Fortinet

Exam Questions FCSS_SOC_AN-7.4

FCSS - Security Operations 7.4 Analyst

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
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 3
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 4
Which FortiAnalyzer connector can you use to run automation stitches9

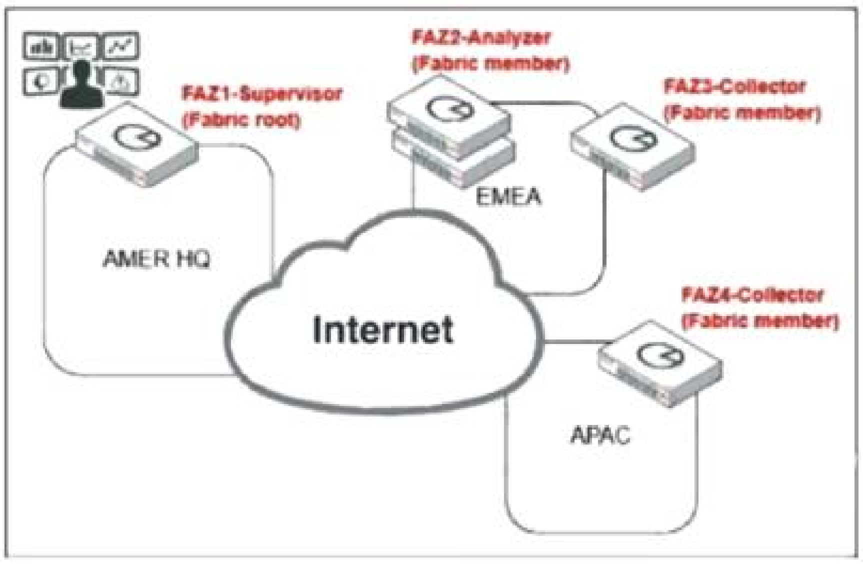
A. FortiCASB
B. FortiMail
C. Local
D. FortiOS

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 5
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.

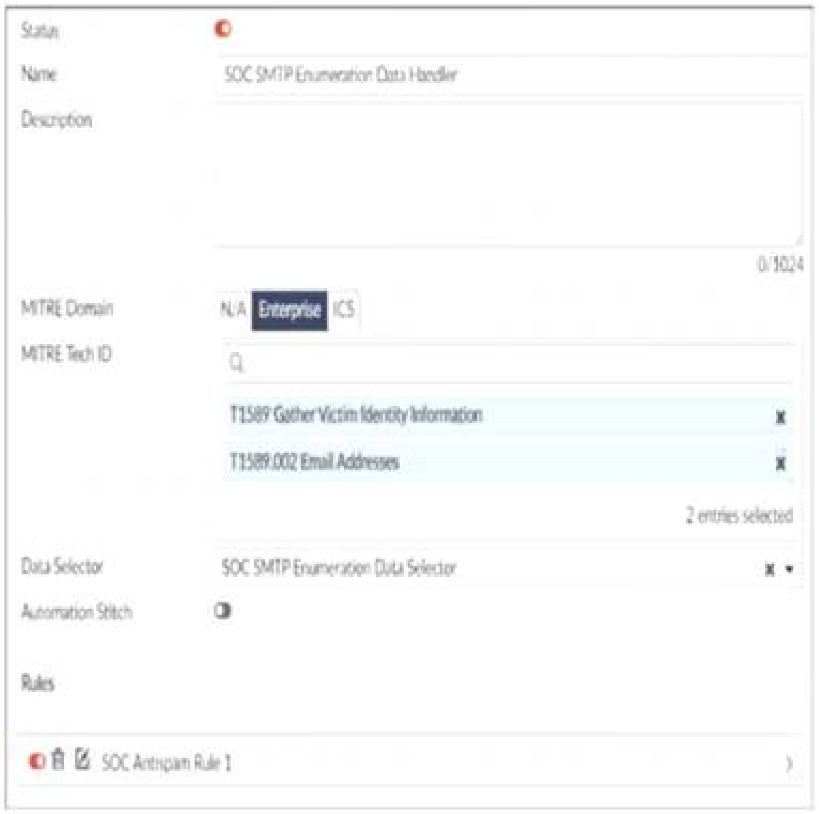
Answer: A

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 6
Refer to the exhibits.

