Tableau de synthèse : Sécurité du SI du CHYNOV

Concept de sécurité	Mise en œuvre dans le projet
Défense en profondeur	Superposition des protections : firewall, VLANs, 802.1X, IDS/IPS, segmentation logique et physique.
Sécurité périmétrique	Firewall principal en frontal entre le WAN et l'architecture interne.
Segmentation logique (VLANs)	11 VLANs isolés : utilisateurs, serveurs, caméras, biomédical, administration, etc.
Segmentation physique	Cloisonnement par switchs physiques selon les zones critiques.
Contrôle d'accès (AAA)	Authentification 802.1X, Active Directory centralisé, gestion des groupes par rôle.
Authentification forte (MFA)	VPN + MFA pour l'accès distant sécurisé (zone sensible via Jumpbox).
Gestion des accès	Comptes revus mensuellement, suppression après 90 jours d'inactivité.
Bastion / Jumpbox	Poste intermédiaire pour administrer les serveurs (Windows 10 avec VPN).
Détection d'intrusion (IDS/IPS)	Outils open source comme Snort ou Suricata pour surveillance réseau.
Sécurité des terminaux (EDR/XDR)	Utilisation de Wazuh ou Crowdstrike pour la supervision des postes.
PSSI et gouvernance	Politique formelle, comité SSI, rôles définis (DPO, RSSI, DSI).
Tests d'intrusion (Pentest)	Exploitation de la faille Zerologon avec Metasploit sur l'AD.
Plan de continuité (PRA/PCA)	Documenté et testé pour les services critiques.
Sensibilisation et formation	Ateliers, formations internes et campagnes anti-phishing.
Surveillance et veille	Veille CERT Santé, indicateurs de sécurité (MFA, logs, accès dormants).
Chiffrement des flux	Chiffrement des communications internes et externes (95% des flux).

Table 1 – Résumé des mécanismes de sécurité déployés dans le SI du CHYNOV