Exam Questions FCSS_SOC_AN-7.4

FCSS - Security Operations 7.4 Analyst

https://www.2passeasy.com/dumps/FCSS_SOC_AN-7.4/

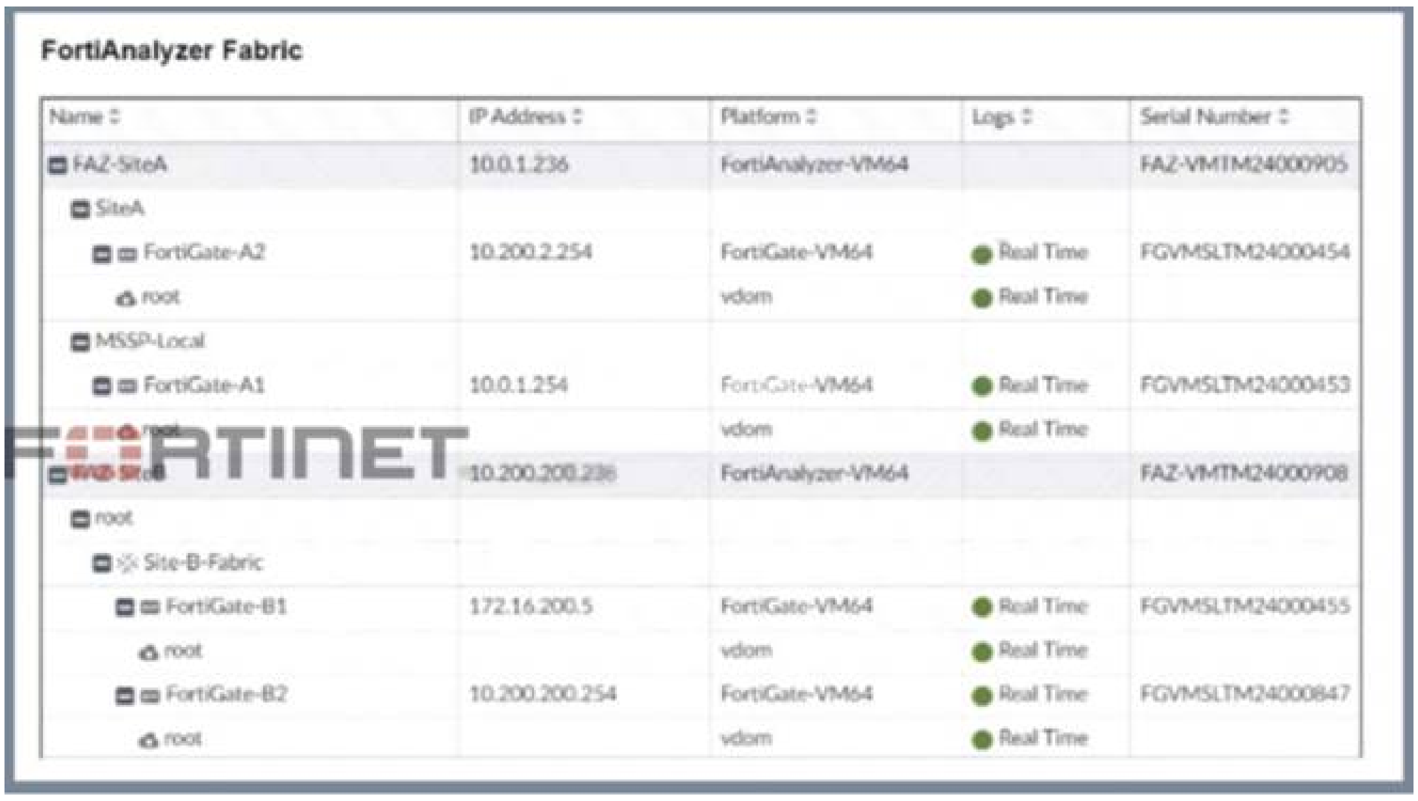
NEW QUESTION 1
Which two playbook triggers enable the use of trigger events in later tasks as trigger variables? (Choose two.)

