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.passapply.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

Which filter would an analyst apply in the Log Activity tab to get a list of log sources not reporting to QRadar?

A. Log source status does not equal active

B. Custom rule equals device stopped sending events

C. Log source type does not equal active

D. Log source status does not equal error

Correct Answer: A

QUESTION 2

An analyst wants to analyze the long-term trending of data from a search. Which chart would be used to display this data on a dashboard?

A. Bar Graph

B. Time Series chart

C. Pie Chart

D. Scatter Chart

Correct Answer: A

Explanation:

You could use a bar graph if you want to track change over time as long as the changes are significant.

Reference: https://www.statisticshowto.com/probability-and-statistics/descriptive-statistics/bar-chart-bargraph-examples/

QUESTION 3

An analyst had been researching an Offense that has now disappeared from the active Offense list.

What is the period of time that has to pass before an active Offense that receives no new contributing events or flows become inactive?

A. 5 days

B. 3 days

C. 24 hours

D. 1 hour

Correct Answer: A

Explanation:

An offense remains in a dormant state for 5 days. If an event is added while an offense is dormant, the five-day counter is reset.

Reference: https://www.ibm.com/docs/en/SS42VS_7.3.2/com.ibm.qradar.doc/b_qradar_users_guide.pdf

QUESTION 4

What does the Assets tab provide?

A unified view of the information that is known about:

A. network devices.

B. triggered Offenses.

C. log sources.

D. events and flows.

Correct Answer: D

Reference: https://www.ibm.com/support/pages/identity-and-how-log-source-events-update-assets-qradarsiem

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