Event Handler



Status ●
Name: SOC SMTP Enumeration Data Handler
Description:
0/1024
MITRE Domain: N/A Enterprise ICS
MITRE Tech ID:
T1589 Gather Victim Identity Information
T1589.002 Email Addresses
2 entries selected
Data Selector: SOC SMTP Enumeration Data Selector
Automation Stitch ○
Rules
SOC Antispam Rule 1

You configured a custom event handler and an associated rule to generate events whenever FortiMail detects spam emails. However, you notice that the event handler is generating events for both spam emails and clean emails.
Which change must you make in the rule so that it detects only spam emails?

A. In the Log Type field, select Anti-Spam Log (spam)
B. Disable the rule to use the filter in the data selector to create the event.
C. In the Trigger an event when field, select Within a group, the log field Spam Name (snane) has 2 or more unique values.

Answer: A

Explanation:
Understanding the Custom Event Handler Configuration:
The event handler is set up to generate events based on specific log data.
The goal is to generate events specifically for spam emails detected by FortiMail.
Analyzing the Issue:
The event handler is currently generating events for both spam emails and clean emails.
This indicates that the rule's filtering criteria are not correctly distinguishing between spam and non-spam emails.
Evaluating the Options:
Option A:Selecting the "Anti-Spam Log (spam)" in the Log Type field will ensure that only logs related to spam emails are considered. This is the most straightforward and accurate way to filter for spam emails.
Option B: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 7
Which statement describes automation stitch integration between FortiGate and FortiAnalyzer?

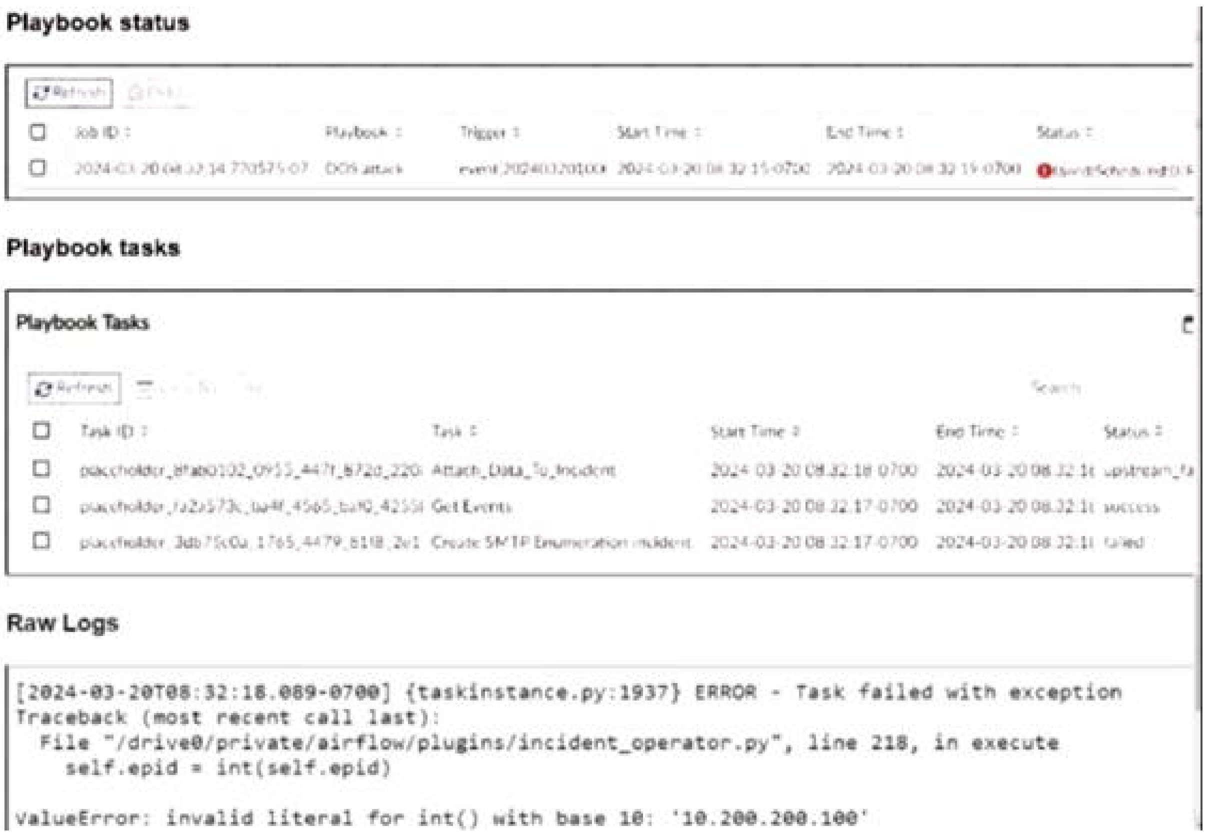
A. An event handler on FortiAnalyzer executes an automation stitch when an event is created.
B. An automation stitch is configured on FortiAnalyzer and mapped to FortiGate using the FortiOS connector.
C. An event handler on FortiAnalyzer is configured to send a notification to FortiGate to trigger an 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 8
Refer to the exhibits.



