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.

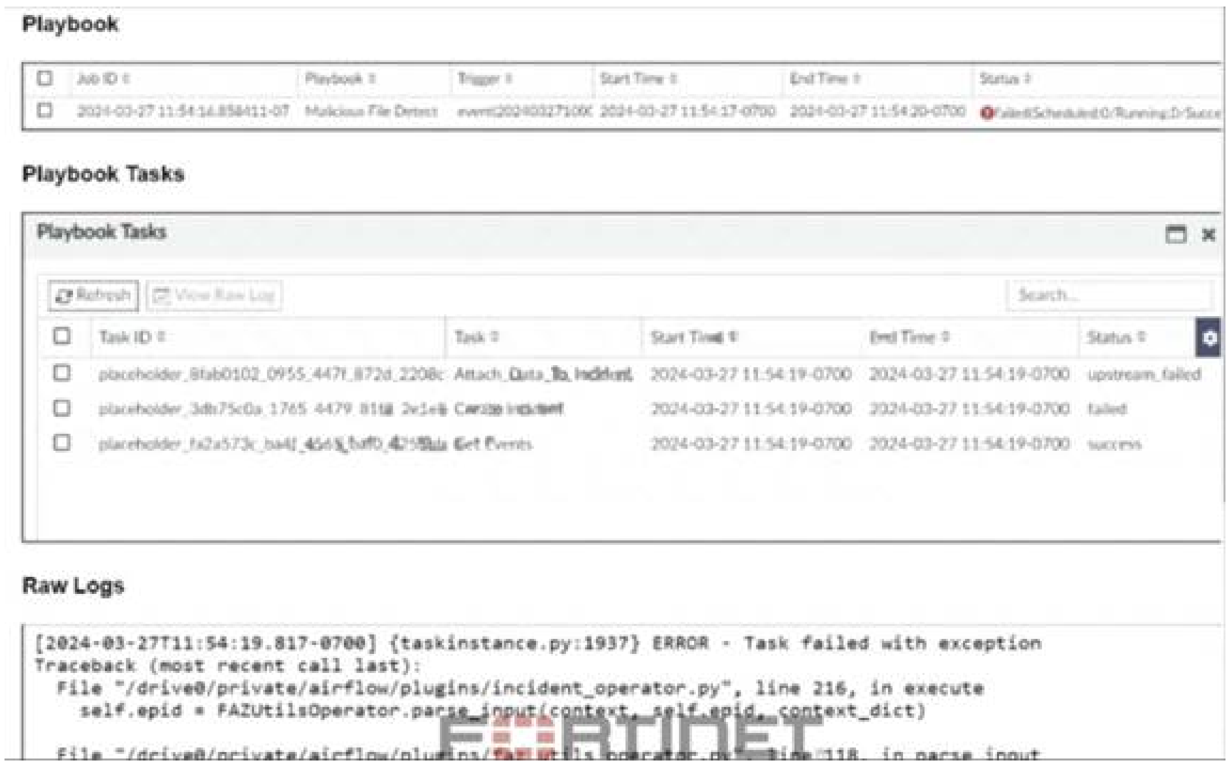
NEW QUESTION 2
A customer wants FortiAnalyzer to run an automation stitch that executes a CLI command on FortiGate to block a predefined list of URLs, if a botnet command-and-control (C&C) server IP is detected.
Which FortiAnalyzer feature must you use to start this automation process?

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.



Playbook

☐	Job ID	Playbook	Trigger	Start Time	End Time	Status
☐	2024-03-27 11:54:14.858411-07	Malicious File Detect	event20240327100(	2024-03-27 11:54:17-0700	2024-03-27 11:54:20-0700	● failed/Scheduled:0/Running:0/Succe

Playbook Tasks

Playbook Tasks

☐	Task ID	Task	Start Time	End Time	Status
☐	placeholder_8fab0102_0955_4471_872d_2208c	Attach_Data_To_Incident	2024-03-27 11:54:19-0700	2024-03-27 11:54:19-0700	upstream_failed
☐	placeholder_3db75c0a_1765_4479_81 [illegible]	Create Incident	2024-03-27 11:54:19-0700	2024-03-27 11:54:19-0700	failed
☐	placeholder_fa2a573c_ba4f_4565_bdf0_425 [illegible]	Get Events	2024-03-27 11:54:19-0700	2024-03-27 11:54:19-0700	success

