



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?



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

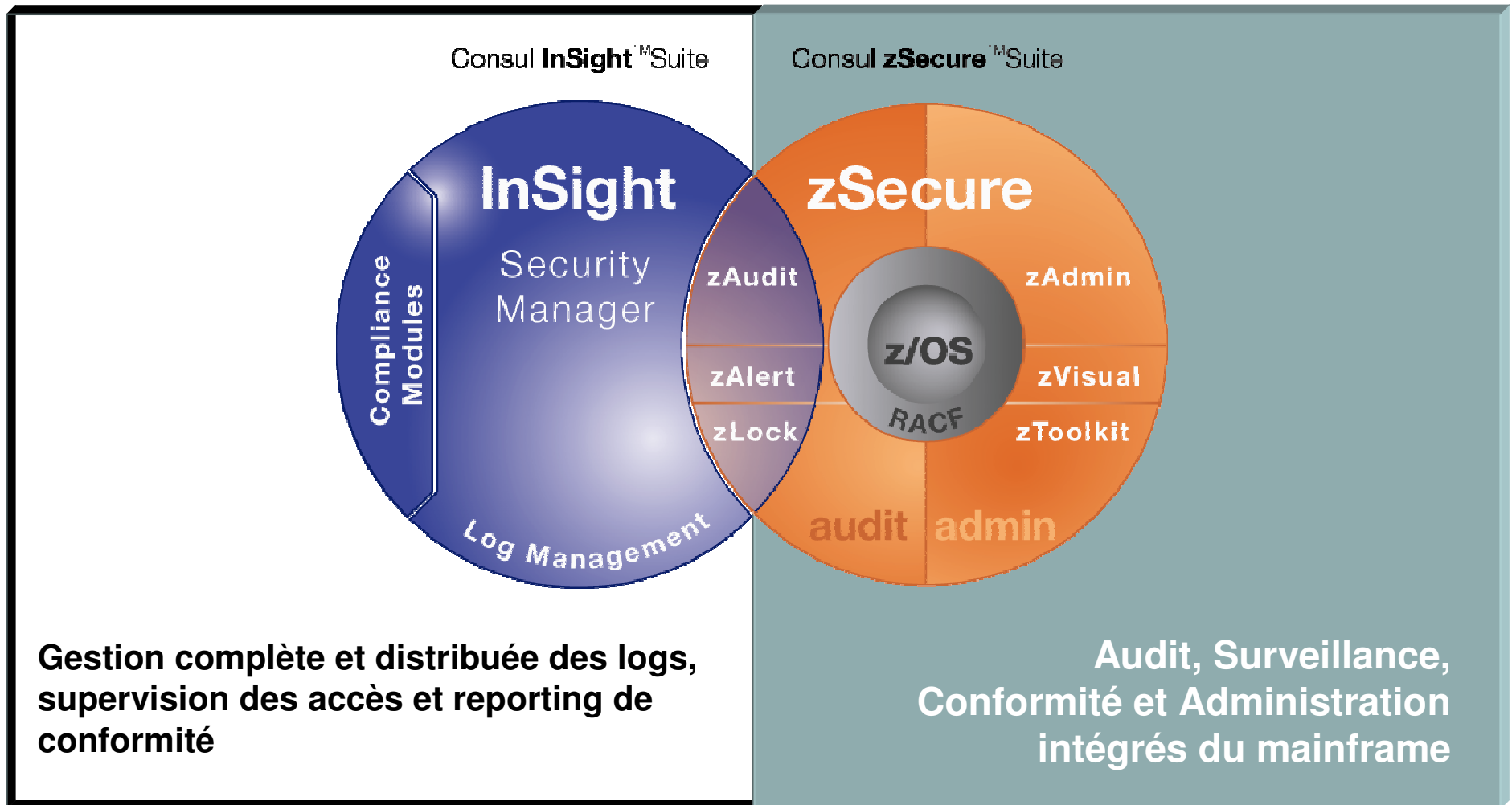
Commentaires du Carnegie Mellon CERT:

- “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



Surveiller les utilisateurs privilégiés n'est plus une option !

