19/11/2025

Compte-rendu

Rendu du cahier des charges

Contexte du rapport 1
Question 1 : Spécifications techniques des ordinateurs portables 2
Question 2 : Sécurité et protection des données. 3
Question 3 : Déploiement de 450 postes 4
Question 4 : Connectivité et accès aux ressources 5
Question 5 : Gestion et remontée des données 7
Question 6 : Gestion des frais et remboursements 9
Question 7 : Accès aux données de personnel 11
Question 8 : Maintenance et support à distance 13
Question 9 : Intégration avec l'infrastructure réseau existante 15
Question 10 : Programme de formation et d'accompagnement 16
Question 11 : Documentation et livrables finaux 18
QCM 20
Réponse aux questions QCM 20
Conclusion : 24

Fait par : Mattéo Mouranchon – Groupe 2

Contexte du rapport

Le laboratoire **G**alaxy **S**wiss **B**ourdin (**GSB**) est le résultat d'une fusion stratégique entre deux acteurs majeurs de l'industrie pharmaceutique. D'un côté, **Galaxy**, géant américain reconnu pour son expertise dans le domaine des maladies virales telles que le SIDA, les hépatites et d'autres pathologies infectieuses. De l'autre, **Swiss-Bourdin**, un conglomérat européen regroupant plusieurs laboratoires spécialisés dans la production de médicaments courants et le développement de traitements thérapeutiques plus traditionnels.

Cette union, motivée par la volonté de renforcer leur position sur le marché mondial, a donné naissance à un groupe pharmaceutique puissant, combinant **innovation scientifique**, **capacité de production** et **réseau commercial étendu**. Toutefois, la fusion a également mis en évidence de nombreux défis organisationnels, notamment en matière de **gestion du personnel**, de **coordination des services** et surtout d'**harmonisation des outils de travail**.

Après deux années de réorganisation interne, GSB a constaté que les visiteurs médicaux - acteurs essentiels pour la promotion des produits et le lien avec les professionnels de santé - utilisaient des équipements informatiques hétérogènes et souvent obsolètes. Certains étaient dotés de matériel fourni par l'entreprise Galaxy, tandis que d'autres recevaient une indemnité bisannuelle pour s'équiper eux-mêmes selon la politique Swiss-Bourdin. Cette absence d'uniformité compliquait non seulement la maintenance, mais également la **sécurisation des données**, la **remontée d'informations terrain**, et l'**organisation des échanges avec les différents services du siège**.

Question 1 : Spécifications techniques des ordinateurs portables

L'entreprise GSB reverse aux visiteur une indemnité pour s'équiper en informatique ou comme une donation pour donner de l'impression aux clients.

Pour un usage professionnel de manière intensif, 3 ordinateurs de type vont être recommander qui vont remplir les conditions suivantes :

- L'ordinateur doit être robuste.
- Le poids de l'ordinateur doit-être dans des condition acceptable, pas trop lourd.
- Être utiliser dans des usage intensif.
- Avoir une autonomie importante.

Voici les 3 modèle : Lenovo ThinkPad, Dell Latitude et HP EliteBook

Quel modèle d'ordinateur portable recommandez-vous et pourquoi ?

Le HP EliteBook 14 pouces est recommandé, car c'est un ordinateur professionnel, robuste, léger et adapté aux déplacements fréquents.

Quelle est la configuration minimale requise ?

- Un Intel Core i5 minimum.
- 16 Go de RAM.
- Un SSD d'au moins 512 Go.
- La batterie doit avoir au moins 8 heures d'autonomie.

Quel poids maximum ne doit pas être dépassé ?

1,5 kg maximum accepté.

Question 2 : Sécurité et protection des données.

Quel système de chiffrement recommandez-vous ? Pourquoi ?

BitLocker est fortement recommander, ce système de chiffrement est intégré à Windows, car il est **fiable, simple à activer** et permet de protéger toutes les données de l'ordinateur en cas de perte ou de vol. Attention à se souvenir de ses mots de passe principal car même l'entreprise elle-même ne pourra pas vous aider.

Comment gérez-vous les clés de récupération ?

Les clés de récupération doivent être **sauvegardées dans un espace sécurisé**, par exemple dans un **compte Microsoft professionnel** ou dans un **coffre-fort numérique** de l'entreprise. Elles ne doivent jamais être stockées sur le PC lui-même. En cas de perte ou oublie de votre mot de passe, veuillez contacter votre responsable pour faire une récupération.

