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

A QRadar SIEM administrator wants to create a Flow Rule that includes a building block definition (BB) that includes applications that indicate communication with file sharing sites. In which group will the administrator find this specified building block?

A. Policy

B. Host Definitions

C. Network Definition

D. Category Definitions

Correct Answer: B

QUESTION 2

Which two ways does QRadar Vulnerability Manager (QVM) provide examine vulnerability data? (Choose two.)

A. VA Scanner

B. Scan Results

C. Custom Event Rules

D. Manage Vulnerabilities

E. Audit Logs and Audit Events

Correct Answer: BC

QUESTION 3

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 4

Which scanners report vulnerabilities on all ports? (Choose two.)

A. Axis

B. NMap

C. Qualys

D. tcpdump

E. nCircle IP360

Correct Answer: BC

QUESTION 5

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