JOSHUA AROUNI | CYBER SECURITY | DAE

1. Create an Incident Response Plan

1. Detection of Security Incidents:

- Method: Implement an Intrusion Detection System (IDS) to monitor network traffic and identify suspicious activities, such as unusual login attempts or large data transfers.

2. Strategy for Containment:

- Isolate affected systems from the network to prevent further spread of the attack.
- Limit user access and revoke permissions for compromised accounts.

3. Steps for Eradication and Recovery:

- Eradication: Conduct a malware scan and remove infected files. Ensure patches and updates are applied to vulnerable software.
- Recovery: Restore data from verified backups and bring systems back online gradually while monitoring for anomalies.

4. Types of Cyber Attacks:

- Example: Ransomware
    - Ransomware encrypts critical files, demanding payment for decryption. This type of attack often spreads via phishing emails or malicious downloads.
    - The response involves isolating affected systems, avoiding ransom payment, and restoring data from backups.

---

2. Develop a Comprehensive Security Policy

1. Key Security Rules/Guidelines:

- Enforce strong password policies requiring complexity and periodic updates.
- Implement multi-factor authentication (MFA) for accessing sensitive systems.
- Conduct regular employee cybersecurity training.

2. Incident Response Plan:

- Steps for a Security Breach:
    1. Detect and validate the incident using monitoring tools.
    2. Contain the breach by isolating affected systems.

3. Notify relevant stakeholders and authorities as required.
4. Investigate to determine the cause and scope of the breach.
5. Eradicate threats and vulnerabilities identified.
6. Recover systems using secure backups and verify integrity.
7. Document lessons learned and update policies.

3. Maintaining the CIA Triad:

- Confidentiality: Use encryption to protect sensitive data.
- Integrity: Implement hashing to verify data authenticity.
- Availability: Regularly update and test backup systems.

---

3. Apply Encryption Techniques

1. Encrypted Text Example:

- **Plain Text: "Confidential Data"**
- **Encryption Method: Advanced Encryption Standard (AES)**
- **Encrypted Text:** `Z3VycF98MTE2Y3wxn29ZX+==`
- **Hashing Example:**
  - **Plain Text: "Confidential Data"**
  - **Hash Function: SHA-256**
  - **Hashed Text:** `a5d5c3cb4b5d47212a3df8f769e8b601d934f3ac2c1aa10ef0c92b3ad2b76b92`

2. Decryption:

- **Using the decryption key for AES, the encrypted text returns to its original form: "Confidential Data."**

---

4. Demonstrate Legal and Ethical Compliance

1. Legal and Ethical Considerations:

- Relevant Laws and Regulations:
  - General Data Protection Regulation (GDPR): Ensures user data privacy and mandates reporting breaches within 72 hours.
  - Health Insurance Portability and Accountability Act (HIPAA): Protects sensitive health information.

2. Ethical Consideration:

- Ensure transparency with affected users by informing them of breaches promptly.
- Avoid practices that compromise user trust, such as withholding breach details.

3. How the Plan Upholds Compliance:

- Regularly audit systems to meet GDPR and HIPAA requirements.
- Include breach notification steps in the incident response plan.
- Train employees on ethical handling of sensitive data to maintain trust and adherence to legal frameworks.