RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

MediaSchool
Campus Strasbourg

IRIS

PROJET GSB

EQUIPEMENT NOMADE SÉCURISÉ

RÉALISÉ PAR :

SOULAIMAN RAYANE
JEREMIE-CEPHAS SEGBEAME
FERDINAND NKONE
ALI MIRNAMI
VALENTIN MISTRAL
AMIR TAJIK HEULIN

NOVEMBRE 2025

SOMMAIRE

NOVEMBRE 2025

CONTEXTE ET ENJEUX DE GSB

01

CONTEXTE ET ENJEUX DE GSB

GSB

entreprise de distribution de matériel médical

100 postes nomades utilisés par les visiteurs médicaux

Manque d’inventaire et procédures non standardisées

Incidents fréquents : perte, vol, fuite de données

Enjeux : performance, confidentialité, RGPD

01

CONTEXTE ET ENJEUX DE GSB

GSB

CONSÉQUENCE :

✓ risque financier

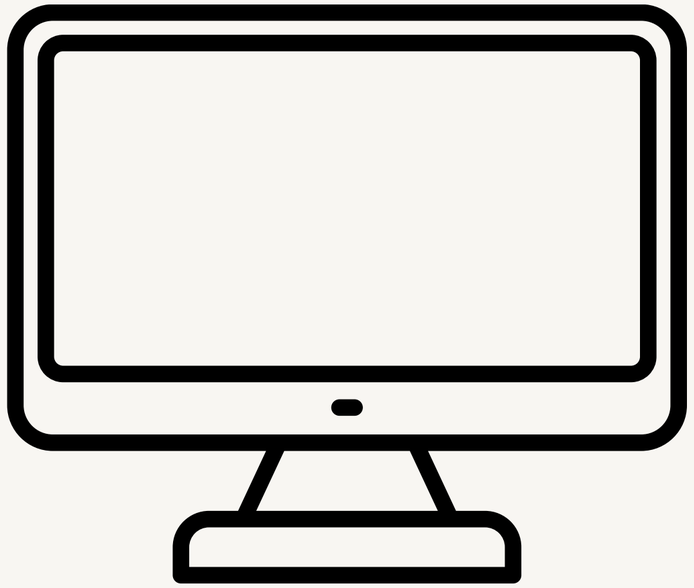
✓ atteinte à l'image

✓ perte de compétitivité

PROBLÈMES IDENTIFIÉS DANS L’EXISTANT

02

PROBLÈMES IDENTIFIÉS DANS L'EXISTANT



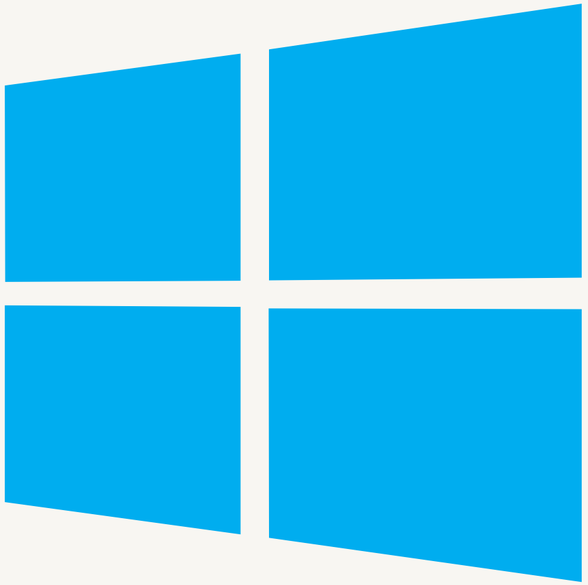
MATÉRIEL

✓ Aucune sécurité physique

✓ Matériel perdu ou volé sans protection

02

PROBLÈMES IDENTIFIÉS DANS L'EXISTANT

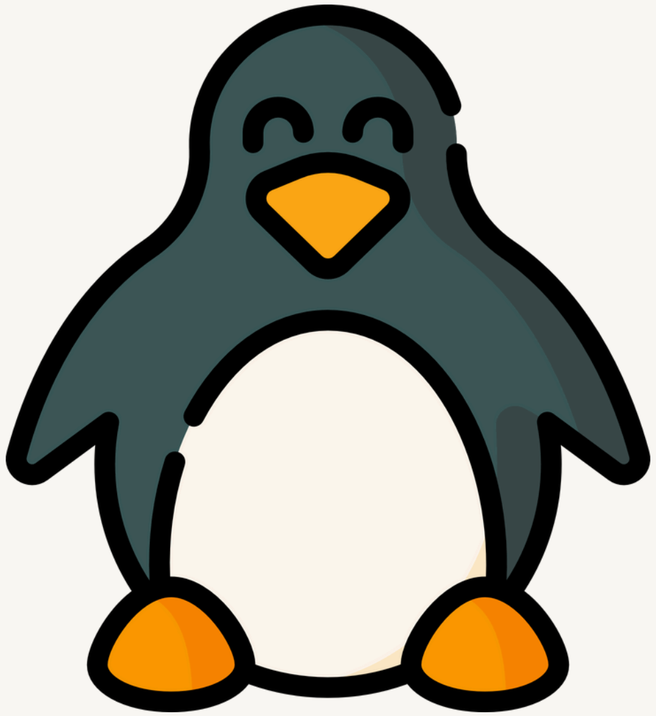


WINDOWS

