Threat Modeling

- **Spoofing:** An attacker pretends to be someone else.
- **Tampering:** An attacker modifies data.
- **Repudiation:** An attacker denies performing an action.
- **Information disclosure:** An attacker accesses unauthorized information.
- **Denial of service:** An attacker prevents legitimate users from accessing a system.
- **Elevation of privilege:** An attacker gains higher-level access.

Framework:

System complexity:

- For simple systems, STRIDE might suffice, while complex systems may benefit from OCTAVE.
- Team expertise: The framework should align with the team's skill set and experience.
- Organizational culture: The framework should fit the organization's risk management approach.
- Regulatory requirements: Some frameworks may be more suitable for specific industries or compliance standards.