Playbook status

□	Job ID ↕	Playbook ↕	Trigger ↕	Start Time ↕	End Time ↕	Status ↕
□	2024-03-20 08:32:14.770575-07	DOS attack	event_20240320100	2024-03-20 08:32:15-0700	2024-03-20 08:32:15-0700	● [illegible]

Playbook tasks

Playbook Tasks

□	Task ID ↕	Task ↕	Start Time ↕	End Time ↕	Status ↕
□	placeholder_8fab0102_0915_447f_8720_220	Attach_Data_To_Incident	2024-03-20 08:32:18-0700	2024-03-20 08:32:1	upstream_fa
□	placeholder_fa2a573c_ba4f_4565_ba40_4255	Get Events	2024-03-20 08:32:17-0700	2024-03-20 08:32:1	success
□	placeholder_3db75c0a_1765_4479_8118_2e1	Create SMTP Enumeration incident	2024-03-20 08:32:17-0700	2024-03-20 08:32:1	failed

Raw Logs

```
[2024-03-20T08:32:18.089-0700] {taskinstance.py:1937} ERROR - Task failed with exception
Traceback (most recent call last):
  File "/drive0/private/airflow/plugins/incident_operator.py", line 218, in execute
    self.epid = int(self.epid)

ValueError: invalid literal for int() with base 10: '10.200.200.100'
```

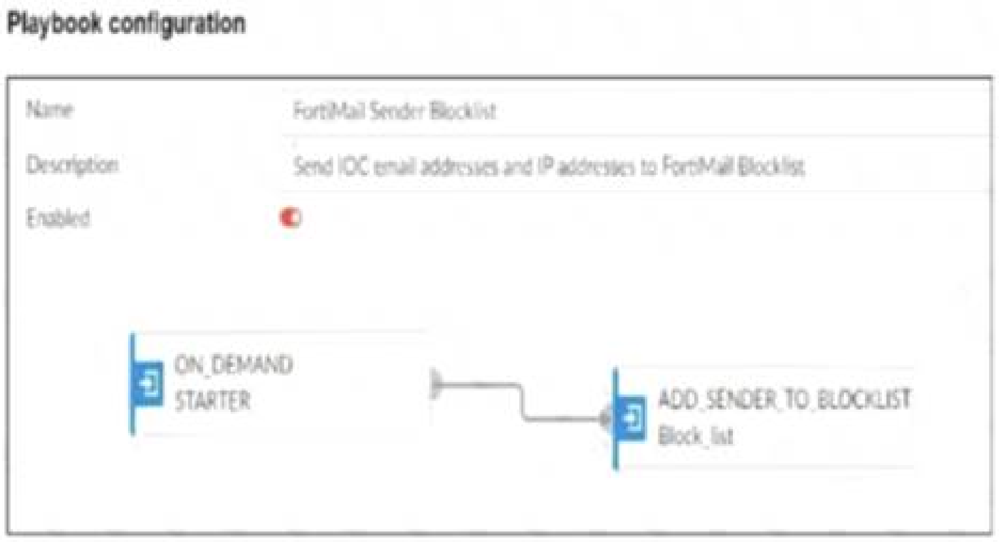
The DOS attack playbook is configured to create an incident when an event handler generates a denial-of-ser/ice (DoS) attack event.
Why did the DOS attack playbook fail to execute?

A. The Create SMTP Enumeration incident task is expecting an integer value but is receiving the incorrect data type
B. The Get Events task is configured to execute in the incorrect order.
C. The Attach_Data_To_Incident task failed.
D. The Attach_Data_To_Incident task is expecting an integer value but is receiving the incorrect data type.

