06:31:04-0700	2024-03-13 06:31:05-0700	failed
☐	placeholder_32b07c26_d3e6_4915_9891_f4b02	Get_Events	2024-03-13 06:31:02-0700	2024-03-13 06:31:05-	success

This task failed because it did not receive the input it was expecting from a preceding task

FORTINET Training Institute

Monitoring Playbooks (Contd)

Fabric View > Automation > Playbook Monitor

Refresh | View Raw Log | Search...

Task ID	Task	Start Time	End Time	Status
placeholder_4c03461e_adea_4970_8029_3abcb	Attach_Date_To_Incident	2024-03-13 06:31:05-0700	2024-03-13 06:31:05-0700	upstream_failed
placeholder_00f4d7f1_fac5_4354_a60a_3127a6	Incident_Spear_Phishing	2024-03-13 06:31:04-0700	2024-03-13 06:31:05-0700	failed
placeholder_32b07c26_d3e6_4915_9891_f4b02	Get_Events	2024-03-13 06:31:02-0700	2024-03-13 06:31:05-0700	success

View the raw logs for failed playbooks to see more details

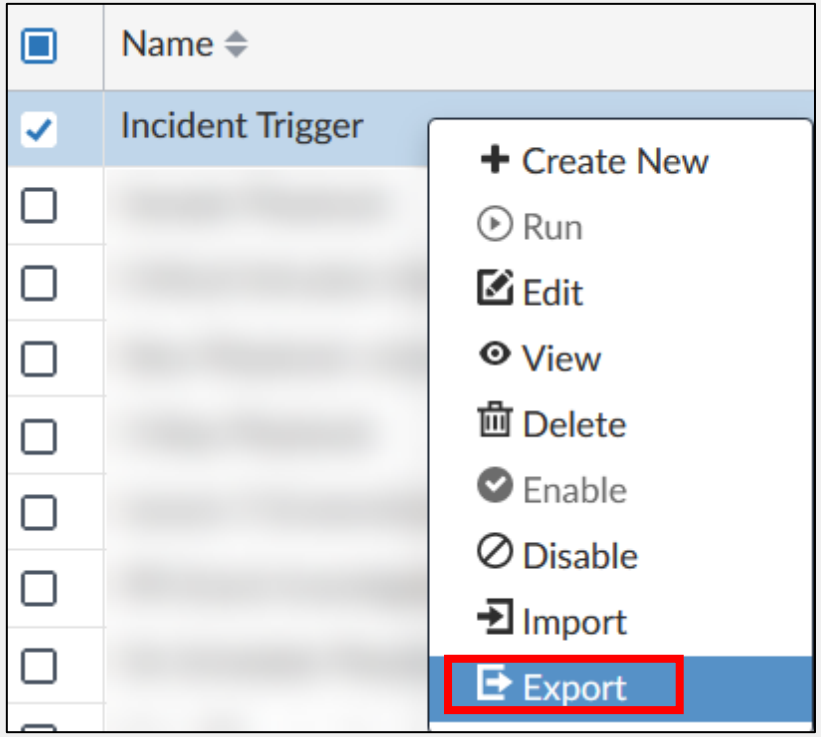
```
[2024-03-13T06:31:05.246-0700] {taskinstance.py:1937} ERROR - Task failed with
exception
Traceback (most recent call last):
  File "/drive0/private/airflow/plugins/incident_operator.py", line 218, in execute
    self.epid = int(self.epid)
                ^^^^^^^^^^^^^^
ValueError: invalid literal for int() with base 10: '100.64.1.20'
[2024-03-13T06:31:05.331-0700] {standard_task_runner.py:104} ERROR - Failed to
execute job 417 for task placeholder_00f4d7f1_fac5_4354_a60a_3127a6bc5cc7 (invalid
literal for int() with base 10: '100.64.1.20'; 1851)
```

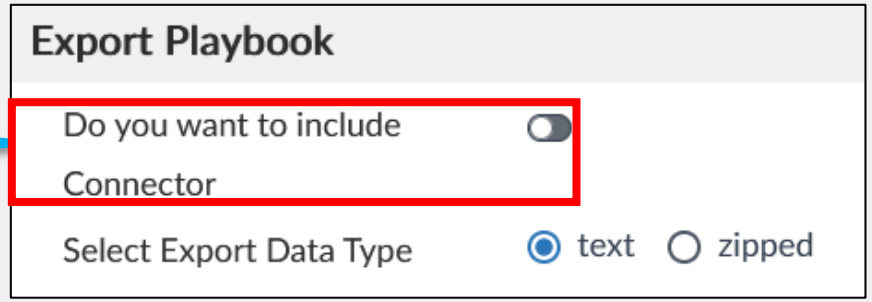
This playbook failed because a task was expecting an integer value for the `epid` variable, but received a `Base 10` value (IP address) instead

Exporting Playbooks

- Playbooks are defined per ADOM
- Export playbooks to use them in a different ADOM or FortiAnalyzer device
- You can include the connectors in the exported file
- The exported file is in JSON format
  - You can also compress the file

