Fortinet

Exam Questions FCSS_SOC_AN-7.4

FCSS - Security Operations 7.4 Analyst

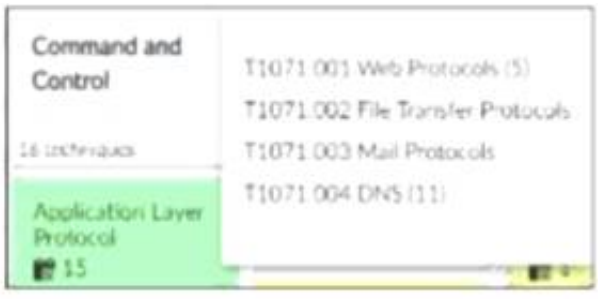
NEW QUESTION 1
A customer wants FortiAnalyzer to run an automation stitch that executes a CLI command on FortiGate to block a predefined list of URLs, if a botnet command-and-control (C&C) server IP is detected.
Which FortiAnalyzer feature must you use to start this automation process?

A. Playbook
B. Data selector
C. Event handler
D. Connector

Answer: C

Explanation:
Understanding Automation Processes in FortiAnalyzer:
FortiAnalyzer can automate responses to detected security events, such as running commands on FortiGate devices.
Analyzing the Customer Requirement:
The customer wants to run a CLI command on FortiGate to block predefined URLs when a botnet C&C server IP is detected.
This requires an automated response triggered by a specific event.
Evaluating the Options:
Option A:Playbooks orchestrate complex workflows but are not typically used for direct event-triggered automation processes.
Option B:Data selectors filter logs based on criteria but do not initiate automation processes.
Option C:Event handlers can be configured to detect specific events (such as detecting a botnet C&C server IP) and trigger automation stitches to execute predefined actions.
Option D:Connectors facilitate communication between FortiAnalyzer and other systems but are not the primary mechanism for initiating automation based on log events.
Conclusion:
To start the automation process when a botnet C&C server IP is detected, you must use anEvent handlerin FortiAnalyzer.
References:
Fortinet Documentation on Event Handlers and Automation Stitches in FortiAnalyzer.
Best Practices for Configuring Automated Responses in FortiAnalyzer.

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.)

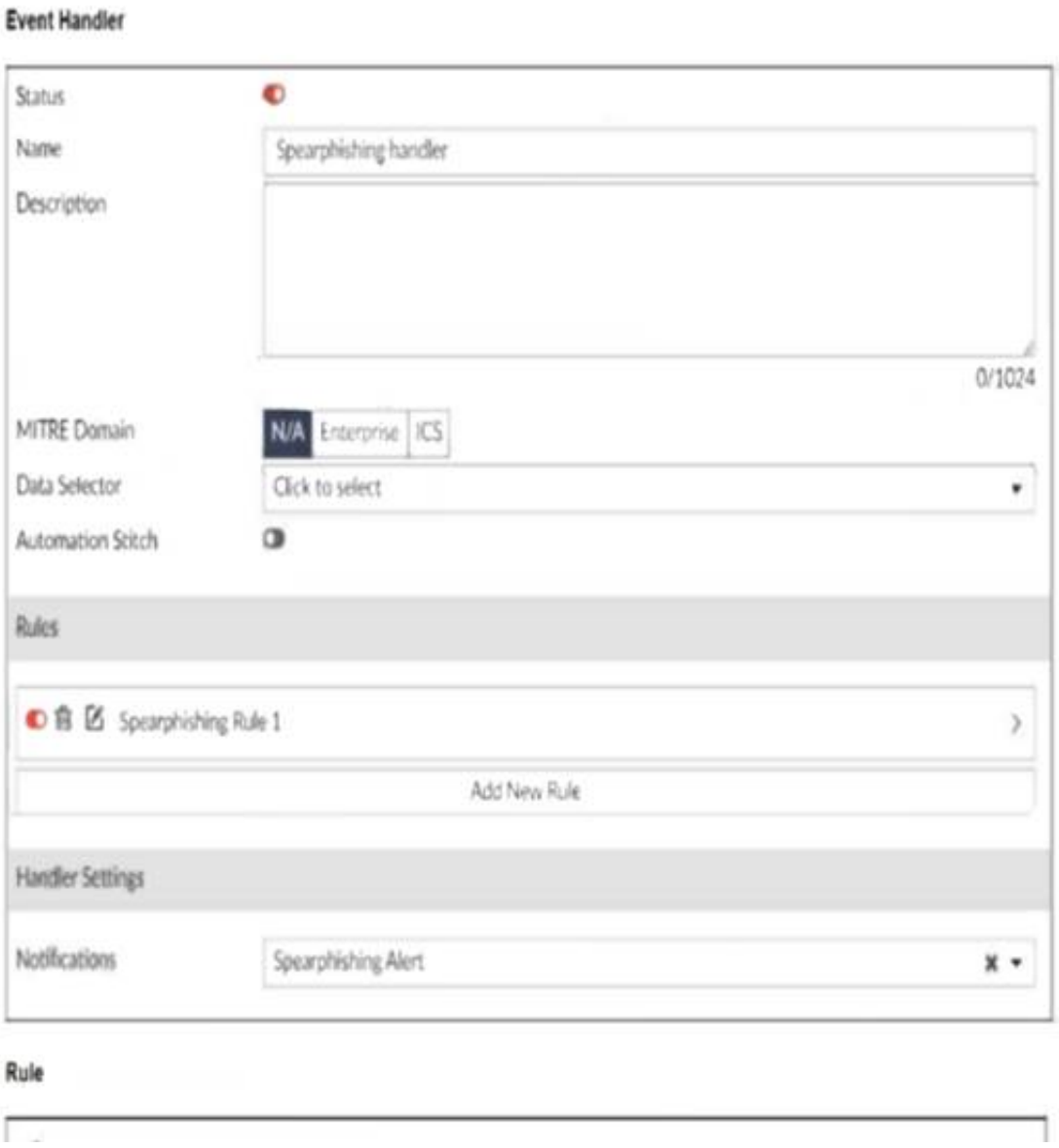
A. There are four techniques that fall under tactic T1071.
B. There are four subtechniques that fall under technique T1071.
C. There are event handlers that cover tactic T1071.
D. There are 15 events associated with the tactic.

