Vendor: IBM

Exam Code: 000-195

Exam Name: IBM Security QRadar V7.0 MR4 Exam

Version: DEMO

QUESTION 1
How does a user search for events by high/low level category?

A. Actions menu > add a filter
B. Display drop-down > select categories
C. Add Filter icon > Category drop-down
D. View drop-down > select By Category drop-down

Answer: C

QUESTION 2
Offenses can be exported to which two file formats? (Choose two.)

A. RTF
B. XML
C. PDF
D. CSV
E. HTML

Answer: BD

QUESTION 3
In the All Offenses dialog box, which column are the offenses sorted by default?

A. Start Date
B. Magnitude
C. Description
D. Offense Type

Answer: B

QUESTION 4
How does a user access the Extract a Custom Property section from a paused event screen in the Log Activity tab?

A. Actions menu > Extract Property
B. Double-click the event > Extract Property
C. Actions menu > Show All > Extract Custom Property
D. Right-click on the event > Properties > Extract Property

Answer: B

QUESTION 5
Why is coalescing important to a non-admin user?

A. It saves space on disk.
B. It saves events per second.
C. It makes it faster to parse the events.

D. It makes events easier to read in the Log Activity screen.

Answer: D

QUESTION 6
An IBM Security QRadar V7.0 MR4 report can be generated into which three formats? (Choose three.)

A. XLS
B. PDF
C. CSV
D. DOC
E. JPEG
F. HTML

Answer: ABF

QUESTION 7
How would a user navigate to the Help menu in the IBM Security QRadar V7.0 MR4 (QRadar) interface?

A. Press Ctrl+H
B. Right-click on Item > Help
C. Help > QRadar Help Content
D. Select from the Action drop-down list

Answer: C

QUESTION 8
Which statement about log source identifiers is true for the same log source identifier to be used more than once?

A. It must always be unique.
B. It must be unique amongst the same protocol.
C. It must be unique amongst the same log source group.
D. It must be unique amongst log sources of the same type

Answer: D

QUESTION 9
What is an Offense Type?

A. The offense response
B. A scoring priority of Set by Event
C. The destination of the e-mail notification sent
D. The index option chosen in the rule that created the offense

Answer: D