



Fortinet

Exam Questions FCSS_SOC_AN-7.4

FCSS - Security Operations 7.4 Analyst

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

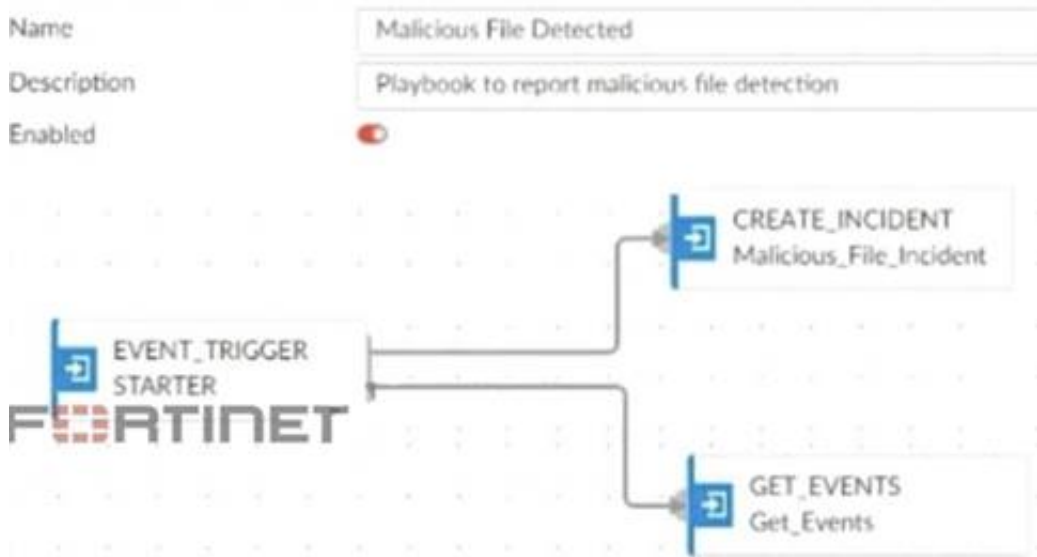
Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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.

FortiAnalyzer Fabric				
Name	IP Address	Platform	Logs	Serial Number
FAZ-SiteA	10.0.1.236	FortiAnalyzer-VM64		FAZ-VMTM24000905
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-VMTM24000908
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	

- 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.

Explanation:

Best Practices for Security Fabric Deployment with FortiAnalyzer.

Refer to the exhibits.

Status

Name

Spearphishing handler

Description

0/1024

MITRE Domain

N/A

Enterprise

ICS

Data Selector

Click to select

Automation Switch

Rules

Spearphishing Rule 1

Add New Rule

Handler Settings

Notifications

Spearphishing Alert

- A. In the Log Type field, change the selection to AntiVirus Log (malware).
- B. Configure a FortiSandbox data selector and add it to the event handler.
- C. In the Log Filter by Text field, type the value: 5 unique malware re..
- D. Change trigger condition by selecting
- E. Within a group, the log field Malware Name (mname) has 2 or more unique values.

Explanation:

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

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 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 areinputandoutput.

References:

Fortinet Documentation on Playbook Configuration and Variable Usage.

General SOC Automation and Orchestration Practices.

NEW QUESTION 6

Refer to Exhibit:



The screenshot shows the FortiAnalyzer configuration interface. Under the 'Data Policy' section, 'Keep Logs for Analytics' is set to 60 Days and 'Keep Logs for Archive' is set to 120 Days. Under the 'Disk Utilization' section, 'Allocated' space is 300 GB, with a note that the 'Maximum Available' is 441.0 GB. The 'Analytics: Archive' ratio is set to 30% for analytics and 70% for archive, with a 'Modify' button next to it. The 'Alert and Delete When Usage Reaches' is set to 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 7

Which FortiAnalyzer feature uses the SIEM database for advance log analytics and monitoring?

