UNIVERSITÉ DU MAINFRAME

Stephane_ly@fr.ibm.com

Présentation des outils Vanguard

jeudi 4 mai 2006

IBM Software Group

Présentation des outils Vanguard

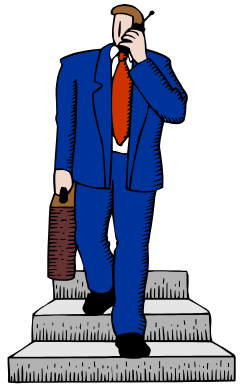
Stephane_ly@fr.ibm.com

Tivoli software

ON DEMAND BUSINESS

Gestion RACF et solutions Vanguard

- **Problématiques de l'administration RACF**
- **Solutions Vanguard**
  - **La société Vanguard**
  - **Vanguard Administrator**
  - **Vanguard Advisor**
  - **Vanguard Analyzer**
  - **Vanguard Enforcer**
  - **Vanguard SecurityCenter**
- **Conclusion**
- **Questions**



Les problèmatiques de l'administration RACF

- Protection des applications et confidentialité des données de l'entreprise
- Consolidation, Fusions, Réorganisation des entreprises
- Manque d'experts pour l'administration de la sécurité
- Remplacement des outils 'maison'

La société Vanguard

Créée en 1986

Capital de fonds privés

Activités : Vente de logiciels autour de sécurité, formation et prestation de services

Clients : 600 dans le monde, 1400 licences vendues

Partenaire de vente : IBM Software Group

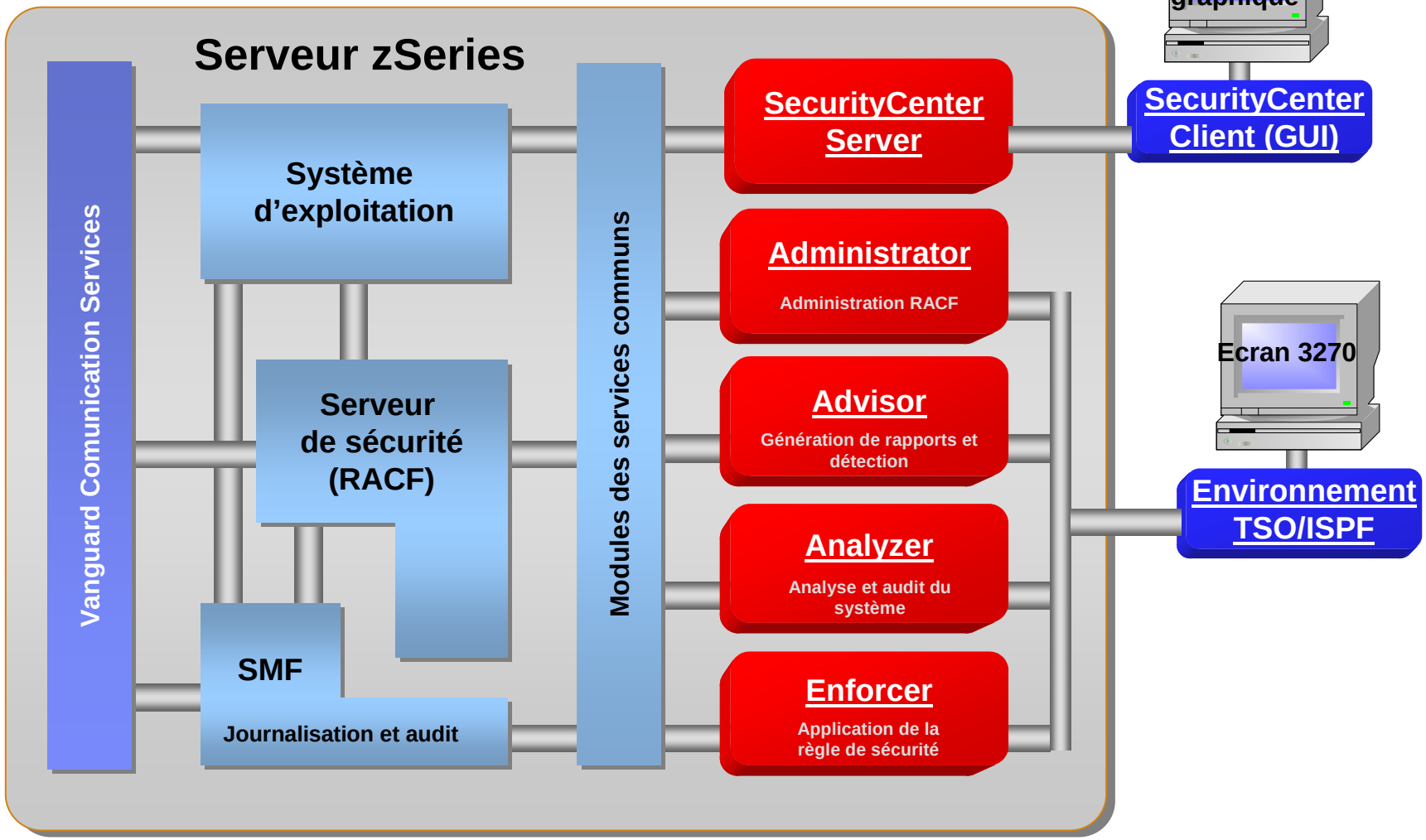
Vanguard Victoria Labs
Victoria, BC, CANADA

