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
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.

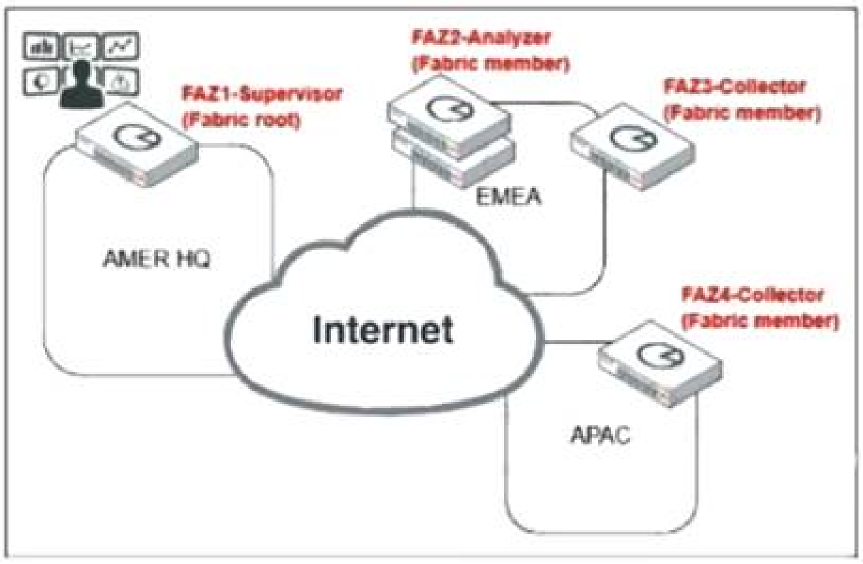
NEW QUESTION 2
Which role does a threat hunter play within a SOC?

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 3
Exhibit:



Which observation about this FortiAnalyzer Fabric deployment architecture is true?

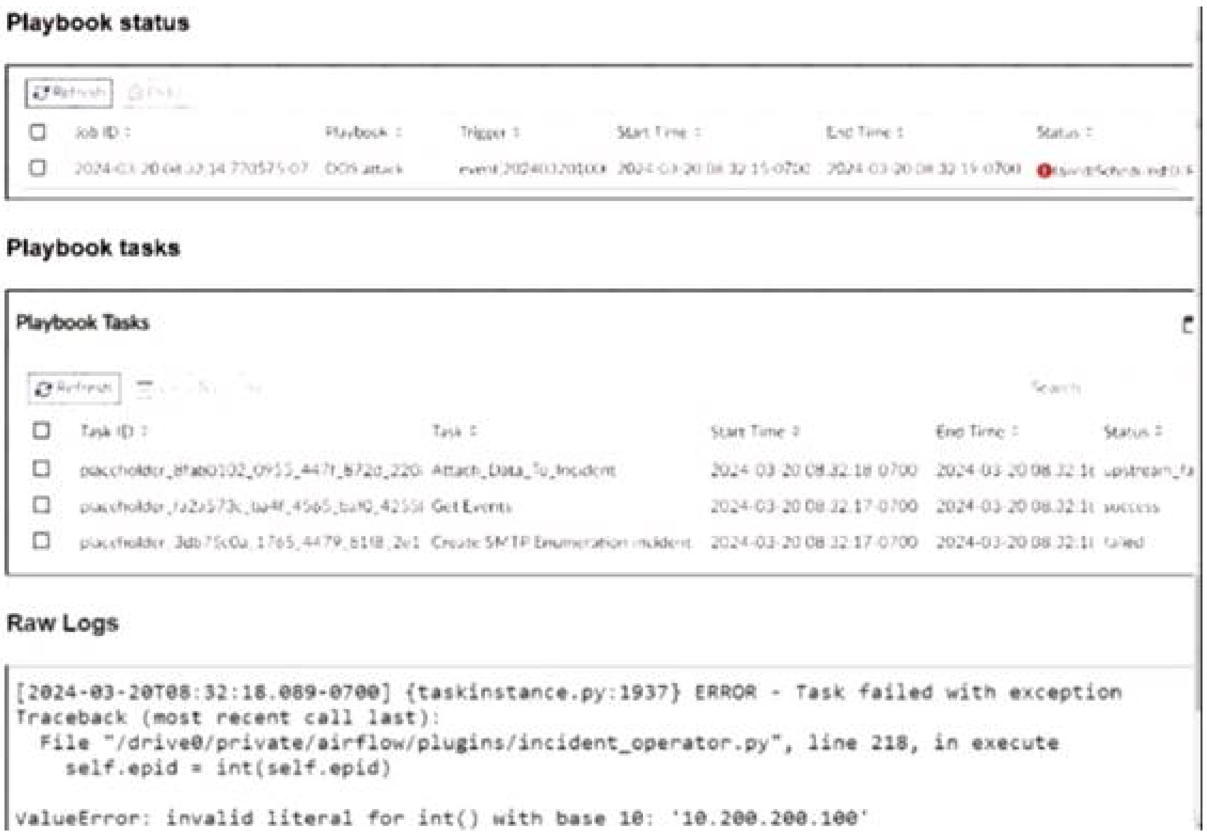
A. The AMER HQ SOC team cannot run automation playbooks from the Fabric supervisor.
B. The AMER HQ SOC team must configure high availability (HA) for the supervisor node.
C. The EMEA SOC team has access to historical logs only.
D. The APAC SOC team has access to FortiView and other reporting functions.

