C2150-612$^{Q\&As}$

IBM Security QRadar SIEM V7.2.6 Associate Analyst

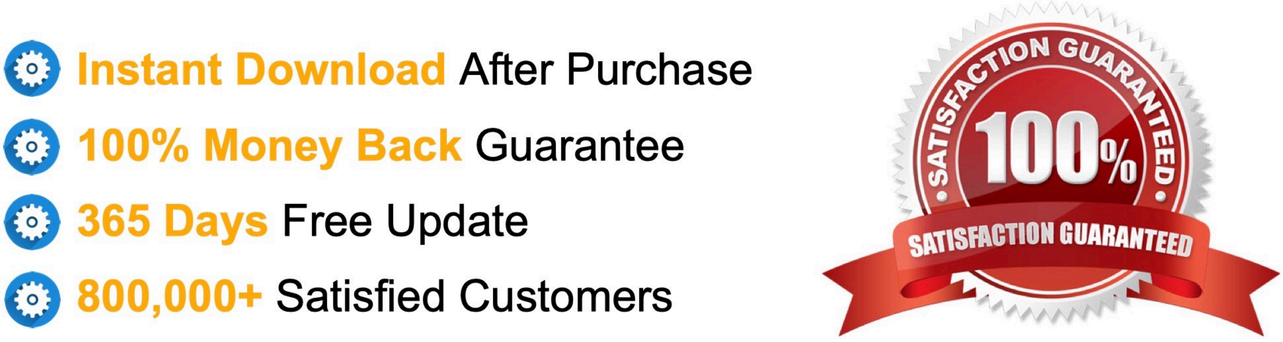
Pass IBM C2150-612 Exam with 100% Guarantee

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
SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

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

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

How is an event magnitude calculated?

A. As the sum of the three properties Severity, Credibility and Relevance of the Event

B. As the sum of the three properties Severity, Credibility and Importance of the Event

C. As a weighted mean of the three properties Severity, Credibility and Relevance of the Event

D. As a weighted mean of the three properties Severity, Credibility and Importance of the Event

Correct Answer: C

QUESTION 4

Which filter in the Log and Network Activity tabs is supported by both flows and events?

A. Source Payload Contains is [Pattern]

B. Application [Indexed] matches [Application]

C. Source ID [Indexed] equals any of [IP Address]

D. Username [Indexed] equals any of [Username]

Correct Answer: B

QUESTION 5

An event is happening regularly and frequently; each event indicates the same target username. There is a rule configured to test for this event which has a rule action to create an offense indexed on the username. What will QRadar do with the triggered rule assuming no offenses exist for the username and no offenses are closed during this time?

A. Each matching event will be tagged with the Rule name, but only one Offense will be created.

B. Each matching event will cause a new Offense to be created and will be tagged with the Rule name.

C. Events will be tagged with the rule name as long as the Rule Response limiter is satisfied. Only one offense will be created.

D. Each matching event will be tagged with the Rule name, and an Offense will be created if the event magnitude is greater than 6.

Correct Answer: C