- FAILLES : SMBV1, NTLMV1, AUTORUN, ABSENCE D'AUDIT
- APPLICATIONS INUTILES INSTALLÉES
- DÉFENDER MAL CONFIGURÉ

02

PROBLÈMES IDENTIFIÉS DANS L'EXISTANT

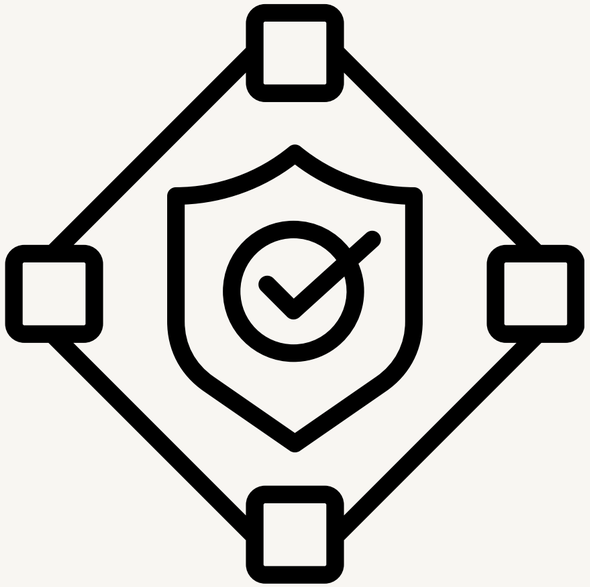


LINUX

- SERVICES INUTILES ACTIFS
- SSH NON SÉCURISÉ
- PAS DE FIREWALL CONFIGURÉ

02

PROBLÈMES IDENTIFIÉS DANS L'EXISTANT



ORGANISATION

- AUCUNE STRATÉGIE DE SÉCURITÉ LOCALE
- TRAVAIL COLLABORATIF VIA SERVICES NON SÛRS (DROPBOX, GDRIVE)

OBJECTIFS DU PROJET

03

OBJECTIFS DU PROJET

- RENFORCER LA SÉCURITÉ PHYSIQUE
- STANDARDISER LES CONFIGURATIONS WINDOWS & LINUX
- DURCIR LES SYSTÈMES D’EXPLOITATION (HARDENING)
- AUTOMATISER SOUS WINDOWS (POWERSHELL OBLIGATOIRE)
- DOCUMENTER ENTIÈREMENT LES PROCÉDURES
- RESPECT STRICT DU RGPD ET DES RECOMMANDATIONS ANSSI

EXIGENCES DU CAHIER DES CHARGES

04

EXIGENCES DU CAHIER DES CHARGES

CONTRAINTES TECHNIQUES

- OS UTILISÉS : WINDOWS 10 ENTREPRISE & LINUX MINT CINNAMON
- SCRIPT POWERSHELL D'AUTOMATISATION (INSTALLATION, DURCISSEMENT)
- POLITIQUE STRICTE DE MOT DE PASSE :
  - 12 CARACTÈRES
  - EXPIRATION : 90 JOURS
  - VERROUILLAGE À 3 TENTATIVES (30 MIN)