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.



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, changethe selection toAntiVirus Log(malware).
B. Configure a FortiSandbox data selector and add it tothe 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 selectin
E. Within a group, the log field Malware Kame (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
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 ofInitial AccessandPersistence.
References:
MITRE ATT&CK Framework documentation on Initial Access and Persistence tactics.
Incident analysis and mapping to MITRE ATT&CK tactics.

NEW QUESTION 5
Your company is doing a security audit To pass the audit, you must take an inventory of all software and applications running on all Windows devices
Which FortiAnalyzer connector must you use?

A. FortiClient EMS
B. ServiceNow
C. FortiCASB
D. Local Host

Answer: A

Explanation:
Requirement Analysis:
The objective is to inventory all software and applications running on all Windows devices within the organization.
This inventory must be comprehensive and accurate to pass the security audit.
Key Components:
FortiClient EMS (Endpoint Management Server):
FortiClient EMS provides centralized management of endpoint security, including software
and application inventory on Windows devices.
It allows administrators to monitor, manage, and report on all endpoints protected by FortiClient.
Connector Options:
FortiClient EMS:
Best suited for managing and reporting on endpoint software and applications.
Provides detailed inventory reports for all managed endpoints.
Selected as it directly addresses the requirement of taking inventory of software and applications on Windows devices.
ServiceNow:
Primarily a service management platform.
While it can be used for asset management, it is not specifically tailored for endpoint software inventory.
Not selected as it does not provide direct endpoint inventory management.
FortiCASB:
Focuses on cloud access security and monitoring SaaS applications.
Not applicable for managing or inventorying endpoint software.
Not selected as it is not related to endpoint software inventory.
Local Host:
Refers to handling events and logs within FortiAnalyzer itself.

Not specific enough for detailed endpoint software inventory.
Not selected as it does not provide the required endpoint inventory capabilities.
Implementation Steps:
Step 1: Ensure all Windows devices are managed by FortiClient and connected to FortiClient EMS.
Step 2: Use FortiClient EMS to collect and report on the software and applications installed on these devices.
Step 3: Generate inventory reports from FortiClient EMS to meet the audit requirements.
References:
Fortinet Documentation on FortiClient EMS FortiClient EMS Administration Guide
By using the FortiClient EMS connector, you can effectively inventory all software and applications on Windows devices, ensuring compliance with the security audit requirements.

NEW QUESTION 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 areinputandoutput.
References:
Fortinet Documentation on Playbook Configuration and Variable Usage.
General SOC Automation and Orchestration Practices.

