INFOTECH

IBM

Guardium®

SAFEGUARDING DATABASES™

Protección y Monitoreo de Bases de Datos en tiempo Real

Ing. Pablo Garula

pablo.garula@infotech.com.uy

Information Management Software

Agenda

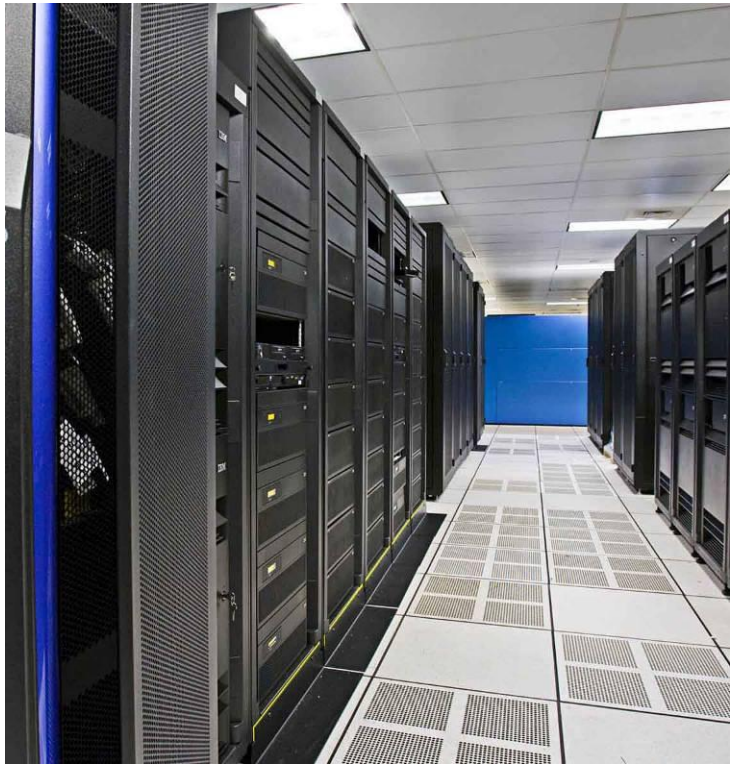
- Introducción
- Tipos de Amenazas
- Las herramientas de auditoria tradicionales
- IBM InfoSphere Guardium
- Ejemplos Funcionales
- Casos de éxito
- Conclusiones

Agenda

- **INTRODUCCIÓN**
- Tipos de Amenazas
- Las herramientas de auditoria tradicionales
- IBM InfoSphere Guardium
- Ejemplos Funcionales
- Casos de éxito
- Conclusiones

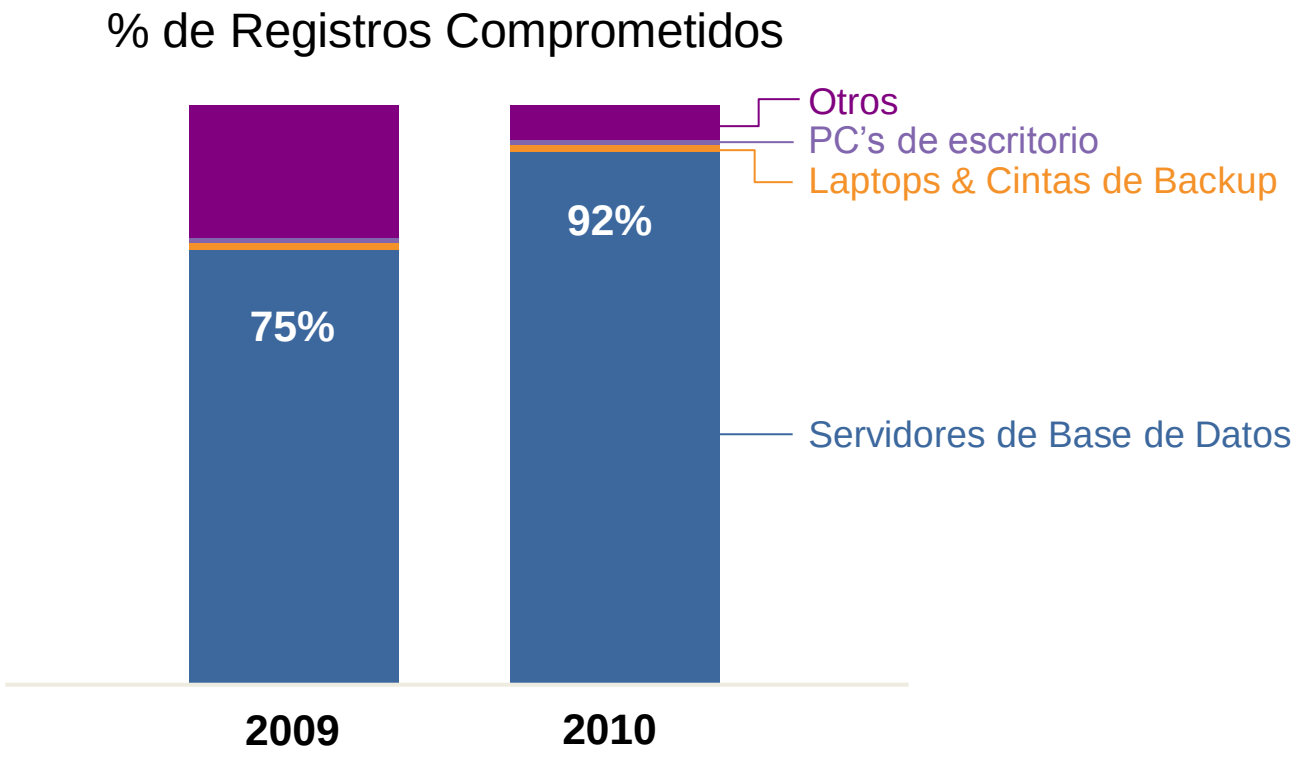
El contenido de las BDs es vital y confidencial

- Se almacenan:
  - Registros financieros
  - Números de tarjetas de crédito
  - Registros de pacientes
  - Información de Clientes
  - Etc.



- Grandes volúmenes de datos
- Contenido Estructurado, FÁCIL acceso a datos

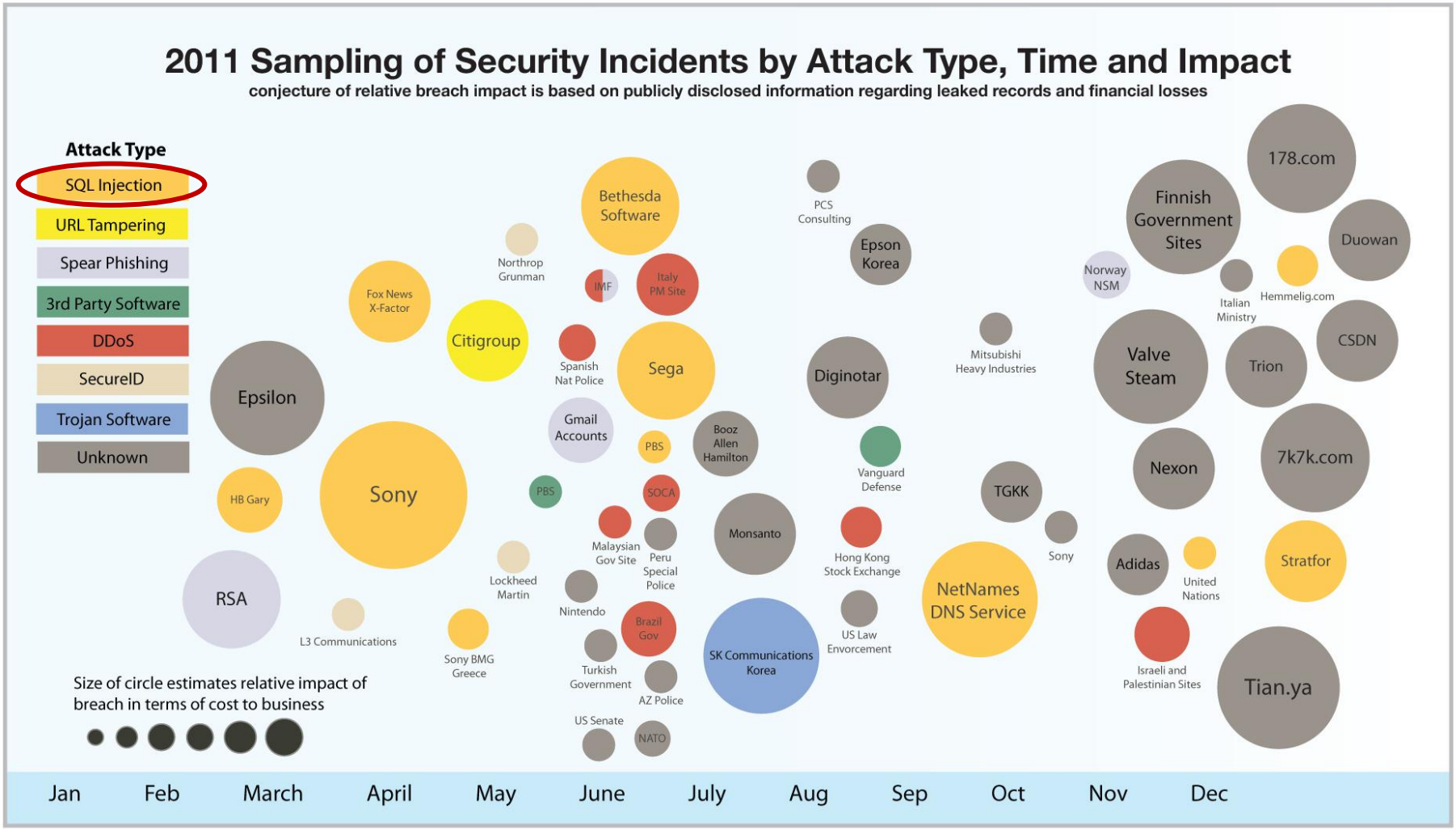
Los servidores de BD están en la mira



Sources: Verizon Business Data Breach Investigations Report 2009, 2010

Se hace mucho hincapié y se costea mas la seguridad en los dispositivos offline, en los dispositivos móviles y sistemas de usuario final cuando estos simplemente no son los puntos mas comprometidos

Ataques en el 2011



Fuente: IBM Security Systems **- IBM X-Force 2011 Trend and Risk Report**

www.ibm.com/security/xforce

2011: SQL Injection en 1er lugar

Event Name	2011 Rank	Trend	2010 Rank	Trend
SQL_Injection	1	Up	2	Down
HTTP_Suspicious_Unknown_Content	2	Down		
SQL_SSRP_Slammer_Worm	3	Slightly Down	1	Down
SNMP_Crack	4	Down		
HTTP_GET_DotDot_Data	5	Up		
Cross_Site_Scripting	6	Slightly Up		
SSH_Brute_Force	7	Slightly Up	4	Slightly Down
HTTP_Unix_Passwords	8	Up	6	Slightly Up
Shell_Command_Injection	9	Up		
Proxy_Bounce_Deep	10	Up		

Table 1: Top MSS high volume signatures and trend line—Year End 2011 vs Year End 2010

***Fuente: IBM Security Systems* - IBM X-Force 2011 Trend and Risk Report**

www.ibm.com/security/xforce

Las defensas perimetrales no son suficientes

- Sistemas distribuidos, varios puntos de ingreso a las bases de datos.
- Muchos sistemas y usuarios tienen acceso a los datos.
- Multas y sanciones por no cumplir con normativas SOX y PCI.