Vanguard Research Institute
Orange, CA, USA

Vanguard Integrity Professionals - Nevada
Las Vegas, NV, USA

Vanguard Integrity Professionals, Ltd.
Berkshire, UK

Administration RACF et outils Vanguard



Vanguard Administrator

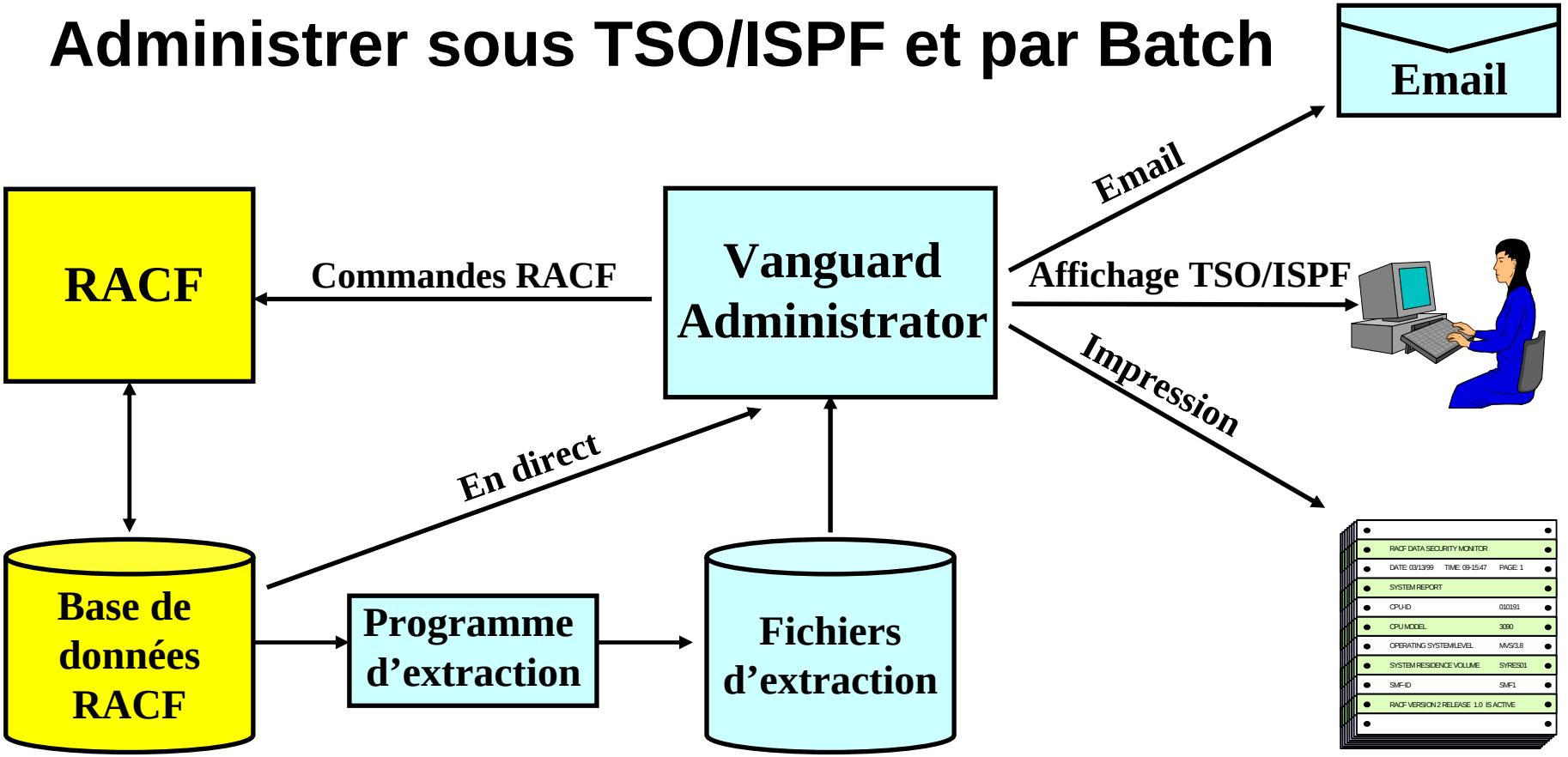
- **What is ‘Vanguard Administrator’ ?**

Vanguard Administrator

- **Simplifier la complexité de l'administration RACF**
- **Générer des commandes RACF**
- **Planifier l'exécution des commandes générés**
- **Générer des Reports sur les définitions dans la base RACF**
- **Analyser les incohérences de protections des ressources**
- **Analyser les protections des fichiers à partir de VTOC disques**
- **Déléguer la gestion des tâches récurrentes à un user sans attribut SPECIAL**

Vanguard Administrator – Vue d'ensemble

Administrer sous TSO/ISPF et par Batch



Vanguard Administrator

- **Outil idéal pour faciliter l'administration RACF**
- **Réduire les risques d'erreurs d'administration RACF**
- **Augmenter la productivité des ingénieurs systèmes ou des administrateurs RACF (débutants ou expérimentés)**
- **Grâce aux :**
  - **Guidage de tâches d'administration avec les menus ISPF conviviaux**
  - **Génération automatique des commandes RACF**
  - **Rapport d'analyse sur des incohérences des protections**
  - **Planification l'exécution des commandes RACF générées**
  - **Décentralisation de gestion des Users et leur mot de passe**
  - **Gestion du champs 'Installation Data' du chaque Userid**
  - **Gestion des fichiers Unix dans l'environnement USS**
  - **Etc …**

