IBM Certified Analyst C2150-612

IBM Security QRadar SIEM V7.2.6 Associate Analyst

Thank You for Downloading C2150-612 Updated Exam Questions

https://www.theexamcerts.com/ibm/c2150-612-pdf-exam-dumps

Version: 8.0

Question: 1

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

Answer: B

Explanation:
References:
IBM Security QRadar SIEM Users Guide. Page: 34

Question: 2

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

Answer: C

Question: 3

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

Answer: A

Explanation:
References:
IBM Security QRadar SIEM Users Guide. Page: 201

Question: 4

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

Answer: C

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.

Answer: D

Explanation:
References:
https://www.ibm.com/developerworks/community/forums/html/topic?id=dd3861e0-f630-4a53-94c3-b426a47b6e02

Question: 6

What is the primary goal of data categorization and normalization in QRadar?

A. It allows data from different kinds of devices to be compared.
B. It preserves original data allowing for forensic investigations.
C. It allows for users to export data and import it into other system.
D. It allows for full-text indexing of data to improve search performance.

Answer: A

THANK YOU FOR DOWNLOADING C2150-612 UPDATED EXAM QUESTIONS

Note: Thanks Again For Trying The Demo Of Our C2150-612 Exam Product

Visit Our Site to Purchase the Full Set of Actual C2150-612 Exam Questions With Answers.

100% Money Back Guarantee

Click The Link Below

https://www.theexamcerts.com/ibm/c2150-612-pdf-exam-dumps