



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

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 an Event handler in FortiAnalyzer.

References:

Fortinet Documentation on Event Handlers and Automation Stitches in FortiAnalyzer.

Best Practices for Configuring Automated Responses in 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:20240327100K	2024-03-27 11:54:17-0700	2024-03-27 11:54:20-0700	Failed: Scheduled: Running: Done

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_3db75c0a_1765_447f_8118_2c1e8	Create Incident	2024-03-27 11:54:19-0700	2024-03-27 11:54:19-0700	failed
placeholder_fa2a573c_ba4f_4563_baff_4258da	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 "/drive@private/airflow/plugins/incident_operator.py", line 216, in execute
    self.epid = FAZUtilsOperator.parse_input(context, self.epid, context_dict)
  File "/drive@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 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

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

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.

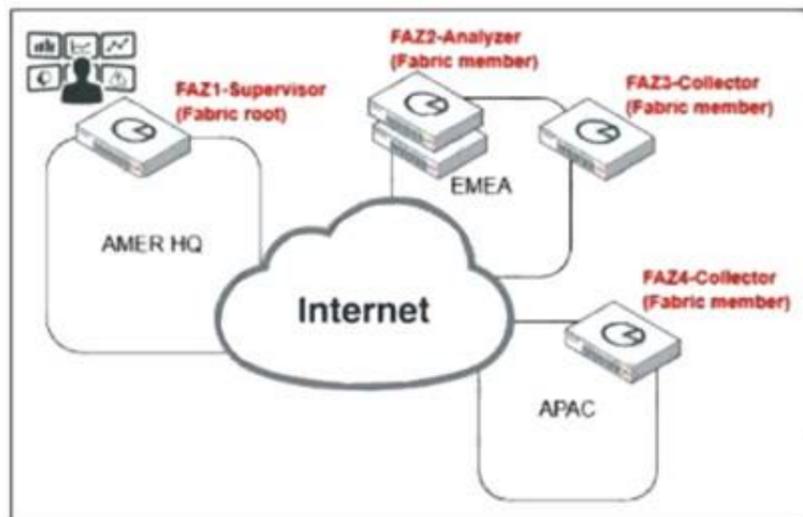
References:

MITRE ATT&CK Framework documentation on Initial Access and Persistence tactics.

Incident analysis and mapping to MITRE ATT&CK tactics.

NEW QUESTION 6

Exhibit:



Which observation about this FortiAnalyzer Fabric deployment architecture is true?

- A. The AMER HQ SOC team cannot run automation playbooks from the Fabric supervisor.
- B. The AMER HQ SOC team must configure high availability (HA) for the supervisor node.
- C. The EMEA SOC team has access to historical logs only.
- D. The APAC SOC team has access to FortiView and other reporting functions.

Answer: A

Explanation:

Understanding FortiAnalyzer Fabric Deployment:

FortiAnalyzer Fabric deployment involves a hierarchical structure where the Fabric root (supervisor) coordinates with multiple Fabric members (collectors and analyzers).

This setup ensures centralized log collection, analysis, and incident response across geographically distributed locations.

Analyzing the Exhibit:

FAZ1-Supervisor is located at AMER HQ and acts as the Fabric root.

FAZ2-Analyzer is a Fabric member located in EMEA.

FAZ3-Collector and FAZ4-Collector are Fabric members located in EMEA and APAC, respectively.

Evaluating the Options:

Option A: The statement indicates that the AMER HQ SOC team cannot run automation playbooks from the Fabric supervisor. This is true because automation playbooks and certain orchestration tasks typically require local execution capabilities which may not be fully supported on the supervisor node.

Option B: High availability (HA) configuration for the supervisor node is a best practice for redundancy but is not directly inferred from the given architecture.

Option C: The EMEA SOC team having access to historical logs only is not correct since FAZ2-Analyzer provides full analysis capabilities.

Option D: The APAC SOC team has access to FortiView and other reporting functions through FAZ4-Collector, but this is not explicitly detailed in the provided architecture.

Conclusion:

The most accurate observation about this FortiAnalyzer Fabric deployment architecture is that the AMER HQ SOC team cannot run automation playbooks from the

Fabric supervisor.

References:

Fortinet Documentation on FortiAnalyzer Fabric Deployment.

Best Practices for FortiAnalyzer and Automation Playbooks.

NEW QUESTION 7

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 8

Refer to the Exhibit:



An analyst wants to create an incident and generate a report whenever FortiAnalyzer generates a malicious attachment event based on FortiSandbox analysis.

The endpoint hosts are protected by FortiClient EMS integrated with FortiSandbox. All devices are logging to FortiAnalyzer.

