

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

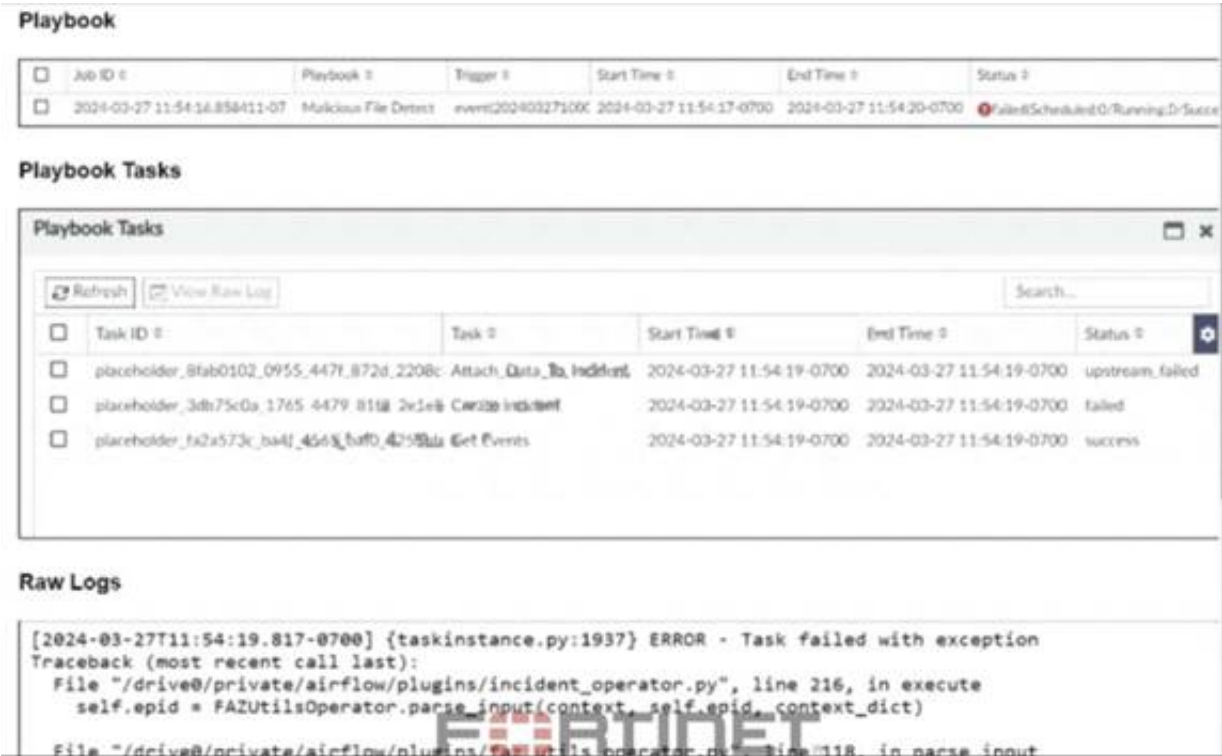
Answer: A

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

Refer to the exhibits.



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 was expecting 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 as Attach_Data_To_Incident, Create Incident, and Get Events.
Analyzing the Playbook Execution:
The exhibit shows that the Create Incident task has failed, and the Attach_Data_To_Incident task has also failed. The Get Events task succeeded, indicating that it was able to retrieve event data.
Reviewing Raw Logs:
The raw logs indicate an error related to parsing input in the incident_operator.py file. 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:
The Create Incident task failure is the root cause since it did not proceed correctly due to incorrect input format. The Attach_Data_To_Incident task subsequently failed because it depends on the successful creation of an incident.
Conclusion:
The primary reason for the playbook execution failure is that the Create Incident task 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 3

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 4

Review the following incident report:

Attackers leveraged a phishing email campaign targeting your employees.

The email likely impersonated a trusted source, such as the IT department, and requested login credentials. An unsuspecting employee clicked a malicious link in the email, leading to the download and execution of a Remote Access Trojan (RAT).

