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.leads4pass.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

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 2

What should be the latency between the primary and secondary HA hosts?

A. Less than 1 millisecond

B. Less than 2 milliseconds

C. Less than 3 milliseconds

D. Less than 4 milliseconds

Correct Answer: B

QUESTION 3

Which view option allows you to view events as they occur?

A. Automatic

B. Live Events

C. Real Time (streaming)

D. Last Interval (auto refresh)

Correct Answer: C

QUESTION 4

Which directory from the QRadar host can be moved to offboard storage?

A. A/ar

B. /store

C. /home

D. /media

Correct Answer: B

QUESTION 5

An off-site source can connect to which component?

A. Flow collector

B. Event collector

C. Flow processor

D. Event processor

Correct Answer: B

QUESTION 6

Which feature of QRadar is used for correlation purposes to help reduce false positives?

A. Flow information

B. Events information

C. Asset port information

D. Asset profile information

Correct Answer: D

QUESTION 7

What does the message in the System Notification Widget in the Dashboard "Disk Sentry: Disk usage exceeded WARNING threshold" tell you?

A. One of your File Systems has exceeded 92%.

B. One of your File Systems has exceeded 95%.

C. One of your File Systems has exceeded 98%.

D. One of your File Systems has exceeded 90%.

Correct Answer: D

QUESTION 8

Which Network Address Translation (NAT) is necessary to enable NAT for a Managed Host?

A. Static NAT translation

B. Active NAT translation

C. Variable NAT translation

D. Dynamic NAT translation

Correct Answer: A

QUESTION 9

What is the maximum height for a custom logo in a report header?

A. 25 pixels

B. 50 pixels

C. 100 pixels

D. 500 pixels

Correct Answer: B

QUESTION 10

Which tab in the QRadar web console allows flows to be monitored and investigated?

A. Admin

B. Assets

C. Offenses

D. Network Activity

Correct Answer: C

QUESTION 11

Who can view all offenses?

A. All users

B. Admin user

C. User who has access to All Log Sources and All Networks

D. Restricted User who has access to a Specific Log Source and Network

Correct Answer: B

QUESTION 12

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 13

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 14

What type of users can view all reports that are created by other users?

A. Auditors

B. Analysts

C. Managers

D. Administrators

Correct Answer: D

QUESTION 15

What does QRadar use to group the event or flow according to the network?

A. Network mapping

B. Network hierarchy

C. Application mapping

D. Application hierarchy

Correct Answer: A