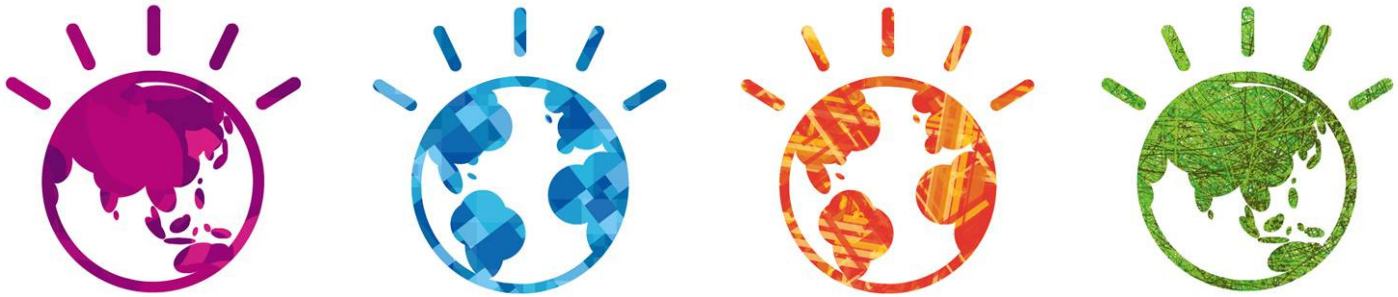
Vicente Gozalbo Moragrega
IBM Security Software Sales Leader Spain

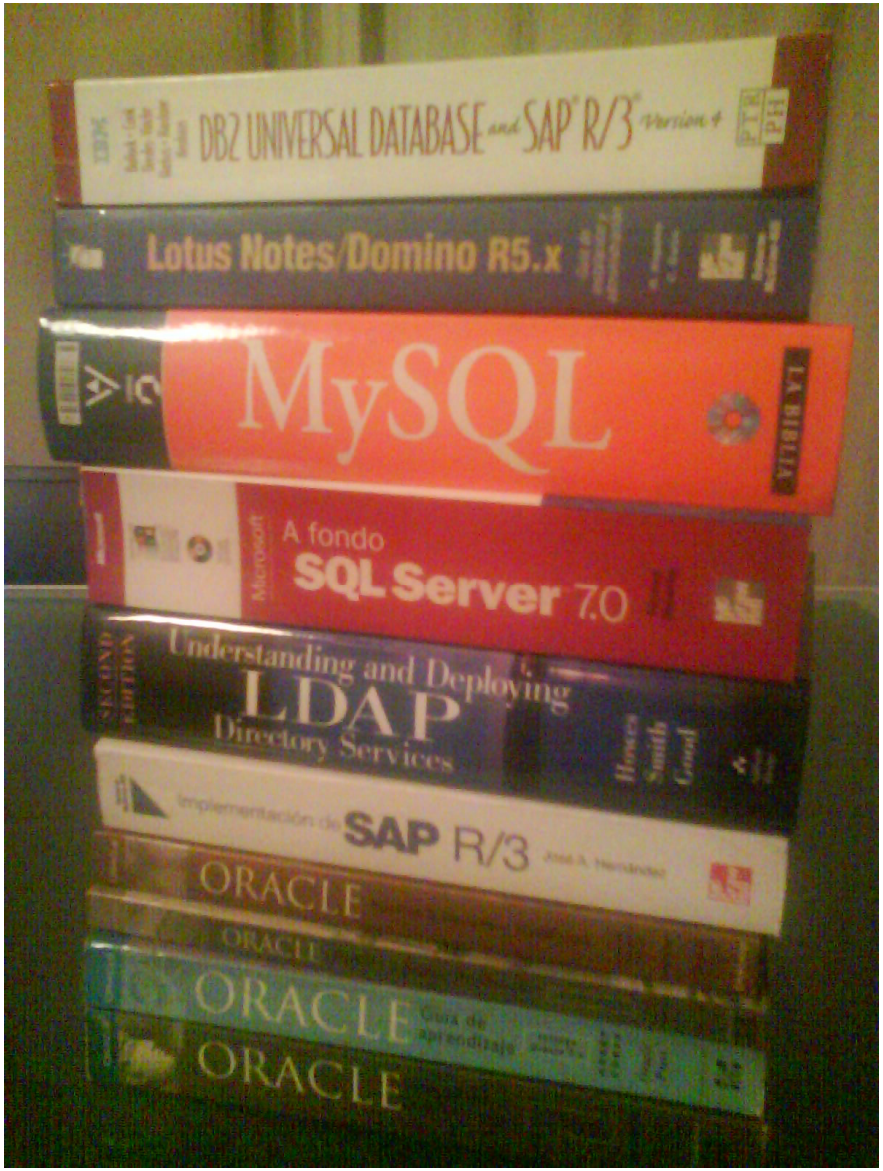
Protección y monitorización de la seguridad en las Bases de Datos con Herramientas SIEM



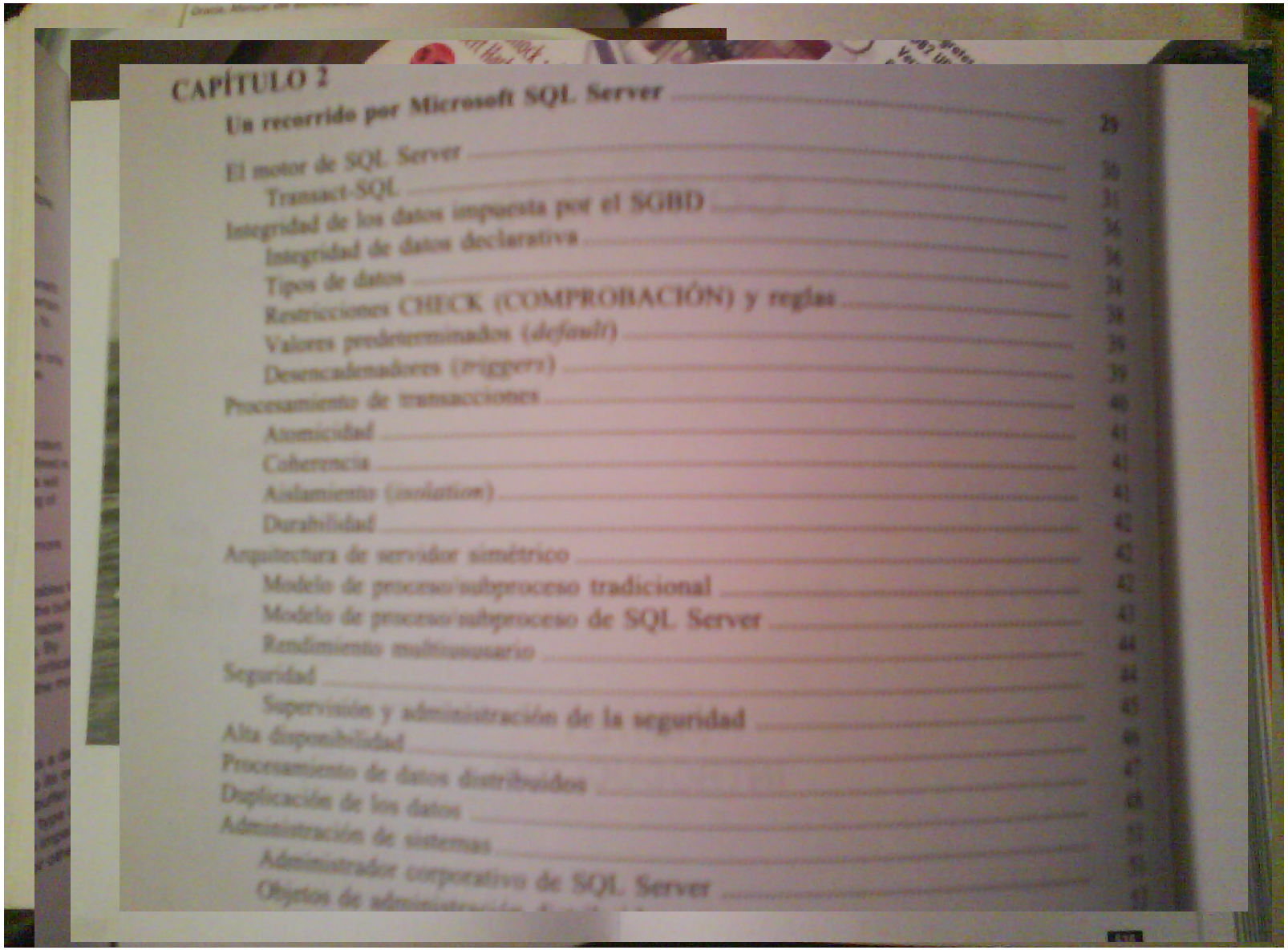
Agenda

- Introducción
- Informes para la protección y monitorización de la seguridad en bases de datos
- Cómo seleccionar una solución de SIEM
- Cómo implementar SIEM para protección de BBDD.
- Estudio de Caso de ROI
- Preguntas y respuestas

Seguridad en Bases De Datos



Seguridad en Bases De Datos



CAPÍTULO 2

Un recorrido por Microsoft SQL Server 29

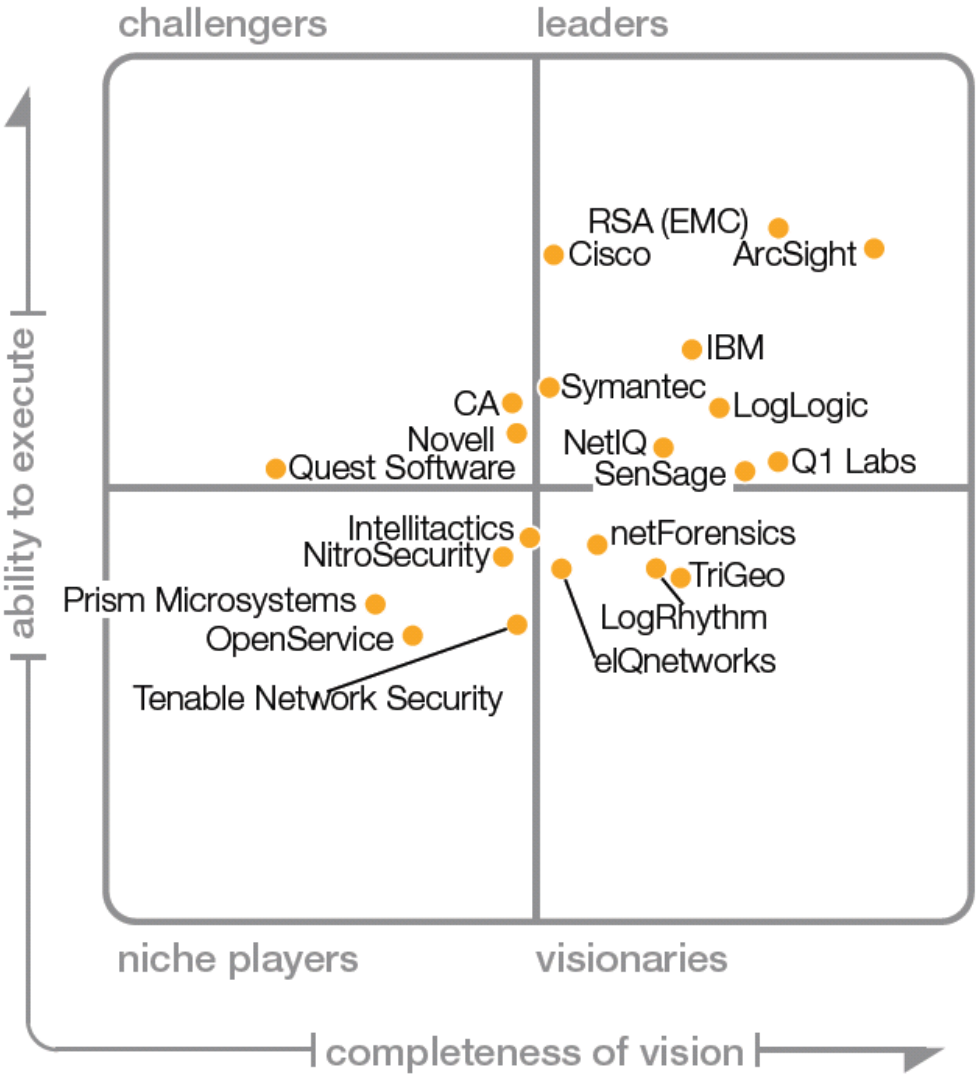
El motor de SQL Server 30
Transact-SQL 31
Integridad de los datos impuesta por el SGBD 34
Integridad de datos declarativa 34
Tipos de datos 34
Restricciones CHECK (COMPROBACIÓN) y reglas 38
Valores predeterminados (*default*) 39
Desencadenadores (*triggers*) 39
Procesamiento de transacciones 40
Atomicidad 41
Coherencia 41
Aislamiento (*isolation*) 41
Durabilidad 42
Arquitectura de servidor simétrico 42
Modelo de proceso/subproceso tradicional 42
Modelo de proceso/subproceso de SQL Server 43
Rendimiento multiusuario 44
Seguridad 44
Supervisión y administración de la seguridad 45
Alta disponibilidad 46
Procesamiento de datos distribuidos 47
Duplicación de los datos 48
Administración de sistemas 50
Administrador corporativo de SQL Server 50
Objetos de administración 52

