TENDANCES LOGICIELLES 2008

Mardi 25 mars 2008 – Hilton Arc de Triomphe

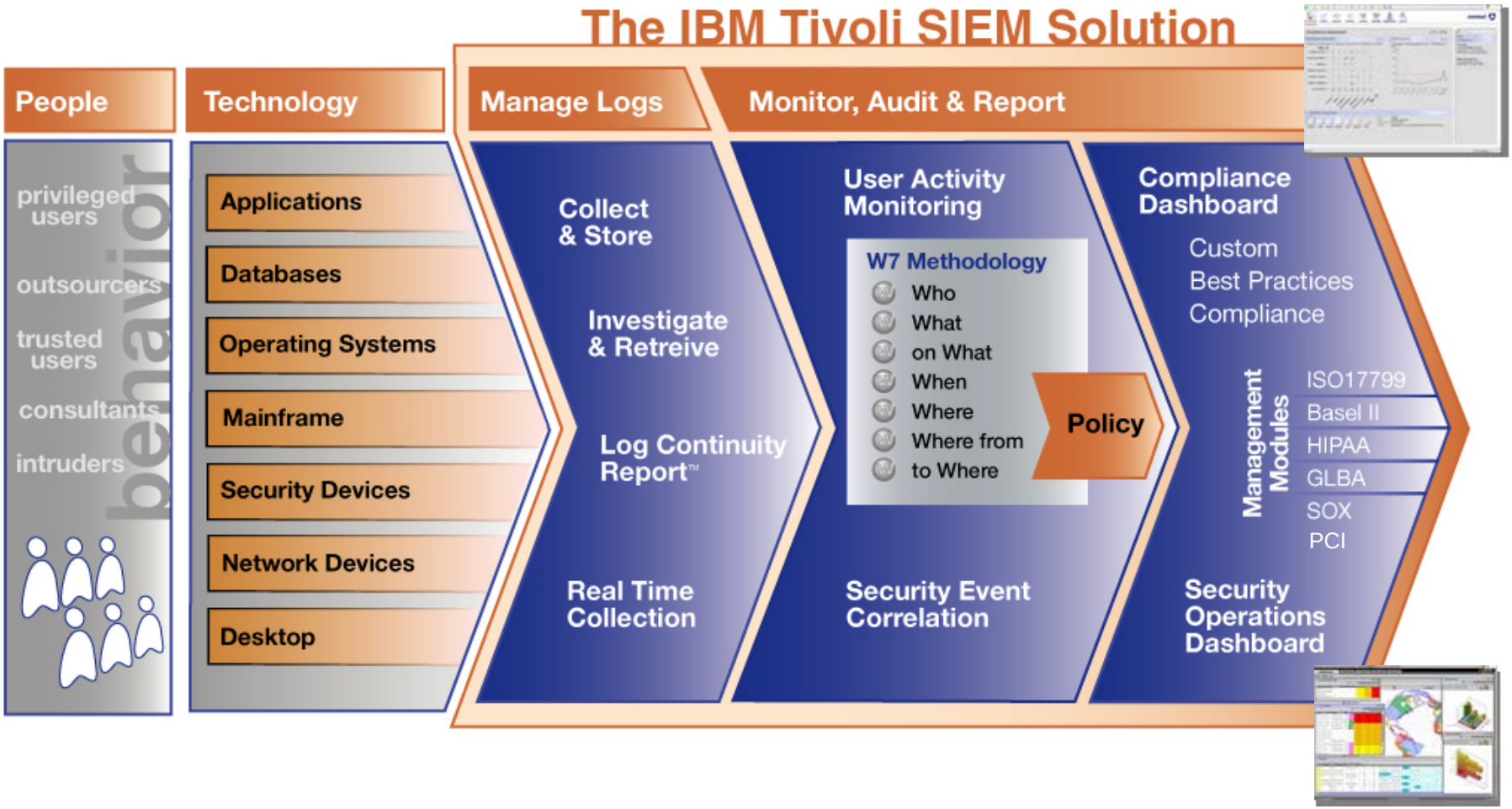
Tivoli Compliance InSight Manager (TCIM)

dans Tivoli Information and Event Management (TSIEM)

Quel est le comportement des utilisateurs sur mes systèmes et mes données sensibles?
… surtout les utilisateurs privilégiés!

