Tivoli software

Security Audit and Compliance

IBM's SIEM solution:
Tivoli Security Information and Event Management

Michael Cable
IBM SIEM Specialist
SouthWest Europe

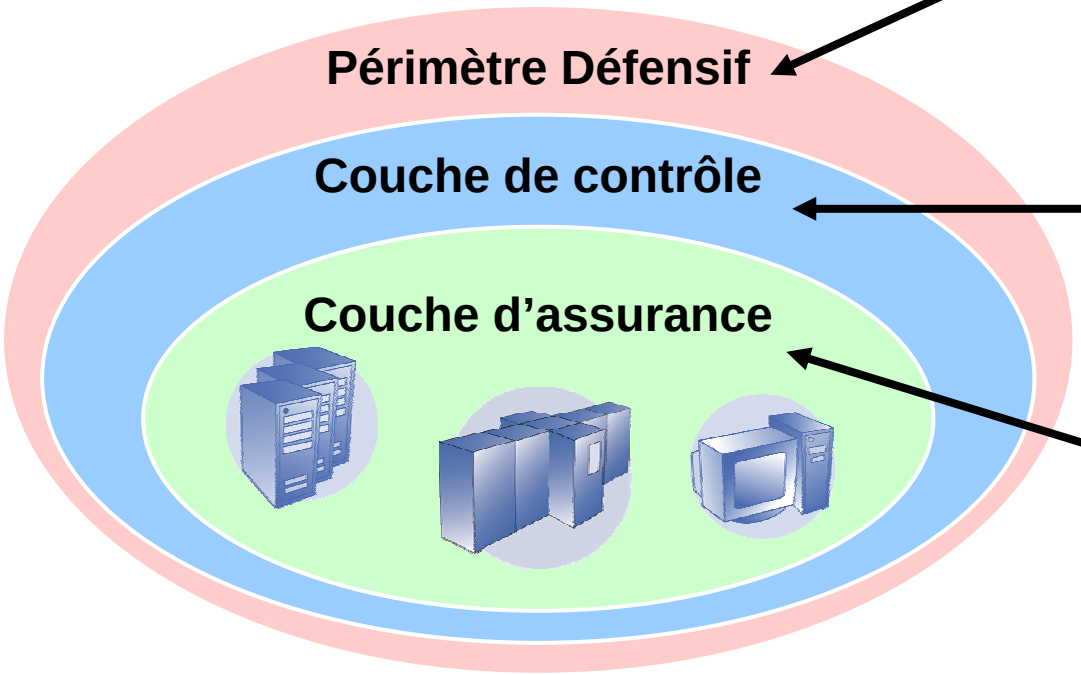
Security Compliance & Audit Solutions

IBM

Agenda

- Présentation de l'Offre Tivoli Security
- Les Challenges de l'Audit et de la Conformité
- SEM versus SIM
- La solution: IBM Tivoli's SIEM
- Architecture
- IBM Value Proposition
- Proven Results
- Questions

IBM et Tivoli sécurité : assurer la sécurité à tous les niveaux



Périmètre défensif

Fermer la porte aux intrus avec:

- Firewalls
- Anti-Virus
- Détection d'intrusion, etc.

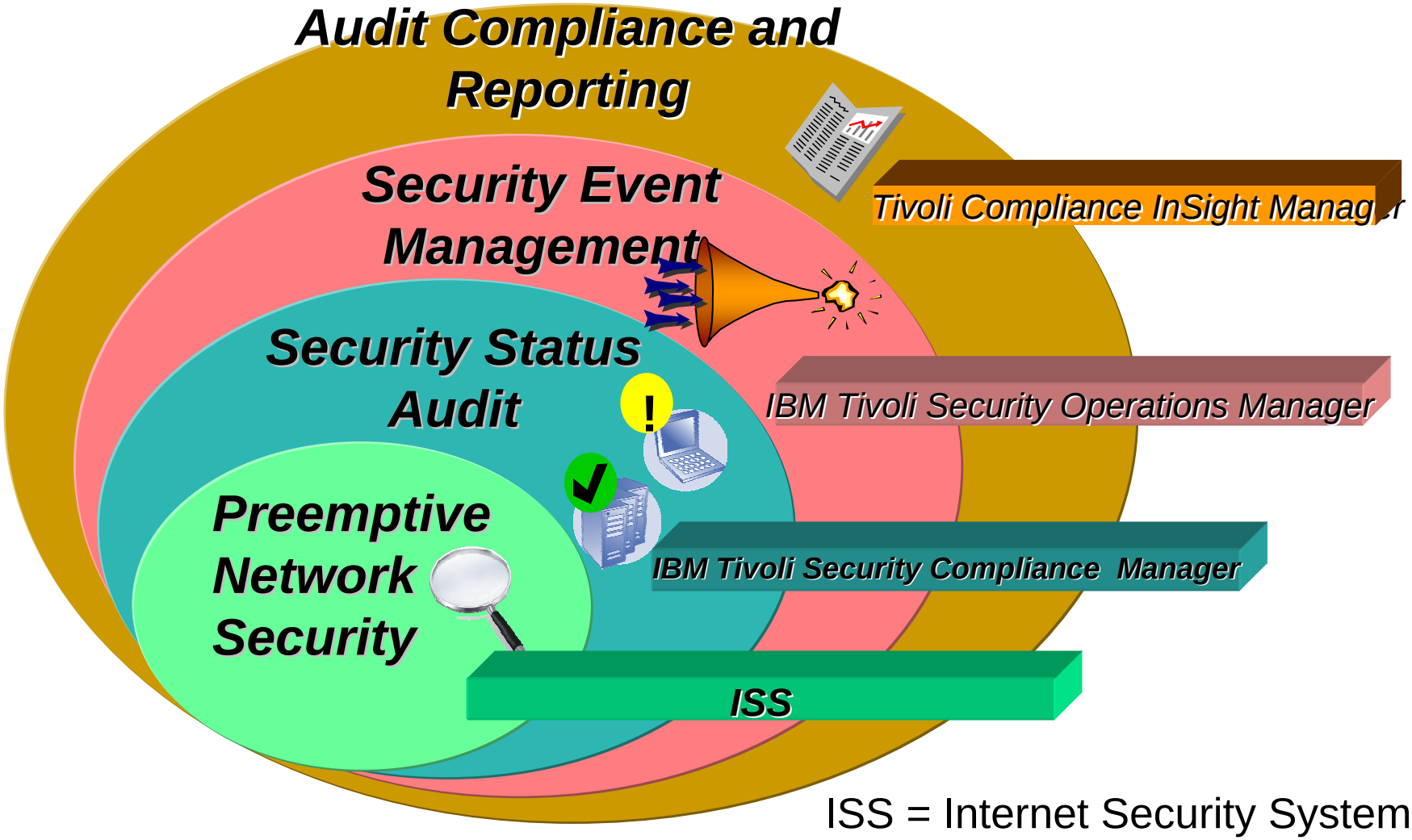
Couche de contrôle

- Qui peut entrer?
- Que peuvent-ils voir et faire?
- Accès liés aux rôles?
- Protection de la vie privée?

Couche d'assurance

- Conformité aux réglementations?
- Rapports et auditabilité?
- Suis-je en situation de risque?
- Réponse aux événements de sécurité?

Sécurité et Conformité à tous les niveaux



ISS = Internet Security Systems

Sécurité et Conformité à tous les niveaux

Problématiques adressées

- Corrélation d'évenements réseau temps réel
- Attaques perpetrées de l'intérieur – comprendre et gérer ce que les utilisateurs internes font
- Satisfaction de l'auditeur et corrélation vers des régulations spécifiques (SOX, Bâle II, ISO, PCI, . . .)

Agenda

Présentation de l'Offre Tivoli Security

Les Challenges de l'Audit et de la Conformité

SEM versus SIM

La solution: IBM Tivoli's SIEM

Architecture

IBM Value Proposition

Proven Results

Questions

Les Challenges de Sécurité et de Conformité

- **Besoins de conformité** croissants
  - Initiatives de conformité toujours plus nombreuses
  - Nouveaux besoins de conformité dans de nombreux secteurs industriels
  - 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
  - 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

Quel impact d'une faille sécurité exploitée?

La sécurité s'applique à l'ensemble de l'entreprise.

Un point faible dans un seul domaine et c'est l'ensemble du métier qui est mis en péril.

- Rupture des fonctions clés de l'entreprise;
- Impact direct sur le chiffre d'affaires;
- Perte de confiance des clients et des partenaires;
- Atteinte à l'image de marque;
- Perte de clients ;
- Vol d'informations confidentielles;
- Risque quant à la conformité avec les régulations en vigueur;
- Responsabilité des dirigeants de l'entreprise;

Coût moyen résultant de l'exploitation d'une faille sérieuse, exploitée: $1.8 million[1]

1. **Bear Stearns and Co: Internet Security, June 2002**

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, Feb. 15, 2007

Ce qui s'est passé:

- Employé partant chez un compétiteur
- Accède aux bases de données
- Transfère des documents sur son nouvel ordinateur portable

Commentaires du Carnegie Mellon CERT:

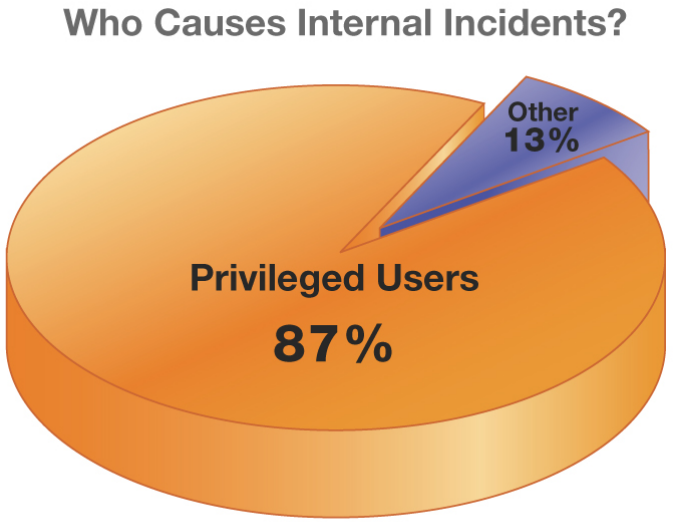
- "75% des … vols d'informations confidentielles étudiés… ont été perpétrés par des employés actifs"
- "45% d'entre eux avaient déjà accepté un nouvel emploi ailleurs"

Commentaires de la CIA:

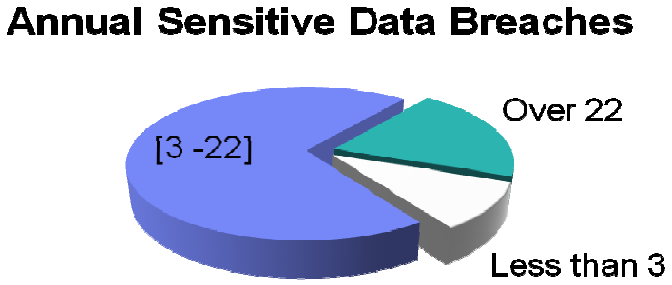
- "…les concepteurs et les scientifiques ont tendance à considérer le capital intellectuel de leur entreprise comme le leur… et souhaitent le garder en partant"

Surveiller les utilisateurs privilégiés n'est plus une option

- **87% des incidents internes sont causés par des utilisateurs privilégiés**
- La plupart sont des **incidents non intentionnels** causés par la violation:
  - Des processus de gestion des changement
  - Des politiques d'utilisation acceptables
- D'autres sont **délibérés**, les motifs étant:
  - Revanche (84%)
  - "Événements négatifs" (92%)
- Quelle que soit leur raison, ces incidents coûtent trop cher 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.

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 nos outsourcers gèrent vos systèmes et données de manière responsable?
- Disposez-vous de rapports sur les changements non autorisés sur notre environnement d’opérations?
- La séparation des tâches fonctionne-t’elle?
- Avez-vous les moyens 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?

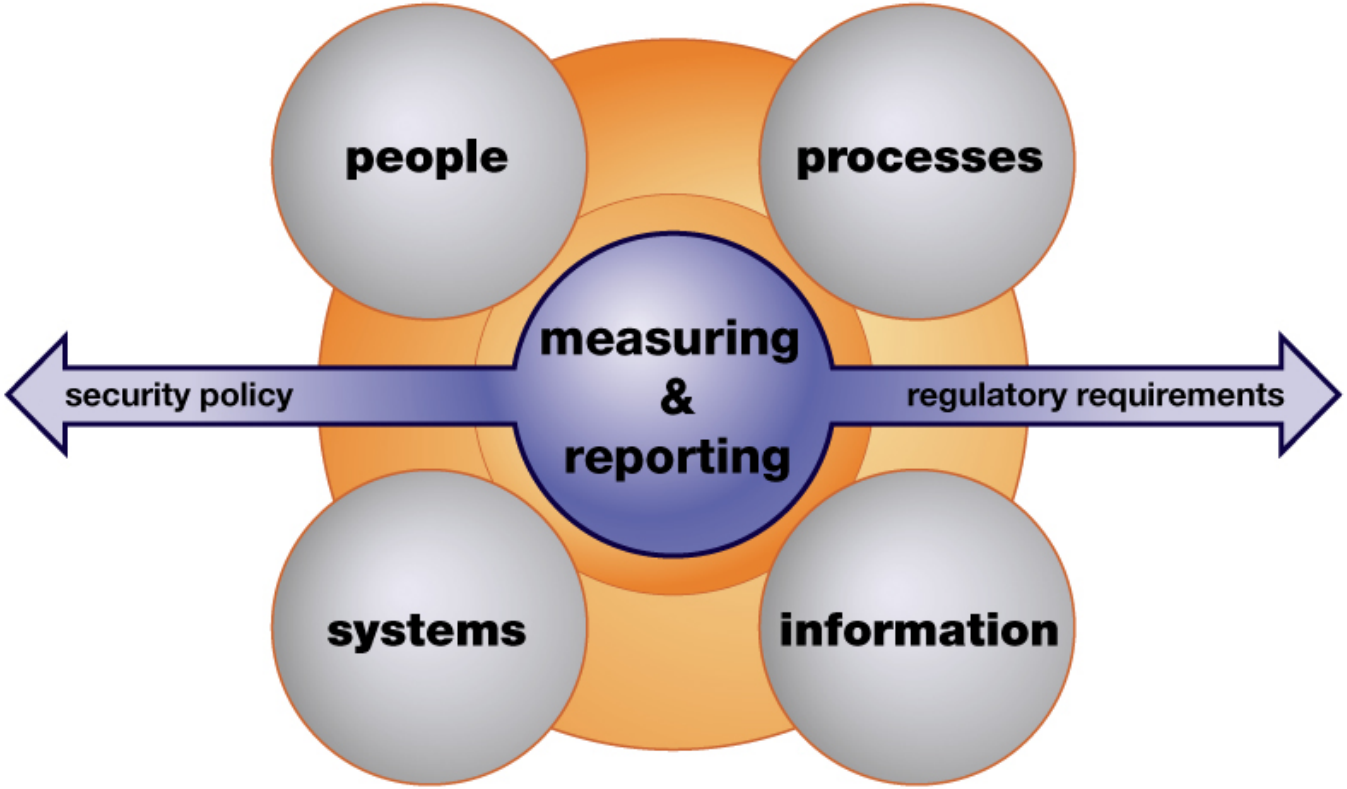
Régulateurs & Auditeurs créent l'urgence

[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 Challenge de l'Audit et de la Conformité



Le Challenge consiste à mesurer et rapporter sur le comportement de personnes et de systèmes à travers l'entreprise sans inhiber ou dégrader la performance du métier.

Agenda

Présentation de l'Offre Tivoli Security

Les Challenges de l'Audit et de la Conformité

La solution: IBM Tivoli's SIEM

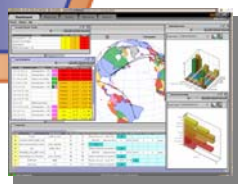
Architecture proposée pour CA-SA

IBM Value Proposition

Proven Results

Questions

The IBM Tivoli SIEM Solution

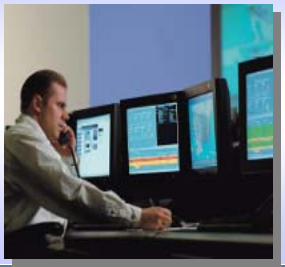
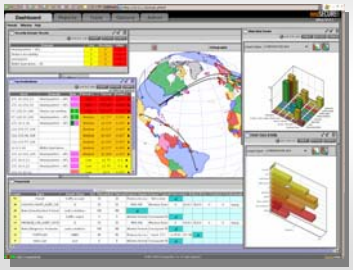


What is Security Information & Event Management (SIEM)?

- **SEM – Security Event Management**
  - Collecting & Manipulating Security Events to address **real-time Security Operation** Requirements
  - Expected Characteristics
    - Collect from a large & diverse range of devices & systems, **especially network devices**
    - Strong correlation & normalization technology
    - Efficient Interface to please Security Operators
    - Operate essentially in Real-Time

- **SIM – Security Information Management**
  - Transform security log events into Information
  - Basic objects are **User's activities, Who touches What data**
  - Expected Characteristics
    - Collect from **systems, middleware & applications**
    - Present information in a format for managers, auditors
    - Address regulations & standard compliances

Tivoli Security Information & Event Management TSIEM

	Opérations IT & sécurité	Audit interne Sécurité IT
Personnes utilisatrices		
Problème:	▪ Attaques & alertes réseau, ▪ Trop de données de sécurité ▪ Pondération des incidents	▪ Sécurité concernant les comportements ▪ Audit des utilisateurs privilégiés ▪ Reporting et conformité
Solution:	**Gestion des Incidents** **Security Event Mgmt (SEM)**	**Audit et surveillance des activités des utilisateurs** **Security Info Mgmt (SIM)**
Produit:	**Security Operations Manager** 	**Compliance Manager** 

Gestion des Incidents temps-réel (SEM)

