

devsecops blueprint

gerardo di giacomo

agenda

- ❑ cosa significa shift left security?
- ❑ come si applica in un contesto devops?

chi sono?

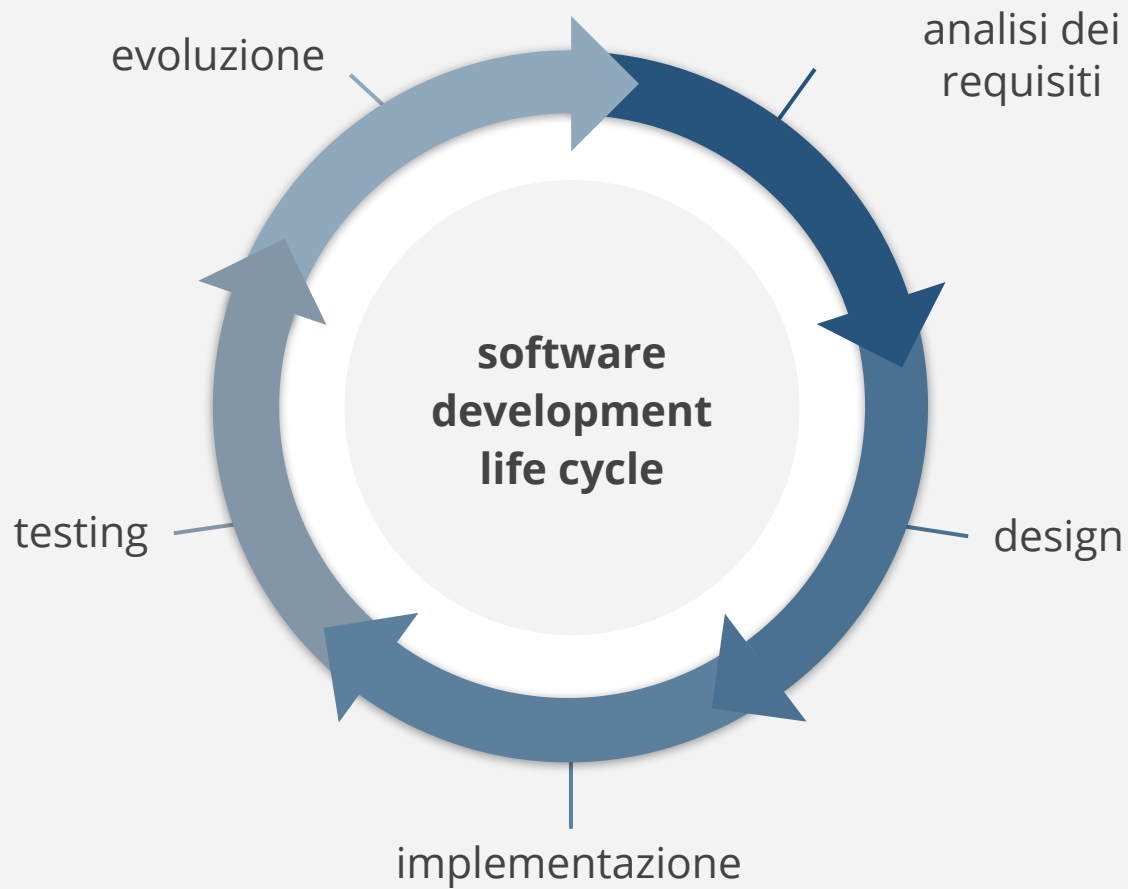
security engineer @ stripe

