

Exam Questions FCSS_SOC_AN-7.4

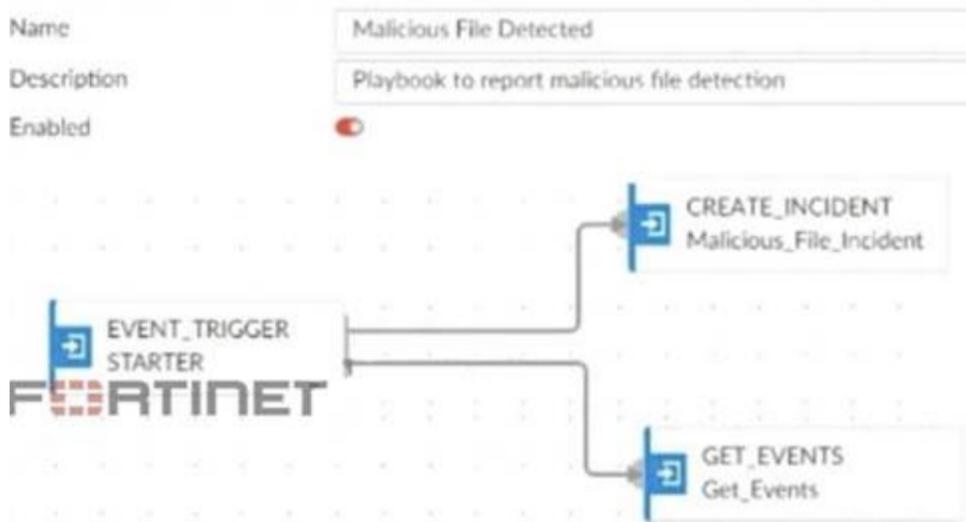
FCSS - Security Operations 7.4 Analyst

https://www.2passeasy.com/dumps/FCSS_SOC_AN-7.4/



NEW QUESTION 1

Refer to Exhibit:



A SOC analyst is creating the Malicious File Detected playbook to run when FortiAnalyzer generates a malicious file event. The playbook must also update the incident with the malicious file event data. What must the next task in this playbook be?

- A. A local connector with the action Update Asset and Identity
- B. A local connector with the action Attach Data to Incident
- C. A local connector with the action Run Report
- D. A local connector with the action Update Incident

Answer: D

Explanation:

Understanding the Playbook and its Components:

The exhibit shows a playbook in which an event trigger starts actions upon detecting a malicious file.

The initial tasks in the playbook include CREATE_INCIDENT and GET_EVENTS.

Analysis of Current Tasks:

EVENT_TRIGGER STARTER: This initiates the playbook when a specified event (malicious file detection) occurs.

CREATE_INCIDENT: This task likely creates a new incident in the incident management system for tracking and response.

GET_EVENTS: This task retrieves the event details related to the detected malicious file.

Objective of the Next Task:

The next logical step after creating an incident and retrieving event details is to update the incident with the event data, ensuring all relevant information is attached to the incident record.

This helps SOC analysts by consolidating all pertinent details within the incident record, facilitating efficient tracking and response.

Evaluating the Options:

Option A: Update Asset and Identity is not directly relevant to attaching event data to the incident.

Option B: Attach Data to Incident sounds plausible but typically, updating an incident involves more comprehensive changes including status updates, adding comments, and other data modifications.

Option C: Run Report is irrelevant in this context as the goal is to update the incident with event data.

Option D: Update Incident is the most suitable action for incorporating event data into the existing incident record.

Conclusion:

The next task in the playbook should be to update the incident with the event data to ensure the incident reflects all necessary information for further investigation and response.

References:

Fortinet Documentation on Playbook Creation and Incident Management.

Best Practices for Automating Incident Response in SOC Operations.

NEW QUESTION 2

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 3

Refer to the exhibit.

