KTest

高品質　より良いサービス



練習問題

https://www.ktest.jp

1年間無料アップデート

Exam : **000-N24**

Title : IBM QRadar Technical Sales Mastery Test v1

Version : Demo

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

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

3.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

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

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