SÉCURITÉ PHYSIQUE DES ÉQUIPEMENTS

05

SÉCURITÉ PHYSIQUE DES ÉQUIPEMENTS

PROTECTION DU MATÉRIEL

- Verrou Kensington pour chaque laptop
- Étiquetage / Code QR pour l'inventaire
- Enregistrement dans GLPI (ou équivalent)

PRÉVENTION DU VOL

- Activation du chiffrement disque :
  - BitLocker (Windows)
  - LUKS (Linux Mint)

05

SÉCURITÉ PHYSIQUE DES ÉQUIPEMENTS

DURCISSEMENT DU BIOS / UEFI

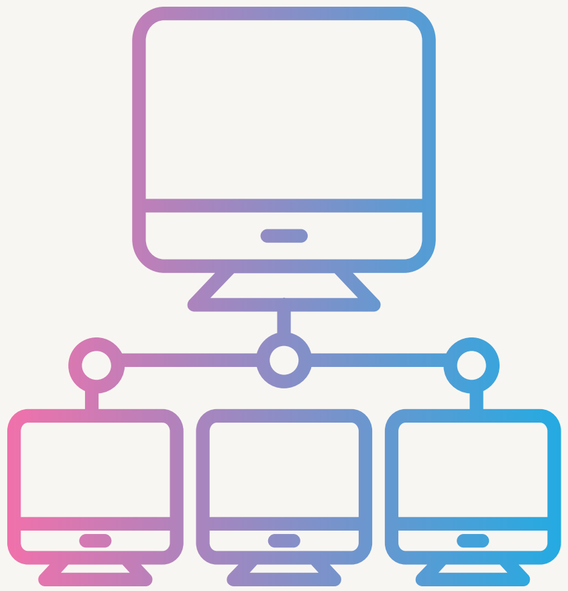
- MOT DE PASSE BIOS
- DÉSACTIVATION DU BOOT USB / CD
- SECURE BOOT ACTIVÉ
- TPM ACTIVÉ POUR BITLOCKER

PROCÉDURE EN CAS DE VOL

- DÉCLARATION + DÉSACTIVATION COMPTE AD
- ROTATION DES MOTS DE PASSE SENSIBLES
- ANALYSE DES DONNÉES SYNCHRONISÉES

ARCHITECTURE DE SÉCURISATION WINDOWS

06 ARCHITECTURE DE SÉCURISATION WINDOWS



MODULES APPLIQUÉS :
Hardening Réseau
Hardening Authentification
Windows Defender & Exploit Guard
GPO locales
Audit avancé
Script PowerShell d’automatisation

Objectif : créer un poste Windows entièrement sécurisé dès l’installation

HARDENING WINDOWS (RÉSEAU, AUTHENTIFICATION, SYSTÈME)

07

HARDENING WINDOWS (RÉSEAU, AUTHENTIFICATION, SYSTÈME)

SÉCURITÉ RÉSEAU

Paramètres activés

- Désactivation SMBv1 (faille WannaCry)
- Désactivation NTLMv1
- Désactivation des requêtes DNS parallèles
- Désactivation mDNS
- Activation stricte de l'UAC

Résultat

- Réduction de la surface d'attaque réseau
- Protection contre les attaques latérales

07

HARDENING WINDOWS (RÉSEAU, AUTHENTIFICATION, SYSTÈME)

AUTHENTIFICATION ET MOTS DE PASSE STRATÉGIE APPLIQUÉE

- Mot de passe ⩾ 12 caractères
- Complexité obligatoire
- Expiration 90 jours
- Historique : 10 mots de passe
- Verrouillage compte : 3 échecs → blocage 30 minutes

SÉCURISATION KERBEROS

- Restriction des protocoles faibles
- Chiffrement AES obligatoire

07

HARDENING WINDOWS (RÉSEAU, AUTHENTIFICATION, SYSTÈME)

WINDOWS : DURCISSEMENT AVANCÉ

ACTIONS MAJEURES

- Désactivation AutoRun
- Désactivation PowerShell V2
- Désinstallation applications inutiles (bloatware)
- Activation SmartScreen
- Renforcement LSA / LSASS
- Signature SMB obligatoire
- Activation des protections cloud Defender

