🛡️ Politique de Sécurité – Solutions Techniques Complémentaires

🔍 Contexte

Les hôpitaux gèrent des données extrêmement sensibles (dossiers médicaux, données personnelles, identifiants patients) et doivent garantir leur sécurité face aux menaces croissantes (ransomware, accès non autorisé, exfiltration de données). Les solutions présentées ici couvrent plusieurs domaines clés pour bâtir une sécurité multicouche dans un environnement hospitalier moderne.

1. 🕒 MEP des politiques de sécurisation des sessions

Objectif : Prévenir les compromissions d'identifiants et bloquer les détournements de session.

Mesures techniques détaillées :

- Expiration automatique des sessions après inactivité prolongée pour limiter les risques d'utilisation non autorisée.
- Re-authentification obligatoire lors d'accès à des fonctions critiques ou sensibles (ex : modification de prescriptions).
- Jetons de session cryptographiquement signés pour empêcher leur falsification ou réutilisation.
- Liste blanche d'adresses IP autorisées pour les sessions d'administration.
- MFA systématique pour les postes d'encadrement et tout personnel accédant à des données médicales.
- Notifications de connexion inhabituelle pour les comptes sensibles (email ou SMS).

2. 🔐 Sécurisation des données

Objectif : Assurer la confidentialité, l'intégrité et la disponibilité de l'information à tout moment.

Mesures techniques détaillées :

- Chiffrement des bases de données et systèmes de fichiers à l'aide d'algorithmes robustes (AES-256 pour les données, RSA-2048 pour les échanges de clés).
- TLS 1.3 pour tous les transferts de données en interne comme en externe (API, VPN, accès client/serveur).
- Mécanismes de tokenisation dans les applications afin de dissocier les données sensibles de leur identifiant direct.
- Contrôle d'accès basé sur les rôles (RBAC) strictement défini dans l'annuaire LDAP ou Active Directory.
- Systèmes DLP pour empêcher le transfert non autorisé de documents (USB, mail, cloud, etc.).
- Hachage sécurisé des mots de passe avec salt (Bcrypt, Argon2), sans stockage de mots de passe en clair.

3. 🔄 Gestion des mises à jour des outils (médicaux ou non)

Objectif : Réduire les surfaces d'attaque en assurant une correction rapide des vulnérabilités.

Mesures techniques détaillées :

- Planification automatisée des mises à jour critiques via outils centralisés (WSUS, SCCM, Landscape, Ansible).
- Suivi des correctifs spécifiques aux dispositifs médicaux selon les recommandations du fabricant et exigences de conformité CE.
- Tests de compatibilité préalable en environnement de recette, en particulier pour les outils critiques (scanner, IRM, etc.).
- Mise en quarantaine des équipements obsolètes jusqu'à la mise à jour ou remplacement.
- Rapports d'intégrité post-mise à jour pour s'assurer du bon fonctionnement après chaque patch.
- Audit automatisé de l'état des mises à jour sur l'ensemble du parc (compliance).

4. 🛰️ Centre de surveillance de la sécurité (SOC)

Objectif : Surveiller, détecter et réagir rapidement aux incidents de sécurité 24h/24.

Mesures techniques détaillées :

- Déploiement d'un SIEM (Security Information & Event Management) pour centraliser les logs système, réseau, applicatif.
- Corrélation des événements de sécurité pour identifier les incidents complexes (ex : élévation de privilège après scan réseau).
- Intégration de règles de détection de comportements anormaux personnalisées au contexte hospitalier (accès multiples aux mêmes dossiers, requêtes non médicales).
- Connectivité avec un SOC externalisé (MSSP) pour une couverture en continu avec SLA de réponse défini.
- Playbooks de réponse aux incidents automatisés (ex. : isolement d'un poste, reset des identifiants, génération de ticket d'alerte).
- Dashboards opérationnels en temps réel pour les RSSI et responsables techniques.

5. 📜 Journalisation et audit

Objectif : Garantir la traçabilité complète des événements de sécurité et assurer la conformité réglementaire (HDS, RGPD).

Mesures techniques détaillées :

- Centralisation des logs horodatés avec synchronisation NTP sur un serveur sécurisé.
- Logs signés numériquement pour empêcher toute modification ou suppression non autorisée.
- Conservation différenciée : 1 an pour les journaux système, 3 à 5 ans pour les accès aux données médicales.
- Audit interne automatisé avec alertes sur anomalies (accès de week-end, nombre d'échecs de login, etc.).
- Contrôle des accès aux fichiers journaux via RBAC et restrictions sur les exports.
- Intégration aux contrôles qualité ISO 27001 et HDS, avec revues mensuelles par la DSI.

6. 🧠 Analyse comportementale

Objectif : Identifier de manière proactive les comportements suspects pouvant précéder une attaque interne ou une compromission externe.

Mesures techniques détaillées :

- UEBA (User & Entity Behavior Analytics) intégrée au SIEM, combinant règles statiques et machine learning.
- Profilage des utilisateurs selon poste, fréquence d'accès, type d'actes médicaux ou administratifs.
- Détection des écarts au comportement habituel : accès massifs à des dossiers patients, connexions en dehors des horaires, consultation de patients non affectés.
- Couplage à l'EDR/XDR pour une réponse automatisée (isolement du poste, suspension du compte).
- Alertes de priorité en fonction du niveau de privilège du compte affecté.
- Reporting de risque individuel transmis régulièrement à la DSI ou au RSSI.

✅ Conclusion

L'intégration coordonnée de ces solutions techniques permet une cybersécurité hospitalière proactive et robuste. La défense repose sur une approche en couches, allant de la prévention à la détection comportementale, tout en assurant traçabilité, conformité, et réactivité. Elle doit être complétée par une PSSI solide, des tests réguliers et la sensibilisation du personnel.