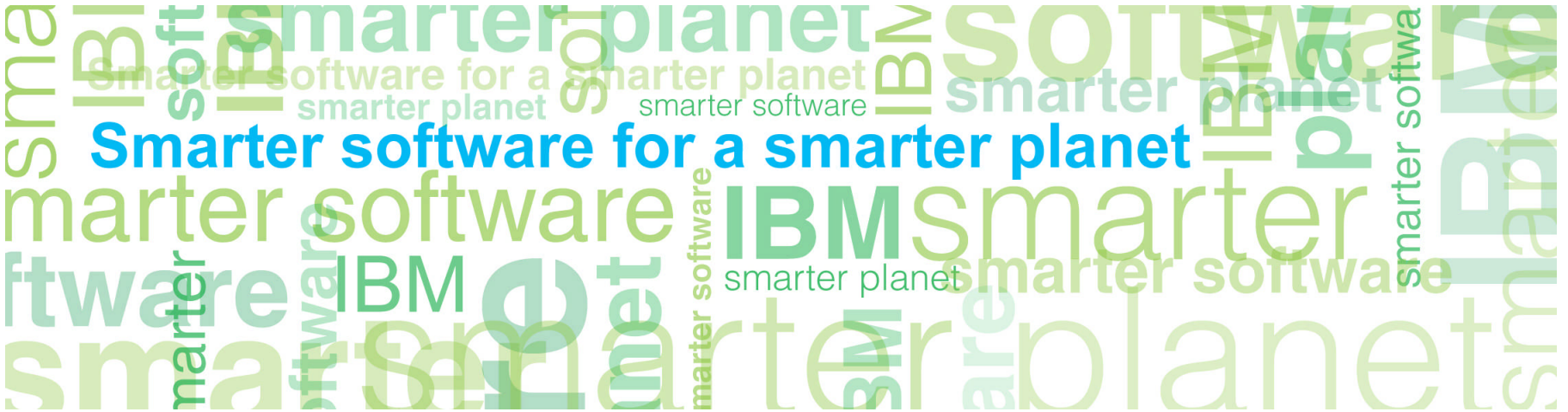
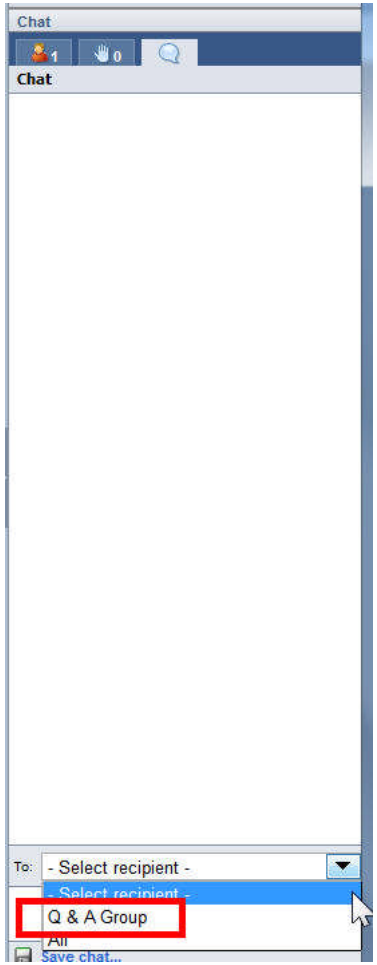
InfoSphere® Guardium® and SAP Tech Talk

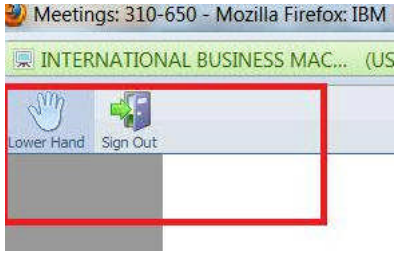


Joe_DiPietro@us.ibm.com

Logistics

- This tech talk is being recorded. If you object, please hang up and leave the webcast now.
- We'll post a copy of slides and link to recording on the Guardium community tech talk wiki page: http://ibm.co/Wh9x0o
- You can listen to the tech talk using audiocast and ask questions in the chat to the Q and A group.
- We'll try to answer questions in the chat or address them at speaker's discretion.
  - If we cannot answer your question, please do include your email so we can get back to you.
- When speaker pauses for questions:
  - We'll go through existing questions in the chat





© 2013 IBM Corporation

Reminder: Guardium Tech Talks

Next tech talk: How to audit and protect SAP systems with InfoSphere Guardium Data Activity Monitor

Speakers: Peter Mandel and Ernie Mancill

Date &Time: Thursday, October 17, 2013

11:30 AM Eastern (75 minutes)

Register here: **http://bit.ly/156DCVX**

- Link to more information about this and upcoming tech talks can be found on the InfoSpere Guardium developerWorks community: http://ibm.co/Wh9x0o
- Please submit a comment on this page for ideas for tech talk topics.

