AP1

LIVRABLE 1
GROUPE N°3

REPONSE AU CAHIER DES CHARGES

Fourniture d'une solution informatique nomade sécurisée

Date limite de réponse : 27 Octobre 2024

BTSSIO

AP1 - LIVRABLE 1

GROUPE N° 3 Samy ALBISSER – Arman ABGARYAN
RÉPONSE AU CAHIER DES CHARGES

A) Composition et Présentation de votre Groupe

Composition du Groupe :

- **ALBISSER Samy : Travail chez Carsat en tant que technicien support utilisateur.**
- **ABGARYAN Arman : Travail chez SDIS 67 en tant qu'administrateur réseau et télécommunication.**

B) Définitions des Rôles et Responsabilités

- **Chef de Projet :**
  - **ALBISSER Samy**
- **Répartition des Tâches :**
  - **Nous ferons toutes les tâches en binôme.**

---

2) Rappel des Besoins et des Objectifs du Projet

A) Présentation de l'Existant

L'entreprise GSB rencontre plusieurs difficultés dans la gestion et la sécurité de son parc informatique, notamment :

- **Pertes de matériel et vols : Des incidents de pertes ou vols de matériel ont conduit à des fuites de données sensibles, causant une perte de contrats et impactant le chiffre d'affaires de l'entreprise.**
- **Processus manuel de configuration : Les postes sont actuellement configurés manuellement, ce qui est chronophage et inefficace, notamment pour une flotte de 100 laptops.**
- **Absence de solution collaborative sécurisée : Les employés utilisent des services non contrôlés tels que Google Drive ou Dropbox, augmentant ainsi le risque de perte ou d'interception d'informations.**

B) Expression des Besoins

Les visiteurs médicaux doivent utiliser des équipements nomades sécurisés pour leurs interactions avec les clients. Les données doivent être protégées conformément aux réglementations (RGPD) et les processus automatisés pour faciliter la gestion des postes.

C) Objectifs à Réaliser

- **Sécurisation des postes nomades : Assurer la sécurité des postes utilisés par les visiteurs médicaux pour diverses tâches professionnelles, en conformité avec le RGPD.**
- **Réduction des coûts : Proposer une solution économique basée sur des logiciels open-source tout en garantissant un niveau de sécurité optimal.**
- **Automatisation des processus : Simplifier la gestion des postes en automatisant la configuration, la sécurisation et les mises à jour afin de gagner du temps et éviter les erreurs humaines.**

---

3) Solution Proposée

A) Solutions Techniques et Logicielles et Justification des Choix

Sécurisation des Systèmes d'Exploitation (ANSSI)

Nous appliquerons les mesures de sécurité recommandées par l'ANSSI pour les systèmes Windows et Linux. Ces mesures comprennent, entre autres, des restrictions d'accès, la configuration de pare-feux (UFW sur Linux), et des paramètres de gestion de mots de passe (longueur, complexité, expiration).

1. Sécurisation de Windows 10 Entreprise

- **Renforcement de l'authentification :**
  - **Utilisation de mots de passe complexes (12 caractères minimum), expiration tous les 90 jours, et verrouillage après 3 tentatives échouées, conformément aux recommandations de l'ANSSI.**
  - **Double authentification (2FA) pour les accès sensibles.**
- **Configuration du pare-feu et des services réseaux :**
  - **Désactivation des protocoles obsolètes comme NTLMv1 et SMBv1.**
  - **Pare-feu Windows configuré pour bloquer les connexions non autorisées.**
  - **Journalisation avancée pour capturer les tentatives d'accès et autres événements critiques.**
- **Chiffrement des données :**
  - **Activation de BitLocker pour chiffrer les disques durs, protégeant les données en cas de vol de matériel.**
- **Automatisation via PowerShell :**
  - **Scripts PowerShell pour appliquer et automatiser les politiques de sécurité sur tous les postes (GPO, chiffrement, services réseau).**

