ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

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? (Choose two answers)

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

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

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:

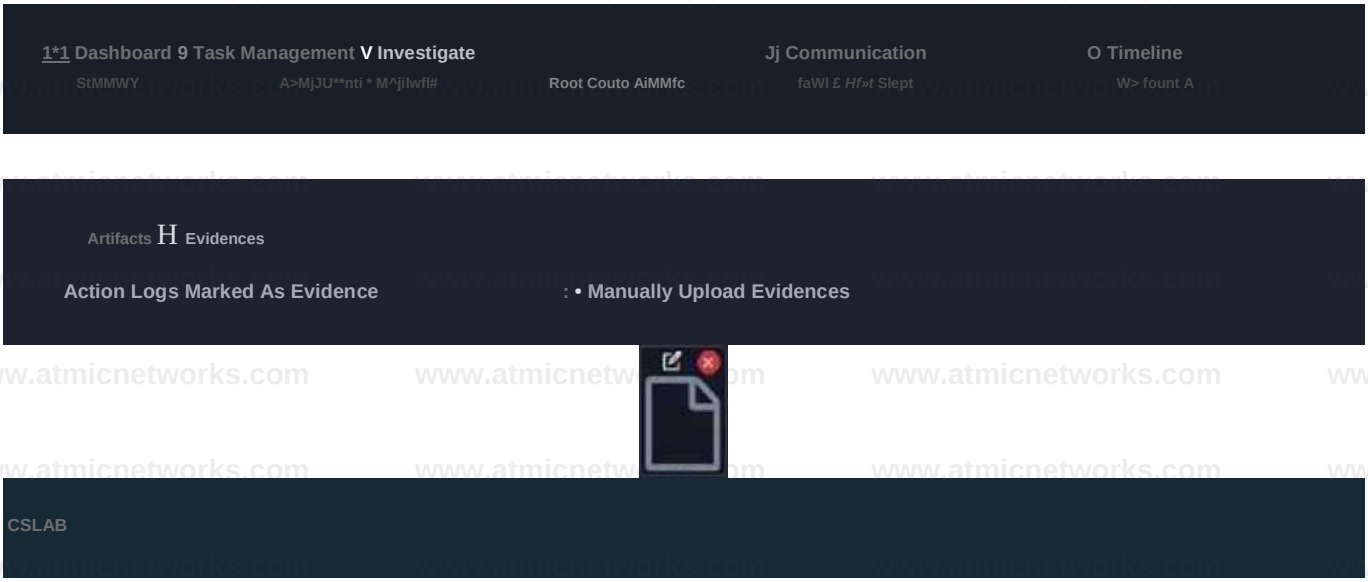
Automate workflows (B): While SOAR is designed for automation, the act of "automating" is a DevOps or SOC engineering task. Threat hunting itself is a proactive investigation; while playbooks

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: 3

Refer to the exhibit.



How do you add a piece of evidence to the Action Logs Marked As Evidence area? (Choose one answer)

A. By tagging output or a workspace comment with the keyword Evidence
B. By linking an indicator to the war room
C. By creating an evidence collection task and attaching a file
D. By executing a playbook with the Save Execution Logs option enabled

Answer: A

Explanation:

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

In FortiSOAR 7.6, the War Room is a collaborative space designed for high-priority incident investigation. The Evidences tab within the Investigate view (as shown in the exhibit) is specifically designed to highlight critical findings found during the investigation process.

Evidence Tagging: To populate the Action Logs Marked As Evidence section, an analyst must specifically tag a relevant log entry, a playbook output, or a comment within the collaboration workspace with the system-defined keyword "Evidence".

Automatic Categorization: Once the tag is applied, FortiSOAR automatically parses these entries and displays them in this centralized view. This allows team members and stakeholders to quickly view substantiated facts and proof gathered during the "Root Cause Analysis" phase without sifting through all raw action logs.

Manual vs. Action Logs: The exhibit shows two distinct areas: "Manually Upload Evidences" (where files like the CSLAB document shown can be dragged and dropped) and "Action Logs Marked As Evidence." The latter is reserved exclusively for system-generated logs or comments that have been promoted to evidence status via tagging.

Why other options are incorrect:

By linking an indicator to the war room (B): Linking indicators associates technical artifacts (like IPs or hashes) with the record, but it does not automatically classify them as evidence within the War Room action log view.

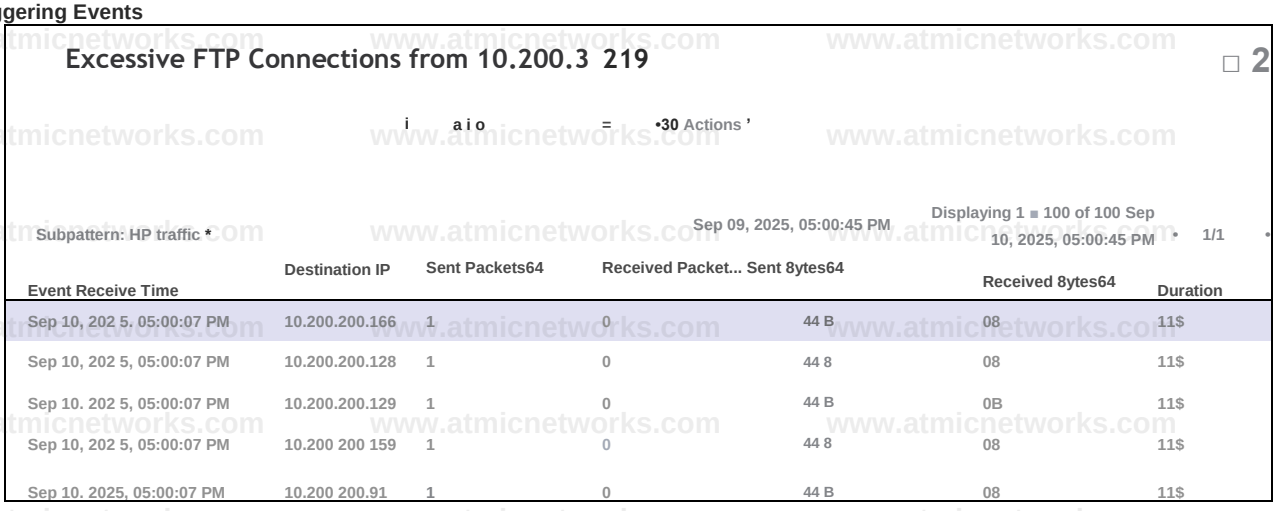
By creating an evidence collection task and attaching a file (C): While this is a valid step in an investigation, attaching a file to a task typically places it in the "Attachments" or "Manually Upload Evidences" area, rather than the "Action Logs" section specifically.

By executing a playbook with the Save Execution Logs option enabled (D): Saving execution logs ensures a trail of what the playbook did, but it does not mark the output as "Evidence" unless the specific logic or a manual analyst action applies the "Evidence" tag to the resulting log entry.

Question: 4

Refer to the exhibits.

Triggering Events



Excessive FTP Connections from 10.200.3 219

□ 2

i a i o = •30 Actions ’

Subpattern: HP traffic * Sep 09, 2025, 05:00:45 PM Displaying 1 ■ 100 of 100 Sep 10, 2025, 05:00:45 PM • 1/1 •

Event Receive Time	Destination IP	Sent Packets64	Received Packet...	Sent 8ytes64	Received 8ytes64	Duration
Sep 10, 202 5. 05:00:07 PM	10.200.200.166	1	0	44 B	08	11$
Sep 10, 202 5, 05:00:07 PM	10.200.200.128	1	0	44 8	08	11$
Sep 10. 202 5, 05:00:07 PM	10.200.200.129	1	0	44 B	0B	11$
Sep 10, 202 5, 05:00:07 PM	10.200 200 159	1	0	44 8	08	11$
Sep 10. 2025, 05:00:07 PM	10.200 200.91	1	0	44 B	08	11$

Raw Logs

Raw Message • o

<l89>date=2025 09 10 time*l3:58:46 devname='FortlGate-ISFW devld«'FGVMSLTM24000847* eventtime* 1757537925873767456 tz=' 0700' logId="0000000013’ type=’traffic' subtype='forward" level-'notice’ vd-'root" srcip*10.200.3.219 srcport*55690 srcintf-'portl' srclntfrole»'undeflned' dstlp*10.200.200.166 dstport*21 dstlntf«*port3' dstlntfrole-’undeflned' srccountry-'Reserved' dstcountry-'Reserved' sessionId=12754790 proto=6 action='tlmeout" pollcyld=1 pollcytype='pollcy' poluuid-'703716b8c06a-51ee-4b75-69d6e<904elC policyname-'Any-Any' service*'FTP' trandlsp-'noop' appcat-'unscanned' duration-11 sent byte-44 rcvdbyte=0 sentpkt’1 rcvdpkt’O

Assume that the traffic flows are identical, except for the destination IP address. There is only one FortiGate in network address translation (NAT) mode in this environment.

Based on the exhibits, which two conclusions can you make about this FortiSIEM incident? (Choose two answers)

A. The client 10.200.3.219 is conducting active reconnaissance.

B. FortiGate is not routing the packets to the destination hosts.

C. The destination hosts are not responding.

D. FortiGate is blocking the return flows.

Answer: A, C

Explanation:

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

Based on the analysis of the Triggering Events and the Raw Message provided in the FortiSIEM 7.3 interface:

Active Reconnaissance (A): The "Triggering Events" table shows a single source IP (10.200.3.219) attempting to connect to multiple different destination IP addresses (10.200.200.166, .128, .129, .159, .91) on the same service (FTP/Port 21). Each attempt consists of exactly 1 Sent Packet and 0 Received Packets. This pattern of "one-to-many" sequential connection attempts is the signature of a horizontal port scan, which is a primary technique in Active Reconnaissance.

