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

- [x] A playbook is an essential tool used in cybersecurity.

Correct

- [ ] A playbook is used to develop compliance regulations.
- [x] A playbook can be used to respond to an incident

Correct

- [x] A playbook improves efficiency when identifying and mitigating an incident.

Correct

2. Fill in the blank: A security team _____ their playbook frequently by learning from past security incidents, then refining policies and procedures. **1 / 1 point**

- (•) updates
- ( ) shortens
- ( ) outlines
- ( ) summarizes

Correct

3. Fill in the blank: Incident response playbooks outline processes for communication and _____ of a security breach. **1 / 1 point**

- ( ) iteration
- (•) documentation
- ( ) concealment
- ( ) implementation

Correct

4. An organization has successfully responded to a security incident. According to their established standards, the organization must share information about the incident to a specific government agency. What phase of an incident response playbook does this scenario describe? **0 / 1 point**

- ( ) Detection and analysis
- (•) Containment
- ( ) Preparation
- ( ) Coordination

Incorrect
Please review the video on the phases of an incident response playbook.

5. Why is the containment phase of an incident response playbook a high priority for organizations? **1 / 1 point**

- ○ It outlines roles and responsibilities of all stakeholders.
- ◉ It helps prevent ongoing risks to critical assets and data.
- ○ It demonstrates how to communicate about the breach to leadership.
- ○ It enables a business to determine whether a breach has occurred.

✓ **Correct**

6. Fill in the blank: During the post-incident activity phase, organizations aim to enhance their overall _____ by determining the incident's root cause and implementing security improvements. **1 / 1 point**

- ○ security audit
- ◉ security posture
- ○ user experience
- ○ employee engagement

✓ **Correct**

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**

- ◉ Preparation
- ○ Coordination
- ○ Eradication and recovery
- ○ Detection and analysis

✓ **Correct**

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

- ☐ Playbooks collect and analyze data.
- ☑ SIEM tools alert the security team to potential problems.

✓ **Correct**

- ☑ SIEM tools detect threats.

✓ **Correct**

- ☑ SIEM tools and playbooks work together to provide a structured way of responding to incidents.

✓ **Correct**