Answer: A

Explanation:

Understanding FortiAnalyzer Fabric Deployment:
FortiAnalyzer Fabric deployment involves a hierarchical structure where the Fabric root (supervisor) coordinates with multiple Fabric members (collectors and analyzers).
This setup ensures centralized log collection, analysis, and incident response across geographically distributed locations.
Analyzing the Exhibit:
FAZ1-Supervisoris located at AMER HQ and acts as the Fabric root.
FAZ2-Analyzeris a Fabric member located in EMEA.
FAZ3-CollectorandFAZ4-Collectorare Fabric members located in EMEA and APAC, respectively.
Evaluating the Options:
Option A:The statement indicates that the AMER HQ SOC team cannot run automation playbooks from the Fabric supervisor. This is true because automation playbooks and certain orchestration tasks typically require local execution capabilities which may not be fully supported on the supervisor node.
Option B:High availability (HA) configuration for the supervisor node is a best practice for redundancy but is not directly inferred from the given architecture.
Option C:The EMEA SOC team having access to historical logs only is not correct since FAZ2-Analyzer provides full analysis capabilities.
Option D:The APAC SOC team has access to FortiView and other reporting functions through FAZ4-Collector, but this is not explicitly detailed in the provided architecture.
Conclusion:
The most accurate observation about this FortiAnalyzer Fabric deployment architecture is that the AMER HQ SOC team cannot run automation playbooks from the Fabric supervisor.
References:
Fortinet Documentation on FortiAnalyzer Fabric Deployment.
Best Practices for FortiAnalyzer and Automation Playbooks.

NEW QUESTION 4
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 08:32:15-0700	● [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_ba90_4255	Get Events	2024-03-20 08:32:17-0700	2024-03-20 08:32:1	success
□	placeholder_3db75c0a_1765_4479_818_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_lncident task failed.
D. The Attach_Data_To_lncident 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.

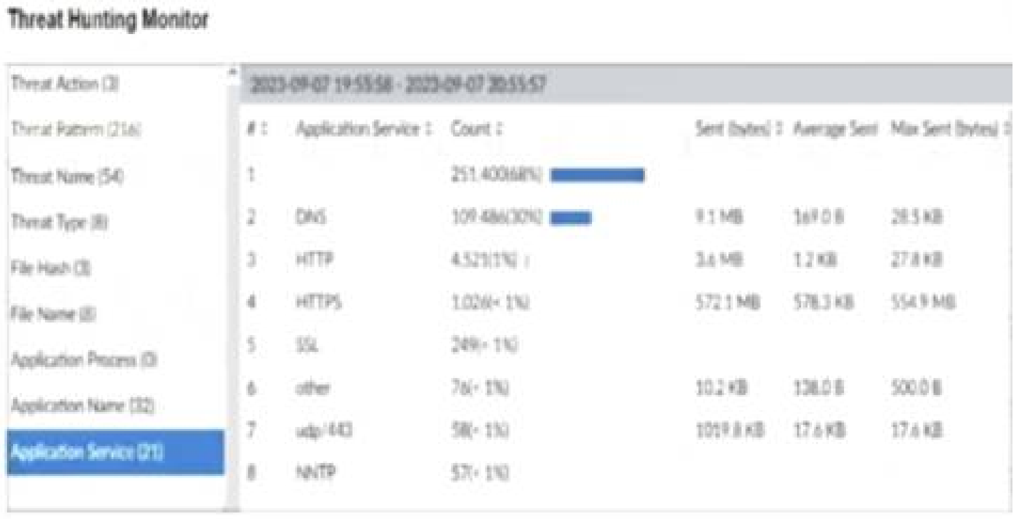
NEW QUESTION 5
Which FortiAnalyzer feature uses the SIEM database for advance log analytics and monitoring?

