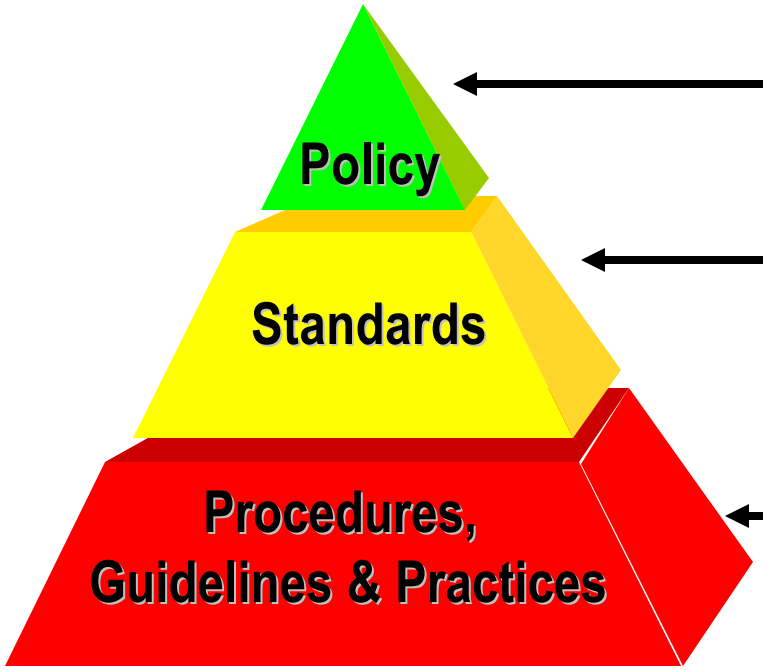
etacheau@symantec.com

Mesurez et quantifiez votre niveau de sécurité !

Agenda

- ✓ Etat de l'art
- ✓ Problématique
- ✓ Symantec Enterprise Security Manager
  - **Concepts clés**
  - **Politique de sécurité**
  - **Architecture**
- ✓ Conclusion

