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.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

Which Log Source Type should be used to add a Log Source with Log Source Extension?

A. Any

B. Custom

C. Universal DSM

D. Log Source Extension

Correct Answer: D

QUESTION 2

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

QUESTION 3

Which three graph types are available for QRadar Log Manager reports? (Choose three.)

A. Pie graph

B. Histogram

C. Bar graph

D. Trivial graph

E. Stacked bar graph

F. Stacked table graph

Correct Answer: ACF

QUESTION 4

Which directory from the QRadar host can be moved to offboard storage?

A. A/ar

B. /store

C. /home

D. /media

Correct Answer: B

QUESTION 5

Which view option allows you to view events as they occur?

A. Automatic

B. Live Events

C. Real Time (streaming)

D. Last Interval (auto refresh)

Correct Answer: C