

## Exam Questions FCSS\_SOC\_AN-7.4

FCSS - Security Operations 7.4 Analyst

[https://www.2passeasy.com/dumps/FCSS\\_SOC\\_AN-7.4/](https://www.2passeasy.com/dumps/FCSS_SOC_AN-7.4/)



**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**

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	10.200.200.236	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.

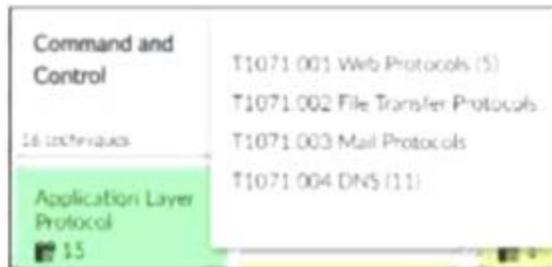
References:

Fortinet Documentation on FortiAnalyzer Fabric Topology and ADOM Configuration.

Best Practices for Security Fabric Deployment with FortiAnalyzer.

### NEW QUESTION 3

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 4

Refer to the exhibits.

## Event Handler

The screenshot shows the configuration for an event handler named 'Spearphishing handler'. The fields are as follows:

- Status:** On (indicated by a red dot).
- Name:** Spearphishing handler
- Description:** (Empty text area)
- MITRE Domain:** N/A, Enterprise, ICS
- Data Selector:** Click to select
- Automation Stitch:** On (indicated by a red dot)
- Rules:** Spearphishing Rule 1
- Handler Settings:** Notifications: Spearphishing Alert

## Rule

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, change the selection to AntiVirus Log (malware).
- B. Configure a FortiSandbox data selector and add it to the 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 selecting
- E. Within a group, the log field Malware Name (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 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**

Which statement best describes the MITRE ATT&CK framework?

- A. It provides a high-level description of common adversary activities, but lacks technical details
- B. It covers tactics, techniques, and procedures, but does not provide information about mitigations.
- C. It describes attack vectors targeting network devices and servers, but not user endpoints.
- D. It contains some techniques or subtechniques that fall under more than one tactic.

**Answer:** D

**Explanation:**

Understanding the MITRE ATT&CK Framework:

The MITRE ATT&CK framework is a comprehensive matrix of tactics and techniques used by adversaries to achieve their objectives.

It is widely used for understanding adversary behavior, improving defense strategies, and conducting security assessments.

Analyzing the Options:

Option A: The framework provides detailed technical descriptions of adversary activities, including specific techniques and subtechniques.

Option B: The framework includes information about mitigations and detections for each technique and subtechnique, providing comprehensive guidance.

Option C: MITRE ATT&CK covers a wide range of attack vectors, including those targeting user endpoints, network devices, and servers.

Option D: Some techniques or subtechniques do indeed fall under multiple tactics, reflecting the complex nature of adversary activities that can serve different objectives.

Conclusion:

The statement that best describes the MITRE ATT&CK framework is that it contains some techniques or subtechniques that fall under more than one tactic.

References:

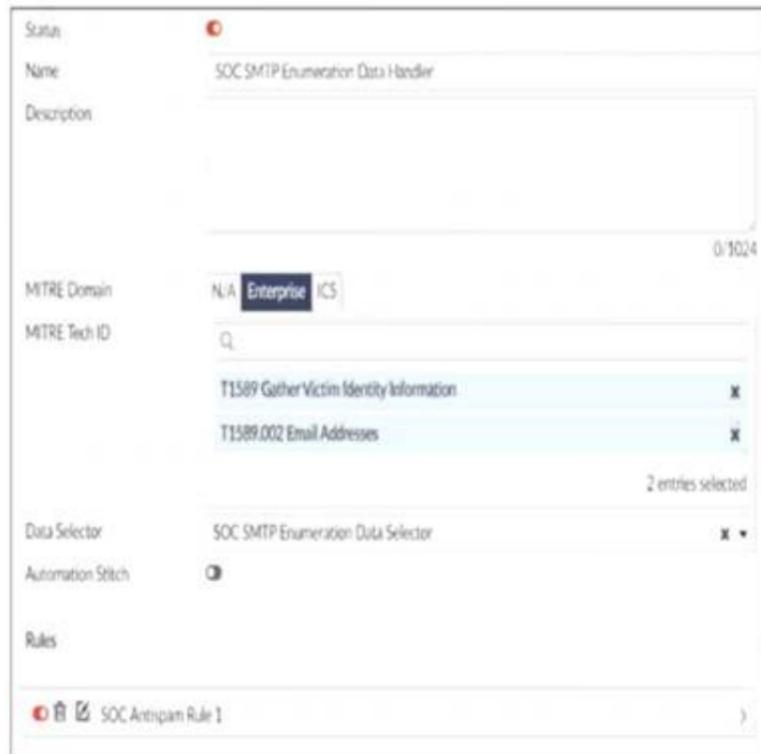
MITRE ATT&CK Framework Documentation.

