

Sauvegarde des données – Mise en place de FreeFileSync

1 Contexte et constat d'audit

Lors de l'audit du patrimoine informatique, il a été constaté que la protection des données reposait exclusivement sur Microsoft OneDrive (abonnement Microsoft 365 Famille). Cette solution assure une synchronisation et une réplication cloud, mais ne constitue pas une stratégie de sauvegarde au sens des bonnes pratiques (ANSSI, règle 3-2-1).

Le point critique est que le dossier local C:\Users\crech\OneDrive et sa réplique cloud ne sont pas deux copies indépendantes : il s'agit de la même donnée synchronisée. Toute suppression accidentelle, tout chiffrement par rançongiciel ou toute compromission du compte Microsoft se propage automatiquement aux deux emplacements. La structure ne disposait donc, en réalité, que d'une seule copie résiliente — c'est-à-dire aucune.

Une copie de sauvegarde indépendante et déconnectable a donc été déployée pour rompre cette chaîne de propagation.

2 Objectifs de la mise en œuvre

- Disposer d'une copie locale indépendante des données, isolée de la synchronisation OneDrive.
- Introduire une rupture physique (support déconnectable) protégeant contre les rançongiciels.
- Conserver l'historique des fichiers modifiés ou supprimés (restauration ponctuelle).
- Fournir un outil simple, exploitable par un personnel non technique en cas de changement de poste.

3 Support de sauvegarde retenu

Support : SSD externe Samsung T7 Shield, dédié à la sauvegarde.

Caractéristique	Choix retenu	Justification
Chiffrement	AES-256 (Samsung Magician)	Confidentialité en cas de vol ou de perte du support
Système de fichiers	NTFS	Compatibilité Windows, pas de limite de taille de fichier
Libellé / lettre	SAUVEGARDE-CRECHE / lettre D: fixe	Fiabilise l'exécution de la tâche planifiée
Disponibilité	Déconnecté 6 jours sur 7	Air gap : un rançongiciel ne peut chiffrer un support non connecté

Le SSD est privilégié face à une clé USB pour sa fiabilité (résistance aux chocs) et sa rapidité.

4 Configuration de FreeFileSync

Le logiciel libre FreeFileSync a été installé sur le poste administratif. La tâche est enregistrée en .ffs_batch et exécutable sans intervention technique.

Paramètre	Valeur	Justification technique
Source	C:\Users\crech\OneDrive	Fichiers forcés « toujours disponibles sur cet appareil » pour éviter de ne sauvegarder que des espaces réservés (0 octet)
Cible	D:\Sauvegarde\Sauvegarde_OneDrive	SSD externe chiffré
Variante	Update (et non Mirror)	Mirror supprimerait sur la cible tout fichier absent de la source : une suppression ou un chiffrement se propagerait. Update ajoute et met à jour sans supprimer
Versioning	D:_Versions	Conserve les versions antérieures écrasées ou supprimées → retour arrière possible après incident
Journalisation	D:_Logs	Traçabilité et détection des échecs
Filtres	Exclusions configurées	Écarte les fichiers temporaires et système inutiles

