Weekly challenge 2

Quiz • 50 min

Congratulations! You passed!

Grade received 90%
Latest Submission Grade 90%
To pass 80% or higher

Go to next item

Review Learning Objectives

Submit your assignment
Due Jun 14, 11:59 PM +08
Attempts 3 every 24 hours
Try again

Receive grade
Your grade 90%
View Feedback
We keep your highest score

Like Dislike Report an issue

1. Fill in the blank: Incident escalation is the process of _____. **1 / 1 point**

- reporting a security incident to a human resource department for compliance purposes
- properly assessing security events
- identifying a potential security incident , triaging it, and handing it off to a more experienced team member
- creating a visual dashboard that shows security stakeholders the amount of security incidents taking place

Correct
To Pass 80% or higher

2. Which skills will help you identify security incidents that need to be escalated? Select two answers. **0.5 / 1 point**

- [x] Attention to detail

  Correct

- [x] Ability to collaborate well with others

  This should not be selected
  Please review the video on the importance of escalation.

- [x] Excellent communication skills

  This should not be selected
  Please review the video on the importance of escalation.

- [x] Ability to follow an organization's escalation guidelines or processes

  Correct

3. Fill in the blank: Entry-level analysts might need to escalate various incident types, including _____. **1 / 1 point**

- noncompliance of tax laws
- improper usage
- mismanagement of funds
- missing software

Correct

4. Which incident type involves an employee violating an organization's acceptable use policy? **1 / 1 point**

- Improper usage
- Unauthorized access
- Phishing
- Malware infection

Correct

5. You are alerted that a hacker has gained unauthorized access to one of your organization's manufacturing applications. At the same time, an employee's account has been flagged for multiple failed login attempts. Which incident should be escalated first? **1 / 1 point**

- Both security incidents should be escalated at the same time.
- The incident involving the employee who is unable to log in to their account should be escalated first.
- The best thing to do is escalate the incident that your supervisor advised you to escalate first.
- The incident involving the malicious actor who has gained unauthorized access to the manufacturing application should be escalated first.

Correct

6. What is a potential negative consequence of *not* properly escalating a small security incident? Select two answers. **0.5 / 1 point**

- [x] The company can suffer a financial loss.

  Correct

- [x] The company's employee retention percentage can decrease drastically.

  This should not be selected
  Please review the video on going from a simple activity to a major data breach.

- [x] The company's antivirus software can be uninstalled.

  This should not be selected

- [x] The company can suffer a loss in reputation.

  Correct

7. Fill in the blank: An escalation policy is a set of actions that outlines _____. **1 / 1 point**

- how to escalate customer service complaints
- how to handle a security incident alert
- how to manage the security stakeholders of an organization
- how to defend an organization's data and assets

Correct

8. Fill in the blank: _____ is important when following a company's escalation policy to ensure you follow the policy correctly. **1 / 1 point**

- Working remotely
- Attention to detail
- Delegating tasks
- Reading quickly

Correct

9. Fill in the blank: An _____ will help an entry-level analyst to know when and how to escalate a security incident. **1 / 1 point**

- employee security handbook
- escalation policy
- executive security dashboard
- blue team CIRT guideline

Correct

10. Unauthorized access to a system with PII is _____ critical than an employee's account being flagged for multiple failed login attempts. **1 / 1 point**

- more
- less
- equally
- marginally

Correct