

## FCSS\_SOC\_AN-7.4 Dumps

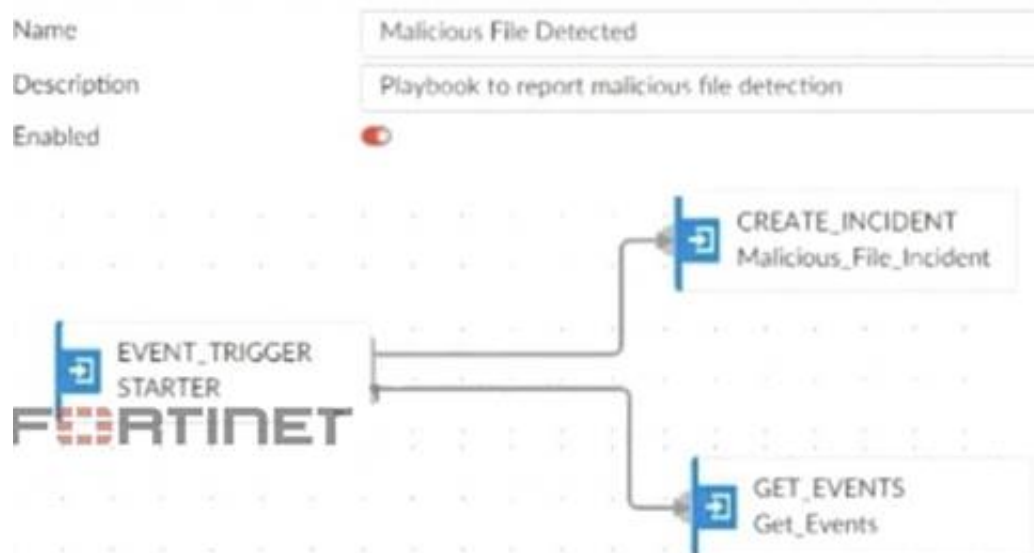
### FCSS - Security Operations 7.4 Analyst

[https://www.certleader.com/FCSS\\_SOC\\_AN-7.4-dumps.html](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,



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 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 of Initial Access and Persistence.

References:

MITRE ATT&CK Framework documentation on Initial Access and Persistence tactics.

Incident analysis and mapping to MITRE ATT&CK tactics.

**NEW QUESTION 5**

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 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**

Which statement best describes the MITRE ATT&CK framework?



- A. It provides a high-level description of common adversary activities, but lacks technical details.
- B. It covers tactics, techniques, and procedures, but does not provide information about mitigations.
- C. It describes attack vectors targeting network devices and servers, but not user endpoints.
- D. It contains some techniques or subtechniques that fall under more than one tactic.

**Answer:** D

**Explanation:**

Understanding the MITRE ATT&CK Framework:

The MITRE ATT&CK framework is a comprehensive matrix of tactics and techniques used by adversaries to achieve their objectives.

It is widely used for understanding adversary behavior, improving defense strategies, and conducting security assessments.

Analyzing the Options:

Option A: The framework provides detailed technical descriptions of adversary activities, including specific techniques and subtechniques.

Option B: The framework includes information about mitigations and detections for each technique and subtechnique, providing comprehensive guidance.

Option C: MITRE ATT&CK covers a wide range of attack vectors, including those targeting user endpoints, network devices, and servers.

Option D: Some techniques or subtechniques do indeed fall under multiple tactics, reflecting the complex nature of adversary activities that can serve different objectives.

Conclusion:

The statement that best describes the MITRE ATT&CK framework is that it contains some techniques or subtechniques that fall under more than one tactic.

References:

MITRE ATT&CK Framework Documentation.

Security Best Practices and Threat Intelligence Reports Utilizing MITRE ATT&CK.

**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 are input and output.

References:

Fortinet Documentation on Playbook Configuration and Variable Usage.

General SOC Automation and Orchestration Practices.

**NEW QUESTION 9**

Which statement describes automation stitch integration between FortiGate and FortiAnalyzer?

