IBM Software Group

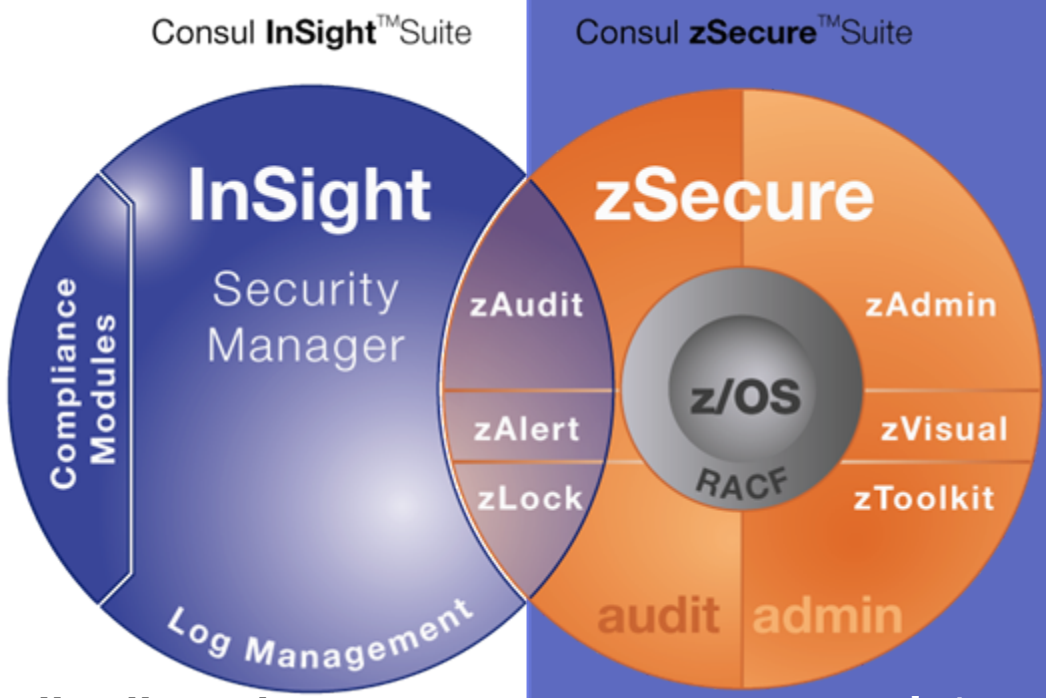
Tivoli Compliance InSight Manager (TCIM)

Quel est le comportement des utilisateurs sur mes systèmes et mes données sensibles?

Michael Cable,
IBM Software Group, Tivoli

Tivoli software

Supervision sur toutes les plate-formes

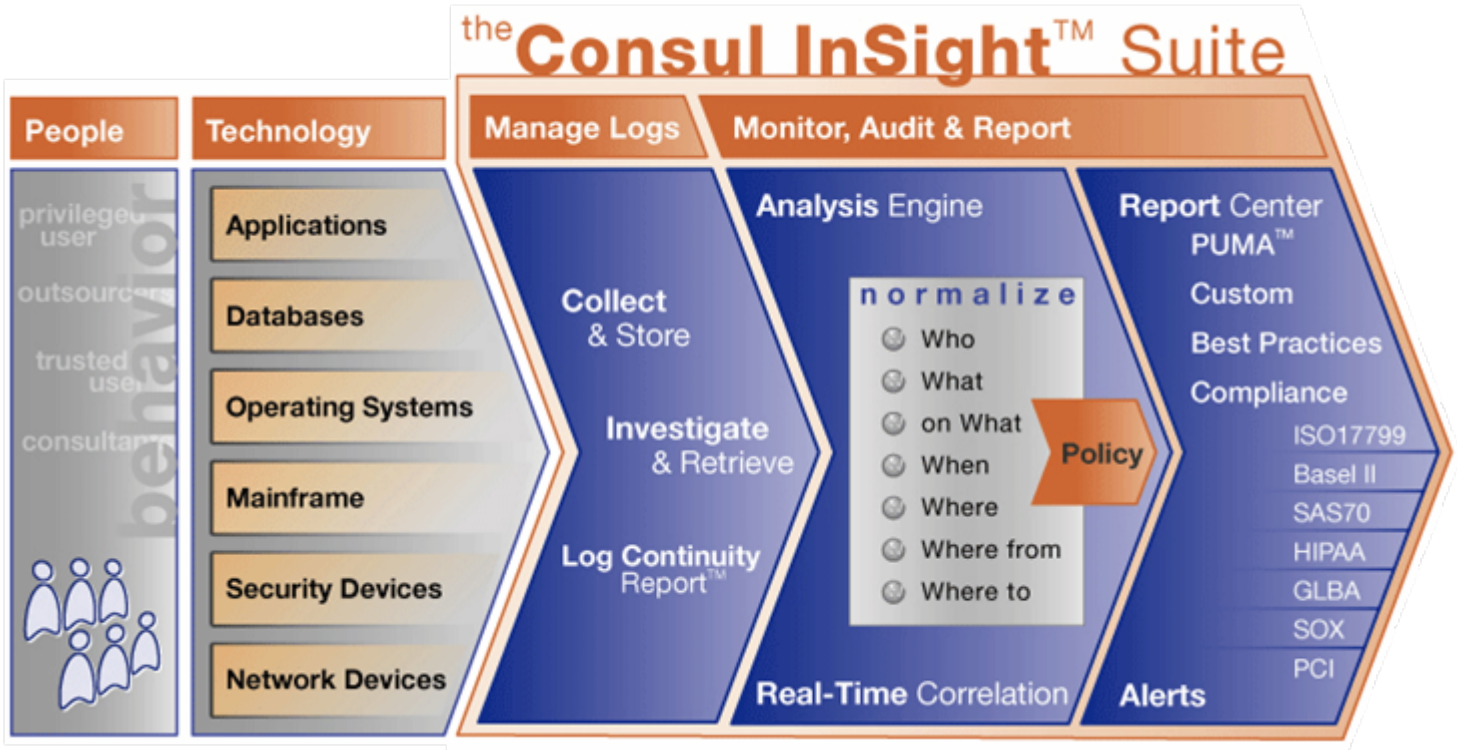


Comprehensive, distributed log management, access monitoring and compliance reporting

Integrated mainframe audit, monitoring, compliance and administration

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 comportement acceptables.



Supervision des Utilisateurs Privilégiés (90% des incidents internes); Audit des accès aux Databases et Application, Compliane/Conformité (ISO, Sarbanes Oxley, …); Comportement des utilisateurs, consultants externes, outsourcers, …

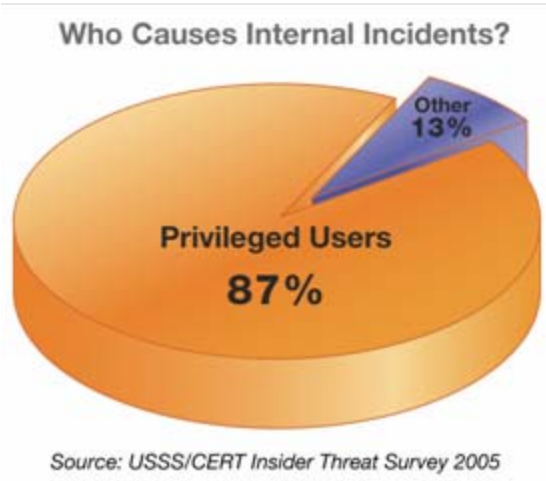
Ferez-vous la prochaine “Une” des journaux?

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Massive Insider Breach At DuPont

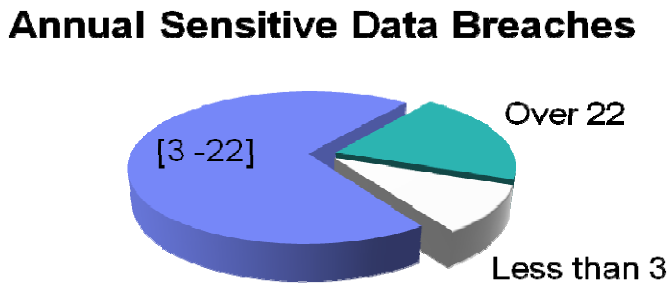
A research chemist who worked for DuPont for 10 years before accepting a job with a competitor downloaded 22,000 sensitive documents and viewed 16,706

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.



