Weekly challenge 3

Try again once you are ready

Grade received 77.50%
Latest Submission grade 77.50%
To pass 80% or higher
Quiz • 50 min
Try again
Review Learning Objectives

1. A security analyst is investigating an alert involving a possible network intrusion. Which of the following tasks is the security analyst likely to perform as part of the Detection and Analysis phase of the incident response lifecycle? Select two answers. **0.5 / 1 point**

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

- [x] Identify the affected devices by system.
  Correct
- [x] Isolate the affected machine from the network.
  Receive grade
  To Pass 80% or higher
  This should not be selected
  Please review the video on detection and analysis.
- [x] Implement a patch to fix the vulnerability.
  Like **Dislike** **Report an issue**
  This should not be selected
  Please review the video on detection and analysis.
- [x] Collect and analyze the network logs to verify the alert.
  Correct

Your grade 77.50%
View Feedback
We keep your highest score

2. What are the benefits of documentation during incident response? Select three answers. **0.75 / 1 point**

- [x] Transparency
  Correct
- [x] Quality
  This should not be selected
  Please review the video on documentation.
- [x] Clarity
  Correct
- [x] Standardization
  Correct

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

- [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
- [x] Meeting cybersecurity insurance 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**

- ( ) Description of the evidence
- ( ) Evidence movement
- (•) Custody log
- ( ) Purpose of transfer

Correct

5. Which statement best describes the functionality of automated playbooks? **1 / 1 point**

- ( ) They use a combination of flowcharts and manual input to execute tasks and response actions.
- (•) They use automation to execute tasks and response actions.
- ( ) They require the use of human intervention to execute tasks.
- ( ) They require the combination of human intervention and automation to execute tasks.

Correct

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

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

Correct

7. After a security incident involving an exploited vulnerability due to outdated software, a security analyst applies patch updates. Which of the following steps does this task relate to? **0 / 1 point**

- (•) Response
- ( ) Prevention
- ( ) Reimaging
- ( ) Eradication

Incorrect
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**

- (•) Recovery
- ( ) Response
- ( ) Eradication
- ( ) 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 how to improve future response processes and procedures.
  Correct
- [x] Determine the person to blame for the incident.
  This should not be selected
  Please review the video on post-incident activity.

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

- ( ) Lessons learned meeting
- ( ) Timeline
- ( ) New technology
- (•) Final report

Correct