Quiz-Creating a Company Culture for Security

Question 1:

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

HIPAA

ISO

IEEE

PCI DSS

Question 2:

What tools can be used to discover vulnerabilities or dangerous misconfigurations in systems and networks?

Vulnerability scanners

Bastion hosts

Firewalls

Antimalware software

Question 3:

Which of the following are examples of security tools that can scan computer systems and networks for vulnerabilities? Select all that apply.

Nessus

OpenVAS

Qualys

Wireshark

Question 4:

Which of the following should be part of an access data request? Select all that apply.

A second signature

Time limit

Provide justification

Specify exact data needed

Question 5:

Which of the following is recommended to secure authentication?

2-factor authentication

Strong encryption

Password rotation

Vulnerability scanning

Question 6:

Which of the following are ways to prevent email phishing attacks against user passwords? Select all that apply.

User education

Cloud email

Virtual private network

Spam filters

Question 7:

When contracting services from a third party, what risk is the organization exposed to?

Malware attacks

Zero-day vulnerabilities

DDoS attacks

Trusting the third party's security

Question 8:

Third-party services that require equipment on-site may require a company to do which of the following? Select all that apply.

Unrestricted access to the network

Provide additional monitoring via a firewall or agentless solution

Provide remote access to third-party service provider

Evaluate hardware in the lab first

Question 9:

Periodic mandatory security training courses can be given to employees in what way? Select all that apply.

Brief quiz

One-on-one interviews

Short video

Interoffice memos

Question 10:

What are the first two steps of incident handling and response?

Incident containment

Incident eradication or removal

Incident recovery

Incident detection