ORADAD et Purple knight

ORADAD

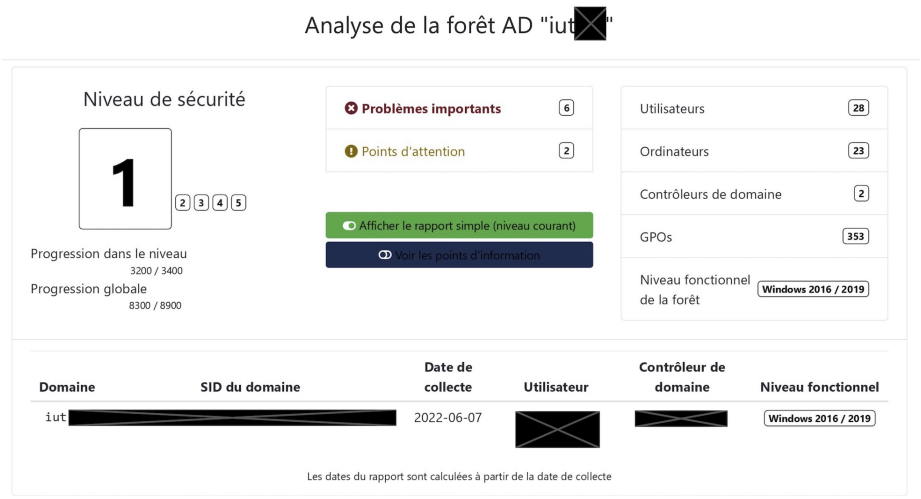
Concept : outil de Récupération Automatique des Données de l'Active Directory

- Utilitaire mis en place par l'ANSSI
- Réservé OIV et OSE
- Demande d'accès à club@ssi.gouv.fr

Utilisation

- https://github.com/ANSSI-FR/ORADAD/releases
- Execution sur une machine du domaine avec un compte sans privilège
- Téléversement sur https://club.ssi.gouv.fr
- Reception d'une archive au format zed
  - https://www.primx.eu/fr/zed-free/
- Mot de passe par sms

Recueil de points de contrôle Travail avec ces points de contrôle depuis ce lien Points de contrôles ANSSI



Niveau	Avancement	Titre (afficher / masquer tout)	
1		Comptes privilégiés dont le mot de passe n'expire jamais	CSV
1		Relations d'approbation sortante de type domaine non filtré	
1		Comptes ayant la propriété adminCount	CSV
1		Compte intégré administrateur du domaine utilisé il y a moins de 30 jours	
2		Comptes dont le mot de passe n'expire jamais	CSV
3		Comptes privilégiés non membres du groupe Protected Users	
4		Algorithmes de chiffrement supportés par les DC/RODC	