



SECURITY SPARRING PARTNER

Ihr externer Security-Experte *auf Abruf* — die Lücke zwischen Pentest und Training.

Die meisten Security-Engagements sind projektbasiert. Aber zwischen Pentest, Training und Workshop bleibt der fortlaufende Strom an Architekturentscheidungen, Designfragen und Trade-offs, mit denen Ihre Teams im Alltag konfrontiert sind. Der Retainer füllt genau diese Lücke — Sie haben jemanden auf Kurzwahl, der Architekturen und Angriffsflächen kennt und Ideen mitdenkt, *bevor* sie ausgeliefert werden.

christian-schneider.net/de/consulting/security-sparring-partner ↗

DREI STUFEN

Sparring DER NIEDRIGSCHWELIGE EINSTIEG

Ein regelmäßiger externer Blick auf Ihre Sicherheitsentscheidungen.

- › Monatlicher Review-Call zu dem, was bei Ihnen ansteht
- › Ad-hoc-Fragen per E-Mail oder Chat — kein Call nötig
- › Proaktives Monitoring Ihres Tech Stacks
- › Bevorzugte Terminierung & Rabatte auf Projektarbeit

Advisory DER STRUKTURIERTE SECURITY-RHYTHMUS

Mehr Einbindung, mehr Struktur, tiefere Integration.

- › Alles aus Sparring, plus:
- › Zweiwöchentliche Review-Calls
- › Findings Triage: Scanner-Output sortieren
- › AI Coding & Agentic Workflow Guidance
- › Vierteljährliches Architektur-Deep-Dive
- › Optional: DNS- & Domain-Monitoring

Embedded ALWAYS-IN-THE-LOOP

Ich werde fester Bestandteil davon, wie Ihr Team über Sicherheit nachdenkt.

- › Alles aus Advisory, plus:
- › Wöchentliche Review-Calls
- › Teilnahme an Design Reviews kritischer Features
- › Laufende Threat-Model-Pflege (Attack Tree / Threagile)
- › Strukturierte Security-Verbesserungs-Roadmap
- › Optional: Externes Attack-Surface-Monitoring
- › Hands-on-Unterstützung bei Security Incidents

WARUM RETAINER STATT STUNDENBUCHUNG?

Bei Stundenbuchung zögern Teams, „eine Stunde zu verbrennen“ für kurze Architektur- oder Dependency-Fragen. Der Retainer dreht das um: die Zeit ist reserviert, also wird sie genutzt — *bevor* Entscheidungen final sind. Kunden engagieren sich 2–3× häufiger; der Fokus verlagert sich von Firefighting zu Prävention.

SCHWERPUNKTE WÄHLEN

- **Allgemeine Security-Architektur**
Dependency-Entscheidungen, Auth-Muster, API-Design, Infrastruktur-Hardening — die alltäglichen Trade-offs.
- **Agentic AI Security**
Threat Modeling für neue Agenten, Reviews bestehender Deployments, MCP- & Tool-Chain-Risiken.
- **Secure Development Lifecycle**
CI/CD-Hardening, Dependency-Mgmt, Secure Coding — inkl. Review von AI-generiertem Code.
- **Cloud & Infrastruktur Security**
IaC-Reviews, Cloud-Configuration-Assessments und Supply-Chain-Hardening.

WIE ES FUNKTIONIERT

- 1 Scoping-Call zu Teamstruktur, Tech Stack und Schwerpunkten.
- 2 Stufe wählen — Mindestlaufzeit i. d. R. 6 Monate.
- 3 Kadenz & Kanäle einrichten: Calls, Chat, E-Mail.
- 4 Teams nutzen den Retainer aktiv — Architektur, Reviews, Triage.
- 5 Stunden gelten „use it or lose it“ — kein Rollover.

SCOPE Advisory-Beziehung — keine CISO-Rolle, kein Compliance-Sign-off, kein dediziertes Pentesting oder mehrtägiges Training. Separat verfügbar, für Retainer-Kunden vergünstigt.



Welche Stufe passt zu Ihrem Team?

Jedes Engagement startet mit einem kostenlosen Scoping-Call, um Stufe, Schwerpunkte und Kadenz auf Ihren Stack und Ihre Teamstruktur zuzuschneiden.

KONTAKT

mail@christian-schneider.net

christian-schneider.net