PROJET GSB

AP1
CAHIER DES CHARGES

Fourniture d'une solution informatique nomade sécurisée

Propriétés	Description
INTITULE	Définition de l'équipement nomade sécurisé, approprié pour l'usage des visiteurs médicaux.
PRESENTATION RAPIDE	Le projet consiste à mettre en œuvre des équipements sécurisés pour les visiteurs médicaux,
POSITIONNEMENT	Semestre 1 Semestre 2 Semestre 3 Semestre 4 >>>>
DUREE ESTIMEE EN SEMAINE	10 semaines
NOTIONS EDM	D5.1 – L'obligation de sécuriser les données numériques EM4.5 – Le système d'information et les risques organisationnels
Modalités de réception	Présentation d'un système opérationnel – recettage d'une solution stephane.beteta@ecp-apprentissage.fr gabriel.beteta@sdir.eu

Lancement : 27/09/2024 – Fin : 21/01/2025

SOMMAIRE

1) CONTEXTE

1.1) Introduction

L'entreprise GSB *(Gabriel&Stéphane BETETA)* commercialise des produits médicaux à destination des professionnels de santé. Plusieurs commerciaux, des « Visiteurs médicaux » vont au contact des clients et prospects.

Afin d'être plus réactif et compétitif, l'entreprise souhaite développer l'administration de son Système d'Informations et les outils métiers.

1.2) Descriptif de l'existant

Actuellement, l'entreprise GSB a une centaine de postes, il y a eu plusieurs incidents par manque de suivi et d'inventaire.

Le matériel est sous la responsabilité de chaque salarié qui a pris en compte le matériel affecté. Le poste est préparé par le Service Informatique avant affectation, c'est une tâche fastidieuse puisque chaque poste est configuré individuellement.

Le matériel ne retourne en maintenance qu'en cas de panne ou de restitution du matériel à la suite du départ du salarié.

Il y a eu des cas de pertes ou de vol, avec très probablement des vols de données. L'entreprise suspecte d'ailleurs des pertes de contrats et donc de Chiffre d'Affaires à la suite de ces incidents.

Par ailleurs, le travail collaboratif n'est pas facilité, il y a beaucoup d'échanges par courriel ou par des services tiers, Google Drive, Dropbox, avec une possible perte ou interception d'informations.

1.3) Expression de besoins

GSB possède une flotte de 100 laptops.

Dernièrement, la moitié des laptops ont été réinstallé avec ***Windows 10 Enterprise*** ; une version adaptée aux besoins des entreprises et normalement plus stable et sécurisé et le reste avec ***Linux Mint Cinammon*** une interface proche de Microsoft Windows.

La Direction de GSB impose de développer la Sécurité des Systèmes d'Informations (SSI).

Lors d'une intervention d'un auditeur en cybersécurité dans l'entreprise, des failles physiques et des failles dans les systèmes d'exploitation Microsoft Windows (toutes versions) et GNU/LINUX ont été démontrés.

De plus ,la société GSB a été sensibilisé au Règlement Général sur la Protection des Données (RGPD), de ce fait, elle impose son DSI et son équipe de trouver une solution technique pour remédier aux différents problèmes dans les 2 environnements ; Windows et Linux.

Les postes de travail nomades sont destinés à :

- La saisie de comptes-rendus
- La visualisation de la documentation technique (au format PDF)
- Un usage professionnel (exploitation de données, tableurs, messagerie électronique, rédaction de lettres diverses, gestion d'un budget d'activité, etc.).

L'usage personnel de l'équipement peut être envisagé, mais cela ne doit pas être fait depuis le profil professionnel. Aucune garantie ou dépannage relatifs aux outils personnels installés sur le matériel ne seront proposés.

2) OBJECTIFS DU PROJET

Chaque groupe devra mettre en œuvre une solution technique répondant aux objectifs suivants :

- Respecter la date de début (27/09/24) et de fin de projet (21/01/25)
- La solution doit être à moindre coût
- Rendre les livrables et effectuer les soutenances aux dates prévues

A REALISER

1) Etude du projet et réponse au cahier des charges (planning, coûts…)

- Sécurisation physique des postes
- Mise en œuvre des solutions informatiques
- Equipements (postes/serveurs…)
- Coût des licences ANNEXE 3
- Coût de la main d'œuvre

2) Sécurisation du système d'exploitation Windows 10 Entreprise/Professionnel

- Application des consignes/paramètres de sécurité ANNEXE 1

3) Sécurisation du système d'exploitation *Linux Mint*

- Application des consignes/paramètres de sécurité ANNEXE 2

4) Outil de déploiement de logiciels

- L'objectif est de faciliter et d'accélérer la préparation d'un poste de travail
- Le déploiement des logiciels et différents outils sous Windows devront se faire de manière automatique sous forme de scripts.

