C2150-400$^{Q\&As}$

IBM Security Qradar SIEM Implementation v 7.2.1

QUESTION 1

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 2

You have been asked to forward all event logs from QRadar to another central syslog server with the IP of

172.16.77.133. You also want the events to be processed by the CRE, but not stored on the system.

What will allow you to do this process?

A. Add a Routing Rule that under Current Filters "Matches All Incoming Events", under Routing Options, add a Forwarding destination for 172.16.77.133 with the "Raw Event" format. Then select the \\'Forward\\' and \\'Drop\\' options. Save and deploy.

B. Add a Routing Rule that, under Current Filters "Matches All Incoming Events", under Routing Options, add a Forwarding destination for 172.16.77.133 with the "Normalized Event" format. Then select the \\'Forward\\' and \\'Drop\\' options. Save and deploy.

C. Add a forwarding Destination for 172.16.77.133 with the "Raw Event" format. Then add a Routing Rule that, under Current Filters "Matches All Incoming Events", under Routing Options, select the Forward destination that matches destination you created. Then select the \\'Forward\\' and \\'Drop\\' options. Save and deploy.

D. Add a forwarding Destination for 172.16.77.133 with the "Normalized Event" format. Then add a Routing Rule that, under Current Filters "Matches All Incoming Events", under Routing Options, select the Forward destination that matches destination you created. Then select the \\'Forward* and \\'Drop* options. Save and deploy.

Correct Answer: A

QUESTION 3

What indicates if an offense is flagged for follow-up?

A. A flag in the Flag column

B. Follow-up System Notification

C. Follow-up email notification from that offense

D. A flag in Offense Note indicating follow-up required

Correct Answer: D

QUESTION 4

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 5

Which line color inside the deployment editor signals that encrypted communication has been selected for the managed hosts in a distributed environment?

A. Blue

B. Grey

C. Black

D. Yellow

Correct Answer: D

QUESTION 6

Which configuration window defines the maximum number of TCP syslog connections?

A. Log Sources

B. System Setting

C. Console Setting

D. Deployment Editor

Correct Answer: D

QUESTION 7

What does the message in the System Notification Widget on the Dashboard "Disk Sentry: Disk Usage exceeded max threshold" tell you?

A. One of your Files Systems has exceeded 92%.

B. One of your Files Systems has exceeded 95%.

C. One of your Files Systems has exceeded 98%

D. One of your Files Systems has exceeded 90%.

Correct Answer: B

QUESTION 8

Given QRadar network hierarchy defined as 9.182.160.0/23 for the CIDR network 9.182.160.0, what is the customer\\'s network IP range?

A. 9.182.160.0 - 9.182.161.255

B. 9.182.160.0 - 9.182.160.255

C. 9.182.160.1 - 9.182.160.255

D. 9.182.160.1 - 9.182.160.127

Correct Answer: B

QUESTION 9

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 10

Which three messages are displayed in the Next Run Time Column while a QRadar Administrator is manually generating a report? (Choose three.)

A. Generating

B. (x hour(s) x min(s))

C. Generating Queues

D. (x hour(s) x min(s) y sec(s))

E. Queued (position in the queue)

F. Queued in the database column

Correct Answer: BDE

QUESTION 11

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 12

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 13

Which network monitoring port does Cisco NetFlow require to be configured in QRadar?

A. Port 514

B. Port 161

C. Port 2055

D. Port 8080

Correct Answer: C

QUESTION 14

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. XLS and full export

B. CSV and full export

C. XML and visible column

D. PDF and visible column

Correct Answer: C

QUESTION 15

Which text box allows you to search event and flow payloads using a text string?

A. Display

B. Add Filter

C. Quick Filter

D. Save Criteria

Correct Answer: C