A. EVENT
B. INCIDENT
C. ON SCHEDULE
D. ON DEMAND

Answer: AB

Explanation:
Understanding Playbook Triggers:
Playbook triggers are the starting points for automated workflows within FortiAnalyzer or FortiSOAR.
These triggers determine how and when a playbook is executed and can pass relevant information (trigger variables) to subsequent tasks within the playbook.
Types of Playbook Triggers:
EVENT Trigger:
Initiates the playbook when a specific event occurs.
The event details can be used as variables in later tasks to customize the response.
Selected as it allows using event details as trigger variables.
INCIDENT Trigger:
Activates the playbook when an incident is created or updated.
The incident details are available as variables in subsequent tasks.
Selected as it enables the use of incident details as trigger variables.
ON SCHEDULE Trigger:
Executes the playbook at specified times or intervals.
Does not inherently use trigger events to pass variables to later tasks.
Not selected as it does not involve passing trigger event details.
ON DEMAND Trigger:
Runs the playbook manually or as required.
Does not automatically include trigger event details for use in later tasks.
Not selected as it does not use trigger events for variables.
Implementation Steps:
Step 1: Define the conditions for the EVENT or INCIDENT trigger in the playbook configuration.
Step 2: Use the details from the trigger event or incident in subsequent tasks to customize actions and responses.
Step 3: Test the playbook to ensure that the trigger variables are correctly passed and utilized.
Conclusion:
EVENT and INCIDENT triggers are specifically designed to initiate playbooks based on specific occurrences, allowing the use of trigger details in subsequent tasks.
References:
Fortinet Documentation on Playbook Configuration FortiSOAR Playbook Guide
By using the EVENT and INCIDENT triggers, you can leverage trigger events in later tasks as variables, enabling more dynamic and responsive playbook actions.

NEW QUESTION 2
Refer to the exhibit.



FortiAnalyzer Fabric

Name	IP Address	Platform	Logs	Serial Number
FAZ-SiteA	10.0.1.236	FortiAnalyzer-VM64		FAZ-VMTM24000905
SiteA				
FortiGate-A2	10.200.2.254	FortiGate-VM64	● Real Time	FGVMSLTM24000454
root		vdom	● Real Time	
MSSP-Local				
FortiGate-A1	10.0.1.254	FortiGate-VM64	● Real Time	FGVMSLTM24000453
root		vdom	● Real Time	
FAZ-SiteB	10.200.200.236	FortiAnalyzer-VM64		FAZ-VMTM24000908
root				
Site-B-Fabric				
FortiGate-B1	172.16.200.5	FortiGate-VM64	● Real Time	FGVMSLTM24000455
root		vdom	● Real Time	
FortiGate-B2	10.200.200.254	FortiGate-VM64	● Real Time	FGVMSLTM24000847
root		vdom	● Real Time	

Assume that all devices in the FortiAnalyzer Fabric are shown in the image.
Which two statements about the FortiAnalyzer Fabric deployment are true? (Choose two.)

A. FortiGate-B1 and FortiGate-B2 are in a Security Fabric.
B. There is no collector in the topology.
C. All FortiGate devices are directly registered to the supervisor.
D. FAZ-SiteA has two ADOMs enabled.

Answer: AD

Explanation:
Understanding the FortiAnalyzer Fabric:
The FortiAnalyzer Fabric provides centralized log collection, analysis, and reporting for connected FortiGate devices.

Devices in a FortiAnalyzer Fabric can be organized into different Administrative Domains (ADOMs) to separate logs and management.
Analyzing the Exhibit:
FAZ-SiteAandFAZ-SiteBare FortiAnalyzer devices in the fabric.
FortiGate-B1andFortiGate-B2are shown under theSite-B-Fabric, indicating they are part of the same Security Fabric.
FAZ-SiteAhas multiple entries under it:SiteAandMSSP-Local, suggesting multiple ADOMs are enabled.
Evaluating the Options:
Option A:FortiGate-B1 and FortiGate-B2 are underSite-B-Fabric, indicating they are indeed part of the same Security Fabric.
Option B:The presence of FAZ-SiteA and FAZ-SiteB as FortiAnalyzers does not preclude the existence of collectors. However, there is no explicit mention of a separate collector role in the exhibit.
Option C:Not all FortiGate devices are directly registered to the supervisor. The exhibit shows hierarchical organization under different sites and ADOMs.
Option D:The multiple entries underFAZ-SiteA(SiteA and MSSP-Local) indicate that FAZ-SiteA has two ADOMs enabled.
Conclusion:
FortiGate-B1 and FortiGate-B2 are in a Security Fabric.
FAZ-SiteA has two ADOMs enabled.
References:
Fortinet Documentation on FortiAnalyzer Fabric Topology and ADOM Configuration.
Best Practices for Security Fabric Deployment with FortiAnalyzer.