Vanguard Advisor

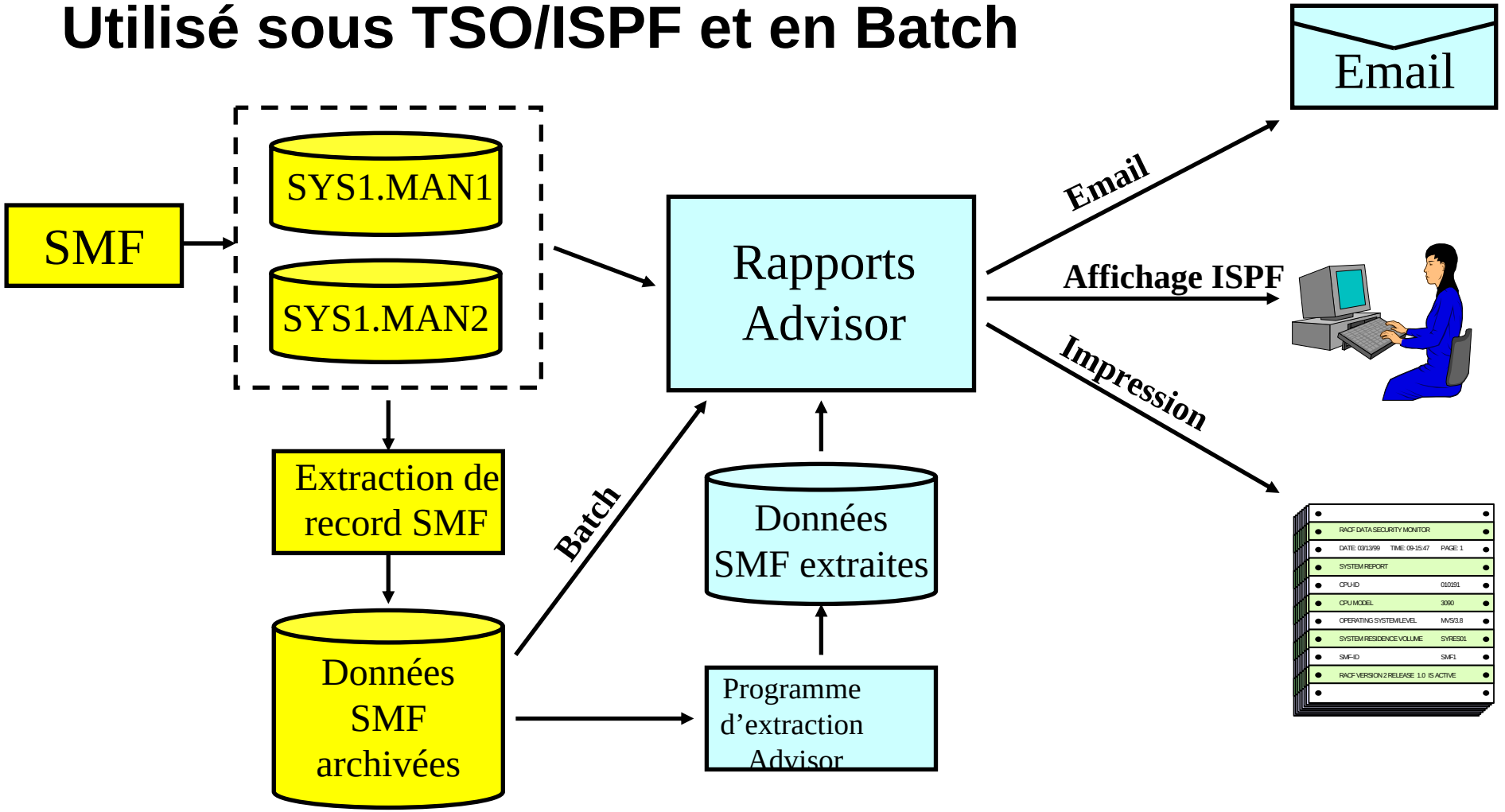
- **What is ‘Vanguard Advisor’ ?**

Vanguard Advisor

- **Analyser des fichiers SMF**
  - **en temps réel : SYS1.MANxx**
  - **archivés (sur disques ou sur cassettes)**
- **Générer des rapports (standards ou personnalisés) sur tous les événements liés aux accès des ressources RACF et aux certaines activités dans les systèmes z/OS.**
- **Alerter en temps réel des événements liés à la sécurité via Email**

