Fortinet.FCSS_SOC_AN-7.4.v2024-12-09.q31

Exam Code:	FCSS_SOC_AN-7.4
Exam Name:	FCSS - Security Operations 7.4 Analyst
Certification Provider:	Fortinet
Free Question Number:	31
Version:	v2024-12-09
# of views:	1213
# of Questions views:	310
https://www.freepdfdumps.com/Fortinet.FCSS_SOC_AN-7.4.v2024-12-09.q31.html	

NEW QUESTION: 1
In managing connectors within a SOC, what is a key benefit of ensuring proper integration?
A. It enhances the aesthetic appeal of the SOC
B. It simplifies the legal compliance of the SOC
C. It reduces the need for cybersecurity training
D. It ensures seamless data exchange and process automation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 2
Which of the following is a crucial consideration when configuring connectors in a SOC playbook?
A. Minimizing the physical space used by servers
B. Facilitating data flow between different security tools
C. Ensuring compatibility with external marketing tools
D. Designing a visually appealing user interface
Answer: B (LEAVE A REPLY)

NEW QUESTION: 3
Which two assets are available with the outbreak alert licensed feature on FortiAnalyzer?
(Choose two.)
A. Custom connectors from FortiGuard
B. Custom outbreak reports
C. Outbreak-specific custom playbooks
D. Custom event handlers from FortiGuard
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 4
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	10.200.200.238	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: A,D (LEAVE A REPLY)

* 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-SiteAandFAZ-SiteBare FortiAnalyzer devices in the fabric.
* FortiGate-B1andFortiGate-B2are shown under theSite-B-Fabric, indicating they are part of the same Security Fabric.
* FAZ-SiteAhas multiple entries under it:SiteAandMSSP-Local, suggesting multiple ADOMs are enabled.
* Evaluating the Options:
* Option A:FortiGate-B1 and FortiGate-B2 are underSite-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 underFAZ-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: 5
What is the primary purpose of configuring playbook triggers in SOC automation?
A. To manually control network traffic
B. To document incident response procedures
C. To initiate automated responses based on specific conditions
D. To schedule regular maintenance windows
Answer: C (LEAVE A REPLY)

NEW QUESTION: 6
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: (SHOW ANSWER)
* 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.

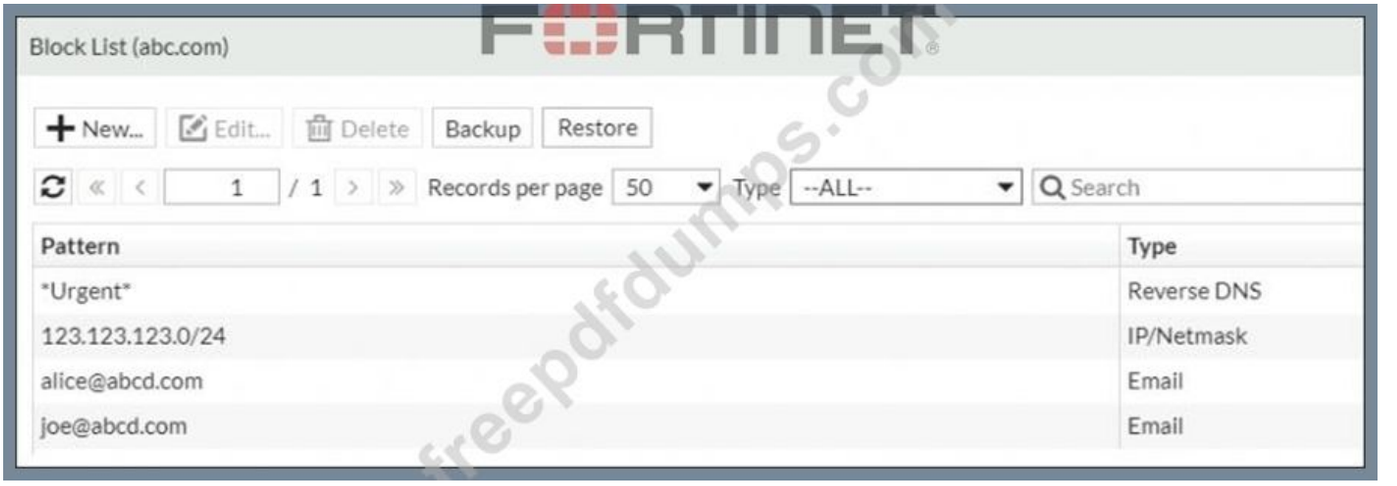
NEW QUESTION: 7
When configuring a FortiAnalyzer to act as a collector device, which two steps must you perform? (Choose two.)
A. Configure Fabric authorization on the connecting interface.
B. Configure log forwarding to a FortiAnalyzer in analyzer mode.

