



Fortinet

Exam Questions FCSS_SOC_AN-7.4

FCSS - Security Operations 7.4 Analyst

NEW QUESTION 1

According to the National Institute of Standards and Technology (NIST) cybersecurity framework, incident handling activities can be divided into phases. In which incident handling phase do you quarantine a compromised host in order to prevent an adversary from using it as a stepping stone to the next phase of an attack?

- A. Containment
- B. Analysis
- C. Eradication
- D. Recovery

Answer: A

Explanation:

NIST Cybersecurity Framework Overview:
The NIST Cybersecurity Framework provides a structured approach for managing and mitigating cybersecurity risks. Incident handling is divided into several phases to systematically address and resolve incidents.
Incident Handling Phases:
Preparation: Establishing and maintaining an incident response capability.
Detection and Analysis: Identifying and investigating suspicious activities to confirm an incident.
Containment, Eradication, and Recovery:
Containment: Limiting the impact of the incident.
Eradication: Removing the root cause of the incident.
Recovery: Restoring systems to normal operation.
Containment Phase:
The primary goal of the containment phase is to prevent the incident from spreading and causing further damage.
Quarantining a Compromised Host:
Quarantining involves isolating the compromised host from the rest of the network to prevent adversaries from moving laterally and causing more harm. Techniques include network segmentation, disabling network interfaces, and applying access controls.

NEW QUESTION 2

Refer to the exhibit.

FortiAnalyzer Fabric				
Name	IP Address	Platform	Logs	Serial Number
FAZ-SiteA	10.0.1.236	FortiAnalyzer-VM64		FAZ-VM1TM24000905
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-VM1TM24000908
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 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:202403271000	2024-03-27 11:54:17-0700	2024-03-27 11:54:20-0700	Failed(Scheduled 0/Running 0/Succes

Playbook Tasks

Playbook Tasks

Refresh

View Raw Log

Search...

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_3db75c0a_1765_4479_8118_2c1e8	Create Incident	2024-03-27 11:54:19-0700	2024-03-27 11:54:19-0700	failed
placeholder_fa2a573c_ba4f_4649_baff0_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: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 Events 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

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 5

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 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

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 8

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 is Attach 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](#)