Aurveil

ON CHERCHE. ON TROUVE. AVANT EUX.

Audit de cybersécurité externe pour les PME et ETI

thibault.py@aurveil-cyber.fr | 06 16 13 80 11

Comment ça marche ?

Votre exposition cyber, cartographiée en 72h. Sans installation ni accès requis.

01

Périmètre cible

Vous nous fournissez simplement votre nom de domaine principal (ex: entreprise.fr). Aucun agent à installer, aucun mot de passe requis.

02

Analyse automatisée

Scans de ports (Nmap), cartographie DNS (WHOIS, sous-domaines exposés) et analyse profonde de la configuration de sécurité de vos emails.

03

Corrélation des failles

Chaque service découvert est croisé avec la base nationale des vulnérabilités (NVD). Les failles (CVE) sont identifiées et scorées.

04

Restitution sous 72h

Livraison d'un rapport comprenant un score global de synthèse pour la direction, et un plan d'action technique priorisé pour votre IT.

Ce que nous détectons de l’extérieur :

• Services & Ports ouverts
Services d'administration indûment exposés sur le web.

• Failles logicielles (CVE)
Versions obsolètes ou serveurs non patchés prêts à être exploités.

• Usurpation Email
Absence ou mauvaise configuration des protocoles SPF, DKIM et DMARC.

thibault.py@aurveil-cyber.fr

Nos Offres d'Audit

SURFACE EXTERNE

Audit d'Exposition

À partir de 290€

- Cartographie complète des sous-domaines
- Scan de ports et détection de CVE
- Audit configuration DNS & Emails
- Livrable : Rapport PDF (Synthèse + IT)

FACTEUR HUMAIN

Simulation de Phishing

À partir de 390€

- Scénarios personnalisés réalistes
- Mesure précise du taux de clic
- Identification des populations cibles
- Contrat d'autorisation strict signé

OSINT

Fuite de Données

À partir de 290€

- Recherche d'identifiants sur le Dark Web
- Analyse des documents publics (métadonnées)
- Cartographie des fuites d'informations

SURVEILLANCE

Veille Mensuelle

Dès 149€ / mois

- Scan récurrent automatisé chaque mois
- Alerte immédiate sous 24h si faille critique
- Synthèse trimestrielle d'évolution

Sans engagement de durée (sur l'abonnement)

06 16 13 80 11

Étude de cas en conditions réelles

Secteur : E-commerce — Région Pays de la Loire (Juin 2026)

Synthèse des vulnérabilités découvertes

Périmètre analysé de l'extérieur sans accès initial

62
SCORE / 100

Sévérité	Vulnérabilité identifiée	Impact Business Potentiel
CRITIQUE	**Configuration Email défaillante**	Usurpation d'identité (Phishing au nom du dirigeant).
IMPORTANT	**Absence de Headers HTTP de Sécurité**	Sensibilité accrue aux vols de sessions utilisateurs.
MODÉRÉ	**Services exposés inutilement**	Attaques par force brute sur SSH (2222) et Nagios (8000).
MODÉRÉ	**Composants Web Obsolètes**	5 failles CVE actives indexées sur l'architecture Nginx.

Plan d'action correctif appliqué :

1. **Priorité immédiate :** Déploiement d'une politique DMARC stricte pour verrouiller le domaine.
2. Injection des 4 entêtes HTTP essentiels dans la configuration du serveur web de production.
3. Whitelisting IP pour restreindre l'accès à SSH et Nagios aux seules connexions de confiance.

Pourquoi agir aujourd'hui ?

60%

des PME victimes d'une cyberattaque fermeture leurs portes dans les 18 mois.

1 / 2

PME n'a configuré aucune protection email solide (SPF/DKIM/DMARC).

35 K€

C'est le coût financier direct moyen d'une attaque sur une PME française.

#1

Les PME et collectivités locales sont les cibles prioritaires (ANSSI).

Les engagements Aurveil

- **Détection proactive :** Bloquer les risques avant l'exploitation par un tiers malveillant.
- **Rapports décisionnels :** Pas de jargon complexe. Un score, 3 priorités claires pour la direction.
- **Analyse de proximité :** Un expert basé dans les Pays de la Loire pour un accompagnement réactif.

Cartographiez votre exposition cyber sous 72h

thibault.py@aurveil-cyber.fr | 06 16 13 80 11