Cumplimiento Normativo

Normativas actuales en cuanto a protección de datos

- Normativa Europea: (DPD) (94/46/CE)
- Constitución Española / Código Penal
- LOPD y sus reglamentos
- Sarbannes Oaxley
- Basilea II
- PCI
- ISO 27000
- …

Cuadrante Mágico de Gartner



Arquitectura lógica

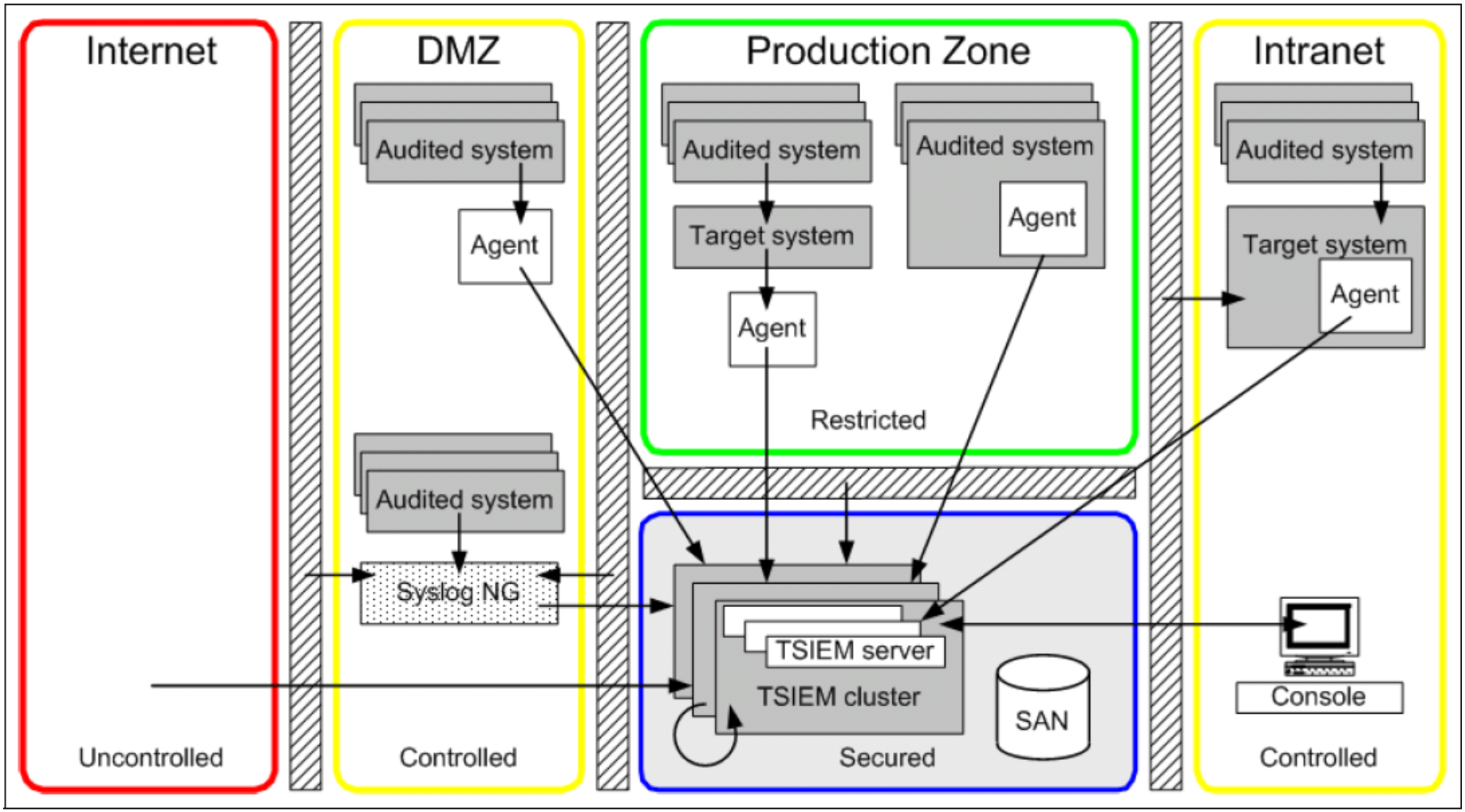
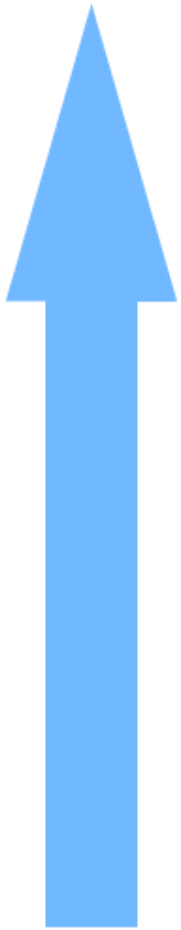


Figure 5-11 Large Tivoli Security Information and Event Manager deployment

Valor de una solución SIEM

Table 3-1 General SIEM requirements versus IBM SIEM solution

Increasing Value	SIEM Capability	IBM SIEM Capability
	Exception Reporting and Meeting compliance head on	▸ Report when a privileged user is doing something suspicious ▸ Privileged user monitoring and audit reporting ▸ Reporting on compliance exceptions
	Alerting and Reacting to risk	▸ Near real-time analytics ▸ Threshold alerting ▸ "Alert me when someone fails to logon multiple times to my Oracle application"
	Log Management and Checkbox compliance	▸ Reliable, verifiable log management ▸ Log management reporting ▸ Collect original log data
	Threat Aware	▸ Intrusion Detection and Intrusion Prevention Systems ▸ Appliance based ▸ Reacting to and protecting from threat

Soluciones de gestión de seguridad
para alcanzar los objetivos de TI

Tivoli. software

Cómo 10 informes pueden ayudarle a enfrentarse a los retos de auditoría de bases de datos más acuciantes

El informe de continuidad de logs hará que las visitas del auditor sean breves, ya que le ayuda a demostrar que recopila los logs.

