Audit Cybersécurité PME 2026 : Coût, Méthode et Aides Disponibles

> Audit cybersécurité PME 2026 : types d'audits, méthodologie PASSI, livrables CVSS, coûts 2K-20K euros et aides ANSSI, Cybermalveillance, Bpifrance.

Les cyberattaques contre les PME françaises ont atteint un niveau record en 2025-2026. Selon les données Cybermalveillance.gouv.fr, 60% des victimes d'incidents cyber accompagnées sont des TPE/PME, et 43% d'entre elles ne s'en remettent jamais pleinement. Pourtant, la grande majorité de ces organisations n'a jamais réalisé d'audit de sécurité informatique. L'audit cybersécurité PME est la première étape indispensable pour passer d'une posture subie à une posture maîtrisée face aux risques cyber. Contrairement aux idées reçues, un audit adapté à la taille et aux enjeux d'une PME n'est pas hors de portée financière : des aides ANSSI, des dispositifs Cybermalveillance et des financements Bpifrance permettent d'en couvrir une partie. Ce guide complet vous explique les différents types d'audits disponibles, la méthodologie étape par étape, les livrables à exiger, les coûts réels en 2026, les critères de choix d'un prestataire compétent, et les aides mobilisables pour réduire la facture. Que vous soyez dirigeant, DSI ou DAF d'une PME de 10 à 500 salariés, ce guide vous donne toutes les clés pour commander et valoriser votre premier audit de cybersécurité.

À RETENIR

À retenir :

60% des victimes d'incidents cyber accompagnées par Cybermalveillance sont des TPE/PME : l'audit n'est plus réservé aux grandes entreprises.

Un audit organisationnel de base coûte entre 2 000 et 5 000 euros ; des aides ANSSI, Cybermalveillance et Bpifrance peuvent en couvrir une partie significative.

La certification PASSI de l'ANSSI est le critère de qualité le plus sérieux pour choisir un prestataire d'audit en France.

> Sans plan de remédiation suivi après l'audit, l'investissement est inutile : l'audit n'a de valeur que si ses recommandations sont implémentées.

Pourquoi une PME a besoin d'un audit cybersécurité en 2026

Les PME sont devenues la cible privilégiée des cybercriminels pour des raisons structurelles : elles possèdent des données de valeur (fichiers clients, données RH, propriété intellectuelle) mais disposent de moyens de protection insuffisants. Selon le rapport Cybermalveillance 2024, les ransomwares, hameçonçages et compressions de comptes sont les trois menaces les plus fréquentes pour les PME.

Les conséquences d'une cyberattaque non antécipée sont souvent catastrophiques pour une PME : interruption d'activité de 15 jours en moyenne (ransomware), coûts de remise en état de 50 000 à 250 000 euros, perte de clients liée à la violation de données, atteinte réputationnelle durable. Par rapport à ces risques, le coût d'un audit préventif est marginal.

Différence audit vs pentest vs diagnostic NIS 2

Ces trois types de prestations sont régulièrement confondus. Il est essentiel de comprendre leurs différences pour commander la bonne prestation selon vos besoins :

> ⚡ **Retour terrain**
>
> Lors de mes missions RSSI externalisé, la valeur principale n'est pas technique mais organisationnelle : créer le lien entre la direction et les équipes IT sur les sujets de sécurité. Dans 80 % des cas, les équipes IT ont identifié les risques depuis longtemps mais n'ont pas les mots ou la légitimité pour les porter au niveau direction. Mon rôle est souvent de traduire 'notre EDR génère trop d'alertes' en 'notre temps de détection moyen est de 4 jours pour un incident critique, contre 8 heures dans le secteur'.

L'audit de sécurité

L'audit évalue la conformité de votre organisation à un référentiel de bonnes pratiques (ISO 27001, ANSSI, CIS Controls). Il combine des interviews avec les responsables métier et IT, des revues documentaires (politiques, procédures), et des contrôles techniques limités (configuration des équipements réseau, paramètres des serveurs). Il répond à la question : "Respectez-vous les bonnes pratiques ?" Il n'exploite pas activement les failles.

Le test d'intrusion (pentest)

Le pentest démontre l'exploitabilité réelle des vulnérabilités en simulant une attaque. Le pentester essaie activement de compromettre vos systèmes. Il répond à la question : "Un attaquant peut-il réellement pirater votre SI ?" C'est plus intrusif, plus coûteux, et nécessite une autorisation écrite explicite.

