Vendor:IBM

Exam Code:C2150-624

Exam Name:IBM Security QRadar Risk Manager V7.2.6 Administration

Version: Demo

QUESTION 1

An Administrator using IBM Security QRadar SIEM V7.2.8 needs to force an instant backup to run. Which option should be selected?

A. Backup Now

B. On Demand Backup

C. Launch On Demand Backup

D. Configure On Demand Backup

Correct Answer: D

QUESTION 2

An IBM Security QRadar SIEM V7.2.8 Administrator notices a specific MAC address added to the Asset

Reconciliation Domain MAC was blacklisted.

What scenario is causing this to occur?

A. When a MAC address is associated to three or more different IP addresses in 2 hours or less.

B. When an IPv4 address is associated to three or more different MAC addresses in 2 hours or less.

C. When a MAC address is associated to three or more different IP addresses in 10 minutes or less.

D. When an IPv4 address is associated to three or more different MAC addresses in 10 minutes or less.

Correct Answer: A

QUESTION 3

When replacing a Console appliance in an IBM Security QRadar SIEM V7.2.8 deployment using a new IP address or host name, what must be the same on the two Console appliances?

A. The amount of storage must be the same.

B. The Basic and Upgrade license must be the same.

C. The software versions of both appliances must match.

D. The Network Configuration and Protocol must be the same.

Correct Answer: C

The software version of the new Console appliance must match the software version of the old Console appliance. QRadar does not allow appliances at different software versions in the deployment. Administrators might be required to reinstall an ISO for the appliance to downgrade or use a Fix Pack (SFS) to upgrade on the new appliance. The paperwork that came with your appliance lists the installed software version.

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

An Administrator has begun configuring the network hierarchy for a customers deployment of IBM Security

QRadar SIEM V7.2.8 and has already configured groups for network devices and network management

devices, non-routable internal address space, DMZ and VPN.

Which additional item could be considered for configuration within the network hierarchy?

A. VoIP

B. Root DNS Servers

C. External trusted FQDNs D. Routable external address spaces

Correct Answer: B

QUESTION 6

An Administrator working with IBM Security QRadar SIEM V7.2.8 is modifying the network hierarchy to

contain a few new subnets contained with the 192.0.0.0/26 range.

What is a valid host range contained in this range?

A. 192.0.0.1 -> 192.0.0.62

B. 192.0.0.1 -> 192.0.0.65

C. 192.0.0.128 -> 192.0.0.192

D. 192.0.0.192 -> 192.0.0.254

Correct Answer: A

QUESTION 7

An Administrator working with a IBM Security QRadar SIEM V7.2.8 deployment needs to build an Ariel

Query to find all events data received in the last 24 hours where the magnitude of the events is larger than

1 but smaller than 5.

What Query needs to be used?

A. SELECT * FROM events WHERE magnitude > 1 AND

B. SELECT * FROM events WHERE magnitude BETWEEN 1 AND 5 LAST 1 DAYS

C. SELECT * FROM eventstable WHERE magnitude BETWEEN 1 and 5 LAST 1 DAYS

D. SELECT * FROM eventstable WHERE magnitude BETWEEN 1 AND 5 LAST 1 DAYS

Correct Answer: A

QUESTION 8

An Administrator needs to see Events per Second (EPS) and Flows per Minute (FPM) coming to IBM Security QRadar SIEM V7.2.8 through a dashboard. How could this be accomplished?

A. Download the dashboard from IBM Security App Exchange.

B. Go to CLI and run the script /opt/qradar/bin/createdashboard.sh

C. Select any dashboard and customize it. Add a system summary item.

D. Create a new dashboard and then go to admin tab. Add item into the dashboard created.

Correct Answer: D

To determine the average EPS rate, users can click the Dashboard tab, then select the System Monitoring dashboard item. This dashboard contains and event per second and flows per minute dashboard item. To see EPS details, click the View in Log Activity link. This will give an estimate of the data size for events per day.

QUESTION 9

An Administrator is tasked with installing additional log sources into an IBM Security QRadar SIEM V7.2.8

deployment, bringing the total number of log source to 900. The deployment is using the default license

and the Administrator is getting an error attempting to add these additional log sources.

Why is this error happening?

A. The default license only allows 250 log sources.

B. The default license only allows 500 log sources.

C. The default license only allows 750 log sources.

D. The default license only allows 800 log sources.

Correct Answer: C

QUESTION 10

The event pipeline for processing event data before viewing and using event data on the IBM Security QRadar SIEM V7.2.8 console consists of many components, what is one component?

A. Indexing Component

B. Flow Data Component

C. Magistrate Component

D. Event Data Component

Correct Answer: C

QUESTION 11

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

QUESTION 12

An Administrator working with IBM Security QRadar SIEM V7.2.8 is constantly receiving the following

message:

"MPC: Unable to process offense. The maximum number of offenses has been reached."

What is the reason for this message?

A. The Multi Packet Capturer cannot handle more than 2500 attacks at the same time.

B. The Magistrate Processor Core has more than 2500 active Offenses or 100000 overall Offenses.

C. The Multi Packet Capturer cannot handle more than 500 offense reports at a certain point in time.

D. The Magistrate Processor Core has reached its maximum amount of network connections at a certain time.

Correct Answer: B