**1. Definition:  
Example in the context of a web application.**  
  
**Assets:**

Assets are the valuable resources that a business relies on to operate, ranging from infrastructure to the individuals who are directly or indirectly involved.

*Example: data center*

**Threats**:

These occur when a malicious adversary exploits a known vulnerability, posing a potential risk to a system.

*Example: SQL injection*

**Vulnerabilities**:

These are weaknesses or flaws in a system that can exploited by a threat.

*Example: Outdated router firmware*

**Attack Vectors**:

These are the tools, techniques, or processes used by a malicious adversary to exploit vulnerabilities and launch threats.

*Example: Phishing email that contains malware*

**Mitigation**:

Measures designed to predict attack vectors, prioritize incidents, document, and develop response plans.

*Example: A runbook that provides guidelines for responding to security alerts*

**2. Applying Threat modeling methodologies, STRIDE**  
  
*The STRIDE methodology is a threat modeling framework used in cybersecurity to identify and mitigate vulnerabilities and threats within a system.*

**Spoofing**:

An attacker uses someone else’s username and password to log in.

*Mitigation: Implement Multi-Factor Authentication (MFA) or One-Time Passcodes (OTP).*

**Tampering**:

A user's banking statements are altered.

Mitigation: *Use HTTPS with SSL/TLS to ensure secure data transmission.*

**Repudiation**:

A customer or attacker claims they didn’t send an email or perform a transaction.

Mitigation: *Implement auditing and transaction logging.*

**Information Disclosure**: A customer's Social Security Number (SSN) is fully exposed without masking.

Mitigation: *Mask and encrypt sensitive data.*

**Denial of Service (DoS):** Customers are unable to access the homepage due to attackers flooding the web server.

Mitigation: *Distribute traffic using load balancing and a web application firewall (WAF).*

**Elevation of Privilege**: A normal user gains administrative control over the system.

Mitigation: *Monitor endpoint devices for abnormal access and enforce the principle of least privilege.*