- A. Threat hunting
- B. Asset Identity Center

- C. Event monitor
D. Outbreak alerts

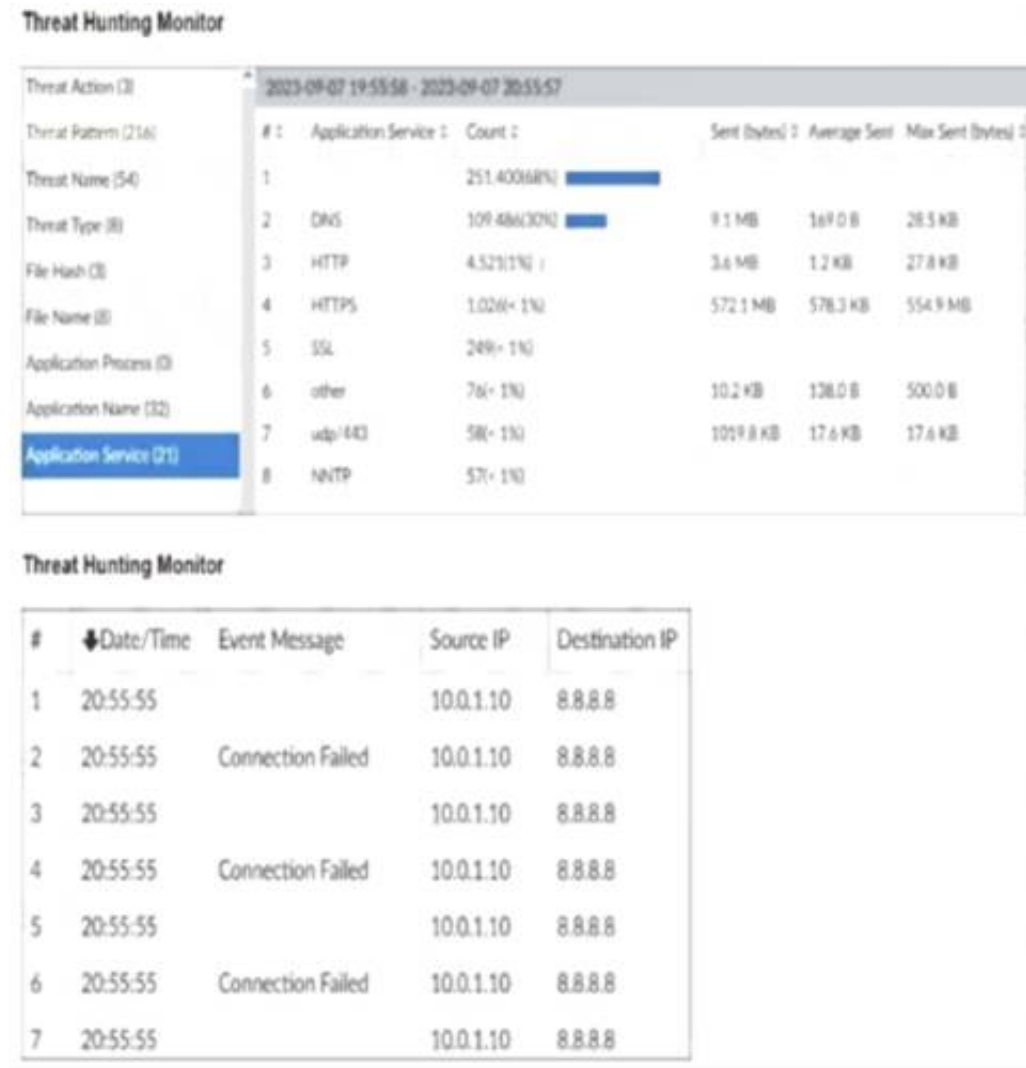
Answer: A

Explanation:

Understanding FortiAnalyzer Features:
FortiAnalyzer includes several features for log analytics, monitoring, and incident response.
The SIEM (Security Information and Event Management) database is used to store and analyze log data, providing advanced analytics and insights.
Evaluating the Options:
Option A: Threat hunting
Threat hunting involves proactively searching through log data to detect and isolate threats that may not be captured by automated tools. This feature leverages the SIEM database to perform advanced log analytics, correlate events, and identify potential security incidents.
Option B: Asset Identity Center
This feature focuses on asset and identity management rather than advanced log analytics.
Option C: Event monitor
While the event monitor provides real-time monitoring and alerting based on logs, it does not specifically utilize advanced log analytics in the way the SIEM database does for threat hunting.
Option D: Outbreak alerts
Outbreak alerts provide notifications about widespread security incidents but are not directly related to advanced log analytics using the SIEM database.
Conclusion:
The feature that uses the SIEM database for advanced log analytics and monitoring in FortiAnalyzer isThreat hunting.
References:
Fortinet Documentation on FortiAnalyzer Features and SIEM Capabilities.
Security Best Practices and Use Cases for Threat Hunting.

NEW QUESTION 8

Refer to the exhibits.



What can you conclude from analyzing the data using the threat hunting module?

- A. Spearphishing is being used to elicit sensitive information.
B. DNS tunneling is being used to extract confidential data from the local network.
C. Reconnaissance is being used to gather victim identityinformation from the mail server.
D. FTP is being used as command-and-control (C&C) technique to mine for data.

Answer: B

Explanation:

Understanding the Threat Hunting Data:
The Threat Hunting Monitor in the provided exhibits shows various application services, their usage counts, and data metrics such as sent bytes, average sent bytes, and maximum sent bytes.
The second part of the exhibit lists connection attempts from a specific source IP (10.0.1.10) to a destination IP (8.8.8.8), with repeated "Connection Failed" messages.
Analyzing the Application Services:
DNS is the top application service with a significantly high count (251,400) and notable sent bytes (9.1 MB).
This large volume of DNS traffic is unusual for regular DNS queries and can indicate the presence of DNS tunneling.
DNS Tunneling:
DNS tunneling is a technique used by attackers to bypass security controls by encoding data within DNS queries and responses. This allows them to extract data from the local network without detection.

The high volume of DNS traffic, combined with the detailed metrics, suggests that DNS tunneling might be in use.

Connection Failures to 8.8.8.8:

The repeated connection attempts from the source IP (10.0.1.10) to the destination IP (8.8.8.8) with connection failures can indicate an attempt to communicate with an external server.

Google DNS (8.8.8.8) is often used for DNS tunneling due to its reliability and global reach.

Conclusion:

Given the significant DNS traffic and the nature of the connection attempts, it is reasonable to conclude that DNS tunneling is being used to extract confidential data from the local network.

Why Other Options are Less Likely:

Spearphishing (A): There is no evidence from the provided data that points to spearphishing attempts, such as email logs or phishing indicators.

Reconnaissance (C): The data does not indicate typical reconnaissance activities, such as scanning or probing mail servers.

FTP C&C (D): There is no evidence of FTP traffic or command-and-control communications using FTP in the provided data.

References:

SANS Institute: "DNS Tunneling: How to Detect Data Exfiltration and Tunneling Through DNS Queries" SANS DNS Tunneling

OWASP: "DNS Tunneling" OWASP DNS Tunneling

By analyzing the provided threat hunting data, it is evident that DNS tunneling is being used to exfiltrate data, indicating a sophisticated method of extracting confidential information from the network.

NEW QUESTION 9

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

.....

Relate Links

100% Pass Your FCSS_SOC_AN-7.4 Exam with Exambible Prep Materials

https://www.exambible.com/FCSS_SOC_AN-7.4-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>