Etat de l'art



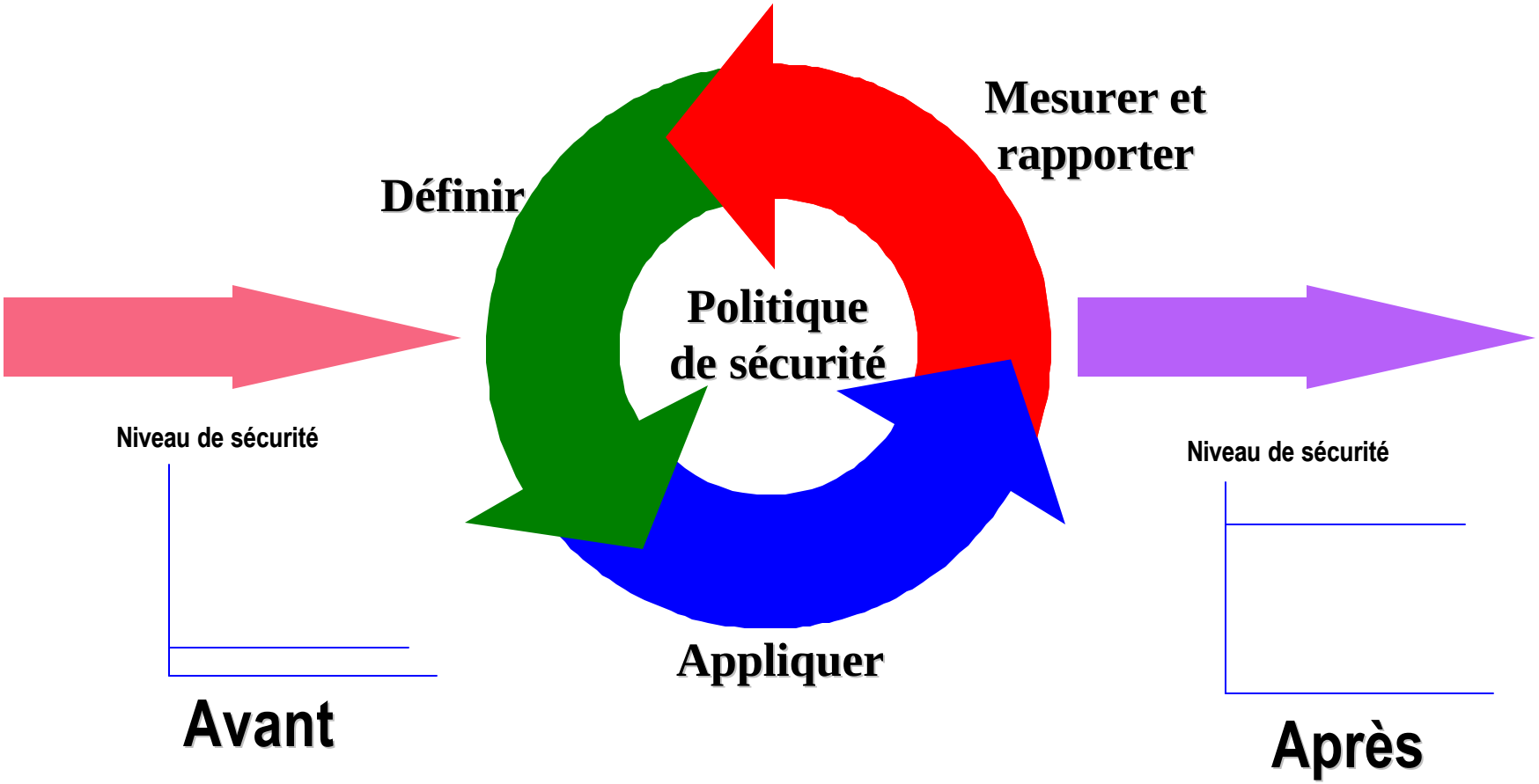
Primordial – Documentations

Méthodes : Marion, Melissa, ISO17799…

Audits de sécurités – Mise en oeuvre de procédures

Au sein de chaque entreprise

Cycle infini … … Cercle vertueux



Problématiques

A partir d'une politique de sécurité donnée, il faut

- ✓ Pouvoir fournir une souplesse de mise en oeuvre
- ✓ S'adapter au système d'information
- ✓ Etre capable de s'adapter aux modifications
- ✓ Rendre, analyser et remonter les informations
- ✓ Prendre en compte les délais de réponses souhaités

Positionnement Enterprise Security Manager

Management de la sécurité

"Quel est notre niveau de sécurité ?"

✓ Quantification

✓ Identification des vulnérabilités

✓ Conformité par rapport à une politique de sécurité

Détection d'intrusion

"Sommes-nous sous l'emprise d'une attaque ?"

