Fortinet NSE7_SOC_AR-7.6 NSE 7 Practice Questions

Shared by Stuart on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

When does FortiAnalyzer generate an event?

Options:

A- When a log matches a filter in a data selector
B- When a log matches an action in a connector
C- When a log matches a rule in an event handler
D- When a log matches a task in a playbook

Answer:

C

Explanation:

Understanding Event Generation in FortiAnalyzer:

FortiAnalyzer generates events based on predefined rules and conditions to help in monitoring and responding to security incidents.

Analyzing the Options:

Option A: Data selectors filter logs based on specific criteria but do not generate events on their own.

Option B: Connectors facilitate integrations with other systems but do not generate events based on log matches.

Option C: Event handlers are configured with rules that define the conditions under which events are generated. When a log matches a rule in an event handler, FortiAnalyzer generates an event.

Option D: Tasks in playbooks execute actions based on predefined workflows but do not directly generate events based on log matches.

Conclusion:

FortiAnalyzer generates an event when a log matches a rule in an event handler.

Fortinet Documentation on Event Handlers and Event Generation in FortiAnalyzer.

Best Practices for Configuring Event Handlers in FortiAnalyzer.

Question 2

Question Type: MultipleChoice

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?

Options:

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.

Fortinet Documentation on Playbook Creation and Incident Management.

Best Practices for Automating Incident Response in SOC Operations.

Question 3

Question Type: MultipleChoice

Which three end user logs does FortiAnalyzer use to identify possible IOC compromised hosts? (Select three answers)

Options:

A- Web filter logs1
B- Email filter logs
C- DNS filter logs2
D- Application filter logs
E- IPS logs

Answer:

A, C, E

Explanation:

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

In the context of the Fortinet Security Fabric, FortiAnalyzer performs Indicator of Compromise (IOC) detection by correlating various security logs against a threat intelligence database.3 The IOC engine specifically analyzes the following logs of each end user to identify potentially compromised hosts:

Web Filter Logs (A): The engine parses web filtering logs to identify access attempts to blacklisted URLs, malicious domains, or IPs associated with known malware distribution sites.4 If a match is found in the threat database, the host is flagged as compromised.

DNS Filter Logs (C): DNS requests are a primary indicator of a compromise. The engine monitors these logs for queries directed at known Command and Control (C2) servers or domains generated by Domain Generation Algorithms (DGA).5

IPS Logs (E): Intrusion Prevention System (IPS) logs provide critical data on signature matches for known attacks. In newer Security Operations (SOC) curricula, IPS logs are used alongside Web and DNS logs to provide a high-fidelity assessment of whether a host is currently infected and attempting to communicate with an external threat actor.

Why other options are incorrect:

Email Filter Logs (B): While important for detecting phishing attempts (Initial Access), email logs are generally used for content filtering and antispam rather than being a primary source for the IOC engine's behavioral 'calling home' detection in the FortiAnalyzer Compromised Hosts view.

Application Filter Logs (D): Application control logs provide visibility into software usage but are less commonly used by the core IOC engine for identifying blacklisted network destinations compared to Web and DNS filtering.

Question 4

Question Type: MultipleChoice

Which statement describes automation stitch integration between FortiGate and FortiAnalyzer?

Options:

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.

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.

Question 5

Question Type: MultipleChoice

Which FortiAnalyzer feature uses the SIEM database for advance log analytics and monitoring?

Options:

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.

Fortinet Documentation on FortiAnalyzer Features and SIEM Capabilities.

Security Best Practices and Use Cases for Threat Hunting.

Question 6

Question Type: MultipleChoice

What are three capabilities of the built-in FortiSOAR Jinja editor? (Choose three answers)

Options:

A- It renders output by combining Jinja expressions and JSON input.
B- It checks the validity of a Jinja expression.
C- It creates new records in bulk.
D- It loads the environment JSON of a recently executed playbook.
E- It defines conditions to trigger a playbook step.

Answer:

A, B, D

Explanation:

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

The built-in Jinja editor in FortiSOAR 7.6 is a powerful utility designed to help playbook developers write and test complex data manipulation logic without having to execute the entire playbook. Its primary capabilities include:

Renders output (A): The editor provides a 'Preview' or 'Evaluation' pane. By combining a Jinja expression with a sample JSON input (manually entered or loaded), the editor dynamically calculates and displays the resulting output. This allows for immediate verification of data transformation logic.

