

FCSS_SOC_AN-7.4 Dumps

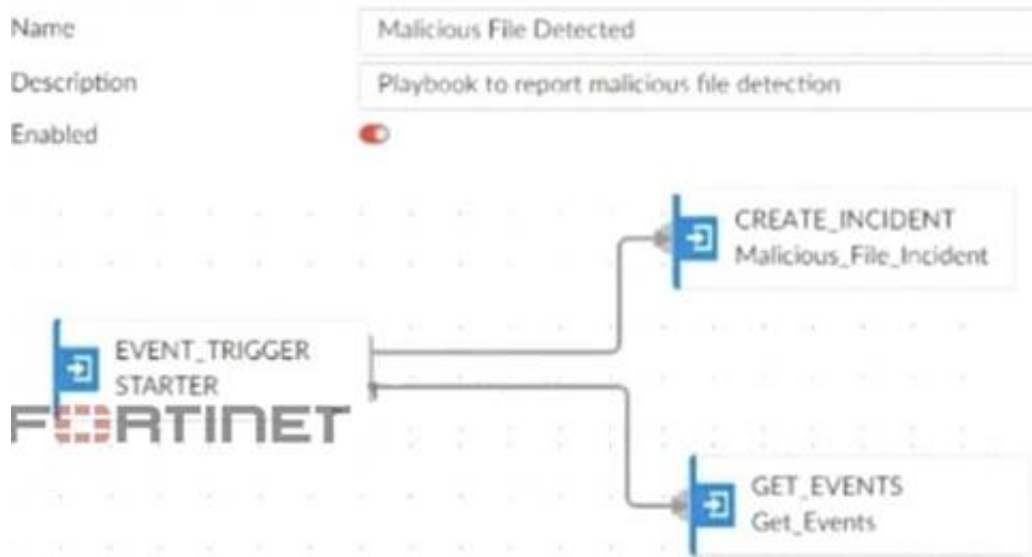
FCSS - Security Operations 7.4 Analyst

https://www.certleader.com/FCSS_SOC_AN-7.4-dumps.html



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 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 2

Which two playbook triggers enable the use of trigger events in later tasks as trigger variables? (Choose two.)

- A. EVENT
- B. INCIDENT
- C. ON SCHEDULE
- D. ON DEMAND

Answer: AB

Explanation:

Understanding Playbook Triggers:

Playbook triggers are the starting points for automated workflows within FortiAnalyzer or FortiSOAR.

These triggers determine how and when a playbook is executed and can pass relevant information (trigger variables) to subsequent tasks within the playbook.

Types of Playbook Triggers:

EVENT Trigger:

Initiates the playbook when a specific event occurs.

The event details can be used as variables in later tasks to customize the response.

Selected as it allows using event details as trigger variables.

INCIDENT Trigger:

Activates the playbook when an incident is created or updated.

The incident details are available as variables in subsequent tasks.

Selected as it enables the use of incident details as trigger variables.

ON SCHEDULE Trigger:

Executes the playbook at specified times or intervals.

Does not inherently use trigger events to pass variables to later tasks.
Not selected as it does not involve passing trigger event details.
ON DEMAND Trigger:
Runs the playbook manually or as required.
Does not automatically include trigger event details for use in later tasks.
Not selected as it does not use trigger events for variables.
Implementation Steps:
Step 1: Define the conditions for the EVENT or INCIDENT trigger in the playbook configuration.
Step 2: Use the details from the trigger event or incident in subsequent tasks to customize actions and responses.
Step 3: Test the playbook to ensure that the trigger variables are correctly passed and utilized.
Conclusion:
EVENT and INCIDENT triggers are specifically designed to initiate playbooks based on specific occurrences, allowing the use of trigger details in subsequent tasks.
References:
Fortinet Documentation on Playbook Configuration FortiSOAR Playbook Guide
By using the EVENT and INCIDENT triggers, you can leverage trigger events in later tasks as variables, enabling more dynamic and responsive playbook actions.

NEW QUESTION 3
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	10.200.208.236	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 4
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 5

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 6

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 7

Refer to the exhibits.

