Question: 1

This functionality provides a simple way to build criteria once, which can be reused in other platform areas.

A. Conditions
B. Favorites
C. Filte Group
D. Filters

Answer: B

Question: 2

To facilitate the remediation of a Vulnerable Item what type of Item is most commonly used?

A. Create a Problem
B. Create a Security Incident
C. Create a KB article
D. Create a Change

Answer: C

Question: 3

After closing the Vulnerable Item (VI), it is recommended to:

A. Update the values in the Vulnerability Score Indicator (VSl) based on the criticality of the Vulnerability.
B. The VI remains active and in place until the Scanner rescans and closes the VI.
C. Mark the CI as exempt from the Vulnerability if the vulnerability was remediated.
D. Compare the Vulnerability with subsequent scans.

Answer: A

Question: 4

Vulnerability Response is a scoped application; which prefix is attached to all items related to the application?

A. cmn_vul
B. vul
C. sn_vul
D. x_vul

Answer: D

Question: 5

Which Vulnerability maturity level provides advanced owner assignment?

A. Enterprise risk trending
B. Automated prioritization
C. Manual operations
D. Improved remediation

Answer: B

Question: 6

Which application provides the opportunity to align security events with organizational controls, automatically appraising other business functions of potential impact?

A. Performance Analytics
B. Event Management
C. Governance. Risk, and Compliance
D. Service Mapping

Answer: C

Question: 7

Ignoring a Vulnerable item:

A. Permanently removes the item from the list of Active Vulnerable items
B. Move the item to the Slushbucket
C. Has no impact on the list of Active Vulnerable Items
D. Temporarily removes the item from the list of Active Vulnerable items

Answer: A

Question: 8

What do Vulnerability Exceptions require?

A. An Approval by default
B. An Exception Workflow
C. A GRC integration
D. A Filter Group

Answer: A