IBM

Michael Cable

Centraliser toutes les informations de sécurité de l'entreprise pour supervision et conformité

TENDANCES LOGICIELLES D'ÉTÉ 2008

SESSION SPÉCIALE GESTION DES RISQUES OPÉRATIONNELS

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

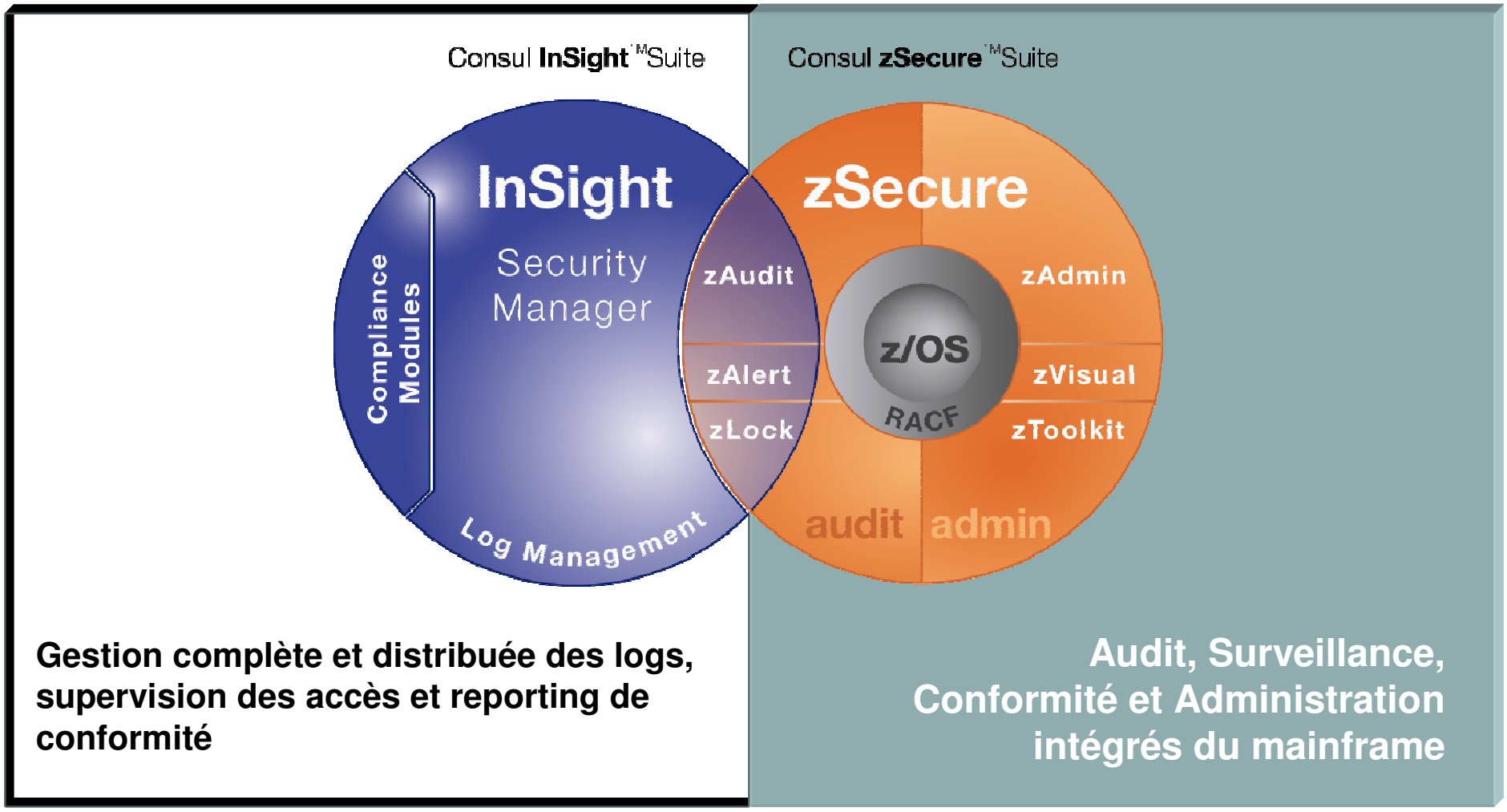
Commentaires du Carnegie Mellon CERT:

- “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”

Supervision sur toutes les plate-formes



Gestion complète et distribuée des logs, supervision des accès et reporting de conformité

Audit, Surveillance, Conformité et Administration intégrés du mainframe

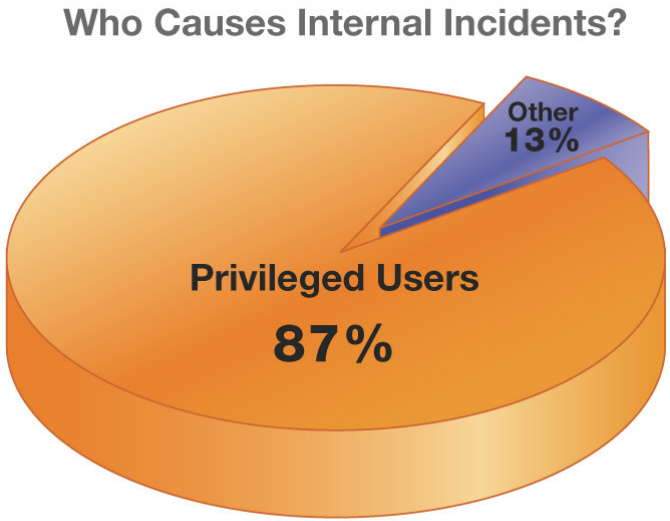
Surveiller les utilisateurs privilégiés n'est plus une option !