-- William J. Lynn III, U.S. Deputy Defense Secretary

Agenda

- Introducción
- ➢ **TIPOS DE AMENAZAS**
- Las herramientas de auditoria tradicionales
- IBM InfoSphere Guardium
- Ejemplos Funcionales
- Casos de éxito
- Conclusiones

Amenazas Externas

Robo de 130 Millones de Tarjetas de Crédito y Débito

Bank accounts News - *Last Updated Monday 17th August 2009*

FREE FINANCE G

US government charge man with theft of 130 million bank card details

Monday 17th August 2009

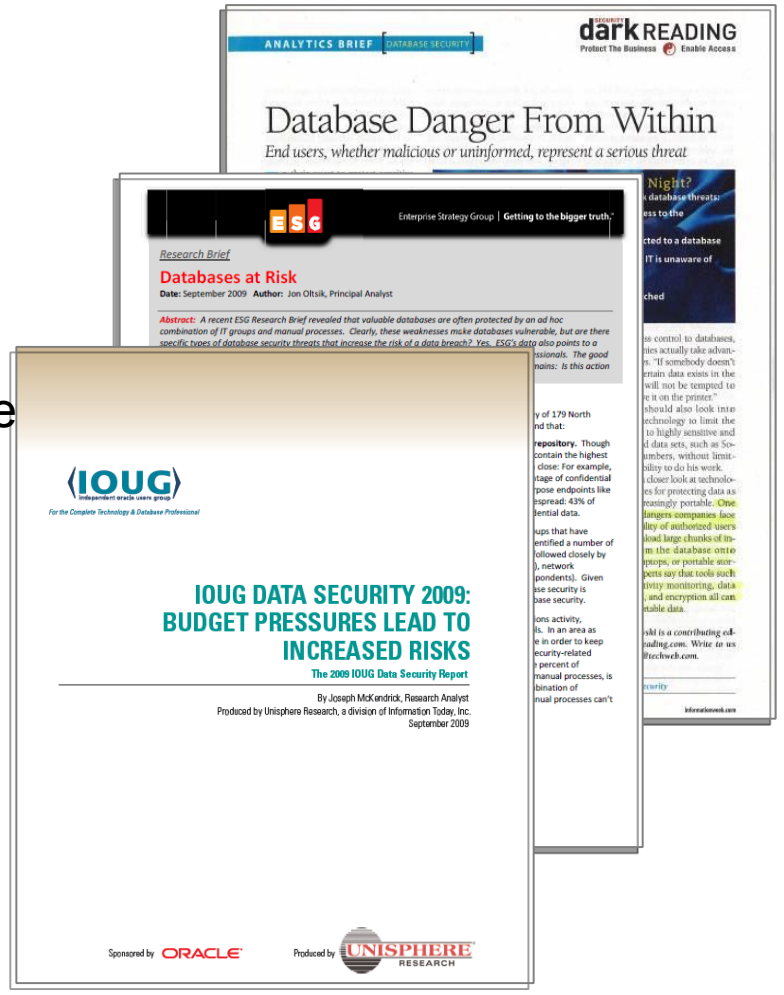
The US government has today charged an alleged fraudster with the theft of 130 million credit and debit card details. If proven in court this will be the largest identity theft ever reported in the US and one of the largest ever in the world. It is alleged that Albert Gonzales, together with two unnamed Russian co-conspirators, managed to hack in to the payment system of prominent US retailers and took copies of credit card and debit card data.

Using complex hacking techniques the alleged fraudsters managed to break down firewalls and gain access to the central information databank where all of the confidential and critical data was held. Albert Gonzales could be on the verge of a 20 year jail sentence and a $500,000 fine if he is convicted of the theft and potentially a further five years for conspiracy.

While many people may jump on the Internet bandwagon and accuse companies of lax security, the truth is that this particular type of fraud could have happened well before the Internet came to the fore. Information has been held on computer systems for years and ultimately while precautions are taken with regards to security, no one system can ever be 100% secure.

Amenazas Internas

- "Las organizaciones no ven el peligro inminente a sus bases de datos: usuarios autorizados." (Dark Reading)
- "Al parecer no existe un grupo único que sea dueño de la seguridad de la base de datos … 63% de las empresas depende de procesos manuales." (ESG)
- Muchas organizaciones (62%) no pueden prevenir que los Super Usuarios lean o modifiquen información sensible … la mayoría ni siquiera pueden detectar que esta ocurriendo … solo 1 de 4 cree que sus activos de datos están asegurados de forma segura (Independent Oracle User Group).



http://www.darkreading.com/database_security/security/app-security/showArticle.jhtml?articleID=220300753
ftp://ftp.software.ibm.com/software//data/sw-library/data-management/guardium/analyst-reports/esg_databases_at_risk.pdf
http://www.oracle.com/database/docs/ioug2009datasecurityreport.pdf

Guardium®

INFOTECH

¿ Quién monitorea a los super usuarios ?

SEARCH

Tech Center: Database Security

E-mail this page | Print this page | BOOKMARK

HSBC Database Breach Highlights Lack Of Accountability For IT Super Users

IT specialist had abused his database privileges to steal records of approximately 24,000 HSBC clients

Mar 25, 2010 | 01:55 PM

By Ericka Chickowski, Special To Dark Reading
DarkReading

As new details continue to emerge this month about an initially undetected large-scale database pilfering by a former IT worker at HSBC, security experts hope it will highlight one of the most glaring weaknesses in many a financial institution's database protection scheme: poor accountability for IT super users.

The breach was initially uncovered late last year, when former HSBC IT specialist Herve Falciani tried to sell the records of an unknown number of Swiss accounts held by French customers to officials in France charged with hunting down tax evaders. The French authorities eventually notified HSBC of a potential data breach and made a deal to rat out Falciani in return for more information on the HSBC clients in question. At the time, HSBC told its customer base that it believed the breach affected less than 10 clients.

Database Security Reports

Protecting Databases from Web Applications
Most external hacks of databases occur because of flaws in Web applications that link to those databases. Yet, enterprises are increasingly exposing their most valuable data to these outward-facing interfaces. In this Dark Reading Tech Center report, we'll discuss how security teams, database administrators and application developers can work together to improve the defenses of both front-end Web applications and back-end databases to prevent these attacks from succeeding, and offer a look at the most frequent Web-borne database attacks.

Database Activity Monitoring: Emerging Technology Keeps Tabs on Assets
You can read about the consequences of not protecting critical data in the daily headlines. In response, security-conscious organizations are tackling the complexities involved in effectively monitoring their databases for potential leaks and compromises. Fortunately, an emerging class of software is stepping up to help. Here's what enterprises need to know about selecting, deploying, and managing DAM technology.

SQL Injection: A Major Threat to Data Security
Of all the attacks taking place on Web sites across the Internet today, SQL injection is the most popular for cybercriminals trying to hack their way into corporate data stores. But for such a pervasive threat, there is still little understanding within the development and database communities about what constitutes a SQL injection vulnerability, how attacks against a SQL injection bug work, and how to mitigate the risk. We examine how these exploits work and what you can do to stop them.

Protecting Your Databases From Careless End Users
While much attention is paid to outside attackers' efforts to crack enterprise databases, IT organizations often overlook an even greater threat: end

Agenda

- Introducción
- Tipos de Amenazas
- **LAS HERRAMIENTAS DE AUDITORIA TRADICIONALES**
- IBM InfoSphere Guardium
- Ejemplos Funcionales
- Casos de éxito
- Conclusiones

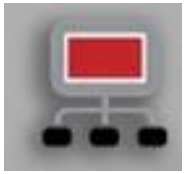
Herramientas “Tradicionales”

- Logeo Nativo
- Scripts hechos a mano (Pearl, C, Shell)
- Muchos Logs en disco

Crear Informe

Revisión Manual

Reparación y seguimiento Manual



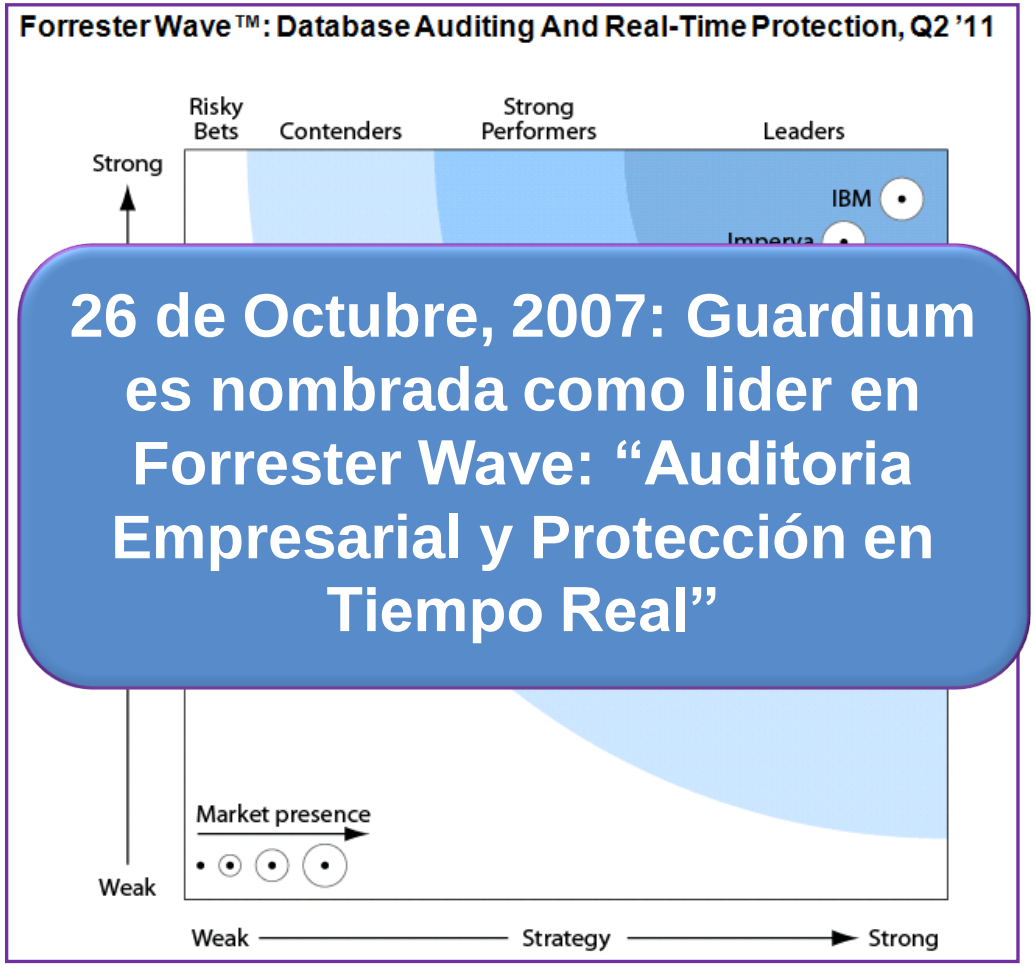
Contras del enfoque “Tradicional”

