

Fortinet.FCSS\_SOC\_AN-7.4.by.Joun.18q

Number: FCSS\_SOC\_AN-7.4  
Passing Score: 800  
Time Limit: 120  
File Version: 2.4

**Exam Code: FCSS\_SOC\_AN-7.4**

**Exam Name: FCSS - Security Operations 7.4 Analyst**



## Exam A

### QUESTION 1

Which FortiAnalyzer connector can you use to run automation stitches?

- A. FortiCASB
- B. FortiMail
- C. Local
- D. FortiOS

**Correct Answer: D**

**Section:**

**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.

FortiMail:

FortiMail is an email security solution. While it can send logs and events to FortiAnalyzer, it is not primarily used for running automation stitches.

Local:

The local connector refers to FortiAnalyzer's ability to handle logs and events generated by itself. This is useful for internal processes but not specifically for integrating with other Fortinet devices for automation stitches.

FortiOS:

FortiOS is the operating system that runs on FortiGate firewalls. FortiAnalyzer can use the FortiOS connector to communicate with FortiGate devices and run automation stitches. This allows FortiAnalyzer to send commands to FortiGate, triggering predefined actions in response to specific events.

Detailed Process:

Step 1: Configure the FortiOS connector in FortiAnalyzer to establish communication with FortiGate devices.

Step 2: Define automation stitches within FortiAnalyzer that specify the actions to be taken when certain events occur.

Step 3: When a triggering event is detected, FortiAnalyzer uses the FortiOS connector to send the necessary commands to the FortiGate device.

Step 4: FortiGate executes the commands, performing the predefined actions such as blocking an IP address, updating firewall rules, or sending alerts.

Conclusion:

The FortiOS connector is specifically designed for integration with FortiGate devices, enabling FortiAnalyzer to execute automation stitches effectively.

Fortinet FortiOS Administration Guide: Details on configuring and using automation stitches.

Fortinet FortiAnalyzer Administration Guide: Information on connectors and integration options.

By utilizing the FortiOS connector, FortiAnalyzer can run automation stitches to enhance the security posture and response capabilities within a network.

### QUESTION 2

Refer to the exhibits.

## Threat Hunting Monitor

Threat Action (3)		2023-09-07 19:55:58 - 2023-09-07 20:55:57				
Threat Pattern (216)	#	Application Service	Count	Sent (bytes)	Average Sent	Max Sent (bytes)
Threat Name (54)	1		251,400(68%)			
Threat Type (8)	2	DNS	109,486(30%)	9.1 MB	169.0 B	28.5 KB
File Hash (3)	3	HTTP	4,521(1%)	3.6 MB	1.2 KB	27.8 KB
File Name (8)	4	HTTPS	1,026(< 1%)	572.1 MB	578.3 KB	554.9 MB
Application Process (0)	5	SSL	249(< 1%)			
Application Name (32)	6	other	76(< 1%)	10.2 KB	138.0 B	500.0 B
Application Service (21)	7	udp/443	58(< 1%)	1019.8 KB	17.6 KB	17.6 KB
	8	NNTP	57(< 1%)			

## Threat Hunting Monitor

#	↓Date/Time	Event Message	Source IP	Destination IP
1	20:55:55		10.0.1.10	8.8.8.8
2	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
3	20:55:55		10.0.1.10	8.8.8.8
4	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
5	20:55:55		10.0.1.10	8.8.8.8
6	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
7	20:55:55		10.0.1.10	8.8.8.8

What can you conclude from analyzing the data using the threat hunting module?

- A. Spearphishing is being used to elicit sensitive information.
- B. DNS tunneling is being used to extract confidential data from the local network.
- C. Reconnaissance is being used to gather victim identity information from the mail server.
- D. FTP is being used as command-and-control (C&C) technique to mine for data.

**Correct Answer: B**

**Section:**

**Explanation:**

Understanding the Threat Hunting Data:

The Threat Hunting Monitor in the provided exhibits shows various application services, their usage counts, and data metrics such as sent bytes, average sent bytes, and maximum sent bytes. The second part of the exhibit lists connection attempts from a specific source IP (10.0.1.10) to a destination IP (8.8.8.8), with repeated 'Connection Failed' messages.

Analyzing the Application Services:

DNS is the top application service with a significantly high count (251,400) and notable sent bytes (9.1 MB).

This large volume of DNS traffic is unusual for regular DNS queries and can indicate the presence of DNS tunneling.

DNS Tunneling:

DNS tunneling is a technique used by attackers to bypass security controls by encoding data within DNS queries and responses. This allows them to extract data from the local network without detection.

