

CIW

CPCS-100

CIW Cyber Specialist

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/cpcs-100>

Latest Version: 6.0

Question: 1

When a business collects customer credit card information, which standard must they comply with to ensure the data is protected?

- A. OSHA
- B. PCI DSS
- C. IEEE 802.11
- D. SMTP

Answer: B

Question: 2

During which phase of the incident response plan does an organization focus on removing the threat from their systems and preventing it from spreading further?

- A. Preparation
- B. Detection
- C. Containment and Eradication
- D. Post-Incident Activity

Answer: C

Question: 3

You are tasked with implementing a security solution that monitors network traffic for suspicious patterns and alerts the administrator, but does not automatically block the traffic. Which technology should you choose?

- A. Intrusion Detection System (IDS)
- B. Intrusion Prevention System (IPS)
- C. Firewall
- D. Virtual Private Network (VPN)

Answer: A

Question: 4

In Public Key Infrastructure (PKI), which key is used by a sender to encrypt a message so that only the intended recipient can read it?

- A. The sender's private key
- B. The sender's public key
- C. The recipient's private key
- D. The recipient's public key

Answer: D

Question: 5

After a security incident is resolved, what is the purpose of a "Lessons Learned" meeting?

- A. To decide which employee should be fired for the security breach.
- B. To calculate the total amount of overtime pay for the IT staff.
- C. To identify what went well and how to improve future responses.
- D. To explain to the public that the incident was not a serious issue.

Answer: C

Question: 6

Which cryptographic algorithm is a widely used asymmetric standard for securing web traffic and digital signatures?

- A. RSA
- B. DES
- C. AES
- D. Caesar Cipher

Answer: A

Question: 7

How does a "Stateful Inspection" firewall differ from a basic packet filter?

- A. It only blocks traffic originating from outside the country.

- B. It tracks the state of active connections to make better decisions.
- C. It requires a physical key to be turned before it starts filtering.
- D. It deletes all incoming emails that contain any attachments.

Answer: B

Question: 8

An individual receives an email that appears to be from their bank, claiming there is suspicious activity and providing a link to "verify" their login credentials. Which type of cyber threat does this scenario describe?

- A. Ransomware
- B. Logic Bomb
- C. Adware
- D. Phishing

Answer: D

Question: 9

Why is cybersecurity considered a critical business risk for small and medium-sized enterprises (SMEs)?

- A. A single data breach can result in total business failure due to costs.
- B. SMEs are never targeted by hackers because they have very little money.
- C. SMEs are legally required to spend 50% of their revenue on firewalls.
- D. Cybersecurity threats only affect businesses that operate entirely online.

Answer: A

Question: 10

What is a key advantage of a Network-based Intrusion Detection System (NIDS) over a Host-based IDS (HIDS)?

- A. It is installed directly on every individual user's smartphone.
- B. It can monitor traffic for an entire subnet of devices at once.
- C. It can see encrypted data that is stored on a local hard drive.
- D. It prevents users from physically entering the server room.

Answer: B

Thank You for Trying Our Product
Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>