



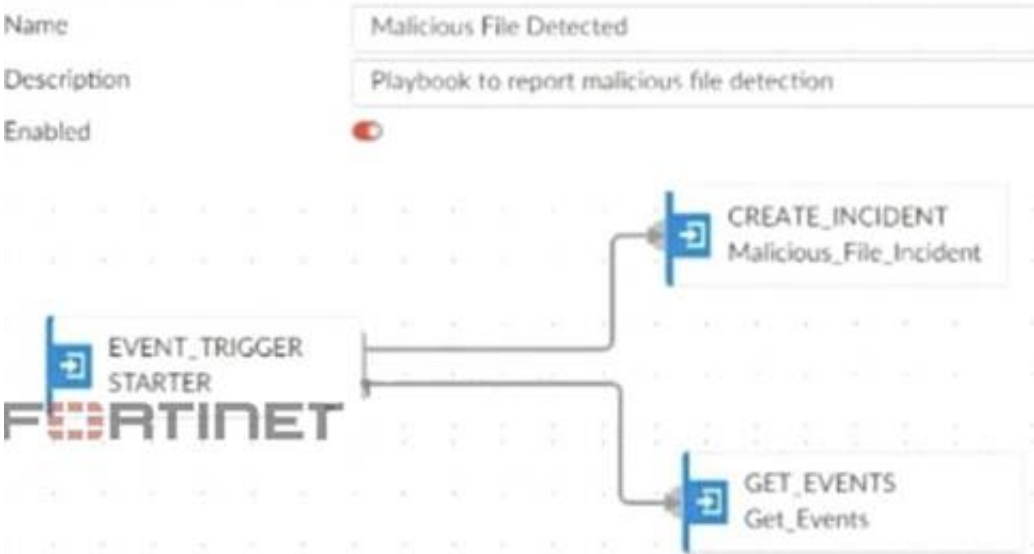
Fortinet

Exam Questions FCSS_SOC_AN-7.4

FCSS - Security Operations 7.4 Analyst

NEW QUESTION 1

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.

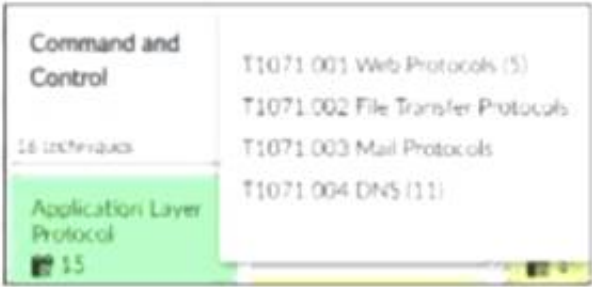
References:

Fortinet Documentation on Playbook Creation and Incident Management.

Best Practices for Automating Incident Response in SOC Operations.

NEW QUESTION 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.

Playbook

Job ID	Playbook	Trigger	Start Time	End Time	Status
2024-03-27 11:54:16.858411-07	Malicious File Detect	event:200403271000	2024-03-27 11:54:17-0700	2024-03-27 11:54:20-0700	FailedScheduled/Running/D/Success

Playbook Tasks

Task ID	Task	Start Time	End Time	Status
placeholder_8fab0102_0955_447f_872d_2208c	Attach_Data_To_Incident	2024-03-27 11:54:19-0700	2024-03-27 11:54:19-0700	upstream_failed
placeholder_3db75cd0_1765_4479_81b8_2c1e8	Create Incident	2024-03-27 11:54:19-0700	2024-03-27 11:54:19-0700	failed
placeholder_fa2a573c_ba4f_4668_baf0_4259da	Get Events	2024-03-27 11:54:19-0700	2024-03-27 11:54:19-0700	success

Raw Logs

```
[2024-03-27T11:54:19.817-0700] {taskinstance.py:1937} ERROR - Task failed with exception
Traceback (most recent call last):
  File "/drive0/private/airflow/plugins/incident_operator.py", line 216, in execute
    self.epid = FAZUtilsOperator.parse_input(context, self.epid, context_dict)
  File "/drive0/private/airflow/plugins/FAZUtilsOperator.py", line 118, in parse_input
```

The Malicious File Detect playbook is configured to create an incident when an event handler generates a malicious file detection event. Why did the Malicious File Detect playbook execution fail?

- A. The Create Incident task was expecting a name or number as input, but received an incorrect data format
- B. The Get Events task did not retrieve any event data.
- C. The Attach_Data_To_Incident incident task was expecting an integer, but received an incorrect data format.
- D. The Attach Data To Incident task failed, which stopped the playbook execution.

Answer: A

Explanation:

Understanding the Playbook Configuration:

The "Malicious File Detect" playbook is designed to create an incident when a malicious file detection event is triggered.

The playbook includes tasks such as Attach_Data_To_Incident, Create Incident, and Get Events.

Analyzing the Playbook Execution:

The exhibit shows that the Create Incident task has failed, and the Attach_Data_To_Incident task has also failed.

The Get Event task succeeded, indicating that it was able to retrieve event data.

