C2150-624 Q&As

IBM Security QRadar Risk Manager V7.2.6 Administration

Pass IBM C2150-624 Exam with 100% Guarantee

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

https://www.pass2lead.com/c2150-624.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Given the following RegEx: (\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b) What data does this expression extract?

A. URL

B. User Name

C. IP address

D. Email Address

Correct Answer: C

QUESTION 2

An IBM Security QRadar SIEM V7.2.8 Administrator is implementing a retention policy of flows and events.

The retention buckets are sequenced in priority order from the top row to the bottom row.

What happens if a record does not match any of the configured retention buckets?

A. The record is dropped and is not stored

B. The record is stored in the default retention bucket

C. The record is stored in a raw format inside /default partition

D. The record is stored in any of the available retention buckets

Correct Answer: B

QUESTION 3

An Administrator has configured a customized log source extension to provide asset updates to IBM Security QRadar SIEM V7.2.8. Instead of QRadar receiving an update that has the host name of the asset that the user logged in to, the log source generates many asset updates that all have the same host name. In this situation what will QRadar report?

A. This will cause stale asset data.

B. This will cause asset growth deviations.

C. This will cause excessive authentication failure events.

D. This will cause excessive flow data to be processed by the Magistrate.

Correct Answer: B

Instead of QRadar receiving an update that has the host name of the asset that the user logged in to, the

log source generates many asset updates that all have the same host name.

In this situation, the asset growth deviation is caused by one asset profile that contains many IP addresses

and user names.

QUESTION 4

Which query, when run from IBM Security QRadar SIEM V7.2.8, will show EPS for log sources?

A. select logsourcename(logsourceid) as LogSource, sum(eventcount) / ((max(endTime) - min (startTime)) / 1000) as EPS from events group by logsourceid order by EPS desc last 24 hours

B. select logsourcename(logsourceqid) as LogSource, sum(eventcount) / ((max(endTime) - min (startTime)) / 1000) as EPS from events group by logsourceqid order by EPS desc last 24 hours

C. select logsourcename(logsourceid) as LogSource, sum(eventcount) / ((max(endTime) - min (startTime)) / 1000) as FPS from events group by logsourceid order by EPS desc last 24 hours

D. select logsourcename(logsourceid) as LogSource, sum(eventcount) / ((max(endTime) - min (startTime)) / 1000) as EPS from events group by logsourceid order by FPS desc last 24 hours

Correct Answer: B

QUESTION 5

An Administrator working with an IBM Security QRadar SIEM V7.2.8 deployment needs to build an Ariel

Query to find all flow data send in the last 24 hours where the amount of bytes being sent and received are

larger than 64 bytes.

What Query needs to be used?

A. SELECT * FROM flows WHERE sourceBytes> 64 anddestinationBytes> 64 LAST 1 DAY

B. SELECT * FROM flows WHERE sourceBytes> 64 AND destinationBytes> 64 LAST 1 DAYS

C. SELECT * FROM flowsdata WHERE sourceBytes> 64 AND destinationBytes> 64 LAST 1 DAY

D. SELECT * FROM flowsdata WHERE sourceBytes> 64 AND destinationBytes> 64 LAST 1 DAYS

Correct Answer: B