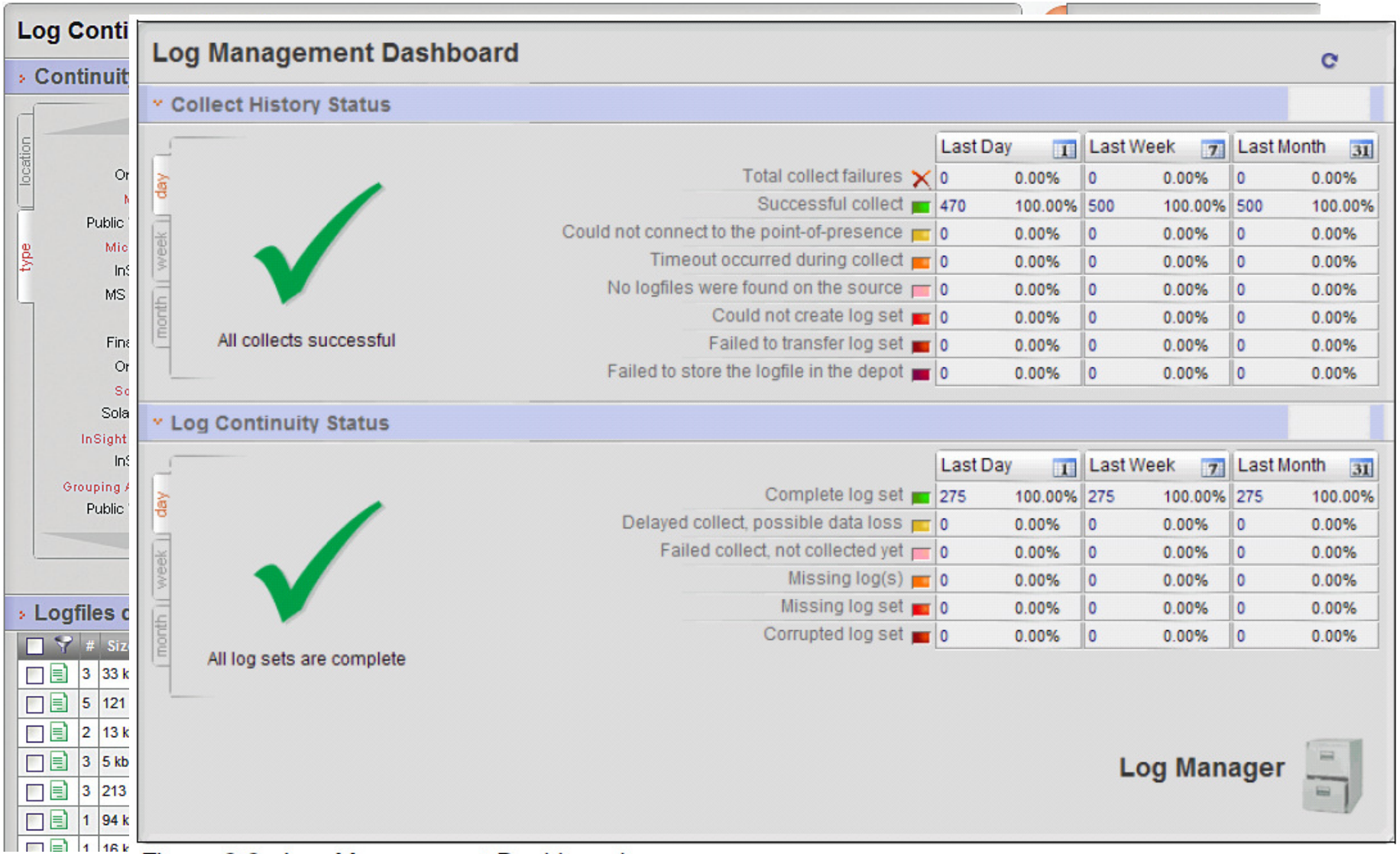
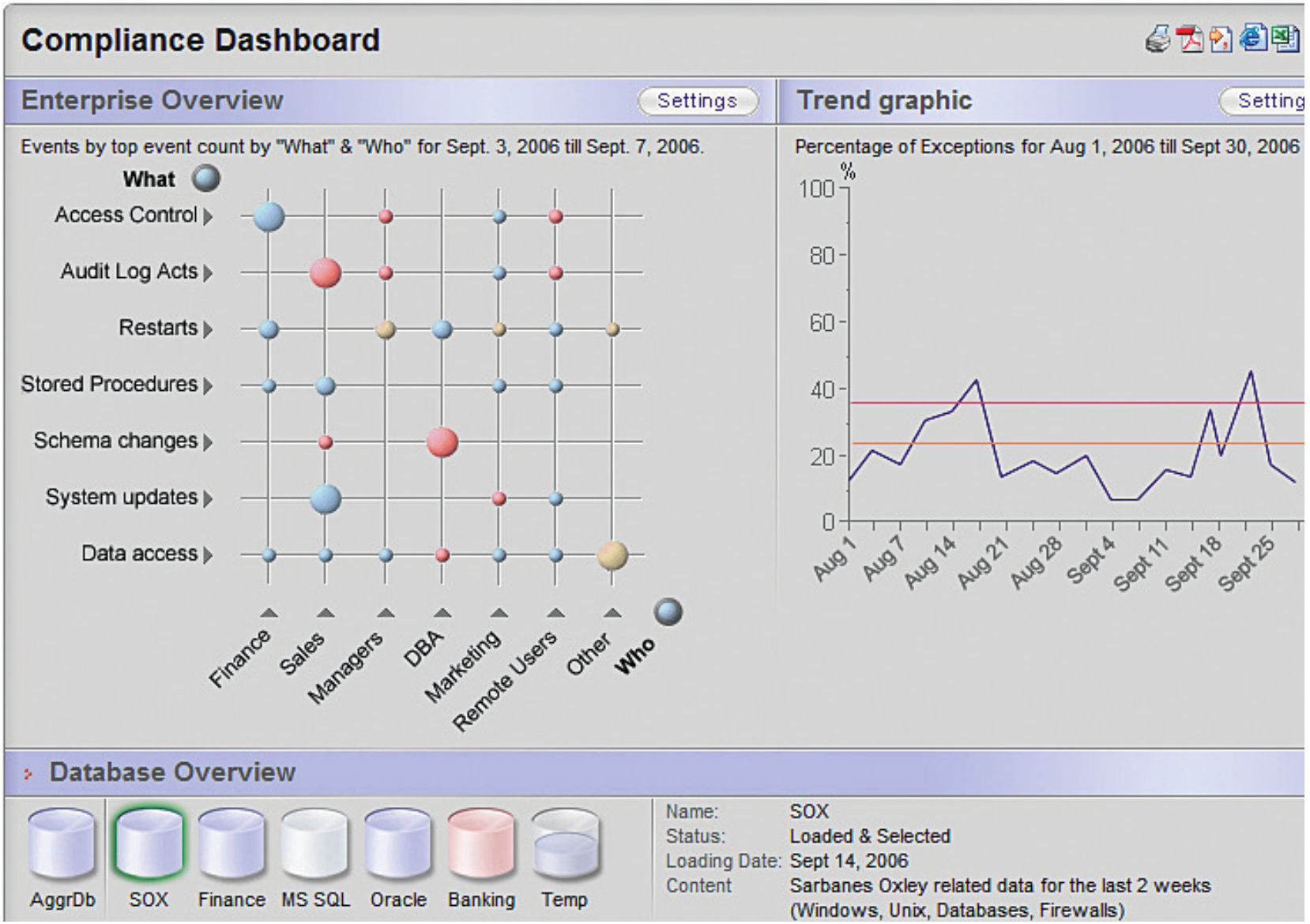


Figure 3-2 Log Management Dashboard

Cuadro de mandos empresarial con la actividad en las bases de datos



El informe de acceso a la base de datos directo le permite ver los accesos a la base de datos desde fuera de la capa de la aplicación.

Direct Database Access Report

Time period setup

	Month	Day	Year	Hour	Min.
Start time	September	3	2006	1	0
End time	September	7	2006	16	0

Execute Reset

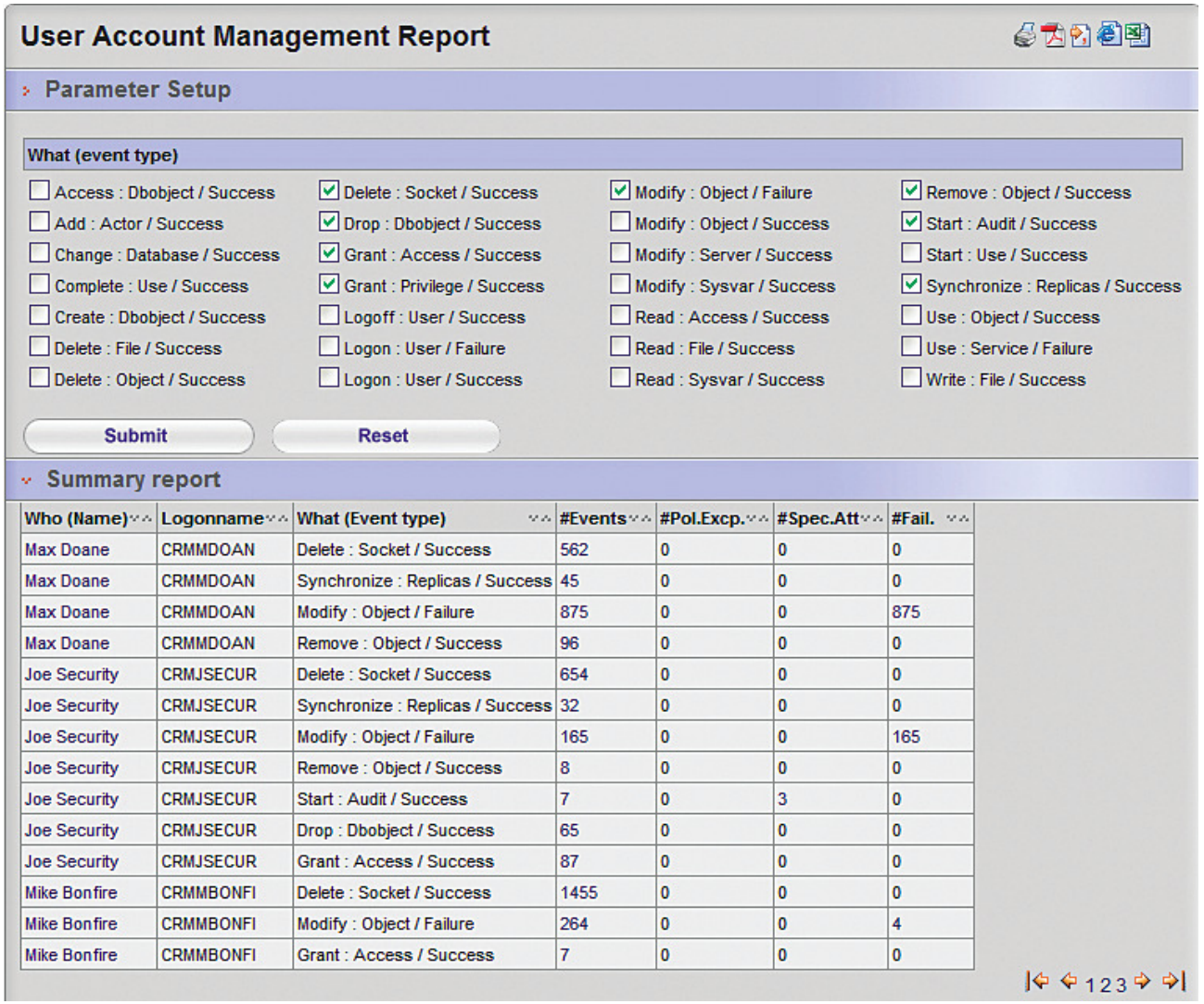
Time zone: Event time zone

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 : Dbobject / 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 : Dbobject / Success	Oracle Finance	Jim Hofferman	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
2	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
50	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
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 : Dbobject / 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 : Dbobject / 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 Hofferman	DB2 Server	DATABASE : - / Unavailable	DB2 Server
50	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
50	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
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 : Dbobject / Success	MS SQL Server	Joe Security	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 : Dbobject / Success	Oracle Finance	Mike Bonfire	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance

1 2 3 4 5 5

Los usuarios privilegiados pueden suponer un riesgo. El informe de gestión de cuentas de usuario le permite supervisar las acciones administrativas y minimizar el riesgo.



User Account Management Report

Parameter Setup

What (event type)

☐ Access : Dbobject / Success	☑ Delete : Socket / Success	☑ Modify : Object / Failure	☑ Remove : Object / Success
☐ Add : Actor / Success	☑ Drop : Dbobject / Success	☐ Modify : Object / Success	☑ Start : Audit / Success
☐ Change : Database / Success	☑ Grant : Access / Success	☐ Modify : Server / Success	☐ Start : Use / Success
☐ Complete : Use / Success	☑ Grant : Privilege / Success	☐ Modify : Sysvar / Success	☑ Synchronize : Replicas / Success
☐ Create : Dbobject / Success	☐ Logoff : User / Success	☐ Read : Access / Success	☐ Use : Object / Success
☐ Delete : File / Success	☐ Logon : User / Failure	☐ Read : File / Success	☐ Use : Service / Failure
☐ Delete : Object / Success	☐ Logon : User / Success	☐ Read : Sysvar / Success	☐ Write : File / Success

Submit Reset

Summary report

Who (Name)	Logonname	What (Event type)	#Events	#Pol.Excp.	#Spec.Att	#Fail.
Max Doane	CRMMDOAN	Delete : Socket / Success	562	0	0	0
Max Doane	CRMMDOAN	Synchronize : Replicas / Success	45	0	0	0
Max Doane	CRMMDOAN	Modify : Object / Failure	875	0	0	875
Max Doane	CRMMDOAN	Remove : Object / Success	96	0	0	0
Joe Security	CRMJSECUR	Delete : Socket / Success	654	0	0	0
Joe Security	CRMJSECUR	Synchronize : Replicas / Success	32	0	0	0
Joe Security	CRMJSECUR	Modify : Object / Failure	165	0	0	165
Joe Security	CRMJSECUR	Remove : Object / Success	8	0	0	0
Joe Security	CRMJSECUR	Start : Audit / Success	7	0	3	0
Joe Security	CRMJSECUR	Drop : Dbobject / Success	65	0	0	0
Joe Security	CRMJSECUR	Grant : Access / Success	87	0	0	0
Mike Bonfire	CRMMBONFI	Delete : Socket / Success	1455	0	0	0
Mike Bonfire	CRMMBONFI	Modify : Object / Failure	264	0	0	4
Mike Bonfire	CRMMBONFI	Grant : Access / Success	7	0	0	0

1 2 3

Informe de operaciones privilegiadas

Events by Type

Event type	#Events	#Pol.Excp.	#Spec.Att	#Fail.
Start : Use / Success	508037	0	0	0
Complete : Use / Success	505028	0	0	0
Modify : Object / Success	3503	400	23	0
Modify : Server / Success	752	0	55	0
Use : Service / Failure	1230	0	0	1230
Delete : Socket / Success	198	0	46	0
Synchronize : Replicas / Success	3	0	0	0
Modify : Object / Failure	10	0	0	10
Remove : Object / Success	1	0	1	0
Logoff : User / Success	119661	0	0	0
Logon : User / Success	120414	0	0	0
Access : Dbobject / Success	35972	96	241	0
Start : Audit / Success	3	0	3	0
Logon : User / Failure	683	0	0	683
Create : Dbobject / Success	2	0	0	0
Drop : Dbobject / Success	4	0	4	0
Grant : Access / Success	2	0	2	0
Change : Database / Success	4	0	2	0
Add : Actor / Success	16	6	6	0
Use : Object / Success	525751	0	0	0
Read : File / Success	452078	0	265	0
Modify : Sysvar / Success	37603	468	15	0
Read : Sysvar / Success	37472	156	0	0
Grant : Privilege / Success	63046	0	875	0

1 2 3

El informe de excepciones de procesos almacenados le ayuda a determinar fácilmente si se ha ejecutado algún procedimiento almacenado "deshonesto".