- Costoso, desarrollo a medida.
- Hay un impacto en la performance
- No es en tiempo real
- No hay separación de tareas, DBA’s
- No hay controles preventivos
- Costo de almacenamiento y manejo de logs ($$$)
- Complicado de mantener

Agenda

- Introducción
- Tipos de Amenazas
- Las herramientas de auditoria tradicionales
- **IBM INFOSPHERE GUARDIUM**
- Ejemplos Funcionales
- Casos de éxito
- Conclusiones

Guardium continua demostrando liderazgo



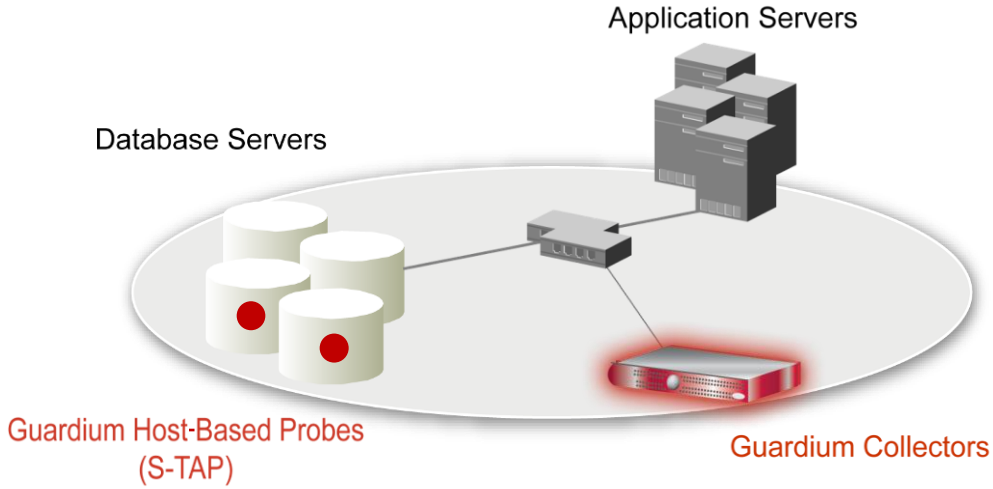
26 de Octubre, 2007: Guardium es nombrada como lider en Forrester Wave: "Auditoria Empresarial y Protección en Tiempo Real"

2007

Source: The Forrester Wave™: Database Auditing And Real-Time Protection, Q2 2011, May 6, 2011. The Forrester Wave is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

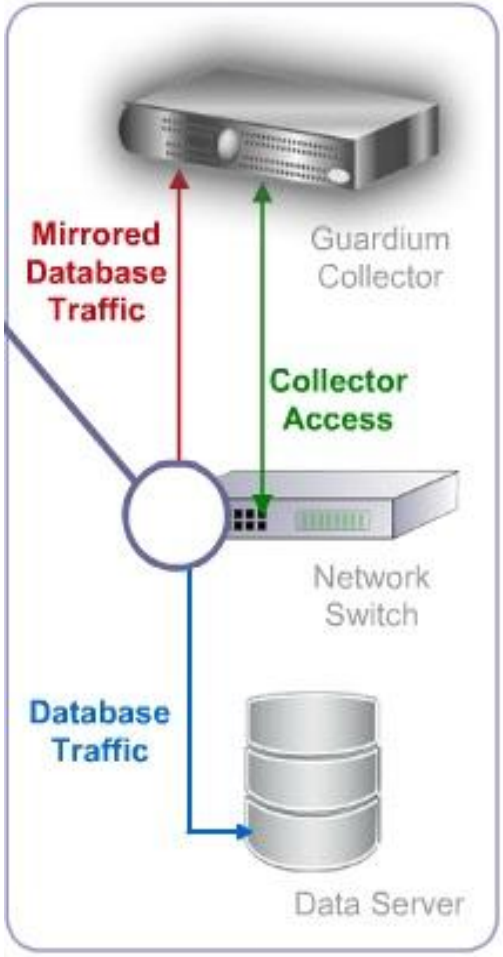
El enfoque IBM Guardium

Monitoreo y protección de Bases de Datos en tiempo real



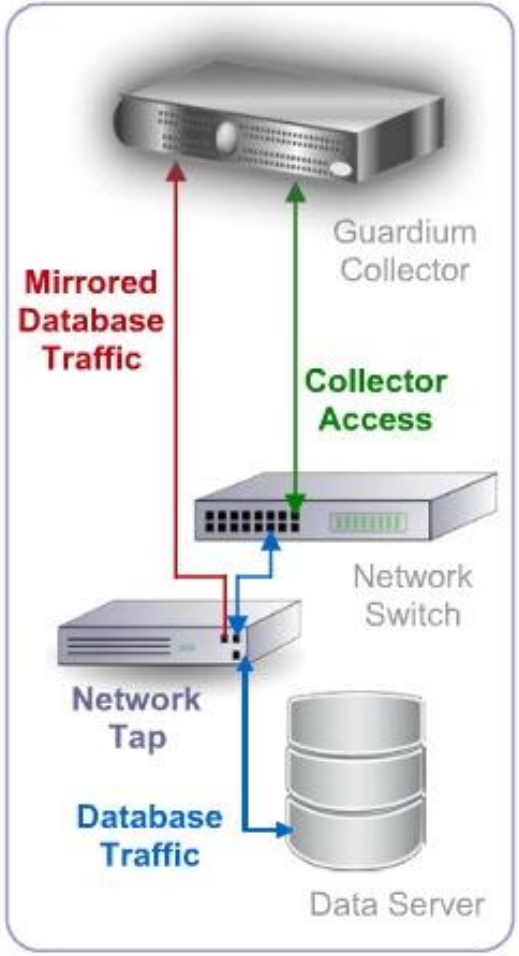
- Arquitectura no-invasiva
  - Fuera de la Base de Datos
  - Sin cambios a los DBMSs o aplicativos
  - Impacto mínimo en performance (2-4%)
- Solución multi-plataforma
- 100% visibilidad incluyendo accesos locales de DBAs
- No depende de los logs nativos del DBMS que pueden ser borrados por atacantes o gente interna
- Cumplimiento de políticas y auditoría en tiempo real
  - *Quién, dónde, cuándo, cómo*
- Reportes automatizados de cumplimiento de normativas (SOX, PCI-DSS, NIST, etc.)

Opciones de monitoreo



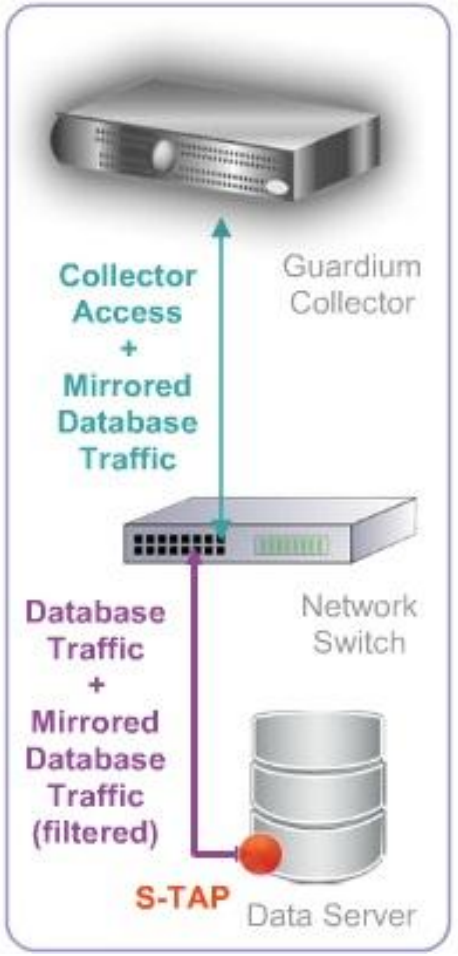
Port Mirroring

Acceso por red



Network Tap

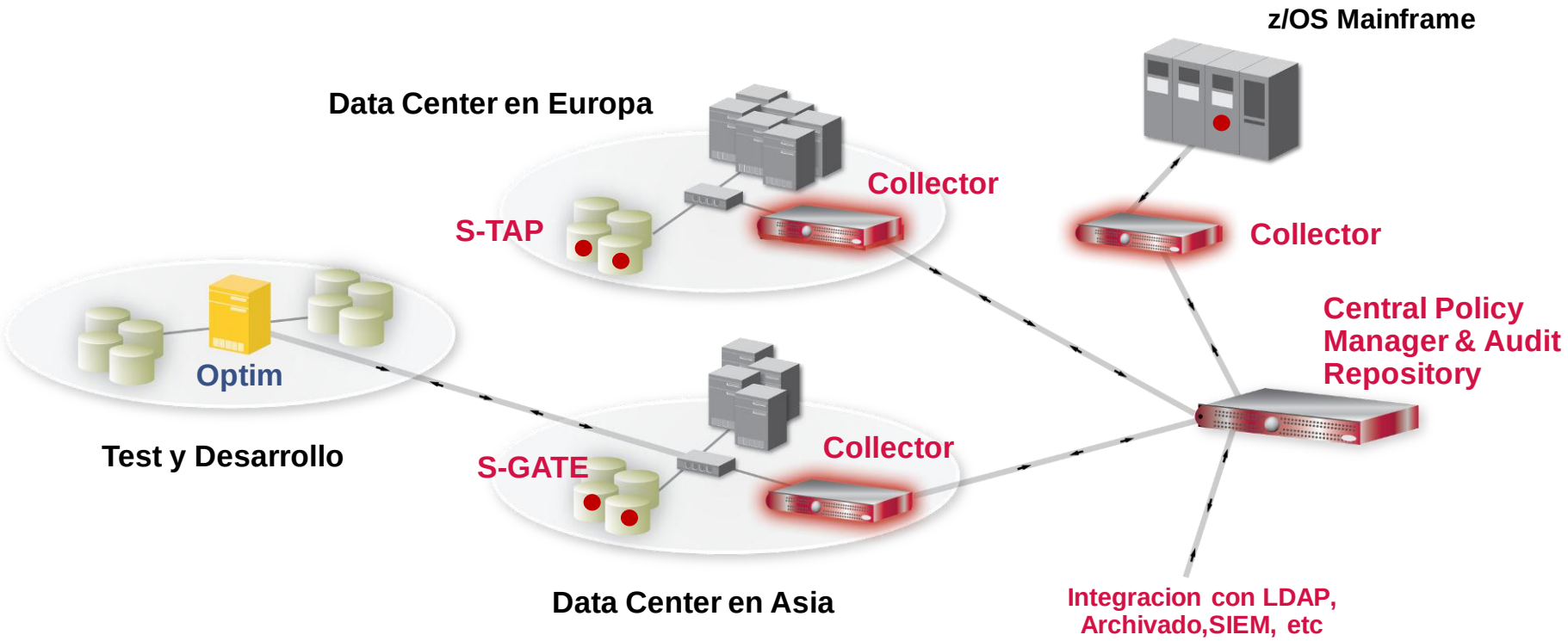
Acceso por red



Software Tap (S-TAP)

