SECUREWAVE

Présentation OSSIR

Le défi de nouvelles plateformes

lundi 10 juin 2002

Marco Peretti
Benoit Fortemps

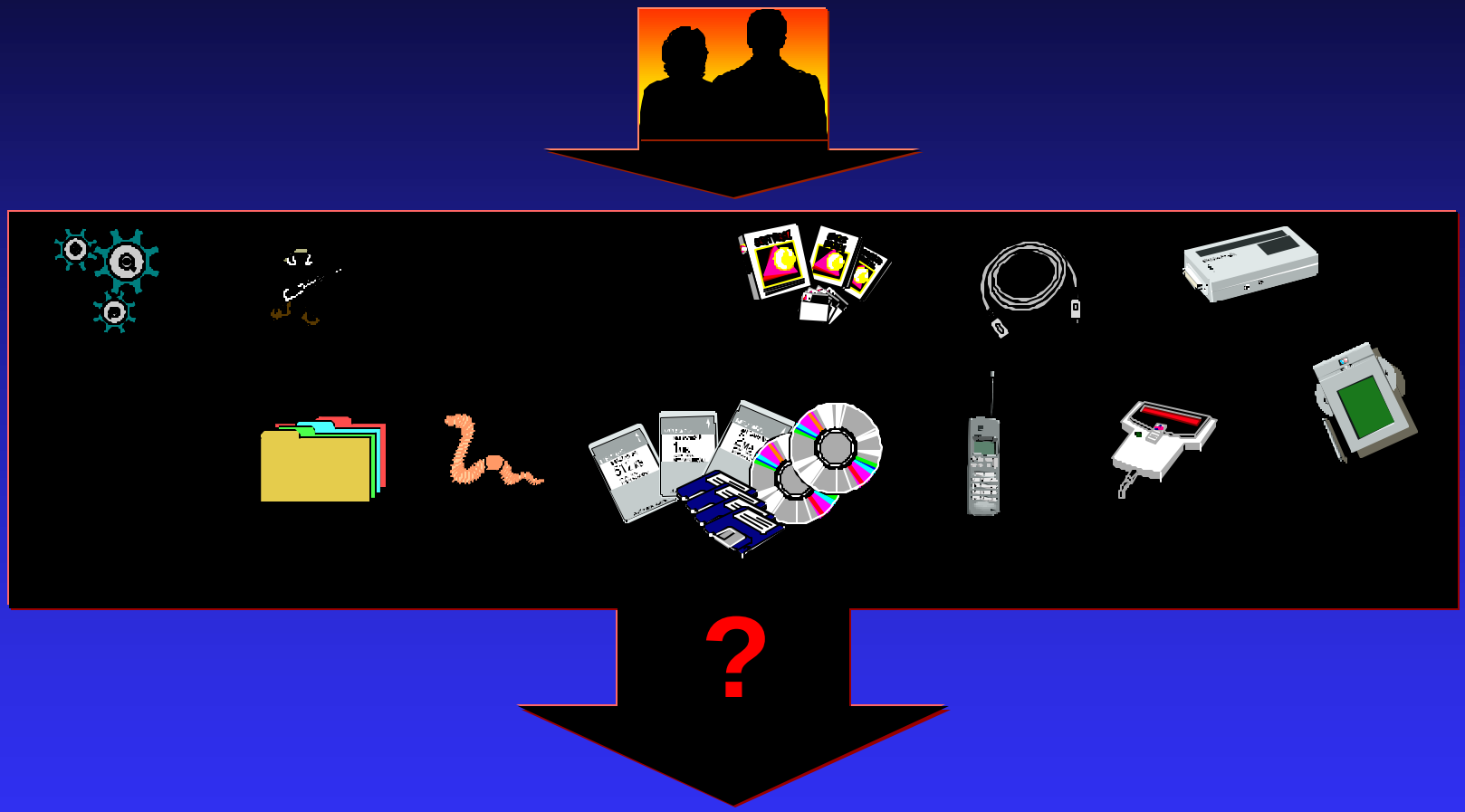
Agenda

- Présentation
- Introduction: la station de travail
- Plug and play
  - Problèmes + démo
  - Solutions classiques
  - SecureNT
- Exécutions abusives
  - Problèmes + démo
  - Solutions Classiques
  - SecureEXE
- Conclusions

