Congratulations! You passed!

Grade received 87.50%

Weekly challenge 3

Latest Submission grade 87.50%

To pass 80% or higher

Quiz • 50 min

Review Learning Objectives

Go to next item

1. Which step of the NIST Incident Response Lifecycle involves the investigation and validation of alerts? **1 / 1 point**

- Detection
- Recovery
- Discovery
- Analysis

Correct

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

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

2. An organization is completing its annual compliance audit. The people performing the audit have access to any relevant information, including records and documents. Which documentation benefit does this scenario outline? **1 / 1 point**

- Organization
- Transparency
- Consistency
- Accuracy

Correct

3. What are examples of how transparent documentation can be useful? Select all that apply. **0.75 / 1 point**

- [x] Meeting cybersecurity insurance requirements

Correct

- [x] Defining an organization's security posture

This should not be selected
Please review the video on documentation.

- [x] Providing evidence for legal proceedings

Correct

- [x] Demonstrating compliance with regulatory requirements

Correct

4. A member of the forensics department of an organization receives a computer that requires examination. On which part of the chain of custody form should they sign their name and write the date? **1 / 1 point**

- Evidence movement
- Purpose of transfer
- Description of the evidence
- Custody log

Correct

5. Which of the following does a semi-automated playbook use? Select two. **0.5 / 1 point**

- [x] Threat intelligence

This should not be selected
Please review the video on playbooks.

- [x] Human intervention

Correct

- [x] Automation

Correct

- [x] Crowdsourcing

This should not be selected
Please review the video on playbooks.

6. What are the steps of the triage process in the correct order? **1 / 1 point**

- Receive and assess, collect and analyze, assign priority
- Assign priority, receive and assess, collect and analyze
- Receive and assess, assign priority, collect and analyze
- Collect and analyze, assign priority, receive and assess

Correct

7. What are the steps of the third phase of the NIST Incident Response Lifecycle? Select three answers. **0.75 / 1 point**

- [x] Recovery

Correct

- [x] Eradication

Correct

- [x] Containment

Correct

- [x] Response

This should not be selected
Please review the video on containment, eradication, and recovery.

8. Which step of the NIST Incident Response Lifecycle involves returning affected systems back to normal operations? **1 / 1 point**

- Response
- Eradication
- Recovery
- Containment

Correct

9. Two weeks after an incident involving ransomware, the members of an organization want to review the incident in detail. Which of the following actions should be done during this review? Select all that apply. **0.75 / 1 point**

- [x] Create a final report.

Correct

- [x] Schedule a lessons learned meeting that includes all parties involved with the security incident.

Correct

- [x] Determine the person to blame for the incident.

This should not be selected
Please review the video on post-incident activity.

- [x] Determine how to improve future response processes and procedures.

Correct

10. Which documentation provides a comprehensive review of an incident? **1 / 1 point**

- Lessons learned meeting
- New technology
- Timeline
- Final report

Correct