Raw Logs

```
[2024-03-27T11:54:19.817-0700] {taskinstance.py:1937} ERROR - Task failed with exception
Traceback (most recent call last):
  File "/drive0/private/airflow/plugins/incident_operator.py", line 216, in execute
    self.epid = FAZUtilsOperator.parse_input(context, self.epid, context_dict)

  File "/drive0/private/airflow/plugins/fazutils_operator.py", line 118, in parse_input
```

The Malicious File Detect playbook is configured to create an incident when an event handler generates a malicious file detection event.
Why did the Malicious File Detect playbook execution fail?

A. The Create Incident task was expecting a name or number as input, but received an incorrect data format
B. The Get Events task did not retrieve any event data.
C. The Attach_Data_To_Incident incident task wasexpecting an integer, but received an incorrect data format.
D. The Attach Data To Incident task failed, which stopped the playbook execution.

Answer: A

Explanation:
Understanding the Playbook Configuration:
The "Malicious File Detect" playbook is designed to create an incident when a malicious file detection event is triggered.
The playbook includes tasks such asAttach_Data_To_Incident,Create Incident, andGet Events.
Analyzing the Playbook Execution:
The exhibit shows that theCreate Incidenttask has failed, and theAttach_Data_To_Incidenttask has also failed.
TheGet Eventstask succeeded, indicating that it was able to retrieve event data.
Reviewing Raw Logs:
The raw logs indicate an error related to parsing input in theincident_operator.pyfile.
The error traceback suggests that the task was expecting a specific input format (likely a name or number) but received an incorrect data format.
Identifying the Source of the Failure:
TheCreate Incidenttask failure is the root cause since it did not proceed correctly due to incorrect input format.
TheAttach_Data_To_Incidenttask subsequently failed because it depends on the successful creation of an incident.
Conclusion:
The primary reason for the playbook execution failure is that theCreate Incidenttask received an incorrect data format, which was not a name or number as expected.
References:
Fortinet Documentation on Playbook and Task Configuration.
Error handling and debugging practices in playbook execution.

NEW QUESTION 4
Which role does a threat hunter play within a SOC?

A. investigate and respond to a reported security incident
B. Collect evidence and determine the impact of a suspected attack
C. Search for hidden threats inside a network which may have eluded detection
D. Monitor network logs to identify anomalous behavior

Answer: C

Explanation:
Role of a Threat Hunter:
A threat hunter proactively searches for cyber threats that have evaded traditional security defenses. This role is crucial in identifying sophisticated and stealthy adversaries that bypass automated detection systems.
Key Responsibilities:
Proactive Threat Identification:
Threat hunters use advanced tools and techniques to identify hidden threats within the network. This includes analyzing anomalies, investigating unusual behaviors, and utilizing threat intelligence.

NEW QUESTION 5
Which FortiAnalyzer connector can you use to run automation stitches9

A. FortiCASB
B. FortiMail
C. Local
D. FortiOS

Answer: D

Explanation:

- Overview of Automation Stitches:
- Automation stitches in FortiAnalyzer are predefined sets of automated actions triggered by specific events. These actions help in automating responses to security incidents, improving efficiency, and reducing the response time.
- FortiAnalyzer Connectors:
- FortiAnalyzer integrates with various Fortinet products and other third-party solutions through connectors. These connectors facilitate communication and data exchange, enabling centralized management and automation.
- Available Connectors for Automation Stitches:
- FortiCASB:
- FortiCASB is a Cloud Access Security Broker that helps secure SaaS applications.

However, it is not typically used for running automation stitches within FortiAnalyzer.

NEW QUESTION 6

Which statement best describes the MITRE ATT&CK framework?

A. Itprovides a high-level description of common adversary activities, but lacks technical details
B. It covers tactics, techniques, and procedures, but does not provide information about mitigations.
C. It describes attack vectors targeting network devices and servers, but not user endpoints.
D. It contains some techniques or subtechniques that fall under more than one tactic.

