Exam Questions FCSS_SOC_AN-7.4

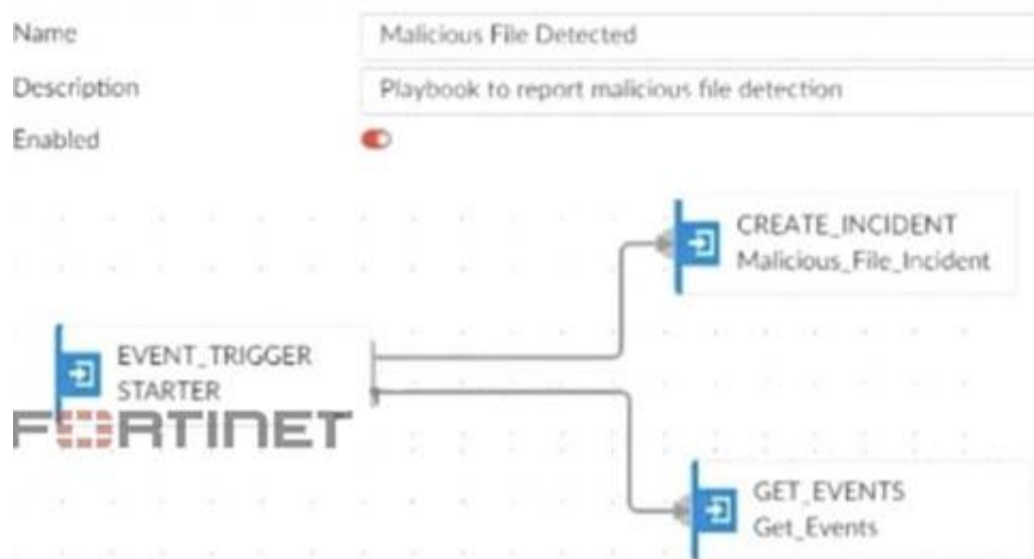FCSS - Security Operations 7.4 Analyst

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
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 3
Refer to the exhibit.

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-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 4
Refer to the exhibit,

which shows the partial output of the MITRE ATT&CK Enterprise matrix on FortiAnalyzer. Which two statements are true? (Choose two.)

A. There are four techniques that fall under tactic T1071.
B. There are four subtechniques that fall under technique T1071.
C. There are event handlers that cover tactic T1071.

D. There are 15 events associated with the tactic.

Answer: BC

Explanation:
Understanding the MITRE ATT&CK Matrix:
The MITRE ATT&CK framework is a knowledge base of adversary tactics and techniques based on real-world observations.
Each tactic in the matrix represents the "why" of an attack technique, while each technique represents "how" an adversary achieves a tactic.
Analyzing the Provided Exhibit:
The exhibit shows part of the MITRE ATT&CK Enterprise matrix as displayed on FortiAnalyzer.
The focus is on technique T1071 (Application Layer Protocol), which has subtechniques labeled T1071.001, T1071.002, T1071.003, and T1071.004.
Each subtechnique specifies a different type of application layer protocol used for Command and Control (C2):
T1071.001 Web Protocols
T1071.002 File Transfer Protocols
T1071.003 Mail Protocols
T1071.004 DNS
Identifying Key Points:
Subtechniques under T1071:There are four subtechniques listed under the primary technique T1071, confirming that statement B is true.
Event Handlers for T1071:FortiAnalyzer includes event handlers for monitoring various tactics and techniques. The presence of event handlers for tactic T1071 suggests active monitoring and alerting for these specific subtechniques, confirming that statement C is true.
Misconceptions Clarified:
Statement A (four techniques under tactic T1071) is incorrect because T1071 is a single technique with four subtechniques.
Statement D (15 events associated with the tactic) is misleading. The number 15 refers to the techniques under the Application Layer Protocol, not directly related to the number of events.
Conclusion:
The accurate interpretation of the exhibit confirms that there are four subtechniques under technique T1071 and that there are event handlers covering tactic T1071.
References:
MITRE ATT&CK Framework documentation.
FortiAnalyzer Event Handling and MITRE ATT&CK Integration guides.

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 ofInitial AccessandPersistence.
References:
MITRE ATT&CK Framework documentation on Initial Access and Persistence tactics.
Incident analysis and mapping to MITRE ATT&CK tactics.

NEW QUESTION 6
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.
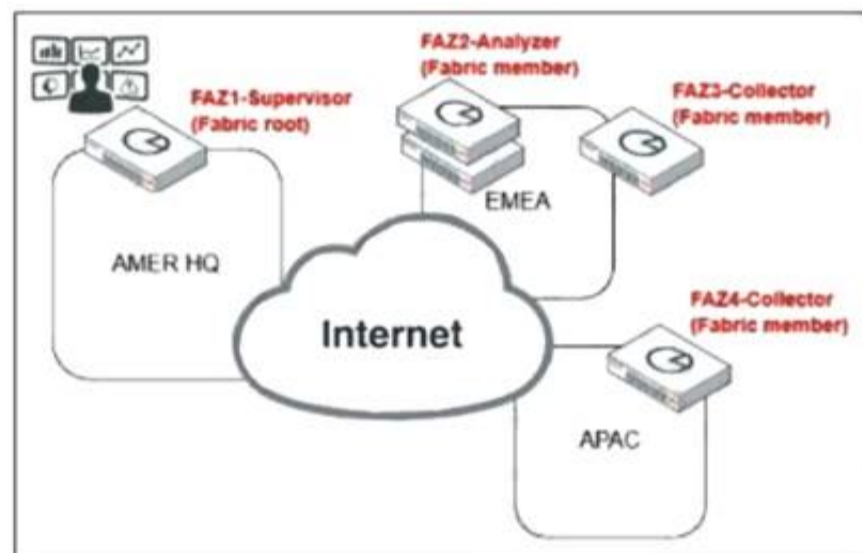Relevant Log Types:
DNS Filter Logs:
DNS requests are a common vector for malware communication. Analyzing DNS filter logs helps in identifying suspicious domain queries, which can indicate malware attempting to communicate with command and control (C2) servers.

NEW QUESTION 7
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-Supervisoris located at AMER HQ and acts as the Fabric root.
FAZ2-Analyzeris a Fabric member located in EMEA.
FAZ3-CollectorandFAZ4-Collectorare 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 8
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: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 9
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 10
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

Explanation:
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 10
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: BD

Explanation:
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 14
......

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