Acceso por red, local o conexión encriptada

Arquitectura escalable



Arquitectura Modular:

- S-TAP
- SPAN port or hardware tap
- S-GATE
- Collector
- Central Policy Manager

Se conecta a un puerto SPAN en un switch para capturar una copia de todo el tráfico de red o se usa un network tap.

Módulos de IBM Guardium

- Prevenir ataques
- Monitorear y bloquear usuarios privilegiados
- Detectar fraude
- Cumplir con controles de cambios
- Alertas en tiempo Real
- Integración SIEM

- Automatizar & centralizar los controles
- Políticas/ Informes preconfigurados
- Sin Cambios en la base
- Impacto mínimo de performance
- Reportes a medida
- Cumplimiento de normativas

- Buscar y clasificar datos Sensitivos
- Continuamente hace un update de las políticas de seguridad
- Descubre bombas lógicas y malware embebido
- Busca DBMS en toda la red

- Evalúa las vulnerabilidades de las bases de datos y comportamiento
- Tests preconfigurados Basados en mejores practicas y estándares (STIG, CIS)

Monitorea continuamente accesos a BDs

- **Prevenir fugas de información**
  - Mitigando amenazas internas y externas

- **Asegurar el control de los datos**
  - Previniendo accesos no autorizados a datos sensibles por parte de usuarios privilegiados
- **Reducir costos para cumplir con las regulaciones**
  - Simplificando procesos de auditoría
  - Tiene impacto mínimo de performance
  - No requiere cambios en los manejadores de BDs.
  - Automatizando & centralizando controles
    - En todas las plataformas de DBMS & aplicaciones
    - Para todas las regulaciones SOX, PCI-DSS, ISO 27002, …

Ayuda a cumplir Regulaciones

Audit Requirements	COBIT (SOX)	PCI-DSS	ISO 27002	Data Privacy & Protection Laws	NIST SP 800-53 (FISMA)
1. Access to Sensitive Data (Successful/Failed SELECTs)		✓	✓	✓	✓
2. Schema Changes (DDL) (Create/Drop/Alter Tables, etc.)	✓	✓	✓	✓	✓
3. Data Changes (DML) (Insert, Update, Delete)	✓		✓		
4. Security Exceptions (Failed logins, SQL errors, etc.)	✓	✓	✓	✓	✓
5. Accounts, Roles & Permissions (DCL) (GRANT, REVOKE)	✓	✓	✓	✓	✓

DDL = Data Definition Language
DML = Data Manipulation Language
DCL = Data Control Language

¿ Quienes son los interesados ?

OPERACION DE SEGURIDAD

- ✓ Políticas Tiempo Real
- ✓ Rastro seguro de auditoria
- ✓ Bloqueo a información sensible
- ✓ Minería de datos & forense

CUMPLIMIENTO DE AUDITORIA

- ✓ Segregación de tareas
- ✓ Reportes Mejores Practicas
- ✓ Controles Automatizados

BASES DE DATOS Y APLICACIONES.

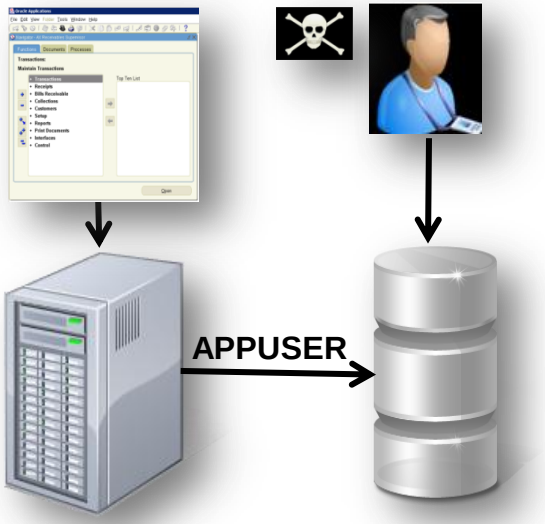
- ✓ Impacto Mínimo
- ✓ Administración de Cambios
- ✓ Seguridad
- ✓ Control de Configuración
- ✓ Patches que corrigen vulnerabilidades instalados

Guardium: 100% Visibilidad & Visión Unificada

Agenda

- Introducción
- Tipos de Amenazas
- Las herramientas de auditoria tradicionales
- IBM InfoSphere Guardium
- **EJEMPLOS FUNCIONALES**
- Casos de éxito
- Conclusiones

