

Audit de sécurité et pentest : à quoi s'attendre

Scan, audit, test d'intrusion : ce que recouvre chaque prestation, comment ça se déroule et ce que vous devez en retirer.

10 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/audit-pentest

Impossible de protéger ce qu'on n'a pas mesuré. L'audit de sécurité photographie votre niveau de risque réel ; le test d'intrusion (pentest) le met à l'épreuve comme le ferait un attaquant. Encore faut-il savoir ce que chaque prestation recouvre — les termes sont souvent employés à tort et à travers.

1. Trois prestations à ne pas confondre

- Le scan de vulnérabilités : un outil automatisé repère les failles connues (versions obsolètes, ports ouverts...). Rapide et peu coûteux, mais brut : beaucoup de faux positifs, aucune mise en perspective
- L'audit de sécurité : un expert examine configurations, organisation, sauvegardes, gestion des accès et pratiques, puis évalue les risques dans votre contexte métier
- Le test d'intrusion : l'expert tente réellement de compromettre le périmètre convenu, avec votre autorisation écrite, pour démontrer ce qu'un attaquant obtiendrait concrètement

2. Comment se déroule un pentest

- Cadrage : périmètre précis (site web, réseau externe, réseau interne...), dates, contacts d'urgence, et une autorisation écrite signée — c'est ce qui distingue le test légal de l'intrusion illégale
- Tests en « boîte noire » (sans information préalable), « boîte grise » (avec un compte utilisateur) ou « boîte blanche » (avec la documentation complète)
- Exploitation contrôlée : l'objectif est de prouver l'impact sans jamais perturber la production
- Restitution : un rapport et une réunion d'explication accessibles aux non-techniciens

3. Ce qu'un bon livrable contient

- Une synthèse pour la direction : les 3 à 5 risques majeurs en langage clair
- Le détail technique de chaque constat, avec preuve et niveau de gravité
- Un plan d'action priorisé par rapport effort/impact — pas une liste de 200 lignes toutes « critiques »
- Idéalement, une contre-vérification quelques mois après pour valider les corrections

4. Quand et à quelle fréquence

Un premier audit fait toujours sens : il fixe le point de départ et hiérarchise les chantiers. Ensuite, le rythme dépend de votre exposition : un audit ou pentest à chaque évolution majeure (nouveau site, migration cloud, ouverture d'accès distants), et une revue périodique — annuelle pour les activités sensibles. Un pentest sur un système jamais audité révélera surtout des évidences : commencez par l'audit, corrigez le socle, puis testez.

5. Bien choisir son prestataire

- Exiger une méthodologie décrite et des références vérifiables dans des contextes comparables au vôtre
- Les qualifications comptent : PASSI (qualification ANSSI) pour les audits exigeants, certifications individuelles des intervenants (OSCP...) pour les pentests
- Fuir les rapports « presse-bouton » : un scan automatisé revendu au prix d'un audit se reconnaît à ses faux positifs non triés et à l'absence de mise en contexte métier
- Vérifier l'assurance professionnelle du prestataire et les clauses de confidentialité
- Un bon signe : le prestataire commence par vous interroger sur votre métier et vos enjeux, pas sur votre budget

ATTENTION

Jamais de test d'intrusion sans autorisation écrite signée définissant périmètre, dates et limites : c'est ce document qui distingue légalement la prestation de sécurité d'une intrusion pénalement répréhensible — et il protège les deux parties. Un « pentesteur » qui propose de commencer sans ce cadre est à écarter immédiatement.

L'essentiel à retenir

- 01 Commencer par un audit global avant d'envisager un pentest
- 02 Exiger un périmètre et une autorisation écrite pour tout test d'intrusion
- 03 Vérifier méthodologie, références et assurances du prestataire
- 04 Demander une synthèse compréhensible par la direction
- 05 Traiter le plan d'action par priorité, pas par ordre de la liste
- 06 Re-tester après corrections et à chaque évolution majeure

Questions fréquentes

Combien coûte un audit ou un pentest pour une PME ?

Ordres de grandeur : un audit d'hygiène pour une TPE se chiffre en jours (quelques milliers d'euros), un pentest ciblé (site web, réseau externe) de même, un audit complet de PME en une à deux semaines d'expertise. Le levier d'économie n'est pas de rogner la prestation mais de bien cadrer le périmètre : mieux vaut un pentest sérieux sur votre vrai point d'exposition qu'un survol de tout.

Le test peut-il perturber notre activité ?

Un pentest professionnel se cadre pour l'éviter : exploitation contrôlée, tests intrusifs planifiés hors heures critiques, contact d'urgence des deux côtés pour tout stopper si besoin. L'incident de production causé par un test est rarissime avec un prestataire sérieux — c'est précisément ce que le cadrage écrit organise.

Que faire du rapport une fois reçu ?

Le transformer en plan daté : chaque constat majeur reçoit un responsable et une échéance, en commençant par le meilleur rapport risque/effort (souvent : MFA, sauvegardes, comptes obsolètes — des correctifs rapides). Le rapport qui finit dans un tiroir est le vrai gaspillage : prévoyez dès la commande une contre-vérification à 3-6 mois.

Sommes-nous trop petits pour intéresser un auditeur ?

Non — l'audit se dimensionne : pour une petite structure, un audit d'hygiène d'une journée sur les fondamentaux (mots de passe, sauvegardes, mises à jour, accès, exposition Internet) révèle déjà l'essentiel et coûte peu. C'est aussi souvent le premier pas exigé par un client grand compte ou un assureur.

Pour aller plus loin

ANSSI — prestataires d'audit qualifiés (PASSI) — cyber.gouv.fr/produits-services-qualifies

Cybermalveillance.gouv.fr — annuaire des prestataires labellisés — www.cybermalveillance.gouv.fr/cherche-prestataire

Structurer sans vous noyer dans la paperasse ?

Audit, mise en conformité, chartes et sensibilisation des équipes : un accompagnement à la taille de votre entreprise.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr