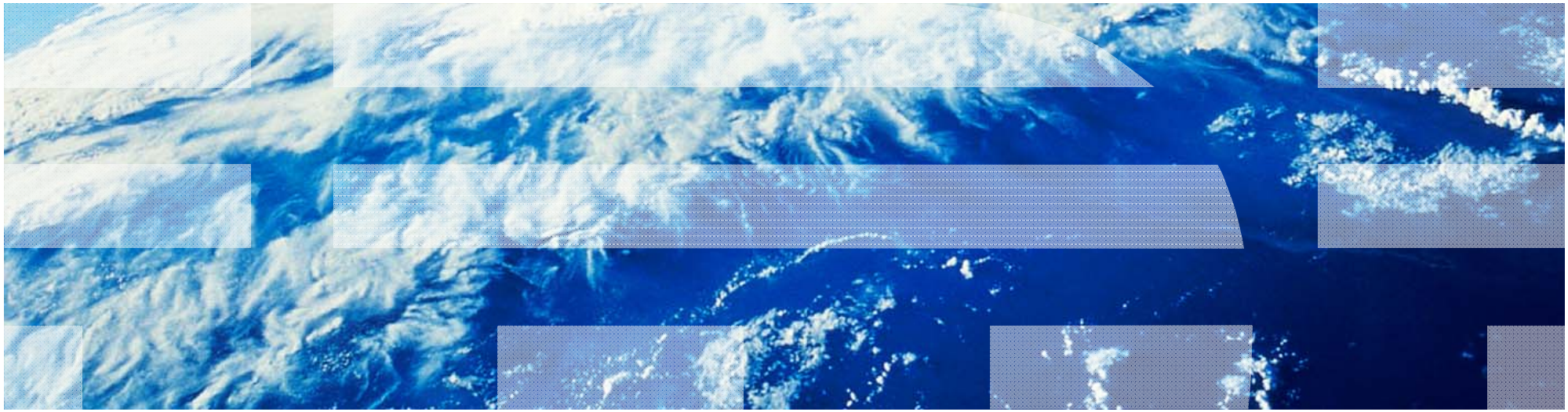
Liher Elgezabal

29 Abril de 2009

IBM Tivoli Compliance Insight Manager



¿Qué es TCIM?

IBM Tivoli® Compliance Insight Manager, es una solución automatizada de **monitorización, investigación y preparación de informes** que permitirá conocer las **actividades de sus usuarios**, obtener una seguridad constante y no intrusiva, así como realizar **pruebas documentales** de que tanto la gestión de sus **datos** como la de sus **sistemas** cumple las **políticas** de la empresa.

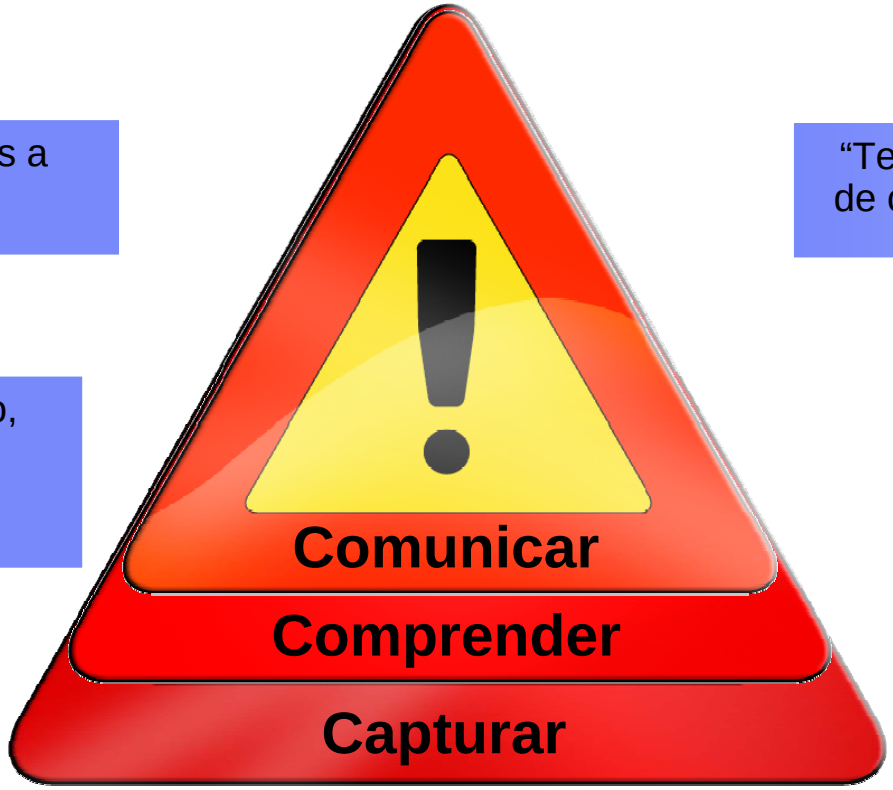
Source: If applicable, describe source origin

¿Qué hace TCIM?

"Tengo que presentar informes a los auditores y reguladores"

"El personal no tiene el tiempo, experiancia o el interes para escanear los logs"

"necesito almacenar los logs para analisis forenses"

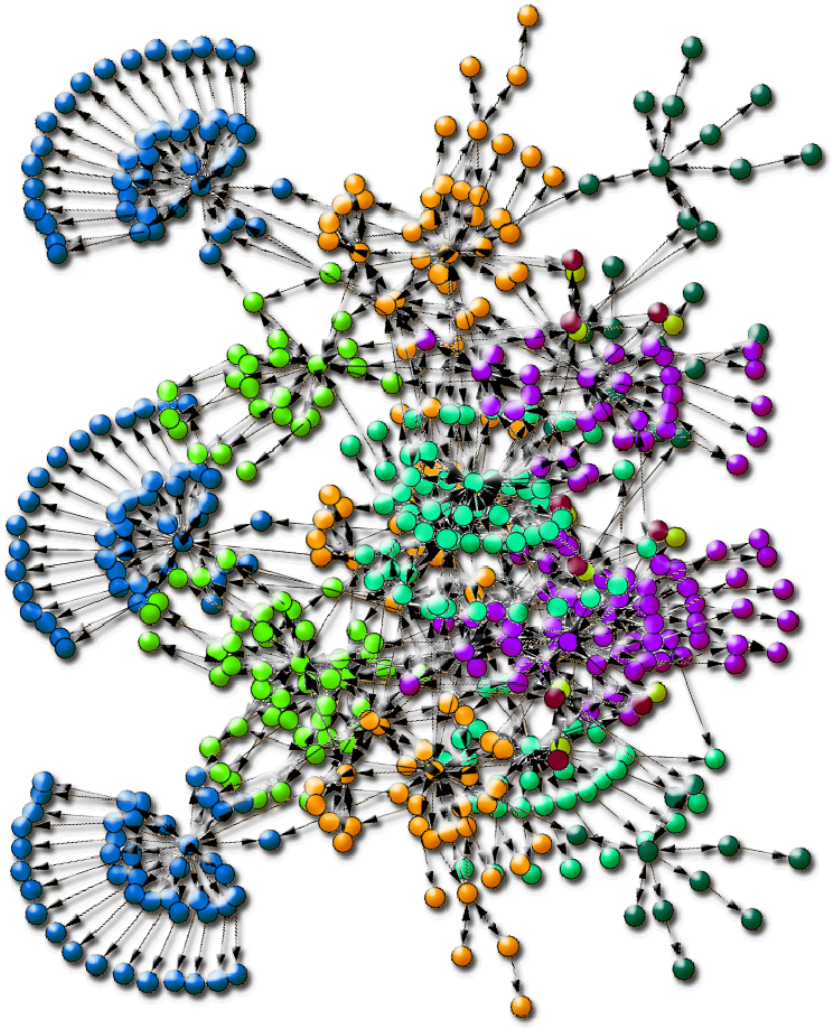


"Tengo que probar que disponemos de controles de seguridad efectivos"