Name	IP Address	Platform	Logs	Serial Number
FAZ-SiteA	10.0.1.236	FortiAnalyzer-VM64		FAZ-VMTM24000905
SiteA				
FortiGate-A2	10.200.2.254	FortiGate-VM64	Real Time	FGVMSLTM24000454
root		vdom	Real Time	
MSSP-Local				
FortiGate-A1	10.0.1.254	FortiGate-VM64	Real Time	FGVMSLTM24000453
root		vdom	Real Time	
root	10.200.208.236	FortiAnalyzer-VM64		FAZ-VMTM24000908
Site-B-Fabric				
FortiGate-B1	172.16.200.5	FortiGate-VM64	Real Time	FGVMSLTM24000455
root		vdom	Real Time	
FortiGate-B2	10.200.200.254	FortiGate-VM64	Real Time	FGVMSLTM24000847
root		vdom	Real Time	

Assume that all devices in the FortiAnalyzer Fabric are shown in the image.

Which two statements about the FortiAnalyzer Fabric deployment are true? (Choose two.)

- A. FortiGate-B1 and FortiGate-B2 are in a Security Fabric.
- B. There is no collector in the topology.
- C. All FortiGate devices are directly registered to the supervisor.
- D. FAZ-SiteA has two ADOMs enabled.

Answer: AD

Explanation:

Understanding the FortiAnalyzer Fabric:

The FortiAnalyzer Fabric provides centralized log collection, analysis, and reporting for connected FortiGate devices.

Devices in a FortiAnalyzer Fabric can be organized into different Administrative Domains (ADOMs) to separate logs and management.

Analyzing the Exhibit:

FAZ-SiteA and FAZ-SiteB are FortiAnalyzer devices in the fabric.

FortiGate-B1 and FortiGate-B2 are shown under the Site-B-Fabric, indicating they are part of the same Security Fabric.

FAZ-SiteA has multiple entries under it: SiteA and MSSP-Local, suggesting multiple ADOMs are enabled.

Evaluating the Options:

Option A: FortiGate-B1 and FortiGate-B2 are under Site-B-Fabric, indicating they are indeed part of the same Security Fabric.

Option B: The presence of FAZ-SiteA and FAZ-SiteB as FortiAnalyzers does not preclude the existence of collectors. However, there is no explicit mention of a separate collector role in the exhibit.

Option C: Not all FortiGate devices are directly registered to the supervisor. The exhibit shows hierarchical organization under different sites and ADOMs.

Option D: The multiple entries under FAZ-SiteA (SiteA and MSSP-Local) indicate that FAZ-SiteA has two ADOMs enabled.

Conclusion:

FortiGate-B1 and FortiGate-B2 are in a Security Fabric.

FAZ-SiteA has two ADOMs enabled.

References:

Fortinet Documentation on FortiAnalyzer Fabric Topology and ADOM Configuration.

Best Practices for Security Fabric Deployment with FortiAnalyzer.

NEW QUESTION 4

Refer to the exhibit,

Command and Control	T1071.001 Web Protocols (5)
	T1071.002 File Transfer Protocols
16 techniques	T1071.003 Mail Protocols
Application Layer Protocol	T1071.004 DNS (11)
15	

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

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 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 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 7

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 8

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 9

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

Refer to Exhibit:

The screenshot shows the configuration interface for a Data Policy and Disk Utilization. Under 'Data Policy', 'Keep Logs for Analytics' is set to 60 days and 'Keep Logs for Archive' is set to 120 days. Under 'Disk Utilization', 'Allocated' is set to 300 GB, with a note that the 'Maximum Available' is 441.0 GB. 'Analytics Archive' is set to 30% with a 'Modify' checkbox checked. 'Alert and Delete When Usage Reaches' is set to 90%.

You are tasked with reviewing a new FortiAnalyzer deployment in a network with multiple registered logging devices. There is only one FortiAnalyzer in the topology.

Which potential problem do you observe?

