Question: 1

What is the correct syntax to count the number of events containing a vendor_action field?

A. count stats vendor_action
B. count stats (vendor_action)
C. stats count (vendor_action)
D. stats vendor_action (count)

Answer: C

Question: 2

By default, which of the following fields would be listed in the fields sidebar under interesting Fields?

A. host
B. index
C. source
D. sourcetype

Answer: A

Question: 3

When looking at a dashboard panel that is based on a report, which of the following is true?

A. You can modify the search string in the panel, and you can change and configure the visualization.
B. You can modify the search string in the panel, but you cannot change and configure the visualization.
C. You cannot modify the search string in the panel, but you can change and configure the visualization.
D. You cannot modify the search string in the panel, and you cannot change and configure the visualization.

Answer: C

Question: 4

Which of the following is a best practice when writing a search string?

A. Include all formatting commands before any search terms
B. Include at least one function as this is a search requirement
C. Include the search terms at the beginning of the search string
D. Avoid using formatting clauses as they add too much overhead

Answer: A

Question: 5

What type of search can be saved as a report?

A. Any search can be saved as a report
B. Only searches that generate visualizations
C. Only searches containing a transforming command
D. Only searches that generate statistics or visualizations

Answer: D

Question: 6

What can be included in the All Fields option in the sidebar?

A. Dashboards
B. Metadata only
C. Non-interesting fields
D. Field descriptions

Answer: C

Question: 7

What syntax is used to link key/value pairs in search strings?

A. action+purchase
B. action=purchase
C. action | purchase
D. action equal purchase

Answer: B

Question: 8

When viewing the results of a search, what is an Interesting Field?

A. A field that appears in any event
B. A field that appears in every event
C. A field that appears in the top 10 events
D. A field that appears in at least 20% of the events

Answer: D

Question: 9

What syntax is used to link key/value pairs in search strings?

A. Parentheses
B. @ or # symbols
C. Quotation marks
D. Relational operators such as =, <, or >

Answer: D

Question: 10

When a Splunk search generates calculated data that appears in the Statistics tab. in what formats can the results be exported?

A. CSV, JSON, PDF
B. CSV, XML JSON
C. Raw Events, XML, JSON
D. Raw Events, CSV, XML, JSON

Answer: D