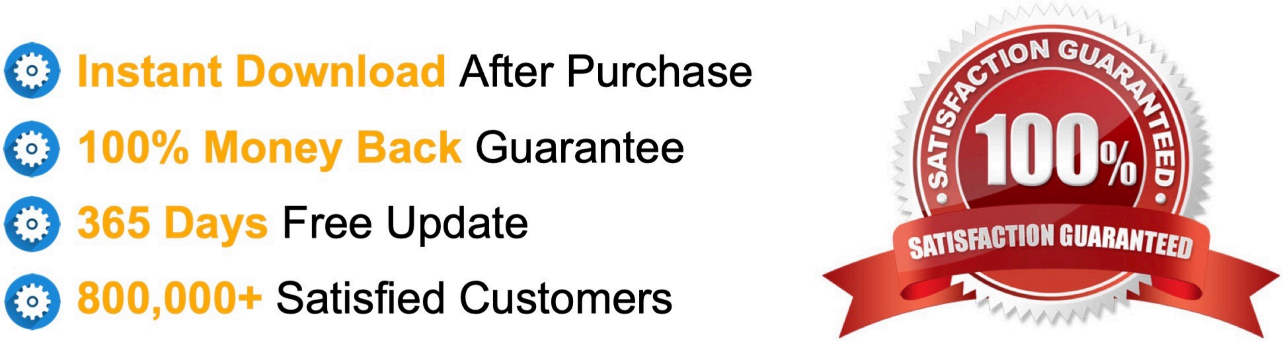
C2150-612^Q&As^

IBM Security QRadar SIEM V7.2.6 Associate Analyst


Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers
SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

Which QRadar component provides the user interface that delivers real-time flow views?

A. QRadar Viewer

B. QRadar Console

C. QRadar Flow Collector

D. QRadar Flow Processor

Correct Answer: B

Reference: http://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.7/com.ibm.qradar.doc/shc_qradar_comps.html

QUESTION 2

What is an effective method to fix an event that is parsed and determined to be unknown or in the wrong QRadar category?

A. Create a DSM extension to extract the category from the payload

B. Create a Custom Property to extract the proper Category from the payload

C. Open the event details, select map event, and assign it to the correct category

D. Write a Custom Rule, and use Rule Response to send a new event in the proper category

Correct Answer: C

Reference: https://www.ibm.com/developerworks/community/forums/html/topic?id=269b4eff-81ad-4ac59f2b-cdeab14a2500

QUESTION 3

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

QUESTION 4

How does a Device Support Module (DSM) function?

A. A DSM is a configuration file that combines received events from multiple log sources and displays them as offenses in QRadar.

B. A DSM is a background service running on the QRadar appliance that reaches out to devices deployed in a network for configuration data.

C. A DSM is a configuration file that parses received events from multiple log sources and converts them to a standard taxonomy format that can be displayed as outputs.

D. A DSM is an installed appliance that parses received events from multiple log sources and converts them to a standard taxonomy format that can be displayed as outputs.

Correct Answer: C

Reference: ftp://public.dhe.ibm.com/software/security/products/qradar/documents/7.3.0/en/ b_qradar_tuning_guide.pdf (32)

QUESTION 5

Which pair of options are available in the left column on the Reports Tab?

A. Reports and Owner

B. Reports and Branding

C. Reports and Report Grouping

D. Reports and Scheduled Reports

Correct Answer: B