Answer: A

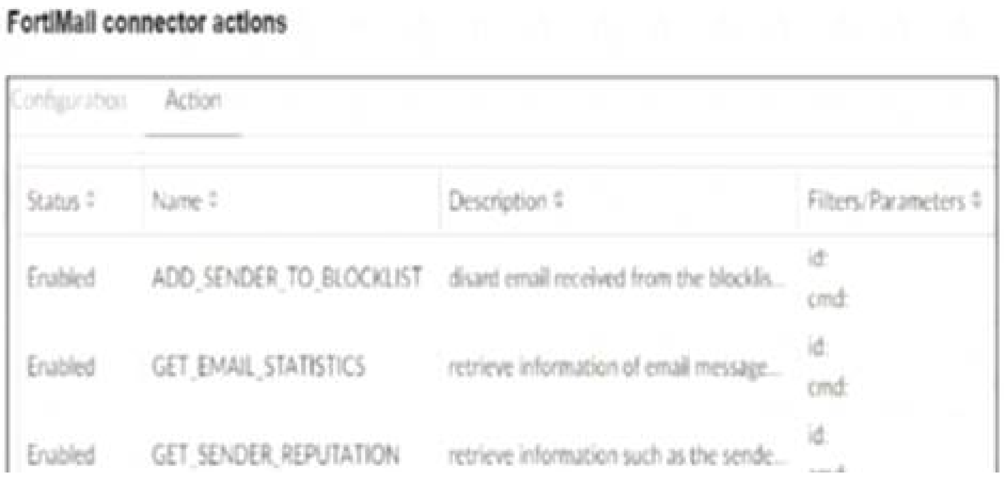
Explanation:
Understanding the Playbook and its Components:
The exhibit shows the status of a playbook named "DOS attack" and its associated tasks.
The playbook is designed to execute a series of tasks upon detecting a DoS attack event.
Analysis of Playbook Tasks:
Attach_Data_To_Incident:Task ID placeholder_8fab0102, status is "upstream_failed," meaning it did not execute properly due to a previous task's failure.
Get Events:Task ID placeholder_fa2a573c, status is "success."
Create SMTP Enumeration incident:Task ID placeholder_3db75c0a, status is "failed."
Reviewing Raw Logs:
The error log shows aValueError: invalid literal for int() with base 10: '10.200.200.100'.
This error indicates that the task attempted to convert a string (the IP address '10.200.200.100') to an integer, which is not possible.
Identifying the Source of the Error:
The error occurs in the file "incident_operator.py," specifically in theexecutemethod.
This suggests that the task "Create SMTP Enumeration incident" is the one causing the issue because it failed to process the data type correctly.
Conclusion:
The failure of the playbook is due to the "Create SMTP Enumeration incident" task receiving a string value (an IP address) when it expects an integer value. This mismatch in data types leads to the error.
References:
Fortinet Documentation on Playbook and Task Configuration.
Python error handling documentation for understandingValueError.

NEW QUESTION 9
Refer to the exhibits.



Playbook configuration

Name	FortiMail Sender Blocklist
Description	Send IOC email addresses and IP addresses to FortiMail Blocklist
Enabled	●



FortiMail connector actions

Status	Name	Description	Filters/Parameters
Enabled	ADD_SENDER_TO_BLOCKLIST	disard email received from the blocklis...	id: cmd:
Enabled	GET_EMAIL_STATISTICS	retrieve information of email message...	id: cmd:
Enabled	GET_SENDER_REPUTATION	retrieve information such as the sende...	id:

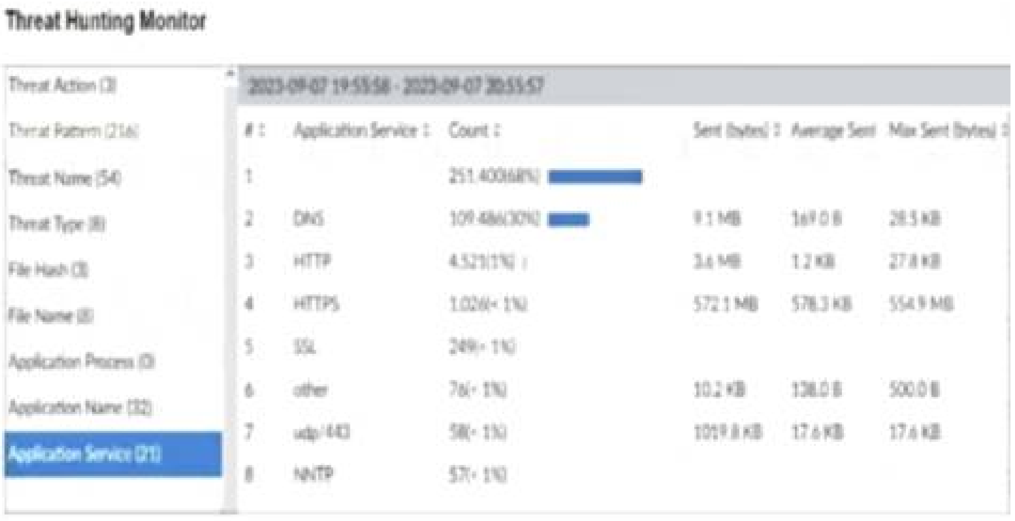
The FortiMail Sender Blocklist playbook is configured to take manual input and add those entries to the FortiMail abc. com domain-level block list. The playbook is configured to use a FortiMail connector and the ADD_SENDER_TO_BLOCKLIST action.
Why is the FortiMail Sender Blocklist playbook execution 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
Refer to the exhibits.