Security Best Practices and Threat Intelligence Reports Utilizing MITRE ATT&CK.

**NEW QUESTION 8**

Refer to the exhibits.

Event Handler



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: Typing type==spam in 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 are input and output.

References:

Fortinet Documentation on Playbook Configuration and Variable Usage.

General SOC Automation and Orchestration Practices.

**NEW QUESTION 10**

When configuring a FortiAnalyzer to act as a collector device, which two steps must you perform?(Choose two.)

- A. Enable log compression.
- B. Configure log forwarding to a FortiAnalyzer in analyzer mode.
- C. Configure the data policy to focus on archiving.
- D. Configure Fabric authorization on the connecting interface.

**Answer: BD**

**Explanation:**

Understanding FortiAnalyzer Roles:

FortiAnalyzer can operate in two primary modes: collector mode and analyzer mode.

Collector Mode: Gathers logs from various devices and forwards them to another FortiAnalyzer operating in analyzer mode for detailed analysis.

Analyzer Mode: Provides detailed log analysis, reporting, and incident management.

Steps to Configure FortiAnalyzer as a Collector Device:

\* A. Enable Log Compression:

While enabling log compression can help save storage space, it is not a mandatory step specifically required for configuring FortiAnalyzer in collector mode. Not selected as it is optional and not directly related to the collector configuration process.

B. Configure Log Forwarding to a FortiAnalyzer in Analyzer Mode:

Essential for ensuring that logs collected by the collector FortiAnalyzer are sent to the analyzer FortiAnalyzer for detailed processing.

Selected as it is a critical step in configuring a FortiAnalyzer as a collector device.

Step 1: Access the FortiAnalyzer interface and navigate to log forwarding settings.

Step 2: Configure log forwarding by specifying the IP address and necessary credentials of the FortiAnalyzer in analyzer mode.

**NEW QUESTION 10**

When does FortiAnalyzer generate an event?

- A. When a log matches a filter in a data selector
- B. When a log matches an action in a connector
- C. When a log matches a rule in an event handler
- D. When a log matches a task in a playbook

**Answer: C**

**Explanation:**

Understanding Event Generation in FortiAnalyzer:

FortiAnalyzer generates events based on predefined rules and conditions to help in monitoring and responding to security incidents.

Analyzing the Options:

Option A: Data selectors filter logs based on specific criteria but do not generate events on their own.

Option B: Connectors facilitate integrations with other systems but do not generate events based on log matches.

Option C: Event handlers are configured with rules that define the conditions under which events are generated. When a log matches a rule in an event handler, FortiAnalyzer generates an event.

Option D: Tasks in playbooks execute actions based on predefined workflows but do not directly generate events based on log matches.

Conclusion:

FortiAnalyzer generates an event when a log matches a rule in an event handler.

References:

Fortinet Documentation on Event Handlers and Event Generation in FortiAnalyzer.

Best Practices for Configuring Event Handlers in FortiAnalyzer.

**NEW QUESTION 14**

Refer to Exhibit:



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 18**

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, and CREATE\_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 the GET\_EVENTS action to use the FortiSandbox connector.