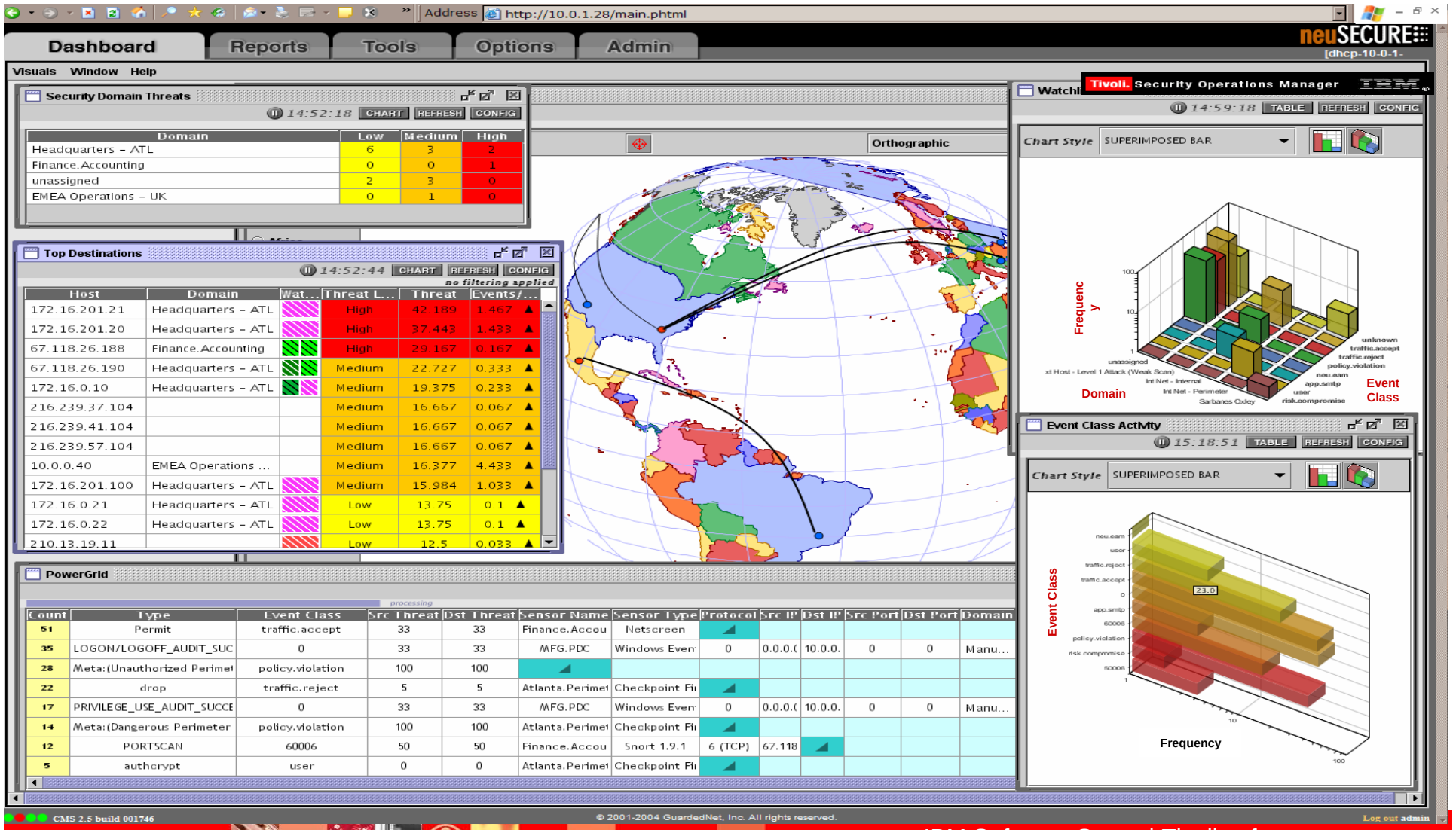
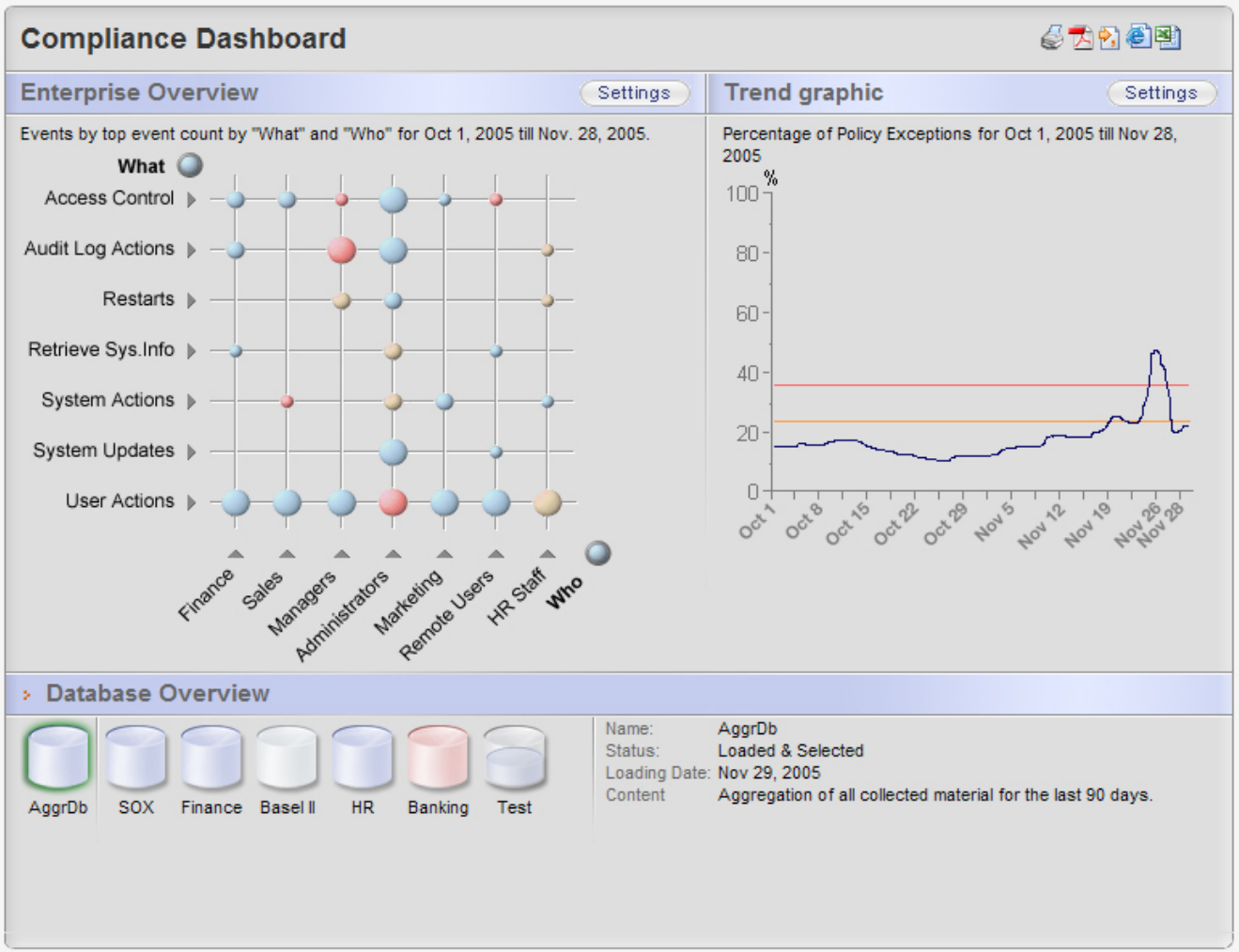


Tableau de bord de conformité (SIM)



Agenda “Gestion des menaces et de la sécurité”

Gestion des logs et audits avec Compliance Insight Manager

1. Capturer – Gestion des logs de l’entreprise
2. Comprendre – Interprétation sophistiquée des logs
3. Communiquer – Reporting et audit de conformité Architecture de la solution

Corrélation d’évenements avec Security Operations Manager

1. Pre-filtrage et aggrégation des évenements de sécurité
2. Corrélation d’événements
3. Investigations, gestion d’incidents et alertes, reporting

Consul Risk Management

Consul Risk Management, founded in 1986, was a privately owned company based in Delft, Netherlands, with a principal office in Herndon, Virginia. IBM acquired Consul in January 2007.

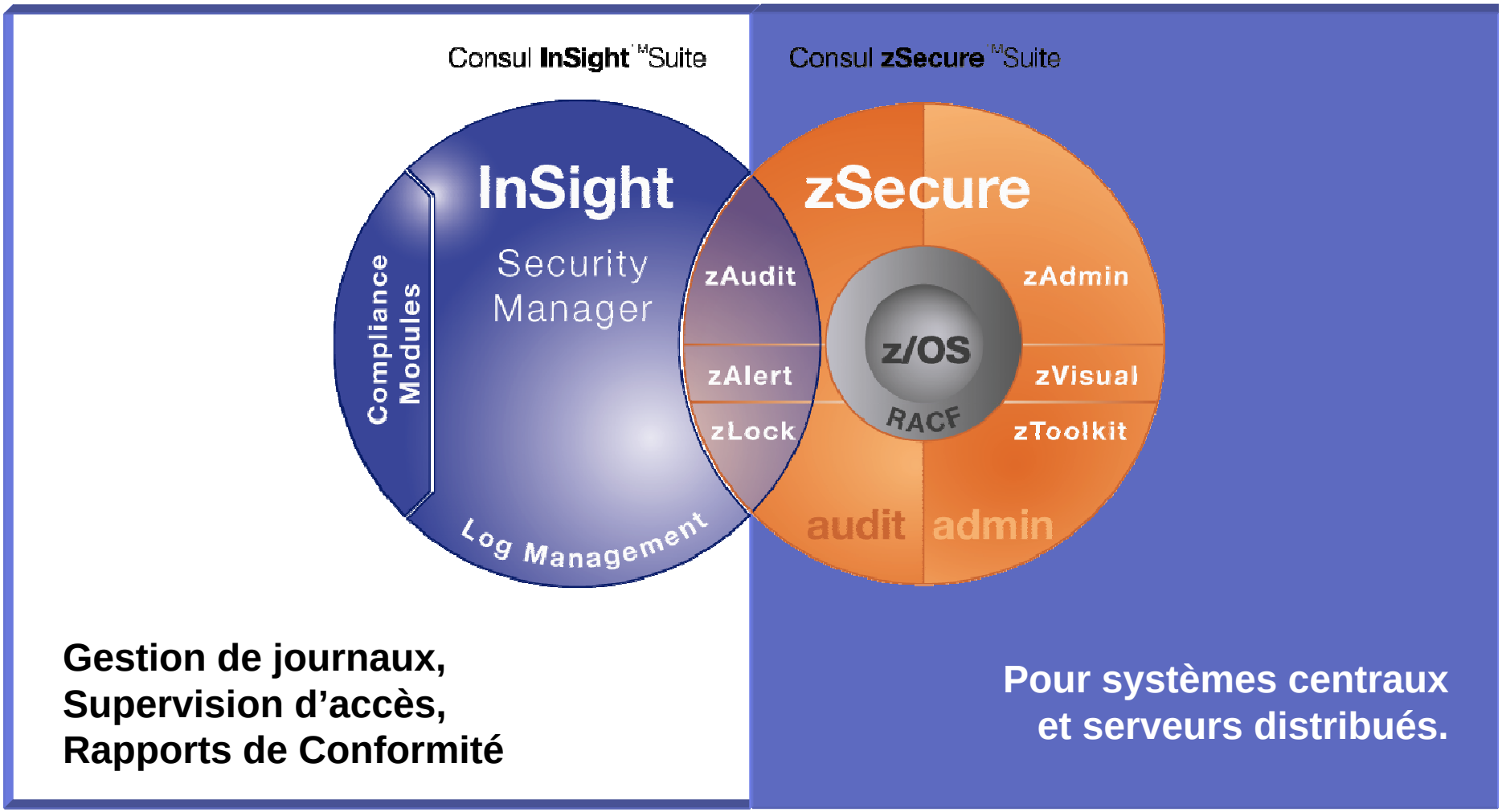
Consul Risk Management's Business Focus

- Providing compliance and audit management software that speeds the delivery and lowers the cost of tracking, investigating and reporting on non-compliant usage of information technology (IT) applications and systems, such as unauthorized access by privileged users.

Consul Risk Management Reputation

- Two decades of experience in security audit and compliance, mainframe roots
- Leader in automated log collection, user monitoring and compliance reporting
- Products installed and used in 100's of customers from 30 countries worldwide
- Partnerships and resellers established around the world

La spécialité de Consul: Supervision et Conformité

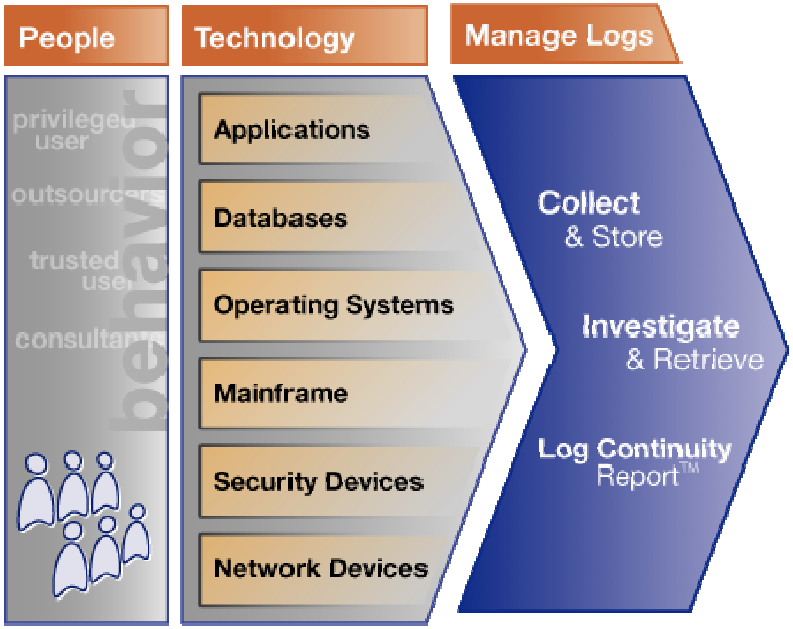


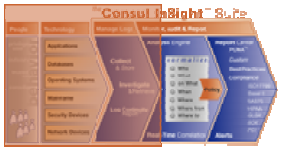
Gestion de journaux,
Supervision d'accès,
Rapports de Conformité

Pour systèmes centraux et serveurs distribués.

Gestion des Logs de toutes les plate-formes

Capturer





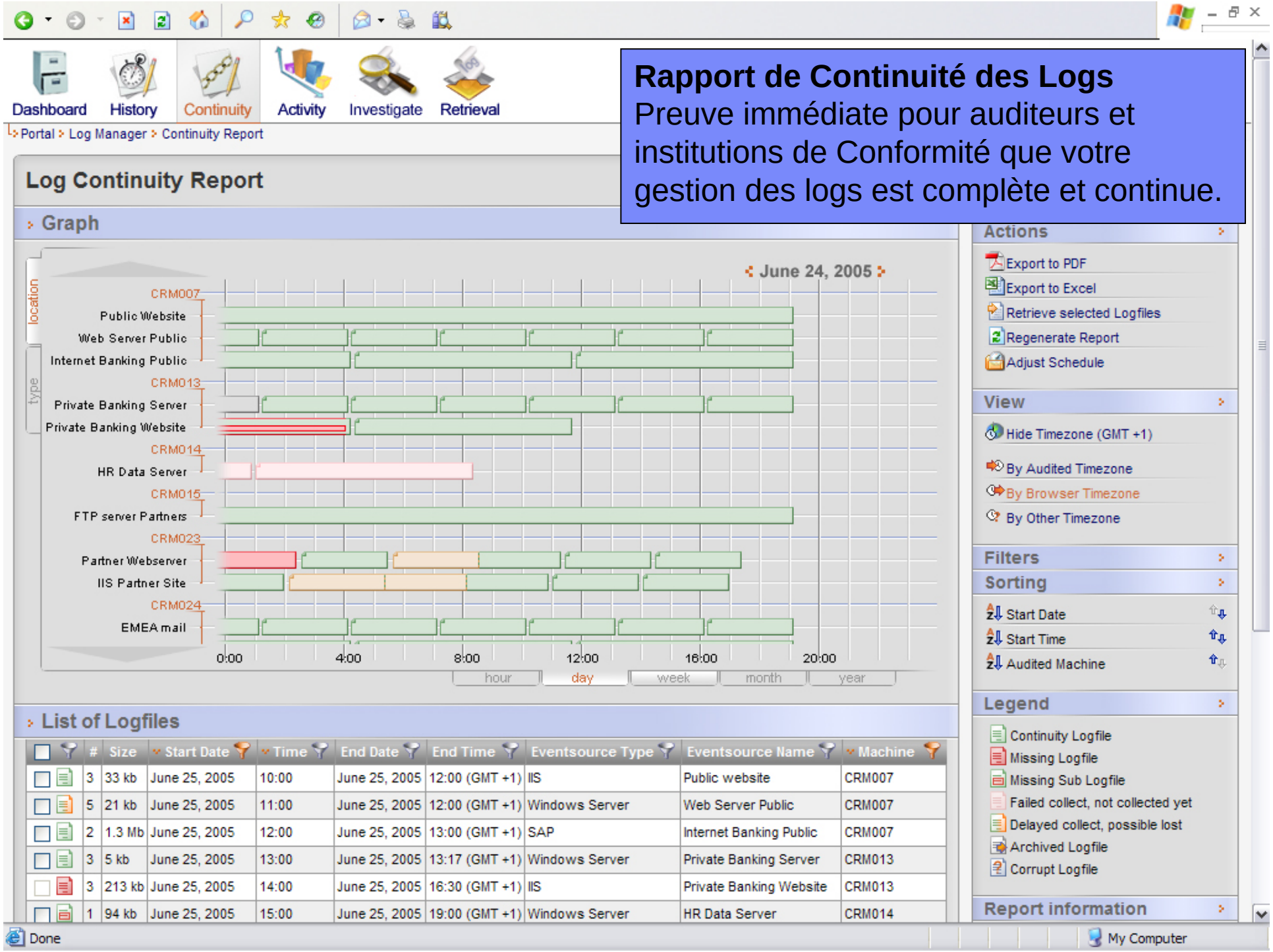
Fonctionnalités:

- Collecte sécurisée et fiable depuis n'importe quelle plate-forme
- Support complet de 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 continuité de la collecte

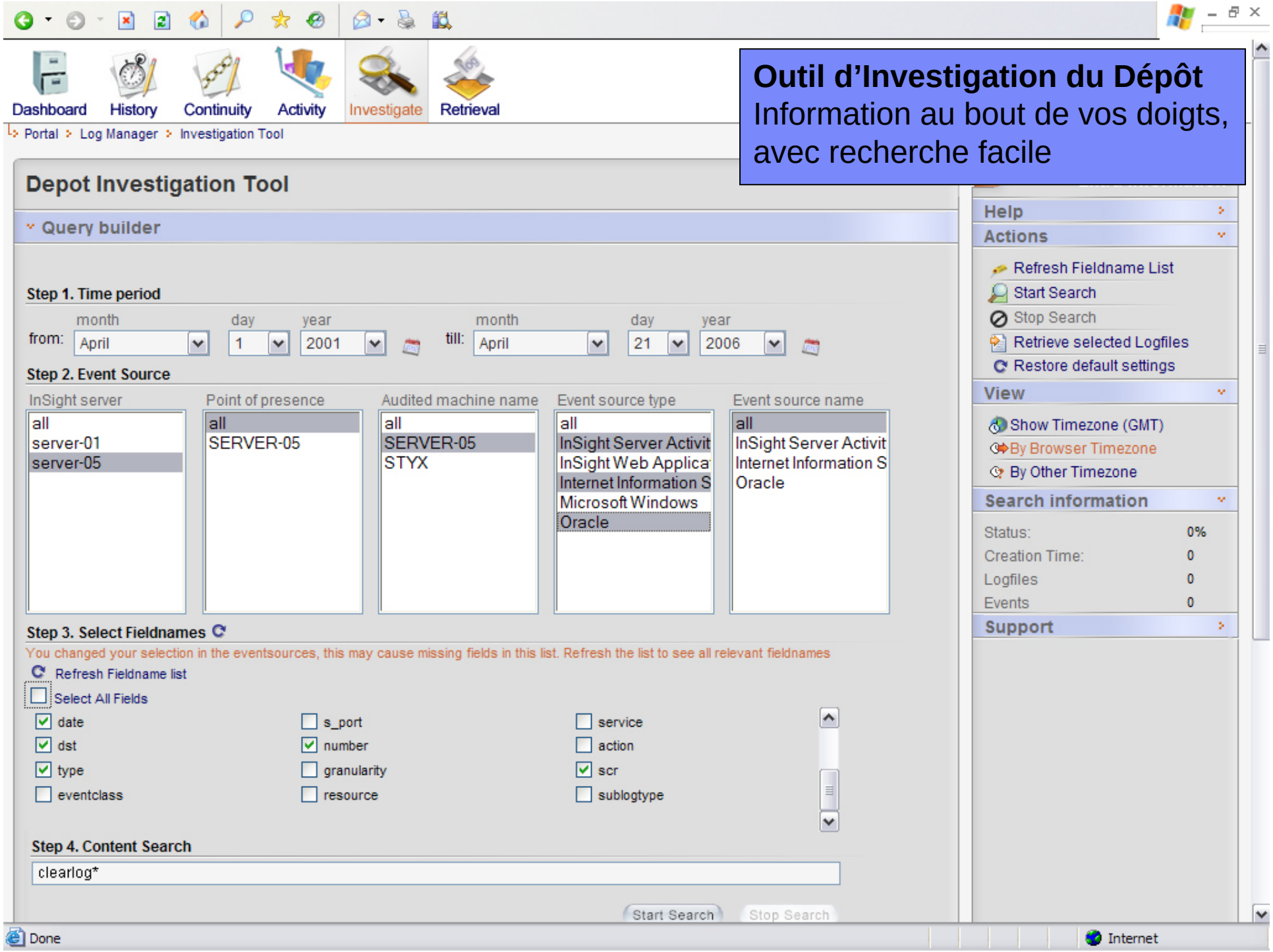
Avantages:

- 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.



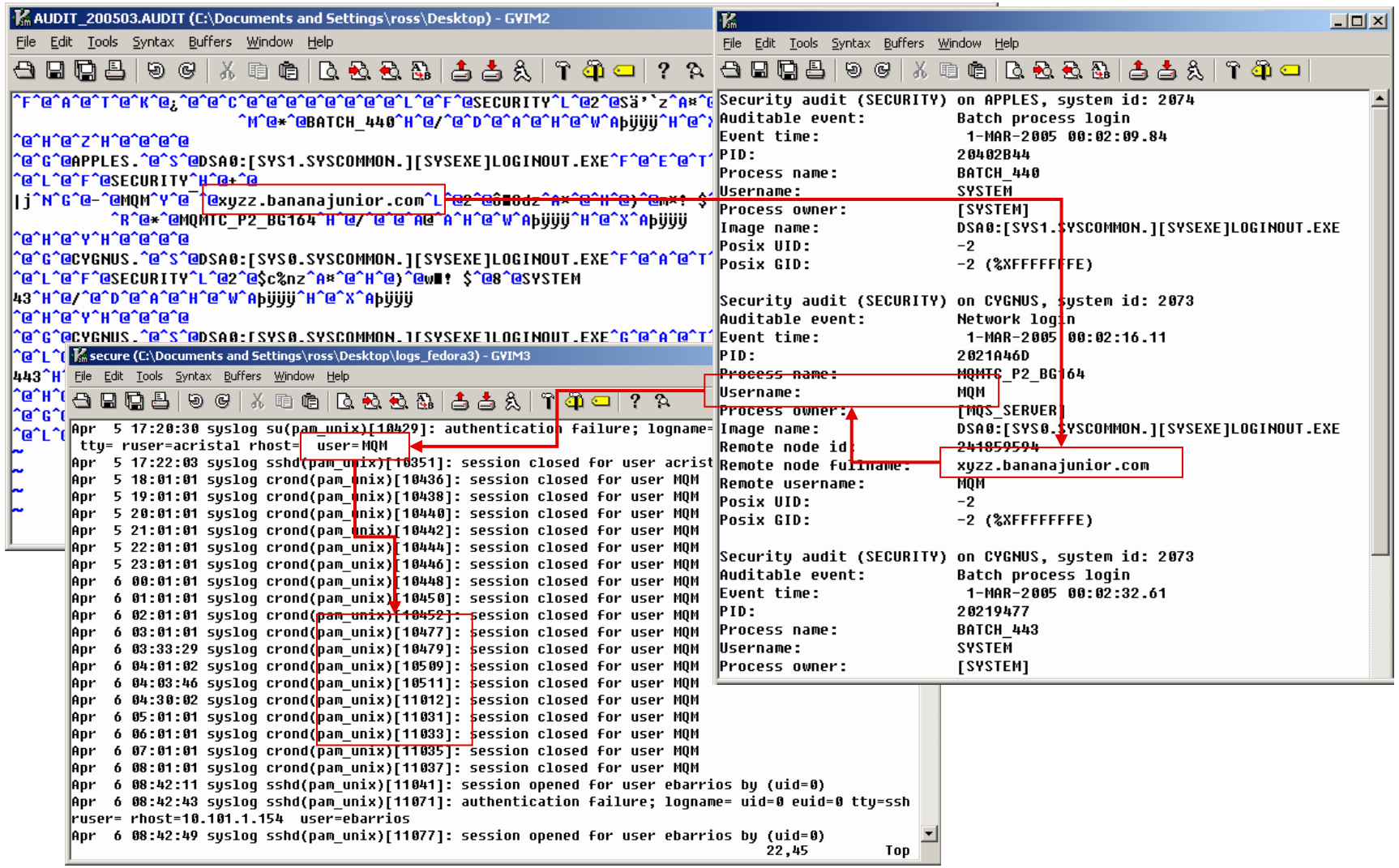
Rapport de Continuité des Logs
Preuve immédiate pour auditeurs et institutions de Conformité que votre gestion des logs est complète et continue.