✓ Détection en temps réels des problématiques

✓ Scénario de réponses automatiques – Contres-mesures

✓ Gérer l'inconnu

Enterprise Security Manager

✓ Fournit une plate-forme unique et centralisée pour la gestion de la sécurité

✓ Permet de définir en ligne la politique de sécurité

✓ Mesure la sécurité actuelle par rapport au référentiel

✓ Détecte les écarts

✓ Mesure la vulnérabilité, déduit les risques

✓ Fournit la synthèse de toute l'entreprise

Security Policy

Quelques concepts…

Architecture 3-tiers

Architecture du produit

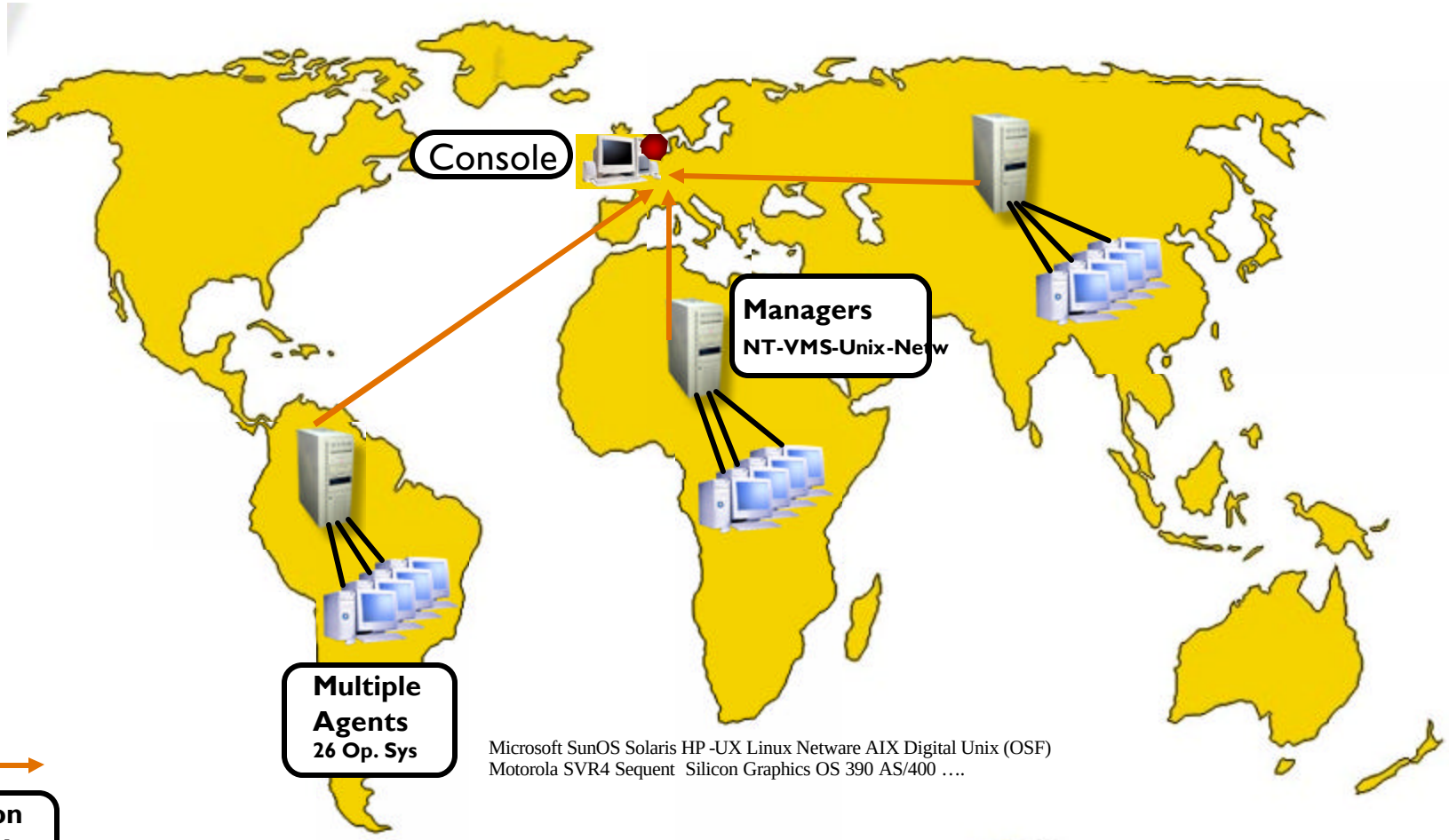
- ✓ Définition d'une région
- ✓ Définition d'un domaine
- ✓ Remontée d'informations au niveau d'un agent