“Le meilleur moyen de sauvegarde contre les incidents internes pour les sociétés est de **superviser les activités anormales lors d’accès au réseau et aux banques de données** et de déterminer un niveau d’utilisation acceptable pour différents types d’utilisateurs”

Source: InformationWeek, Feb. 15, 2007



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

Le questionnaire “Security Audit and Compliance”

IT and Business management’s questions:

- 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?
- Avez-vous des 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 d’investiguer des incidents sans délais?

Your auditors’ questions:

- 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?

Conformité aux législations

[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.

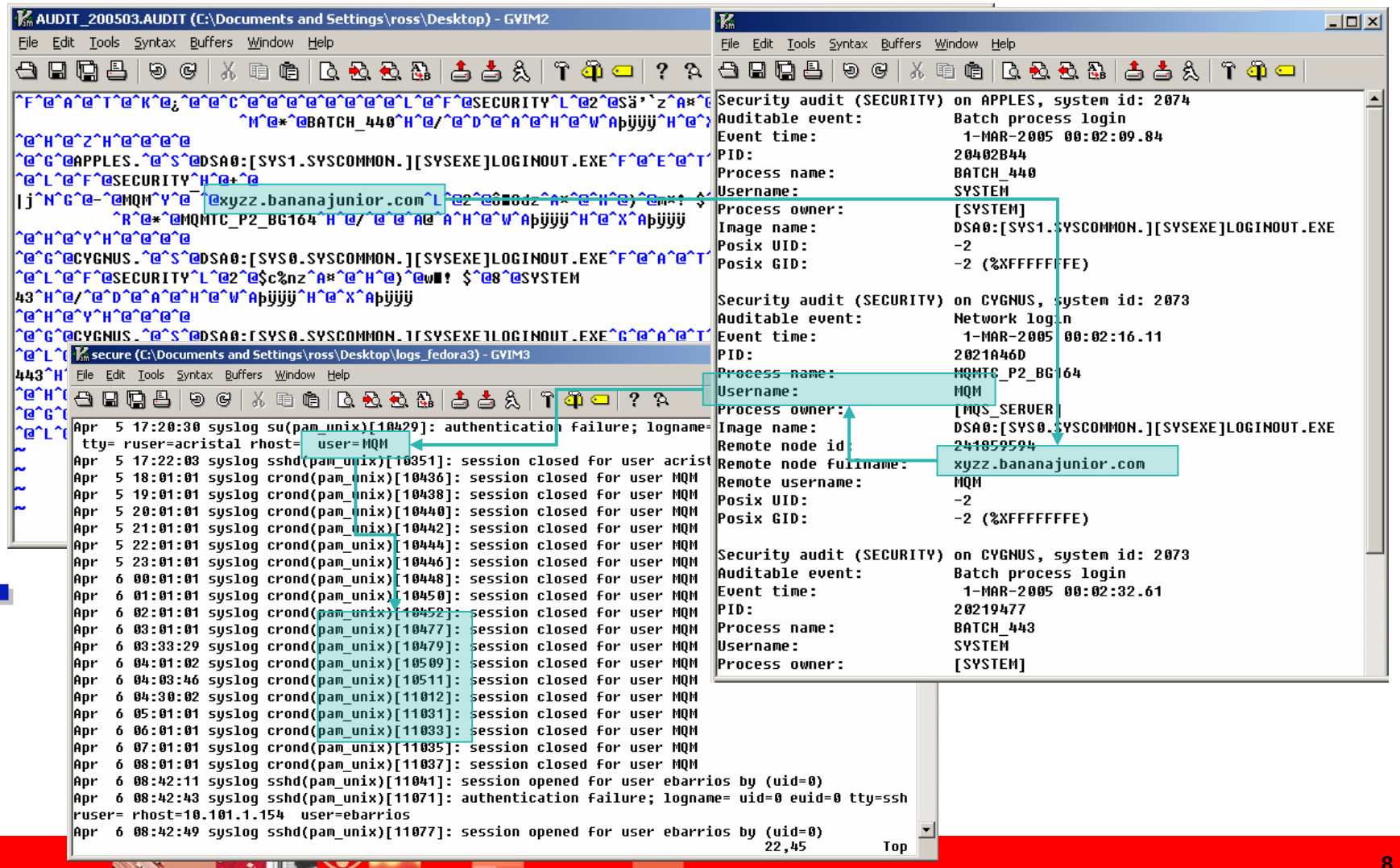
Que font les utilisateurs sur mes systèmes?

