1001_M6_Basic_Transforming_Commands_Quiz

1. Which option shows the correct placement of the pipe (`|`) in this search string: "index=security sourcetype=access_* status=200 stats count by price"?
   A. index=security sourcetype=access_* status=200 stats | count by price
   B. index=security sourcetype=access_* status=200 | stats count by price
   C. index=security sourcetype=access_* status=200 | stats count | by price
   D. index=security sourcetype=access_* | status=200 | stats count by price

2. What constraints can be applied when using the top command?
   A. limit
   B. percshow
   C. addtotals
   D. countcolumns

3. Which of the following constraints are commonly used with the top command?
   A. limits, countfield
   B. count, showpercent
   C. limit, count
   D. showperc, countfield

4. What is the proper syntax to count events containing the field vendor_action?
   A. count stats vendor_action
   B. count stats(vendor_action)
   C. stats count(vendor_action)
   D. stats vendor_action(count)

5. What is the function of the rare command?
   A. Returns the least common field values of a given field in the results.
   B. Returns the most common field values of a given field in the results.
   C. Returns the top 10 field values of a given field in the results.
   D. Returns the lowest 10 field values of a given field in the results.

6. What does the values function within the stats command return?
   A. Lists positive values of a given field.
   B. List unique values of a given field.
   C. Returns a count of unique values of a given field.
   D. Returns the count of events that match the search.

7. Which stats function counts the number of unique values for a field in the result set?
   A. dc(field)
   B. count(field)
   C. count-by(field)
   D. distinct-count(field)

8. Why would you include a by clause when using the stats command?
   A. To group the results by one or more fields
   B. To calculate numerical statistics of each field
   C. To specify the number of delimited values in a list
   D. To partition the input data based on the split-by fields

9. In a statistics table, how can you drill down to view the underlying events?
   A. Creating a pivot table.
   B. Clicking on the visualization tab.
   C. Viewing your results in a dashboard.
   D. Clicking on any field value in the table.

10. Which of the following are valid functions of the stats command?
   A. count, sum, add
   B. count, sum, less
   C. sum, avg, values
   D. sum, values, table

11. What is the purpose of the stats command?
   A. Correlating multiple fields automatically
   B. Change field values into numerical values
   C. Calculates statistics on data that matches the search criteria.
   D. Analyzes numerical fields for their ability to predict another discrete field.

12. Which statement about the top command is correct?
   A. It returns the top 10 results.
   B. It displays the output in table format.
   C. It returns the count and percent columns per row.
   D. All of the above.

13. Which command automatically generates percent and count columns in its results?

A. top
B. stats
C. table
D. percent

14. Which search correctly limits results to the 5 most common values of a field?
A. | rare top=5
B. | top rare=5
C. | top limit=5
D. | rare limit=5

15. Which search returns the 15 least common values for the field src_ip?
A. sourcetype=firewall | rare num=15 src_ip
B. sourcetype=firewall | rare last=15 src_ip
C. sourcetype=firewall | rare count=15 src_ip
D. sourcetype=firewall | rare limit=15 src_ip