© 2013 IBM Corporation

Agenda

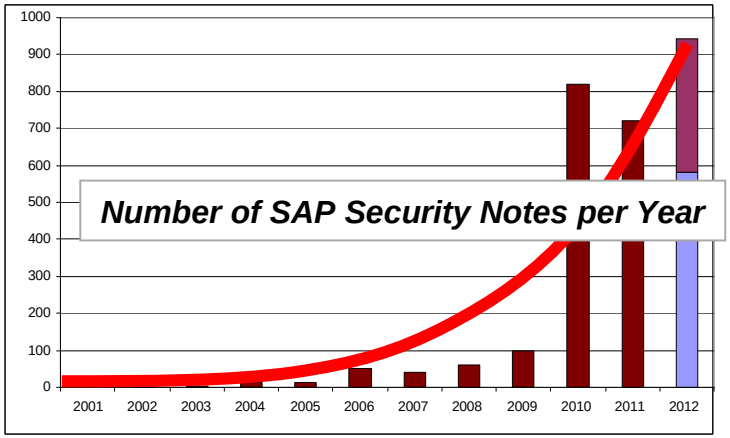
- SAP threat background
- Guardium auditing options
- Reports

© 2013 IBM Corporation

SAP – A Rising Threat

The number of SAP Security Notes has increased drastically over the last years.

- Security Notes usually address one or more vulnerabilities.
- Most of these issues affect the Business Runtime.



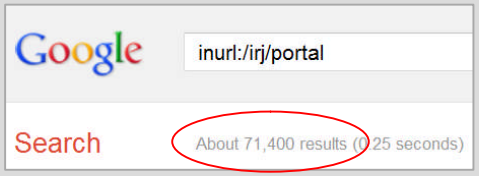
SAP Security Notes - By Oct 22, 2012, a total of 2432 notes
Source: https://service.sap-ag.de/securitynotes

MYTH: SAP systems attacks available only for insiders

Data about SAP systems can be collected in the WEB
- Various stats by countries, applications, versions
- Information from Google, Shodan, Nmap scan, etc

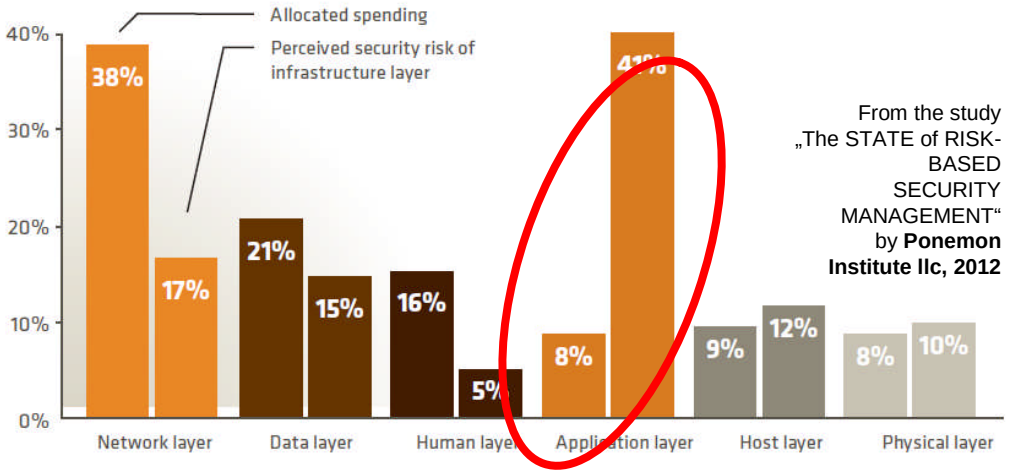
An increasing number of SAP systems are exposed to the internet, including Dispatcher, Message server, SapHostcontrol, Web Services, Solution Manager, etc

The different SAP components can be searched through different search items, such as:
- inurl:/irj/portal (Enterprise Portal)
- inurl:/sap/bc/bsp (SAP Web Application Server)
- inurl:/scripts/wgate (SAP ITS)
- inurl:infoviewapp (SAP Business Objects)



„Over 95% of the SAP systems we evaluated were exposed to espionage, sabotage and fraud cyber attacks“ (Onapsis, March 2012)

Gap between allocated spending and perceived security risk for the application layer



