Phase A : Initialisation

1. Liste des moyens techniques de l'infrastructure

Matériels :

- Routeur Cisco ISR 1100
- Switchs Cisco Catalyst 9200
- Serveurs physiques Dell PowerEdge R740
- Points d'accès WiFi Aruba AP-515
- Postes de travail HP EliteDesk 800 G6

Logiciels :

- Systèmes d'exploitation : Windows Server 2022, Ubuntu 22.04
- Logiciels de virtualisation : VMware vSphere 8, VirtualBox
- Pare-feu : pfSense
- Serveur web : Apache2
- Gestion des utilisateurs : Active Directory (AD)
- Sauvegardes : Veeam Backup & Replication
- Docker pour le développement et la conteneurisation

2. Identification des technologies à surveiller (veille technologique):

1. WiFi 7 (802.11be):

- L'évolution vers le WiFi 7 est une priorité en raison de ses performances accrues (débits allant jusqu'à 46 Gbps) et de ses améliorations en matière de latence. Cette technologie répond à des besoins critiques pour GSB, comme la connexion simultanée de plusieurs appareils dans des espaces denses, tout en améliorant la sécurité grâce à des protocoles renforcés. Cependant, le coût des équipements et la formation nécessaire pour les administrateurs imposent une veille rigoureuse.

2. Firewalls de nouvelle génération (NGFW):

- Les NGFW intègrent des fonctions avancées comme l'inspection SSL, la prévention des intrusions (IPS) et l'analyse comportementale. Ces dispositifs permettent de mieux protéger l'infrastructure de GSB contre les menaces émergentes, notamment les attaques ciblant les données sensibles des patients. Une veille sur ces technologies est essentielle pour évaluer les coûts, la compatibilité et les avantages potentiels.

3. Conteneurisation avec Docker et Kubernetes:

- Docker, associé à Kubernetes pour l'orchestration, est une technologie incontournable pour moderniser les déploiements applicatifs. La flexibilité qu'elle offre en termes de gestion des environnements de production et de tests est essentielle pour maintenir une infrastructure agile et réactive. Une veille s'impose pour identifier les innovations et évaluer les besoins en formation.

4. Solutions de sauvegarde dans le cloud:

- Avec l'augmentation des cyberattaques (ransomware), les sauvegardes dans le cloud, telles qu'AWS Backup ou Azure Backup, offrent une solution redondante et sécurisée. Cette veille permettra à GSB de comparer les coûts et la compatibilité des différentes offres disponibles.

Phase B : Choix des sujets:

1. Éléments retenus pour la veille technologique

WiFi 7 :

-Risques fonctionnels : configuration incorrecte, problèmes de compatibilité avec les appareils existants.
- Impact sur la productivité : ralentissement ou coupure du réseau.
- Risques financiers : coûts élevés pour l'équipement et la formation.

Firewalls NGFW :

- Risques fonctionnels : surcharge du système, erreurs dans les règles de filtrage.
- Impact sur la sécurité : vulnérabilités liées à une mauvaise configuration.
- Risques financiers : investissement initial important, suivi des coûts de licence.

2. Éléments non retenus pour la veille technologique:

Docker et Kubernetes :

- Moins critique à court terme, mais présente un potentiel à long terme.
- Risque de complexité pour les administrateurs sans expérience.

Solutions de sauvegarde dans le cloud :

- Risques légaux (conformité RGPD) et financiers élevés.

Phase C : Mise en place de la veille:

Phase C non réalisée en raison d'un oubli .