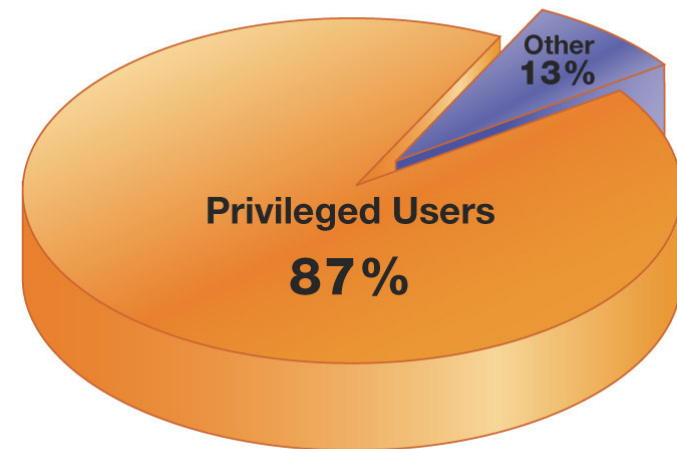
87% des incidents internes sont causés par des utilisateurs privilégiés

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:

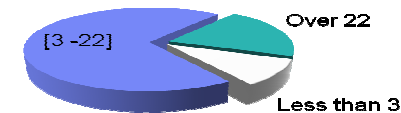
- Les attaques internes représentent 6% du chiffre d'affaire annuel
- Aux USA, ceci représente un coût de 400 milliards de dollars

Who Causes Internal Incidents?



Source: USSS/CERT Insider Threat Survey 2005

Annual Sensitive Data Breaches



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

The IBM Tivoli SIEM Solution



TENDANCES LOGICIELLES D'ÉTÉ 2008

SESSION SPÉCIALE GESTION DES RISQUES OPÉRATIONNELS



Security Information and Event Management

$$\text{SIEM} = \text{SEM} + \text{SIM}$$

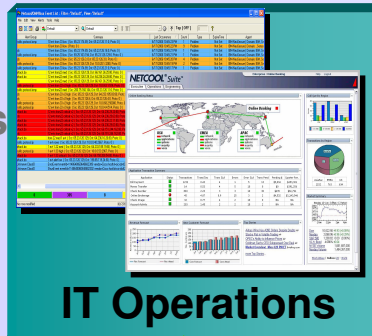
Gestion des Incidents

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

IT Security
Internal Audit

Policy-based

Who?

SIM

Syslogs, SNMP traps, ...



Network Infrastructure



Network Security



Desktops



Servers



Applications



Databases

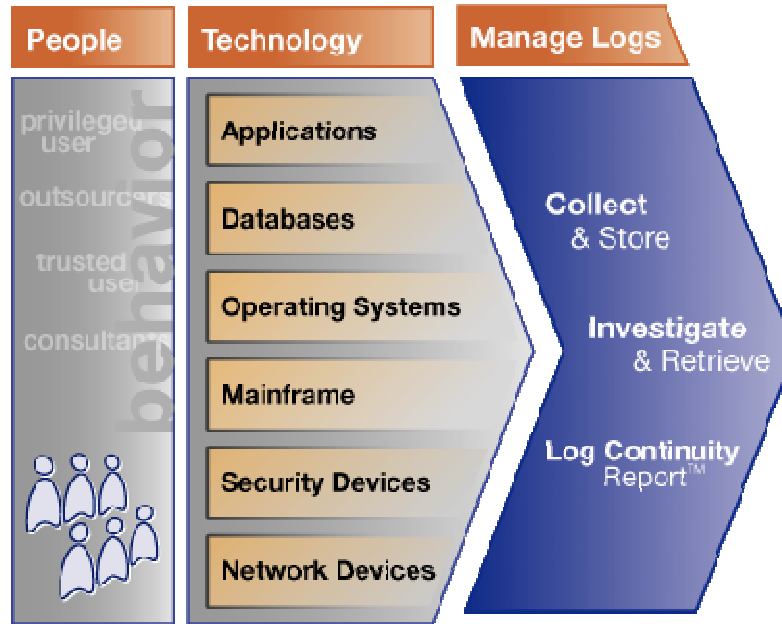


User focused log sources

Audit trails, extended security events, ...