87% des incidents internes sont causés par des utilisateurs privilégiés

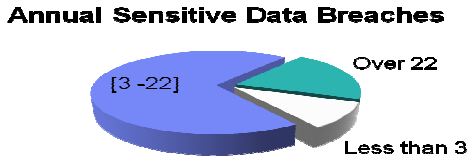
1. La plupart sont des **incidents non intentionnels** causés par la violation:
   - Des processus de gestion des changement
   - Des politiques d'utilisation acceptables
2. D'autres sont **malveillants**, les motifs étant:
   - Revanche (84%)
   - "Événements négatifs" (92%)

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.

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 crédibilité.

- **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.

Et l'utilité tactique est évidente

Le questionnaire “Security Audit and Compliance”

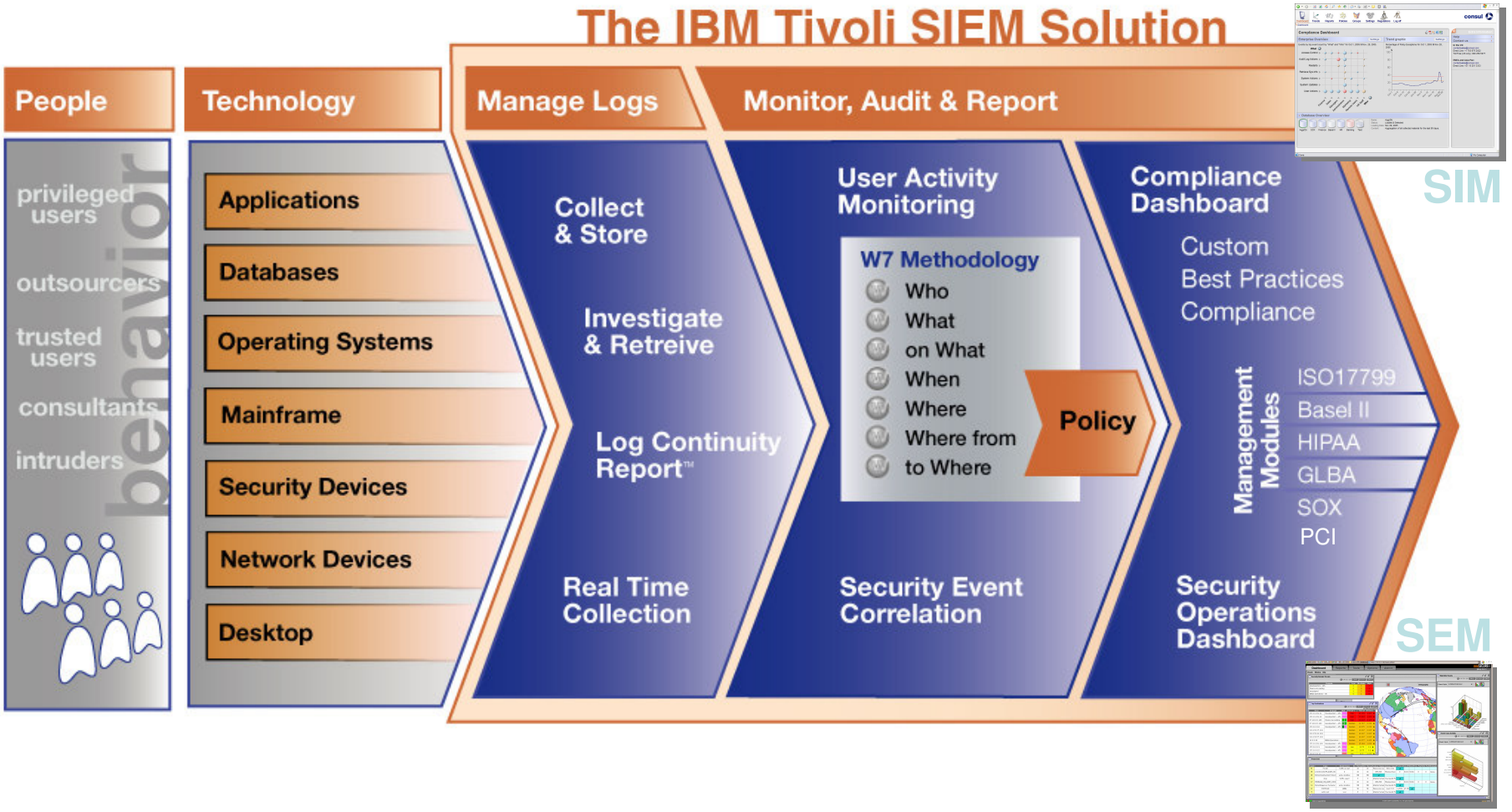
Questions de la Direction Informatique et du Métier:

- 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?

Tivoli Security Information & Event Management
TSIEM



Security Information and Event Management

SIEM = SEM + SIM

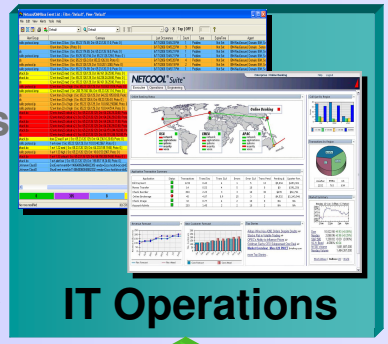
Gestion des Incidents

Aggregation, Correlation

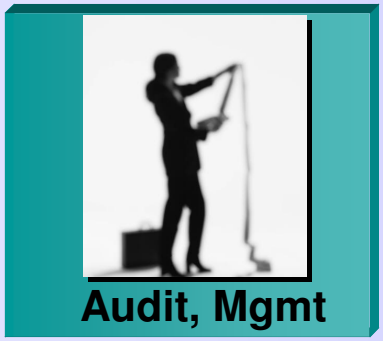
Real-time Threat & Incident Handling

SOC dashboard

Operational reports



IT Operations



Audit, Mgmt

Supervision Utilisateurs

Policy Evaluation and enforcement

Compliance Dashboard

Historical Analysis

Audit reports, exception alert

Security Ops (SOC)

Rules-based

IP address

SEM

SIM

IT Security Internal Audit

Policy-based

Who?

