

Audit cybersécurité

Identifier les portes ouvertes avant qu'elles soient utilisées contre vous.

LA PROBLÉMATIQUE

74 % des PME françaises ont subi une cyberattaque en 2025. Les ransomwares ciblent désormais en priorité les structures de 20 à 200 personnes · moins protégées, plus rentables.

DURÉE

**5 jours d'audit · 6 mois
d'accompagnement**

TARIF HT

À partir de 6 800 € HT

FORMAT

Visio + ateliers ponctuels

DOMAINE

**Cybersécurité &
conformité**

DURÉE	TARIF HT	FORMAT
5 jours d'audit · 6 mois d'accompagnement	À partir de 6 800 € HT	Visio + ateliers ponctuels

01 La problématique

74 % des PME françaises ont subi une cyberattaque en 2025. Les ransomwares ciblent désormais en priorité les structures de 20 à 200 personnes · moins protégées, plus rentables.

02 Contexte d'intervention

Pourquoi c'est urgent

03 Objectifs de la mission

À l'issue de la mission, vous obtenez :

Avoir une vision claire de vos vraies failles · ce qui peut être attaqué chez vous, par où, à quelle fréquence

Sortir avec un plan de remise à niveau priorisé · 5 à 8 actions, classées de la plus urgente à la plus tranquille

Mettre au clair votre conformité NIS2 ou DORA si vous êtes concerné · état des lieux honnête, pas un audit pour le tiroir

Repérer les 2 ou 3 trous par lesquels passe vraiment un ransomware (souvent pas là où vous pensez)

Préparer vos collaborateurs aux mails piégés · une formation courte qui tient dans le temps, pas un PDF jamais lu

Tester votre capacité à redémarrer après une attaque · vérification simple de vos sauvegardes, repérage des trous avant qu'il soit trop tard

04 Notre approche, étape par étape

ÉTAPE 01 État des lieux technique

l'expert dédié scanne vos accès, vos comptes, votre réseau interne, vos contrats SaaS sensibles

ÉTAPE 02 Entretiens

vous, votre informaticien (interne ou prestataire), 2 ou 3 collaborateurs, et la personne qui gère les départs RH

ÉTAPE 03 Faux phishing

1 campagne ciblée envoyée à tous vos collaborateurs, on mesure qui clique et on en tire des conclusions sans donner de nom

ÉTAPE 04 Plan de remise à niveau

l'expert priorise par gain/effort, distingue les corrections rapides des chantiers plus longs

ÉTAPE 05 Restitution

1 doc pour vous, 1 doc pour votre informaticien, 1 réunion finale et remise du dossier de conformité

05 Livrables

Documents et outils que vous emportez à la fin de la mission :

Rapport d'audit complet · 25 à 40 pages, lisible côté dirigeant, avec annexes techniques pour votre informaticien

Carte des risques · matrice gravité/probabilité, 1 fichier Excel utilisable

Plan de remise à niveau · 1 doc PDF, 5 à 8 actions chiffrées, jalons à 30 / 60 / 90 jours

Dossier de conformité NIS2 ou DORA (si concerné) · état des lieux et actions à mener pour être en règle

Résultats de la campagne phishing · anonymes, avec un plan de sensibilisation sur 6 mois

Note 3 pages · à présenter à votre assureur cyber, votre comptable ou un partenaire qui demande des garanties

06 Bénéfices attendus

- Vous savez précisément ce qui peut tomber, quand, et combien ça coûterait · la peur de l'inconnu laisse place à des décisions chiffrées
- Vous présentez un dossier propre à votre assureur cyber · la prime peut être renégociée ou une exclusion levée
- Vous traitez NIS2 ou DORA dans les temps sans tomber dans le piège de la conformité-papier
- Vos collaborateurs reconnaissent un mail piégé · le risque humain baisse de façon mesurable en 6 mois
- Vous évitez le coût caché d'un ransomware · le coût moyen d'un incident est 20 fois celui d'un audit

07 Public & prérequis

PUBLIC CONCERNÉ

Dirigeants concernés par NIS2/DORA · Cabinets ayant des données sensibles · PME post-incident

+ Pour aller plus loin

74 % des PME françaises ont subi une cyberattaque en 2025. Les ransomwares ciblent désormais en priorité les structures de 20 à 200 personnes · moins protégées, plus rentables.

Engager la mission

Premier échange de cadrage gratuit avec votre futur expert dédié. Vous repartez avec un avis indépendant et un budget réaliste, même si la mission ne se fait pas.

FRANCE NUM

groupe-mda.fr/conseil/audit-cybersecurite