The RAT provided the attackers with remote access and a foothold in the compromised system. Which two MITRE ATT&CK tactics does this incident report capture? (Choose two.)

- A. Initial Access
- B. Defense Evasion
- C. Lateral Movement
- D. Persistence

Answer: AD

Explanation:

Understanding the MITRE ATT&CK Tactics:

The MITRE ATT&CK framework categorizes various tactics and techniques used by adversaries to achieve their objectives.

Tactics represent the objectives of an attack, while techniques represent how those objectives are achieved.

Analyzing the Incident Report:

Phishing Email Campaign: This tactic is commonly used for gaining initial access to a system.

Malicious Link and RAT Download: Clicking a malicious link and downloading a RAT is indicative of establishing initial access.

Remote Access Trojan (RAT): Once installed, the RAT allows attackers to maintain access over an extended period, which is a persistence tactic.

Mapping to MITRE ATT&CK Tactics:

Initial Access:

This tactic covers techniques used to gain an initial foothold within a network.

Techniques include phishing and exploiting external remote services.

The phishing campaign and malicious link click fit this category.

Persistence:

This tactic includes methods that adversaries use to maintain their foothold.

Techniques include installing malware that can survive reboots and persist on the system.

The RAT provides persistent remote access, fitting this tactic.

Exclusions:

Defense Evasion:

This involves techniques to avoid detection and evade defenses.

While potentially relevant in a broader context, the incident report does not specifically describe actions taken to evade defenses.

Lateral Movement:

This involves moving through the network to other systems.

The report does not indicate actions beyond initial access and maintaining that access.

Conclusion:

The incident report captures the tactics of Initial Access and Persistence.

References:

MITRE ATT&CK Framework documentation on Initial Access and Persistence tactics.

Incident analysis and mapping to MITRE ATT&CK tactics.

NEW QUESTION 5

Which three end user logs does FortiAnalyzer use to identify possible IOC compromised hosts? (Choose three.)

- A. Email filter logs
- B. DNS filter logs
- C. Application filter logs
- D. IPS logs
- E. Web filter logs

Answer: BDE

Explanation:

Overview of Indicators of Compromise (IoCs): Indicators of Compromise (IoCs) are pieces of evidence that suggest a system may have been compromised. These can include unusual network traffic patterns, the presence of known malicious files, or other suspicious activities.

FortiAnalyzer's Role: FortiAnalyzer aggregates logs from various Fortinet devices to provide comprehensive visibility and analysis of network events. It uses these logs to identify potential IoCs and compromised hosts.

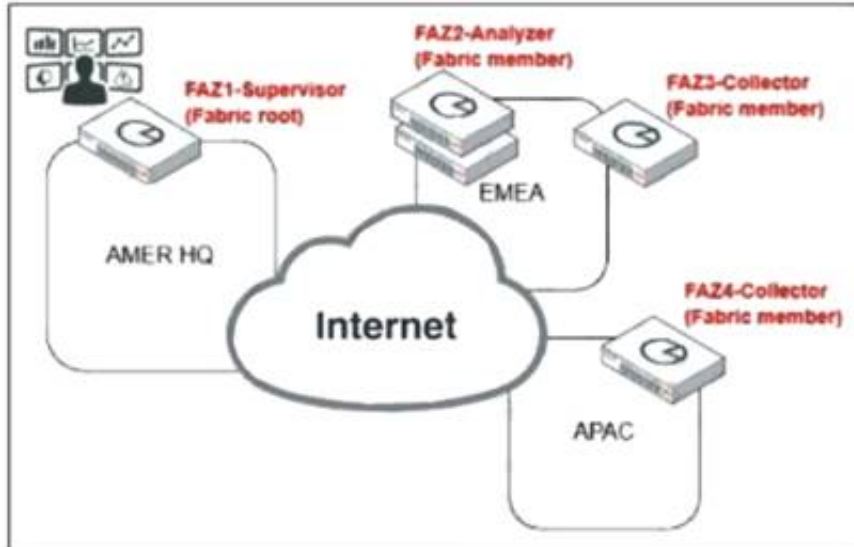
Relevant Log Types:

DNS Filter Logs:

DNS requests are a common vector for malware communication. Analyzing DNS filter logs helps in identifying suspicious domain queries, which can indicate malware attempting to communicate with command and control (C2) servers.