Reglas detalladas, Alertas en Tiempo Real

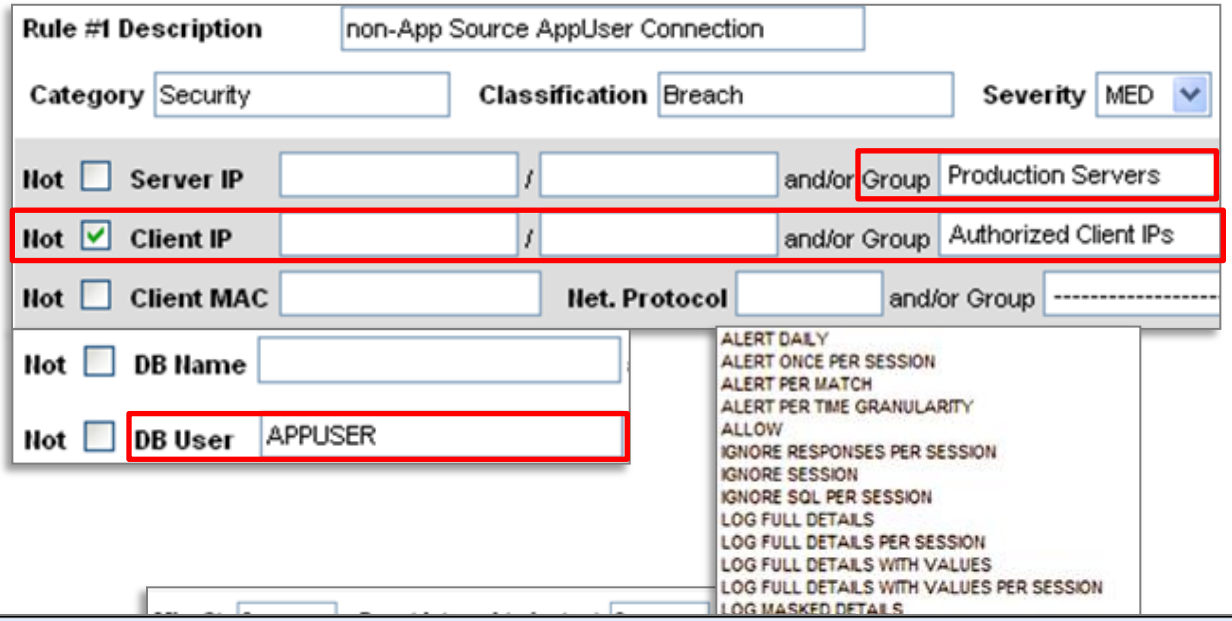


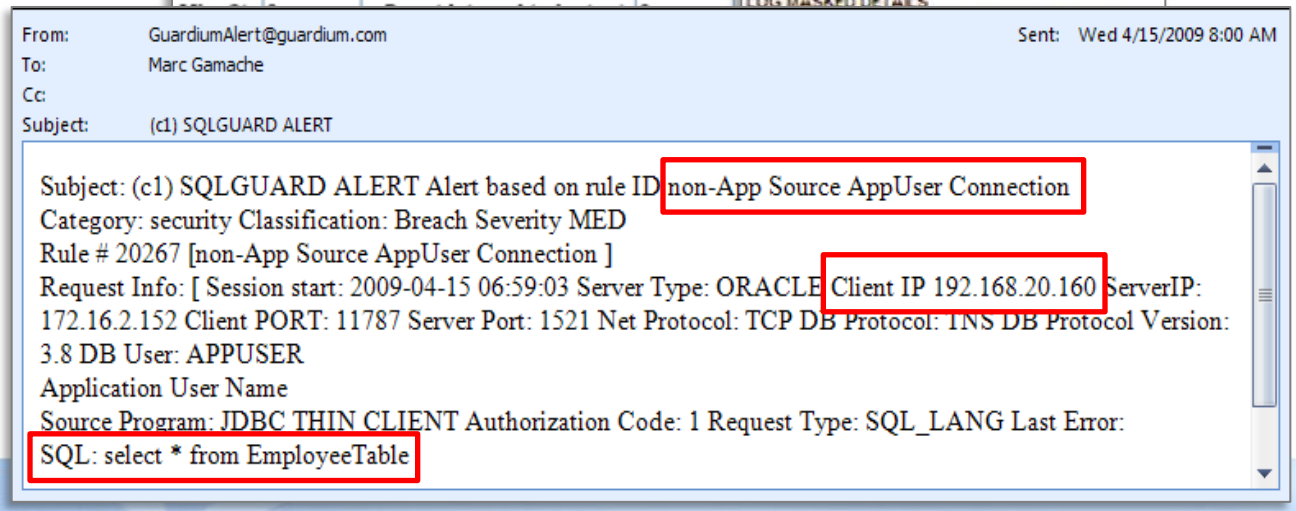
Application Server

10.10.9.244

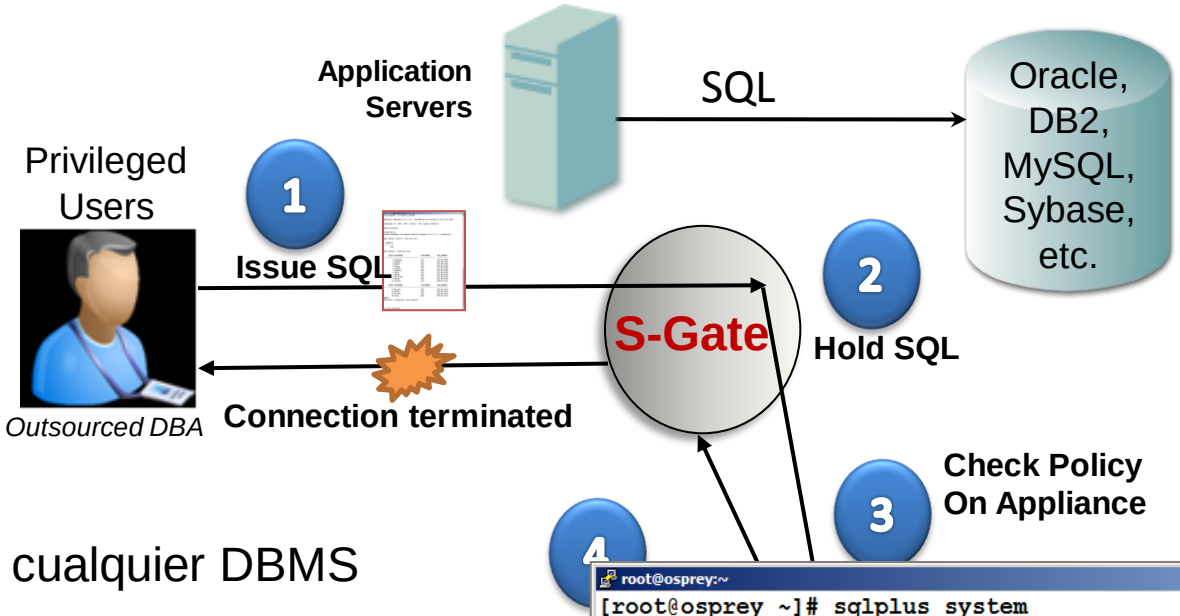
Database Server

10.10.9.56





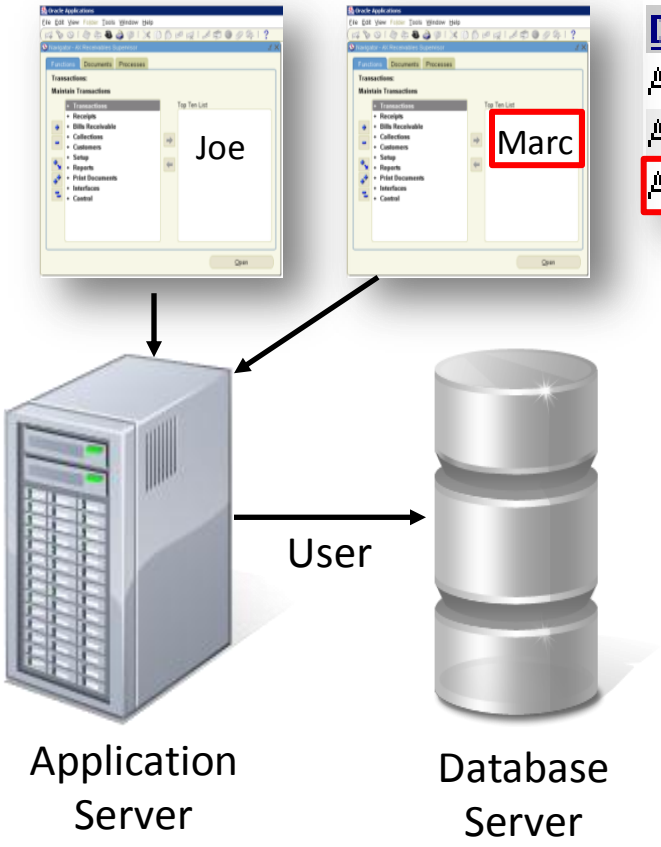
Bloqueo de Transacciones (S-GATE)



- Políticas para cualquier DBMS
- Bloquea acciones de usuarios privilegiados
- Sin cambios en la base de datos
- Sin cambios en los aplicativos
- No aumenta el trafico en la red

```
root@osprey:~
[root@osprey ~]# sqlplus system

SQL*Plus: Release 10.2.0.1.0 - Production on Tue May 27 01:13:32 20

Copyright (c) 1982, 2005, Oracle.  All rights reserved.

Enter password:

Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production

SQL> select * from creditcard;
select * from creditcard
*
ERROR at line 1:
ORA-03113 end-of-file on communication channel

                                                    Session Terminated
SQL>
```

Identificar Fraude al Nivel de la Aplicación



DB User Name	Application User	Sql
APPUSER	joe	select * from EmployeeRoleView where UserName=?
APPUSER	joe	select * from EmployeeTable
APPUSER	marc	insert into EmployeeTable values (?,?,?,?,?,?,?,?)

- ***Problema***: El servidor de aplicaciones utiliza un usuario genérico para accesar la base de datos
  - ***No identifica quién es el usuario*** que inició la transacción (pool de conexiones)

- ***Solución***: Guardium monitorea los accesos del ***usuario de la aplicación y lo asocia con los comandos específicos de SQL***
  - Soporte inmediato para Oracle EBS, PeopleSoft, SAP, Siebel, Business Objects, Cognos… y aplicaciones en (WebSphere, WebLogic, ….)
  - Deterministico vs. basado en timestamps “adivinar”
  - Sin cambios en las aplicaciones

Seguimiento a Usuarios que usan "su"

- **Problema:** Cómo dar seguimiento a usuarios que hacen “switch” entre cuentas (quizás para borrar su rastro)?
- El logging/auditoría nativa & las herramientas SIEM NO pueden capturar información del Sistema
- Otras soluciones de monitoreo de BD solo proveen la información de la cuenta shell que se utilizó

Actividad del usuario

```
login as: joe
joe@192.168.30.152's password:
Last login: Tue Apr 14 15:17:12 2009 from 192.168.20.160
[joe@u2 ~]$ su - oracle
Password:
-bash-3.00$ sqlplus system

SQL*Plus: Release 10.2.0.1.0 - Production on Tue Apr 14 15:17:39 2009

Copyright (c) 1982, 2005, Oracle.  All rights reserved.

Enter password:

Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production

SQL> insert into AppUser.EmployeeTable values (1001,6,'Joe','Smith','Salary','Bonus',500000,1);

1 row created.

SQL>
```

Que muestra Guardium

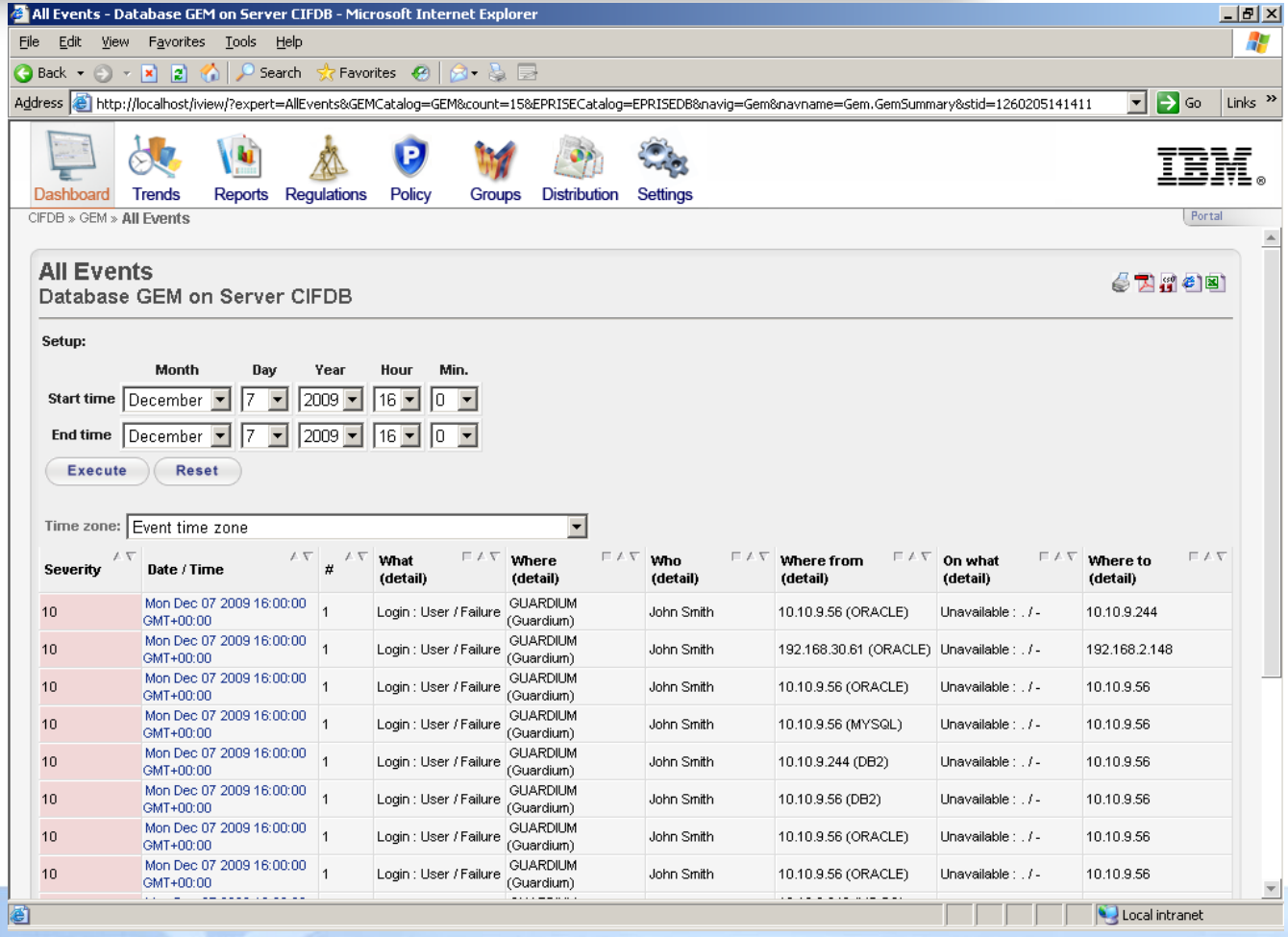
DB User Name	ShellAcct	OSUser	Sql
SYSTEM	ORACLE	joe	insert into AppUser.EmployeeTable values (?,?,?,?,?,?,?,?,?)

