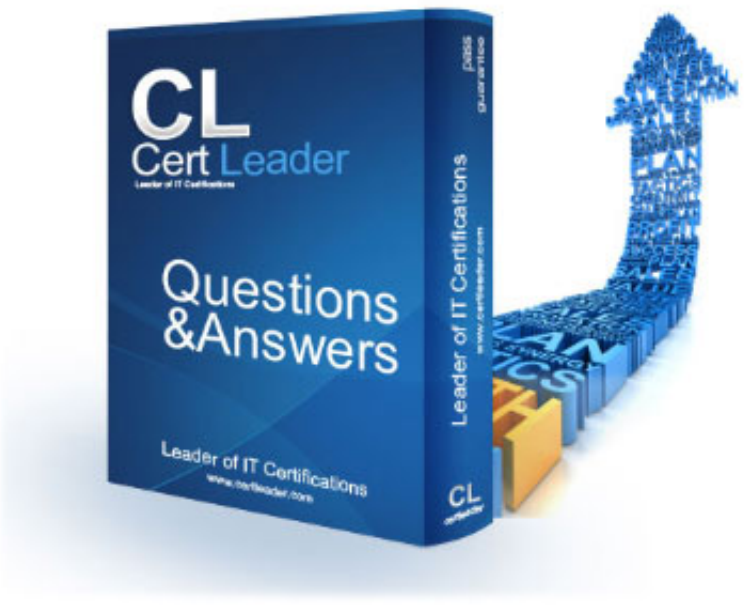
FCSS_SOC_AN-7.4 Dumps

FCSS - Security Operations 7.4 Analyst

https://www.certleader.com/FCSS_SOC_AN-7.4-dumps.html



NEW QUESTION 1
Refer to the exhibit,

which shows the partial output of the MITRE ATT&CK Enterprise matrix on FortiAnalyzer. Which two statements are true? (Choose two.)

A. There are four techniques that fall under tactic T1071.
B. There are four subtechniques that fall under technique T1071.
C. There are event handlers that cover tactic T1071.
D. There are 15 events associated with the tactic.

Answer: BC

Explanation:
Understanding the MITRE ATT&CK Matrix:
The MITRE ATT&CK framework is a knowledge base of adversary tactics and techniques based on real-world observations.
Each tactic in the matrix represents the "why" of an attack technique, while each technique represents "how" an adversary achieves a tactic.
Analyzing the Provided Exhibit:
The exhibit shows part of the MITRE ATT&CK Enterprise matrix as displayed on FortiAnalyzer.
The focus is on technique T1071 (Application Layer Protocol), which has subtechniques labeled T1071.001, T1071.002, T1071.003, and T1071.004.
Each subtechnique specifies a different type of application layer protocol used for Command and Control (C2):
T1071.001 Web Protocols
T1071.002 File Transfer Protocols
T1071.003 Mail Protocols
T1071.004 DNS
Identifying Key Points:
Subtechniques under T1071:There are four subtechniques listed under the primary technique T1071, confirming that statement B is true.
Event Handlers for T1071:FortiAnalyzer includes event handlers for monitoring various tactics and techniques. The presence of event handlers for tactic T1071 suggests active monitoring and alerting for these specific subtechniques, confirming that statement C is true.
Misconceptions Clarified:
Statement A (four techniques under tactic T1071) is incorrect because T1071 is a single technique with four subtechniques.
Statement D (15 events associated with the tactic) is misleading. The number 15 refers to the techniques under the Application Layer Protocol, not directly related to the number of events.
Conclusion:
The accurate interpretation of the exhibit confirms that there are four subtechniques under technique T1071 and that there are event handlers covering tactic T1071.
References:
MITRE ATT&CK Framework documentation.
FortiAnalyzer Event Handling and MITRE ATT&CK Integration guides.

NEW QUESTION 2
Refer to the exhibits.

