

Inciter l'innovation

**Grille
d'autoévaluation**
logiciels sur mesure

Votre **logiciel** sur
mesure respecte-t-il
les standards de
sécurité?

Évaluez les risques de votre logiciel sur mesure avec notre grille spécialisée

Pourquoi cette évaluation est-elle essentielle?

La sécurité et la conformité sont devenues des priorités incontournables pour les entreprises qui modernisent leurs technologies. En 2024, **38 % des entreprises** considèrent ces critères comme la principale raison de mise à jour de leurs logiciels, un chiffre qui atteint 55 % pour les grandes entreprises.

Avec l'évolution constante des cybermenaces, un logiciel vulnérable peut compromettre vos données, votre réputation et votre conformité réglementaire. Notre grille d'évaluation rapide vous permet d'identifier les failles potentielles et d'agir avant qu'il ne soit trop tard.

La grille d'évaluation Kezber est un outil simple et efficace qui vous aide à :

Repérer les vulnérabilités

Identifiez rapidement les failles critiques de sécurité qui pourraient compromettre vos données et vos opérations.

Évaluer l'état de votre logiciel

Déterminez si une mise à jour mineure suffit ou si une refonte complète est nécessaire pour répondre aux normes actuelles.

Réduire les risques

Agissez de manière proactive pour limiter les menaces et améliorer la résilience de votre logiciel face aux cyberattaques.



Vos données et votre réputation sont-elles en sécurité?

Cochez les points applicables à votre logiciel pour identifier les vulnérabilités potentielles.*

Signes de vulnérabilité

- ☐ Le logiciel a été développé il y a plus de cinq ans.
- ☐ Absence de correctifs ou de mises à jour réguliers.
- ☐ Le logiciel ne respecte pas les normes de conformité réglementaire telles que la Loi 25, le RGPD, l'ISO 27001 ou le PCI-DSS.
- ☐ Absence de journalisation ou d'audits, il est impossible de tracer les activités utilisateurs ou de détecter les comportements suspects.
- ☐ La gestion des accès est obsolète, le logiciel ne permet pas la gestion des permissions par rôle utilisateur.
- ☐ Le logiciel ne propose pas d'authentification multifacteurs (MFA), laissant les comptes utilisateurs vulnérables à des accès non autorisés.

Indicateurs liés à l'utilisation

- ☐ Les utilisateurs expriment un besoin croissant de nouvelles fonctionnalités.
- ☐ Le logiciel fait l'objet d'attaques récurrentes, ce qui peut indiquer une architecture ou des protections obsolètes.

Problèmes liés à l'environnement technique

- ☐ Le logiciel utilise des protocoles de communication obsolètes, tels que SSL 2.0/3.0 ou TLS 1.0/1.1, qui ne sont plus considérés comme sécurisés.
- ☐ Les données sensibles ne sont pas chiffrées, ce qui augmente le risque de fuite
- ☐ Le logiciel est hébergé sur des systèmes ou serveurs qui ne respectent pas les normes actuelles de sécurité, compromettant ainsi sa fiabilité.
- ☐ Le logiciel repose sur des technologies ou des langages de programmation qui ne sont plus supportés, comme Python 2 ou PHP 5.
- ☐ Le logiciel est incompatible avec les solutions modernes de sécurité, comme les antivirus, les pare-feu, ou les outils de monitoring de sécurité.
- ☐ Il n'existe aucune solution de redondance ou de sauvegarde sécurisée, exposant l'organisation à des pertes de données en cas de panne ou d'attaque.
- ☐ Il n'existe aucun système de surveillance des menaces, ce qui empêche une détection proactive.



- * Cet outil offre un premier aperçu des vulnérabilités potentielles, mais il ne remplace en aucun cas une évaluation approfondie réalisée par un expert de Kezber, qui saura vous guider vers des solutions adaptées et sécurisées.

Interprétation de vos résultats

✓ 0 à 1 case cochée

Félicitations ! Vos pratiques de sécurité sont exemplaires. Continuez à maintenir une rigueur dans la gestion et les mises à jour de votre logiciel.

✓ 2 à 4 cases cochées

Votre logiciel présente certaines vulnérabilités. Il est important de mettre en place un plan de mise à jour rapidement afin de renforcer sa sécurité et d'éviter toute exposition aux cyberattaques.

✓ 5 cases et plus cochées

Votre logiciel pourrait comporter des failles majeures et représenter un risque élevé de cyberattaques. Une mise à niveau importante ou une refonte complète peuvent être nécessaires pour assurer sa sécurité.

Passez à l'action dès maintenant!

Les résultats de cet outil vous donnent un premier aperçu des vulnérabilités potentielles de votre logiciel. Pour aller plus loin, une évaluation approfondie par un expert de Kezber est essentielle. Nos spécialistes vous aideront à analyser en détail vos besoins, à identifier les solutions adaptées et à mettre en place des actions concrètes pour garantir la sécurité et la conformité de vos outils.

Ne laissez pas les failles de sécurité compromettre la sécurité de votre entreprise

**Contactez-nous
pour une consultation
personnalisée!**



« La sécurité logicielle n'est plus un luxe, c'est une responsabilité. Identifier les vulnérabilités est la première étape pour protéger votre entreprise et vos utilisateurs. »

Louis-David Robillard
Directeur du développement logiciel chez Kezber

Préparer l'avenir. Ensemble.

Nous avons l'expertise nécessaire pour vous aider à repenser l'utilisation de vos outils numériques.

Vous souhaitez découvrir comment nous pouvons mettre en place une solution adaptée à votre entreprise ?

Contactez-nous dès aujourd'hui.