NEW QUESTION 3
When configuring a FortiAnalyzer to act as a collector device, which two steps must you perform?(Choose two.)

A. Enable log compression.
B. Configure log forwarding to a FortiAnalyzer in analyzer mode.
C. Configure the data policy to focus on archiving.
D. Configure Fabric authorization on the connecting interface.

Answer: BD

Explanation:
Understanding FortiAnalyzer Roles:
FortiAnalyzer can operate in two primary modes: collector mode and analyzer mode.
Collector Mode: Gathers logs from various devices and forwards them to another FortiAnalyzer operating in analyzer mode for detailed analysis.
Analyzer Mode: Provides detailed log analysis, reporting, and incident management.
Steps to Configure FortiAnalyzer as a Collector Device:
* A. Enable Log Compression:
While enabling log compression can help save storage space, it is not a mandatory step specifically required for configuring FortiAnalyzer in collector mode.
Not selected as it is optional and not directly related to the collector configuration process.
B. Configure Log Forwarding to a FortiAnalyzer in Analyzer Mode:
Essential for ensuring that logs collected by the collector FortiAnalyzer are sent to the analyzer FortiAnalyzer for detailed processing.
Selected as it is a critical step in configuring a FortiAnalyzer as a collector device.
Step 1: Access the FortiAnalyzer interface and navigate to log forwarding settings.
Step 2: Configure log forwarding by specifying the IP address and necessary credentials of the FortiAnalyzer in analyzer mode.

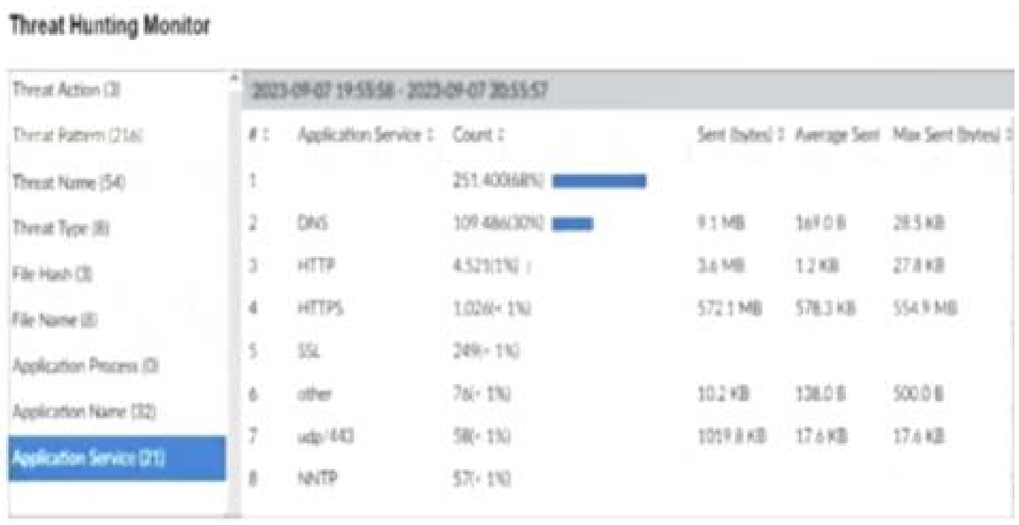
NEW QUESTION 4
When does FortiAnalyzer generate an event?

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.

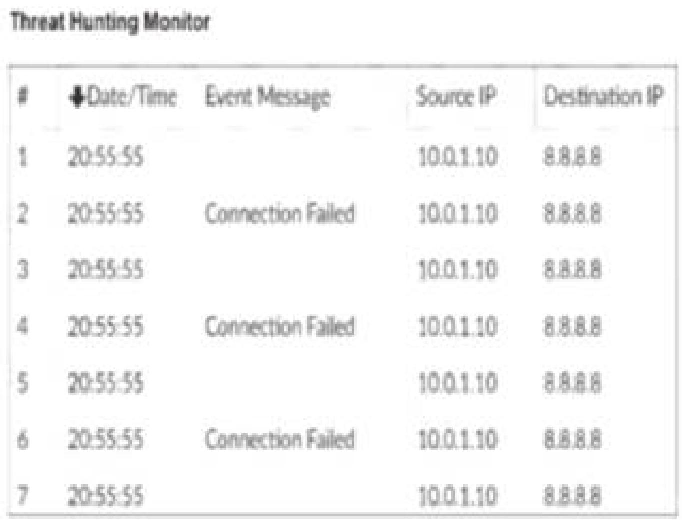
NEW QUESTION 5
Refer to the exhibits.