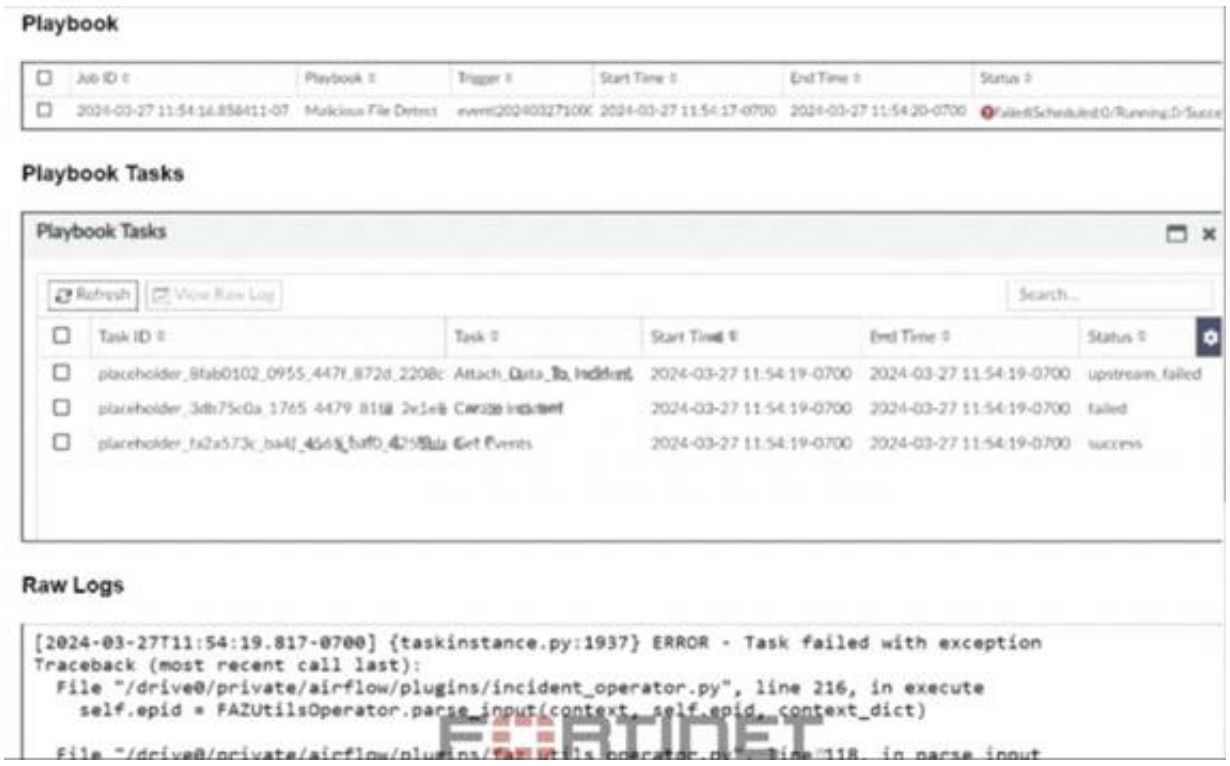
You configured a spearphishing event handler and the associated rule. However. FortiAnalyzer did not generate an event.
When you check the FortiAnalyzer log viewer, you confirm that FortiSandbox forwarded the appropriate logs, as shown in the raw log exhibit.
What configuration must you change on FortiAnalyzer 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 lwa 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 3
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 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
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 ofInitial AccessandPersistence.
References:
MITRE ATT&CK Framework documentation on Initial Access and Persistence tactics.
Incident analysis and mapping to MITRE ATT&CK tactics.

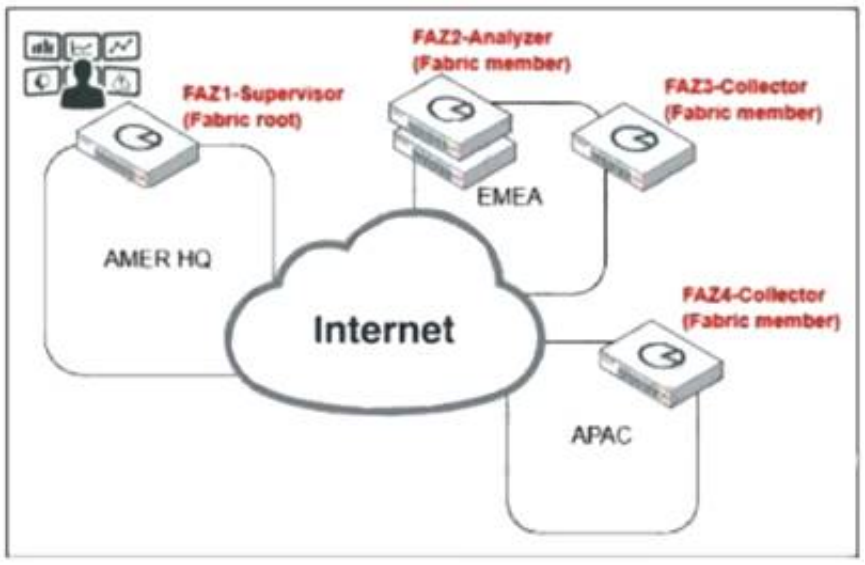
NEW QUESTION 6
Your company is doing a security audit To pass the audit, you must take an inventory of all software and applications running on all Windows devices
Which FortiAnalyzer connector must you use?