Stored Procedures Exceptions Report

- Time period setup
- Event List

When	#	What detail	Where detail	Who logonID	Who group	onWhat detail	onWhat Name
Fri Sep 15 2006 09:58:35 GMT-05:00	1	Access : Dbobject / Success	MS SQL Server	CRMMDOAN	IT	DBOBJECT : Master/sp_trace_create / Sp_trace_create	Sp_trace_create
Fri Sep 15 2006 09:58:35 GMT-05:00	932	Access : Dbobject / Success	MS SQL Server	CRMMDOAN	IT	DBOBJECT : Master/sp_trace_setevent / Sp_trace_setevent	Sp_trace_setevent
Fri Sep 15 2006 09:58:36 GMT-05:00	498	Access : Dbobject / Success	MS SQL Server	CRMMDOAN	IT	DBOBJECT : Master/sp_trace_setevent / Sp_trace_setevent	Sp_trace_setevent
Fri Sep 15 2006 09:58:36 GMT-05:00	1	Access : Dbobject / Success	MS SQL Server	CRMMDOAN	IT	DBOBJECT : Master/sp_trace_setstatus / Sp_trace_setstatus	Sp_trace_setstatus
Fri Sep 15 2006 13:36:00 GMT-05:00	1	Access : Dbobject / Success	Oracle	CRMJSECUR	Administrators	DBOBJECT : Master/sp_mssqldmo80_version / Sp_mssqldmo80_version	Sp_mssqldmo80_version
Fri Sep 15 2006 13:36:01 GMT-05:00	1	Access : Dbobject / Success	Oracle	CRMJSECUR	Administrators	DBOBJECT : Master/sp_msdbuserpriv / Sp_msdbuserpriv	Sp_msdbuserpriv
Fri Sep 15 2006 13:36:01 GMT-05:00	1	Access : Dbobject / Success	Oracle	CRMJSECUR	Administrators	DBOBJECT : Master/sp_msgetversion / Sp_msgetversion	Sp_msgetversion
Fri Sep 15 2006 13:36:02 GMT-05:00	1	Access : Dbobject / Success	Oracle	CRMJSECUR	Administrators	DBOBJECT : Master/sp_get_distributor / Sp_get_distributor	Sp_get_distributor
Fri Sep 15 2006 13:36:02 GMT-05:00	1	Access : Dbobject / Success	Oracle	CRMJSECUR	Administrators	DBOBJECT : Master/sp_msenum_agents / Sp_msenum_replication_agents	Sp_msenum_agents
Fri Sep 15 2006 13:36:13 GMT-05:00	3	Access : Dbobject / Success	DB2	CRMJSECUR	Administrators	DBOBJECT : Master/sp_msdbuseraccess / Sp_msdbuseraccess	Sp_msdbuseraccess
Fri Sep 15 2006 13:36:15 GMT-05:00	4	Access : Dbobject / Success	DB2	CRMJSECUR	Administrators	DBOBJECT : Master/sp_executesql / Sp_executesql	Sp_executesql
Fri Sep 15 2006 13:36:15 GMT-05:00	4	Access : Dbobject / Success	Oracle	CRMMBONFI	Administrators	DBOBJECT : Master/sp_msrepl_isdbowner / Sp_msrepl_isdbowner	Sp_msrepl_isdbowner
Fri Sep 15 2006 13:36:15 GMT-05:00	2	Access : Dbobject /	Oracle	CRMMBONFI	Administrators	DBOBJECT :	Sp_helpreplicationdboption

El informe de eventos del sistema de bases de datos le ayuda a controlar los riesgos en sistemas de bases de datos.

Database System Events

Time period setup

	Month	Day	Year	Hour	Min.
Start time	September	3	2006	1	0
End time	September	7	2006	16	0

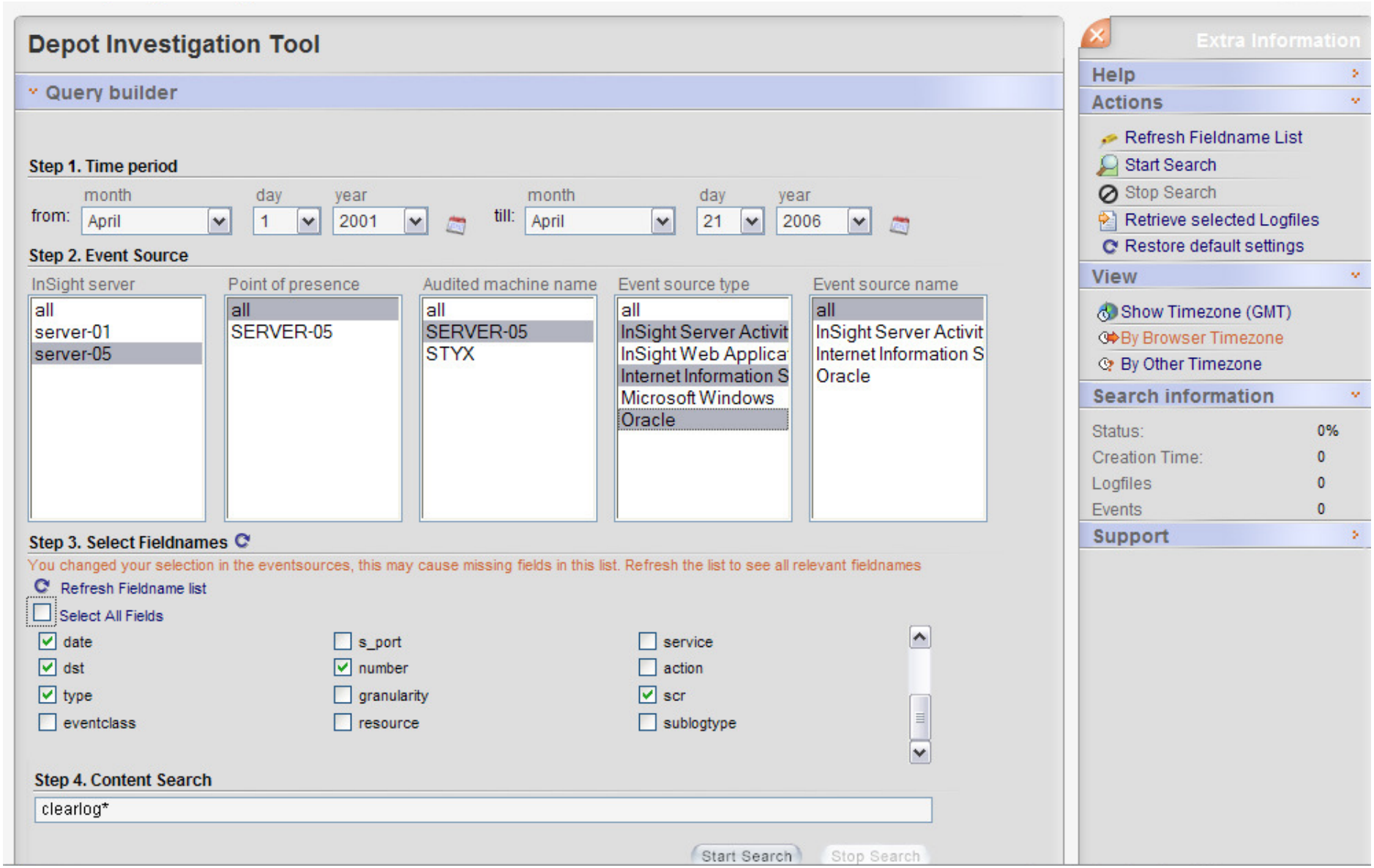
Execute Reset

Time zone: Event time zone

Event List

When	#	What class	Where field	Who logonID	Who group	Wherefrom field	onWhat detail
Fri Sep 15 2006 09:53:38 GMT-05:00	1	Stop	MSSQLSRV	SYSTEM	System	MSSQLSRV	SERVICE : - / Mssqlsrv
Fri Sep 15 2006 09:53:38 GMT-05:00	1	Stop	MSSQLSRV	SYSTEM	Unknown	MSSQLSRV	SERVICE : - / Mssqlsrv
Fri Sep 15 2006 09:58:30 GMT-05:00	1	Start	MSSQLSRV	SYSTEM	System	MSSQLSRV	SERVICE : - / Mssqlsrv
Fri Sep 15 2006 09:58:30 GMT-05:00	1	Start	MSSQLSRV	SYSTEM	Unknown	MSSQLSRV	SERVICE : - / Mssqlsrv
Fri Sep 15 2006 09:58:36 GMT-05:00	1	Start	MSSQLSRV	sa	IT	MSSQLSRV	AUDITLOG : - / Unavailable
Fri Sep 15 2006 09:58:36 GMT-05:00	1	Start	MSSQLSRV	sa	Unknown	MSSQLSRV	AUDITLOG : - / Unavailable
Fri Sep 15 2006 09:58:36 GMT-05:00	1	Start	MSSQLSRV	sa	Administrators	MSSQLSRV	AUDITLOG : - / Unavailable
Fri Sep 15 2006 09:58:36 GMT-05:00	1	Start	MSSQLSRV	sa	Database Admin	MSSQLSRV	AUDITLOG : - / Unavailable
Fri Sep 15 2006 13:36:02 GMT-05:00	1	Create	MSSQLSRV	CRMMDOAN	IT	MSSQLSRV	DBOBJECT : Master/ucsnapshot / Ucsnapshot
Fri Sep 15 2006 13:36:02 GMT-05:00	1	Create	MSSQLSRV	CRMMDOAN	Unknown	MSSQLSRV	DBOBJECT : Master/ucsnapshot / Ucsnapshot
Fri Sep 15 2006 13:36:02 GMT-05:00	1	Create	MSSQLSRV	CRMMDOAN	Systems Admin	MSSQLSRV	DBOBJECT : Master/ucsnapshot / Ucsnapshot
Fri Sep 15 2006 13:36:02 GMT-05:00	1	Create	MSSQLSRV	CRMMDOAN	Administrators	MSSQLSRV	DBOBJECT : Master/ucsnapshot / Ucsnapshot
Fri Sep 15 2006 13:36:02 GMT-05:00	1	Create	MSSQLSRV	CRMJSECUR	Systems Admin - Production	MSSQLSRV	DBOBJECT : Master/ucsnapshot / Ucsnapshot
Fri Sep 15 2006 13:36:13 GMT-05:00	1	Drop	MSSQLSRV	CRMJSECUR	IT	MSSQLSRV	DBOBJECT : Tempdb/#tmpdbuserprofile...
Fri Sep 15 2006 13:36:13 GMT-05:00	1	Drop	MSSQLSRV	CRMJSECUR	IT	MSSQLSRV	DBOBJECT : Tempdb/#tmpout...