Threat Hunting Monitor

2023-09-07 19:55:58 - 2023-09-07 20:55:57

#	Application Service	Count	Sent (bytes)	Average Sent	Max Sent (bytes)
1		251,400(68%)			
2	DNS	109,486(30%)	9.1 MB	169.0 B	28.5 KB
3	HTTP	4,521(1%)	3.6 MB	1.2 KB	27.8 KB
4	HTTPS	1,026(< 1%)	572.1 MB	578.3 KB	554.9 MB
5	SSL	249(< 1%)			
6	other	76(< 1%)	10.2 KB	138.0 B	500.0 B
7	udp/443	58(< 1%)	1019.8 KB	17.6 KB	17.6 KB
8	NNTP	57(< 1%)			



Threat Hunting Monitor

#	Date/Time	Event Message	Source IP	Destination IP
1	20:55:55		10.0.1.10	8.8.8.8
2	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
3	20:55:55		10.0.1.10	8.8.8.8
4	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
5	20:55:55		10.0.1.10	8.8.8.8
6	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
7	20:55:55		10.0.1.10	8.8.8.8

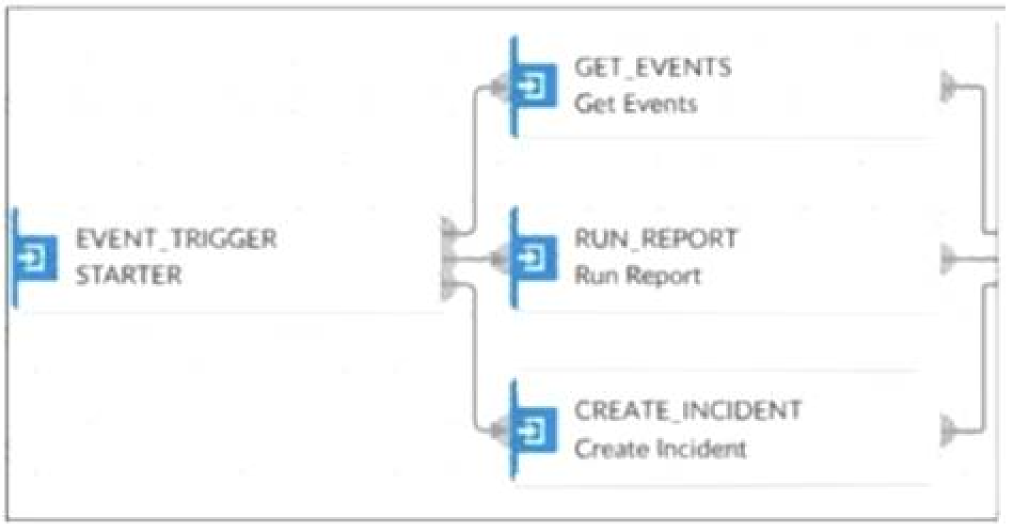
What can you conclude from analyzing the data using the threat hunting module?

A. Spearphishing is being used to elicit sensitive information.
B. DNS tunneling is being used to extract confidential data from the local network.
C. Reconnaissance is being used to gather victim identityinformation from the mail server.
D. FTP is being used as command-and-control (C&C) technique to mine for data.

