Fortinet

Exam Questions FCSS_SOC_AN-7.4

FCSS - Security Operations 7.4 Analyst

NEW QUESTION 1
According to the National Institute of Standards and Technology (NIST) cybersecurity framework, incident handling activities can be divided into phases.
In which incident handling phase do you quarantine a compromised host in order to prevent an adversary from using it as a stepping stone to the next phase of an attack?

A. Containment
B. Analysis
C. Eradication
D. Recovery

Answer: A

Explanation:
NIST Cybersecurity Framework Overview:
The NIST Cybersecurity Framework provides a structured approach for managing and mitigating cybersecurity risks. Incident handling is divided into several phases to systematically address and resolve incidents.
Incident Handling Phases:
Preparation: Establishing and maintaining an incident response capability.
Detection and Analysis: Identifying and investigating suspicious activities to confirm an incident.
Containment, Eradication, and Recovery:
Containment: Limiting the impact of the incident.
Eradication: Removing the root cause of the incident.
Recovery: Restoring systems to normal operation.
Containment Phase:
The primary goal of the containment phase is to prevent the incident from spreading and causing further damage.
Quarantining a Compromised Host:
Quarantining involves isolating the compromised host from the rest of the network to prevent adversaries from moving laterally and causing more harm.
Techniques include network segmentation, disabling network interfaces, and applying access controls.

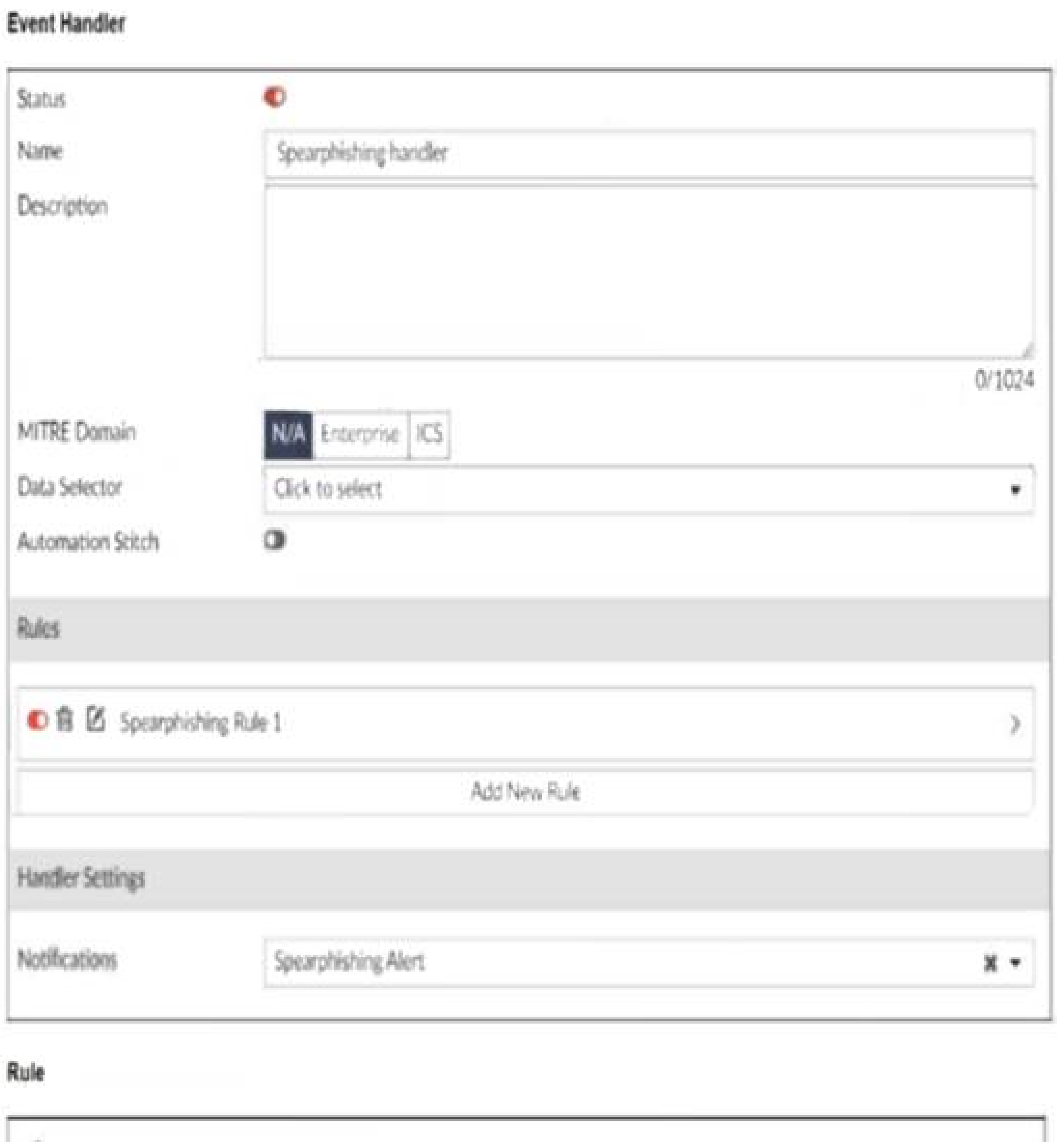
NEW QUESTION 2
A customer wants FortiAnalyzer to run an automation stitch that executes a CLI command on FortiGate to block a predefined list of URLs, if a botnet command-and-control (C&C) server IP is detected.
Which FortiAnalyzer feature must you use to start this automation process?