Le diagnostic NIS 2

Le diagnostic NIS 2 est une évaluation spécifique de votre conformité aux exigences de la directive NIS 2 (transposée en France depuis octobre 2024). Il identifie les écarts par rapport aux 21 mesures de sécurité NIS 2, notamment pour les PME sous-traitantes d'OES ou d'OIV. Notre guide NIS 2 complet couvre en détail ces exigences.

Types d'audits pour PME : organisationnel, technique, réseau, AD, cloud

Il n'existe pas "un" audit de sécurité : plusieurs types de prestations correspondent à des besoins et des maturités différents. Voici les cinq types principaux adaptés aux PME :

Audit organisationnel et politique

Cible : toutes les PME, quel que soit leur niveau de maturité technique. Évalue les politiques de sécurité, la gestion des habilitations, les procédures de sauvegarde et de PCA, la sensibilisation des utilisateurs, la gestion des prestataires. Durée : 2-3 jours. Livrable : rapport d'écarts avec recommandations priorisées.

Audit technique de configuration

Revue des configurations des éléments réseau critiques : firewall, switch, serveurs, postes de travail. Vérifie les mises à jour, les règles de filtrage, les paramètres de sécurité des systèmes d'exploitation. Durée : 2-5 jours selon le périmètre. Nécessite un accès aux équipements (pas de test actif).

Audit réseau et infrastructure

Combine revue de configuration et scans actifs (cartographie réseau, détection de services exposés, scan de vulnérabilités). Couvre le périmètre internet (exposition externe), le réseau

interne (segmentation, exposition des serveurs) et les accès distants (VPN, RDP). Durée : 3-5 jours.

Audit Active Directory

Pour les PME disposant d'un Active Directory, c'est l'audit le plus critique : l'AD est la cible principale des ransomwares et des attaquants APT. Il évalue les GPO de sécurité, les comptes privilégiés, les délégations, les SPN Kerberoastables, les mots de passe faibles, et la configuration LAPS. Voir notre guide d'audit AD automatisé PowerShell.

Audit cloud (AWS, Azure, GCP)

Pour les PME ayant migré tout ou partie de leur SI vers le cloud. Évalue la configuration IAM, les politiques de bucket S3 (ou équivalent), les règles de firewall cloud, les journaux d'audit activés, et la conformité aux benchmarks CIS pour AWS/Azure/GCP.

Méthodologie étape par étape : du pré-audit à la restitution

Une prestation d'audit de sécurité bien conduite suit une méthodologie structurée en 5 étapes. Voici le détail de chaque phase :

1. Pré-audit : cadrage et préparation

Définition du périmètre exact (quels systèmes, quels processus, quelles applications), des objectifs (conformité ISO 27001, pré-audit NIS 2, identification des risques prioritaires), du calendrier et des contacts clés. Le prestataire remet un questionnaire de préparation pour optimiser le temps sur site. L'entreprise prépare les éléments demandés : inventaire du SI, schéma réseau, liste des comptes admin, politiques existantes.

2. Collecte sur site et entretiens

Entretiens avec les responsables métier et IT (DSI, RSSI, DPO, RH, DAF), revue documentaire des politiques et procédures existantes, collecte des configurations techniques. Pour les audits techniques, exécution des scans et des contrôles automatiques (Nessus, Lynis, PingCastle pour l'AD).

```
 # Outils de collecte automatique utilises en audit PME

# PingCastle - audit AD en 5 minutes
./PingCastle.exe --healthcheck --server votre-dc.domaine.local
# Genere un rapport HTML avec score de risque AD sur 100

# Lynis - audit de configuration Linux
lynis audit system --quick

# OpenVAS - scan de vulnerabilites
# Nessus Essentials - gratuit pour 16 IPs

# Nmap - cartographie reseau
nmap -sV --script vuln 192.168.1.0/24 -oA audit_reseau
```

3. Analyse et qualification

Le prestataire analyse les données collectées, qualifie chaque vulnérabilité ou écart identifié (gravité CVSS, contexte spécifique PME), et rédige les recommandations de remédiation adaptées aux ressources de l'organisation. Phase la plus longue : 2-5 jours de travail analytique selon le périmètre.