Michael Cable,
Security Audit & Compliance champion
IBM Software Group, SouthWest Europe

Tivoli Security Information & Event Management TSIEM



Tivoli Security Information & Event Management TSIEM

	Opérations, IT & sécurité	Audit interne, Sécurité IT, Métier
Pour qui?		
Problèmes:	▪ Attaques & Alertes réseau ▪ Trop de données de sécurité ▪ Pondération des incidents	▪ Sécurité concernant les comportements ▪ Audit des utilisateurs privilégiés ▪ Reporting et Conformité
Solution:	**SEM: Security Event Mgmt** **Gestion des Incidents**	**SIM: Security Information Mgmt** **Audit et surveillance des activités des utilisateurs**
Produit:	**Security Operations Manager** 	**Compliance Manager** 

Ferez-vous la prochaine “Une” des journaux?

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Massive Insider Breach At DuPont

A research chemist who worked for DuPont for 10 years before accepting a job with a competitor downloaded 22,000 sensitive documents and viewed 16,706

The Delaware U.S. attorney on Thursday revealed a massive insider data breach at chemicals company DuPont where a former scientist late last year pleaded guilty to trying to steal $400 million worth of company trade secrets. He now faces up to a decade in prison, a fine of $250,000, and restitution when sentenced in March.

“Pour les sociétés, le meilleur moyen de prévenir les incidents internes est de **superviser les activités anormales lors d’accès au réseau et aux bases de données** et de déterminer un niveau d’utilisation acceptable pour différents types d’utilisateurs”

Source: InformationWeek, Février 15, 2007

Ce qui s’est passé:

- Employé quittant pour un concurrent
- Accède aux bases de données
- Transfère des documents sur son nouvel ordinateur portable

Commentaires du Carnegie Mellon CERT:

- “75% des … vols d’informations confidentielles étudiés… ont été perpétrés par des employés actifs”
- “45% d’entre eux avaient déjà accepté un nouvel emploi ailleurs”

Commentaires de la CIA:

- “…les concepteurs et les scientifiques ont tendance à considérer le capital intellectuel de leur entreprise comme le leur… et souhaitent le garder en partant”

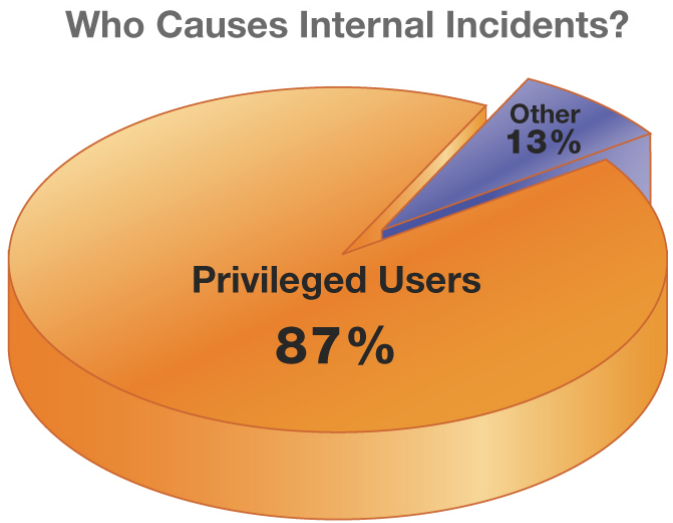
Surveiller les utilisateurs privilégiés n'est plus une option !

87% des incidents internes sont causés par des utilisateurs privilégiés

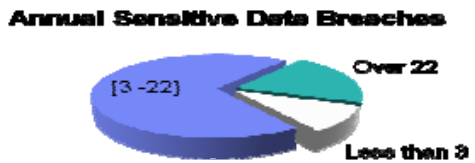
1. La plupart sont des **incidents non intentionnels** causés par la violation:
   - Des processus de gestion des changement
   - Des politiques d'utilisation acceptables
2. D'autres sont **malveillants**, les motifs étant:
   - Revanche (84%)
   - "Événements négatifs" (92%)

Quelle que soit leur raison, ces incidents coûtent trop chers et ne peuvent être ignorés:

- Les attaques internes représentent 6% du chiffre d'affaire annuel
- Aux USA, ceci représente un coût de 400 milliards de dollars



Source: USSS/CERT Insider Threat Survey 2005



Source: "Taking Action to Protect Sensitive Data," IT Policy Compliance Group, March 2007

Sources: Forrester research, IdM Trends 2006; USSS/CERT Insider Threat Survey 2005; CSI/FBI Survey, 2005; National Fraud Survey; CERT, various documents.