Politique(s) de sécurité au sens ESM

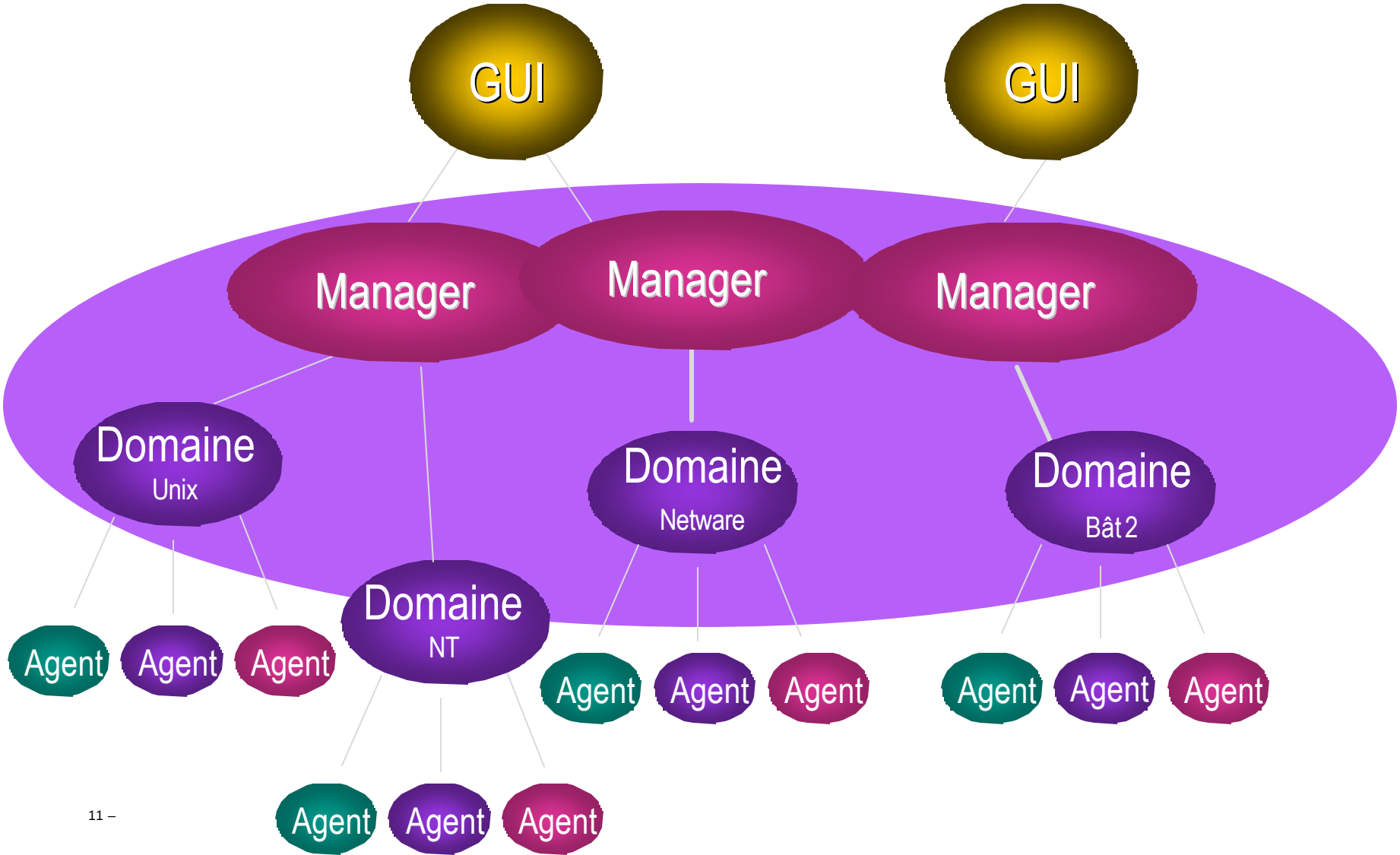
Niveaux de sécurité

Reporting

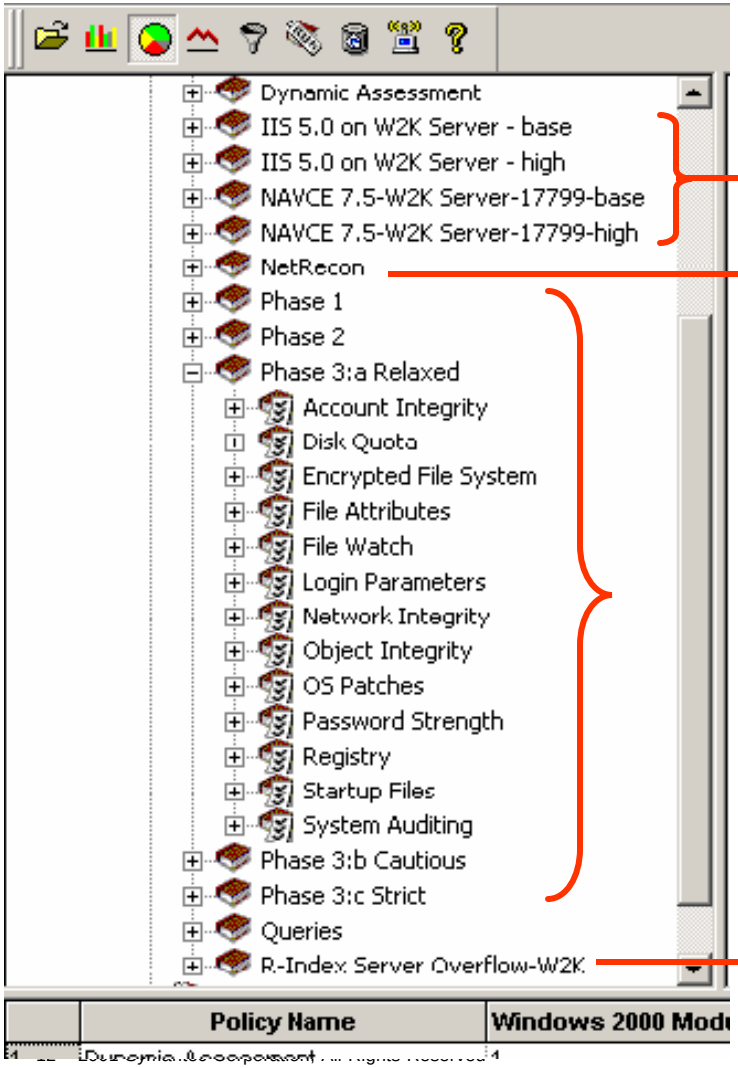
Architecture 3-tiers



Reflet de l'organisation ESM



Politiques de sécurité avec ESM



Politiques “Best Practices”

