1001_M9_Creating_Scheduled_Reports_&_Alerts_Quiz

1. What defines the range of data included in a scheduled report?
    A. All data accessible to the User role will appear in the report.
    B. All data accessible to the owner of the report will appear in the report.
    C. All data accessible to all users will appear in the report until the next time the report is run.
    D. The owner of the report can configure permissions so that the report uses either the User role or the owner's profile at run time.

2. What is the main purpose of a scheduled report?
    A. Auto-detect changes in performance.
    B. Auto-generated PDF reports of overall data trends.
    C. Regularly scheduled archiving to keep disk space low.
    D. Triggering an alert in your Splunk instance when certain conditions are met.

3. If an alert action is set to run a script, Splunk must locate it. Which directory is one possible location Splunk checks for the script?
    A. $SPLUNK_HOME/bin/scripts
    B. $SPLUNK_HOME/etc/scripts
    C. $SPLUNK_HOME/bin/etc/scripts
    D. $SPLUNK_HOME/etc/scripts/bin

4. Which of the following statements about Splunk alerts is correct?
    A. Alerts are based on searches that are either run on a scheduled interval or in real-time.
    B. Alerts are based on searches and when triggered will only send an email notification.
    C. Alerts are based on searches and require cron to run on scheduled interval.
    D. Alerts are based on searches that are run exclusively as real-time.

5. In the Splunk UI, alerts can be filtered by which attributes?
    A. App, owner, Severity, and Type
    B. App, owner, Priority, and Status
    C. App, Dashboard, Severity, and Type
    D. App, Time Window, Type, and Severity

6. Under what condition does an alert get triggered?
    A. When Splunk encounters a syntax error in a search.
    B. When a trigger action meets the predefined conditions.
    C. When an event in a search matches up with a data model.

D. When results of a search meet a specifically defined condition.

7. A SOC manager reports that a scheduled alert for failed login attempts generated 200 emails. They still want email alerts for failed logins but with fewer notifications. Which solution would address this issue?
   A. Change the schedule so that alert runs more frequently.
   B. Disable the alert entirely.
   C. Change the trigger from “For each result” to “Once”.
   D. Change the alert action from email to webhook.

8. By default, which Splunk role has the minimum permissions necessary to write alerts?
   A. Alerting
   B. Admin
   C. Power
   D. User