Reviewing Raw Logs:

The raw logs indicate an error related to parsing input in the incident_operator.py file.

The error traceback suggests that the task was expecting a specific input format (likely a name or number) but received an incorrect data format.

Identifying the Source of the Failure:

The Create Incident task failure is the root cause since it did not proceed correctly due to incorrect input format.

The Attach_Data_To_Incident task subsequently failed because it depends on the successful creation of an incident.

Conclusion:

The primary reason for the playbook execution failure is that the Create Incident task received an incorrect data format, which was not a name or number as expected.

References:

Fortinet Documentation on Playbook and Task Configuration.

Error handling and debugging practices in playbook execution.

NEW QUESTION 4

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: Typing type==spam in 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 5

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 6

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 7

Refer to Exhibit:



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%
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.

Answer: B

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 theanalytics-to-archive ratiobeing misconfigured. This misconfiguration can significantly impact the effectiveness of the FortiAnalyzer in real-time log analysis, potentially leading to delayed threat detection and response.

References:

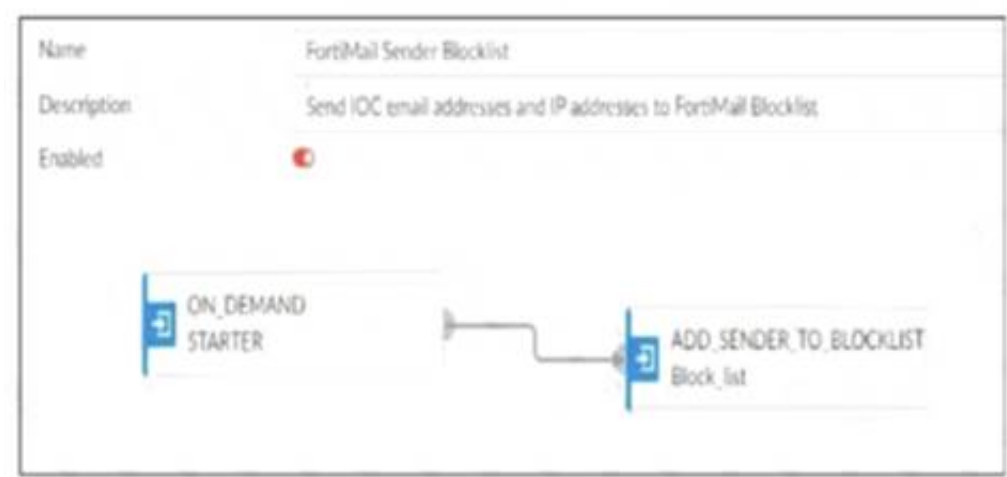
Fortinet Documentation on FortiAnalyzer Data Policies and Disk Management.

Best Practices for FortiAnalyzer Log Management and Disk Utilization.

NEW QUESTION 8

Refer to the exhibits.

Playbook configuration



FortiMail connector actions

Configurations		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:	---

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

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).

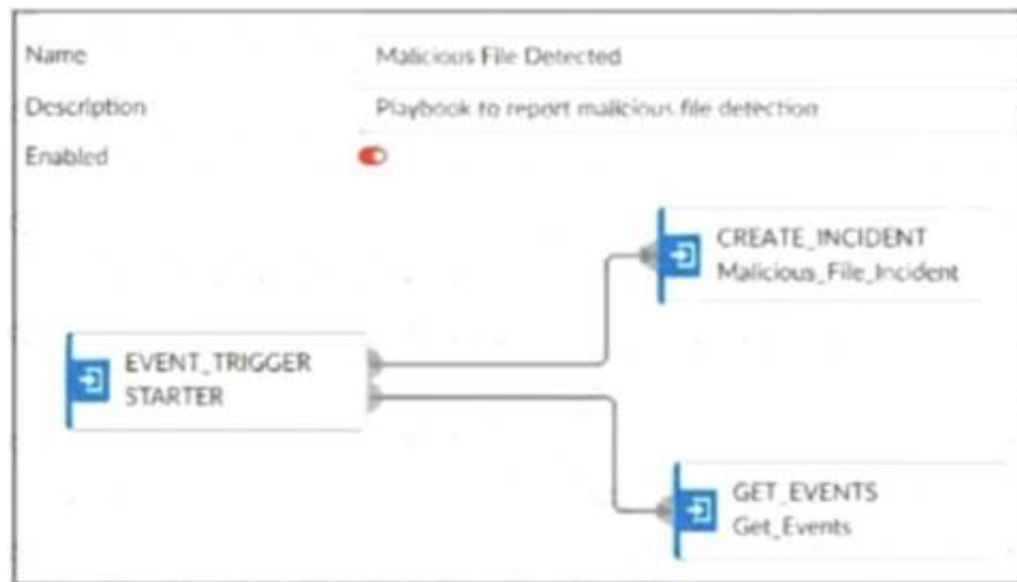
References:

Fortinet Documentation on FortiMail Connector Actions.

Best Practices for Configuring FortiMail Block Lists.

NEW QUESTION 9

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 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.

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 - 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](#)