Outil d'Investigation du Dépôt
Information au bout de vos doigts, avec recherche facile

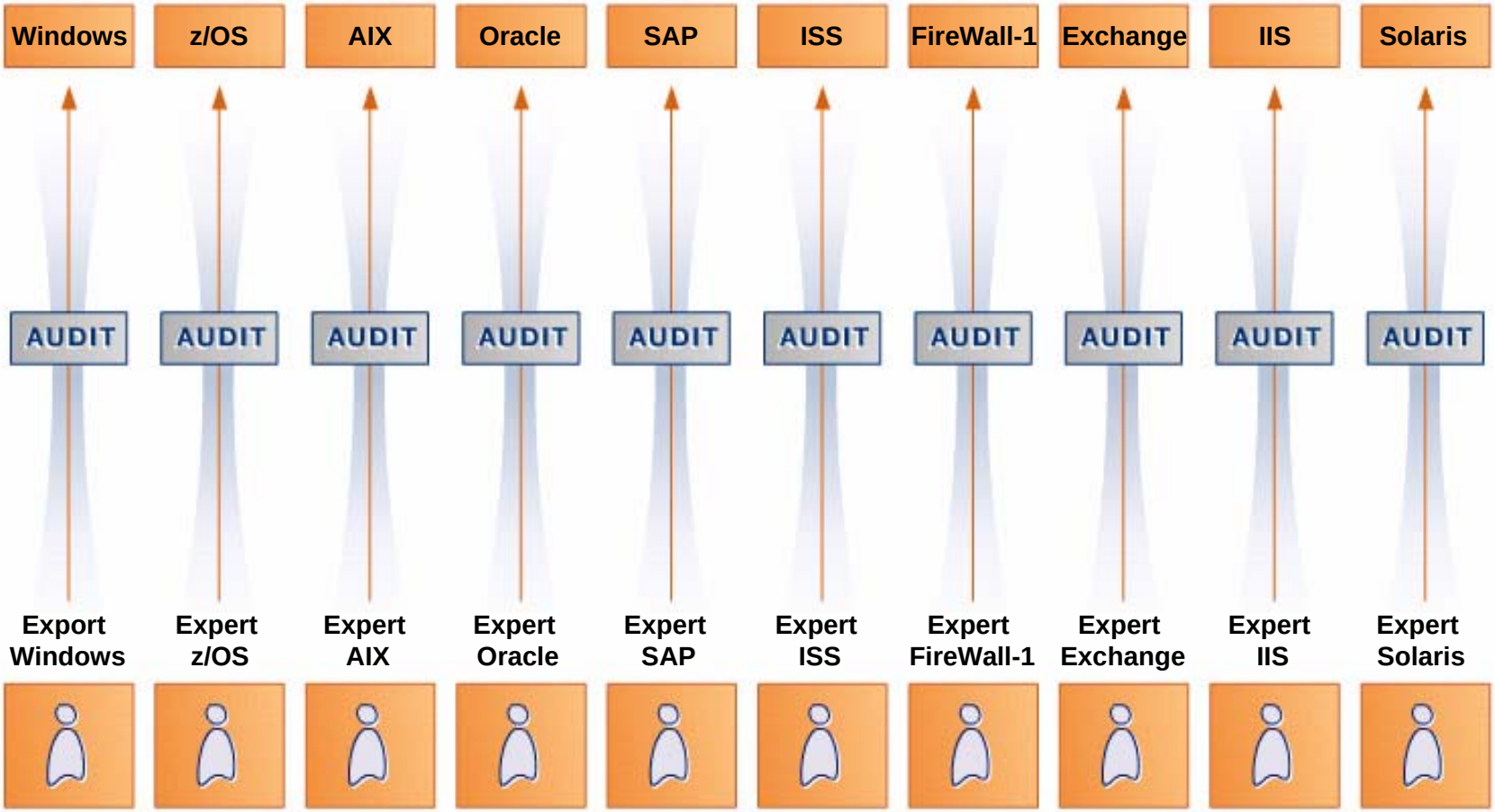
Comprendre

Comment comprendre tous ces différents formats et informations?



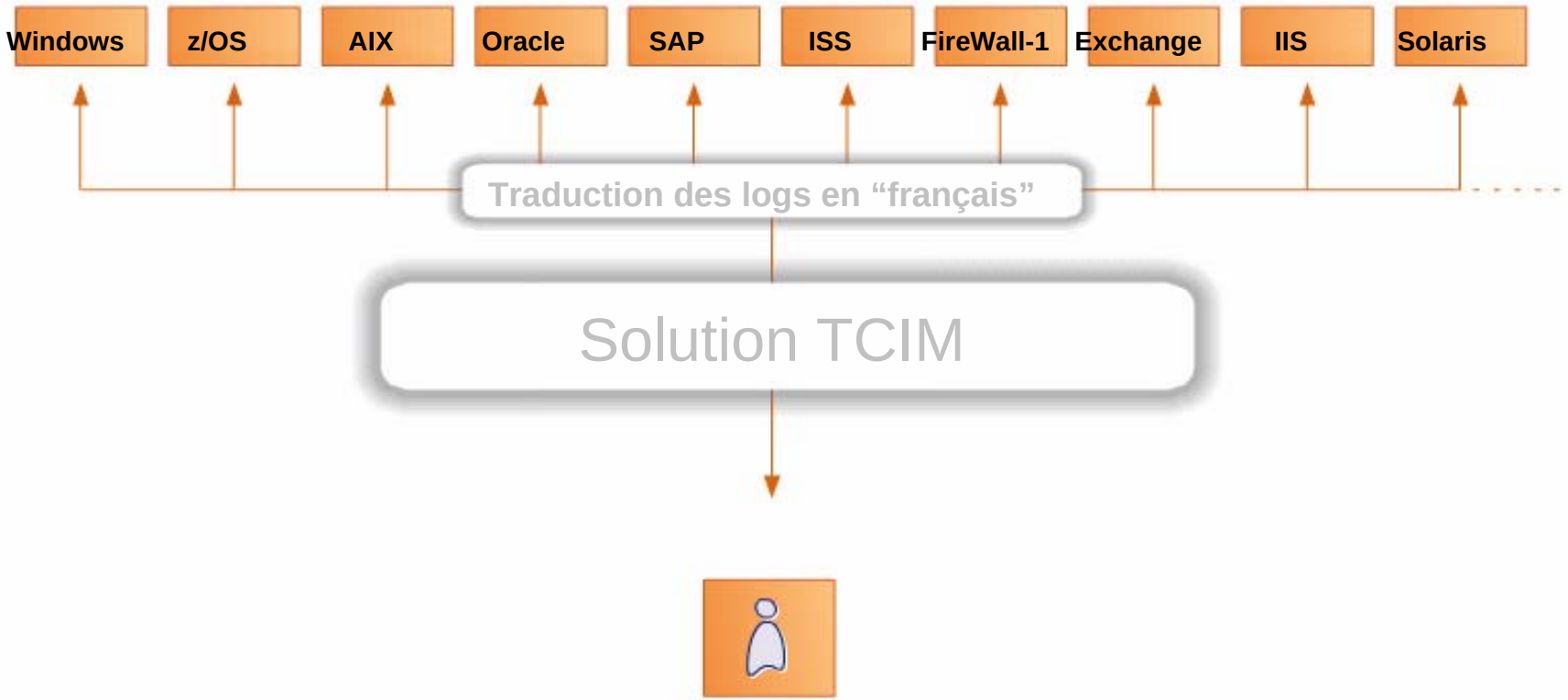
Plutôt que de recourir à de nombreux experts…

Comprendre



Comprendre

Tous les journaux sont traduits en un même language



InSight épargne temps et argent à l’équipe de sécurité de l’information et de conformité en automatisant la supervision à travers toute l’entreprise.

Traduire les journaux dans un langage compréhensible la méthodologie W7

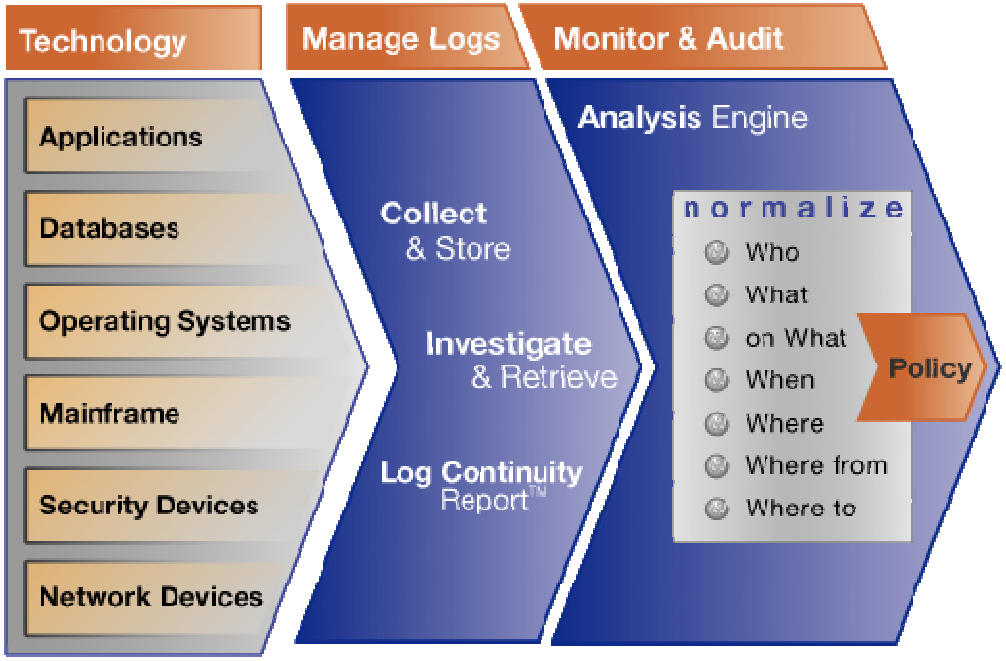
Comprendre

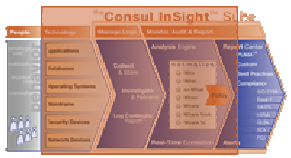
1. **Who** did
2. **What** type of action
3. **on What** file/data
4. **When** did he do it and
5. **Where**
6. **from Where**
7. **Where to**

Nous faisons le travail de traduction,
à votre place!

Interpretation et Corrélation sophistiquée

Comprendre





Fonctionalités:

- W7 : normalisation
- Interpretation de n'importe quel log ou format
- Comparaison de milliards d'événements avec les politiques et règles permises

Avantages:

- Interprêter and superviser tous les logs avec moins de ressources manuelles et chères
- Détecter et résoudre les problèmes de sécurité rapidement.

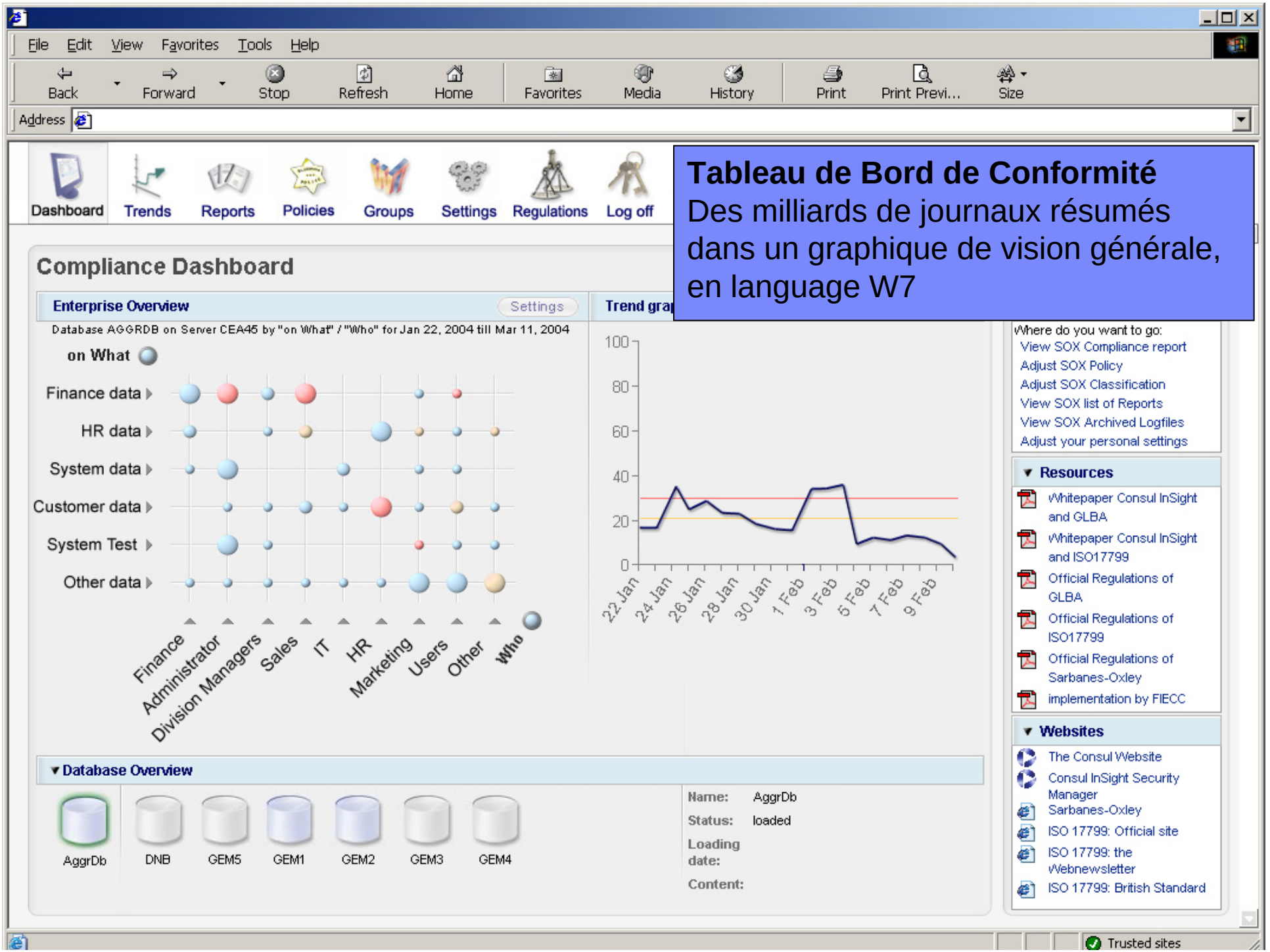
Normalisation out-of-the-box

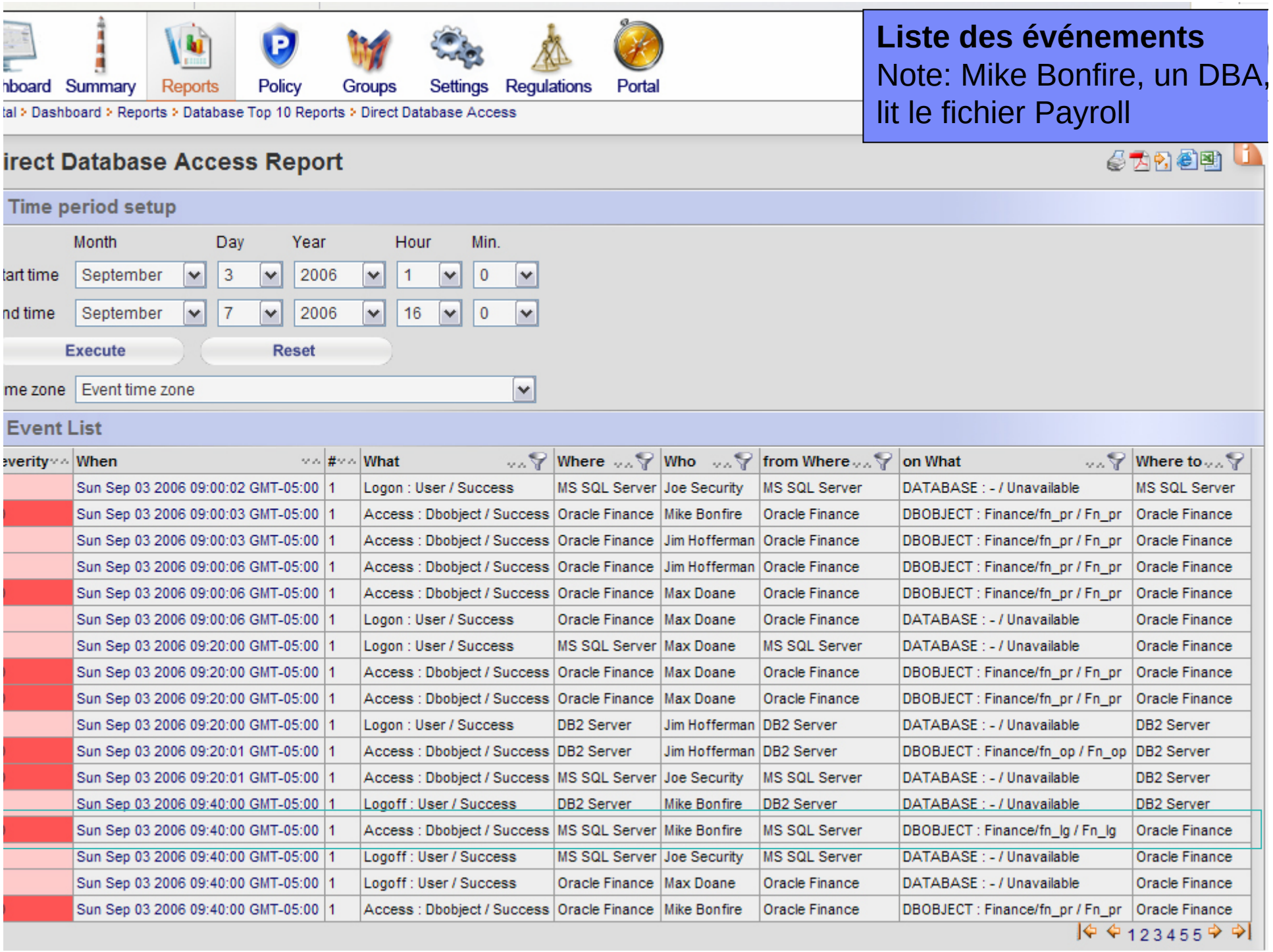
Que font les utilisateurs sur mes systèmes et données sensibles?

Comprendre

Comparer le comportement "Désiré" par rapport au "Réel"

87% des incidents internes sont causés par des utilisateurs privilégiés.