"me preocupan los usuarios privilegiados"

"no sé como recoger los logs ni cuales recoger

Capturar datos distribuidos y hetereogeneos



Capturar

Operating Systems

CA ACF2 through zAudit ACF2	8.0
CA eTrust Access Control for AIX	5.0
CA eTrust Access Control for HP-UX	5.0
CA eTrust Access Control for Solaris	5.0
CA eTrust Access Control for Windows	4.10
CA Top Secret for VSE/ESA	3.0
CA Top Secret for z/OS via z/Audit	5.2
Hewlett-Packard HP NonStop (Tandem) SafeGuard	D42
Hewlett-Packard HP-UX audit trail	10.2, 11i
Hewlett-Packard HP-UX syslog	10.2, 11i
Hewlett-Packard OpenVMS	7.3.2
Hewlett-Packard Tru64	4.0, 5.1, 5.1B
IBM AIX audit trail	4.x, 5.1, 5.2, 5.3
IBM AIX syslog	4.x, 5.1, 5.2, 5.3
IBM OS/400 journals	4.5, 5r1-r2-r3
IBM z/OS RACF - excl. DB2 through zAudit RACF Lite	R10 to 1.7
IBM z/OS RACF through (already) installed zAudit RACF	R10 to 1.7
IBM z/OS ACF2 -excl. DB2 through zAudit ACF2 Lite	R10 to 1.7
IBM z/OS RACF through (already) installed zAudit ACF2	R10 to 1.7
IBM z/OS TopSecret - excl. DB2 through zAudit Lite	R10 to 1.7
Microsoft Windows security event log	NT4, 2000, 2003, XP
Novell Novell Netware	4, 5, 6, 6.5 (via Nsure Audit)
Novell Novell Nsure Audit	1.0.1, 1.0.2, 1.0.3
Novell Novell Suse Linux	8.2, 9.x
Red Hat Linux syslog	6.2,7.2,8.0,9.0, ES 4, Fedora Core
Stratus VOS	13.x, 14.x, 15.x
SUN Solaris audit trail (32 bit & 64 bit)	7, 8, 9, 10
SUN Solaris syslog	7, 8, 9, 10

User Information Sources	
Hewlett-Packard HP HP-UX	10.2,11i
IBM IBM AIX	4.x, 5.1, 5.2, 5.3
IBM IBM OS/400	4.5, 5.1, 5.2, 5.3
IBM IBM z/OS	R10 to 1.7
Microsoft Microsoft NT Domain Windows	NT4, 2000, 2003
Microsoft Microsoft Active Directory Windows	2000, 2003
SUN Solaris	7, 8, 9, 10
Authentication Servers	
BMC Identity Manager on AIX / Oracle via ODBC	3.2.0.3
CA eTrust (Netegrity) SiteMinder (from Windows)	5.5
IBM Tivoli Access Manager	4.1
RSA Authentication Server (Ace)	6.0
Mail Servers and Groupware	
IBM Lotus Domino (Notes) on Windows Max. of 3000 users	5.0, 6.0, 6.5
Microsoft Exchange Server Max. of 3000 users	2000, 2003
Proxy Servers	
Blue Coat Systems ProxySG series	SGOS 3.2.5
Web Servers	
Microsoft Internet Information Server (IIS) on Windows	4.0, 5.0, 6.0
SUN iPlanet Web Server on Solaris	4.0, 6.0

Application Packages	
Misys OPICS	5, 6, 6.1
SAP R/3 on Windows Number of applications	4.6, 4.7
SAP R/3 on HP-UX Number of applications	4.6, 4.7
SAP R/3 on AIX Number of applications	4.6, 4.7
SAP R/3 on Solaris Number of applications	4.6, 4.7
Databases	
IBM DB2 on z/OS through zAudit Lite	7.x, 8.x
IBM UDB on Windows	8.2
IBM UDB on Solaris	8.2
IBM UDB on AIX	8.2
Microsoft SQL Server application logs	6.5, 7.0, 2000
Microsoft SQL Server trace files	2000, 2005
Oracle database server on Windows	8i, 9i, 10g
Oracle database server on Solaris	8i, 9i, 10g
Oracle database server on AIX	8i, 9i, 10g
Oracle database server on HP-UX	8i, 9i, 10g
Oracle database server FGA on Windows	9i, 10g
Oracle database server FGA on Solaris	9i, 10g
Oracle database server FGA on AIX	9i, 10g
Oracle database server FGA on HP-UX	9i, 10g
Sybase ASE on Windows	12.5, 15
Sybase ASE on Solaris	12.5, 15
Sybase ASE on AIX	12.5, 15
Sybase ASE on HP-UX	12.5, 15
Firewalls	

Firewalls	
Check Point FireWall-1 (via SNMP)	4.1, NG, NGX
Cisco PIX (from AIX)	6.0 – 6.3.3
Cisco PIX (from Windows)	6.0 – 6.3.3
Cisco PIX (via SNMP)	6.0 – 6.3.3
Cisco PIX (via Syslog)	6.0 – 6.3.3
Symantec (Raptor) Enterprise Firewall (via SNMP)	6.0, 6.5, 7.0
Symantec (Raptor) Enterprise Firewall (via Syslog)	6.0, 6.5, 7.0
IDS, IPS	
ISS RealSecure (alerts) via SNMP	6.0
ISS RealSecure (operational messages, Windows)	6.0
McAfee IntruShield IPS Manager (via Syslog)	1.9
Snort (Open Source) IDS (via Syslog)	2.1.3, 2.2.0, 2.3.3
Routers	
Cisco Router (from AIX)	IOS 12.x
Cisco Router (from Windows)	IOS 12.x
Cisco Router (via SNMP)	IOS 12.x
Cisco Router (via Syslog)	IOS 12.x
Switches	
Hewlett-Packard ProCurve switch (via SNMP)	Managed units, 2500 series & up
Virus Scanners	
McAfee ePolicy Orchestrator (ePO)	3.5.2
TrendMicro ScanMail for Domino on Windows	5.3
TrendMicro Scanmail for MS Exchange	5.3
TrendMicro ServerProtect 5 for NT	5.3
Symantec AntiVirus Corporate Edition for Windows	9.0
VPN	
Cisco VPN Concentrator 3000 (via Syslog)	4.1
Vulnerability Scanners	
ISS System Scanner (from Windows)	4.2

