GSB

Présentation du Laboratoire GSB:

En 2009, naissait le laboratoire GSB, acronyme de Galaxy Swiss Bourdin, fruit de la fusion entre deux entités distinctes. Galaxy, mastodonte américain spécialisé dans la lutte contre les maladies virales telles que le VIH et les hépatites, s'associait à Swiss Bourdin, conglomérat européen issu de la réunion de trois laboratoires dédiés aux médicaments conventionnels.

Le siège administratif établi à Paris, le laboratoire s'enracine également à Philadelphie, Pennsylvanie, aux États-Unis. Cette fusion stratégique vise à optimiser les opérations, réalisant des économies d'échelle tout en tirant le meilleur des deux mondes en termes de produits concurrents.

Organisation du Système Informatique et Ses Besoins:

L'infrastructure informatique du laboratoire se déploie principalement au 6e étage sécurisé à Paris, avec une extension aux États-Unis. Serveurs physiques et virtualisés cohabitent, assurant les services essentiels du réseau, les communications, l'hébergement des applications spécifiques à la pharmacologie, ainsi que les fonctions générales de l'entreprise.

La redondance des serveurs et des équipements réseau, conjuguée à une vigilance 24h/24, minimise les risques de coupure de service.

Le réseau, divisé en 12 VLAN, offre une flexibilité structurée, tandis que les postes de travail des employés, les stations de recherche et les ordinateurs portables constituent un écosystème informatique diversifié.

Domaine d'Étude:

Le travail se focalise sur l'amélioration des interactions entre les acteurs mobiles (visiteurs médicaux et délégués régionaux) et les services parisiens.

L'objectif est d'instaurer un système de suivi des visites plus efficient, offrant un accès direct aux données du personnel. De plus, la gestion des frais des acteurs mobiles sera revue pour limiter les excès et faciliter le traitement comptable.

Ce projet nécessite la mise en place d'applications dédiées, impliquant les équipes de développement, réseau et système.

Le tout en préservant la sécurité des données personnelles, la protection des équipements et la garantie de disponibilité, intégrité et confidentialité des services informatiques demeurent des priorités, répondant aux exigences de sécurité de l'entreprise face aux cybermenaces.