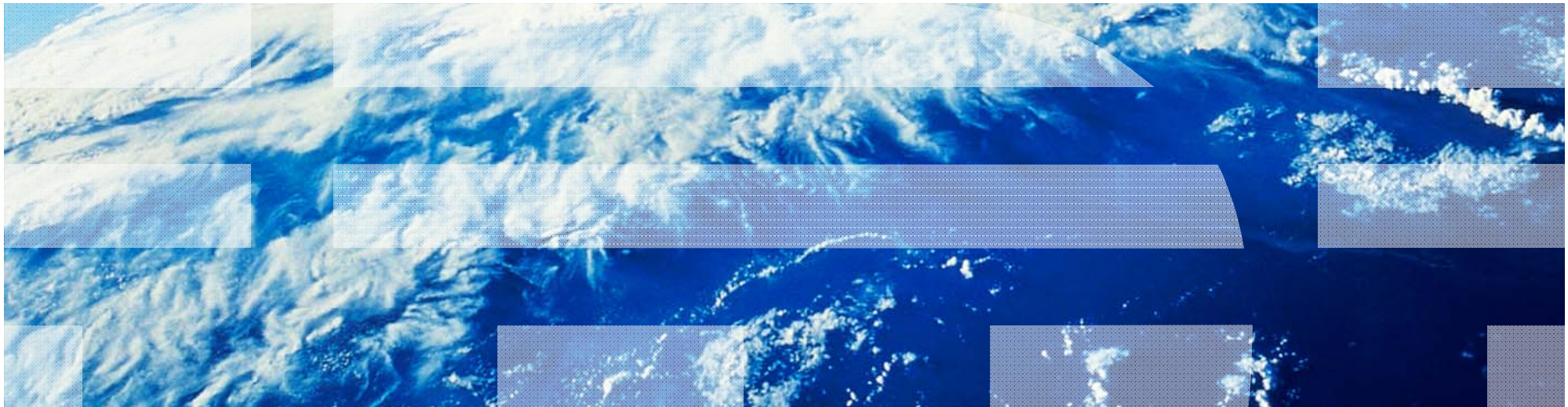


IBM Tivoli Compliance Insight Manager



¿Qué es TCIM?

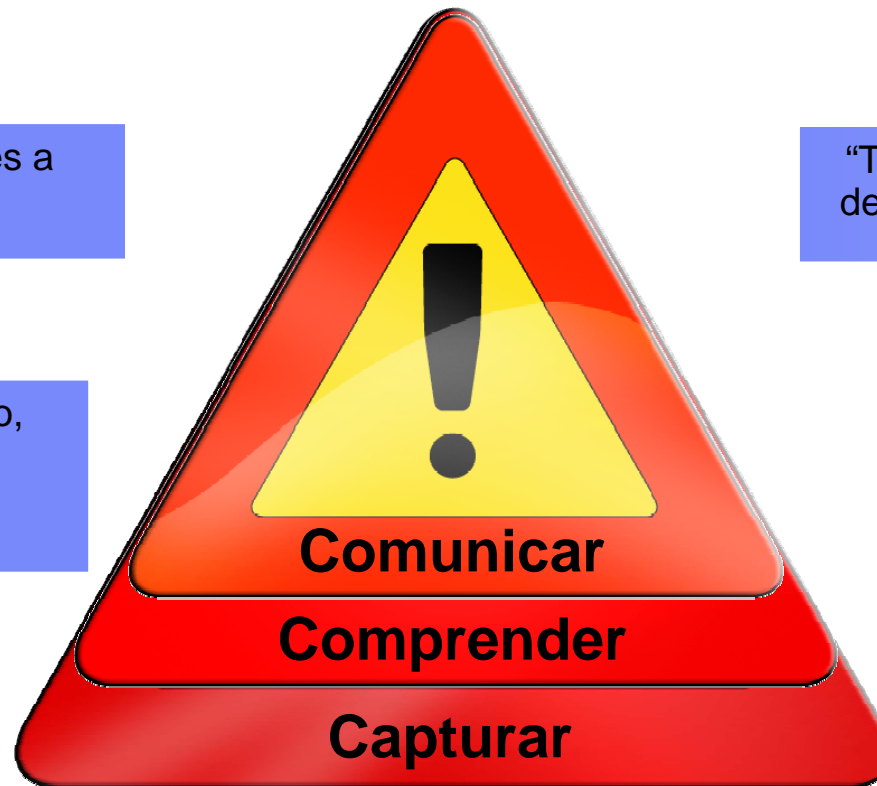
IBM Tivoli® Compliance Insight Manager, es una solución automatizada de **monitorización, investigación y preparación de informes** que permitirá conocer las **actividades de sus usuarios**, obtener una seguridad constante y no intrusiva, así como realizar **pruebas documentales** de que tanto la gestión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

¿Qué hace TCIM?