Informe de Continuidad de Logs

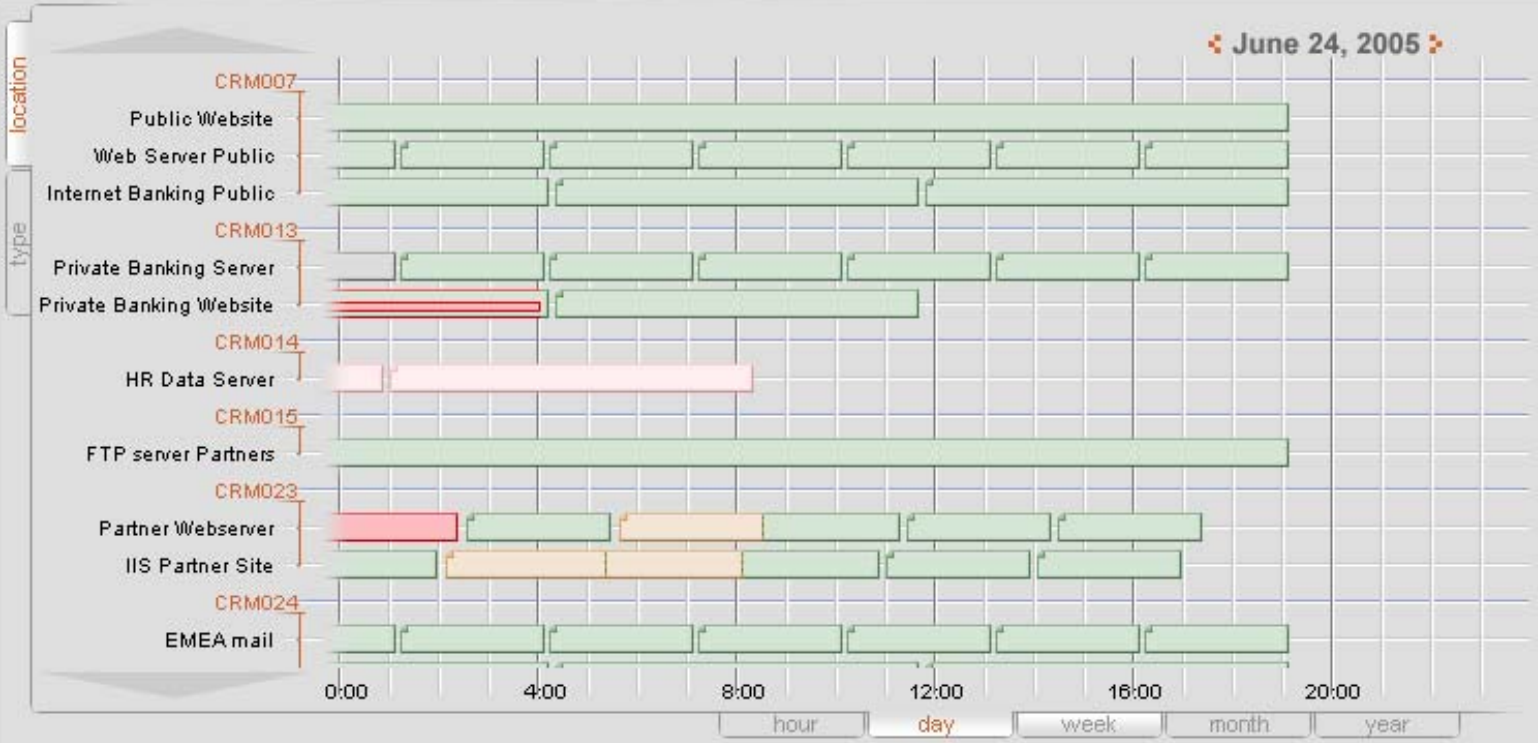
Prueba inmediata para los auditores de que el programa de gestión de logs es completo y continuo

Dashboard | History | Continuity | Activity | Investigate | Retrieval

Portal > Log Manager > Continuity Report

Log Continuity Report

Graph



List of Logfiles

#	Size	Start Date	Time	End Date	End Time	Eventsource Type	Eventsource Name	Machine
3	33 kb	June 25, 2005	10:00	June 25, 2005	12:00 (GMT +1)	IIS	Public website	CRM007
5	21 kb	June 25, 2005	11:00	June 25, 2005	12:00 (GMT +1)	Windows Server	Web Server Public	CRM007
2	1.3 Mb	June 25, 2005	12:00	June 25, 2005	13:00 (GMT +1)	SAP	Internet Banking Public	CRM007
3	5 kb	June 25, 2005	13:00	June 25, 2005	13:17 (GMT +1)	Windows Server	Private Banking Server	CRM013
3	213 kb	June 25, 2005	14:00	June 25, 2005	16:30 (GMT +1)	IIS	Private Banking Website	CRM013
1	94 kb	June 25, 2005	15:00	June 25, 2005	19:00 (GMT +1)	Windows Server	HR Data Server	CRM014

Actions
- Export to PDF
- Export to Excel
- Retrieve selected Logfiles
- Regenerate Report
- Adjust Schedule

View
- Hide Timezone (GMT +1)
- By Audited Timezone
- By Browser Timezone
- By Other Timezone

Filters

Sorting
- Start Date
- Start Time
- Audited Machine

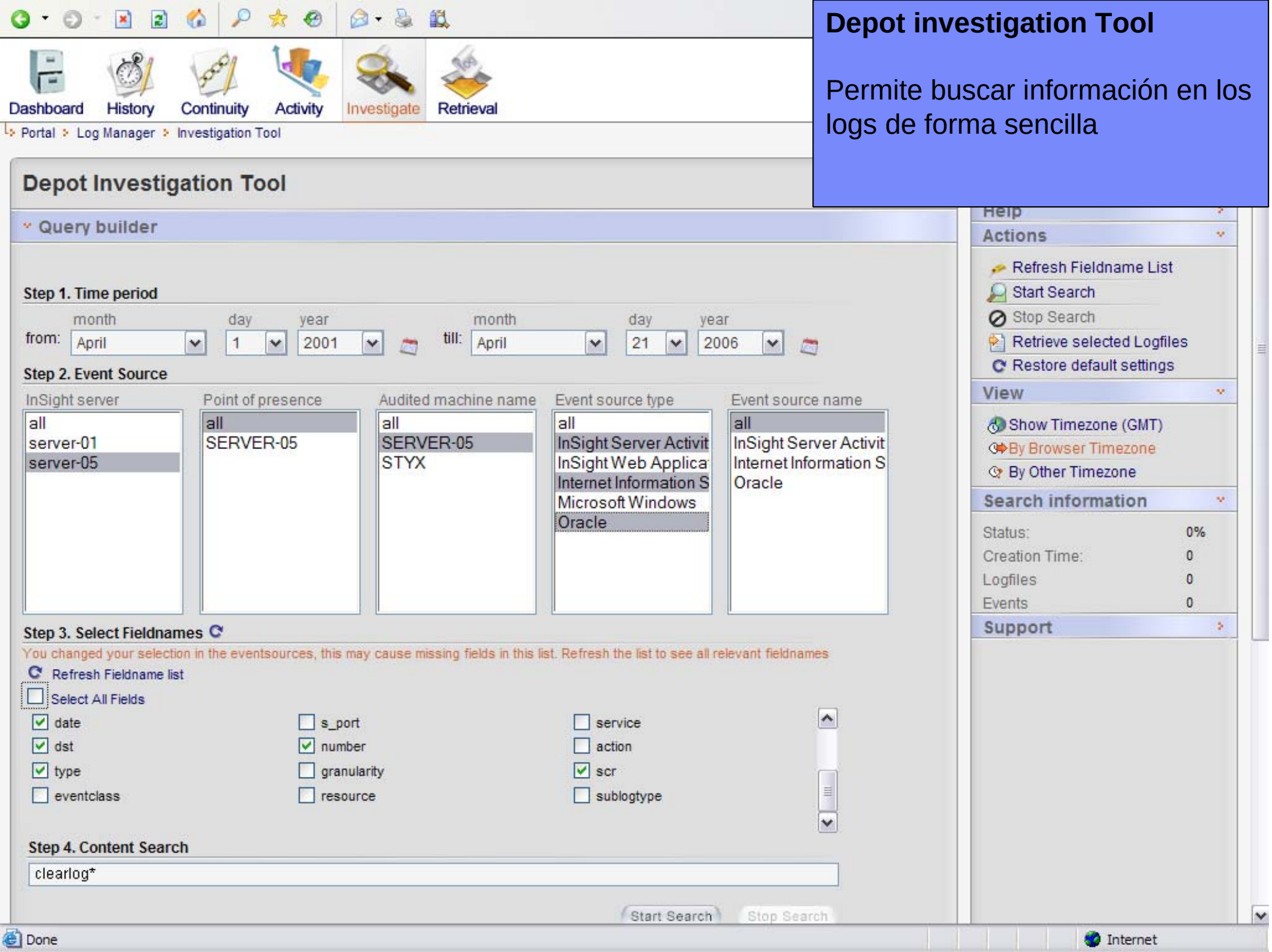
Legend
- Continuity Logfile
- Missing Logfile
- Missing Sub Logfile
- Failed collect, not collected yet
- Delayed collect, possible lost
- Archived Logfile
- Corrupt Logfile