Destination hosts are not responding (C): The Raw Log shows the action as "timeout" and specifically lists "sentpkt=1 rcvdpkt=0". In FortiGate log logic (which FortiSIEM parses), a "timeout" with zero received packets indicates that the firewall allowed the packet out (Action was not 'deny'), but no SYN-ACK or response was received from the target host within the session timeout period. This confirms the destination hosts are either ofline, non-existent, or silently dropping the traffic.

Why other options are incorrect:

FortiGate is not routing (B): If the FortiGate were not routing the packets, the logs would typically not show a successful session initialization ending in a "timeout," or they would show a routing

error/deny. The fact that 44 bytes were sent indicates the FortiGate processed and attempted to forward the traffic.

FortiGate is blocking return flows (D): If the return flow were being blocked by a security policy on the FortiGate, the action

would typically be logged as "deny" for the return traffic, and the session state would reflect a policy violation rather than a generic session "timeout".

Question: 5

When you use a manual trigger to save user input as a variable, what is the correct Jinja expression to reference the variable? (Choose one answer)

A. {{ vars.input.params.<variable_name> }}

B. {{ globalVars.<variable_name> }}

C. {{ vars.item.<variable_name> }}

D. {{ vars.steps.<variable_name> }}

Answer: A

Explanation:

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

In FortiSOAR 7.6, the playbook engine utilizes Jinja2 expressions to handle dynamic data. When a playbook is configured with a Manual Trigger, the administrator can define input fields (such as text, picklists, or checkboxes) that an analyst must fill out when executing the playbook from a record.

Input Parameter Mapping: Any data entered by the user during this manual trigger phase is automatically mapped to the input.params dictionary within the vars object. Therefore, the syntax to retrieve a specific input value is {{ vars.input.params.variable_name }}.

Scope of Variables: This specific path ensures that the variable is pulled from the initial user input rather than from the output of a subsequent step (vars.steps) or a globally defined variable (globalVars).

Question: 6

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? (Choose two answers)

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.

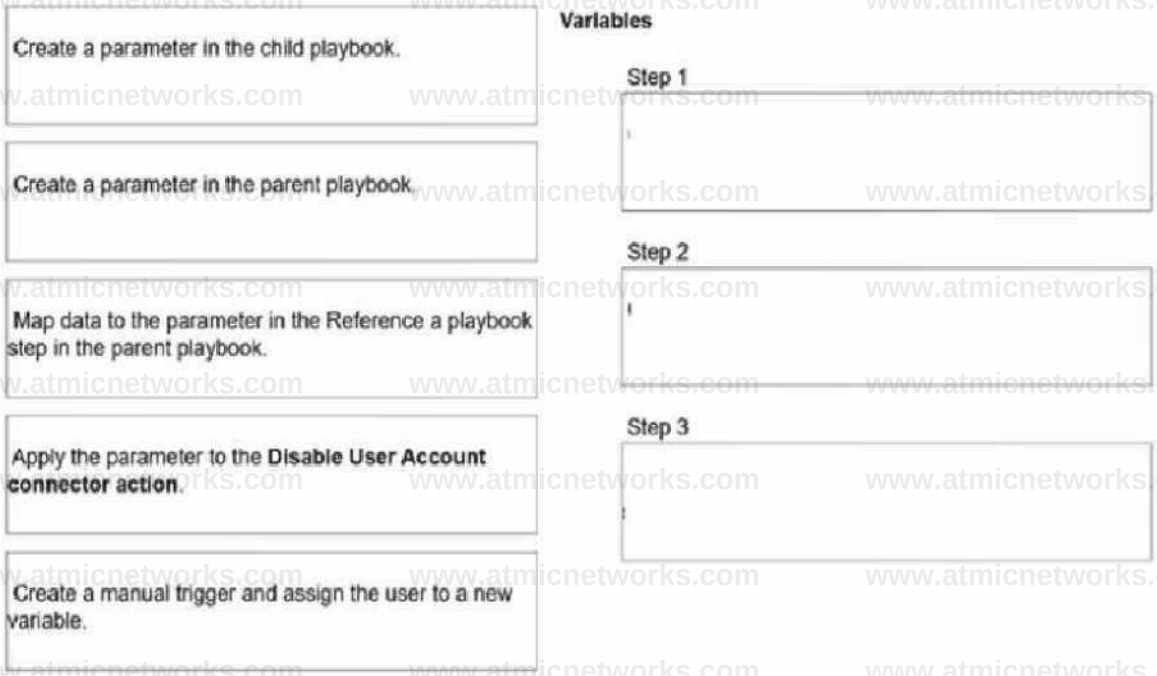
Question: 7

DRAG DROP

Refer to the exhibits.

You have a playbook that, depending on whether an analyst deems the alert to be a true positive, could reference a child playbook. You need to pass variables from the parent playbook to the child playbook.

Place the steps needed to accomplish this in the correct order.



Answer:

Explanation:

1. Create a parameter in the child playbook.
2. Apply the parameter to the Disable User Account connector action.
3. Map data to the parameter in the Reference a playbook step in the parent playbook.

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

In FortiSOAR 7.6, the methodology for passing data between playbooks—specifically from a parent to a "Referenced" (child) playbook—follows a strict data flow hierarchy:

Step 1: Create a parameter in the child playbook. Before a parent can send data, the child playbook must be configured to receive it. This is done by adding "Input Parameters" in the Start step of the child playbook (configured as a "Referenced" trigger). These parameters act as the "inbox" for external data.

Step 2: Apply the parameter to the connector action. Once the child playbook has the parameter defined (e.g., user_id), you must use a Jinja expression like {{vars.input.params.user_id}} within the child's action steps (such as the Active Directory: Disable User Account connector) so that the child playbook actually utilizes the data it receives.

Step 3: Map data to the parameter in the parent playbook. Finally, in the parent playbook, when you

add the Reference a Playbook step and select the child playbook, FortiSOAR automatically displays the parameters created in Step 1. You then map existing variables from the parent's environment (e.g., from a previous "Search by SamAccountName" step) into these fields to complete the hand-off.

Why other options are excluded:

Create a manual trigger and assign the user to a new variable: While manual triggers capture data, they are not the mechanism for passing data between nested playbooks; they are for user-to-system interaction.

Create a parameter in the parent playbook: Parameters in a parent playbook are used to receive data from outside (like an external API or manual input), not to send data down to a child. The child defines what it needs; the parent simply provides it in the Reference step.

Question: 8

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)

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: 9

Refer to the exhibit.

Query configuration

Filter By: Event Keywords | Event Attribute | CMDB Attribute — Clear All | Load | Save

Paren	Attribute	Operator	Value	Paren	Next	Row
© 0	Destination Country	IN	v Group: Europe	©	Q AND OR	+ m
© 0	Destination Country	IN	* Group: Asia	©	Q AND OR	+ 1
© 0	Destination Country	IS HOT	* null	©	0 AND OR	+ S
© 0	Source IP	IN	V 10.0.0.0,10.700.200.254	©	0 AND OR	+ i

Time Range: Real-time Relative Absolute

Last 30 Days »

You are trying to find traffic flows to destinations that are in Europe or Asia, for hosts in the local LAN segment. However, the query returns no results. Assume these logs exist on FortiSIEM.

Which three mistakes can you see in the query shown in the exhibit? (Choose three answers)

A. The null value cannot be used with the IS NOT operator.

B. The time range must be Absolute for queries that use configuration management database (CMDB) groups.

C. There are missing parentheses between the first row (Group: Europe) and the second row (Group: Asia).

D. The Source IP row operator must be BETWEEN 10.0.0.0, 10.200.200.254.

E. The logical operator for the first row (Group: Europe) must be OR.

Answer: C, D, E

Explanation:

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

Analyzing the Query Configuration exhibit in the context of FortiSIEM 7.3 search logic reveals several syntax and logical errors that prevent the query from returning results:

Logical Operator Error (E): The user intends to find traffic to Europe OR Asia. In the exhibit, the first row (Group: Europe) is followed by a default AND operator. This forces the query to look for a single flow where the destination is simultaneously in Europe and Asia, which is logically impossible. It must be changed to OR.

Missing Parentheses (C): When combining OR and AND logic in FortiSIEM, parentheses are required to define the order of operations. Without them, the query might evaluate "Asia AND Destination Country IS NOT null AND Source IP IN..." first. To correctly find (Europe OR Asia) that also matches the LAN segment, parentheses must group the first two rows.

Incorrect Operator for IP Range (D): The exhibit uses the IN operator for the value 10.0.0.0, 10.200.200.254. In FortiSIEM, the IN operator is used for a comma-separated list of specific values or CMDB groups. To specify a continuous range of IP addresses (the "LAN segment"), the BETWEEN operator must be used.

Why other options are incorrect:

IS NOT null (A): In FortiSIEM, "IS NOT null" is a valid operator/value combination used to ensure a specific attribute has been successfully parsed and populated in the event record.

Time Range (B): There is no requirement for a time range to be "Absolute" when using CMDB groups; "Relative" time ranges (like the "Last 30 Days" shown) are commonly used and fully supported for such queries.

SOC Concepts and Frameworks

Question: 10

Refer to the exhibit.

Which method most effectively reduces the attack surface of this organization? (Choose one answer)

A. Forward all firewall logs to the security information and event management (SIEM) system.

B. Enable deep inspection on firewall policies.

C. Implement macrosegmentation.

D. Remove unused devices.

Answer: D

Explanation:

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

In the context of the Attack Surface Management modules within the FortiSIEM 7.3 and FortiSOAR 7.6 security frameworks, "reducing the attack surface" refers to the process of minimizing the number of possible entry points (attack vectors) that an unauthorized user could exploit.