Les Challenges de Sécurité et de Conformité

- **Besoins de conformité** croissants
  - Initiatives de conformité toujours plus nombreuses
  - Besoins de mesurer la conformité à ses règles et pratiques internes
  - Surveillance et contrôles fiables sont nécessaires pour gérer les risques et éviter des pénalités ou la perte de business
- **Complexité** croissante
  - Les technologies et les infrastructures disparates fragmentent et alourdissent les efforts de supervision, de corrélation, d'analyse, et d'audit de conformité
  - Lier la conformité de l'infrastructure à celle du business est souhaitable, mais difficile
- **Coût** croissant
  - Main d'œuvre chère incite à l'automatisation
  - Peu de prédictibilité et de visibilité sur des infrastructures complexes conduit à une inflation rapide des coûts
  - Ne pas atteindre la conformité ou ne pas prévenir des menaces peu imposer des coûts énormes

43% of CFOs think that improving governance, controls and risk management is their top challenge.

CFO Survey: Current state & future direction, IBM Business Consulting Services

Les Régulateurs & Auditeurs créent l'urgence

[ISO17799:2005]
10.10.1 Audit logging

Audit logs recording user activities, exceptions, and information security events should be **produced and kept** for an agreed period to assist in future investigations and access control monitoring.

Mais l'utilité tactique est évidente

Le questionnaire “Security Audit and Compliance”

Questions de la Direction Informatique et du Métier:

- Pouvez vous surveiller si quelqu’un a touché ou modifié des données sensibles de manière inappropriée?
- Pouvez-vous vérifier si vos outsourcers gèrent vos systèmes et données de manière responsable?
- Disposez-vous de rapports sur les changements non autorisés sur votre environnement d’opérations?
- Etes-vous alerté quand des comptes administrateurs interdits sont créés?
- Avez-vous les moyens de détecter et d’investiguer des incidents sans délais?

Questions de vos auditeurs:

- Les journaux des vos application, databases, OS et dispositifs réseaux sont-ils archivés et analysés?
- Les activités de vos administrateurs et opérateurs système sont-ils enregistrés et analysés régulièrement?
- Archivez-vous tous les accès aux données sensibles – incluant les accès root/administrateur et DBA?
- Avez-vous des outils automatisés pour analyser les enregistrements d’audit?
- Les incidents de sécurité et les activités suspectes sont-ils analysés, investigués? Et les actions de remédiations sont-elles prises?

Que font les utilisateurs sur mes systèmes et données sensibles?

Comprendre

Comparer le comportement "Désiré"

au comportement "Réel".

Est-il "conforme"?

Gestion des Logs de toutes les plateformes

Capturer

Fonctionnalités:

- Capture sécurisée et fiable de n'importe quelle plate-forme
- Support complet pour collecte de logs natifs (Syslogs, audit trails, SNMP, LDAP, Active Directory, etc.)
- Archivage dans un dépôt efficace et compressé
- Accéder aux informations à la demande
- Recherche à travers tous les logs
- Rapports prouvant la collecte correcte

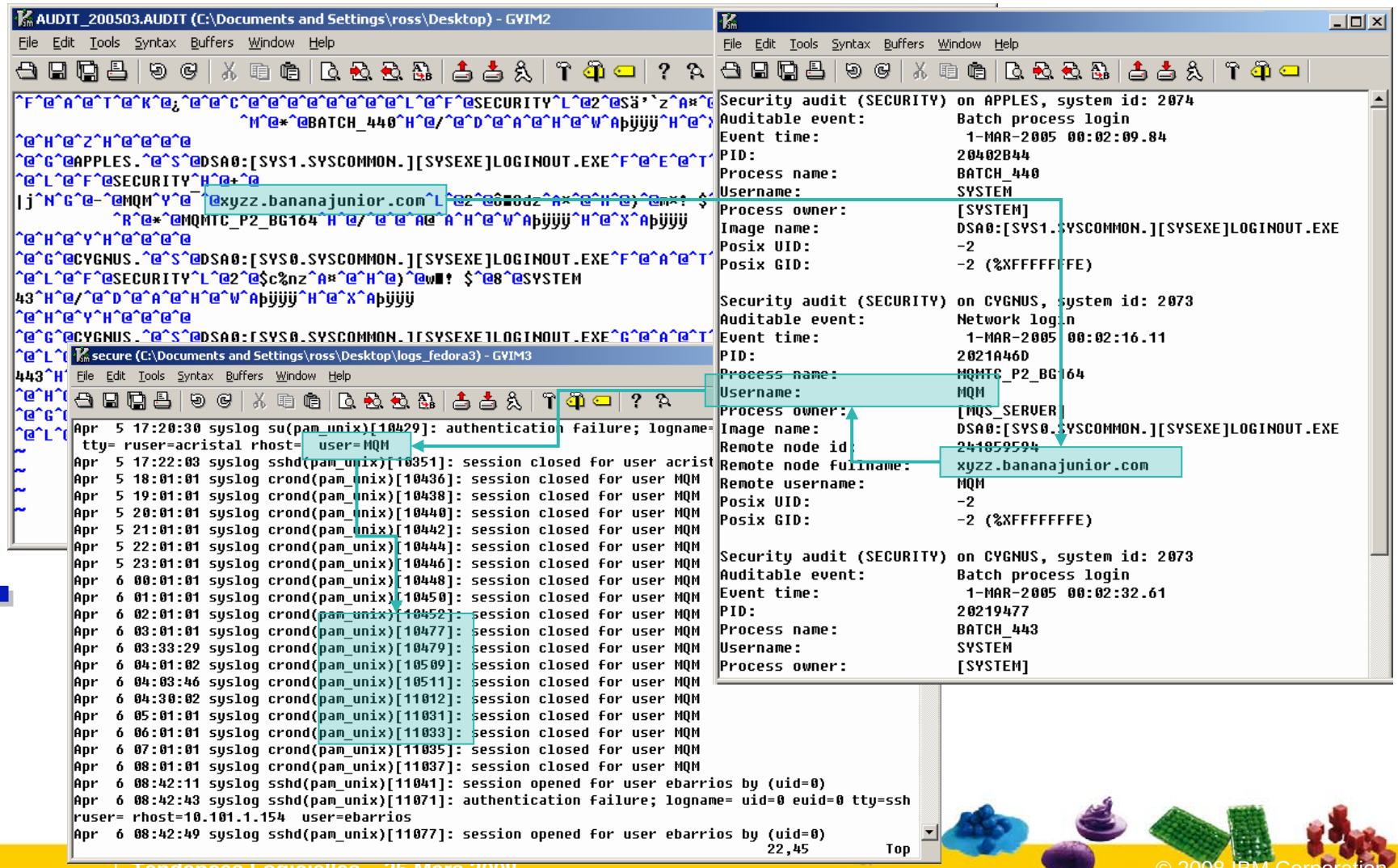
Avantages:

