Testpassport Q&A

La meilleure qualité le meilleur service

http://www.testpassport.fr

Service de mise à jour gratuit pendant un an

Exam : C2150-612

Title : IBM Security QRadar SIEM V7.2.6 Associate Analyst

Version : DEMO

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:
Reference: IBM Security QRadar SIEM Users Guide. Page: 34

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

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:
Reference: IBM Security QRadar SIEM Users Guide. Page: 201

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

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

b426a47b6e02