“Tengo que presentar informes a los auditores y reguladores”

“El personal no tiene el tiempo, experiencia o el interés para escanear los logs”

“necesito almacenar los logs para analisis forenses”



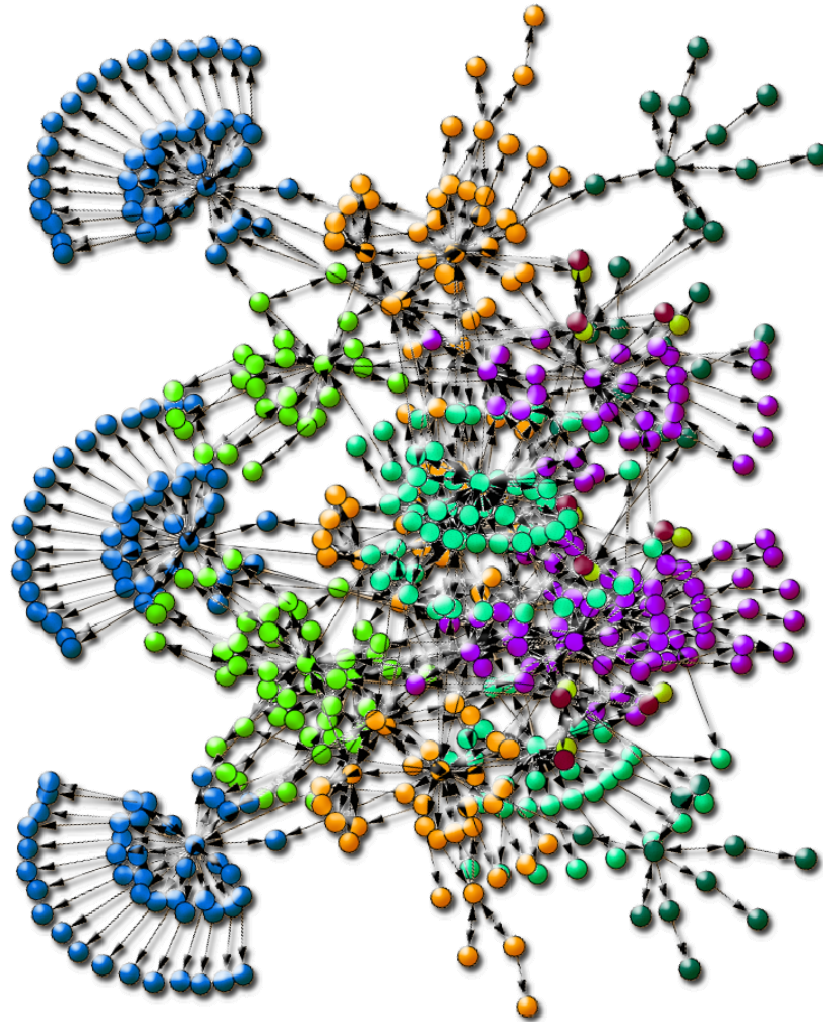
“Tengo que probar que disponemos de controles de seguridad efectivos”

“me preocupan los usuarios privilegiados”

“no sé como recoger los logs ni cuales recoger”

Capturar datos distribuidos y heterogeneos

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 <i>Max. of 3000 users</i>	5.0, 6.0, 6.5
Microsoft Exchange Server <i>Max. of 3000 users</i>	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

