Vendor: IBM

Exam Code: 000-N24

Exam Name: IBM QRadar Technical Sales Mastery Test v1

Version: DEMO

QUESTION 1
Write a regular expression that extracts only the username from the string: Username=miths Write a regular expression that extracts only the username from the string: Username=miths

A. \smith)\\smith)\
B. Ame=.*)\Ame=.*)\
C. =\.*)
D. ame\=\.*)\ame\=\.*)\

Answer: D

QUESTION 2
Which method can be used to deliver log data to QRadar?

A. Syslog
B. Opsec/LEA
C. TFTP
D. Both A and B are correct

Answer: D

QUESTION 3
Write a regular expression that extracts only the username from the string: serID: smiths Write a regular expression that extracts only the username from the string: serID: smiths

A. rID\:\s(.*)\s
B. Use\:\s(.*)\s
C. rID\:(\d+)\s
D. serid\:(.*)\serid\:(.*)\

Answer: A

QUESTION 4
What characteristic distinguishes QRadar from other SIM/SIEM solutions?

A. QRadar is the only solution that works in a heterogeneous environment.
B. QRadar has the best correlation engine.
C. QRadar supports many more devices.
D. QRadar is the only SIM/SIEM solution that natively processes flows.

Answer: D

QUESTION 5
How do you add a new (supported) DSM to the system?

A. Download the rpm to the console and use the rpm command to add it.
B. You cannot add new DSMs to the system.
C. Configure autoupdate on the admin tab and manually add the DSM using the rpm command on the console.

D. Both A and C are correct.

Answer: D

QUESTION 6
The only way QRadar can get asset information is by importing it from active scanners?

A. True
B. False

Answer: B

QUESTION 7
What are the two backup options available in Q1 Radar?

A. Config and log data
B. Config and screenshot
C. Data and audit log
D. Data and system log

Answer: A

QUESTION 8
QRadar can accept data input from:

A. Event Log Sources
B. Flows from network devices
C. Vulnerability assessment tools
D. All of the above

Answer: D