Fabric View > Automation > Playbook



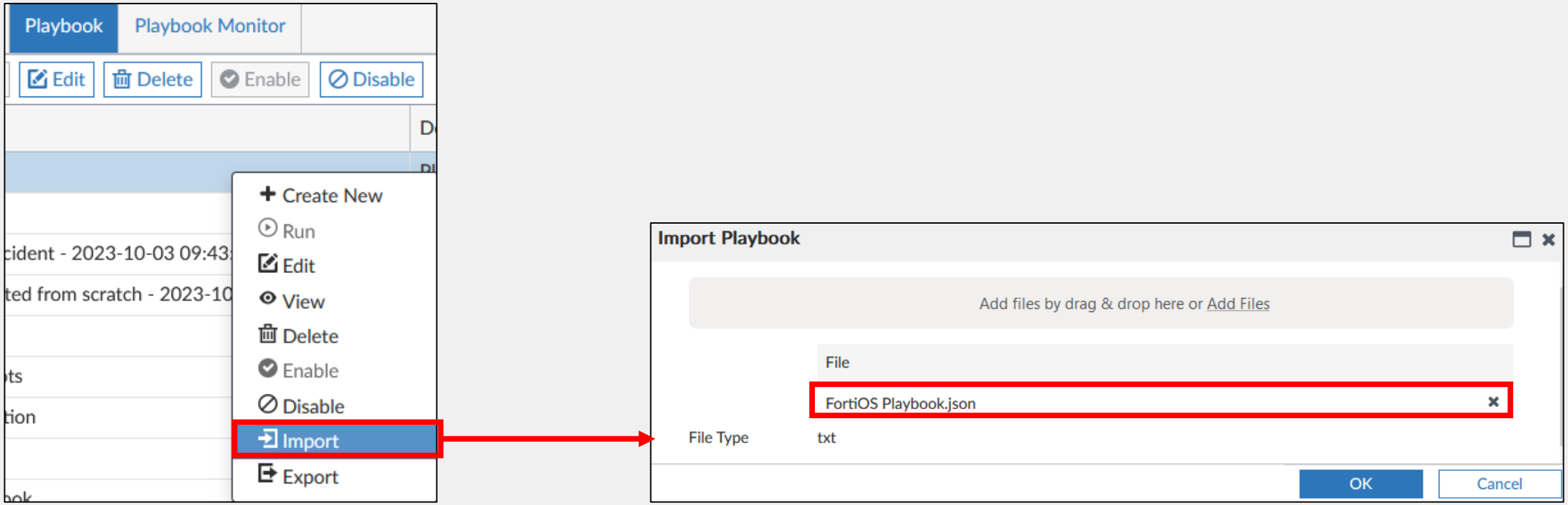


Including the connectors ensures all required components are exported

Importing Playbooks

- Import a previously exported playbook on the destination ADOM or device

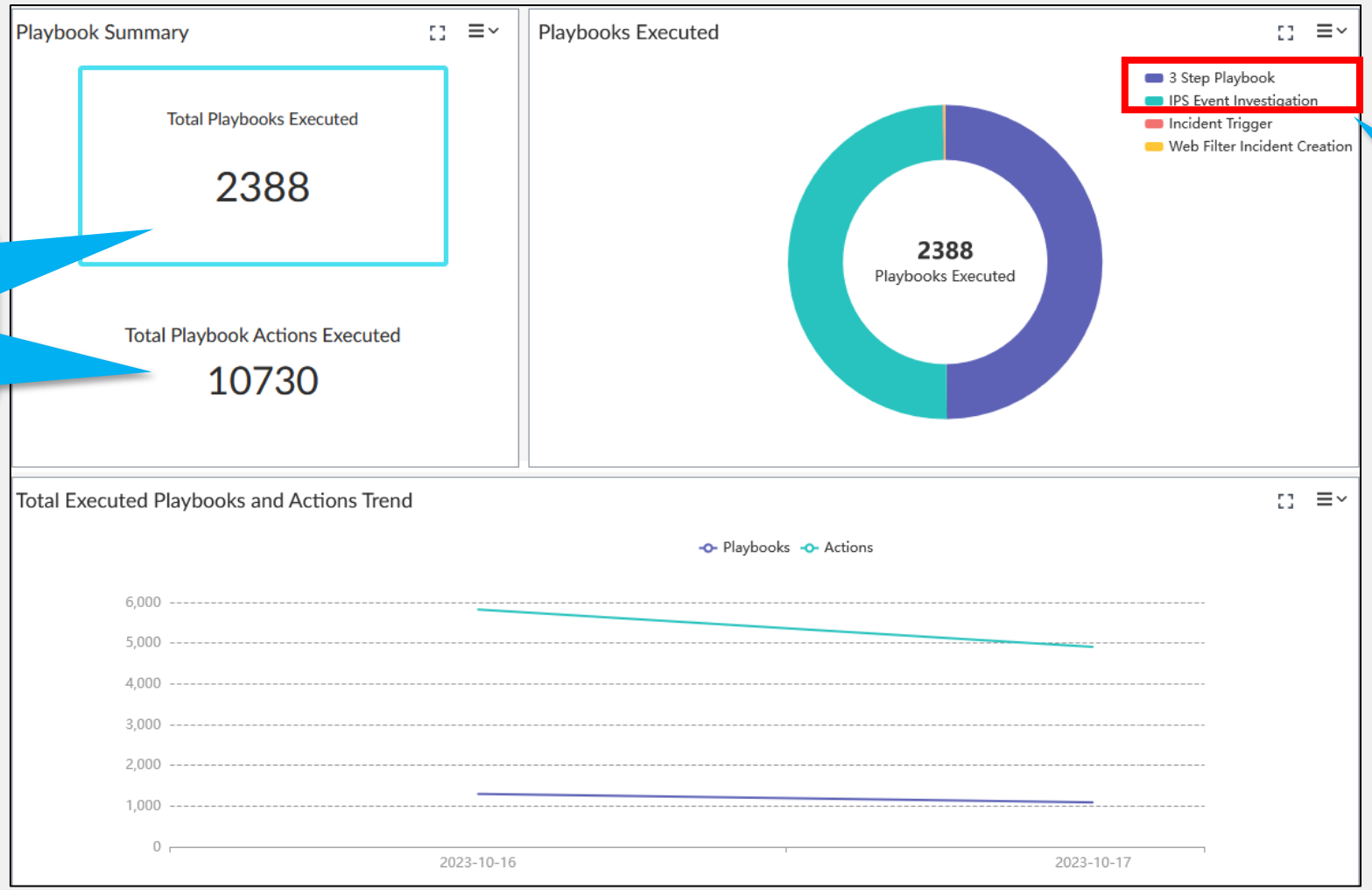
Fabric View > Automation > Playbook



Playbooks Dashboard

- This dashboard tracks all playbooks executed in the last *seven* days

Fabric View > Automation > Summary



A playbook can have multiple actions

These two playbooks have run more than all of the other playbooks, which could be normal or caused by a misconfiguration

Use Case—Healthcare Sector

Your organization is a hospital targeted by cybercriminals through a phishing attack to ransom private data