Zoom Out

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

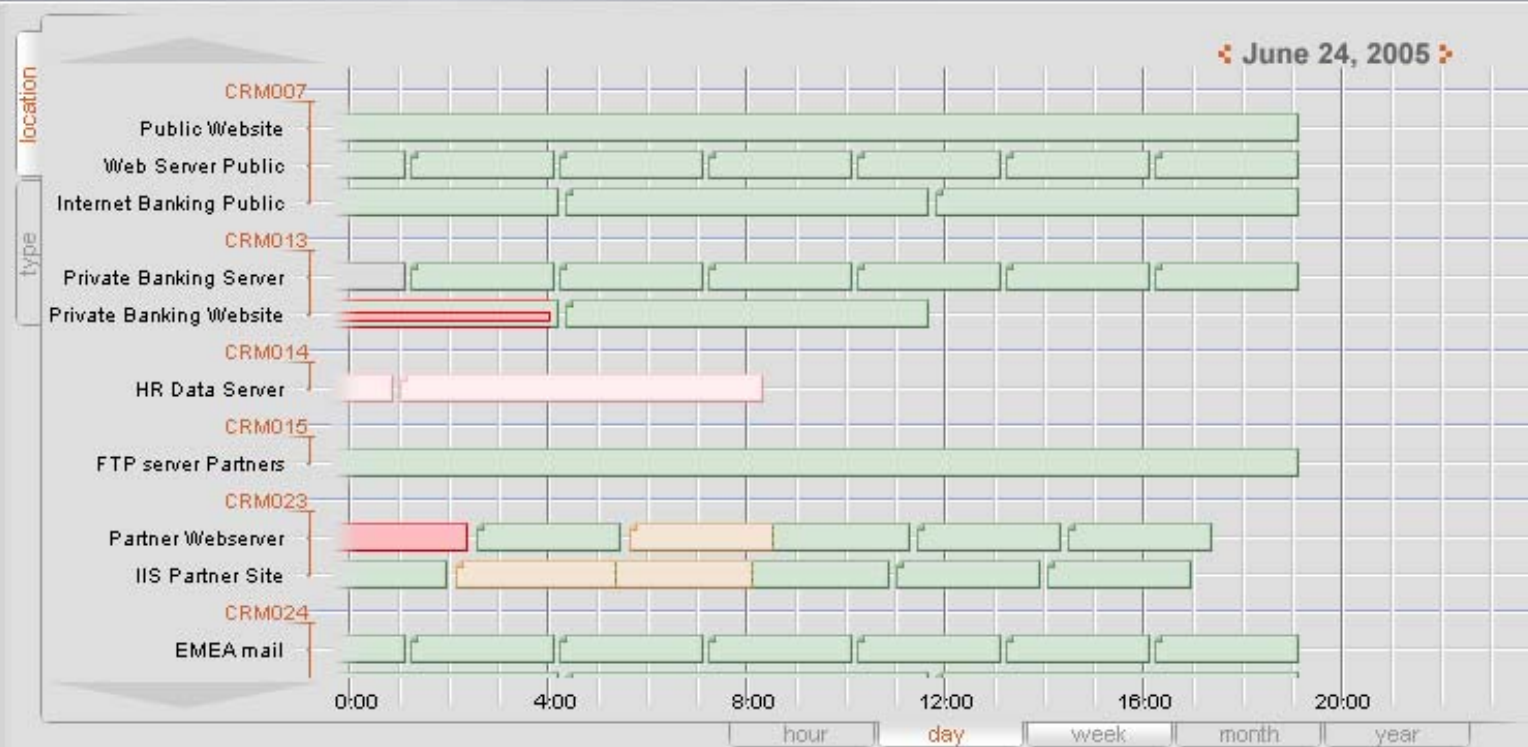
Prueba inmediata para los auditores de que el programa de gestión de logs es completo y continuo



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

Depot investigation Tool

Permite buscar información en los logs de forma sencilla



Portal > Log Manager > Investigation Tool

Depot Investigation Tool

Query builder

Step 1. Time period

from: month: April, day: 1, year: 2001, till: month: April, day: 21, year: 2006

Step 2. Event Source

InSight server	Point of presence	Audited machine name	Event source type	Event source name
all	all	all	all	all
server-01	SERVER-05	SERVER-05	InSight Server Activit	InSight Server Activit
server-05		STYX	InSight Web Applica	Internet Information S
			Internet Information S	Oracle
			Microsoft Windows	
			Oracle	

Step 3. Select Fieldnames

You changed your selection in the eventsources, this may cause missing fields in this list. Refresh the list to see all relevant fieldnames

Refresh Fieldname list

Select All Fields

- date
- dst
- type
- eventclass
- s_port
- number
- granularity
- resource
- service
- action
- scr
- sublogtype

Step 4. Content Search

clearlog*

Start Search Stop Search

Help

Actions

- Refresh Fieldname List
- Start Search
- Stop Search
- Retrieve selected Logfiles
- Restore default settings