A. Playbook
B. Data selector
C. Event handler
D. Connector

Answer: C

Explanation:
Understanding Automation Processes in FortiAnalyzer:
FortiAnalyzer can automate responses to detected security events, such as running commands on FortiGate devices.
Analyzing the Customer Requirement:
The customer wants to run a CLI command on FortiGate to block predefined URLs when a botnet C&C server IP is detected.
This requires an automated response triggered by a specific event.
Evaluating the Options:
Option A:Playbooks orchestrate complex workflows but are not typically used for direct event-triggered automation processes.
Option B:Data selectors filter logs based on criteria but do not initiate automation processes.
Option C:Event handlers can be configured to detect specific events (such as detecting a botnet C&C server IP) and trigger automation stitches to execute predefined actions.
Option D:Connectors facilitate communication between FortiAnalyzer and other systems but are not the primary mechanism for initiating automation based on log events.
Conclusion:
To start the automation process when a botnet C&C server IP is detected, you must use anEvent handlerin FortiAnalyzer.
References:
Fortinet Documentation on Event Handlers and Automation Stitches in FortiAnalyzer.
Best Practices for Configuring Automated Responses in FortiAnalyzer.

NEW QUESTION 3
Refer to the exhibits.



Event Handler

Status ●

Name Spearphishing handler

Description

0/1024

MITRE Domain N/A | Enterprise | ICS

Data Selector Click to select

Automation Stitch

Rules

Spearphishing Rule 1

Add New Rule

Handler Settings

Notifications Spearphishing Alert

Rule

You configured a spearphishing event handler and the associated rule. However. FortiAnalyzer did not generate an event.
When you check the FortiAnalyzer log viewer, you confirm that FortiSandbox forwarded the appropriate logs, as shown in the raw log exhibit.
What configuration must you change on FortiAnalyzer in order for FortiAnalyzer to generate an event?

A. In the Log Type field, changethe selection toAntiVirus Log(malware).
B. Configure a FortiSandbox data selector and add it tothe event handler.
C. In the Log Filter by Text field, type the value:.5 ub t ype ma Iwa re..
D. Change trigger condition by selectin
E. Within a group, the log field Malware Kame (mname> has 2 or more unique values.

