PROTEGO MAXIMA— N°4

**Prompt :**

Nous sommes en travail de groupe et devons réaliser plusieurs missions en rapport avec l'IA, chaque groupe de la classe est concurrent les uns des autres, la mission sur laquelle je travaille actuellement est la défense de nos données de travail, voici l'intitulé :

"La défense aux intrusions sera également récompensée, TOUS les coups sont permis pour la défense !

Nous avons déjà réfléchi aux différentes défenses possibles et les défenses les plus ingénieuses marqueront plus de points !

Une documentation de chaque action vous sera demandée et devra être apporter au conseil des ministres afin qu’il vous attribue le nombre de points mérités."

Nous stockons nos données dans un google drive et communiquons certaines informations dans discord tel que le lien du google drive, des images et vidéos générées par IA, etc. Les groupes sont dans la même salle donc il faut également sécuriser les PC en cas d'absence, lors des pauses notamment.

Élabore toutes les actions de défense et réalise la documentation demandée.

# 1. Sécurisation des accès numériques

## 1.1 Google Drive

- Activation de la double authentification sur tous les comptes.  
- Suppression des accès publics et restriction aux adresses vérifiées.  
- Renommage neutre des liens.  
- Mot de passe et chiffrement des fichiers critiques.

## 1.2 Discord

- Suppression ou modification des messages contenant des liens sensibles.  
- Utilisation de canaux privés avec permissions restreintes.  
- Double authentification activée.  
- Nommage non reconnaissable des fichiers sensibles.

# 2. Sécurisation physique

## 2.1 Postes informatiques

- Verrouillage systématique des sessions (Windows+L).  
- Mot de passe fort et désactivation de l'autologin.  
- Gestionnaire de mots de passe sécurisé.  
- Aucun périphériques USB

# 3. Chiffrement et brouillage

## 3.1 Chiffrement des données sensibles

- Archivage chiffré des fichiers critiques (mot de passe fort).  
- Gestion sécurisée des clés de chiffrement.

## 3.2 Appâts et fausses pistes

- Création de dossiers factices pour détecter les intrusions.  
- Nommage banal des vrais dossiers.  
- Surveillance de l'historique d'accès Drive.

# 4. Hygiène opérationnelle

## 4.1 Gestion des comptes

- Compte central unique pour le Drive.  
- Révocation immédiate des accès en cas de besoin.  
- Rotation régulière des mots de passe.

## 4.2 Comportement en salle

- Silence sur les stratégies.  
- Briefings discrets.  
- Gardiens de poste en rotation.

# 5. Défenses actives

- Script d’alerte Drive pour détection d’accès inconnus.  
- Faux Drive pour repérer les tentatives de vol.  
- Surveillance manuelle des logs.  
- Mots de passe intégrés dans les noms de fichiers.

# 6. Plan documentaire

1. Présentation de l’architecture de sécurité  
2. Liste des comptes autorisés  
3. Captures de configuration Drive et Discord  
4. Procédure de chiffrement  
5. Photos et preuves de sécurisation physique  
6. Journal de surveillance et rotation interne  
7. Description des appâts et défenses actives  
8. Tableau de responsabilités

# 7. Résultat attendu

- Accès extérieur quasi impossible.  
- Données illisibles si volées.  
- Détection rapide de toute tentative d’intrusion.  
- Preuves solides pour attribution des points.  
- Points bonus pour ingéniosité.