Step 4: Set up the RUN\_REPORT and CREATE\_INCIDENT actions based on the fetched events.

**References:**

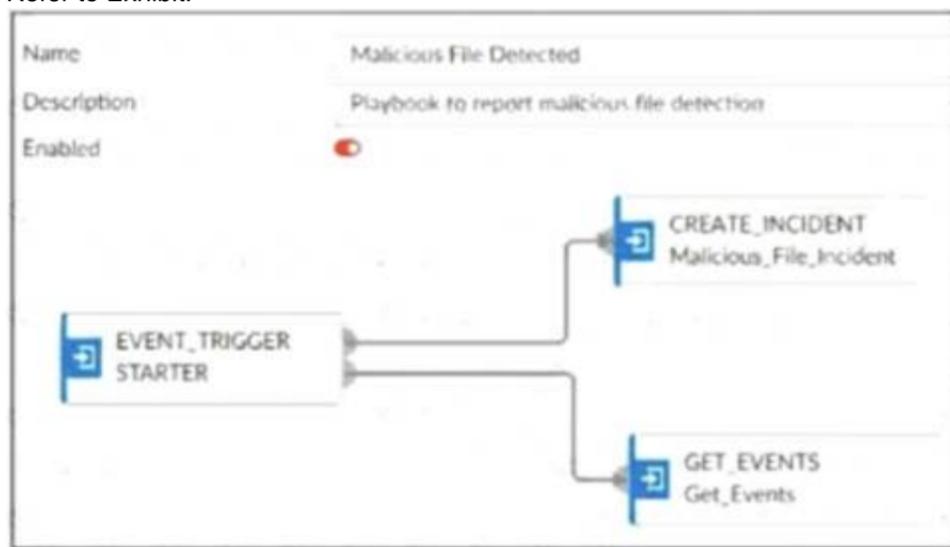
Fortinet Documentation on FortiSandbox Integration FortiSandbox Integration Guide

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 22**

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.

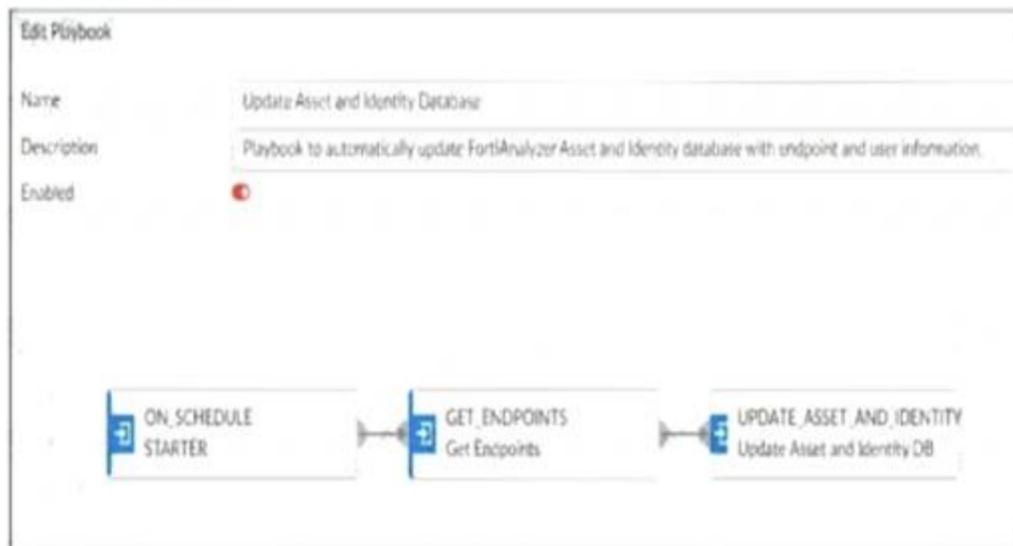
References:

Fortinet Documentation on Playbook Creation and Incident Management.

Best Practices for Automating Incident Response in SOC Operations.

**NEW QUESTION 27**

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 28**

.....

## 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/](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