- A. An event handler on FortiAnalyzer executes an automation stitch when an event is created.
- B. An automation stitch is configured on FortiAnalyzer and mapped to FortiGate using the FortiOS connector.
- C. An event handler on FortiAnalyzer is configured to send a notification to FortiGate to trigger an automation stitch.
- D. A security profile on FortiGate triggers a violation and FortiGate sends a webhook call to FortiAnalyzer.

**Answer:** D

**Explanation:**

Overview of Automation Stitches: Automation stitches in Fortinet solutions enable automated responses to specific events detected within the network. This automation helps in swiftly mitigating threats without manual intervention.

FortiGate Security Profiles:

FortiGate uses security profiles to enforce policies on network traffic. These profiles can include antivirus, web filtering, intrusion prevention, and more.

When a security profile detects a violation or a specific event, it can trigger predefined actions.

Webhook Calls:

FortiGate can be configured to send webhook calls upon detecting specific security events.

A webhook is an HTTP callback triggered by an event, sending data to a specified URL. This allows FortiGate to communicate with other systems, such as FortiAnalyzer.

FortiAnalyzer Integration:

FortiAnalyzer collects logs and events from various Fortinet devices, providing centralized logging and analysis.

Upon receiving a webhook call from FortiGate, FortiAnalyzer can further analyze the event, generate reports, and take automated actions if configured to do so.

Detailed Process:

Step 1: A security profile on FortiGate triggers a violation based on the defined security policies.

Step 2: FortiGate sends a webhook call to FortiAnalyzer with details of the violation.

Step 3: FortiAnalyzer receives the webhook call and logs the event.

Step 4: Depending on the configuration, FortiAnalyzer can execute an automation stitch to respond to the event, such as sending alerts, generating reports, or

triggering further actions.

References:

Fortinet Documentation: FortiOS Automation Stitches

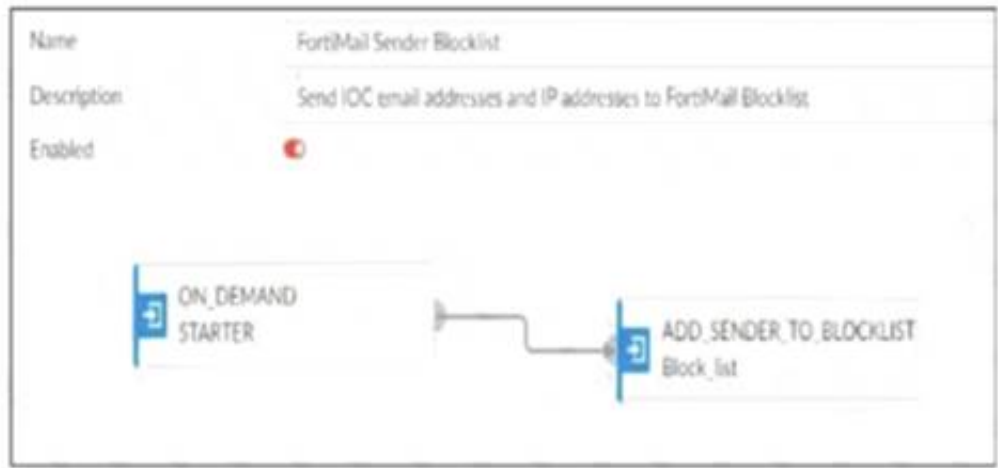
FortiAnalyzer Administration Guide: Details on configuring event handlers and integrating with FortiGate.

FortiGate Administration Guide: Information on security profiles and webhook configurations. By understanding the interaction between FortiGate and FortiAnalyzer through webhook calls and automation stitches, security operations can ensure a proactive and efficient response to security events.

NEW QUESTION 10

Refer to the exhibits.

Playbook configuration



FortiMail connector actions

Configurations		Action	
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 failing?

- 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 FortiAnalyzer 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 is Threat hunting.

