Fortinet

Exam Questions FCSS_SOC_AN-7.4

FCSS - Security Operations 7.4 Analyst

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

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

Answer: AB

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

NEW QUESTION 2
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 3
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 4
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 5
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 6
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 7
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 8
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

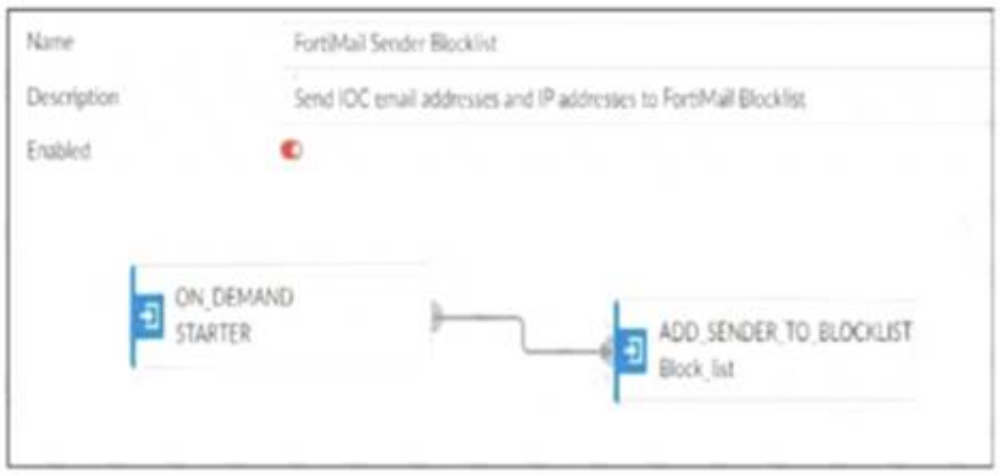
Answer: A

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 9
Refer to the exhibits.

Playbook configuration



FortiMail connector actions

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.

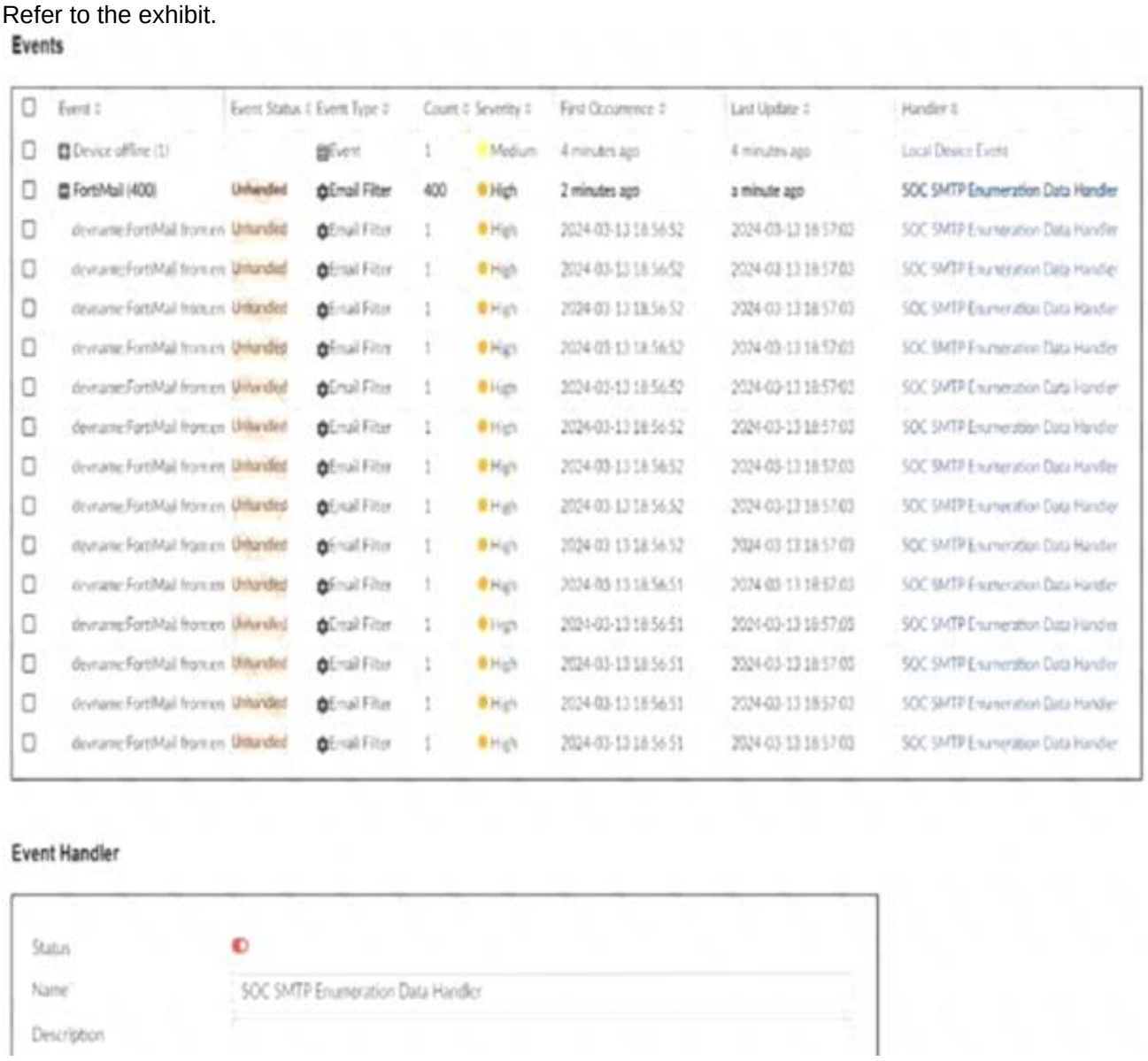
NEW QUESTION 10
Which two statements about the FortiAnalyzer Fabric topology are true? (Choose two.)

A. Downstream collectors can forward logs to Fabric members.
B. Logging devices must be registered to the supervisor.
C. The supervisor uses an API to store logs, incidents, and events locally.
D. Fabric members must be in analyzer mode.

Answer: BD

Explanation:
The FortiAnalyzer Fabric topology is designed to centralize logging and analysis across multiple devices in a network.
It involves a hierarchy where the supervisor node manages and coordinates with other Fabric members.
Analyzing the Options:
Option A:Downstream collectors forwarding logs to Fabric members is not a typical configuration. Instead, logs are usually centralized to the supervisor.
Option B:For effective management and log centralization, logging devices must be registered to the supervisor. This ensures proper log collection and coordination.
Option C:The supervisor does not primarily use an API to store logs, incidents, and events locally. Logs are stored directly in the FortiAnalyzer database.
Option D:For the Fabric topology to function correctly, all Fabric members need to be in analyzer mode. This mode allows them to collect, analyze, and forward logs appropriately within the topology.
Conclusion:
The correct statements regarding the FortiAnalyzer Fabric topology are that logging devices must be registered to the supervisor and that Fabric members must be in analyzer mode.
References:
Fortinet Documentation on FortiAnalyzer Fabric Topology.
Best Practices for Configuring FortiAnalyzer in a Fabric Environment.

NEW QUESTION 12
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 15
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 18
.....

Relate Links

100% Pass Your FCSS_SOC_AN-7.4 Exam with Exambible Prep Materials

https://www.exambible.com/FCSS_SOC_AN-7.4-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/