SSDLC 80-20 checklist (SWE)

1. Design / Planering

- [ ] Gör en snabb **hot-analys**: vad kan gå fel? (auth, dataläckor, missbruksscenarier)
- [ ] Definiera **tillitgränser** (var opålitlig input kommer in i systemet).

2. Implementation

- [ ] Följ **säkra kodningsstandarder** (OWASP Top 10, validera input, parameteriserade SQL frågor).
- [ ] Inga **hemligheter i koden** (API-nycklar, lösenord, tokens → använd secret manager).
- [ ] Lägg till en **säkerhetschecklista i kodgranskningar**:
  - [ ] Är autentisering & behörigheter verifierade?
  - [ ] Är input validerad & output kodad?
  - [ ] Är felmeddelanden säkra (inga stacktraces eller känslig info)?
  - [ ] Är känslig data krypterad vid lagring/överföring?

3. Testning / CI-CD

- [ ] Kör **SAST** (statisk kodanalys) på varje PR.
- [ ] Kör **SCA** (beroende-sårbarhetskontroll).
- [ ] Kör **DAST** (grundläggande webscanner) på staging/huvudendpoints.

4. Driftsättning

- [ ] Hantera hemligheter via **vault / moln-secret manager**.
- [ ] Endast **minsta möjliga rättigheter** för tjänstkonton & molnroller (IAM).
- [ ] Aktivera säkerhetsrubriker (CSP, HSTS, osv.).

5. Drift

- [ ] **Logga säkerhetshändelser** (auth-försök, rättighetsfel, felmeddelanden).
- [ ] Sätt upp **larm** för misstänkt beteende.
- [ ] Ha en **grundläggande incidentplan**: vem kontaktas, vad kontrolleras, hur isolera.

✅ **Gör detta konsekvent för att täcka 80 % av riskerna.**
💡 Håll det enkelt: automatisera där det går, och lägg säkerhetskontroller så nära utvecklingsflödet som möjligt.