Syslogs, SNMP traps, …

Audit trails, extended ecurity events, …

Network Infrastructure

Network Security

Desktops

Servers

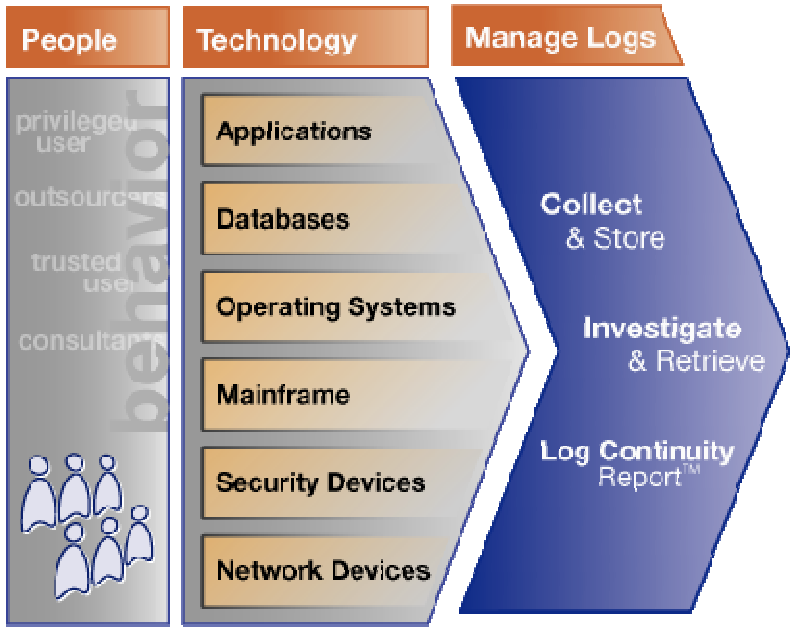
Applications

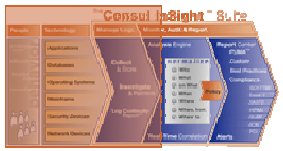
Databases

User focused log sources

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

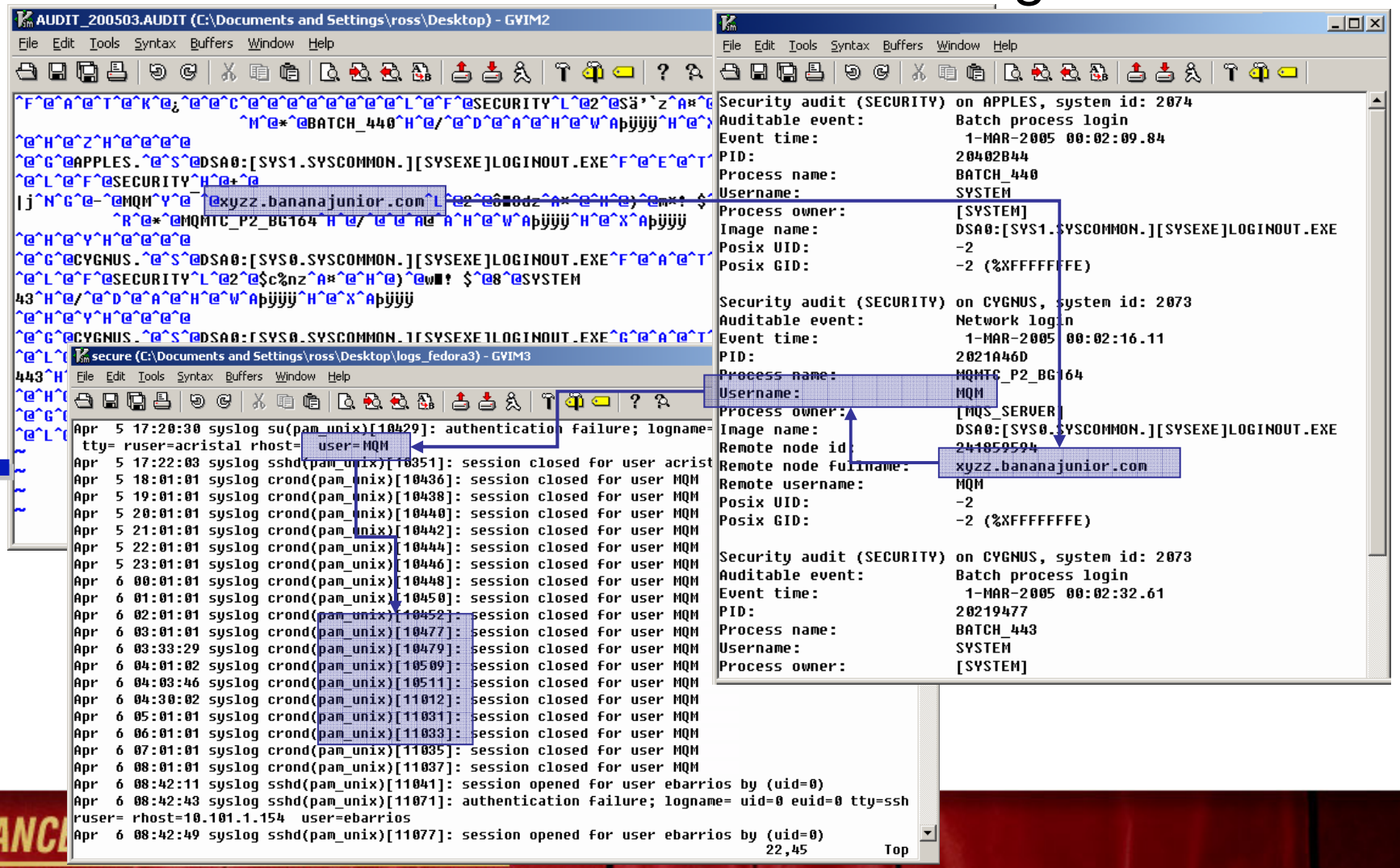
Avantages:

