IBM

C2150-614
IBM Security QRadar SIEM V7.2.7 Deployment

Question: 1

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: 2

A Deployment Professional is asked to schedule the forwarding of events when the network is quiet, usually around 2 to 3 a.m. console time. The customer states that there is no restriction to bandwidth on the available 1 Gbp/s WAM connection during this time.
Which value should be used for the forward transfer rate?

A. 0
B. 1
C. 1,000,000
D. 10,000,000

Answer: A

Explanation:
For the forward transfer rate, a value of 0 means that the transfer rate is unlimited.
References: http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/t_qradar_adm_create_store_fwd_sch.html

Question: 3

A Deployment Professional working with IBM Security QRadar SIEM V7.2.7 is noticing system notifications relating to performance degradation of the CRE relating to expensive rules. Upon locating the rules that are being expensive they need to be modified to no longer trigger this notification.
What are three causes for a rule to become expensive? (Choose three.)

A. Containing payload matches tests
B. Rule consisting of a large scope
C. Containing payload contains tests
D. Rule consisting of a narrow scope
E. Utilizing non-standard regular expressions
F. Utilizing non-optimized regular expressions

Answer: B,C,F

Explanation:
A user can create a custom rule that has a large scope, uses a regex pattern that is not efficient, includes Payload contains tests, or combines the rule with regular expressions. When this custom rule is used, it negatively impacts performance, which can cause events to be incorrectly routed directly to storage. Events are indexed and normalized but they don't trigger alerts or offenses.
References: http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/38750120.html

Question: 4

A Deployment Professional is working with IBM Security QRadar SIEM V7.2.7. for a new customer that is trying to create their network hierarchy. The customer currently has more than the maximum of 1,000 network objects and CIDR ranges. A few of the CIDRs of the customer are:
Which supernet should be used to shrink the amount of network objects for the supplied group of CIDRs?

A. 209.60.128.0/22
B. 209.60.129.0/23
C. C. 209.60.128.0/23
D. D. 209.60.127.0/27

Answer: C

Explanation:
Supernetting, also called Classless Inter-Domain Routing (CIDR), is a way to aggregate multiple Internet addresses of the same class.
Using supernetting, the network address 209.60.128.0/24 and an adjacent address 209.60.129.0/24 can be merged into 209.60.128.0/23. The "23" at the end of the address says that the first 23 bits are the network part of the address, leaving the remaining nine bits for specific host addresses.
References: http://searchnetworking.techtarget.com/definition/supernetting

Question: 5

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: 6

A customer has existing complex network infrastructure with many redundant links and the IP packets are taking different paths for inbound and outbound traffic. A Deployment Professional needs to configure SFlow.
What should be configured in IBM Security QRadar SIEM V7.2.7 to support this specific case?

A. Enable flow forwarding
B. Disable flow forwarding
C. Enable asymmetric flows
D. Disable symmetric flows

Answer: C

Explanation:
In some networks, traffic is configured to take alternate paths for inbound and outbound traffic. This routing is called asymmetric routing.

However, if you want to combine flows from multiple QRadar QFlow Collector components, you must configure flow sources in the Asymmetric Flow Source Interface(s) parameter in the QRadar QFlow Collector configuration.
The Yes option enables the QRadar QFlow Collector to recombine asymmetric flows.
The No option prevents the QRadar QFlow Collector from recombining asymmetric flows.
References: http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/t_qradar_adm_config_qflow_col.html

For More Information – **Visit link below:**

http://www.testsexpert.com/

Features:

- Money Back Guarantee……..……...…. 

- 100% Course Coverage…… 

- 90 Days Free Updates…… 

- Instant Email Delivery after Order…… 

We Accept

PayPal™