Réf : PROT-SEC-005
Cible : Data-at-Rest / Protection des Scellés Numériques
Statut : OPÉRATIONNEL

FICHE RESSOURCE : PROTOCOLE_VERACRYPT (V1.0)

Un mot de passe de session Windows, c'est une blague pour n'importe quel analyste Forensics. Si tu ne chiffres pas tes volumes de travail, tu ne protèges pas tes preuves, tu les laisses à l'abandon. VeraCrypt, c'est ton coffre-fort en titane. Si tu perds la clé, même moi je ne peux rien pour toi.

01. LA CRÉATION DU CONTENEUR (LE LEURRE)

- **Concept** : Créer un fichier "conteneur" qui ressemble à une archive banale (`.iso`, `.sys` ou `.dat`) mais qui abrite un disque virtuel chiffré.
- **L'astuce de la Sentinelle** : Ne l'appelle pas 'Preuves_Cyber'. Appelle-le `system_backup_win10.dat` et planque-le dans un dossier système. La première règle de la sécurité, c'est la discrétion.

02. L'ALGORITHME DE CHIFFREMENT

- **Standard :** AES (256 bits) est le plus rapide.
- **Paranoïa (Recommandé) :** Utilise le mode cascade `AES(Twofish(Serpent))`. C'est trois couches de chiffrement différentes. Si une faille est découverte sur l'un, les deux autres tiennent toujours la porte.

03. LA PASSPHRASE (LA CLÉ DE VOÛTE)

Pas de date de naissance, pas de nom de chien. Utilise une phrase de 5 à 6 mots aléatoires. VeraCrypt utilise des itérations de hachage (PIM) qui rendent l'attaque par brute-force pratiquement impossible sur une phrase longue.

04. LE VOLUME CACHÉ (DENI PLOTABLE)

- **La technique :** Créer un volume dans le volume.
- **Scénario de terrain :** Si on te force à donner ton mot de passe sous la contrainte, tu donnes celui du volume extérieur. Dedans, tu mets des fichiers sans importance. Le vrai dossier d'enquête, celui qui contient les scellés, reste mathématiquement invisible dans la partition cachée.

[ALERTE_SÉCURITÉ]

Attention : VeraCrypt n'est utile que si ta machine est 'propre'. Si tu as un keylogger sur ton OS hôte, ton mot de passe est déjà compromis. C'est pour ça qu'on utilise toujours VeraCrypt **à l'intérieur** d'une VM isolée ou sur un Tails OS.