C2150-612 Q&As

IBM Security QRadar SIEM V7.2.6 Associate Analyst

Pass IBM C2150-612 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/c2150-612.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IBM Official Exam Center

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

QUESTION 1

Which saved searches can be included on the Dashboard?

A. Event and Flow saved searches

B. Asset and Network saved searches

C. User and Vulnerability saved searches

D. Network Activity and Risk saved searches

Correct Answer: A

QUESTION 2

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

QUESTION 3

Which QRadar add-on component can generate a list of the unencrypted protocols that can communicate from a DMZ to an internal network?

A. QRadar Risk Manager

B. QRadar Flow Collector

C. QRadar Incident Forensics

D. QRadar Vulnerability Manager

Correct Answer: A

QUESTION 4

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 5

Which QRadar rule could detect a possible potential data loss?

A. Apply "Potential data loss" on event of flows which are detected by the local system and when any IP is part of any of the following XForce premium Premium_Malware

B. Apply "Potential data loss" on flows which are detected by the local system and when at least 1000 flows are seen with the same Destination IP and different Source IP in 2 minutes

C. Apply "Potential data loss" on events which are detected by the local system and when the event category for the event is one of the following Authentication and when any of Username are contained in any of Terminated_User

D. Apply "Potential data loss" on flows which are detected by the local system and when the source bytes is greater than 200000 and when at least 5 flows are seen with the same Source IP, Destination IP, Destination Port in 12 minutes

Correct Answer: D

QUESTION 6

What is the maximum number of supported dashboards for a single user?

A. 10

B. 25

C. 255

D. 1023

Correct Answer: C

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

QUESTION 7

A Security Analyst has noticed that an offense has been marked inactive.

How long had the offense been open since it had last been updated with new events or flows?

A. 1 day + 30 minutes

B. 5 days + 30 minutes

C. 10 days + 30 minutes

D. 30 days + 30 minutes

Correct Answer: B

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/com.ibm.qradar.doc/c_qradar_Off_Retention.html

QUESTION 8

Which two are top level options when right clicking on an IP Address within the Offense Summary page? (Choose two.)

A. WHOIS

B. Navigate

C. DNS Lookup

D. Information

E. Asset Summary Page

Correct Answer: BD

QUESTION 9

Which kind of information do log sources provide?

A. User login actions

B. Operating system updates

C. Flows generated by users

D. Router configuration exports.

Correct Answer: A

QUESTION 10

Which log source and protocol combination delivers events to QRadar in real time?

A. Sophos Enterprise console via JDBC

B. McAfee ePolicy Orchestrator via JDBC

C. McAfee ePolicy Orchestrator via SNMP

D. Solaris Basic Security Mode (BSM) via Log File Protocol

Correct Answer: C

QUESTION 11

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 12

What is the definition of asset profile on QRadar?

A. It is any network endpoint that sends or receives data across a network infrastructure.

B. It is all the information that IBM Security QRadar SIEM collected over time about a specific asset.

C. It is the information servers and hosts in a network provide to assist users when resolving security issues.

D. It is an application used to configure and distribute settings to devices and computers in an organization, school, or business.

Correct Answer: B

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.6/com.ibm.qradar.doc/c_qradar_ug_asset_prof_about.html

QUESTION 13

Which two pieces of information can be found under the Log Activity tab? (Choose two.)

A. Offenses

B. Vulnerabilities

C. Firewall events

D. Destination Bytes

E. Internal QRadar messages

Correct Answer: AD

QUESTION 14

Which type of search uses a structured query language to retrieve specified fields from the events, flows, and simarc tables?

A. Add Filter

B. Asset Search

C. Quick Search

D. Advanced Search

Correct Answer: D

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

c_qradar_ug_search_bar.html

QUESTION 15

What are three examples of a custom Dashboard? (Choose three.)

A. Asset View

B. Top Applications

C. Most Recent Offenses

D. Tabs which are accessible

E. Source and Destination DNS

F. Internet Threat Information Center

Correct Answer: CDE