C2150-400 Q&As

IBM Security Qradar SIEM Implementation v 7.2.1

Pass IBM C2150-400 Exam with 100% Guarantee

Following Questions and Answers are all new published by IBM Official Exam Center

QUESTION 1

Which feature of QRadar is used for correlation purposes to help reduce false positives?

A. Flow information

B. Events information

C. Asset port information

D. Asset profile information

Correct Answer: D

QUESTION 2

What will be restored when restoring event data or flow data for a particular period to a MH?

A. Only data sent to the console for that time period is restored to the MH.

B. Only event data or flow data for the MH being restored will be restored to that MH.

C. Only data that was accumulated for reports and searches will be restored to the MH.

D. All data for all MHs for a specific time period is restored to its respective hosts in the deployment.

Correct Answer: B

QUESTION 3

Which Network Address Translation (NAT) is necessary to enable NAT for a Managed Host?

A. Static NAT translation

B. Active NAT translation

C. Variable NAT translation

D. Dynamic NAT translation

Correct Answer: A

QUESTION 4

Which character is used for naming subgroups when using the option Add Group in the Network Hierarchy editor?

A. +(plus)

B. . (period)

C. \ (Backslash)

D. /(Forward Slash)

Correct Answer: B

QUESTION 5

What is used to collect security events in a QRadar Distributed Deployment?

A. QRadar 3124 Console

B. QRadar 1724 Processor

C. QRadar 1624 Processor

D. QRadar 1310 QFlow Collector

Correct Answer: D