- **1 - IDENTIFYING THE NEED FOR SECURITY IN YOUR SOFTWARE PROJECTS**
- Identify Security Requirements and Expectations

  Identify Factors That Undermine Software Security

  Find Vulnerabilities in Your Software

  Gather Intelligence on Vulnerabilities and Exploits

---

- **2 - HANDLING VULNERABILITIES**
- Handle Vulnerabilities Due to Software Defects and Misconfiguration

  Handle Vulnerabilities Due to Human Factors

  Handle Vulnerabilities Due to Process Shortcomings

---

- **3 - DESIGNING FOR SECURITY**
- Apply General Principles for Secure Design

  Design Software to Counter Specific Threats

---

- **4 - DEVELOPING SECURE CODE**
- Follow Best Practices for Secure Coding

  Prevent Platform Vulnerabilities

  Prevent Privacy Vulnerabilities

---

- **5 - IMPLEMENTING COMMON PROTECTIONS**
- Limit Access Using Login and User Roles

  Protect Data in Transit and At Rest

  Implement Error Handling and Logging

Protect Sensitive Data and Functions

Protect Database Access

---

- **6 - TESTING SOFTWARE SECURITY**
- Perform Security Testing

  Analyze Code to find Security Problems

  Use Automated Testing Tools to Find Security Problems

---

- **7 - MAINTAINING SECURITY IN DEPLOYED SOFTWARE**
- Monitor and Log Applications to Support Security

  Maintain Security after Deployment