Definition of Attack Surface: The attack surface consists of all the different points where an attacker could try to enter data to or extract data from an environment. This includes hardware, software, SaaS components, and network interfaces.

Effectiveness of Asset Removal: Removing unused devices, services, or software is the most fundamental and effective way to reduce the attack surface. By decommissioning an unused server

or workstation (as shown in the LAN/Server diagram), you completely eliminate all potential vulnerabilities associated with that asset, its operating system, and its active services.

Contrast with other methods:

Forwarding logs (A) and Deep Inspection (B) are detective and preventive controls, respectively. They help manage the risk within the existing attack surface but do not actually shrink the size of the surface itself.

Macrosegmentation (C) limits the "blast radius" or lateral movement after a compromise has occurred. While it secures the interior, it does not remove the initial entry points that define the external attack surface.

Why other options are incorrect:

Forwarding logs (A): This increases visibility but does not remove potential vulnerabilities.

Deep Inspection (B): This is a security measure to detect threats within existing traffic but does not eliminate the target (the device) itself.

Implement macrosegmentation (C): While highly recommended for security, it is a network architecture strategy to contain threats, whereas the prompt asks for the most effective method to reduce the surface. Removing the asset entirely (D) is the most absolute reduction possible.

Question: 11

DRAG DROP

Match the FortiSIEM device type to its description. Select each FortiSIEM device type in the left column, hold and drag it to the blank space next to its corresponding description in the column on the right.

FortiSIEM Device Types	Descnption
Agent	Offloads log collection and performance monitoring at remote sites
Collector	Executes real-time event correlation, analytics, and historical searches to handle processing load
Supervisor	Acts as the central management node, hosting the UI. CMDB, dashboards, and reports
Tenant	Collects endpoint logs and system changes
Worker	
Secure Message Exchange	

Answer:

Explanation:

Collector 2. Worker 3. Supervisor 4. Agent

The FortiSIEM 7.3 architecture is built upon a distributed multi-tenant model consisting of several distinct functional roles to ensure scalability and performance:

Supervisor: This is the primary management node in a FortiSIEM cluster. It hosts the Graphical User Interface (GUI), the Configuration Management Database (CMDB), and manages the overall system configurations, reporting, and dashboarding.

Worker: These nodes are responsible for the heavy lifting of data processing. They execute real-time event correlation against the rules engine, perform historical search queries, and handle the analytics workload to ensure the Supervisor node is not overwhelmed.

Collector: Collectors are typically deployed at remote sites or different network segments to ofload log collection from the central cluster. They receive logs via Syslog, SNMP, or WMI, compress the data, and securely forward it to the Workers or Supervisor. They also perform performance monitoring of local devices.

Agent: These are lightweight software components installed directly on endpoints (Windows/Linux). Their primary role is to collect local endpoint logs, monitor file integrity (system changes), and track user activity that cannot be captured via traditional network-based logging.

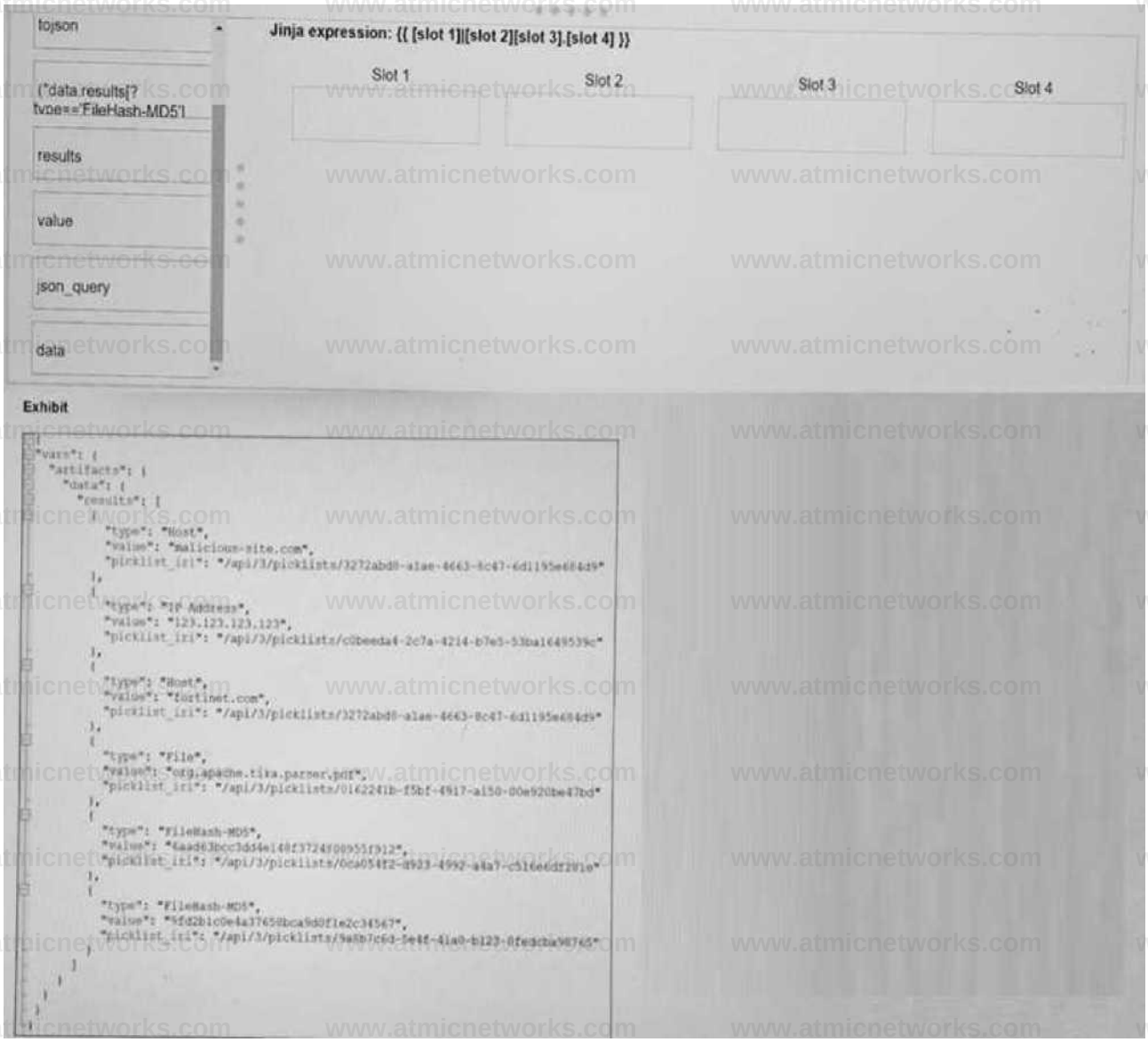
Question: 12

DRAG DROP

Refer to the exhibit. What is the correct Jinja expression to filter the results to show only the MD5 hash values?

{{ [slot 1] | [slot 2] [slot 3].[slot 4] }}

Select the Jinja expression in the left column, hold and drag it to a blank position on the right. Place the four correct steps in order, placing the first step in the first slot.



Answer:

Explanation:

Slot 1: data Slot 2: json_query Slot 3: ("results[?type=='FileHash-MD5']") Slot 4: value

Final Expression: {{ vars.artifacts.data | json_query("results[?type=='FileHash-MD5']") .value }}

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

In FortiSOAR 7.6, advanced data manipulation within playbooks often requires the use of JMESPath queries via the json_query Jinja filter. To extract specific data from a complex JSON object (like the vars.artifacts dictionary shown in the exhibit), the analyst must follow the structural hierarchy:

Slot 1 (data): Based on the exhibit, the root of the artifact information is located under vars.artifacts.dat

a. Therefore, "data" is the starting point for the filter.

Slot 2 (json_query): To perform advanced filtering (searching for a specific type), the json_query filter must be applied. This allows the playbook to traverse the list and find items matching a specific keyvalue pair.

Slot 3 ("results[?type=='FileHash-MD5']"): This is the JMESPath expression. It looks into the results array and applies a filter [?...] to find only those objects where the type attribute exactly matches FileHash-MD5.

Slot 4 (value): Once the correct object(s) are found, the expression needs to return the actual hash. In the JSON exhibit, the MD5 string is stored in the key named value.