- 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"

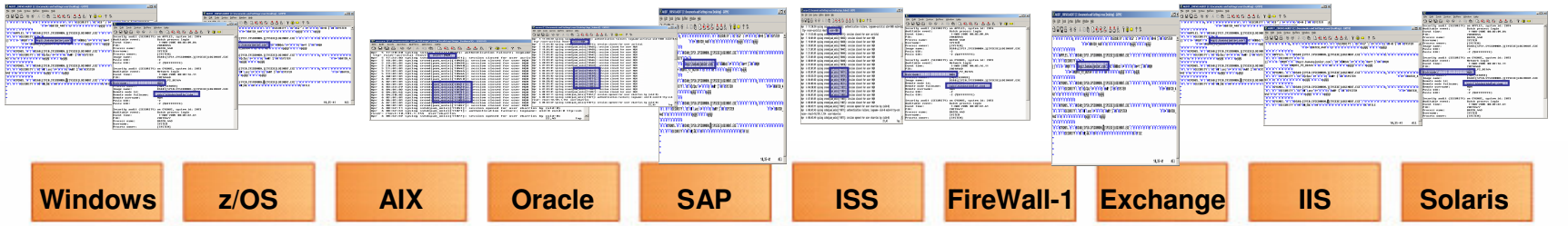
Comment comprendre tous ces différents formats et informations contenus dans les logs?

Comprendre



Tous les journaux sont traduits en un même langage

Comprendre



Windows | z/OS | AIX | Oracle | SAP | ISS | FireWall-1 | Exchange | IIS | Solaris

Traduire les logs en "Français"

