Veille Technologique

Qu'est-ce que la veille technologique ?

La veille technologique consiste à surveiller les évolutions techniques et les innovations dans un secteur donné. Elle permet d'anticiper les changements et d'évaluer l'impact des nouvelles menaces sur l'organisation. Pour un futur administrateur SISR, cette démarche est vitale pour passer d'une posture purement défensive à une véritable stratégie de **cyber-résilience**.

Les principaux outils de ma veille

Ma veille s'appuie sur des sources institutionnelles et spécialisées pour garantir une information fiable :

- **Feedly :** Agrégateur de flux RSS pour suivre des médias comme *DSIH* (spécialiste de l'informatique hospitalière) et *ZDNet*.
- **CERT-FR (ANSSI) :** Pour les alertes immédiates sur les vulnérabilités exploitées.
- **Health-ISAC :** Centre de partage et d'analyse d'informations sur les menaces spécifiques à la santé mondiale.
- **Plateforme e-santé.gouv.fr :** Pour suivre l'évolution de la doctrine technique et réglementaire en France.

Sujet de ma veille

Ma thématique centrale pour la période 2025-2026 est : **"La mutation de la cybersécurité en santé : entre explosion des menaces automatisées et nouvelles obligations de résilience."**

Ma veille repose sur 3 thèmes d'actualité :

Thème 1 : Une année 2025 de records pour les violations de données

Bilan 2025 : Plus de 57 millions de patients touchés

31 décembre 2025

L'année 2025 a été marquée par une intensité record. Rien qu'aux États-Unis, 642 violations majeures ont été signalées, affectant près de 57 millions de personnes. Le coût moyen d'une compromission dans la santé atteint désormais 7,42 millions de dollars par incident. *Source : HIPAA Journal*

L'attaque massive contre Yale New Haven Health

12 avril 2025

Le plus grand système de santé du Connecticut a révélé une intrusion ayant exposé les données sensibles de 5,6 millions de patients. Cette attaque illustre la vulnérabilité des grands réseaux hospitaliers face aux accès non autorisés. *Source : Healthcare Dive*

Sanction pour défaut d'habilitation

11 février 2026

La CNIL et les autorités de contrôle durcissent le ton : un établissement de santé a été récemment sanctionné pour une mauvaise configuration des règles d'accès de son personnel aux dossiers médicaux. La gestion des droits d'accès devient un enjeu juridique majeur en 2026. *Source : DSIH*

Thème 2 : Le virage réglementaire et la souveraineté (NIS2 & HDS)

Entrée en vigueur de NIS 2 dans le secteur de la santé

21 janvier 2026

La directive européenne NIS 2 impose désormais aux hôpitaux et laboratoires des exigences strictes en matière de gestion des risques et de continuité d'activité. Les sanctions peuvent atteindre 10 millions d'euros ou 2 % du chiffre d'affaires mondial. *Source : Veeam / PwC France*

HDS Version 2 : Un nouveau cadre pour l'hébergement

Janvier 2025

Le référentiel de certification des Hébergeurs de Données de Santé (HDS) a évolué pour simplifier les procédures tout en renforçant l'authentification multifacteur (MFA) et le chiffrement des données. *Source : Agence du Numérique en Santé*

Vers un cloud souverain SecNumCloud pour la santé

10 février 2026

Sous l'impulsion du gouvernement, la Plateforme des données de santé (Health Data Hub) a acté sa migration vers un cloud souverain qualifié **SecNumCloud** d'ici fin 2026, abandonnant les solutions étrangères pour garantir la protection des données nationales. *Source : Rédaction DSIH*

Thème 3 : L'IA, entre menace automatisée et aide au diagnostic

L'essor des attaques générées par l'IA

3 février 2026

En 2026, l'IA n'est plus seulement un outil de productivité mais une arme. 66 % des responsables IT considèrent désormais les attaques automatisées par l'IA comme la menace la plus lourde, devant les ransomwares classiques. *Source : Veeam Survey 2026*

L'IA générative intégrée aux pratiques cliniques

18 décembre 2025

La tendance majeure pour 2026 est l'intégration de l'IA générative dans les hôpitaux pour l'aide au diagnostic et le tri médical. Cela pose d'immenses défis de "cybersécurité par design" pour éviter que ces algorithmes ne soient corrompus. *Source : Buzz-esanté*

Sécurisation des accès : La généralisation d'Hospiconnect

6 février 2026

Pour contrer le phishing (qui reste le vecteur n°1 avec 63 % des attaques), le dispositif **Hospiconnect** entre dans une phase de généralisation pour sécuriser les identités numériques des professionnels de santé. *Source : Journal Officiel / DSIH*

Conclusion et Bilan

Cette veille montre qu'en 2025-2026, la cybersécurité n'est plus un simple sujet technique mais une condition indispensable de la qualité des soins. La tendance n'est plus seulement à la prévention, mais à la capacité de l'infrastructure à encaisser un incident et à restaurer les services vitaux en un temps record (RTO).