El informe de todos los eventos le permite ver de un vistazo todos los eventos de DBMS.



El informe de resumen de usuario permite investigar las acciones de cualquier usuario y detectar rápidamente cualquier comportamiento sospechoso.

User Summary of Max Doane as CRM\Admin\MDOANE

User information

Name	Max Doane
Logonname	CRM\Admin\MDOANE
#Events	15436
#Attention	245
#Exception	103
#Logon	21
#Logoff	20
#LogonFail	2
#Failure	65

Who

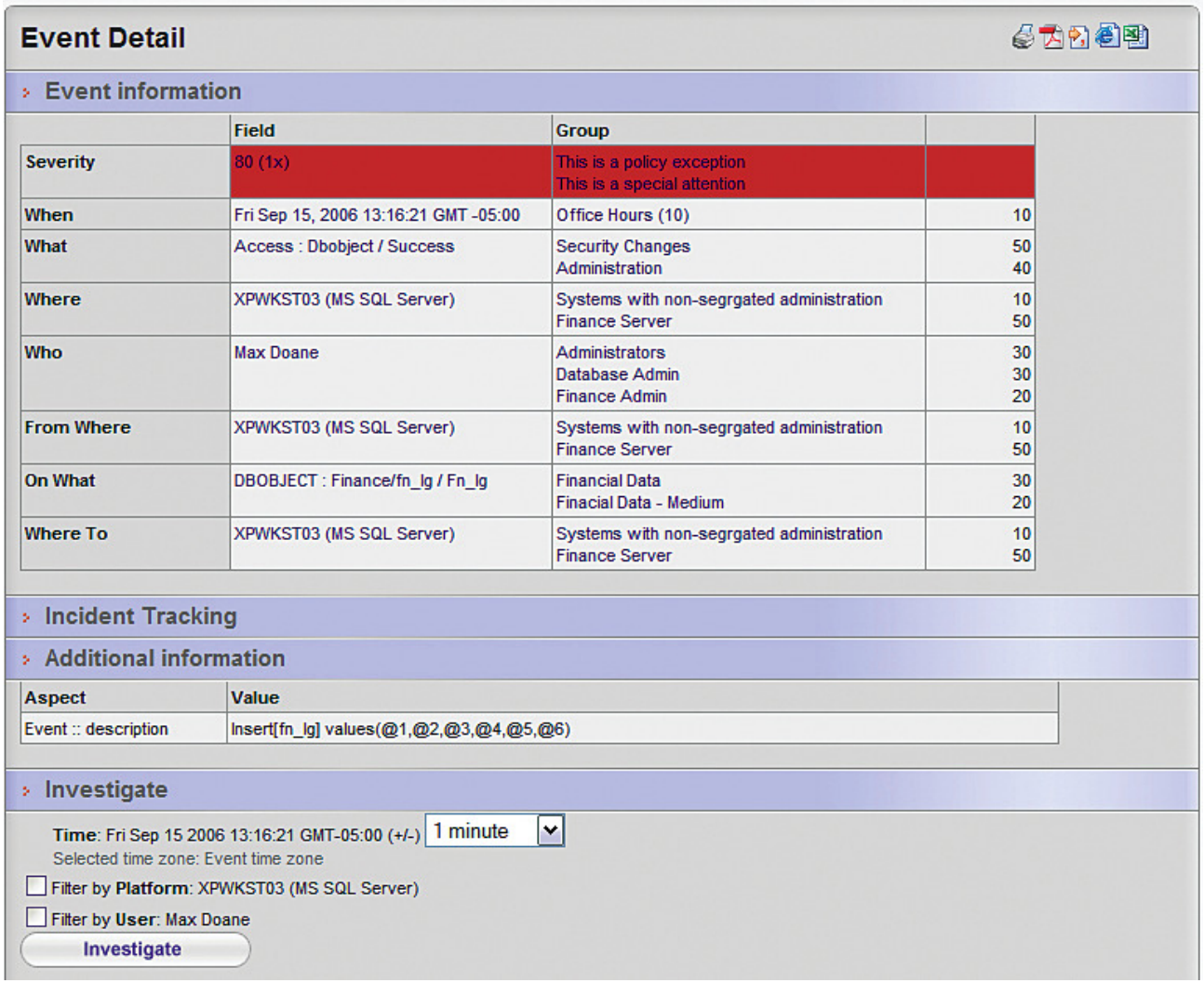
Who (Source group)
Administrators
Database Admin
Finance Admin

When

What on What

What (Event group)	**On What (Object group)**	**#Events**
Application Access	Financial Data (Oracle)	356
Application Access	HR Data (MS SQL)	2
Backup - DB	Financial Data (Oracle)	56
Backup - DB	HR Data (MS SQL)	6
DB - Logon_off	Financial Data (Oracle)	56
DB - Logon_off	HR Data (MS SQL)	16
DB Administration	Financial Data (Oracle)	43
DBA - StoreProcedures	Financial Data (Oracle)	461
DBA - StoreProcedures	HR Data (MS SQL)	16

El informe de detalles de evento le permite ver de manera instantánea todos los detalles de una acción potencialmente fraudulenta.



Event Detail

Event information

	Field	Group	
Severity	80 (1x)	This is a policy exception This is a special attention	
When	Fri Sep 15, 2006 13:16:21 GMT -05:00	Office Hours (10)	10
What	Access : Dbobject / Success	Security Changes Administration	50 40
Where	XPWKST03 (MS SQL Server)	Systems with non-segrgated administration Finance Server	10 50
Who	Max Doane	Administrators Database Admin Finance Admin	30 30 20
From Where	XPWKST03 (MS SQL Server)	Systems with non-segrgated administration Finance Server	10 50
On What	DBOBJECT : Finance/fn_lg / Fn_lg	Financial Data Finacial Data - Medium	30 20
Where To	XPWKST03 (MS SQL Server)	Systems with non-segrgated administration Finance Server	10 50

Incident Tracking

Additional information

Aspect	Value
Event :: description	Insert[fn_lg] values(@1,@2,@3,@4,@5,@6)

Investigate

Time: Fri Sep 15 2006 13:16:21 GMT-05:00 (+/-) 1 minute

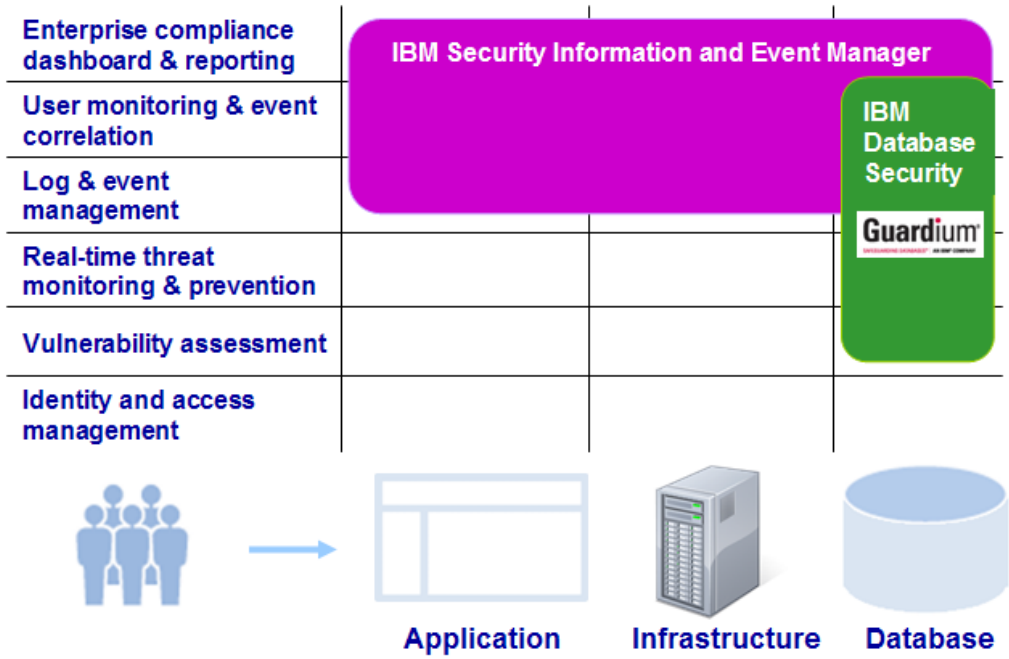
Selected time zone: Event time zone

Filter by **Platform**: XPWKST03 (MS SQL Server)

Filter by **User**: Max Doane

Investigate

Introducing Security Activity Monitoring for the Enterprise with TSIEM and Guardium

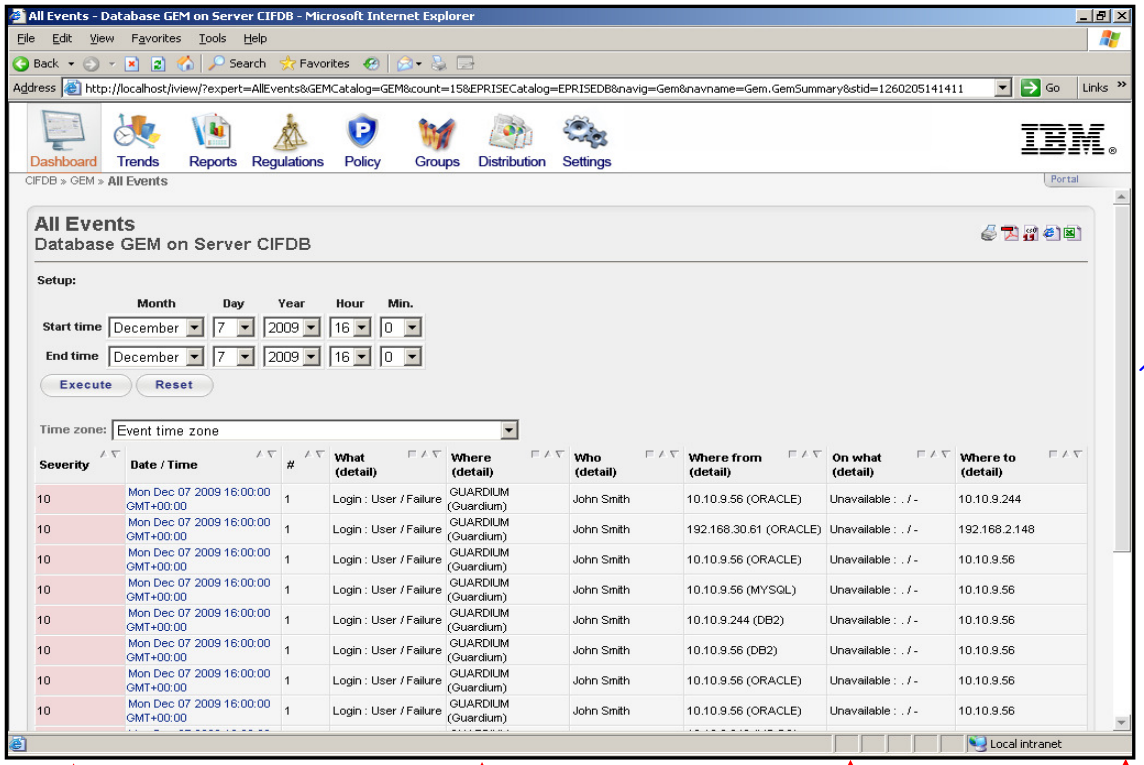


- Enterprise dashboard with compliance management modules and regulation-specific reports
- Broadest coverage, collecting and correlating logs and events across systems, devices, middleware and applications
- With Guardium, IBM:
  - Monitors all DB activities in *real-time*, including privileged users, without the performance impact and separation of duties issues of native DB logging
  - Provides capabilities such as blocking, workflow management and vulnerability assessments

