Weekly challenge 2

Congratulations! You passed!

Grade received 100%
Latest Submission Grade 100%
To pass 80% or higher
Quiz • 50 min

Go to next item

Review Learning Objectives

1. What security term describes the identification of a potential security event, triaging it, and handing it off to a more experienced team member? **1 / 1 point**

- SOC operations
- Data security protection
- Incident escalation
- Social engineering

Correct

2. Fill in the blank: ____ is a skill that will help you identify security incidents that need to be escalated. **1 / 1 point**

- Linux operations
- Leadership
- Graphics design
- Attention to detail

Correct

3. What elements of security do terms like unauthorized access, malware infections, and improper usage describe? **1 / 1 point**

- Public press releases
- Company job descriptions
- Incident classification types
- Phishing attempts

Correct

4. An employee attempting to access software on their work device for personal use can be an example of what security incident type? **1 / 1 point**

- Social engineering
- Improper usage
- Unauthorized access
- 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**

- 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.
- The incident involving the employee who is unable to log in to their account should be escalated first.
- Both security incidents should be escalated at the same time.

Correct

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

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

Correct

- [ ] The company's employee retention percentage can decrease drastically.
- [x] The company can suffer a loss in reputation.

Correct

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

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

- 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
- how to escalate customer service complaints

Correct

8. Why is it important for analysts to follow a company's escalation policy? Select two answers. **1 / 1 point**

- [ ] An escalation policy can help analysts determine which tools to use to solve an issue.
- [ ] An escalation policy can help analysts determine the best way to cross-collaborate with other members of their organization.
- [x] An escalation policy instructs analysts on the right person to contact during an incident.

Correct

- [x] An escalation policy can help analysts prioritize which security events need to be escalated with more or less urgency.

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**

- escalation policy
- employee security handbook
- 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