Vanguard Advisor Reporting

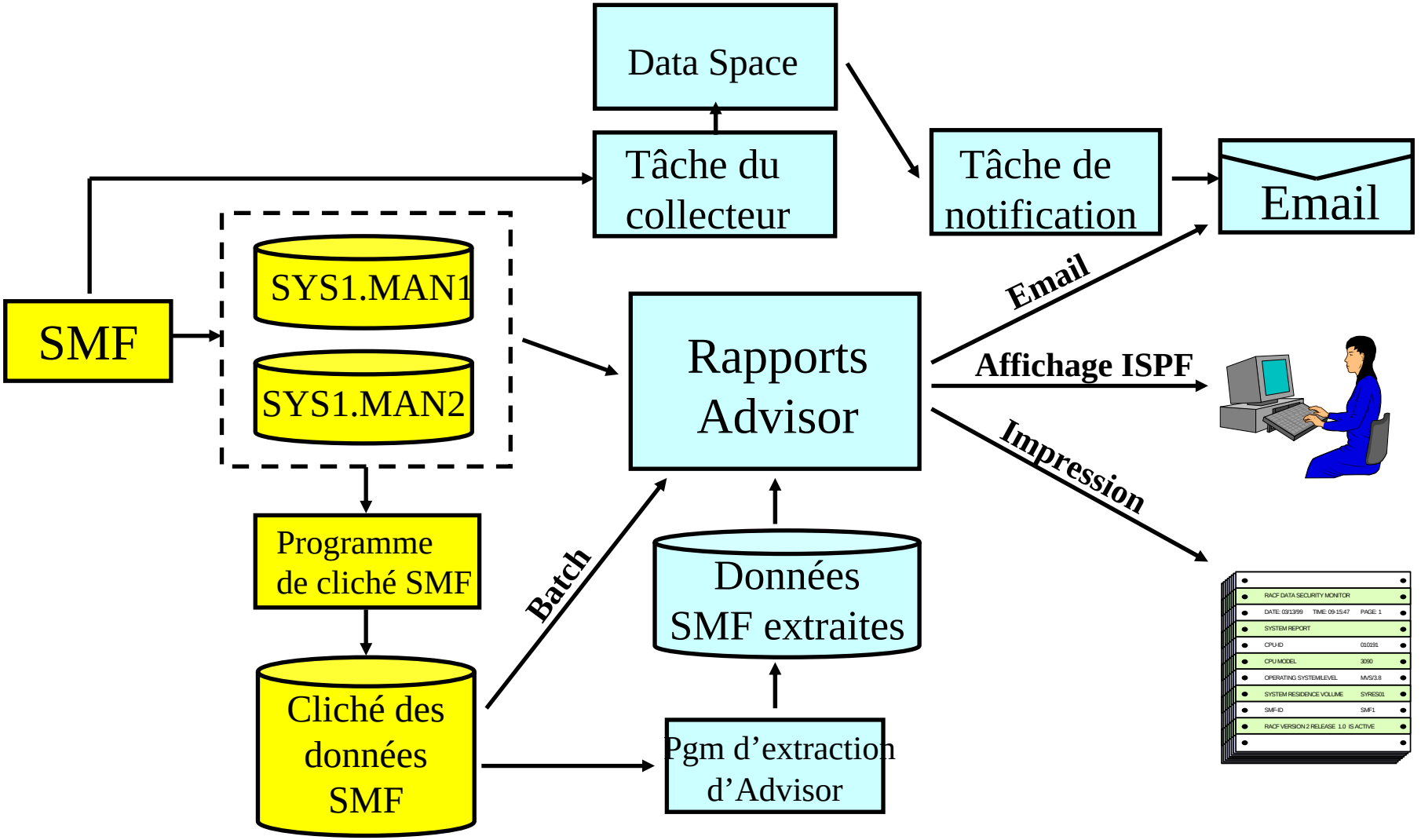
Utilisé sous TSO/ISPF et en Batch



Vanguard Advisor

- **Analyser des records SMF (archivés ou en temps réel) et générer des rapports sur tous les événements liés aux accès des ressources RACF et des systèmes z/OS.**
- **Menus ISPF proposent des modèles de reports standards ou personnalisables (détaillés ou synthétiques) avec des prédicats, références croisées.**
- **Exemples des événements qu'on peut analyser dans les rapports générés :**
  - **Violations des règles de sécurité**
  - **Accès aux ressources protégés par RACF**
  - **Commandes RACF exécutées**
  - **Activités des Users (logon/logoff TSO, Jobs ou STC)**
  - **USS (Unix System Services)**
  - **TCPIP (activités FTP)**
  - **JES2/JES3 (Start, Stop et des activités RJE ou NJE)**
  - **IPL système z/OS**
  - **Activités des fichiers VSAM ou non VSAM (Open, Scratch, Rename)**
  - **Activités de "Scheduler" de Vanguard administrator**
- **Ces rapports générés peuvent être envoyés aux responsables de sécurité via Email (aussi être affichés sur les écrans ou stockés sur des fichiers).**
- **Génération des commandes RACF à partir des événements détectés**
- **Alerter en temps réel des événements liés à la sécurité**

Fonction de notification en temps réel de Vanguard Advisor



Alertes en temps réel sur des événements suivants

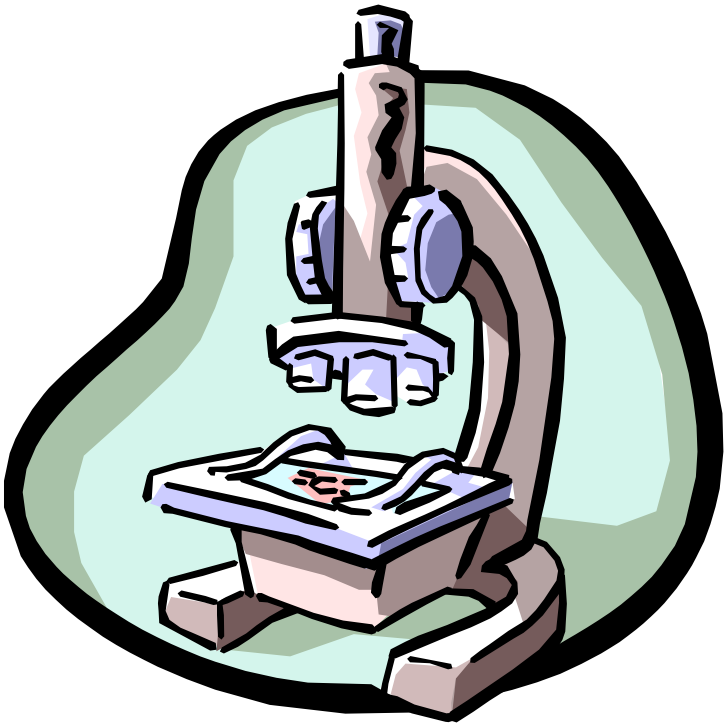
- Tous types de Violations
- Modifcation des attributs SPECIAL, OPERATIONS, AUDITOR
- Modifcation de Group-SPECIAL, Group-OPERATIONS, Group-AUDITOR, CREATE, CONNECT, JOIN Authority
- Modification de l'attribut UACC de Data Set Profile
- Accès autorisés via des Profiles en mode WARNING
- Détection des intrusions pour les "Invalid Passwords" pendant un délai de courte durée
- Changement de Password en trop peu de temps
- Activation ou Désactivation des Class de General Resource
- Détection de perte des données SMF
- User Id Revoké suite aux tentatives infructueuses ("invalid Password")
- Etc …

Vanguard Advisor

- **Outil convivial et puissant pour générer, en quelques secondes, les rapports permettant l'analyse et les suivis des événements RACF et des activités dans le système z/OS**
- **Faciliter l'audit, l'analyse et la résolution des problèmes de sécurité**
- **Surveiller et détecter, en temps réel, les événements RACF ou z/OS**
- **Alerter, en temps réel et via Email, des événements liés à la sécurité**
- **Eliminer tout développement de programmes spécifiques de génération des rapports relatifs à la sécurité RACF et à l'activité z/OS.**
- **Par :**
  - **Génération des rapports basés sur les choix des modèles proposés.**
  - **Possibilité de personnaliser des modèles de reports choisis.**
  - **Possibilité de générer des commandes RACF relatives aux problèmes ou événements détectés.**