2. Sécurisation de Linux Mint

- **Pare-feu et contrôle des accès :**
  - **UFW (Uncomplicated Firewall) pour contrôler les connexions réseau et limiter les accès non autorisés.**
  - **SSH sécurisé avec clés publiques et limitation des accès par IP approuvées.**
  - **fail2ban pour bloquer les tentatives de force brute.**
- **Mises à jour et correctifs :**
  - **Mises à jour régulières via apt pour corriger rapidement les vulnérabilités.**
  - **Notifications des mises à jour critiques à appliquer.**
- **Chiffrement et intégrité des données :**
  - **Chiffrement des disques via LVM pour protéger les données en cas de vol ou perte.**
  - **Outils comme AIDE (Advanced Intrusion Detection Environment) pour surveiller les modifications des fichiers système.**

3. Conformité RGPD et gestion des incidents

- **Journalisation et audit :**
  - **Journalisation activée pour suivre les événements critiques (accès, modifications de fichiers).**
  - **Conservation des journaux conformément aux recommandations de l'ANSSI.**
- **Plan de gestion des incidents :**
  - **En cas d'incident, un plan de réponse basé sur les recommandations ANSSI sera activé. Ce plan inclura la détection, l'analyse, la correction et la notification des violations.**

Automatisation du Déploiement des Logiciels

- **Linux (apt) : Utilisation d'apt pour le déploiement des logiciels sous Linux avec des scripts Bash exécutés via SSH pour garantir une mise à jour centralisée.**
- **Windows (winget & Chocolatey) : Utilisation de winget et Chocolatey pour les logiciels non disponibles nativement. Intégration dans des scripts PowerShell pour standardiser la configuration logicielle.**

Améliorations pour un cadre d'entreprise

- **Ivanti : Gestion centralisée des mises à jour, correctifs, et déploiements logiciels avec granularité.**
- **FOG Project : Déploiement rapide des systèmes via réseau.**

Sauvegarde et Restauration

- **Rescuezilla : Sauvegarde et restauration via des images complètes des postes, chiffrées pour respecter le RGPD. Sauvegardes sur disques externes sécurisés.**

Améliorations pour un cadre d'entreprise

- **Chiffrement des images de sauvegarde.**
- **Stockage sécurisé : Images sur serveurs sécurisés, avec accès restreint.**

- **Plan de tests de restauration pour garantir l'intégrité des sauvegardes.**

Justification des Choix

- **Coût : Solutions open-source pour réduire les coûts de licences.**
- **Sécurité : Alignement sur les bonnes pratiques de l'ANSSI, avec une conformité RGPD.**
- **Facilité de déploiement : Scripts pour automatiser et standardiser les configurations.**

B) Présentation des Matériels, Logiciels et Descriptifs de Fonctionnements + Bonus coût interne / externe

Version Étudiant BTS SIO (Open Source)

Coûts des logiciels (Open Source) :

- **Linux Mint (Open Source) : 0 €**
- **Rescuezilla (Open Source) : 0 €**
- **ClamAV (Open Source Antivirus) : 0 €**
- **UFW (Pare-feu Linux) : 0 €**
- **apt et winget/chocolatey (Outils de déploiement Linux/Windows) : 0 €**
- **Total logiciels : 0 €**

Coût de la main-d'œuvre (étudiants) :

- **Nombre d'heures par étudiant : 4 heures/jour × 30 jours = 120 heures/étudiant**
- **Coût horaire estimé pour étudiants : 15 €/heure**
- **Total main-d'œuvre : 15 €/heure × 120 heures × 2 étudiants = 3 600 €**

Coût global (gestion du parc informatique) :

- **Hypothèse d'une gestion continue : 5 heures par mois**
- **Coût total annuel : 15 €/heure × 5 heures × 12 mois = 900 € par an**

Pertes évitées et gains potentiels :

- **Hypothèse de pertes de contrats à cause de failles : ~50 000 € par an**
- **Avec la sécurisation, gain potentiel grâce à la protection des données : 50 000 €**

Version Entreprise (Logiciels payants et gestion plus complexe)

Coûts des logiciels (version entreprise) :

- **Windows 10 Enterprise (100 postes) : 80 €/poste × 100 postes = 8 000 €**
- **Ivanti (Gestion de déploiement logiciel) : 20 €/poste × 100 postes = 2 000 €**
- **ClamAV (Support entreprise) : 12 €/poste × 100 postes = 1 200 €**
- **Solution de gestion FOG Project : 10 €/poste × 100 postes = 1 000 €**
- **Total logiciels : 12 200 €**

