Splunk Best Practices Quiz

1. What should a search query include? * (1 Point)

☐ filtering fields

☐ index

☐ sourcetype

☑ All of the above

2. what does the " | stats " represent in SPL (Splunk Processing Language)? * (1 Point)

○ Function

● Transforming command

○ A Field

3. What is a use case for using kv store? (Choose all that apply) * (1 Point)

☐ creating a file to enrich existing data set with dynamically updated records

☑ Dataset that needs to get updated frequently

☐ Dumping all error logs over time

4. which of the below searches can limit the number of events? (choose all that apply) * (1 Point)

☑ index=sample | head 10

□ None of the above

☑ index=sample | top 10

□ index=sample | last 10

5. What mode returns the best results for searches and reports, also it is the default mode? * (1 Point)

○ Fast Mode

● Smart Mode

6. Which search is more efficient? * (1 Point)

☑ index=rocket_plant where sourcetype=access_* | lookup vin OUTPUT model_type | stats count() by vin

□ index=rocket_plant where sourcetype=access_* | stats count() by vin | lookup vin OUTPUT model_type

7. How can you write a better search, avoiding the append
index=splunkquiz | eval score=100 | append [
search index=answers | eval score=90]
* (1 Point)

○ None of the above

● Use OR between the 2 indexes, (index=splunkquiz) OR (index=answers) , then add the 2 evals

○ Use OR between the 2 indexes, (index=splunkquiz) OR (index=answers) | eval score=case(index=="splunkquiz","100",index=="answers","90")

8. which search should be avoided from the below according to Splunk best practices? (choose all that apply) * (1 Point)

☐ index=sample field1="*google_org"

☑ index=sample field1="*google_org*"

☐ index=sample field1="google_org*"

9. What is a good use case to avoid using lookups? (Choose all that apply) * (1 Point)

☑ Static data set that is rarely updated

☐ Dynamic file updated daily

10. which search is faster to run from the below? * (1 Point)

○ index=sample | table vin, type, model

● index=sample | fields vin, type, model

11. What are the three different modes for searching in Splunk * (1 Point)

● Fast, Smart, Verbose modes

○ Fast, Smart, informational modes

○ Fast , Summarized, Verbose modes

12. Which is a best practice when searching? * (1 Point)

□ index=*

☑ index=index_name sourcetype=my_sourceype status=500

□ Set time range to All Time

13. What are some use cases for using lookup commands?   (Choose all that apply) * (1 Point)

□ Retrieve an information to identify an ID in your app logs

☑ Correlating a VIN model code with model type through model code lookup

☑ Summarizing your application logs

14. How can you optimize the given search?
sourcetype=my_source | lookup my_lookup_file check_field_inlookup OUTPUT Looked_up_field
| eval E=L/T
| search A=25 Looked_up_field >100 E>50 (Choose all that apply)
* (1 Point)

☑ Specifying the index

☑ Move the filtering for "E" field before the Eval command

☑ Move the "Looked_up_field" earlier in the search after the lookup command

□ None of the above

15. Job Inspector tool can be used to triage search time and help in optimizing a search, what is 1 of it's key components? * (1 Point)

☑ scanCount/second

□ Tags

☑ Splunk Search head

16. Which of the searches not following a best practice, choose all that apply? * (1 Point)

□ Narrow Search time window

☑ Using the word "Not" in the search

□ Specify index, source and sourcetype

□ filtering after the transforming commands (Stats, table, etc..)