5) Mettre en œuvre une solution de sauvegarde et restauration d'un poste de travail (local privilégié)

- L'objectif est de faciliter l'installation ou la réinstallation des postes de travail
- Identifier une solution de sauvegarde complète permettant la préparation d'une image de poste de travail (masterisation), prête à être restaurée/déployée sur un poste.
- Préparer un poste de travail, prêt à l'emploi, avec la partition Linux et Windows demandée. Il n'est pas obligatoire que ce soit une solution client/serveur (via réseaux).

6) Réaliser une documentation complète de l'ensemble du projet

- Chaque logiciel, installation, matériel doit être documenté
  (A la manière d'un mode d'emploi, captures d'écrans, explications)
- Chaque apprenant est responsable de sa documentation

En compléments des objectifs fixés, voici les contraintes de sécurité à respecter

A) Sécurité

1. Le Système d'Informations doit être accessible aux seuls acteurs de l'entreprise GSB.
2. La Stratégie de sécurité locale doit être modifiée sur chaque poste pour prendre en compte les paramètres suivants :
   - Stratégie de mot de passe : longueur minimale 12 caractères, durée de vie : 90 jours, verrouillage de compte à 3 tentatives, durée de verrouillage 30 minutes.

Vous pouvez prendre connaissance des documents mis à disposition par l'Agence Nationale de la Sécurité des Systèmes d'Informations

2.2) Responsabilités

- Le commanditaire fournira à la demande toute information sur le contexte nécessaire à la mise en place de l'infrastructure.
- Le prestataire est à l'initiative de toute proposition technique.
- Le prestataire fournira un système opérationnel sous forme de machines virtuelles
- Le prestataire présentera une maquette

4) GROUPES ET EVALUATIONS

4.1) Constitution des groupes

- Chaque groupe auto-constituée sera composé de 2 apprenants.
- Chaque groupe désigne un Chef de Projet, qui sera l'unique interlocuteur auprès des formateurs pour toutes questions en dehors des séances.
- Chaque apprenant qui met en œuvre une solution doit créer la documentation technique associée

4.2) Planning prévisionnel

9 séances dont 2 d'évaluations

1. Vendredi 27/09/24 matin : LANCEMENT DU PROJET :

Tour de table (Qui vous êtes et pourquoi vous êtes là ?) / Règles et cadre de travail / assistance Teams-Mails / Création des groupes de travail / Présentation des examens E4-E5 / Présentation du sujet / Remue-Méninges de solutions

2. Vendredi 11/10/24 matin : Etude du cahier des charges et préparation de réponses

Dimanche 27 octobre 2024 : LIVRABLE 1 à déposer dans vos dossiers partagés

Réponse des formateurs le lundi 04/11/24 - EVALUATION-GROUPE-X.docx dans vos dossiers partagés

3. Vendredi 08/11/24 matin : ORAL 1- Réponse au cahier des charges
4. Vendredi 22/11/24 matin : Réalisation maquette/expérimentation
5. Vendredi 06/12/24 matin : Réalisation maquette/expérimentation
6. Vendredi 20/12/24 matin : Maquettage et tests en commun

Mardi 31/12/24 : LIVRABLE 2 à déposer dans vos dossiers partagés

7. Vendredi 10/01/25 matin : Poursuite maquettage et tests en commun
8. Mardi 21/01/25 matin : Préparation de clôture
9. Mardi 21/01/25 après-midi : ORAL 2 / Clôture du projet

Mardi 21/01/25 : LIVRABLE 3 à déposer dans vos dossiers partagés

Aide méthodologique :

1. Constitution du groupe de 2 personnes
2. Lire le sujet
3. Créer une liste des tâches
4. Établir le travail nécessaire à chaque tâche en heures ou jours *(par exemple)*
5. Définir l'ordre chronologique des tâches (tâches en parallèles ou après qu'une soit terminée)
6. Calculer la planification du projet *(combien d'heures ou de jours au total pour réaliser le projet ?)*
7. Affecter les tâches aux personnes
8. Organiser le travail, agenda partagé, outils comme Trello, fixer les dates et les tâches

NB : Vous avez le droit d'organiser des sessions de travail en ligne sous forme de « soutien » / réaliser un travail collaboratif entre les groupes

4.3) Notations

La notation est individuelle.

