# **CTF Topic: Introduction Defensive Security**



# **Introduction**



Defensive security refers to the strategies, processes, and technologies used to protect an organization's digital assets, including data, networks, systems, and applications, from cyber threats and attacks. It involves proactive measures aimed at preventing, detecting, and responding to security incidents.

# **Why Needed**

Defensive security is essential due to the increasing frequency and sophistication of cyber threats. Without adequate defenses, organizations are vulnerable to data breaches, financial losses, reputational damage, and legal consequences. Implementing defensive security measures helps mitigate these risks and ensures the confidentiality, integrity, and availability of sensitive information.

# **How to Implement**

**Risk Assessment**: Identify and assess potential security risks and vulnerabilities.

**Access Control:** Limit access to sensitive data and systems based on the principle of least privilege.

**Security Policies:** Develop and enforce security policies and procedures.

**Network Security**: Use firewalls, intrusion detection/prevention systems, and secure configurations to protect networks.

**Monitoring and Response**: Deploy security monitoring tools and establish incident response plans.

**Endpoint Security**: Install antivirus software, conduct regular patching, and implement device encryption.

# **Question**

Flag 1 What principle should access control be based on?

Answer: Privilege

Flag Captured

Flag 2 What should be deployed to monitor security?

Answer: Security Tools

Flag Captured

Flag 3 Which security Install antivirus software?

Answer: Endpoint Security

Flag Captured