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.passapply.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

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 2

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

QUESTION 3

Which two proxy options are required to be set when using a Proxy Server for Auto Updates in QRadar? (Choose two.)

A. Proxy Type

B. Proxy Name

C. Proxy Schedule

D. Proxy Server URL

E. Proxy Port number

Correct Answer: BD

QUESTION 4

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 5

Which three tasks can an administrator perform from the QRadar SIEM reports tab? (Choose three.)

A. Brand reports

B. Ability to create custom reports

C. Ability to create custom compliance templates

D. Present statistics derived from source IP and destination IP

E. Present measurements and statistics derived from real time data

F. Present measurements and statistics derived from events, flows and offenses

Correct Answer: BDF