Christian Schneider
Security Architect · Hacker · Trainer

SECURE SDLC PROCESS REVIEW

Security doesn't stop at your *application code*.

You can pentest an app and fix every finding — and still get breached because the build pipeline was compromised or a dependency auto-update pulled in a malicious package. This is a practical, **conversational review of how your team builds software securely across the whole lifecycle**. Inspired by OWASP SAMM and BSIMM, but not a maturity audit — no scores to defend, no homework.

christian-schneider.net/service/secure-sdlc-process-review ↗

THE LIFECYCLE, END TO END

A guided conversation with the people who actually write, review, ship and run the code. We walk each stage — the profile step routes later questions, so containers, mobile or external contributors only come up when they apply to you.

1. **Context & ownership**
   What you build and who looks after security today.
2. **Delivery & runtime profile**
   How the software is delivered and run — this routes the later sections.
3. **People & guidance**
   The developers, the training and the guidance around them.
4. **Requirements & design**
   Where and how security shows up early, before code is written.
5. **Code & repository**
   What happens in the code and in the repository day to day.
6. **Test & verify**
   How you test, scan and verify — and what happens to the results.
7. **Build & release**
   How you build and ship: pipeline, artifacts, base images, secrets.
8. **Run & operate**
   How you run and patch in production, and DFIR readiness for breaches.

\+ **Coding agent security** OPTIONAL
Secure use of AI coding agents — Copilot, Cursor, Claude Code, MCP. Governance, secrets, supply chain and sandboxing, if that surface is in play for you.

WHY IT MATTERS

- → Compromised build pipelines & supply-chain attacks on the paths code takes into production
- → Scanners that flood teams, then get ignored or switched off — findings, false-positives, baselines
- → Secrets checked into repos, unprotected cloud buckets, weak key & certificate handling
- → DFIR readiness — can you isolate, preserve evidence and rotate keys *before* a breach?

WHAT YOU WALK AWAY WITH

- → An **individual audit catalog**, built with your security team
- → A **scorecard & levels** ("belts") to measure and maintain
- → A prioritised **improvement roadmap** aimed at best leverage
- → Progress made visible — dashboards & trends across the org

IN THE ROOM · WHAT TO BRING

Who: key developers and a tech lead or architect, plus whoever owns the build pipeline, releases or operations. One or two people wearing several hats is completely fine.

Bring: a rough idea of your toolchain — where code lives, how it's built and deployed. No preparation required.

Every engagement starts with a free scoping call.

Most process reviews are individual to your company and current needs. We shape the audit catalog together, then run a streamlined review and improvement roadmap. Let's talk.

GET IN TOUCH
mail@christian-schneider.net
+49 178 3081340 · christian-schneider.net