A. FortiClient EMS
B. ServiceNow
C. FortiCASB
D. Local Host

Answer: A

Explanation:
Requirement Analysis:
The objective is to inventory all software and applications running on all Windows devices within the organization.
This inventory must be comprehensive and accurate to pass the security audit.
Key Components:
FortiClient EMS (Endpoint Management Server):
FortiClient EMS provides centralized management of endpoint security, including software
and application inventory on Windows devices.
It allows administrators to monitor, manage, and report on all endpoints protected by FortiClient.
Connector Options:
FortiClient EMS:
Best suited for managing and reporting on endpoint software and applications.
Provides detailed inventory reports for all managed endpoints.
Selected as it directly addresses the requirement of taking inventory of software and applications on Windows devices.
ServiceNow:
Primarily a service management platform.
While it can be used for asset management, it is not specifically tailored for endpoint software inventory.
Not selected as it does not provide direct endpoint inventory management.
FortiCASB:
Focuses on cloud access security and monitoring SaaS applications.
Not applicable for managing or inventorying endpoint software.
Not selected as it is not related to endpoint software inventory.
Local Host:
Refers to handling events and logs within FortiAnalyzer itself.
Not specific enough for detailed endpoint software inventory.
Not selected as it does not provide the required endpoint inventory capabilities.
Implementation Steps:
Step 1: Ensure all Windows devices are managed by FortiClient and connected to FortiClient EMS.
Step 2: Use FortiClient EMS to collect and report on the software and applications installed on these devices.
Step 3: Generate inventory reports from FortiClient EMS to meet the audit requirements.
References:
Fortinet Documentation on FortiClient EMS FortiClient EMS Administration Guide
By using the FortiClient EMS connector, you can effectively inventory all software and applications on Windows devices, ensuring compliance with the security audit requirements.

NEW QUESTION 7
Exhibit:



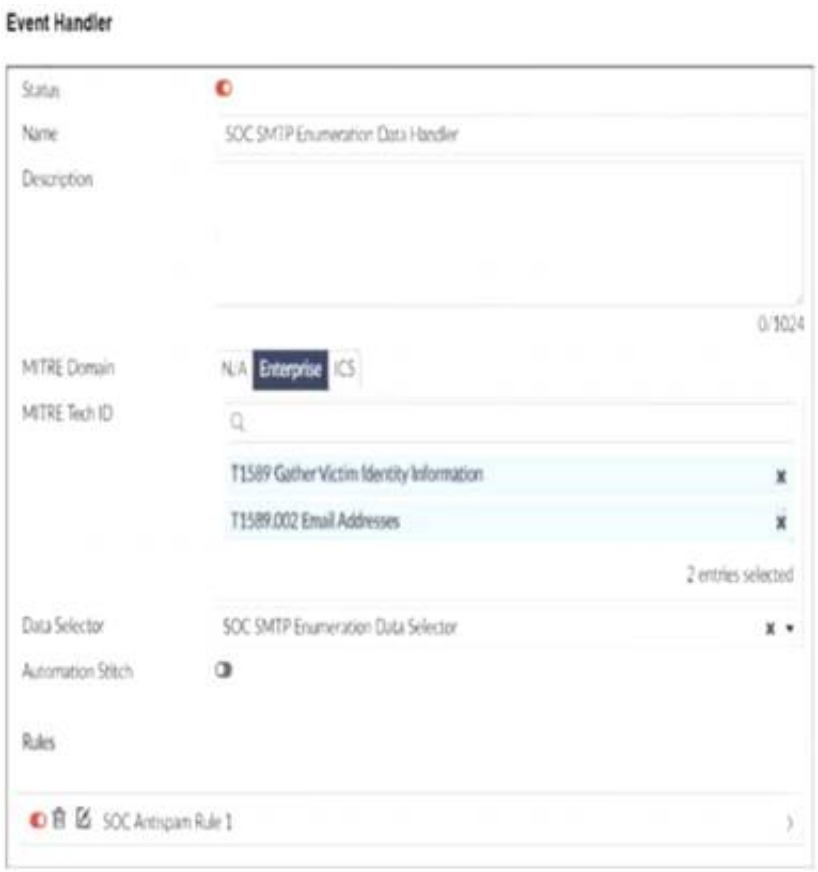
Which observation about this FortiAnalyzer Fabric deployment architecture is true?

