Software Ekoizpen Segurua (SSDLC)

1. Helburua

Segurtasuna softwarearen bizi-ziklo osoan integratzea (DevSecOps), kodea ekoizpenera iritsi aurretik ahultasunak detektatzeko.

2. Prozedura

Fase 1: Diseinua

- **Mehatxuen Modelizazioa:** Identifikatu eraso bektore posibleak diseinu fasean.
- **Segurtasun Eskakizunak:** Definitu hasieratik (adib. “Datu guztiak HTTPS bidez joan behar dira”).

Fase 2: Garapena (Coding)

- Erabili IDE-an integratutako Linter-ak eta segurtasun plugin-ak (adib. SonarLint).
- **Ez kodetu sekreturik:** Pasahitzak eta API gakoak EZ jarri kodean (`.env` fitxategiak erabili).
- Jarraitu OWASP Top 10 gomendioak (Input Validation, Output Encoding).

Fase 3: Proba Automatizatuak (CI/CD Pipeline)

- **SAST (Static Application Security Testing):** Kode iturburua aztertu (SonarQube).
- **SCA (Software Composition Analysis):** Mendekotasunen ahultasunak aztertu (npm audit, OWASP Dependency Check).
- **DAST (Dynamic Application Security Testing):** Aplikazioa exekutatzen ari dela erasoak simulatu (OWASP ZAP).

Fase 4: Berrikusketa (Code Review)

- Pull Request bakoitza beste garatzaile batek berrikusi behar du.
- Segurtasun checklist bat erabili.

Fase 5: Hedapena (Deployment)

- Azpiegitura Kode gisa (IaC) erabili inguruneak errepikagarriak izateko.

- Ziurtatu ekoizpeneko konfigurazioak gotortuta daudela (Debug modua itzalita).