DUMPSARENA

FCPFortiSIEM 7.2 Analyst

Fortinet FCP_FSM_AN-7.2

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, CMDB	2
Topic 2, Event management	3
Topic 3, Analytics	18
Total	23

QUESTION NO: 1

An analyst needs to determine which destination received the greatest volume of outbound traffic from a set of monitored hosts. The relevant events contain a Sent Bytes attribute. Which Analytics configuration provides the required result?

A. Group the events by Destination IP and calculate the sum of Sent Bytes.

B. Group the events by Destination IP and calculate the count of events.

C. Group the events by Destination IP and calculate the average of Sent Bytes.

D. Group the events by Source IP and calculate the sum of Sent Bytes.

ANSWER: A

Explanation:

Group the events by Destination IP and calculate the sum of Sent Bytes is correct. Grouping establishes one result per destination, and summing Sent Bytes measures the total outbound volume associated with each destination. The analyst can then sort the aggregated results to identify the largest value.

Counting events measures the number of records, not the amount of transferred data. Averaging Sent Bytes identifies typical event size rather than total volume. Grouping by Source IP would summarize the monitored hosts instead of the receiving destinations.

QUESTION NO: 2

An analyst is investigating repeated authentication failures. The analyst must identify source IP addresses that generated at least 25 failures during the selected time range. Which Analytics search configuration is most appropriate?

A. Filter for the authentication-failure events, group the results by Source IP, and aggregate the event count.

B. Filter for the authentication-failure events and search separately for each suspected Source IP.

C. Group all events by Reporting Device and review the resulting event totals.

D. Filter for the authentication-failure events and sort the individual event records by Source IP.

ANSWER: A

Explanation:

Filter for the authentication-failure events, group the results by Source IP, and aggregate the event count is correct. The event filter restricts the data set to the relevant failures, while grouping by Source IP creates one result set per originating address. Applying an event-count aggregation allows the analyst to identify the groups that meet the threshold.

Filtering only by Source IP requires an address to be known in advance. Grouping without an event-count aggregation does not establish whether a source met the required threshold. Grouping by Reporting Device identifies the system that sent the logs, rather than the clients that generated the authentication attempts.