D. Calculated fields automatically calculate the simple moving average for indexed fields.

Correct Answer: B

QUESTION 120
The transaction command allows you to _____ events across multiple sources

A. duplicate
B. correlate
C. persist
D. tag

Correct Answer: B

QUESTION 121
How is a Search Workflow Action configured to run at the same time range as the original search?

A. Set the earliest time to match the original search.
B. Select the same time range from the time-range picker.
C. Select the "Use the same time range as the search that created the field listing" checkbox.
D. Select the "Overwrite time range with the original search" checkbox.

Correct Answer: C

QUESTION 122
Which of the following search control will not re-rerun the search? (Select all that apply.)

A. zoom out
B. selecting a bar on the timeline
C. deselect
D. selecting a range of bars on the timelines

Correct Answer: BCD

QUESTION 123
The eval command 'if' function requires the following three arguments (in order):

A. Boolean expression, result if true, result if false
B. Result if true, result if false, boolean expression
C. Result if false, result if true, boolean expression
D. Boolean expression, result if false, result if true

Correct Answer: A

QUESTION 124
Select this in the fields sidebar to automatically pipe you search results to the rare command

A. events with this field
B. rare values
C. top values by time

D. top values

Correct Answer: B

QUESTION 125
When using the timechart command, how can a user group the events into buckets based on time?

A. Using the span argument.
B. Using the duration argument.
C. Using the interval argument.
D. Adjusting the fieldformat options.

Correct Answer: A

QUESTION 126
What is a limitation of searches generated by workflow actions?

A. Searches generated by workflow action cannot use macros.
B. Searches generated by workflow actions must be less than 256 characters long.
C. Searches generated by workflow action must run in the same app as the workflow action.
D. Searches generated by workflow action run with the same permissions as the user running them.

Correct Answer: D

QUESTION 127
It is mandatory for the lookup file to have this for an automatic lookup to work.

A. Source type
B. At least five columns
C. Timestamp
D. Input filed

Correct Answer: D

QUESTION 128
Which of the following statements describes the use of the Filed Extractor (FX)?

A. The Field Extractor automatically extracts all field at search time.
B. The Field Extractor uses PERL to extract field from the raw events.
C. Field extracted using the Extracted persist as knowledge objects.
D. Fields extracted using the Field Extractor do not persist and must be defined for each search.

Correct Answer: C

QUESTION 129
Where are the results of eval commands stored?

A. In a field.

B. In an index.
C. In a KV Store.
D. In a database.

Correct Answer: A

QUESTION 130
Which of the following about reports is/are true?

A. Reports are knowledge objects.
B. Reports can be scheduled.
C. Reports can run a script.
D. All of the above.

Correct Answer: D

QUESTION 131
Which of the following statements would help a user choose between the transaction and stats commands?

A. state can only group events using IP addresses.
B. The transaction command is faster and more efficient.
C. There is a 1000 event limitation with the transaction command.
D. Use state when the events need to be viewed as a single event.

Correct Answer: C

QUESTION 132
A data model can consist of what three types of datasets?

A. Pivot, searches, and events.
B. Pivot, events, and transactions.
C. Searches, transactions, and pivot.
D. Events, searches, and transactions.

Correct Answer: D

QUESTION 133
What is the correct format for naming a macro with multiple arguments?

A. monthly_sales(argument 1, argument 2, argument 3)
B. monthly_sales(3)
C. monthly_sales[3]
D. monthly_sales[argument 1, argument 2, argument 3)

Correct Answer: C

QUESTION 134
What happens when a user edits the regular expression (regex) field extraction generated in the Field Extractor (FX)?

A. There is a limit to the number of fields that can be extracted.
B. The user is unable to preview the extractions.
C. The extraction is added at index time.
D. The user is unable to return to the automatic field extraction workflow.

Correct Answer: A

QUESTION 135
When using | timchart by host, which filed is representted in the x-axis?

A. date
B. host
C. time
D. -time

Correct Answer: A

QUESTION 136
What does the fillnull command replace null values with, if the value argument is not specified?

A. 0
B. N/A
C. NaN
D. NULL

Correct Answer: A

QUESTION 137
When is a GET workflow action needed?

A. To send field values to an external resource.
B. To retrieve information from an external resource.
C. To use field values to perform a secondary search.
D. To define how events flow from forwarders to indexes.

Correct Answer: B

QUESTION 138
Which of the following searches show a valid use of a macro? (Choose all that apply.)

A. index=main source=mySource oldField=* |'makeMyField(oldField)'| table _time newField
B. index=main source=mySource oldField=* | stats if(`makeMyField(oldField)') | table _time newField
C. index=main source=mySource oldField=* | eval newField='makeMyField(oldField)'| table _time newField
D. index=main source=mySource oldField=* | '"newField(`makeMyField(oldField)')"' | table _time newField

Correct Answer: AC

QUESTION 139
Which of the following is one of the pre-configured data models included in the Splunk Common

Information Model (CIM) add-on?

A. Access
B. Accounting
C. Authorization
D. Authentication

Correct Answer: D

QUESTION 140
This function of the stats command allows you to identify the number of values a field has.

A. max
B. distinct_count
C. fields
D. count

Correct Answer: D

QUESTION 141
Alert throttling is used to _____.

A. verify each alert
B. stagger search request in a time sequenced order
C. stop spamming yourself with alerts
D. check severity

Correct Answer: C

QUESTION 142
What other syntax will produce exactly the same results as | chart count over vendor_action by user?

A. | chart count by vendor_action, user
B. | chart count over vendor_action, user
C. | chart count by vendor_action over user
D. | chart count over user by vendor_action

Correct Answer: A

QUESTION 143
Using the export function, you can export search results as _____.(Select all that apply)

A. Xml
B. Json
C. Html
D. A php file

Correct Answer: AB

QUESTION 144