Answer: B

Explanation:
Understanding the Threat Hunting Data:
The Threat Hunting Monitor in the provided exhibits shows various application services, their usage counts, and data metrics such as sent bytes, average sent bytes, and maximum sent bytes.
The second part of the exhibit lists connection attempts from a specific source IP (10.0.1.10) to a destination IP (8.8.8.8), with repeated "Connection Failed" messages.
Analyzing the Application Services:
DNS is the top application service with a significantly high count (251,400) and notable sent bytes
(9.1 MB).
This large volume of DNS traffic is unusual for regular DNS queries and can indicate the presence of DNS tunneling.
DNS Tunneling:
DNS tunneling is a technique used by attackers to bypass security controls by encoding data within DNS queries and responses. This allows them to extract data from the local network without detection.
The high volume of DNS traffic, combined with the detailed metrics, suggests that DNS tunneling might be in use.
Connection Failures to 8.8.8.8:
The repeated connection attempts from the source IP (10.0.1.10) to the destination IP (8.8.8.8) with connection failures can indicate an attempt to communicate with an external server.
Google DNS (8.8.8.8) is often used for DNS tunneling due to its reliability and global reach.
Conclusion:
Given the significant DNS traffic and the nature of the connection attempts, it is reasonable to conclude that DNS tunneling is being used to extract confidential data from the local network.
Why Other Options are Less Likely:
Spearphishing (A): There is no evidence from the provided data that points to spearphishing attempts, such as email logs or phishing indicators.
Reconnaissance (C): The data does not indicate typical reconnaissance activities, such as scanning or probing mail servers.
FTP C&C (D): There is no evidence of FTP traffic or command-and-control communications using FTP in the provided data.
References:
SANS Institute: "DNS Tunneling: How to Detect Data Exfiltration and Tunneling Through DNS Queries" SANS DNS Tunneling
OWASP: "DNS Tunneling" OWASP DNS Tunneling
By analyzing the provided threat hunting data, it is evident that DNS tunneling is being used to exfiltrate data, indicating a sophisticated method of extracting confidential information from the network.

NEW QUESTION 6
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?

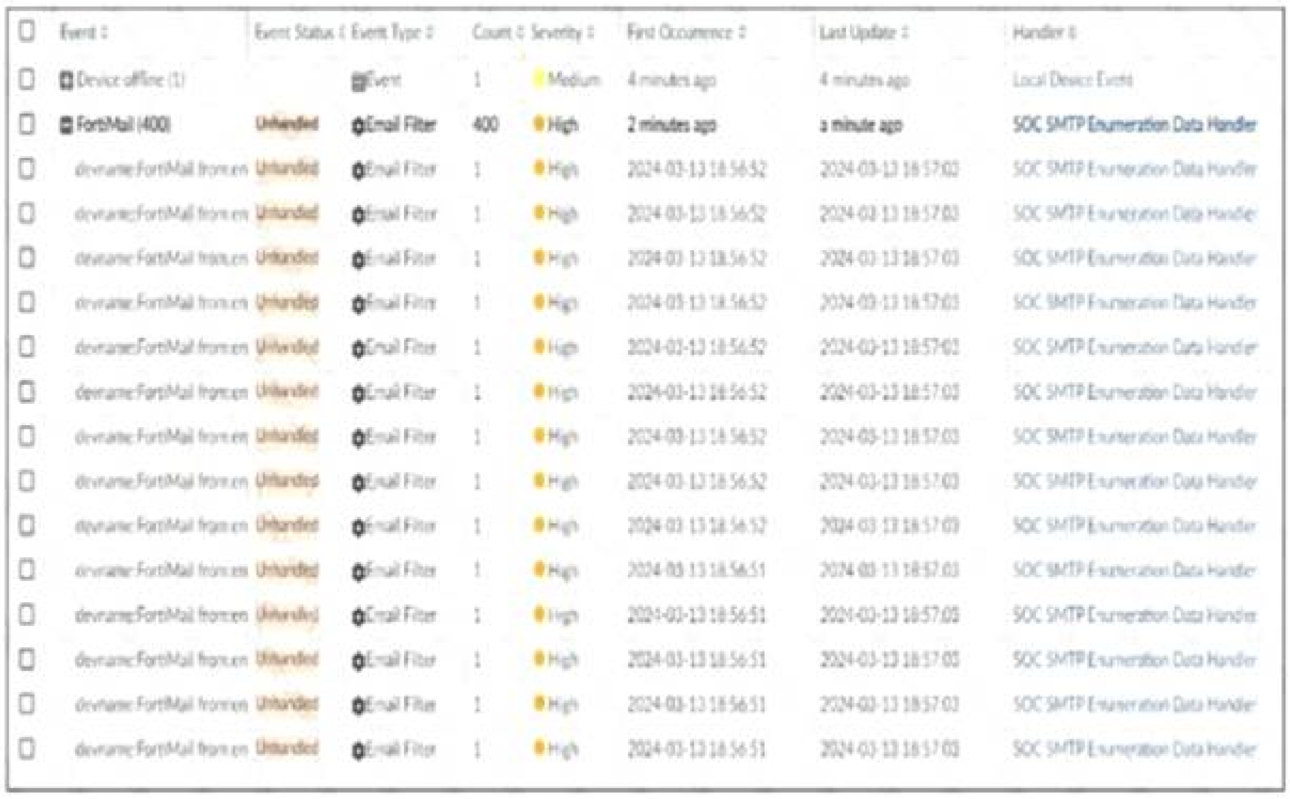
A. FortiSandbox connector
B. FortiClient EMS connector
C. FortiMail connector
D. Local connector

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.

