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.geekcert.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 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 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 a Squid server:

```
1286536310.075    452 192.168.0.227 TCP_MISS/200 5067 GET http://www.test.com/vi/TeYOZBVfnuY
/default.jpg - DIRECT/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://www.test.com/get_video? -
DIRECT/10.12.231.136 text/html
1153239176.287    632 172.16.10.98 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 a custom property?

A. \w+/\d+\s+(\d+)\s+

B. \w+/\d+\s+(\d+)\S+

C. \w+/\d+\S+(\d+)\s+

D. \w+/\D+\s+(\D+)\s+

Correct Answer: A

QUESTION 3

What are the two support formats for exporting an Assets list from QRadar console? (Choose two.)

A. XML

B. RTF

C. PDF

D. CSV

E. HTML

Correct Answer: AE

QUESTION 4

You notice the following message in the System Notification Widget on the Dashboard:

"Unable to automatically detect the associated log source for IP address."

When you hover over the message, you see this pop-up message:

Payload: Apr 11 01:00:01 127.0.0.1 [[type=com.eventgnosis.system.ThreadedEventProcessor] [parent=red6.color.inc:ecs0/EC/TrafficAnalysis1/TrafficAnalysis]] com.q1labs.semsources.filters.trafficanalysis.TrafficAnalysisFilter: [WARN] [NOT:0070014101] [172.16.77.25/- -] [-/- -]Unable to determine associated log source for IP address <192.168.2.90>. Unable to automatically detect the associated log source for IP address.

What is the issue?

A. There are events coming from IP 127.0.0.1 that cannot be autodiscovered and a Log Source Created

B. There are events coming from IP 192.168.2.90 that cannot be autodiscovered and a Log Source Created

C. There are events coming from IP 172.16.77.25 that cannot be autodiscovered and a Log Source Created

D. There are events coming from hostname red6.color.com that cannot be autodiscovered and a Log Source Created

Correct Answer: C

QUESTION 5

What is used to collect netflow and jflow traffic in a QRadar Distributed Deployment?

A. QRadar 3124 Console

B. QRadar 1624 Processor

C. QRadar 1724 Processor

D. QRadar 700 Risk Manager

Correct Answer: A