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 two actions can be performed on the Offense tab? (Choose two.)

A. Adding notes

B. Deleting notes

C. Hiding offenses

D. Deleting offenses

E. Creating offenses

Correct Answer: AC

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

QUESTION 2

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 3

When might a Security Analyst want to review the payload of an event?

A. When immediately after login, the dashboard notifies the analyst of payloads that must be investigated

B. When "Review payload" is added to the offense description automatically by the "System: Notification" rule

C. When the event is associated with an active offense, the payload may contain information that is not normalized or extracted fields

D. When the event is associated with an active offense with a magnitude greater than 5, the payload should be reviewed, otherwise it is not necessary

Correct Answer: C

QUESTION 4

What is the default view when a user first logs in to QRadar?

A. Report Tab

B. Offense Tab

C. Dashboard tab

D. Messages menu

Correct Answer: C

Reference: http://www.ibm.com/support/knowledgecenter/SSKMKU/com.ibm.qradar.doc/c_qradar_dash_tab.html

QUESTION 5

What is the effect of toggling the Global/Local option to Global in a Custom Rule?

A. It allows a rule to compare events and flows in real time.

B. It allows a rule to analyze the geographic location of the event source.

C. It allows rules to be tracked by the central processor for detection by any Event Processor.

D. It allows a rule to inject new events back into the pipeline to affect and update other incoming events.

Correct Answer: C