# Adwin Chee

adwin.hansen@gmail.com | linkedin.com/in/adwin-chee | github.com/cs-ach

## Education

**Taylor's University** — Subang Jaya, Malaysia
*Bachelor of Software Engineering (Hons), Extension in Cybersecurity* — *Expected Dec. 2026*

## Experience

**Software Engineer Intern** — Apr. 2026 – Dec. 2026 (Expected)
*SeeSharp Solutions Sdn Bhd* — *Malaysia*

- Delivered features across **seven repositories** (.NET/ABP, Next.js dashboards, native iOS Swift/Android Kotlin, Gatling suite), authoring **500+ commits**.
- Built multi-tenant infrastructure for a **WhatsApp Business SaaS**: per-tenant connection strings, Meta Cloud API template quality tracking, consent opt-in/opt-out, and **Stripe add-on billing** with prorated rates.
- Implemented sign-in, sign-out, and redirect flows for an **authentication consolidation** of three apps onto one commercial site, with JWT, auto-logout on token expiry, and cross-app redirects.
- Added **server-side authorization guards** to campaign and automation services after finding inactive templates were rejected only client-side, bypassable via direct API calls.
- Cut a recipient-resolution hot path from an **N+1 query per recipient to a single batched fetch**, and paginated an unbounded conversation endpoint that loaded entire tenant histories.
- Co-built an internal **desktop test-automation platform** (Electron, .NET, PostgreSQL) unifying Playwright and Gatling, with script recording, nested preconditions, and a CI layer with API-key auth and remote headless execution.
- Ran **load, stress, and breakpoint testing** of a high-traffic client web platform across test, staging, and production, fixing **user-ID collisions** across concurrent virtual users that silently corrupted results.
- Shipped an **invoice dashboard** (Next.js, TypeScript) with queue-based WhatsApp reminders, plus booking, membership, and shop features for a consumer app's native **iOS and Android** clients.

## Projects

**Zero Trust Architecture Platform** | *Node.js, React, TypeScript, JWT, WebCrypto* — Oct. 2025 – Dec. 2025

- Designed a **continuous-verification session engine** that scores every request rather than trusting a valid credential, accumulating risk from IP changes, idle time, and request-rate anomalies to maintain a live per-session trust score.
- Bound **token lifetime to trust level** — 2 hours at full trust, degrading to 5 minutes below a 70 threshold — with automatic session revocation under 60 and **step-up authentication** triggered in the 60–80 band.
- Implemented **hybrid encryption** for file storage: AES-256-GCM authenticated encryption with per-payload IVs, wrapped by RSA-2048 OAEP key encapsulation, plus PBKDF2-SHA256 password hashing at 200,000 iterations.
- Defended against token tampering by pairing JWT signature validation with an independent **HMAC-SHA256 nonce** and device-ID binding, recomputed and verified on every request.

**Neobank Prototype** | *Node.js, Express, WebCrypto* — Dec. 2025

- Applied the zero-trust session and cryptography layers to a **digital banking prototype**, placing account and transaction endpoints behind the same continuous-verification model.
- Layered the backend (route, service, infrastructure) with centralised logging and encrypted-at-rest account records.

## Technical Skills

**Languages**: C#, TypeScript, JavaScript, Java, Swift, Kotlin, Python, SQL, HTML/CSS
**Frameworks**: .NET, ABP Framework, React, Next.js, Node.js, Electron, Express, Hangfire
**Security**: Zero Trust architecture, AES-256-GCM, RSA-OAEP, PBKDF2, HMAC, JWT, OAuth/OpenIddict, threat modelling
**Testing**: Playwright, Gatling, load, stress & breakpoint testing
**Tools & Databases**: Git, Docker, GitHub Actions, Postman, Maven, PostgreSQL, SQLite, Stripe