File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Favorites Media History Print Print Previ... Size
Address
Dashboard Trends Reports Policies Groups Settings Regulations Log off
Tableau de Bord de Conformité
Des milliards de journaux résumés dans un graphique de vision générale, en language W7
Compliance Dashboard
Enterprise Overview
Settings
Database AGGRDB on Server CEA45 by "on What" / "Who" for Jan 22, 2004 till Mar 11, 2004
on What
Finance data
HR data
System data
Customer data
System Test
Other data
Finance
Administrator
Division Managers
Sales
IT
HR
Marketing
Users
Other
Who
Trend gra
100
80
60
40
20
0
22 Jan
24 Jan
26 Jan
28 Jan
30 Jan
1 Feb
3 Feb
5 Feb
7 Feb
9 Feb
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
Database Overview
AggrDb
DNB
GEM5
GEM1
GEM2
GEM3
GEM4
Name: AggrDb
Status: loaded
Loading date:
Content:
Trusted sites

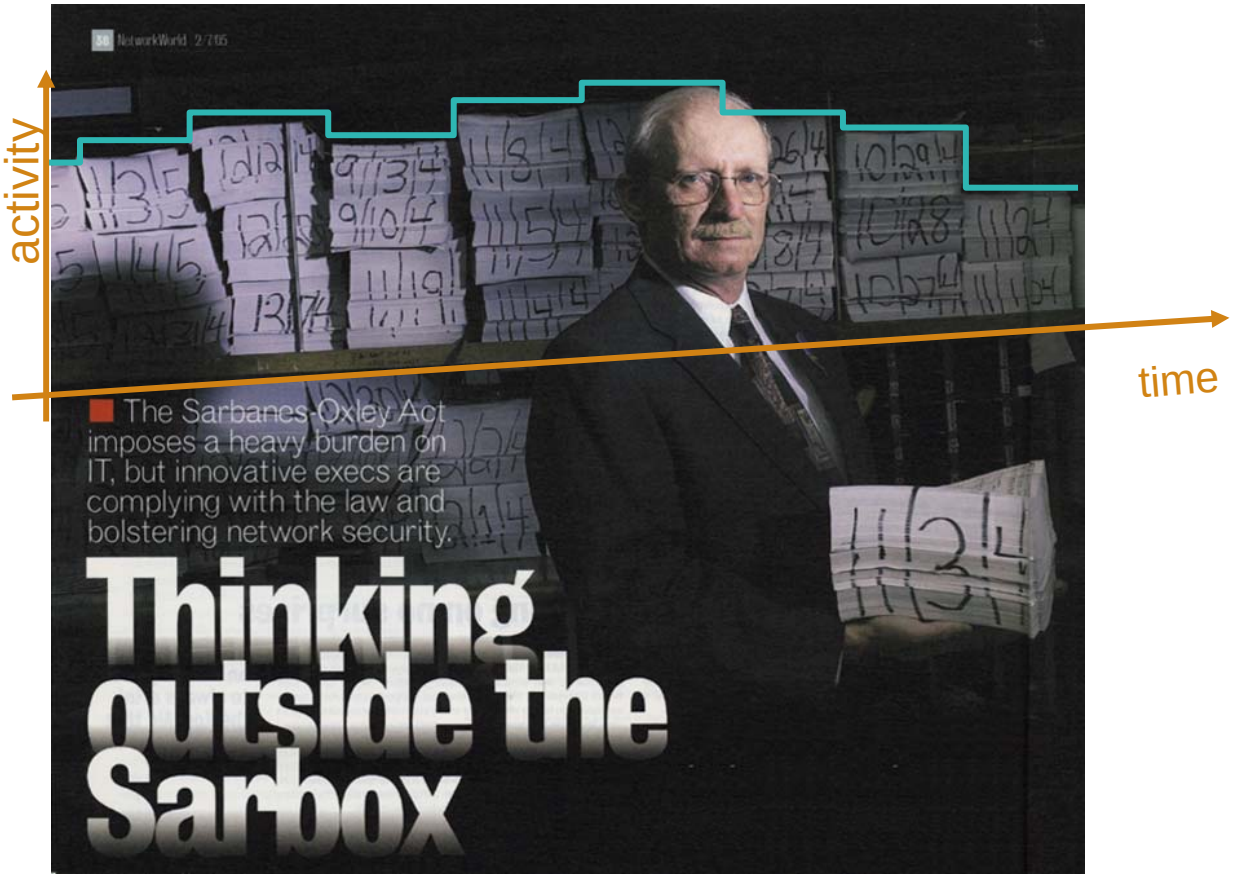


Liste des événements

Note: Mike Bonfire, un DBA, lit le fichier Payroll

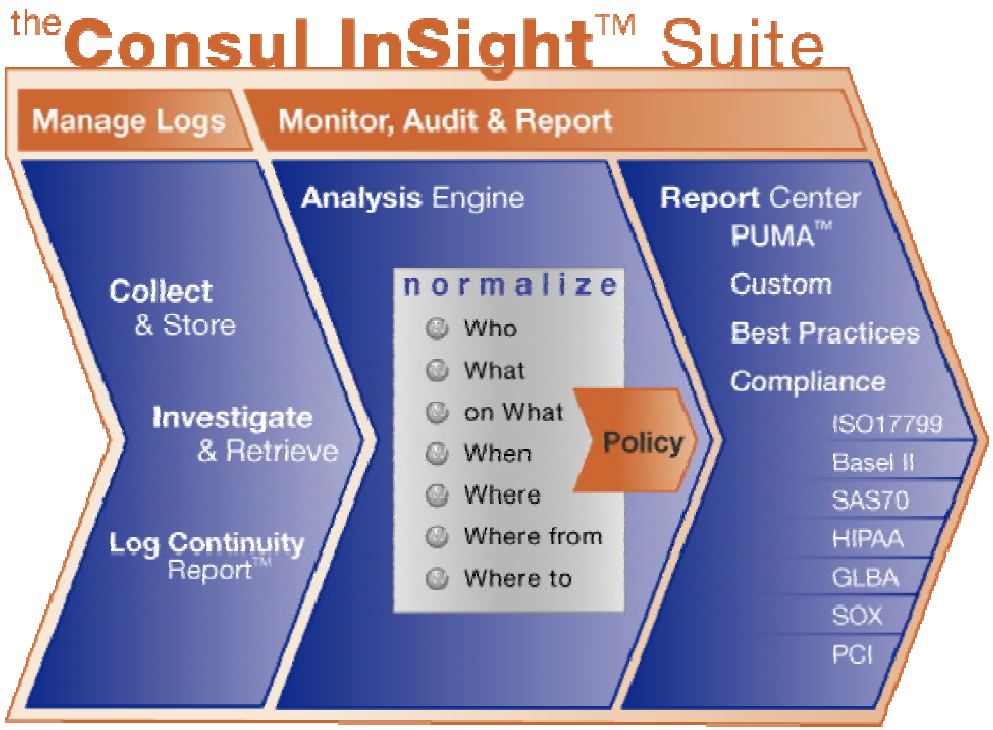
Des rapports, tout prêts, pour communiquer…

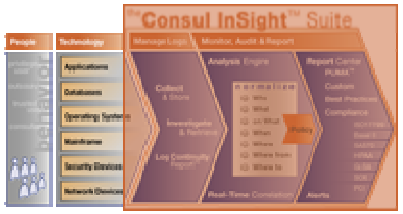
Communiquer



Rapports d'Audit et de Conformité

Communicate



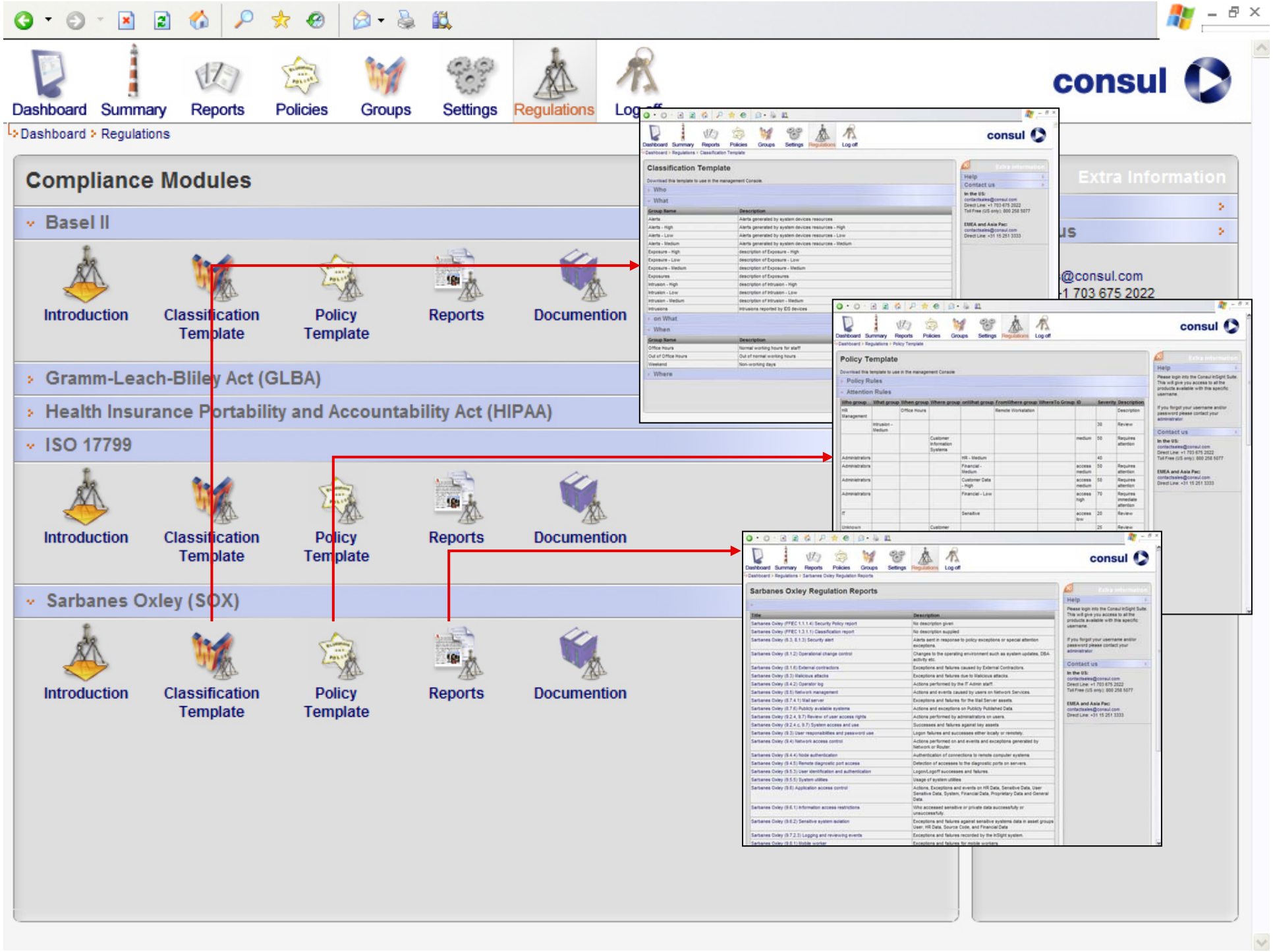


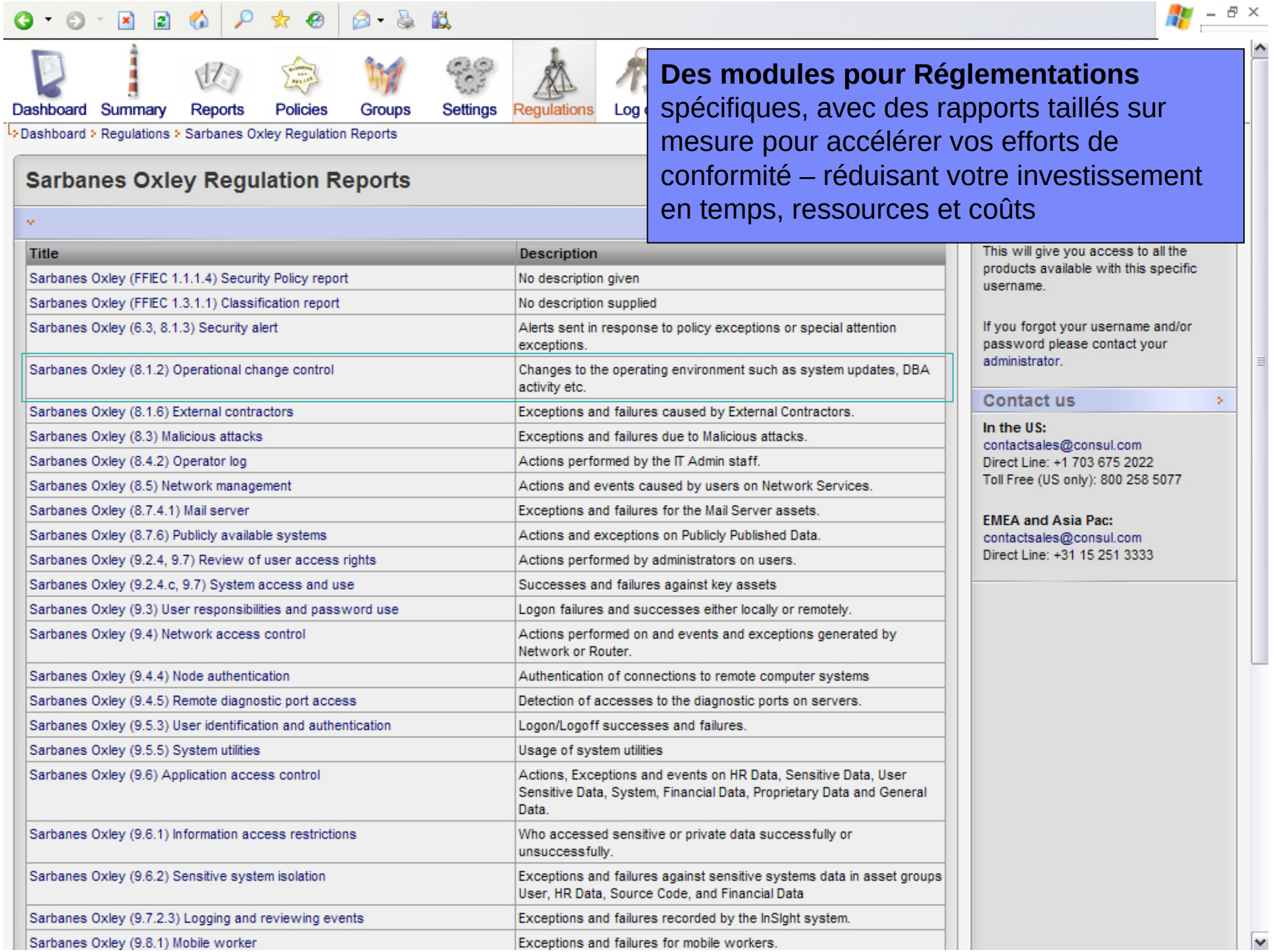
Fonctionalités:

- Centaine de rapports prédéfinis
- Modules de Conformité
- Alertes "Special Attention"
- Rapports personnalisés

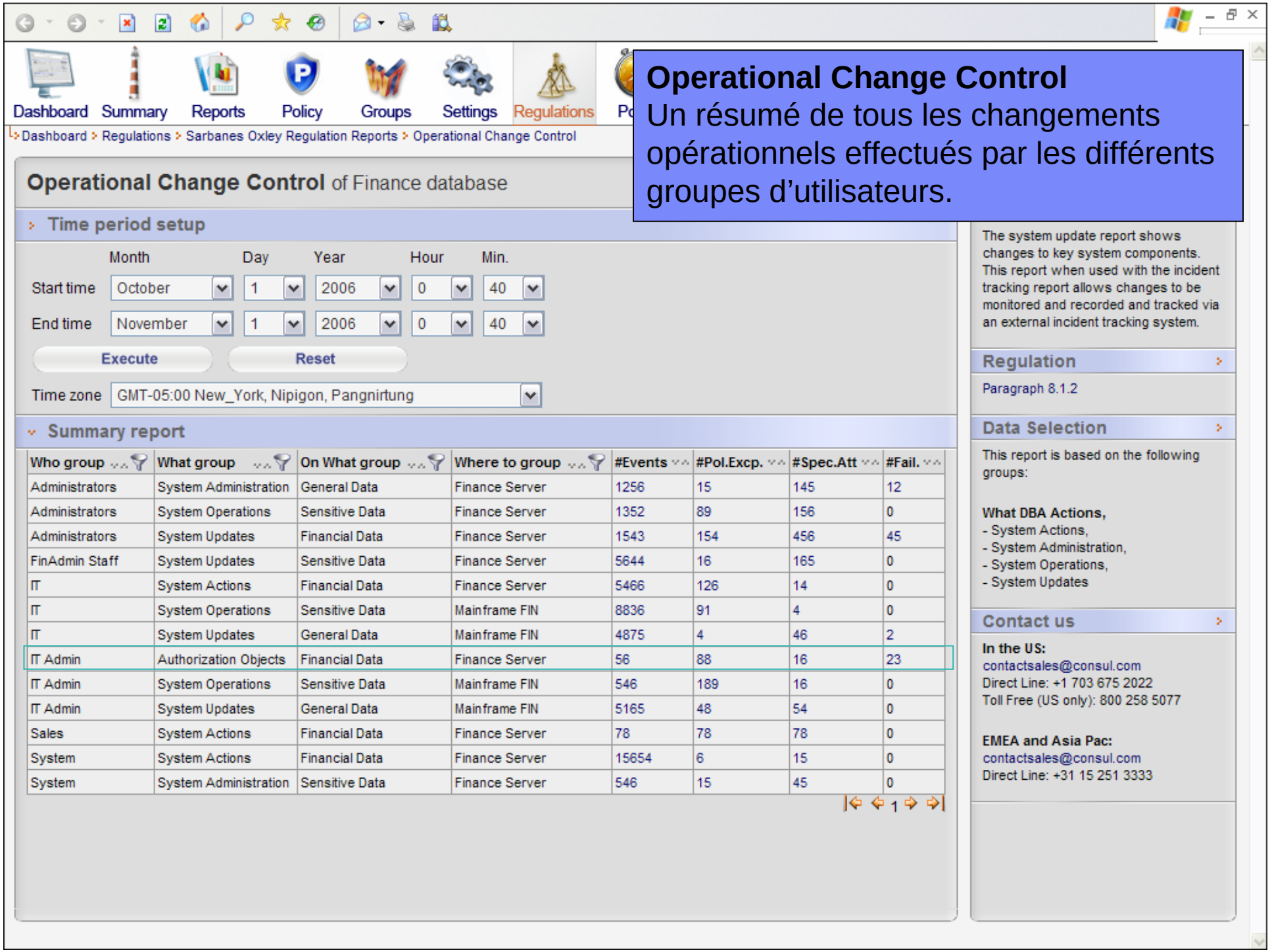
Avantages:

- Réduire le temps et l'effort de réponse aux audits
- Rapports instantanés, sans perte de temps
- Réduire le risque de menace interne: :
  - Protection de l'information
  - contrôle du changement
  - User management


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
Classification Template
Policy Template
Sarbanes Oxley Regulation Reports

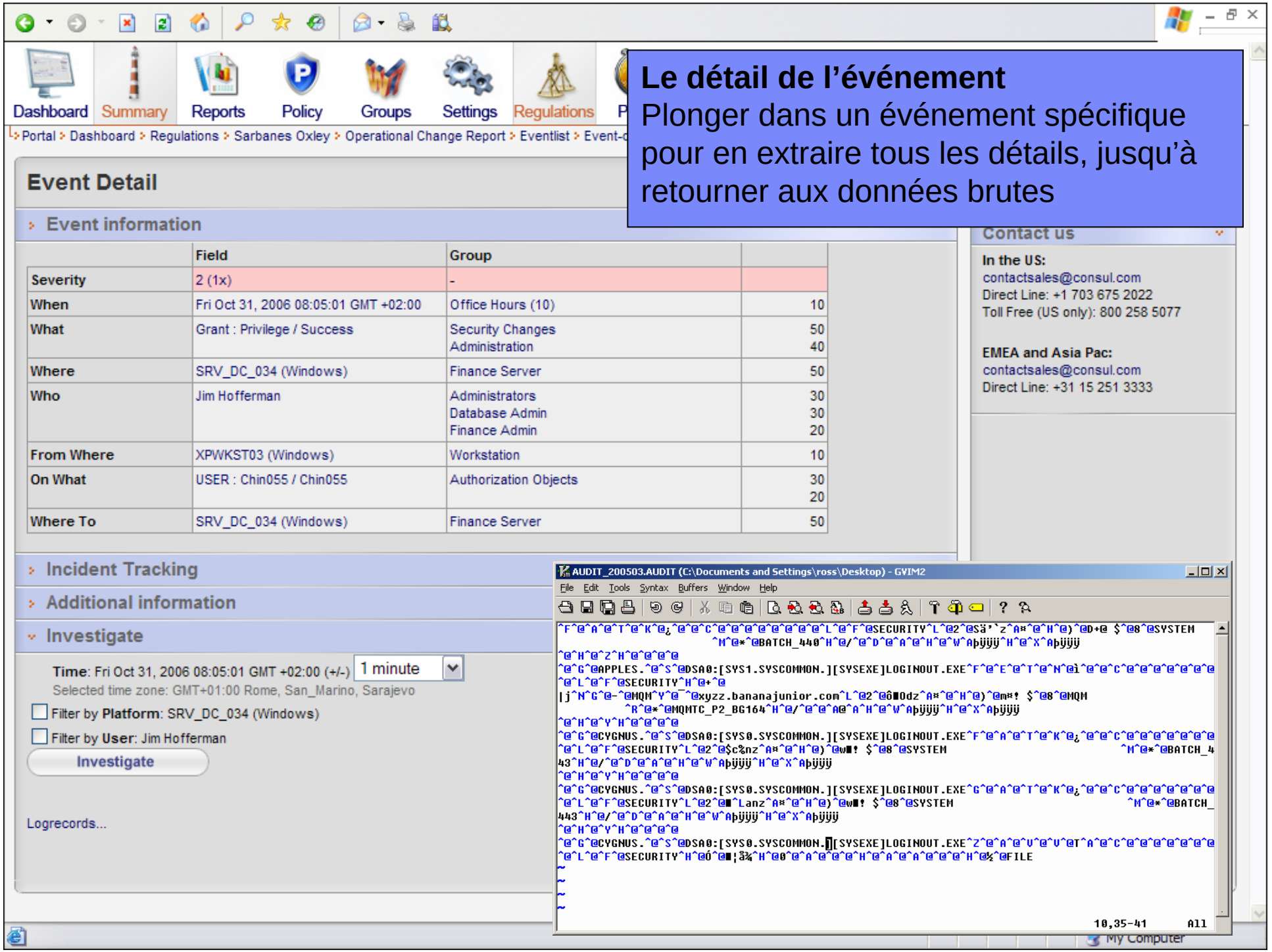


Des modules pour Réglementations spécifiques, avec des rapports taillés sur mesure pour accélérer vos efforts de conformité – réduisant votre investissement en temps, ressources et coûts


