CYBERESIST

PLATEFORME D'AUDITS DE CYBERSÉCURITÉ AUTOMATISÉS

SOLUTION DE PENTESTS-AS-A-SERVICE

POUR VOS SURFACES D'ATTAQUE EXTERNE, INTERNE ET CLOUD

- Pré-Scan pour déterminer le nombre de sous-domaines et valider le périmètre d'audit
- Recherche des fuites de données et OSINT
- Scan complet avec tests semi-offensifs
  - Analyse et cotation des vulnérabilités
  - Test des identifiants et mots de passe piratés
  - Analyse des chemins d'attaque
- Génération d'un Rapport d'audit détaillé
  - Synthèse managériale claire
  - Recommandations de solutions
  - Plan d'action et suivi de la remédiation

ABONNEMENT POUR MONITORING EN CONTINU

- Pour renouveler régulièrement les audits
- Recherche de nouvelles fuites et vulnérabilités, mesure d'écart entre les audits, la gestion d'alertes…

ANALYSE DES VULNÉRABILITÉS

Tableaux de bord complets

Analyse et classement par gravité et typologie

Pourquoi choisir CYBERESIST ?

Solution souveraine avec architecture sécurisée, hébergée en France chez OVH.

Audits 100% automatisés : personnalisation des tests pour découvrir vos angles morts de sécurité.

Rapports en Français

JE CHOISIS LA FRENCH TECH

FRANCE CYBER SECURITY LABEL FRANCE CYBERSECURITY 2026

80% des organisations auditées ont des données sensibles référencées dans les moteurs de recherche et une vulnérabilité issue du top 10 OWASP permet de **prendre le contrôle d'un serveur ou d'accéder à des données confidentielles**.

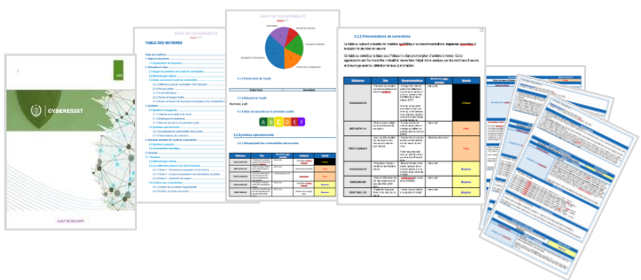
70% des organisations auditées ne possèdent aucun mécanisme de protection implémenté.

50% des organisations diagnostiquées n'ont jamais réalisé d'audit de sécurité.

40% des audits permettent de découvrir des serveurs à l'abandon ou non inventoriés.

RAPPORT AUTOMATISÉ & PLAN D'ACTION

CYBERESIST vous propose des correctifs que vous pouvez directement gérer dans un **tableau de bord pour le suivi de la remédiation.**



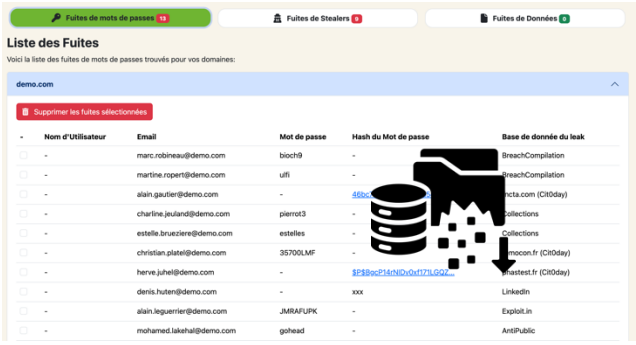
CYBERESIST

CYBERESIST AUTOMATISE LES TESTS DE SÉCURITÉ DES SURFACES D'ATTAQUE

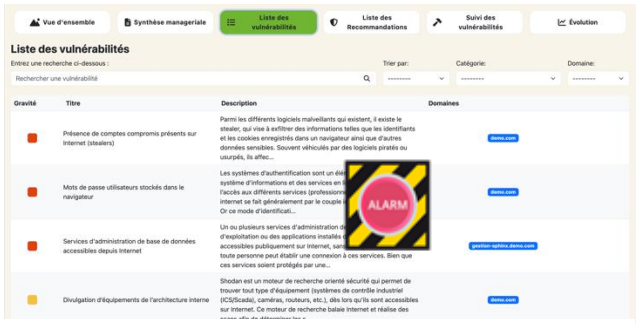
Détecte toutes les failles de sécurité que les hackeurs peuvent exploiter
et présente les facteurs de risque avec un plan d'actions correctives.

