Congratulations! You passed!
TO PASS 80% or higher

Keep Learning

GRADE
100%

Creating a Company Culture for Security

LATEST SUBMISSION GRADE
100%

1. Question — 1 / 1 point

What characteristics are used to assess the severity of found vulnerabilities? Check all that apply.

- [x] Remotely exploitable or not
  - Correct: Woohoo! Things to consider when evaluating a vulnerability are how likely it is to be exploited, the type of access an attacker could get, and whether or not the vulnerability is exploitable remotely.
- [x] Type of access gained
  - Correct: Woohoo! Things to consider when evaluating a vulnerability are how likely it is to be exploited, the type of access an attacker could get, and whether or not the vulnerability is exploitable remotely.
- [x] Chance of exploitation
  - Correct: Woohoo! Things to consider when evaluating a vulnerability are how likely it is to be exploited, the type of access an attacker could get, and whether or not the vulnerability is exploitable remotely.
- [ ] Use of encryption or not

Correct
Great, you got all the right answers.

2. Question — 1 / 1 point

What risk are you exposing your organization to when you contract services from a third party?

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

Correct
Yep! You're trusting this third party to have reasonable security in place to protect the data or access you're entrusting them with.

3. Question — 1 / 1 point

What's a quick and effective way of evaluating a third party's security?

- (•) A security assessment questionnaire
- ( ) A comprehensive penetration testing review
- ( ) A manual evaluation of all security systems
- ( ) A signed contract

Correct
You nailed it! A security assessment questionnaire would help you understand how well-defended a third party is, before deciding to do business with them.

4. Question — 1 / 1 point

When handling credit card payments, your organization needs to adhere to the ____.

- ( ) HIPAA
- ( ) ISO
- ( ) IEEE
- (•) PCI DSS

Correct
Great work! When handling credit card payments, your organization needs to adhere to the Payment Card Industry Data Security Standard (PCI DSS).

5. Question — 1 / 1 point

Security risk assessment starts with ____.

- ( ) Payment processing
- (•) Threat modeling
- ( ) Attack impact
- ( ) Outside attackers

Correct
You got it! Security risk assessment starts with threat modeling.

6. Question — 1 / 1 point

Your company wants to establish good privacy practices in the workplace so that employee and customer data is properly protected. Well-established and defined privacy policies are in place, but they also need to be enforced. What are some ways to enforce these privacy policies? Check all that apply.

- [x] Audit access logs
  - Correct: You nailed it! Auditing access logs will ensure sensitive information is only being accessed by individuals that are authorized to access it.
- [ ] Print customer information
- [ ] VPN connection
- [x] Lease privilege
  - Correct: You nailed it! Apply the principle of least privilege by not allowing access to specific data by default.

Correct
Great, you got all the right answers.

7. Question — 1 / 1 point

Which of these are bad security habits commonly seen amongst employees in the workplace? Check all that apply.

- [ ] Lock desktop screen
- [x] Leave laptop logged in and unattended
  - Correct: Great work! Leaving a laptop logged in and unattended is a bad security habit.
- [x] Password on a post-it note
  - Correct: Great work! Writing down passwords on a post-it is a bad security habit.
- [ ] Log out of website session

Correct
Great, you got all the right answers.

8. Question — 1 / 1 point

When considering third-party service providers to host sensitive data, you should conduct a vendor risk review. What actions does this include? Check all that apply.

- [ ] Talk to vendor employees.
- [ ] Ask vendor for a cost comparison.
- [x] Ask vendor to fill out a security questionnaire.
  - Correct: You got it! The questionnaire will cover various aspects of their security policies, procedures, and defenses in place.
- [x] Test the vendor's hardware or software.
  - Correct: You got it! Test the software or hardware to evaluate it for potential security vulnerabilities.

Correct
Great, you got all the right answers.

9. Question — 1 / 1 point

Management wants to build a culture where employees keep security in mind. Employees should be able to access information freely and provide feedback or suggestions without worry. Which of these are great ideas for this type of culture? Check all that apply.

- [ ] Bring your own device
- [x] Designated mailing list
  - Correct: Awesome! A mailing list is where people can ask questions or report things related to security.
- [x] Posters promoting good security behavior
  - Correct: Awesome! Posters or other informational flyers help to encourage or reinforce good security behaviors.
- [ ] Desktop monitoring software

Correct
Great, you got all the right answers.

10. Question — 1 / 1 point

The very first step of handling an incident is ____ the incident.

- (•) detecting
- ( ) blaming
- ( ) ignoring
- ( ) understanding

Correct
Great work! The very first step of handling an incident is detecting the incident.

11. Question — 1 / 1 point

Once the scope of the incident is determined, the next step would be ____.

- ( ) escalation
- ( ) documentation
- ( ) remediation
- (•) containment

Correct
Nice job! Once the scope of the incident is determined, the next step would be containment.