Event Handler

The screenshot shows the 'Event Handler' configuration page in FortiAnalyzer. The 'Name' field is 'SOC SMTP Enumeration Data Handler'. The 'Description' field is empty. The 'MITRE Domain' field is 'N/A'. The 'MITRE Tech ID' field is expanded, showing a list of selected entries: 'T1589 Gather Victim Identity Information' and 'T1589.002 Email Addresses'. The 'Data Selector' field is expanded, showing the selected entry: 'SOC SMTP Enumeration Data Selector'. The 'Automation Stitch' field is set to 'On'. The 'Rules' field is empty.

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 8

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 9

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 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 10

Refer to Exhibit:

The screenshot shows two configuration sections. The 'Data Policy' section has 'Keep Logs for Analytics' set to 60 Days and 'Keep Logs for Archive' set to 120 Days. The 'Disk Utilization' section shows 'Allocated' space as 300 GB, with a 'Maximum Available' of 441.0 GB. The 'Analytics: Archive' ratio is set to 30% : 70%, and 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 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 14

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 is Threat hunting.

References:

Fortinet Documentation on FortiAnalyzer Features and SIEM Capabilities.

Security Best Practices and Use Cases for Threat Hunting.

NEW QUESTION 16

Refer to the exhibits.

Threat Hunting Monitor



Threat Hunting Monitor

#	Date/Time	Event Message	Source IP	Destination IP
1	20:55:55		10.0.1.10	8.8.8.8
2	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
3	20:55:55		10.0.1.10	8.8.8.8
4	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
5	20:55:55		10.0.1.10	8.8.8.8
6	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
7	20:55:55		10.0.1.10	8.8.8.8

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 identity information 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 20

Refer to the exhibit.



Which two options describe how the Update Asset and Identity Database playbook is configured? (Choose two.)

- A. The playbook is using a local connector.
- B. The playbook is using a FortiMail connector.
- C. The playbook is using an on-demand trigger.
- D. The playbook is using a FortiClient EMS connector.

Answer: AD

Explanation:

Understanding the Playbook Configuration:

The playbook named "Update Asset and Identity Database" is designed to update the FortiAnalyzer Asset and Identity database with endpoint and user information.

The exhibit shows the playbook with three main components: ON_SCHEDULE STARTER, GET_ENDPOINTS, and UPDATE_ASSET_AND_IDENTITY.

Analyzing the Components:

ON_SCHEDULE STARTER: This component indicates that the playbook is triggered on a schedule, not on-demand.

GET_ENDPOINTS: This action retrieves information about endpoints, suggesting it interacts with an endpoint management system.

UPDATE_ASSET_AND_IDENTITY: This action updates the FortiAnalyzer Asset and Identity database with the retrieved information.

Evaluating the Options:

Option A: The actions shown in the playbook are standard local actions that can be executed by the FortiAnalyzer, indicating the use of a local connector.

Option B: There is no indication that the playbook uses a FortiMail connector, as the tasks involve endpoint and identity management, not email.

Option C: The playbook is using an "ON_SCHEDULE" trigger, which contradicts the description of an on-demand trigger.

Option D: The action "GET_ENDPOINTS" suggests integration with an endpoint management system, likely FortiClient EMS, which manages endpoints and retrieves information from them.

Conclusion:

The playbook is configured to use a local connector for its actions.

It interacts with FortiClient EMS to get endpoint information and update the FortiAnalyzer Asset and Identity database.

References:

Fortinet Documentation on Playbook Actions and Connectors.

FortiAnalyzer and FortiClient EMS Integration Guides.

NEW QUESTION 24

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 25

Refer to the exhibit.

Events

<input type="checkbox"/>	Event 1	Event Status 1	Event Type 1	Count 1	Severity 1	First Occurrence 1	Last Update 1	Handler 1
<input type="checkbox"/>	Device offline (1)		Event	1	Medium	4 minutes ago	4 minutes ago	Local Device Event
<input type="checkbox"/>	FortiMail (400)	Unhandled	Email Filter	400	High	2 minutes ago	a minute ago	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:52	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:51	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:51	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:51	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler
<input type="checkbox"/>	devname:FortiMail from:en	Unhandled	Email Filter	1	High	2024-03-13 18:56:51	2024-03-13 18:57:03	SOC SMTP Enumeration Data Handler

Event Handler

Status

Name

SOC SMTP Enumeration Data Handler

Description

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

Explanation:

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 30

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your FCSS_SOC_AN-7.4 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCSS_SOC_AN-7.4-dumps.html