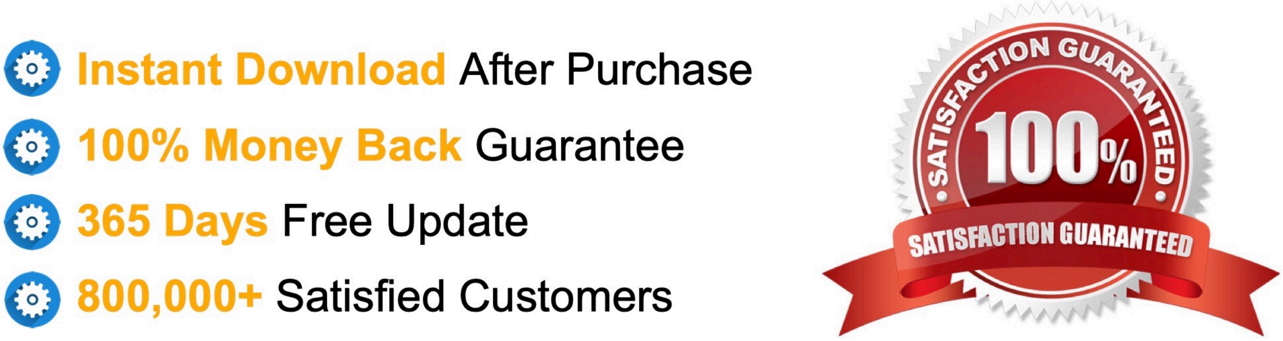
C2150-400$^{\text{Q\&As}}$

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


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

QUESTION 1

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 2

Where do you save the "Login Message File" on the system when setting up a banner message for the authentication page?

A. /opt/qradar/conf/

B. /opt/qradar/www

C. /opt/tomcat/conf/

D. /opt/qradar/webapps

Correct Answer: A

QUESTION 3

A QRadar SIEM administrator wants to create a Flow Rule that includes a building block definition (BB) that includes applications that indicate communication with file sharing sites. In which group will the administrator find this specified building block?

A. Policy

B. Host Definitions

C. Network Definition

D. Category Definitions

Correct Answer: B

QUESTION 4

A QRadar SIEM administrator wants to report when a local system connects to the internet on more than 100 destination ports over a 2 hour period. The administrator created an anomaly rule to capture this scenario.

Which type of rule should be selected in the rule creation wizard in this situation?

A. Flow Tule

B. Event Rule

C. Offense Rule

D. Common rule

Correct Answer: B

QUESTION 5

A customer has log files from Windows-based systems and wants to push those logs to the QRadar console.

What options should the customer use in WinCollect to collect and forward these logs?

A. File Forwarder

B. Flow Forwarder

C. Event Forwarder

D. Windows-based Event Log Forwarder

Correct Answer: C