Fortinet

Exam Questions FCSS_SOC_AN-7.4

FCSS - Security Operations 7.4 Analyst

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

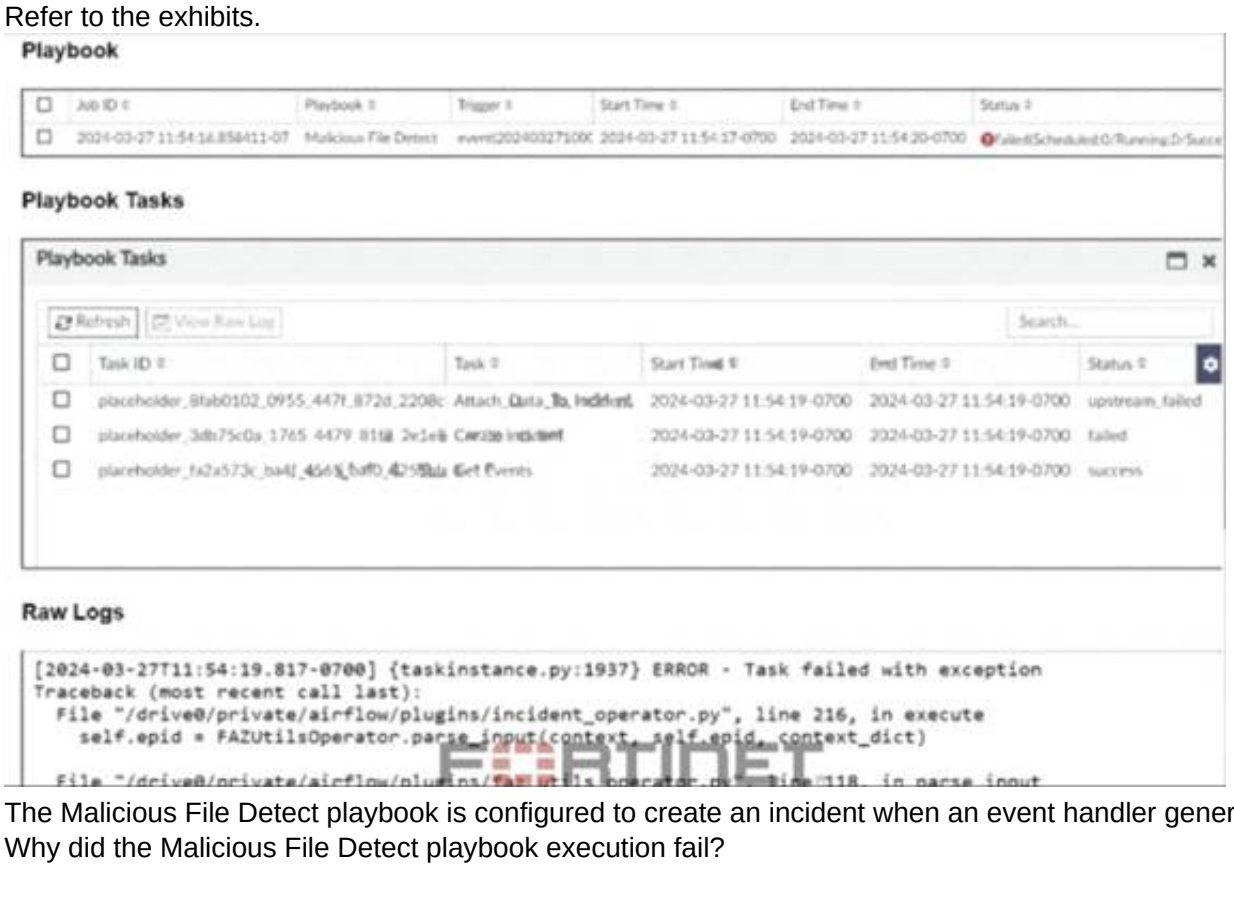
NEW QUESTION 1
A customer wants FortiAnalyzer to run an automation stitch that executes a CLI command on FortiGate to block a predefined list of URLs, if a botnet command-and-control (C&C) server IP is detected.
Which FortiAnalyzer feature must you use to start this automation process?