C. Configure the data policy to focus on archiving.
D. Enable log compression.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 8
What role do outbreak alert handlers play in a SOC?
A. They facilitate corporate mergers and acquisitions.
B. They coordinate marketing campaigns.
C. They predict stock market changes.
D. They provide automated responses to detected outbreaks.
Answer: D (LEAVE A REPLY)

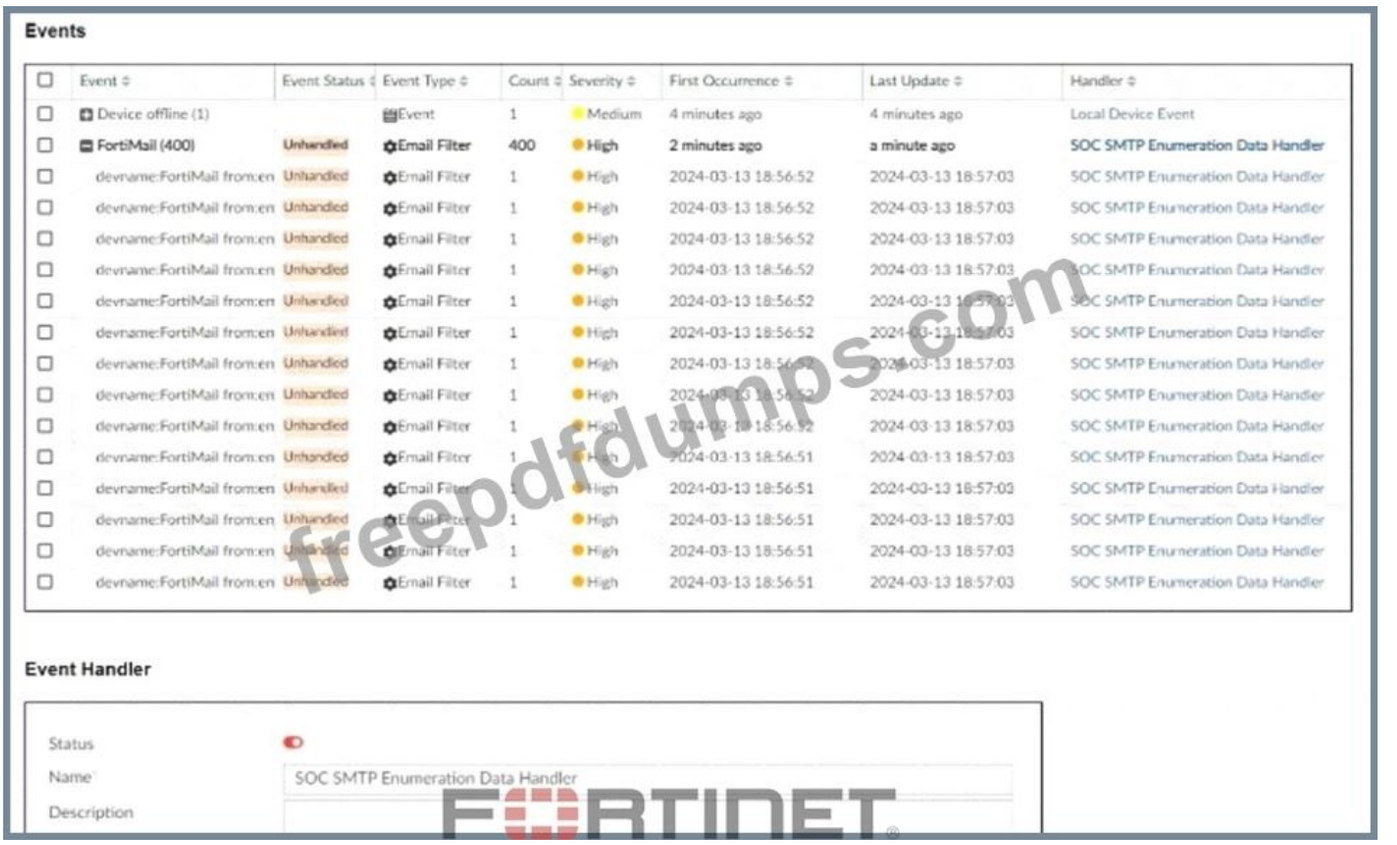
NEW QUESTION: 9
Refer to the exhibits.
Domain List:

Domain abc.com:



Which connector and action on FortiAnalyzer can you use to add the entries show in the exhibits?
A. The FortiClient EMS connector and the quarantine action
B. The Local connector and the update asset and identity action
C. The FortiMail connector and the get sender reputation action
D. The FortiMail connector and the add send to blocklist action
Answer: (SHOW ANSWER)

NEW QUESTION: 10
Refer to the exhibit.



