TASK 1

(1) CYBERSECURITY AND CIA TRAID

At its simplest level, **Cybersecurity** is the practice of protecting systems, networks, and programs from digital attacks.

Think of it like the security for a physical bank: you have vaults (data protection), guards (firewalls/monitoring), and ID checks (passwords) to ensure that only the right people get in and nothing is stolen or damaged.

In the professional world, this is built on a "Golden Rule" called the **CIA Triad**. As an intern at Elevate Labs, understanding this will be the foundation of almost every task you do.

1. The CIA Triad (The Core Pillars)

To say a system is "secure," it must satisfy these three conditions:

- **Confidentiality (Privacy):** Ensuring that sensitive information is only accessed by authorized people.
    - *Real-world example:* When you log into your banking app, only you should be able to see your balance. If a stranger can see it, confidentiality is breached.
    - *Tools used:* Encryption, Passwords, Multi-Factor Authentication (MFA).
- **Integrity (Accuracy):**[8] Ensuring that data is correct and has not been changed or tampered with by an unauthorized person.
    - *Real-world example:* If you send $100 to a friend, but a hacker changes the amount to $1,000 in the bank's database, the integrity of that transaction is lost.
    - *Tools used:* Digital signatures, Hashing (digital fingerprints).
- **Availability (Reliability):** Ensuring that systems and data are available to users when they need them.

- *Real-world example:* If a hospital's patient records system crashes during an emergency, doctors can't treat patients. Even if the data is "private" and "accurate," the system failed because it wasn't available.
- *Threats:* DDoS attacks (flooding a site with traffic so it crashes).

Why is it so important right now?

1. **Financial Protection:** Attacks like Ransomware can cost companies millions of dollars.
2. **Trust:** If a company like WhatsApp or Instagram loses your private messages, you'll stop using them.
3. **National Security:** Modern warfare isn't just physical; hackers can target power grids, water supplies, and government secrets.

(2) DIFFERENT TYPES OF ATTACKERS

Here are the common types of cyber attackers:

1. Script Kiddies

- **Who they are:** Unskilled individuals who do not typically write their own code.
- **How they work:** They use existing software, scripts, or "off-the-shelf" tools created by others to launch attacks.
- **Motivation:** Often just for fun, to gain attention, or to see what they can get away with.

2. Insiders

- **Who they are:** Current or former employees, contractors, or business partners who have authorized access to a company's network.
- **Why they are dangerous:** They are already "inside" the defenses, making them one of the hardest threats to detect.
- **Motivation:** Can be malicious (revenge, financial gain) or accidental (falling for a phishing scam).

3. Hacktivists

- **Who they are:** Attackers who use hacking as a form of protest.
- **How they work:** They often target high-profile organizations to deface websites or leak data to draw attention to a cause.
- **Motivation:** Political, social, or ideological reasons rather than money.

4. Nation-State Actors

- **Who they are:** Highly sophisticated groups sponsored or employed by national governments.
- **Why they are dangerous:** They have massive budgets and focus on **Advanced Persistent Threats (APTs)**—infiltrating a network and staying hidden for years to steal secrets.

- **Motivation:** Espionage, political sabotage, or gaining a military advantage.

5. Cybercriminals (For-Profit)

- **Who they are:** Individuals or organized syndicates.
- **Motivation:** Almost exclusively **financial gain** through methods like ransomware or selling stolen credit card data.

---

(3) COMMON ATTACK SURFACES

In cybersecurity, the **attack surface** is the total sum of all possible points (entry and exit points) where an unauthorized user can try to enter or extract data from a system. Think of it as the total number of "doors and windows" a hacker could use to break into a building.

The smaller the attack surface, the easier it is to protect the organization.

1. The Three Main Types of Attack Surfaces

Based on your task, you should document these three key areas:

- **Digital Attack Surface:** This covers everything reachable through the internet or a network.
    - **Web Applications & Websites:** Login pages, search fields, and contact forms.
    - **APIs:** The bridges that allow different software to communicate.
    - **Cloud Infrastructure:** Misconfigured storage buckets (like Amazon S3) or servers.
    - **Network Ports:** Open ports (like SSH or FTP) that are not properly secured.
- **Physical Attack Surface:** This involves hardware and physical assets that an attacker can touch.
    - **Endpoint Devices:** Laptops, mobile phones, and USB drives.
    - **Facility Access:** Server rooms, data centers, or even discarded hard drives.

- **Human (Social Engineering) Attack Surface:** This refers to the people within an organization who can be tricked.
    - **Phishing:** Employees clicking on malicious email links.
    - **Weak Passwords:** Users choosing simple passwords that are easy to guess.

---

(4) Data Flow Mapping (The Journey)

A standard data flow for modern applications involves four main "stops":

1. **User (The Origin):** The journey starts when a user interacts with a device (like a phone or laptop) to enter information, such as login credentials or a search query.
2. **Application (The Logic):** The data travels over the internet (the Network Layer) to the application code. This is where the business logic lives—it decides what to do with your request (e.g., "Is this password correct?").
3. **Server (The Host):** The application runs on a physical or cloud server. The server manages the resources (CPU, Memory) needed to keep the application running.
4. **Database (The Vault):** Finally, the application talks to the database to store or retrieve permanent records, like your account balance or chat history.

---

(5) Identifying Attack Points

Every time data moves from one stage to the next, it crosses a **Trust Boundary**, creating an opportunity for an attack.

Stage of Flow	Potential Attack Type	Why it happens

User → Internet	**Phishing / MITM**	Attackers trick users into giving away data or intercept it while it's in transit.
At the Application	**Broken Access Control**	The app logic fails to check if the user is allowed to perform a certain action.
App → Server	**Command Injection**	An attacker sends malicious code that the server accidentally executes as a system command.
Server → Database	**SQL Injection**	The application doesn't "clean" user input, allowing a hacker to send commands directly to the database to steal all records.
At the Database	**Data Breach**	Sensitive information is stolen because it was stored without encryption or had weak permissions.