- Réduction de coûts par l'automatisation et la centralisation de la collecte et de l'archivage
- Réduire la longueur des audits internes ou externes.

Implementation: "plug and play"

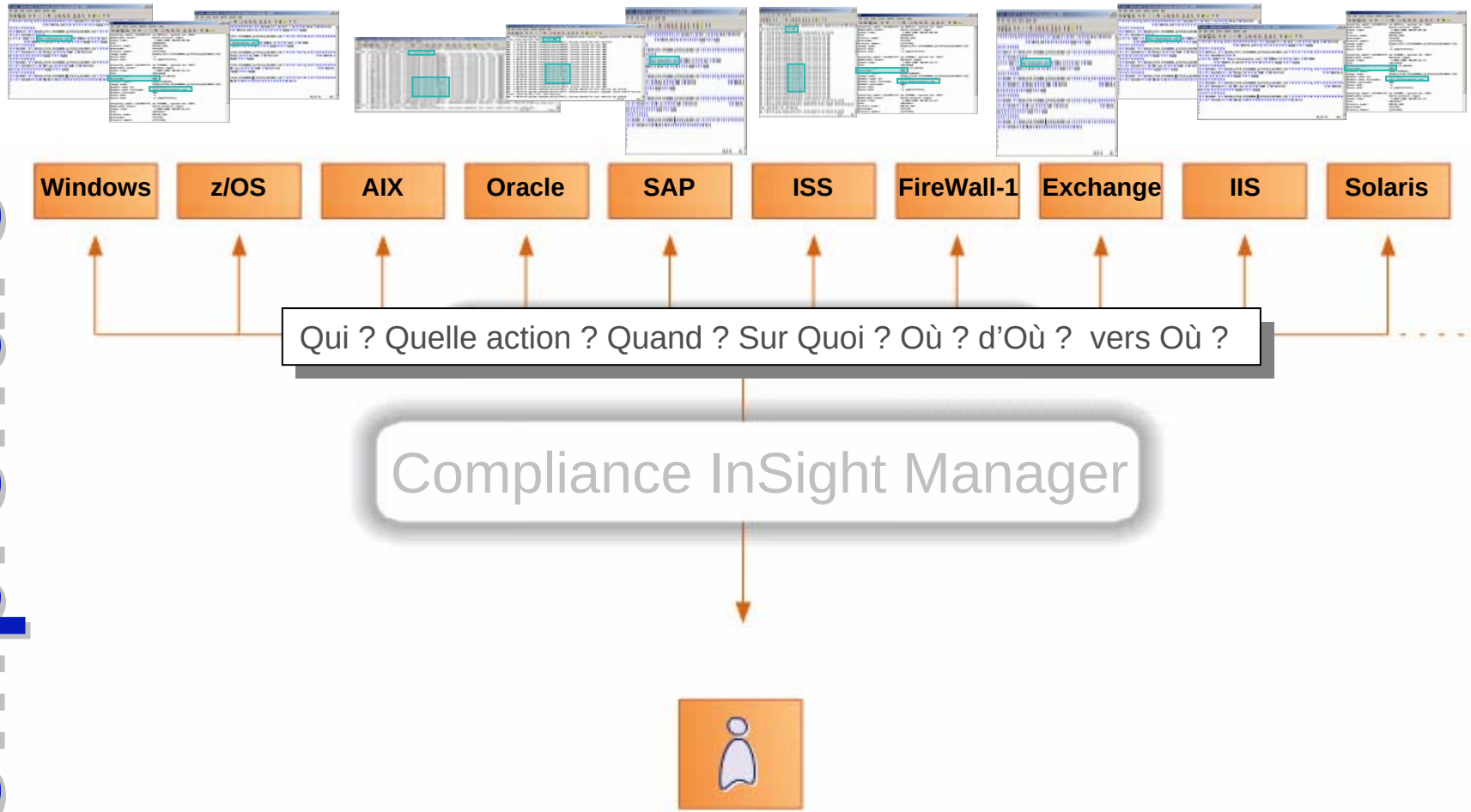
Comment comprendre tous ces différents formats et informations contenus dans les logs?