Checks validity (B): The editor includes built-in linting and syntax validation. It alerts the developer to errors such as unclosed brackets, incorrect filter usage, or invalid syntax, ensuring that only valid Jinja code is saved into the playbook step.

Loads environment JSON (D): One of the most significant features for troubleshooting is the ability to load the environment JSON from a recent execution. This populates the editor's variable context (vars) with the actual data from a specific playbook run, allowing the developer to test expressions against real-world data that recently passed through the system.

Why other options are incorrect:

Creates new records in bulk (C): While Jinja expressions are used to format the data that goes into a record, the actual creation of records is handled by the 'Create Record' step or specific Connectors, not by the Jinja editor utility itself.

Defines conditions to trigger a playbook step (E): Jinja is the language used to write conditions within a 'Decision' step or 'Step Utilities,' but the Jinja Editor is a tool for evaluating and testing those expressions. The definition of the condition logic and the triggering behavior is a function of the Playbook Engine and Step configuration, not the editor's standalone capabilities.

Question 7

Question Type: MultipleChoice

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?

Options:

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_lncident 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 as Attach_Data_To_Incident, Create Incident, and Get Events.

Analyzing the Playbook Execution:

The exhibit shows that the Create Incident task has failed, and the Attach_Data_To_Incident task has also failed.

The Get Events task succeeded, indicating that it was able to retrieve event data.

Reviewing Raw Logs:

The raw logs indicate an error related to parsing input in the incident_operator.py file.

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:

The Create Incident task failure is the root cause since it did not proceed correctly due to incorrect input format.

The Attach_Data_To_Incident task subsequently failed because it depends on the successful creation of an incident.

Conclusion:

The primary reason for the playbook execution failure is that the Create Incident task received an incorrect data format, which was not a name or number as expected.

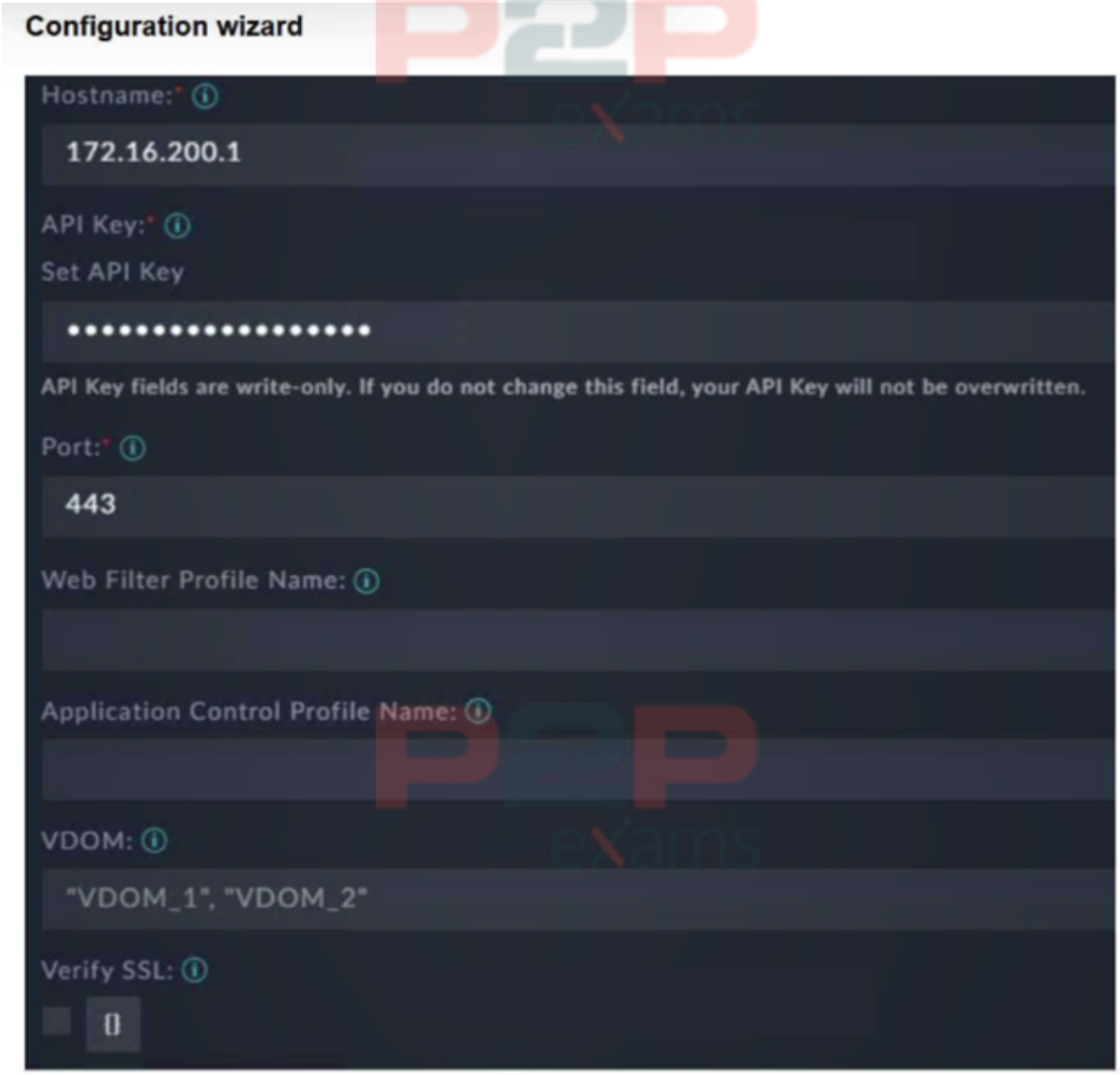
Fortinet Documentation on Playbook and Task Configuration.