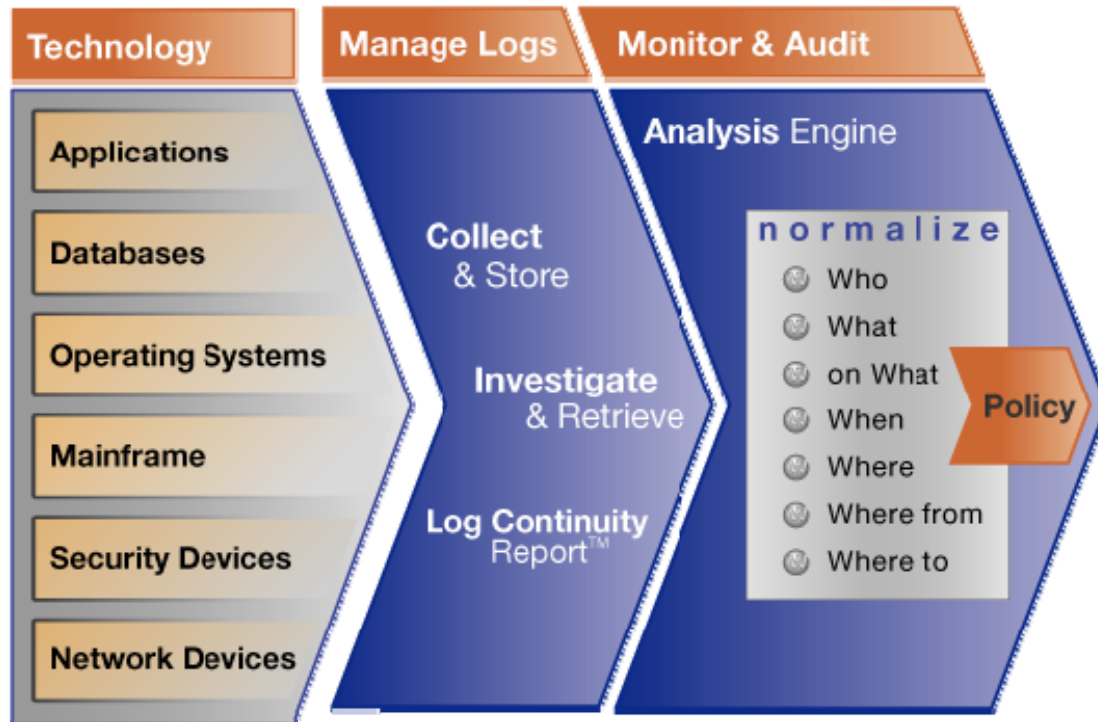
View

- Show Timezone (GMT)
- By Browser Timezone
- By Other Timezone

Search information

Status:	0%
Creation Time:	0
Logfiles:	0
Events:	0

Support



Características:

- 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 recursos y menos costosos