Comprendre



Tous les journaux sont traduits en un même langage

Comprendre



Utiliser un langage compréhensible pour le métier, le management et les auditeurs: **la méthodologie W7**

Comprendre

1. **Who** did
2. **What** type of action
3. **on What** file/data
4. **When** did he do it and
5. **Where**
6. **from Where**
7. **Where to**

- **Qui ?**
- **Quelle action ?**
- **Sur Quoi ?**
- **Quand ?**
- **Où ?**
- **d'Où ?**
- **vers Où ?**

Nous faisons le travail de traduction,
à votre place!

Tableau de Bord de Conformité
Des milliards de journaux résumés dans un graphique de vision générale, en langage W7

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Favorites Media

Address

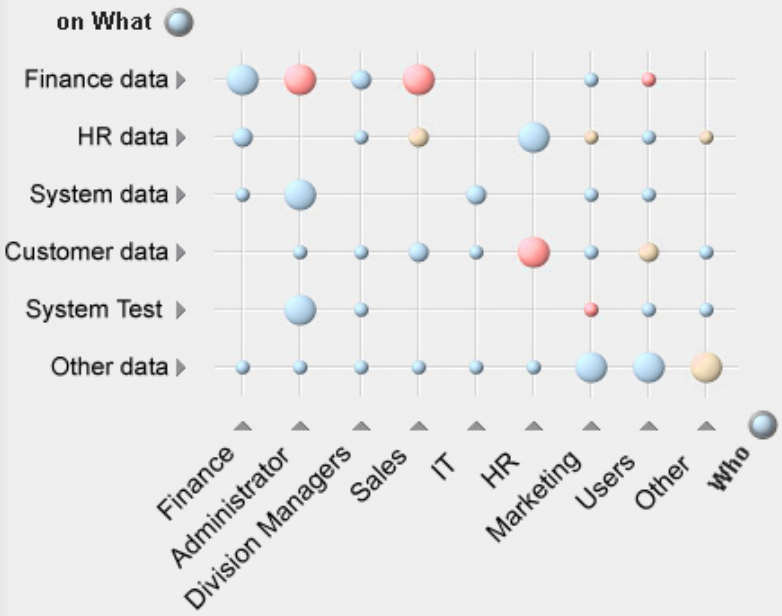
Dashboard | Trends | Reports | Policies | Groups | Settings | Regulations | Log off

Compliance Dashboard

Enterprise Overview

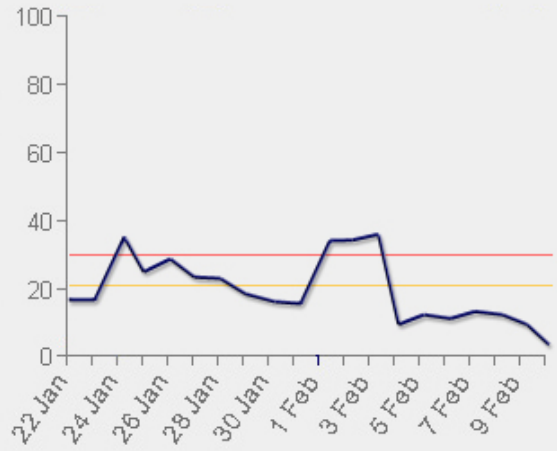
Settings

Database AGGRDB on Server CEA45 by "on What" / "Who" for Jan 22, 2004 till Mar 11, 2004