Threat: Potential breach exposing thousands of patients' data and putting patients at risk.

Our goal: *Automate actions using playbooks and connectors on FortiAnalyzer*

Domain: Enterprise

Attacker: Group ABC

Blue Team Plan of Action—Automation

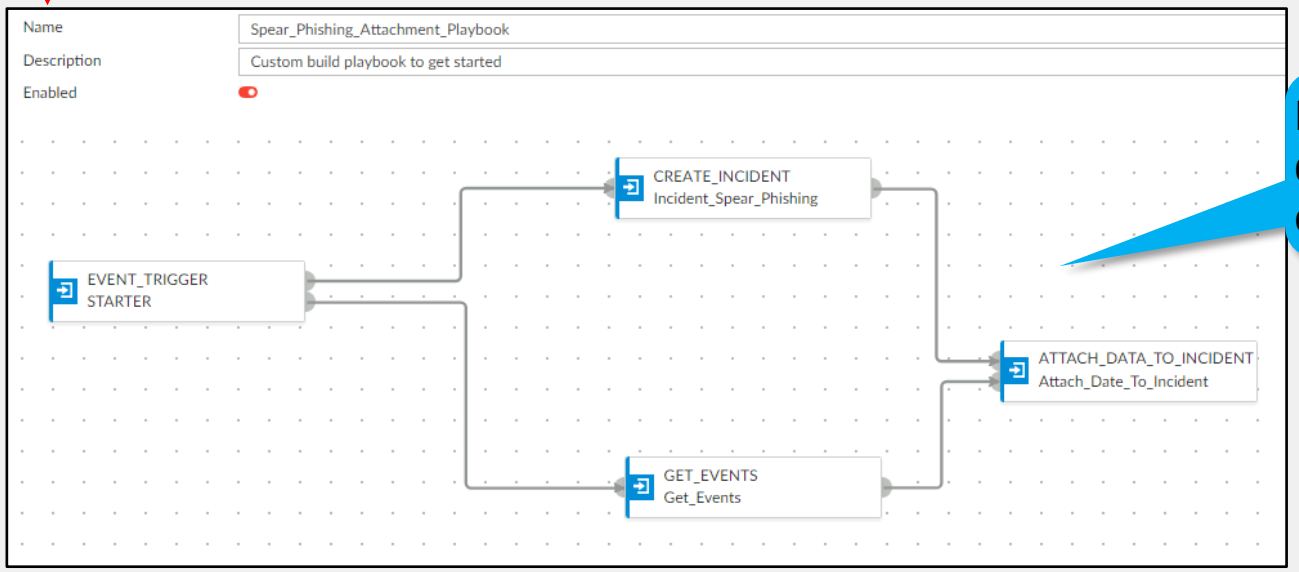
- Configure playbooks to run because of the following detection events:
  - Probing attacks that target email systems in search of valid email accounts
  - Spearphishing emails with attached malicious Microsoft Office macro-enabled files
- Configure the FortiClient EMS connector and playbooks to automate the following tasks:
  - Retrieve a list of all endpoints with FortiClient site and UUID information
  - Quarantine identified compromised host (*containment*)
  - Release sanitized host from quarantine (*recovery*)