Comparer le comportement "Désiré" Versus "Réel"

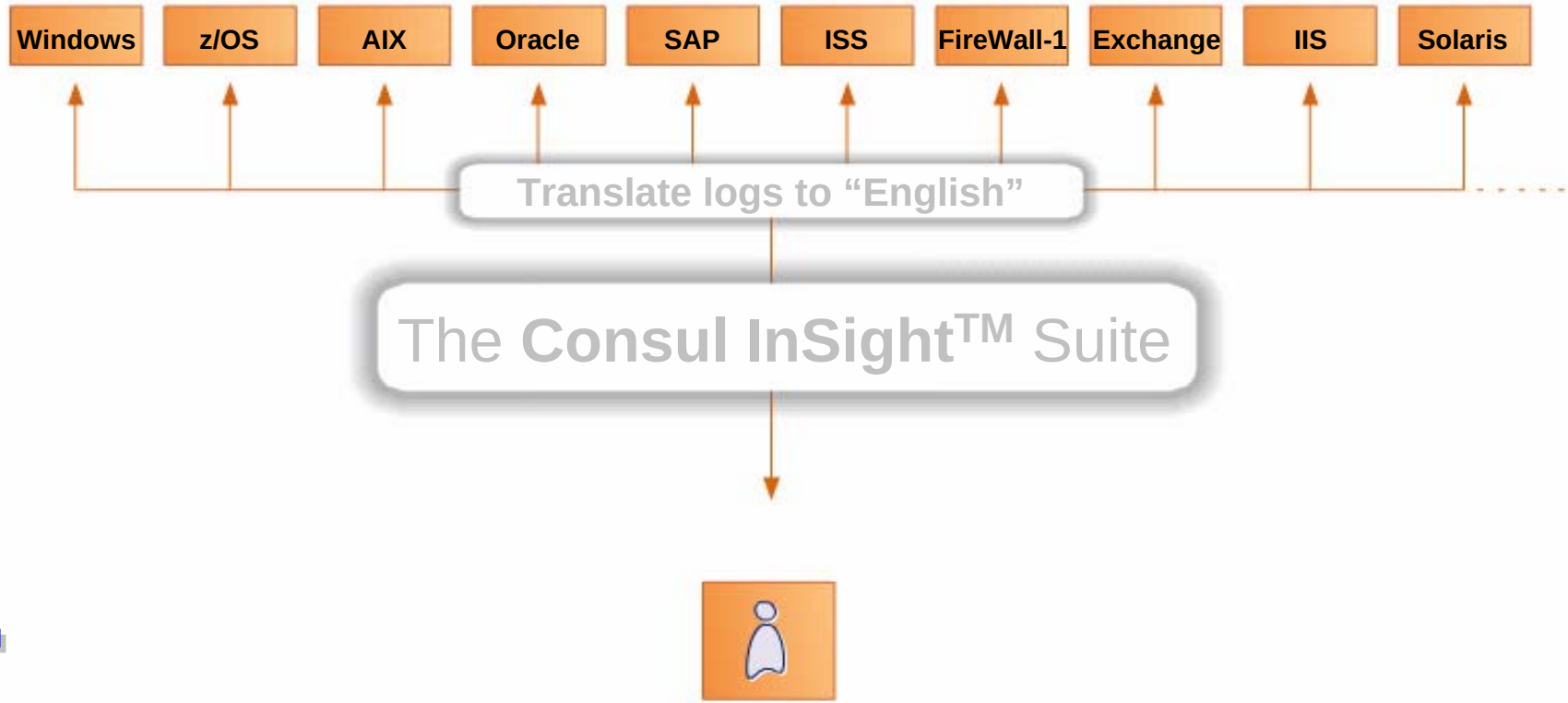
Comprendre

Comment comprendre tous ces différents formats et informations?

Comprendre



Tous les journaux sont traduits en un même language



Comprendre

Traduire les journaux dans un language efficace: 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!