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

Compliance InSight Manager

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

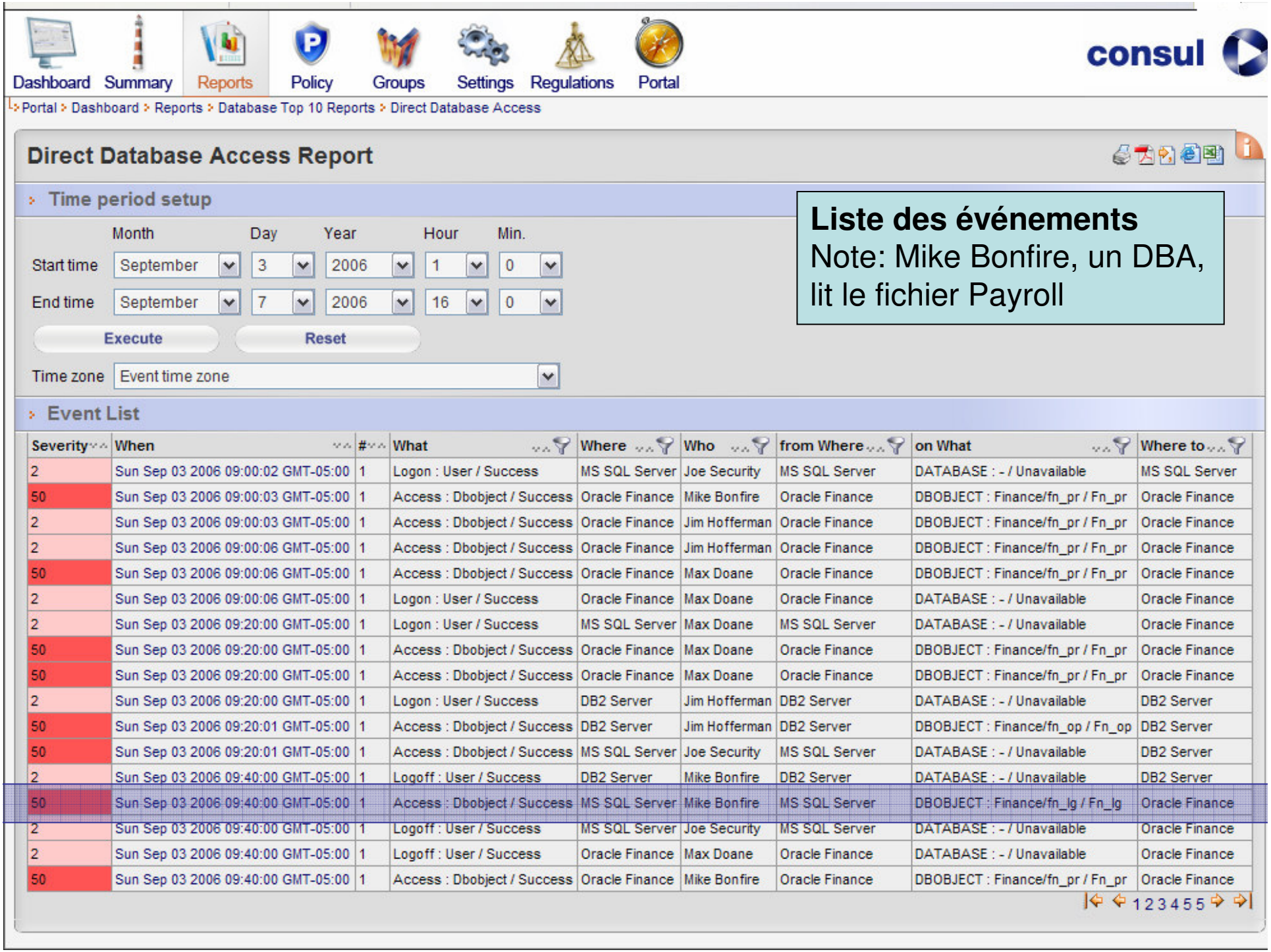
Comprendre

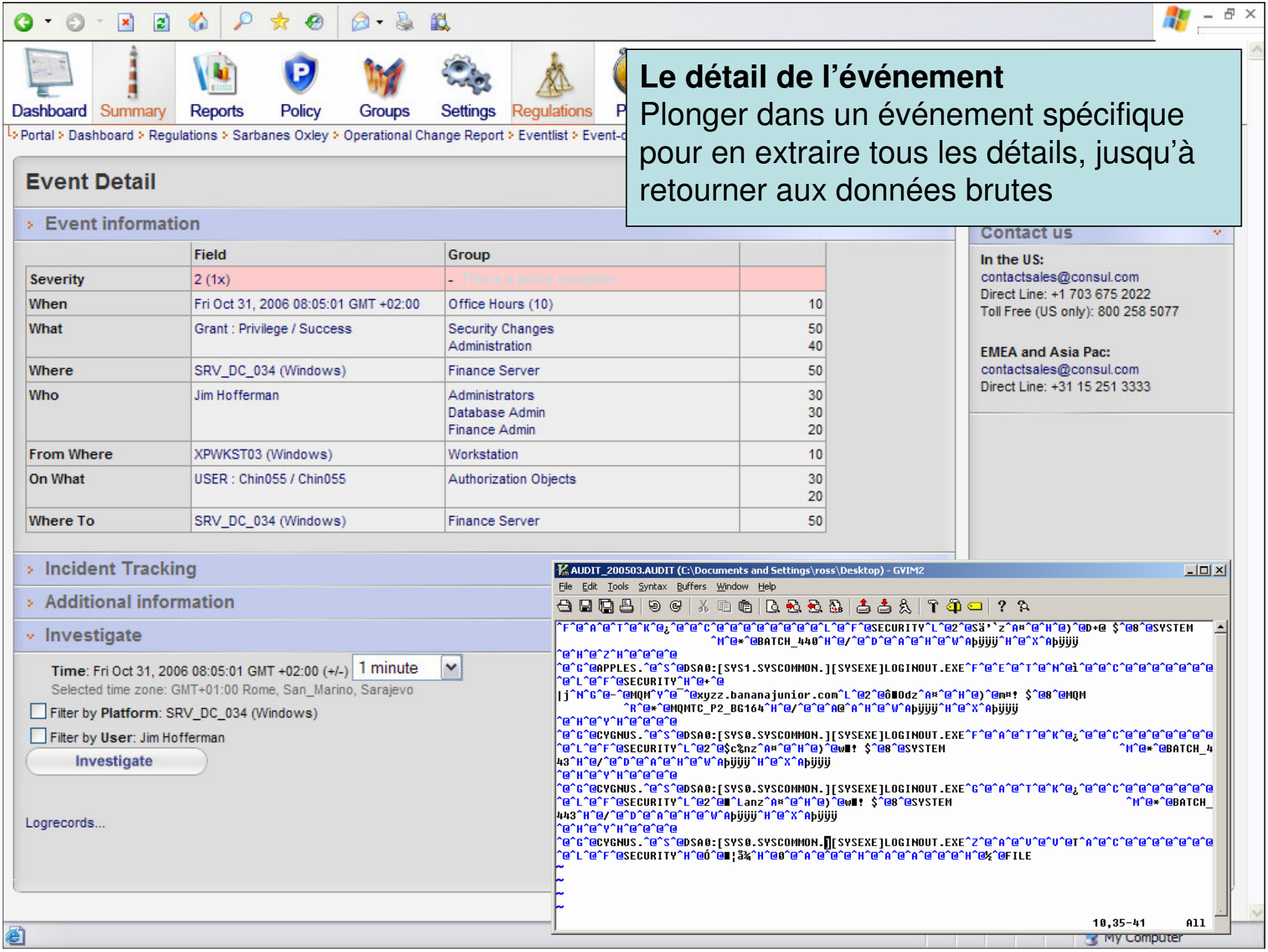
1. **Who** did
2. **What** type of action
3. **on What** file/data
4. **When** did he do it and
5. **Where**
6. **from Where**
7. **Where to**

1. **Qui ?**
2. **Quelle action ?**
3. **Sur Quoi ?**
4. **Quand ?**
5. **Où ?**
6. **d'Où ?**
7. **vers Où ?**

Nous faisons le travail de traduction, à votre place!

