Question 1
In the event of a security incident, when would it be appropriate to refer to an incident response playbook? 1 / 1 point
Only when the incident first occurs
At least one month after the incident is over
Throughout the entire incident
Only prior to the incident occurring
Correct
In the event of a security incident, it is appropriate to refer to an incident response playbook throughout the entire incident. An incident response playbook is a guide with six phases used to help mitigate and manage security incidents from beginning to end.

Question 2
Fill in the blank: During the _____ phase, security professionals use tools and strategies to determine whether a breach has occurred and to evaluate its potential magnitude. 1 / 1 point
containment
detection and analysis
preparation
coordination
Correct
During the detection and analysis phase, security professionals use tools and strategies to determine whether a breach has occurred and to evaluate its potential magnitude.

Question 3
In which incident response playbook phase would a security team document an incident to ensure that their organization is better prepared to handle future security events? 1 / 1 point
Coordination
Post-incident activity
Eradication and recovery
Containment
Correct
In the post-incident activity phase, a security team documents an incident to ensure that their organization is better prepared to handle future incidents.

Question 4
What is the relationship between SIEM tools and playbooks? 1 / 1 point
They work together to predict future threats and eliminate the need for human intervention.
They work together to provide a structured and efficient way of responding to security incidents.
Playbooks detect threats and generate alerts, then SIEM tools provide the security team with a proven strategy.
Playbooks collect and analyze data, then SIEM tools guide the response process.

Correct
SIEM tools and playbooks work together to provide a structured and efficient way of responding to security incidents.