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.passapply.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 data collection types are supported for SAINT scanner configurations? (Choose two.)

A. App Scan

B. Live Scan

C. Report Only

D. Passive Scan

E. Vulnerability Scan

Correct Answer: BC

QUESTION 2

A QRadar administrator needs to tune the system by enabling or disabling the appropriate rules in order to ensure that the QRadar console generates meaningful offenses for the environment. Which role permission is required for enabling and disabling the rule?

A. Offenses > Maintain CRE Rules

B. Offenses > Toggle Custom Rules

C. Offenses > Manage Custom Rules

D. Offenses > Maintain Custom Rules

Correct Answer: C

QUESTION 3

Which scanners report vulnerabilities on all ports? (Choose two.)

A. Axis

B. NMap

C. Qualys

D. tcpdump

E. nCircle IP360

Correct Answer: BC

QUESTION 4

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 5

Which Permission Precedence should be applied in the Security Profile so the users can see events from the "Windows Servers" log source group and from other log sources that match the destination or source network "Windows"?

A. No Restrictions

B. Log Sources Only

C. Networks OR Log Sources

D. Networks AND Log Sources

Correct Answer: B

[Latest C2150-400 Dumps](#)   [C2150-400 PDF Dumps](#)   [C2150-400 Practice Test](#)