You notice that the custom event handler you configured to detect SMTP reconnaissance activities is creating a large number of events. This is overwhelming your notification system. How can you fix this?

A. Increase the trigger count so that it identifies and reduces the count triggered by a particular group.

B. Disable the custom event handler because it is not working as expected.

C. Decrease the time range that the custom event handler covers during the attack.

D. Increase the log field value so that it looks for more unique field values when it creates the event.

Answer: A (LEAVE A REPLY)

* Understanding the Issue:

* The custom event handler for detecting SMTP reconnaissance activities is generating a large number of events.

* This high volume of events is overwhelming the notification system, leading to potential alert fatigue and inefficiency in incident response.

* Event Handler Configuration:

* Event handlers are configured to trigger alerts based on specific criteria.

* The frequency and volume of these alerts can be controlled by adjusting the trigger conditions.

* Possible Solutions:

* A. Increase the trigger count so that it identifies and reduces the count triggered by a particular group:

* By increasing the trigger count, you ensure that the event handler only generates alerts after a higher threshold of activity is detected.

* This reduces the number of events generated and helps prevent overwhelming the notification system.
* Selected as it effectively manages the volume of generated events.
* B. Disable the custom event handler because it is not working as expected:
* Disabling the event handler is not a practical solution as it would completely stop monitoring for SMTP reconnaissance activities.
* Not selected as it does not address the issue of fine-tuning the event generation.
* C. Decrease the time range that the custom event handler covers during the attack:
* Reducing the time range might help in some cases, but it could also lead to missing important activities if the attack spans a longer period.
* Not selected as it could lead to underreporting of significant events.
* D. Increase the log field value so that it looks for more unique field values when it creates the event:
* Adjusting the log field value might refine the event criteria, but it does not directly control the volume of alerts.
* Not selected as it is not the most effective way to manage event volume.
* Implementation Steps:
* Step 1: Access the event handler configuration in FortiAnalyzer.
* Step 2: Locate the trigger count setting within the custom event handler for SMTP reconnaissance.
* Step 3: Increase the trigger count to a higher value that balances alert sensitivity and volume.
* Step 4: Save the configuration and monitor the event generation to ensure it aligns with expected levels.
* Conclusion:
* By increasing the trigger count, you can effectively reduce the number of events generated by the custom event handler, preventing the notification system from being overwhelmed.
References:
* Fortinet Documentation on Event Handlers and Configuration FortiAnalyzer Administration Guide
* Best Practices for Event Management Fortinet Knowledge Base
By increasing the trigger count in the custom event handler, you can manage the volume of generated events and prevent the notification system from being overwhelmed.

NEW QUESTION: 11
How does identifying adversary behavior benefit SOC operations in terms of incident response?
A. By reducing the importance of endpoint security
B. By allowing for a quicker isolation of affected systems
C. By providing data for marketing strategies
D. By increasing the time it takes to respond to incidents
Answer: B (LEAVE A REPLY)

NEW QUESTION: 12
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: B,D (LEAVE A REPLY)
* Understanding FortiAnalyzer Fabric Topology:
* 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: 13
Which feature should be prioritized when configuring collectors in a high-traffic network environment?
A. Low-latency data processing
B. High-frequency log rotation
C. Periodic storage expansion
D. Aesthetic interface adjustments
Answer: A (LEAVE A REPLY)

NEW QUESTION: 14
Which trigger type requires manual input to run a playbook?
A. ON_DEMAND

B. INCIDENT_TRIGGER
C. EVENT_TRIGGER
D. ON_SCHEDULE
Answer: (SHOW ANSWER)

NEW QUESTION: 15
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 (LEAVE A REPLY)
* 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: 16
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: (SHOW ANSWER)
* 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: 17

Which of the following should be a priority when monitoring SOC playbooks?

A. Ensuring that playbooks are printed and distributed

B. Checking for the timely execution of tasks

C. Watching for unusual increases in playbook file sizes

D. Monitoring the personal emails of SOC analysts

Answer: B (LEAVE A REPLY)

NEW QUESTION: 18

Refer to the exhibits.

You configured a spearphishing event handler and the associated rule. However. FortiAnalyzer did not generate an event.

When you check the FortiAnalyzer log viewer, you confirm that FortiSandbox forwarded the appropriate logs, as shown in the raw log exhibit.