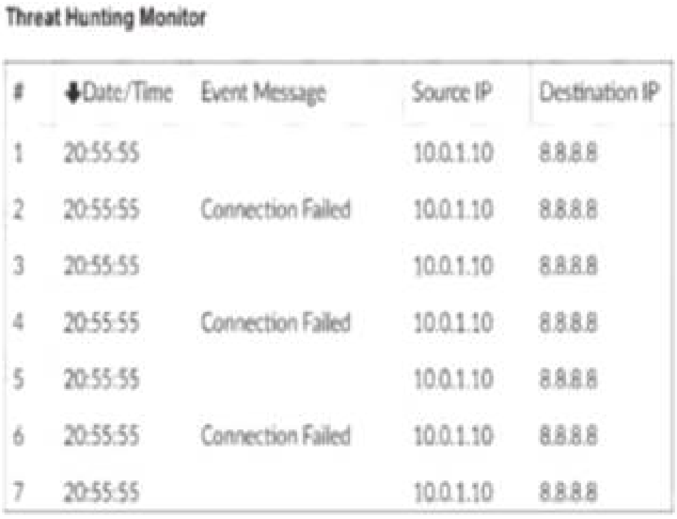


Threat Hunting Monitor

Threat Action (3)
Threat Pattern (216)
Threat Name (54)
Threat Type (8)
File Hash (3)
File Name (8)
Application Process (0)
Application Name (32)
Application Service (21)

2023-09-07 19:55:58 - 2023-09-07 20:55:57

#	Application Service	Count	Sent (bytes)	Average Sent	Max Sent (bytes)
1		251,400(68%)			
2	DNS	109,486(30%)	9.1 MB	169.0 B	28.5 KB
3	HTTP	4,521(1%)	3.6 MB	1.2 KB	27.8 KB
4	HTTPS	1,026(< 1%)	572.1 MB	578.3 KB	554.9 MB
5	SSL	249(< 1%)			
6	other	76(< 1%)	10.2 KB	138.0 B	500.0 B
7	udp/443	58(< 1%)	1019.8 KB	17.6 KB	17.6 KB
8	NNTP	57(< 1%)			



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

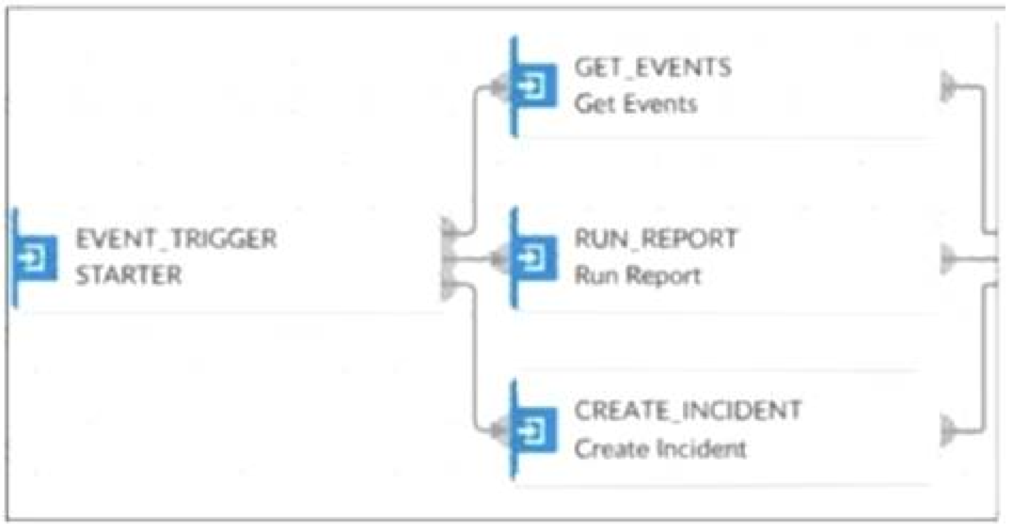
What can you conclude from analyzing the data using the threat hunting module?