Error handling and debugging practices in playbook execution.

Question 8

Question Type: MultipleChoice

Refer to the exhibit.



You must configure the FortiGate connector to allow FortiSOAR to perform actions on a firewall. However, the connection fails. Which two configurations are required? (Choose two answers)

Options:

A- Trusted hosts must be enabled and the FortiSOAR IP address must be permitted.
B- The VDOM name must be specified, or set to VDOM_1, if VDOMs are not enabled on FortiGate.
C- HTTPS must be enabled on the FortiGate interface that FortiSOAR will communicate with.
D- An API administrator must be created on FortiGate with the appropriate profile, along with a generated API key to configure on the connector.

Answer:

C, D

Explanation:

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

To establish a successful integration between FortiSOAR 7.6 and a FortiGate firewall via the FortiGate connector, specific administrative and network requirements must be met on the FortiGate side:

API Administrator and Key (D): FortiSOAR does not use standard UI login credentials. Instead, it requires a REST API Administrator account to be created on the FortiGate. This account must be assigned an administrative profile with the necessary permissions (e.g., Read/Write for Firewall policies or Address objects). Upon creation, the FortiGate generates a unique API Key, which must be entered into the 'API Key' field of the FortiSOAR configuration wizard as shown in the exhibit.

HTTPS Management Access (C): The connector communicates with the FortiGate using REST API calls over HTTPS (port 443 by default). Therefore, the physical or logical interface on the FortiGate that corresponds to the 'Hostname' IP (172.16.200.1) must have HTTPS enabled under 'Administrative Access' in its network settings. If HTTPS is disabled, the connection will time out or be refused.

Why other options are incorrect:

Trusted hosts (A): While it is a best practice to restrict API access to specific IPs (like the FortiSOAR IP), the integration can technically function without 'Trusted hosts' enabled if the network allows the traffic. However, the absence of an API key or HTTPS access will definitively cause a failure regardless of trusted host settings.

VDOM name (B): In the exhibit, the VDOM field contains multiple values ('VDOM_1', 'VDOM_2'). If VDOMs are disabled on the FortiGate, this field should generally be left blank or set to the default 'root.' Setting it specifically to 'VDOM_1' when VDOMs are disabled is not a universal requirement for connectivity; the primary handshake depends on the API key and HTTPS connectivity.

Question 9

Question Type: MultipleChoice

Which two ways can you create an incident on FortiAnalyzer? (Choose two answers)

Options:

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

Answer:

A, D

Explanation:

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

In FortiAnalyzer 7.6 and related SOC versions, incidents serve as centralized containers for tracking and analyzing security events. There are two primary automated and manual methods to initiate an incident:

Using a custom event handler (A): In FortiAnalyzer, event handlers are used to generate events from raw logs.1 A critical feature in recent versions is the Automatically Create Incident setting within a custom event handler.2 When enabled, the system automatically elevates a triggered event into a new incident record, allowing analysts to bypass the manual review of every individual event before an incident is raised.3

By running a playbook (D): Playbooks provide a powerful way to automate the incident lifecycle.4 A playbook can be configured with an Event Trigger, meaning it executes as soon as an event matches specific criteria. One of the core actions available within these playbooks is the Create Incident action, which can automatically populate incident details, severity, and category based on the triggering event's data.5 This ensures high-fidelity events are consistently captured for investigation.