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

Answer: B

Explanation:

Understanding FortiAnalyzer Data Policy and Disk Utilization:

FortiAnalyzer uses data policies to manage log storage, retention, and disk utilization.

The Data Policy section indicates how long logs are kept for analytics and archive purposes.

The Disk Utilization section specifies the allocated disk space and the proportions used for analytics and archive, as well as when alerts should be triggered based on disk usage.

Analyzing the Provided Exhibit:

Keep Logs for Analytics:60 Days

Keep Logs for Archive:120 Days

Disk Allocation:300 GB (with a maximum of 441 GB available)

Analytics: Archive Ratio:30% : 70%

Alert and Delete When Usage Reaches:90%

Potential Problems Identification:

Disk Space Allocation:The allocated disk space is 300 GB out of a possible 441 GB, which might not be insufficient if the log volume is high, but it is not the primary concern based on the given data.

Analytics-to-Archive Ratio:The ratio of 30% for analytics and 70% for archive is unconventional. Typically, a higher percentage is allocated for analytics since real-time or recent data analysis is often prioritized. A common configuration might be a 70% analytics and 30% archive ratio. The misconfigured ratio can lead to insufficient space for analytics, causing issues with real-time monitoring and analysis.

Retention Periods:While the retention periods could be seen as lengthy, they are not necessarily indicative of a problem without knowing the specific log volume and compliance requirements. The length of these periods can vary based on organizational needs and legal requirements.

Conclusion:

Based on the analysis, the primary issue observed is the analytics-to-archive ratio being misconfigured. This misconfiguration can significantly impact the effectiveness of the FortiAnalyzer in real-time log analysis, potentially leading to delayed threat detection and response.

References:

Fortinet Documentation on FortiAnalyzer Data Policies and Disk Management.

Best Practices for FortiAnalyzer Log Management and Disk Utilization.

NEW QUESTION 10

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 is Threat hunting.

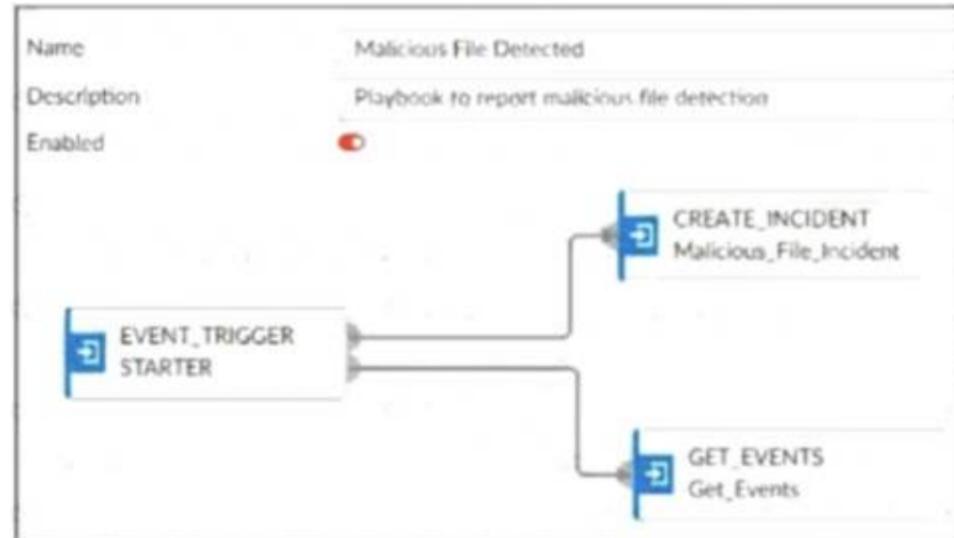
References:

Fortinet Documentation on FortiAnalyzer Features and SIEM Capabilities.

Security Best Practices and Use Cases for Threat Hunting.

