PassQueen
a.k.a dumpsqueen.com

Fortinet NSE 5 - FortiSIEM 6.3

Fortinet NSE5_FSM-6.3

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, FortiSIEM Architecture	3
Topic 2, Discovery	2
Topic 3, Monitoring	2
Topic 4, Analytics	5
Topic 5, Rules	8
Topic 6, CMDB	1
Topic 7, Administration	2
Total	23

QUESTION NO: 1

A performance rule must identify a sustained disk-utilization problem on individual hosts. A single utilization sample above the threshold should not create an incident; the rule should require multiple matching samples from the same host.

Which configuration is required?

A. Group By Host with a count aggregation

B. Group By Event Type with a count aggregation

C. No Group By definition with an average aggregation

D. Group By Severity with a count aggregation

ANSWER: A

Explanation:

Grouping by host with a count aggregation is correct because Group By Host prevents samples from separate systems from contributing to the same threshold, while the count aggregation requires multiple matching events. A filter alone identifies the high-utilization samples but does not enforce repeated occurrence for each individual host.

QUESTION NO: 2

A rule is intended to identify a large number of failed logins from one source IP address. The rule filter correctly selects failed login events, but the administrator finds that failures from all source IP addresses contribute to one incident threshold.

Which change corrects the rule behavior?

A. Add source IP address to the subpattern Group By definition.

B. Add source IP address only as an incident display attribute.

C. Change the Event Type value in the rule filter.

D. Apply a separate notification policy for each source IP address.

ANSWER: A

Explanation:

Adding source IP address to the subpattern Group By definition is correct. Group By partitions matching events into independent evaluation groups, so each source address has its own aggregation count and threshold evaluation. Adding source IP address only as a displayed incident attribute does not affect rule evaluation. Changing the Event Type can change which events match but does not separate the matched events by source. A notification policy operates after an incident is generated.