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 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 10
Refer to the Exhibit:



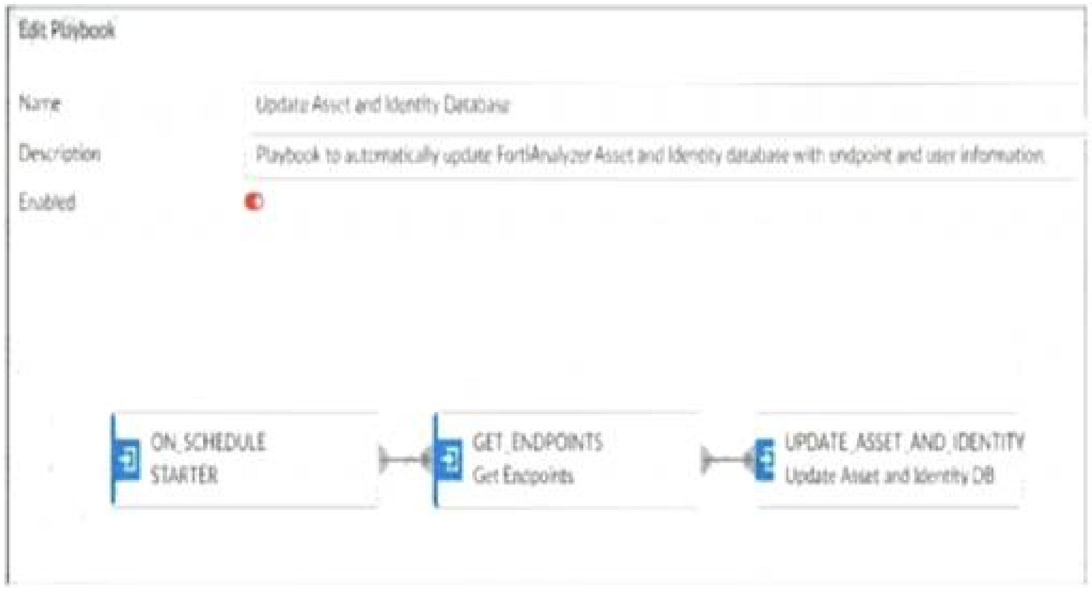
An analyst wants to create an incident and generate a report whenever FortiAnalyzer generates a malicious attachment event based on FortiSandbox analysis.
The endpoint hosts are protected by FortiClient EMS integrated with FortiSandbox. All devices are logging to FortiAnalyzer.
Which connector must the analyst use in this playbook?

A. FortiSandbox connector
B. FortiClient EMS connector
C. FortiMail connector
D. Local connector

Answer: A

Explanation:
Understanding the Requirements:
The objective is to create an incident and generate a report based on malicious attachment events detected by FortiAnalyzer from FortiSandbox analysis.
The endpoint hosts are protected by FortiClient EMS, which is integrated with FortiSandbox. All logs are sent to FortiAnalyzer.
Key Components:
FortiAnalyzer: Centralized logging and analysis for Fortinet devices.
FortiSandbox: Advanced threat protection system that analyzes suspicious files and URLs.
FortiClient EMS: Endpoint management system that integrates with FortiSandbox for endpoint protection.
Playbook Analysis:
The playbook in the exhibit consists of three main actions:GET_EVENTS,RUN_REPORT, andCREATE_INCIDENT.
EVENT_TRIGGER: Starts the playbook when an event occurs.
GET_EVENTS: Fetches relevant events.
RUN_REPORT: Generates a report based on the events.
CREATE_INCIDENT: Creates an incident in the incident management system.
Selecting the Correct Connector:
The correct connector should allow fetching events related to malicious attachments analyzed by FortiSandbox and facilitate integration with FortiAnalyzer.
Connector Options:
FortiSandbox Connector:
Directly integrates with FortiSandbox to fetch analysis results and events related to malicious attachments.
Best suited for getting detailed sandbox analysis results.
Selected as it is directly related to the requirement of handling FortiSandbox analysis events.
FortiClient EMS Connector:
Used for managing endpoint security and integrating with endpoint logs.
Not directly related to fetching sandbox analysis events.
Not selected as it is not directly related to the sandbox analysis events.
FortiMail Connector:
Used for email security and handling email-related logs and events.
Not applicable for sandbox analysis events.
Not selected as it does not relate to the sandbox analysis.
Local Connector:
Handles local events within FortiAnalyzer itself.
Might not be specific enough for fetching detailed sandbox analysis results.
Not selected as it may not provide the required integration with FortiSandbox.
Implementation Steps:
Step 1: Ensure FortiSandbox is configured to send analysis results to FortiAnalyzer.
Step 2: Use the FortiSandbox connector in the playbook to fetch events related to malicious attachments.
Step 3: Configure theGET_EVENTSaction to use the FortiSandbox connector.
Step 4: Set up theRUN_REPORTandCREATE_INCIDENTactions based on the fetched events.
References:
Fortinet Documentation on FortiSandbox Integration FortiSandbox Integration Guide
Fortinet Documentation on FortiAnalyzer Event Handling FortiAnalyzer Administration Guide
By using the FortiSandbox connector, the analyst can ensure that the playbook accurately fetches events based on FortiSandbox analysis and generates the required incident and report.