Coût de la main-d'œuvre (professionnel) :

- **Chef de projet : 50 €/heure × 100 heures = 5 000 €**

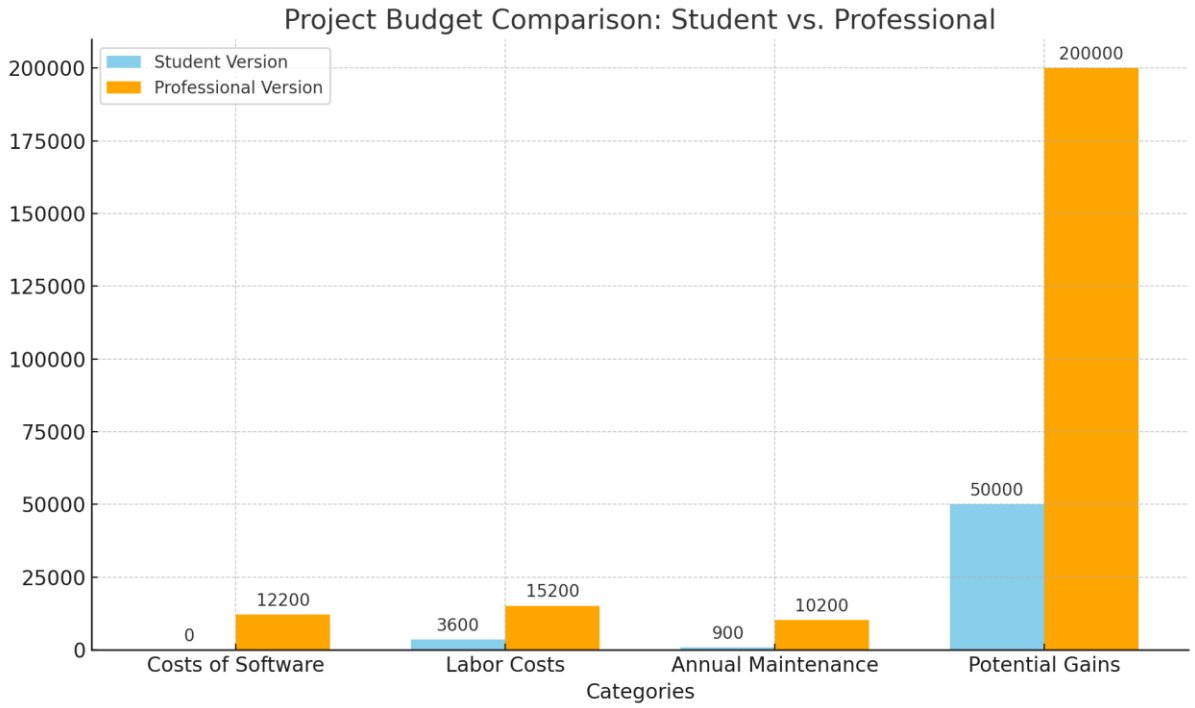
- **Développeur (pour les scripts et automatisations) : 40 €/heure × 150 heures = 6 000 €**
- **Administrateur systèmes : 35 €/heure × 120 heures = 4 200 €**
- **Total main-d'œuvre : 15 200 €**

Coût global (gestion du parc informatique) :

- **Gestion mensuelle de 10 heures (Chef de projet et administrateur) :**
- **Coût annuel : (50 €/heure + 35 €/heure) × 10 heures × 12 mois = 10 200 € par an**

Pertes évitées et gains potentiels :

