

Sécurisez ce que votre entreprise *expose*.

Préparation à la conformité, évaluation de sécurité et tests d'intrusion pour PME et SaaS — pour répondre aux exigences de vos clients, assureurs et partenaires.

Notre différence : nous développons aussi les systèmes que nous testons.

Web / API

Pentest

SOC 2 readiness

PIPA

OWASP

Bilingue FR / EN

On développe *aussi* des logiciels.

La plupart des consultants en sécurité vous remettent une liste de constats et s'en vont. Nous écrivons du logiciel en production — donc quand nous trouvons quelque chose, nous vous disons comment le corriger, dans des termes que vos développeurs peuvent appliquer. Et si vous préférez qu'on le corrige avec vous, c'est possible.

Double compétence

Nous développons et nous testons. La remédiation est livrée, pas seulement la faille.

Méthodologie documentée

Sept phases, OWASP / PTES / NIST. Un périmètre défini par écrit, pas d'improvisation.

Présence locale

Basés à Edmonton, disponibles sur rendez-vous. Un interlocuteur unique.

Bilingue

Service bilingue en français et en anglais — rare sur ce marché.

La plupart des entreprises n'achètent pas de la sécurité parce qu'elles en ont envie. *Elles en achètent parce qu'un assureur, ou un client, demande une preuve.*

Nous aidons les PME à répondre à ces exigences — clairement, à prix fixe, et sans programme de six mois.

100+

écoles sur notre propre produit SaaS

7

phases dans notre méthodologie de sécurité

FR / EN

service bilingue, depuis Edmonton

Trois expertises, *une seule discipline.*

S / 01

Préparation à la conformité

Savoir où vous en êtes avant que quelqu'un d'autre vous le dise. Analyse d'écart sur un référentiel, inventaire des contrôles, feuille de route priorisée et modèles de politiques.

SOC 2 • ISO 27001 • PIPA • PIPEDA (selon le contexte) • PCI-DSS (paiements) • Questionnaires clients

S / 02

Évaluation de surface

Ce qu'un attaquant voit de votre organisation depuis l'extérieur — exposition, services, configuration. Aucun test intrusif.

Exposition internet • DNS • TLS • Technologies • Configuration

S / 03

Test d'intrusion web & API

Test d'intrusion applicatif complet, méthodologie en sept phases. Périmètre écrit, prix ferme, rapport exploitable.

OWASP Top 10 • API REST / GraphQL • Multi-tenant & IDOR • Logique métier • CVSS 3.1

Si l'une des deux révèle quelque chose de sérieux, c'est là qu'on parle d'un test d'intrusion complet — chiffré séparément, également à prix fixe.

Nous construisons aussi *ce que nous testons.*

Du portail client au SaaS complet, avec les fondations cloud qui vont avec. Sécurisé dès la conception — pas testé après coup. C'est notre avantage, pas notre message d'ouverture.

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

NOTRE APPROCHE

Secure by design — *la sécurité n'est pas une option.*

01

Cadrage

Discovery structurée. Nous identifions vos enjeux réels avant de proposer la moindre solution technique.

03

Développement

Stack moderne, secure coding, revues, tests. Le code que nous écrivons est conçu pour durer.

05

Déploiement

Infrastructure cloud sécurisée, CI/CD, monitoring actif. Vous lancez sereinement.

02

Conception

Architecture, données, sécurité, scalabilité — pensées ensemble dès le départ, pas après coup.

04

Audit

Méthodologie en sept phases : reconnaissance, authentification et sessions, contrôles d'accès, OWASP Top 10, API, logique métier, journalisation et détection.

06

Suivi

Maintenance, évolutions, veille sécurité. Nous restons partenaires après la livraison initiale.

Toutes les phases ne s'appliquent pas à tous les mandats. Le périmètre — ce qui est testé et ce qui ne l'est pas — est défini par écrit avant chaque intervention.

Méthode en *sept phases*.

Méthodologie de test en sept phases fondée sur OWASP, PTES et NIST SP 800-115, avec notation de gravité CVSS 3.1.

- 01 Reconnaissance
- 02 Authentification et sessions
- 03 Contrôles d'accès et IDOR
- 04 OWASP Top 10
- 05 Tests d'API
- 06 Logique métier
- 07 Journalisation et détection

Toutes les phases ne s'appliquent pas à tous les mandats — le périmètre est fixé par écrit.

NOTRE FAÇON DE TRAVAILLER

Prix fixe

Toujours chiffré par écrit. Aucun périmètre ouvert.

Rien ne commence sans autorisation

Périmètre signé, autorisation de test signée, accord de confidentialité signé. Sans exception.

Constats critiques signalés immédiatement

Pas retenus jusqu'au rapport final.

Périmètre écrit

Ce qu'on teste — et explicitement ce qu'on ne teste pas.

Préproduction par défaut

Production uniquement sur votre demande écrite, avec procédure d'arrêt convenue.

Assurés

Responsabilité professionnelle (E&O) et cyber-responsabilité en vigueur.

Parlons de *votre projet*.

Que vous ayez besoin d'une plateforme à concevoir, d'un test de sécurité indépendant sur une application existante, ou simplement d'un avis structuré sur une décision technique — nous prenons le temps de comprendre avant de proposer.

COURRIEL	contact@kemaintech.ca
----------	-----------------------

TÉLÉPHONE / WHATSAPP	+1 438 220 7176
----------------------	-----------------

SIÈGE	Edmonton, Alberta, Canada
-------	---------------------------

DÉLAI DE RÉPONSE	Sous 24 heures ouvrées
------------------	------------------------

Toho Kemingnan Privat

ANALYSTE EN CYBERSÉCURITÉ & CEO

Les descriptions sont indicatives. L'énoncé de travaux (SOW) signé fait foi pour chaque mandat. Les services de préparation et d'évaluation ne confèrent aucun statut de conformité.