Dashboard
Summary
Reports
Policy
Groups
Settings
Regulations
Dashboard › Regulations › Sarbanes Oxley Regulation Reports › Operational Change Control
Operational Change Control of Finance database
Time period setup
Month
Day
Year
Hour
Min.
Start time
October
1
2006
0
40
End time
November
1
2006
0
40
Execute
Reset
Time zone
GMT-05:00 New_York, Nipigon, Pangnirtung
Summary report
Who group
What group
On What group
Where to group
#Events
#Pol.Excp.
#Spec.Att
#Fail.
Administrators System Administration General Data Finance Server 1256 15 145 12
Administrators System Operations Sensitive Data Finance Server 1352 89 156 0
Administrators System Updates Financial Data Finance Server 1543 154 456 45
FinAdmin Staff System Updates Sensitive Data Finance Server 5644 16 165 0
IT System Actions Financial Data Finance Server 5466 126 14 0
IT System Operations Sensitive Data Mainframe FIN 8836 91 4 0
IT System Updates General Data Mainframe FIN 4875 4 46 2
IT Admin Authorization Objects Financial Data Finance Server 56 88 16 23
IT Admin System Operations Sensitive Data Mainframe FIN 546 189 16 0
IT Admin System Updates General Data Mainframe FIN 5165 48 54 0
Sales System Actions Financial Data Finance Server 78 78 78 0
System System Actions Financial Data Finance Server 15654 6 15 0
System System Administration Sensitive Data Finance Server 546 15 45 0
1
Operational Change Control
Un résumé de tous les changements opérationnels effectués par les différents groupes d'utilisateurs.
The system update report shows changes to key system components. This report when used with the incident tracking report allows changes to be monitored and recorded and tracked via an external incident tracking system.
Regulation
Paragraph 8.1.2
Data Selection
This report is based on the following groups:
What DBA Actions,
- System Actions,
- System Administration,
- System Operations,
- System Updates
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

Liste des évènements

Zoomer dans chaque action que l'administrateur a effectué sur un système financier et voir la création du compte utilisateur Chin055


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)
-
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
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...
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
AUDIT_200503.AUDIT (C:\Documents and Settings\ross\Desktop) - GVIM2
File Edit Tools Syntax Buffers Window Help
10,35-41 All
My Computer

Agenda “Gestion des menaces et de la sécurité”

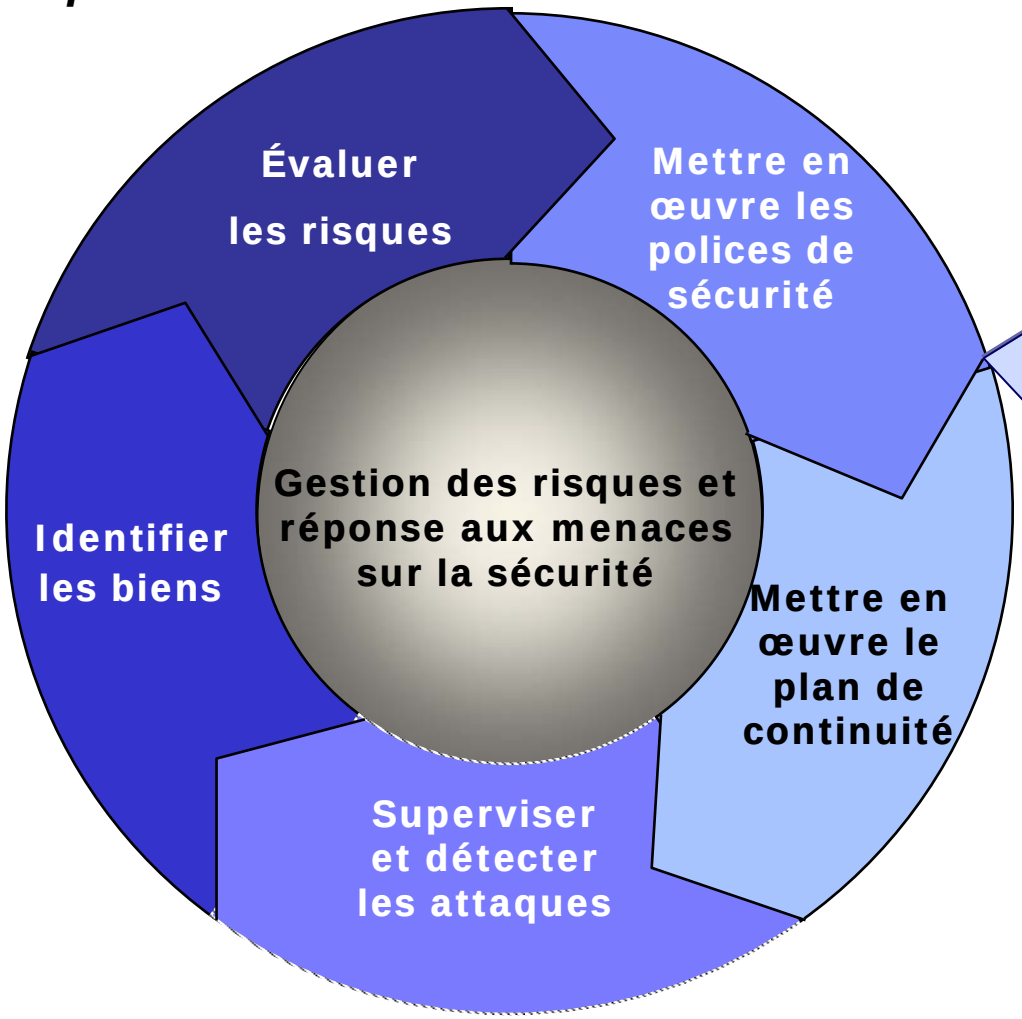
Gestion des logs et audits avec Tivoli Compliance Insight Manager

1. Capturer – Gestion des logs de l’entreprise
2. Comprendre – Interprétation sophistiquée des logs
3. Communiquer – Reporting et audit de conformité Architecture de la solution

Corrélation d’évenements avec Tivoli Security Operations Manager

1. Pre-filtrage et aggrégation des évenements de sécurité
2. Corrélation d’évenements
3. Investigations, gestion d’incidents et alertes, reporting

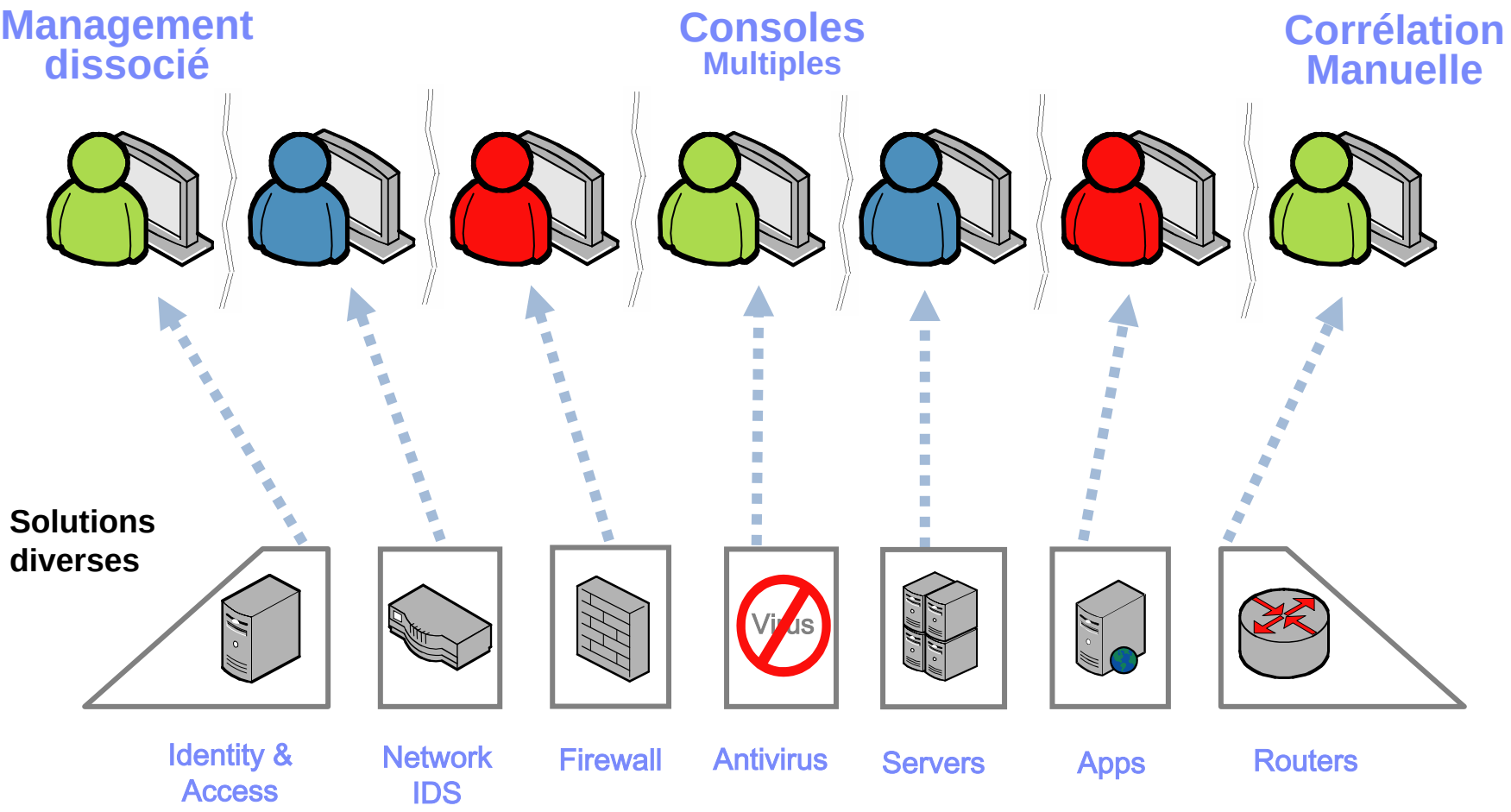
Les tentatives de protection des biens de l'entreprise ont engendré un pilotage complexe de la sécurité



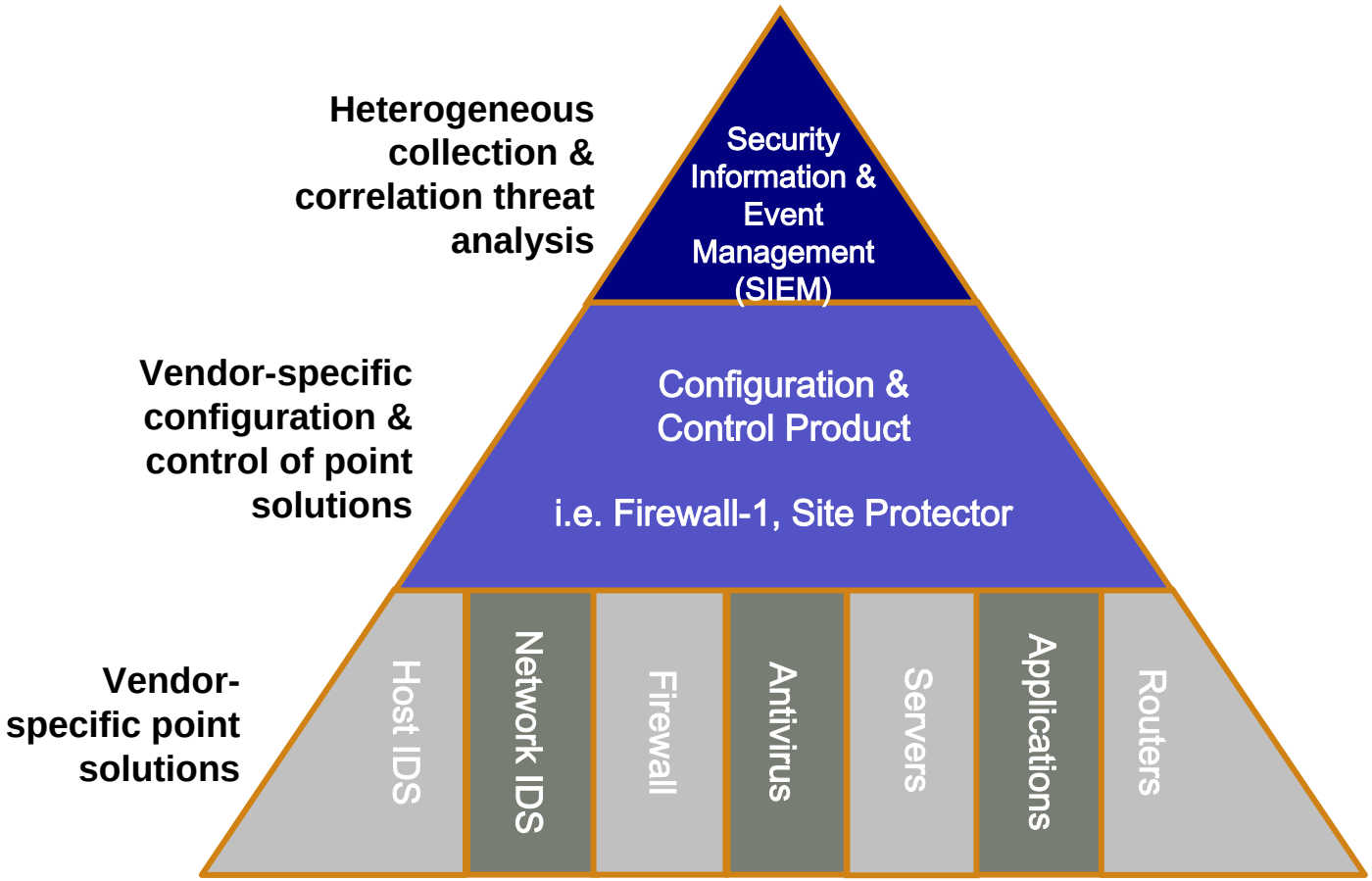
Le déploiement d'outils et d'équipements de sécurité multiples implique:

- Un pilotage complexe de la sécurité;
- Aucune vue consolidée de la sécurité du SI;
- Difficulté à isoler les véritables menaces;
- De multiples alarmes et alertes redondantes avec faux positifs
- Difficulté à gérer les priorités et les escalades
- Une perception erronée du niveau réel de sécurité
- Mauvaise compréhension de l'exposition réelle de l'entreprise

La problématique : Sources et Environnements multiples



La solution : Une Interface SIEM unique pour une collecte hétérogène



Une solution de pilotage de la sécurité opérationnelle

TSOM est aujourd'hui utilisé par les plus grandes sociétés (banques, opérateurs télécom, gouvernements).

✓Consolidation des données de sécurité de l'infrastructure

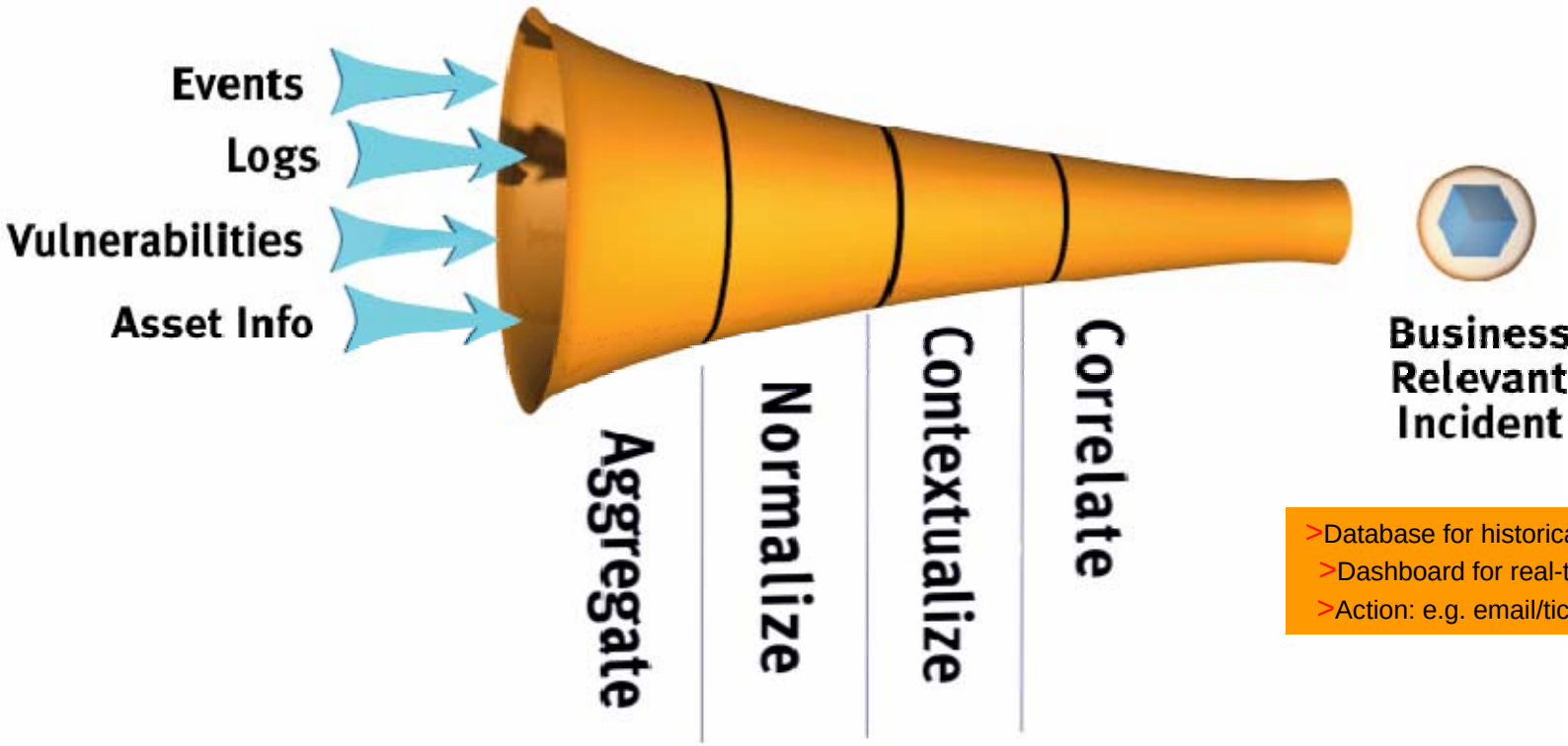
✓Gestion du risque pour les applications métiers critiques

✓Fournisseurs de solutions de pilotage de la sécurité hébergés (MSSP)

Aperçu de Security Operations Manager

- TSOM est un outil de pilotage de la sécurité et de gestion des incidents; il est conçu pour améliorer l'efficacité opérationnelle du SOC en offrant une solution intégrée d'analyse et de résolution des problèmes:
  - Agrégation et centralisation des logs provenant d'environnements hétérogènes
  - Corrélation inter équipements et gestion des priorités en temps réel sur détection d'un incident
  - Outils intégrés d'investigation et remédiation aux problèmes détectés
  - Tableaux de bord temps réel du statut du périmètre sécurité supervisé
  - Gestion intégrée des incidents grâce au système de tickets
  - Reporting détaillé sur l'efficacité opérationnel, le pilotage et la conformité aux standards **(SOX, Basel II, PCI…)**
  - Pondération des biens métiers afin de prendre en compte cette dimension dans la gestion du risque

Méthode de détection des incidents sécurité



>Database for historical analysis
>Dashboard for real-time view
>Action: e.g. email/ticket/script

"TSOM automates the aggregation and correlation process. It mitigates false positives and alerts my team to real threats in a timely manner. The product is more or less what I would have designed and built myself, given four years and a pool of developers."

