IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **C1000-055**

Title : IBM QRadar SIEM V7.3.2 Deployment

Version : DEMO

1.A client uses the IBM Security QRadar Vulnerability Manager to discover vulnerabilities on the network devices, applications, and software. They run the QRadar Vulnerability Manager from an All-in-one system, where the scanning and processing functions are on the Console. As the client's QRadar deployment is growing, they are also considering deploying scanners.
What is a valid client motivation for deploying additional scanners?
A. To scan an asset in the same geographic region as the QRadar Vulnerability Manager processor.
B. To patch assets for their vulnerabilities.
C. To avoid scanning through a firewall that is a log source.
D. To find more vulnerabilities on a given system.
Answer: D

2.A deployment professional found the System Activity Reporting (SAR) notifications alert "Performance degradation was detected in the event pipeline. Expensive DSM extensions were found". From the Log Sources under date creation, it can be seen that a new DSM was installed by another team member today.
To troubleshoot this issue, what steps can the deployment professional take? (Choose two)
A. Review the debug file /var/log/qradar.dsm.debug
B. Review the payload of the notification to determine which expensive DSM extension in the pipeline affects performance.
C. Ensure that the log source extension is applied to all of the log sources.
D. Run the DSM Editor and select Optimize over DSM payload to correct this error.
E. Order your log source parsers from the log sources with the most sent events to the least and disable unused parsers.
Answer: B

3.A customer is building a big data solution which aims to perform long term analysis of security data. Security events that are processed by QRadar are also relevant for the system and according to the QRadar administrator the most straightforward option for data ingestion is to configure event forwarding on QRadar. The customer would like to make use of QRadar's parsing capability and its built-in parsers instead of developing new parsers for the big data platform. A deployment professional is asked for advice about the data format to configure for the event forwarding.
Which available option should the deployment professional propose?
A. Normalized
B. Payload
C. XML
D. JSON
Answer: A

4.A deployment professional decides to improve visibility in the network and successfully installs the Flow Collector.
What should the deployment professional connect the Flow Collector to?
A. WAN port
B. SPAN port
C. LAN port

D. SAN port
Answer: B

5.A deployment professional needs to configure the IBM QRadar systems so that data is forwarded to one or more vendor systems, such as ticketing or alerting systems.
Which event format options can the deployment professional use for forwarding destination configuration?
A. payioad, normalized and json
B. leef, json and cef
C. normalized, json and cef
D. json, cef and payload
Answer: C