Answer: B

Explanation:
Understanding the Event Handler Configuration:
The event handler is set up to detect specific security incidents, such as spearphishing, based on logs forwarded from other Fortinet products like FortiSandbox.
An event handler includes rules that define the conditions under which an event should be triggered.
Analyzing the Current Configuration:
The current event handler is named "Spearphishing handler" with a rule titled "Spearphishing Rule 1".
The log viewer shows that logs are being forwarded by FortiSandbox but no events are generated by FortiAnalyzer.
Key Components of Event Handling:
Log Type: Determines which type of logs will trigger the event handler.
Data Selector: Specifies the criteria that logs must meet to trigger an event.
Automation Stitch: Optional actions that can be triggered when an event occurs.
Notifications: Defines how alerts are communicated when an event is detected.
Issue Identification:
Since FortiSandbox logs are correctly forwarded but no event is generated, the issue likely lies in the data selector configuration or log type matching.
The data selector must be configured to include logs forwarded by FortiSandbox.
Solution:
* B. Configure a FortiSandbox data selector and add it to the event handler:
By configuring a data selector specifically for FortiSandbox logs and adding it to the event handler, FortiAnalyzer can accurately identify and trigger events based on the forwarded logs.
Steps to Implement the Solution:
Step 1: Go to the Event Handler settings in FortiAnalyzer.
Step 2: Add a new data selector that includes criteria matching the logs forwarded by FortiSandbox (e.g., log subtype, malware detection details).
Step 3: Link this data selector to the existing spearphishing event handler.
Step 4: Save the configuration and test to ensure events are now being generated.
Conclusion:
The correct configuration of a FortiSandbox data selector within the event handler ensures that FortiAnalyzer can generate events based on relevant logs.
References:
Fortinet Documentation on Event Handlers and Data Selectors FortiAnalyzer Event Handlers
Fortinet Knowledge Base for Configuring Data Selectors FortiAnalyzer Data Selectors
By configuring a FortiSandbox data selector and adding it to the event handler, FortiAnalyzer will be able to accurately generate events based on the appropriate logs.

NEW QUESTION 4
Which two ways can you create an incident on FortiAnalyzer? (Choose two.)

A. Using a connector action

B. Manually, on the Event Monitor page
C. By running a playbook
D. Using a custom event handler

Answer: BD

Explanation:
Understanding Incident Creation in FortiAnalyzer:
FortiAnalyzer allows for the creation of incidents to track and manage security events.
Incidents can be created both automatically and manually based on detected events and predefined rules.
Analyzing the Methods:
Option A:Using a connector action typically involves integrating with other systems or services and is not a direct method for creating incidents on FortiAnalyzer.
Option B:Incidents can be created manually on the Event Monitor page by selecting relevant events and creating incidents from those events.
Option C:While playbooks can automate responses and actions, the direct creation of incidents is usually managed through event handlers or manual processes.
Option D:Custom event handlers can be configured to trigger incident creation based on specific events or conditions, automating the process within FortiAnalyzer.
Conclusion:
The two valid methods for creating an incident on FortiAnalyzer are manually on the Event Monitor page and using a custom event handler.
References:
Fortinet Documentation on Incident Management in FortiAnalyzer.
FortiAnalyzer Event Handling and Customization Guides.