Integración con sistemas SIEM

Violación de una regla dentro de Guardium

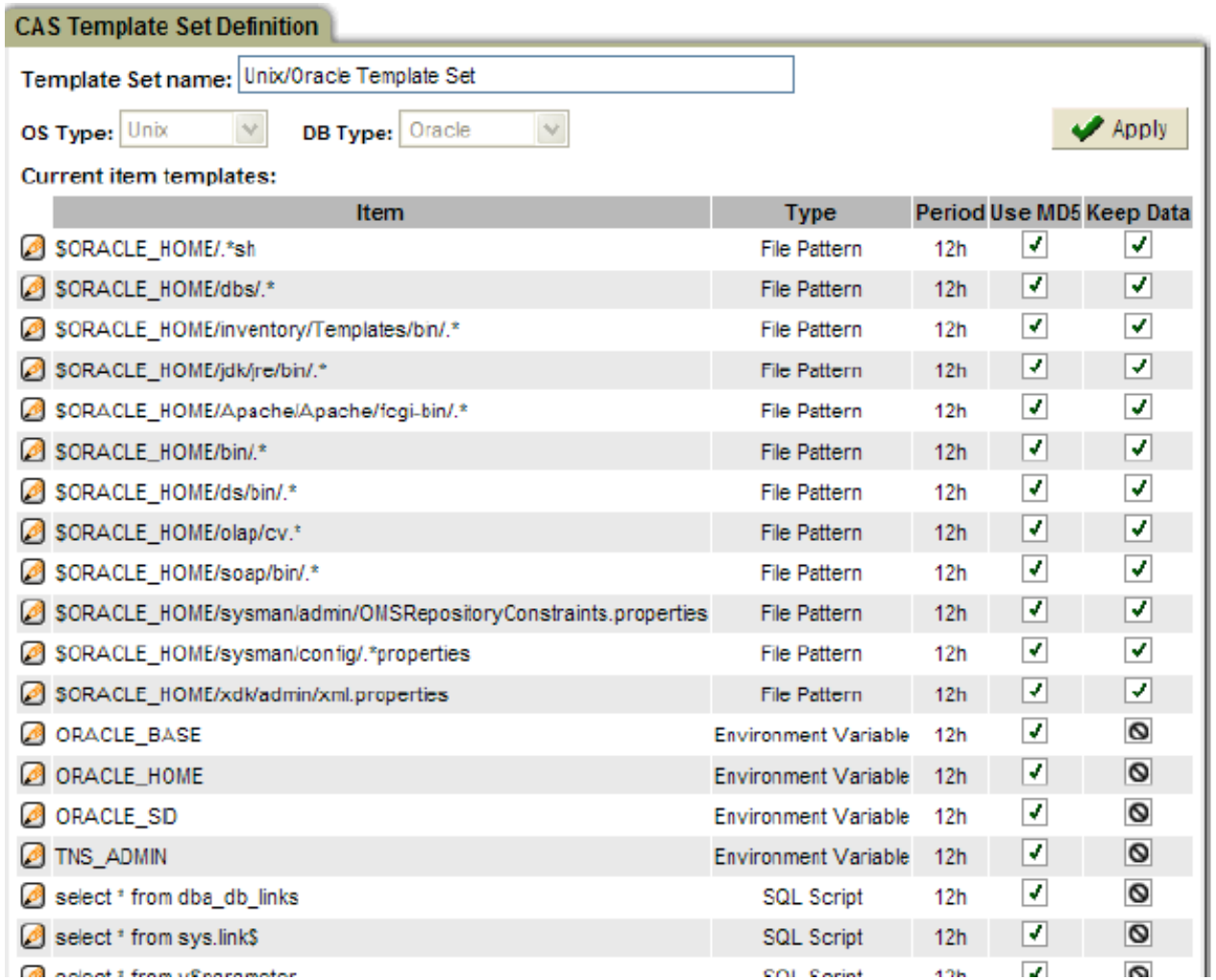
Category Name	Access Rule Description	Client IP	Server IP	DB User Name
security	Login Failures to Production Database Server	10.10.9.56	10.10.9.56	APPUSER

Eventos en un SIEM IBM



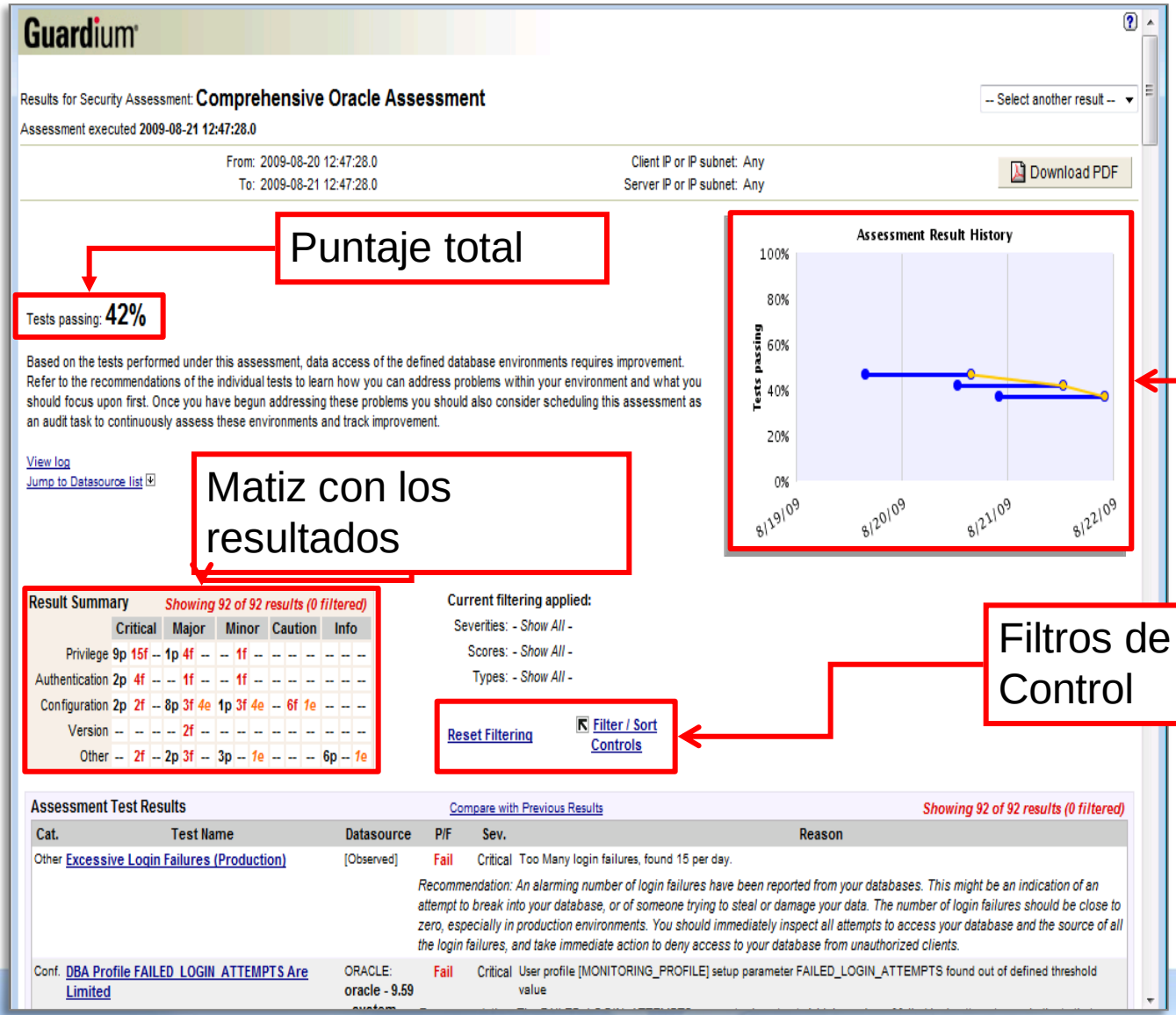
Auditar Cambios en Configuraciones de BD

- Detecta los cambios que hay en los archivos de configuración, variables de entorno, registro, scripts, etc, incluyendo cambios en los privilegios
- 200+ templates preconfigurados con mejores prácticas para los SO/DBMS más utilizados
  - Se pueden customizar via scripts, SQL, etc. (pruebas a la medida)

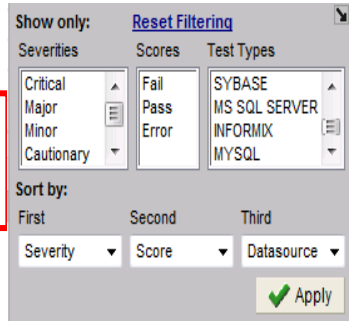


Item	Type	Period	Use MD5	Keep Data
$ORACLE_HOME/.*sh	File Pattern	12h	✓	✓
$ORACLE_HOME/dbs/.*	File Pattern	12h	✓	✓
$ORACLE_HOME/inventory/Templates/bin/.*	File Pattern	12h	✓	✓
$ORACLE_HOME/jdk/jre/bin/.*	File Pattern	12h	✓	✓
$ORACLE_HOME/Apache/Apache/fcgi-bin/.*	File Pattern	12h	✓	✓
$ORACLE_HOME/bin/.*	File Pattern	12h	✓	✓
$ORACLE_HOME/ds/bin/.*	File Pattern	12h	✓	✓
$ORACLE_HOME/olap/cv.*	File Pattern	12h	✓	✓
$ORACLE_HOME/soap/bin/.*	File Pattern	12h	✓	✓
$ORACLE_HOME/sysman/admin/OMSRepositoryConstraints.properties	File Pattern	12h	✓	✓
$ORACLE_HOME/sysman/config/.*properties	File Pattern	12h	✓	✓
$ORACLE_HOME/xdk/admin/xml.properties	File Pattern	12h	✓	✓
ORACLE_BASE	Environment Variable	12h	✓	⊘
ORACLE_HOME	Environment Variable	12h	✓	⊘
ORACLE_SD	Environment Variable	12h	✓	⊘
TNS_ADMIN	Environment Variable	12h	✓	⊘
select * from dba_db_links	SQL Script	12h	✓	⊘
select * from sys.link$	SQL Script	12h	✓	⊘

Análisis de vulnerabilidades usando estándares



Progreso Histórico de puntajes



Filtros de Control

Identificar uso inapropiado de los usuarios autorizados

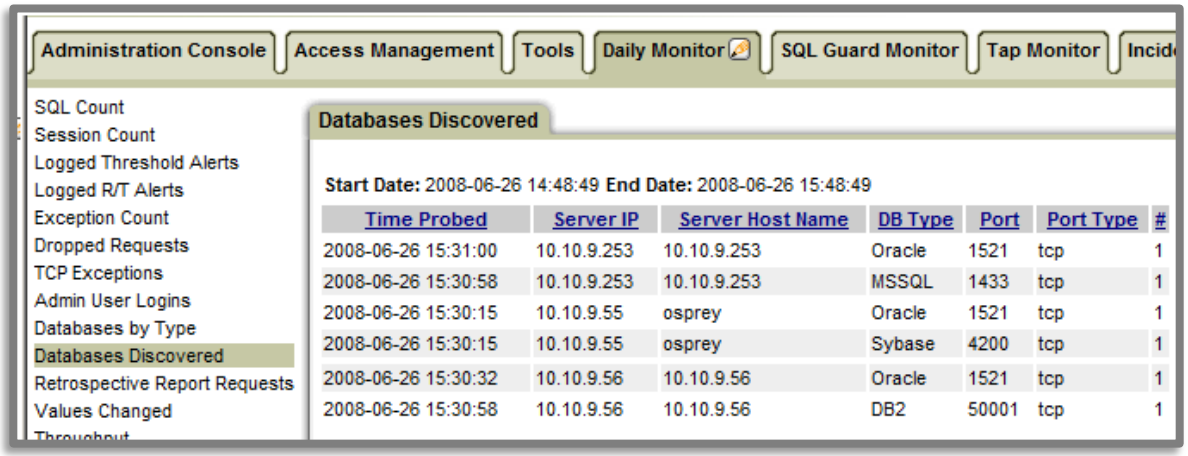
Esta bien que mi empleado vea 99 registros cuando el promedio por hora es 4?
Es normal ?