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

consul

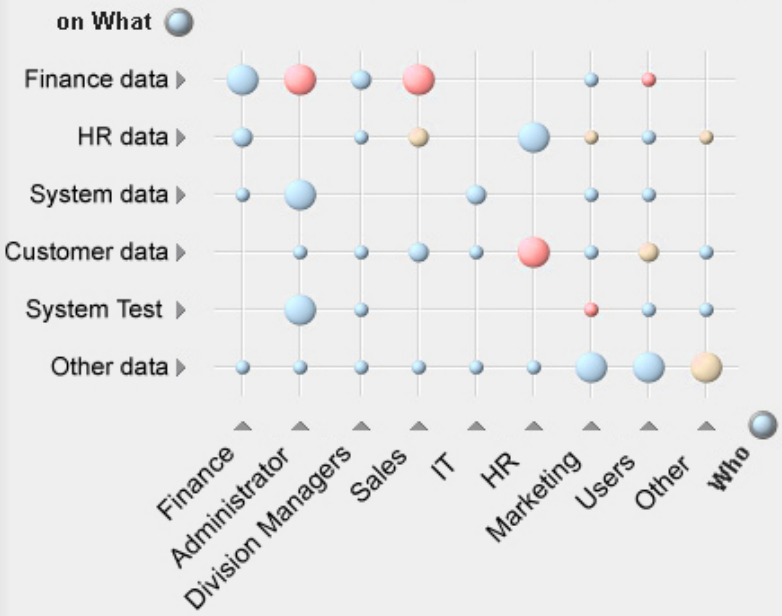
Compliance Dashboard
Logs after W7 – Billions of log files summarized on one overview graphic!

Compliance Dashboard

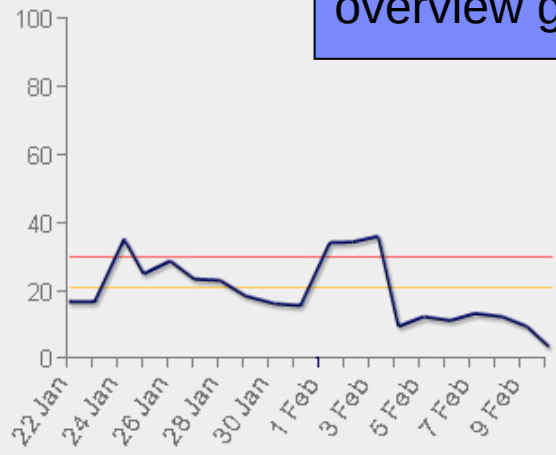
Enterprise Overview

Settings

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



Trend graphic



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

W7 Eventlist
Note!: Mike Bonfire, a DBA, is reading the payroll

al > Dashboard > Reports > Database Top 10 Reports > Direct Database Access

irect Database Access Report

Time period setup

	Month	Day	Year	Hour	Min.
art time	September	3	2006	1	0
nd time	September	7	2006	16	0