Comment assurer la séparation données pro/perso ?

Il faut utiliser **deux espaces séparés** :

- Un **compte professionnel** pour les données de l'entreprise, réservé que pendant le travail professionnel.

- Un **compte personnel** ou un **conteneur séparé** pour les fichiers privés et personnelle. Cela évite ainsi toute confusion ou fuite accidentelle.

Quelle procédure en cas de perte ou vol ?

En cas de perte ou de vol, il faut **déclarer immédiatement l'incident au service informatique**, qui pourra :

- Bloquer l'accès aux comptes.
- Déclencher un **effacement à distance** si possible.
- Utiliser BitLocker pour empêcher l'accès aux données.

Comment empêcher l'installation de logiciels non autorisés ?

On peut activer les **P**olitiques de **S**écurité **W**indows (**GPO**), qui bloquent l'installation de logiciels sans autorisation.
On peut aussi utiliser un **antivirus professionnel** et limiter le PC à des **droits utilisateurs**, empêchant l'installation de programmes inconnus.

Question 3 : Déploiement de 450 postes

Quelle solution de masterisation recommandez-vous ? Pourquoi ?

Je recommande d'utiliser une solution de déploiement automatisé comme **WDS** (**W**indows **D**eployment **S**ervices), car elles permettent de créer une image système unique et de la déployer rapidement sur un grand nombre d'ordinateurs.

Source : https://learn.microsoft.com/fr-fr/windows/win32/wds/windows-deployment-services-portal

Quelle procédure de test après déploiement ?

Après le déploiement d'un poste, une procédure de test complète doit être effectuée avant la remise à l'utilisateur. Elle comprend :

1. Vérifie que le démarrage Windows fonctionne correctement et que Windows soit actif.
2. Tester la connexion du réseau via l'invite de commande et vérifier que le poste reçois bien les paquets entre lui et le serveur.
3. Vérifie que les applications les plus utiliser fonctionne correctement au bon fonctionnement.
4. Vérifier que Windows soit bien à sa dernière version.
5. Vérifier que toute la sécurité du poste soit active, en partie BitLocker, la présence de l'antivirus et le paramétrage recommander
6. Répéter les 5 étapes sur les 450 Postes/Machines à déployer

Comment mettre à jour l'image de déploiement ?

Afin de mettre à jour l'image, veuillez :

1. Prends un PC modèle.
2. Installe les nouvelles version mises à jour et logiciels.
3. Vérifie que tout fonctionne.
4. Re-capture l'image dans WDS.
5. La redéployé lors des prochaines installations.

Question 4 : Connectivité et accès aux ressources

Je recommande une solution **SSL-VPN** ou **IPsec** fournie par un équipement professionnel comme **Fortinet** (**FortiClient**), **Cisco AnyConnect**, ou **OpenVPN Access Server**.
Ces solutions offrent :

- Un haut niveau de sécurité.
- Une connexion stable.
- Une authentification forte (mot de passe + MFA),
- Et une compatibilité avec Windows.
  Elles permettent aux visiteurs médicaux d'accéder aux ressources internes depuis n'importe où.

Comment configurez-vous l'accès Wifi sécurisé ?

Pour sécuriser le Wifi, il faut mettre en place un réseau décidé pour l'entreprise en version **WPA2-Enterprise ou WPA3-Enterprise**, qui utilise :

- Une authentification par identifiant professionnel (**RADIUS**).
- Un mot de passe fort ou un certificat (Bitlocker).
- Et une connexion automatique sur les postes configurés.
  Cette méthode évite que le mot de passe Wifi circule et cela garantit que seuls les appareils autorisés peuvent se connecter sans problème.

Quelle sont les politiques pour les connexions WiFi publiques ?

Pour les WiFi publics (cafés, hôtels, transports), les règles sont simples :

- Le **VPN** obligatoire dès la connexion.
- Interdiction d'accéder à des données sensibles sans **VPN** ou en cas de non VPN installé, veuillez ne pas vous connecter.
- Bloqué les sites ou services dangereux.
- Activer l'antivirus et le pare-feu Windows.

Cela protège contre les risques fréquents : écoute du trafic, faux hotspots, vol de données, fuite de donnée, etc.

