

# Rapport technique

## 1. Surveillance des fichiers

La surveillance des fichiers utilise des fonctions de parcours de fichiers fournies par le cmdlet `Get-ChildItem` :

- Le script demande à l'utilisateur de spécifier un chemin de dossiers ou fichiers à surveiller.
- Chaque fichier dans le dossier spécifié est parcouru de manière récursive (incluant les sous-dossiers).
- Les fichiers sont traités un par un, et des hashes sont calculés pour chacun d'eux.

## 2. Hashing des fichiers

Pour détecter les modifications apportées aux fichiers, le script utilise la fonction de hachage SHA-256, fournie par le cmdlet `Get-FileHash` de PowerShell :

- Lors de la première exécution du script, un hash SHA-256 est calculé pour chaque fichier spécifié. Ce hash est unique pour le contenu du fichier et est stocké dans un fichier JSON dans un dossier désigné (par défaut, `C:\hash_store`).
- Lors des vérifications ultérieures, les hashes des fichiers sont recalculés et comparés aux hashes précédemment enregistrés.
- Si un hash ne correspond pas, cela signifie que le fichier a été modifié.

## 3. Génération et stockage des hashes

Le stockage des hashes des fichiers surveillés est réalisé sous la forme d'un fichier JSON, ce qui permet une récupération facile et une compatibilité avec les fonctionnalités intégrées de PowerShell.

- **Structure des hashes** : Le fichier JSON est utilisé pour stocker chaque fichier surveillé et son hash correspondant dans un format clé-valeur, où la clé est le chemin du fichier et la valeur est le hash SHA-256.
- **Sauvegarde initiale** : Avant la première vérification, une sauvegarde initiale des hashes est effectuée pour établir une base de référence à partir de laquelle les changements peuvent être détectés.

## 4. Envoi d'alertes par e-mail

Pour alerter l'administrateur des modifications de fichiers, des créations ou des suppressions, le script utilise un mécanisme d'envoi d'e-mails basé sur le protocole SMTP.

- **Authentification SMTP** : Le script utilise un serveur SMTP de Gmail (`smtp.gmail.com`) pour envoyer les e-mails. Il est nécessaire de configurer un mot de

mot de passe d'application spécifique dans les paramètres de sécurité du compte Google pour permettre au script de s'authentifier et d'envoyer des e-mails de manière sécurisée.

- **Configuration personnalisée** : L'utilisateur doit entrer son adresse Gmail, le mot de passe d'application et les adresses e-mail de destination pour les alertes.
- **Fonction d'envoi** : Une fonction `Send-EmailAlert` est utilisée pour envoyer les alertes, en incluant des informations détaillées sur le type d'alerte (modification, création, suppression) et le fichier concerné.