Politique d’intégration NetRecon

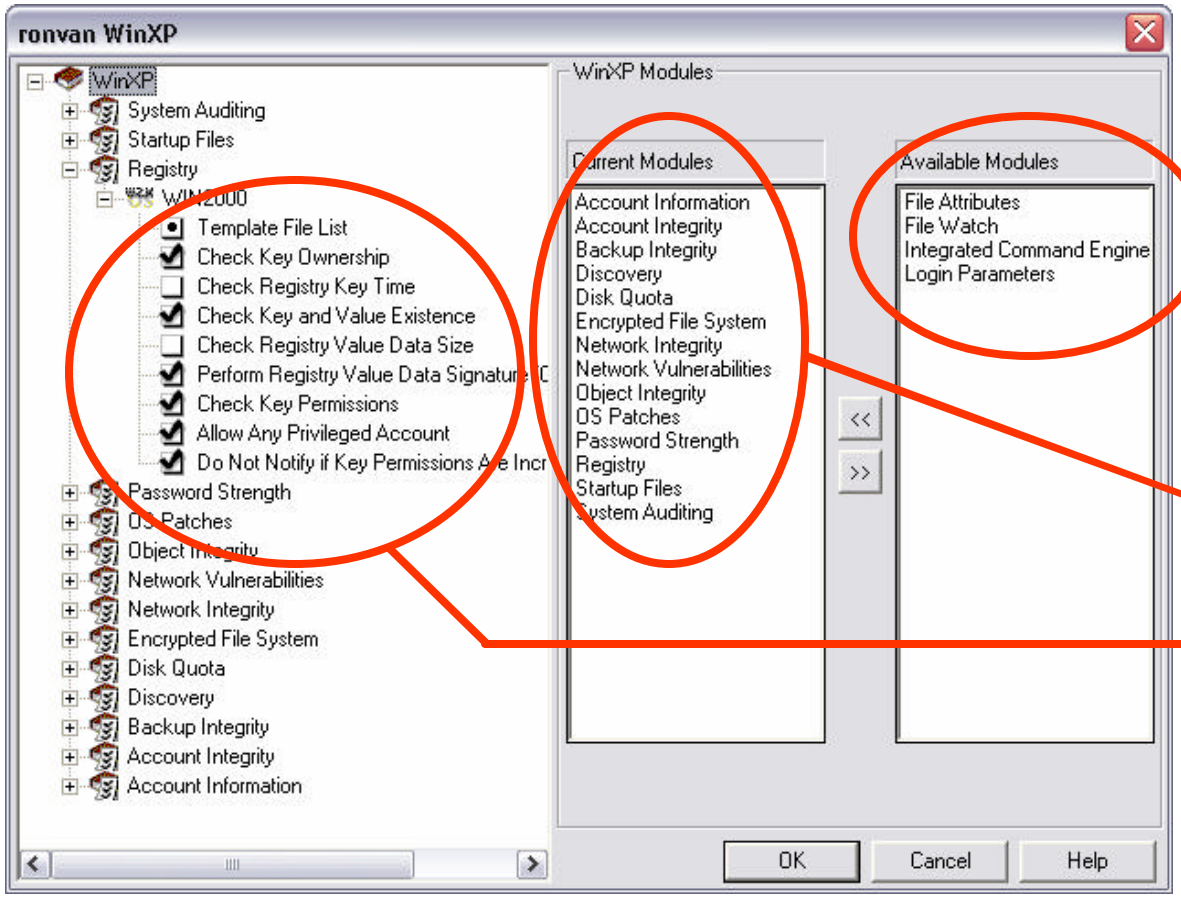
Par défaut

- ✓ Phase 1 – Orientée Users
- ✓ Phase 2 – Aspect réseau - système de fichiers
- ✓ Phase 3 – Problématiques plus strictes

Security Response – Ex: Nimda

Adéquation au S.I.