4. Rédaction du rapport

Le rapport final comprend un executive summary (2-3 pages pour la direction), un tableau de vulnérabilités classées par priorité, un plan de remédiation priorisé avec coûts et délais estimés, et les preuves techniques des vulnérabilités identifiées (screenshots, sorties de commandes).

5. Restitution et plan d'action

Présentation des résultats à la direction (focus risques métiers) et aux équipes techniques (détails des vulnérabilités, procédures de correction). Définition du plan d'action avec hiérarchisation des quick wins (corrections immédiates à faible coût) et des projets plus lourds.

Livrables typiques : rapport exécutif, CVSS et plan de remédiation

La qualité des livrables est le principal facteur différenciant entre prestataires. Un rapport de qualité doit inclure au minimum :

```
 STRUCTURE RAPPORT AUDIT PME - LIVRABLE MINIMUM
================================================

1. EXECUTIVE SUMMARY (2-3 pages)
   - Score global de maturite (ex: 42/100)
   - Top 3 risques critiques pour l'activite
   - Budget de remediation estime
   - Recommandation prioritaire

2. TABLEAU DES VULNERABILITES
   - ID | Titre | Categorie | CVSS | Priorite | Effort
   - Ex: VULN-001 | Mots de passe AD faibles | Auth | 8.1 | P1 | Faible
   - Ex: VULN-002 | RDP expose sur internet | Reseau | 9.8 | P0 | Faible

3. PLAN DE REMEDIATION
   - Mesure | Echance | Pilote | Cout estime | Statut
   - Quick wins (<1 semaine, <1000 euros)
   - Projets moyen terme (1-3 mois)
   - Projets long terme (3-12 mois)

4. ANNEXES TECHNIQUES
   - Preuves des vulnerabilites
   - Sorties d'outils
   - Configurations recommandees
```

Pour les audits avancés avec composante Active Directory, notre guide d'audit AD automatisé PowerShell fournit les scripts de collecte et d'analyse utilisés par les prestataires PASSI.

Coûts 2026 : fourchettes par type d'audit

Les tarifs des audits de cybersécurité varient selon le type d'audit, l'étendue du périmètre, la certification du prestataire et la région. Voici les fourchettes observées en France en 2026 :

Audits organisationnels

Audit organisationnel de base (revue politique, processus, sensibilisation) : 2 000 à 5 000 euros pour une PME de 20-100 salariés. Inclut généralement 2 jours de prestation et un rapport de 30-50 pages.

Diagnostic NIS 2 / pré-audit ISO 27001 : 3 000 à 8 000 euros. Plus approfondi, inclut un plan de mise en conformité détaillé et une estimation de l'effort de certification.

Audits techniques

Audit réseau et infrastructure : 3 000 à 8 000 euros. Couvre la cartographie réseau, les scans de vulnérabilités et la revue de configuration des équipements.

Audit Active Directory : 2 500 à 6 000 euros. Spécialisé, à réaliser en priorité si vous disposez d'un AD (90% des PME françaises).

Pentest web application : 3 000 à 8 000 euros. Test d'une application web en boîte grise, 3-5 jours de test, rapport CVSS.

Pentest interne complet : 8 000 à 20 000 euros. Simule une compromission depuis le réseau interne, inclut AD, mouvements latéraux, élévation de privilèges. Détaillé dans notre guide pentest interne 2026.

Critères de choix d'un prestataire : PASSI, CREST, références

Le marché des prestataires de sécurité est hétérogène. Voici les critères de sélection par ordre de priorité :

Qualification PASSI ANSSI

La qualification PASSI de l'ANSSI est le niveau de confiance le plus élevé en France. Elle garantit que le prestataire a été audité sur sa méthodologie, ses compétences et ses processus qualité. La liste des prestataires qualifiés est publique sur le site de l'ANSSI. Pour les PME sous-traitantes d'OES/OIV ou soumises à des exigences contractuelles élevées, un prestataire PASSI est très recommandé.

Certifications individuelles des auditeurs

Les certifications individuelles reconnues en France : OSCP (Offensive Security), CEH (EC-Council), GPEN/GWAPT (SANS GIAC), CREST (certification UK/internationale). Demander les CV des auditeurs affectés à votre mission, pas seulement les certifications de l'entreprise.

