Try again once you are ready

Grade received 62.50% • Latest Submission Grade 62.50% • To pass 80% or higher • Try again

Creating a Company Culture for Security

Quiz • 55 min

Submit your assignment Due Jul 2, 11:59 PM +08 Attempts 3 every 24 hours

Resume assignment

1. In the Payment Card Industry Data Security Standard (PCI DSS), what are the requirements for the "regularly monitor and test networks" objective? Select all that apply **0.5 / 1 point**

- [x] Track and monitor all access to network resources and cardholder data

  Correct

- [x] Regularly test security systems and processes

  Correct

- [x] Encrypt the transmission of cardholder data across open public networks

  This should not be selected
  Please review the video about security goals

- [x] Develop and maintain secure systems and applications

  This should not be selected
  Please review the video about security goals

Receive grade
To Pass 80% or higher
Your grade 62.50%
View Feedback
We keep your highest score

2. What is the first step in performing a security risk assessment? **1 / 1 point**

- ( ) Logs analysis
- (•) Threat modeling
- ( ) Penetration testing
- ( ) Vulnerability scanning

Correct

3. Which of the following are examples of security tools that can scan computer systems and networks for vulnerabilities? Select all that apply. **0.75 / 1 point**

- [x] Nessus

  Correct

- [x] Qualys

  Correct

- [x] Wireshark

  This should not be selected
  Please review the video about measuring and assessing risk

- [x] OpenVAS

  Correct

4. Which of the following devices are considered a risk when storing confidential information? **0.5 / 1 point**

Select all that apply.

- [x] CD drives

  Correct

- [x] Encrypted portable hard drives

  This should not be selected
  Please review the video about measuring and assessing risk

- [x] USB sticks

  Correct

- [x] Limited access file shares

  This should not be selected
  Please review the video about measuring and assessing risk

5. Which of the following is recommended to secure authentication? **1 / 1 point**

- ( ) Strong encryption
- (•) 2-factor authentication
- ( ) Password rotation
- ( ) Vulnerability scanning

Correct

6. Which of the following are ways to prevent email phishing attacks against user passwords? Select all that apply. **0.5 / 1 point**

- [x] Cloud email

  This should not be selected
  Please review the video about user habits

- [x] Spam filters

  Correct

- [x] User education

  Correct

- [x] Virtual private network

  This should not be selected
  Please review the video about user habits

7. When contracting services from a third party, what risk is the organization exposed to? **1 / 1 point**

- ( ) DDoS attacks
- ( ) Malware attacks
- ( ) Zero-day vulnerabilities
- (•) Trusting the third party's security

Correct

8. Third-party services that require equipment on-site may require a company to do which of the following? Select all that apply. **0 / 1 point**

- [x] Provide additional monitoring via a firewall or agentless solution

  Correct

- [x] Evaluate hardware in the lab first

  Correct

- [x] Provide remote access to third-party service provider

  Correct

- [x] Unrestricted access to the network

  This should not be selected
  Please review the video about third-party security

9. Periodic mandatory security training courses can be given to employees in what way? Select all that apply. **0.5 / 1 point**

- [x] Short video

  Correct

- [x] One-on-one interviews

  This should not be selected
  Please review the video about security training

- [x] Brief quiz

  Correct

- [x] Interoffice memos

  This should not be selected
  Please review the video about security training

10. What are the first two steps of incident handling and response? **0.5 / 1 point**

- [x] Incident detection

  Correct

- [x] Incident containment

  Correct

- [x] Incident recovery

  This should not be selected
  Please review the video about incident reporting and analysis

- [x] Incident eradication or removal

  This should not be selected
  Please review the video about incident reporting and analysis