NEW QUESTION 11
Refer to the exhibit.



Edit Playbook

Name: Update Asset and Identity Database

Description: Playbook to automatically update FortiAnalyzer Asset and Identity database with endpoint and user information.

Enabled: ●

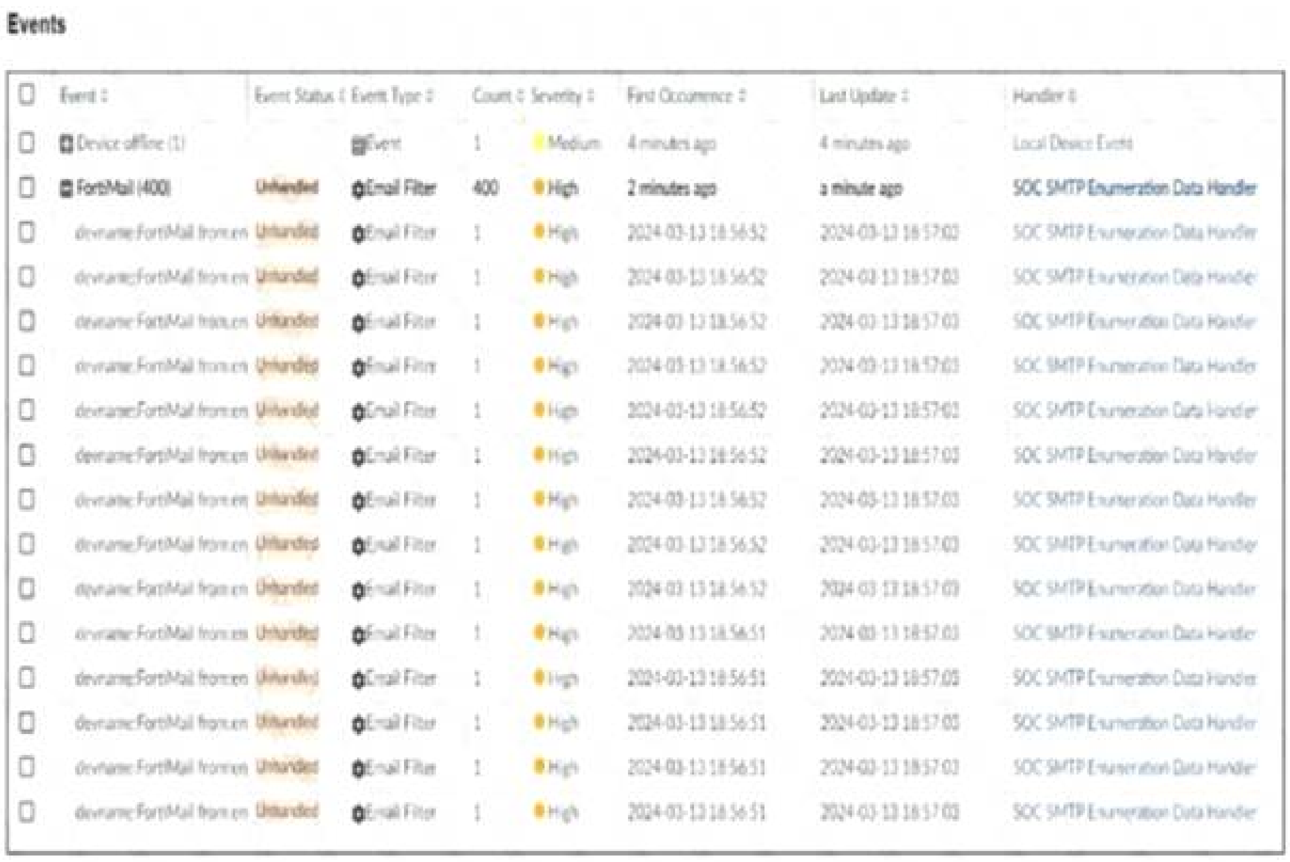
Which two options describe how the Update Asset and Identity Database playbook is configured? (Choose two.)