- Detectar y resolver antes los problemas de seguridad

Normalización Out of the box!

Comprender

The image shows three overlapping windows from a Linux system:

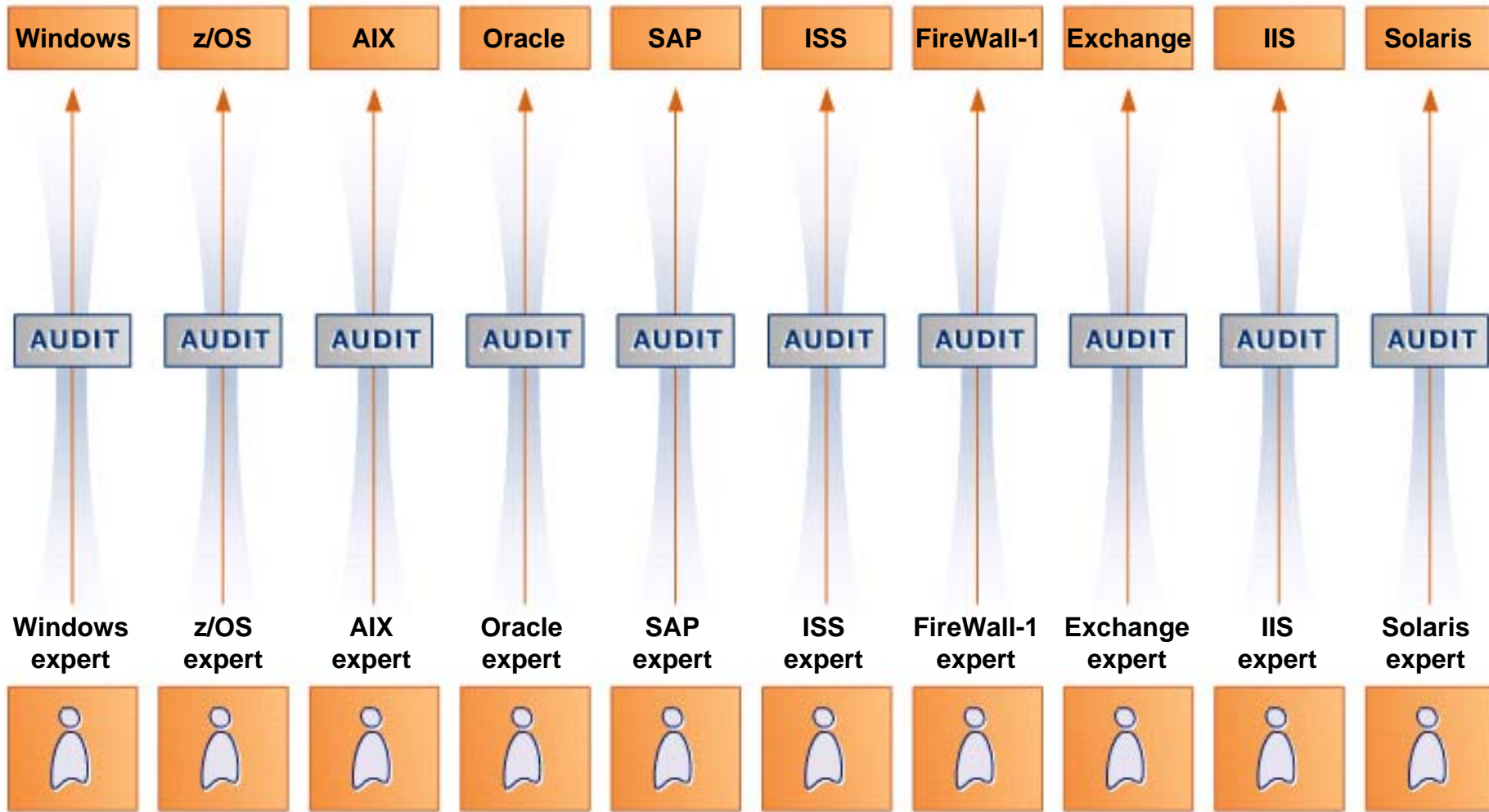
- Top Left Window (GVIM2):** Displays system logs. A red box highlights the entry:

