Weekly challenge 4

Congratulations! You passed!

Grade received 87.50%

Latest Submission Grade 78.13%

To pass 80% or higher

Quiz • 40 min

Go to next item

Review Learning Objectives

1. Which of the following statements accurately describe playbooks? Select three answers. **0.75 / 1 point**

A playbook improves efficiency when identifying and mitigating an incident.

Correct

A playbook is an essential tool used in cybersecurity.

Correct

A playbook can be used to respond to an incident

Correct

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

A playbook is used to develop compliance regulations.

This should not be selected
Please review the video on the phases of an incident response playbook.

Submit your assignment **Try again**

Due Jun 25, 11:59 PM +08 **Attempts** 3 every 24 hours

Receive grade

To Pass 80% or higher

Your grade 87.50%

View Feedback

We keep your highest score

2. What does a security team do when updating and improving a playbook? Select all that apply. **0.75 / 1 point**

Discuss ways to improve security posture

Correct

Improve antivirus software performance

This should not be selected
Please review the video on using an incident response playbook.

Consider learnings from past security incidents

Correct

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

- (•) guides
- ( ) examinations
- ( ) inquiries
- ( ) exercises

Correct

4. A security analyst reports to stakeholders about a security breach. They provide details based on the organization's established standards. What phase of an incident response playbook does this scenario describe? **0 / 1 point**

- ( ) Coordination
- ( ) Eradication and recovery
- (•) Detection and analysis
- ( ) Preparation

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

5. Which phase of an incident response playbook is primarily concerned with preventing further damage and reducing the immediate impact of a security incident? **1 / 1 point**

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

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**

- ( ) user experience
- (•) security posture
- ( ) security audit
- ( ) employee engagement

Correct

7. A security analyst establishes incident response procedures. They also educate users on what to do in the event of a security incident. What phase of an incident response playbook does this scenario describe? **1 / 1 point**

- ( ) Eradication and recovery
- ( ) Containment
- (•) Preparation
- ( ) Detection and analysis

Correct

8. In what ways do SIEM tools and playbooks help security teams respond to an incident? Select all that apply. **0.75 / 1 point**

SIEM alerts provide security teams with specific steps to identify and respond to security incidents.

This should not be selected
Please review the video on the phases of an incident response playbook.

SIEM alerts inform security teams of potential threats.

Correct

SIEM tools analyze data.

Correct

SIEM tools and playbooks work together to provide an efficient way of handling security incidents.

Correct