Vanguard Analyzer

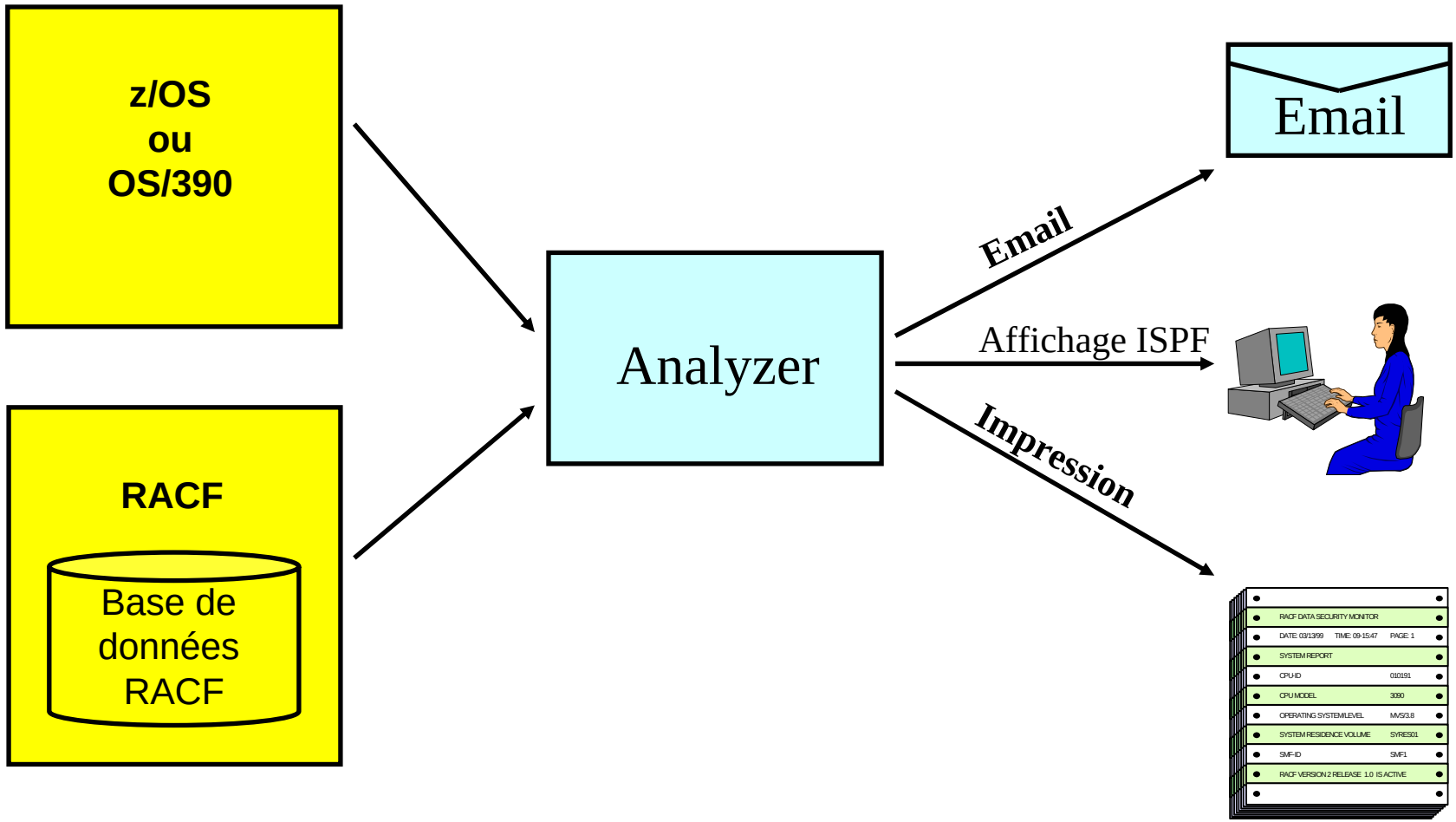
- **What is ‘Vanguard Analyzer’ ?**



Vanguard Analyzer

- **Analyser en temps réel les blocs de contrôle dans les zones mémoire z/OS représentant des paramètres d'implémentation du RACF et de mise en oeuvre du système z/OS.**
- **Effectuer une véritable expertise technique pour identifier les risques potentiels et les déviations aux "Best practices" de l'implémentation de RACF et du système z/OS.**
- **Proposer des solutions ou des recommandations adéquates (Best practices) pour les risques détectés (SmartAssist)**

Vanguard Analyzer



Vanguard Analyzer

- **Analyser en temps réel les blocs de contrôle en mémoire des paramétres du système z/OS, et les options utilisées par RACF afin d'auditer :**
  - **L'implémentation de RACF**
    (RACF Databases, CDT, User Caller table, Exits, Router Table, POSIT number, STARTED Class, SETROPS…)
  - **L'implémentation du système z/OS**
    (PPT, APF, LPA, Linklst, PARMLIB, SVC, Subsystems, paramétrage TSO, SMF, Exits, JES2, modes de protection des fichiers systèmes….)
- **Effectuer une véritable expertise pour identifier les risques potentiels et les déviations aux "Best practices" de l'implémentation de RACF et de z/OS**
- **Proposer des solutions ou des recommandations adéquates (Best pratices) pour les risques détectés (SmartAssist)**
- **Comparer les snapshots entre les différents bilans d'expertise**

Vanguard Analyzer

- **Outil d'audit, à chaud, de l'implémentation et l'utilisation des options RACF et des paramètres actifs de système z/OS.**
- **Cet outil permet de :**

  - Détecter les défauts ou erreurs de paramétrages RACF et z/OS.

  - Proposer des solutions préconisées par les "Best practices" et recommandées par des experts techniques.

Vanguard Enforcer

- **What is ‘Vanguard Enforcer’ ?**

Vanguard Enforcer

Détection automatique des intrusions ou des infractions aux ressources critiques.
Action immédiate pour rétablir la situation initiale et envoyer des alertes via GSM.