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

Security audit (SECURITY) on APPLES, system id: 2074
Auditable event: Batch process login
Event time: 1-MAR-2005 00:02:09.84
PID: 20402844
Process name: BATCH_440
Username: SYSTEM
Process owner: [SYSTEM]
Image name: DSA0:[SYS1.SYSCOMMON.][SYSEXE]LOGINOUT.EXE
Posix UID: -2
Posix GID: -2 (%FFFFFFFFE)

Security audit (SECURITY) on CYGNUS, system id: 2073
Auditable event: Network login
Event time: 1-MAR-2005 00:02:16.11
PID: 2021A46D
Process name: MQMTC_P2_BG164
Username: MQM
Process owner: [MQS_SERVER]
Image name: DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE
Remote node id: 241859594
Remote node fullname: xyzz.bananajunior.com
Remote username: MQM
Posix UID: -2
Posix GID: -2 (%FFFFFFFFE)

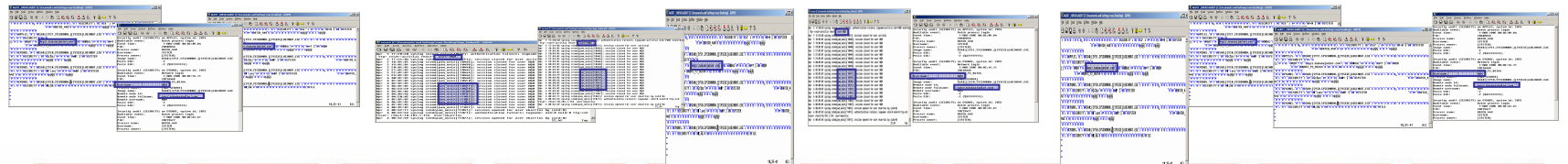
Security audit (SECURITY) on CYGNUS, system id: 2073
Auditable event: Batch process login
Event time: 1-MAR-2005 00:02:32.61
PID: 20219477
Process name: BATCH_443
Username: SYSTM
Process owner: [SYSTEM]

secure (C:\Documents and Settings\ross\Desktop\logs_fedora3) - GVIM3
Apr 5 17:20:30 syslog su(pam_unix)[10429]: authentication failure; logname=tty=ruser=acrystal rhost= user=MQM
Apr 5 17:22:03 syslog sshd(pam_unix)[10351]: session closed for user acristal
Apr 5 18:01:01 syslog crond(pam_unix)[10436]: session closed for user MQM
Apr 5 19:01:01 syslog crond(pam_unix)[10438]: session closed for user MQM
Apr 5 20:01:01 syslog crond(pam_unix)[10440]: session closed for user MQM
Apr 5 21:01:01 syslog crond(pam_unix)[10442]: session closed for user MQM
Apr 5 22:01:01 syslog crond(pam_unix)[10444]: session closed for user MQM
Apr 5 23:01:01 syslog crond(pam_unix)[10446]: session closed for user MQM
Apr 6 00:01:01 syslog crond(pam_unix)[10448]: session closed for user MQM
Apr 6 01:01:01 syslog crond(pam_unix)[10450]: session closed for user MQM
Apr 6 02:01:01 syslog crond(pam_unix)[10452]: session closed for user MQM
Apr 6 03:01:01 syslog crond(pam_unix)[10477]: session closed for user MQM
Apr 6 03:33:29 syslog crond(pam_unix)[10479]: session closed for user MQM
Apr 6 04:01:02 syslog crond(pam_unix)[10509]: session closed for user MQM
Apr 6 04:03:46 syslog crond(pam_unix)[10511]: session closed for user MQM
Apr 6 04:30:02 syslog crond(pam_unix)[11012]: session closed for user MQM
Apr 6 05:01:01 syslog crond(pam_unix)[11031]: session closed for user MQM
Apr 6 06:01:01 syslog crond(pam_unix)[11033]: session closed for user MQM
Apr 6 07:01:01 syslog crond(pam_unix)[11035]: session closed for user MQM
Apr 6 08:01:01 syslog crond(pam_unix)[11037]: session closed for user MQM
Apr 6 08:42:11 syslog sshd(pam_unix)[11041]: session opened for user ebarrios by (uid=0)
Apr 6 08:42:43 syslog sshd(pam_unix)[11071]: authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.101.1.154 user=ebarrios
Apr 6 08:42:49 syslog sshd(pam_unix)[11077]: session opened for user ebarrios by (uid=0)
22,45 Top