The high volume of DNS traffic, combined with the detailed metrics, suggests that DNS tunneling might be in use.

Connection Failures to 8.8.8.8:

The repeated connection attempts from the source IP (10.0.1.10) to the destination IP (8.8.8.8) with connection failures can indicate an attempt to communicate with an external server.

Google DNS (8.8.8.8) is often used for DNS tunneling due to its reliability and global reach.

Conclusion:

Given the significant DNS traffic and the nature of the connection attempts, it is reasonable to conclude that DNS tunneling is being used to extract confidential data from the local network.

Why Other Options are Less Likely:

Spearphishing (A): There is no evidence from the provided data that points to spearphishing attempts, such as email logs or phishing indicators.

Reconnaissance (C): The data does not indicate typical reconnaissance activities, such as scanning or probing mail servers.

FTP C&C (D): There is no evidence of FTP traffic or command-and-control communications using FTP in the provided data.

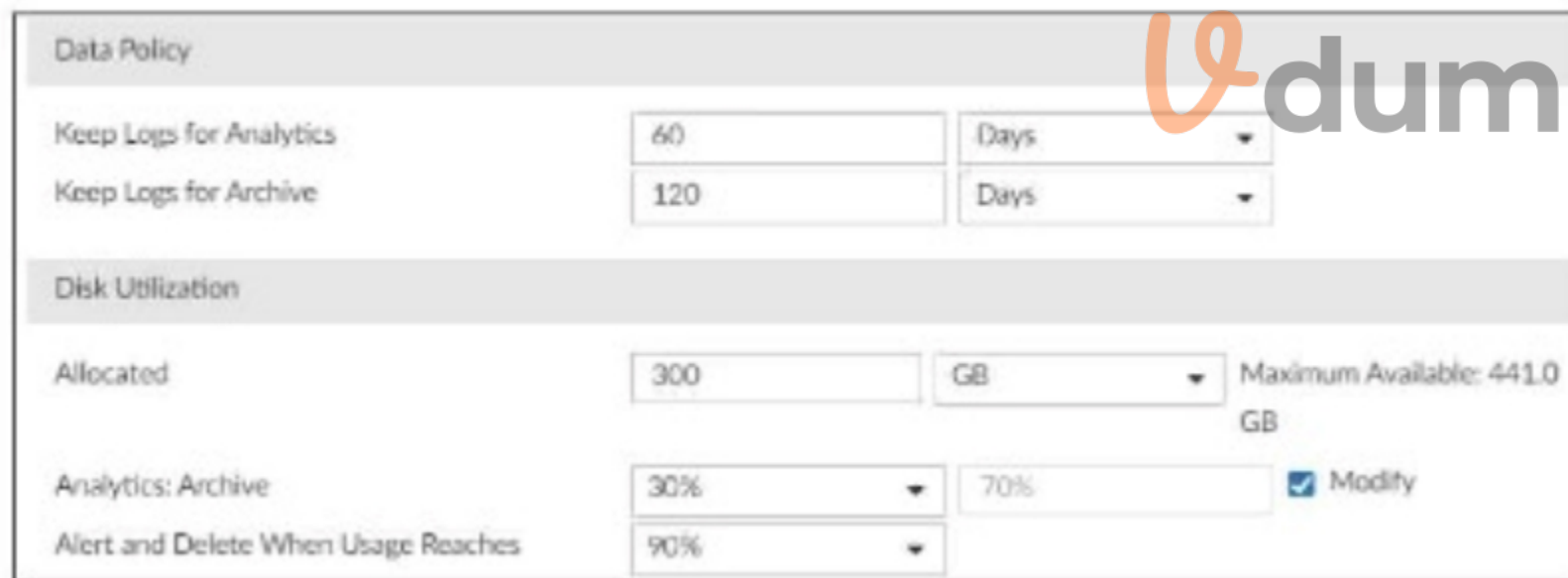
SANS Institute: 'DNS Tunneling: How to Detect Data Exfiltration and Tunneling Through DNS Queries' SANS DNS Tunneling

OWASP: 'DNS Tunneling' OWASP DNS Tunneling

By analyzing the provided threat hunting data, it is evident that DNS tunneling is being used to exfiltrate data, indicating a sophisticated method of extracting confidential information from the network.

### QUESTION 3

Refer to Exhibit:



The screenshot shows the configuration for a FortiAnalyzer device. It is divided into two sections: 'Data Policy' and 'Disk Utilization'. In the 'Data Policy' section, 'Keep Logs for Analytics' is set to 60 Days and 'Keep Logs for Archive' is set to 120 Days. In the 'Disk Utilization' section, 'Allocated' space is 300 GB, with a 'Maximum Available' of 441.0 GB. The 'Analytics: Archive' setting is 30%, and the 'Alert and Delete When Usage Reaches' is set to 90%. There is a 'Modify' button next to the 70% value in the 'Analytics: Archive' row.