Why other options are incorrect:

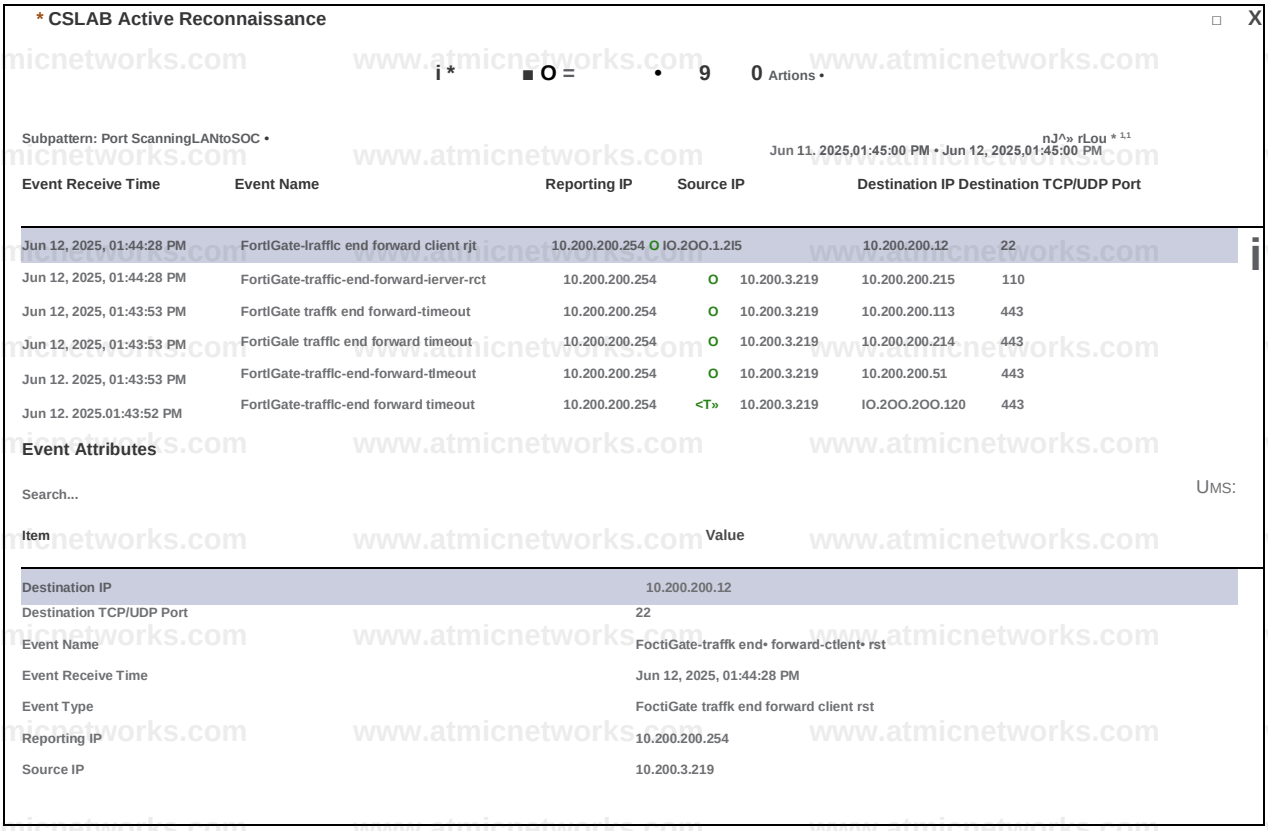
tojson: This filter converts a dictionary/list into a JSON string, which would break the ability to further query the object for the "value" field.

results (as a standalone slot): While "results" is part of the path, it is handled inside the json_query string to allow for conditional filtering.

Question: 13

Refer to the exhibit.

Triggering events



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)

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.

Question: 14

Which three statements accurately describe step utilities in a playbook step? (Choose three answers)

A. The Timeout step utility sets a maximum execution time for the step and terminates playbook execution if exceeded.

B. The Loop step utility can only be used once in each playbook step.

C. The Variables step utility stores the output of the step directly in the step itself.

D. The Condition step utility behavior changes depending on if a loop exists for that step.

E. The Mock Output step utility uses HTML format to simulate real outputs.

Answer: A, B, D

Explanation:

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

In FortiSOAR 7.6, step utilities are advanced configurations applied to individual playbook steps to control logic, timing, and data processing. According to the Playbook Engine architecture:

Timeout (A): The Timeout utility allows an administrator to define a maximum duration for a step to complete. If the step does not finish within this designated window, the playbook engine terminates the step and the overall playbook execution to prevent hung processes and resource exhaustion.

Loop (B): The Loop utility is used for iterative processing (e.g., performing a lookup for every IP in a list). A playbook step can only contain one Loop utility configuration. If multiple iterations are required across different data sets, they must be handled in separate steps or nested child playbooks.

Condition (D): The Condition utility (Decision Step logic) behaves differently when a Loop is present. If there is no loop, the condition determines if the step executes once. If a loop is present, the condition is evaluated for each item in the loop, effectively acting as a filter for which iterations proceed.

Why other options are incorrect:

Variables (C): The Variables utility (Set Variable) is used to define new custom variables within the scope of that step for later use. It does not "store the output of the step directly in the step itself"; step outputs are automatically stored in the vars.steps.<step_name> object by the engine regardless of the utility used.

Mock Output (E): The Mock Output utility is used for testing and development to simulate successful data returns without actually executing a connector. It uses JSON format, not HTML, to ensure the simulated data structure matches what the playbook engine expects for downstream Jinja processing.

Question: 15

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)

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.

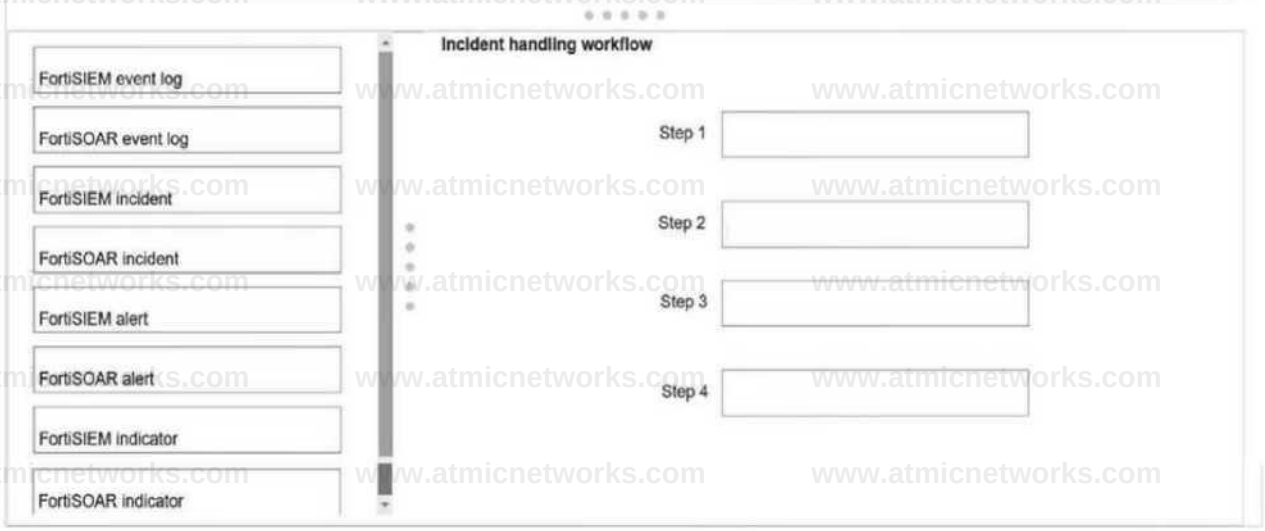
VDOM name (B): In the exhibit, the VDOM field contains multiple values ("VDOM_1", "VDOM_2"). If VDOMs are disabled on the FortiGate, this field should generally be left blank or set to the default "root." Setting it specifically to "VDOM_1" when VDOMs are disabled is not a universal requirement for connectivity;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

Question: 16

DRAG DROP

Using the default data ingestion wizard in FortiSOAR, place the incident handling workflow from FortiSIEM to FortiSOAR in the correct sequence. Select each workflow component in the left column,

hold and drag it to a blank position in the column on the right. Place the four correct workflow components in order, placing the first step in the first position at the top of the column.



Answer:

Explanation:

1. FortiSIEM incident 2. FortiSOAR alert 3. FortiSOAR indicator 4. FortiSOAR incident

In the standard integration between FortiSIEM 7.3 and FortiSOAR 7.6, the data ingestion wizard follows a specific object mapping hierarchy to ensure that high-fidelity security events are managed correctly.

Step 1: FortiSIEM incident: The workflow begins in FortiSIEM. When a correlation rule triggers, it generates an Incident (not just a raw log). The FortiSOAR connector polls the FortiSIEM API specifically for these incident records.

Step 2: FortiSOAR alert: By default, ingested FortiSIEM incidents are mapped to the Alerts module in FortiSOAR. This serves as a "triage" layer where automated playbooks can perform initial analysis before a human determines if it warrants a full-scale investigation.

Step 3: FortiSOAR indicator: As the alert is processed (either during ingestion or immediately after), the playbook extracts technical artifacts (IPs, hashes, URLs) and creates Indicator records. This allows for automated threat intelligence lookups and cross-referencing against other alerts.

Step 4: FortiSOAR incident: If the alert is validated (either through automated playbook scoring or

manual analyst review), it is promoted to a FortiSOAR Incident. This represents a confirmed security issue that requires formal tracking, remediation, and reporting.

Question: 17

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)

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: 18

Refer to the exhibits.

Investigation Actions

Investigation Actions:

1. **Identify and Isolate Affected Systems: Begin by identifying the systems associated with the incident, specifically those linked to the IP addresses FortiGate-ISFW.FortiGate-NGFW, 10.200.200.254, and 100.64.2.21. Isolate these systems to prevent further data exfiltration.**
2. **Analyze Network Traffic: Examine network logs to trace the data flow and identify any unusual patterns or unauthorized data transfers. Focus on traffic related to the technique 'Exfiltration Over Unencrypted/Obfuscated Non C2 Protocol' (T1048.003).**
3. **Review Security Alerts and Logs: Check security alerts and logs from the incident reporting device and other security tools to gather more context about the exfiltration attempt.**
4. **Conduct a Forensic Analysis: Perform a forensic analysis on the affected systems to uncover any malware or unauthorized access points that facilitated the exfiltration.**
5. **Assess Data Impact: Determine the type and volume of data exfiltrated to assess the potential impact on the organization.**
6. **Implement Mitigation Measures: Based on findings, apply necessary security patches, update firewall rules, and enhance monitoring to prevent future incidents.**

Remediation Actions

Remediation Actions:

1. **Immediate Containment: Isolate the affected systems, including the devices with IPs FortiGate-ISFW.FortiGate.NGFW and 10.200.200.254, to prevent further data exfiltration. Disconnect these systems from the network to halt any ongoing unauthorized data transfers.**
2. **Incident Analysis: Conduct a thorough investigation to understand the scope and impact of the exfiltration. Analyze logs and network traffic to identify the data accessed and the method used for exfiltration.**
3. **Patch and Update: Ensure all systems, especially those involved in the incident, are updated with the latest security patches to close any vulnerabilities that may have been exploited.**
4. **Enhance Monitoring: Implement enhanced monitoring and alerting for unusual data transfer activities, particularly focusing on non-standard protocols that may be used for exfiltration.**
5. **User Training: Conduct cybersecurity awareness training for employees to recognize and report suspicious activities, emphasizing the importance of data protection.**
6. **Review and Update Security Policies: Reassess and update security policies and procedures to address any gaps identified during the incident analysis.**

How is the investigation and remediation output generated on FortiSIEM? (Choose one answer)

A. By exporting an incident

B. By running an incident report

C. By using FortiAI to summarize the incident

D. By viewing the Context tab of an incident

Answer: C

Explanation:

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

In FortiSIEM 7.3, a key innovation is the integration of FortiAI, which provides generative AI capabilities to assist SOC

analysts during the triage and response process.