A. Threat hunting
B. Asset Identity Center
C. Event monitor
D. Outbreak alerts

Answer: A

Explanation:
Understanding FortiAnalyzer Features:
FortiAnalyzer includes several features for log analytics, monitoring, and incident response.
The SIEM (Security Information and Event Management) database is used to store and analyze log data, providing advanced analytics and insights.
Evaluating the Options:
Option A: Threat hunting
Threat hunting involves proactively searching through log data to detect and isolate threats that may not be captured by automated tools.
This feature leverages the SIEM database to perform advanced log analytics, correlate events, and identify potential security incidents.
Option B: Asset Identity Center
This feature focuses on asset and identity management rather than advanced log analytics.
Option C: Event monitor
While the event monitor provides real-time monitoring and alerting based on logs, it does not specifically utilize advanced log analytics in the way the SIEM database does for threat hunting.
Option D: Outbreak alerts
Outbreak alerts provide notifications about widespread security incidents but are not directly related to advanced log analytics using the SIEM database.
Conclusion:
The feature that uses the SIEM database for advanced log analytics and monitoring in
FortiAnalyzer isThreat hunting.
References:
Fortinet Documentation on FortiAnalyzer Features and SIEM Capabilities.
Security Best Practices and Use Cases for Threat Hunting.

NEW QUESTION 6
Refer to the exhibits.

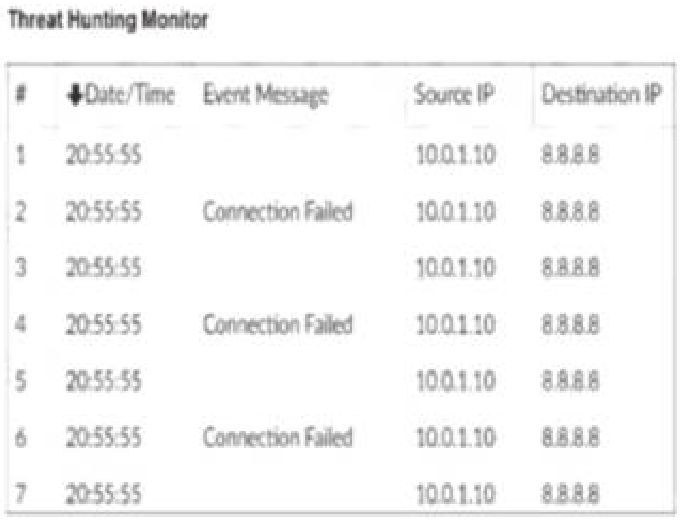


Threat Hunting Monitor

Threat Action (3)
Threat Pattern (216)
Threat Name (54)
Threat Type (8)
File Hash (3)
File Name (8)
Application Process (0)
Application Name (32)
Application Service (21)

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?

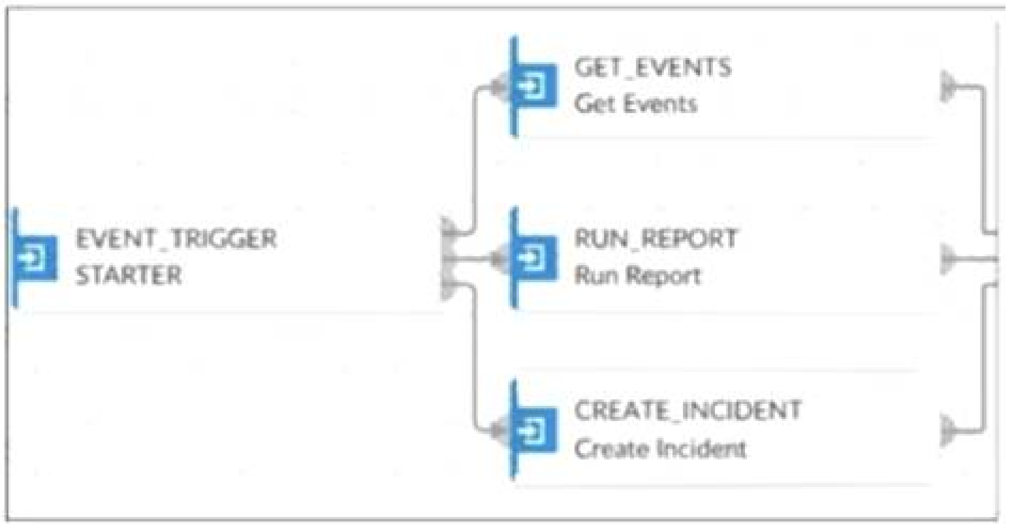
A. Spearphishing is being used to elicit sensitive information.
B. DNS tunneling is being used to extract confidential data from the local network.
C. Reconnaissance is being used to gather victim identityinformation from the mail server.
D. FTP is being used as command-and-control (C&C) technique to 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 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 10

......