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

A customer has configured NetApp storage device to send events to QRadar SIEM. The customer wants an alert to be generated whenever error messages (Improper power supply in the shelf for NetApp device) appear on the console.

How can a QRadar administrator generate the alert whenever error message appear on the QRadar console?

A. Offenses > Rules > Actions > New Event Rule

B. Offenses > Rules > Click on Rule Wizard Button

C. Admin Tab > Rule Management > New Event Rule

D. Admin Tab > Rule Management > Actions > New Event Rule

Correct Answer: A

QUESTION 2

What should the format of a CSV file be while importing assets on the QRadar console?

A. ip,portweight,description

B. ip,name,weightmagnitude

C. ip.name.weight.description

D. ip.name.severity.description

Correct Answer: C

QUESTION 3

A flow is sequence of packets that have which common characteristics?

A. Same source, MAC address, flow source and destination IP address

B. Same source IP address, flow source and transport layer port information

C. Same source and destination IP address and transport layer port information

D. Same destination IP address, source bytes and transport layer port information

Correct Answer: D

QUESTION 4

Which line color inside the deployment editor signals that encrypted communication has been selected for the managed hosts in a distributed environment?

A. Red

B. Blue

C. Black

D. Green

Correct Answer: D

QUESTION 5

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

[C2150-400 Study Guide](#)   [C2150-400 Exam Questions](#)   [C2150-400 Braindumps](#)