Data Policy			
Keep Logs for Analytics	60	Days	
Keep Logs for Archive	120	Days	
Disk Utilization			
Allocated	300	GB	Maximum Available: 441.0 GB
Analytics: Archive	30%	70%	<input checked="" type="checkbox"/> Modify
Alert and Delete When Usage Reaches	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.

**Correct Answer: B**

**Section:**

**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.

Fortinet Documentation on FortiAnalyzer Data Policies and Disk Management.

Best Practices for FortiAnalyzer Log Management and Disk Utilization.

#### QUESTION 4

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

**Correct Answer: A**

#### Section:

#### 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.

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.

#### QUESTION 5

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

**Correct Answer: A, B**

**Section:**

**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.

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.

### QUESTION 6

Refer to the exhibit.

#### Events

<input type="checkbox"/>	Event ⇅	Event Status ⇅	Event Type ⇅	Count ⇅	Severity ⇅	First Occurrence ⇅	Last Update ⇅	Handler ⇅
<input type="checkbox"/>	📱 Device offline (1)		📱 Event	1	🟡 Medium	4 minutes ago	4 minutes ago	Local Device Event
<input type="checkbox"/>	📧 FortiMail (400)	Unhandled	⚙️ Email Filter	400	🟡 High	2 minutes ago	3 minutes ago	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	⚙️ Email Filter	1	🟡 High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	⚙️ Email Filter	1	🟡 High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	⚙️ Email Filter	1	🟡 High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	⚙️ Email Filter	1	🟡 High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	⚙️ Email Filter	1	🟡 High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	⚙️ Email Filter	1	🟡 High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	⚙️ Email Filter	1	🟡 High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	⚙️ Email Filter	1	🟡 High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	⚙️ Email Filter	1	🟡 High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	⚙️ Email Filter	1	🟡 High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	⚙️ Email Filter	1	🟡 High	2024-03-13 18:56:51	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	⚙️ Email Filter	1	🟡 High	2024-03-13 18:56:51	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	⚙️ Email Filter	1	🟡 High	2024-03-13 18:56:51	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	⚙️ Email Filter	1	🟡 High	2024-03-13 18:56:51	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	⚙️ Email Filter	1	🟡 High	2024-03-13 18:56:51	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler

#### Event Handler

Status	<input checked="" type="checkbox"/>
Name*	SOC SMTP Enumeration Data Handler
Description	

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.

**Correct Answer: A**

**Section:**

**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.

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.

