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

What is the correct procedure for closing an offense?

A. From the Offenses Tab, select the offense(s), click on Actions, select Close

B. From the Dashboard, select the offense(s) in question, right click and select Close

C. From the Offense Summary Page, click Display and select Close and select the reason

D. From the Offenses Tab, select the offense(s), right click on selection, select Close

Correct Answer: A

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

QUESTION 2

What is indicated by an event on an existing log in QRadar that has a Low Level Category of "Unknown"?

A. That event could not be parsed

B. That event arrived out of order from the original device

C. That event was from a device that is not supported by QRadar

D. That the event was parsed, but not mapped to an existing QRadar category

Correct Answer: D

Reference: https://www.ibm.com/support/knowledgecenter/SSKMKU/com.ibm.dsm.doc/c_DSM_guide_UniversalLEEF_eventmap.html#c_dsm_guide_universalleef_eventmap

QUESTION 3

A mapping of a username to a user\\'s manager can be stored in a Reference Table and output in a search

or a report.

Which mechanism could be used to do this?

A. Quick Search filters can select users based on their manager\\'s name.

B. Reference Table lookup values can be accessed in an advanced search.

C. Reference Table lookup values can be accessed as custom event properties.

D. Reference Table lookup values are automatically used whenever a saved search is run.

Correct Answer: B

QUESTION 4

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

QUESTION 5

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