

Secure what your business *exposes*.

Compliance readiness, security assessment and penetration testing for SMBs and SaaS — to meet the requirements of your clients, insurers and partners.

Our edge: we also build the systems we test.

Web / API

Pentest

SOC 2 readiness

PIPA

OWASP

Bilingual EN / FR

We build software *too*.

Most security consultants hand you a list of findings and leave. We write production software — so when we find something, we tell you how to fix it, in terms your developers can act on. And if you would rather we fix it with you, we can.

Dual expertise

We build and we test. The remediation plan is delivered, not just the finding.

Documented methodology

Seven phases, OWASP / PTES / NIST. A scope defined in writing, no improvisation.

Local presence

Based in Edmonton, available by appointment. A single point of contact.

Bilingual

Bilingual service in French and English — rare in this market.

Most companies don't buy security because they want it. *They buy it because an insurer, or a customer, is asking for proof.*

We help small and mid-sized companies answer those requirements — clearly, at a fixed price, and without a six-month program.

100+

schools running on our own SaaS product

7

phases in our security methodology

EN / FR

bilingual delivery, from Edmonton

Three specialities, *one discipline*.

S / 01

Compliance readiness

Know where you stand before someone else tells you. Gap analysis against one framework, control inventory, prioritized roadmap and policy templates.

SOC 2 • ISO 27001 • PIPA • PIPEDA (where applicable) • PCI-DSS (payments) • Client questionnaires

S / 02

Attack surface assessment

What an attacker sees of your organization from outside — exposure, services, configuration. No intrusive testing.

Internet exposure • DNS • TLS • Technologies • Configuration

S / 03

Web & API penetration testing

Full application penetration test, seven-phase methodology. Written scope, firm price, actionable report.

OWASP Top 10 • REST / GraphQL API • Multi-tenant & IDOR • Business logic • CVSS 3.1

If either one turns up something serious, that is when we talk about a full penetration test — quoted separately, also at a fixed price.

We also build *what we test*.

From client portal to full SaaS, with the cloud foundations that come with it. Secure by design — not tested as an afterthought. It's our edge, not our opening line.

B2B SaaS · Client portals · REST & GraphQL APIs · Multi-tenant · Next.js · Cloudflare · CI/CD

OUR APPROACH

Secure by design — *security is not optional*.

01

Scoping

Structured discovery. We identify your real challenges before proposing any technical solution.

03

Development

Modern stack, secure coding, reviews, tests. The code we write is built to last.

05

Deployment

Secure cloud infrastructure, CI/CD, active monitoring. You launch with confidence.

02

Design

Architecture, data, security, scalability — designed together from the start, not bolted on.

04

Audit

Seven-phase methodology: reconnaissance, authentication and sessions, access control, OWASP Top 10, API, business logic, logging and detection.

06

Follow-up

Maintenance, evolutions, security watch. We stay partners after the initial delivery.

Not every phase applies to every engagement. The scope — what is tested and what is not — is defined in writing before any work begins.

METHOD

Method in *seven phases*.

Seven-phase security testing methodology built on OWASP, PTES and NIST SP 800-115, with CVSS 3.1 severity scoring.

- 01 Reconnaissance
- 02 Authentication & sessions
- 03 Access controls & IDOR
- 04 OWASP Top 10
- 05 API testing
- 06 Business logic
- 07 Logging & detection

Not every phase applies to every engagement — the scope is set in writing.

HOW WE WORK

Fixed price

Always quoted in writing. No open-ended scope.

Nothing starts without authorization

Signed scope, signed testing authorization, signed NDA. No exceptions.

Critical findings, reported immediately

Not held back for the final report.

Written scope

What we test — and explicitly what we don't.

Staging by default

Production only on your written request, with an agreed stop procedure.

Insured

Professional liability (E&O) and cyber liability in force.

Let's talk about *your project*.

Whether you need a platform designed, an independent security test of an existing application, or simply a structured opinion on a technical decision — we take the time to understand before proposing.

EMAIL contact@kemaintech.ca

PHONE / WHATSAPP +1 438 220 7176

HEAD OFFICE Edmonton, Alberta, Canada

RESPONSE TIME Within 24 business hours

Toho Kemingnan Privat

CYBER SECURITY ANALYST & CEO

Descriptions are indicative. The written scope of work (SOW) governs every engagement. Preparation and assessment services do not confer any compliance status.