– Jeff Hartley, Cox Communications

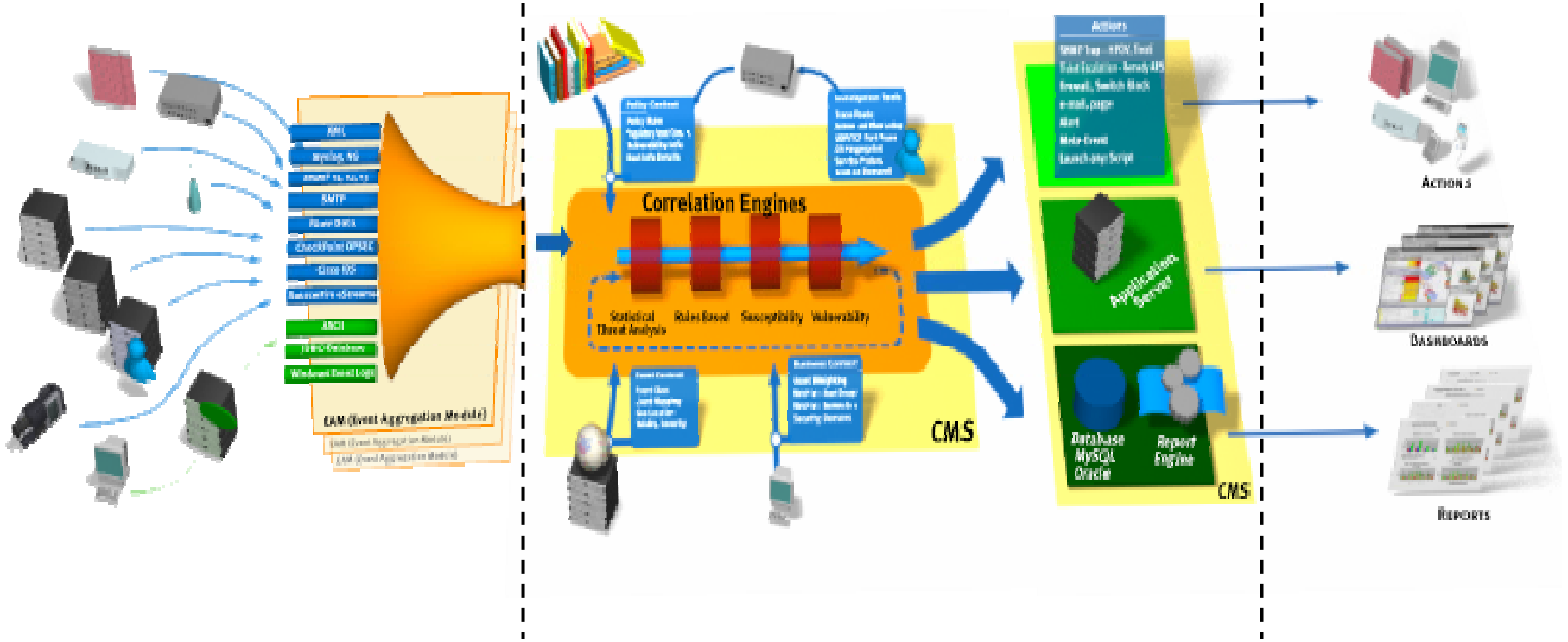
Architecture de Security Operations Manager

EAM

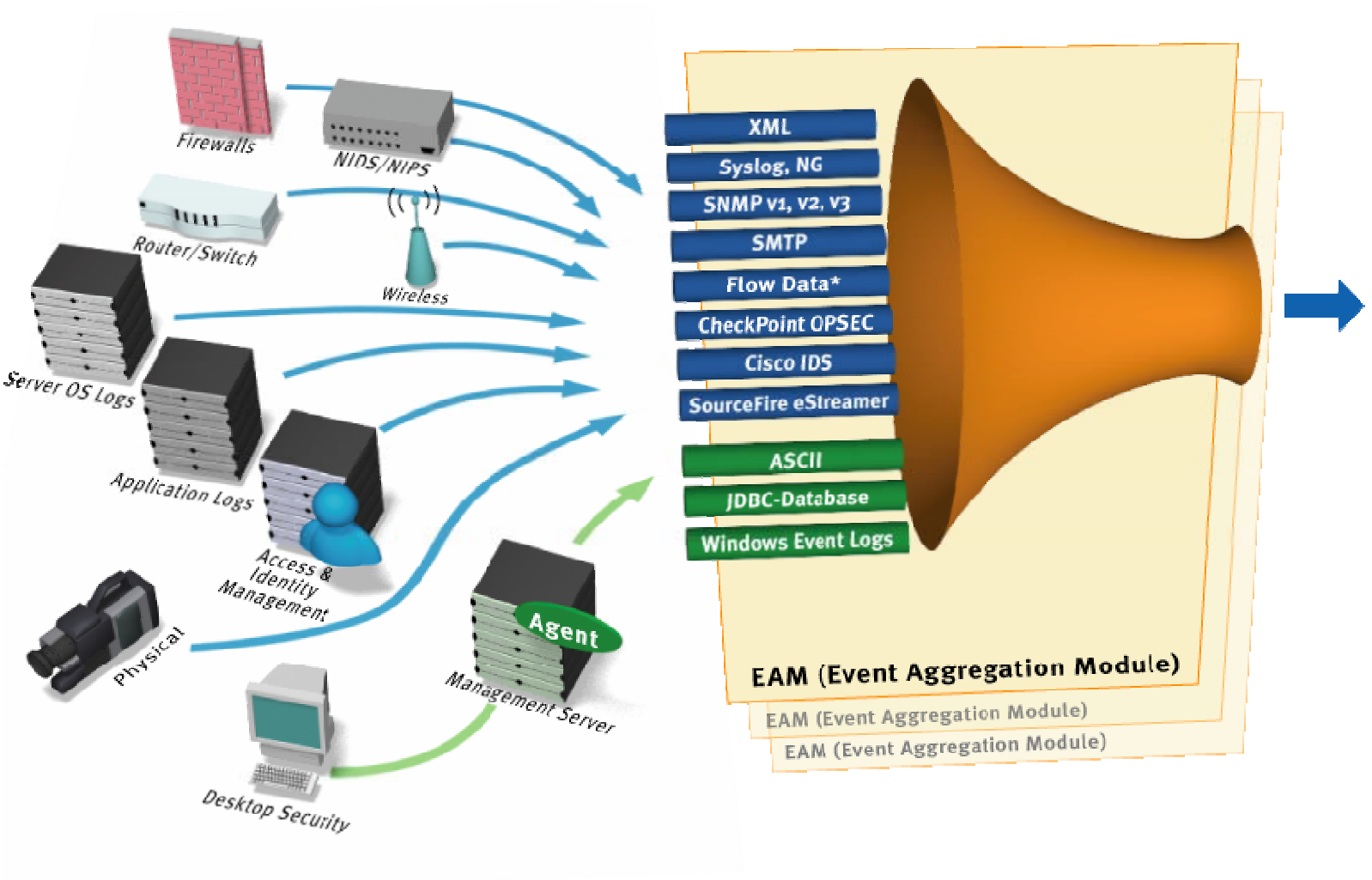
(Event Aggregation Module)

CMS

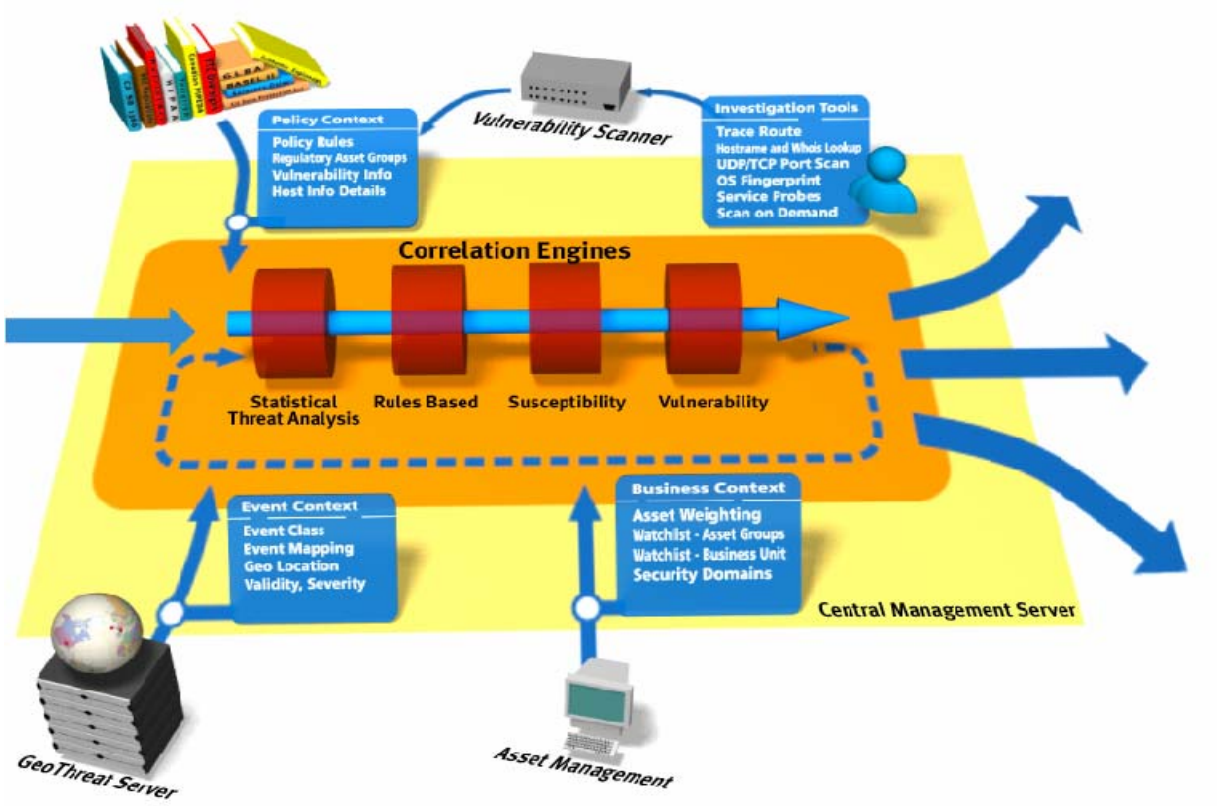
(Central Management Server)



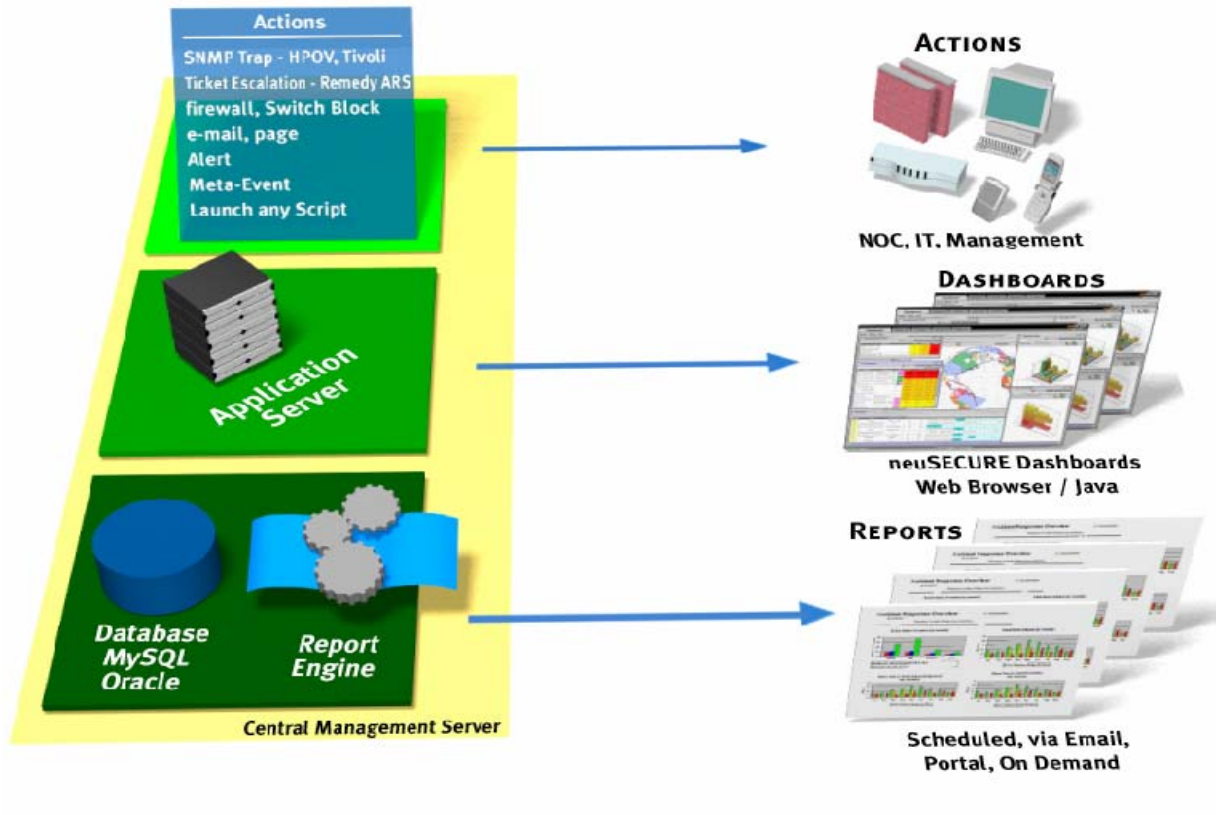
Event Collection



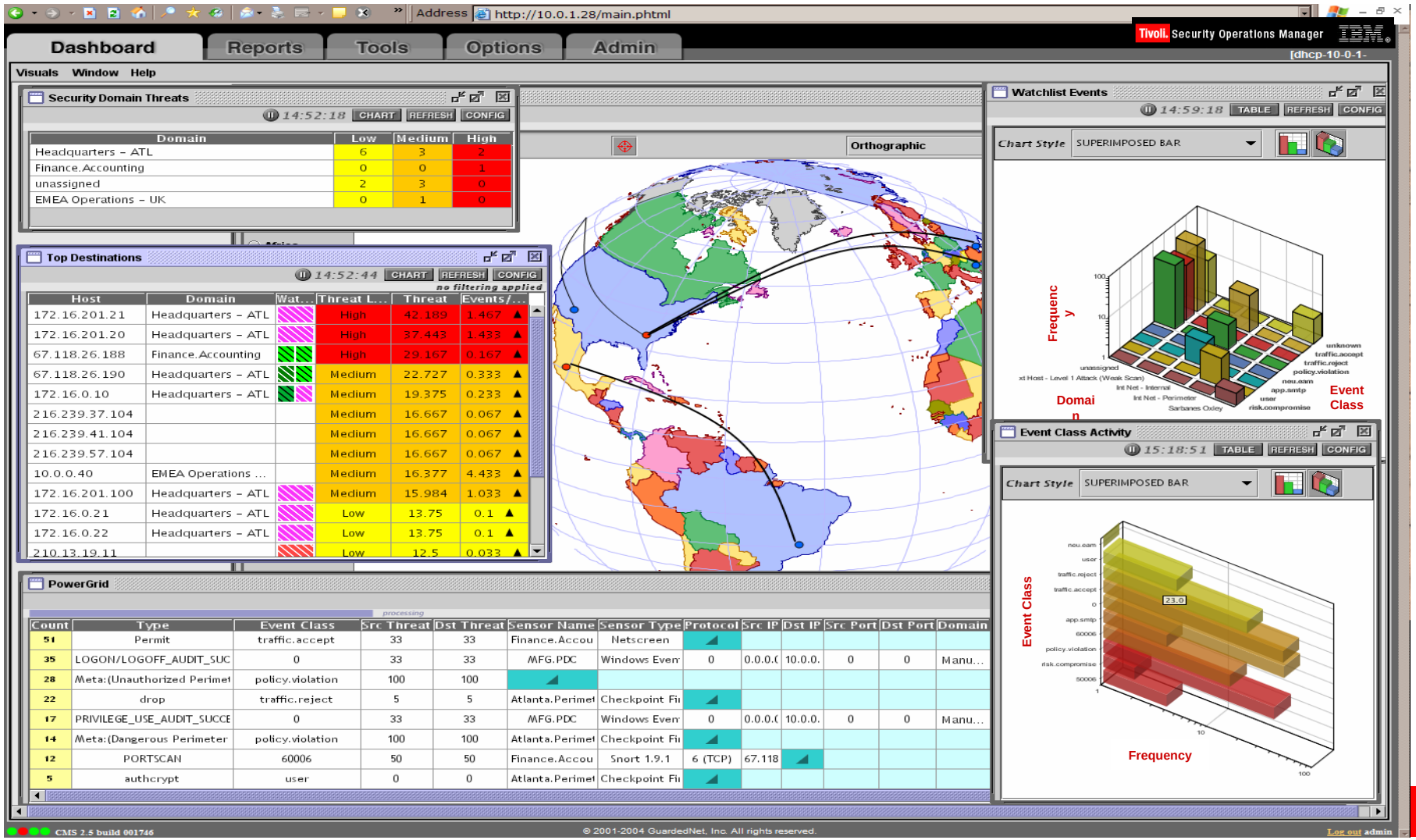
Event Correlation



Result


Actions
SNMP Trap - HPOV, Tivoli
Ticket Escalation - Remedy ARS
firewall, Switch Block
e-mail, page
Alert
Meta-Event
Launch any Script
Application Server
Database MySQL Oracle
Report Engine
Central Management Server
ACTIONS
NOC, IT, Management
DASHBOARDS
neuSECURE Dashboards
Web Browser / Java
REPORTS
Scheduled, via Email,
Portal, On Demand