Generative AI Summary: When an incident occurs, FortiAI can automatically analyze the underlying logs, correlation logic, and MITRE ATT&CK techniques (such as "Exfiltration Over Alternative Protocol" shown in the exhibit) to generate a human-readable summary.

Structured Output: The output displayed in the exhibit—specifically the categorized Investigation Actions (identifying affected systems, analyzing traffic) and Remediation Actions (immediate containment, patching, user training)—is the typical result of a FortiAI summary request.

Analyst Efficiency: This feature is designed to reduce the "mean time to respond" (MTTR) by providing analysts with immediate, actionable steps without requiring them to manually piece together the recommended response plan from static documentation or disparate log views.

Why other options are incorrect:

Exporting an incident (A): Exporting an incident typically results in a raw data file (CSV/JSON/PDF) containing the log data and metadata, rather than an AI-generated strategic plan for investigation and remediation.

Running an incident report (B): Standard incident reports provide statistical and historical data about incidents over time. They do not dynamically generate specific, numbered investigation steps tailored to the unique context of a single live incident.

Context tab (D): The Context tab in FortiSIEM is primarily used to view the CMDB information of the

involved assets (e.g., host details, owner, location) and related historical events. While it provides the data needed for an investigation, it does not provide the list of actions to take.

Question: 19

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

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.

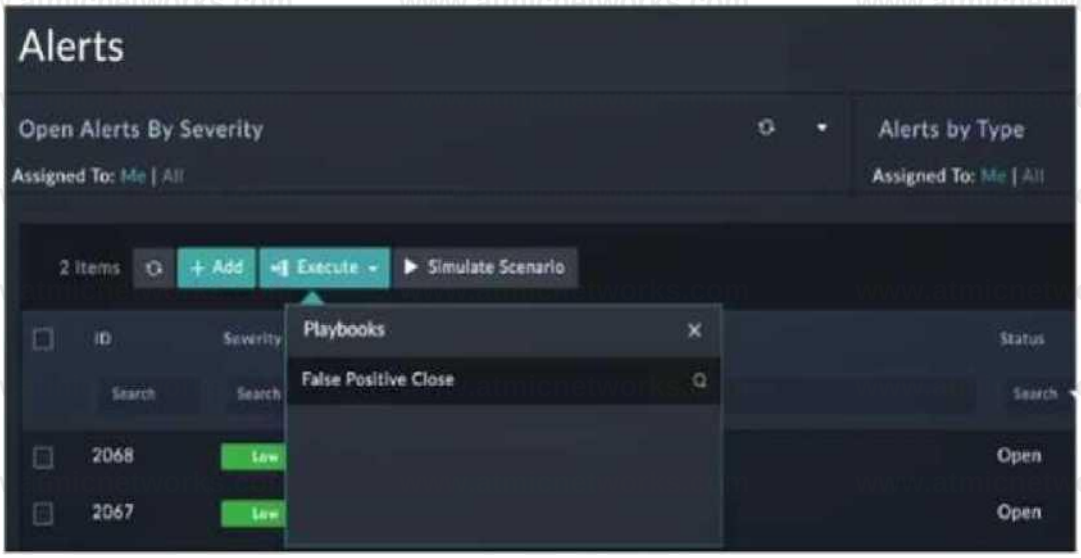
Why other options are incorrect:

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: 20

Refer to the exhibit.



You configured a playbook named False Positive Close, and want to run it to verify if it works.

However, when you click Execute and search for the playbook, you do not see it listed. Which two reasons could be the cause of the problem? (Choose two answers)

A. The playbook must first be published using the Application Editor.

B. Another instance of the playbook is currently executing.

C. The Alerts module is not among the list of modules the playbook can execute on.

D. The manual trigger is configured to require record input to run.

Answer: C, D

Explanation:

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

In FortiSOAR 7.6, manual playbooks appear in the Execute menu of a record only if they meet specific configuration criteria defined in the Manual Trigger step:

Module Scope (C): When creating a playbook with a manual trigger, the administrator must explicitly select which modules (e.g., Alerts, Incidents, Indicators) can execute the playbook. If the Alerts module is not selected in the "Applicable Modules" section of the trigger configuration, the playbook will remain hidden from the Execute menu when an analyst is viewing the Alerts module.

Trigger Execution Requirements (D): Manual triggers can be configured to execute on no records, a single record, or multiple records. If a playbook is configured with the "Requires record input to run" setting but is specifically restricted to a different input type (or if there is a mismatch in the selection logic), it will not appear in the menu unless the correct number of

records are selected. Furthermore, if a playbook is designed to run only when no record is selected (global utility), it will not show up in the context-sensitive menu of a specific record.

Why other options are incorrect:

Publishing (A): FortiSOAR playbooks do not require a separate "publishing" step via an Application Editor to become visible. Once they are saved and active (toggled on), they are immediately available for use based on their trigger settings.

Concurrent Execution (B): FortiSOAR allows multiple instances of the same playbook to run simultaneously. An active execution of a playbook does not hide it from the menu for other analysts or subsequent runs.

Question: 21

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

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: 22

Which two best practices should be followed when exporting playbooks in FortiAnalyzer? (Choose two answers)

A. Disable playbooks before exporting them.

B. Include the associated connector settings.

C. Move playbooks between ADOMs rather than exporting playbooks and re-importing them.

D. Ensure the exported playbook's names do not exist in the target ADOM.

Answer: A, B

Explanation:

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

According to the FortiAnalyzer 7.4 SOC Analyst official training material (Lesson 5: Automation) and supporting documentation for FortiSOAR 7.6 and FortiSIEM 7.3 integration, the following best practices are recommended for playbook portability:

Disable playbooks before exporting (A): When a playbook is exported, its current status (Enabled or Disabled) is preserved in the export file. If an Enabled playbook is imported into a destination ADOM

where its trigger conditions are immediately met, it will start executing automatically. Disabling the playbook before export is a critical best practice to prevent unintended automated actions from occurring in the new environment before the analyst has had a chance to verify local configurations.

Include the associated connector settings (B): FortiAnalyzer allows you to include required connector configurations during the export process. By selecting this option, the exported file includes the necessary metadata and configurations for the connectors that the playbook relies on to execute its tasks. This ensures the playbook remains functional and portable across different FortiAnalyzer units or ADOMs without requiring the manual recreation of every connector.

Why other options are incorrect:

Move playbooks between ADOMs (C): There is no native "Move" function for automation playbooks between ADOMs in the same sense as moving a device. The standard supported workflow for transferring automation logic is the Export and Import process.

Ensure names do not exist in target (D): While maintaining unique names is good practice, it is not a required "best practice" for the export process itself because FortiAnalyzer automatically handles name conflicts. If an imported playbook shares a name with an existing one, the system automatically appends a timestamp to the new playbook's name to avoid a conflict.

Question: 23

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

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: 24

Which of the following are critical when analyzing and managing events and incidents in a SOC? (Choose two answers)

A. Accurate detection of threats

B. Immediate escalation for all alerts

C. Rapid identification of false positives

D. Periodic system downtime for maintenance

Answer: A, C

Explanation:

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

In a modern Security Operations Center (SOC) environment powered by FortiSIEM 7.3 and FortiSOAR 7.6, the efficiency of the incident response lifecycle depends on two primary pillars of analysis:

Accurate detection of threats (A): The primary goal of a SOC is to identify genuine malicious activity. Using FortiSIEM's correlation rules and machine learning (UEBA), the system must be tuned to detect patterns that signify real risk. Accuracy ensures that the SOC is not blinded by noise and can focus on critical security events that impact the organization's posture.

Rapid identification of false positives (C): "Alert Fatigue" is one of the greatest challenges in a SOC. Analysts must be able to quickly distinguish between legitimate anomalies (false positives) and actual threats. FortiSOAR assists in this by using automated playbooks to perform initial triage and "pre-processing"—such as checking IP reputations or verifying user activity—to automatically close or demote alerts that do not represent a true threat, thereby freeing up analysts for high-priority investigations.

Why other options are incorrect:

Immediate escalation for all alerts (B): This is a poor SOC practice. Escalating every alert without triage leads to analyst burnout and overloads senior responders with low-value tasks. The goal of a tiered SOC (Tier 1, Tier 2, Tier 3) is to filter alerts so only significant incidents are escalated.

Periodic system downtime (D): SOC systems (SIEM/SOAR) are considered "Mission Critical" and must operate on a 24/7/365 basis. Maintenance should be performed using High Availability (HA) configurations or during "low-flow" windows without causing a complete stop in monitoring, as attackers often leverage downtime to strike.