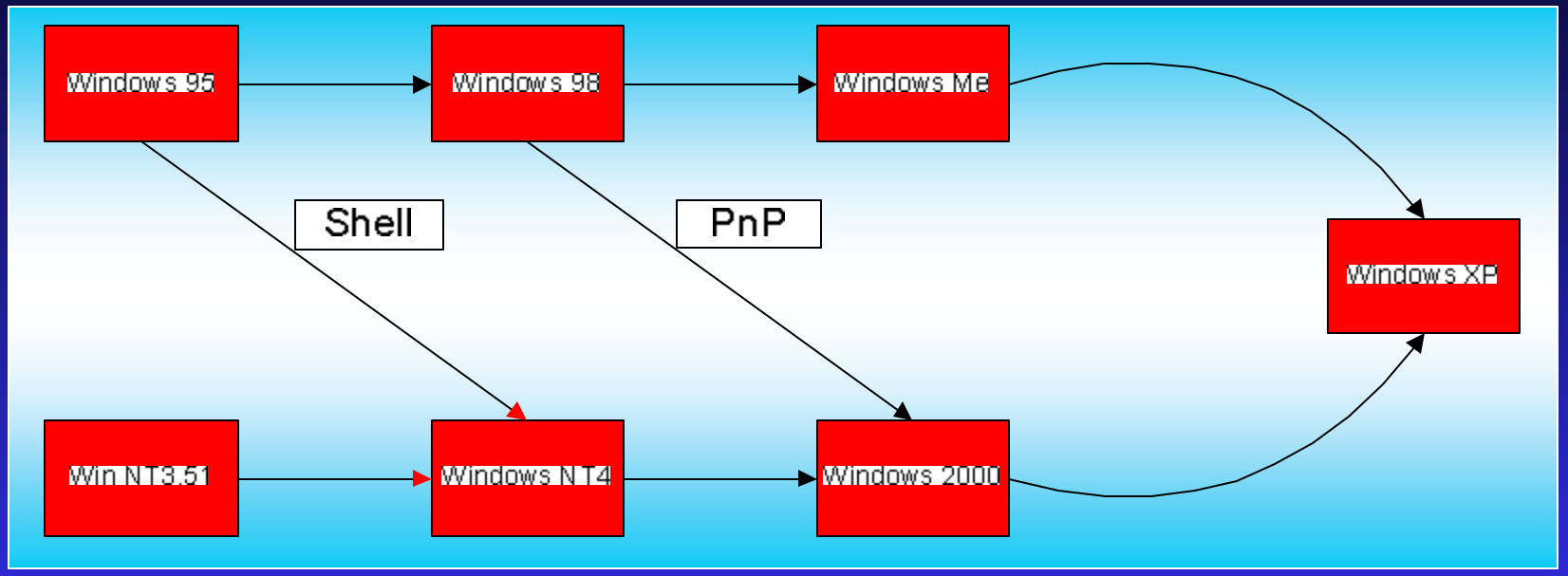
Présentation

- Solutions orientées vers la station de travail plutôt que le périmètre
- Prévention plutôt que détection
- Contrôle centralisé => Maîtrise TCO
- Basé sur le concept du moindre privilège (least privilege principle)

Le facteur humain



Evolution de la station de travail



- Plateformes tendent à se rassembler
- Shell Win 95 -> Windows NT4
- PnP Win 9x -> Windows 2000
- Nouvelles fonctionnalités => Nouveaux problèmes

=> Nouveaux défis

Plug And Play

Définition :
le *plug and play* a pour objectif de permettre à l'ordinateur de reconnaître et d'adapter les changements de configuration matériel avec peu ou pas d'intervention de l'utilisateur.

Historique:

- NT 4 : pas grand chose
- Win95 : Début
- Win 2k : ACPI: L'O.S. prend le contrôle

Risques:

- fuite de données sensibles
- introduction d'informations non autorisées
- introduction de logiciels ou virus

Les périphériques PnP

Bus : USB, IEEE1394, PCMCIA, LPT, etc.

