

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 proxy options are supported by QRadar Auto Update Advanced settings? (Choose two.)

- A. Proxy Port
- B. Proxy Type
- C. Proxy Name
- D. Proxy Category
- E. Proxy Username

Correct Answer: DE

QUESTION 2

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

QUESTION 3

A customer wants to view Log Sources based on functionality on QRadar console. The customer wants to categorize its Log Sources into multiple groups, which allows the customer to efficiently view and track its log sources.

What is the maximum number of log sources a log source group can display on the QRadar console?

- A. 100
- B. 500
- C. 750
- D. 1000

Correct Answer: B

QUESTION 4

On the QRadar console you have received notification that CVE ID: CVE-2010-000 is being actively used. What search parameter should you select from the list of search parameters in this situation?

- A. Collateral Damage Reference
- B. Vulnerability External Reference
- C. Vulnerability Information System
- D. Vulnerability Internal System Reference

Correct Answer: C

QUESTION 5

What is a benefit of enabling indexes on event properties?

- A. Improved Offense Correlation
- B. Improved search performance
- C. Improved Performance of Custom Rules
- D. Improved accuracy of auto-discovery log sources

Correct Answer: B

[C2150-400 Study Guide](#)

[C2150-400 Exam Questions](#)

[C2150-400 Braindumps](#)