

Secure software. *Tested software.*

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.

WHERE WE USUALLY START

S / 02

Attack surface assessment

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

Short, prioritized report

Internet exposure • DNS • TLS • Technologies • Configuration

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.

Gap matrix • roadmap • policy pack • debrief

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

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

WHO THIS IS FOR

- SaaS companies selling to enterprise
- Businesses facing an insurance renewal
- Companies that just received a security questionnaire from a customer
- Teams launching a new application

WHAT MAKES US DIFFERENT

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.

The same people who know how systems are built know where they break.

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.

METHOD

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.

TRACK RECORD

100+

schools running on our own SaaS product

7

phases in our security methodology

EN / FR

bilingual delivery, from Edmonton

**Toho Kemingnan Privat**

CYBER SECURITY ANALYST & CEO

contact@kemaintech.ca

kemaintech.ca

+1 438 220 7176

Edmonton, Alberta

Working languages: English · French