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 anEvent handlerin FortiAnalyzer.
References:
Fortinet Documentation on Event Handlers and Automation Stitches in FortiAnalyzer.
Best Practices for Configuring Automated Responses in FortiAnalyzer.

NEW QUESTION 2
Refer to the exhibits.



The Malicious File Detect playbook is configured to create an incident when an event handler generates a malicious file detection event.
Why did the Malicious File Detect playbook execution fail?

A. The Create Incident task was expecting a name or number as input, but received an incorrect data format
B. The Get Events task did not retrieve any event data.
C. The Attach_Data_To_Incident incident task wasexpecting an integer, but received an incorrect data format.
D. The Attach Data To Incident task failed, which stopped the playbook execution.

Answer: A

Explanation:
Understanding the Playbook Configuration:
The "Malicious File Detect" playbook is designed to create an incident when a malicious file detection event is triggered.
The playbook includes tasks such asAttach_Data_To_Incident,Create Incident, andGet Events.
Analyzing the Playbook Execution:
The exhibit shows that theCreate Incidenttask has failed, and theAttach_Data_To_Incidenttask has also failed.
TheGet Eventstask succeeded, indicating that it was able to retrieve event data.
Reviewing Raw Logs:
The raw logs indicate an error related to parsing input in theincident_operator.pyfile.
The error traceback suggests that the task was expecting a specific input format (likely a name or number) but received an incorrect data format.
Identifying the Source of the Failure:
TheCreate Incidenttask failure is the root cause since it did not proceed correctly due to incorrect input format.
TheAttach_Data_To_Incidenttask subsequently failed because it depends on the successful creation of an incident.
Conclusion:
The primary reason for the playbook execution failure is that theCreate Incidenttask received an incorrect data format, which was not a name or number as

expected.
References:
Fortinet Documentation on Playbook and Task Configuration.
Error handling and debugging practices in playbook execution.

NEW QUESTION 3
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: C

Explanation:
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 4
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.

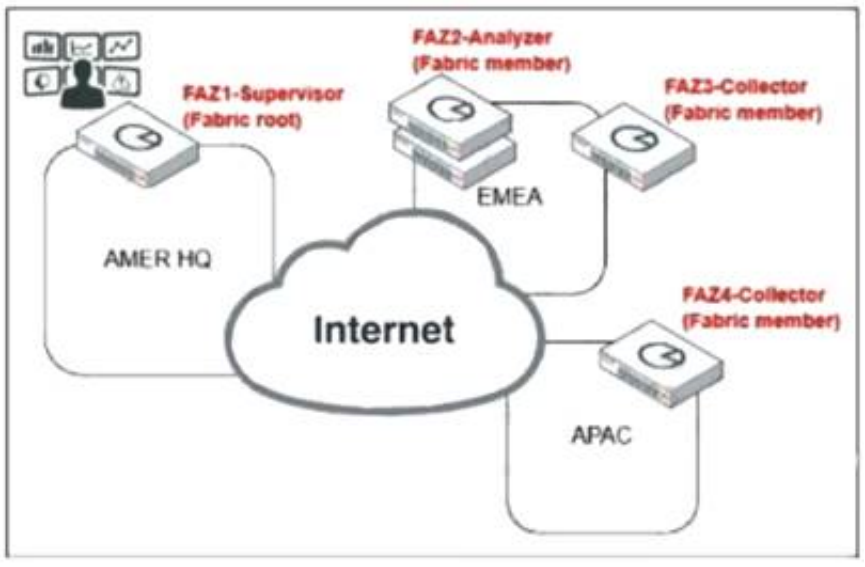
NEW QUESTION 5
Your company is doing a security audit To pass the audit, you must take an inventory of all software and applications running on all Windows devices
Which FortiAnalyzer connector must you use?

