Vendor: IBM

Exam Code: 000-196

Exam Name: IBM Security QRadar SIEM V7.1 Implementation

Version: DEMO

QUESTION 1
Which string creates a network hierarchy group called MailServers inside a group called DMZ?

A. DMZ.MailServers
B. DMZ-MailServers
C. DMZ MailServers
D. DMZ+MailServers

Answer: A

QUESTION 2
What will the transfer rate be for a value of 0 when configuring event forwarding from an event collector to an event processor?

A. Throttled
B. Disabled
C. Unlimited
D. Based on the number of events stored

Answer: C

QUESTION 3
An ip_context_menu.xml plug-in was created to assist in finding additional details for selected lP addresses. Where must this file be placed so the plug-in can be used?

A. /opt/qradar/init
B. /opt/qradar/bi n
C. /opt/qradar/conf
D. /opt/qradar/webplugins

Answer: C

QUESTION 4
Which two tabs can be used to access the False Positive Tuning window in order to minimize the offenses that are being generated? (Choose two.)

A. Admin
B. Offenses
C. Dashboard
D. Log Activity
E. Network Activity

Answer: DE

QUESTION 5
SCSI can be configured in a standard IBM Security Qradar SIEM V7.1 deployment or in a High Availability environment. The initiator name is used to identify the iSCSI device volume where the/store or /store/ariel file system should be mounted. Where is the initiator name file stored?

A. /etc/iscsi/initiatorname.iscsi
B. /optliscsi/initiatorname.iscsi
C. /proc/etc/iscsi/initiatorname.iscsi
D. /optlqradar/conf/initiatorname.iscsi

Answer: A

QUESTION 6
How would an IBM Security QRadar administrator know if asymmetric superflows are enabled?

A. Use the System Notification mechanism (e.g. pop-up)
B. Use the QFlow Collector configuration in the Deployment Editor
C. Investigate the contents of the BB:AsymmetricSuperFlowSource building block
D. Check for any log events of the High Level Category Flow and a Low Level Category Unidirectional

Answer: B

QUESTION 7
Where does Universal DSM data appear in the IBM Security Qradar SIEM V7.1 user interface?

A. Dashboard
B. Log Activity tab
C. Network Activity tab
D. Admin tab > Log Sources

Answer: B