Report information

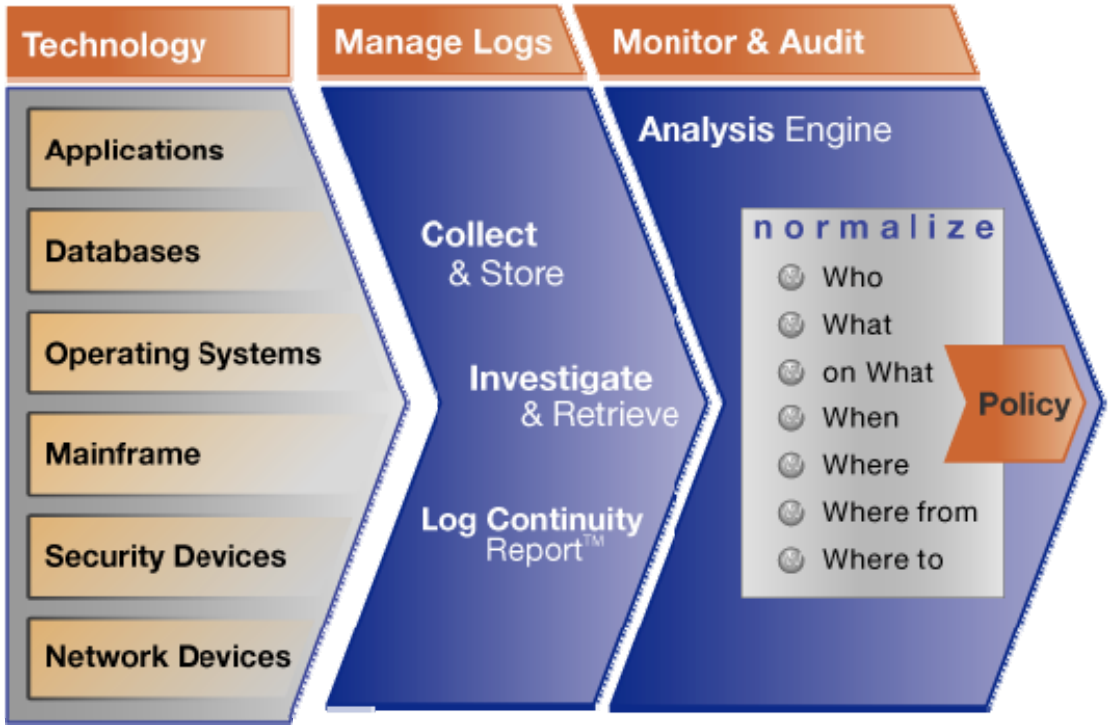
Done | My Computer

Depot investigation Tool

Permite buscar información en los logs de forma sencilla



Comprender

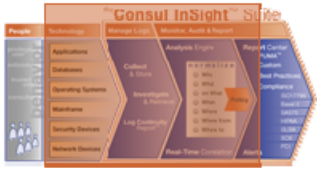


Caracteristicas:

- Normalización W7
- Interpretar CUALQUIER log (Syslog y logs nativos) al Inglés
- Comparar billones de logs a las políticas de base

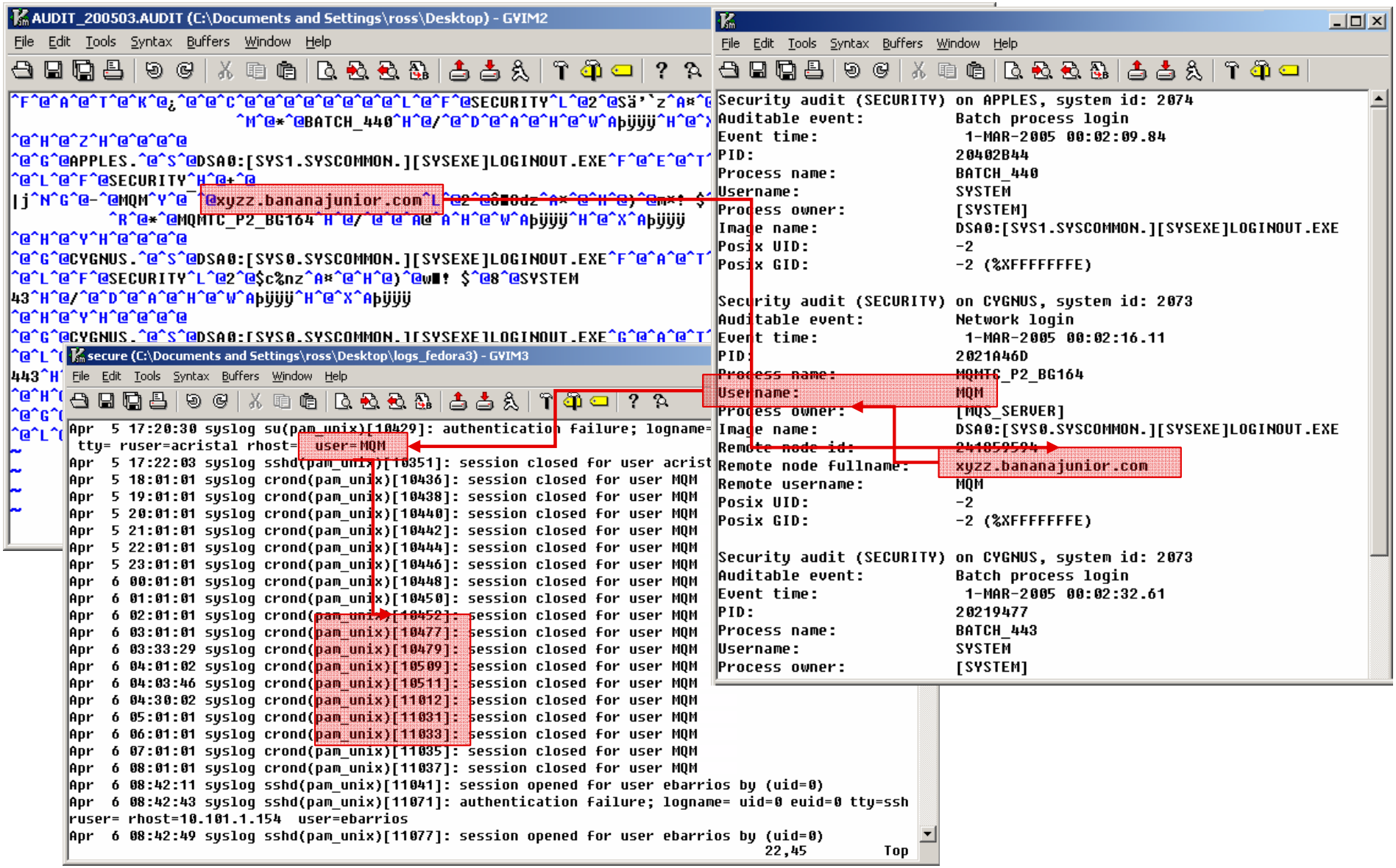
Beneficios:

