Fortinet

NSE7_SOC_AR-7.6

Fortinet NSE 7 - Security Operations 7.6 Architect

For More Information – Visit link below:

https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 6.0

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)

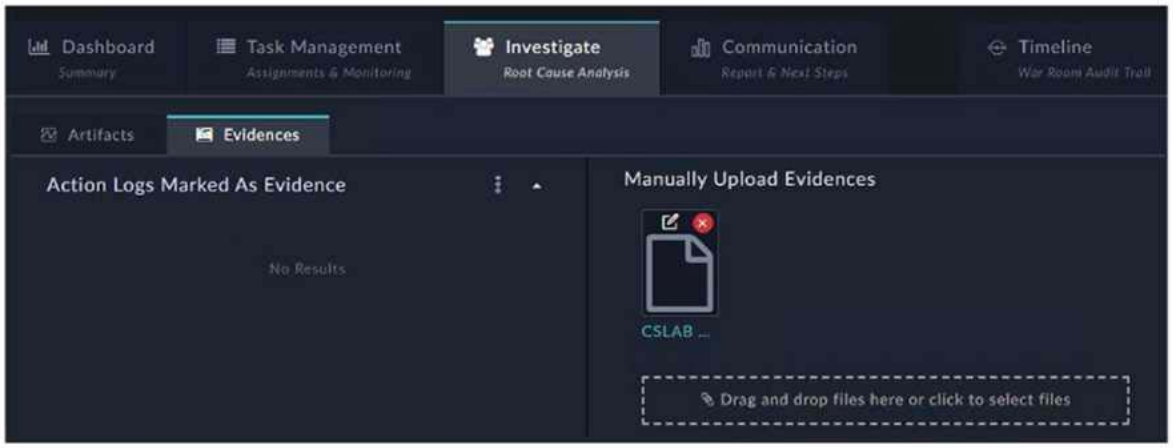
A. Enrich records with threat intelligence.
B. Automate workflows.
C. Generate a hypothesis.
D. Perform packet analysis.
E. Tune correlation rules.

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

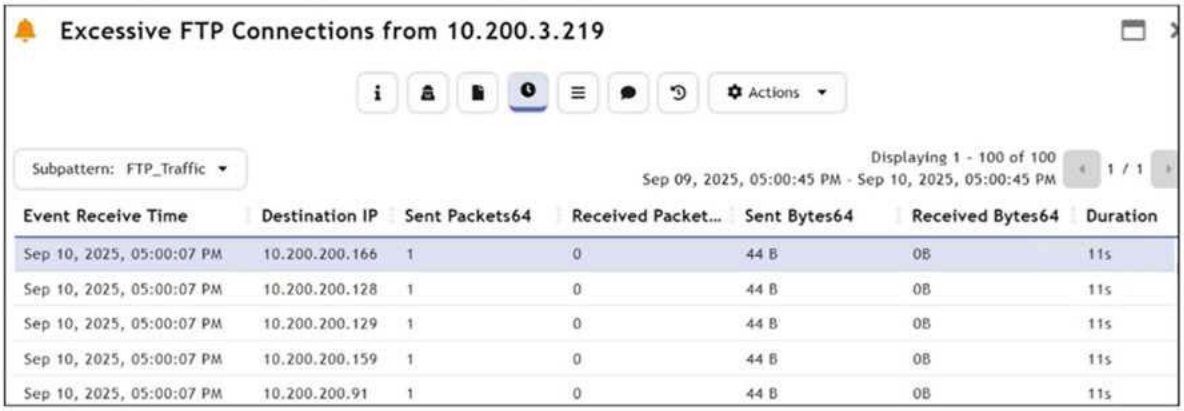
Explanation:
Comprehensive and Detailed Explanation From FortiSOAR 7.6., FortiSIEM 7.3 Exact Extract study guide:
In FortiSOAR 7.6, the War Room is a collaborative space designed for high-priority incident investigation. The Evidences tab within the Investigate view (as shown in the exhibit) is specifically 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



Raw Logs

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 offline, 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).

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/