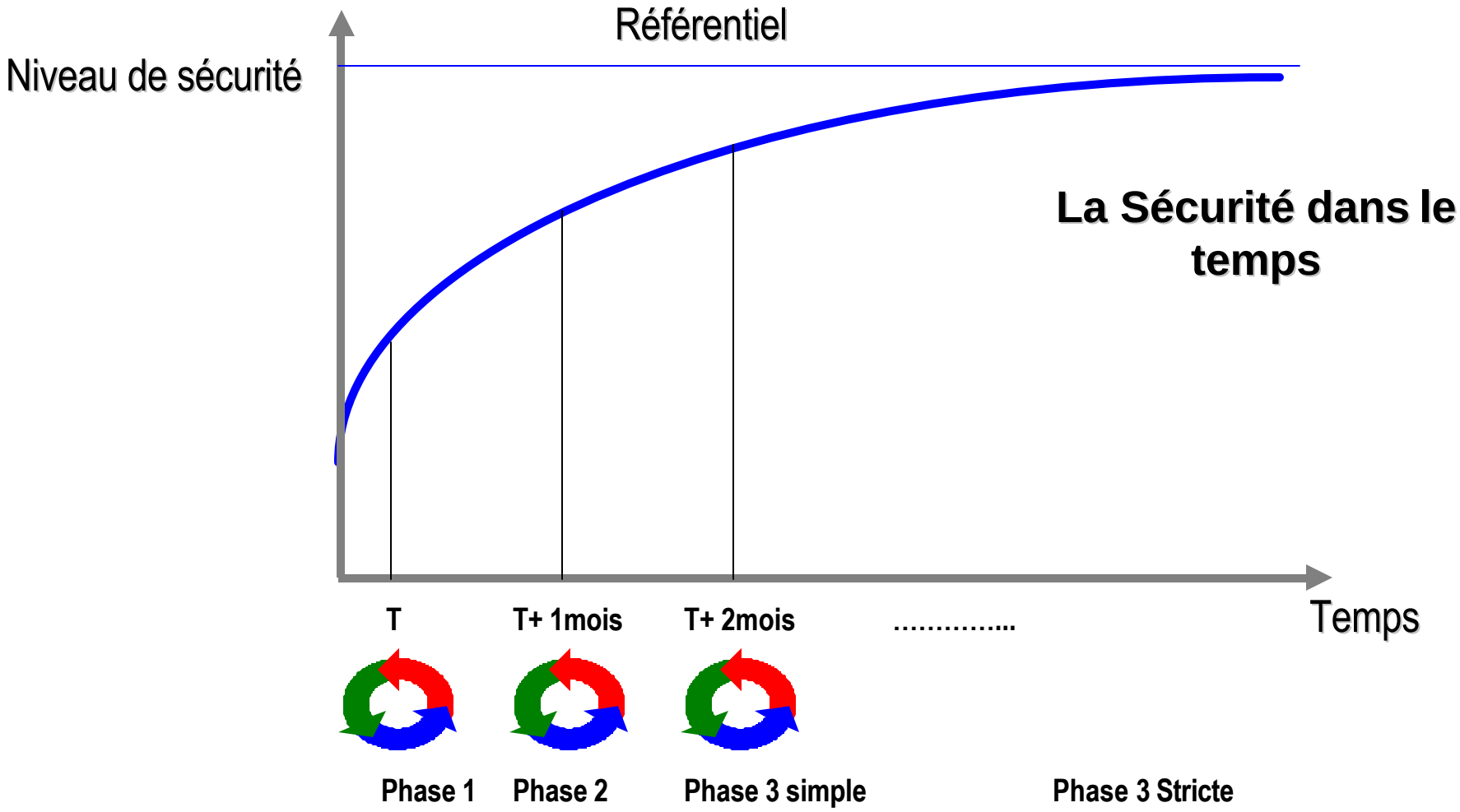
A partir de 17 modules et 2000 vérifications !



