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

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

What does Server discovery do?

A. Defines rules for hosts

B. Creates asset searches

C. Populates host definition building blocks

D. Builds complex search queries for events flows

Correct Answer: C

QUESTION 2

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

QUESTION 3

In which two ways can an administrator view all the events that are related to an offense from the Offense Details screen? (Choose two.)

A. Top 5 Source IPs section

B. Click on Display > Sources

C. Click on Display > Destinations

D. Click on Event/Flow Count field\\'s Events link

E. Click on Events button in Last 10 Events section

Correct Answer: BD

QUESTION 4

What does the message in the System Notification Widget on the Dashboard "Disk sentry: System disk usage back to normal levels." tell you?

A. One of your File Systems has been reduced to below 92%.

B. One of your File Systems has been reduced to below 95%.

C. One of your File Systems has been reduced to below 98%.

D. One of your File Systems has been reduced to below 90%.

Correct Answer: A

QUESTION 5

How do you view Raw Events on the Log Activity tab?

A. Select "Raw Events" from the View list box

B. Select "Raw Events" from the Actions list box

C. Select "Raw Events" from the Display list box

D. Select "Raw Events" from the Quick Searches list box

Correct Answer: C

Latest C2150-400 Dumps   C2150-400 PDF Dumps   C2150-400 VCE Dumps