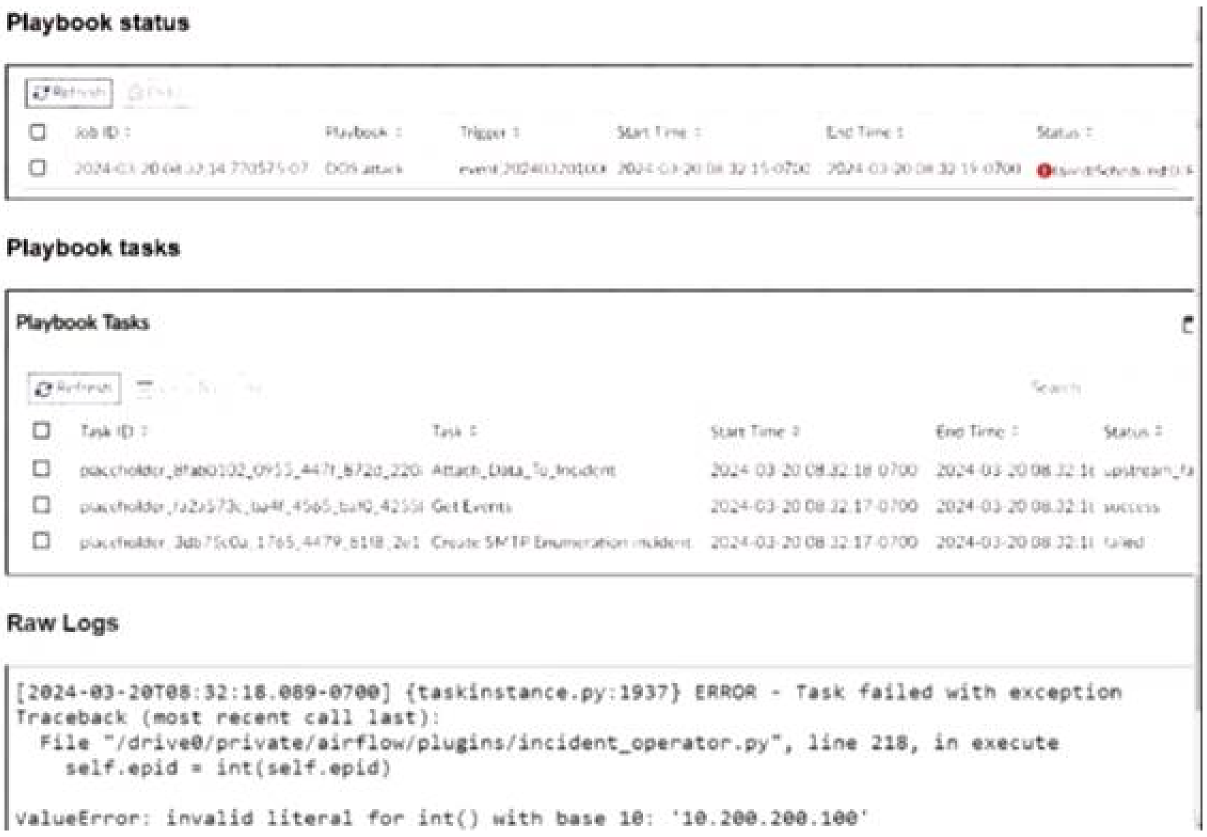
NEW QUESTION 5
When does FortiAnalyzer generate an event?

A. When a log matches a filter in a data selector
B. When a log matches an action in a connector
C. When a log matches a rule in an event handler
D. When a log matches a task in a playbook

Answer: C

Explanation:
Understanding Event Generation in FortiAnalyzer:
FortiAnalyzer generates events based on predefined rules and conditions to help in monitoring and responding to security incidents.
Analyzing the Options:
Option A:Data selectors filter logs based on specific criteria but do not generate events on their own.
Option B:Connectors facilitate integrations with other systems but do not generate events based on log matches.
Option C:Event handlers are configured with rules that define the conditions under which events are generated. When a log matches a rule in an event handler, FortiAnalyzer generates an event.
Option D:Tasks in playbooks execute actions based on predefined workflows but do not directly generate events based on log matches.
Conclusion:
FortiAnalyzer generates an event when a log matches a rule in an event handler.
References:
Fortinet Documentation on Event Handlers and Event Generation in FortiAnalyzer.
Best Practices for Configuring Event Handlers in FortiAnalyzer.

NEW QUESTION 6
Refer to the exhibits.