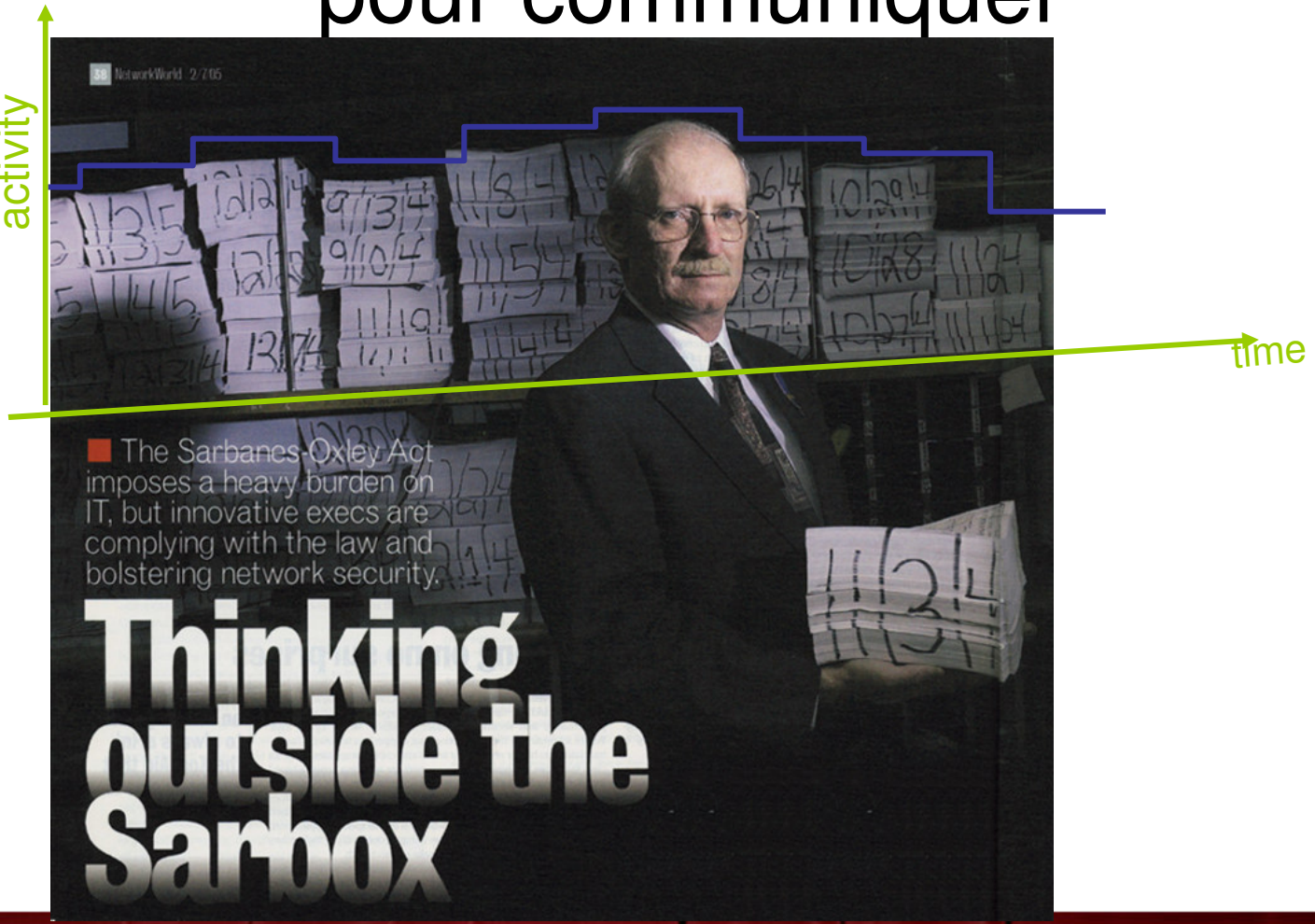
Tableau de Bord de Conformité
Des milliards de journaux résumés dans un graphique de vision générale, en langage W7