AUDIT

- Logs agrandis (Security, PowerShell, System)
- Journalisation commande → ProcessCreation

SCRIPT POWERSHELL (AUTOMATISATION)

08 SCRIPT POWERSHELL (AUTOMATISATION)

Objectifs du script

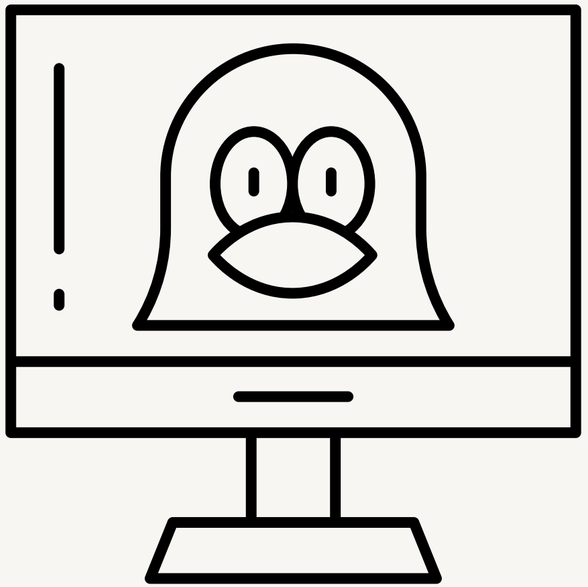
- Appliquer 100% du hardening automatiquement
- Désinstaller les applications inutiles
- Activer Defender + Exploit Guard
- Désactiver SMBv1 / NTLMv1
- Configurer Windows Update
- Appliquer les stratégies de sécurité locales

08 SCRIPT POWERSHELL (AUTOMATISATION)

ARCHITECTURE DE SÉCURISATION LINUX

09

ARCHITECTURE DE SÉCURISATION LINUX

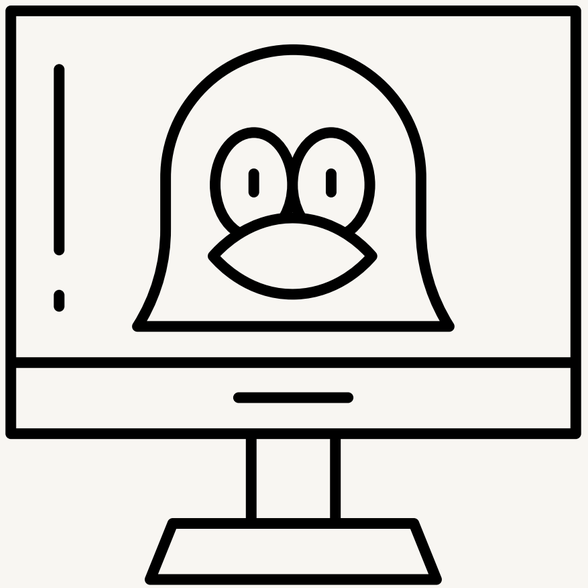


Composants déployés

- UFW (pare-feu)
- SSH sécurisé par clés
- fail2ban
- ClamAV
- auditd
- Désactivation services non essentiels
- Chiffrement LUKS

09

ARCHITECTURE DE SÉCURISATION LINUX



Sécurisation réseau

UFW configuré

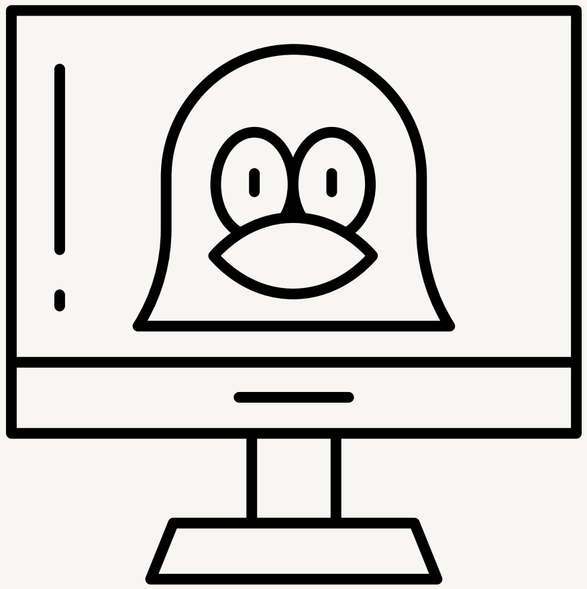
- Default : deny incoming / allow outgoing
- SSH autorisé sur port 22 uniquement
- Logs activés