Références et spécialisation sectorielle

Demandez des références de clients PME similaires (même secteur, taille comparable). Un prestataire spécialisé dans votre secteur (santé, industrie, collectivité) connaît les risques et réglementations spécifiques. Les associations professionnelles comme Hexatrust regroupent des prestataires français vérifiés.

Checklist pré-audit : ce que vous devez préparer

Une bonne préparation permet de maximiser le temps d'audit et la qualité des recommandations. Voici la checklist à préparer avant l'arrivée du prestataire :

```
 CHECKLIST PRE-AUDIT PME
=======================
[ ] Inventaire du parc informatique (postes, serveurs, équipements réseau)
[ ] Schéma réseau actuel (avec VLANs si existants)
[ ] Liste des applications métier critiques
[ ] Liste des comptes admin (Windows, Linux, applicatifs)
[ ] Derniers rapports de vulnérabilités disponibles (scans, audits précédents)
[ ] Politiques de sécurité existantes (PSSI, charte utilisateur)
[ ] Inventaire des prestataires avec accès au SI
[ ] Procédures de sauvegarde actuelles (RTO/RPO)
[ ] Contrats assurance cyber en cours
[ ] Liste des incidents de sécurité des 24 derniers mois
```

La procédure d'homologation ANSSI exige également une analyse de risques complète, pour laquelle l'audit préalable est un prérequis précieux.

Aides et financements : ANSSI, Cybermalveillance, Bpifrance

Le financement d'un audit de sécurité pour une PME bénéficie de plusieurs dispositifs publics dont peu d'entreprises ont connaissance :

Dispositif MonAideCyber (ANSSI)

L'ANSSI propose le programme MonAideCyber, un diagnostic de sécurité gratuit de 4 heures réalisé par un réseau de 2 000 aidants bénévoles qualifiés. Il fournit une liste de 6 recommandations prioritaires adaptées à votre contexte. Ce n'est pas un audit complet, mais un point de départ excellent et gratuit.

Cybermalveillance.gouv.fr

Le portail national d'assistance aux victimes d'incidents cyber met en relation les PME avec des prestataires référencés à tarifs maîtrisés. En 2026, il propose également des diagnostics préventifs à tarif réduit pour les organisations adhérentes.

Dispositifs Bpifrance

Bpifrance propose des aides au diagnostic cyber dans le cadre du Plan Cyber PME. Renseignez-vous auprès de votre chargé d'affaires Bpifrance régional pour les dispositifs en vigueur dans votre région (les montants et conditions varient). Des aides régionales complémentaires existent également via les Conseils Régionaux dans le cadre des contrats de plan État-Région.

FAQ — Questions fréquentes sur l'audit cybersécurité PME

Quelle est la fréquence recommandée pour un audit cybersécurité PME ?

La fréquence optimale dépend de la maturité et du secteur. Pour une première approche, commencer par un audit organisationnel global. Ensuite, un audit annuel est recommandé pour toute PME d'au moins 20 salariés. Les PME dans des secteurs réglementés (santé, finance, sous-traitants d'OES/OIV) doivent viser une fréquence plus élevée : audit organisationnel annuel + audit technique bisannuel + test d'intrusion tous les 2-3 ans. Après un incident de sécurité significatif, un audit de post-incident est recommandé indépendamment du calendrier prévu. Les changements majeurs du SI (migration cloud, fusion-acquisition, déploiement ERP) justifient également un audit spécifique.

Combien de temps dure un audit cybersécurité pour une PME ?

La durée dépend du type et du périmètre. Un audit organisationnel de base pour une PME de 20-50 salariés dure généralement 2 jours sur site + 2 jours d'analyse et rédaction = livraison du

rapport en 1-2 semaines. Un audit technique réseau + AD pour une PME de 100 salariés : 3-5 jours sur site + 3-5 jours d'analyse = 2-4 semaines. Un audit complet (organisationnel + technique + cloud) : 2-3 semaines de prestation + 2-3 semaines d'analyse et rédaction = 4-6 semaines. Exiger un calendrier précis dès le devis et un point d'avancement à mi-prestation.

La certification PASSI est-elle obligatoire pour auditer une PME ?