Why other options are incorrect:

Using a connector action (B): While connectors allow FortiAnalyzer to communicate with external systems (like ITSM or Security Fabric devices), the act of 'creating an incident' inside FortiAnalyzer is a function of the internal event engine or playbook automation, not a standalone connector action used for external integration.

Manually, on the Event Monitor page (C): While you can view, filter, and acknowledge events on

the Event Monitor page, the process of manually raising an incident typically occurs from the Incidents module or by right-clicking an event to 'Raise Incident' in the Log View or FortiView, rather than being a core function defined as occurring 'on the Event Monitor page' in the same architectural sense as handlers and playbooks.

Question 10

Question Type: MultipleChoice

Which three are threat hunting activities? (Choose three answers)

Options:

A- Enrich records with threat intelligence.
B- Automate workflows.
C- Generate a hypothesis.
D- Perform packet analysis.
E- Tune correlation rules.

Answer:

A, C, D

Explanation:

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

According to the specialized threat hunting modules and frameworks within FortiSOAR 7.6 and the advanced analytics capabilities of FortiSIEM 7.3, threat hunting is defined as a proactive, human-led search for threats that have bypassed automated security controls. The three selected activities are core components of this lifecycle:

Generate a hypothesis (C): This is the fundamental starting point of a 'Structured Hunt.' Analysts develop a testable theory---based on recent threat intelligence (such as a new TTP identified by FortiGuard) or environmental risk---about how an attacker might be operating undetected in the network.

Enrich records with threat intelligence (A): During the investigation phase, hunters use the Threat Intelligence Management (TIM) module in FortiSOAR to enrich technical data (IPs, hashes, URLs) with external context. This helps determine if an anomaly discovered during the hunt is indeed malicious or part of a known campaign.

Perform packet analysis (D): Since advanced threats often live in the 'gaps' between log files, hunters frequently perform deep-packet or network-flow analysis using FortiSIEM's query tools or integrated NDR (Network Detection and Response) data to identify suspicious lateral movement or C2 (Command and Control) communication patterns that standard alerts might miss.

Why other options are excluded:

Automate workflows (B): While SOAR is designed for automation, the act of 'automating' is a DevOps or SOC engineering task. Threat hunting itself is a proactive investigation; while playbooks can assist a hunter (e.g., by automating the data gathering), the act of hunting remains a manual or semi-automated cognitive process.

Tune correlation rules (E): Tuning rules is a reactive maintenance task or a 'post-hunt' activity. Once a threat hunter finds a new attack pattern, they will then tune SIEM correlation rules to ensure that specific threat is detected automatically in the future. The tuning is the result of the hunt, not the activity of hunting itself.

Question 11

Question Type: MultipleChoice

When configuring a FortiAnalyzer to act as a collector device, which two steps must you perform? (Choose two.)

Options:

A- Enable log compression.
B- Configure log forwarding to a FortiAnalyzer in analyzer mode.
C- Configure the data policy to focus on archiving.
D- Configure Fabric authorization on the connecting interface.

Answer:

B, D

Explanation:

Understanding FortiAnalyzer Roles:

FortiAnalyzer can operate in two primary modes: collector mode and analyzer mode.

Collector Mode: Gathers logs from various devices and forwards them to another FortiAnalyzer

operating in analyzer mode for detailed analysis.

Analyzer Mode: Provides detailed log analysis, reporting, and incident management.

Steps to Configure FortiAnalyzer as a Collector Device:

A . Enable Log Compression:

While enabling log compression can help save storage space, it is not a mandatory step specifically required for configuring FortiAnalyzer in collector mode.

Not selected as it is optional and not directly related to the collector configuration process.

B . Configure Log Forwarding to a FortiAnalyzer in Analyzer Mode:

Essential for ensuring that logs collected by the collector FortiAnalyzer are sent to the analyzer FortiAnalyzer for detailed processing.

Selected as it is a critical step in configuring a FortiAnalyzer as a collector device.

Step 1: Access the FortiAnalyzer interface and navigate to log forwarding settings.

Step 2: Configure log forwarding by specifying the IP address and necessary credentials of the FortiAnalyzer in analyzer mode.