Playbook status

☐	Job ID	Playbook	Trigger	Start Time	End Time	Status
☐	2024-03-20 08:32:14.770575-07	DOS attack	event.20240320100x	2024-03-20 08:32:15-0700	2024-03-20 08:32:19-0700	● [illegible]

Playbook tasks

Playbook Tasks

☐	Task ID	Task	Start Time	End Time	Status
☐	placeholder_8fab0102_0955_447f_872d_220	Attach_Data_To_Incident	2024-03-20 08:32:18-0700	2024-03-20 08:32:1	upstream_fa
☐	placeholder_fa2a573c_ba4f_4565_ba10_4255	Get Events	2024-03-20 08:32:17-0700	2024-03-20 08:32:1	success
☐	placeholder_3db75c0a_1765_4479_8118_2e1	Create SMTP Enumeration incident	2024-03-20 08:32:17-0700	2024-03-20 08:32:1	failed

Raw Logs

```
[2024-03-20T08:32:18.089-0700] {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: '10.200.200.100'
```

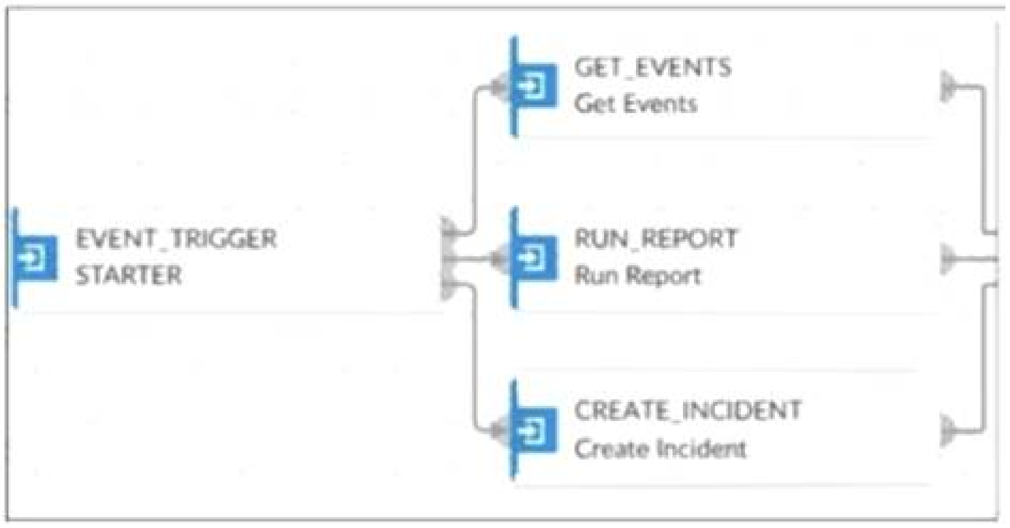
The DOS attack playbook is configured to create an incident when an event handler generates a denial-of-ser/ice (DoS) attack event.
Why did the DOS attack playbook fail to execute?

A. The Create SMTP Enumeration incident task is expecting an integer value but is receiving the incorrect data type
B. The Get Events task is configured to execute in the incorrect order.
C. The Attach_Data_To_Incident task failed.
D. The Attach_Data_To_Incident task is expecting an integer value but is receiving the incorrect data type.

Answer: A

Explanation:
Understanding the Playbook and its Components:
The exhibit shows the status of a playbook named "DOS attack" and its associated tasks.
The playbook is designed to execute a series of tasks upon detecting a DoS attack event.
Analysis of Playbook Tasks:
Attach_Data_To_Incident:Task ID placeholder_8fab0102, status is "upstream_failed," meaning it did not execute properly due to a previous task's failure.
Get Events:Task ID placeholder_fa2a573c, status is "success."
Create SMTP Enumeration incident:Task ID placeholder_3db75c0a, status is "failed."
Reviewing Raw Logs:
The error log shows aValueError: invalid literal for int() with base 10: '10.200.200.100'.
This error indicates that the task attempted to convert a string (the IP address '10.200.200.100') to an integer, which is not possible.
Identifying the Source of the Error:
The error occurs in the file "incident_operator.py," specifically in theexecutemethod.
This suggests that the task "Create SMTP Enumeration incident" is the one causing the issue because it failed to process the data type correctly.
Conclusion:
The failure of the playbook is due to the "Create SMTP Enumeration incident" task receiving a string value (an IP address) when it expects an integer value. This mismatch in data types leads to the error.
References:
Fortinet Documentation on Playbook and Task Configuration.
Python error handling documentation for understandingValueError.

