• COMPTE-RENDU

14e Congrès National de la SSI Santé — APSSIS

Le Mans · 23–25 juin 2026

L'ESSENTIEL

La cybersécurité n'est plus l'affaire des seuls informaticiens : elle est devenue une condition de la continuité des soins, et donc celle de l'ingénieur(e) biomédical(e). Ce congrès a confirmé une bascule — IA dans les services, durcissement réglementaire (NIS 2, Cyber Resilience Act), industrialisation des attaques — où le parc d'équipement biomédical doit devenir un sujet de cybersécurité à part entière. Longtemps délaissés, les dispositifs médicaux sont aujourd'hui à la fois des cibles potentielles et les plus difficiles à sécuriser dans la durée.

LES CHIFFRES DU CONGRÈS

764
incidents au CERT Santé en 2025 (+15 %), majoritairement malveillants

400 000
connexions du personnel d'un seul CHU vers des IA publiques

75 %
des hôpitaux ne peuvent patcher tous leurs équipements au quotidien

LES TEMPS FORTS

1 Menace & cadre national

Le secteur santé clairement dans le viseur.

CERT Santé 2025 : 764 incidents (plus de la moitié malveillants), recul des rançongiciels (< 30 %) au profit de l'exfiltration de données. Côté État : amende CNIL de 5 M€ contre France Travail, attaque touchant 12 ministères, et une Stratégie nationale cyber (janvier 2026) en 5 axes pilotée par l'ANSSI.

POUR LE BIOMÉDICAL

L'attaquant vise désormais les flux et les identifiants, y compris les comptes de télémaintenance et les consoles constructeurs. Le cloisonnement réseau du parc est sans doute la mesure à mettre en place en priorité sur nos installations.

2 Réglementaire — NIS 2 & Cyber Resilience Act

Le CRA arrive : l'impact sur les éditeurs.

Le CRA impose aux fabricants la sécurité dès la conception, des correctifs gratuits pendant 5 ans minimum, un point de contact pour les vulnérabilités et le marquage CE. Échéances : 11 septembre 2026 (déclaration des vulnérabilités via l'ENISA) et 11 décembre 2027 (application intégrale). L'enquête présentée est sévère : 75 % des RSSI jugent que les éditeurs ne corrigent pas les failles signalées, et 76 % des éditeurs méconnaissent leurs obligations CRA.

POUR LE BIOMÉDICAL

Point de vigilance : les dispositifs médicaux sont aujourd'hui exclus du CRA (régis par les règlements DM de 2017). À actionner : des clauses de sécurité dans nos marchés (Clausier Club RSSI Santé / CAIH / AFIB) et le droit de signalement volontaire à l'ANSSI en cas de défaillance.

➜ Disponible ici
CYBER RESIDENT ACT

➜ Disponible ici
NIS2

3 Intelligence artificielle

Déjà dans les services, souvent sans personne aux commandes.

Le « Shadow AI » a dominé le congrès : un CHU a relevé 400 000 connexions de son personnel vers des IA publiques (15 000/h pour les seules secrétaires médicales). Risques : fuite de données patients, perte de traçabilité de la décision médicale. L'AI Act entre en vigueur en août 2026, la santé étant classée « risque haut ».

➜ Disponible ici
L'IA- ACT

4 SOC — modèles & retour d'expérience

Le biomédical entre enfin dans le périmètre.

Le GHT de Martinique a mutualisé son SOC sans laisser aucun périmètre de côté — biomédical inclus — et s'en sert comme socle de preuves de conformité (HAS, NIS 2). Quand un EDR est impossible, sur des environnements hétérogènes comme le biomédical, la détection réseau (NDR/IDS) permet d'identifier, de prévenir et de traiter les menaces dans le trafic de façon proactive.

POUR LE BIOMÉDICAL

Fait marquant : la Martinique a intégré la sauvegarde et le parc biomédical dès le périmètre initial du SOC. C'est sans doute une action à mettre en place dans nos établissements.

5 Gestion des accès privilégiés (PAM)

Maîtriser la télémaintenance des prestataires.

Un GHT de 5 000 agents a déployé un bastion PAM couvrant les accès de télémaintenance : environ 600 comptes nominatifs pour une centaine de sociétés, traçabilité des sessions et coupure instantanée en cas de menace détectée. La clé du succès : cartographier les usages avant de déployer l'outil.

POUR LE BIOMÉDICAL

Cartographier nos réseaux doit devenir une priorité lors de nos renouvellements d'équipements. Combien de nos contrats de maintenance reposent encore sur des comptes génériques partagés et des accès distants peu tracés? Le bastion répond à ce point faible : à intégrer au cahier des charges des marchés de maintenance.

6 Tests d'intrusion

Le pentest s'invite sur les équipements biomédicaux.

Une approche présentée cible spécifiquement les équipements biomédicaux, souvent exemptés d'EDR pour cause de marquage CE : recherche de vulnérabilités et d'expositions courantes (CVE) et « rapport éditeur » directement transmissible au fabricant. Cas concret sur un CHR de 950 lits : une faille CVSS 9.3 transmise aux fournisseurs un vendredi, corrigée et déployée le mardi suivant.

POUR LE BIOMÉDICAL

« Exempté d'EDR pour cause de marquage CE » : c'est notre quotidien. On peut auditer notre parc biomédical sans casser la certification du DM et produire des preuves opposables à nos fournisseurs en cas de faille relevée.

7 Souveraineté & dépendances numériques

Nos dépendances invisibles.

La conférence a mis en perspective nos « dépendances invisibles » : derrière chaque outil ou équipement médical (dictée, imagerie, plateformes constructeurs…), il faut identifier le fournisseur d'infrastructure de dernier rang, souvent un hébergeur étranger. Illustration : la défaillance d'un seul fournisseur a affecté 759 hôpitaux en 2024.

POUR LE BIOMÉDICAL

Inscrire dans nos évaluations d'achat la question « où vont les données, et chez quel hébergeur de dernier rang ? », aussi importante que les spécifications techniques. Une vraie question de souveraineté.

À METTRE EN PLACE DÈS LA RENTRÉE

1	**Clauses de sécurité dans nos marchés —** support, correctifs, fiche réflexe pour vos plans de continuité d'activité.
2	**Cartographier avant d'outiller —** équipements connectés, accès de télémaintenance, hébergement des données.
3	**Faire entrer le biomédical dans le SOC —** en lien avec vos RSSI : remontée de logs, détection réseau quand l'EDR est impossible.
4	**Monter en compétence —** poursuivre la formation cyber-biomédicale à l'AFIB.

NEWS · CLAUSIER CONFORMITÉ NUMÉRIQUE

• NOUVEAUTÉ 2026

La version 2026 du clausier conformité numérique est disponible !

Fruit d'un travail collaboratif entre le **Club RSSI** et l'**AFIB**, la nouvelle édition met à disposition un ensemble de clauses types prêtes à l'emploi pour sécuriser vos contrats et intégrer les exigences de conformité numérique au plus près de vos besoins. Enrichie et actualisée au regard des évolutions réglementaires et des retours du terrain, elle traduit l'engagement de nos deux structures à outiller concrètement les professionnels.

→ Disponible dès maintenant
Retrouvez le clausier 2026 sur le site de l'AFIB