AYI NEDJIMI Consultants

Pentest Entreprise 2026 : Méthodologie & Rapport Type

16 mai 2026 • Mis à jour le 17 mai 2026 • 19 min de lecture •

3883 mots • 20 vues •

> À retenir — Pentest entreprise 2026 Un pentest entreprise est une simulation contrôlée d'attaquant offensive contre tout ou partie du SI d'une organisation, livrant rapport et.

À RETENIR

À retenir — Pentest entreprise 2026

Un pentest entreprise est une simulation contrôlée d'attaquant offensive contre tout ou partie du SI d'une organisation, livrant rapport et plan de remédiation.

Quatre formats principaux : **pentest externe** (Internet), **pentest interne** (réseau LAN), **pentest applicatif** (web/mobile/API), **red team** (TTPs APT).

Méthodologies standards : **PTES**, **OWASP WSTG**, **OSSTMM**, référentiel ANSSI **PASSI** obligatoire pour OIV.

Livrables obligatoires : rapport exécutif (8-15 pages), rapport technique (40-120 pages), scoring CVSS 3.1/4.0, plan d'action priorisé, restitution orale 2h.

Budget marché 2026 : **4 000-200 000 € HT** selon ampleur — PME 5-15K€, ETI 15-50K€, grand compte/OIV 50-200K€.

Un **pentest entreprise** est devenu en 2026 une démarche standard pour toute organisation soucieuse de mesurer sa résilience face aux cyberattaques. Au-delà de l'audit déclaratif et du scan de vulnérabilités, le test d'intrusion fournit une **preuve concrète** de la posture sécurité — il démontre par démonstration ce qu'un attaquant peut réellement faire, et ne laisse aucune place à l'interprétation. Cet article synthétise la méthodologie complète d'un pentest entreprise 2026 : les 4 formats principaux (externe, interne, applicatif, red team), les phases standard alignées PTES et OWASP WSTG, la structure du rapport type, le scoring CVSS 3.1 et 4.0, les budgets marché, et les pièges à éviter côté client et prestataire. Issu de 100+ missions menées sur PME, ETI, OIV et OSE françaises 2024-2026.

Réponse sous 24h

Devis gratuit →