NEW QUESTION 6

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-Supervisor is located at AMER HQ and acts as the Fabric root.

FAZ2-Analyzer is a Fabric member located in EMEA.

FAZ3-Collector and FAZ4-Collector are 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 7

Which two types of variables can you use in playbook tasks? (Choose two.)

- A. input
- B. Output
- C. Create
- D. Trigger

Answer: AB

Explanation:

Understanding Playbook Variables:

Playbook tasks in Security Operations Center (SOC) playbooks use variables to pass and manipulate data between different steps in the automation process.

Variables help in dynamically handling data, making the playbook more flexible and adaptive to different scenarios.

Types of Variables:

Input Variables:

Input variables are used to provide data to a playbook task. These variables can be set manually or derived from previous tasks.

They act as parameters that the task will use to perform its operations.

Output Variables:

Output variables store the result of a playbook task. These variables can then be used as inputs for subsequent tasks.

They capture the outcome of the task's execution, allowing for the dynamic flow of information through the playbook.

Other Options:

Create: Not typically referred to as a type of variable in playbook tasks. It might refer to an action but not a variable type.

Trigger: Refers to the initiation mechanism of the playbook or task (e.g., an event trigger), not a type of variable.

Conclusion:

The two types of variables used in playbook tasks are input and output.

References:

Fortinet Documentation on Playbook Configuration and Variable Usage.

General SOC Automation and Orchestration Practices.

NEW QUESTION 8

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 9

Which statement describes automation stitch integration between FortiGate and FortiAnalyzer?

- A. An event handler on FortiAnalyzer executes an automation stitch when an event is created.
- B. An automation stitch is configured on FortiAnalyzer and mapped to FortiGate using the FortiOS connector.
- C. An event handler on FortiAnalyzer is configured to send a notification to FortiGate to trigger an automation stitch.
- D. A security profile on FortiGate triggers a violation and FortiGate sends a webhook call to FortiAnalyzer.

Answer: D

Explanation:

Overview of Automation Stitches: Automation stitches in Fortinet solutions enable automated responses to specific events detected within the network. This automation helps in swiftly mitigating threats without manual intervention.

FortiGate Security Profiles:

FortiGate uses security profiles to enforce policies on network traffic. These profiles can include antivirus, web filtering, intrusion prevention, and more.

When a security profile detects a violation or a specific event, it can trigger predefined actions.

Webhook Calls:

FortiGate can be configured to send webhook calls upon detecting specific security events.

A webhook is an HTTP callback triggered by an event, sending data to a specified URL. This allows FortiGate to communicate with other systems, such as FortiAnalyzer.

FortiAnalyzer Integration:

FortiAnalyzer collects logs and events from various Fortinet devices, providing centralized logging and analysis.

Upon receiving a webhook call from FortiGate, FortiAnalyzer can further analyze the event, generate reports, and take automated actions if configured to do so.

Detailed Process:

Step 1: A security profile on FortiGate triggers a violation based on the defined security policies.

Step 2: FortiGate sends a webhook call to FortiAnalyzer with details of the violation.

Step 3: FortiAnalyzer receives the webhook call and logs the event.

Step 4: Depending on the configuration, FortiAnalyzer can execute an automation stitch to respond to the event, such as sending alerts, generating reports, or triggering further actions.

References:

Fortinet Documentation: FortiOS Automation Stitches

FortiAnalyzer Administration Guide: Details on configuring event handlers and integrating with FortiGate.

FortiGate Administration Guide: Information on security profiles and webhook configurations. By understanding the interaction between FortiGate and FortiAnalyzer through webhook calls and automation

stitches, security operations can ensure a proactive and efficient response to security events.

NEW QUESTION 10

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 10

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 11

Refer to the exhibits.

