RESINFO - Groupe de travail **SWMB**

Gabriel Moreau - Coordinateur

20-22 octobre 2026 / Sète

Resinfo.org



SWMB (Secure Windows Mode Batch)

- Comité de pilotage : Gabriel Moreau, Olivier de Marchi (LEGI), Philippe Hortolland (LP2N)
- Besoin de sécuriser Microsoft Windows **11**
- Outil **modulaire** avec des **règles** et des **anté-règles**
- Outil en **production** sur le LEGI et déployé *a minima* sur quelques sites
- Règle particulière pour chiffrer les disques
- Packaging `setup.exe`, OCS, WAPT, PDQ Deploy
- **Kit SWLN** pour déployer une version adaptée de SWMB à son site
  SWLN - Secure Windows Local Network
- 47 personnes sur la liste swmb-gt du GT (**+3**)

Actions réalisées ou projetées

- ~~Communiquer régulièrement sur la liste ASR~~ (en sommeil cette année)
- Fiabilisation du kit SWLN
- Meilleure prise en charge de Windows 11 - (en pratique, les fonctionalités étaient déjà souvent actives dans Windows 10 !)
- Ajout de nombreux tweaks et mise à jour de l'interface graphique
- Amélioration de la qualité du logiciel

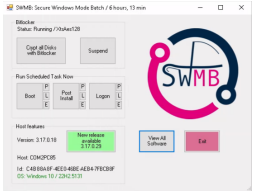
- Intégration de **53 recommandations du STIG Windows 11** (DoD)
  258 recommandations dont 28 de niveau high
- Création du kit **SWCE** autonome pour faire de l'audit régulier des GPO actives
  SWCE - Secure Windows Compliance Enforcement

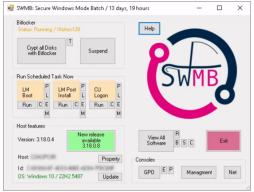
- Une **présentation au JRES (Tours)** de 15 min en décembre 2026 :
  SWCE : Tester la conformité des GPO sur son parc machine Windows avec un outil SWMB

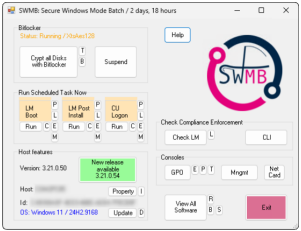
Projection pour 2027

- ↪ Interaction avec le GT Secure-IT et le sous groupe GPO du poste de travail (JoSy ?)
- ↪ Fabriquer (sous Linux) un installeur qui n'alerte pas les antivirus
  Quelle technologie utiliser ?
- ↪ Des sessions Discotech dans le pipe
- ↪ Communiquer mieux, encore et toujours









Licence

Merci à toutes les personnes et entités
nous ayant aidés ou ayant participé depuis le début

Cette présentation est sous : Licence Art Libre

http://artlibre.org/