IPTABLES

- DROP par défaut
- Protection contre ping flood
- Blocage ports inutilisés

09

ARCHITECTURE DE SÉCURISATION LINUX



Sécurisation système

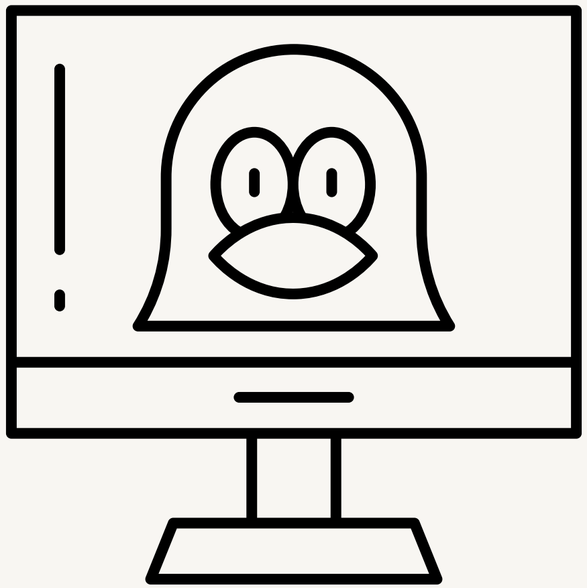
Actions

- Désactivation services inutiles (cups, bluetooth...)
- Interdiction de connexion SSH root
- Authentification par clé uniquement
- Désactivation exécution dans /tmp
- Droits stricts : /var/log, /etc/ssh/*

Résultat

- Surface d’attaque réduite
- SSH durci
- Résistance accrue aux scripts malveillants

09 ARCHITECTURE DE SÉCURISATION LINUX



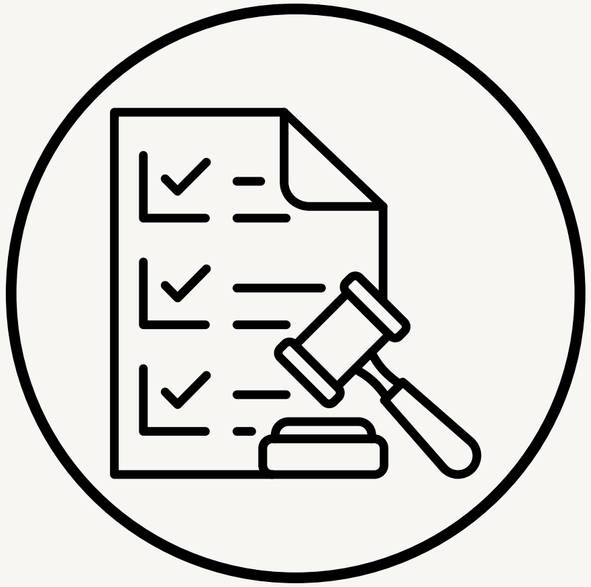
Audit & Protection

- Lynis : audit complet du système
- ClamAV : scan périodique
- auditd : journalisation des accès
- fail2ban : blocage IP brute-force SSH

CONFORMITÉ RGPD & RECOMMANDATIONS ANSSI

10

CONFORMITÉ RGPD & RECOMMANDATIONS ANSSI



Mesures mises en place

- Chiffrement systématique
- Authentification forte
- Journalisation des accès
- Traçabilité complète
- Sécurisation des données locales
- Limitation des risques de fuite

CONCLUSION

11 CONCLUSION

OBJECTIFS ATTEINTS :

Sécurisation de Windows 10 & Linux Mint
Automatisation via PowerShell
Standardisation de la flotte
Documentation exhaustive
Maquette fonctionnelle prête à déployer

MAQUETTE TECHNIQUE & DÉMONSTRATION PRÉVUE

MERCI POUR VOTRE ATTENTION