## 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.

**Correct Answer: D**



**Section:**

**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:

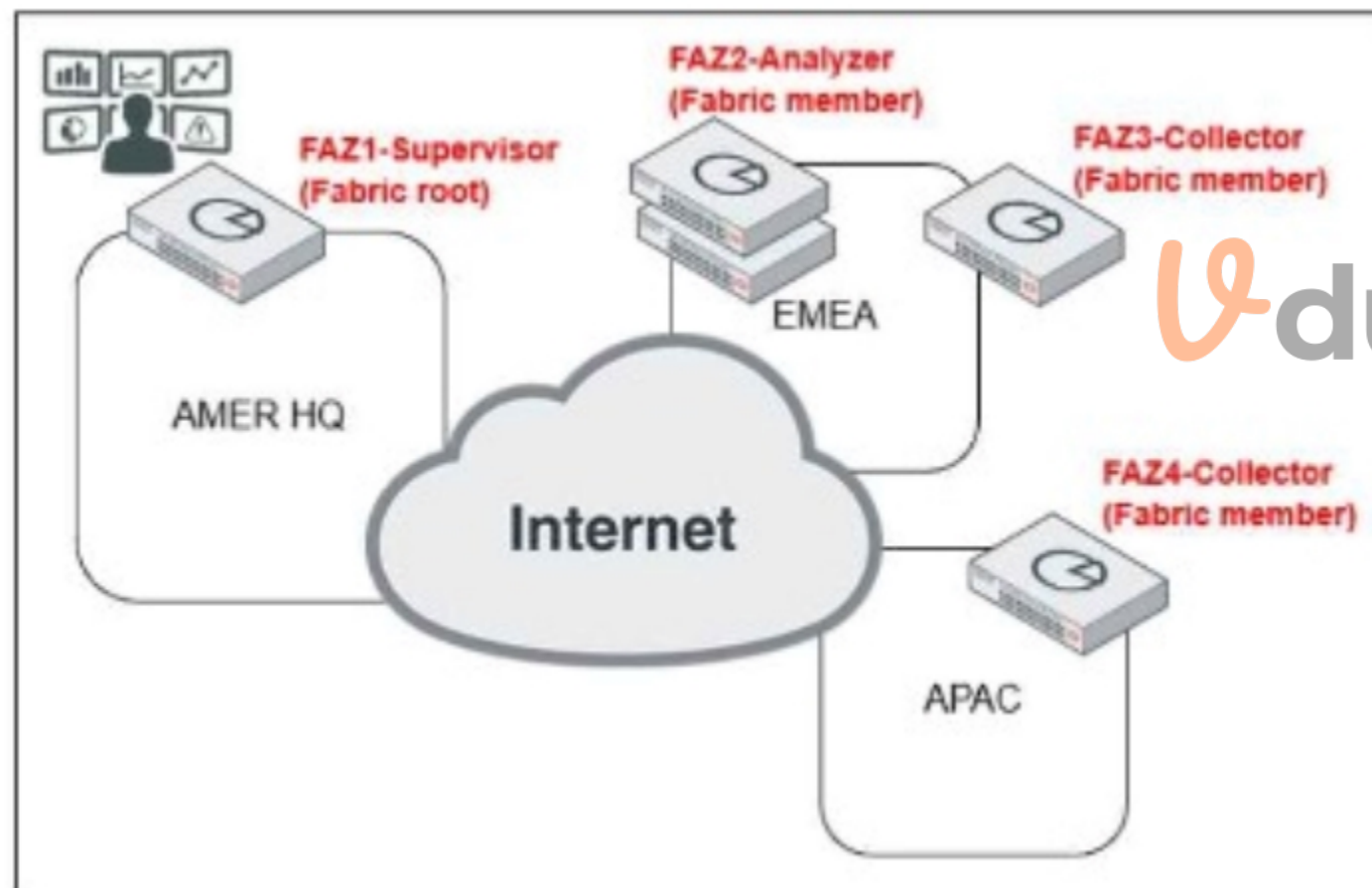
The statement that best describes the MITRE ATT&CK framework is that it contains some techniques or subtechniques that fall under more than one tactic.

MITRE ATT&CK Framework Documentation.

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

**QUESTION 8**

Exhibit:



Which observation about this FortiAnalyzer Fabric deployment architecture is true?

- A. The AMER HQ SOC team cannot run automation playbooks from the Fabric supervisor.
- B. The AMER HQ SOC team must configure high availability (HA) for the supervisor node.
- C. The EMEA SOC team has access to historical logs only.
- D. The APAC SOC team has access to FortiView and other reporting functions.

**Correct Answer: A**

**Section:****Explanation:**

Understanding FortiAnalyzer Fabric Deployment:

FortiAnalyzer Fabric deployment involves a hierarchical structure where the Fabric root (supervisor) coordinates with multiple Fabric members (collectors and analyzers). This setup ensures centralized log collection, analysis, and incident response across geographically distributed locations.

Analyzing the Exhibit:

FAZ1-Supervisor is located at AMER HQ and acts as the Fabric root.

FAZ2-Analyzer is a Fabric member located in EMEA.

FAZ3-Collector and FAZ4-Collector are Fabric members located in EMEA and APAC, respectively.

Evaluating the Options:

Option A: The statement indicates that the AMER HQ SOC team cannot run automation playbooks from the Fabric supervisor. This is true because automation playbooks and certain orchestration tasks typically require local execution capabilities which may not be fully supported on the supervisor node.

Option B: High availability (HA) configuration for the supervisor node is a best practice for redundancy but is not directly inferred from the given architecture.

Option C: The EMEA SOC team having access to historical logs only is not correct since FAZ2-Analyzer provides full analysis capabilities.

Option D: The APAC SOC team has access to FortiView and other reporting functions through FAZ4-Collector, but this is not explicitly detailed in the provided architecture.

Conclusion:

The most accurate observation about this FortiAnalyzer Fabric deployment architecture is that the AMER HQ SOC team cannot run automation playbooks from the Fabric supervisor.

Fortinet Documentation on FortiAnalyzer Fabric Deployment.

Best Practices for FortiAnalyzer and Automation Playbooks.

**QUESTION 9**

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.



**Correct Answer: B, D**

**Section:****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.

C . Configure the Data Policy to Focus on Archiving:

Data policy configuration typically relates to how logs are stored and managed within FortiAnalyzer, focusing on archiving may not be specifically required for a collector device setup.

Not selected as it is not a necessary step for configuring the collector mode.