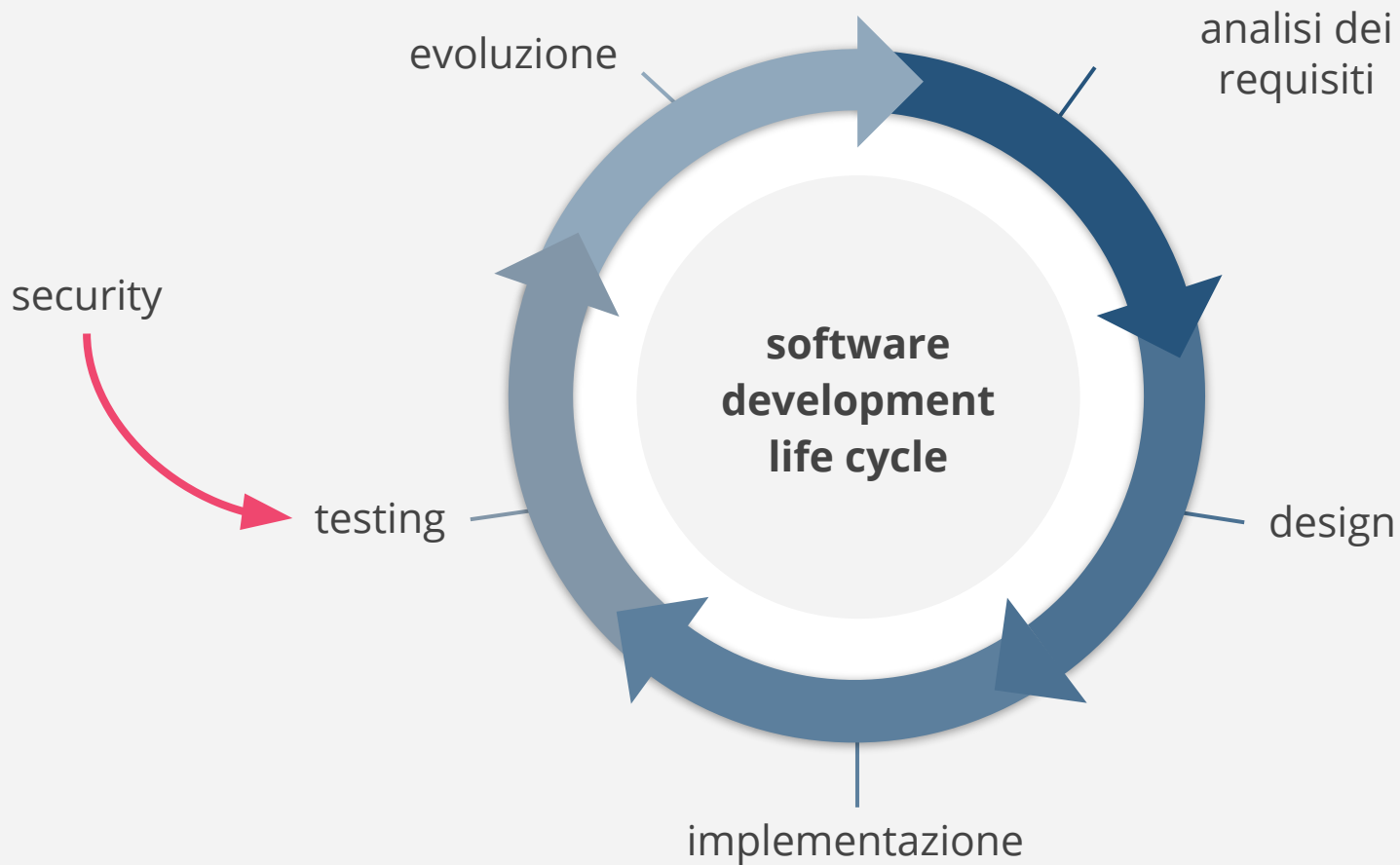
application/product security dal 2002