1. Un changement imprévu des droits d'accès à un fichier critique (Ex : la Paie du Personnel).

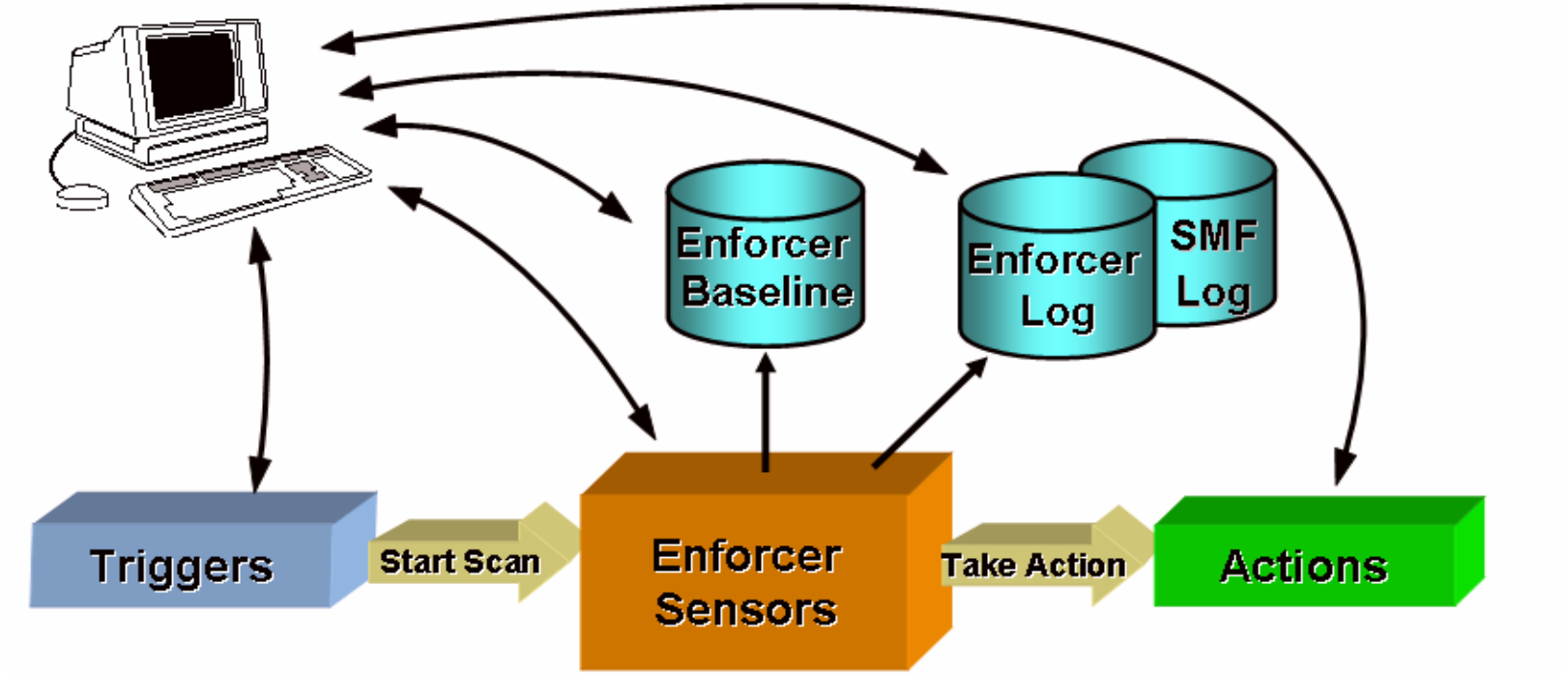
INTRUSION détectée

Date/Time: 04/12/05 5:00pm
Resource: Payroll File
User ID: MYTAILOR

3. Les responsables reçoivent un appel GSM et le message, ils prennent une décision.

2. Vanguard Enforcer détecte l'événement, ré-initialise immédiatement les droits d'accès conformes à la politique de sécurité d'entreprise, envoie une alerte aux responsables de sécurité avec un message détaillé.

Vanguard Enforcer



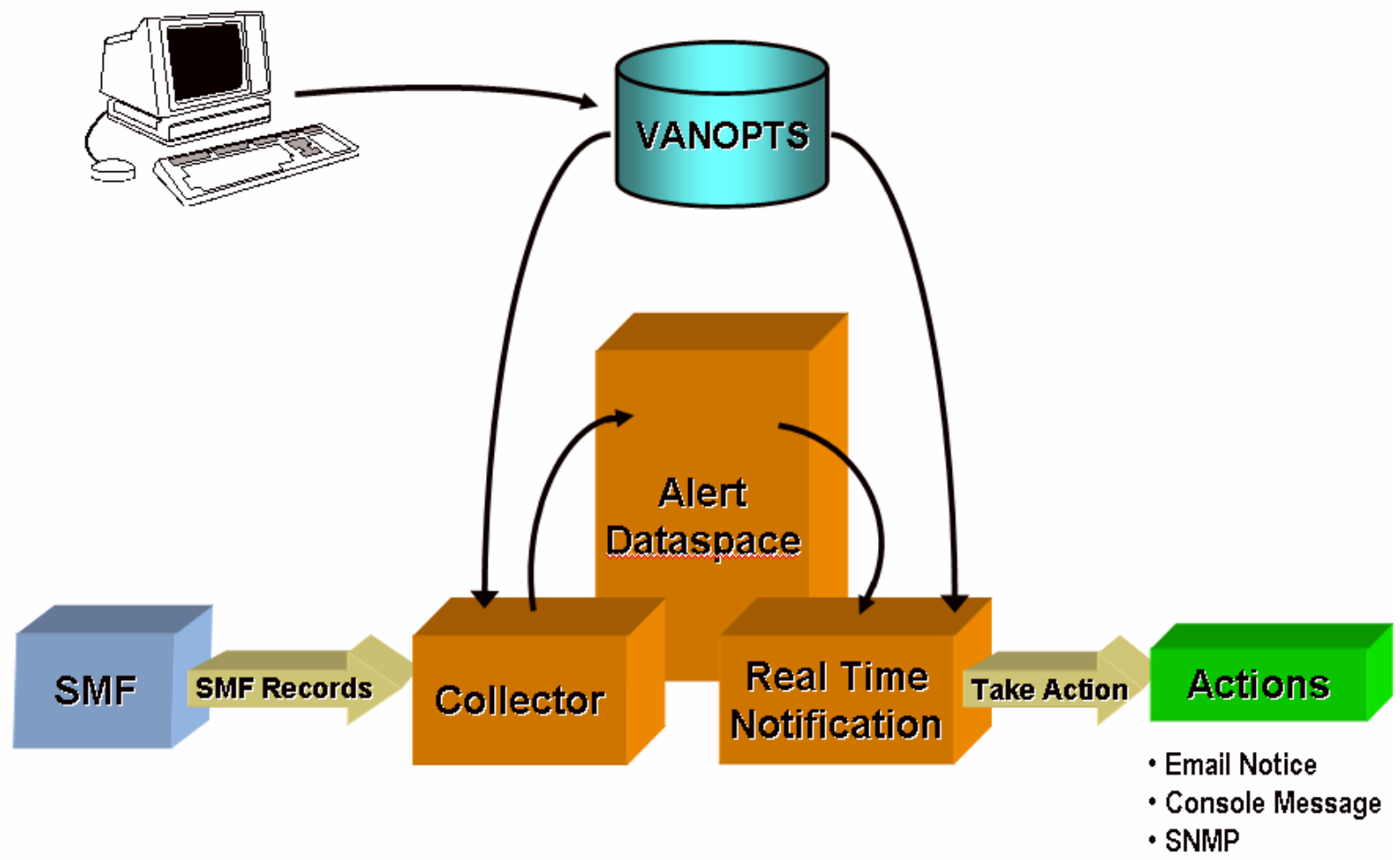
- Startup
- Manual
- Time-Interval

- Critical Data Sets
- Critical Volumes
- Critical Generic Res
- Critical Groups
- Privileged Users
- APF Libraries
- LINKLST Libraries

- RACF Options
- LPA List
- PPT
- SVCs
- Started Tasks
- Restricted Utilities
- Temporary Access

- Email Notice
- TSO Send Message
- Console Message
- SNMP
- Enforcer Log
- Generate RACF Commands
- Automatic Correction