TENDANCE

SESSION SPÉCIALE GESTION DES RISQUES OPÉRATIONNELS

Tous les journaux sont traduits en un même langage

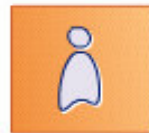


Windows z/OS AIX Oracle SAP ISS FireWall-1 Exchange IIS Solaris

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!

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

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

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 graphic Settings

Actions

- 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

Direct Database Access Report



Time period setup

Start time: Month: Day: Year: Hour: Min.:
 End time: Month: Day: Year: Hour: Min.:

 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 : Dbject / 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 : Dbject / Success	Oracle Finance	Jim Hofferan	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
2	Sun Sep 03 2006 09:00:06 GMT-05:00	1	Access : Dbject / Success	Oracle Finance	Jim Hofferan	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
50	Sun Sep 03 2006 09:00:06 GMT-05:00	1	Access : Dbject / 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 : Dbject / 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 : Dbject / 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 Hofferan	DB2 Server	DATABASE : - / Unavailable	DB2 Server
50	Sun Sep 03 2006 09:20:01 GMT-05:00	1	Access : Dbject / Success	DB2 Server	Jim Hofferan	DB2 Server	DBOBJECT : Finance/fn_op / Fn_op	DB2 Server
50	Sun Sep 03 2006 09:20:01 GMT-05:00	1	Access : Dbject / 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 : Dbject / 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 : Dbject / Success	Oracle Finance	Mike Bonfire	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance

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 P

Portal > Dashboard > Regulations > Sarbanes Oxley > Operational Change Report > Eventlist > Event-

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 50 Administration 40
Where	SRV_DC_034 (Windows)	Finance Server 50
Who	Jim Hofferma	Administrators 30 Database Admin 30 Finance Admin 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 Hofferma

Investigate

Logrecords...

