Fortinet NSE7_SOC_AR-7.6 Practice Test

Shared by Salas on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Review the incident report:

An attacker identified employee names, roles, and email patterns from public press releases, which were then used to craft tailored emails.

The emails were directed to recipients to review an attached agenda using a link hosted off the corporate domain.

Which two MITRE ATT&CK tactics best fit this report? (Select two answers)

Options:

A- Reconnaissance
B- Discovery
C- Initial Access
D- Defense Evasion

Answer:

A, C

Explanation:

Comprehensive and Detailed Explanation From FortiSOAR 7.6., FortiSIEM 7.3 Exact Extract study guide:

Based on the official documentation for FortiSIEM 7.3 (which utilizes the MITRE ATT&CK mapping for incident correlation) and FortiSOAR 7.6 (which uses these tactics for incident classification and playbook triggering):

Reconnaissance (Tactic TA0043): This tactic consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting. In this scenario, the attacker identifies 'employee names, roles, and email patterns from public press releases.' This is categorized under Gather Victim Org Information (T1591) and Search Open Technical Databases (T1596). Since this activity happens prior to the compromise and involves gathering intelligence, it is strictly Reconnaissance.

Initial Access (Tactic TA0001): This tactic covers techniques that use various entry vectors to gain an initial foothold within a network. The act of sending 'tailored emails... to recipients to review an attached agenda using a link' is the definition of Phishing: Spearphishing Link (T1566.002). This is the specific delivery mechanism used to gain the initial entry.

Why other options are incorrect:

Discovery (B): This tactic involves techniques an adversary uses to gain knowledge about the internal network after they have already gained access. Since the attacker is looking at public press releases, they are operating outside the perimeter.

Defense Evasion (D): This tactic consists of techniques that adversaries use to avoid detection throughout their compromise. While using an external link might bypass some basic reputation filters, the primary goal described in the report is the act of establishing contact and access, which is the core of the Initial Access tactic.

Question 2

Question Type: MultipleChoice

Which FortiAnalyzer connector can you use to run automation stitches9

Options:

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.

FortiMail:

FortiMail is an email security solution. While it can send logs and events to FortiAnalyzer, it is not primarily used for running automation stitches.

Local:

The local connector refers to FortiAnalyzer's ability to handle logs and events generated by itself. This is useful for internal processes but not specifically for integrating with other Fortinet devices for automation stitches.

FortiOS:

FortiOS is the operating system that runs on FortiGate firewalls. FortiAnalyzer can use the FortiOS connector to communicate with FortiGate devices and run automation stitches. This allows FortiAnalyzer to send commands to FortiGate, triggering predefined actions in response to specific events.

Detailed Process:

Step 1: Configure the FortiOS connector in FortiAnalyzer to establish communication with FortiGate devices.

Step 2: Define automation stitches within FortiAnalyzer that specify the actions to be taken when certain events occur.

Step 3: When a triggering event is detected, FortiAnalyzer uses the FortiOS connector to send the necessary commands to the FortiGate device.

Step 4: FortiGate executes the commands, performing the predefined actions such as blocking an IP address, updating firewall rules, or sending alerts.

Conclusion:

The FortiOS connector is specifically designed for integration with FortiGate devices, enabling FortiAnalyzer to execute automation stitches effectively.

Fortinet FortiOS Administration Guide: Details on configuring and using automation stitches.

Fortinet FortiAnalyzer Administration Guide: Information on connectors and integration options.

By utilizing the FortiOS connector, FortiAnalyzer can run automation stitches to enhance the security posture and response capabilities within a network.

Question 3

Question Type: MultipleChoice

Review the incident report:

Packet captures show a host maintaining periodic TLS sessions that imitate normal HTTPS traffic but run on TCP 8443 to a single external host. An analyst flags the traffic as potential command-and-control. During the same period, the host issues frequent DNS queries with oversized TXT payloads to an attacker-controlled domain, transferring staged files.

Which two MITRE ATT&CK techniques best describe this activity? (Choose two answers)

Options:

A- Non-Standard Port
B- Exploitation of Remote Services
C- Exfiltration Over Alternative Protocol
D- Hide Artifacts

Answer:

A, C

Explanation:

Comprehensive and Detailed Explanation From FortiSOAR 7.6., FortiSIEM 7.3 Exact Extract study guide:

In accordance with the MITRE ATT&CK mapping utilized by FortiSIEM 7.3 and FortiSOAR 7.6, the described behaviors correspond to the following techniques:

Non-Standard Port (T1571): This technique involves adversaries communicating using a protocol and port pairing that are typically not associated. The incident report identifies HTTPS (TLS) traffic running on TCP 8443 rather than the standard port 443. FortiSIEM specifically includes built-in correlation rules, such as 'Suspicious Typical Malware Back Connect Ports,' designed to detect these protocol-port mismatches.

