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.pass2lead.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 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 2

What is used to define the server types in the server discovery screen?

A. Ports

B. Hostname

C. Mac address

D. IP addresses

Correct Answer: A

QUESTION 3

In QRadar SIEM, customer wants to tune one of the firewall deny event which shows firewall deny for all events coming from a Syslog Server and has been identified as false positive. The customer clicked on the "false positive" button to tune the specific event.

What are the traffic directions that will be available during declaring this event as a false positive? (Choose two.)

A. SourceIP to Local Network

B. SourceIP to Any Destination

C. Any source to Any Destination

D. Destination IP to Local Network

E. Source IP to Destination Network

Correct Answer: BE

QUESTION 4

There are unknown log records from unsupported security device events in the Log activity tab. You are planning to write an LSX for an unsupported security device type based on UDSM.

What is the file format and payload option for exporting the unknown log records?

A. PDF and full export

B. CSV and full export

C. XML and visible column

D. CSV and visible column

Correct Answer: C

QUESTION 5

Which statement is true with regard to auto discovery functionality?

A. All supported DSMs are auto discovered.

B. Only 50 Log Sources can be auto discovered.

C. Auto discovered log sources are assigned to a generic log source group.

D. QRadar license key defines the maximum number of log sources that can be auto discovered.

Correct Answer: C