Blue Team Plan of Action—Playbooks

Fabric View > Automation > Playbook

Name	Description	Status	Created Time
Spear_Phishing_Attachment_Playbook	Custom build playbook to get started	Enabled	02/08/2024
SOC_SMTP_Enumeration_Playbook	Playbook to generate incident and add event data for SMTP Enumeration eve...	Enabled	Yesterday at 3:00 AM
Update Asset and Identity Database (EMS Connector)	Playbook to automatically update FortiAnalyzer Asset and Identity database ...	Enabled	Last Sunday at 11:35 PM
Get Vulnerabilities from EMS (EMS Connector)	Playbook to get vulnerabilities from EMS	Enabled	Last Sunday at 11:35 PM
Get Software Inventory from EMS (EMS Connector)	Playbook to get software inventory from EMS	Enabled	Last Sunday at 11:35 PM
Quarantine Endpoint by EMS	Playbook to quarantine endpoint by EMS connector	Enabled	Yesterday at 5:21 AM
Unquarantine Endpoint by EMS	Playbook to unquarantine endpoint by EMS connector	Enabled	Yesterday at 5:40 AM

List of playbooks created by the blue team to detect attacks, and to quarantine and release hosts



Playbook configured to detect a spearphishing event

Blue Team Plan of Action—Playbooks (Cont)

Fabric View > Automation > Playbook

Refresh | Delete | Search...

Job ID	Playbook	Trigger	Start Time	End Time	Status
2024-03-11 02:35:40.462977-07	Update Asset and Identity Database (EMS Connector)		2024-03-12 02:35:40-0700	2024-03-12 02:35:47-0700	success(Scheduled:0/Running:0/Success:2/Fa
2024-03-11 02:35:40.204669-07	Get Vulnerabilities from EMS (EMS Connector)		2024-03-12 02:35:40-0700	2024-03-12 02:35:45-0700	success(Scheduled:0/Running:0/Success:1/Fa
2024-03-11 02:35:40.203954-07	Get Software Inventory from EMS (EMS Connector)		2024-03-12 02:35:40-0700	2024-03-12 02:35:45-0700	success(Scheduled:0/Running:0/Success:1/Fa
2024-03-11 07:27:35-07	Update Asset and Identity Database (EMS Connector)	user(admin)	2024-03-11 07:27:38-0700	2024-03-11 07:27:43-0700	success(Scheduled:0/Runni
2024-03-11 05:45:37-07	Unquarantine Endpoint by EMS	user(admin)	2024-03-11 05:45:40-0700	2024-03-11 05:45:45-0700	succes
2024-03-11 05:41:57-07	Unquarantine Endpoint by EMS	user(admin)	2024-03-11 05:42:00-0700	2024-03-11 05:42:0	cheduled:0/Running:0/Success:1/Failed:1
2024-03-11 05:30:00-07	Quarantine Endpoint by EMS	user(admin)	2024-03-11 05:30:03-0700	11 05:30:08-0700	success(Scheduled:0/Running:0/Success:2/Failec
2024-03-11 05:22:57-07	Update Asset and Identity Database (EMS Connector)	user(admin)	2024-03-11 05:23:00-0700	2024-03-11 05:23:06-0700	success(Scheduled:0/Running:0/Success:2/Failec
2024-03-11 04:11:23.810909-07	Spear_Phishing_Attachment_Playbook	event(202403111000	2024-03-11 04:11:24-0700	2024-03-11 04:11:27-0700	success(Scheduled:0/Running:0/Success:3/Failec
2024-03-10 01:35:40.462977-08	Update Asset and Identity Database (EMS Connector)		2024-03-11 02:35:40-0700	2024-03-11 02:35:47-0700	success(Scheduled:0/Running:0/Success:2/Failec

All the playbooks that were run when FortiAnalyzer detected different attacks from the adversary Group ABC

Playbook Tasks

Refresh | View Raw Log | Search...

Task ID	Task	Start Time	End Time	Status
placeholder_4c03461e_adea_4970_8029_3abcb	Attach_Date_To_Incident	2024-03-11 04:11:27-0700	2024-03-11 04:11:27-0700	success
placeholder_32b07c26_d3e6_4915_9891_f4b02	Get_Events	2024-03-11 04:11:25-0700	2024-03-11 04:11:26-0700	success
placeholder_00f4d7f1_fac5_4354_a60a_3127a	Incident_Spear_Phishing	2024-03-11 04:11:25-0700	2024-03-11 04:11:26-0700	success

Incident Number	Incident Date / Time	Last Update Date / Time	Incident Reporter	Incident Category	Severity	Status	Affected Endpoint
IN00000002	2024-03-11 04:11:26	2024-03-11 05:45:44	Spear_Phishing_Attachment_Playbook	Uncate			
IN00000001	2024-03-08 08:55:40	2024-03-08 08:55:40	admin				

Incident auto generated by spearphishing playbook that was configured by the blue team

