Question 1
Which of the following statements accurately describe playbooks? Select three answers. 1 / 1 point

A playbook is an essential tool used in cybersecurity.
Correct
A playbook can be used to respond to an incident
Correct
A playbook improves efficiency when identifying and mitigating an incident.
Correct

A playbook is used to develop compliance regulations.

Question 2
A security team is considering what they learned during past security incidents. They also discuss ways to improve their security posture and refine response strategies for future incidents. What is the security team's goal in this scenario? 1 / 1 point

Educate clients
Assess employee performance
Delete biometric data
Update a playbook

Correct

Question 3
Fill in the blank: Incident response playbooks are _____ used to help mitigate and manage security incidents from beginning to end. 1 / 1 point

inquiries
exercises
examinations
guides
Correct

Question 4
A security analyst wants to ensure an organized response and resolution to a security breach. They share information with key stakeholders based on the organization's established standards. What phase of an incident response playbook does this scenario describe? 1 / 1 point

Coordination
Detection and analysis
Eradication and recovery
Containment
Correct

Question 5
What are the primary goals of the containment phase of an incident response playbook? Select two answers. 1 / 1 point

Assess the damage
Prevent further damage
Correct
Analyze the magnitude of the breach
Reduce the immediate impact
Correct

Question 6
Fill in the blank: During the post-incident activity phase, security teams may conduct a full-scale analysis to determine the _____ of an incident and use what they learn to improve the company's overall security posture. 1 / 1 point

root cause
end point
structure
target
Correct

Question 7
A security analyst documents procedures to be followed in the event of a security breach. They also establish staffing plans and educate employees. What phase of an incident response playbook does this scenario describe? 1 / 1 point

Eradication and recovery
Coordination
Detection and analysis
Preparation
Correct

Question 8
In what ways do SIEM tools and playbooks help security teams respond to an incident? Select all that apply. 1 / 1 point

After receiving a SIEM alert, security teams use playbooks to guide their response process.
Correct
SIEM tools generate alerts.
Correct
SIEM tools collect data.
Correct
Playbooks analyze data to detect threats.