Il y aura plusieurs coefficients :

- Coeff. 1 pour chaque Oral / QCM
- Coeff. 2 pour chaque production écrite
- Coeff. 3 pour la démonstration technique (maquette VMs)

4.4) Evaluations - Livrables et Oraux

- Le groupe livrera/déposera sur le dossier partagé avec les formateurs les différents livrables, dans les délais. Chaque membre du groupe aura accès au dossier partagé (OneDrive ECP)
- A chaque séance, il faudra compléter le tableau de suivi partagé avec les formateurs sur Teams
- Rendre compte de problèmes par courriel aux formateurs ou conversation Teams (avec les deux formateurs invités dans la conversation).

TEAMS : AVANT LE VENDREDI 27 SEPTEMBRE 2024 (16H30)
Chaque groupe complètera le document « Liste des groupes » partagé dans le canal AP1 sur Teams

LIVRABLE 1 : PROPOSTION TECHNIQUE ET COMMERCIALE
A RENDRE LE DIMANCHE 27 OCTOBRE 2024 (avant 23h59)

Rédaction d'un document de réponse argumentée au Cahier des Charges, selon le modèle proposé : « LIVRABLE_1_Reponse_CDC ».
1 seul document pour chaque groupe (*annexes autorisées, ex : schéma, diagrammes…*)

Ce document contiendra à minima :

- La composition et présentation de votre groupe
- Le rappel des besoins et objectifs du projet
- Votre solution argumentée :
  - *Présentation de chaque solution + arguments du choix par rapport au cahier des charges*
- La liste des tâches prévisionnelle de votre projet
  (Lister les tâches dans l'ordre chronologique ; pour vous aider, identifier les tâches que vous pouvez réaliser sans attendre qu'une autre soit terminée)

- Planning prévisionnel consolidé par le groupe
  (Tableau avec liste des tâches dans l'ordre chronologique et dates + dates importantes du projet, oraux, livrables…)

    - BONUS : *Diagramme de Gantt*
      Doit permettre de déterminer le temps nécessaire à la réalisation du projet et son ordonnancement. Combien de jours/heures sont nécessaires ? -> coût de la main d'œuvre

- (Bonus) Budget / Coût du projet (devis en 2 versions, Interne / Externe)

ORAL 1 : LE VENDREDI 08 NOVEMBRE 2024 MATIN

- PRESENTATION ORALE DE REPONSE AU CAHIER DES CHARGES : 20 minutes
  10 minutes de présentation puis 10 minutes de questions / réponses
  Le diaporama sera déposé dans le dossier partagé avec les formateurs

Chaque groupe présentera aux formateurs sa réponse au cahier des charges (la solution proposée) à l'aide d'un support projeté.

Le contenu reprendra les éléments du livrable 1, mais la forme de la présentation doit être concise pour respecter le temps de soutenance.

LIVRABLE 2 : DOCUMENTATION D'INSTALLATION V1
A RENDRE LE MARDI 31 DECEMBRE 2024 (avant 23h59)

Chaque groupe livrera une première version de la documentation d'installation du projet selon le modèle proposé « LIVRABLE_2_Doc_V1_installation_du_projet_GROUPE_X_YYYYMMJJ_HHMM.docx »

La version finale sera remise au livrable 3.

Chaque apprenant qui met en œuvre est responsable de la production de sa documentation

--

ORAL 2 : LE MARDI 21 JANVIER 2025- APRES-MIDI

- PHASE 1 - PRESENTATION ORALE DE CLÔTURE DU PROJET : 20 minutes
  10 minutes de présentation puis 10 minutes de questions / réponses
  Le diaporama sera déposé dans le dossier partagé avec les formateurs

  Chaque groupe présentera à l'oral son bilan du projet, à l'aide d'un support projeté. ATTENTION, ne pas reprendre le contenu de l'ORAL-1 (un léger rappel de la présentation du groupe, des objectifs et de la solution prévue à mettre en œuvre est toléré mais il faut surtout expliquer les écarts et expliquer les difficultés rencontrées ou les problèmes en cours).