- Interpretar y monitorizar todos los logs con menos y recursos y menos costosos
- Detectar y resolver antes los problemas de seguridad

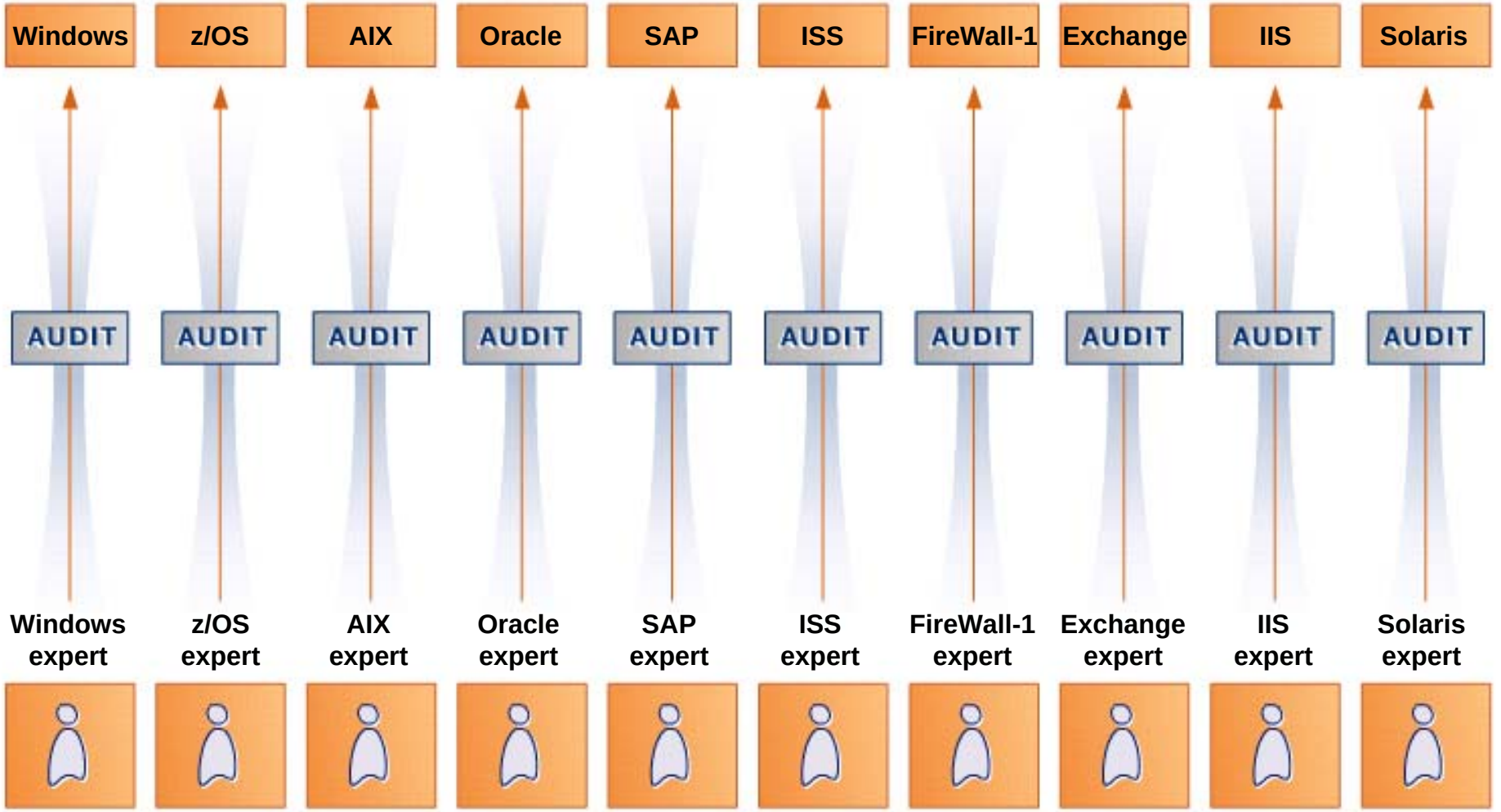


Normalización Out of the box!