- « Memory stick »
- Lecteur de disquettes
- Zip ou LS-120
- Disque dur externe ou amovible
- Graveur de CDROM
- PDA
- Modem
- Appareil photo numérique
- Etc.

www.sony.com

Pour tester chez vous

Description produit	Systèmes supportés	Prix
Compaq flash +Reader (16MB-1GB) http://www.sandisk.com/main.htm	Win2000 / XP	<50€
Diskgo (8-128MB) www.mydisgo.com	Win2000 / XP	<50€
Floppy USB http://www.lacie.com/	Win2000/XP	100€
Memory stick + reader (16MB-1GB) http://www.sandisk.com/main.htm	Win XP (natif)	<50€
Iomega ZIP http://www.iomega.com/	Win2000 / XP	85€

Solutions Classiques

- Stratégie de sécurité
- Retirer Physiquement les périphériques
- BIOS
- Clés Physiques
  1000 Machines = 1000 Clés ou clé Passe-partout
- Stratégie de groupes (cfr. suivant)
- Profils matériels
  Floppy.sys, cdrom.sys, etc
- Changement registry,
  - USB: HKLM\SYSTEM\CurrentControlSet\Services\usbhub
  - Firewire: HKLM\SYSTEM\CurrentControlSet\Services\Arp1394
- FlopLock
  Du kit des ressources techniques

GPO en détail

Les possibilités offertes:

- Turn off autoplay
- Allow to (format and) eject removable NTFS media
- Explorer: remove cd burning feature (2000 and xp)
- Hide drive from my computer
- Prevent access to drive from my computer (XP)

