

Your software has vulnerabilities. The question is who finds them first.

Security gaps rarely announce themselves. They show up in a deal that stalls, an audit that takes too long, or a question you can't answer confidently.

DOES THIS SOUND LIKE YOU?

Nobody flagged security as a problem until it became one. A bigger deal came in, which should have been good news, and it came with a questionnaire attached. Sixty-odd questions about encryption, access controls, audit logs, and compliance certifications. You forwarded it to your CTO, expecting it back by the end of the day. It came back two days later with half the answers missing or hedged. The deal slowed down. No breach happened, no alarm went off, nothing dramatic. But somewhere along the way, your software stopped being good enough for the clients you're now trying to win, and nobody noticed until it was sitting in the way of a signature.

SOUND FAMILIAR?



"We'll get to the security audit eventually"
You've been saying that for two years. A client just made it urgent.



"I'll need a few days to pull that together"
Every compliance request turns into a scramble nobody budgeted for.



"The deal is on hold pending security review"
And you already know some of the answers won't be good enough.



"We're not sure who had access to that"
If something went wrong, you'd be piecing it together after the fact.

COMMON RISK EXPOSURE IN LEGACY SYSTEMS	
Unpatched third-party libraries (CVEs)	CRITICAL
No role-based access control (RBAC)	CRITICAL
Weak or missing encryption at rest	HIGH
No activity audit trail	HIGH
Non-compliant data retention policies	MEDIUM

1

Know where you actually stand | 2 weeks

Most companies have a rough sense that there are gaps. What they don't have is a precise picture of where they are, how serious they are, and what a client or auditor would find if they looked closely. We go through your codebase, dependencies, infrastructure, and access controls and document everything. You leave with a risk-scored report that tells you what's urgent, what can wait, and what you can now answer confidently the next time a security questionnaire lands in your inbox.

2

Prioritized remediation | months 1–3

We fix the highest-risk vulnerabilities first: critical CVEs, access controls, encryption. We work directly in your codebase, no reports that sit on a shelf. Each sprint closes real security gaps, which means each sprint moves you closer to being able to say yes to the next enterprise deal.

3

Compliance framework delivery | months 3–6

Audit trail, data retention policies, RBAC, and access documentation. Everything you need to answer any security questionnaire without a two-day scramble. At project close, you have a compliance pack ready to share and a system that generates audit logs automatically. Enterprise deals that used to stall now close.

Ready to talk through it?

Most companies don't know exactly where their security gaps are until something forces the question, a client audit, a deal that stalls, a questionnaire they can't answer. By that point, the pressure is already on. A first conversation costs nothing, and you'll leave with a clearer picture of where you actually stand, before someone else finds out for you.

Book a 30-min call

WHO WE ARE

We are a Berlin-based software engineering company with 100+ engineers and 15 years of experience delivering complex projects for mid-market companies across the Netherlands, the UK, Scandinavia and others. Our engineering teams operate across Serbia, Bosnia & Herzegovina, and Portugal. We've spent 15 years inside the kind of systems that need modernizing. We know exactly how they break, and how to fix them. We offer both managed modernization projects and dedicated engineering teams, depending on what works best for your organization.

TRUSTED BY TEAMS AT



Mercedes-Benz



bms



mobile.de



intersport



KERBEROS



KAMAX



Gumtree



EnBW



VISUALVEST



ebay



1&1