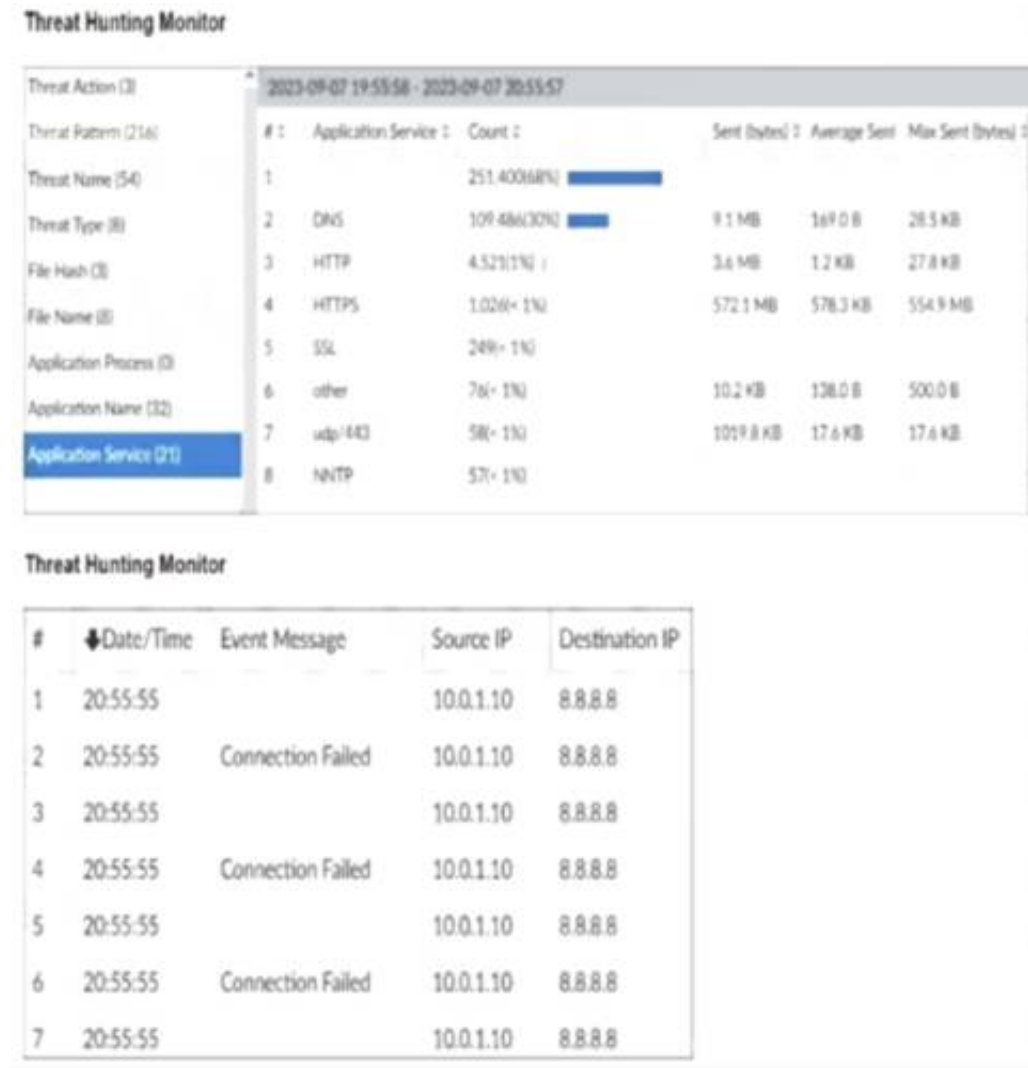
References:

Fortinet Documentation on FortiAnalyzer Features and SIEM Capabilities.

Security Best Practices and Use Cases for Threat Hunting.

**NEW QUESTION 15**

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 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

.....



## 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](https://www.certleader.com/FCSS_SOC_AN-7.4-dumps.html)