

Du logiciel sécurisé. *Du logiciel testé.*

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.

PAR OÙ ON COMMENCE HABITUELLEMENT

S / 02

Évaluation de surface

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

Rapport court et priorisé

Exposition internet • DNS • TLS • Technologies • Configuration

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.

Matrice d'écarts • feuille de route • trousse de politiques • restitution

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

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.

POUR QUI

- Entreprises SaaS vendant à de grands comptes
- Entreprises venant de recevoir un questionnaire de sécurité d'un client
- Entreprises face à un renouvellement d'assurance
- Équipes lançant une nouvelle application

CE QUI NOUS DISTINGUE

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.

Ceux qui savent comment un système se construit savent où il casse.

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.

MÉTHODE

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.

REPÈRES

100+

écoles sur notre propre produit SaaS

7

phases dans notre méthodologie de sécurité

FR / EN

service bilingue, depuis Edmonton

**Toho Kemingnan Privat**

ANALYSTE EN CYBERSÉCURITÉ & CEO

contact@kemaintech.ca

kemaintech.ca

+1 438 220 7176

Edmonton, Alberta

Langues de travail : français · anglais