Vanguard Enforcer



Vanguard Enforcer

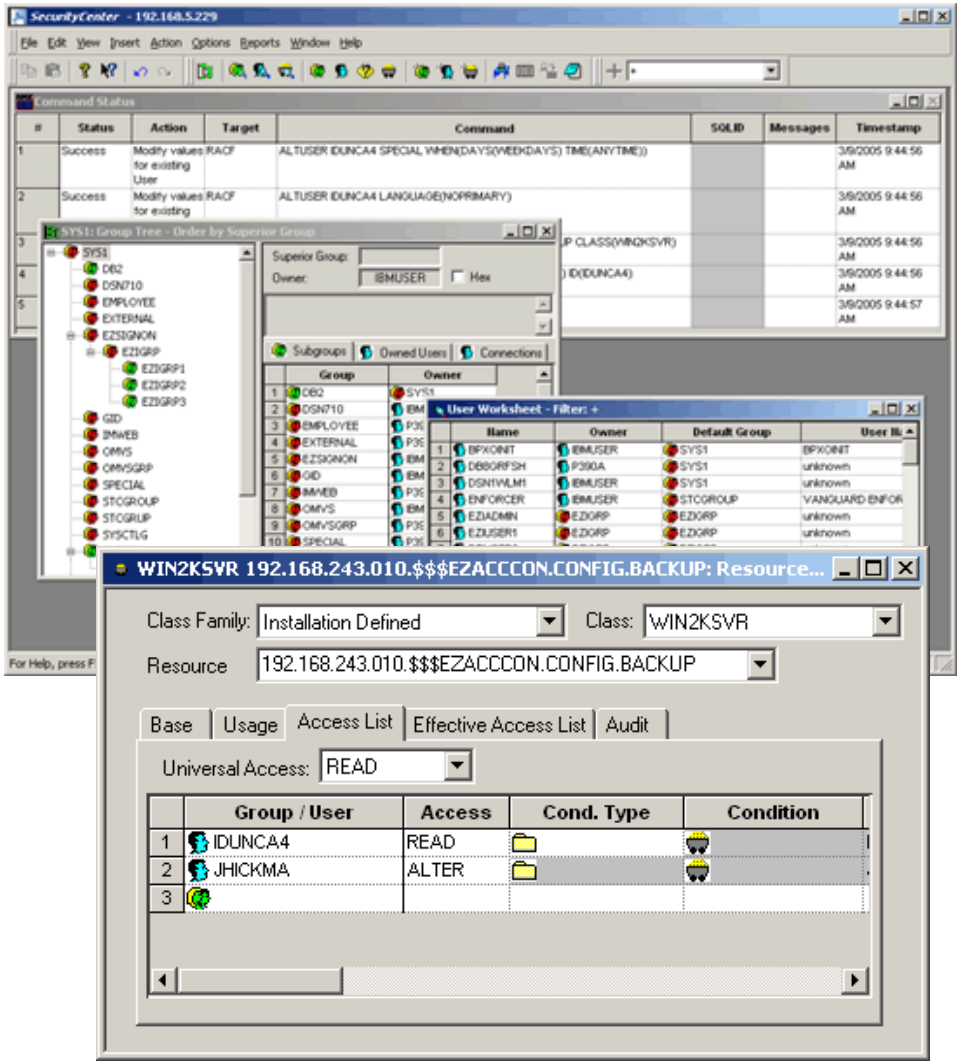
- **Outil de surveillance pour le respect strict de la politique de sécurité RACF**
- **(7J/ 7 et 24H/24) sans intervention humaine**
- **Alertes immédiates de toutes modifications non conformes aux règles de sécurité définies dans une base de référence**
  - **Email (ou Gsm)**
  - **Messages TSO**
  - **SNMP**
  - **Messages à la console**
- **Correction automatique des infractions afin de restaurer, à leur état initial, les droits d'accès aux ressources, conformes à la politique de sécurité d'entreprise**
- **Possibilité de limiter, dans une période précise, des autorisations exceptionnelles des droits RACF**

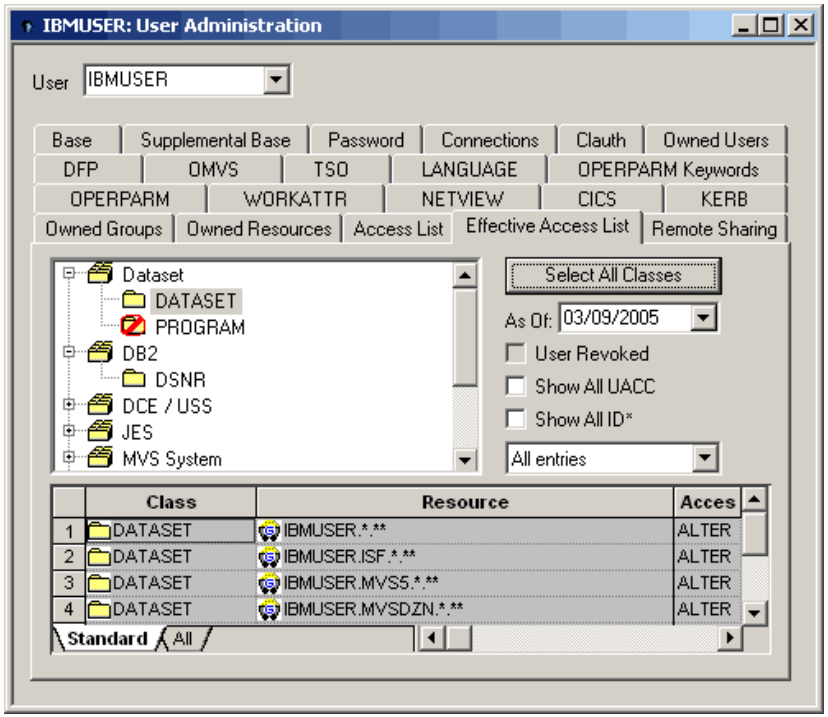
Vanguard SecurityCenter

- **What is ‘Vanguard SecurityCenter’ ?**

```
                        RACF - SERVICES OPTION MENU

SELECT ONE OF THE FOLLOWING:

   1  DATA SET PROFILES

   2  GENERAL RESOURCE PROFILES

   3  GROUP PROFILES AND USER-TO-GROUP CONNECTIONS

   4  USER PROFILES AND YOUR OWN PASSWORD

   5  SYSTEM OPTIONS

   6  REMOTE SHARING FACILITY

   7  DIGITAL CERTIFICATES AND KEY RINGS
  99  EXIT
                  Licensed Materials - Property of IBM
                  5647-A01 (C) Copyright IBM Corp. 1983, 2000
PF 1=HELP       2=SPLIT     3=END       4=RETURN    5=RFIND     6=RCHANGE
PF 7=UP         8=DOWN      9=SWAP      10=LEFT     11=RIGHT    12=RETRIEVE

OPTION ===> _
MA    a                                                        24/014
```