Question: 25

You are trying to create a playbook that creates a manual task showing a list of public IPv6 addresses. You were successful in extracting all IP addresses from a previous action into a variable called ip_list, which contains both private and public IPv4 and IPv6 addresses. You must now filter the results to display only public IPv6 addresses. Which two Jinja expressions can accomplish this task? (Choose two answers)

A. {{ vars.ip_list | ipv6addr('public') }}

B. {{ vars.ip_list | ipaddr('public') | ipv6 }}

C. {{ vars.ip_list | ipaddr('!private') | ipv6 }}

D. {{ vars.ip_list | ipv6 | ipaddr('public') }}

Answer: B, D

Explanation:

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

In FortiSOAR 7.6, the playbook engine utilizes the powerful ipaddr family of Jinja filters (derived from the Ansible netaddr library) to manipulate network data. To isolate public IPv6 addresses from a mixed list, the order of operations in the filter chain ensures the correct data is extracted:

Double Filtering Sequence (B): In the expression {{ vars.ip_list | ipaddr('public') | ipv6 }}, the first filter ipaddr('public') processes the entire list and retains only public addresses, including both IPv4 and IPv6 versions. The second filter in the pipe, | ipv6, then takes that subset of public addresses and filters them again to keep only those that conform to the IPv6 standard. The final result is a list containing only public IPv6 addresses.

Version-First Filtering (D): In the expression {{ vars.ip_list | ipv6 | ipaddr('public') }}, the logic is reversed but equally effective. The first filter | ipv6 immediately strips all IPv4 and non-IP strings from the list, leaving only IPv6 addresses (both private and public). The subsequent filter | ipaddr('public') then evaluates these IPv6 addresses and discards any that fall within the private/unique-local ranges (like ULA or link-local), resulting in the same set of public IPv6 addresses.

Why other options are incorrect:

A (ipv6addr 'public'): While ipv6addr is a valid filter in many Ansible environments, FortiSOAR's

standard documentation for manual task creation and data manipulation primarily emphasizes the use of the generic ipaddr filter with specific flags or chained version filters (like | ipv6) to ensure cross-compatibility with the underlying Python libraries used by the SOAR engine.

C (!private syntax): The ipaddr filter utilizes specific keywords for classification. While "not private" is the logical requirement, the filter expects positive assertions such as 'public', 'private', or 'multicast'. The !private syntax is not a supported or documented operator for this filter within the Fortinet SOC ecosystem.

Question: 26

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.

Reference:

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: 27

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.

Reference: Fortinet Documentation on DNS Filtering FortiOS DNS Filter

IPS Logs:

Intrusion Prevention System (IPS) logs detect and block exploit attempts and malicious activities. These logs are critical for identifying compromised hosts based on detected intrusion attempts or behaviors matching known attack patterns.

Reference: Fortinet IPS Overview FortiOS IPS

Web Filter Logs:

Web filtering logs monitor and control access to web content. These logs can reveal access to malicious websites, download of malware, or other web-based threats, indicating a compromised host.

Reference: Fortinet Web Filtering FortiOS Web Filter

Why Not Other Log Types:

Email Filter Logs:

While important for detecting phishing and email-based threats, they are not as directly indicative of compromised hosts as DNS, IPS, and Web filter logs.

Application Filter Logs:

These logs control application usage but are less likely to directly indicate compromised hosts compared to the selected logs.

Detailed Process:

Step 1: FortiAnalyzer collects logs from FortiGate and other Fortinet devices.

Step 2: DNS filter logs are analyzed to detect unusual or malicious domain queries.

Step 3: IPS logs are reviewed for any intrusion attempts or suspicious activities.

Step 4: Web filter logs are checked for access to malicious websites or downloads.

Step 5: FortiAnalyzer correlates the information from these logs to identify potential IoCs and compromised hosts.

Reference:

Fortinet Documentation: FortiOS DNS Filter, IPS, and Web Filter administration guides.

FortiAnalyzer Administration Guide: Details on log analysis and IoC identification.

By using DNS filter logs, IPS logs, and Web filter logs, FortiAnalyzer effectively identifies possible compromised hosts, providing critical insights for threat detection and response.

Question: 28

Which role does a threat hunter play within a SOC?

A. investigate and respond to a reported security incident

B. Collect evidence and determine the impact of a suspected attack

C. Search for hidden threats inside a network which may have eluded detection

D. Monitor network logs to identify anomalous behavior

Answer: C

Explanation:

Role of a Threat Hunter:

A threat hunter proactively searches for cyber threats that have evaded traditional security defenses. This role is crucial in

identifying sophisticated and stealthy adversaries that bypass automated detection systems.

Key Responsibilities:

Proactive Threat Identification:

Threat hunters use advanced tools and techniques to identify hidden threats within the network.

This includes analyzing anomalies, investigating unusual behaviors, and utilizing threat intelligence.

Reference: SANS Institute, "Threat Hunting: Open Season on the Adversary" SANS Threat Hunting

Understanding the Threat Landscape:

They need a deep understanding of the threat landscape, including common and emerging tactics, techniques, and procedures (TTPs) used by threat actors.

Reference: MITRE ATT&CK Framework MITRE ATT&CK

Advanced Analytical Skills:

Utilizing advanced analytical skills and tools, threat hunters analyze logs, network traffic, and endpoint data to uncover signs of compromise.

Reference: Cybersecurity and Infrastructure Security Agency (CISA) Threat Hunting Guide CISA Threat Hunting

Distinguishing from Other Roles:

Investigate and Respond to Incidents (A):

This is typically the role of an Incident Responder who reacts to reported incidents, collects evidence, and determines the impact.

Reference: NIST Special Publication 800-61, "Computer Security Incident Handling Guide" NIST Incident Handling

Collect Evidence and Determine Impact (B):

This is often the role of a Digital Forensics Analyst who focuses on evidence collection and impact assessment post-incident.

Monitor Network Logs (D):

This falls under the responsibilities of a SOC Analyst who monitors logs and alerts for anomalous behavior and initial detection.

Conclusion:

Threat hunters are essential in a SOC for uncovering sophisticated threats that automated systems may miss. Their proactive approach is key to enhancing the organization's security posture.

Reference:

SANS Institute, "Threat Hunting: Open Season on the Adversary"

MITRE ATT&CK Framework

CISA Threat Hunting Guide

NIST Special Publication 800-61, "Computer Security Incident Handling Guide"

By searching for hidden threats that elude detection, threat hunters play a crucial role in maintaining the security and integrity of an organization's network.

Question: 29

According to the National Institute of Standards and Technology (NIST) cybersecurity framework, incident handling activities can be divided into phases.

In which incident handling phase do you quarantine a compromised host in order to prevent an adversary from using it as a stepping stone to the next phase of an attack?

A. Containment

B. Analysis

C. Eradication

D. Recovery

Answer: A

Explanation:

NIST Cybersecurity Framework Overview:

The NIST Cybersecurity Framework provides a structured approach for managing and mitigating cybersecurity risks. Incident handling is divided into several phases to systematically address and resolve incidents.

Incident Handling Phases:

Preparation: Establishing and maintaining an incident response capability.

Detection and Analysis: Identifying and investigating suspicious activities to confirm an incident.

Containment, Eradication, and Recovery:

Containment: Limiting the impact of the incident.

Eradication: Removing the root cause of the incident.

Recovery: Restoring systems to normal operation.

Containment Phase:

The primary goal of the containment phase is to prevent the incident from spreading and causing further damage.

Quarantining a Compromised Host:

Quarantining involves isolating the compromised host from the rest of the network to prevent adversaries from moving laterally and causing more harm.

Techniques include network segmentation, disabling network interfaces, and applying access controls.

Reference: NIST Special Publication 800-61, "Computer Security Incident Handling Guide" NIST Incident Handling

Detailed Process:

Step 1: Detect the compromised host through monitoring and analysis.

Step 2: Assess the impact and scope of the compromise.

Step 3: Quarantine the compromised host to prevent further spread. This can involve disconnecting the host from the network or applying strict network segmentation.

Step 4: Document the containment actions and proceed to the eradication phase to remove the threat completely.

Step 5: After eradication, initiate the recovery phase to restore normal operations and ensure that

the host is securely reintegrated into the network.

Importance of Containment:

Containment is critical in mitigating the immediate impact of an incident and preventing further damage. It buys time for responders to investigate and remediate the threat effectively.

Reference: SANS Institute, "Incident Handler's Handbook" SANS Incident Handling

Reference:

NIST Special Publication 800-61, "Computer Security Incident Handling Guide"

SANS Institute, "Incident Handler's Handbook"

By quarantining a compromised host during the containment phase, organizations can effectively limit the spread of the incident and protect their network from further compromise.

Question: 30

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.

Reference: Fortinet FortiCASB Documentation FortiCASB

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.

Reference: Fortinet FortiMail Documentation FortiMail

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.

Reference: Fortinet FortiAnalyzer Administration Guide FortiAnalyzer Local

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.

Reference: Fortinet FortiOS Administration Guide FortiOS

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.

Reference:

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: 31

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.

Reference:

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.

Question: 32

Refer to the exhibits.

You configured a spearphishing event handler and the associated rule. However. FortiAnalyzer did not generate an event.

When you check the FortiAnalyzer log viewer, you confirm that FortiSandbox forwarded the appropriate logs, as shown in the raw log exhibit.

What configuration must you change on FortiAnalyzer in order for FortiAnalyzer to generate an event?

A. In the Log Type field, change the selection to AntiVirus Log(malware).

B. Configure a FortiSandbox data selector and add it tothe event handler.

C. In the Log Filter by Text field, type the value: .5 ub t ype ma Iwa re..

D. Change trigger condition by selecting. Within a group, the log field Malware Kame (mname> has 2 or more unique values.