Comment garantir l'accès aux ressources internes ?

L'accès se fait via :

- Le **VPN**, qui va crée un tunnel sécurisé (ex : Cloud FLARE).
- Une authentification forte **(MFA)** pour vérifier l'identité de l'utilisateur,
- Des **règles réseau** qui autorisent uniquement les applications internes nécessaires (CRM, intranet, messagerie…).
  Cela garantit que seuls les utilisateurs autorisés accèdent aux ressources de l'entreprise.

Quel sont les impacts du VPN sur les performances ?

Le VPN peut :

- Réduire légèrement le **débit Internet**.
- Augmenter de peu la **latence**.
  Parce que, il chiffre toutes les données et les fait passer par un serveur sécurisé (ex : Nord VPN).
  Cependant, sur une bonne connexion 4G/5G ou WiFi, l'impact est **faible** et n'empêche pas le bon fonctionnement des applications métier.

Question 5 : Gestion et remontée des données

Quelles données doivent être sauvegardées automatiquement ?

Les données à sauvegarder automatiquement en backup sont :

- Les documents professionnels (rapports, comptes-rendus).

- Les fichiers liés aux applications métier.

- Les données synchronisées (notes, formulaires, tableaux).

- Et les paramètres importants de l'utilisateur.

L'objectif est que rien d'important ne soit perdu en cas de panne, d'erreur ou de perte de données.

Quelle fréquence de sauvegarde est recommandez ?

Il est recommandé de faire une sauvegarde **quotidienne**, voire **en temps réel** grâce à une synchronisation automatique (comme OneDrive Entreprise).
Cela garantit que les fichiers sont toujours à jour et qu'il n'est pas d'oubli de la part du service informatique.

Où sont stockées les sauvegardes auxiliaires ?

Les sauvegardes auxiliaires sont stockées :

- Dans le **cloud professionnel de l'entreprise** (OneDrive Entreprise).
- Et dans les **serveurs sécurisés** de l'entreprise.
  Ce stockage externe protège les données est utile si l'ordinateur est perdu ou en panne.

Comment restaurer les données en cas de panne ?

En cas de panne :

1. Veuillez réinstalle l'ordinateur avec l'image système.
2. L'utilisateur doit se reconnecte à son compte professionnel.
3. Les fichiers se **relyncheront automatiquement** depuis **OneDrive** ou le **serveur de l'entreprise**.
   Il retrouve ainsi toutes ses données perdues sans manipulation complexe. Avant de faire de procédé, veuillez contacter votre administrateur pour procéder à la restauration des données.

Comment assurer la remontée des informations terrain ?

Pour assurer la remontée des informations terrain, on utilise :

- La synchronisation automatique via le **OneDrive**.

- Une connexion stable (Wifi, 4G/5G, VPN si nécessaire).

- Et des logiciels métiers configurés pour envoyer les données dès qu'Internet est disponible.
  Ainsi, les données collectées pendant les visites remontent automatiquement au siège social.

Question 6 : Gestion des frais et remboursements

Quelle solution pour la saisie électronique des notes de frais ?

Il est recommandé d'utiliser **Indy**, car c'est une solution simple et complète qui permet :

- De **scanner automatiquement les justificatifs** (reçus, factures, tickets).

- De **catégoriser les dépenses** automatiquement (juge si la dépense est légère ou lourde).

- D'éviter la saisie manuelle grâce à la **reconnaissance automatique**.

- De synchroniser les mouvements bancaires pour faciliter le suivi des frais.

Grace à l'automatisation du logiciel, Indy facilite la saisie des notes de frais, réduit les risques d'erreurs et le délai d'attente.

Comment intégrer avec le système comptable existant ?

Indy permet d'**exporter les dépenses en PDF ou Excel**, ce qui facilite l'intégration dans n'importe quel logiciel comptable.
Pour certains outils, l'export peut se faire au **format comptable**, ce qui simplifie encore plus l'importation par la comptabilité.

Quelle sont les procédures de validation des frais ?

Avec Indy, la procédure est la suivante :

1. L'utilisateur doit ajouter son ticket via une photo ou faire le scan pour l'envoyer.
2. Le logiciel va identifier automatiquement la dépense.
3. Le manager doit valider la note de frais et en juger si elle est nécessaire ou pas.
4. Le service de la comptable récupère directement les justificatifs via l'export.