NEW QUESTION 7
Refer to the Exhibit:



An analyst wants to create an incident and generate a report whenever FortiAnalyzer generates a malicious attachment event based on FortiSandbox analysis. The endpoint hosts are protected by FortiClient EMS integrated with FortiSandbox. All devices are logging to FortiAnalyzer.
Which connector must the analyst use in this playbook?

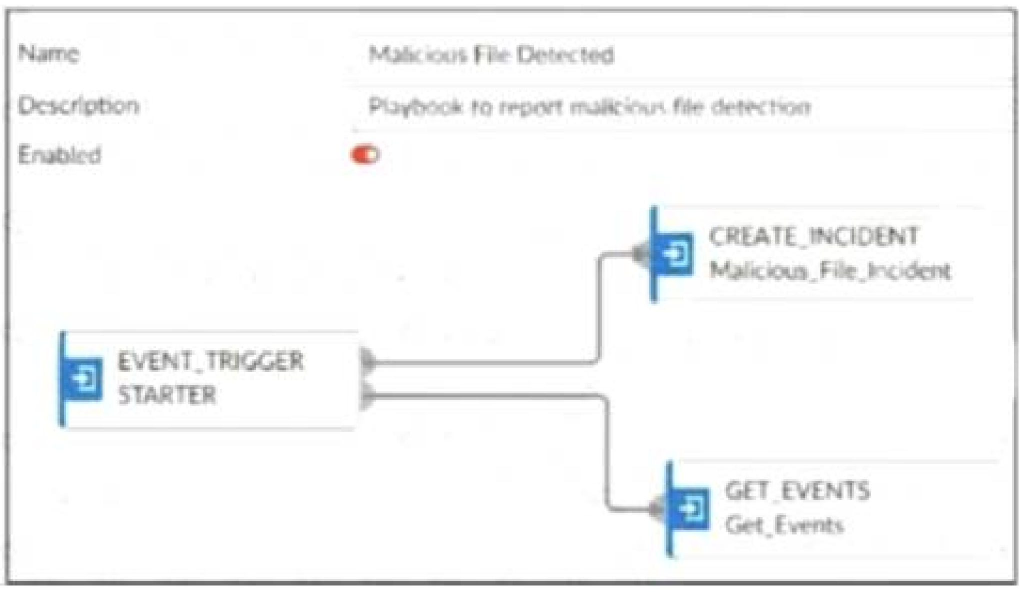
A. FortiSandbox connector
B. FortiClient EMS connector
C. FortiMail connector
D. Local connector