DES RÉSULTATS CLAIRS ET COMPLETS

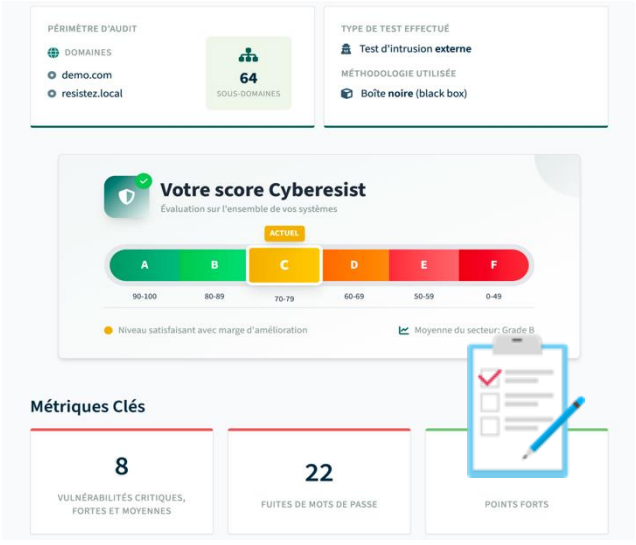
Recherche des fuites de données et comptes piratés, analyse de messagerie, DNS takeover, contrefaçons…



Détection des vulnérabilités et scénarios d'attaque



Calcul de votre cyber score



ACN
Alliance pour la confiance numérique

Membre du groupe de travail Cybersécurité de l'Alliance pour la Confiance Numérique

AUDIT DE SURFACE D'ATTAQUE EXTERNE

Tests réalisés sans sonde, ni agent, ni collecte de journaux d'évènements pour limiter l'impact.

- **Cartographie** des systèmes exposés (Shadow-IT).
- **Recherche des fuites de données :** dark web, forums cybercriminels, comptes compromis, fuites de code-sources, etc.
- **OSINT :** recherches customisées sur les moteurs de recherche, adresses email piratées, DNS takeover…
- **Test de vulnérabilités** pour chaque composant détecté
- **Top 10 OWASP**, inclus des tests d'Injection de données
- **Tests Bruteforce** (découverte de mots de passe)
- **Exploration post-login** avec des compte piratés

ACTIVE DIRECTORY & INFRASTRUCTURE PKI

Prérequis : exécution d'un outil sur une machine connectée au réseau interne avec un compte standard.

- **Identification des comptes à privilèges mal protégés.**
- **Vérification des paramètres critiques :** NTLMv1, LDAP anonyme, SMBv1, Spooler/PetitPotam.
- **Audit de gestion des mots de passe :** rotation, RC4, mots de passe exposés dans SYSVOL et partages.
- **Cartographie des chemins d'attaque :** via ACLs, trusts et templates PKI vulnérables (ESC1–ESC11).
- **Évaluation de la résilience opérationnelle :** sauvegardes, recycle bin, monitoring, machines obsolètes.
- **Audit de station de travail :** mots de passe dans le navigateur, gestionnaire de mot de passe, etc.

AZURE ENTRA-ID & MICROSOFT 365

Prérequis : exécution d'un outil sur une machine connectée au réseau interne (avec un compte administrateur.

- **Identification des comptes à privilèges mal protégés.**
- **Sécurité des accès :** MFA, comptes privilégiés, legacy auth, break-glass.
- **Privilèges & identités :** rôles admins, PIM, apps sans propriétaire, principaux services à risque.
- **Posture sécurité tenant :** Secure Score, EDR/AV, Intune, journaux & rétention.
- **Analytics & détection :** sign-ins à risque, activités suspectes, connexions inhabituelles.
- **Conformité & résilience :** GDPR, politiques de rétention, backup & réponse aux incidents