C1000-018$^{\text{Q\&As}}$

IBM QRadar SIEM V7.3.2 Fundamental Analysis

Pass IBM C1000-018 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/c1000-018.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IBM Official Exam Center

QUESTION 1

An auditor has requested a report for all Offenses that have happened in the past month. This report generates at the end of every month but the auditor needs to have it for a meeting that is in the middle of the month.

What will happen to the scheduled report if the analyst manually generates this report?

A. The scheduled report needs to be reconfigured.

B. The analyst needs to delete the scheduled report and create a new one.

C. The report will get duplicated so the analyst can then run one manually.

D. The report still generates on the schedule initially configured.

Correct Answer: B

Explanation: Shared schedules must be deleted manually using the Schedules page in the web portal or the Shared Schedules folder in Management Studio. If you delete a shared schedule that is in use, all references to it are replaced with report-specific schedules. If you delete a shared schedule that is used by multiple reports and subscriptions, the report server will create individual schedules for each report and subscription that previously used the shared schedule. Each new individual schedule will contain the date, time, and recurrence pattern that was specified in the shared schedule. Note that Reporting Services does not provide central management of individual schedules. If you delete a shared schedule, you will now have to maintain the schedule information for each individual item.

Reference: https://docs.microsoft.com/en-us/sql/reporting-services/subscriptions/create-modify-anddelete-schedules?view=sql-server-ver15

QUESTION 2

Which are the supported protocol configurations for Check Point integration with QRadar? (Choose two.)

A. CHECKPOINT REST API

B. SYSLOG

C. JDBC

D. SFTP

E. OPSEC/LEA

Correct Answer: BE

QUESTION 3

An analyst needs to find all events that are creating offenses that are triggered by rules that contain the word suspicious in the rule name.

Which query can the analyst use as a working sample?

A. SELECT LOGSOURCETYPE(logsourceid), “from log_events where RULENAME(creeventlist) ILIKE ‘%suspicious%’

B. SELECT LOGSOURCERULES(logsourceid), “from rule_events where RULENAME(creeventlist) ILIKE ‘%suspicious%’

C. SELECT LOGGEDOFFENSE(logsourceid), *from offense_events where RULENAME(creeventlist) ILIKE ‘%suspicious%’

D. SELECT LOGSOURCENAME(logsourceid), * from events where RULENAME(creeventlist) ILIKE ‘%suspicious%’

Correct Answer: D

Reference: https://www.ibm.com/docs/en/qradar-on-cloud?topic=searches-advanced-search-options

QUESTION 4

When an Offense is triggered, it only shows the events that triggered the Offense. The analyst wants to investigate further to see more events around the incident, not only those that triggered the Offense. The analyst clicks on the event count and sees the events belonging to the Offense.

How can the analyst proceed to see a more detailed picture of what occurred?

A. Right-click on the source IP, and choose More Options, then Information, and then Search Events.

B. Right-click on the destination IP, and choose More Options, then Raw Events.

C. Right-click on the source IP, and choose View in DSM Editor.

D. Right-click and filter on the Destination IP.

Correct Answer: D

Reference: https://www.ibm.com/docs/en/qradar-on-cloud?topic=events-filtering

QUESTION 5

What is displayed in the status bar of the Log Activity tab when streaming events?

A. Average number of results that are received per second.

B. Average number of results that are received per minute.

C. Accumulated number of results that are received per second.

D. Accumulated number of results that are received per minute.

Correct Answer: A

Explanation:

Status bar

When streaming events, the status bar displays the average number of results that are received per

second.

Reference: https://www.ibm.com/docs/en/qradar-on-cloud?topic=investigation-log-activity-tab-overview