Checklist audit de sécurité informatique

35 points de contrôle · PME & ETI · 2026

Sources : ANSSI Panorama de la cybermenace 2024 · Verizon DBIR 2025 · Microsoft Digital Defense Report 2024

Cette checklist couvre les 9 domaines clés d'un audit de sécurité informatique. Utilisez-la comme base de travail avant ou pendant votre audit. Chaque point est accompagné d'une note explicative et d'un niveau de priorité. Les points **Critiques** sont à traiter en priorité absolue.

PRIORITÉ			
	■ **Critique** — Action immédiate requise	■ **Élevée** — À traiter sous 30 jours	■ **Moyenne** — À planifier dans les 90 jours

■ INVENTAIRE & CARTOGRAPHIE

☐	**Inventaire complet des actifs informatiques** Postes, serveurs, VMs, équipements réseau, services cloud, accès VPN, postes nomades	■ Critique
☐	**Cartographie des flux réseau réalisée** Identifier les flux entrants/sortants, les zones DMZ, les interconnexions avec partenaires	■ Critique
☐	**Inventaire des applications métier et de leurs dépendances** Versions, éditeurs, fin de support, données traitées, niveau de criticité	■ Élevée

■ POSTES DE TRAVAIL & DURCISSEMENT

☐	**Score CIS-CAT des postes Windows supérieur à 70 %** Un parc non durci obtient 30-40 % en moyenne. Outil : CIS-CAT Pro ou Lite (gratuit)	■ Critique
☐	**SMBv1 désactivé sur l'ensemble du parc** Vérification via PowerShell : Get-SmbServerConfiguration | Select EnableSMB1Protocol	■ Critique
☐	**PowerShell en mode ConstrainedLanguage ou signé** Limiter l'exécution aux scripts signés — réduit drastiquement la surface d'attaque	■ Élevée
☐	**LAPS (Local Administrator Password Solution) déployé** Mot de passe admin local unique par poste — bloque les mouvements latéraux par Pass-the-Hash	■ Élevée
☐	**Chiffrement des disques activé (BitLocker ou équivalent)** Obligatoire sur tous les portables et postes nomades — exigence RGPD et cyber-assurance	■ Élevée

■ ACCÈS & IDENTITÉS

☐	**MFA activé sur tous les comptes administrateurs** Microsoft : 99 % des attaques d'identité bloquées par le MFA. Priorité absolue	■ Critique
☐	**MFA activé sur les accès distants (VPN, RDP, cloud)** Verizon DBIR 2025 : identifiants compromis = 1er vecteur d'accès initial (22 % des violations)	■ Critique
☐	**Politique de mots de passe documentée et appliquée** 12 caractères minimum, sans réutilisation, idéalement couplée à un gestionnaire de mots de passe	■ Élevée
☐	**Revue des comptes privilégiés réalisée (< 6 mois)** Supprimer les comptes dormants, réduire les droits admin au strict nécessaire (principe du moindre privilège)	■ Élevée
☐	**Comptes de service inventoriés et sécurisés** Mots de passe complexes, droits limités, surveillance des connexions anormales	■ Moyenne
☐	**Active Directory — audit des délégations et des GPO** Semperis 2024 : AD est la cible de 9 attaques ransomware sur 10. Auditer Tier 0 en priorité	■ Critique

■ RÉSEAU & PÉRIMÈTRE

☐	**VPN et pare-feu à jour (correctifs < 30 jours)** ANSSI 2024 : équipements en bordure de SI = plus de 50 % des opérations de cyberdéfense	■ Critique
☐	**Scan de ports externes réalisé (surface d'attaque externe)** Outils : Shodan, Nmap, Qualys External Scan — identifier les services exposés non nécessaires	■ Élevée
☐	**Segmentation réseau en place (VLAN, zones)** Isoler les serveurs critiques, les postes industriels (OT/IT) et les équipements IoT	■ Élevée
☐	**Logs réseau activés et centralisés (SIEM ou syslog)** Durée de rétention minimale recommandée par l'ANSSI : 12 mois	■ Moyenne

■ CLOUD & APPLICATIONS

☐	**Revue des permissions cloud (Azure AD, AWS IAM, GCP)** Supprimer les accès inutilisés, vérifier les rôles Owner/Admin non nécessaires	■ Élevée
☐	**Authentification forte activée sur Microsoft 365 / Google Workspace** Désactiver l'authentification legacy (Basic Auth) — vecteur courant de compromission	■ Critique
☐	**Politique de rétention et de classification des données définie** RGPD : durées de conservation, données sensibles identifiées et protégées	■ Moyenne
☐	**Sécurité des APIs vérifiée (authentification, rate limiting, logs)** OWASP API Security Top 10 — applicable aux applications exposées en ligne	■ Moyenne

■ SAUVEGARDES & CONTINUITÉ

☐	**Sauvegardes testées régulièrement et stockées hors-ligne** Règle 3-2-1 : 3 copies, 2 supports différents, 1 hors-site. Test de restauration trimestriel	■ Critique
☐	**Sauvegardes isolées du réseau principal (air gap ou coffre immuable)** Les ransomwares ciblent et chiffrent les sauvegardes connectées au réseau. Isolation obligatoire	■ Critique
☐	**RTO et RPO définis et testés** Recovery Time Objective et Recovery Point Objective documentés et validés par un test annuel	■ Élevée
☐	**Plan de continuité d'activité (PCA) rédigé et à jour** Procédures de crise, contacts d'urgence, chaîne de décision, exercice annuel recommandé	■ Moyenne

■ GESTION DES INCIDENTS

☐	**Procédure de réponse aux incidents documentée** Qui fait quoi, dans quel ordre, avec quels outils. Doit être testée en simulation annuelle	■ Élevée
☐	**Contacts CERT/ANSSI et cyber-assureur identifiés et accessibles** CERT-FR : cert-fr.cert.ssi.gouv.fr — numéro d'astreinte de l'assureur disponible hors réseau	■ Élevée
☐	**Journaux d'événements (logs) activés sur les systèmes critiques** Windows Event Log, logs Active Directory, logs pare-feu — rétention min. 12 mois	■ Moyenne

■ FOURNISSEURS & TIERS

☐	**Accès des prestataires revus et limités dans le temps** Comptes nominatifs, accès JIT (Just-In-Time), révocation automatique à fin de mission	■ Élevée
☐	**Clauses de sécurité dans les contrats fournisseurs (NIS2, RGPD)** DPA (Data Processing Agreement) signé pour tout sous-traitant traitant des données personnelles	■ Élevée
☐	**Évaluation du niveau de sécurité des fournisseurs critiques** Questionnaire sécurité annuel ou audit tiers pour les prestataires avec accès au SI	■ Moyenne

■ SENSIBILISATION & CONFORMITÉ

☐	**Sensibilisation au phishing réalisée dans les 12 derniers mois** Verizon DBIR 2025 : 60 % des violations impliquent le facteur humain. Simulation recommandée	■ Élevée
☐	**Charte informatique signée par tous les collaborateurs** Inclure BYOD, télétravail, règles de mots de passe, signalement des incidents	■ Moyenne
☐	**Rapport d'audit de sécurité datant de moins de 12 mois disponible** Requis pour cyber-assurance, conformité NIS2 et démonstration de diligence auprès des régulateurs	■ Élevée