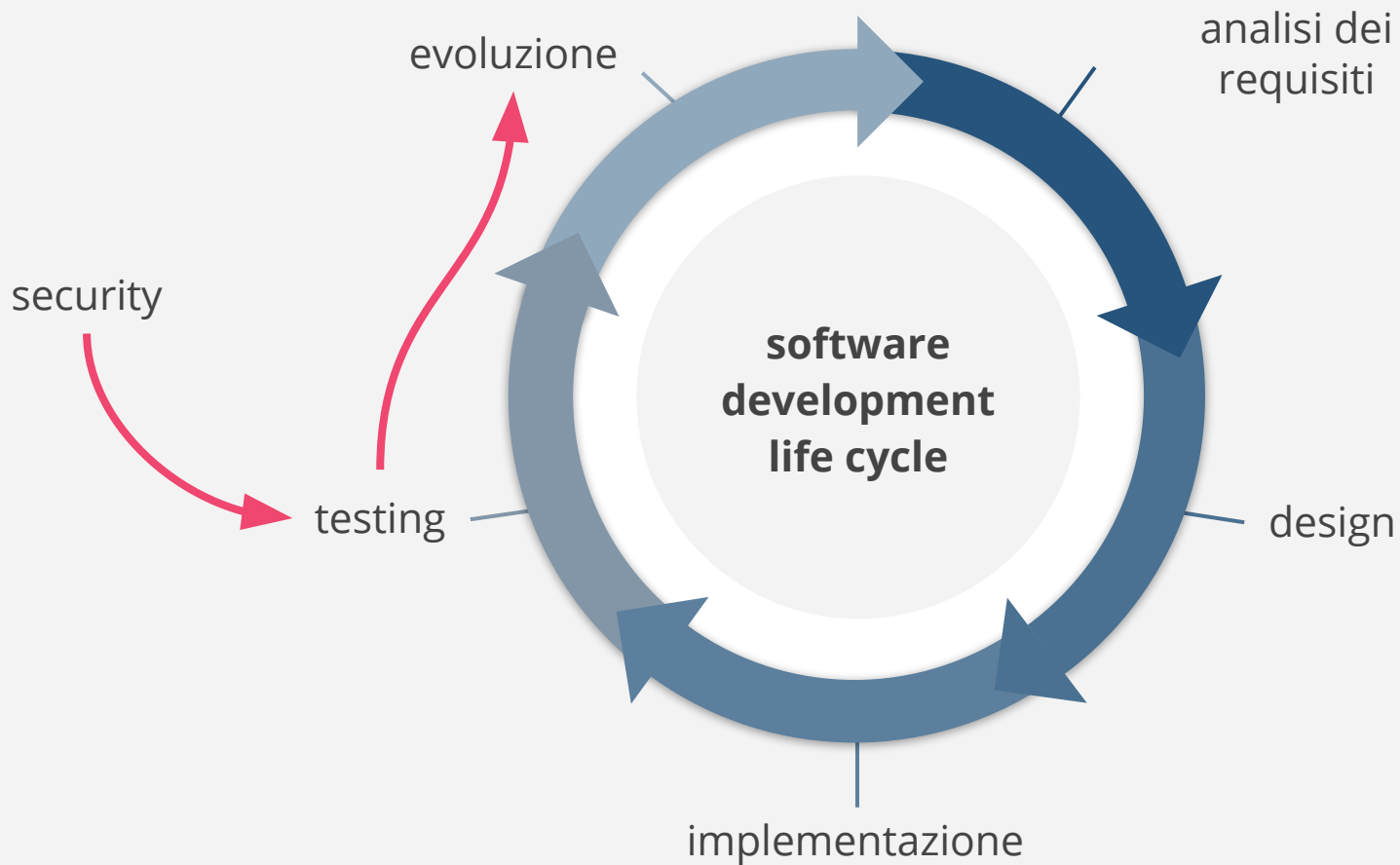


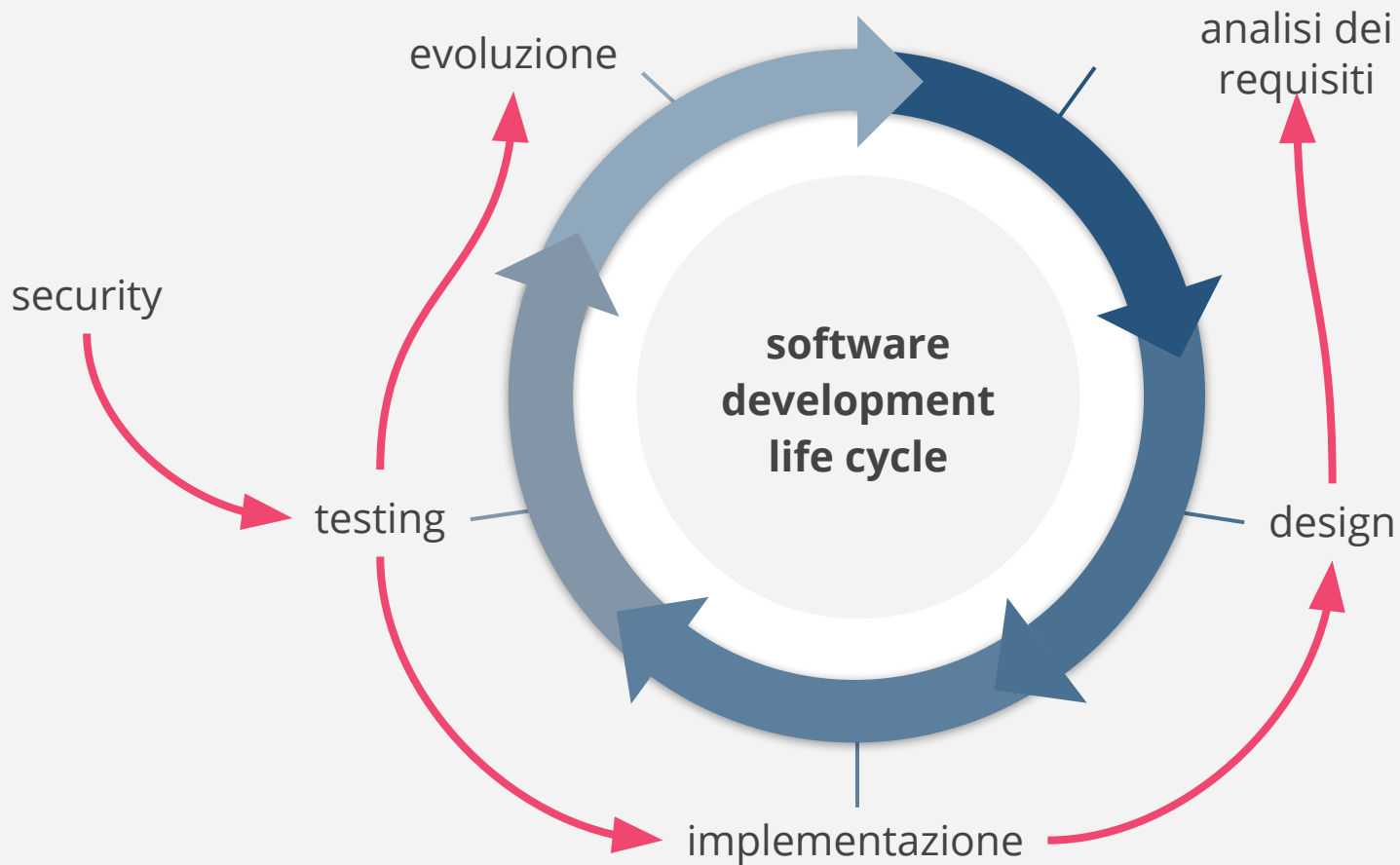
@gedigi

shift left security?

