C2150-400 Q&As

IBM Security Qradar SIEM Implementation v 7.2.1

Pass IBM C2150-400 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/c2150-400.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which two types of charts are available on QRadar SIEM Report editor? (Choose two.)

A. Top Events

B. Top Source IPs

C. Top Login Failures

D. Top Destination IPs

E. Top Access Failures

Correct Answer: BD

QUESTION 2

How many days does QRadar keep record of Closed Offense by default?

A. 1 day

B. 5 days

C. 3 days

D. 7 days

Correct Answer: C

QUESTION 3

There are unknown log records from unsupported security device events in the Log activity tab. You are planning to write an LSX for an unsupported security device type based on UDSM.

What is the file format for exporting the unknown log records?

A. CSV

B. PDF

C. XLS

D. Text

Correct Answer: D

QUESTION 4

What is QRadar QFlow Collector combined with QRadar SIEM designed to do?

A. Encryption

B. Netflow collection

C. Syslog forwarding

D. Layer 7 application visibility

Correct Answer: B

QUESTION 5

Which two fields are required to be filled out when adding a new network to the network hierarchy? (Choose two.)

A. Weight

B. IP and CIDR

C. Capture Filter

D. Flow Source Interface

E. Flow Retention Length

Correct Answer: AD