

# Fortinet

## Exam Questions FCSS\_SOC\_AN-7.4

FCSS - Security Operations 7.4 Analyst



### 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,



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

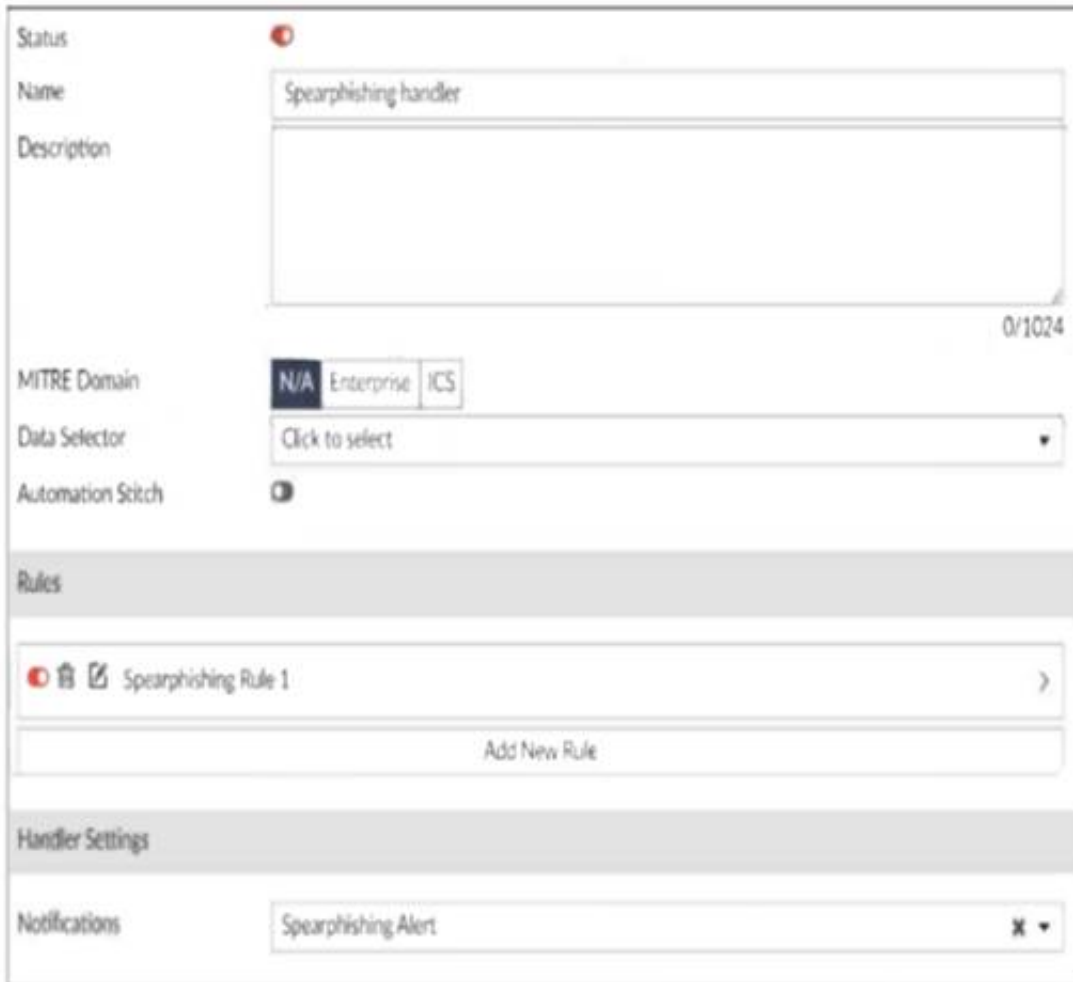
Identifying Key Points:

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 3

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 icon).
- Name:** Spearphishing handler
- Description:** (Empty text area)
- MITRE Domain:** N/A, Enterprise, ICS (Buttons)
- Data Selector:** Click to select (Dropdown menu)
- Automation Stitch:** 3 (Icon)
- Rules:**
  - Spearphishing Rule 1 (with edit and delete icons)
  - Add New Rule (button)
- Handler Settings:**
  - Notifications:** Spearphishing Alert (with close and dropdown icons)

#### 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 unique malware.
- 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 4

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 5

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 6

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 7**

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 8**

Which two ways can you create an incident on FortiAnalyzer? (Choose two.)

- A. Using a connector action
- B. Manually, on the Event Monitor page
- C. By running a playbook
- D. Using a custom event handler

**Answer:** BD

**Explanation:**

Understanding Incident Creation in FortiAnalyzer:

FortiAnalyzer allows for the creation of incidents to track and manage security events.

Incidents can be created both automatically and manually based on detected events and predefined rules.

Analyzing the Methods:

Option A: Using a connector action typically involves integrating with other systems or services and is not a direct method for creating incidents on FortiAnalyzer.

Option B: Incidents can be created manually on the Event Monitor page by selecting relevant events and creating incidents from those events.

Option C: While playbooks can automate responses and actions, the direct creation of incidents is usually managed through event handlers or manual processes.

Option D: Custom event handlers can be configured to trigger incident creation based on specific events or conditions, automating the process within FortiAnalyzer.

Conclusion:

The two valid methods for creating an incident on FortiAnalyzer are manually on the Event Monitor page and using a custom event handler.

References:

Fortinet Documentation on Incident Management in FortiAnalyzer.

FortiAnalyzer Event Handling and Customization Guides.

**NEW QUESTION 10**

.....

## 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](#)**