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.pass4itsure.com/c2150-400.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IBM Official Exam Center

QUESTION 1

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 2

A customer is observing the Asset tab on the QRadar console and is getting duplicate assets in the console.

What is the reason for this asset duplication?

A. There are multiple heterogeneous assets present in environment.

B. There are multiple assets having same configuration details present in environment.

C. QRadar creates duplicate assets after a specific periodic interval without considering asset activity or inactivity.

D. Asset doesn\\'t appear in network for specific time period; when it came back QRadar detects it and

created a new asset for the same.

Correct Answer: C

QUESTION 3

A mail server typically communicates with 50 hosts per second in the middle of the night and then suddenly starts communicating with 1.000 hosts a second. The administrator wants to get an email alert whenever this situation is being observed.

Which type of rule should an administrator create to monitor this situation?

A. Flow Rule

B. Anomaly Rule

C. Threshold Rule

D. Behavioral Rule

Correct Answer: C

QUESTION 4

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

A. SecureID

B. Client Certificates

C. System Authentication

D. Extensible Authentication Protocol (EAP)

E. Lightweight Directory Access Protocol (LDAP)

Correct Answer: CE

QUESTION 5

Which Permission Precedence should be applied to the users security profile assuming the administrators only want the group to have access to Windows events and flows and not events from other networks?

A. No Restrictions

B. Log Sources Only

C. Networks OR Log Sources

D. Networks AND Log Sources

Correct Answer: D