Tableaux de bord consolidés et temps réel

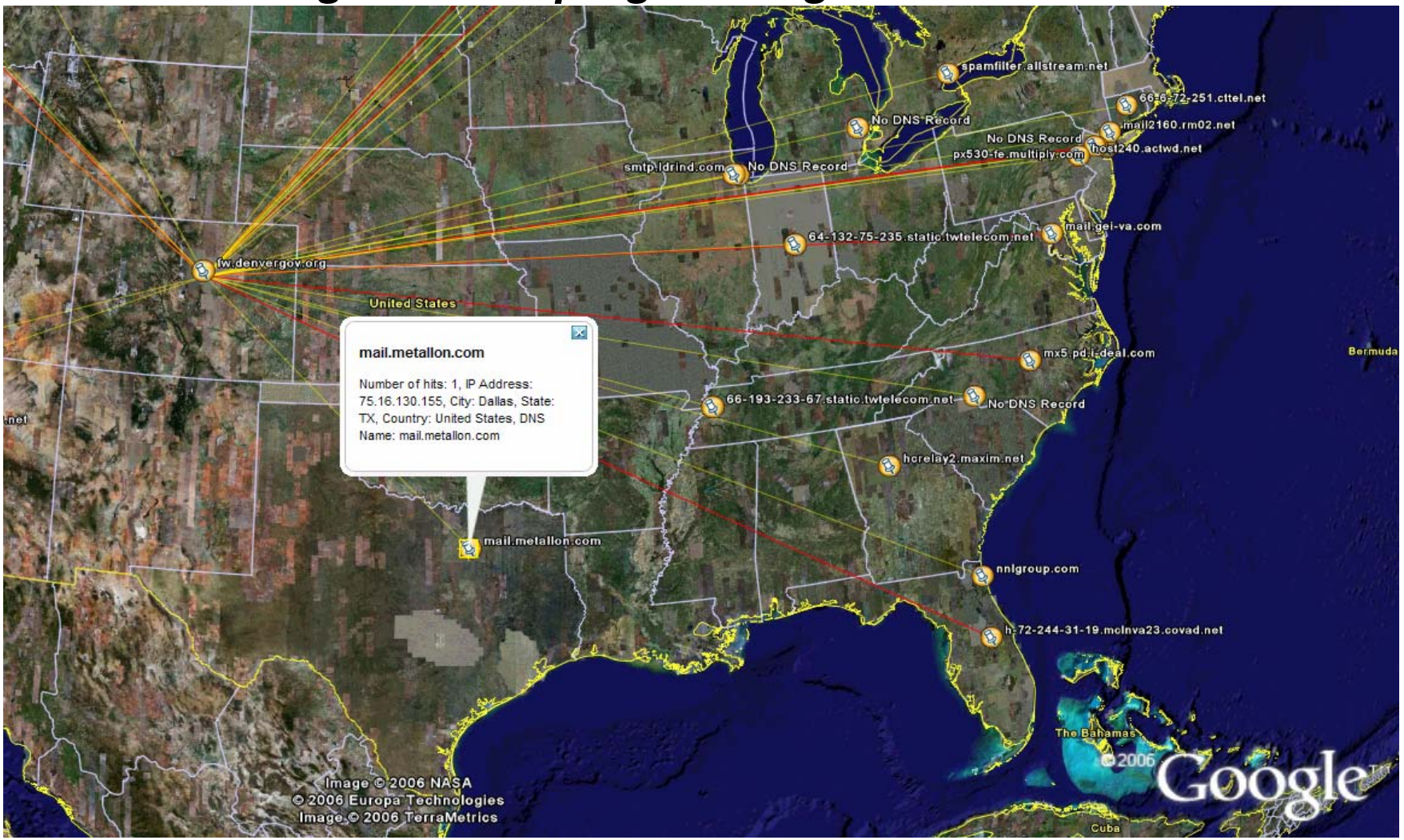


Un exemple : Logs PIX au format brut

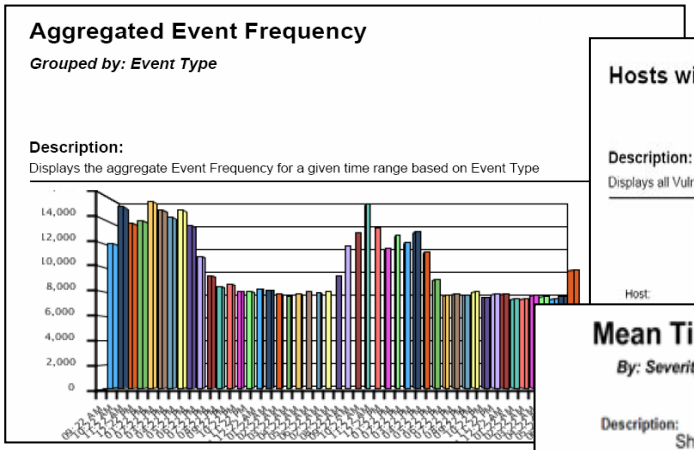
root@secsrv:~

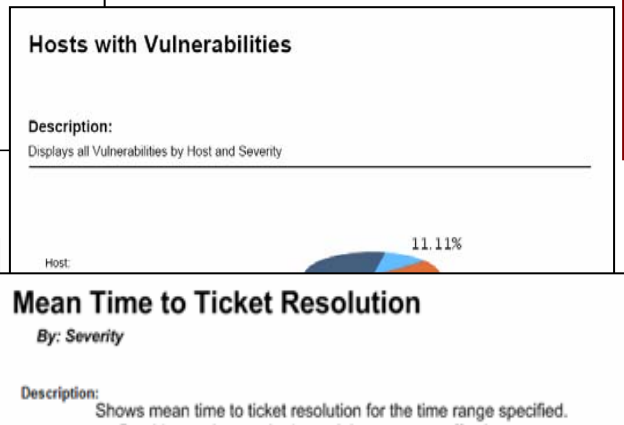
```
Oct 11 23:00:17 10.146.1.3 %PIX-4-106023: Deny tcp src outside:129.250.137.135/22789 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:17 10.146.1.3 %PIX-4-106023: Deny tcp src outside:208.213.162.234/41294 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:17 10.146.1.3 %PIX-4-106023: Deny tcp src outside:88.36.205.34/34169 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:17 10.146.1.3 %PIX-4-106023: Deny tcp src outside:193.60.199.89/54368 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:17 10.146.1.3 %PIX-4-106023: Deny tcp src outside:194.171.180.8/4856 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:17 10.146.1.3 %PIX-4-106023: Deny tcp src outside:66.9.3.114/17252 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:17 10.146.1.3 %PIX-4-106023: Deny tcp src outside:64.109.192.3/50953 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:17 10.146.1.3 %PIX-4-106023: Deny tcp src outside:206.108.184.244/11774 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:17 10.146.1.3 %PIX-4-106023: Deny tcp src outside:210.11.172.77/58919 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:17 10.146.1.3 %PIX-4-106023: Deny tcp src outside:12.160.0.85/8418 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:17 10.146.1.3 %PIX-4-106023: Deny tcp src outside:75.16.130.155/24621 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:17 10.146.1.3 %PIX-6-106015: Deny TCP (no connection) from 58.209.30.69/11294 to 199.239.30.102/25 flags RST  on interface outside
Oct 11 23:00:17 10.146.1.3 %PIX-4-106023: Deny tcp src outside:194.139.33.72/54668 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:17 10.146.1.3 %PIX-6-106015: Deny TCP (no connection) from 38.116.146.175/25 to 204.56.42.128/2303 flags FIN PSH ACK  on interface outsi
Oct 11 23:00:17 10.146.1.3 %PIX-4-106023: Deny tcp src outside:81.223.187.74/42114 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:17 10.146.1.3 %PIX-6-106015: Deny TCP (no connection) from 70.42.39.14/2703 to 199.239.30.107/59488 flags RST  on interface outside
Oct 11 23:00:17 10.146.1.3 %PIX-4-106023: Deny tcp src outside:194.167.143.7/31962 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:17 10.146.1.3 %PIX-4-106023: Deny tcp src outside:129.41.78.34/51859 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:17 10.146.1.3 %PIX-6-106015: Deny TCP (no connection) from 68.101.43.8/6234 to 204.56.46.227/25 flags FIN ACK  on interface outside
Oct 11 23:00:18 10.146.1.3 %PIX-4-106023: Deny tcp src outside:151.11.85.135/40748 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:18 10.146.1.3 %PIX-6-106015: Deny TCP (no connection) from 38.116.146.175/25 to 204.56.42.212/3018 flags FIN PSH ACK  on interface outsi
Oct 11 23:00:18 10.146.1.3 %PIX-4-106023: Deny tcp src outside:216.74.162.15/19560 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:18 10.146.1.3 %PIX-4-106023: Deny tcp src outside:69.9.43.74/34357 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:18 10.146.1.3 %PIX-4-106023: Deny tcp src outside:217.7.138.151/38036 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:18 10.146.1.3 %PIX-4-106023: Deny tcp src outside:192.38.94.2/53025 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:18 10.146.1.3 %PIX-4-106023: Deny tcp src outside:12.109.62.139/51831 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:18 10.146.1.3 %PIX-6-106015: Deny TCP (no connection) from 10.4.9.27/3065 to 205.178.146.50/80 flags RST  on interface inside
Oct 11 23:00:18 10.146.1.3 %PIX-4-106023: Deny tcp src outside:216.84.124.34/55794 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:18 10.146.1.3 %PIX-4-106023: Deny tcp src outside:166.84.0.211/58510 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:18 10.146.1.3 %PIX-4-106023: Deny tcp src outside:64.132.75.235/2432 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:18 10.146.1.3 %PIX-4-106023: Deny tcp src outside:72.244.31.19/4144 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:19 10.146.1.3 %PIX-4-106023: Deny tcp src outside:209.25.152.168/47268 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:19 10.146.1.3 %PIX-4-106023: Deny tcp src outside:134.157.0.129/52903 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:19 10.146.1.3 %PIX-4-106023: Deny tcp src outside:64.81.236.90/2275 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:19 10.146.1.3 %PIX-4-106023: Deny tcp src outside:64.81.188.26/8261 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:19 10.146.1.3 %PIX-4-106023: Deny tcp src outside:213.252.49.30/49673 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:19 10.146.1.3 %PIX-6-106015: Deny TCP (no connection) from 10.143.2.212/3045 to 69.15.190.186/143 flags RST  on interface inside
Oct 11 23:00:19 10.146.1.3 %PIX-4-106023: Deny tcp src outside:66.193.233.67/25280 dst inside:204.56.46.233/25 by access-group "outside_acl"
Oct 11 23:00:19 10.146.1.3 %PIX-6-106015: Deny TCP (no connection) from 217.157.198.116/60991 to 199.239.30.107/25 flags RST  on interface outside
```

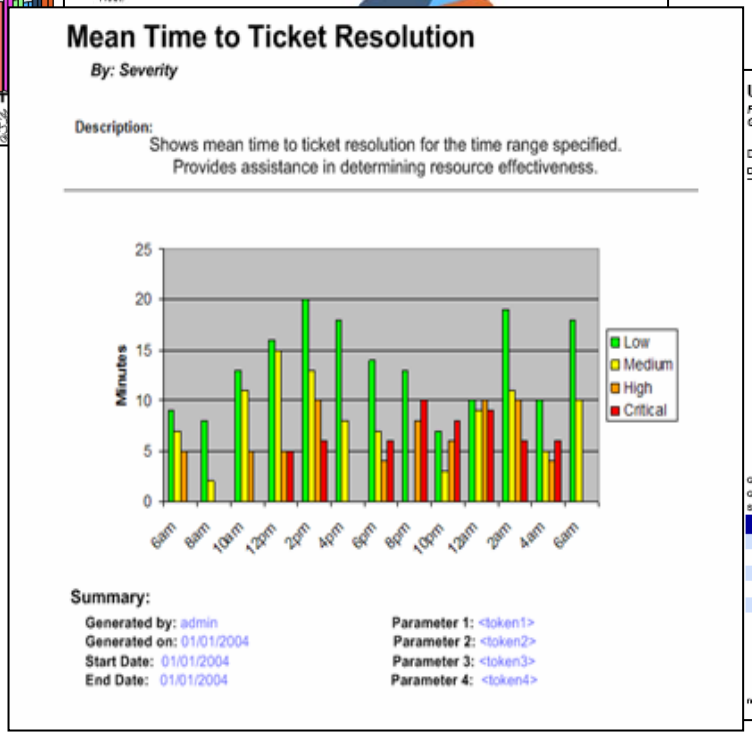
Les mêmes logs avec le plugin Google Earth

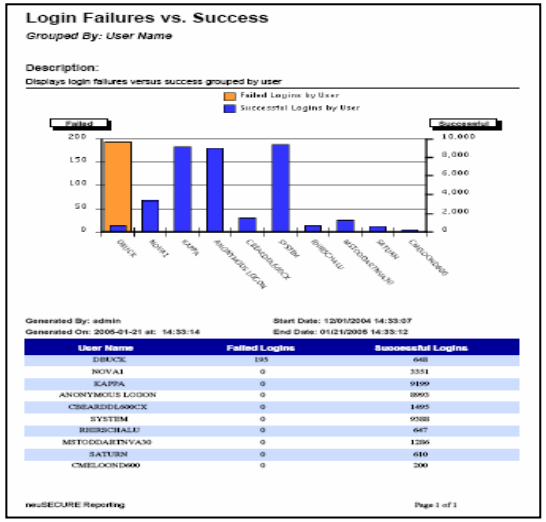


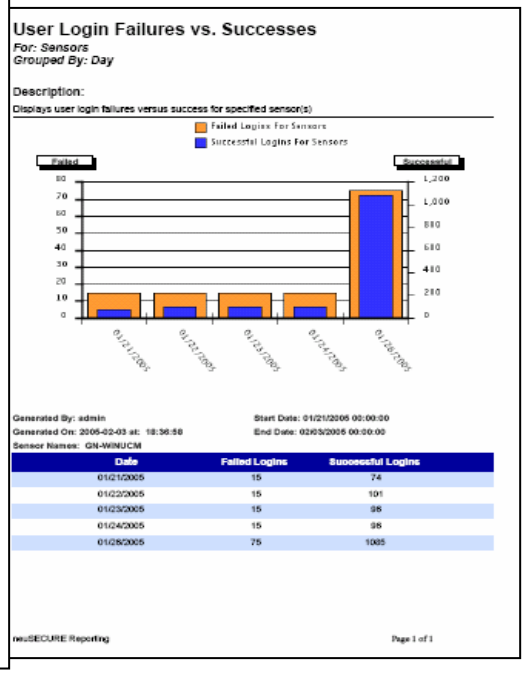
Reporting centralisé











Powerful Reporting Engine

Leveraging the power of TSOM complete set of reports and report templates provides a comprehensive view of your security posture over time. (**68 standard reports +**)

TSOM - Support de plus de 230 event & log sources, incluant :

Firewalls
Check Point Firewall-1
Cisco PIX
CyberGuard
Fortinet FortiGate
GNATBox
Juniper (Netscreen)
Linux IP Tables
Lucent Brick
Microsoft ISA Server
Nortel Switched Firewall
Stonesoft's StoneGate
Secure Computing's Sidewinder
Symantec's Enterprise Firewall
SonicWALL
Sun SunScreen

Vulnerability Assessment
ISS Enterprise Scanner
ISS Internet Scanner
Nessus
Vigilante QualysGuard
Foundstone
eEye Retina, REM
SPI Dynamics WebInspect
nCircle IP360
Harris STAT
Tenable Lightning

Routers/Switches
Cisco Routers
Cisco Catalyst Switches
Cisco RCMD
Foundry Switches
F5 Big IP, 3-DNS
Juniper JunOS
TACACS / TACACS+
Nortel Ethernet Routing Switch 5500, 8300, 8600, 400 series
Extreme Networks

Policy Compliance
Vericept

Application Security
Blue Coat Proxy
Nortel ITM (Intelligent Traffic Mgmt)
Teros APS
Sentryware Hive
IBM DataPower(coming soon)

Discovery Tools
Lumeta IPSonar
NMAP
Sourcefire RNA

Applications
Apache
Microsoft IIS
IBM WebSphere
Oracle Database Server
Lotus Domino
SAP R3
Peoplesoft

Operating Systems
Logs, Logging Platforms
Solaris (Sun) *
AIX (IBM)
OS/400 (I Series)
RedHat Linux
SuSE Linux
HP/UX
Microsoft Windows Event Log (W2K3 DHCP, W2K DHCP, IIS)
Microsoft SNMP Trap Sender
Nokia IPSO
Novell NetWare
OpenBSD
Tandem Non-Stop OS (HP)
Tru64
Tripplight UPS
Monitorware SYSLOG
KiwiSyslog

zOS-Mainframe IDS
Consul zAlert (coming Soon)

Antivirus
CipherTrust IronMail
McAfee Virus Scan
Norton AntiVirus (Symantec)
McAfee ePO
Trend Micro InterScan

Network Intrusion Detect/Prevention
McAfee Intrushield
Sourcefire Network Sensor
Sourcefire RNA
Juniper IDP
ISS Proventia G
ISS Proventia M
ISS Proventia ADS
ISS RealSecure Network Sensor
ISS BlackICE Sentry
Cisco Secure IDS
SNORT IDS
Enterasys Dragon
Nortel Threat Protection System (TPS)
Intrusion's SecureNetPro
Mirage Networks
NFR NID
Symantec ManHunt
ForeScout ActiveScout
QRadar
Top Layer Attack Mitigator
Labrea TarPit
IP Angel
Lancope StealthWatch
Tipping Point UnityOne NDS
Arbor Networks PeakflowX
Mazu Networks

Host-based Intrusion Detect/Prevention
ISS Proventia Server & Deskitop
ISS Server & OS Sensor
Type80 SMA_RT (zOS-Mainframe RACF)
PowerTech (iSeries-AS/400)
Cisco CSA
NFR HID
IBM Netcool SSMs
Sana
Snare
Symantec Intruder Alert (ITA)
Sygate Secure Enterprise
Tripwire
McAfee Entercept

Management Systems
Source of events into TSOM:
Check Point Provider-1
CiscoWorks
IBM Netcool (Micromuse)
ISS SiteProtector
ISS Fusion Module
Juniper Global Pro (Netscreen)
Juniper NSM (Netscreen)
Tripwire Manager
Intrusion, Inc. SecureNet Manager
McAfee ePO
Nortel Defense Center
Sourcefire Defense Center
Q1 QRadar Mgmt Server

VPN
Juniper SSL VPN
Nortel VPN Router (Contivity)
Check Point
Cisco IOS VPN, Cisco VPN 3000
Juniper VPN, Nortel VPN Gateway (SSL VPN)

Access and Identity Management
IBM Tivoli Access Manager
IBM Tivoli Identity Manager
Microsoft Active Directory
CA eTrust Access
CA eTrust Secure Proxy Server
CA eTrust Siteminder (Netegrity)
RSA SecureID RADIUS
Oracle Identity Management (Oblix)
Sun Java System Directory Server
Cisco ACS

Wireless Security
AirMagnet
AirDefense

Management Systems
TSOM escalates
IBM Netcool (Micromuse)
IBM/Tivoli Enterprise Console
Cisco Information Center
Remedy ARS
HP OpenView
CA Unicenter

Les différentiateurs de Tivoli Security Operations Manager (TSOM)

✓**COUVERTURE**: *Support de plus de 230 équipements en standard*

TSOM collecte les événements pertinents de la plus large liste d'équipements sécurité du marché (e.g. firewalls, IDS, IPS, VPN, AV, Routers, Servers, OS's, hosts, apps).

✓**MONTEE EN CHARGE**: *Plusieurs milliers d'événements par seconde*

L'architecture sans agent et modulaire de TSOM permet aux architectures SOC a plusieurs domaines de montée en puissance avec la base client.

✓**PERFORMANCE**: *Gestion de la sécurité en temps réel*

La conception modulaire de TSOM permet de tenir la charge de d'un flux extrêmement important d'événements et d'assurer un stockage tout en offrant la fonction de haute disponibilité.

✓**EFFICACITE**: *Optimiser la productivité grâce à l'automatisation*

L'automatisation possible grâce à TSOM et les fonctions d'intégration permettent au NOC d'améliorer l'efficacité des équipes et d'améliorer la disponibilité de l'infrastructure et des applications.

✓**CONNAISSANCE**: *Mise en avant de notre expertise sécurité*

L'expertise sécurité est construite dans le produit avec des algorithmes de corrélation brevetés, des règles prédéfinies, des rapports préexistants et tout un ensemble d'outil d'analyse des incidents sécurité.

Agenda

Présentation de l'Offre Tivoli Security

Les Challenges de l'Audit et de la Conformité

La solution: IBM Tivoli's SIEM

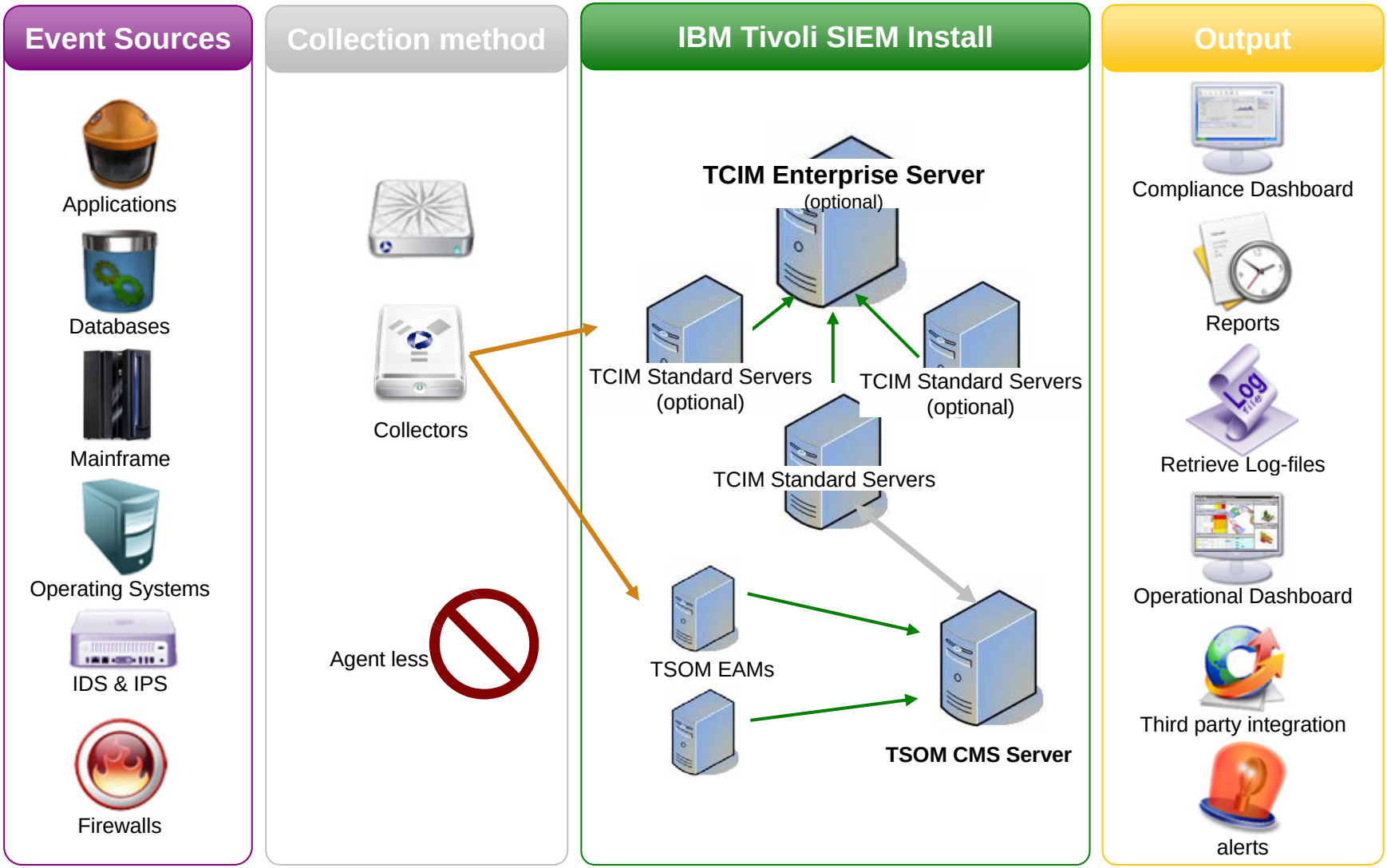
Architecture

IBM Value Proposition

Proven Results

Questions

Architecture d'intégration: Tivoli Security and Compliance



Tivoli software

Roadmap

Security Compliance & Audit Solutions

IBM

High Level Integration Roadmap Tivoli SIEM

TSOM

- **Cross-product alerting**
- **Integrated event & log collection infrastructure**
- **Combined storage infrastructure**
- **User Interface**
  - Contextual links, Tivoli common UI framework
- **Integrated reporting**

TCIM

2007 2008 2009 2010

TSOM & TCIM evolving into single, integrated product family

TSOM

Tivoli Security Operations Manager 4.1
Improved event processing, filtering, and correlation architecture

Simplified, centralized device configuration

Dashboard - customizable, higher performance

Localized Language versions & Internationalization support

Improved Incident investigation, case management, KB

DB2 support

Compliance Module
- *COBIT*

Compliance Module
- *ISO 27001 update*

Compliance Module
- *PCI*
- *ITIL*

Tivoli SIEM integrated release
Integrated release, but can purchase SEM/SIM/Log Mgmt components
Harmonized, Integrated collection layer for events and logs
UI integration
Common Reporting Engine
Ticketing gateway, MRO integration
Full Unix or Windows deployment
SSO across components
SEM Device Wizard
Globalization
Common Compliance Modules
Integrated Terminology and Docs

Tivoli SIEM Log Management
Integrated Log Management Infrastructure & configuration
Single Log depot
Log reporting

- Integrated GUI, Tivoli UI
- Extended security intelligence, pre-built KCIs & KRIs and content
- Risk Management
- Centralized agent rollout
- Unified data storage
- Single and centralized policy
- Enhanced Usability
- Appliances

TCIM

Tivoli Compliance Insight Manager 8.0
Enhanced reporting
Automated Report Distribution
Toolkits for building indexers
Agentless i-Series Collect

Event Sources
- Tivoli Identity Manager:
- Tivoli Access Manager

Event Sources
- Oracle Financials
- mySAP
- Tivoli Fed. Identity Mgr, TDS, TCM
- Tivoli Configuration Manager

Ongoing Event Sources
- Continued Realtime Event Source integration with IBM and 3rd party products
- Extended correlation rules & security content
- Additional Reports
- ISS native events API
- Native Netflow data

2007 2008 2009 2010

Agenda

Présentation de l'Offre Tivoli Security

Les Challenges de l'Audit et de la Conformité

SEM versus SIM

La solution: IBM Tivoli's SIEM

Architecture

IBM Value Proposition

Proven Results

Questions

Tivoli software

Aspects Financiers

Security Compliance & Audit Solutions

IBM

Principes de tarification

- **Prise en considération des équipements réseau et applicatifs**
- **Nombre de Serveurs :** AIX, Solaris, HP-UX, Windows, i5/OS, Linux, Netware, OpenVMS, Tandem, Stratus)
- **Nombre d'équipements Réseau :** Routeurs, Switches, Hubs & Bridges
- **Nombre d'équipements de Sécurité** : Firewalls, IDS, IPS, VPNs, anti-virus gateways, Fltrage de conteny (Web, email), solution de détection des comportents réseau anormaux et appliances de sécurité multi- fonctions.
- **Nombre d'applications & bases de données :** DB2, Oracle, SQL Server, Sybase; incluant DB2 sur le mainframe. Les applications incluent SAP, MS Exchange, Lotus Domino, et les middlewares comme les solutions de Gestion des identités et des Accès. (par exemple les solutions IBM Tivoli TIM, TAM, TFIM, TDS, etc
- **Nombre de partition logiques du Mainframe**

Tivoli software

IBM est Stratégique

Security Compliance & Audit Solutions

IBM

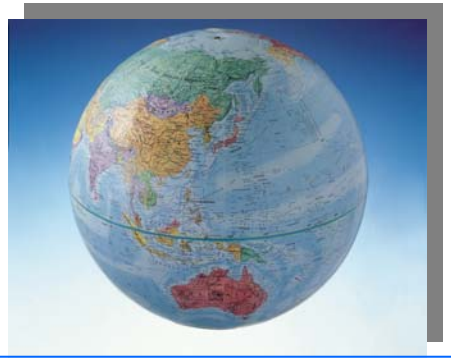
IBM Tivoli Software – Leader In Infrastructure Management

IBM Tivoli Software is used by over 20,000 enterprise customers worldwide:

- *95% of Fortune 500 companies worldwide*

IBM Tivoli Security software is used by:

- *4 of the top 5 telecommunications companies worldwide*
- *15 of the top 20 commercial bank companies worldwide*
- *6 top health care companies worldwide*
- *6 of the top 10 aerospace and defense companies worldwide*
- *7 of the top 10 computer and data service companies worldwide*



IBM Tivoli – A Global Support & Development team:

- *2100 development professionals in 6 worldwide labs*
- *Only Infrastructure Management vendor with 500 people Lab in Europe*
- *Global presence with local delivery in Europe and Latin America, using consistent proven methodology, intellectual capital and best practices worldwide*
- *24x7 Support*

Tivoli : Innovation et leadership

Mise à jour : IBM rachète MRO pour 740 M$

Edition du 05/08/2006 - par Michel Bourdier / IDG News Service

Avec MRO, IBM pousse encore la promotion de son architecture SOA et signe probablement son plus gros rachat d'ici la fin de l'année. Surtout Big Blue répond u… après à HP qui avait très tôt gonflé OpenView en in… Peregrine pour la gestion d'actifs.

