

DESCRIPTION D'UNE SITUATION PROFESSIONNELLE

PARCOURS	SISR <input checked="" type="checkbox"/>	SLAM <input type="checkbox"/>
----------	--	-------------------------------

Lieu de réalisation	CERFAL Campus Montsouris	
Période de réalisation	Du : 05/03/2024	Au : 05/03/2024
Modalité de réalisation	SEUL <input type="checkbox"/>	EN EQUIPE <input checked="" type="checkbox"/>

Intitulé de la mission	Création d'un agent de récupération pour le chiffrement EFS (Encrypting File System)
Description du contexte de la mission	Dans le cadre de la sécurisation des données stockées sur les postes utilisateurs sous Windows, j'ai été amené à mettre en place un agent de récupération EFS. L'objectif de cette mission était de comprendre le fonctionnement du chiffrement EFS

Contraintes & Résultat	<p>Ressources fournies / contraintes techniques / Résultats attendu</p> <p>Contraintes :</p> <ul style="list-style-type: none"> • Utiliser les outils intégrés à Windows (MMC, GPO, certificats). • La récupération de fichiers chiffrés devait être testée et validée. <p>Résultat :</p> <ul style="list-style-type: none"> • Un certificat de récupération a été généré pour un compte administrateur. • La stratégie de groupe locale a été configurée pour enregistrer cet agent comme agent de récupération EFS. • Un test de chiffrement et de récupération de fichier a été effectué avec succès.
Productions associées	<p>Liste des documents produits et description</p> <ul style="list-style-type: none"> • Procédure de création agent



Description détaillée de la situation professionnelle retenue et des productions réalisées en mettant en évidence la démarche suivie, les méthodes et les techniques utilisées

Cette mission m'a permis de découvrir le fonctionnement d'EFS (Encrypting File System), le système de chiffrement de fichiers intégré à Windows. Elle s'est déroulée en plusieurs étapes logiques.

1. Compréhension d'EFS et de ses limites

Avant toute configuration, j'ai étudié le fonctionnement d'EFS :

- Chaque utilisateur chiffre ses fichiers avec une clé liée à son profil.
- Si le profil est supprimé ou corrompu, les fichiers deviennent illisibles.
C'est pour cela qu'il est essentiel de mettre en place un agent de récupération, capable de déchiffrer les fichiers en cas de problème.

2. Génération du certificat de récupération

J'ai lancé la console MMC (Microsoft Management Console) et ajouté le module Certificats pour le compte administrateur.

J'ai ensuite généré un certificat de récupération EFS auto-signé depuis la console et l'ai exporté au format .pfx pour usage ultérieur.

3. Configuration de l'agent de récupération

À l'aide de la console secpol.msc (ou des stratégies locales de sécurité), j'ai défini une stratégie de récupération EFS :

- J'ai importé le certificat précédemment généré pour l'associer à l'agent de récupération.
- Cette stratégie a été appliquée localement pour que le compte administrateur puisse déchiffrer les fichiers chiffrés par d'autres utilisateurs.

4. Tests de chiffrement et de récupération

Pour valider la configuration, j'ai :

- Crée un utilisateur test,
- Activé le chiffrement EFS sur un fichier à l'aide du clic droit > Propriétés > Avancé > Chiffrer le contenu,
- Supprimé l'accès de l'utilisateur test,
- Ouvert la session administrateur avec l'agent de récupération,
- Et réussi à récupérer et lire le fichier chiffré.