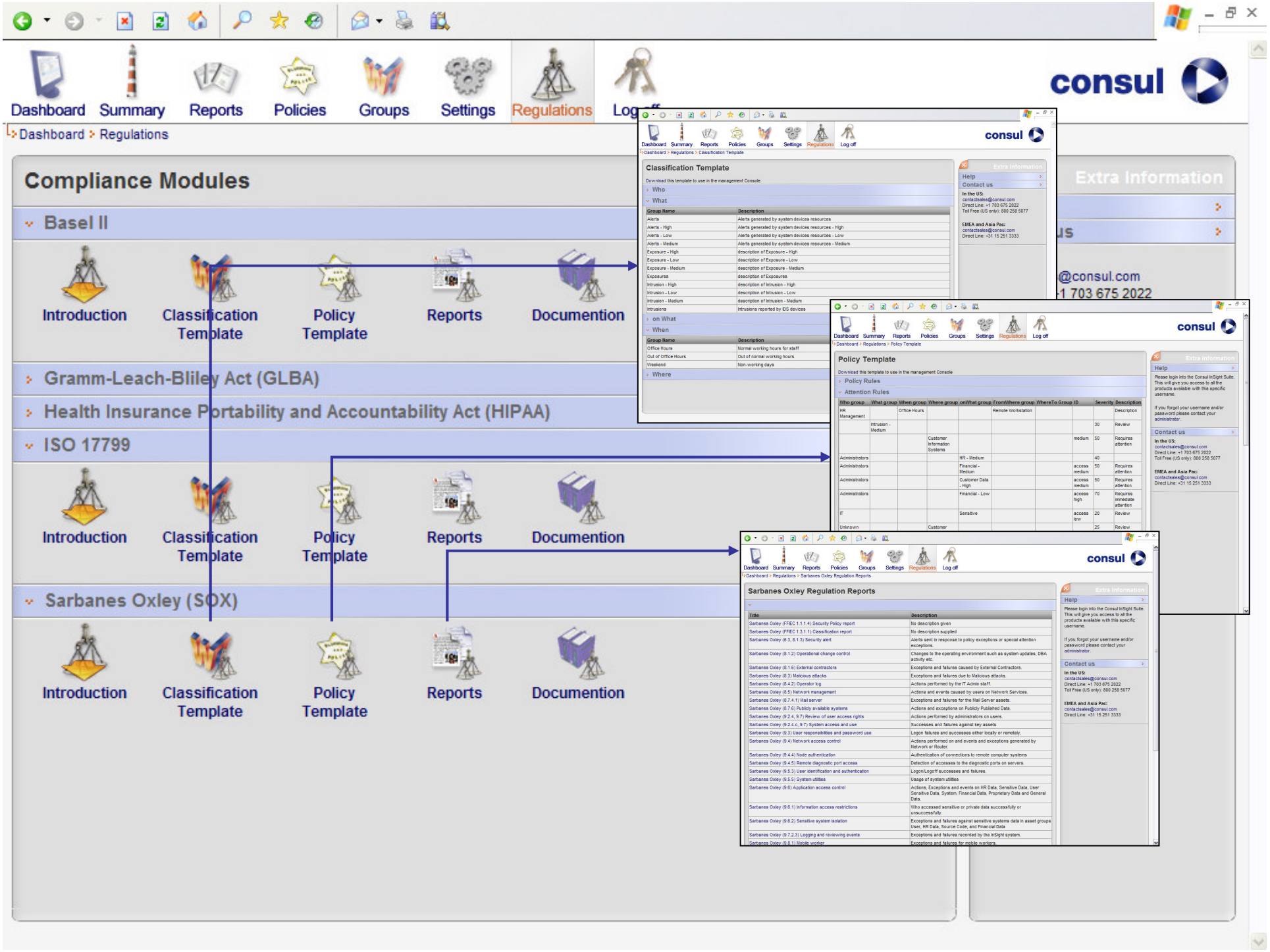

Dashboard
Summary
Reports
Policy
Groups
Settings
Regulations
Portal
consul
Portal > Dashboard > Reports > Database Top 10 Reports > Direct Database Access
Direct Database Access Report
Time period setup
Month
Day
Year
Hour
Min.
Start time
September
3
2006
1
0
End time
September
7
2006
16
0
Execute
Reset
Time zone
Event time zone
Liste des événements
Note: Mike Bonfire, un DBA, lit le fichier Payroll
Event List
Severity
When
#
What
Where
Who
from Where
on What
Where to
2 Sun Sep 03 2006 09:00:02 GMT-05:00 1 Logon : User / Success MS SQL Server Joe Security MS SQL Server DATABASE : - / Unavailable MS SQL Server
50 Sun Sep 03 2006 09:00:03 GMT-05:00 1 Access : Dbobject / Success Oracle Finance Mike Bonfire Oracle Finance DBOBJECT : Finance/fn_pr / Fn_pr Oracle Finance
2 Sun Sep 03 2006 09:00:03 GMT-05:00 1 Access : Dbobject / Success Oracle Finance Jim Hofferman Oracle Finance DBOBJECT : Finance/fn_pr / Fn_pr Oracle Finance
2 Sun Sep 03 2006 09:00:06 GMT-05:00 1 Access : Dbobject / Success Oracle Finance Jim Hofferman Oracle Finance DBOBJECT : Finance/fn_pr / Fn_pr Oracle Finance
50 Sun Sep 03 2006 09:00:06 GMT-05:00 1 Access : Dbobject / Success Oracle Finance Max Doane Oracle Finance DBOBJECT : Finance/fn_pr / Fn_pr Oracle Finance
2 Sun Sep 03 2006 09:00:06 GMT-05:00 1 Logon : User / Success Oracle Finance Max Doane Oracle Finance DATABASE : - / Unavailable Oracle Finance
2 Sun Sep 03 2006 09:20:00 GMT-05:00 1 Logon : User / Success MS SQL Server Max Doane MS SQL Server DATABASE : - / Unavailable Oracle Finance
50 Sun Sep 03 2006 09:20:00 GMT-05:00 1 Access : Dbobject / Success Oracle Finance Max Doane Oracle Finance DBOBJECT : Finance/fn_pr / Fn_pr Oracle Finance
50 Sun Sep 03 2006 09:20:00 GMT-05:00 1 Access : Dbobject / Success Oracle Finance Max Doane Oracle Finance DBOBJECT : Finance/fn_pr / Fn_pr Oracle Finance
2 Sun Sep 03 2006 09:20:00 GMT-05:00 1 Logon : User / Success DB2 Server Jim Hofferman DB2 Server DATABASE : - / Unavailable DB2 Server
50 Sun Sep 03 2006 09:20:01 GMT-05:00 1 Access : Dbobject / Success DB2 Server Jim Hofferman DB2 Server DBOBJECT : Finance/fn_op / Fn_op DB2 Server
50 Sun Sep 03 2006 09:20:01 GMT-05:00 1 Access : Dbobject / Success MS SQL Server Joe Security MS SQL Server DATABASE : - / Unavailable DB2 Server
2 Sun Sep 03 2006 09:40:00 GMT-05:00 1 Logoff : User / Success DB2 Server Mike Bonfire DB2 Server DATABASE : - / Unavailable DB2 Server
50 Sun Sep 03 2006 09:40:00 GMT-05:00 1 Access : Dbobject / Success MS SQL Server Mike Bonfire MS SQL Server DBOBJECT : Finance/fn_lg / Fn_lg Oracle Finance
2 Sun Sep 03 2006 09:40:00 GMT-05:00 1 Logoff : User / Success MS SQL Server Joe Security MS SQL Server DATABASE : - / Unavailable Oracle Finance
2 Sun Sep 03 2006 09:40:00 GMT-05:00 1 Logoff : User / Success Oracle Finance Max Doane Oracle Finance DATABASE : - / Unavailable Oracle Finance
50 Sun Sep 03 2006 09:40:00 GMT-05:00 1 Access : Dbobject / Success Oracle Finance Mike Bonfire Oracle Finance DBOBJECT : Finance/fn_pr / Fn_pr Oracle Finance
1 2 3 4 5 5