Answer: A

Explanation:
Understanding the Requirements:
The objective is to create an incident and generate a report based on malicious attachment events detected by FortiAnalyzer from FortiSandbox analysis.
The endpoint hosts are protected by FortiClient EMS, which is integrated with FortiSandbox. All logs are sent to FortiAnalyzer.
Key Components:
FortiAnalyzer: Centralized logging and analysis for Fortinet devices.
FortiSandbox: Advanced threat protection system that analyzes suspicious files and URLs.
FortiClient EMS: Endpoint management system that integrates with FortiSandbox for endpoint protection.
Playbook Analysis:
The playbook in the exhibit consists of three main actions:GET_EVENTS,RUN_REPORT, andCREATE_INCIDENT.
EVENT_TRIGGER: Starts the playbook when an event occurs.
GET_EVENTS: Fetches relevant events.
RUN_REPORT: Generates a report based on the events.
CREATE_INCIDENT: Creates an incident in the incident management system.
Selecting the Correct Connector:
The correct connector should allow fetching events related to malicious attachments analyzed by FortiSandbox and facilitate integration with FortiAnalyzer.
Connector Options:
FortiSandbox Connector:
Directly integrates with FortiSandbox to fetch analysis results and events related to malicious attachments.
Best suited for getting detailed sandbox analysis results.
Selected as it is directly related to the requirement of handling FortiSandbox analysis events.
FortiClient EMS Connector:
Used for managing endpoint security and integrating with endpoint logs.
Not directly related to fetching sandbox analysis events.
Not selected as it is not directly related to the sandbox analysis events.
FortiMail Connector:
Used for email security and handling email-related logs and events.
Not applicable for sandbox analysis events.
Not selected as it does not relate to the sandbox analysis.
Local Connector:
Handles local events within FortiAnalyzer itself.
Might not be specific enough for fetching detailed sandbox analysis results.

Not selected as it may not provide the required integration with FortiSandbox.
Implementation Steps:
Step 1: Ensure FortiSandbox is configured to send analysis results to FortiAnalyzer.
Step 2: Use the FortiSandbox connector in the playbook to fetch events related to malicious attachments.
Step 3: Configure theGET_EVENTSaction to use the FortiSandbox connector.
Step 4: Set up theRUN_REPORTandCREATE_INCIDENTactions based on the fetched events.
References:
Fortinet Documentation on FortiSandbox Integration FortiSandbox Integration Guide
Fortinet Documentation on FortiAnalyzer Event Handling FortiAnalyzer Administration Guide
By using the FortiSandbox connector, the analyst can ensure that the playbook accurately fetches events based on FortiSandbox analysis and generates the required incident and report.

NEW QUESTION 8
Refer to Exhibit:



Name Malicious File Detected
Description Playbook to report malicious file detection
Enabled

A SOC analyst is creating the Malicious File Detected playbook to run when FortiAnalyzer generates a malicious file event. The playbook must also update the incident with the malicious file event data.
What must the next task in this playbook be?

A. A local connector with the action Update Asset and Identity
B. A local connector with the action Attach Data to Incident
C. A local connector with the action Run Report
D. A local connector with the action Update Incident

Answer: D

Explanation:
Understanding the Playbook and its Components:
The exhibit shows a playbook in which an event trigger starts actions upon detecting a malicious file.
The initial tasks in the playbook includeCREATE_INCIDENTandGET_EVENTS.
Analysis of Current Tasks:
EVENT_TRIGGER STARTER: This initiates the playbook when a specified event (malicious file detection) occurs.
CREATE_INCIDENT: This task likely creates a new incident in the incident management system for tracking and response.
GET_EVENTS: This task retrieves the event details related to the detected malicious file.
Objective of the Next Task:
The next logical step after creating an incident and retrieving event details is to update the incident with the event data, ensuring all relevant information is attached to the incident record.
This helps SOC analysts by consolidating all pertinent details within the incident record, facilitating efficient tracking and response.
Evaluating the Options:
Option A:Update Asset and Identityis not directly relevant to attaching event data to the incident.
Option B:Attach Data to Incidentsounds plausible but typically, updating an incident involves more comprehensive changes including status updates, adding comments, and other data modifications.
Option C:Run Reportis irrelevant in this context as the goal is to update the incident with event data.
Option D:Update Incidentis the most suitable action for incorporating event data into the existing incident record.
Conclusion:
The next task in the playbook should be to update the incident with the event data to ensure the incident reflects all necessary information for further investigation and response.
References:
Fortinet Documentation on Playbook Creation and Incident Management.
Best Practices for Automating Incident Response in SOC Operations.

NEW QUESTION 10
......