Non, la qualification PASSI n'est obligatoire que pour les audits des OIV (Opérateurs d'Importance Vitale) et dans certains contextes OES réglementés. Pour une PME standard, elle est un gage de qualité et de sérieux, pas une obligation. Cependant, si votre PME est sous-traitante d'un grand groupe ou d'une administration exigeant PASSI dans leurs contrats, vous devrez respecter cette exigence. La qualité d'un audit dépend avant tout des compétences des auditeurs affectés : vérifiez leurs certifications individuelles et demandez des rapports anonymisés de missions similaires.

Que faire concrètement après réception du rapport d'audit ?

Après réception du rapport : (1) Présentez l'executive summary à la direction avec une demande de budget pour les corrections prioritaires, (2) Identifiez les quick wins (corrections gratuites ou peu coûteuses) à implémenter immédiatement : désactivation des comptes inutilisés, activation de l'authentification MFA, configuration des sauvegardes offline, mise à jour des systèmes non patchés, (3) Intégrez les corrections plus complexes au budget IT annuel avec des échéances réalistes, (4) Demandez un retest partiel au prestataire 3-6 mois après, ciblé sur les vulnérabilités critiques corriges, (5) Documentez les corrections apportées et les risques résiduels acceptés pour votre dossier de sécurité.

Pour aller plus loin

Les concepts présentés dans cet article constituent une base solide pour approfondir le sujet. Ces ressources complémentaires permettent d'aller plus loin dans la compréhension et la mise en pratique.

Ressources officielles de référence

ANSSI — Guides et recommandations techniques — La bibliothèque technique de l'ANSSI publie régulièrement des guides à jour sur tous les aspects de la sécurité des systèmes d'information. Disponibles gratuitement sur ssi.gouv.fr.

NIST Cybersecurity Framework — Référentiel international structurant la gestion des risques cyber en 6 fonctions. Version 2.0 publiée en 2024, disponible sur nist.gov.

MITRE ATT&CK — Base de connaissances des techniques adversariales, régulièrement mise à jour avec les nouvelles menaces observées dans le monde réel.

Formation continue

Certifications professionnelles reconnues : CISSP, CISM (management), OSCP, CEH (technique)

Plateformes de formation pratique : HackTheBox, TryHackMe, Hack The Box Academy

Veille quotidienne : bulletins CERT-FR, alertes CISA, flux RSS NVD

Mise en réseau professionnel

La communauté cybersécurité française est active et ouverte : les clubs RSSI, l'OSSIR, le CLUSIF, et les conférences comme le FIC (Forum International de la Cybersécurité) et les SSTIC sont des points de rencontre essentiels pour les professionnels du secteur. Ces échanges permettent de rester à jour sur les menaces émergentes et les bonnes pratiques réelles.

Synthèse et perspectives 2026

Les techniques et recommandations présentées dans ce guide s'inscrivent dans un contexte de menaces en constante évolution. La cybersécurité offensive et défensive sont deux faces d'une même médaille : comprendre les mécanismes d'attaque est indispensable pour construire des défenses robustes et résilientes face aux acteurs malveillants les plus sophistiqués.

Pour les équipes sécurité, l'enjeu de 2026 est double : maintenir une veille continue sur les nouvelles techniques publiées par la communauté de recherche (CVE, exploit-db, GitHub, Secrech, SSTIC) tout en assurant le durcissement progressif de l'infrastructure existante. Le référentiel MITRE ATT&CK reste le fil conducteur le plus efficace pour structurer un programme de détection et de réponse face aux tactiques, techniques et procédures des groupes APT ciblant les secteurs critiques.

La formation continue des équipes, la simulation régulière d'incidents (exercices tabletop, exercices Red/Blue/Purple Team), et l'automatisation des tâches répétitives via des outils SOAR constituent les piliers d'une organisation cyber mature. Les organisations qui investissent dans ces trois axes démontrent systématiquement de meilleures métriques de détection et de réponse (MTTD et MTTR réduits de 40% en moyenne selon les benchmarks sectoriels) face aux incidents de sécurité. Pour les PME qui n'ont pas les ressources pour un audit annuel complet, une approche modulaire en trois phases (revue documentaire trimestrielle, tests techniques biannuels, audit complet annuel) offre un rapport qualité-coût optimal tout en maintenant une posture de sécurité acceptable face aux menaces qui les ciblent.