C2150-624 Q&As

IBM Security QRadar Risk Manager V7.2.6 Administration

Pass IBM C2150-624 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/c2150-624.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IBM Official Exam Center

QUESTION 1

When upgrading IBM Security QRadar SIEM V7.2.8, the upgrade file needs to be made accessible to the

operating system.

Which command will accomplish this task?

A. mount -o loop -t iso9660 .iso /media/updates/

B. mount -o loop -t squashfs.sfs /media/updates/

C. umount -o loop -t iso9660 .iso /media/updates/

D. umount -o loop -t squashfs.sfs /media/updates/

Correct Answer: B

QUESTION 2

What are three protocols that collect flow data from network devices, such as routers, and send this data to IBM Security QRadar SIEM V7.2.8?

A. NetFlow, J-Flow and sFlow

B. NetFlow, IPFIX and syslog

C. NetFlow, rsyslog and sFlow

D. NetFlow, Packeteer and syslog

Correct Answer: A

NetFlow, J-Flow, and sFlow are protocols that collect flow data from network devices, such as routers, and send this data to QRadar.

QUESTION 3

A retention policy allows an IBM Security QRadar SIEM V7.2.8 Administrator to define how long the system is required to keep certain types of data and what to do when data reaches a certain age. If a 3month retention policy is defined for all events, then the system will not delete event data until it\\'s on disk timestamp is 3 months in the past. Which two choices are available in the `delete data in this bucket\\'? (Choose two.)

A. When the index is full

B. Upon reboot of the system

C. When storage space is required

D. When performance is heavily affected

E. Immediately after retention period has expired

Correct Answer: CE

From the list box, select a deletion policy. Options include: ?When storage space is required - Select this option if you want events or flows that match the Keep data placed in this bucket for parameter to remain in storage until the disk monitoring system detects that storage is required. If used disk space reaches 85% for records and 83% for payloads, data will be deleted. Deletion continues until the used disk space reaches 82% for records and 81% for payloads. When storage is required, only events or flows that match the Keep data placed in this bucket for parameter are deleted. Immediately after the retention period has expired ?Select this option if you want events to be deleted immediately on matching the Keep data placed in this bucket for parameter. The events or flows are deleted at the next scheduled disk maintenance process, regardless of free disk space or compression requirements.

QUESTION 4

What are the four categories of notifications found in IBM Security QRadar SIEM V7.2.8 system notifications?

A. Errors, Critical, Minor and Information

B. Errors, Warning, Information, and Health

C. Warning, Information, System and Critical

D. Errors, Warning, Information, and Performance

Correct Answer: B

QUESTION 5

What key point should be understood about how flow information in IBM Security QRadar SIEM V7.2.8 is used?

A. Flow information generates the response that is configured in the custom rule.

B. Flow information is sent to QRadarQFlow Collector which normalizes raw log source events.

C. Flow information is actively gathered from the QRadar Event Collector and provides views, reports and alerts to the administrator.

D. Flow information is used to detect threats and other suspicious activity that might be missed if only event information were tracked.

Correct Answer: D