Trend graphic

Settings



Database Overview

Name: AggrDb
Status: loaded
Loading date:
Content:

Info

Actions

Where do you want to go:
- View SOX Compliance report
- Adjust SOX Policy
- Adjust SOX Classification
- View SOX list of Reports
- View SOX Archived Logfiles
- Adjust your personal settings

Resources

- Whitepaper Consul InSight and GLBA
- Whitepaper Consul InSight and ISO17799
- Official Regulations of GLBA
- Official Regulations of ISO17799
- Official Regulations of Sarbanes-Oxley
- implementation by FIECC

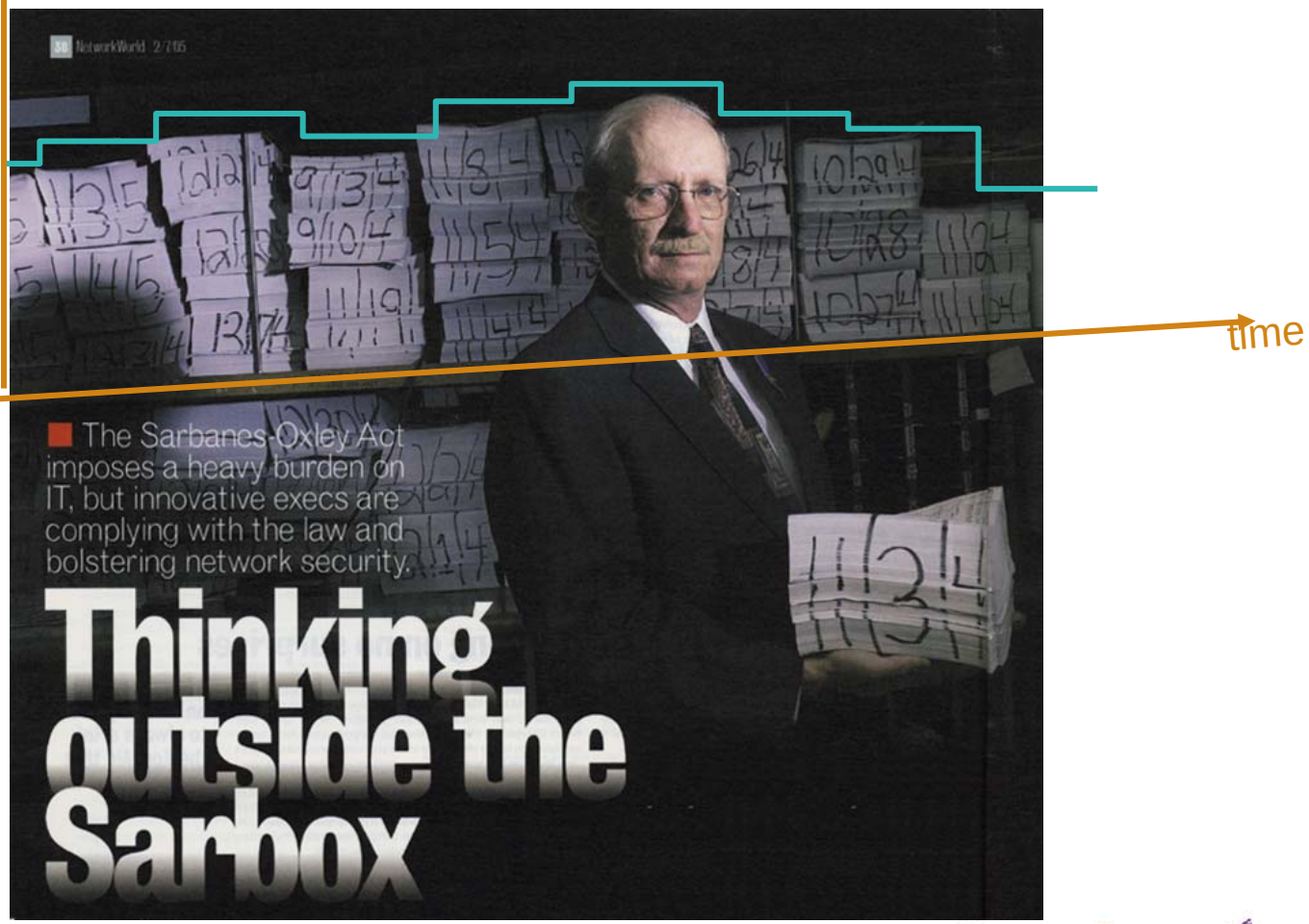
Websites

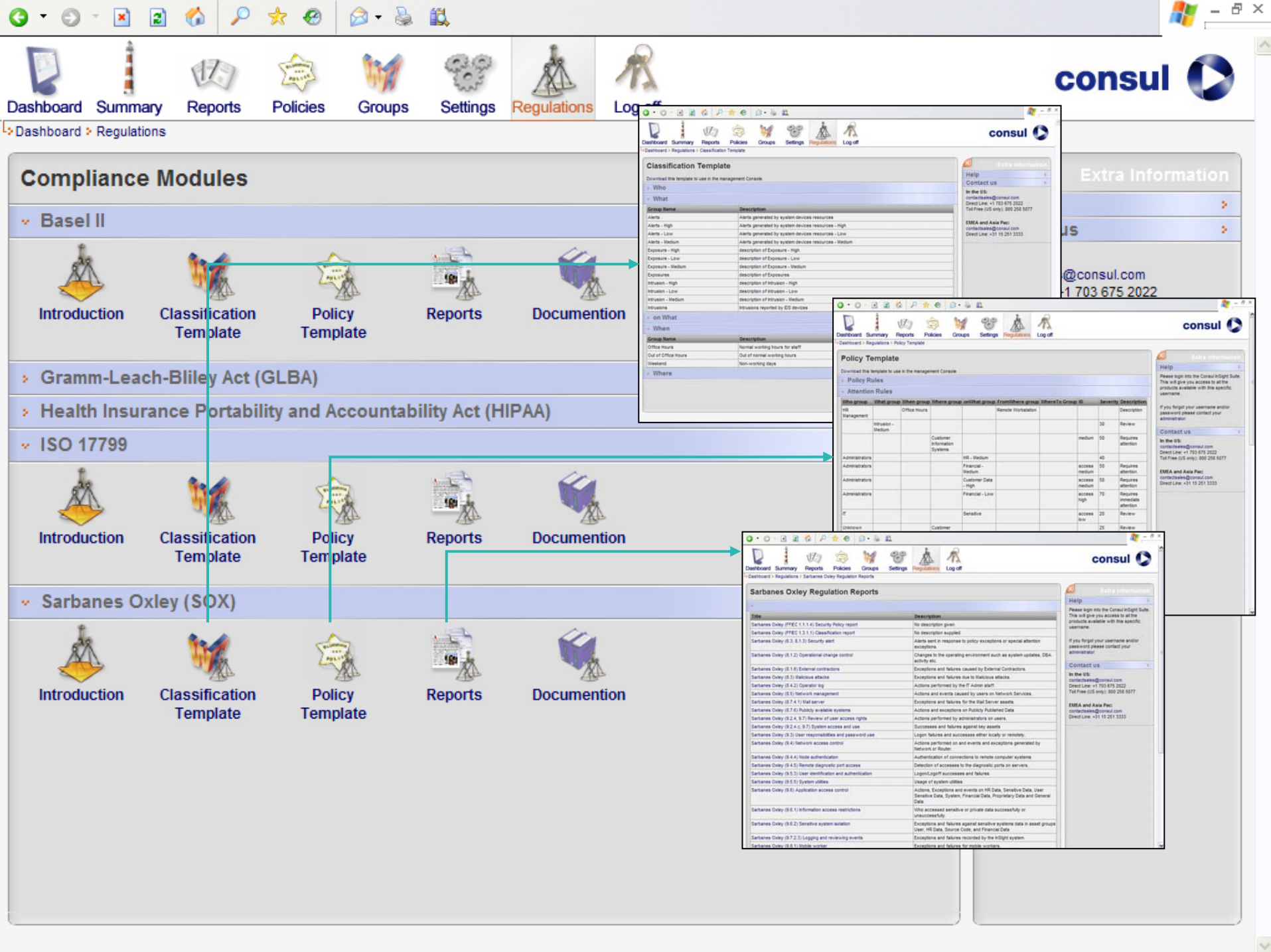
- The Consul Website
- Consul InSight Security Manager
- Sarbanes-Oxley
- ISO 17799: Official site
- ISO 17799: the Webnewsletter
- ISO 17799: British Standard