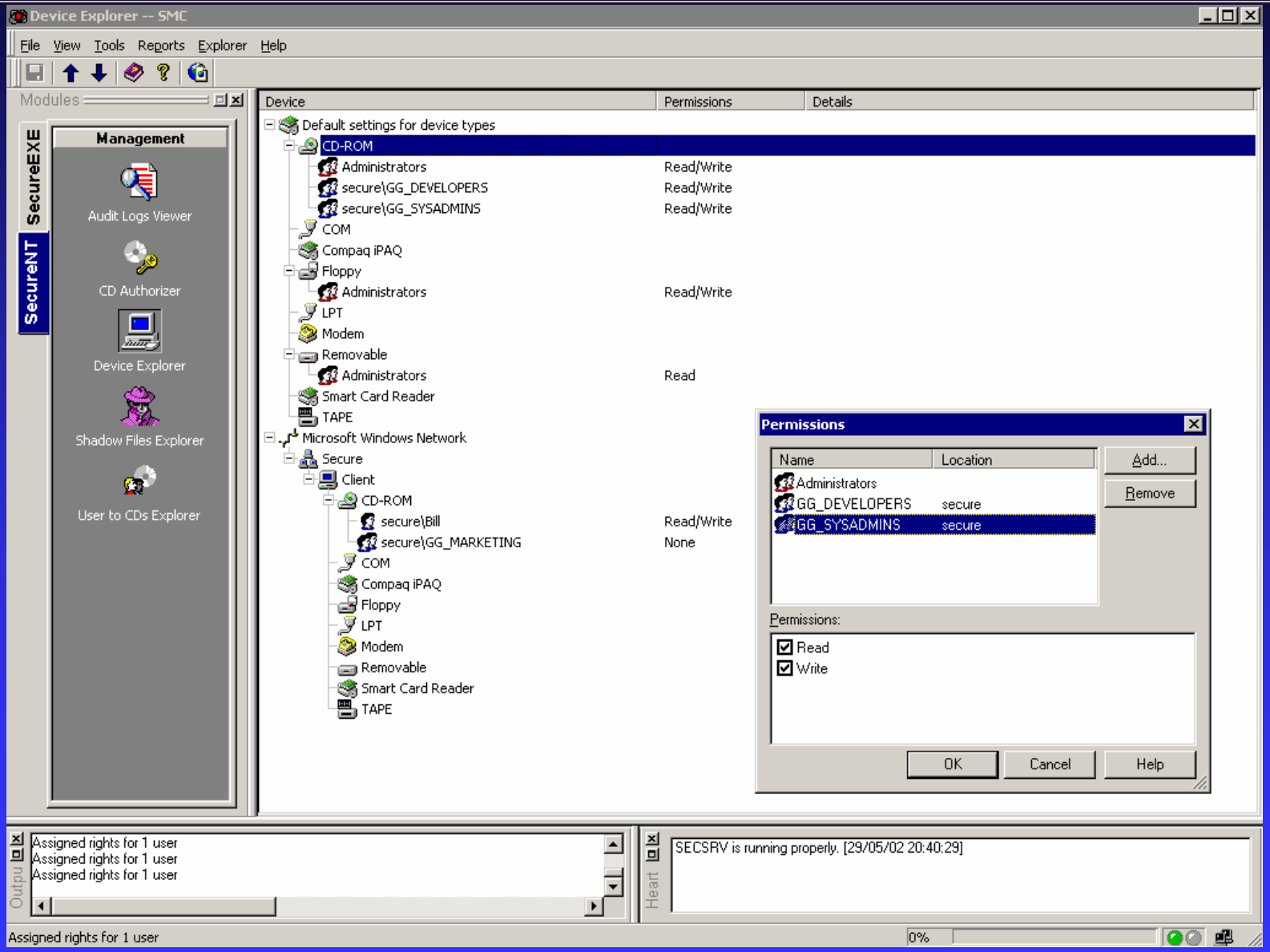
D’autres solutions

- Laptop sans PnP ni PCMCIA
- Boucher les ports PnP avec soit:
  - Du béton,
  - Du silicone,
  - Du sparadrap.
- Alimenter le port USB avec du 220V
- Dégotter des carte mères supportant des PII 266MHz sans USB, ni slot d’extension.
- Dessouder sur la carte mère les puces USB, FireWire, etc.
- Informer les utilisateurs que n’ont pas le droit d’utiliser les ports PnP et leur faire confiance
- Faire l’autruche, marche aussi très bien

SecureNT

- Control d'accès aux périphériques d'E/S:
  - **Floppy,**
  - **CD-ROM,**
  - **LPT & COM ports**
  - **Tape Drive**
  - **Modem**
  - **Disques amovibles**
- Basé sur les ACL (lecture, lecture/écriture, pas d'accès)
- **Plug and play**
- Accès Temporaire/permanent/planifié
- Audit

Démo SecureNT



Exécutions sauvages

Logiciel non autorisés

- Spyware / espiogiciel
- Outils de piratages
- Virus
- Chevaux de Troie
- Vers/worms
- Outils d'intrusion distribuée
- Économiseur d'écran
- Pas de licence

Venant de beaucoup de sources différentes:

- Internet,
- E-mail,
- Partages réseaux,
- CDROM de magasines,
- Etc.

Les solutions classiques

- Stratégie de sécurité
- Retirer les fichiers exécutables
- Retirer les raccourcis
- Bloquer aux frontières (fichiers attachés)
- ACL de NTFS (cfr. suivant)
- Stratégies de groupes (cfr. suivant)
- SRP Software Restriction Policies (…)
- Antivirus

ACL (Access Control List)

- DumpSec pour vérifier les droits sur un disque/partage/etc.
- Exemple de quelques répertoires en accès lecture/écriture/exécution
  - C:\
  - C:\documents and settings\All users\Application Data\Microsoft\HTML Help\
  - C:\documents and settings\All users\Documents\
  - C:\documents and settings\All users\DRM\
  - C:\documents and settings\%username%\
  - C:\winnt\tasks
- Utilisation de XCACLS du reskit pour scripter des changements de droits (Voir ZAK).

GPO

- Prevent users from installing printer drivers
- Unsigned driver installation behavior
- Unsigned non-driver installation behavior
- IE: Disable automatic install of internet explorer component
- Scheduler: Prevent Task run and end
- MSI: always installs with elevate privileges
- MSI: Prohibit rollback
- MSI: prohibit patching
- Allow Administrator to install from terminal services session
- Prohibit users installs
- Restrict these program from being launch from help
- Do not process the run once list
- Do not process the legacy run list
- Windows Automatic update
- Restricted permitted snap-ins
- Control Panel: add/remove program
- Code signing for device drivers
- Prevent access to the command prompt
- Prevent access to registry editing tools
- **Run only allowed windows applications**
- **Don’t run specified windows applications**

SRP (Software Restriction Policies)

- Introduit dans Windows XP
- Unrestricted Vs Disallowed
- Enforcement (all files, all users)
- Rules
  - Path rules
  - Hash rules
  - Certificate rules
  - Internet Zone rules
- Rule applied if file name matches extension

Vers une nouvelle approche

Limites des solutions actuelles:

- AV uniquement vers les virus et basés sur une liste de Virus connus
- Frontières ne sont pas imperméables
- ACL ne s'appliquent que sur NTFS
- Sécurité basée sur le nom de fichier ou son extension.