Le détail de l'événement
Plonger dans un événement spécifique pour en extraire tous les détails, jusqu'à retourner aux données brutes
Dashboard
Summary
Reports
Policy
Groups
Settings
Regulations
Portal › Dashboard › Regulations › Sarbanes Oxley › Operational Change Report › Eventlist › Event-d
Event Detail
Event information
Field
Group
Severity
2 (1x)
- This is a policy exception
When
Fri Oct 31, 2006 08:05:01 GMT +02:00
Office Hours (10)
10
What
Grant : Privilege / Success
Security Changes
Administration
50
40
Where
SRV_DC_034 (Windows)
Finance Server
50
Who
Jim Hofferman
Administrators
Database Admin
Finance Admin
30
30
20
From Where
XPWKST03 (Windows)
Workstation
10
On What
USER : Chin055 / Chin055
Authorization Objects
30
20
Where To
SRV_DC_034 (Windows)
Finance Server
50
Contact us
In the US:
contactsales@consul.com
Direct Line: +1 703 675 2022
Toll Free (US only): 800 258 5077
EMEA and Asia Pac:
contactsales@consul.com
Direct Line: +31 15 251 3333
Incident Tracking
Additional information
Investigate
Time: Fri Oct 31, 2006 08:05:01 GMT +02:00 (+/-)
1 minute
Selected time zone: GMT+01:00 Rome, San_Marino, Sarajevo
Filter by Platform: SRV_DC_034 (Windows)
Filter by User: Jim Hofferman
Investigate
Logrecords...
AUDIT_200503.AUDIT (C:\Documents and Settings\ross\Desktop) - GVIM2
File Edit Tools Syntax Buffers Window Help
10,35-41 All
My Computer

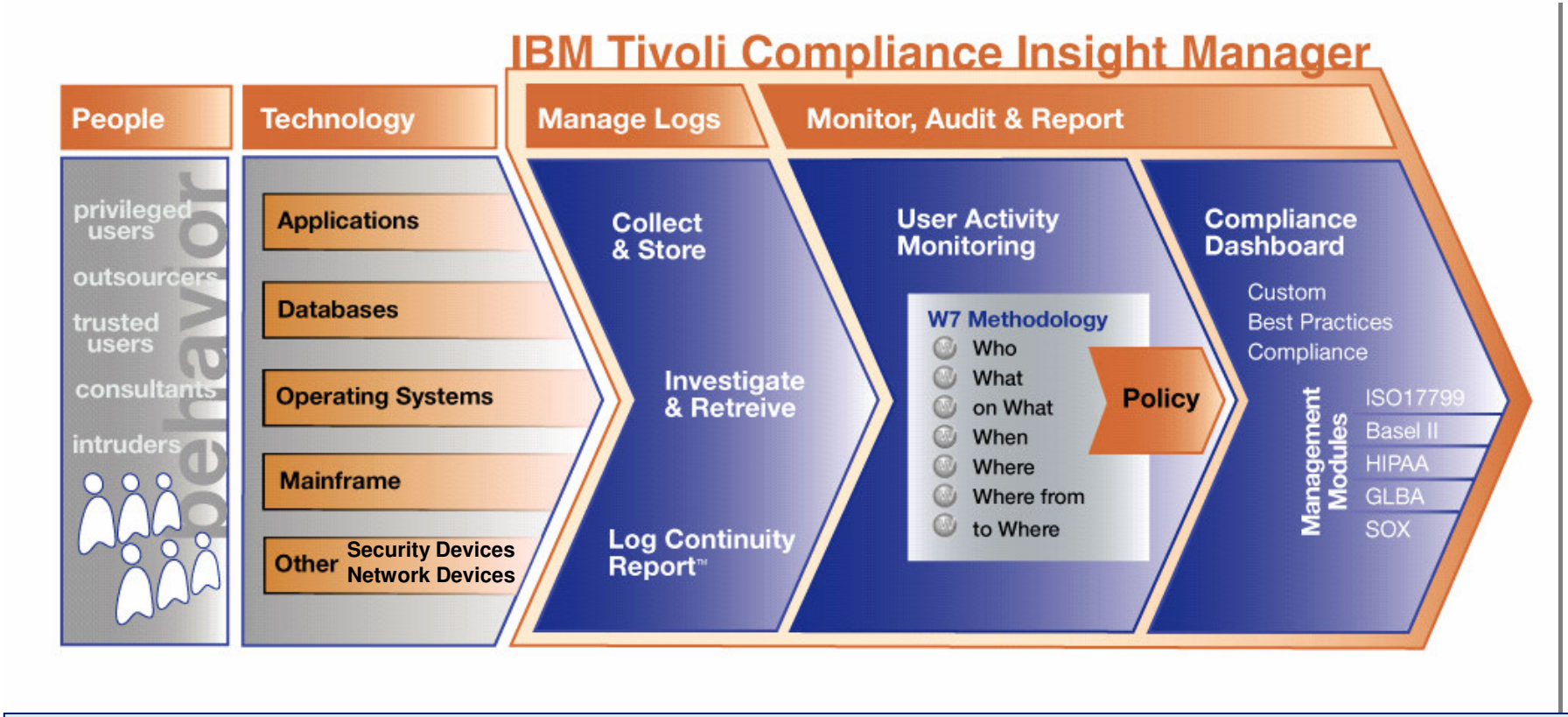
Des rapports, automatiques et tout prêts, pour communiquer

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 …