

TIP 2.10

Protéger un poste : mises à jour, antivirus et pare-feu

Fiche de révision - Équipements numériques

1. Les protections essentielles

Protection	Rôle
Mises à jour	Corrigent notamment des vulnérabilités et des bugs.
Antivirus / anti-malware	Détecte et neutralise des logiciels malveillants.
Pare-feu	Contrôle les communications réseau selon des règles.
Paramètres de sécurité	Réduisent l'exposition et encadrent le comportement du poste.

Méthode à retenir :
Mettre à jour → Protéger → Contrôler → Tester → Corriger → Valider

2. Menace, vulnérabilité, correctif

Notion	Définition
Menace	Élément susceptible de provoquer un incident : malware, attaquant, phishing, etc.
Vulnérabilité	Faiblesse qui peut être exploitée.
Correctif	Modification publiée pour corriger un problème ou une vulnérabilité.

3. Windows Update et applications

Vérifier les mises à jour disponibles, les erreurs éventuelles et les redémarrages requis. En entreprise, les mises à jour peuvent être pilotées centralement : ne pas contourner la politique parce qu'une option est grisée ou qu'une version plus récente existe.

À maintenir	Exemples
Système	Windows et composants associés.
Applications	Navigateurs, lecteur PDF, bureautique, visioconférence, runtimes.
Logiciels métiers	Uniquement selon la version validée par l'organisation.

4. Microsoft Defender : commandes utiles

Commande	Utilité
Get-MpComputerStatus	Affiche l'état de plusieurs fonctions Defender.
Update-MpSignature	Demande la mise à jour des renseignements de sécurité.
Start-MpScan -ScanType QuickScan	Lance une analyse rapide.
Start-MpScan -ScanType FullScan	Lance une analyse complète, plus longue et plus coûteuse en ressources.

5. Protection en temps réel et détection

La protection en temps réel surveille l'activité du poste. En cas de détection, un élément peut être bloqué, mis en quarantaine ou remonté à une console centralisée. Ne jamais restaurer ou exclure immédiatement un fichier uniquement parce que l'utilisateur en a besoin.

Faux positif : si un fichier légitime semble bloqué à tort, vérifier sa provenance, sa signature, son hash et suivre la procédure interne avant toute exclusion.

6. Pare-feu Windows

Le pare-feu contrôle les communications réseau selon des règles. Même lorsqu'un pare-feu réseau existe, la protection locale du poste reste utile, notamment sur les portables qui peuvent être utilisés en dehors du réseau interne.

Profil	Contexte général
Domaine	Poste connecté à un réseau correspondant à son domaine Active Directory.
Privé	Réseau considéré comme privé selon la configuration Windows.
Public	Réseau non approuvé ; profil généralement plus restrictif.

7. Commandes pare-feu

Commande	Utilité
Get-NetFirewallProfile	Affiche l'état des profils Domaine, Privé et Public.
Get-NetFirewallRule	Affiche les règles du pare-feu.
Test-NetConnection serveur -Port 443	Teste la connectivité vers un service avant de conclure à un problème de pare-feu.

8. Ne pas désactiver pour dépanner

Si une application ne communique plus, ne pas désactiver durablement le pare-feu ou l'antivirus. Identifier d'abord le programme, la destination, le protocole, le port et le profil réseau réellement nécessaires, puis appliquer uniquement une règle ou une exception validée.

9. Checklist avant livraison

Contrôle	État attendu
Windows Update	État conforme et redémarrages terminés.
Applications	Versions conformes à la politique.
Antivirus	Actif et sans menace non traitée.
Temps réel	Protection active selon la politique.
Renseignements sécurité	Récents / à jour.
Pare-feu	Profils actifs conformément à la politique.
Exceptions	Aucune exclusion non justifiée.
Gestion centralisée	Agent enregistré si l'organisation l'utilise.

10. À retenir

Ne jamais désactiver une protection simplement pour contourner un problème.
Mettre à jour le système et les applications, vérifier l'état de l'antivirus, contrôler la protection en temps réel, valider les profils pare-feu et tester la connectivité avant toute modification.