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.geekcert.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 purpose of coalescing?

A. To reduce the number of events which count against EPS licenses

B. To reduce the amount of data received by QRadar event collectors

C. To reduce the amount of data going through the pipeline and stored onto disk

D. To reduce the number of offenses generated by QRadar as part of the tuning process

Correct Answer: A

Reference: https://developer.ibm.com/answers/questions/438469/out-eps-licence-is-10k-im-attaching-twoscreenshot/

QUESTION 2

What is the default reason for closing an Offense within QRadar?

A. Actioned

B. Non-Issue

C. Blocked Traffic

D. Acceptable Traffic

Correct Answer: B

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.1/com.ibm.qradar.doc_7.2.1/
t_qradar_closing_offenses.html?pos=2

QUESTION 3

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 4

What does the Network Hierarchy provide relating to the "whole picture" that is helpful during an investigation?

A. It allows hosts that are marked to be known to have vulnerabilities to be seen quickly.

B. It allows for the isolation of traffic between the hosts in question for more in depth analysis.

C. It allows for the removal of infected hosts from the network before being added back into the network.

D. It allows for the identification of known hosts on the network versus those that aren\\'t members of the network.

Correct Answer: D

QUESTION 5

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

C2150-612 PDF Dumps   C2150-612 Practice Test   C2150-612 Exam Questions