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.certbus.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

What is used to collect security events in a QRadar Distributed Deployment?

A. QRadar 3124 Console

B. QRadar 1724 Processor

C. QRadar 1624 Processor

D. QRadar 1310 QFlow Collector

Correct Answer: D

QUESTION 2

A QRadar administrator needs to tune the system by enabling or disabling the appropriate rules in order to ensure that the QRadar console generates meaningful offenses for the environment. Which role permission is required for enabling and disabling the rule?

A. Offenses > Maintain CRE Rules

B. Offenses > Toggle Custom Rules

C. Offenses > Manage Custom Rules

D. Offenses > Maintain Custom Rules

Correct Answer: C

QUESTION 3

Which string creates a network hierarchy group called WebServers inside a group called DMZ?

A. DMZ/WebServers

B. DMZ_WebServers

C. DMZWebServers

D. DMZ+WebServers

Correct Answer: A

QUESTION 4

Which two formats can reports be generated in? (Choose two.)

A. JPEG image (JPG)

B. Comma Separated Values (CSV)

C. Microsoft Word Document (DOC)

D. Hypertext Markup Language (HTML)

E. Adobe Portable Document Format (PDF)

Correct Answer: DE

QUESTION 5

Which two primary data sources send updates to the Asset profiler? (Choose two.)

A. Source IP

B. Source Port

C. Scan Result

D. Destination IP

E. Identity Events

Correct Answer: AB

QUESTION 6

How many days does QRadar keep record of Closed Offense by default?

A. 1 day

B. 5 days

C. 3 days

D. 7 days

Correct Answer: C

QUESTION 7

What does the message in the System Notification Widget on the Dashboard "Disk sentry: System disk usage back to normal levels." tell you?

A. One of your File Systems has been reduced to below 92%.

B. One of your File Systems has been reduced to below 95%.

C. One of your File Systems has been reduced to below 98%.

D. One of your File Systems has been reduced to below 90%.

Correct Answer: A

QUESTION 8

Which network monitoring port does Juniper Jflow require to be configured in QRadar?

A. Port 80

B. Port 443

C. Port 1080

D. Port 2055

Correct Answer: D

QUESTION 9

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 10

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 11

A customer is observing the Asset tab on the QRadar console and is getting duplicate assets in the console.

What is the reason for this asset duplication?

A. There are multiple heterogeneous assets present in environment.

B. There are multiple assets having same configuration details present in environment.

C. QRadar creates duplicate assets after a specific periodic interval without considering asset activity or inactivity.

D. Asset doesn\\'t appear in network for specific time period; when it came back QRadar detects it and

created a new asset for the same.

Correct Answer: C

QUESTION 12

Where does the information about total number of Assets and Vulnerability processed appear?

A. Asset table in Assets tab

B. VA Scanner Configuration screen

C. Vulnerabilities Tab > Scan Result

D. Mouse Ober popup on Schedule Scan Status field

Correct Answer: C

QUESTION 13

Which statement is correct for patching an HAed server?

A. If the Secondary host is in an Active state, the patch should be applied to the Secondary.

B. The patch should be applied to the Primary first and the patch should be applied to the Secondary.

C. Remove Secondary, then apply the patch on Primary, and then add the Secondary again.

D. Run the patch on the Primary and the Secondary will be updated Automatically.

Correct Answer: B

QUESTION 14

How frequently does the Automated Update Process run if Configuration files are updated on Primary and then Deploy

Changes is not performed, and the updates are made on the Secondary host through an Automated Update Process?

A. Every 10 minutes

B. Every 15 minutes

C. Every 30 minutes

D. Every 60 minutes

Correct Answer: D

QUESTION 15

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