SPECIALIST SKILL / APPLICATION SECURITY

Fix weaknesses at the point they recur.

Connect code review, dependency governance and delivery controls to the actual application. Prioritize findings the team can reproduce and verify that the remediation changes the exposed behavior.

WHAT WE CAN BUILD FOR YOU

Security review before a major release

Map threats, inspect relevant code and dependencies, and give engineers a prioritized remediation path.

Value: The team spends effort on consequential exposure rather than a context-free issue list.

Controls that survive the next release

Add dependency and pipeline checks around recurring vulnerability patterns and verify the fixes.

Value: The same weakness is less likely to re-enter unnoticed through ordinary development.

WHAT THE ENGAGEMENT INCLUDES

- Threat modelling
- Code review
- Dependency governance
- Pipeline controls

WHAT YOU TAKE AWAY

- Threat model
- Prioritised findings
- Remediation verification

HOW WE MAKE THE VALUE VISIBLE

Verified fixes / Reintroduced findings / Remediation lead time

ILLUSTRATIVE APPLICATIONS / SCOPED TO YOUR SYSTEMS

Let’s scope the first useful step.

Bring the application boundary, release context and findings that repeatedly return.

Talk to BELTO