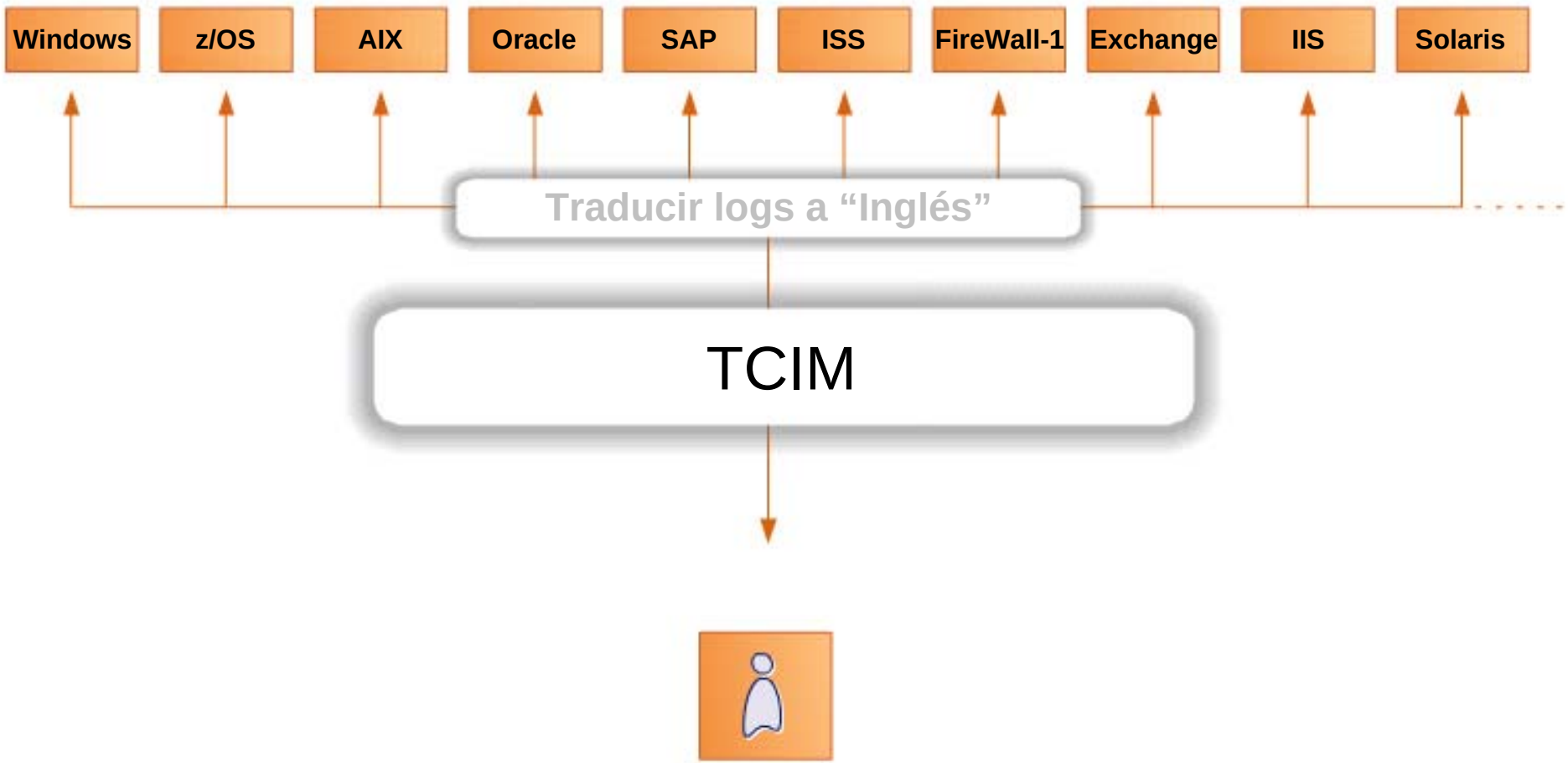
Comprender



Comprender

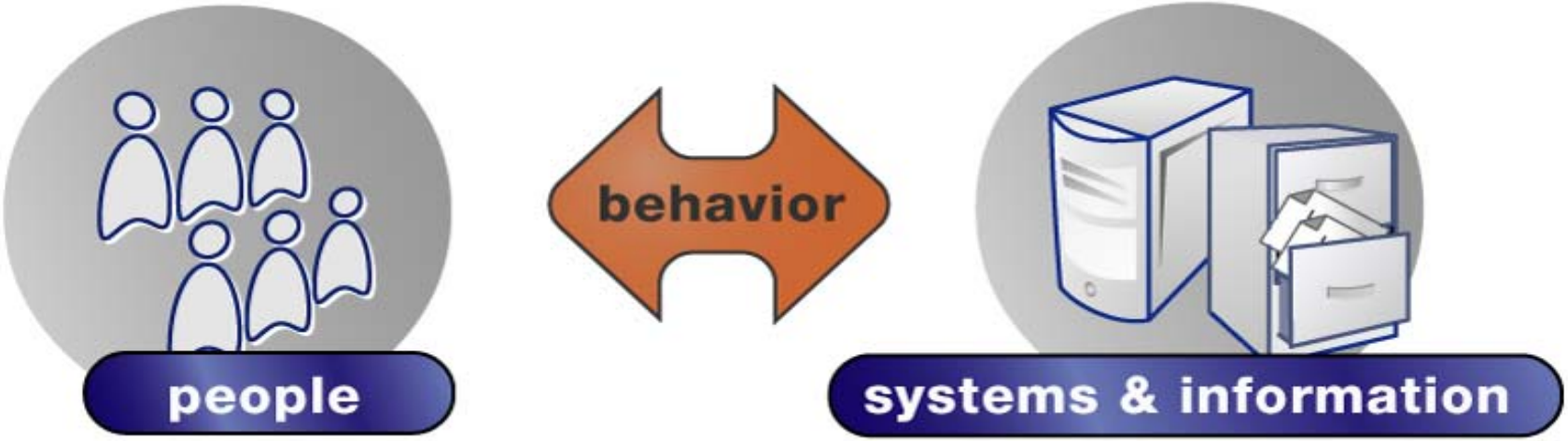


Comprender



Consul InSight automatiza la monitorización de toda la empresa

Requerimientos de Auditoria y Cumplimiento



Usuarios:
- Usuarios Privilegiados
- Usuarios Externos
- Consultores

Acciones:
- Fallos y errores humanos
- Sabotaje en datos o sitemas
- Robo de información
- Introducción de codigos erroneos
- Instalación de software no autorizado

Sistemas e
- Aplicaciones
- Bases de Datos
- Sist Operativos
- Mainframes
- Dispositivos

Información:
- Datos de Clientes
- datos financieros
- registros de RRHH

Estas acciones pueden resultar en periodos de falta de disponibilidad de sistemas, pérdida de confianza de los clientes, responsabilidades legales o deficiencias de auditoría.
El resultado son pérdidas reflejadas en el negocio.

Comprender

modelo W7

Comprender

1. Who **quién**
2. What **realiza la acción**
3. on What **en que recurso**

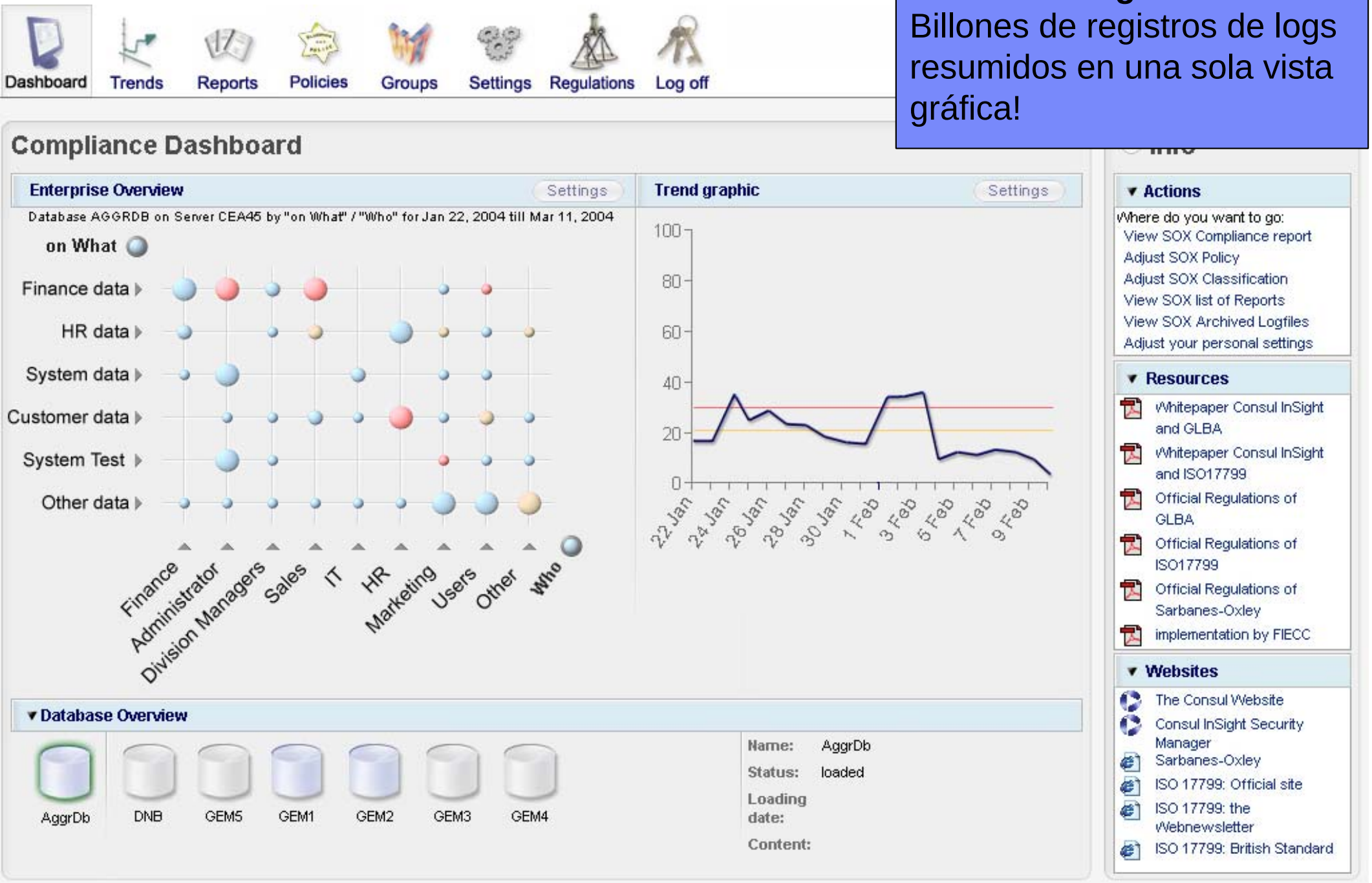
(fichero/dato/dispositivo)