DB User Name	Sql	Records
STEVE	select * from ar.creditcard where i>? and i<?	4
HARRY	select * from ar.creditcard where i<?	4
JOE	select * from ar.creditcard where i<?	99

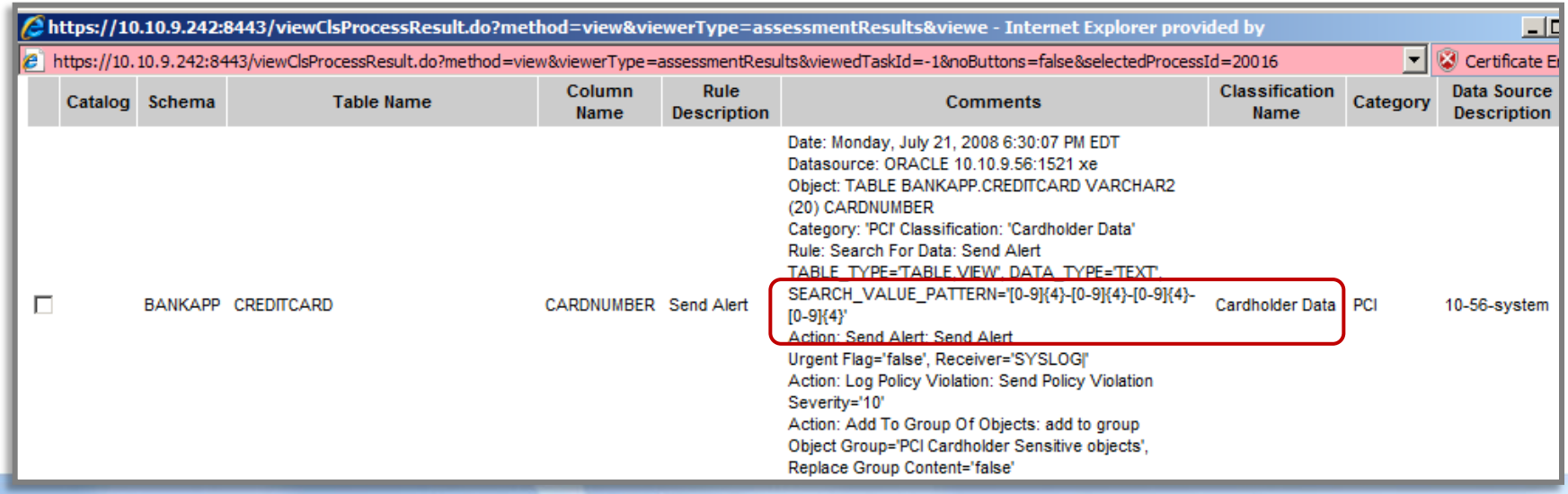
HARRY	select * from ar.creditcard where i<?	**********0002, **********0003, **********0004
JOE	select * from ar.creditcard where i<?	**********0001
JOE	select * from ar.creditcard where i<?	**********0002, **********0003, **********0004, **********0005, **********0006, **********0007, **********0008, **********0009, **********0010, **********0011, **********0012, **********0013, **********0014, **********0015, **********0016
JOE	select * from ar.creditcard where i<?	**********0017, **********0018, **********0019, **********0020, **********0021, **********0022, **********0023, **********0024, **********0025, **********0026, **********0027, **********0028, **********0029, **********0030, **********0031
JOE	select * from ar.creditcard where i<?	**********0032, **********0033, **********0034, **********0035, **********0036, **********0037, **********0038, **********0039, **********0040, **********0041, **********0042, **********0043, **********0044, **********0045, **********0046
JOE	select * from ar.creditcard where i<?	**********0047, **********0048, **********0049, **********0050, **********0051, **********0052, **********0053, **********0054, **********0055, **********0056, **********0057, **********0058, **********0059, **********0060, **********0061
JOE	select * from ar.creditcard where i<?	**********0062, **********0063, **********0064, **********0065, **********0066, **********0067, **********0068, **********0069, **********0070, **********0071, **********0072, **********0073, **********0074, **********0075, **********0076
JOE	select * from ar.creditcard where i<?	**********0077, **********0078, **********0079, **********0080, **********0081, **********0082, **********0083, **********0084, **********0085, **********0086, **********0087, **********0088, **********0089, **********0090, **********0091
JOE	select * from ar.creditcard where i<?	**********0092, **********0093, **********0094, **********0095, **********0096, **********0097, **********0098, **********0099

Que vio Joe?

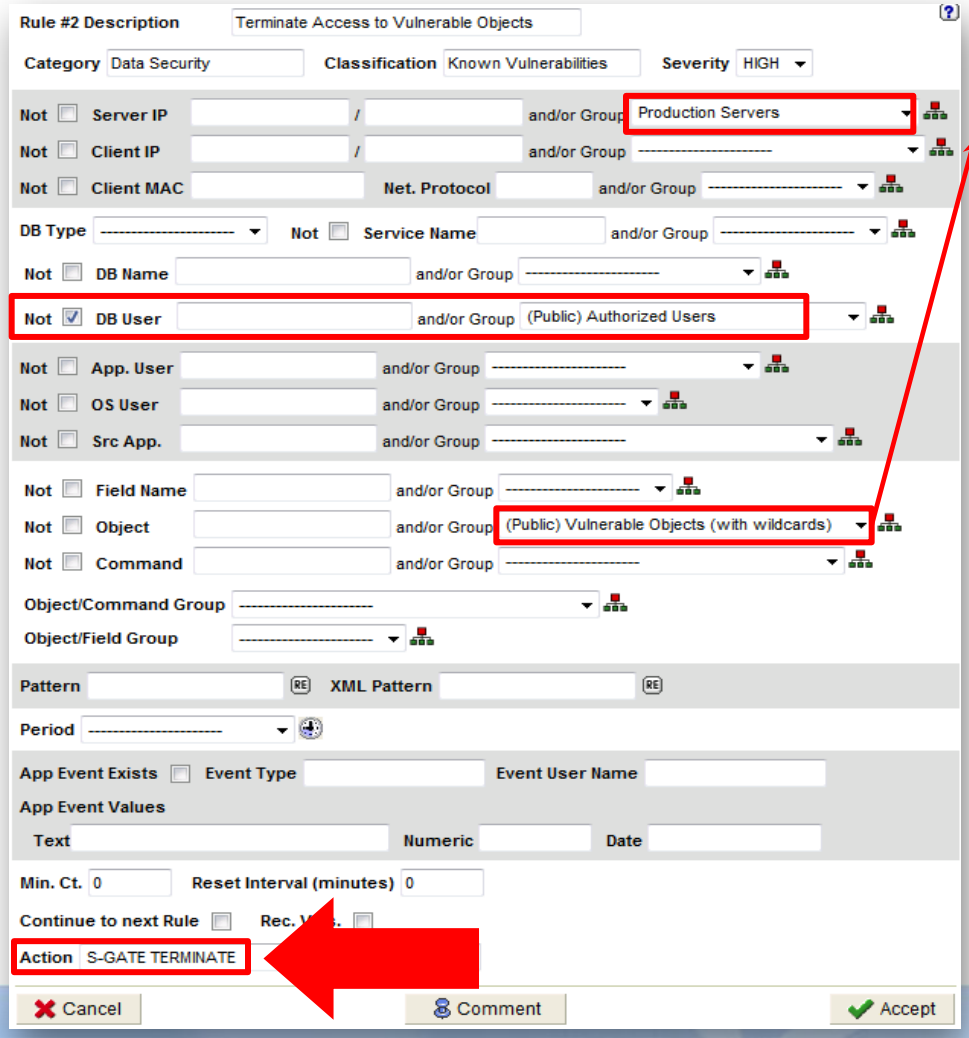
Encontrar bases de datos e identificar datos sensibles

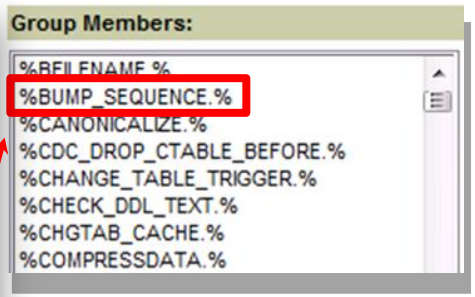


- Buscar por la red para encontrar instancias no catalogadas
- Buscar Información Sensible dentro de una base de datos
- Acciones basadas en reglas
  - Alertar
  - Agregar a un grupo de objetos sensibles



