Congratulations! You passed!

Grade received 100%

Weekly challenge 3

Latest Submission Grade 100%

To pass 80% or higher

Quiz • 50 min

Review Learning Objectives

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

Go to next item

1. In the NIST Incident Response Lifecycle, what is the term used to describe the prompt discovery of security events? **1 / 1 point**

- Detection
- Validation
- Investigation
- Preparation

Correct **To Pass** 80% or higher

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

Try again

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

Receive grade

Your grade 100%

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**

- Transparency
- Organization
- Accuracy
- Consistency

Correct

3. After a ransomware incident, an organization discovers their ransomware playbook needs improvements. A security analyst is tasked with changing the playbook documentation. Which documentation best practice does this scenario highlight? **1 / 1 point**

- Be accurate
- Know your audience
- Be concise
- Update regularly

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**

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

Correct

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

- [ ] Threat intelligence
- [x] Human intervention

Correct

- [x] Automation

Correct

- [ ] Crowdsourcing

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

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

Correct

7. Fill in the blank: Containment is the act of limiting and _____ additional damage caused by an incident. **1 / 1 point**

- preventing
- detecting
- eradicating
- removing

Correct

8. Which of the following is an example of a recovery task? **1 / 1 point**

- Applying a patch to address a server vulnerability
- Disconnecting an infected system from the network
- Reinstalling the operating system of a computer infected by malware
- Monitoring a network for intrusions

Correct

9. What questions can be asked during a lessons learned meeting? Select three answers. **1 / 1 point**

- [x] What could have been done differently?

Correct

- [ ] Which employee is to blame?
- [x] What were the actions taken for recovery?

Correct

- [x] What time did the incident happen?

Correct

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

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

Correct