Fortinet

Exam Questions FCSS_SOC_AN-7.4

FCSS - Security Operations 7.4 Analyst

NEW QUESTION 1
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 2
Which statement best describes the MITRE ATT&CK framework?

A. Itprovides 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 3

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 4
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 5
When does FortiAnalyzer generate an event?

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

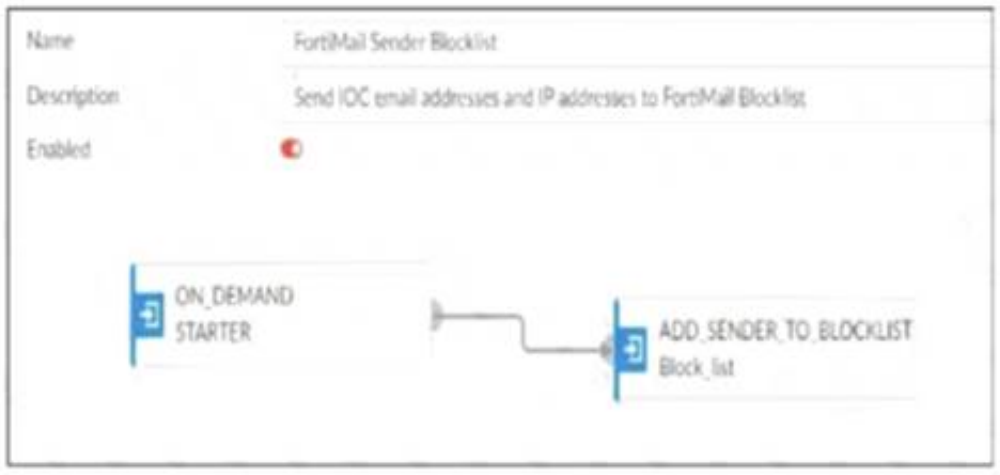
Answer: C

Explanation:
Understanding Event Generation in FortiAnalyzer:
FortiAnalyzer generates events based on predefined rules and conditions to help in monitoring and responding to security incidents.
Analyzing the Options:
Option A:Data selectors filter logs based on specific criteria but do not generate events on their own.
Option B:Connectors facilitate integrations with other systems but do not generate events based on log matches.
Option C:Event handlers are configured with rules that define the conditions under which events are generated. When a log matches a rule in an event handler, FortiAnalyzer generates an event.
Option D:Tasks in playbooks execute actions based on predefined workflows but do not directly generate events based on log matches.
Conclusion:
FortiAnalyzer generates an event when a log matches a rule in an event handler.
References:
Fortinet Documentation on Event Handlers and Event Generation in FortiAnalyzer.
Best Practices for Configuring Event Handlers in FortiAnalyzer.

NEW QUESTION 6

Refer to the exhibits.

Playbook configuration



FortiMail connector actions

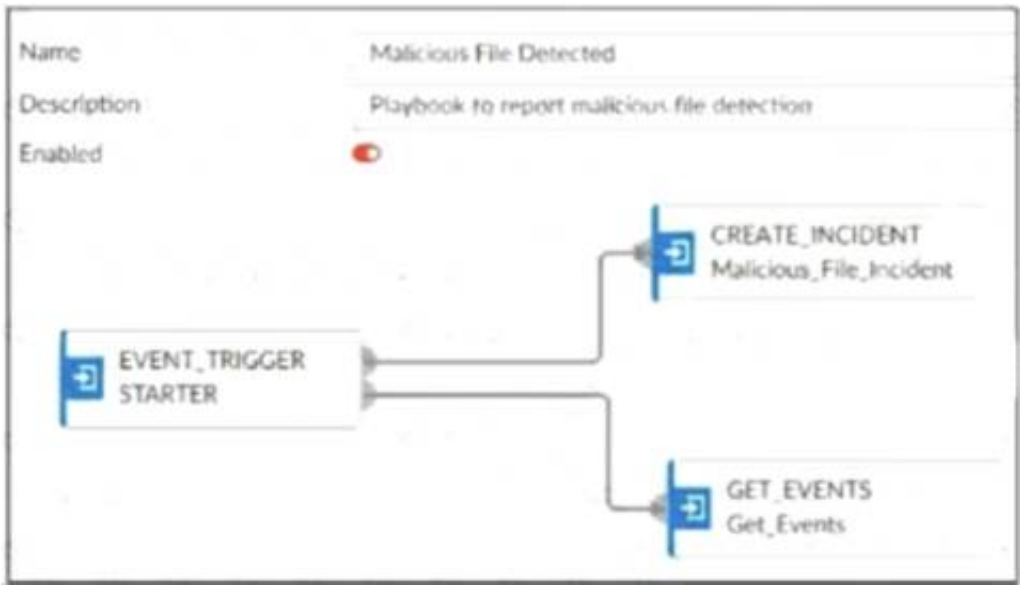
The FortiMail Sender Blocklist playbook is configured to take manual input and add those entries to the FortiMail abc. com domain-level block list. The playbook is configured to use a FortiMail connector and the ADD_SENDER_TO_BLOCKLIST action.
Why is the FortiMail Sender Blocklist playbook execution failing7

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

Answer: B

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 actionADD_SENDER_TO_BLOCKLIST.
Analyzing the Playbook Execution:
The configuration and actions provided show that the playbook is straightforward, starting with anON_DEMAND STARTERand proceeding to theADD_SENDER_TO_BLOCKLISTaction.
The action description indicates it is intended to block senders based on email addresses or domains.
Evaluating the Options:
Option A:UsingGET_EMAIL_STATISTICSis 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).
References:
Fortinet Documentation on FortiMail Connector Actions.
Best Practices for Configuring FortiMail Block Lists.

NEW QUESTION 7
Refer to Exhibit:



A SOC analyst is creating the Malicious File Detected playbook to run when FortiAnalyzer generates a malicious file event. The playbook must also update the incident with the malicious file event data.
What must the next task in this playbook be?

A. A local connector with the action Update Asset and Identity
B. A local connector with the action Attach Data to Incident
C. A local connector with the action Run Report
D. A local connector with the action Update Incident

Answer: D

Explanation:
Understanding the Playbook and its Components:
The exhibit shows a playbook in which an event trigger starts actions upon detecting a malicious file.
The initial tasks in the playbook includeCREATE_INCIDENTandGET_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 Identityis not directly relevant to attaching event data to the incident.
Option B:Attach Data to Incidentsounds plausible but typically, updating an incident involves more comprehensive changes including status updates, adding comments, and other data modifications.
Option C:Run Reportis irrelevant in this context as the goal is to update the incident with event data.
Option D:Update Incidentis the most suitable action for incorporating event data into the existing incident record.
Conclusion:
The next task in the playbook should be to update the incident with the event data to ensure the incident reflects all necessary information for further investigation and response.
References:
Fortinet Documentation on Playbook Creation and Incident Management.
Best Practices for Automating Incident Response in SOC Operations.

NEW QUESTION 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