



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 the exhibit.

Name	IP Address	Platform	Logs	Serial Number
FAZ-SiteA	10.0.1.236	FortiAnalyzer-VM64		FAZ-VM2M24000905
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-VM2M24000908
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 2

Which three end user logs does FortiAnalyzer use to identify possible IOC compromised hosts? (Choose three.)

- A. Email filter logs
- B. DNS filter logs
- C. Application filter logs
- D. IPS logs
- E. Web filter logs

Answer: BDE

Explanation:

Overview of Indicators of Compromise (IoCs): Indicators of Compromise (IoCs) are pieces of evidence that suggest a system may have been compromised. These can include unusual network traffic patterns, the presence of known malicious files, or other suspicious activities.

FortiAnalyzer's Role: FortiAnalyzer aggregates logs from various Fortinet devices to provide comprehensive visibility and analysis of network events. It uses these logs to identify potential IoCs and compromised hosts.

Relevant Log Types:

DNS Filter Logs:

DNS requests are a common vector for malware communication. Analyzing DNS filter logs helps in identifying suspicious domain queries, which can indicate malware attempting to communicate with command and control (C2) servers.

NEW QUESTION 3

Which FortiAnalyzer connector can you use to run automation stitches?

- A. FortiCASB
- B. FortiMail
- C. Local
- D. FortiOS

Answer: D

Explanation:

- > Overview of Automation Stitches:
- > Automation stitches in FortiAnalyzer are predefined sets of automated actions triggered by specific events. These actions help in automating responses to security incidents, improving efficiency, and reducing the response time.
- > FortiAnalyzer Connectors:
- > FortiAnalyzer integrates with various Fortinet products and other third-party solutions through connectors. These connectors facilitate communication and data exchange, enabling centralized management and automation.
- > Available Connectors for Automation Stitches:
- > FortiCASB:
- > FortiCASB is a Cloud Access Security Broker that helps secure SaaS applications. However, it is not typically used for running automation stitches within FortiAnalyzer.

NEW QUESTION 4

Which statement best describes the MITRE ATT&CK framework?

- A. It provides 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 5

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 (sname) 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.

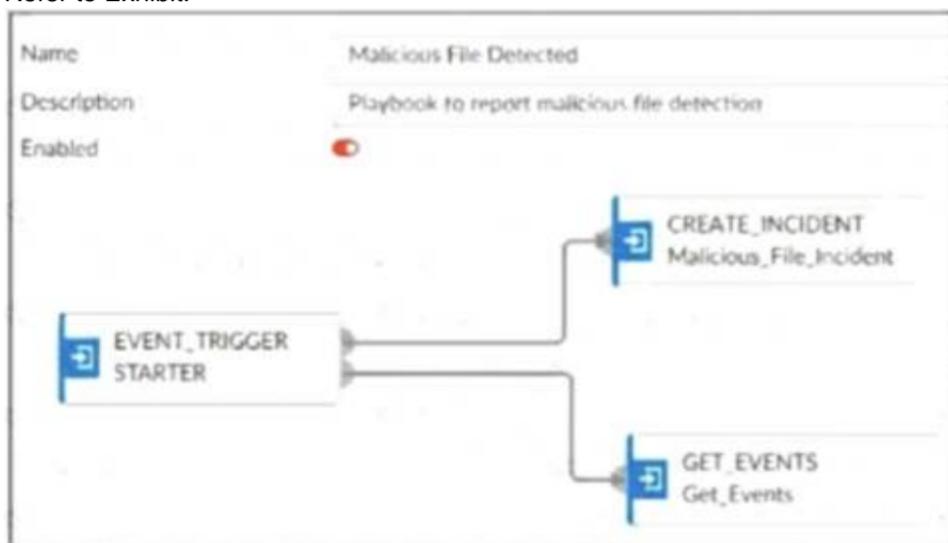
References:

Fortinet Documentation on Event Handlers and Log Types.

Best Practices for Configuring FortiMail Anti-Spam Settings.

NEW QUESTION 6

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

.....

Relate Links

100% Pass Your FCSS_SOC_AN-7.4 Exam with Examible 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/>