| **Step** | **Activity** | **Example for Hospital System** |
| --- | --- | --- |
| **1. Define the Scope** | Identify the system, assets, and boundaries. | - System: Hospital Senior Management System (cloud-based) - Assets: Patient records, doctor schedules, medical inventory, network control panel - Trust Boundaries: Internal hospital network vs. cloud services |
| **2. Identify Threats** | Use STRIDE to identify threats. | - **Spoofing**: Unauthorized access to admin dashboard  - **Tampering**: Manipulation of medical records  - **Repudiation**: Lack of logs for user actions  - **Information Disclosure**: Leak of patient info via weak API  - **Denial of Service**: Attack on cloud services causing downtime  - **Elevation of Privilege**: Nurse gaining admin access |
| **3. Create a Model** | Draw DFDs and map vulnerabilities. | - DFD includes: Admin Panel → Cloud API → Database - Weakness: No API key rotation - Vulnerability: Admin panel exposed over public internet |
| **4. Assess Risks** | Prioritize threats. | - High Risk: Patient info leak (Information Disclosure) - Medium Risk: No action logs (Repudiation) - Low Risk: Infrequent backup system |
| **5. Implement Mitigation Strategies** | Apply controls and tools. | - Encrypt all data at rest and in transit - Use Azure Key Vault or AWS KMS for secrets - Enable Multi-Factor Authentication for all roles - Use Microsoft Threat Modeling Tool to refine |
| **6. Validate & Iterate** | Test and improve regularly. | - Penetration test every 6 months - Audit logs weekly - Update model after each new feature added to system |