100 DAY CHALLENGE

DAY 5 - CHALLENGE 5

THREAT MODELLING

1. Threats

- **Cyber Attacks:** Hacking, phishing, malware, ransomware.
- **Insider Threats:** Disgruntled employees or those with malicious intent.
- **Fraud:** Identity theft, account takeover, card skimming.
- **Physical Theft:** Theft of hardware or documents from bank premises.
- **Natural Disasters:** Floods, fires, earthquakes affecting physical infrastructure.
- **Operational Errors:** Mistakes by employees or system failures.
- **Regulatory Non-compliance:** Failure to adhere to regulations leading to legal issues.

2. Vulnerabilities

- **Software Bugs:** Flaws in banking software that could be exploited.
- **Outdated Systems:** Legacy systems that lack modern security features.
- **Weak Authentication:** Insufficient password policies or lack of multi-factor authentication (MFA).
- **Insecure Communication Channels:** Unencrypted data transmission.
- **Human Error:** Mistakes or lack of training among staff.
- **Third-Party Risks:** Vulnerabilities in systems provided by external vendors.

3. Risks

- **Financial Loss:** Loss of money due to fraud, cyber-attacks, or operational failures.
- **Reputation Damage:** Loss of customer trust and negative publicity.
- **Legal Penalties:** Fines or legal action due to regulatory non-compliance.
- **Operational Disruption:** Service outages or interruptions affecting customer access.
- **Data Breach:** Exposure of sensitive customer information.

4. Attacks

- **Phishing:** Attempts to trick users into divulging confidential information.
- **DDoS (Distributed Denial of Service):** Overloading the bank's systems to cause downtime.
- **SQL Injection:** Exploiting vulnerabilities in databases to access or manipulate data.
- **Man-in-the-Middle Attacks:** Intercepting and altering communications between users and the bank.
- **Ransomware:** Encrypting bank data and demanding payment for decryption.

5. Exploits

- **Zero-Day Exploits:** Attacks using previously unknown vulnerabilities.
- **Privilege Escalation:** Gaining unauthorized access to higher-level permissions.
- **Social Engineering:** Manipulating individuals into divulging confidential information or performing actions that compromise security.
- **SQL Injection:** Injecting malicious SQL code to access or alter database information.
- **Cross-Site Scripting (XSS):** Injecting malicious scripts into web pages viewed by other users.

6. Assets

- **Customer Data:** Personal and financial information.
- **Banking Systems:** Core banking systems, ATMs, and online platforms.
- **Intellectual Property:** Proprietary algorithms, software, and business processes.
- **Physical Infrastructure:** Branches, servers, and data centers.
- **Financial Resources:** Cash, investments, and reserves.

7. Impact

- **Financial Impact:** Direct loss of money and resources, increased costs for remediation and insurance.
- **Reputational Impact:** Loss of customer trust and damage to the bank's brand.
- **Operational Impact:** Service interruptions, loss of productivity, and recovery costs.
- **Legal Impact:** Fines, legal fees, and compliance costs.
- **Customer Impact:** Loss of personal data, financial losses, and inconvenience.