Cybersecurity Task 1: Understanding Cybersecurity Basics & Attack Surface

1. What is Cybersecurity and the CIA Triad?
Cybersecurity is the practice of protecting systems, networks, and data from cyber threats such as unauthorized access, attacks, damage, or theft.

The CIA Triad is the foundation of cybersecurity and consists of three principles:

Confidentiality: Ensures that sensitive data is accessible only to authorized users.
Examples include data encryption, passwords, and access controls.
A real-world example is the ESHYFT healthcare data breach, where over 86,000 records were exposed due to a public cloud storage configuration.

Integrity: Ensures that data remains accurate and unaltered.
Examples include hashing, audit logs, and file integrity monitoring.
In one financial system incident, attackers modified billing logs to hide fraudulent activity during a maintenance window when integrity checks were disabled.

Availability: Ensures systems and data are accessible when needed.
Examples include backups, redundancy, and DDoS protection.
A ransomware attack on NHS-linked hospitals caused system outages and delayed thousands of medical procedures, demonstrating an availability failure.

2. Types of Cyber Attackers
Script Kiddies: Inexperienced attackers using ready-made tools.
Hacktivists: Politically motivated attackers targeting organizations or governments.
Cybercriminals: Financially motivated attackers using phishing and ransomware.
Insider Threats: Employees who intentionally or accidentally cause harm.
Nation-State Actors: Government-backed attackers targeting critical infrastructure.

3. What is an Attack Surface?
An attack surface includes all possible entry points an attacker can use to exploit a system.
Digital attack surfaces include websites, applications, APIs, and cloud systems.
Physical attack surfaces include laptops, USB drives, and IoT devices.
Social attack surfaces include employees vulnerable to phishing and social engineering.

4. OWASP Top 10 Overview
The OWASP Top 10 lists the most critical web application security risks.
Key risks include Broken Access Control, Security Misconfiguration, Cryptographic Failures, and Injection attacks.
It helps organizations prioritize security efforts and reduce common vulnerabilities.

5. What is a Data Flow Diagram (DFD)?
A Data Flow Diagram shows how data moves through a system from input to processing to storage and output.
Levels include Context Diagram (Level 0), Level 1, and Level 2 diagrams.
DFDs help identify potential attack points and improve system security.

Conclusion
Understanding the CIA Triad, attacker types, attack surfaces, OWASP Top 10, and data flow diagrams builds a strong foundation in cybersecurity and threat awareness.