SecurityCenter – Administrer RACF avec interface graphique



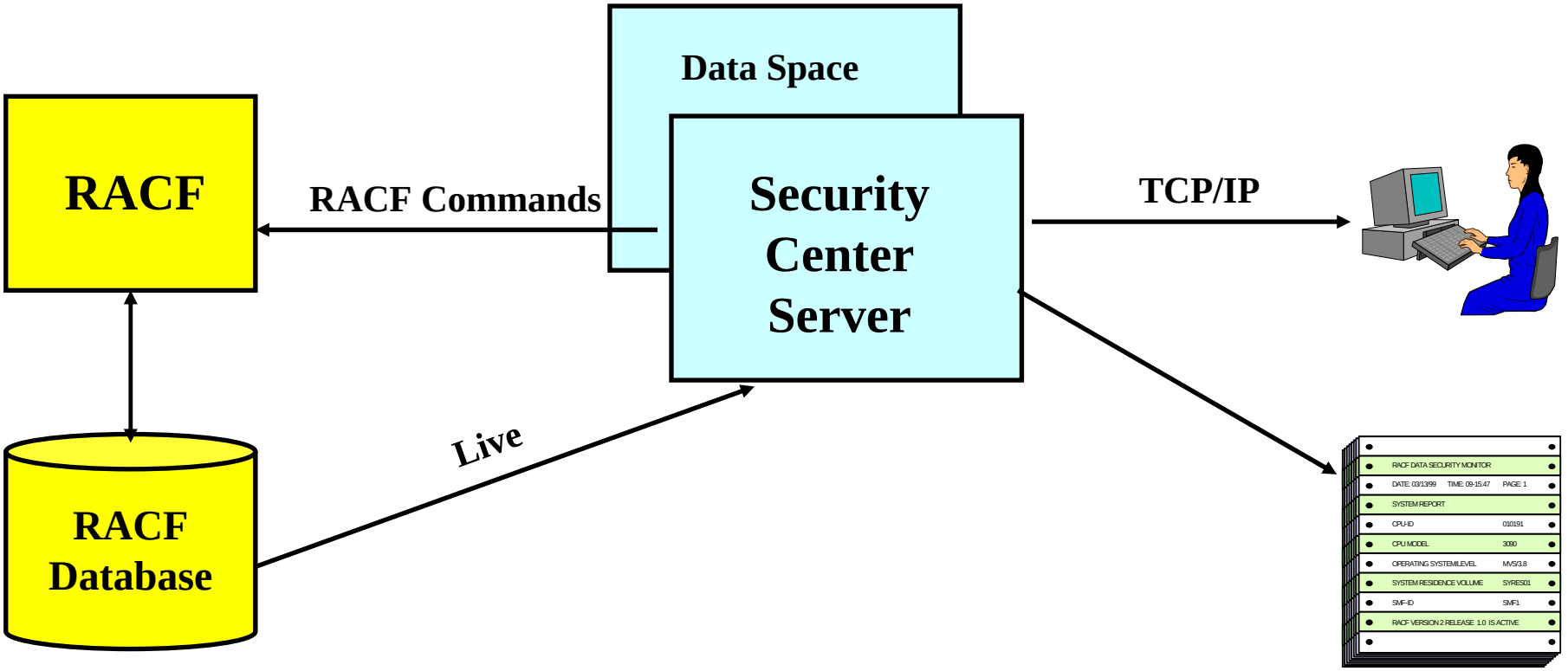


SecurityCenter fournit une représentation graphique de l'administration RACF dans une interface Windows que vous manipulez par pointer-cliquer et glisser-déposer.

Il permet aux administrateurs de sécurité de plateformes différentes de gérer RACF sans avoir à apprendre les commandes RACF.

Vanguard SecurityCenter

Operates without TSO/ISPF



Vanguard SecurityCenter

- **GUI (Graphic User Interface) très convivial pour administrer RACF**
-  **+ “Drag & Drop”…**
- **Plus besoin de définir les USER TSO pour les administrateurs de sécurité.**
- **Permettre aux personnes, ayant très peu de notions RACF ou z/OS d’administrer la sécurité.**
- **Outil idéal pour les services “Help Desk”**

Conclusion

- Vanguard Administrator
  - Simplifie la complexité de l'administration RACF (Menu ISPF, Scheduling, Reports..)
  - Analyse les incohérences de protection des ressources
- Vanguard Advisor
  - Analyse des records SMF et génère des Reports sur les événements RACF et z/OS
  - Facilite l'audit, l'analyse et la résolution des problèmes de sécurité RACF et z/OS
  - Alerte, en temps réel et via Email, des événements liés à la sécurité.
- Vanguard Analyzer
  - Apporte une véritable expertise pour identifier les risques potentiels ou les déviations aux "Best practices" de l'implémentation de RACF et z/OS
  - Propose les recommandations ou les solutions sur les risques détectés
- Vanguard Enforcer
  - Alerte, 24h/24 et 7j/7, sur toutes modifications non conformes aux règles de sécurité définies dans une base de référence
  - Corrige en temps réel les non respects des droits d'accès aux ressources critiques
- Vanguard Security Center
  - Fournit l'interface graphique GUI sous Windows pour l'administration RACF

Questions

Tivoli software

ON DEMAND BUSINESS

धन्यवाद
Hindi

多謝
Traditional Chinese

ขอบคุณ
Thai

Спасибо
Russian

Gracias
Spanish

Thank You
English

شكرا
Arabic

Obrigado
Brazilian Portuguese

多谢
Simplified Chinese

Danke
German

Grazie
Italian

Merci
French

நன்றி
Tamil

ありがとうございました
Japanese

감사합니다
Korean