Comment gérer les différents types de frais ?

C'est simple, Indy va classer automatiquement les dépenses dans les classes suivantes :

- Transport
- Repas
- Hébergement
- Déplacements (carburant, péages)

Avec tout ceci, cela félicite encore plus le travail pour le département de la comptable et les classes peuvent être modifiées facilement.

Quels est le délai de remboursement ?

Avec Indy, les notes de frais étant centralisées et automatisées, un délai de **7 à 10 jours** est réaliste après validation, toutes les informations sont classées et prêtes pour le département de la comptable qui l'examineront la demande.

Question 7 : Accès aux données de personnel

Quelles données RH doivent être accessibles ?

Les utilisateurs doivent accéder uniquement aux données et information nécessaires à leur mission donnée :

- Les Informations de base (nom, prénom, poste).
- Les coordonnées professionnelles au client ou autres.
- planning, absences et disponibilités.
- Utiliser les documents RH utiles (contrats, fiches de paie, attestations).

Les données sensibles (santé, sanctions, salaire détaillé...) doivent rester réservées au service RH.

Comment garantir la confidentialité des données ?

Les mesures pour garantir que les données sont protégées via :

- Un accès sécurisé via le **VPN avec une authentification forte (MFA)**,
- Chiffrement des données en transit et au repos.
- Vérification régulière du journal des accès (les info de quel personne à utiliser à quelle heure et quand)
- Le respect du RGPD avec droits strictement limités et aux respect de son règlement.

Quels niveaux d'accès différenciés mettre en place ?

Le niveau d'accès vari selon le grade de la personne si c'est un employé, un délégué ou un responsable.

Plusieurs niveaux :

- Utilisateur standard : accès à ses propres données uniquement.

- Manager : accès aux données de son équipe (planning, absences).

- RH (Ressource Humaine) : accès complet à toutes les données des personnes qui travaille dans l'entreprise.

- Administrateur : accès technique uniquement (pas aux données privées).

Comment intégrer avec le système RH existant ?

L'intégration peut se faire via :

- Une API fournie par le RH (par exemple Talentsoft, Silae, Lucca),

- Une synchronisation automatique des utilisateurs (annuaire Active Directory, SSO),

- Un tableau qui va centraliser le tous les données pour éviter les doublons ou dispersions.

Quelle procédure pour les nouveaux arrivants ?

La procédure d'intégration permet pour un nouveau salarié de garantir qu'il dispose rapidement de tous les accès nécessaires. Les étapes sont complètes et doit être suivis dans l'ordre :

1. Création du compte RH + mail professionnel,
2. Attribution des droits selon le poste du nouveau arrivant.
3. Remise des documents RH (contrat, règlement).
4. Formation aux l'outils RH,
5. Vérification des accès possédant dans la première semaine.

Question 8 : Maintenance et support à distance

Quels outils de surveillance à distance recommandez-vous ?

- **TeamViewer** ou **AnyDesk** pour la prise en main à distance pour la prise de contrôle à distance

- **GLPI** pour l'inventaire et le suivi du matériel,

- **Centreon** ou **Zabbix** pour la surveillance des performances.

Avec ceci, le technicien aura les logiciels nécessaires pour prendre le contrôle à distance des appareils, faire le suivi de matériel et surveiller les performances

Comment diagnostiquer un problème à distance ?

Les diagnostiquer à distance se font par étape :

1. Le technicien doit contacte l'utilisateur pour comprendre le problème.
2. Le technicien doit se connecte pour une **prise en main à distance** via TeamViewer ou AnyDesk.
3. Le technicien doit vérifier : messages d'erreur, mises à jour, connexion Internet, logiciels pour trouver les erreur/problèmes.
4. Le technicien applique les maintenance *correctifs ou *1préventif nécessaires si besoin.

*correctif : résoudre les glich ou bug.

*1préventif : mettre à jour, le préparé en ajoutant des protections comme des antivirus ou vérification.

Quelle procédure pour les pannes matérielles ?

En cas de panne matérielle, le technicien doit :

1. Faire un diagnostic rapide (à distance ou par téléphone).
2. Si la panne est confirmée :

- Remplacement du matériel ou pièce défectueux

- ou envoie de la garantie constructrice pour qui en envoie un autres sans payer.