A. FortiClient EMS
B. ServiceNow
C. FortiCASB
D. Local Host

Answer: A

Explanation:
Requirement Analysis:
The objective is to inventory all software and applications running on all Windows devices within the organization.
This inventory must be comprehensive and accurate to pass the security audit.
Key Components:
FortiClient EMS (Endpoint Management Server):
FortiClient EMS provides centralized management of endpoint security, including software
and application inventory on Windows devices.
It allows administrators to monitor, manage, and report on all endpoints protected by FortiClient.
Connector Options:
FortiClient EMS:
Best suited for managing and reporting on endpoint software and applications.
Provides detailed inventory reports for all managed endpoints.
Selected as it directly addresses the requirement of taking inventory of software and applications on Windows devices.
ServiceNow:
Primarily a service management platform.
While it can be used for asset management, it is not specifically tailored for endpoint software inventory.
Not selected as it does not provide direct endpoint inventory management.
FortiCASB:
Focuses on cloud access security and monitoring SaaS applications.
Not applicable for managing or inventorying endpoint software.
Not selected as it is not related to endpoint software inventory.
Local Host:
Refers to handling events and logs within FortiAnalyzer itself.
Not specific enough for detailed endpoint software inventory.
Not selected as it does not provide the required endpoint inventory capabilities.
Implementation Steps:
Step 1: Ensure all Windows devices are managed by FortiClient and connected to FortiClient EMS.
Step 2: Use FortiClient EMS to collect and report on the software and applications installed on these devices.
Step 3: Generate inventory reports from FortiClient EMS to meet the audit requirements.
References:
Fortinet Documentation on FortiClient EMS FortiClient EMS Administration Guide
By using the FortiClient EMS connector, you can effectively inventory all software and applications on Windows devices, ensuring compliance with the security audit requirements.

NEW QUESTION 6
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 7
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 8
Which two ways can you create an incident on FortiAnalyzer? (Choose two.)

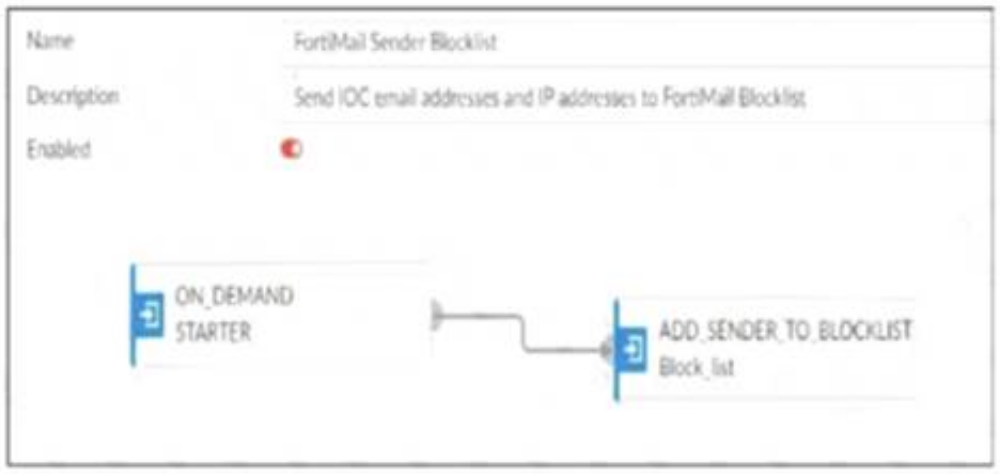
A. Using a connector action
B. Manually, on the Event Monitor page
C. By running a playbook
D. Using a custom event handler

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 9
Refer to the exhibits.

Playbook configuration



FortiMail connector actions

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 failing7

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 FortiAnalzyer 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 10
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 isThreat hunting.
References:
Fortinet Documentation on FortiAnalyzer Features and SIEM Capabilities.
Security Best Practices and Use Cases for Threat Hunting.

NEW QUESTION 10
Refer to the exhibits.

What can you conclude from analyzing the data using the threat hunting module?

