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.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

Given the network IP range of 192.168.160.1 to 192.168.160.127, what format would this be entered into a network hierarchy object?

A. 192.168.160.128/24

B. 192.168.160.0/24

C. 192.168.160.0/23

D. 192.168.160.0/25

Correct Answer: B

QUESTION 2

What does Server discovery allow the QRadar administrator to do?

A. Discover

B. Define rules for hosts

C. Create host searches

D. Populate host definition building blocks

Correct Answer: A

QUESTION 3

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

QUESTION 4

Which Security Profile Permission Precedence should be applied so the users of that profile can only see the flows related to the "Windows Servers" network?

A. Network Only

B. No Restrictions

C. Log Sources Only

D. Network AND Log Source

Correct Answer: D

QUESTION 5

Assuming a Squid Proxy has logs in the following format:

time elapsed remotehost code/status bytes method URL rfc931 peerstatus/peerhost type And these are some sample logs from Squid server:

1286536310.075 452 192.168.0.227 TCP_MISS/200 5067 GET http://www.test.com/vi/VfnuY/default.jpgDIRECT/10.20.153.118 image/jpeg 1286536310.524 935 192.168.0.68 TCP_MISS/200 1021 POST http://www.test.com/services DIRECT/172.16.41.128 application/xml 1286536310.550 495 192.168.0.227 TCP_MISS/204 406 GET http://test.com/get_video? DIRECT/10.12.231.1.136 text/html 1153239176.287 632 172.16.10.92 TCP_IMS_HIT/304 215 GET http:// www.test.com/index.html - NONE/-text/html

Which regular expression would you use to pull out the bytes field into custom property?

A. \w+/\d+\s+(\d+)\s+(POST|GET)

B. \w+/\d+\S+(\d+)\S+(POST|GET)

C. \w+/\d+\s+(\d+)\s+^(POST|GET)

D. \W+/\D+\D+(\D+)\D+(POST|GET)

Correct Answer: D