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

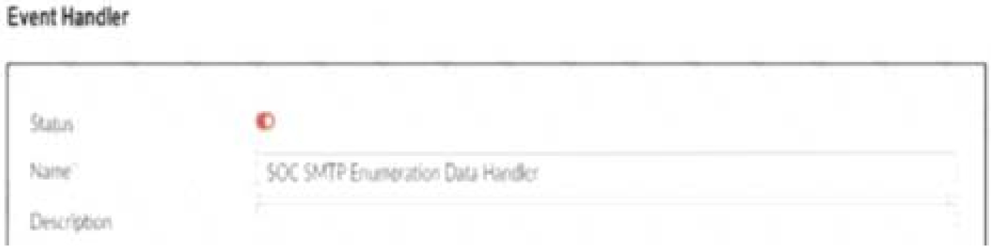
Explanation:
Understanding the Playbook Configuration:
The playbook named "Update Asset and Identity Database" is designed to update the FortiAnalyzer Asset and Identity database with endpoint and user information.
The exhibit shows the playbook with three main components: ON_SCHEDULE STARTER, GET_ENDPOINTS, 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 13
Refer to the exhibit.



Events

□	Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Handler
□	Device offline (1)		Event	1	Medium	4 minutes ago	4 minutes ago	Local Device Event
□	FortiMail (400)	Unhandled	Email Filter	400	High	2 minutes ago	a minute ago	SOC SMTP Enumeration Data Handler
□	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
□	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
□	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
□	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
□	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
□	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
□	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
□	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
□	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
□	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
□	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
□	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
□	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
□	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

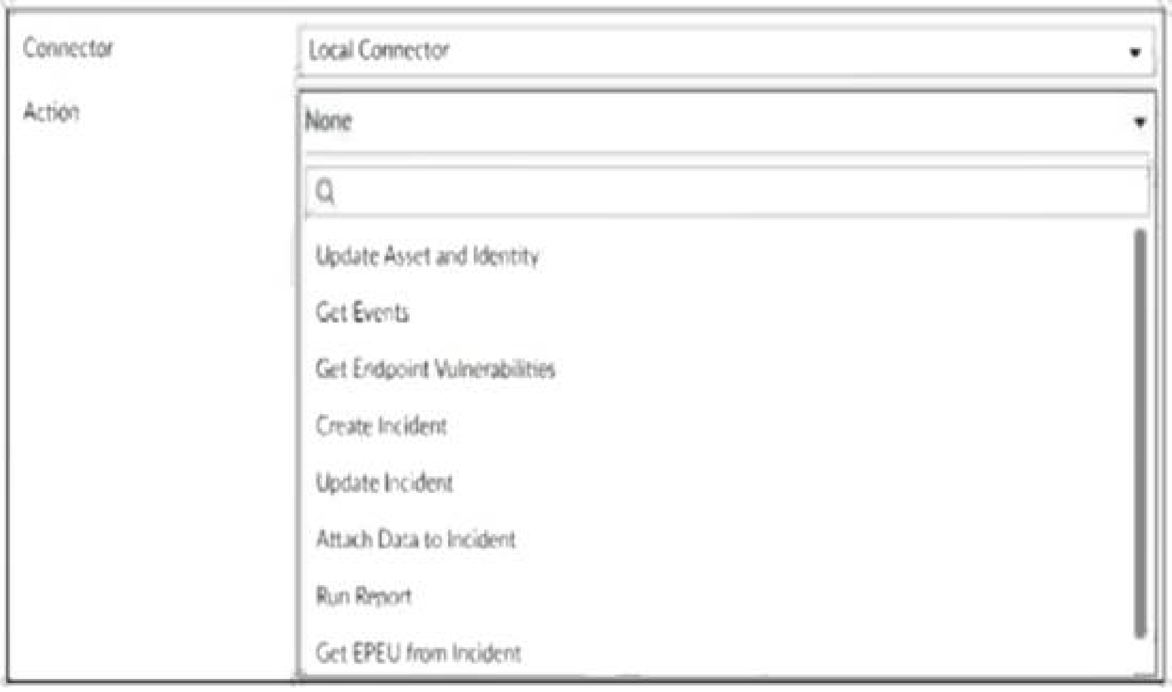
You notice that the custom event handler you configured to detect SMTP reconnaissance activities is creating a large number of events. This is overwhelming your notification system.
How can you fix this?

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 14
Refer to Exhibit:



Connector: Local Connector

Action: None

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 16
......