# Aurveil

***On cherche. On trouve. Avant eux.***

Audit de cybersecurité pour les PME et ETI

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

# Aurveil

CYBERSECURITE

*On cherche.* *On trouve.* *Avant eux.*

## Votre exposition cyber, cartographiée en 72h.

Sans accès a vos systèmes. Sans installation. Sans jargon.

## Comment ça marche — 3 étapes, 72h, zéro accès

01

### ① Vous nous donnez votre domaine (ex: monentreprise.fr)

Nmap scanne vos ports et services exposés. WHOIS analyse votre domaine. SSL, SPF/DKIM/DMARC, CVE : tout est vérifié automatiquement. Zéro accès à vos systèmes, zéro installation chez vous.

02

### ② Aurveil analyse votre exposition en moins de 72h

Chaque service détecté est croisé avec la NVD (National Vulnerability Database). Les CVE actives sont scorées CVSS (0 à 10). Réputation IP, listes noires spam, sous-domaines exposés : rien n'échappe au scan.

03

### Vérification de votre configuration email

SPF, DKIM, DMARC : on vérifie si votre domaine peut-être usurpé pour envoyer des emails de phishing en votre nom. Faille très fréquente chez les PME.

04

### ③ Vous recevez votre rapport PDF sous 72h

Page 1 — Score global /100 + top 3 priorités (pour le dirigeant). Page 2 — Détail technique : CVE, ports, config email (pour votre IT). Page 3 — Plan d'action classé par urgence et niveau de risque.

## Ce qu'on détecte — sans accés à vos systèmes

- **Ports ouverts inutilement**
  Services exposés qui ne devraient pas l'être
- **Certificats SSL expirés**
  Connexions non securisées, alertes navigateur
- **CVE actives sur vos services**
  Vulnérabilités connues et scorées CVSS
- **Config email faillible**
  Domaine usurpable pour phishing (SPF/DKIM/DMARC)
- **Sous-domaines exposés**
  Entrées oubliées accessibles depuis internet
- **Réputation IP/domaine**
  Présence dans des listes noires spam ou malware

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

# Aurveil

CYBERSECURITE

*On cherche.* *On trouve.* *Avant eux.*

## Nos offres

### Audit Surface Externe — DECOUVERTE

**À partir de 290€**

Scan complet de votre périmètre expose : ports, services, SSL, DNS, configuration email. Score global /100 et plan d'action

- Sans accés a vos systmes
- Rapport PDF dirigeant + IT
- Livraison sous 72h

### Simulation Phishing — HUMAIN

**À partir de 390€**

Campagne de phishing simulé sur vos equipes. Mesure du taux de clics, identification des profils a risque.

- Contrat d'autorisation signé
- Aucun contenu malveillant
- Rapport detaillé inclus

### Audit OSINT/Fuite de données — OSINT

**À partir de 290€**

Cartographie des informations publiques et sensibles de votre entreprise accessibles aux attaquants. Recherche d'identifiants compromis sur le Clear et Dark Web.

- Zéro intrusion de vos systèmes
- Détection de mots de passes fuités
- Rapport de compromission

### Veille Mensuelle Abonnement — — ABONNEMENT

**à partir de 149€/mois**

Scan automatisé chaque mois. Alerte immédiate si CVE critique détectée. Rapport mensuel + synthèse trimestrielle.

- Rapport mensuel automatique
- Alerte critique sous 24h
- Sans engagement 3 mois

## Pourquoi Aurveil

- **Détection avant réaction**
  On intervient avant l'incident, pas après.
- **Rapport lisible par votre direction**
  Un score, trois priorités. Pas 80 pages de jargon.
- **Expert local, Pays de la Loire**
  Intervention rapide sous 5 jours. Pas une hotline nationale.
- **Transparent**
  Pas de surprise, pas de commission cachée, pas de sous-traitance.

**Recevez votre rapport d'exposition cyber en 72h**

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

# Aurveil

On cherche. On trouve. Avant eux.

## Ce qu'Aurveil a trouvé — Cas client réel :

Client e-commerce — Pays de la Loire | Audit Surface Externe | Juin 2026 | CONFIDENTIEL

**62** / 100
**Risques modérés**

**7**
ports ouverts

**5**
CVE détectées

**0**
critique

CRITIQUE **Domaine usurpable**

### Résultats de l'audit

DKIM absent + DMARC absent → n'importe qui peut envoyer un email en votre nom

IMPORTANT **Headers HTTP manquants**

4 protections absentes sur 5 : anti-clickjacking, anti-sniffing MIME, CSP, Referrer-Policy

MODÉRÉ **5 CVE détectées sur nginx**

Versions exposées sur ports 8085 et 8086 — à patcher ou isoler

MODÉRÉ **Services exposés inutilement**

SSH port 2222 + Nagios port 8000 visibles depuis internet

✓ OK SSL valide 87 jours | Domaine actif |0 CVE critique

**Recommandations prioritaires**
**① Configurer SPF strict + DKIM + DMARC reject sur le domaine — priorité immédiate**
**② Ajouter les 4 headers de sécurité HTTP manquants (X-Frame-Options, CSP, X-Content-Type, Referrer-Policy)**
**③ Isoler ou patcher les services nginx exposés sur ports 8085/8086**
**④ Restreindre l'accès SSH (port 2222) et Nagios (port 8000) aux seules IP internes**
**⑤ Mettre en place une veille mensuelle automatisée — Aurveil**

Livré en 72h • Sans accès à leurs systèmes • Sans installation

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

# Aurveil

## 60%

**des PME victimes d'une cyberattaque ferment dans les 18 mois la suivant**

## 1/2

**des PME n'a aucune protection email**

anti-phishing (SPF/DKIM/DMARC)

## 35 000 €

**coût moyen d'une cyberattaque**

**pour une PME française**

## Cibles #1

**Les collectivités locales**
dans le viseur depuis 2023 (ANSSI)

**Aurveil détecte ces failles avant qu'elles soient exploitées.**
Sans accès à vos systèmes. Sans jargon. En 72h.

**Recevez votre rapport d'exposition cyber en 72h**

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