Trusted sites

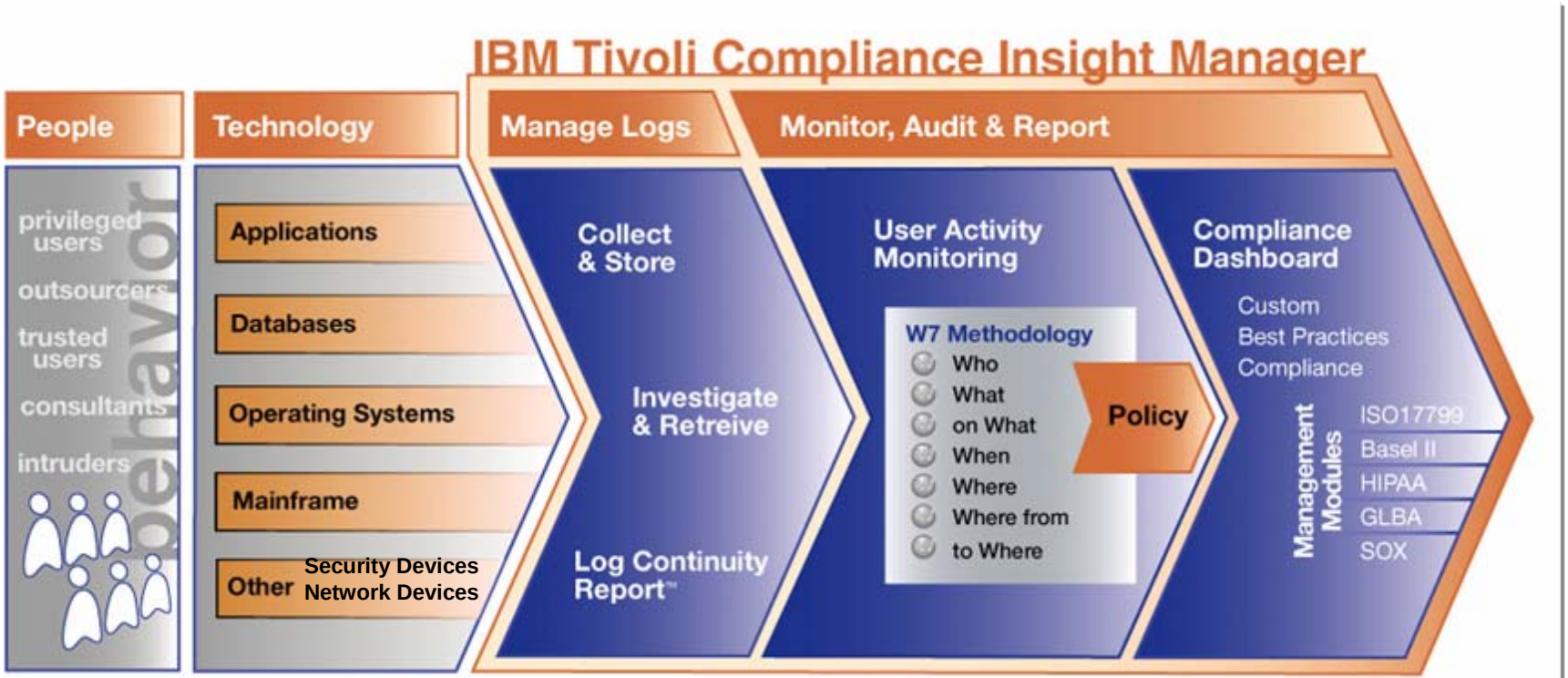
Des rapports, automatiques et tout prêts, pour communiquer

Communiquer




Dashboard
Summary
Reports
Policies
Groups
Settings
Regulations
Log off
consul
Dashboard › Regulations
Compliance Modules
Basel II
Introduction
Classification Template
Policy Template
Reports
Documention
Gramm-Leach-Bliley Act (GLBA)
Health Insurance Portability and Accountability Act (HIPAA)
ISO 17799
Introduction
Classification Template
Policy Template
Reports
Documention
Sarbanes Oxley (SOX)
Introduction
Classification Template
Policy Template
Reports
Documention
Extra Information
@consul.com
1 703 675 2022
Classification Template
Policy Template
Sarbanes Oxley Regulation Reports

Quel est le comportement de mes utilisateurs sur mes données sensibles? Comment le prouver?



InSight consolide toute l'information contenue dans les journaux des serveurs, databases et applications de l'entreprise, et rapporte toute exception aux politiques et comportements acceptables.

TEC - Technical Exploration Center - @ Paris

Accélérer le cycle de découverte des logiciels IBM

Les ressources hardware et software du TEC
à Noisy-Le Grand / Marne La Vallée
sont disponibles <u>gratuitement</u> :

une adresse E-mail à retenir:
TecParis@fr.ibm.com

- EOTs - Exploration of Technology
  - Découvrir la valeur des logiciels IBM: Présentations, vidéos, démonstrations
- POTs – Proof of Technology, Ateliers/Workshops,
  - Démontrer les capacités des logiciels IBM
    - Présentations
    - Labs et hands-on …