Playbook status

Job ID	Playbook	Trigger	Start Time	End Time	Status
2024-03-20 08:32:14 770525-07	DOS attack	event:202403201008	2024-03-20 08:32:15-0700	2024-03-20 08:32:15-0700	Failed (Status: Failed)

Playbook tasks

Task ID	Task	Start Time	End Time	Status
paccholder_8fab0102_0955_447f_872d_220	Attach_Data_To_Incident	2024-03-20 08:32:18-0700	2024-03-20 08:32:18-0700	upstream_fa
paccholder_fa2a573c_ba4f_4565_ba10_4255a	Get Events	2024-03-20 08:32:17-0700	2024-03-20 08:32:18-0700	success
paccholder_3db75c0a_1765_4479_81b8_2e1	Create SMTP Enumeration incident	2024-03-20 08:32:17-0700	2024-03-20 08:32:18-0700	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 12

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

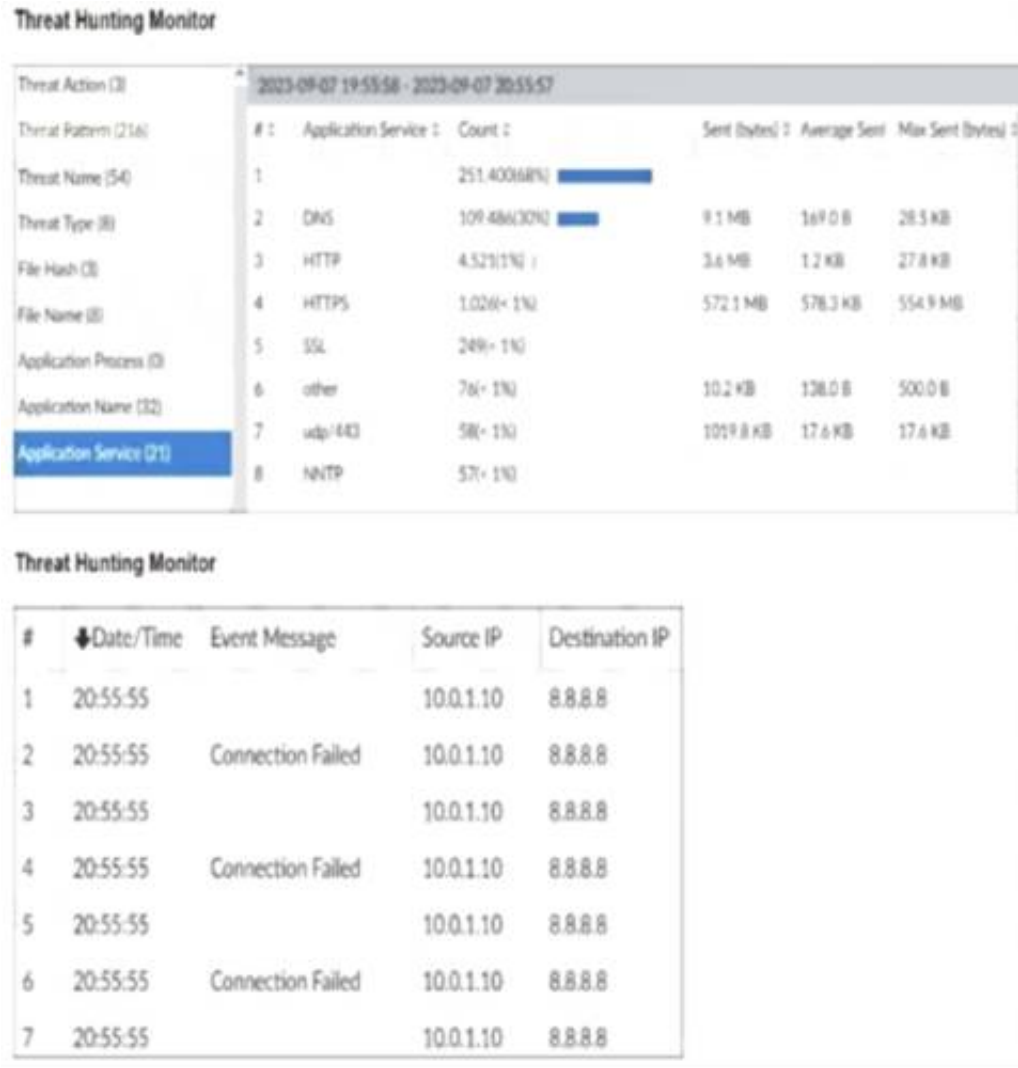
Answer: A

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 14

Refer to the exhibits.