NEW QUESTION 14

Refer to Exhibit:



A SOC analyst is creating the Malicious File Detected playbook to run when FortiAnalyzer generates a malicious file event. The playbook must also update the incident with the malicious file event data.

What must the next task in this playbook be?

- A. A local connector with the action Update Asset and Identity

- B. A local connector with the action Attach Data to Incident
- C. A local connector with the action Run Report
- D. A local connector with the action Update Incident

Answer: D

Explanation:

Understanding the Playbook and its Components:

The exhibit shows a playbook in which an event trigger starts actions upon detecting a malicious file.

The initial tasks in the playbook include CREATE_INCIDENT and GET_EVENTS.

Analysis of Current Tasks:

EVENT_TRIGGER STARTER: This initiates the playbook when a specified event (malicious file detection) occurs.

CREATE_INCIDENT: This task likely creates a new incident in the incident management system for tracking and response.

GET_EVENTS: This task retrieves the event details related to the detected malicious file.

Objective of the Next Task:

The next logical step after creating an incident and retrieving event details is to update the incident with the event data, ensuring all relevant information is attached to the incident record.

This helps SOC analysts by consolidating all pertinent details within the incident record, facilitating efficient tracking and response.

Evaluating the Options:

Option A: Update Asset and Identity is not directly relevant to attaching event data to the incident.

Option B: Attach Data to Incident sounds plausible but typically, updating an incident involves more comprehensive changes including status updates, adding comments, and other data modifications.

Option C: Run Report is irrelevant in this context as the goal is to update the incident with event data.

Option D: Update Incident is the most suitable action for incorporating event data into the existing incident record.

Conclusion:

The next task in the playbook should be to update the incident with the event data to ensure the incident reflects all necessary information for further investigation and response.

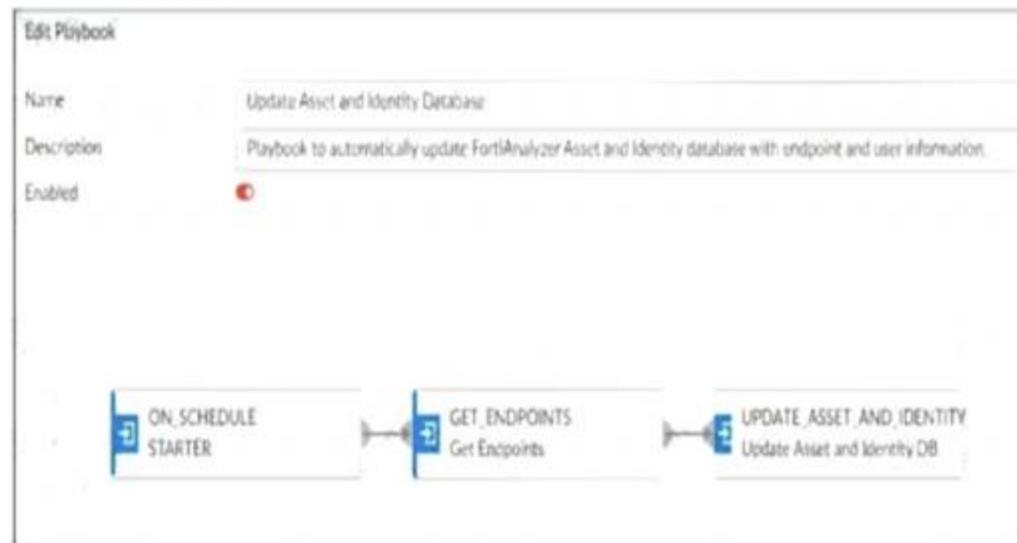
References:

Fortinet Documentation on Playbook Creation and Incident Management.

Best Practices for Automating Incident Response in SOC Operations.

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 18

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCSS_SOC_AN-7.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCSS_SOC_AN-7.4 Product From:

https://www.2passeasy.com/dumps/FCSS_SOC_AN-7.4/

Money Back Guarantee

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