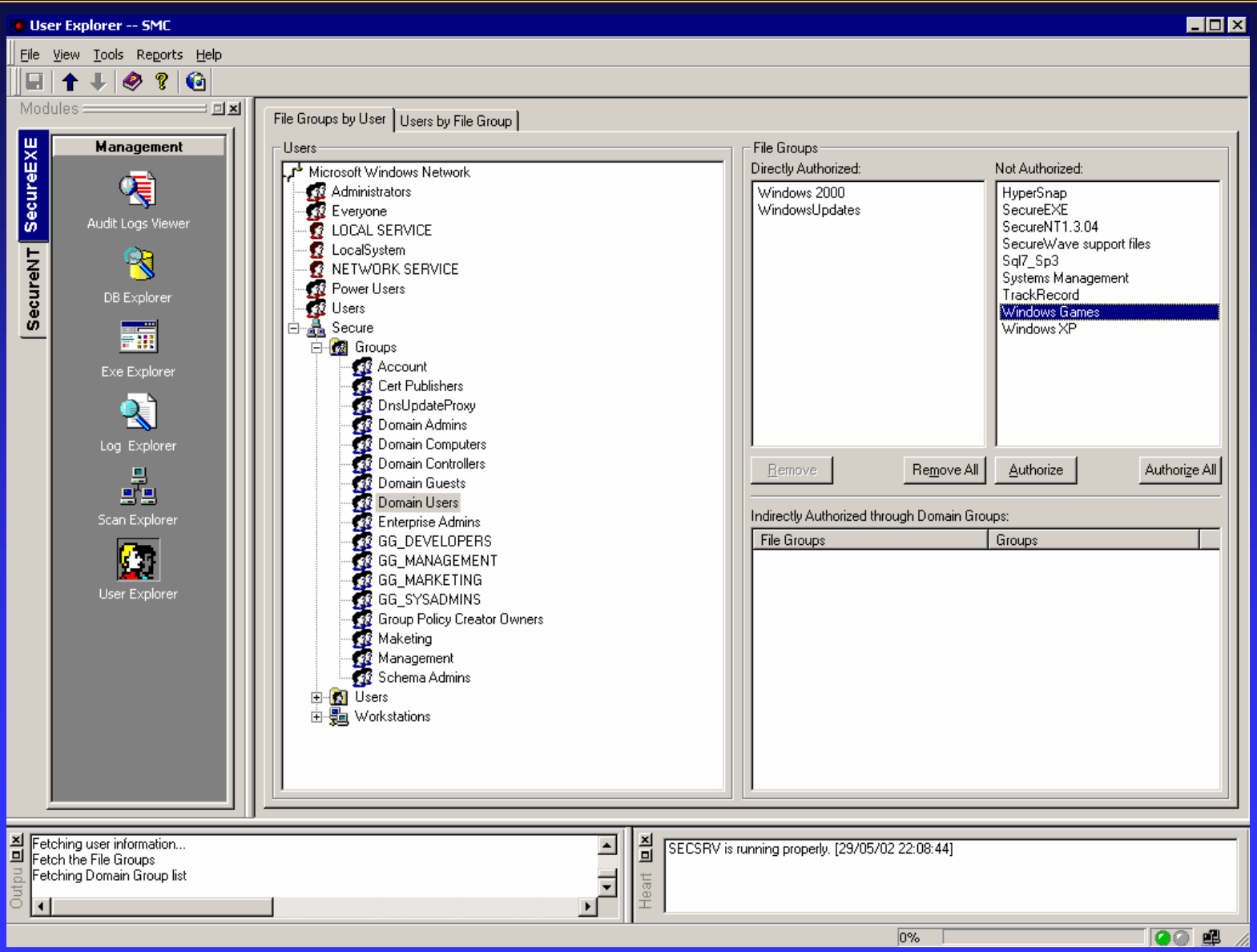
SecureEXE

Objectif: limiter l'exécution à ce qui est connu et autorisé
« contrôle qui exécute quoi »

- Identification et Authentification fortes, basées sur un HASH (SHA-1)
- Immunité face aux nouvelles menaces

- AD ou NTDS
- Gestion centralisée et à distance
- Support pour Terminal Server + Citrix MetaFrame

Démo SecureEXE



Pour tester chez vous

Description produit	Systèmes supportés
DebPloit http://www.eweek.com/article/0,3658,s=1884&a=24761,00.asp	Win NT4/2000
Dump Sec http://www.somarsoft.com/	Win NT4/2000/XP
Zero Administration Kit http://www.microsoft.com/ntworkstation/downloads/Recommended/Featured/NTZAK.asp	Win NT4/2000/XP

Conclusions

Les solutions SecureWave, permet aux entreprises d’appliquer un contrôle plus stricte sur l’usage de la station de travail, réduisant ainsi les coûts de gestion du parc informatique.

Contacts

- Marco Peretti, CEO
  marco@securewave.com
- Benoit Fortemps, Ingénieur systeme
  benoitf@securewave.com

- **SecureWave**
  Route de Luxembourg, 66
  L-4221 Esch sur Alzette
  +352 265 364 11