What configuration must you change on FortiAnalyzer in order for FortiAnalyzer to generate an event?

A. In the Log Type field, changethe selection toAntiVirus Log(malware).

B. Configure a FortiSandbox data selector and add it tothe event handler.

C. In the Log Filter by Text field, type the value:.5 ub t ype ma lwa re..

D. Change trigger condition by selecting. Within a group, the log field Malware Kame (mname> has 2 or more unique values.

Answer: B (LEAVE A REPLY)

* Understanding the Event Handler Configuration:
* 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: 19
Why is it crucial to configure playbook triggers based on accurate threat intelligence?
A. To increase the number of digital advertisements
B. To prevent the triggering of irrelevant or false positive actions
C. To facilitate easier management of office supplies
D. To ensure SOC parties are well-attended
Answer: B (LEAVE A REPLY)

NEW QUESTION: 20
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 (LEAVE A REPLY)
* 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: 21
What should be a priority when configuring playbook tasks to ensure effective SOC automation?
A. Making tasks visible to external stakeholders

B. Limiting tasks to non-critical alerts
C. Ensuring tasks are scheduled during office hours only
D. Aligning tasks with the specific stages of incident response
Answer: D (LEAVE A REPLY)

NEW QUESTION: 22
What is a key objective of managing outbreak alert handlers in a SOC?
A. To quickly contain and mitigate threats
B. To minimize the impact of false positives
C. To increase sales and marketing efforts
D. To ensure seamless business operations
Answer: A (LEAVE A REPLY)

NEW QUESTION: 23
When designing a FortiAnalyzer Fabric deployment, what is a critical consideration for ensuring high availability?
A. Implementing a minimalistic user interface
B. Designing redundant network paths
C. Regular firmware updates
D. Configuring single sign-on
Answer: B (LEAVE A REPLY)

NEW QUESTION: 24
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: B,D (LEAVE A REPLY)
* 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: 25
Which configuration would enhance the efficiency of a FortiAnalyzer deployment in terms of data throughput?
A. Decreasing the report generation frequency
B. Lowering the security settings
C. Reducing the number of backup locations
D. Increasing the number of collectors
Answer: (SHOW ANSWER)

NEW QUESTION: 26
Which elements should be included in an effective SOC report?
(Choose Three)
A. Summary of incidents and their statuses
B. Marketing analysis for the quarter
C. Detailed analysis of every logged event
D. Recommendations for improving security posture
E. Action items for follow-up
Answer: A,D,E (LEAVE A REPLY)

NEW QUESTION: 27
During a security incident analysis, if an adversary's behavior is identified as 'Credential Dumping', it maps to which MITRE ATT&CK technique?
A. T1059
B. T1003
C. T1566
D. T1110
Answer: (SHOW ANSWER)

NEW QUESTION: 28
Which role does a threat hunter play within a SOC?
A. investigate and respond to a reported security incident
B. Monitor network logs to identify anomalous behavior

C. Collect evidence and determine the impact of a suspected attack
D. Search for hidden threats inside a network which may have eluded detection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 29
In the context of threat hunting, which information feeds are most beneficial?
A. Corporate governance updates
B. Marketing data
C. Cyber threat intelligence
D. Stock market trends
Answer: (SHOW ANSWER)

NEW QUESTION: 30
Refer to the exhibits.

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. In the Log filter by Text field, type type==spam.
C. Disable the rule to use the filter in the data selector to create the event.

D. 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 (LEAVE A REPLY)

* 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:Typingtype==spamin 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: 31

Configuring playbook triggers correctly is crucial for which aspect of SOC automation?

A. Increasing the manual tasks in the SOC

B. Automating responses to detected incidents based on predefined conditions

C. Ensuring that all security incidents receive a human response

D. Making sure that SOC analysts are kept busy

Answer: B (LEAVE A REPLY)

answers have been corrected get the **newest** Actual4test.com FCSS_SOC_AN-7.4 dumps with Test Engine here: https://www.actual4test.com/FCSS_SOC_AN-7.4_examcollection.html (**90** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

Valid FCSS_SOC_AN-7.4 Dumps shared by Actual4test.com for Helping Passing FCSS_SOC_AN-7.4 Exam! Actual4test.com now offer the **newest FCSS_SOC_AN-7.4 exam dumps**, the Actual4test.com FCSS_SOC_AN-7.4 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com FCSS_SOC_AN-7.4 dumps with Test Engine here: https://www.actual4test.com/FCSS_SOC_AN-7.4_examcollection.html (**90** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)