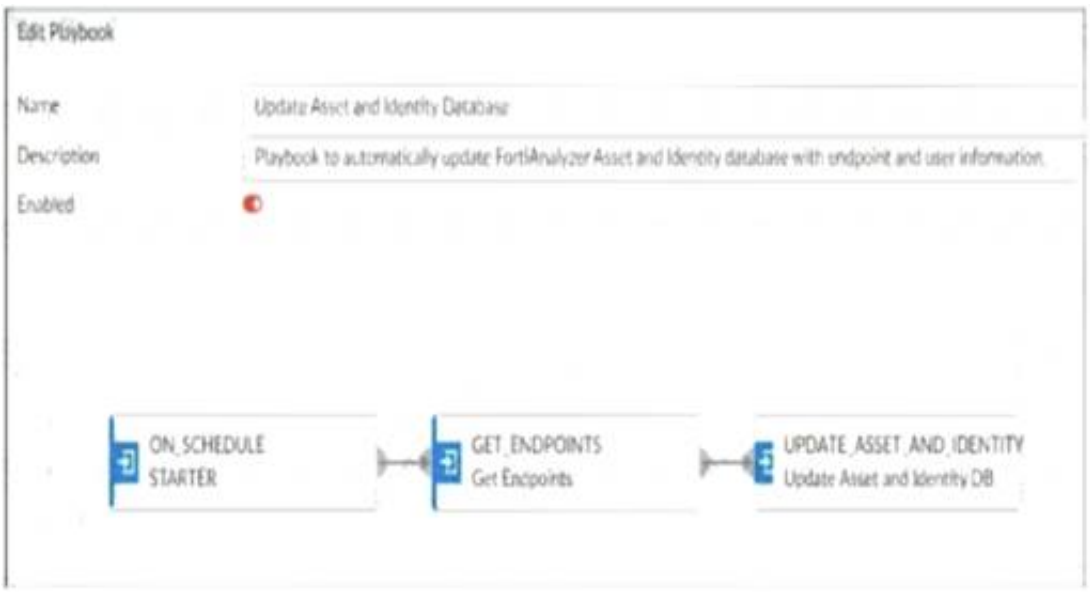
A. Spearphishing is being used to elicit sensitive information.
B. DNS tunneling is being used to extract confidential data from the local network.
C. Reconnaissance is being used to gather victim identityinformation from the mail server.
D. FTP is being used as command-and-control (C&C) technique to 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 14
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 18
Refer to Exhibit:

A SOC analyst is designing a playbook to filter for a high severity event and attach the event information to an incident.
Which local connector action must the analyst use in this scenario?

A. Get Events
B. Update Incident
C. Update Asset and Identity

D. Attach Data to Incident

Answer: D

Explanation:
Understanding the Playbook Requirements:
The SOC analyst needs to design a playbook that filters for high severity events.
The playbook must also attach the event information to an existing incident.
Analyzing the Provided Exhibit:
The exhibit shows the available actions for a local connector within the playbook.
Actions listed include:
Update Asset and Identity
Get Events
Get Endpoint Vulnerabilities
Create Incident
Update Incident
Attach Data to Incident
Run Report
Get EPEU from Incident
Evaluating the Options:
Get Events:This action retrieves events but does not attach them to an incident.
Update Incident:This action updates an existing incident but is not specifically for attaching event data.
Update Asset and Identity:This action updates asset and identity information, not relevant for attaching event data to an incident.
Attach Data to Incident:This action is explicitly designed to attach additional data, such as event information, to an existing incident.
Conclusion:
The correct action to use in the playbook for filtering high severity events and attaching the event information to an incident isAttach Data to Incident.
References:
Fortinet Documentation on Playbook Actions and Connectors.
Best Practices for Incident Management and Playbook Design in SOC Operations.

NEW QUESTION 23
.....

Relate Links

100% Pass Your FCSS_SOC_AN-7.4 Exam with Exambible Prep Materials

https://www.exambible.com/FCSS_SOC_AN-7.4-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/