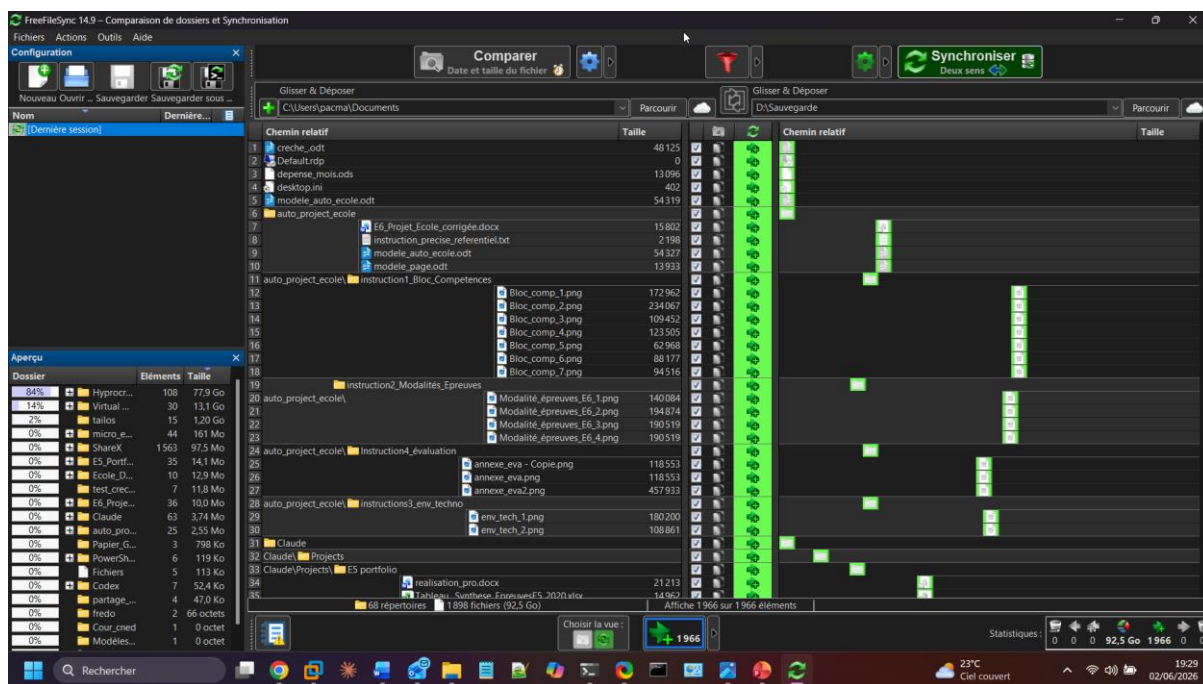
Le choix combiné Update + Versioning est central : il garantit qu'une donnée saine n'est jamais écrasée par une donnée corrompue, ce que le simple OneDrive ne permet pas dans la limite de son historique.

5 procédure utilisateur

La sauvegarde est exécutée manuellement **vendredi à 17 h 00**, avec 3 tentatives en cas d'échec.

Le SSD étant déconnecté 6 jours sur 7, la procédure imposée à l'utilisateur est la suivante :

1. Connecter le SSD SAUVEGARDE-CRECHE si possible le vendredi, avant 17 h 00.
2. Effectuer la guide laissé dans le PC au format word pour effectuer la sauvegarde de manière propre



Une procédure imprimée a été également remise à la directrice afin d'assurer la continuité du service en cas de changement de personnel.

6 Tests et validation

Test	Procédure	Résultat attendu
Sauvegarde initiale	Première exécution complète	Arborescence copiée sur D:, journal sans erreur
Versioning	Modification d'un fichier puis nouvelle exécution	Version précédente conservée dans D:_Versions
Restauration	Suppression volontaire d'un fichier test, puis restauration depuis le SSD	Fichier récupéré à l'identique
Échec planifié	Lancement de la tâche SSD débranché	Échec journalisé, 3 tentatives, alerte à vérifier

Le test de restauration est réalisé et documenté : une sauvegarde non testée ne peut être considérée comme valide.

7. Analyse de risque

Avant intervention : une seule donnée résiliente (OneDrive local + cloud = même fichier synchronisé) ; aucune copie indépendante ; propagation directe d'une suppression ou d'un chiffrement.

Après intervention : trois copies sur deux types de supports, dont une déconnectable → conformité à la règle 3-2-1 ; rupture de propagation par air gap ; historique de versions ; restauration locale rapide.

	Avant	Après
Niveau de risque	Moyen à élevé	Faible à moyen (sous réserve du respect des procédures et d'un test de restauration périodique)

8. Recommandations complémentaires

- Effectuer la sauvegarde au minimum une fois par semaine.
- Maintenir le SSD déconnecté hors période de sauvegarde.
- Réaliser si possible un test de restauration mensuel.
- Surveiller éventuellement les journaux D:_Logs afin de détecter les exécutions échouées (SSD oublié).