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 identity information 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 15

Refer to the exhibit.



Which two options describe how the Update Asset and Identity Database playbook is configured? (Choose two.)

- A. The playbook is using a local connector.
- B. The playbook is using a FortiMail connector.
- C. The playbook is using an on-demand trigger.
- D. The playbook is using a FortiClient EMS connector.

Answer: AD

Explanation:

Understanding the Playbook Configuration:

The playbook named "Update Asset and Identity Database" is designed to update the FortiAnalyzer Asset and Identity database with endpoint and user information.

The exhibit shows the playbook with three main components: ON_SCHEDULE STARTER, GET_ENDPOINTS, and UPDATE_ASSET_AND_IDENTITY.

Analyzing the Components:

ON_SCHEDULE STARTER: This component indicates that the playbook is triggered on a schedule, not on-demand.

GET_ENDPOINTS: This action retrieves information about endpoints, suggesting it interacts with an endpoint management system.

UPDATE_ASSET_AND_IDENTITY: This action updates the FortiAnalyzer Asset and Identity database with the retrieved information.

Evaluating the Options:

Option A: The actions shown in the playbook are standard local actions that can be executed by the FortiAnalyzer, indicating the use of a local connector.

Option B: There is no indication that the playbook uses a FortiMail connector, as the tasks involve endpoint and identity management, not email.

Option C: The playbook is using an "ON_SCHEDULE" trigger, which contradicts the description of an on-demand trigger.

Option D: The action "GET_ENDPOINTS" suggests integration with an endpoint management system, likely FortiClient EMS, which manages endpoints and

retrieves information from them.
Conclusion:
The playbook is configured to use a local connector for its actions.
It interacts with FortiClient EMS to get endpoint information and update the FortiAnalyzer Asset and Identity database.
References:
Fortinet Documentation on Playbook Actions and Connectors.
FortiAnalyzer and FortiClient EMS Integration Guides.

NEW QUESTION 20
Refer to Exhibit:



A SOC analyst is designing a playbook to filter for a high severity event and attach the event information to an incident. Which local connector action must the analyst use in this scenario?

A. Get Events
B. Update Incident
C. Update Asset and Identity
D. Attach Data to Incident

Answer: D

Explanation:

Understanding the Playbook Requirements:
The SOC analyst needs to design a playbook that filters for high severity events.
The playbook must also attach the event information to an existing incident.
Analyzing the Provided Exhibit:
The exhibit shows the available actions for a local connector within the playbook.
Actions listed include:
Update Asset and Identity
Get Events
Get Endpoint Vulnerabilities
Create Incident
Update Incident
Attach Data to Incident
Run Report
Get EPEU from Incident
Evaluating the Options:
Get Events:This action retrieves events but does not attach them to an incident.
Update Incident:This action updates an existing incident but is not specifically for attaching event data.
Update Asset and Identity:This action updates asset and identity information, not relevant for attaching event data to an incident.
Attach Data to Incident:This action is explicitly designed to attach additional data, such as event information, to an existing incident.
Conclusion:
The correct action to use in the playbook for filtering high severity events and attaching the event information to an incident isAttach Data to Incident.
References:
Fortinet Documentation on Playbook Actions and Connectors.
Best Practices for Incident Management and Playbook Design in SOC Operations.

NEW QUESTION 25
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

FCSS_SOC_AN-7.4 Practice Exam Features:

- * FCSS_SOC_AN-7.4 Questions and Answers Updated Frequently
- * FCSS_SOC_AN-7.4 Practice Questions Verified by Expert Senior Certified Staff
- * FCSS_SOC_AN-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCSS_SOC_AN-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The FCSS_SOC_AN-7.4 Practice Test Here](#)