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 8
Refer to the exhibits.



You configured a custom event handler and an associated rule to generate events whenever FortiMail detects spam emails. However, you notice that the event handler is generating events for both spam emails and clean emails.
Which change must you make in the rule so that it detects only spam emails?

A. In the Log Type field, select Anti-Spam Log (spam)
B. Disable the rule to use the filter in the data selector to create the event.
C. In the Trigger an event when field, select Within a group, the log field Spam Name (snane) has 2 or more unique values.

Answer: A

Explanation:
Understanding the Custom Event Handler Configuration:
The event handler is set up to generate events based on specific log data.
The goal is to generate events specifically for spam emails detected by FortiMail.
Analyzing the Issue:
The event handler is currently generating events for both spam emails and clean emails.
This indicates that the rule's filtering criteria are not correctly distinguishing between spam and non-spam emails.
Evaluating the Options:
Option A:Selecting the "Anti-Spam Log (spam)" in the Log Type field will ensure that only logs related to spam emails are considered. This is the most straightforward and accurate way to filter for spam emails.
Option B:Typingtype==spamin the Log filter by Text field might help filter the logs, but it is not as direct and reliable as selecting the correct log type.
Option C:Disabling the rule to use the filter in the data selector to create the event does not address the issue of filtering for spam logs specifically.
Option D:Selecting "Within a group, the log field Spam Name (snane) has 2 or more unique values" is not directly relevant to filtering spam logs and could lead to incorrect filtering criteria.
Conclusion:
The correct change to make in the rule is to select "Anti-Spam Log (spam)" in the Log Type field.
This ensures that the event handler only generates events for spam emails.
References:
Fortinet Documentation on Event Handlers and Log Types.
Best Practices for Configuring FortiMail Anti-Spam Settings.

NEW QUESTION 9
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 areinputandoutput.
References:
Fortinet Documentation on Playbook Configuration and Variable Usage.
General SOC Automation and Orchestration Practices.

NEW QUESTION 10
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 13
Refer to the exhibits.

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 17
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 19
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?

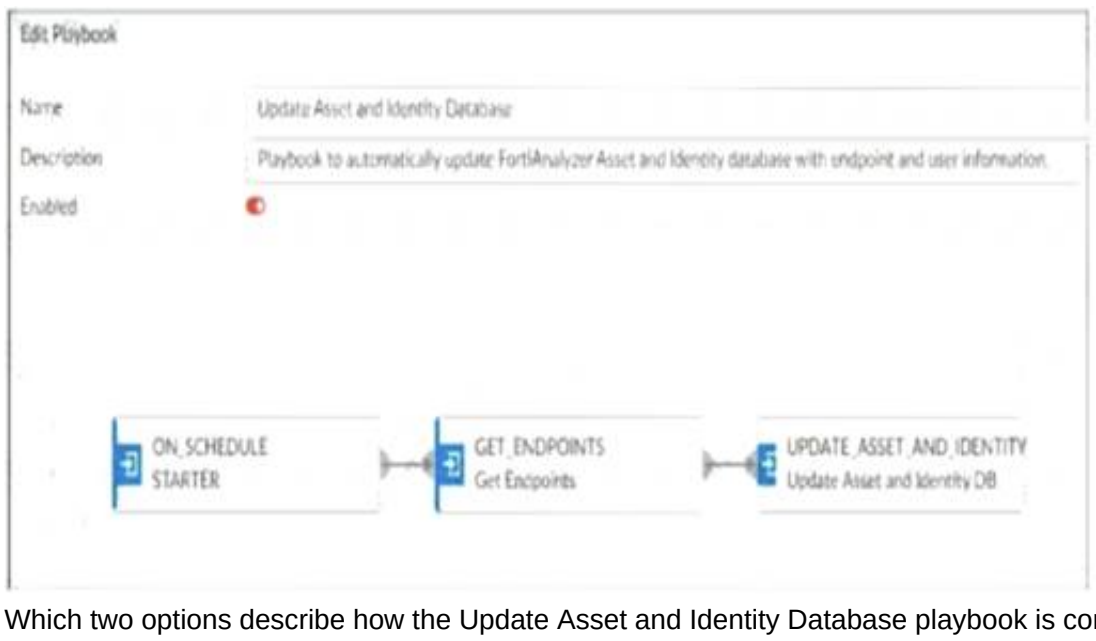
A. FortiSandbox connector
B. FortiClient EMS connector
C. FortiMail connector
D. Local connector

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 24
Refer to the exhibit.



