Question 1
Playbooks are permanent, best-practice documents, so a security team should not make changes to them. 1 / 1 point
True
False
Correct
Playbooks are living documents, so a security team will make frequent changes, updates, and improvements to address new threats and vulnerabilities.

Question 2
A business recently experienced a security breach. Security professionals are currently restoring the affected data using a clean backup that was created before the incident. What playbook phase does this scenario describe? 1 / 1 point
Post-incident activity
Detection and analysis
Containment
Eradication and recovery
Correct
This scenario describes eradication and recovery. This phase involves removing the incident's artifacts and restoring the affected environment to a secure state.

Question 3
Fill in the blank: Once a security incident is resolved, security analysts perform various post-incident activities and _____ efforts with the security team. 1 / 1 point
preparation
detection
coordination
eradication
Correct
Once a security incident is resolved, security analysts perform various post-incident activities and coordination efforts with the security team. Coordination involves reporting incidents and sharing information based on established standards.

Question 4
Which action can a security analyst take when they are assessing a SIEM alert? 1 / 1 point
Analyze log data and related metrics
Isolate an infected network system
Restore the affected data with a clean backup
Create a final report
Correct
An action that a security analyst can take when they are assessing a SIEM alert is to analyze log data and related metrics. This helps in identifying why the alert was generated by the SIEM tool and determining if the alert is valid.