Execute Reset

me zone Event time zone

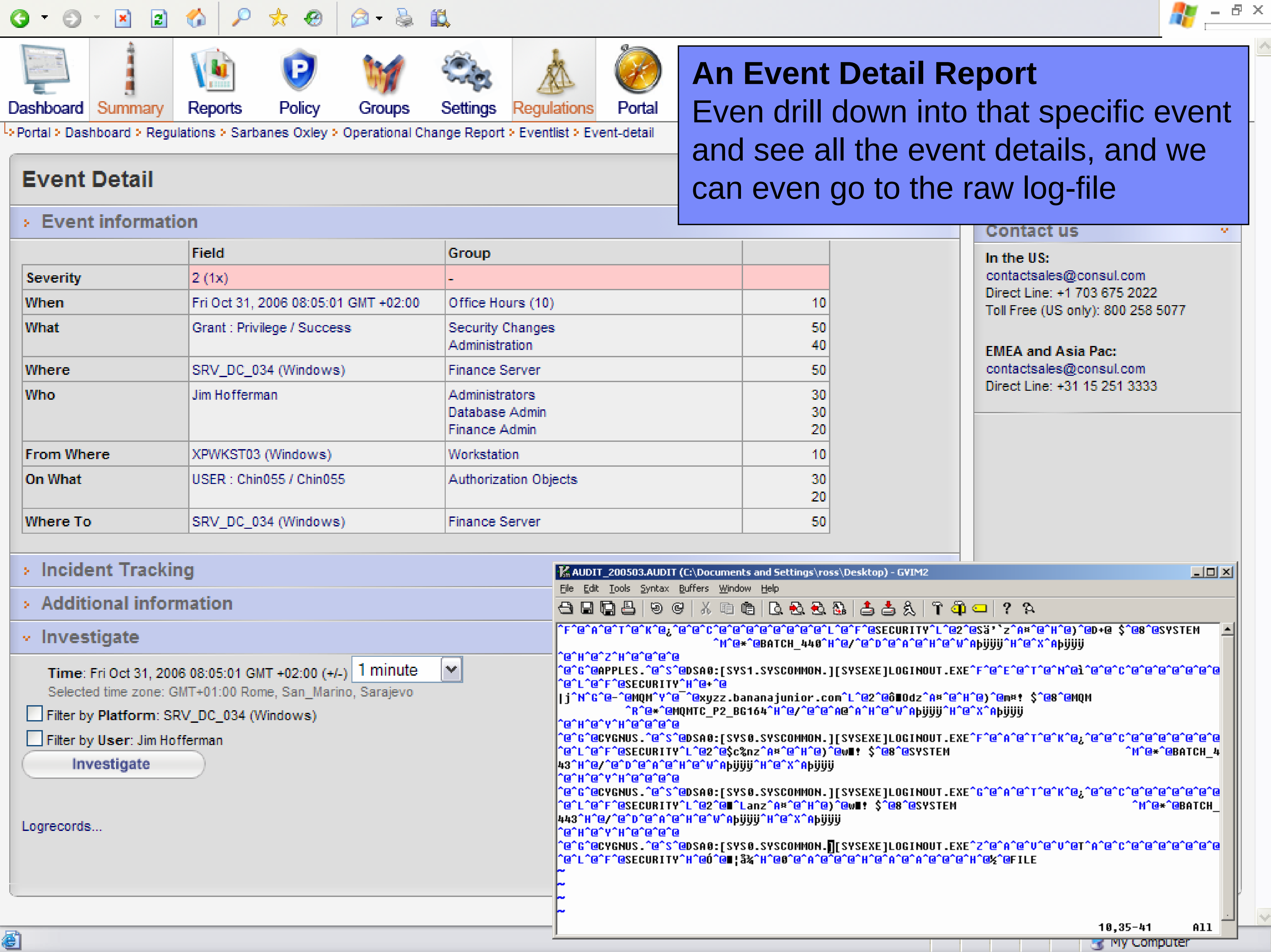
Event List

everity	When	#	What	Where	Who	from Where	on What	Where to
	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
	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
	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
	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
	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
	Sun Sep 03 2006 09:00:06 GMT-05:00	1	Logon : User / Success	Oracle Finance	Max Doane	Oracle Finance	DATABASE : - / Unavailable	Oracle Finance
	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
	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
	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
	Sun Sep 03 2006 09:20:00 GMT-05:00	1	Logon : User / Success	DB2 Server	Jim Hofferman	DB2 Server	DATABASE : - / Unavailable	DB2 Server
	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
	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
	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Logoff : User / Success	DB2 Server	Mike Bonfire	DB2 Server	DATABASE : - / Unavailable	DB2 Server
	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
	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
	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Logoff : User / Success	Oracle Finance	Max Doane	Oracle Finance	DATABASE : - / Unavailable	Oracle Finance
	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

