A2150-195 Q&As

Assess: IBM Security QRadar V7.0 MR4 Fundamentals

Pass IBM A2150-195 Exam with 100% Guarantee

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

https://www.pass2lead.com/a2150-195.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

What are three data types provided by right-clicking IP address > More Options list > Information menu? (Choose three.)

A. Port Scan

B. DateyTime

C. DNS lookup

D. WHOIS lookup

E. Source Summary

F. Destination Summary

Correct Answer: ACD

QUESTION 2

When working with rules, why do some rules specify QID values and some specify events?

A. Only low and high level categories can be specified within rules.

B. It is a matter of convention; QIDmap and event names are the same.

C. Event names are more precise; multiple events can be to the same QIDmap entry.

D. QID values are more precise; multiple QIDmap entries can be to same event name.

Correct Answer: D

QUESTION 3

Using the regex * (RecordNumber) = (. *?)\s\\', which capture group should be used to capture the digits?

A. 0

B. 1

C. 2

D. 3

Correct Answer: C

QUESTION 4

Which tab displays correlated security alerts in IBM Security QRadar V7.0 MR4?

A. Admin

B. Reports

C. Offenses

D. Log Activity

Correct Answer: C

QUESTION 5

The remote directory field can be left blank for which protocol?

A. FTP

B. TFTP

C. SFTP

D. FTPS

Correct Answer: A