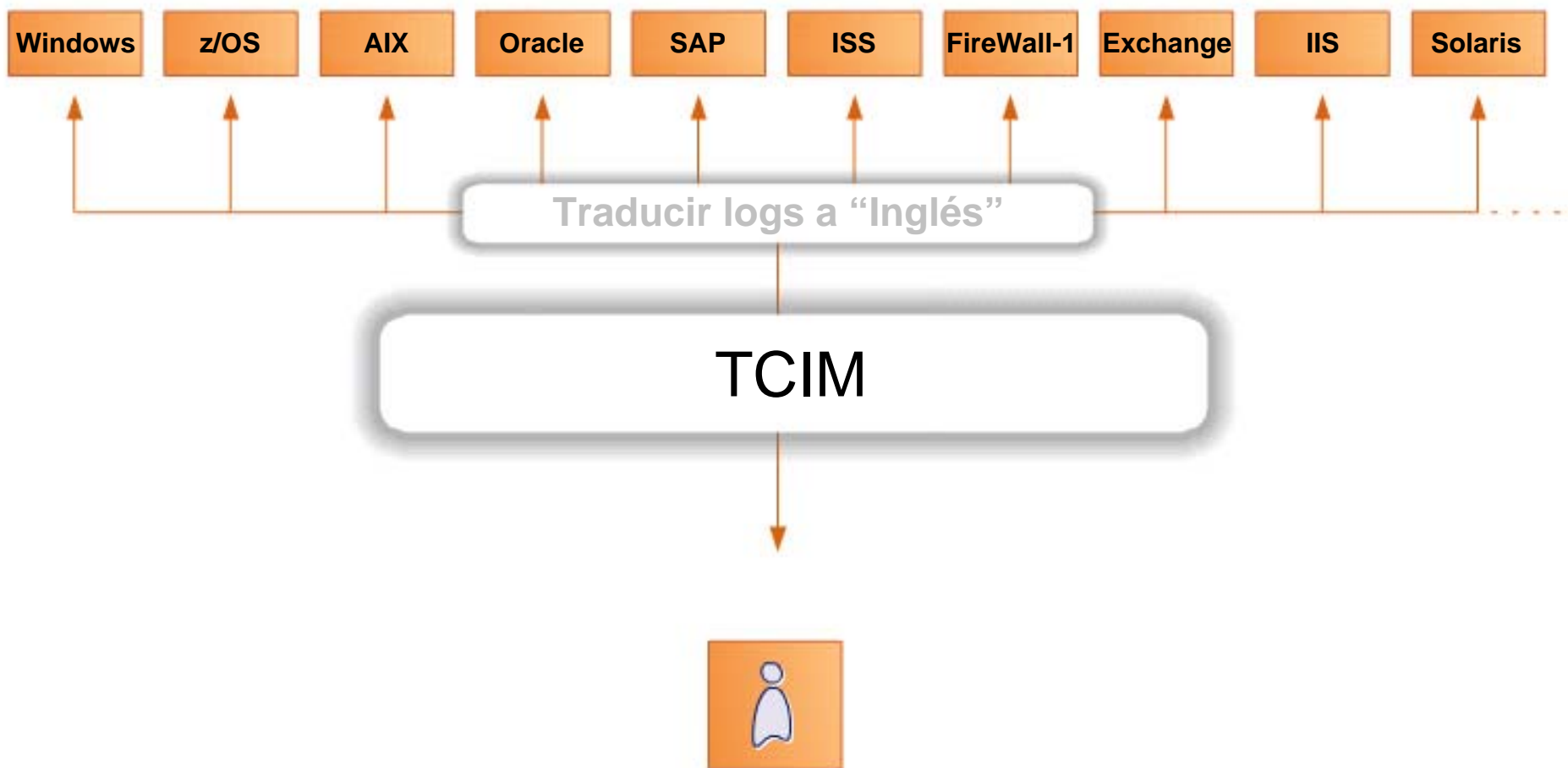

```
Apr 5 17:20:38 syslog su(pam_unix)[10429]: authentication failure; logname=
tty= ruser=acristal rhost= user=MQM
```
- Top Right Window (GVIM2):** Shows security audit details for two events:
 - Event 1:** Batch process login on APPLES (system id: 2074). Fields include: Event time: 1-MAR-2005 00:02:09.84, PID: 20402B44, Process name: BATCH_440, Username: SYSTEM, Process owner: [SYSTEM], Image name: DSA0:[SYS1.SYSCOMMON.][SYSEXE]LOGINOUT.EXE, Posix UID: -2, Posix GID: -2 (%XFFFFFFFFE).
 - Event 2:** Network login on CYGNUS (system id: 2073). Fields include: Event time: 1-MAR-2005 00:02:16.11, PID: 2021A460, Process name: MQMTC_P2_BG164, Username: MQM, Process owner: [MQS_SERVER], Image name: DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE, Remote node id: 241059594, Remote node fullname: xyzz.bananajunior.com, Remote username: MQM, Posix UID: -2, Posix GID: -2 (%XFFFFFFFFE).
- Bottom Left Window (GVIM3):** Displays a log of session closures for 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)
```

Red boxes and arrows connect the highlighted log entries to the corresponding fields in the security audit windows, illustrating the correlation between system logs and audit records.

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 sistemas
- Robo de información
- Introducción de códigos erróneos