Integrated Solution Facts:

- TSIEM Enterprise dashboard and compliance reports fully support Guardium events
- Integrated solution offering with Quick-Start will give the customer pre-defined set of integrated reports AND custom alerts (include Quick-Start Services in all deals)
- Enhanced out of the box integration capability in Q310

Integración de eventos generados por tecnologías especializadas



IT Operations Escalation
- *Netcool Omnibus*
- *Tivoli Service Request Mgr.*
- *TEC*
- *BA Dashboards*

Long-term log storage/archiving

Guardium
- DB2 (Host/Distributed)
- DB2/z
- Sybase
- Oracle Database
- Teradata
- SQL Server,

SiteProtector
- Applications (Rational AppScan)
- Virtualized Resources (VSP)
- Network (Network IPS)
- Hosts (Host IPS)

IAA
- Tivoli Identity Manager
- Tivoli Unified Single Sign On
- Tivoli Security Operations Manager

Others
- Data and Applications
- NOC/SOC devices

Guía del comprador de Tecnologías SIEM

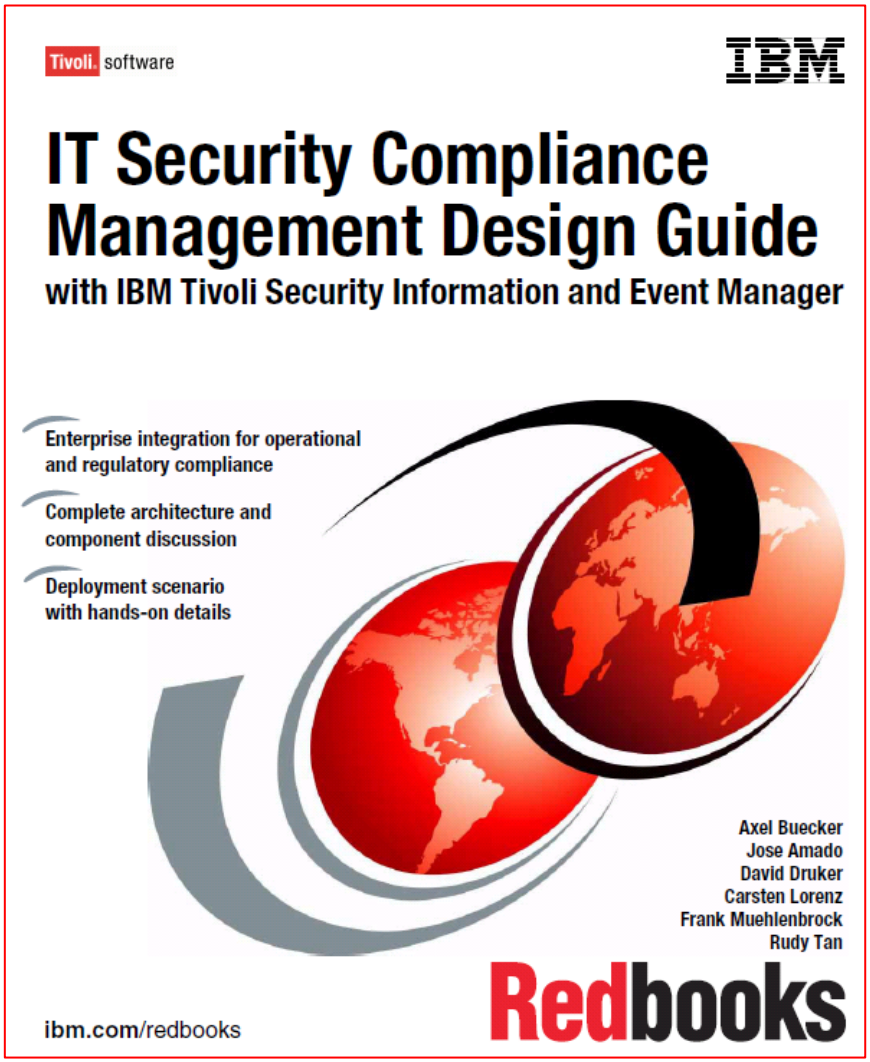
Gestión centralizada de logs		
Buscar una solución que:	**IBM**	**Otro proveedor**
Proporcione un proceso de gestión de logs fiable y verificable.	✓	
Incluya un panel de control de gestión de logs para ver el estado global del proceso de dicha gestión.	✓	
Proporcione a los administradores un informe histórico de recopilación de logs que les permita ver el historial del proceso de recogida, determinar si se ejecuta correctamente y realizar un nivel de diagnóstico utilizando el informe.	✓	

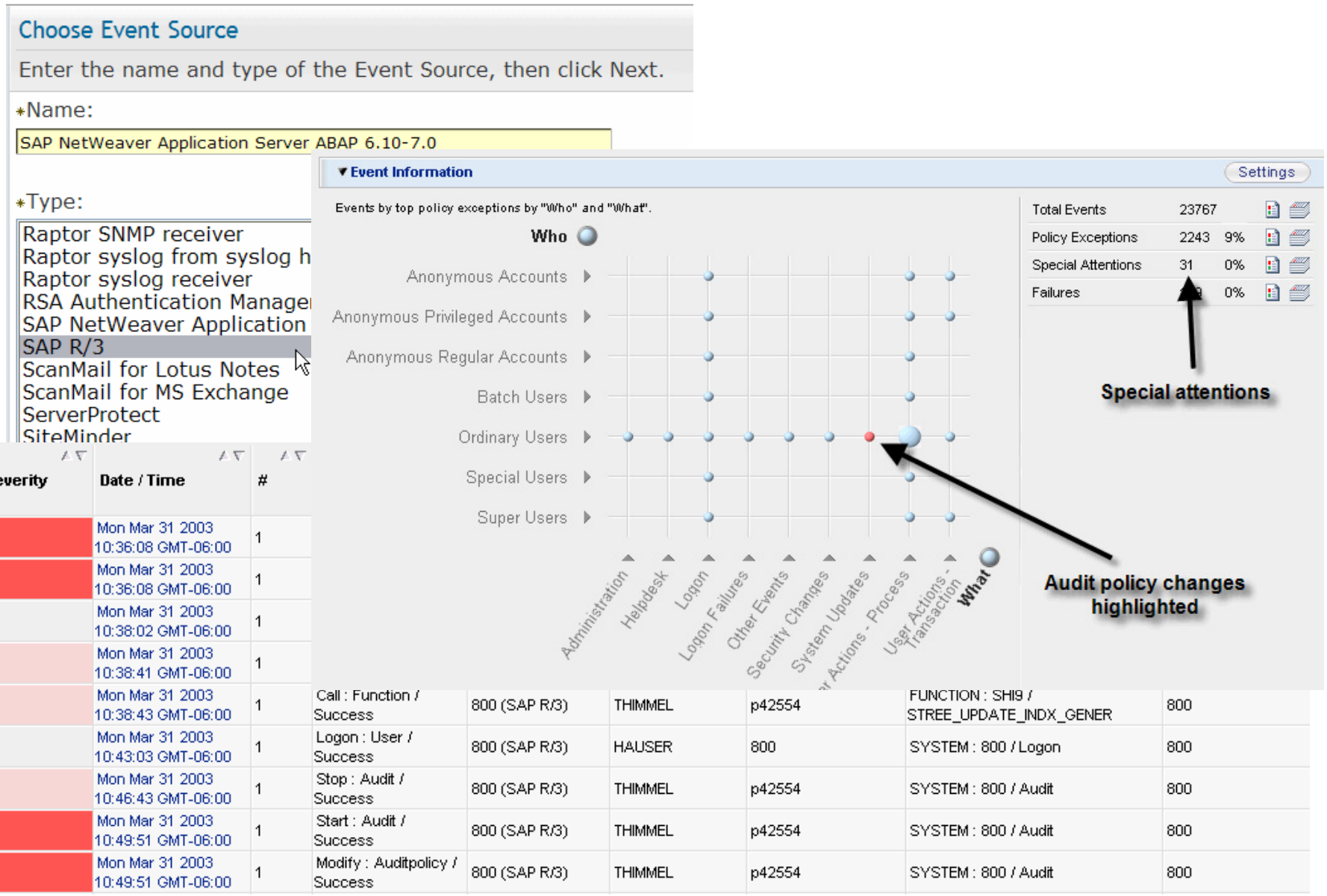
Gestión centralizada de logs		
Buscar una solución que:	**IBM**	**Otro proveedor**
Permita a los auditores y personal de seguridad supervisar y auditar de forma efectiva la recogida de datos de log para asegurar que no se pierden datos.	✓	
Proporcione a los auditores un informe de continuidad de log (en formato gráfico y de tabla) para permitirles ver qué dispositivos y aplicaciones se están supervisando, determinar si existe un conjunto continuo de logs recopilados para dichos dispositivos e indicar los problemas que hay que atender.	✓	
Incluya una herramienta de investigación de logs con un servicio de búsqueda similar al de Google para buscar los datos de log sin procesar recopilados para eventos o datos específicos.	✓	
Incluya una herramienta de recuperación de logs que permita al usuario buscar y recuperar archivos de log específicos del almacén de logs.	✓	
Proporcione alerta proactiva sobre la recopilación de errores para que las pérdidas potenciales de datos de auditoría se puedan minimizar o eliminar.	✓	
Proporcione alerta proactiva sobre la recopilación de errores para que las pérdidas potenciales de datos de auditoría se puedan minimizar o eliminar.	✓	
Proporcione informes programados en base a una planificación definida por el usuario.	✓	
Permita la exportación de informes en formatos como PDF y CSV, para conexión con otras aplicaciones y flujos de trabajo.	✓	
Aproveche las herramientas avanzadas de informes (BIRT en inglés) para crear nuevos informes personalizados que se ajusten a sus necesidades específicas.	✓	
Organice los logs recopilados utilizando un esquema de indexación para una identificación y almacenamiento más sencillos.	✓	
Almacene logs en formato comprimido para reducir las necesidades de almacenamiento.	✓	

Informe para auditoría y cumplimiento de normativas		
Buscar una solución que:	**IBM**	**Otro proveedor**
Le permita ordenar y revisar fácilmente una gran cantidad de eventos y analizarlos desde distintas perspectivas.	✓	
Proporcione informes en un lenguaje sencillo que pueda ser entendido por auditores o demás personal no técnico.	✓	
Incluya el nombre real del usuario tal y como está en el directorio o el sistema de seguridad, para que el informe sea más legible.	✓	
Proporcione módulos de gestión de cumplimiento normativo con funciones de informes específicas para sus necesidades, cubriendo las normativas y mejores prácticas más importantes, incluyendo la International Organization for Standardization (ISO 27001), Sarbanes-Oxley (SOX), Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Basel II, Federal Information Security Management Act (FISMA), etc.	✓	
Incluya más de 50 informes de auditoría parametrizados (equivalentes a varios cientos e incluso miles de informes individuales).	✓	
Utilice un modelo de normalización sólido (patente en curso).	✓	
Incluya un desarrollador de informes personalizados que sea flexible y esté optimizado para el modelo de normalización, lo que le permite crear sus propios informes de auditoría y cumplimiento normativo sin necesidad de saber SQL.	✓	
Incluya un sistema de distribución de informes para distribuir informes de cumplimiento normativo y auditorías a los propietarios de la empresa o accionistas, para su revisión, aprobación, comentarios o toma de decisiones.	✓	
Proporcione plantillas de clasificación específicas para el cumplimiento normativo.	✓	
Proporcione una plantilla de política específica para cumplimiento normativo que represente los controles dentro de una normativa.	✓	