Which connector must the analyst use in this playbook?

- A. FortiSandbox connector
- B. FortiClient EMS connector
- C. FortiMail connector
- D. Local connector

Answer: A

Explanation:

Understanding the Requirements:

The objective is to create an incident and generate a report based on malicious attachment events detected by FortiAnalyzer from FortiSandbox analysis.

The endpoint hosts are protected by FortiClient EMS, which is integrated with FortiSandbox. All logs are sent to FortiAnalyzer.

Key Components:

FortiAnalyzer: Centralized logging and analysis for Fortinet devices.

FortiSandbox: Advanced threat protection system that analyzes suspicious files and URLs.

FortiClient EMS: Endpoint management system that integrates with FortiSandbox for endpoint protection.

Playbook Analysis:

The playbook in the exhibit consists of three main actions: GET_EVENTS, RUN_REPORT, and CREATE_INCIDENT.

EVENT_TRIGGER: Starts the playbook when an event occurs.

GET_EVENTS: Fetches relevant events.

RUN_REPORT: Generates a report based on the events.

CREATE_INCIDENT: Creates an incident in the incident management system.

Selecting the Correct Connector:

The correct connector should allow fetching events related to malicious attachments analyzed by FortiSandbox and facilitate integration with FortiAnalyzer.

Connector Options:

FortiSandbox Connector:

Directly integrates with FortiSandbox to fetch analysis results and events related to malicious attachments.

Best suited for getting detailed sandbox analysis results.

Selected as it is directly related to the requirement of handling FortiSandbox analysis events.

FortiClient EMS Connector:

Used for managing endpoint security and integrating with endpoint logs.

Not directly related to fetching sandbox analysis events.

Not selected as it is not directly related to the sandbox analysis events.

FortiMail Connector:

Used for email security and handling email-related logs and events.

Not applicable for sandbox analysis events.

Not selected as it does not relate to the sandbox analysis.

Local Connector:

Handles local events within FortiAnalyzer itself.

Might not be specific enough for fetching detailed sandbox analysis results.

Not selected as it may not provide the required integration with FortiSandbox.

Implementation Steps:

Step 1: Ensure FortiSandbox is configured to send analysis results to FortiAnalyzer.

Step 2: Use the FortiSandbox connector in the playbook to fetch events related to malicious attachments.

Step 3: Configure the GET_EVENTS action to use the FortiSandbox connector.

Step 4: Set up the RUN_REPORT and CREATE_INCIDENT actions based on the fetched events.

References:

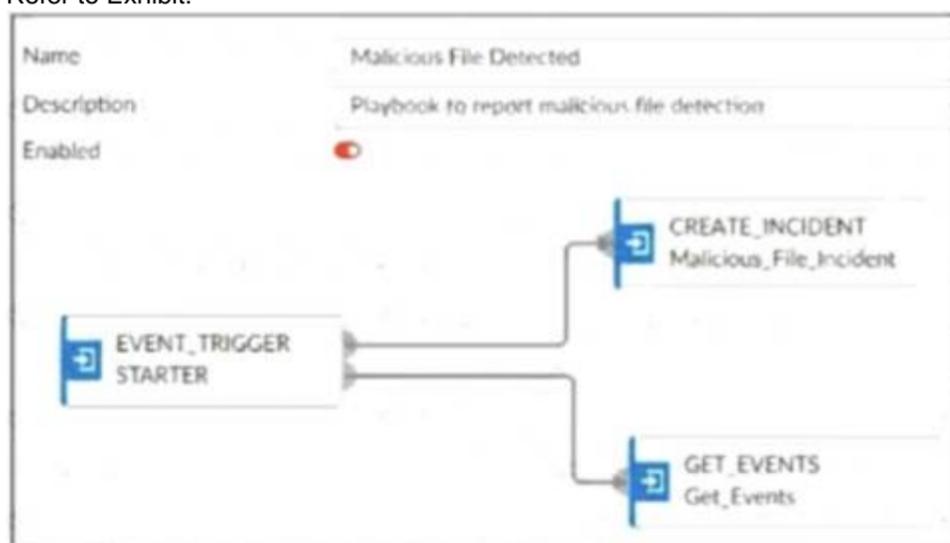
Fortinet Documentation on FortiSandbox Integration FortiSandbox Integration Guide

Fortinet Documentation on FortiAnalyzer Event Handling FortiAnalyzer Administration Guide

By using the FortiSandbox connector, the analyst can ensure that the playbook accurately fetches events based on FortiSandbox analysis and generates the required incident and report.

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](#)