



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



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**.

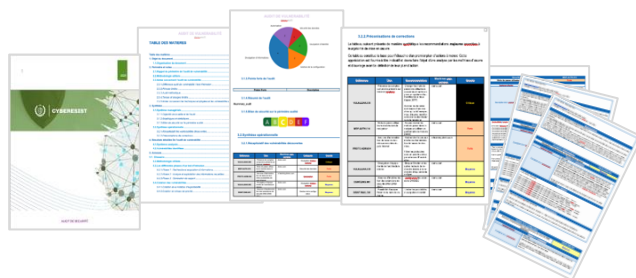
70% des organisations auditées ne possèdent aucun mécanisme de protection implémenté.

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 AUTOMATISE LES TESTS DE SÉCURITÉ DES SURFACES D'ATTAQUE

Détecte toutes les failles de sécurité que les hackers 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...

Voici la liste des fuites de mots de passe trouvés pour vos domaines:

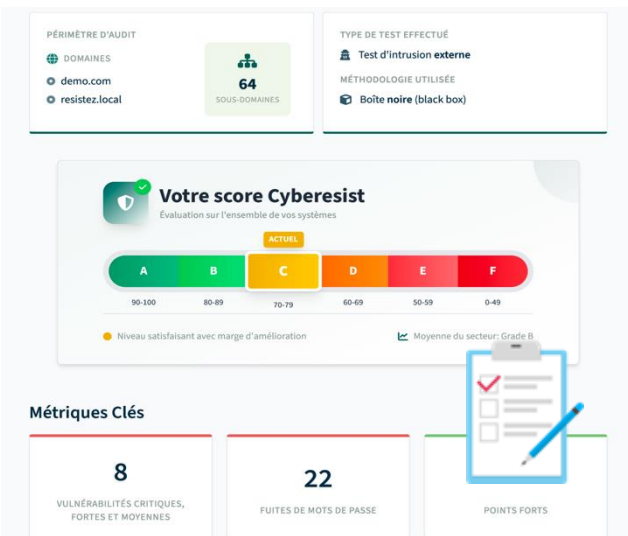
Nom d'utilisateur	Email	Mot de passe	Hash du Mot de passe	Base de données du leak
marc.robinet@demo.com	marc.robinet@demo.com	blach9	-	breachCompilation
martine.rp@demo.com	martine.rp@demo.com	ufl	-	breachCompilation
alain.gautier@demo.com	alain.gautier@demo.com	-	60a0c...	breachCompilation (CIRday)
charline.jeuland@demo.com	charline.jeuland@demo.com	piemot3	-	collections
estelle.bruciere@demo.com	estelle.bruciere@demo.com	estelles	-	collections
christian.platel@demo.com	christian.platel@demo.com	35700LMF	-	procon.fr (CIRday)
herve.juhel@demo.com	herve.juhel@demo.com	-	\$P\$BocP34nDv0u172LGG...	procon.fr (CIRday)
denis.huten@demo.com	denis.huten@demo.com	xxx	-	LinkedIn
alain.leguerrier@demo.com	alain.leguerrier@demo.com	JMRAUFUK	-	Exploit.in
mohamed.lakehal@demo.com	mohamed.lakehal@demo.com	gohead	-	AntiPublic

Détection des vulnérabilités et scénarios d'attaque

Voici la liste des vulnérabilités :

Gravité	Titre	Description	Domaines
Haute	Présence de comptes compromis présents sur Internet (stealers)	Permet les différents logiciels malveillants qui existent, il existe le stealer, qui vise à extraire des informations telles que les identifiants et les cookies enregistrés dans un navigateur ainsi que d'autres données sensibles. Souvent véhiculé par des logiciels piratés ou usurpés, il affecte...	demo.com
Moyenne	Mots de passe utilisateurs stockés dans le navigateur	Les systèmes d'authentification sont un des systèmes d'information et des services en accès aux différents services professionnels Internet ou fait globalement par le couple. Or ce mode d'authentification...	demo.com
Moyenne	Services d'administration de base de données accessibles depuis Internet	Un ou plusieurs services d'administration d'exploitation ou des applications installées accessibles publiquement sur Internet, sans toute personne peut établir une connexion à ces services. Bien que ces services soient protégés par une...	demo.com
Basse	Divulguation d'équipements de l'architecture interne	Shodan est un moteur de recherche orienté sécurité qui permet de trouver tout type d'équipement (systèmes de contrôle industriel (SCADA), caméras, routeurs, etc.) dès lors qu'ils sont accessibles sur Internet. Ce moteur de recherche balaye Internet et réalise des...	demo.com

Calcul de votre cyber score



AUDIT DE SURFACE D'ATTAQUE EXTERNE

Tests réalisés sans sonde, ni agent, ni collecte de journaux d'événements 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