Exfiltration Over Alternative Protocol (T1048): This technique describes adversaries stealing data by exfiltrating it over a different protocol than the primary command and control (C2) channel. In this scenario, while the C2 channel is established via HTTPS on port 8443, the adversary is transferring staged files using DNS queries with oversized TXT payloads. DNS is a common 'alternative protocol' used to bypass standard data transfer monitoring and egress filtering.

Analysis of Incorrect Options:

Exploitation of Remote Services (B): This technique falls under Initial Access or Lateral Movement tactics, focusing on gaining entry into a system via vulnerabilities in network services like SMB or RDP. It does not apply to the maintenance of an established C2 channel or the exfiltration of data.

Hide Artifacts (D): This is a Defense Evasion technique where an adversary attempts to conceal their presence by removing traces such as log files or registry keys. While the attacker is 'imitating normal traffic,' the specific acts of using a non-standard port and DNS exfiltration are primary behavioral signatures defined by their own more specific techniques.

Question 4

Question Type: MultipleChoice

Which three factors does the FortiSIEM rules engine use to determine the count when it evaluates the aggregate condition COUNT (Matched Events) on a specific subpattern? (Choose three answers)

Options:

A- Group By attributes
B- Data source
C- Time window
D- Search filter
E- Incident action

Answer:

A, C, D

Explanation:

Comprehensive and Detailed Explanation From FortiSOAR 7.6., FortiSIEM 7.3 Exact Extract study guide:

The FortiSIEM rules engine evaluates subpatterns to detect complex attack behaviors. When a rule uses an aggregate condition like COUNT (Matched Events), the engine calculates this value based on specific architectural parameters:

Group By attributes (A): The engine maintains a separate counter for each unique combination of 'Group By' attributes defined in the subpattern. For example, if you group by 'Source IP,' the engine tracks the count of events for each unique IP address independently.

Time window (C): The count is relative to a specific time duration (e.g., 5 minutes). The engine only counts events that fall within this sliding or fixed window. Once an event falls outside this window, it is no longer included in the aggregate count.

Search filter (D): Only events that satisfy the specific 'Search Filter' criteria (e.g., Event Type = 'Failed Login') are considered 'Matched Events.' The filter defines the scope of the data that the rules engine processes before applying the count.

Why other options are incorrect:

Data source (B): While the data source determines where the logs come from, the rules engine itself uses the parsed attributes (defined in the search filter) rather than the raw data source to determine the count. Multiple data sources might contribute to the same filter and count.

Incident action (E): Incident actions (such as sending an email or triggering a SOAR playbook) are the result of a rule firing. They do not influence the internal logic or calculation of the event count during the evaluation phase.

Question 5

Question Type: MultipleChoice

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?

Options:

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, and CREATE_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 the GET_EVENTS action to use the FortiSandbox connector.

Step 4: Set up the RUN_REPORT and CREATE_INCIDENT actions based on the fetched events.

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.

Question 6

Question Type: MultipleChoice

Refer to the exhibit.

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

Options:

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:

A, D

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.

Fortinet Documentation on Playbook Actions and Connectors.

FortiAnalyzer and FortiClient EMS Integration Guides.

Question 7

Question Type: MultipleChoice

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

Options:

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

Answer:

A, B

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.

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.

Question 8

Question Type: MultipleChoice

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.)

Options:

A- Initial Access
B- Defense Evasion
C- Lateral Movement
D- Persistence

Answer:

A, D

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.

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

Incident analysis and mapping to MITRE ATT&CK tactics.

Question 9

Question Type: MultipleChoice

Refer to Exhibit:

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?

Options:

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.