IBM adapte Tivoli Identity Manager aux PME

Edition du 22/02/2006 - par Elian Cordoue

IBM se lance à l'assaut des PME/PMI avec Tivoli Express

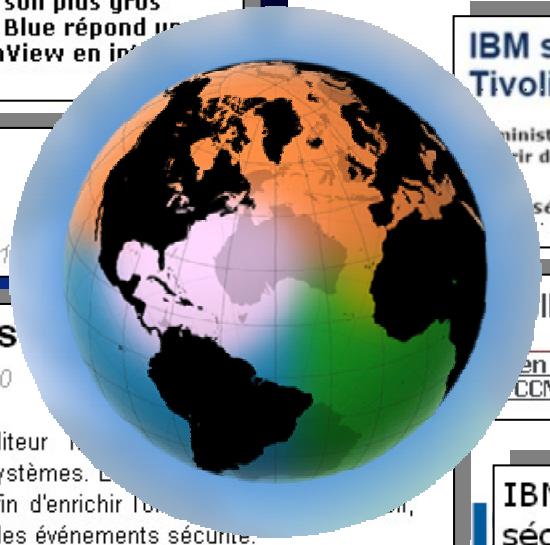
…inistrer; sécuriser, superviser : les PME vont pouvoir …ir des solutions abordables

…sé Diz

Toute l'actualité ▸ Business ▸ Article.

IBM avale ISS

par Christophe Dupont-Elise, le 23/8/2006 à 1…



…lles solutions IT Service Management,

…en exclusivité ses nouvelles solutions IT Service …CCMDB.

IBM s'offre Micromus…

par Jerome Saiz, le 21/12/2005 à 16:50

IBM annonce l'acquisition de l'éditeur … surveillance des applications et des systèmes. … des technologies complémentaires afin d'enrichir l'… notamment en matière de corrélation des événements sécurité.

IBM renforce ses outils d'audit en sécurité et en conformité avec Consul Risk Management

Edition du 06/12/2006 - par Elian Cordoue

IBM muscle la gestion des actifs dans sa gamme Tivoli

Par Laurent Dupin
ZDNet France
17 août 2005

IBM rachète Vallent

Edition du 30/11/2006 - par Elian Cordoue

IBM dope sa gamme Tivoli avec ses récentes acquisitions

Edition du 06/10/2006 - par Christophe Bardy

Tivoli software

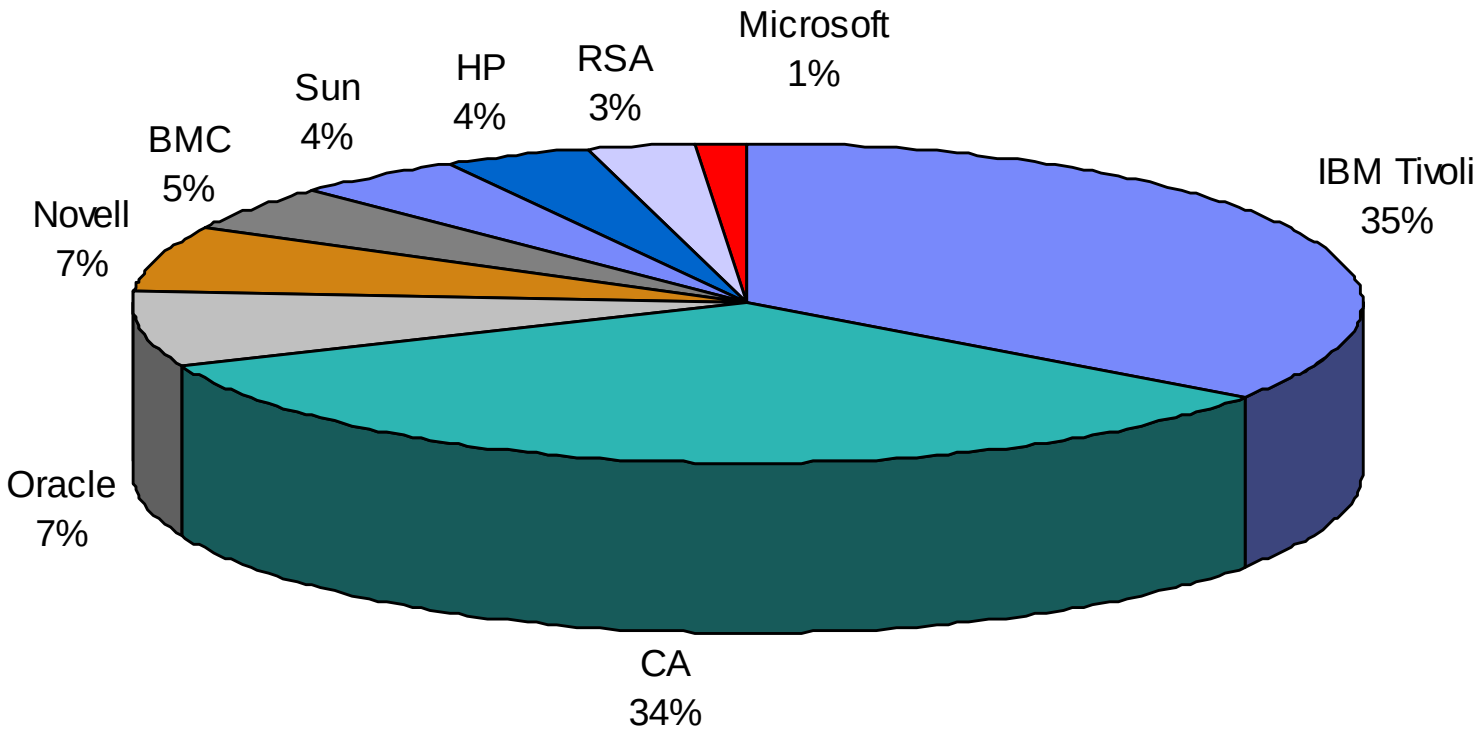
IBM Tivoli
leader sur les marchés
IAM, SIEM et SOA

La vue des Analystes

Security Compliance & Audit Solutions

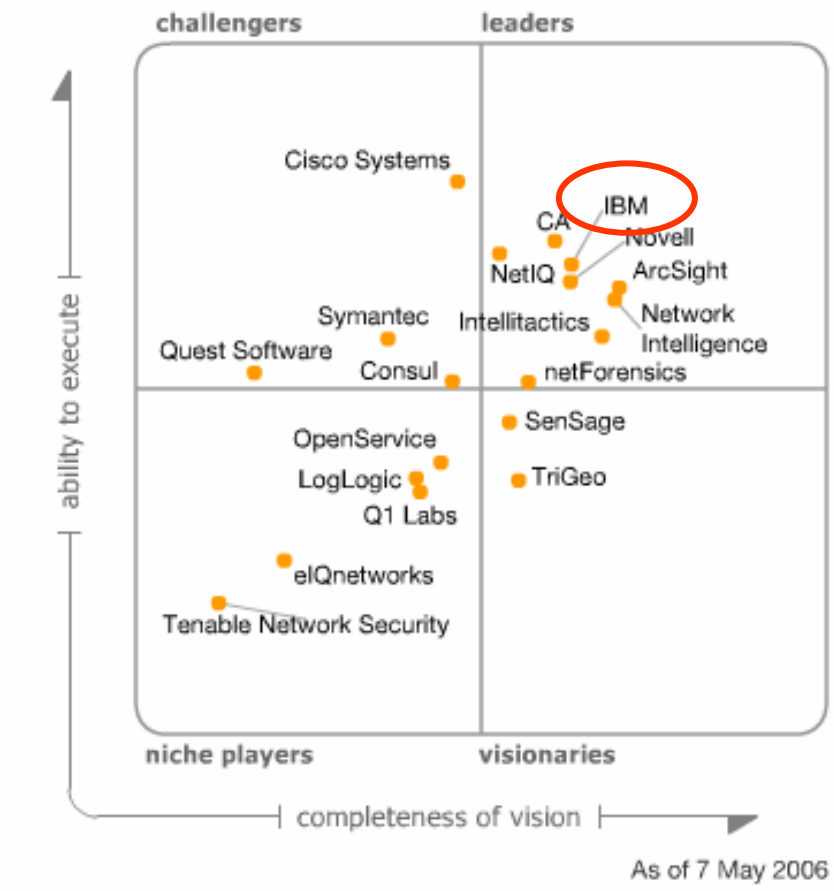
IBM

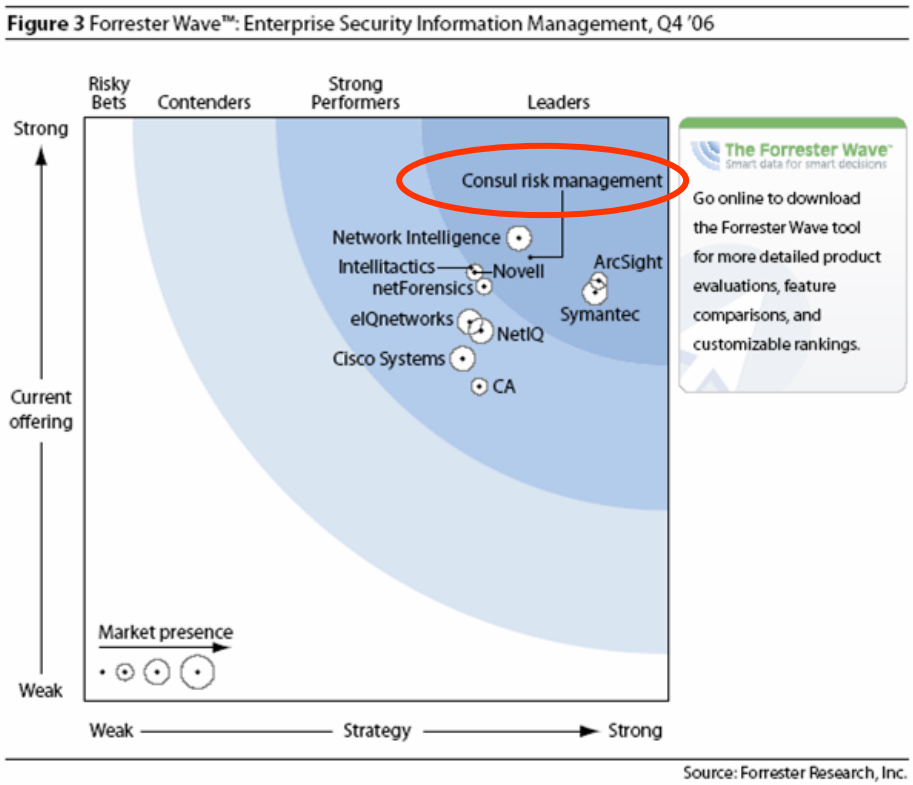
IBM - # 1 by Market Share in Security Software *(IDC 2006)*



IBM - # 1 in Security & Event Management

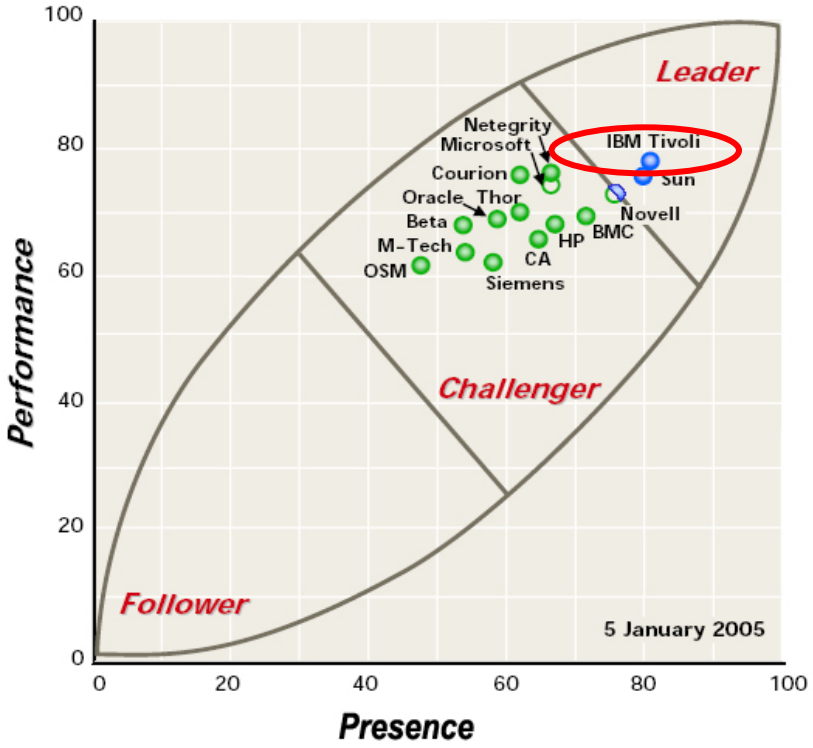
Gartner Magic Quadrant & Forrester Wave - for Security Information and Event Management



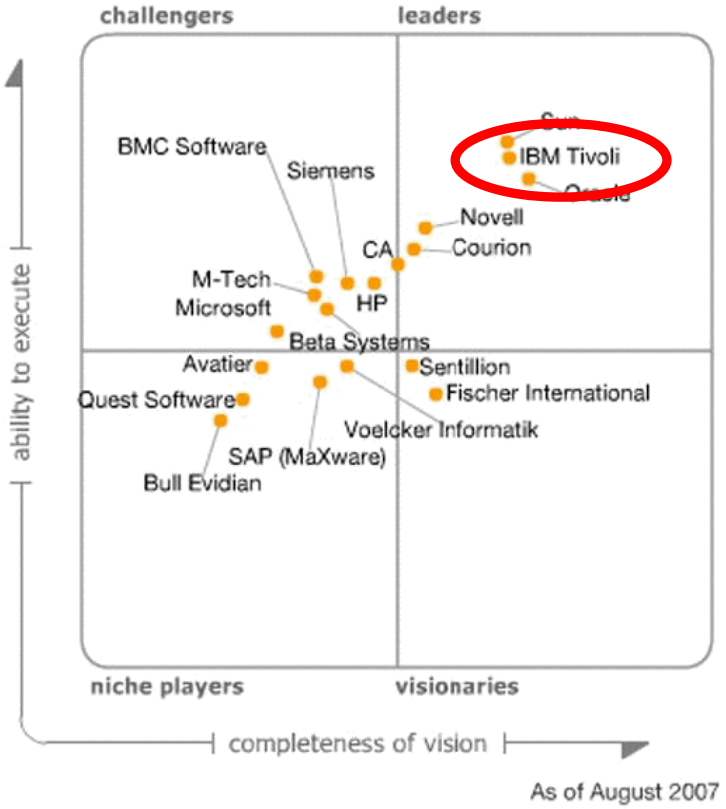


IBM - # 1 in Identity Management

Meta: ITIM Product Leadership



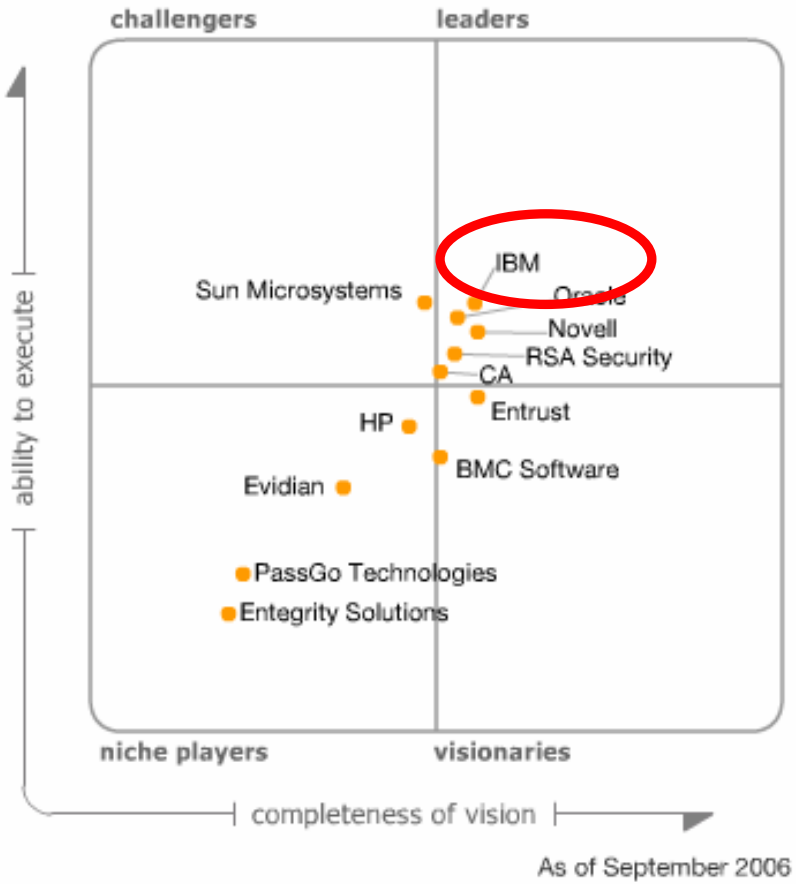
Gartner : Magic Quadrant for User Provisioning



IBM - # 1 in Access Management

Gartner Magic Quadrant for Web Access Management

Figure 1. Magic Quadrant for Web Access Management, 2H06



Note: Formerly called the Magic Quadrant for Extranet Access Management

Source: Gartner (September 2006)

IBM - # 1 in Enterprise Single Sign-On

Gartner Magic Quadrant for Enterprise Single Sign-On

Tivoli Access Manager for Enteprise Single Sign-On (TAM eSSO) is an OEM product from Passlogix

Tivoli software

IBM Tivoli

References

Security Compliance & Audit Solutions

IBM

Références SIEM

Multinational Insurance Company	To close compliance gaps for SOX; centralize collection, monitoring, and reporting of millions of log files; and provide transparency into the activities of privileged users across a heterogeneous network.
Major US Payment Processor	To prepare for federal regulations and to meet the requirements of the VISA CISP, this large payment processor brought Consul onboard to help audit enterprise IT.
Major Office Supplies Store	The Manager of Data Security began looking for a solution to audit their entire enterprise IT environment.
Large US Grocery Chain	
Industrial Cleaning Firm	Needed IT audit solution they could roll-out across the corporate network to audit AIX, mainframe, UNIX, Windows and OS/400, and then to 2,500 stores.
Major Office Equipment Manufacturer	In order to meet SOX requirements and IT Security best practices, the Director of IT Security began looking for a product that could help them manage their log data.
Global Food Manufacturer	Company received a mandate from their CEO to comply with federal regulatory requirements, specifically Sarbanes-Oxley

Références IAM

- **IDENTITY MANAGEMENT**
  - ING Group : **113 000 utilisateurs**
  - Alcatel : 88 000 utilisateurs (France)
  - Royald Ahold : 70 000 utilisateurs
  - Beyond Petroleum : 155 000 utilisateurs
  - France Télécom : **200 000 utilisateurs** (France)

WEB ACCESS MANAGEMENT

- T Rowe Price : **1,5 Millions utilisateurs**
- Orange : 10 Millions d'utilisateurs
- La Banque Postale : **15 Millions d'utilisateurs**
- AT&T : 500 000 utilisateurs
- IBM : 300 000 utilisateurs
- Fortis : 120 000 personnes

Références françaises IAM

Tivoli software

CONCLUSIONS

Security Compliance & Audit Solutions

IBM

Tivoli software

Questions?

Customers Worldwide

Recognized by the press and analysts