- 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.

modelo W7

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 fácilmente comprensible!!

Cuadro de Mandos

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

Dashboard
 Trends
 Reports
 Policies
 Groups
 Settings
 Regulations
 Log off

Compliance Dashboard

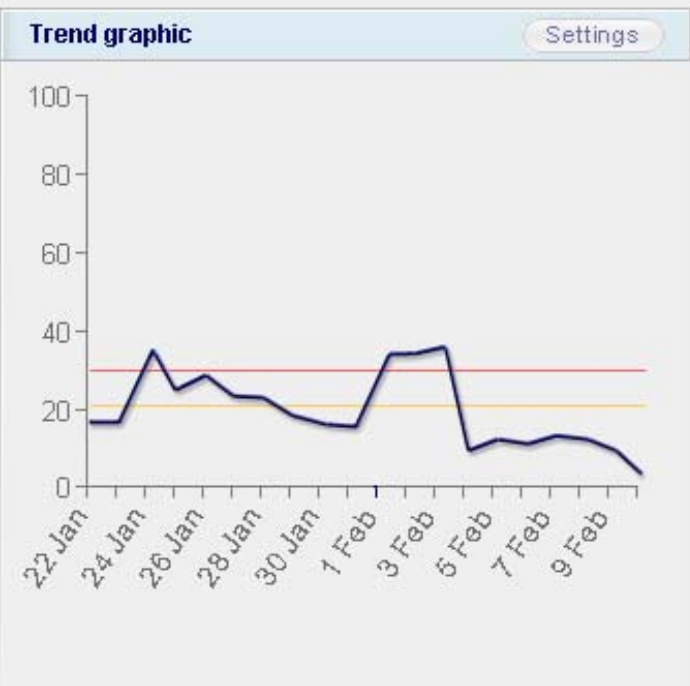
Enterprise Overview Settings

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



Database Overview

AggrDb	DNB	GEM5	GEM1	GEM2	GEM3	GEM4

Name: AggrDb

Status: loaded

Loading date:

Content:

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

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 Hofferan	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 Hofferan	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 Hofferan	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 Hofferan	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 Hofferan	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 (Windows)	USER : Ralph037 / Ralph037	SRV_DC_034 (Windows)

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

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

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 (+/-)
 Selected time zone: GMT+01:00 Rome, San_Marino, Sarajevo

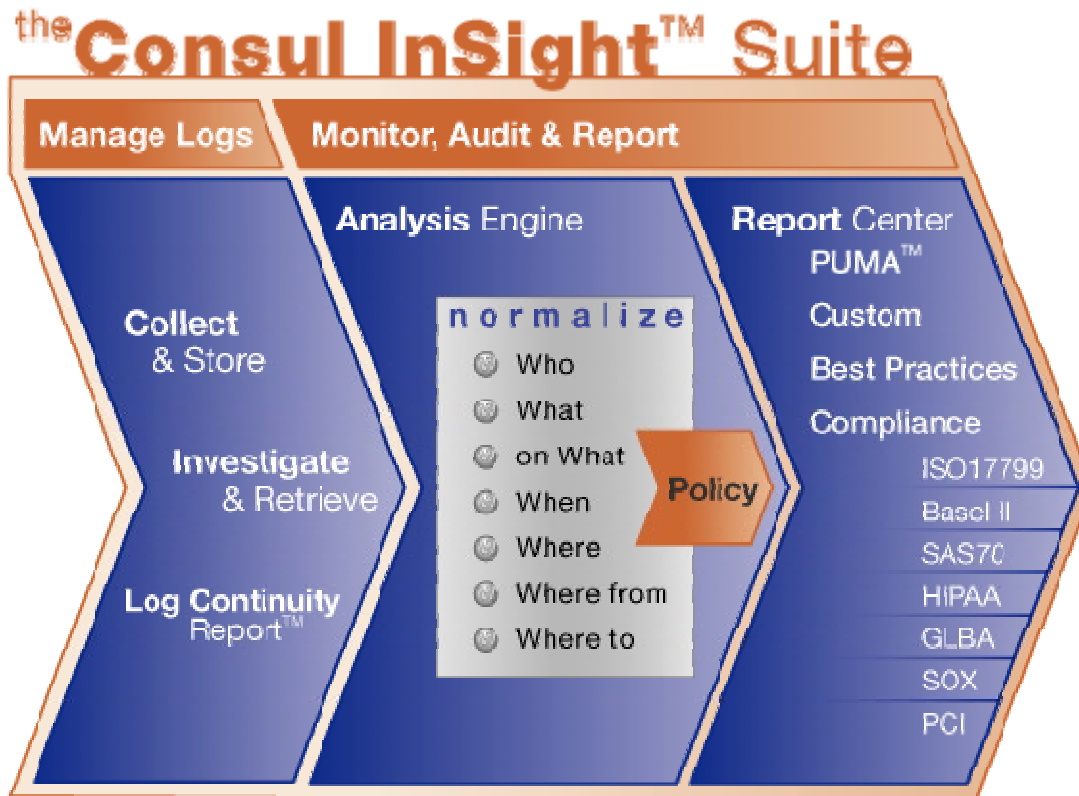
Filter by Platform: SRV_DC_034 (Windows)

Filter by User: Jim Hofferman

Logrecords...

