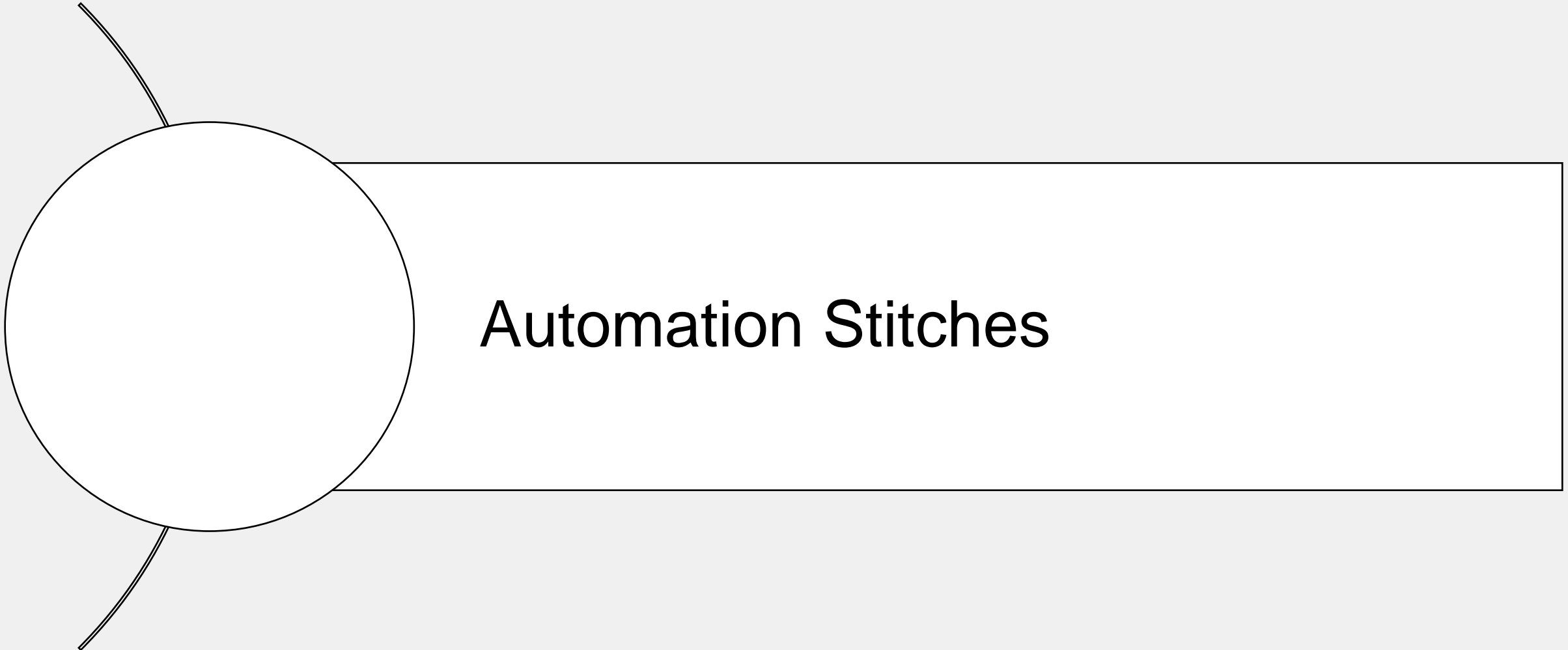


Security Operations Analyst

SOC Automation

Lesson Overview

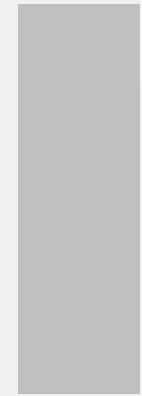




Automation Stitches



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

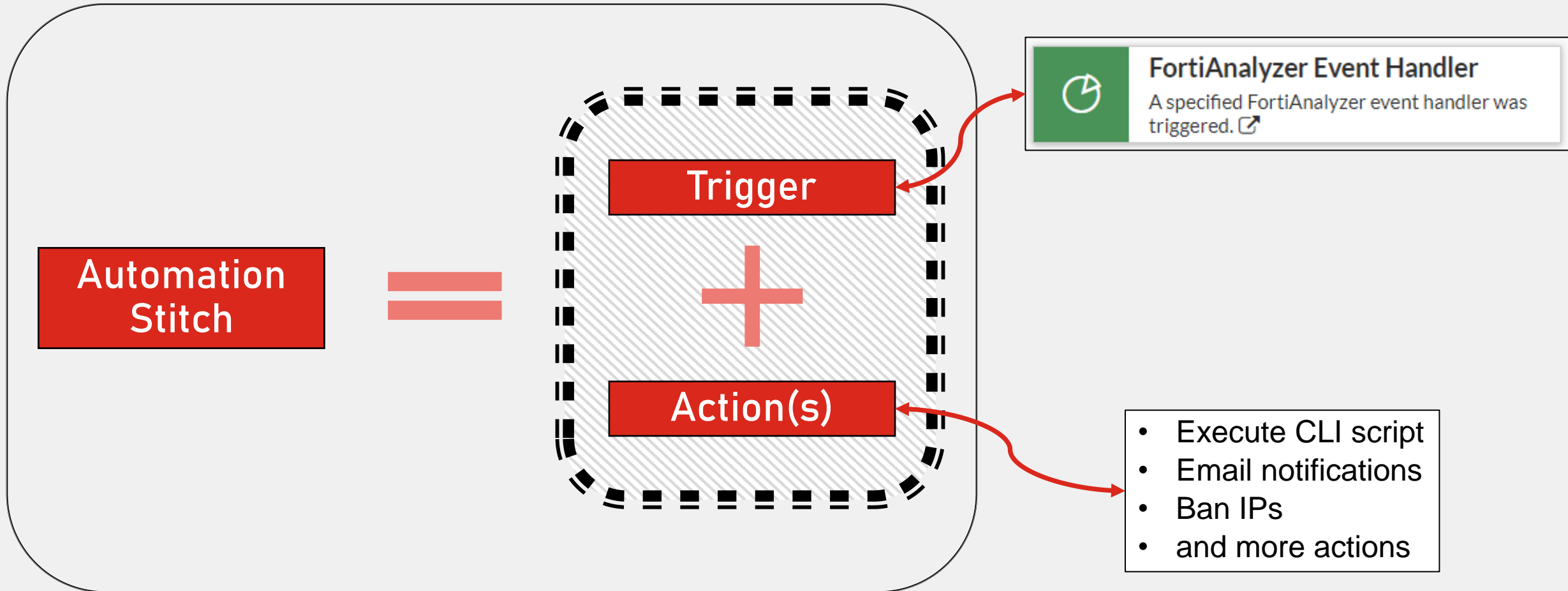
FortiAnalyzer Event Handler

Status	<input checked="" type="checkbox"/>
Name *	Default-Botnet-Communication-Detection
Description	Default event handler to detect botnet communication and report to FortiGate
MITRE Tech ID	<input type="text"/> T1584.005 Botnet T1071 Application Layer Protocol
Data Selector	Click to select
Automation Stitch	<input checked="" type="checkbox"/>

FortiGate Automation Trigger

	FortiAnalyzer Event Handler	A specified FortiAnalyzer event handler was triggered. ↗
Name	<input type="text"/>	
Description	<input type="text"/> 0/255	
FortiAnalyzer Event Handler		
Event handler name	Default-Botnet-Communication-Detection ▼	
Event severity	<input type="checkbox"/>	<input type="text"/> Search <input type="button" value="+ Create"/>
Event tag	<input type="checkbox"/>	FortiAnalyzer (2)
	Default-Botnet-Communication-Detection	
	Default-FFW-Botnet-Communication-Detect	

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

Status	<input checked="" type="checkbox"/>
Name *	Web Filter IP Ban
Description	
MITRE Tech ID	<input type="text"/> Click to select
Data Selector	Click to select
Automation Stitch	<input checked="" type="checkbox"/>

Event Handler Rule

Log Device Type	FortiGate	
Log Type	Web Filter (webfilter)	
The system will categorize logs into smaller groups based on the chosen log fields.		
Log Field ⓘ	Destination IP (dstip) ▼	Not in use
Refine Your Logs		
Once logs are grouped, you can refine the data within each group by applying filter with retained within each group.		
Log Filters	All Filters Any One of the Filters	
	Log Field	Match Criteria
Log Filter by Text ⓘ	catdesc='Social Networking'	

FortiAnalyzer and FortiGate Automation Stitch (Contd)

- This slide shows the FortiGate configuration

Automation Stitch

Name: Web Filter Social Networking Block

Status: ☒ Enable ☐ Disable

FortiGate(s): All FortiGates

Action execution: ☒ Sequential ☐ Parallel

Description: 0/255

Stitch

Trigger
Web Filter IP Ban Trigger

Add delay

Action
IP Ban

Workflow

FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

You have tried to access a web page that is in violation of your Internet usage policy.

Category: Social Networking

URL: <https://www.facebook.com/>

To have the rating of this web page re-evaluated [please click here](#).

Client goes to facebook.com

1

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

An event is created on FortiAnalyzer


2

3

FortiGate bans the client

```
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
```

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



Automation Stitches

Review

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