KillTest

質量更高　服務更好

學習資料

http://www.killtest.net

一年免費更新服務

Exam : **NSE6_FSM_AN-7.4**

Title : Fortinet NSE 6 - FortiSIEM 7.4 Analyst

Version : DEMO

1.A SOC analyst is reviewing a failed VPN login event in FortiSIEM. The analyst needs to quickly search for other events with the same source IP, user, and login result during the last 60 minutes.
Which action best supports this investigation?
A. Add the event to a static report
B. Pivot from the selected event fields
C. Change the incident clear condition
D. Rebuild the related device group
Answer: B
Explanation:
Pivoting from selected event fields is the most efficient way to create a focused search using values already present in the event. Reports, clear conditions, and device groups do not provide the fastest event-to-search investigation path.

2.An analyst is asked to identify which internal servers received the highest number of failed SSH logins during the previous day.
Which search design should the analyst use?
A. Filter SSH failures and sort by event time
B. Search all SSH logs and display raw messages
C. Filter Linux events and sort by source IP
D. Group failed SSH events by target host
Answer: D
Explanation:
The analyst must compare failure volume by target host, so grouping failed SSH events by target host and counting events is the correct approach. Sorting or displaying raw logs does not produce a ranked host-level view.

3.During a lateral movement investigation, an analyst wants events where destination port equals 445 and the destination belongs to the server subnet.
Which FortiSIEM search approach is most appropriate?
A. Apply field filters for port and subnet
B. Search only by the firewall hostname
C. Group all events by reporting device
D. Export firewall logs before filtering
Answer: A
Explanation:
Field-based filters on destination port and destination IP range provide a precise dataset for the investigation. Device-only searches and exports are broader and less efficient.

4.A FortiSIEM search returns thousands of matching events. The analyst needs a concise table showing source IP, destination IP, user, event type, and event count.
What should the analyst adjust?
A. Incident notification targets
B. Device discovery schedule
C. Display fields and grouping

D. System parser priority
Answer: C
Explanation:
Display fields and grouping control how search results are presented and summarized. Notification targets, discovery schedules, and parser priority do not create the required analytic view.

5.A malware search includes both production systems and lab systems. Production status is maintained as an asset attribute in FortiSIEM.
How should the analyst limit the results?
A. Filter by incident owner
B. Use CMDB asset context
C. Match the report category
D. Change the collector group
Answer: B
Explanation:
CMDB asset context can be used to filter or enrich searches based on asset attributes such as environment, owner, role, or business unit. Incident owner, report category, and collector group are not the right criteria for asset classification.