4. When **cuando**
5. Where **donde**
6. from Where **desde donde**
7. Where to **accediendo a donde**

información clara, concisa y facilmente comprensible!!

Cuadro de Mandos

Información global
Billones de registros de logs resumidos en una sola vista gráfica!



Investigación de eventos visualizar todas las acciones realizadas por el administrador de IT en el servidor de Finanzas

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

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

Eventlist of IT Admin doing Authorization Objects on Financial Data on the Finance Server

Time period setup

Event List

Severity	When	#	What	Where	Who	from Where	on What	Where to
2	Tue Oct 24 2006 14:32:44 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	WS_03442 (Windows)	USER : David088 / David088	SRV_DC_034 (Windows)
2	Tue Oct 24 2006 16:09:39 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	WS_03442 (Windows)	USER : David088 / David088	SRV_DC_034 (Windows)
2	Tue Oct 24 2006 16:20:49 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Jim Hofferman	WS_03442 (Windows)	USER : Administrator / Administrator	SRV_DC_034 (Windows)
2	Tue Oct 24 2006 16:20:52 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Jim Hofferman	WS_03442 (Windows)	USER : Administrator / Administrator	SRV_DC_034 (Windows)
2	Sat Oct 28 2006 11:21:26 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Jim Hofferman	SRV_DC_034 (Windows)	USER : Administrator / Administrator	SRV_DC_034 (Windows)
2	Sat Oct 28 2006 11:21:49 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	SRV_DC_034 (Windows)	USER : Unavailable / Unavailable	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:03:02 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Max Doane	SRV_DC_034 (Windows)	USER : Richard019 / Richard019	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:03:02 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Max Doane	SRV_DC_034 (Windows)	USER : Richard019 / Richard019	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:05:01 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Jim Hofferman	SRV_DC_034 (Windows)	USER : Chin055 / Chin055	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:05:01 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Jim Hofferman	SRV_DC_034 (Windows)	USER : Chin055 / Chin055	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:05:01 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Joe Security	SRV_DC_034 (Windows)	USER : Sean031 / Sean031	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:05:01 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Joe Security	SRV_DC_034 (Windows)	USER : Sean031 / Sean031	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:10:00 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	SRV_DC_034 (Windows)	USER : Rick053 / Rick053	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:10:00 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	SRV_DC_034 (Windows)	USER : Rick053 / Rick053	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:30:00 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	SRV_DC_034 (Windows)	USER : Ralph037 / Ralph037	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:30:00 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	SRV_DC_034	USER : Ralph037 /	SRV_DC_034

Informe de Detalles del evento
Posibilidad de ver el detalle de los eventos e incluso acceder al log en bruto!

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

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

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

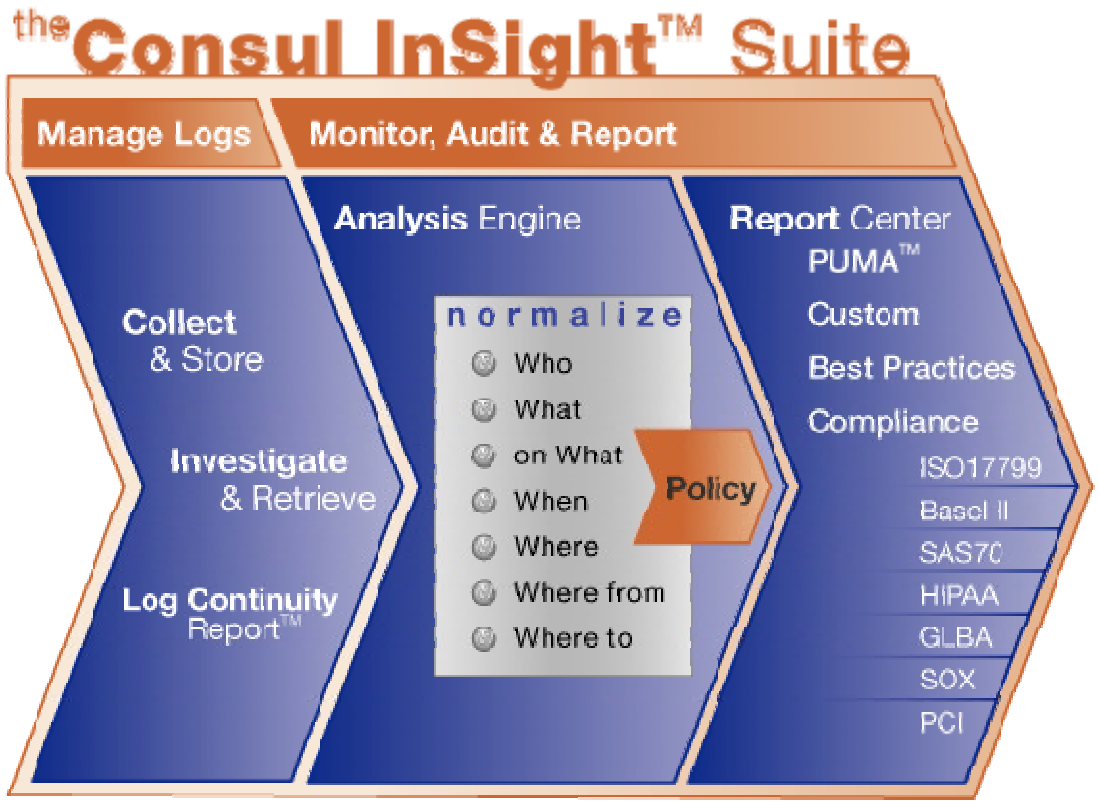
AUDIT_200503.AUDIT (C:\Documents and Settings\ross\Desktop) - GVIM2

