Weekly challenge 4

Congratulations! You passed!

Grade received 100%

Latest Submission Grade 100%

To pass 80% or higher

Quiz • 40 min

Retake the assignment in **23h 56m**

Go to next item

Review Learning Objectives

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

- [x] A playbook improves accuracy when identifying and mitigating an incident.
  - **Correct**
- [x] A playbook helps security teams respond to urgent situations quickly.
  - **Correct**
- [x] Organizations use different types of playbooks for different situations.
  - **Correct**
- [ ] Organizations keep playbooks consistent by applying the same procedures to different business events.

2. What does a security team do when updating and improving a playbook? Select all that apply. **1 / 1 point**

- [x] Refine response strategies for future incidents
  - **Correct**
- [x] Consider learnings from past security incidents
  - **Correct**
- [x] Discuss ways to improve security posture
  - **Correct**
- [ ] Improve antivirus software performance

3. Fill in the blank: Incident response is an organization's quick attempt to _____ an attack, contain the damage, and correct its effects. **1 / 1 point**

- ( ) ignore
- (•) identify
- ( ) disclose
- ( ) expand

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? **1 / 1 point**

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

Correct

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

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

Correct

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

- ( ) eradication and recovery
- ( ) containment
- ( ) detection and analysis
- (•) post-incident activity

Correct

7. A security analyst wants to set the foundation for successful incident response. They outline roles and responsibilities of each security team member. What phase of an incident response playbook does this scenario describe? **1 / 1 point**

- ( ) Containment
- ( ) Detection and analysis
- (•) Preparation
- ( ) Post-incident activity

Correct

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

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

Submit your assignment

Try again

Retake the quiz in **23h 56m**

Receive grade

To Pass 80% or higher

Your grade
100%

View Feedback

We keep your highest score

Like **Dislike** **Report an issue**