  C'est une synthèse qui permettra de :
    - Formaliser les écarts finaux entre les résultats obtenus et les résultats attendus (Objectifs)
    - Cristalliser les bonnes pratiques à pérenniser et garder trace des erreurs à ne plus commettre
    - Faire partager à toute l'équipe de projet l'analyse finale du projet

- PHASE 2 - DEMONSTRATION TECHNIQUE ET FONCTIONNELLE DE LA SOLUTION : 20/30 minutes
  Chaque groupe présentera techniquement la solution validée par le client à l'Oral 1 (CdC).

  Les maquettes devront permettre aux formateurs de vérifier le bon fonctionnement de l'ensemble de la solution ainsi que la cohérence des éléments entre eux dans la solution.

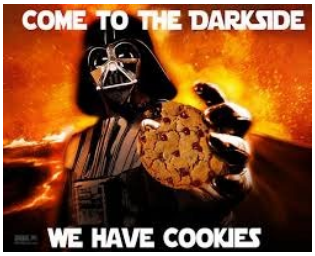
  Nous souhaitons que chaque membre du groupe pratique, répartissez-vous les tâches de façon à ce que chacun puisse nous démontrer et expliquer quelque chose. Nous poserons des questions.

LIVRABLE 3 : DOCUMENTATION TECHNIQUE
A RENDRE LE MARDI 21 JANVIER 2025 (avant 23h59)

- Remise de la documentation technique finale (Installation/exploitation)
  Modèle : LIVRABLE_3_Documentation_technique_GROUPE_X_YYYYMMJJ_HHMM.docx

*(À la façon d'un mode d'emploi, rédigée et mise en forme à rendre sous format électronique .**DOCX et .PDF, obligatoire.)***

4.5) Pénalités et Bonus



- Les productions écrites appelés « Livrables » ont des dates de remise à respecter. Chaque jour de retard entraîne le retrait d'1 point (1/20), à l'exception du livrable 3 (dernier livrable), sanctionné d'un 0/20.

- La remise aux formateurs des attestations de réussite des MOOC suivants seront comptabilisés (note sur 20 coeff. 1).

SecNumacadémie.gouv.fr
Formez-vous à la sécurité du numérique

pix CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

https://secnumacademie.gouv.fr/ - https://atelier-rgpd.cnil.fr/ - https://pix.fr -
https://www.netacad.com/fr/courses/cybersecurity - https://www.netacad.com/fr/courses/iot

Networking Academy

SITOGRAPHIE

https://www.ecp-apprentissage.fr/

https://www.ssi.gouv.fr/administration/bonnes-pratiques/

OUTILS

https://trello.com

https://www.notion.so/fr-fr/product/projects

ANNEXES

ANNEXE 1 : SECURISATION DE MICROSOFT WINDOWS

ANNEXE 2 : SECURISATION DE GNU/LINUX

ANNEXE 3 : LICENCES CLIENTS WINDOWS

ANNEXE 1

Sécurisation de Microsoft Windows

Actions à effectuer :

1. **Paramètres Biométriques et d'Écran de Verrouillage :**
   - Amélioration de la protection anti-spoofing pour la reconnaissance faciale.
   - Désactivation de l'utilisation de la caméra sur l'écran de verrouillage.
   - Empêchement de l'activation vocale des applications sur un appareil verrouillé.

2. **DNS et Sécurité Réseau :**
   - Désactivation de la diffusion DNS Multicast et des requêtes parallèles A et AAAA.
   - Désactivation de NTLMv1.
   - Désactivation de SMBv1.
   - Activation de l'UAC et configuration des paramètres associés.

3. **Sécurité des Mots de Passe et de l'Authentification :**
   - Désactivation de l'enregistrement des mots de passe en clair en mémoire.
   - Restriction des types de chiffrement Kerberos.
   - Désactivation de PowerShell V2.
   - Désactivation d'AutoRun.

4. **Protection Réseau :**
   - Activation de la signature SMB/LDAP.
   - Configuration des paramètres de sécurité des membres de domaine.
   - Activation de SmartScreen.

5. **Paramètres de Windows Defender :**
   - Activation de diverses protections dans Windows Defender.
   - Configuration des fonctionnalités cloud et des protections contre les exploits système.

6. **Sécurité MS Office :**
   - Sécurisation de diverses versions de MS Office contre les attaques de malspam.

7. **Journalisation des Événements Windows :**
   - Augmentation de la taille des journaux d'événements de sécurité.
   - Activation de la journalisation des données de ligne de commande pour la création de processus.