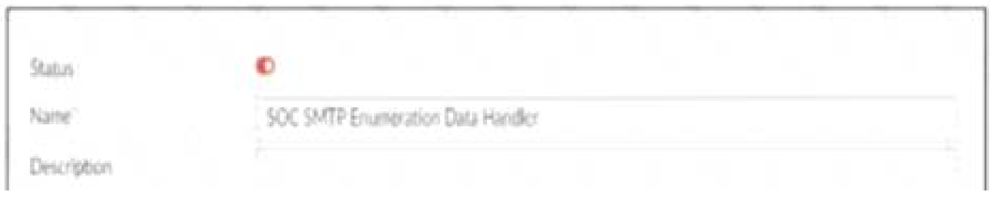
NEW QUESTION 7
Refer to the exhibit.

Events



☐	Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Handler
☐	Device offline (1)		Event	1	Medium	4 minutes ago	4 minutes ago	Local Device Event
☐	FortiMail (400)	Unhandled	Email Filter	400	High	2 minutes ago	a minute ago	SOC SMTP Enumeration Data Handler
☐	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
☐	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
☐	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
☐	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
☐	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
☐	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
☐	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
☐	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
☐	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
☐	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:51	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
☐	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:51	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
☐	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:51	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
☐	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:51	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
☐	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:51	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler

Event Handler



Status ●
Name SOC SMTP Enumeration Data Handler
Description

You notice that the custom event handler you configured to detect SMTP reconnaissance activities is creating a large number of events. This is overwhelming your notification system.
How can you fix this?

A. Increase the trigger count so that it identifies and reduces the count triggered by a particular group.
B. Disable the custom event handler because it is not working as expected.
C. Decrease the time range that the custom event handler covers during the attack.
D. Increase the log field value so that it looks for more unique field values when it creates the event.

Answer: A

Explanation:
Understanding the Issue:
The custom event handler for detecting SMTP reconnaissance activities is generating a large number of events.
This high volume of events is overwhelming the notification system, leading to potential alert fatigue and inefficiency in incident response.
Event Handler Configuration:
Event handlers are configured to trigger alerts based on specific criteria.
The frequency and volume of these alerts can be controlled by adjusting the trigger conditions.
Possible Solutions:
* A. Increase the trigger count so that it identifies and reduces the count triggered by a particular group:
By increasing the trigger count, you ensure that the event handler only generates alerts after a higher threshold of activity is detected.
This reduces the number of events generated and helps prevent overwhelming the notification system.
Selected as it effectively manages the volume of generated events.
* B. Disable the custom event handler because it is not working as expected:
Disabling the event handler is not a practical solution as it would completely stop monitoring for SMTP reconnaissance activities.
Not selected as it does not address the issue of fine-tuning the event generation.
* C. Decrease the time range that the custom event handler covers during the attack:
Reducing the time range might help in some cases, but it could also lead to missing important activities if the attack spans a longer period.
Not selected as it could lead to underreporting of significant events.
* D. Increase the log field value so that it looks for more unique field values when it creates the event:
Adjusting the log field value might refine the event criteria, but it does not directly control the volume of alerts.
Not selected as it is not the most effective way to manage event volume.
Implementation Steps:
Step 1: Access the event handler configuration in FortiAnalyzer.
Step 2: Locate the trigger count setting within the custom event handler for SMTP reconnaissance.
Step 3: Increase the trigger count to a higher value that balances alert sensitivity and volume.
Step 4: Save the configuration and monitor the event generation to ensure it aligns with expected levels.
Conclusion:
By increasing the trigger count, you can effectively reduce the number of events generated by the custom event handler, preventing the notification system from being overwhelmed.
References:
Fortinet Documentation on Event Handlers and Configuration FortiAnalyzer Administration Guide
Best Practices for Event Management Fortinet Knowledge Base
By increasing the trigger count in the custom event handler, you can manage the volume of generated events and prevent the notification system from being overwhelmed.

NEW QUESTION 10
......