

CYBERSÉCURITÉ

Outil d'auto-évaluation pour les SPSTI

Ressources :

- ▶ [Presanse.fr](#) ▶ Ressources
- ▶ Organisation, SI et RH ▶ Systèmes d'Information

Les cyberattaques contre les établissements et organisations du secteur de la santé en France sont en recrudescence.

L'ANSSI - Agence Nationale de la Sécurité des Systèmes d'Information - alerte : ces intrusions compromettent la disponibilité des systèmes et la confidentialité des données médicales.

Le secteur de la santé est désormais une cible prioritaire pour les cybercriminels, et la tendance est à l'intensification.

Face à cette menace, les SPSTI doivent renforcer leurs défenses. Première étape : identifier les zones de vulnérabilité pour agir efficacement et orienter les actions prioritaires.

Pour accompagner cette démarche, Présanse propose un outil d'auto-évaluation inédit, conçu comme un complément à la PGSSI-S Politique Générale de Sécurité des Systèmes d'Information de Santé.

Accessible et simple, il permet aux SPSTI de mesurer leur maturité en cybersécurité, d'évaluer les risques et de bâtir un plan d'action.

Fruit d'un travail collaboratif par et pour les SPSTI, testé auprès d'un panel représentatif, cet outil se présente sous la forme d'un fichier Excel articulé autour de trois volets :

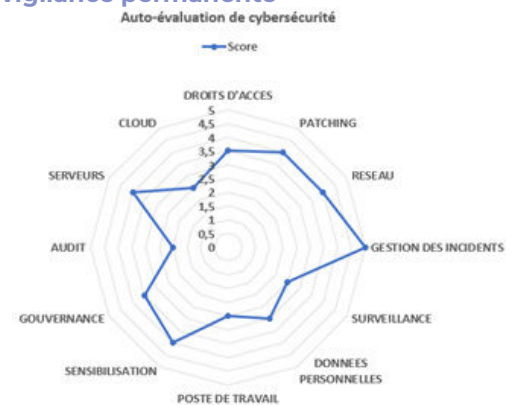
- ▶ Un mode d'emploi clair
- ▶ Un questionnaire structuré
- ▶ Et une synthèse visuelle en radar, pour une lecture immédiate des scores : une approche qui permet, en un coup d'œil, de situer le niveau de risque et de bâtir un plan d'action concret.

La grille couvre 12 domaines de sécurité informatique, chacun évalué pour produire un score global :

1. Gouvernance et organisation
2. Gestion des identités et des accès

3. Protection des postes et serveurs
4. Sécurisation des réseaux
5. Sauvegardes et plan de reprise
6. Gestion des mises à jour
7. Protection des données sensibles
8. Conformité réglementaire (RGPD, santé)
9. Sensibilisation des utilisateurs
10. Gestion des incidents
11. Sécurité des prestataires
12. Continuité et résilience

Un outil pédagogique, mais une vigilance permanente



Cette auto-évaluation constitue une étape clé pour solidifier la sécurité des systèmes d'information.

Il convient toutefois de rappeler qu'un bon score de maturité obtenu via cet auto-diagnostic ne garantit pas une protection totale contre les cyberattaques : la vigilance et l'action doivent rester permanentes.

Le score global représente la moyenne des scores des 12 axes notés de zéro à 5

- Une évaluation inférieure à 3 implique que votre SI est en risque critique
- Une évaluation entre 3 et 4 implique que votre SI est en risque majeur
- Une évaluation de 5 implique que votre SI est en risque mineur

La gestion du risque de sécurité informatique doit ainsi s'inscrire dans une logique d'amélioration continue, du fait de l'évolution permanente des techniques de cyberattaque : des actions sans relâche sont nécessaires pour renforcer la sécurité des systèmes d'information. ■