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

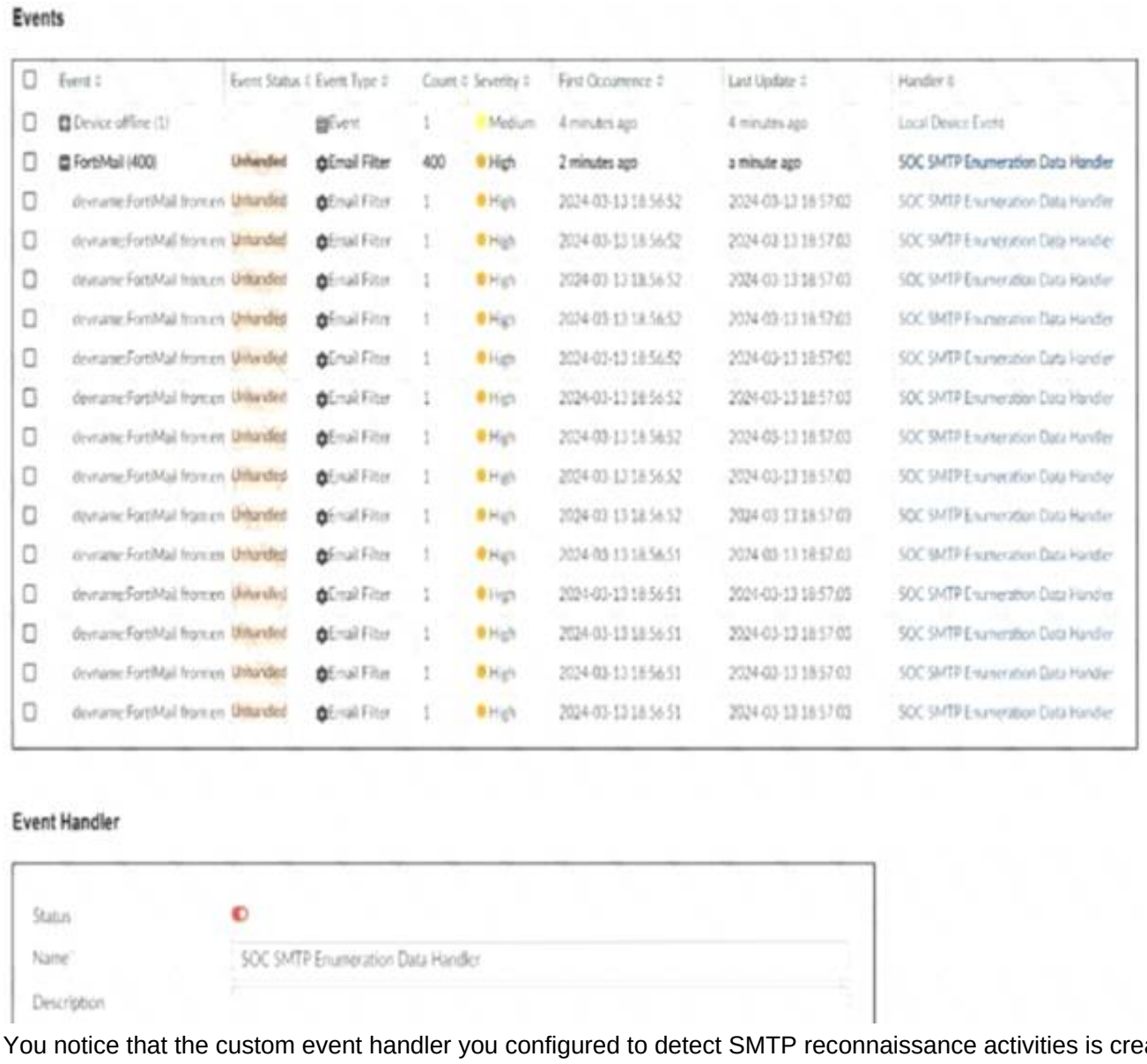
A. The playbook is using a local connector.
B. The playbook is using a FortiMail connector.
C. The playbook is using an on-demand trigger.
D. The playbook is using a FortiClient EMS connector.

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 27
Refer to the exhibit.



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 30
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your FCSS_SOC_AN-7.4 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCSS_SOC_AN-7.4-dumps.html