

# Fortinet

## Exam Questions FCSS\_SOC\_AN-7.4

FCSS - Security Operations 7.4 Analyst



NEW QUESTION 1

Refer to the exhibit.

FortiAnalyzer Fabric				
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	
FAZ-SiteB	10.200.200.236	FortiAnalyzer-VM64		FAZ-VMTM24000908
root				
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 2

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 3

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 4**

Which FortiAnalyzer connector can you use to run automation stitches?

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

**Answer:** D

**Explanation:**

➤ Overview of Automation Stitches:

➤ Automation stitches in FortiAnalyzer are predefined sets of automated actions triggered by specific events. These actions help in automating responses to security incidents, improving efficiency, and reducing the response time.

➤ FortiAnalyzer Connectors:

➤ FortiAnalyzer integrates with various Fortinet products and other third-party solutions through connectors. These connectors facilitate communication and data exchange, enabling centralized management and automation.

➤ Available Connectors for Automation Stitches:

➤ FortiCASB:

➤ FortiCASB is a Cloud Access Security Broker that helps secure SaaS applications.

However, it is not typically used for running automation stitches within FortiAnalyzer.

**NEW QUESTION 5**

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:

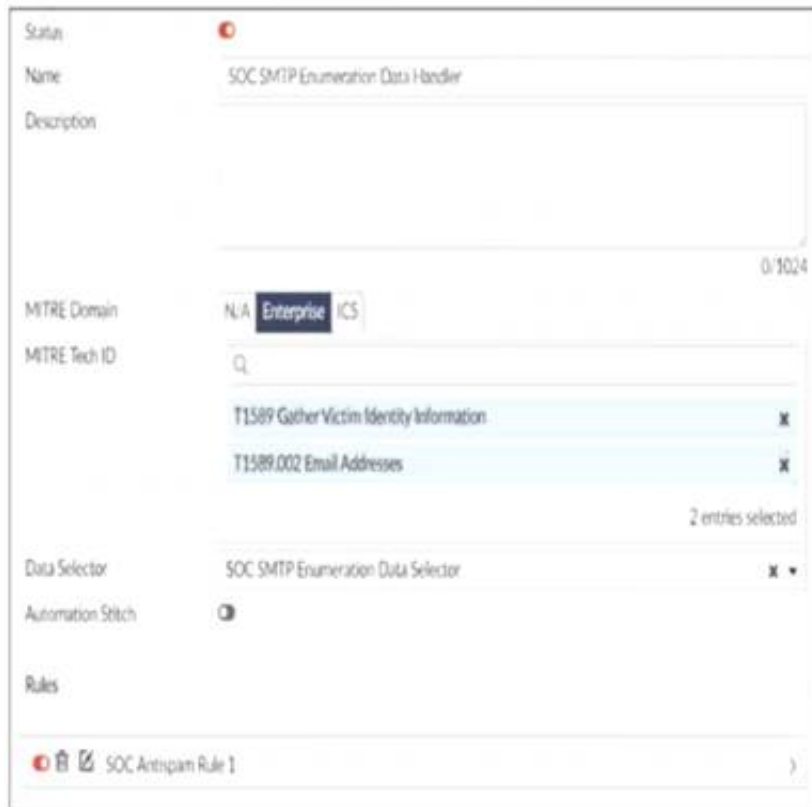
Option A: The framework provides detailed technical descriptions of adversary activities, including specific techniques and subtechniques.

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 6

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: Typingtype==spamin the Log filter by Text field might help filter the logs, but it is not as direct and reliable as selecting the correct log type.

Option C: Disabling the rule to use the filter in the data selector to create the event does not address the issue of filtering for spam logs specifically.

Option D: Selecting "Within a group, the log field Spam Name (snane) has 2 or more unique values" is not directly relevant to filtering spam logs and could lead to incorrect filtering criteria.

Conclusion:

The correct change to make in the rule is to select "Anti-Spam Log (spam)" in the Log Type field.

This ensures that the event handler only generates events for spam emails.

References:

Fortinet Documentation on Event Handlers and Log Types.

Best Practices for Configuring FortiMail Anti-Spam Settings.

## NEW QUESTION 7

Which statement describes automation stitch integration between FortiGate and FortiAnalyzer?

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

**Answer: D**

### Explanation:

Overview of Automation Stitches: Automation stitches in Fortinet solutions enable automated

responses to specific events detected within the network. This automation helps in swiftly mitigating threats without manual intervention.

FortiGate Security Profiles:

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

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

Webhook Calls:

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

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

FortiAnalyzer Integration:

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

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

Detailed Process:

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

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

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

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

References:

Fortinet Documentation: FortiOS Automation Stitches

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

FortiGate Administration Guide: Information on security profiles and webhook configurations. By understanding the interaction between FortiGate and FortiAnalyzer through webhook calls and automation

stitches, security operations can ensure a proactive and efficient response to security events.

### NEW QUESTION 8

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 theGET\_EVENTSaction to use the FortiSandbox connector.  
Step 4: Set up theRUN\_REPORTandCREATE\_INCIDENTactions based on the fetched events.  
References:  
Fortinet Documentation on FortiSandbox Integration FortiSandbox Integration Guide  
Fortinet Documentation on FortiAnalyzer Event Handling FortiAnalyzer Administration Guide  
By using the FortiSandbox connector, the analyst can ensure that the playbook accurately fetches events based on FortiSandbox analysis and generates the required incident and report.

**NEW QUESTION 9**

Refer to Exhibit:



A SOC analyst is designing a playbook to filter for a high severity event and attach the event information to an incident. Which local connector action must the analyst use in this scenario?

- A. Get Events
- B. Update Incident
- C. Update Asset and Identity
- D. Attach Data to Incident

**Answer:** D

**Explanation:**

Understanding the Playbook Requirements:  
The SOC analyst needs to design a playbook that filters for high severity events.  
The playbook must also attach the event information to an existing incident.  
Analyzing the Provided Exhibit:  
The exhibit shows the available actions for a local connector within the playbook.  
Actions listed include:  
Update Asset and Identity  
Get Events  
Get Endpoint Vulnerabilities  
Create Incident  
Update Incident  
Attach Data to Incident  
Run Report  
Get EPEU from Incident  
Evaluating the Options:  
Get Events:This action retrieves events but does not attach them to an incident.  
Update Incident:This action updates an existing incident but is not specifically for attaching event data.  
Update Asset and Identity:This action updates asset and identity information, not relevant for attaching event data to an incident.  
Attach Data to Incident:This action is explicitly designed to attach additional data, such as event information, to an existing incident.  
Conclusion:  
The correct action to use in the playbook for filtering high severity events and attaching the event information to an incident isAttach Data to Incident.  
References:  
Fortinet Documentation on Playbook Actions and Connectors.  
Best Practices for Incident Management and Playbook Design in SOC Operations.

**NEW QUESTION 10**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### 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

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The FCSS\\_SOC\\_AN-7.4 Practice Test Here](#)**