Audit History

Expand All

2024-03-12 11:16:09 NOW

Comment Attached to ...
By Playbook: Unquarantine Endpoint by EMS

Comment Attached to ...
By Playbook: Quarantine Endpoint by EMS

Events Attached to Inc...
By Playbook: Spear_Phishing_Attachment_Playbook

New Incident Created
By Playbook: Spear_Phishing_Attachment_Playbook

START 2024-03-11 05:11:26

Knowledge Check

1. Which two playbook export formats are supported?
   - ✔ A. JSON, ZIP
   - B. CSV, YAML

2. When exporting playbooks, which connector configuration can you also export?
   - A. Local connector
   - ✔ B. FortiClient EMS connector

Lesson Progress

- ✓ Playbook Concepts
- ✓ Creating Playbooks
- ✓ Managing Playbooks
- Automation Stitches

Automation Stitches

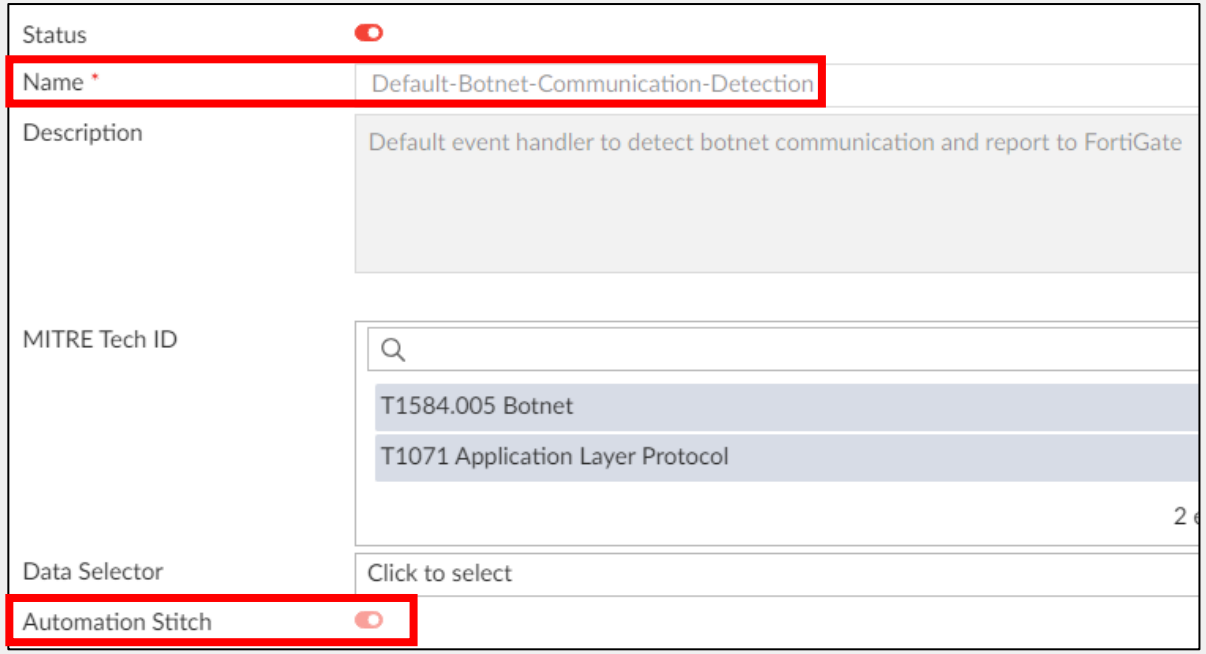
Objectives

- Describe FortiAnalyzer and FortiGate automation stitches
- Configure an automation stitch
- Configure an event handler with an automation stitch enabled

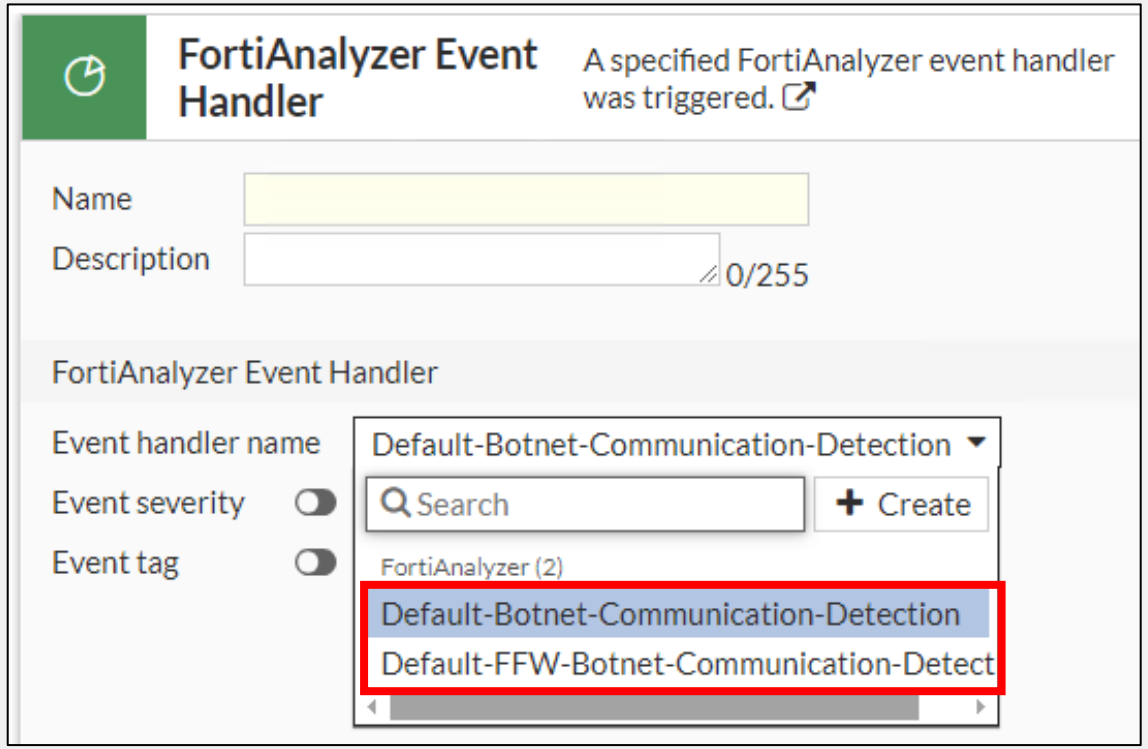
FortiAnalyzer and FortiGate Automation Stitch

