RESINFO - Groupe SWMB

David Gras / Gabriel Moreau - Coordinateurs

8-10 décembre 2020 / Visio-conférence

Resinfo

Bilan depuis l'origine

Comité de pilotage

- David Gras (DR11 / Grenoble)
- Gabriel Moreau (LEGI / Grenoble)
- **Olivier de Marchi** (LEGI / Grenoble)
- Clément Deiber (DR11 / Grenoble)

SWMB (Secure Windows Mode Batch)

- Besoin de sécuriser Microsoft Windows 10
- Fiches ANSSI que chacun doit s'approprier et refaire
- Beaucoup d'unités sans AD (mais avec Windows en client...)
- Possibilité de capitaliser, de mutualiser au sein de l'ESR
- Paramétrage existant de GPO dans AD (DR11 par ex.)
- Des scripts déjà existants (LEGI par ex.)
- Une suite logique à l'ANF SIARSv2 concernant la partie Windows

Première maquette 2020

- Petit noyau dur pour réaliser une maquette fonctionnelle / preuve de concept
- Projet modulaire, lisible, simple, extensible basé sur un projet amont
- 500 règles à ce jour dont 50 RESINFO (enable / disable. . .)
- Prendre l'avis du COPIL RESINFO et du RSSI du CNRS avant d'élargir
- Élargissement du groupe - annonce sur la liste ASR en octobre
- 11 abonnés sur la liste de diffusion `swmb-gt`
- 21 réunions de travail hebdomadaire de 1h (mini)
- Pad de travail de 900 lignes + cloud + chat IN2P3 (`#resinfo-gt-ftto`)

Bilan 2020

- Un logo, une page web sur le site RESINFO !
- Étagère de scripts, bibliothèques de scripts, paquet OCS Inventory
- Documentation
- URL du projet `https://gitlab.in2p3.fr/resinfo-gt/swmb/resinfo-swmb`
- Travail en cours sur l'intégration de Bitlocker / TPM !

Projets 2021

- Paquet WAPT
- Plus de scripts : post-install, boot, daily...
- Des sites en production avec SWMB
- Une meilleure documentation pour utiliser et comprendre SWMB
- Intégration du pare-feu Windows
- Ajout de règles Kaspersky / Windows Defender ?
- Élargissement du groupe
- Une proposition pour les JRES 2021
- Contact avec l'ANSSI ?

- Un projet à l'écoute de ses nouveaux membres

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/