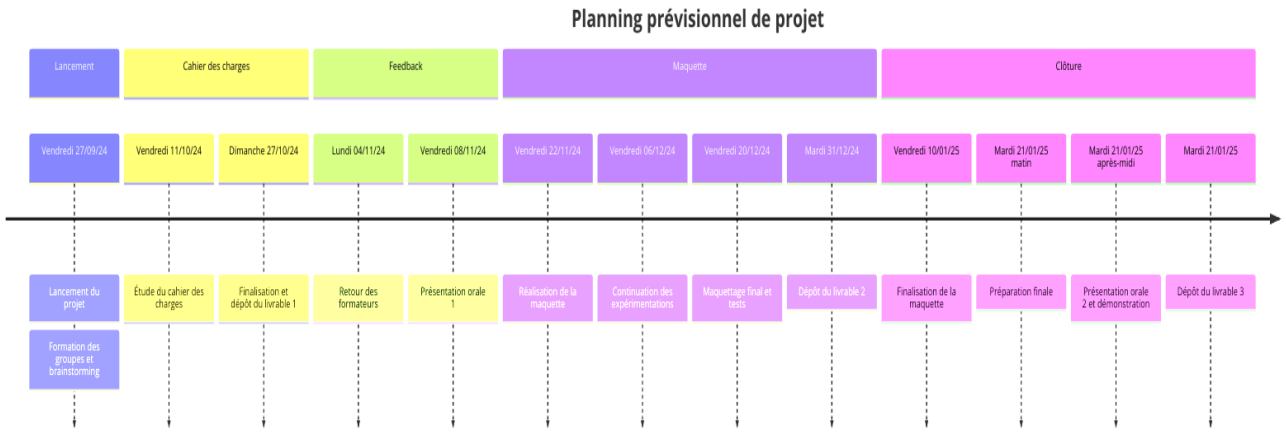
- **Hypothèse de pertes annuelles dues à la cyberattaque : 200 000 €**
- **Gain potentiel grâce à une sécurisation renforcée : 200 000 € par an**



C) Planning Prévisionnel / Liste des Tâches

N°	Date	Tâches	Livrables/Événements
1	Vendredi 27/09/2024	Lancement du projet, présentation des solutions	Formation des groupes, premières idées
2	Vendredi 11/10/2024	Étude du cahier des charges, préparation des réponses	Discussion sur les solutions

3	**Dimanche 27/10/2024**	**Finalisation et dépôt du Livrable 1**	**Réponse au cahier des charges**
4	**Lundi 04/11/2024**	**Réception des retours des formateurs**	**Feedback**
5	**Vendredi 08/11/2024**	**ORAL 1 : Présentation du cahier des charges**	**Première soutenance orale**
6	**Vendredi 22/11/2024**	**Réalisation de la maquette, début des expérimentations**	**Avancement de la maquette**
7	**Vendredi 06/12/2024**	**Continuation des expérimentations et ajustements**	**Tests et ajustements**
8	**Vendredi 20/12/2024**	**Maquettage final et tests en commun**	**Préparation de la documentation**
9	**Mardi 31/12/2024**	**Dépôt de Livrable 2 : Documentation d'installation**	**Livrable 2**
10	**Vendredi 10/01/2025**	**Finalisation de la maquette, tests et corrections**	**Ajustements finaux**
11	**Mardi 21/01/2025 (matin)**	**Préparation de la clôture du projet**	**Préparation finale pour l'oral**
12	**Mardi 21/01/2025 (après-midi)**	**ORAL 2 : Clôture du projet et démonstration technique**	**Deuxième soutenance**
13	**Mardi 21/01/2025**	**Dépôt de Livrable 3 : Documentation technique finale**	**Livrable 3**



Conclusion

Notre solution répond aux objectifs du cahier des charges, notamment :

- **Sécurisation des postes nomades : Les mesures proposées garantissent la protection des données et respectent le RGPD.**
- **Automatisation des processus : Les scripts permettent de réduire les interventions manuelles et d'améliorer la productivité.**
- **Réduction des coûts : Grâce à l'utilisation de logiciels open-source, nous proposons une solution économique sans sacrifier la sécurité.**

En version professionnelle, des outils comme Ivanti ou FOG Project permettraient une gestion à grande échelle avec des déploiements automatisés. La version BTS SIO, quant à elle, offre une approche minimaliste mais efficace, respectant les contraintes budgétaires strictes. Le gain potentiel en termes de réduction des pertes dues à des failles de sécurité est significatif, justifiant pleinement la mise en œuvre de cette solution.

Bonus : Diagramme de GANTT :