# 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**

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 2**

What is used to collect netflow and jflow traffic in a QRadar Distributed Deployment?

A. QRadar 3124 Console

B. QRadar 1624 Processor

C. QRadar 1724 Processor

D. QRadar 700 Risk Manager

Correct Answer: A

**QUESTION 3**

From which screen can a Secondary Host be added to an HA host?

A. Admin -> System Settings

B. Admin -> Deployment Editor

C. Admin -> Store and Forward

D. Admin -> System and License Management

Correct Answer: D

**QUESTION 4**

With a Data Deletion Policy of "When storage is required", data will remain in storage until which scenario is reached?

A. If used disk space reaches 88% for records and 85% for payloads.

B. If used disk space reaches 85% for records and 88% for payloads.

C. If used disk space reaches 85% for records and 83% for payloads.

D. If used disk space reaches 83% for records and 85% for payloads.

Correct Answer: C

**QUESTION 5**

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 6**

Which proxy option can be set in the QRadar Auto Update Advanced settings?

A. Proxy Type

B. Proxy Name

C. Proxy Schedule

D. Proxy Password

Correct Answer: D

**QUESTION 7**

Which two statements are true regarding QRadar Log Sources and DSMs? (Choose two.)

A. One log source must have one DSM.

B. One DSM must have many log sources.

C. One log source must have many DSMs.

D. One DSM can have only one log source.

E. One DSM can be used in many log sources.

Correct Answer: CE

**QUESTION 8**

Which NetFlow versions does QRadar SIEM support?

A. 1, 2, 3, and 4

B. 1, 4, 7, and 9

C. 1, 3, 5, and 9

D. 1, 5, 7, and 9

Correct Answer: D

**QUESTION 9**

What functionalities of QRadar provide the ability to collect, understand, and properly categorize events from external sources?

A. Log sources

B. Flow sources

C. Syslog sources

D. External sources

Correct Answer: A

**QUESTION 10**

Which network monitoring port does Cisco NetFlow require to be configured in QRadar?

A. Port 514

B. Port 161

C. Port 2055

D. Port 8080

Correct Answer: C

**QUESTION 11**

Which two IP Addresses are required to setup NATed environment? (Choose two.)

A. Public IP Address

B. Private IP Address

C. Remote IP Address

D. Secondary IP Address

E. Destination IP Address

Correct Answer: DE

**QUESTION 12**

Which two authentication methods for the QRadar User Interface are valid? (Choose two.)

A. SecureID

B. Digital Signatures

C. Password Authentication Protocol (PAP)

D. Remote Authentication Dial In User Service (RADIUS)

E. Terminal Access Controller Access-Control System (TACACS)

Correct Answer: DE

**QUESTION 13**

Which two IP Addresses are required to Add a HA host? (Choose two.)

A. Public IP Address

B. Private IP Address

C. Cluster IP Address

D. Remote IP Address

E. IP Address of Secondary Host

Correct Answer: CE

**QUESTION 14**

An off-site target can connect to which component

A. Flow collector

B. Event collector

C. Flow processor

D. Event processor

Correct Answer: D

**QUESTION 15**

Which operating system is supported for creating a bootable flash drive for recovery?

A. IBM AIX

B. MAC OS X

C. Ubuntu Linux

D. Windows OS

Correct Answer: C