RESINFO - Groupe SWMB

Gabriel Moreau - Coordinateur

17-18 janvier 2023 / Visio

Resinfo

SWMB

Bilan depuis l'origine

Comité de pilotage

- Gabriel Moreau (LEGI / Grenoble)
- **Olivier de Marchi** (LEGI / Grenoble)
- Clément Deiber (DR11 / Grenoble) - co-animateur

SWMB (Secure Windows Mode Batch)

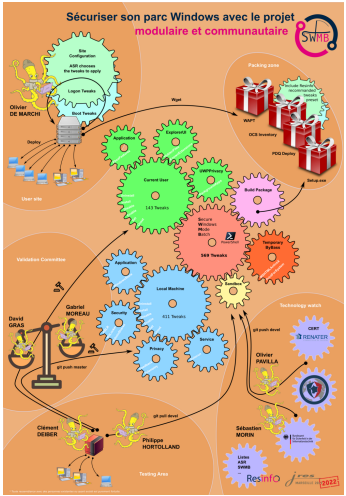
- Besoin de sécuriser Microsoft Windows 10
- Outil modulaire avec des règles et des anté-règles
- Outil en production sur le LEGI
- Règle particulière pour **supprimer Kaspersky** dans tous les cas (mot de passe Kaspersky et/ou Agent ou pas) $\Longrightarrow$ distribution spécifique de l'outil
- Règle particulière pour chiffrer les disques
- Packaging `setup.exe`, OCS, WAPT, PDQ Deploy
- 27 personnes sur la liste du GT

Actions 2022

- Plus de sites en production avec SWMB
- Plus de règles actives par défaut (574 règles au total) - ok
- Être plus réactif sur les alertes de sécurité (groupe plus élargi) - en cours
- Intégration du pare-feu Windows ?
- Ajout de règles Kaspersky / Windows Defender ? - suppression
- Une meilleure documentation pour utiliser et comprendre SWMB (voir article des JRES) - ok
- Finaliser le poster pour les JRES 2021 - ok
- Conférence à la journée sécurité de Min2rien (vidéo) à Lille (40 min) - non prévu
- Ajout de règles pour supprimer des logiciels qui n'ont rien à faire sur votre parc (comme OpenOffice, RealPlayer, WinRAR...)
- Ajout de règles sur la gestion de mot de passe et des groupes de sécurité en fin d'année

JRES 2021/22 Marseille

- 6 mois de travail collectif
- Visioconférence tous les 15 jours
- Poster
- Article de 30 pages
- Référence hal-03608835



Objectif 2023

- Améliorer les pages du GT sur le site RESINFO
- Plus communiquer sur la liste ASR
- Plus de sites en production avec SWMB
- Plus de règles actives par défaut
- Être plus réactif sur les alertes de sécurité (groupe plus élargi)
- Intégration du pare-feu Windows ?
- Monter des ateliers en visio de prise en main de l'outil

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/