1001_M3_Basic_Searching_In_Splunk_Quiz

1. Which statement about Booleans is correct when writing searches in Splunk?
    A. They must be lowercase
    B. They must be uppercase
    C. They must contain quotations marks
    D. They must be used with parenthesis

2. How are events displayed once a search has been executed?
    A. In chronological order
    B. Randomly by default
    C. In reverse chronological order
    D. Alphabetically following the field name

3. Which time range picker setting would display real-time events from the last 30 seconds?
    A. Preset – Relative: 30-seconds ago
    B. Relative – Earliest: 30-seconds ago, Latest: Now
    C. Real-time – Earliest: 30-seconds ago, Latest: Now
    D. Advanced – Earliest: 30-seconds ago, Latest: Now

4. Which Boolean operator is automatically assumed between two search terms if none is specified?
    A. XOR
    B. OR
    C. AND
    D. NOT

5. Which user interface element allows you to select a time range?
    A. Data summary
    B. Time range picker
    C. Search time picker
    D. Events Timeline

6. Which search query will return only events that contain “fail”, 500, and “error” together?
    A. error AND (fail AND 500)
    B. error OR (fail and 500)
    C. error AND (fail OR 500)

D. error OR fail OR 500

7. In a multi-index deployment, what happens if a search is run without specifying an index?
   A. No events will be returned
   B. You can't run a search without an index
   C. All non-indexed events to which the user has access will be returned
   D. Events from every index searched by default to which the user has access will be returned.

8. Which options are available after clicking on an item in the search results?
   A. Adding the item to a report
   B. Adding the item to the search
   C. Adding the item to a macro
   D. Saving the search to a CSV file

9. What does the time range `earliest=-72h@h latest=@d` represent?
   A. Look back 3 days ago and prior.
   B. Look back 72 hours, up to one day ago.
   C. Look back 72 hours, up to the end of today.
   D. Look back 3 days ago, up to the beginning of today.

10. What is the main purpose of the timeline displayed below the search bar?
    A. To show hidden data in search results
    B. To sort the events returned by the search in chronological order.
    C. To zoom in and out, although this does not change the scale of the chart.
    D. To show peaks and/or valleys in the timeline, which can indicate spikes in activity or downtime.

11. According to Splunk best practices, where should a wildcard be placed for the most efficient search?
    A. fa*l
    B. *fail
    C. fail*
    D. *fail*

12. Which character(s) can be used as a wildcard in Splunk?
    A. =

B. >
C. !
D. *

13. What is the purpose of the Search Assistant in Splunk?
    A. It is a mandatory feature used by admins during search
    B. Such a feature does not exist in Splunk.
    C. Shows options to complete the search string.
    D. None of the above

14. Which options can be used to define the start and end times of a search query?
    A. earliest=, latest=
    B. begin=, end=
    C. start=, end=
    D. All of the above

15. Which file formats are available for exporting search results from Splunk?
    A. PDF
    B. JSON
    C. XLS
    D. RTF

16. By default, how long does Splunk keep a search job?
    A. 10 Minutes
    B. 20 Minutes
    C. 1 Day
    D. 7 Days