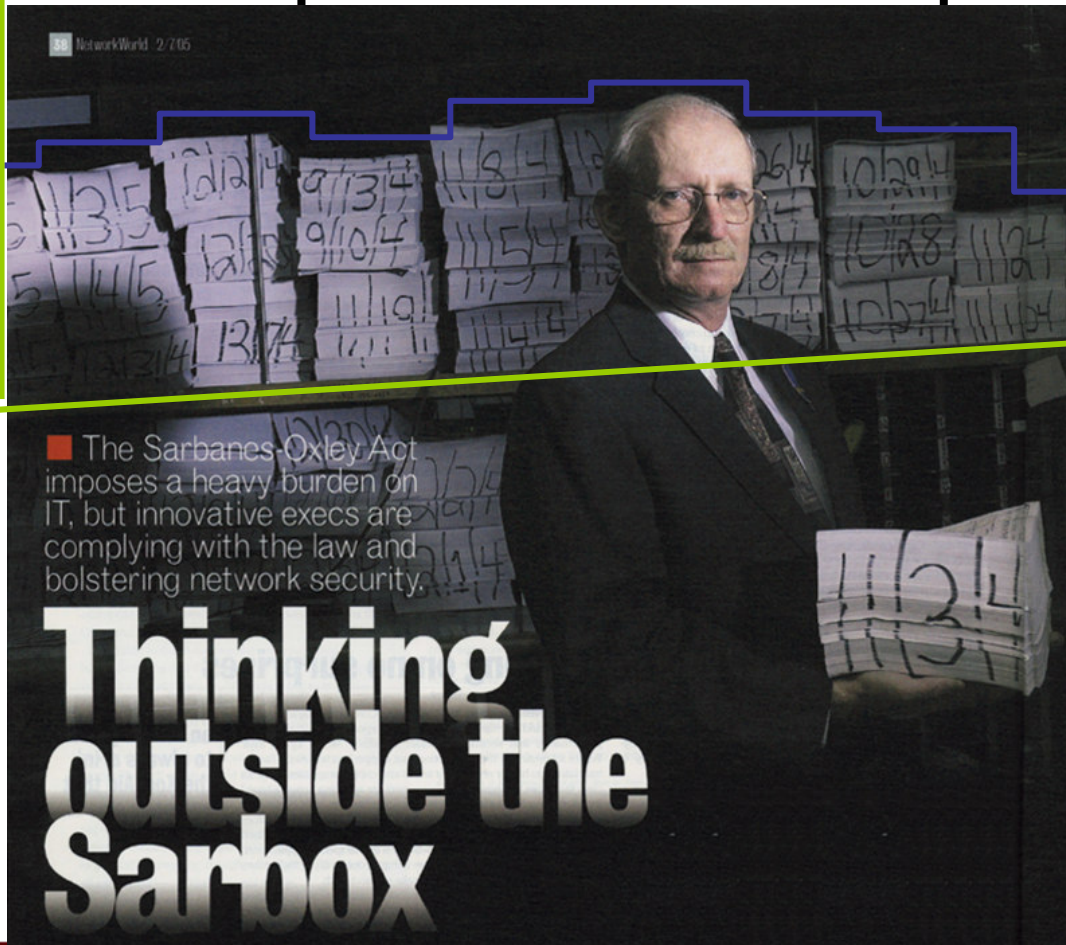
```

AUDIT_200503.AUDIT (C:\Documents and Settings\ross\Desktop) - GVIM2
File Edit Tools Syntax Buffers Window Help
^F^A^@T^@k^@;^@^C^@^@^@^@^@^@L^@F^@SECURITY^L^@2^@S3^`z^A^@H^@)^@D^@ $^@8^@SYSTEM
^H^@z^H^@^@^@
^G^@APPLES.^@S^@DSA0:[SYS1.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^F^@E^@T^@N^@i^@^C^@^@^@^@^@
^L^@F^@SECURITY^H^@+^@
|j^N^G^@-^@MQM^V^@~^@xyzz.bananajunior.com^L^@2^@0d0dz^A^@H^@)^@m^! $^@8^@MQM
^R^@*^@MQMTC_P2_BG164^H^@/^@^@A^@A^@H^@M^@p^@j^@j^@H^@X^@p^@j^@j^@
^H^@v^H^@^@^@
^G^@CYGNUS.^@S^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^F^@A^@T^@k^@;^@^C^@^@^@^@^@
^L^@F^@SECURITY^L^@2^@Lanz^A^@H^@)^@w^! $^@8^@SYSTEM ^H^@*^@BATCH_4
443^H^@/^@^@A^@^@H^@M^@p^@j^@j^@H^@X^@p^@j^@j^@
^H^@v^H^@^@^@
^G^@CYGNUS.^@S^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^Z^@A^@U^@U^@T^@A^@C^@^@^@^@^@
^L^@F^@SECURITY^H^@0^@;^@H^@0^@A^@^@H^@^@A^@^@A^@^@H^@0^@FILE
~
~
~
10,35-41 ALL
My Computer
  
```


Des rapports, automatiques et tout prêts,
pour communiquer

Communiquer

activity ↑



■ The Sarbanes-Oxley Act imposes a heavy burden on IT, but innovative execs are complying with the law and bolstering network security.

**Thinking
outside the
Sarbox**

time →

Dashboard > Regulations

Compliance Modules

- Basel II
 - Introduction
 - Classification Template
 - Policy Template
 - Reports
 - Documentation
- Gramm-Leach-Bliley Act (GLBA)
 - Introduction
 - Classification Template
 - Policy Template
 - Reports
 - Documentation
- Health Insurance Portability and Accountability Act (HIPAA)
 - Introduction
 - Classification Template
 - Policy Template
 - Reports
 - Documentation
- ISO 17799
 - Introduction
 - Classification Template
 - Policy Template
 - Reports
 - Documentation
- Sarbanes Oxley (SOX)
 - Introduction
 - Classification Template
 - Policy Template
 - Reports
 - Documentation

Classification Template

Download the template to use in the management Console.