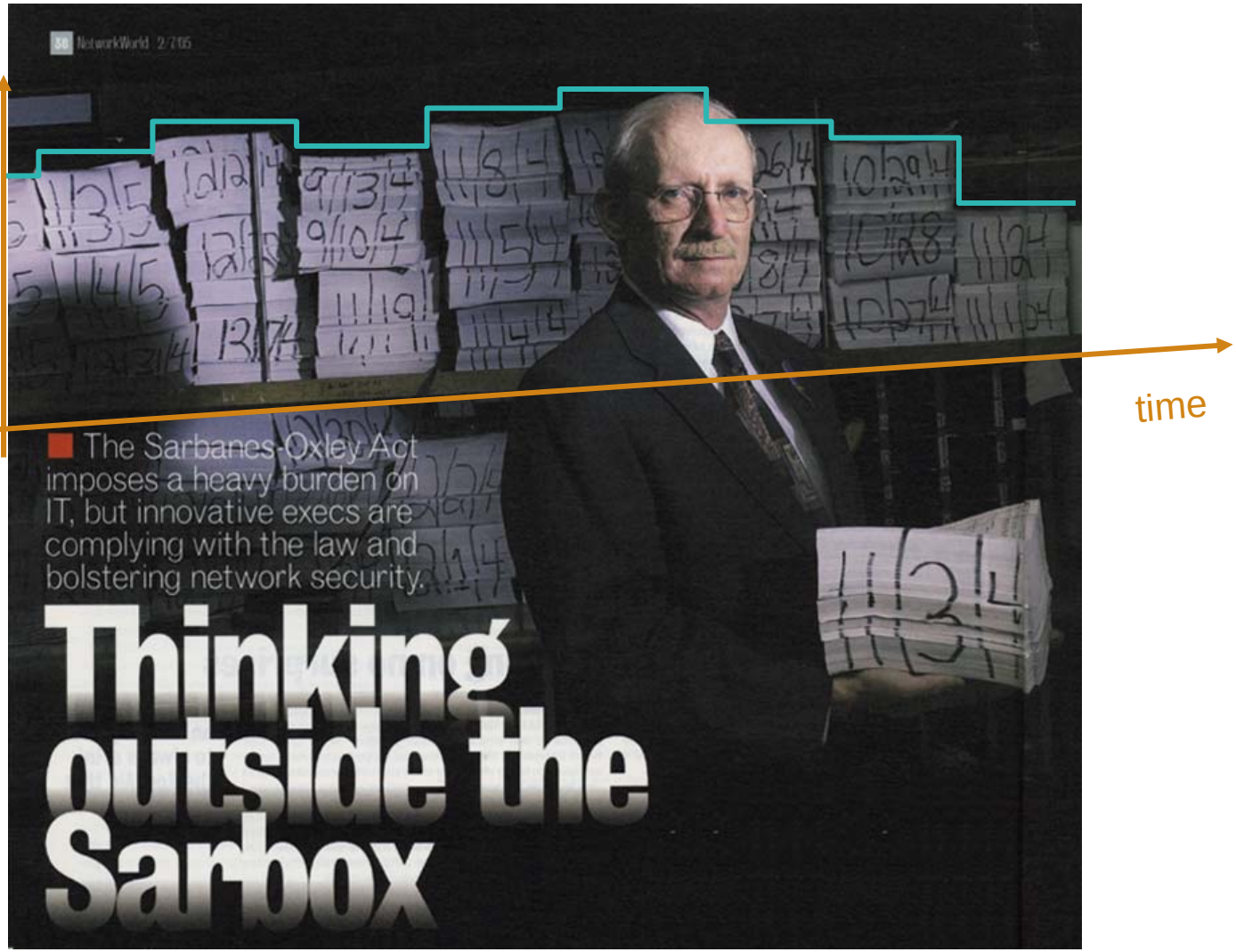
An Event Detail Report

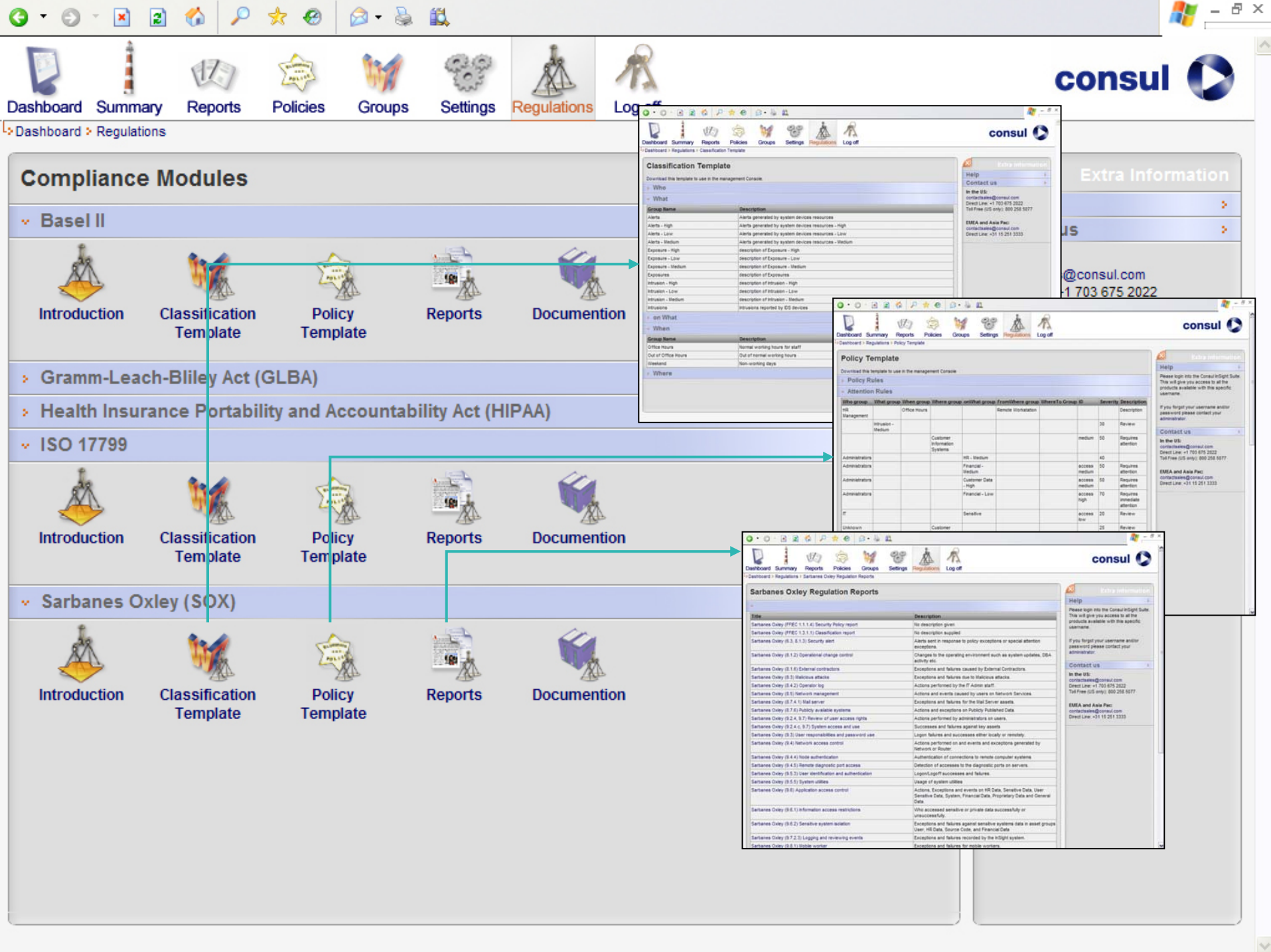
Even drill down into that specific event and see all the event details, and we can even go to the raw log-file



Des rapports, 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

Regulation specific modules with tailored reports to jumpstart your compliance efforts – saving you staff time and reducing audit costs

Sarbanes Oxley Regulation Reports

Title	Description
Sarbanes Oxley (FFIEC 1.1.1.4) Security Policy report	No description given
Sarbanes Oxley (FFIEC 1.3.1.1) Classification report	No description supplied
Sarbanes Oxley (6.3, 8.1.3) 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, DBA 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) Publicly available systems	Actions and exceptions on Publicly Published Data.
Sarbanes Oxley (9.2.4, 9.7) Review of user access rights	Actions performed by administrators on users.
Sarbanes Oxley (9.2.4.c, 9.7) System access and use	Successes and failures against key assets
Sarbanes Oxley (9.3) User responsibilities and password use	Logon failures and successes either locally or remotely.
Sarbanes Oxley (9.4) Network access control	Actions performed on and events and exceptions generated by Network or Router.
Sarbanes Oxley (9.4.4) Node authentication	Authentication of connections to remote computer systems
Sarbanes Oxley (9.4.5) Remote diagnostic port access	Detection of accesses to the diagnostic ports on servers.
Sarbanes Oxley (9.5.3) User identification and authentication	Logon/Logoff 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 (9.7.2.3) Logging and reviewing events	Exceptions and failures recorded by the InSIght system.
Sarbanes Oxley (9.8.1) Mobile worker	Exceptions and failures for mobile workers.

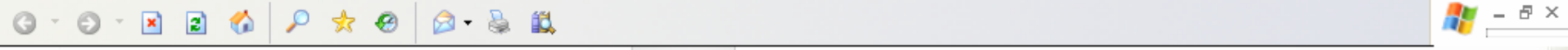
Please login into the Consul InSight Suite. This will give you access to all the products available with this specific username.

If you forgot your username and/or password please contact your administrator.

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



Dashboard | Summary | Reports | Policy | Groups | Settings | Regulations | Portal

Dashboard › Regulations › Sarbanes Oxley Regulation Reports › Operational Change Control

Operational Change Control Report
See a summary of all the operational changes made by different groups

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

Usage Help

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