8. **Mesures de Sécurité Avancées :**
   - Activation des paramètres de sécurité avancés.
   - Activation de la journalisation des modules PowerShell et des blocs de scripts.
   - Configuration des politiques d'audit.

9. **Sécurité lsass :**

- Renforcement de lsass contre le vol d'informations d'identification.

10. **Désinstallation des Applications Indésirables :**

- Suppression des applications intégrées inutiles.

11. **Pare-feu et Blocage des Connexions :**

- Activation du Pare-feu Windows.
- Blocage des connexions à partir de binaires spécifiques (LOLBins).

12. **Mises à Jour Windows et AutoRun :**

- Activation des mises à jour automatiques de Windows.
- Désactivation de l'autorun pour les dispositifs non volumineux.

Notes Importantes

- L'idéal est de faire un script PowerShell qui doit être exécuté avec des privilèges administratifs (BONUS !).

- Assurez-vous d'avoir une sauvegarde avant d'appliquer des changements, car certaines modifications peuvent affecter le comportement du système.

ANNEXE 2

Sécurisation de GNU/Linux

Actions à effectuer :

1. **Mise à Jour du Système :**
   - Les mises à jour du système incluent des correctifs de sécurité critiques qui corrigent les vulnérabilités découvertes. En maintenant le système à jour, vous réduisez le risque d'exploitation de failles de sécurité connues.
2. **Configuration du Pare-feu UFW :**
   - Un pare-feu bien configuré limite les connexions non autorisées à votre système. UFW (Uncomplicated Firewall) est un outil convivial pour configurer le pare-feu sur Linux, aidant à bloquer ou autoriser le trafic réseau de manière contrôlée.
3. **Désactivation des Services Non Nécessaires :**
   - La désactivation de services non nécessaires réduit la surface d'attaque potentielle. Chaque service actif peut être une porte d'entrée potentielle pour les attaquants. En désactivant les services inutiles, vous minimisez les risques de sécurité.
4. **Sécurisation de SSH :**
   - SSH (Secure Shell) est une porte d'entrée majeure pour de nombreux systèmes Linux. En sécurisant SSH, en désactivant l'accès root et en n'autorisant que l'authentification par clé, vous renforcez la sécurité des connexions distantes.
5. **Installation de ClamAV et Lynis :**
   - ClamAV est un logiciel antivirus pour Linux qui peut détecter et éliminer les logiciels malveillants. Lynis est un outil d'audit de sécurité qui analyse le système à la recherche de vulnérabilités. L'installation de ces outils renforce la capacité de détection et d'audit de votre système.
6. **Restriction d'Accès aux Journaux Système :**
   - Limiter l'accès aux journaux système renforce la confidentialité des informations contenues dans ces journaux, réduisant ainsi le risque de manipulation ou d'exploitation par des utilisateurs non autorisés.
7. **Activation de l'Audit Système :**
   - L'audit système permet de suivre et de surveiller les activités du système, contribuant ainsi à la détection des comportements malveillants et à la prévention des attaques.

8. **Configuration des Règles iptables :**

   - iptables est un outil puissant pour configurer les règles de pare-feu sur Linux. La configuration appropriée des règles iptables contribue à contrôler le trafic réseau entrant et sortant, renforçant ainsi la sécurité.

9. **Désactivation de l'Exécution de Scripts dans /tmp :**

   - Désactiver l'exécution de scripts dans le répertoire /tmp limite les risques d'exécution de scripts malveillants, renforçant ainsi la sécurité du système.

10. **Restriction des Droits sur les Fichiers Sensibles :**

    - Limiter les droits sur les fichiers sensibles garantit que seuls les utilisateurs autorisés peuvent accéder et modifier ces fichiers, renforçant ainsi la confidentialité et l'intégrité des données.

11. **Installation de fail2ban :**

    - fail2ban est un outil de prévention des intrusions qui protège le système en détectant et en bloquant les adresses IP suspectes. Son installation renforce la sécurité du système contre les attaques par force brute.

12. **Chiffrement du Disque avec LVM :**

    - Le chiffrement du disque avec LVM (Logical Volume Manager) contribue à protéger les données sensibles en cas de perte ou de vol du matériel. Cela renforce la confidentialité des informations stockées sur le disque.

Remarque Importante

Assurez-vous d'avoir une sauvegarde avant d'appliquer des changements, car certaines modifications peuvent affecter le comportement du système