```

AUDIT_200503.AUDIT (C:\Documents and Settings\ross\Desktop) - GVIM2
File Edit Tools Syntax Buffers Window Help
~
^F^A^T^K^z^c^e^e^e^e^e^e^L^@2^@Sä^`z^A^H^@^@D+@ $^@8^@SYSTEM
^M^*^@BATCH_440^H^@/^@D^A^H^@W^A^p^j^j^H^@X^A^p^j^j^
^@H^@Z^H^@e^@
^@G^@APPLES.^@s^@DSA0:[SYS1.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^F^A^T^K^z^c^e^e^e^e^e^e^L^@2^@Sä^`z^A^H^@^@D+@ $^@8^@SYSTEM
^@L^@F^@SECURITY^H^@+^@
|j^N^G^e^@MQM^Y^e^@xyzz.bananajunior.com^L^@2^@0d^z^A^H^@^@D+@ $^@8^@MQM
^R^@*^@MQMTC_P2_BG164^H^@/^@D^A^H^@W^A^p^j^j^H^@X^A^p^j^j^
^@H^@V^H^@e^@
^@G^@CYGNUS.^@s^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^F^A^T^K^z^c^e^e^e^e^e^e^L^@2^@Sä^`z^A^H^@^@D+@ $^@8^@SYSTEM
^@L^@F^@SECURITY^L^@2^@Sä^`z^A^H^@^@D+@ $^@8^@SYSTEM
43^H^@/^@D^A^H^@W^A^p^j^j^H^@X^A^p^j^j^
^@H^@V^H^@e^@
^@G^@CYGNUS.^@s^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^G^A^T^K^z^c^e^e^e^e^e^e^L^@2^@Sä^`z^A^H^@^@D+@ $^@8^@SYSTEM
^@L^@F^@SECURITY^L^@2^@Sä^`z^A^H^@^@D+@ $^@8^@SYSTEM
443^H^@/^@D^A^H^@W^A^p^j^j^H^@X^A^p^j^j^
^@H^@V^H^@e^@
^@G^@CYGNUS.^@s^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^Z^A^U^@V^@T^A^C^e^e^e^e^e^e^L^@2^@Sä^`z^A^H^@^@D+@ $^@8^@SYSTEM
^@L^@F^@SECURITY^H^@ö^@||;ä^H^@0^A^H^@W^A^p^j^j^H^@X^A^p^j^j^@F^@I^@E
~
~
~
  
```



Características:

- 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:

Compliance Modules

Basel II

Introduction Classification Template Policy Template Reports Documentation

Gramm-Leach-Bliley Act (GLBA)

Health Insurance Portability and Accountability Act (HIPAA)

ISO 17799

Introduction Classification Template Policy Template Reports Documentation

Sarbanes Oxley (SOX)

Introduction Classification Template Policy Template Reports Documentation

consul

Dashboard > Regulations > Classification Template

Download this 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

on What

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

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

@consul.com
1 703 675 2022

consul

Dashboard > Regulations > Policy Template

Download this template to use in the management Console

Policy Rules

Attention Rules

Who group	What group	When group	Where group	on/what group	From/where group	WhereTo Group ID	Severity	Description
IT Management	Intrusion - Medium				Remote Workstation		30	Review
Administrators			Customer Information Systems				medium	Requires attention
Administrators				HR - Medium			45	Requires attention
Administrators				Financial - Medium			50	Requires attention
Administrators				Customer Data - High			50	Requires attention
Administrators				Financial - Low			70	Requires immediate attention
IT				Sensitive			20	Review
Unknown			Customer				25	Review

Extra Information

Help

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

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

Contact us

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

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

consul

Dashboard > Regulations > Sarbanes Oxley Regulation Reports

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 (5.2.6.1.2) Security alert	Alerts sent in response to policy exceptions or special attention exceptions
Sarbanes Oxley (5.1.2) Operational change control	Changes to the operating environment such as system updates, DBA activity etc.
Sarbanes Oxley (5.1.6) External contractors	Exceptions and failures caused by External Contractors.
Sarbanes Oxley (5.2) Malicious attacks	Exceptions and failures due to Malicious attacks.
Sarbanes Oxley (5.4.2) Operator log	Actions performed by the IT Admin staff
Sarbanes Oxley (5.5) Network management	Actions and events caused by users on Network Services.
Sarbanes Oxley (5.7.1) Mail server	Exceptions and failures for the Mail Server assets.
Sarbanes Oxley (5.7.6) Publicly available systems	Actions and exceptions on Publicly Published Data.
Sarbanes Oxley (5.2.4.5.7) Review of user access rights	Actions performed by administrators on users.
Sarbanes Oxley (5.2.4.6.7) System access and use	Successes and failures against key assets
Sarbanes Oxley (5.3) User responsibilities and password use	Login failures and successes either locally or remotely.
Sarbanes Oxley (5.4) Network access control	Actions performed on and events and exceptions generated by Network or Router.
Sarbanes Oxley (5.4.4) Node authentication	Authentication of connections to remote computer systems
Sarbanes Oxley (5.4.5) Remote diagnostic port access	Detection of accesses to the diagnostic ports on servers.
Sarbanes Oxley (5.5.3) User identification and authentication	Login/Logout successes and failures.
Sarbanes Oxley (5.5.5) System utilities	Usage of system utilities.
Sarbanes Oxley (5.6) 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 (5.6.1) Information access restrictions	Who accessed sensitive or private data successfully or unsuccessfully.
Sarbanes Oxley (5.7.2) Sensitive system escalation	Exceptions and failures against sensitive systems data in asset group User, HR Data, Source Code, and Financial Data.
Sarbanes Oxley (5.7.2.3) Logging and reviewing events	Exceptions and failures recorded by the iDlight system.
Sarbanes Oxley (5.8.1) Mobile worker	Exceptions and failures for mobile workers.

Extra Information

Help

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

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

Contact us

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

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

Módulos específicos 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