Ces modules ne sont pas appliqués

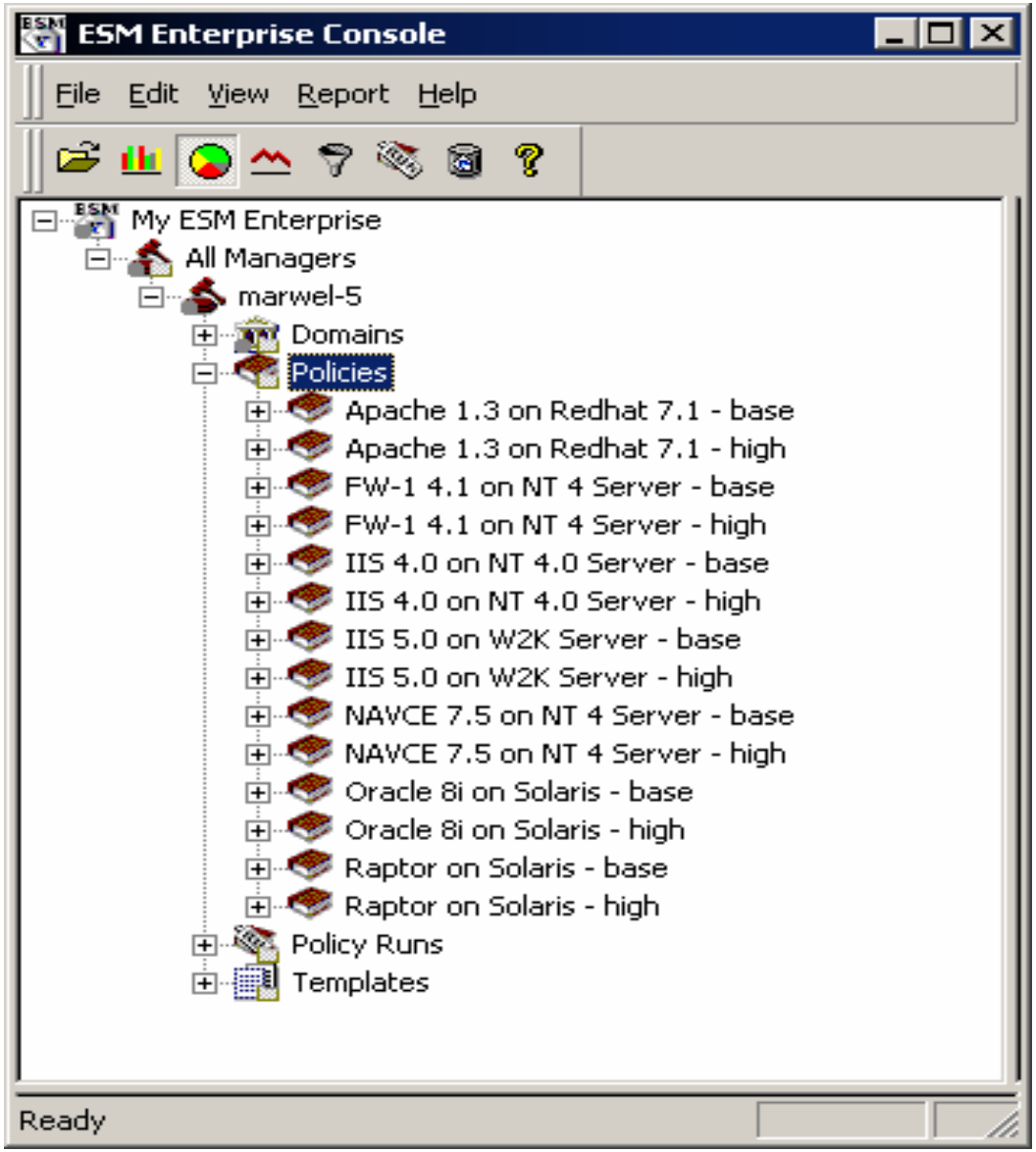
Ces modules avec les vérifications paramétrées spécifiquement

Souplesse d'implémentation



Best Practices

Combiner l'expertise
et la sécurité :



Security Responses

Des exemples de security responses

- Enterprise Security Manager™ Response Templates for MS02-018 IIS Cumulative Patch (11 Avril 2002)
- Enterprise Security Manager™ Response Policy for PHP Buffer Overflow Vulnerability (28 Fév 2002)
- Enterprise Security Manager Response Policy for CDE Buffer Overflow (18 janv 2002)
- Enterprise Security Manager Response Policy for Windows XP Unchecked Buffer in Universal Plug and Play response policy for Windows XP (20 Déc 2001)
- Enterprise Security Manager Response Policy for Solaris Login Buffer Overflow (20 Déc 2001) …..

