IBM

Exam C2150-614

IBM Security QRadar SIEM V7.2.7 Deployment

Verson: Demo

[Total Questions: 10]

Question No : 1

A Deployment Professional working with IBM SecurityQRadar SIEM V7.2.7 is configuring scanners for dynamic scanning and is working with a customer to explain how dynamic scanning works, presenting the following example.

Asset IP: 10.2.2.3

Scanner A CIDR: 10.2.2.0/24

Scanner B CIDR: 10.2.2.3/32

How is this asset scanned when utilizing dynamic scanning?

A. Scanner A would scan this asset as it has the bigger CIDR for accuracy.
B. Scanner B would try the scan first then Scanner A would make an attempt.
C. Scanner B would scan this asset as it has the smaller CIDR for accuracy.
D. Scanner A & B would scan this asset as it is contained within both their CIDRs.

Answer: A

Explanation:

In QRadar Vulnerability Manager you can assign different scanners to network CIDR ranges. During a scan, each asset in the CIDR range that you want to scan is dynamically associated with the correct scanner.

Question No : 2

A client has reached the maximum of 5000 EPS for their 3128 All-in-One appliance. They have just completed an acquisition of a competitor company and would like to get them on-board with collecting events for correlation in QRadar. It has been determined that the newly acquired company has a large number of log sources, and it is estimated that its total EPS will be approx. 22000 EPS.

What will meet the hardware requirements when changing to a distributed environment?

A. 1605 Event Processor
B. 1622 Event Processor
C. 1624 Event Processor

D. 1628 Event Processor

Answer: D

Explanation:

QRadar Event Processor 1628, with a Basic Licence, can process 2500 events per second (EPS), and with Upgraded license it can process 40,000 events per second.

Question No : 3

How can a Deployment Professional fix rules that are not distinguishing between remote and local hosts?

A. Configure the NetFlow
B. Create a Reference Set
C. Configure the VA Scanners
D. Create the Network Hierarchy

Answer: D

Explanation:

IBM Security QRadar uses the network hierarchy to understand your network traffic and provide you with the ability to view activity for your entire deployment.

IBM Security QRadar considers all networks in the network hierarchy as local.

Question No : 4

During a new IBM Security QRadar V7.2.7 deployment, a Deployment Professional is performing a deployment in a client environment where there is no tab or SPAN to take advantage of QRadar's Internal Flow sources.

What could be a valid External flow source for collecting flows?

A. Network card
B. Napatech Card
C. NetFlow protocol

D. SNMP protocol

Answer: C

Explanation:

External flow sources might include the following sources:

NetFlow (QRadar supports NetFlow versions 1, 5, 7, and 9)

IPFIX

sFlow

J-Flow

PacketeerPacketeer

Flowlog file

Question No : 5

A Deployment Professional is alerted that flows between two assets within a local network are communicating at a higher rate than normal between midnight and 2 a.m. The Deployment Professional is asked to determine why this is occurring and decides to create an alert that will send a notification when the communication happens again.

Which action could be used?

A. Run an AQL query
B. Perform Quick search
C. Perform Custom search
D. Create rule to test for events/flows

Answer: D

Explanation:

IBM Security QRadar includes rules that detect a wide range of activities, including excessive firewall denies, multiple failed login attempts, and potential botnet activity. You can also create your own rules to detect unusual activity.

Question No : 6

A Deployment Professional has detected a big spike in a customer's "Malware infection detected" rule that monitors their endpoint anti-virus solution. The spike happened over the weekend, but when the rule was checked, it was not changed. Since Monday morning, the rule has spiked and has not yet stopped generating offenses.

What was added to the customer's QRadar log sources that caused this problem?

A. Proxies
B. Flow Collectors
C. Domain Controllers
D. Guest network in their offices.

Answer: B

Explanation:

Rules perform tests on events, flows, or offenses. If all the conditions of a test are met, the rule generates a response.

QRadar QFlow Collector passively collects traffic flows from your network through span ports or network taps. The IBM Security QRadar QFlow Collector also supports the collection of external flow-based data sources, such as NetFlow.

References:
http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/shc_qradar_comps.html
http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/c_qradar_gs_rules.html

Question No : 7

A Deployment Professional needs to handle event logs from Point-of-Sale (POS) devices on cruise ships which have sporadic connectivity to the rest of the deployment.

Which appliance can be used to store and forward these events?

A. QRadar Flow Collector 1201
B. QRadar Flow Processor 1705
C. QRadar Event Processor 1628
D. QRadar Event Collector 1501

Answer: D

Explanation:

The IBM Security QRadar Event Collector 1501 (MTM 4380-Q2C) appliance is a dedicated event collector. By default, a dedicated event collector collects and parses event from various log sources and continuously forwards these events to an event processor. You can configure the QRadar Event Collector 1501 appliance to temporarily store events and only forward the stored events on a schedule.

Question No : 8

A Deployment Professional is asked to help create a virtual QRadar SIEM deployment containing a dedicated IBM Security QRadar Console, IBM Security QRadar Risk Manager, and 1 each of IBM Security QRadar SIEM Event and Flow Processors. It needs to handle 20,000 EPS/ 300,000 FPM.

What are the total minimum specs (CPU/RAM) to accomplish this goal?

A. 28 processors and 72GB RAM
B. 32 processors and 56GB RAM
C. 36 processors and 32GB RAM
D. 40 processors and 192GB RAM

Answer: D

Explanation:

xx28 collectors and processors use 28 processors and 128 GB of RAM.

xx05 collectors and processors use 12 processors and 64 GB of RAM.

Pair xx28 collectors and processors with the QRadar 3128 (Console) to increase performance.

Note: The IBM Security QRadar 3128 with an upgrade license has the capacity of 300,000 FPM and 15,000 EPS.

References:
http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.8/com.ibm.qradar.doc/c_qradar_comps2_deployment_guide.html

Question No : 9

A System Notification on a QRadar Console states “An allocated license has expired and is no longer valid”. After an investigation, the Deployment Professional notices that the X-Force feed license has expired.

How will this expiration affect the system?

A. QRadar will work normally, but X-Force feed will not be updated anymore.
B. QRadar will work normally because the expired feature license has no effect.
C. QRadar will not collect any events until the license has been renewed or removed.
D. QRadar will collect events normally, but events are not correlated with X-Force feed.

Answer: A

Explanation:

If the X-Force license expires on the QRadar Console, the IP reputation and URL databases will no longer receive updates and rules will leverage the existing values provided from the last good content update.

References: http://www-01.ibm.com/support/docview.wss?uid=swg21701213#expires

Question No : 10

Which two permissions are required to modify custom properties? (Choose two.)

A. Maintain Custom Rules
B. Normalized Event Properties
C. User Defined Flow Properties
D. User Defined Event Properties
E. Normalized Flow Properties

Answer: C,D

Explanation:

To create custom properties if you have the correct permission.
You must have the User Defined Event Properties or the User Defined Flow Properties permission.

References:
http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.3/com.ibm.qradar.doc_7.2.3/c_qradar_req_perm_cus_prop.html