Answer: B

Explanation:

Understanding the Event Handler Configuration:

The event handler is set up to detect specific security incidents, such as spearphishing, based on logs forwarded from other Fortinet products like FortiSandbox.

An event handler includes rules that define the conditions under which an event should be triggered.

Analyzing the Current Configuration:

The current event handler is named "Spearphishing handler" with a rule titled "Spearphishing Rule 1".

The log viewer shows that logs are being forwarded by FortiSandbox but no events are generated by FortiAnalyzer.

Key Components of Event Handling:

Log Type: Determines which type of logs will trigger the event handler.

Data Selector: Specifies the criteria that logs must meet to trigger an event.

Automation Stitch: Optional actions that can be triggered when an event occurs.

Notifications: Defines how alerts are communicated when an event is detected.

Issue Identification:

Since FortiSandbox logs are correctly forwarded but no event is generated, the issue likely lies in the data selector configuration or log type matching.

The data selector must be configured to include logs forwarded by FortiSandbox.

Solution:

B . Configure a FortiSandbox data selector and add it to the event handler:

By configuring a data selector specifically for FortiSandbox logs and adding it to the event handler, FortiAnalyzer can accurately identify and trigger events based on the forwarded logs.

Steps to Implement the Solution:

Step 1: Go to the Event Handler settings in FortiAnalyzer.

Step 2: Add a new data selector that includes criteria matching the logs forwarded by FortiSandbox (e.g., log subtype, malware detection details).

Step 3: Link this data selector to the existing spearphishing event handler.

Step 4: Save the configuration and test to ensure events are now being generated.

Conclusion:

The correct configuration of a FortiSandbox data selector within the event handler ensures that FortiAnalyzer can

generate events based on relevant logs.

Reference:

Fortinet Documentation on Event Handlers and Data Selectors FortiAnalyzer Event Handlers

Fortinet Knowledge Base for Configuring Data Selectors FortiAnalyzer Data Selectors

By configuring a FortiSandbox data selector and adding it to the event handler, FortiAnalyzer will be able to accurately generate events based on the appropriate logs.

Question: 33

While monitoring your network, you discover that one FortiGate device is sending significantly more logs to FortiAnalyzer than all of the other FortiGate devices in the topology.

Additionally, the ADOM that the FortiGate devices are registered to consistently exceeds its quota.

What are two possible solutions? (Choose two.)

A. Increase the storage space quota for the first FortiGate device.

B. Create a separate ADOM for the first FortiGate device and configure a different set of storage policies.

C. Reconfigure the first FortiGate device to reduce the number of logs it forwards to FortiAnalyzer.

D. Configure data selectors to filter the data sent by the first FortiGate device.

Answer: BC

Explanation:

Understanding the Problem:

One FortiGate device is generating a significantly higher volume of logs compared to other devices, causing the ADOM to exceed its storage quota.

This can lead to performance issues and difficulties in managing logs effectively within FortiAnalyzer.

Possible Solutions:

The goal is to manage the volume of logs and ensure that the ADOM does not exceed its quota, while still maintaining effective log analysis and monitoring.

Solution A: Increase the Storage Space Quota for the First FortiGate Device:

While increasing the storage space quota might provide a temporary relief, it does not address the root cause of the issue, which is the excessive log volume.

This solution might not be sustainable in the long term as log volume could continue to grow.

Not selected as it does not provide a long-term, efficient solution.

Solution B: Create a Separate ADOM for the First FortiGate Device and Configure a Different Set of Storage Policies:

Creating a separate ADOM allows for tailored storage policies and management specifically for the high-log-volume device.

This can help in distributing the storage load and applying more stringent or customized retention and storage policies.

Selected as it effectively manages the storage and organization of logs.

Solution C: Reconfigure the First FortiGate Device to Reduce the Number of Logs it Forwards to FortiAnalyzer:

By adjusting the logging settings on the FortiGate device, you can reduce the volume of logs forwarded to FortiAnalyzer.

This can include disabling unnecessary logging, reducing the logging level, or filtering out less critical logs.

Selected as it directly addresses the issue of excessive log volume.

Solution D: Configure Data Selectors to Filter the Data Sent by the First FortiGate Device:

Data selectors can be used to filter the logs sent to FortiAnalyzer, ensuring only relevant logs are forwarded.

This can help in reducing the volume of logs but might require detailed configuration and regular updates to ensure critical logs are not missed.

Not selected as it might not be as effective as reconfiguring logging settings directly on the FortiGate device.

Implementation Steps:

For Solution B:

Step 1: Access FortiAnalyzer and navigate to the ADOM management section.

Step 2: Create a new ADOM for the high-log-volume FortiGate device.

Step 3: Register the FortiGate device to this new ADOM.

Step 4: Configure specific storage policies for the new ADOM to manage log retention and storage.

For Solution C:

Step 1: Access the FortiGate device's configuration interface.

Step 2: Navigate to the logging settings.

Step 3: Adjust the logging level and disable unnecessary logs.

Step 4: Save the configuration and monitor the log volume sent to FortiAnalyzer.

Reference:

Fortinet Documentation on FortiAnalyzer ADOMs and log management FortiAnalyzer Administration Guide

Fortinet Knowledge Base on configuring log settings on FortiGate FortiGate Logging Guide

By creating a separate ADOM for the high-log-volume FortiGate device and reconfiguring its logging settings, you can effectively manage the log volume and ensure the ADOM does not exceed its quota.

Question: 34

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, 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.

Reference:

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: 35

Your company is doing a security audit To pass the audit, you must take an inventory of all software and applications running on all Windows devices

Which FortiAnalyzer connector must you use?

A. FortiClient EMS

B. ServiceNow

C. FortiCASB

D. Local Host

Answer: A

Explanation:

Requirement Analysis:

The objective is to inventory all software and applications running on all Windows devices within the organization.

This inventory must be comprehensive and accurate to pass the security audit.

Key Components:

FortiClient EMS (Endpoint Management Server):

FortiClient EMS provides centralized management of endpoint security, including software and application inventory on Windows devices.

It allows administrators to monitor, manage, and report on all endpoints protected by FortiClient.

Connector Options:

FortiClient EMS:

Best suited for managing and reporting on endpoint software and applications.

Provides detailed inventory reports for all managed endpoints.

Selected as it directly addresses the requirement of taking inventory of software and applications on Windows devices.

ServiceNow:

Primarily a service management platform.

While it can be used for asset management, it is not specifically tailored for endpoint software inventory.

Not selected as it does not provide direct endpoint inventory management.

FortiCASB:

Focuses on cloud access security and monitoring SaaS applications.

Not applicable for managing or inventorying endpoint software.

Not selected as it is not related to endpoint software inventory.

Local Host:

Refers to handling events and logs within FortiAnalyzer itself.

Not specific enough for detailed endpoint software inventory.

Not selected as it does not provide the required endpoint inventory capabilities.

Implementation Steps:

Step 1: Ensure all Windows devices are managed by FortiClient and connected to FortiClient EMS.

Step 2: Use FortiClient EMS to collect and report on the software and applications installed on these devices.

Step 3: Generate inventory reports from FortiClient EMS to meet the audit requirements.

Reference:

Fortinet Documentation on FortiClient EMS FortiClient EMS Administration Guide

By using the FortiClient EMS connector, you can effectively inventory all software and applications on Windows devices, ensuring compliance with the security audit requirements.

Question: 36

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.

Reference:

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: 37

Refer to the exhibit.

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.

Reference:

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.

Question: 38

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

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: BD

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.

Reference: Fortinet Documentation on Log Forwarding FortiAnalyzer Log Forwarding

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.

Reference: Fortinet Documentation on Fabric Authorization FortiAnalyzer Fabric Authorization

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.

Reference:

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: 39

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?

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.

Reference:

Fortinet Documentation on FortiAnalyzer Data Policies and Disk Management.

Best Practices for FortiAnalyzer Log Management and Disk Utilization.

Question: 40

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.

Reference:

MITRE ATT&CK Framework documentation.

FortiAnalyzer Event Handling and MITRE ATT&CK Integration guides.

Question: 41

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.

Reference:

Fortinet Documentation on Playbook Creation and Incident Management.

Best Practices for Automating Incident Response in SOC Operations.

Question: 42

Refer to the exhibits.

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 a ValueError: 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 the execute method.

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.

Reference:

Fortinet Documentation on Playbook and Task Configuration.

Python error handling documentation for understanding ValueError.

Question: 43

Which two statements about the FortiAnalyzer Fabric topology are true? (Choose two.)

A. Downstream collectors can forward logs to Fabric members.

B. Logging devices must be registered to the supervisor.

C. The supervisor uses an API to store logs, incidents, and events locally.

D. Fabric members must be in analyzer mode.

Answer: BD

Explanation:

Understanding FortiAnalyzer Fabric Topology:

The FortiAnalyzer Fabric topology is designed to centralize logging and analysis across multiple devices in a network.

It involves a hierarchy where the supervisor node manages and coordinates with other Fabric members.

Analyzing the Options:

Option A: Downstream collectors forwarding logs to Fabric members is not a typical configuration. Instead, logs are usually centralized to the supervisor.

Option B: For effective management and log centralization, logging devices must be registered to the supervisor. This ensures proper log collection and coordination.

Option C: The supervisor does not primarily use an API to store logs, incidents, and events locally. Logs are stored directly in the FortiAnalyzer database.

Option D: For the Fabric topology to function correctly, all Fabric members need to be in analyzer mode. This mode allows them to collect, analyze, and forward logs appropriately within the topology.