D . Configure Fabric Authorization on the Connecting Interface:

Necessary to ensure secure and authenticated communication between FortiAnalyzer devices within the Security Fabric.

Selected as it is essential for secure integration and communication.

Step 1: Access the FortiAnalyzer interface and navigate to the Fabric authorization settings.

Step 2: Enable Fabric authorization on the interface used for connecting to other Fortinet devices and FortiAnalyzers.

Implementation Summary:

Configure log forwarding to ensure logs collected are sent to the analyzer.

Enable Fabric authorization to ensure secure communication and integration within the Security Fabric.

Conclusion:

Configuring log forwarding and Fabric authorization are key steps in setting up a FortiAnalyzer as a collector device to ensure proper log collection and forwarding for analysis.

Fortinet Documentation on FortiAnalyzer Roles and Configurations FortiAnalyzer Administration Guide

By configuring log forwarding to a FortiAnalyzer in analyzer mode and enabling Fabric authorization on the connecting interface, you can ensure proper setup of FortiAnalyzer as a collector device.

#### QUESTION 10

Which statement describes automation stitch integration between FortiGate and FortiAnalyzer?

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

**Correct Answer: D**

**Section:**

**Explanation:**

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

FortiGate Security Profiles:

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

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

Webhook Calls:

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

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

FortiAnalyzer Integration:

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

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

Detailed Process:

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

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

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

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

Fortinet Documentation: FortiOS Automation Stitches

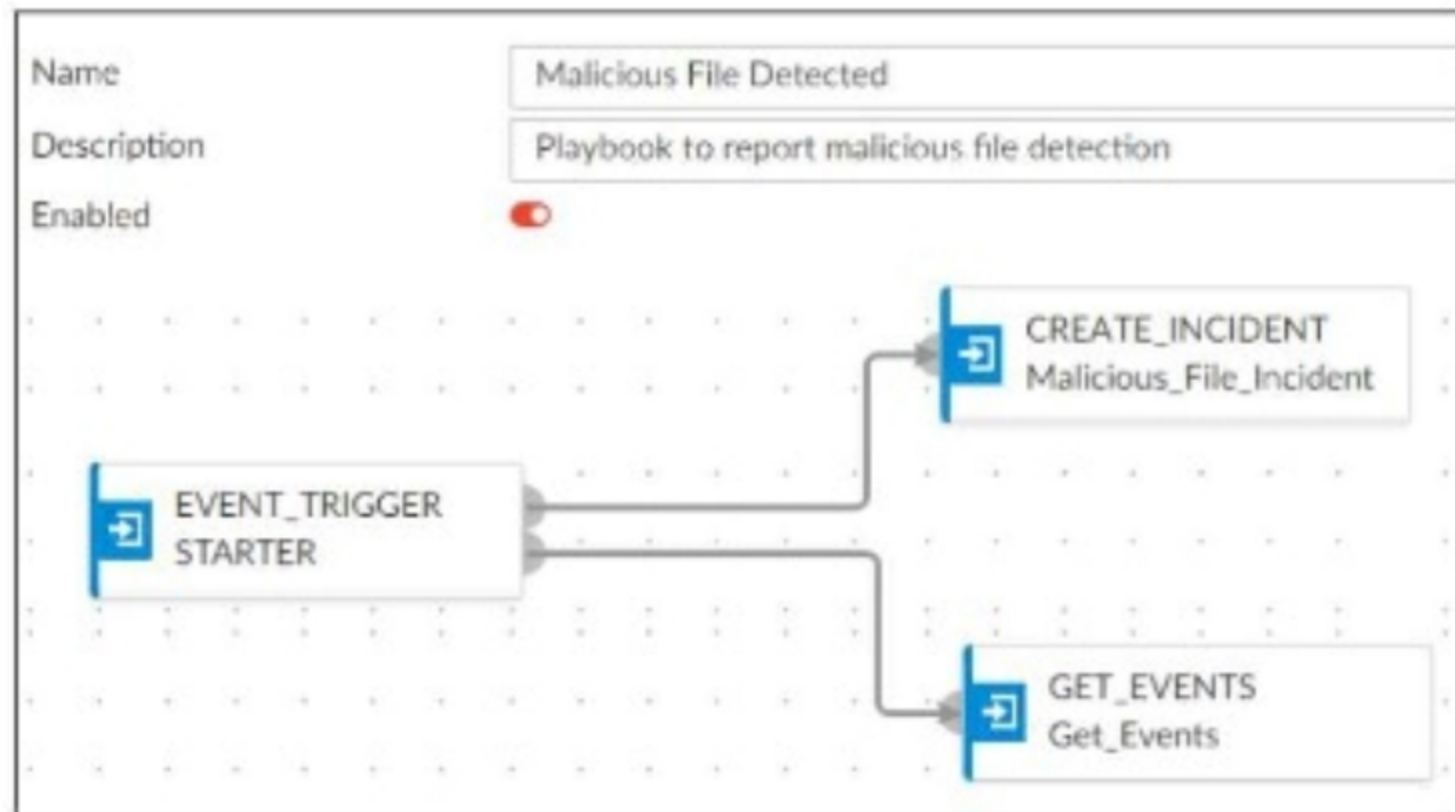
FortiAnalyzer Administration Guide: Details on configuring event handlers and integrating with FortiGate.