Who

What

Group Name	Description
Alerts	Alerts generated by system devices resources
Alerts - High	Alerts generated by system devices resources - High
Alerts - Low	Alerts generated by system devices resources - Low
Alerts - Medium	Alerts generated by system devices resources - Medium
Exposure - High	description of Exposure - High
Exposure - Low	description of Exposure - Low
Exposure - Medium	description of Exposure - Medium
Intrusion - High	description of Intrusion - High
Intrusion - Low	description of Intrusion - Low
Intrusion - Medium	description of Intrusion - Medium
Intrusions	Intrusions reported by IDS devices

When

Group Name	Description
Office Hours	Normal working hours for staff
Out of Office Hours	Out of normal working hours
Weekend	Non-working days

Where

Extra Information

Help

Contact us

In the US:
contactusa@consul.com
Direct Line: +1 703 675 2022
Toll Free (US only): 800 258 5077

EMEA and Asia Pac:
contactasia@consul.com
Direct Line: +31 15 251 3333

@consul.com
1 703 675 2022

Policy Template

Download the template to use in the management Console.

Policy Rules

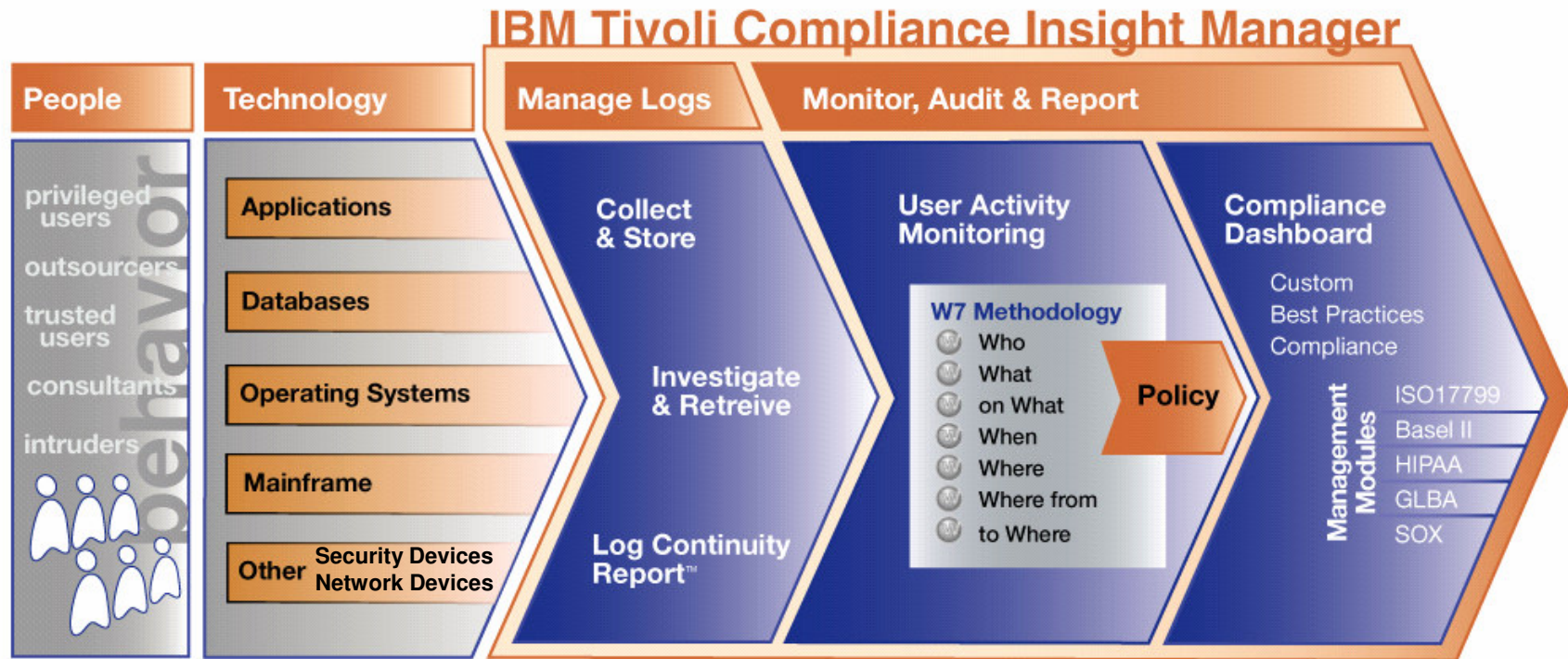
Attention Rules

Who group	What group	When group	Where group	outthat group	From/where group	WhereTo Group ID	Severity	Description
HR Management	Intrusion - Medium	Office Hours					30	Review
	Customer Information Systems						50	Requires attention
Administrators			HR - Medium				40	Requires attention
Administrators			Financial - Medium				50	Requires attention
Administrators			Customer Data				50	Requires attention
Administrators			Financial - High				70	Requires immediate attention
IT			Sensitive				20	Review
Unknown	Customer						25	Review

Sarbanes Oxley Regulation Reports

Title	Description
Sarbanes Oxley (FFEC 1.1.4) Security Policy report	No description given
Sarbanes Oxley (FFEC 1.3.1) Classification report	No description supplied
Sarbanes Oxley (8.3.1.3) Security alert	Alerts sent in response to policy exceptions or special attention exceptions
Sarbanes Oxley (8.1.2) Operational change control	Changes to the operating environment such as system updates, O&A activity etc.
Sarbanes Oxley (8.1.6) External contractors	Exceptions and failures caused by External Contractors