File Edit Tools Syntax Buffers Window Help

```
^F^@^A^@^T^@^K^@¿^@^@^C^@^@^@^@^@^@^@^@^L^@^F^@SECURITY^L^@2^@Sä'`z^A¤^@^H^@)^@D+@ $^@8^@SYSTEM
                    ^M^@*^@BATCH_440^H^@/^@^D^@^A^@^H^@^W^Aþÿÿÿ^H^@^X^Aþÿÿÿ
^@^H^@^Z^H^@^@^@^@
^@^G^@APPLES.^@^S^@DSA0:[SYS1.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^F^@^E^@^T^@^N^@ì^@^@^C^@^@^@^@^@^@^@
^@^L^@^F^@SECURITY^H^@+^@
|j^N^G^@-^@MQM^Y^@¯^@xyzz.bananajunior.com^L^@2^@ô■Odz^A¤^@^H^@)^@m¤! $^@8^@MQM
          ^R^@*^@MQMTC_P2_BG164^H^@/^@^@^A@^A^H^@^W^Aþÿÿÿ^H^@^X^Aþÿÿÿ
^@^H^@^Y^H^@^@^@^@
^@^G^@CYGNUS.^@^S^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^F^@^A^@^T^@^K^@¿^@^@^C^@^@^@^@^@^@^@
^@^L^@^F^@SECURITY^L^@2^@$c%nz^A¤^@^H^@)^@w■! $^@8^@SYSTEM                    ^M^@*^@BATCH_4
43^H^@/^@^D^@^A^@^H^@^W^Aþÿÿÿ^H^@^X^Aþÿÿÿ
^@^H^@^Y^H^@^@^@^@
^@^G^@CYGNUS.^@^S^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^G^@^A^@^T^@^K^@¿^@^@^C^@^@^@^@^@^@^@
^@^L^@^F^@SECURITY^L^@2^@■^Lanz^A¤^@^H^@)^@w■! $^@8^@SYSTEM                    ^M^@*^@BATCH_
443^H^@/^@^D^@^A^@^H^@^W^Aþÿÿÿ^H^@^X^Aþÿÿÿ
^@^H^@^Y^H^@^@^@^@
^@^G^@CYGNUS.^@^S^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^Z^@^A^@^U^@^U^@T^A^@^C^@^@^@^@^@^@^@
^@^L^@^F^@SECURITY^H^@Ó^@■¦ã¾^H^@0^@^A^@^@^@^H^@^A^@^A^@^@^@^H^@½^@FILE
~
~
~
~
                                                                10,35-41      All
```

My Computer

Comunicar

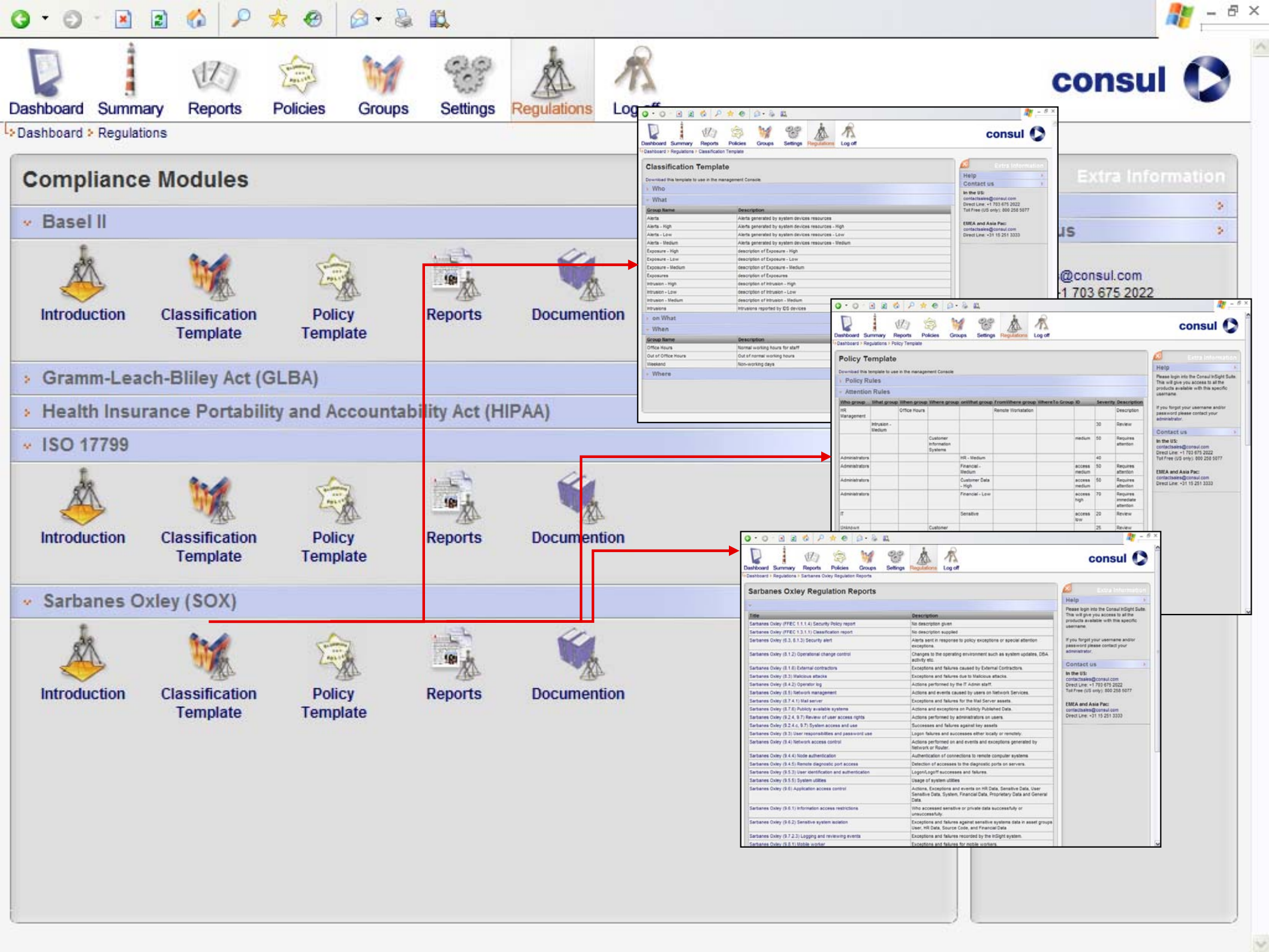


Caracteristicas:

- Cientos de informes
- Módulos de cumplimiento
- Alertas de atención especial
- Informes personalizables

Beneficios:

- Reducir el esfuerzo y el tiempo necesario para las auditorías
- Informes en un instante
- Reducir el riesgo de intrusiones desde el interior:


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

Dashboard Summary Reports Policies Groups Settings Regulations Log off

Dashboard > Regulations > Sarbanes Oxley Regulation Reports

Módulos especificos de cumplimiento de regulaciones listas para auditorías

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

Arquitectura