

Exam Questions FCSS_SOC_AN-7.4

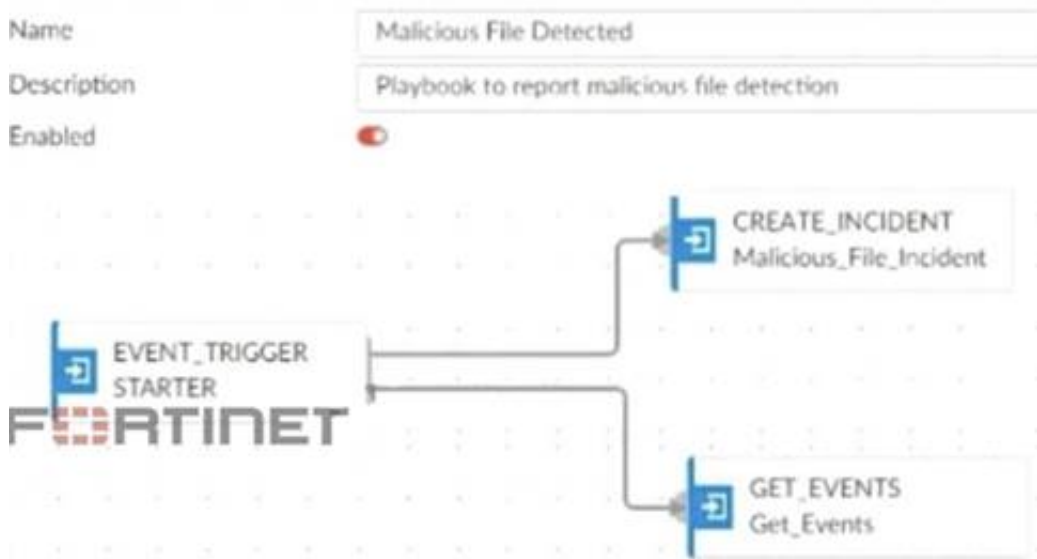
FCSS - Security Operations 7.4 Analyst

https://www.2passeasy.com/dumps/FCSS_SOC_AN-7.4/



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	
Site-B-Fabric	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	

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

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 4

Refer to the exhibits.

Event Handler

The screenshot shows the 'Event Handler' configuration page in FortiMail. The 'Name' field is 'SOC SMTP Enumeration Data Handler'. The 'MITRE Domain' is 'N/A'. The 'MITRE Tech ID' field has a search bar and two selected entries: 'T1589 Gather Victim Identity Information' and 'T1589.002 Email Addresses'. The 'Data Selector' is 'SOC SMTP Enumeration Data Selector'. The 'Automation Switch' is turned on. The 'Rules' section shows 'SOC Antispam Rule 1'.

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

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%	<input checked="" type="checkbox"/> Modify
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 the analytics-to-archive ratio being 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

Refer to the exhibits.

Playbook configuration

Name

FortiMail Sender Blocklist

Description

Send IOC email addresses and IP addresses to FortiMail Blocklist

Enabled

ON_DEMAND STARTER

ADD_SENDER_TO_BLOCKLIST

Block_list

FortiMail connector actions

Configuration	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 8

Which two statements about the FortiAnalyzer Fabric topology are true? (Choose two.)

- A. Downstream collectors can forward logs to Fabric members.
- B. Logging devices must be registered to the supervisor.
- C. The supervisor uses an API to store logs, incidents, and events locally.
- D. Fabric members must be in analyzer mode.

Answer: BD

Explanation:

The FortiAnalyzer Fabric topology is designed to centralize logging and analysis across multiple devices in a network. It involves a hierarchy where the supervisor node manages and coordinates with other Fabric members.
Analyzing the Options:
Option A:Downstream collectors forwarding logs to Fabric members is not a typical configuration. Instead, logs are usually centralized to the supervisor.
Option B:For effective management and log centralization, logging devices must be registered to the supervisor. This ensures proper log collection and coordination.
Option C:The supervisor does not primarily use an API to store logs, incidents, and events locally. Logs are stored directly in the FortiAnalyzer database.
Option D:For the Fabric topology to function correctly, all Fabric members need to be in analyzer mode. This mode allows them to collect, analyze, and forward logs appropriately within the topology.

Conclusion:

The correct statements regarding the FortiAnalyzer Fabric topology are that logging devices must be registered to the supervisor and that Fabric members must be in analyzer mode.

References:

Fortinet Documentation on FortiAnalyzer Fabric Topology.

Best Practices for Configuring FortiAnalyzer in a Fabric Environment.

NEW QUESTION 10

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCSS_SOC_AN-7.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCSS_SOC_AN-7.4 Product From:

https://www.2passeasy.com/dumps/FCSS_SOC_AN-7.4/

Money Back Guarantee

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