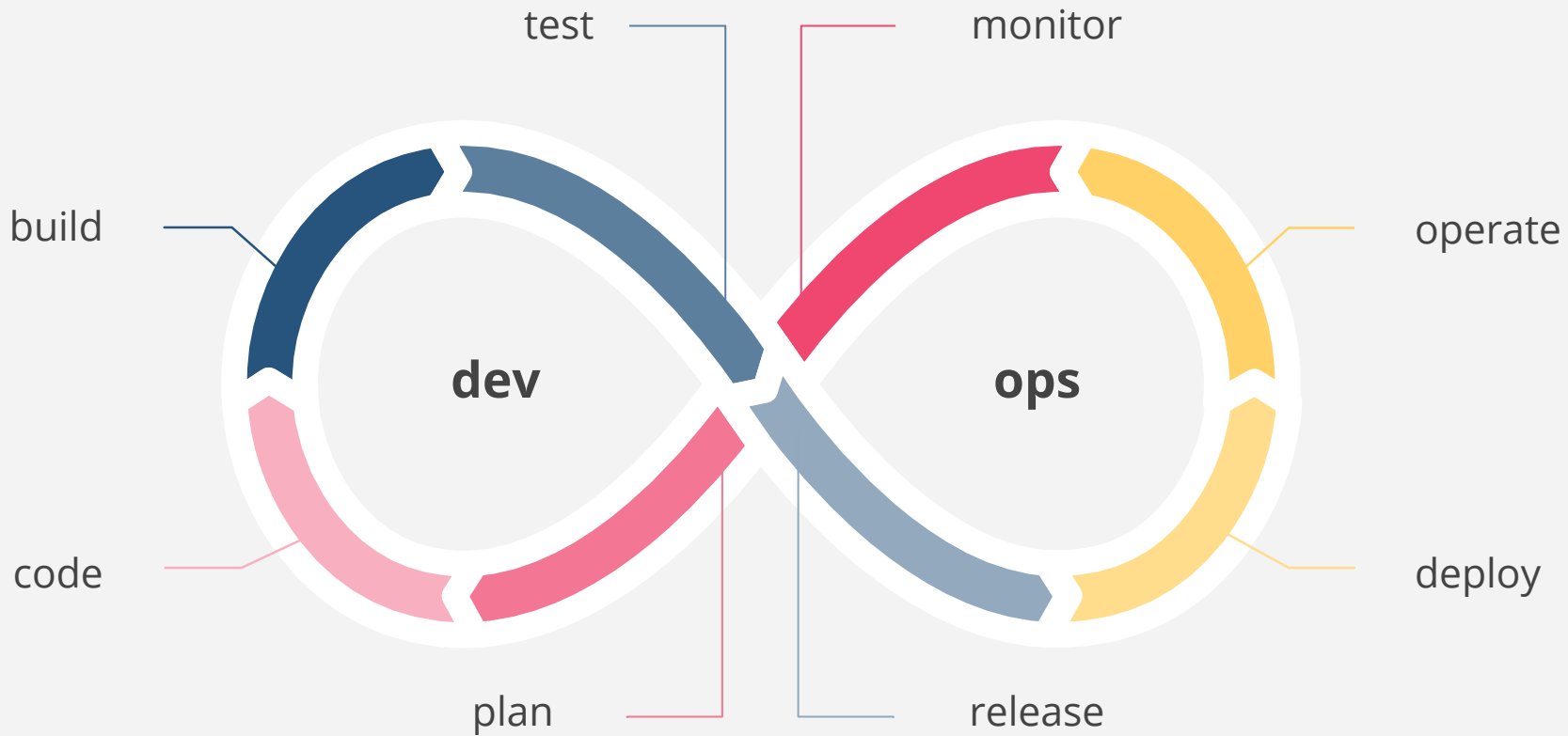








shift left security + devops?



security requirements/stories
security policy/standards
design review
threat modeling



plan

linting
librerie e framework
segreti
commit firmati



code

code review
gestione dipendenze
firma artefatti



build

analisi statica
analisi dinamica
validazione requirements



test

verifica artefatti
penetration test



release

blue/green
infrastructure as code



deploy

autenticazione multi-fattore

least privilege

security update

confidential computing



operate

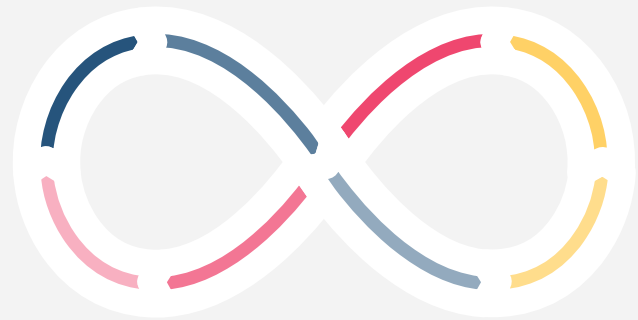
security logs
security tools logs/health
threat detection & incident response



monitor

come?

buy-in aziendale
unico stack tecnologico
miglioramento continuo
automazione



domande?