Pentest
sur mesure.

Un scanner liste des failles possibles. Un pentest vérifie ce qu'un attaquant peut vraiment faire chez vous. Nos experts cherchent, exploitent et poussent jusqu'où le périmètre le permet. Vous repartez avec un rapport pour la direction, un rapport pour l'IT, et un re-test à 30 jours pour valider vos corrections.

TARIF

Sur devis

selon périmètre et durée

Durée	5 à 10 j
Re-test	Inclus J+30
Rapports	Exécutif + tech
Restitution	Live 2 h

OWASP et MITRE ATT&CK. Accord écrit obligatoire avant toute action offensive.

POUR QUI

PROFIL

Pour les entreprises qui veulent **vérifier concrètement leur protection** avant un lancement, un audit client, une exigence assureur, ou simplement parce qu'aucun test offensif n'a encore été fait. Vous choisissez le périmètre, on mène l'attaque.

POURQUOI MAINTENANT

Nouveau produit en production. Un client demande une preuve. Votre assureur pose des questions. Ou vous voulez enfin savoir **où un attaquant passerait chez vous**.

PÉRIMÈTRES TESTABLES

Quatre familles de cibles. Vous en choisissez une ou plusieurs selon le risque à couvrir.

Web et API

Apps web, API REST / GraphQL, portails. Injection, XSS, auth, logique métier.

Infra et AD

Réseau interne, Active Directory, serveurs. Escalade, mouvements latéraux.

Cloud

AWS, Azure, GCP. IAM, stockage exposé, Kubernetes, conteneurs.

Mobile

iOS et Android. Stockage local, chiffrement, interception du trafic.

MODES D'INTERVENTION

Ce schéma montre combien d'information on reçoit avant le test. Plus la barre est remplie, plus le testeur part avec des infos.

Boîte blanche WHITE BOX	 Info fournie : maximale	Code source, schémas, comptes admin. Couverture large, y compris menace interne à hauts privilèges.
Boîte grise GREY BOX, RECOMMANDÉE	 Info fournie : comptes de test	On simule un attaquant **déjà authentifié**. Meilleur rapport couverture / budget pour un premier pentest.
Boîte noire BLACK BOX	 Info fournie : minimale	Presque rien au départ. Plus proche d'une attaque externe, plus long à cadrer.

DÉROULEMENT

Cinq temps, du cadrage au re-test. Rien ne démarre sans accord écrit.

01

Cadrage

Périmètre, mode (blanche / grise / noire), règles. **Accord écrit obligatoire.**

02

Reconnaissance

On cartographie ce qui est exposé et accessible depuis l'extérieur.

03

Exploitation

On tente d'entrer et d'avancer. **Alerte le jour même si critique.**

04

Restitution

Session live. Impact métier et plan d'action priorisé.

05

Re-test

À J+30, on vérifie les correctifs. **Attestation remise.**

AVANT LE TIR

Cadre juridique

Aucune action offensive sans **accord écrit** et règles d'engagement validées. Périmètre, horaires, exclusions et contacts d'urgence sont fixés avant le démarrage.

Fournisseurs cloud

Si la cible est chez AWS, Azure, GCP ou un hébergeur équivalent, on vous aide à **prévenir le fournisseur** pour éviter le blocage de nos IP.

NIVEAUX D'IMPACT

On priorise selon ce qu'une attaque vous coûterait vraiment, pas seulement selon un score technique.

Prise de contrôle du SI

Ransomware, exfiltration, arrêt d'activité

Chiffrement, vol de base clients, comptes admin. Plusieurs jours d'arrêt possibles, avec obligations RGPD ou NIS2. Alerte le jour même.

Compromission ciblée

Compte utilisateur, données partielles, point d'entrée

Le pied dans la porte. Pas la catastrophe immédiate, mais ça ne reste pas contenu sans correction. À traiter sous quelques semaines.

Exposition utile à l'attaquant

Information, surface d'attaque, tremplin

Infos ou portes mal fermées qui préparent une vraie attaque. Moins urgent seul, à traiter une fois les points critiques fermés.

CE QUE VOUS RECEVEZ

Rapport direction

Niveau de risque, failles critiques, impact métier, 3 actions immédiates. **Prêt pour le COMEX.**

Rapport IT

Chaque faille détaillée avec correctif. **Exploitable par vos équipes ou votre prestataire.**

Restitution live

Session avec direction et équipes pour expliquer les findings et bâtir le plan d'action.

Attestation J+30

Après vérification des corrections. **Présentable clients et assureur.**

CONDITIONS

Sur devis, selon périmètre, mode et durée (5 à 10 jours en général).

Convention signée et règles d'engagement validées avant toute action. Notification cloud si besoin.

Re-test inclus à J+30. Restitution live 2 h comprise.

Méthodologie **OWASP et MITRE ATT&CK**. Interlocuteur unique du devis au rapport.

SUITE NATURELLE

Red *Team*

Scénario multi-vecteurs (technique, phishing, physique) avec objectif métier. À partir de 14 000 €.

Pack *NIS2 / ISO 27001*

Gap analysis, plan de remédiation et documentation pour l'auditeur. À partir de 7 500 €.

Cyber *Résilience*

Programme annuel : pentest récurrent, supervision continue, exercice de crise. Sur devis.