Protección de vulnerabilidades con parcheo virtual



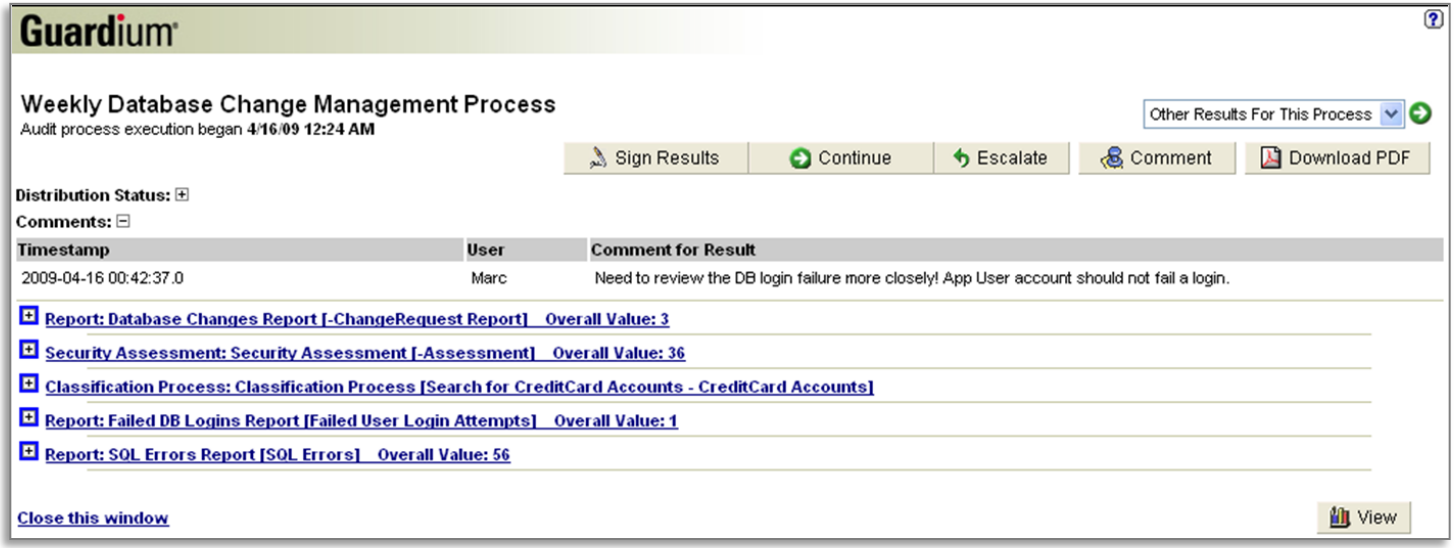


Procedimiento vulnerable que no se puede parchear de momento

Que ve el usuario

```
[root@ora-vm1 va-notes]# sqlplus joe

SQL*Plus: Release 10.2.0.1.0 - Production on Fri Aug 21 23:37:50 2009

Copyright (c) 1982, 2005, Oracle.  All rights reserved.

Enter password:

Connected to:
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Production
With the Partitioning, OLAP and Data Mining options

SQL> @bump_sequence.sql
DECLARE
*
ORA-03113: end-of-file on communication channel


ERROR:
ORA-03114: not connected to ORACLE


SQL>
```

Automatizar los informes de cumplimiento de regulaciones



- Automatiza el flujo de trabajo
  - Distribución de informes a diferentes equipos
  - Firma digital
  - Permite escalar, agregar comentarios & manejar excepciones
- Cumple con los requerimientos de los auditores
- Los resultados son almacenados en un repositorio central
- Agiliza y simplifica los procesos para el cumplimiento de requerimientos

Agenda

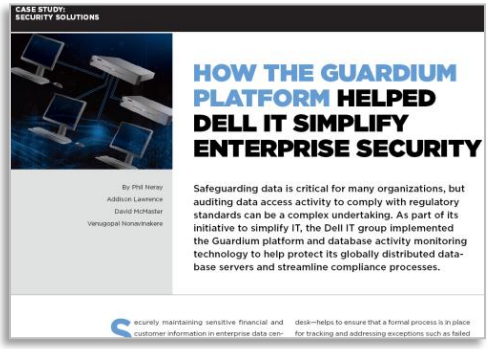
- Introducción
- Tipos de Amenazas
- Las herramientas de auditoria tradicionales
- IBM InfoSphere Guardium
- Ejemplos Funcionales
- **CASOS DE ÉXITO**
- Conclusiones

McAfee.com, cumplimiento de normativa PCI

- **Quien:** Empresa Global de Seguridad
- **Necesidad:** Proteger millones de transacciones PCI
  - Mantener los estrictos SLA's con clientes ISP (Comcast, COX, etc.)
  - Automatizar los controles PCI
- **Entorno:** Se implemento Guardium en menos de 48 horas
  - Muchos centros de cómputos; bases de datos en clusters
  - Integración con ArcSight SIEM
  - Expandirse luego para cubrir SAP así se cumple con SOX
- **Solución Anterior:** Repositorio central con la información auditada, logeo nativo en DBMS
  - Volúmenes de datos en cantidades enormes; performance & la confianza en los mismos.
  - Problemas con la separación de obligaciones/tareas (SOD)
- **Resultados:**

"McAfee necesitaba una solución que de forma continua y en tiempo real mantenga la visibilidad de los datos sensitivos de tarjetas de crédito - con el fin de detectar rápidamente cualquier actividad no autorizada y cumplir con PCI-DSS -dada nuestra gran cantidad de transacciones diarias , el rendimiento y confianza eran cruciales.

Dell, simplificar la seguridad empresarial


CASE STUDY:
SECURITY SOLUTIONS

HOW THE GUARDIUM PLATFORM HELPED DELL IT SIMPLIFY ENTERPRISE SECURITY

By Phil Neray
Addison Lawrence
David McMaster
Venugopal Nonavinakere

Safeguarding data is critical for many organizations, but auditing data access activity to comply with regulatory standards can be a complex undertaking. As part of its initiative to simplify IT, the Dell IT group implemented the Guardium platform and database activity monitoring technology to help protect its globally distributed database servers and streamline compliance processes.

Securely maintaining sensitive financial and customer information in enterprise data cen- desk—helps to ensure that a formal process is in place for tracking and addressing exceptions such as failed

Published case study in Dell Power Solutions

- **Quien:** Se conecta con mas de 5.4 millones de usuarios/día.
- **Necesidad:**
  - Mejorar la seguridad para cumplir con SOX, PCI & SAS70
  - Simplificar y automatizar los controles para cumplir con las normativas
- **Implementación de Guardium:**
  - Fase 1: Instalado en 300 servidores BD en 10 centros de cómputos (12 semanas)
  - Fase 2: Implementado adicionalmente en 725 servidores de bases de datos
- **Entorno:**
  - Oracle & SQL Server sobre Windows, Linux; Oracle RAC, SQL Server clusters
  - Oracle EBS, JDE, Hyperion
- **Solución Anterior :** Logeo nativo (MS y Oracle) con scripts (desarrollo)
  - Problemas de compatibilidad; mucho tiempo para los DBA; mucho volumen de datos; problemas con separación de tareas..
- **Resultados:** Informes automáticos; alertas en tiempo real; políticas centralizadas; Control de cambios

"Guardium cumplió con nuestros requisitos sin causar interrupciones en las bases de datos, produjo una reducción significante en los gastos generales de la auditoria de las BD."

Elegido por más de 500 organizaciones líderes a nivel mundial

5 de los 5
bancos top globales

2 de los 3
retailers top globales

5 de las 6
aseguradoras top
globales

El nombre mas
reconocido en PC's

4 de los 4 hospitales top
mundiales

Agencias mas
importantes de
gobierno

8 del las 10
telcos top globales

Agenda

- Introducción
- Tipos de Amenazas
- Las herramientas de auditoria tradicionales
- IBM InfoSphere Guardium
- Ejemplos Funcionales
- Casos de éxito

➢ **CONCLUSIONES**

Conclusiones

- Manejo de logs tradicionales, escaneo de redes y SIEM son insuficientes para asegurar el valor de las bases de datos

- Guardium es las solución más utilizada, en centros de datos a nivel mundial de gran demanda
  - Arquitectura escalable
  - Soporte múltiples plataformas
  - Control granular
  - Automatización para reducir la carga de trabajo

Visibilidad

Comprender los accesos a los datos
(quién, qué, cuándo, dónde, cómo)

Detección

Accesos no-autorizados en *tiempo-real*
(cambios en esquemas, errores, logins fallidos)

Prevención

Detener accesos no autorizados
(pasivo o en-linea)

MUCHAS GRACIAS !!!

E-Mail: pablo.garula@infotech.com.uy

Web Site: www.infotech.com.uy

Plataformas Soportadas de BD y S.O.

Supported Platform	Supported Versions
Oracle	8i, 9i, 10g (r1, r2), 10g RAC,11gR1, 11gR2, 11g RAC
Oracle (ASO, SSL)	9i, 10g (r1, r2), 11gR1, 11gR2
Microsoft SQL Server	MS SQL Cluster, 2000, 2005, 2005 x64, 2005 IA64, 2008, 2008 x64, 2008 IA64, 2008 R2 x64/x32/Cluster
Microsoft SharePoint	2007, 2010
IBM DB2 (Linux, Unix, Linux for System z)	9.1, 9.5, 9.7
IBM DB2 (Windows)	9.1, 9.5, 9.7
IBM DB2 Purescale	9.8
IBM DB2 for z/OS	8.1, 9.1, 10.1
IBM DB2 for iSeries	V5R2, V5R3, V5R4, V6R1
IMS	9, 10,11,12 (12 when available)
VSAM	see OS version support, part of z/OS (not separately versioned)
IBM Informix	7, 9, 10, 11, 11.50, 11.70
Sun MySQL and MySQL Cluster	4.1, 5.0, 5.1, 5.5
Sybase ASE	12, 15, 15.5
Sybase IQ	12.6, 12.7, 15
IBM Netezza	NPS 4.5, 4.6, 5,0, 6.0, 6.02
PostgreSQL	8, 9, 9.03, 9.04
Teradata	6.x, 12, 13, 13.10
FTP	
Window File Share (WFS)	Windows 2003, 2008

OS Type	Version	32-Bit & 64-Bit
AIX	5.2, 5.3	Both
	6.1, 7.1	64-Bit
z/OS	1.10, 1.11, 1.12	
HP-UX	11.11, 11.23, 11.31	Both
Red Hat Enterprise Linux	3, 4, 5,6	Both
Red Hat Enterprise Linux for System z	5.4	
SUSE Enterprise Linux	9, 10, 11	Both
SUSE Enterprise Linux for System z	9, 10, 11	
Solaris - SPARC	8, 9, 10, 11	Both
Solaris - Intel/AMD	10, 11	10-Both, 11-64-Bit only
Tru64	5.1A, 5.1B	64-Bit
Windows	2000, 2003, 2008	Both
iSeries	i5/OS*	

Aplicaciones y Aplication Servers Soportados

Supported Enterprise Applications
Oracle E-Business Suite
PeopleSoft
Siebel
SAP
Cognos
Business Objects Web Intelligence
+ Others based on customer demand

Supported Application Server Platforms (for other enterprise & custom developed applications)
IBM WebSphere
BEA WebLogic
Oracle Application Server (AS)
JBoss Enterprise Application Platform
+ Others based on customer demand