Mise à jour - Liveupdate

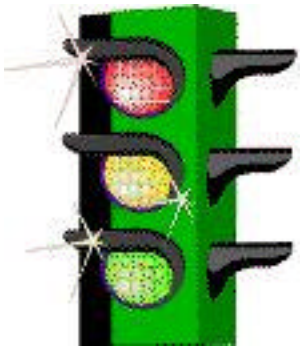
ESM SUs:

- ✓ Fournir chaque trimestre des mises à jour pour ESM
- ✓ Inclure le support de nouveaux operating systemes et de nouvelles vérifications demandées
- ✓ Délivrer des politiques de sécurités spécifiques aux systèmes d'exploitations à partir de ISO17799

Integration Live Update ™ **for NT, W2K and UNIX**

- ✓ Récupère les SU à partir des serveurs Symantec LiveUpdate dans le monde entier – Automatiquement sur les agents
- ✓ Spécification du manager par agent
- ✓ Désactivation de Liveupdate pour mettre à jour manuellement les systèmes qui doivent l'être
- ✓ Mise à jour de l'ensemble des managers à partir d'un point central unique

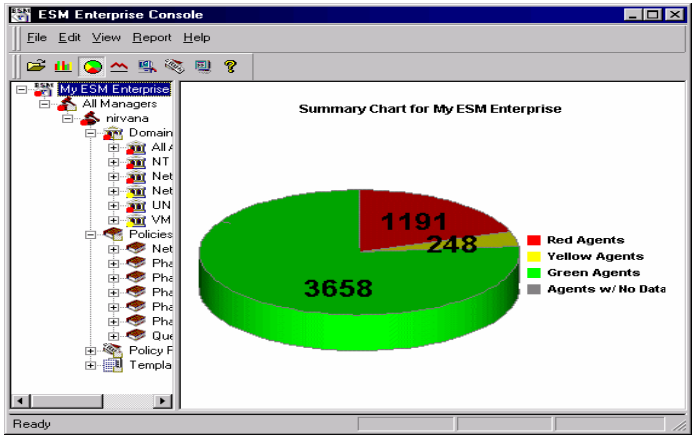
Niveaux de sécurité - Evaluations



- ✓ Rouge : Sérieux problème de sécurité !
  - Vulnérabilités recherchées activement par les hackers & script kiddies
  - Non adéquation avec la politique de sécurité
- ✓ Jaune : Problème potentiel de sécurité
  - Hackers experts pourront trouver ces failles
  - Mise en garde
- ✓ Vert : Notifications

Valeurs

- ✓ Nb politiques executées par domaine
- ✓ Indice de problématique
- ✓ Référence quotidienne
- ✓ Sécurité indicée mnémotechniquement



Séparation des rôles

Les utilisateurs se connectent sur les managers avec le GUI

Les utilisateurs ESM possèdent des comptes privilégiés à plusieurs niveaux

- Créer, modifier, lancer, exploiter -> Managers, domaines, Agents, “policies”,

Les utilisateurs ESM n’ont pas besoin de comptes utilisateurs sur les machines Agents

Créer des espaces de travails personnalisés avec différentes vues (région, domaine, agents)

Compte spécifiques pour l’installation des agents

Intégration - reporting

Rapports pré-définis

Crystal Report – export fichiers html, office, xml…..

Import – Export de données

- ✓ Export des données ESM vers Oracle, MS SQL Server ou MS-Access
- ✓ Consolider les données de plusieurs managers vers une même base de données
- ✓ Créer des requêtes spécifiques par rapport à vos applications

Intégration avec TIVOLI, HPOV ITO via SESA

Intégration avec SESA – Symantec Enterprise Security Architecture

Common Logging & Reporting

Conclusion

Véritable produit de gestion de politique de sécurité

- ✓ Gestion Globale (plus de 25 OS !)
- ✓ Adéquation du logiciel à l'organisation de l'entreprise
- ✓ Architecture 3 tiers
- ✓ Génération de Rapports étendus
- ✓ Séparation des tâches et responsabilités
- ✓ Tout, à partir d'un point central
- ✓ Intégration dans des Frameworks

Questions