Answer: D

Explanation:
Understanding the MITRE ATT&CK Framework:
The MITRE ATT&CK framework is a comprehensive matrix of tactics and techniques used by adversaries to achieve their objectives.
It is widely used for understanding adversary behavior, improving defense strategies, and conducting security assessments.
Analyzing the Options:
Option A:The framework provides detailed technical descriptions of adversary activities, including specific techniques and subtechniques.
Option B:The framework includes information about mitigations and detections for each technique and subtechnique, providing comprehensive guidance.
Option C:MITRE ATT&CK covers a wide range of attack vectors, including those targeting user endpoints, network devices, and servers.
Option D:Some techniques or subtechniques do indeed fall under multiple tactics, reflecting the complex nature of adversary activities that can serve different objectives.
Conclusion:
The statement that best describes the MITRE ATT&CK framework is that it contains some techniques or subtechniques that fall under more than one tactic.
References:
MITRE ATT&CK Framework Documentation.
Security Best Practices and Threat Intelligence Reports Utilizing MITRE ATT&CK.

NEW QUESTION 7

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 8

When does FortiAnalyzer generate an event?

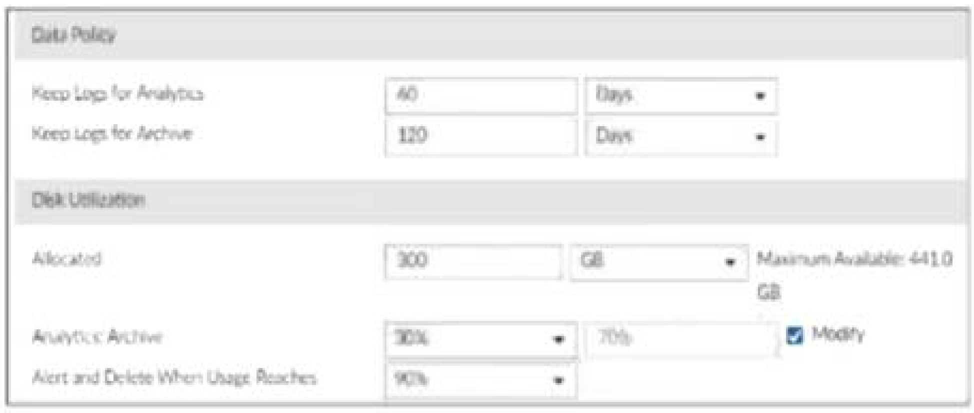
A. When a log matches a filter in a data selector
B. When a log matches an action in a connector
C. When a log matches a rule in an event handler
D. When a log matches a task in a playbook

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 9
Refer to Exhibit:



Data Policy

Keep Logs for Analytics 40 Days

Keep Logs for Archive 120 Days

Disk Utilization

Allocated 300 GB Maximum Available: 441.0 GB

Analytics: Archive 30% 70% ☑ Modify

Alert and Delete When Usage Reaches 90%

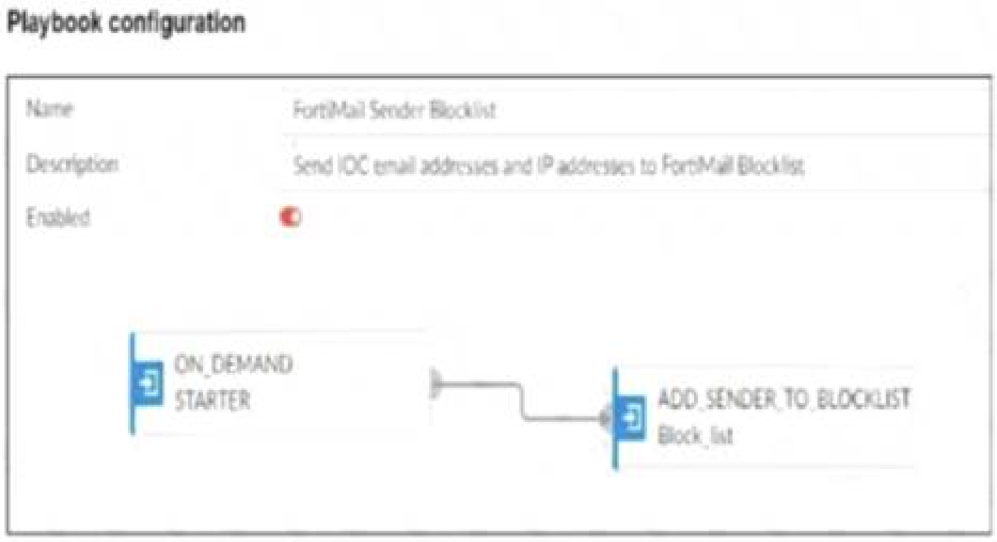
You are tasked with reviewing a new FortiAnalyzer deployment in a network with multiple registered logging devices. There is only one FortiAnalyzer in the topology.
Which potential problem do you observe?