Sarbanes Oxley (8.3) Malicious attacks	Exceptions and failures due to Malicious attacks
Sarbanes Oxley (8.4.2) Operator log	Actions performed by the IT Admin staff
Sarbanes Oxley (8.5) Network management	Actions and events caused by users on Network Services
Sarbanes Oxley (8.7.4.1) Mail server	Exceptions and failures for the Mail Server assets
Sarbanes Oxley (8.7.6) Policy available systems	Actions and exceptions on Policy Holder Data
Sarbanes Oxley (9.2.4.9.7) Review of user access rights	Actions performed by administrators on users
Sarbanes Oxley (9.2.4.9.7) System access and use	Successes and failures against key assets
Sarbanes Oxley (9.3) User responsibilities and password use	Login failures and successes either locally or remotely
Sarbanes Oxley (8.4) Network access control	Actions performed on and events and exceptions generated by Network or Router
Sarbanes Oxley (8.4.4) Node authentication	Authentication of connections to remote computer systems
Sarbanes Oxley (8.4.5) Remote diagnostic port access	Detection of accesses to the diagnostic ports on servers
Sarbanes Oxley (9.5.3) User identification and authentication	Login/Logout successes and failures
Sarbanes Oxley (9.5.5) System utilities	Usage of system utilities
Sarbanes Oxley (9.6) Application access control	Actions, Exceptions and events on HR Data, Sensitive Data, User Sensitive Data, System, Financial Data, Proprietary Data and General Data
Sarbanes Oxley (9.6.1) Information access restrictions	Who accessed sensitive or private data successfully or unsuccessfully
Sarbanes Oxley (9.6.2) Sensitive system isolation	Exceptions and failures against sensitive systems data in asset groups User, HR Data, Source Code, and Financial Data
Sarbanes Oxley (9.7.3) Logging and reviewing events	Exceptions and failures recorded by the iSDigit system
Sarbanes Oxley (9.8.1) Mobile access	Exceptions and failures for mobile workers

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 gratuitement :

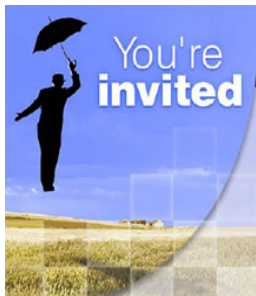
une adresse E-mail à retenir:
TecParis@fr.ibm.com

– 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 ...



You're invited

« Les équipes Sales et TechSales de IBM Software, sont à votre disposition pour réserver des machines et des ateliers »