Informe para auditoría y cumplimiento de normativas

Buscar una solución que:	**IBM**	**Otro proveedor**
Proporcione informes específicos de cumplimiento normativo que le permitan supervisar los aspectos de cumplimiento contra controles concretos.	✓	
Proporcione informes de cumplimiento diseñados, creados y basados en estándares (frente al simple cambio de nombre de informes operacionales).	✓	
Proporcione un panel de control para el cumplimiento normativo que muestre el estado actual de cumplimiento utilizando el lenguaje de las normativas y políticas actuales, para su fácil lectura.	✓	
Proporcione información de tendencias a nivel del panel de control, que le ayuden a indicar la tendencia del estado de cumplimiento y asegurar el cumplimiento de los objetivos.	✓	
Proporcione detalles desde el más alto nivel del panel de control de cumplimiento hasta los detalles internos de los eventos, para una investigación más detallada.	✓	
Proporcione informes a nivel de log sin procesar, utilizando un sencillo mecanismo de consulta para investigaciones de tipo legal.	✓	
Incluya un motor de informes completo, con informes programados.	✓	
Automatice la distribución de los informes a los propietarios del negocio para su revisión y aprobación, como parte del proceso empresarial global y de cumplimiento normativo.	✓	
Incluya un diseñador de informes personalizado que no precise de conocimientos especiales (como saber lenguajes de script o SQL) para crear informes rápidamente.	✓	
Facilite la comunicación de niveles de amenaza y actividades de seguridad a través de las plantillas de informes estándar y personalizables incluidas, controladas desde un planificador automatizado de informes.	✓	
Proporcione una amplia variedad de formatos de salida para los informes, incluyendo HTML, PDF, CSV y XLS, exportando todos los gráficos y diagramas.	✓	
Incluya plantillas predeterminadas para los informes de cumplimiento normativo específico de regulaciones.	✓	



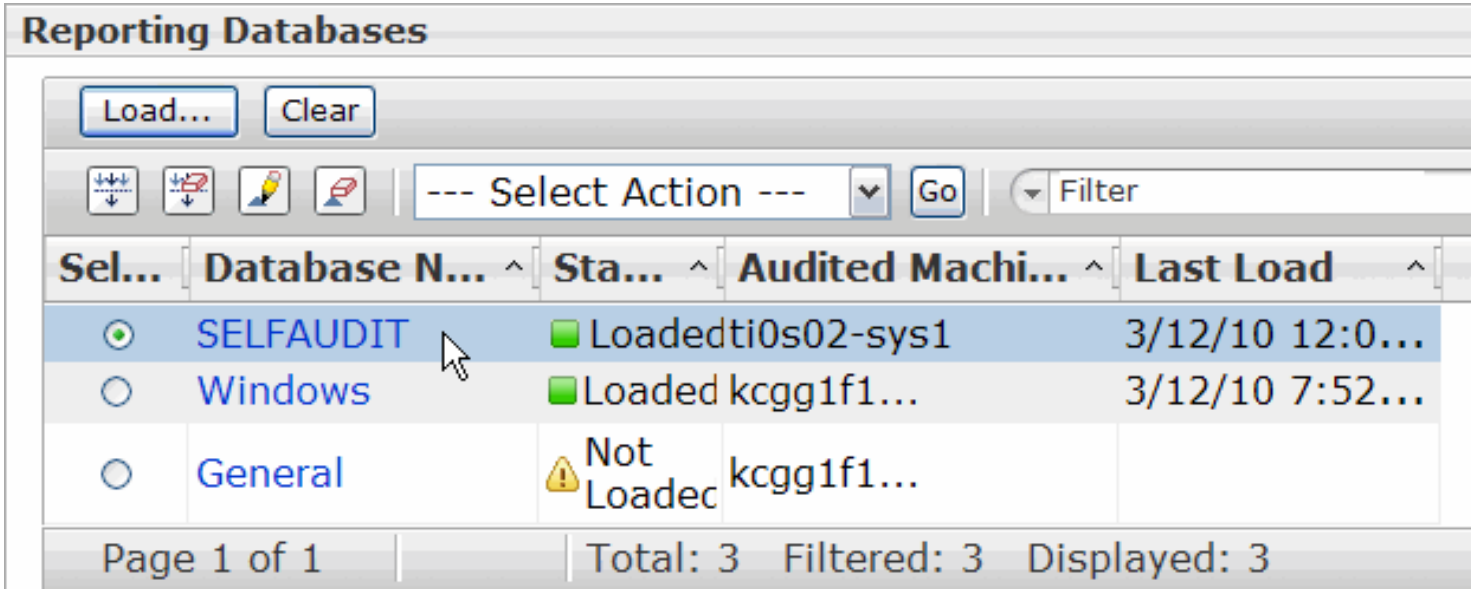


Integración

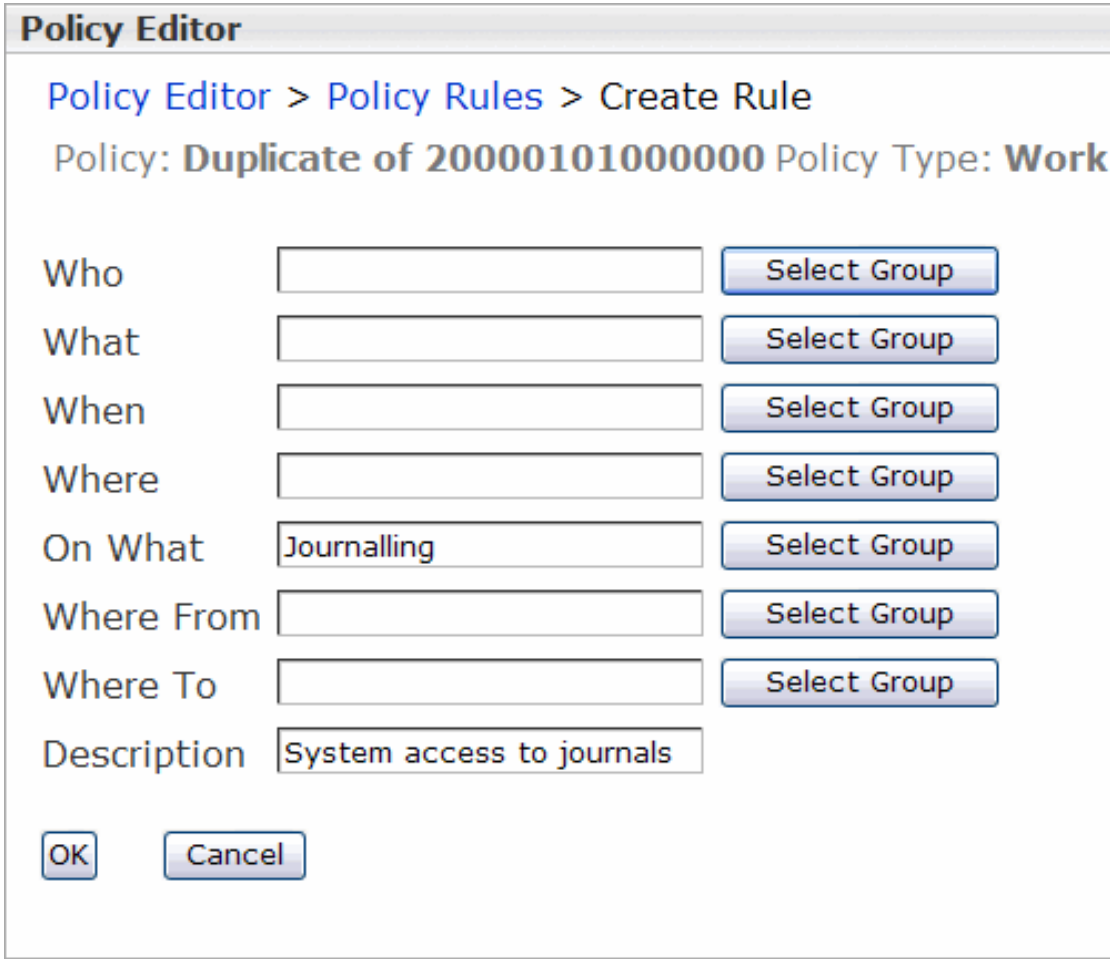
- Agent-less data collection

Tivoli Security Information and Event Manager supports agent-less collection on Microsoft® Windows, Novell, IBM System i® (formerly known as AS/400® or iSeries®), and UNIX® platforms.

Autoauditoría



Cómo crear nuevas políticas



Ejemplo: Políticas para Basilea II

Policy Template

download

▼ **Policy Rules**

Who group	What group	When group	Where group	On What group	From Where group	Where To group	Description
Sales Management				Customer Data			
HR Staff		Office Hours		HR Data	Local Workstation		
Finance Staff		Office Hours		Financial Data			
	Logon						
Managers		Office Hours					
Marketing		Office Hours		Customer Data			
	System Operations						
	System Processes						
IT							
HR Management		Out of Office Hours		HR Data			
Users		Office Hours		General Data			
Administrators			Systems with non-segregated administration				
Sales Staff		Office Hours		Customer Data			

▶ **Attention Rules**

Ejemplo: reglas de atención para Basilea II

Policy Template

download

▶ **Policy Rules**

▼ **Attention Rules**

Who group	What group	When group	Where group	On What group	From Where group	Where To group	ID	Severity	Description
IT				Customer Data - Low			access low	20	Review
IT				Organizational Data			access low	25	Review
	User Actions - File			Administration Objects			medium	40	Requires attention
IT				HR Data - Medium			access medium	50	Requires attention
	Collect Failure						collect_failure	70	Requires immediate attention
IT				Customer Data - Medium			access medium	50	Requires attention
Administrators				Organizational Data			access medium	50	Review
	Intrusion - High						high	70	Requires immediate attention
	Alerts - Medium						medium	50	Requires attention
IT				Proprietary Data			access low	25	Review
IT				Non-Public Data			access low	25	Review