Conclusion:

The correct statements regarding the FortiAnalyzer Fabric topology are that logging devices must be registered to the supervisor and that Fabric members must be in analyzer mode.

Reference:

Fortinet Documentation on FortiAnalyzer Fabric Topology.

Best Practices for Configuring FortiAnalyzer in a Fabric Environment.

Question: 44

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.

Reference:

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

Incident analysis and mapping to MITRE ATT&CK tactics.

Question: 45

Refer to Exhibit:

A SOC analyst is designing a playbook to filter for a high severity event and attach the event information to an incident.

Which local connector action must the analyst use in this scenario?

A. Get Events

B. Update Incident

C. Update Asset and Identity

D. Attach Data to Incident

Answer: D

Explanation:

Understanding the Playbook Requirements:

The SOC analyst needs to design a playbook that filters for high severity events.

The playbook must also attach the event information to an existing incident.

Analyzing the Provided Exhibit:

The exhibit shows the available actions for a local connector within the playbook.

Actions listed include:

Update Asset and Identity

Get Events

Get Endpoint Vulnerabilities

Create Incident

Update Incident

Attach Data to Incident

Run Report

Get EPEU from Incident

Evaluating the Options:

Get Events: This action retrieves events but does not attach them to an incident.

Update Incident: This action updates an existing incident but is not specifically for attaching event data.

Update Asset and Identity: This action updates asset and identity information, not relevant for attaching event data to an incident.

Attach Data to Incident: This action is explicitly designed to attach additional data, such as event information, to an existing incident.

Conclusion:

The correct action to use in the playbook for filtering high severity events and attaching the event information to an incident is Attach Data to Incident.

Reference:

Fortinet Documentation on Playbook Actions and Connectors.

Best Practices for Incident Management and Playbook Design in SOC Operations.

Question: 46

Refer to the exhibit.

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

A. The playbook is using a local connector.

B. The playbook is using a FortiMail connector.

C. The playbook is using an on-demand trigger.

D. The playbook is using a FortiClient EMS connector.

Answer: AD

Explanation:

Understanding the Playbook Configuration:

The playbook named "Update Asset and Identity Database" is designed to update the FortiAnalyzer Asset and Identity database with endpoint and user information.

The exhibit shows the playbook with three main components: ON_SCHEDULE STARTER, GET_ENDPOINTS, and UPDATE_ASSET_AND_IDENTITY.

Analyzing the Components:

ON_SCHEDULE STARTER: This component indicates that the playbook is triggered on a schedule, not on-demand.

GET_ENDPOINTS: This action retrieves information about endpoints, suggesting it interacts with an endpoint management system.

UPDATE_ASSET_AND_IDENTITY: This action updates the FortiAnalyzer Asset and Identity database with the retrieved information.

Evaluating the Options:

Option A: The actions shown in the playbook are standard local actions that can be executed by the FortiAnalyzer, indicating the use of a local connector.

Option B: There is no indication that the playbook uses a FortiMail connector, as the tasks involve endpoint and identity management, not email.

Option C: The playbook is using an "ON_SCHEDULE" trigger, which contradicts the description of an on-demand trigger.

Option D: The action "GET_ENDPOINTS" suggests integration with an endpoint management system, likely FortiClient EMS, which manages endpoints and retrieves information from them.

Conclusion:

The playbook is configured to use a local connector for its actions.

It interacts with FortiClient EMS to get endpoint information and update the FortiAnalyzer Asset and Identity database.

Reference:

Fortinet Documentation on Playbook Actions and Connectors.

FortiAnalyzer and FortiClient EMS Integration Guides.

Question: 47

Refer to the exhibits.

The Malicious File Detect playbook is configured to create an incident when an event handler generates a malicious file detection event.

Why did the Malicious File Detect playbook execution fail?

A. The Create Incident task was expecting a name or number as input, but received an incorrect data format

B. The Get Events task did not retrieve any event data.

C. The Attach_Data_To_Incident incident task wasexpecting an integer, but received an incorrect data format.

D. The Attach Data To Incident task failed, which stopped the playbook execution.

Answer: A

Explanation:

Understanding the Playbook Configuration:

The "Malicious File Detect" playbook is designed to create an incident when a malicious file detection event is triggered.

The playbook includes tasks such 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.

Reference:

Fortinet Documentation on Playbook and Task Configuration.

Error handling and debugging practices in playbook execution.

Question: 48

Refer to the exhibit.

Assume that all devices in the FortiAnalyzer Fabric are shown in the image.

Which two statements about the FortiAnalyzer Fabric deployment are true? (Choose two.)

A. FortiGate-B1 and FortiGate-B2 are in a Security Fabric.

B. There is no collector in the topology.

C. All FortiGate devices are directly registered to the supervisor.

D. FAZ-SiteA has two ADOMs enabled.

Answer: AD

Explanation:

Understanding the FortiAnalyzer Fabric:

The FortiAnalyzer Fabric provides centralized log collection, analysis, and reporting for connected FortiGate devices.

Devices in a FortiAnalyzer Fabric can be organized into different Administrative Domains (ADOMs) to separate logs and management.

Analyzing the Exhibit:

FAZ-SiteA and FAZ-SiteB are FortiAnalyzer devices in the fabric.

FortiGate-B1 and FortiGate-B2 are shown under the Site-B-Fabric, indicating they are part of the same Security Fabric.

FAZ-SiteA has multiple entries under it: SiteA and MSSP-Local, suggesting multiple ADOMs are enabled.

Evaluating the Options:

Option A: FortiGate-B1 and FortiGate-B2 are under Site-B-Fabric, indicating they are indeed part of the same Security Fabric.

Option B: The presence of FAZ-SiteA and FAZ-SiteB as FortiAnalyzers does not preclude the existence of collectors. However, there is no explicit mention of a separate collector role in the exhibit.

Option C: Not all FortiGate devices are directly registered to the supervisor. The exhibit shows hierarchical organization under different sites and ADOMs.

Option D: The multiple entries under FAZ-SiteA (SiteA and MSSP-Local) indicate that FAZ-SiteA has two ADOMs enabled.

Conclusion:

FortiGate-B1 and FortiGate-B2 are in a Security Fabric.

FAZ-SiteA has two ADOMs enabled.

Reference:

Fortinet Documentation on FortiAnalyzer Fabric Topology and ADOM Configuration.

Best Practices for Security Fabric Deployment with FortiAnalyzer.

Question: 49

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.

Reference:

Fortinet Documentation on Playbook Configuration and Variable Usage.

General SOC Automation and Orchestration Practices.

Question: 50

Refer to the exhibits.

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 action ADD_SENDER_TO_BLOCKLIST.

Analyzing the Playbook Execution:

The configuration and actions provided show that the playbook is straightforward, starting with an ON_DEMAND STARTER and proceeding to the ADD_SENDER_TO_BLOCKLIST action.

The action description indicates it is intended to block senders based on email addresses or domains.

Evaluating the Options:

Option A: Using GET_EMAIL_STATISTICS is 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).

Reference:

Fortinet Documentation on FortiMail Connector Actions.

Best Practices for Configuring FortiMail Block Lists.

Question: 51

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

A. Using a connector action

B. Manually, on the Event Monitor page

C. By running a playbook

D. Using a custom event handler

Answer: BD

Explanation:

Understanding Incident Creation in FortiAnalyzer:

FortiAnalyzer allows for the creation of incidents to track and manage security events.

Incidents can be created both automatically and manually based on detected events and predefined rules.

Analyzing the Methods:

Option A: Using a connector action typically involves integrating with other systems or services and is not a direct method for creating incidents on FortiAnalyzer.

Option B: Incidents can be created manually on the Event Monitor page by selecting relevant events and creating incidents from those events.

Option C: While playbooks can automate responses and actions, the direct creation of incidents is usually managed through event handlers or manual processes.

Option D: Custom event handlers can be configured to trigger incident creation based on specific events or conditions, automating the process within FortiAnalyzer.

Conclusion:

The two valid methods for creating an incident on FortiAnalyzer are manually on the Event Monitor page and using a custom event handler.

Reference:

Fortinet Documentation on Incident Management in FortiAnalyzer.

FortiAnalyzer Event Handling and Customization Guides.

Question: 52

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.

Reference:

MITRE ATT&CK Framework Documentation.

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

Question: 53

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 EMEASOC team has access to historical logs only.

D. The APAC SOC team hasaccess 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-Supervisor is located at AMER HQ and acts as the Fabric root.

FAZ2-Analyzer is a Fabric member located in EMEA.

FAZ3-Collector and FAZ4-Collector are 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.

Reference:

Fortinet Documentation on FortiAnalyzer Fabric Deployment.

Best Practices for FortiAnalyzer and Automation Playbooks.

Question: 54

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.

Reference:

Fortinet Documentation on FortiAnalyzer Features and SIEM Capabilities.

Security Best Practices and Use Cases for Threat Hunting.

Question: 55

Refer to the exhibits.

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. In the Log filter by Text field, type type==spam.

C. Disable the rule to use the filter in the data selector to create the event.

D. 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 nonspam 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: Typing type==spam in 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.

Reference:

Fortinet Documentation on Event Handlers and Log Types.

Best Practices for Configuring FortiMail Anti-Spam Settings.

Question: 56

When does FortiAnalyzer generate an event?

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.

Reference:

Fortinet Documentation on Event Handlers and Event Generation in FortiAnalyzer.

Best Practices for Configuring Event Handlers in FortiAnalyzer.

Question: 57

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 an Event handler in FortiAnalyzer.

Reference:

Fortinet Documentation on Event Handlers and Automation Stitches in FortiAnalyzer.

Best Practices for Configuring Automated Responses in FortiAnalyzer.