- FortiAnalyzer can activate an automation stitch on authorized FortiGate devices
- An event handler must have the automation stitch option enabled
  - This allows FortiGate to detect the event handler from a list of potential triggers

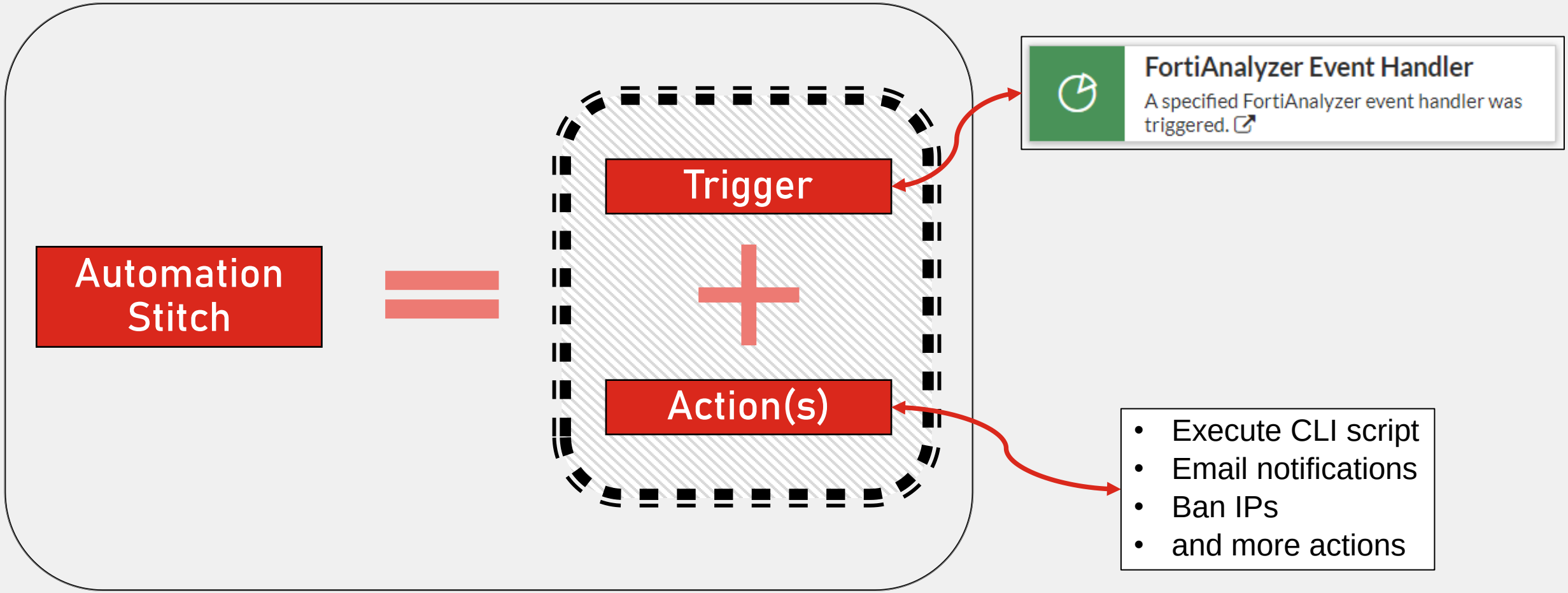
FortiAnalyzer Event Handler



FortiGate Automation Trigger



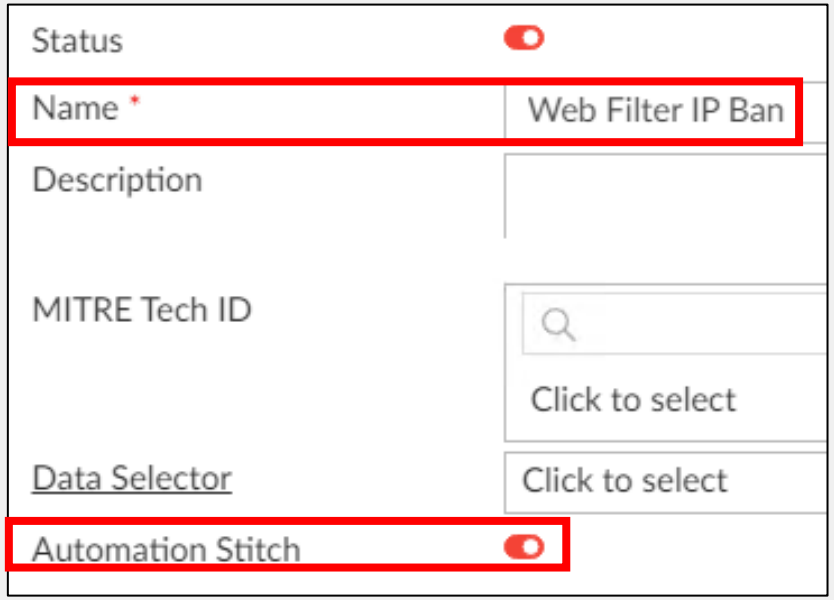