A. The disk space allocated is insufficient.
B. The analytics-to-archive ratio is misconfigured.
C. The analytics retention period is too long.
D. The archive retention period is too long.

Answer: B

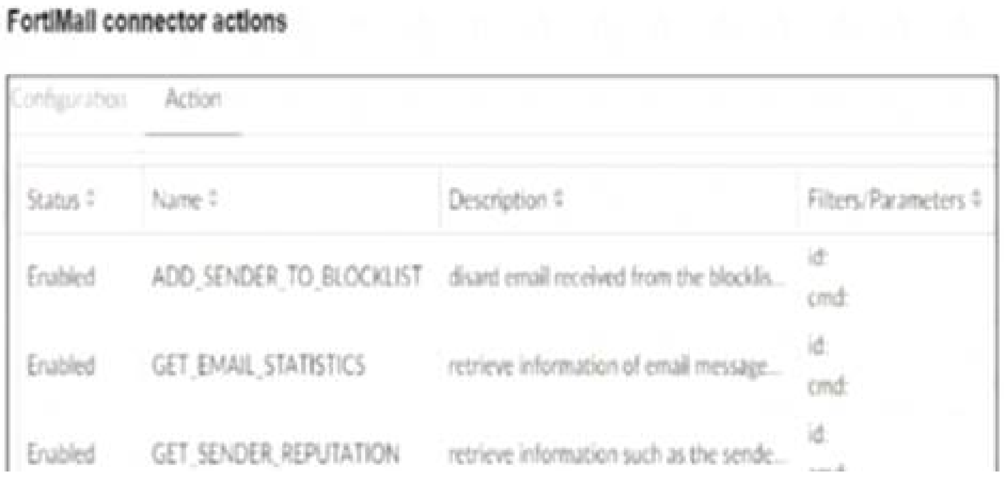
Explanation:
Understanding FortiAnalyzer Data Policy and Disk Utilization:
FortiAnalyzer uses data policies to manage log storage, retention, and disk utilization.
The Data Policy section indicates how long logs are kept for analytics and archive purposes.
The Disk Utilization section specifies the allocated disk space and the proportions used for analytics and archive, as well as when alerts should be triggered based on disk usage.
Analyzing the Provided Exhibit:
Keep Logs for Analytics:60 Days
Keep Logs for Archive:120 Days
Disk Allocation:300 GB (with a maximum of 441 GB available)
Analytics: Archive Ratio:30% : 70%
Alert and Delete When Usage Reaches:90%
Potential Problems Identification:
Disk Space Allocation:The allocated disk space is 300 GB out of a possible 441 GB, which might not be insufficient if the log volume is high, but it is not the primary concern based on the given data.
Analytics-to-Archive Ratio:The ratio of 30% for analytics and 70% for archive is unconventional. Typically, a higher percentage is allocated for analytics since real-time or recent data analysis is often prioritized. A common configuration might be a 70% analytics and 30% archive ratio. The misconfigured ratio can lead to insufficient space for analytics, causing issues with real-time monitoring and analysis.
Retention Periods:While the retention periods could be seen as lengthy, they are not necessarily indicative of a problem without knowing the specific log volume and compliance requirements. The length of these periods can vary based on organizational needs and legal requirements.
Conclusion:
Based on the analysis, the primary issue observed is theanalytics-to-archive ratiobeing misconfigured. This misconfiguration can significantly impact the effectiveness of the FortiAnalyzer in real-time log analysis, potentially leading to delayed threat detection and response.
References:
Fortinet Documentation on FortiAnalyzer Data Policies and Disk Management.
Best Practices for FortiAnalyzer Log Management and Disk Utilization.

NEW QUESTION 10
Refer to the exhibits.