C . Configure the Data Policy to Focus on Archiving:

Data policy configuration typically relates to how logs are stored and managed within FortiAnalyzer, focusing on archiving may not be specifically required for a collector device setup.

N ot selected as it is not a necessary step for configuring the collector mode.

D . Configure Fabric Authorization on the Connecting Interface:

Necessary to ensure secure and authenticated communication between FortiAnalyzer devices within the Security Fabric.

Selected as it is essential for secure integration and communication.

Step 1: Access the FortiAnalyzer interface and navigate to the Fabric authorization settings.

Step 2: Enable Fabric authorization on the interface used for connecting to other Fortinet devices and FortiAnalyzers.

Implementation Summary:

Configure log forwarding to ensure logs collected are sent to the analyzer.

Enable Fabric authorization to ensure secure communication and integration within the Security Fabric.

Conclusion:

Configuring log forwarding and Fabric authorization are key steps in setting up a FortiAnalyzer as a collector device to ensure proper log collection and forwarding for analysis.

Fortinet Documentation on FortiAnalyzer Roles and Configurations FortiAnalyzer Administration Guide

By configuring log forwarding to a FortiAnalyzer in analyzer mode and enabling Fabric authorization on the connecting interface, you can ensure proper setup of FortiAnalyzer as a collector device.

Question 12

Question Type: MultipleChoice

Based on the Pyramid of Pain model, which two statements accurately describe the value of an indicator and how difficult it is for an adversary to change? (Select two answers)

Options:

A- IP addresses are easy because adversaries can spoof them or move them to new resources.
B- Tactics, techniques, and procedures are hard because adversaries must adapt their methods.
C- Artifacts are easy because adversaries can alter file paths or registry keys.
D- Tools are easy because often, multiple alternatives exist.

Answer:

A, B

Explanation:

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

The Pyramid of Pain (David Bianco) is a core concept taught in FortiSIEM 7.3 and FortiSOAR 7.6 curriculum to help SOC analysts prioritize threat intelligence and detection logic. The model ranks indicators based on the 'pain' or effort they cause an adversary to change:

IP Addresses (Easy): These are classified as 'Easy' to change. An attacker can simply rotate through a proxy service, use a different VPS, or utilize a new compromised host to continue their campaign. While more valuable than a file hash, they provide relatively low-long term value to the defender because they are so ephemeral.

TTPs (Tough/Hard): This is the apex of the pyramid. TTPs (Tactics, Techniques, and Procedures) represent the fundamental way an adversary operates. If a defender successfully detects and

blocks a Tactic (e.g., a specific way an attacker performs privilege escalation), the adversary is forced to reinvent their entire operational process, which is time-consuming and difficult.

Why other options are incorrect:

Artifacts (C): According to the pyramid, Network/Host Artifacts are classified as 'Annoying', not 'Easy'. While an attacker can change them, it requires modifying their code or script behavior, which causes more friction than simply switching an IP address.

Tools (D): Tools are classified as 'Challenging'. While alternatives exist, an adversary usually invests significant time mastering a specific toolset; losing the ability to use that tool effectively disrupts their efficiency significantly.

Question 13

Question Type: MultipleChoice

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?

Options:

A- Playbook
B- Data selector
C- Event handler
D- Connector

Answer:

C

Explanation:

Understanding Automation Processes in FortiAnalyzer:

FortiAnalyzer can automate responses to detected security events, such as running commands on FortiGate devices.

Analyzing the Customer Requirement:

The customer wants to run a CLI command on FortiGate to block predefined URLs when a

botnet C&C server IP is detected.

This requires an automated response triggered by a specific event.

Evaluating the Options:

Option A: Playbooks orchestrate complex workflows but are not typically used for direct event-triggered automation processes.

Option B: Data selectors filter logs based on criteria but do not initiate automation processes.

Option C: Event handlers can be configured to detect specific events (such as detecting a botnet C&C server IP) and trigger automation stitches to execute predefined actions.

Option D: Connectors facilitate communication between FortiAnalyzer and other systems but are not the primary mechanism for initiating automation based on log events.

Conclusion:

To start the automation process when a botnet C&C server IP is detected, you must use an Event handler in FortiAnalyzer.

Fortinet Documentation on Event Handlers and Automation Stitches in FortiAnalyzer.

Best Practices for Configuring Automated Responses in FortiAnalyzer.