3. L'utilisateur reçoit un PC de remplacement pour continuer à travailler.
4. Les données sont restaurées via OneDrive ou via un disque dur externe qui contient les données nécessaires pour continuer.

Comment gérer le remplacement rapide d'un équipement ?

Pour aller vite :

- Prévoir un **stock de secours** (2 ou 3 PC préconfigurés ou de pièce de rechange).

- Utiliser une **image système** (ISO) prête à être déployer.

- Réattribuer un équipement en moins d'une heure,

- Synchroniser automatiquement les données via OneDrive ou le transfert des donné de l'ancien poste au nouveau.

Avec ceci, le technicien est optimal pour faire les tâches à replacer le poste de la personne avec un temps optimal et organisé.

Quels indicateurs de suivi mettre en place ?

Les indicateurs utiles pour suivre sont :

- Temps de prise en charge d'un ticket.

- Temps de résolution.

- Nombre d'incidents par mois.

- Type de panne (logicielle/matérielle).

- Taux de satisfaction des utilisateurs.

- Taux de disponibilité des équipements.

Question 9 : Intégration avec l'infrastructure réseau existante

Comment intégrer les nouveaux équipements dans la segmentation VLAN existante

On intègre les nouveaux équipements en :

- Les affectant au VLAN correspondant à leur usage (ex : VLAN Visiteurs, VLAN Personnel, VLAN Administration, VLAN RH, etc...).

- Configurant les ports des switchs en mode “access” pour chaque équipement.

- En utilisant des plans d’adressage IP séparés pour chaque VLAN à chaque type d’attributions.
Cela garantit que chaque appareil est isolé selon son rôle avec pas d’emballement des données autre qui ne leur concerne pas et pour plus de sécurité.

Quelle est la politique d'accès Wifi pour les visiteurs en déplacement ?

La politique recommandée est :

- Une Wifi **“Visiteurs” isolé**, avec accès Internet uniquement sans passer par les serveurs.

- Un mot de passe de type WPA2/WPA3 a changé régulièrement.

- Aucun accès aux données internes.

- Un portail captif si nécessaire (page d’authentification).

Cela protège le réseau interne tout en offrant un accès simple aux visiteurs.

Comment garantir la sécurité des connexions distantes ?

Pour garder sécuriser les connexions distantes :

- Utilisation d’un VPN (SSL ou IPsec),

-Une Authentification forte (MFA),

- Filtrage des accès via un firewall,

- Chiffrement complet des données.

Seul le personnel de l’entreprise est autorisés peuvent accéder au réseau interne.

Quelle bande passante nécessaire pour 450 utilisateurs mobiles ?

La bande passante est en moyenne :

- 1 utilisateur = 2 à 5 Mb/s nécessaires (web, mails, outils pro).
- Pour 450 utilisateurs → environ **1 à 2 Gb/s** de capacité totale.

Cela dépend de l'usage et aussi de l'environnement mais une fibre **1 Gb/s minimum** est recommandée.

Comment monitorer l'utilisation du réseau ?

On peut surveiller le réseau avec des outils comme :

- Centreon (français),

- Zabbix.

- Nagios.

- ou des outils intégrés aux firewall (Fortinet, Stormshield, etc...).

La surveillance permet de suivre :

- La charge du réseau,
- Les pics d'utilisation,
- Les problèmes de performances,
- Les risques de saturation.
- Arrêter toute tentative de piratage.

Question 10 : Programme de formation et d'accompagnement

Quel format de formation recommandez-vous ?

Je recommande une formation de type **mixte**, c'est-à-dire :

- Présentiel pour expliquer les bases et répondre aux questions,

- vidéos / tutoriels en ligne pour revoir les procédures,

- Exercices pratiques pour manipuler le matériel et les logiciels de différent secteur ou filière pour découvrir.

Avec cela, c'est le format le plus efficace pour des visiteurs sur le terrain pour montrer comment les nouveaux sont formés.

Quelle est durée de formation par visiteur ?

La durée est de **1 journée complète** est suffisant :

- Matin : prise en main du matériel et outils numériques,

- Après-midi : exercices pratiques et configuration personnalisée pour tester leur capacité.

Quels sont les points essentiels à couvrir ?

Les points à aborder sont :

- L'utilisation de l'ordinateur et de la confidentialité.

- Se connecter au WiFi/VPN

- Utiliser les outils du métier (CRM, messagerie, rapports).