FortiGate Administration Guide: Information on security profiles and webhook configurations.

By understanding the interaction between FortiGate and FortiAnalyzer through webhook calls and automation stitches, security operations can ensure a proactive and efficient response to security events.

#### QUESTION 11

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



**Correct Answer: D**

**Section:**

**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.

**QUESTION 12**

Refer to the exhibits.

### Playbook status

<input type="button" value="Refresh"/> <input type="button" value="Delete"/>						
<input type="checkbox"/>	Job ID	Playbook	Trigger	Start Time	End Time	Status
<input type="checkbox"/>	2024-03-20 08:32:14.770575-07	DOS attack	event(20240320100X	2024-03-20 08:32:15-0700	2024-03-20 08:32:19-0700	<span style="color: red;">❌</span> failed[Scheduled:0/F

### Playbook tasks

Playbook Tasks						
<input type="button" value="Refresh"/> <input type="button" value="View Raw Log"/> <input type="text" value="Search..."/>						
<input type="checkbox"/>	Task ID	Task	Start Time	End Time	Status	
<input type="checkbox"/>	placeholder_8fab0102_0955_447f_872d_220	Attach_Data_To_Incident	2024-03-20 08:32:18-0700	2024-03-20 08:32:18-0700	upstream_fa	
<input type="checkbox"/>	placeholder_fa2a573c_ba4f_4565_baf0_4255	Get Events	2024-03-20 08:32:17-0700	2024-03-20 08:32:17-0700	success	
<input type="checkbox"/>	placeholder_3db75c0a_1765_4479_81f8_2e1	Create SMTP Enumeration incident	2024-03-20 08:32:17-0700	2024-03-20 08:32:17-0700	failed	

### Raw Logs

```
[2024-03-20T08:32:18.089-0700] {taskinstance.py:1937} ERROR - Task failed with exception
Traceback (most recent call last):
  File "/drive0/private/airflow/plugins/incident_operator.py", line 218, in execute
    self.epid = int(self.epid)

ValueError: invalid literal for int() with base 10: '10.200.200.100'
```

The DOS attack playbook is configured to create an incident when an event handler generates a denial-of-service (DoS) attack event. Why did the DOS attack playbook fail to execute?

- A. The Create SMTP Enumeration incident task is expecting an integer value but is receiving the incorrect data type
- B. The Get Events task is configured to execute in the incorrect order.
- C. The Attach\_Data\_To\_Incident task failed.



D. The Attach\_Data\_To\_Incident task is expecting an integer value but is receiving the incorrect data type.

**Correct Answer: A**

**Section:**

**Explanation:**

Understanding the Playbook and its Components:

The exhibit shows the status of a playbook named 'DOS attack' and its associated tasks.

The playbook is designed to execute a series of tasks upon detecting a DoS attack event.

Analysis of Playbook Tasks:

Attach\_Data\_To\_Incident: Task ID placeholder\_8fab0102, status is 'upstream\_failed,' meaning it did not execute properly due to a previous task's failure.

Get Events: Task ID placeholder\_fa2a573c, status is 'success.'

Create SMTP Enumeration incident: Task ID placeholder\_3db75c0a, status is 'failed.'

Reviewing Raw Logs:

The error log shows a ValueError: invalid literal for int() with base 10: '10.200.200.100'.

This error indicates that the task attempted to convert a string (the IP address '10.200.200.100') to an integer, which is not possible.

Identifying the Source of the Error:

The error occurs in the file 'incident\_operator.py,' specifically in the execute method.

This suggests that the task 'Create SMTP Enumeration incident' is the one causing the issue because it failed to process the data type correctly.

Conclusion:

The failure of the playbook is due to the 'Create SMTP Enumeration incident' task receiving a string value (an IP address) when it expects an integer value. This mismatch in data types leads to the error.

Fortinet Documentation on Playbook and Task Configuration.

Python error handling documentation for understanding ValueError.

### QUESTION 13

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.

