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.passapply.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 advantage of a report helps distinguish it from a search?

A. Scheduling is available.

B. It can be added as a dashboard item.

C. It can be labeled for later use.

D. A report can be assigned to specific users.

Correct Answer: A

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

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 4

What is a benefit of using a span port, mirror port, or network tap as flow sources for QRadar?

A. These sources are marked with a current timestamp.

B. These sources show the ASN number of the remote system.

C. These sources show the username that generated the flow.

D. These sources include payload for layer 7 application analysis.

Correct Answer: D

Reference: https://www.ibm.com/developerworks/community/forums/html/topic?id=dd3861e0-f630-4a53-94c3b426a47b6e02

QUESTION 5

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 6

Which three optional items can be added to the Default and Custom Dashboards without requiring additional licensing? (Choose three.)

A. Offenses

B. Log Activity

C. Risk change

D. Flow Search

E. Risk Monitoring

F. Asset Management

Correct Answer: ABF

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/b_qradar_users_guide.pdf

QUESTION 7

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 8

Which information can be found under the Network Activity tab?

A. Flows

B. Events

C. Reports

D. Offenses

Correct Answer: A

QUESTION 9

Which three log sources are supported by QRadar? (Choose three.)

A. Log files via SFTP

B. Barracuda Web Filter

C. TLS multiline Syslog

D. Oracle Database Listener

E. Sourcefire Defense Center

F. Java Database Connectivity (JDBC)

Correct Answer: DEF

QUESTION 10

Where can a user add a note to an offense in the user interface?

A. Dashboard and Offenses Tab

B. Offenses Tab and Offense Detail Window

C. Offenses Detail Window, Dashboard, and Admin Tab

D. Dashboard, Offenses Tab, and Offense Detail Window

Correct Answer: B

Reference:

IBM Security QRadar SIEM Users Guide. Page: 34

QUESTION 11

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

QUESTION 12

Which key elements does the Report Wizard use to help create a report?

A. Layout, Container, Content

B. Container, Orientation, Layout

C. Report Classification, Time, Date

D. Pagination Option, Orientation, Date

Correct Answer: A

Reference:

IBM Security QRadar SIEM Users Guide. Page: 201

QUESTION 13

A Security Analyst is looking on the Assets Tab at an asset with offenses associated to it.

With a "Right Click" on the IP address, where could the Security Analyst go to obtain all offenses associated with it?

A. Information > Asset Profile

B. Navigate > View by Network

C. Run Vulnerability Scan > Source offenses

D. Navigate > View Source Summary or Destination Summary

Correct Answer: A

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/b_qradar_users_guide.pdf

QUESTION 14

What is the difference between TCP and UDP?

A. They use different port number ranges

B. UDP is connectionless, whereas TCP is connection based

C. TCP is connectionless, whereas UDP is connection based

D. TCP runs on the application layer and UDP uses the Transport layer

Correct Answer: B

QUESTION 15

What are two common uses for a SIEM? (Choose two.)

A. Managing and normalizing log source data

B. Identifying viruses based on payload MD5s

C. Blocking network traffic based on rules matched

D. Enforcing governmental compliance auditing and remediation

E. Performing near real-time analysis and observation of a network and its devices

Correct Answer: AB