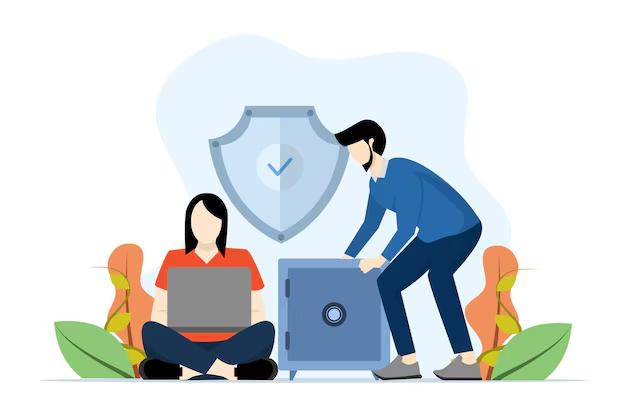
**CTF Challenge: Introduction to Defensive Security**

****

****

## 

## 

## 

## 

## **Introduction to Defensive Security: Building a Fortress**

Defensive security is the proactive approach to protecting information systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction. It's the shield that organizations use to defend themselves against the ever-evolving landscape of cyber threats.



**Core Principles:**

* **Prevention:** Implementing security controls to prevent attacks from happening in the first place. This includes firewalls, intrusion detection systems (IDS), and secure coding practices.
* **Detection:** Continuously monitoring systems and networks for suspicious activity that might indicate a security breach. This involves security information and event management (SIEM) systems and log analysis.
* **Response:** Having a plan in place to respond to security incidents efficiently. This includes isolating compromised systems, containing the damage, and eradicating the threat.
* **Recovery:** Restoring systems and data to a known good state after a security incident. This requires backups and disaster recovery plans.

**Defensive Security Roles:**

* **Security Analysts:** Monitor systems for suspicious activity, investigate security incidents, and analyze security data.
* **Security Engineers:** Design, implement, and maintain security controls such as firewalls and intrusion detection systems.
* **Security Architects:** Develop and implement overall security strategies for the organization.
* **Security Awareness and Training:** Educate employees on cyber security best practices to reduce the risk of human error.

# **Capture the Flag (CTF) Challenges**

**Flag 1. Defensive security focuses on a proactive approach to protecting systems from attacks. What is the first principle, aiming to prevent attacks from happening in the first place?**

Answer: Prevention

**Flag 2. Serverless functions are often triggered by events. A core defensive principle involves granting functions only the minimum permissions needed to perform their tasks. What is this principle called?**

Answer: Privilege

**Flag 3. Security Information and Event Management (SIEM) systems are valuable tools for security analysts to monitor for suspicious activity in serverless environments. What type of analysis do SIEM systems perform?**

Answer: Log

**Flag 4. Firewalls and Intrusion Detection Systems (IDS) are traditional security controls that can also be used in some serverless environments for prevention purposes. These controls fall under which core principle of defensive security?**

Answer: Prevention

**Flag 5. In case of a security breach, a crucial step in recovery is restoring data to a known good state. Backups are essential for achieving this. What is the defensive principle associated with recovery?**

Answer: Response