**Correct Answer: B, D**

**Section:**

**Explanation:**

Understanding FortiAnalyzer Fabric Topology:

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.

Fortinet Documentation on FortiAnalyzer Fabric Topology.

Best Practices for Configuring FortiAnalyzer in a Fabric Environment.

### QUESTION 14

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

**Correct Answer: A, D**

**Section:**

**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.

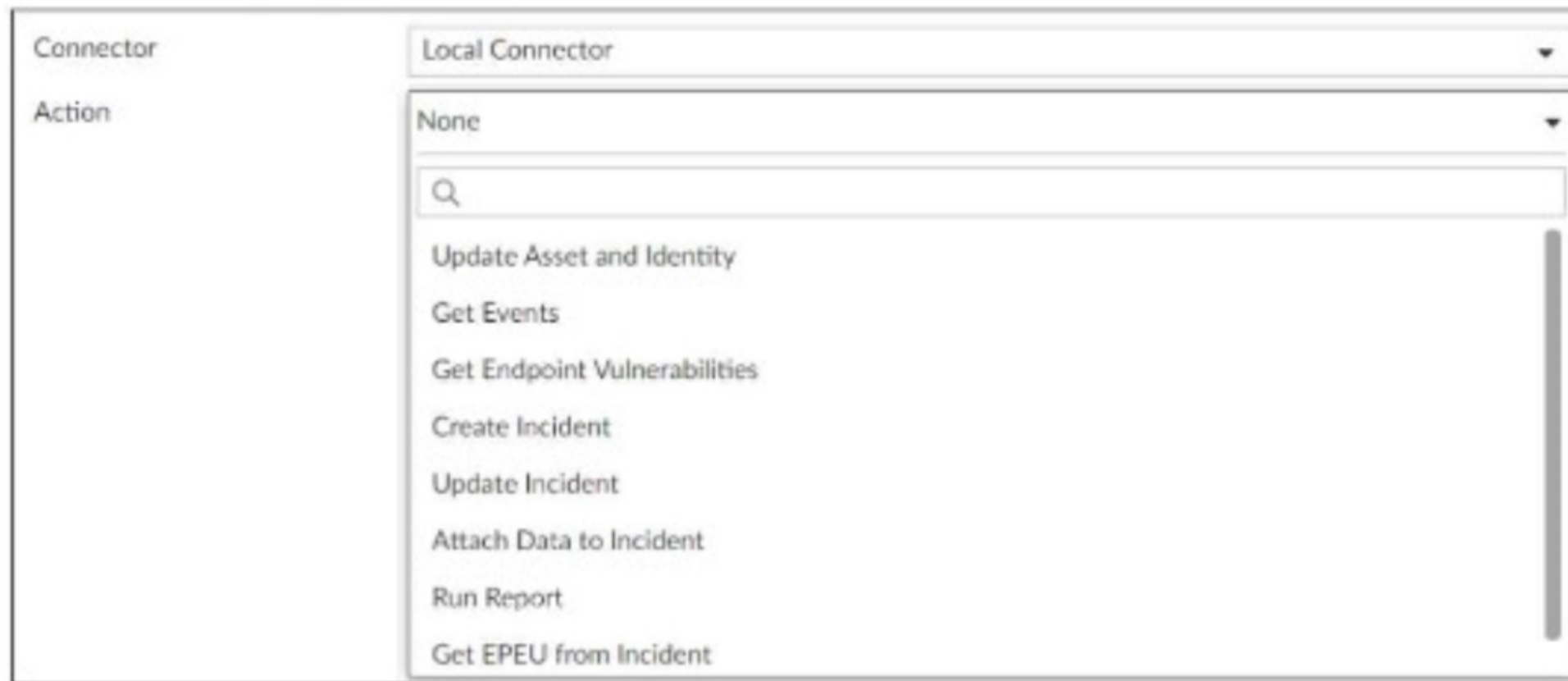
MITRE ATT&CK Framework documentation on Initial Access and Persistence tactics.

Incident analysis and mapping to MITRE ATT&CK tactics.



#### 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



**Correct Answer: D**

**Section:**

**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 is Attach Data to Incident.

Fortinet Documentation on Playbook Actions and Connectors.

Best Practices for Incident Management and Playbook Design in SOC Operations.

#### QUESTION 16

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

**Correct Answer: A**

**Section:**

**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.

Detailed Process:

Step 1: Detect the compromised host through monitoring and analysis.

Step 2: Assess the impact and scope of the compromise.

Step 3: Quarantine the compromised host to prevent further spread. This can involve disconnecting the host from the network or applying strict network segmentation.

Step 4: Document the containment actions and proceed to the eradication phase to remove the threat completely.