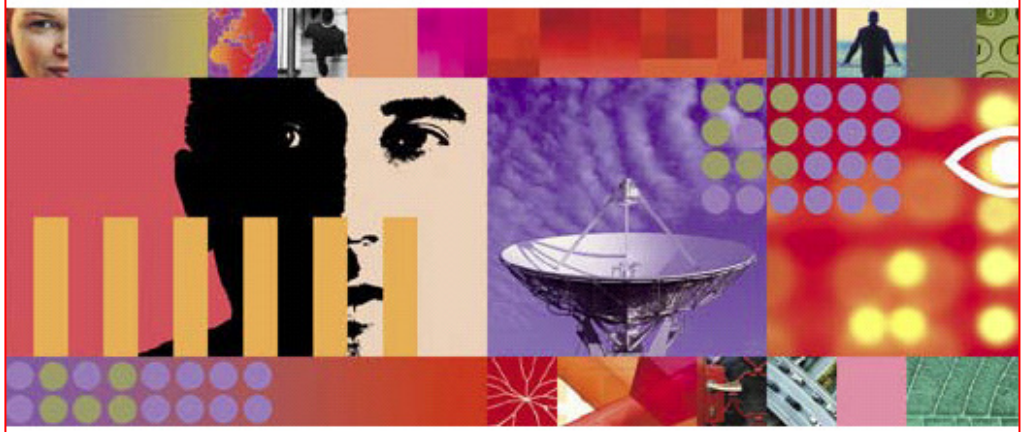
BASEL II Regulation Reports

Add custom report | Import custom reports

BASEL II

Title	Description	Action
BASEL II Internal attacks - quarterly trend	Number of exceptions NOT in the Exposure and Intrusion groups quarter over quarter	
BASEL II (,) External attacks - monthly trend	Number of exceptions in the Exposure and Intrusion groups month over month	
BASEL II (,) External attacks - quarterly trend	Number of exceptions in the Exposure and Intrusion groups quarter over quarter	
BASEL II (,) Internal attacks - monthly trend	Number of exceptions NOT in the Exposure and Intrusion groups month over month	
BASEL II (,) Policy Exceptions - monthly trend	Number of exceptions month over month	
BASEL II (,) Policy Exceptions - quarterly trend	Number of exceptions quarter over quarter	
BASEL II (5.2,5.2) Classification	Assets defined to the system.	
BASEL II (6.3,8.1.3,8.1.3) Security alert	Alerts sent in response to policy exceptions or special attention exceptions.	
BASEL II (6.3.4,8.1.3,8.1.3) Incident tracking	Policy exceptions and incident tickets recorded against them.	
BASEL II (8.1.2,8.1.2) Operational change control	Changes to the operating environment such as system updates, DBA activity, and so on.	
BASEL II (8.1.6,8.1.6) External contractors	Exceptions and Failures Caused by External Contractors.	
BASEL II (8.3,8.3) Malicious attacks	Exceptions and failures due to Malicious attacks.	
BASEL II (8.4,9.7.1,9.7.1) Log archive	Log archive dates and locations.	
BASEL II (8.4,9.7.1,9.7.1) Log collection	Log collection schedule and platforms.	
BASEL II (8.4,9.7.1,9.7.1) Log storage	Log storage report for all platforms.	
BASEL II (8.4.2,8.4.2) Operator log	Actions performed by the IT Admin staff.	
BASEL II (8.5,8.5) Network management	Actions and events caused by users on Network Services.	

Tivoli software



Tivoli Business Value Analyst Product Savings for Security

Versión 3.7.4

➔ **IBM Tivoli Compliance Insight Manager:**

Tivoli Compliance Insight Manager proporciona un sencillo panel de instrumentos de conformidad de seguridad que resume miles de millones de archivos de registro en un gráfico general. Una solución completa y automatizada para supervisar, investigar e informar sobre las actividades de los usuarios en toda la empresa, Tivoli Compliance Insight Manager puede proporcionar garantías y pruebas documentales, continuas y no intrusivas, de que sus datos y sistemas están siendo gestionados de acuerdo con las políticas de la empresa. Basado en más de dos décadas de experiencia en auditorías de seguridad y gestión de la conformidad, Tivoli Compliance Insight Manager ofrece una solución líder del sector para el análisis de registros, supervisión y auditoría de usuarios privilegiados e informes sobre conformidad y auditorías de toda la empresa, desde el perímetro y dispositivos de red hasta aplicaciones, bases de datos y sistemas operativos.

- Reducciones de costes de IT/ahorro en plantilla de gestión de seguridad
  - Gestión de políticas 15%

    InSight permite codificar reglas "w7" prácticas tipo "Quién puede hacer qué, Cuándo, Dónde, Desde dónde y Adónde" para que puedan supervisarse y aplicarse de forma automática políticas de uso aceptable y de gestión de cambios.
  - Gestión de intrusiones 5%

    Los intrusos suelen ser a menudo usuarios de confianza y con autorización que tienen acceso a la red pero que aún resultan peligrosos. InSight rastrea, supervisa y alerta cuando usuarios de confianza entran en datos confidenciales y propietarios.
  - Reparación y resolución 5%

    Clientes en todo el mundo utilizan las funciones investigadoras de gestión de registros y seguridad de InSight para localizar errores o infracciones de los procedimientos de gestión de cambio y aislar la causa raíz de los problemas para proceder a su reparación y resolución.
  - Análisis forense 15%

    Las funciones de recopilación ubicua de registros, análisis forense y gestión de InSight permiten almacenar, recuperar e investigar los registros en busca de comportamientos de los usuarios en cualquier servidor, aplicación, base de datos o dispositivo.
  - Gestión e informes de conformidad 25%

    InSight automatiza la gestión de los registros permitiendo la recopilación universal, almacenamiento, recuperación e investigación de los datos de registro de seguridad y, a continuación, formatea y procesa automáticamente los registros para crear informes sobre conformidad e investigación. Los módulos de normativas específicas, como SOX, HIPAA, ISO y GLBA, ahorran incluso más tiempo al automatizar los informes.
  - Gestión de registros 40%

    InSight automatiza la gestión de los registros permitiendo la recopilación universal, almacenamiento, recuperación e investigación de los datos de registro de seguridad y, a continuación, formatea y procesa automáticamente los registros para crear informes sobre conformidad e investigación.
  - Personaliz., gestión y mant. herram. de seguridad 10%

    Con InSight no necesita crear sus propias herramientas para la gestión de registros y los informes de conformidad.
  - Evitar costes de sistemas de seguridad actuales 8%

    Con InSight no necesita crear sus propias herramientas para la gestión de registros y los informes de conformidad.

17

Caso de ROI

Número de empleados/Usuarios	1000
Facturación anual	100.000.000,00 €
Proyecto típico SIEM	30.000,00 €
Coste empresa DBA	60.000,00 €
Coste Emprresa Auidotría seguridad anual	30.000,00 €
Presupuesto empresa en seguridad (Anual) (10% del Presupuesto IT)	30.000,00 €
Presupuesto IT	300.000,00 €
Coste persona/Año/Tareas IT/Seguridad	50.000,00 €
Coste licencias software y desarrollos internos (33% del coste IT)	100.000,00 €
Fraude Potencial (0,05% de la facturación)	50.000,00 €

Caso de ROI . Coste del Software - 55K aprox.

Descripción	Qty
Servidor	1
Agentes para servidores centrales	4
Clientes	1000
Dispositivos de red	4
dispositivos de Seguridad IPS/FW	2
ISO27000/PCI/Basel II/SOX	1
Instancias de bases de datos	2

Estudio de ROI con parámetros tangibles

• Gestión de políticas	15%	9.000,00 €
InSight permite codificar reglas “w7” prácticas tipo “Quién puede hacer qué, Cuándo, Dónde, Desde dónde y Adónde” para que puedan supervisarse y aplicarse de forma automática políticas de uso aceptable y de gestión de cambios.		
• Gestión de intrusiones	5%	1.500,00 €
Los intrusos suelen ser a menudo usuarios de confianza y con autorización que tienen acceso a la red pero que aún resultan peligrosos. InSight rastrea, supervisa y alerta cuando usuarios de confianza entran en datos confidenciales y propietarios.		
• Reparación y resolución	5%	15.000,00 €
Clientes en todo el mundo utilizan las funciones investigadoras de gestión de registros y seguridad de InSight para localizar errores o infracciones de los procedimientos de gestión de cambio y aislar la causa raíz de los problemas para proceder a su reparación y resolución.		
• Análisis forense	15%	4.500,00 €
Las funciones de recopilación ubicua de registros, análisis forense y gestión de InSight permiten almacenar, recuperar e investigar los registros en busca de comportamientos de los usuarios en cualquier servidor, aplicación, base de datos o dispositivo.		
• Gestión e informes de conformidad	25%	15.000,00 €
InSight automatiza la gestión de los registros permitiendo la recopilación universal, almacenamiento, recuperación e investigación de los datos de registro de seguridad y, a continuación, formatea y procesa automáticamente los registros para crear informes sobre conformidad e investigación. Los módulos de normativas específicas, como SOX, HIPAA, ISO y GLBA, ahorran incluso más tiempo al automatizar los informes.		
• Gestión de registros de logs	40%	20.000,00 €
InSight automatiza la gestión de los registros permitiendo la recopilación universal, almacenamiento, recuperación e investigación de los datos de registro de seguridad y, a continuación, formatea y procesa automáticamente los registros para crear informes sobre conformidad e investigación.		
• Personaliz., gestión y mant. herram. de seguridad	10%	5.000,00 €
Con InSight no necesita crear sus propias herramientas para la gestión de registros y los informes de conformidad.		
		125.500,00 €

Soluciones para resolver los requerimientos PCI

The products outlined in this chart highlight IBM capabilities. Please call your local IBM executive for a full listing of all products and services that map to PCI requirements

IBM PROFESSIONAL SERVICES

11 TEST SECURITY SYSTEMS AND PROCESS

- IBM ISS Products & Services
- Tivoli Security Compliance Manager
- IBM Proventia Network Anomaly Detection System (ADS)
- IBM Global Services
- IBM Rational AppScan

12 SECURITY POLICY FOR EMPLOYEES & CONTRACTORS

- IBM Global Services
- Tivoli Console Insight Manager

IBM SOFTWARE SOLUTIONS

1 FIREWALL TO PROTECT CARDHOLDER DATA

- IBM Proventia Server Intrusion Prevention System (IPS)
- IBM Proventia Network (IPS)
- IBM Global Services

2 NO DEFAULT PASSWORDS OR SECURITY PARAMETERS

- IBM Tivoli Access Manager
- IBM Proventia Network Multi-Function Security
- (MFS) –IBM Global Services

10 MONITOR ACCESS

- IBM Tivoli Compliance Insight Manager
- IBM Tivoli Security Operations Manager
- IBM Proventia Server IPS
- IBM Global Services

3 PROTECT STORED CARDHOLDER DATA

- IBM Storage Manager
- IBM Proventia Server IPS
- IBM PKI Services
- IBM Global Services
- IBM System z Encryption Solutions
- IBM IMS and DB2 Encryption Tool

9 RESTRICT PHYSICAL ACCESS

- IBM Digital Video Surveillance
- IBM Biometric Access Control
- IBM Global Services

SECURE & PROTECT CARDHOLDER DATA

8 UNIQUE IDs

- IBM Tivoli Identity Manager
- IBM Tivoli Federated Identity Manager
- IBM Global Services

4 ENCRYPT TRANSMISSION

- IBM Data Encryption of IMS and DB2
- IBM System z network encryption
- DataPower XML Security Gateway
- Proventia Network Intrusion Prevention System

6 SECURE SYSTEMS & APPLICATIONS

- IBM Software Development Platform
- IBM Tivoli CCMBD
- IBM Global Services
- IBM Rational AppScan
- IBM Systems and Storage

7 RESTRICT ACCESS

- IBM Tivoli Access Manager
- IBM Tivoli zSecure Admin
- IBM Tivoli Compliance Insight Manager
- IBM Global Services

IBM MANAGED SERVICES

5 USE & UPDATE ANTI-VIRUS SOFTWARE

- IBM Proventia Desktop Endpoint Security
- IBM Proventia Network Enterprise Scanner
- IBM Global Services

IBM HARDWARE

Gracias