- Prendre des notes de frais et synchronisation des données.

- Avoir une bonne pratique de sécurité (mots de passe, sauvegardes).

Comment évaluer l'acquisition des compétences ?

On peut l'acquérir avec :

- Un quiz rapide.

- une mise en situation (se connecter au VPN, envoyer un rapport…).

- une validation par le formateur ou du personnel **RH**.

Quel support post-formation est à prévoir ?

Il faut prévoir des supports de type :

- **FAQ en ligne**,
- Une **vidéo courte**,
- Un accès au **support technique** (téléphone),
- Un petit **guide PDF** remis aux visiteurs.

Comment gérer la formation des nouveaux arrivants ?

On met en place une procédure simple :

1. On planifier une session d'accueil chaque semaine/mois aux nouveaux.
2. Fournir un ordinateur préconfiguré.
3. Faire une installation automatique des logiciels via l'image système (ISO).
4. Faire passer la même formation rapide que les autres.
5. Suivre la montée en compétence pendant les 2 premières semaines.

Question 11 : Documentation et livrables finaux

Quels documents techniques doive être fournir ?

Il est impératif de fournir les doc technique suivantes :

- La **documentation réseau** (VLAN, Wifi, VPN).

- La **documentation système** (image Windows, logiciels installés).

- Les **procédures de déploiement**.

- Les **paramètres de sécurité** (BitLocker, antivirus, accès).

Quelle documentation d'utilisateur est nécessaire ?

La documentation suivante et simple pour les visiteurs est :

- Un guide de prise en main du PC,

- Connexion Wifi et VPN,

- L'utilisation des outils métier (CRM, mails, notes de frais),

- Avoir une bonne pratique de sécurité.

-Un format conseillé : **PDF** + **vidéos courtes**.

Quelles procédures opérationnelles devrions décrire ?

Les procédures à rédiger recommander :

- Une procédure de **déploiement d'un poste**.
- Une procédure de **restauration des données**.
- Une procédure de **signalement de panne**.
- Une procédure de cas de **perte/vol** du matériel.

Ceci aidera en cas de problème pour le futur personnel.

Comment documentez la configuration de sécurité ?

Pour pouvoir documentez la configuration, il est recommandé de tester et puis le rédigé aux :

- Chiffrement **BitLocker**,
- Les règles du pare-feu,
- La gestion des comptes et mots de passe,
- Les droits d'accès selon les rôles,
- Les mises à jour automatiques.

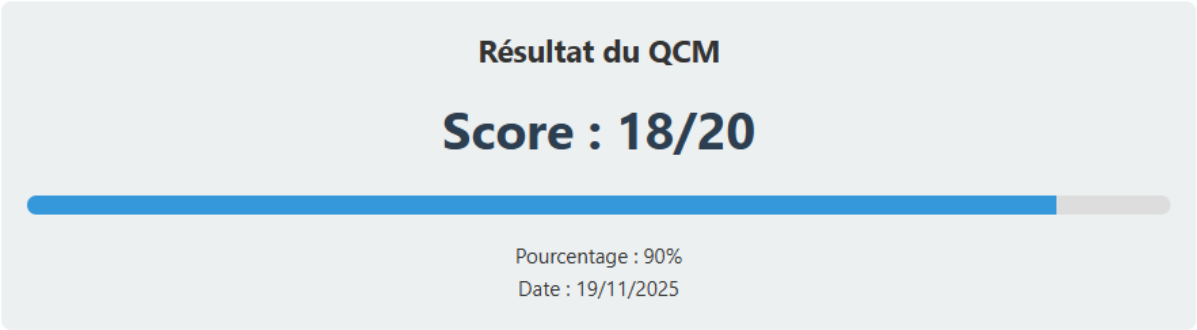
Maintenant que Tout est réuni dans un **document de politique de sécurité informatique**, la personne pourra le suivre puisque il l'a rédigé lui-même et s'il oublie, il a sa documentation.

Quels indicateurs de suivi proposez-vous ?