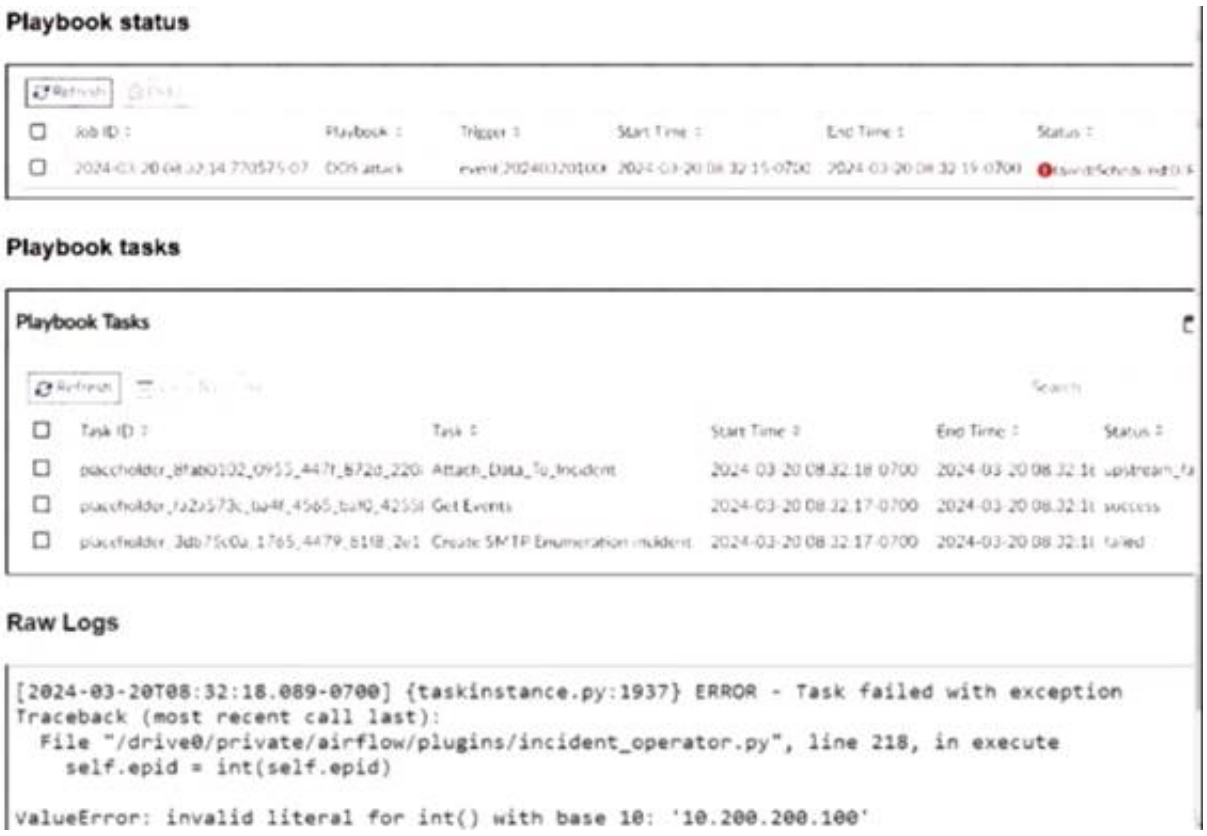
NEW QUESTION 7
When configuring a FortiAnalyzer to act as a collector device, which two steps must you perform?(Choose two.)

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
Refer to the exhibits.



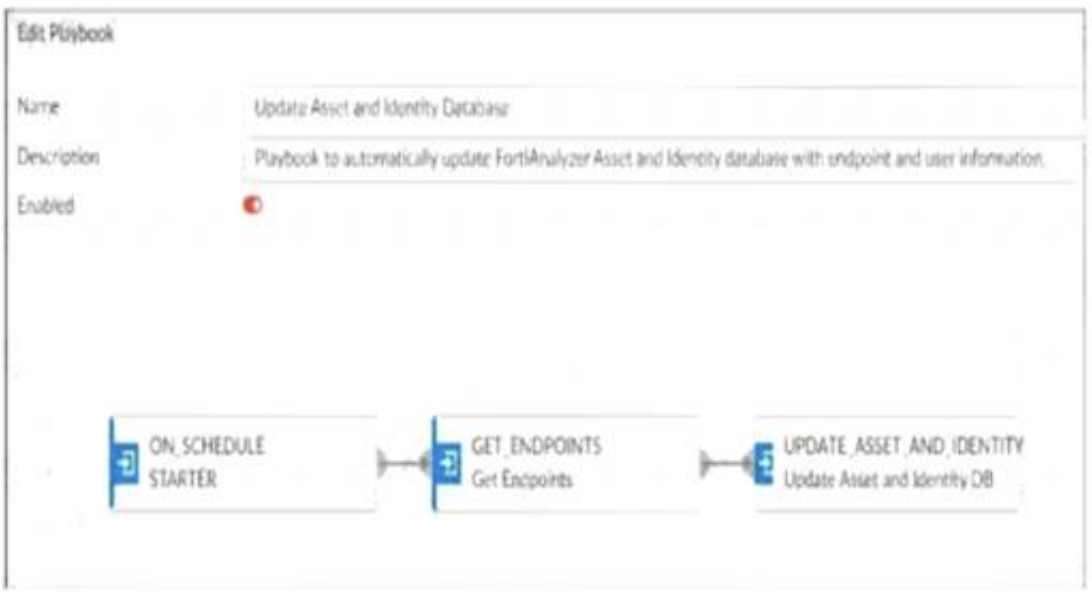
The DOS attack playbook is configured to create an incident when an event handler generates a denial-of-ser/ice (DoS) attack event.
Why did the DOS attack playbook fail to execute?

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.

Answer: A

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 aValueError: 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 theexecutemethod.
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.
References:
Fortinet Documentation on Playbook and Task Configuration.
Python error handling documentation for understandingValueError.

NEW QUESTION 9
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 10
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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