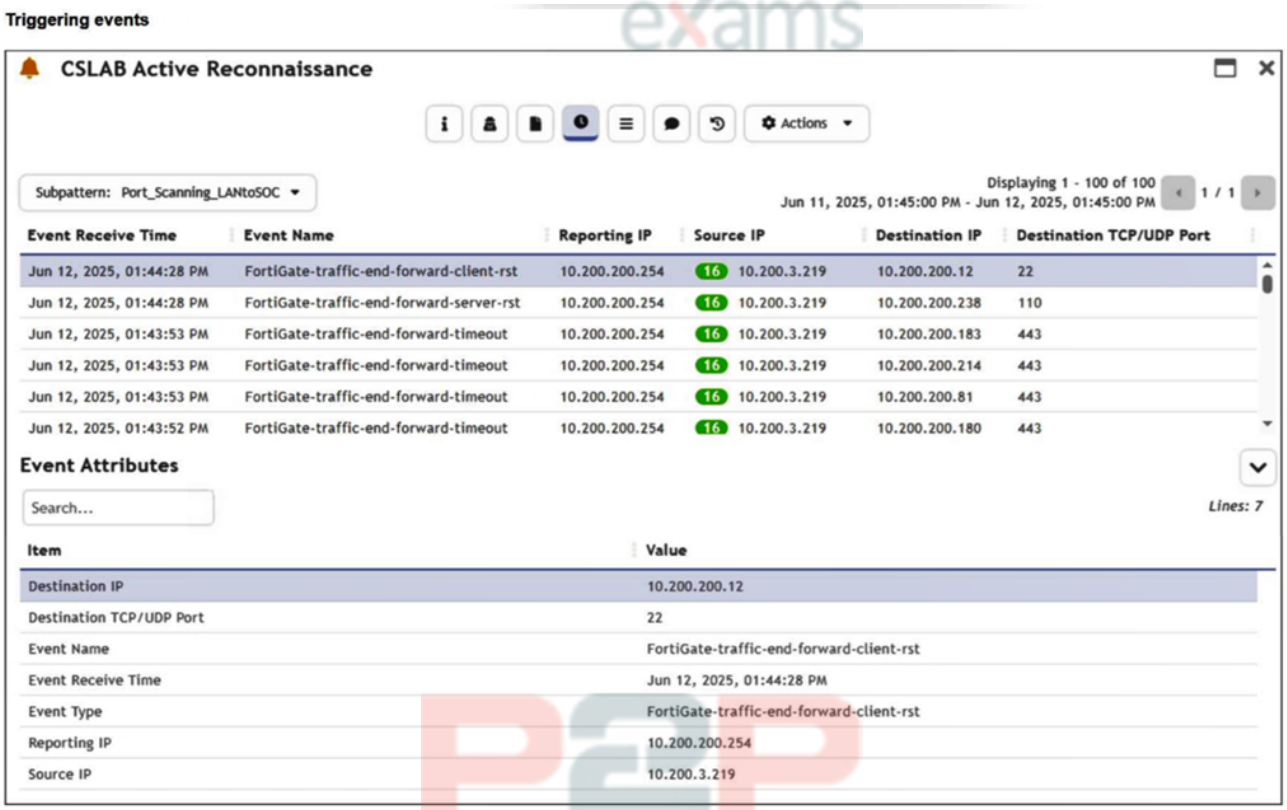
Fortinet Documentation on FortiAnalyzer Data Policies and Disk Management.

Best Practices for FortiAnalyzer Log Management and Disk Utilization.

Question 10

Question Type: MultipleChoice

Refer to the exhibit.



You are reviewing the Triggering Events page for a FortiSIEM incident. You want to remove the Reporting IP column because you have only one firewall in the topology. How do you accomplish this? (Choose one answer)

Options:

A- Clear the Reporting IP field from the Triggered Attributes section when you configure the Incident Action.
B- Disable correlation for the Reporting IP field in the rule subpattern.
C- Remove the Reporting IP attribute from the raw logs using parsing rules.

D- Customize the display columns for this incident.

Answer:

D

Explanation:

Comprehensive and Detailed Explanation From FortiSOAR 7.6., FortiSIEM 7.3 Exact Extract study guide:

In FortiSIEM 7.3, the Triggering Events view is a dynamic table that displays the individual logs that caused a specific rule to fire. To manage the visibility of data within this specific view:

Interface Customization: The 'Triggering Events' tab includes a column management feature. By clicking on the column headers or the table settings icon (typically found at the top right of the event list), an analyst can customize the display columns. This allows the user to uncheck the 'Reporting IP' attribute, effectively hiding it from the view without altering the underlying data or rule logic.

Operational Efficiency: This is a common task in environments with a simplified topology where the 'Reporting IP' is redundant information. Customizing the view helps the analyst focus on the most relevant data points, such as 'Source IP,' 'Destination IP,' and 'Destination Port.'

Why other options are incorrect:

A (Incident Action): Clearing a field from the Incident Action configuration affects what data is sent in an email alert or passed to a SOAR platform, but it does not change the layout of the FortiSIEM GUI 'Triggering Events' page.

B (Disable Correlation): Disabling correlation for an attribute determines whether that attribute is used by the rules engine to group events. It does not control the visual display of columns in the incident dashboard.

C (Parsing Rules): Removing attributes via parsing rules is a destructive process that prevents the SIEM from indexing that data entirely. This would make the 'Reporting IP' unavailable for all searches and reports, which is excessive for a simple display preference.