Playbook configuration

Name	FortiMail Sender Blocklist
Description	Send IOC email addresses and IP addresses to FortiMail Blocklist
Enabled	●



FortiMail connector actions

Status ⇕	Name ⇕	Description ⇕	Filters/Parameters ⇕
Enabled	ADD_SENDER_TO_BLOCKLIST	disard email received from the blocklis...	id: cmd:
Enabled	GET_EMAIL_STATISTICS	retrieve information of email message...	id: cmd:
Enabled	GET_SENDER_REPUTATION	retrieve information such as the sende...	id:

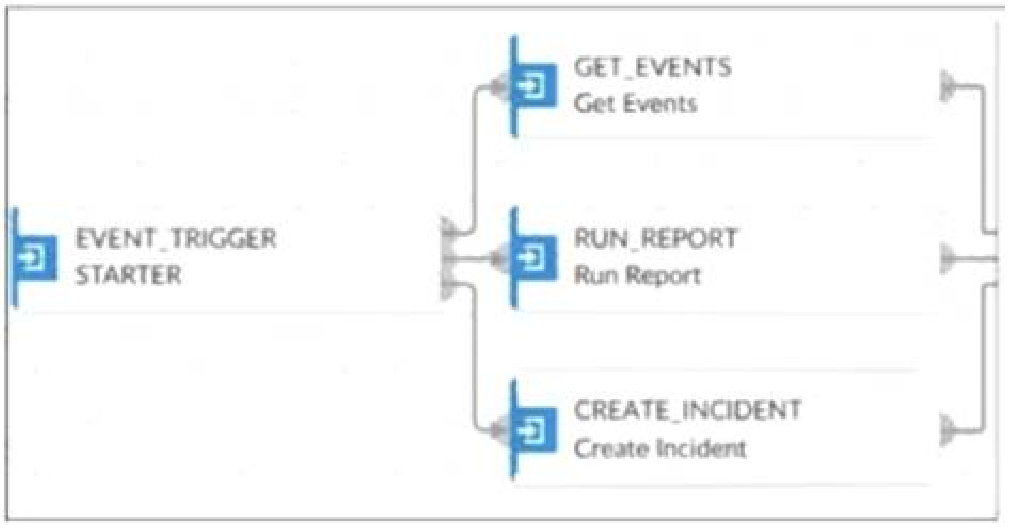
The FortiMail Sender Blocklist playbook is configured to take manual input and add those entries to the FortiMail abc. com domain-level block list. The playbook is configured to use a FortiMail connector and the ADD_SENDER_TO_BLOCKLIST action.
Why is the FortiMail Sender Blocklist playbook execution failing7

A. You must use the GET_EMAIL_STATISTICS action first to gather information about email messages.
B. FortiMail is expecting a fully qualified domain name (FQDN).
C. The client-side browser does not trust the FortiAnalzyer self-signed certificate.
D. The connector credentials are incorrect

Answer: B

Explanation:
Understanding the Playbook Configuration:
The playbook "FortiMail Sender Blocklist" is designed to manually input email addresses or IP addresses and add them to the FortiMail block list.
The playbook uses a FortiMail connector with the actionADD_SENDER_TO_BLOCKLIST.
Analyzing the Playbook Execution:
The configuration and actions provided show that the playbook is straightforward, starting with anON_DEMAND STARTERand proceeding to theADD_SENDER_TO_BLOCKLISTaction.
The action description indicates it is intended to block senders based on email addresses or domains.
Evaluating the Options:
Option A:UsingGET_EMAIL_STATISTICSis not required for the task of adding senders to a block list. This action retrieves email statistics and is unrelated to the block list configuration.
Option B:The primary reason for failure could be the requirement for a fully qualified domain name (FQDN). FortiMail typically expects precise information to ensure the correct entries are added to the block list.
Option C:The trust level of the client-side browser with FortiAnalyzer's self-signed certificate does not impact the execution of the playbook on FortiMail.
Option D:Incorrect connector credentials would result in an authentication error, but the problem described is more likely related to the format of the input data.
Conclusion:
The FortiMail Sender Blocklist playbook execution is failing because FortiMail is expecting a fully qualified domain name (FQDN).
References:
Fortinet Documentation on FortiMail Connector Actions.
Best Practices for Configuring FortiMail Block Lists.

NEW QUESTION 10
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 13
......