Step 5: After eradication, initiate the recovery phase to restore normal operations and ensure that the host is securely reintegrated into the network.

Importance of Containment:

Containment is critical in mitigating the immediate impact of an incident and preventing further damage. It buys time for responders to investigate and remediate the threat effectively.

NIST Special Publication 800-61, 'Computer Security Incident Handling Guide'

SANS Institute, 'Incident Handler's Handbook'

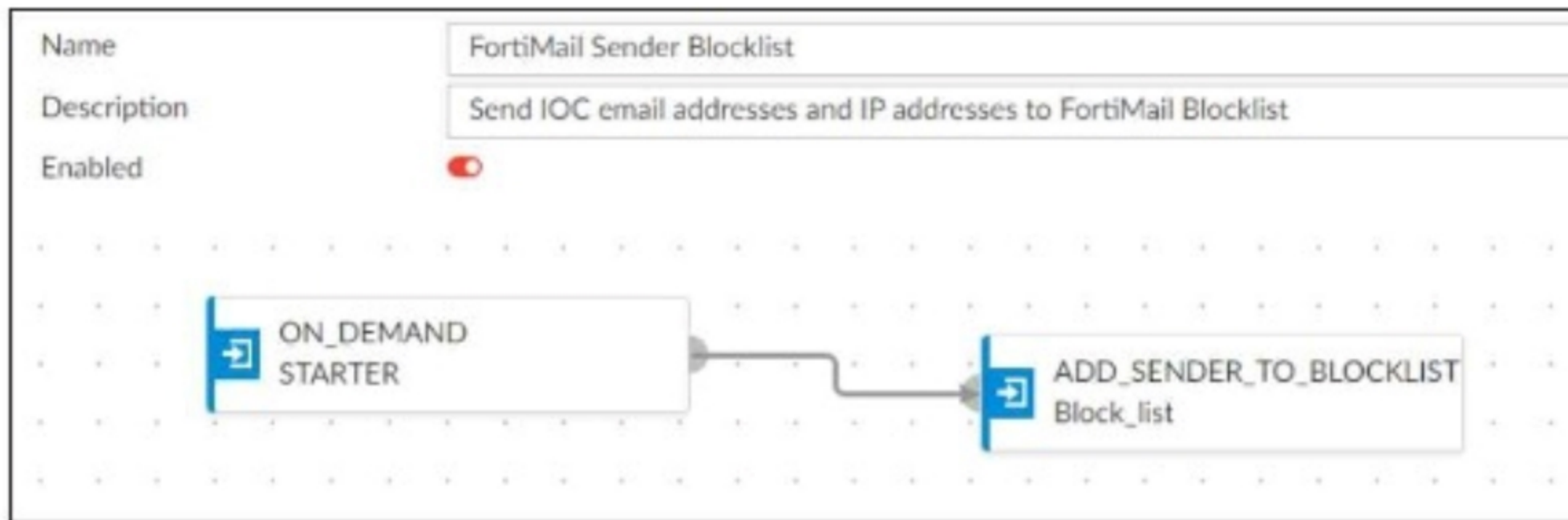
By quarantining a compromised host during the containment phase, organizations can effectively limit the spread of the incident and protect their network from further compromise.

#### QUESTION 17

Refer to the exhibits.



## Playbook configuration



## FortiMail connector actions

Configuration	Action		
Status	Name	Description	Filters/Parameters
Enabled	ADD_SENDER_TO_BLOCKLIST	disard email received from the blocklis...	id: cmd:
Enabled	GET_EMAIL_STATISTICS	retrieve information of email message...	id: cmd:
Enabled	GET_SENDER_REPUTATION	retrieve information such as the sende...	id: cmd:

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 failing?

- 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 FortiAnalyzer self-signed certificate.
- D. The connector credentials are incorrect

**Correct Answer: B**

**Section:**

**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 action ADD\_SENDER\_TO\_BLOCKLIST.

Analyzing the Playbook Execution:

The configuration and actions provided show that the playbook is straightforward, starting with an ON\_DEMAND STARTER and proceeding to the ADD\_SENDER\_TO\_BLOCKLIST action.

The action description indicates it is intended to block senders based on email addresses or domains.

Evaluating the Options:

Option A: Using GET\_EMAIL\_STATISTICS is 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).

Fortinet Documentation on FortiMail Connector Actions.

Best Practices for Configuring FortiMail Block Lists.

### QUESTION 18

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

**Correct Answer: B, D**

**Section:**

**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.

Fortinet Documentation on Incident Management in FortiAnalyzer.

FortiAnalyzer Event Handling and Customization Guides.