Les indicateurs utiles à voir sont :

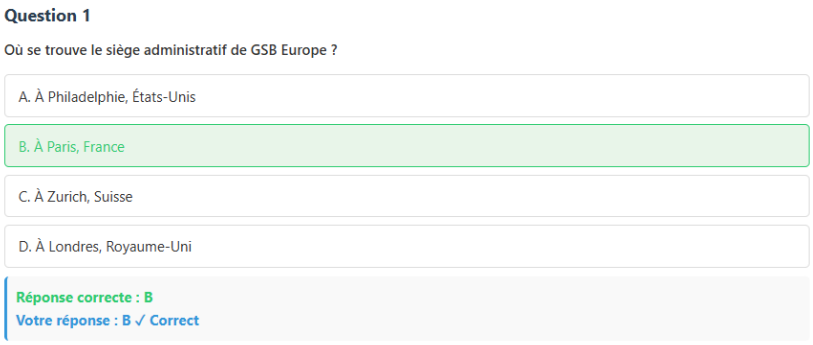
- Le taux de déploiement des postes (le temps de finir la tâche).
- Le nombre d'incidents par mois (nombre de fois qui y a eu un problème).
- Temps de résolution des tickets.
- La satisfaction des utilisateurs (leur avis).
- La conformité des postes aux règles de sécurité (les règles de politique)

QCM



Réponse aux questions QCM

Question 1 :



Question 2 :

Question 3 :

Question 3

Combien de visiteurs médicaux GSB compte-t-il en France métropolitaine ?

A. 250

B. 380

C. 480

D. 550

Réponse correcte : C
Votre réponse : C ✓ Correct

Question 4 :

Question 4

Quel est le format des adresses de messagerie chez GSB ?

A. nomUtilisateur@gsb.com

B. nomUtilisateur@swiss-galaxy.com

C. prenom.nom@gsb-europe.com

D. nomUtilisateur@galaxy-swiss.com

Réponse correcte : B
Votre réponse : B ✓ Correct

Question 5 :

Question 5

Quelle technologie est utilisée pour segmenter le réseau chez GSB ?

A. Sous-réseaux IP

B. VLAN

C. DMZ

D. VPN

Réponse correcte : B
Votre réponse : B ✓ Correct

Question 6 :

Question 6

Quel est l'adressage IP du VLAN 'Serveurs' ?

A. 192.168.10.0/24

B. 172.16.0.0/24

C. 10.0.0.0/24

D. 192.168.100.0/24

Réponse correcte : B
Votre réponse : B ✓ Correct

Question 7 :

Question 7

Quel VLAN est dédié aux visiteurs avec un accès limité à Internet uniquement ?

A. VLAN 10

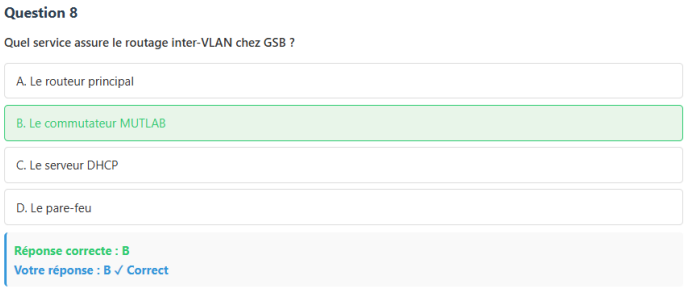
B. VLAN 100

C. VLAN 150

D. VLAN 200

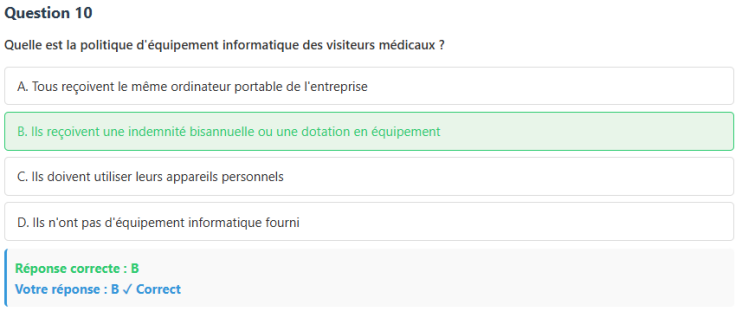
Réponse correcte : C
Votre réponse : C ✓ Correct

Question 8 :

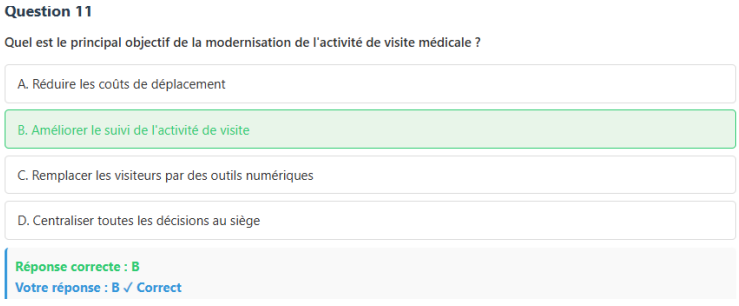


Question 9 :

Question 10 :



Question 11 :



Question 12 :

Question 13 :

Question 13

Quelle est la particularité de la salle 'Démonstration' ?