FortiAnalyzer and FortiGate Automation Stitch (Contd)



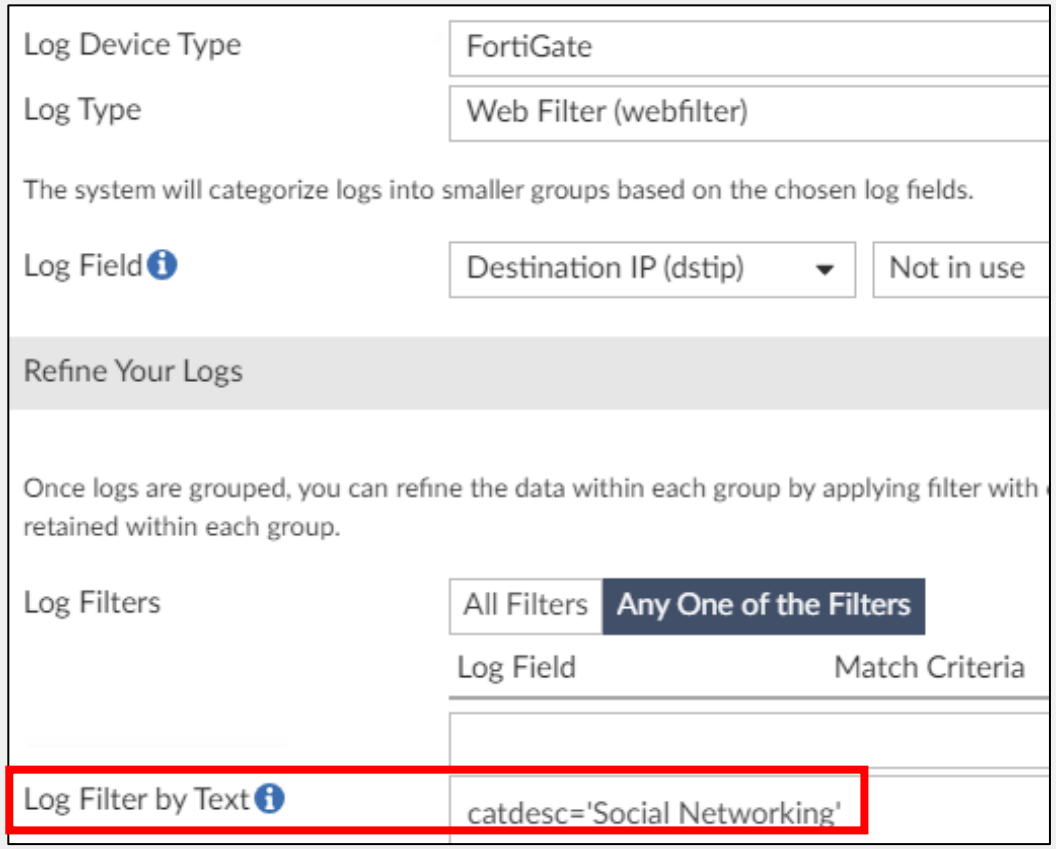
FortiAnalyzer and FortiGate Automation Stitch (Contd)

- This example automation stitch bans an IP address on FortiGate if the web filter violation category description matches social networking
- This slide shows the FortiAnalyzer configuration

