C2150-612$^{\text{Q\&As}}$

IBM Security QRadar SIEM V7.2.6 Associate Analyst

QUESTION 1

Which feature of a Next Generation Firewall is not available on previous firewalls?

A. VPN Support

B. Layer 3 based firewall rules

C. Integrated signature based IPS engine

D. Network and Port-Address Translation (NAT)

Correct Answer: C

QUESTION 2

When reviewing Network Activity, a flow shows a communication between a local server on port 443, and a random, remote port. The bytes from the local destination host are 2 GB, and the bytes from the remote, source host address are 40KB.

What is the flow bias of this session?

A. Other

B. Mostly in

C. Near-same D. Mostly out

Correct Answer: D

QUESTION 3

Which two high level Event Categories are used by QRadar? (Choose two.)

A. Policy

B. Direction

C. Localization

D. Justification

E. Authentication

Correct Answer: AE

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_adm_h_level_evt_categories.html

QUESTION 4

In a distributed QRadar deployment with multiple Event Collectors, from where can syslog and JDBC log sources collected?

A. Syslog log sources and JDBC log sources may be collected by any Event Collector.

B. One Event Collector must collect ALL syslog events and another Event Collector must collect ALL JDBC events.

C. Syslog log sources and JDBC log sources are always collected by the collector assigned in the log source definition.

D. Syslog log sources may be collected by any Event Collector, but JDBC log sources will always be collected by the collector assigned in the log source definition.

Correct Answer: A

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/ b_siem_deployment.pdf (12)

QUESTION 5

Which approach allows a rule to test for Active Directory (AD) group membership?

A. Import the AD membership information into the Asset Database using AXIS and use an asset rule test

B. Use the build-in LDAP integration to execute a search for each event as it is received by the Event Processor to test for group membership

C. Maintain reference data for the AD group(s) of interest containing lists of usernames and then add rule tests to see if the normalized username is in the reference data

D. Export the AD group membership information to a CSV file and place it in the /store/AD_mapping.csv

file on the console, then use the `is a member of AD group\\' test in the rule

Correct Answer: A