A. Elle est réservée aux réunions de direction

B. Elle dispose de paillasses et d'équipements de laboratoire

C. Elle est équipée de bornes WiFi haute performance

D. Elle héberge les serveurs principaux

Réponse correcte : B
Votre réponse : A ✗ Incorrect

Question 14 :

Question 14

Comment sont sécurisés les accès à la salle serveur ?

A. Par un système de reconnaissance faciale

B. Par un gardien présent 24h/24 et des accès contrôlés

C. Par des caméras de surveillance uniquement

D. Par des portes verrouillées avec code numérique

Réponse correcte : B
Votre réponse : B ✓ Correct

Question 15 :

Question 15

Quelle est la principale fonction du commutateur MUTLAB ?

A. Fournir une connexion Internet redondante

B. Assurer le routage inter-VLAN avec des ACL

C. Gérer les sauvegardes des serveurs

D. Contrôler l'accès WiFi des visiteurs

Réponse correcte : B
Votre réponse : B ✓ Correct

Question 16 :

Question 16

Quels services peuvent être accessibles depuis le VLAN 'Visiteurs' ?

A. Tous les services internes de l'entreprise

B. Uniquement les serveurs DNS et DHCP

C. Les serveurs de messagerie et intranet

D. Les bases de données métier

Réponse correcte : B
Votre réponse : C ✗ Incorrect

Question 17 :

Question 17

Quelle est la structure hiérarchique des visiteurs médicaux ?

A. Visiteur → Délégué régional → Responsable de secteur

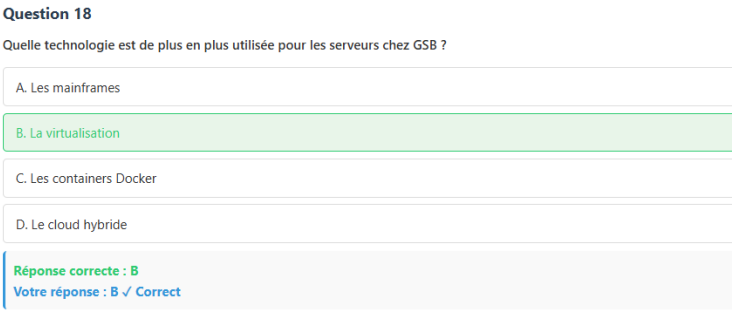
B. Visiteur → Responsable de secteur → Délégué régional

C. Visiteur → Directeur commercial → DSI

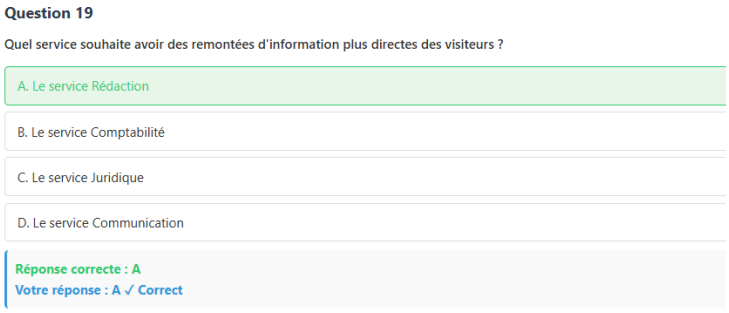
D. Visiteur → Service RH → Direction

Réponse correcte : A
Votre réponse : A ✓ Correct

Question 18 :



Question 19 :



Question 20 :

Conclusion :

Au cours du TP, j'ai trouvé cela intéressant car elle a permis de m'élargir les connaissances à mener une recherche, d'améliorer ma capacité à analyser des documents et à la compréhension.

J'ai trouvé ce TP très enrichissant aux connaissances.