Event Handler



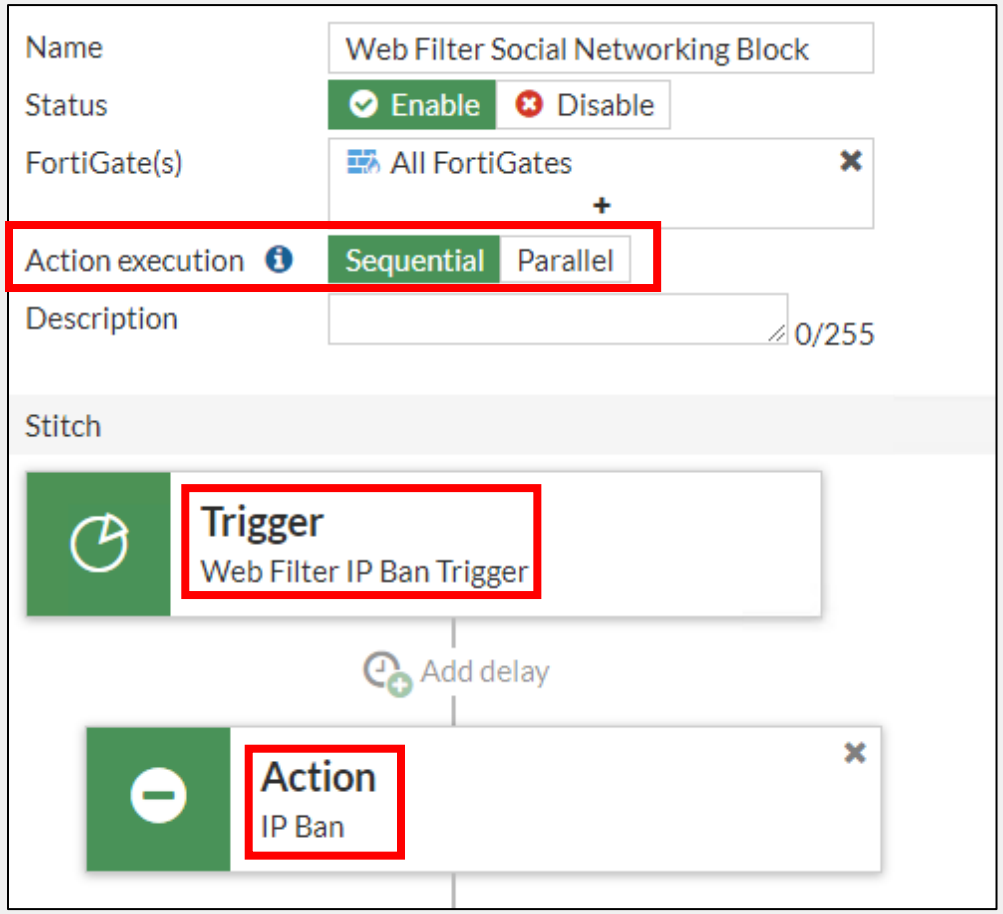
Event Handler Rule



FortiAnalyzer and FortiGate Automation Stitch (Contd)

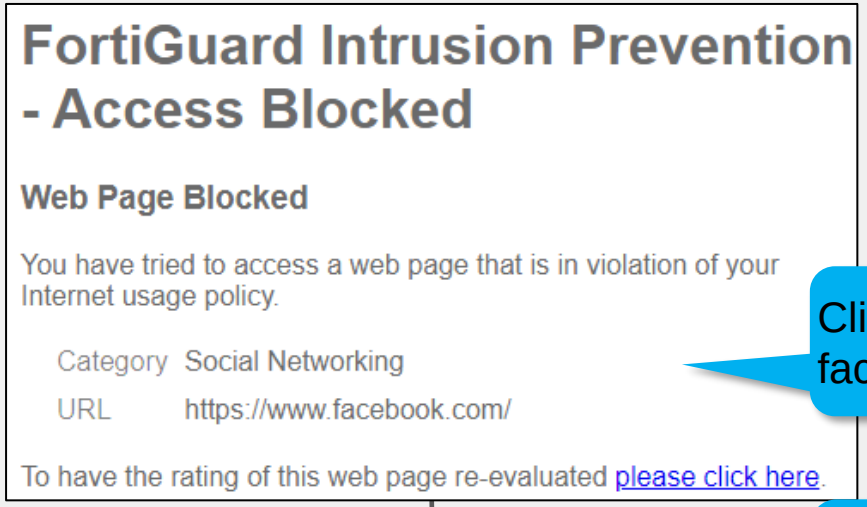
- This slide shows the FortiGate configuration

Automation Stitch



Workflow

1



Client goes to facebook.com

2

31.13.80.36 (1)	Web Filter IP Ban
dstip:31.13.80.36	Web Filter IP Ban

An event is created on FortiAnalyzer

3

```
FortiGate# diagnose user banned-ip list
src-ip-addr     created                    expires      cause
10.200.3.219    Sun Aug 18 14:20:01 2024 indefinite   Administrative
```

FortiGate bans the client

Knowledge Check

1. How many triggers and actions can each automation stitch support?
   A. One trigger and one action
   ✔ B. One trigger and multiple actions
   C. Multiple triggers and multiple actions

Lesson Progress

- ✓ Playbook Concepts
- ✓ Creating Playbooks
- ✓ Managing Playbooks
- ✓ Automation Stitches

Review

- ✓ Identify playbook components
- ✓ Describe trigger types and their properties
- ✓ Create and customize playbooks from a template
- ✓ Create new playbooks from scratch
- ✓ Use variables in tasks
- ✓ Monitor playbooks
- ✓ Export and import playbooks
- ✓ Describe FortiAnalyzer and FortiGate automation stitches
- ✓ Configure an automation stitch
- ✓ Configure an event handler with an automation stitch enabled