TASK-1

1.CIA TRAID

The three letters in "CIA triad" stand for Confidentiality, Integrity, and Availability. The CIA triad is a common model that forms the basis for the development of security systems. They are used for finding vulnerabilities and methods for creating solutions.

The confidentiality, integrity, and availability of information is crucial to the operation of a business, and the CIA triad segments these three ideas into separate focal points. This differentiation is helpful because it helps guide security teams as they pinpoint the different ways in which they can address each concern.

CONFIDENTIALITY:

Basically confidential things are the matter under cyber secutiy, confidentiality means how you protect the data from the third party or person, Because data's are the 21'st centuries biggest assert. We can protect our data from outsiders by encryption, strong password and giving confidential resources to the authorized and specialist persons, by restricting access to everyone.

For example, those who work with an organization's finances should be able to access the spreadsheets, bank accounts, and other information related to the flow of money. However, the vast majority of other employees and perhaps even certain executives—may not be granted access. To ensure these policies are followed, stringent restrictions have to be in place to limit who can see what.

However, not all violations of confidentiality are intentional. Human error or insufficient security controls may be to blame as well. Like not providing a strong password to the restricted places and share the credentials to others or targeting a employee or victim to grab the information by attending some illegal activities like phishing.

Example: In bank, customer details and credential information should be securely protected from outsiders and unauthorized persons.

INTEGRITY:

It involves make sure the data is complete or trustworthy and free from tampering. The integrity of your data is maintained only if the data is authentic, accurate, and reliable. To protect the integrity of your data, you can use hashing, encryption, digital certificates, or digital signatures. For websites, you can employ trustworthy certificate authorities (CAs) that verify the authenticity of your website so visitors know they are getting the site they intended to visit.

In bank, the transactions are should in upto date manner, give any transaction is not registered it became an issue to the both bank and customer.

AUTHENTICITY:

Even if data is kept confidential and its integrity maintained, it is often useless unless it is available to those in the organization and the customers they serve. This means that systems, networks, and applications must be functioning as they should and when they should. Also, individuals with access to specific information must be able to consume it when they need to, and getting to the data should not take an inordinate amount of time.

To ensure availability, organizations can use redundant networks, servers, and applications. These can be programmed to become available when the primary system has been disrupted or broken. You can also enhance availability by staying on top of upgrades to software packages and security systems. In this way, you make it less likely for an application to malfunction or for a relatively new threat to infiltrate your system. Backups and full disaster recovery plans also help a company regain availability soon after a negative event.

Authorized persons like manager like high rank officers should be give access to the vault. Because to avoid the theft and credentials.

2.ATTACKERS IN DIGITAL WORLD:

Attackers are those who try to steal the information or assert of an individual or an organisation in unauthorized way.

TYPES OF ATTACKERS AND BRIEF NOTE

- **Script Kiddies (The Amateurs)**
  - Unskilled individuals, often juveniles or "thrill-seekers," who do not have the technical depth to write their own exploits.
  - They rely on "pre-packaged" scripts, open-source tools, and malware created by others. They often frequent forums to find easy-to-use hacking kits.
  - Primarily driven by curiosity, a desire to impress peers, or the simple thrill of causing chaos.
  - Targets of opportunity they look for anyone with well-known, unpatched vulnerabilities or weak configurations rather than choosing a specific victim.

- **Insiders (The Threat from Within)**
  - Who they are: Current or former employees, contractors, or business partners who have legitimate access to an organization's network.
  - They are the hardest to detect because their activity often looks like normal authorized work until the damage is done.

- **Hacktivists (The Ideologues)**
  - Hacker activists who use digital attacks to promote a social, political, or religious agenda.
  - Common methods include website defacement (changing the homepage to show a message), DDoS attacks to take

down services, and "doxing" (releasing private info to embarrass a target).

- They see themselves as digital protesters. Their goal is usually high visibility and public awareness rather than financial gain.
- The collective Anonymous, known for targeting government agencies or corporations they view as unethical.

➢ **Nation-State Actors (The Professionals)**

- Highly sophisticated, government-sponsored groups (often referred to as APTs or Advanced Persistent Threats).
- They use zero-day exploits (vulnerabilities unknown to the public) and custom-built malware. They are extremely patient, often staying hidden in a network for months or years.
- Strategic interests such as international espionage, stealing industrial secrets (intellectual property), disrupting critical infrastructure (power grids), or spreading disinformation.
- Unlike the other groups, they have nearly unlimited funding, specialized training, and legal protection from their home country.

3. Attack surfaces and its types:

The attack surface is the number of all possible points, or attack vectors, where an unauthorized user can access a system and extract data. The smaller the attack surface, the easier it is to protect.

The attack surfaces are commonly classified into 2 ways physical and digital attack surface.

The common types of attack surface are:

- web applications
- mobile apps
- APIs
- networks
- cloud infrastructure.

1. Web Applications
Web apps are often the most exposed part of an organization because they must be accessible via the internet, like SQL Injection (SQLi) where attackers send malicious code through a search bar or login form. Weaknesses in session management that allow hackers to hijack user accounts.

Cross-Site Scripting (XSS): Injecting malicious scripts into pages viewed by other users.

2. Mobile Applications
Mobile apps expand the surface to the user's pocket, involving device hardware and public app stores. Insecure Data Storage: Saving sensitive info (like passwords) in plain text on the phone. Data intercepted over unencrypted public Wi-Fi (Man-in-the-Middle attacks).Sending so many login requests that a user eventually hits "Approve" just to stop the notifications.

3.APIs (Application Programming Interfaces)
APIs are the "connectors" between software. Because they are designed for machine-to-machine talk, they are often less monitored by humans. Broken Object-Level Authorization (BOLA): An attacker changing a user ID in a URL .
(e.g., changing /api/user/101 to /api/user/102) to see someone else's data.

Lack of Rate Limiting: Allowing an attacker to "spam" the API millions of times to crash it or guess passwords.

4. Networks

The network attack surface includes all the "roads" and "gates" (ports) data travels through.

Open Ports: Unused digital "doors" left open (like Port 80 for unsecured web traffic).

- Unpatched Hardware: Routers or switches running old software with known bugs.
- Shadow IT: Employees using unauthorized devices (like a personal laptop) on a secure corporate network.

5. Cloud Infrastructure

Cloud security is unique because it's a "shared responsibility" between you and the provider (like AWS or Google Cloud).

Key Vulnerabilities: Misconfigured Buckets: Leaving cloud storage (like S3) set to "Public" so anyone can download the data.

- Overly Permissive IAM Roles: Giving a basic user "Administrator" powers they don't need.
- Orphaned Resources: A "test server" you created for a project but forgot to delete, which still has an active connection to the internet