From the study „The STATE of RISK-BASED SECURITY MANAGEMENT“ by **Ponemon Institute llc, 2012**

© 2013 IBM Corporation

The SAP Security Challenge

The SAP and Enterprise Security Landscape

- **Corporate application landscapes continue to grow in complexity**
- **Global integration is rapidly increasing the number of interconnected systems**
- **SAP Systems and Application landscapes are no longer just traditional business applications**
- **SAP has increased function, platforms, reach, components, and business solutions to include Cloud, Database technology, Business Analytics, etc.**
- **SAP solutions support critical systems replete with proprietary and confidential Corporate data**
- **SAP systems are highly visible and valuable targets for disruption and malicious attacks**
- **Many SAP applications were designed for back-end operations but are now publically accessible**

Third Party Code Exposures

- **Many SAP Enterprises rely on custom ABAP applications**
- **Custom code means no one else has tested it**
- **ABAP development is frequently outsourced**

Compliance, Expertise, and Application Lifecycle Management

- Compliance demands for critical systems
- Security testing of SAP Java (NetWeaver) applications requires robust web application security expertise
- Manual Security testing of ABAP application code time consuming and requires SAP expertise
- Early detection during the Security and application lifecycle management

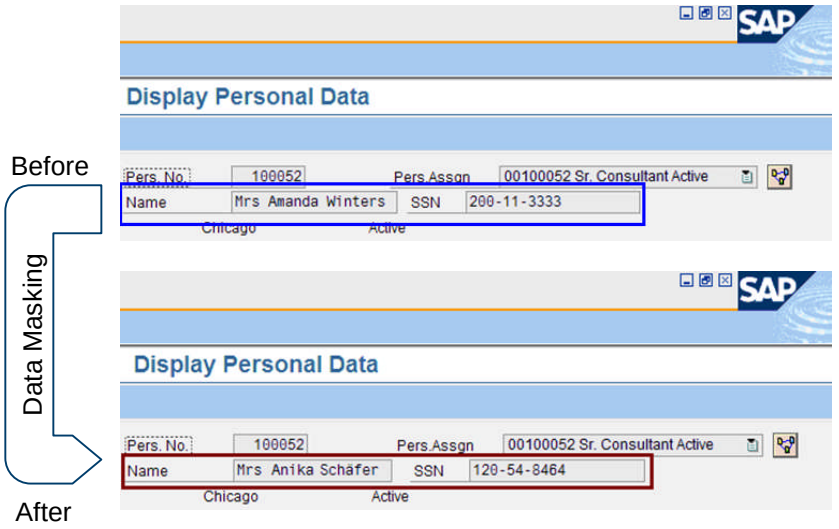
That all makes SAP more vulnerable, provides a larger attack surface.

© 2013 IBM Corporation

Data - Protect and monitor sensitive data in SAP

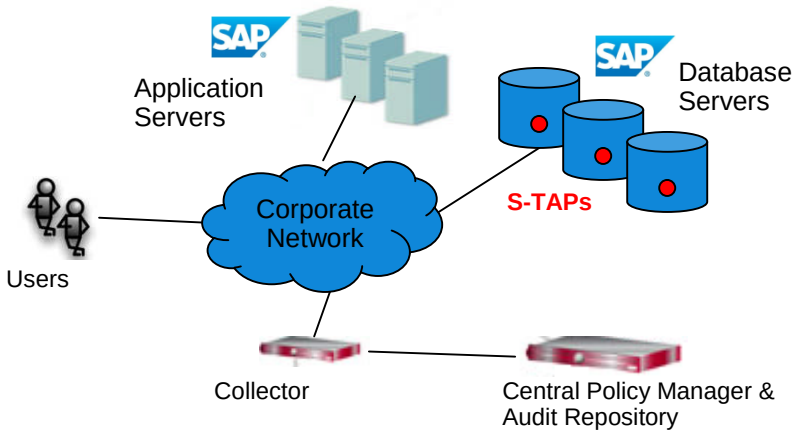
Integrate SAP with Enterprise Data Privacy with Optim Data Masking Solution for SAP

- Contextual, application-aware, persistent masking techniques to protect confidential data with predefined templates for masking the sensitive fields in SAP system
- Comprehensive capabilities to conceal sensitive data across non-production environments, while still providing realistic data for use in development, testing or training.



Managing security & compliance requirements for SAP systems IBM InfoSphere Guardium

- Safeguards financial and ERP information, customer and cardholder data
- Prevents unauthorized access from privileged and other users
- Monitors SAP enterprise application databases and provides compliance controls over the entire database infrastructure
- Integrates with SAP solutions to identify individual user from a pooled database connection

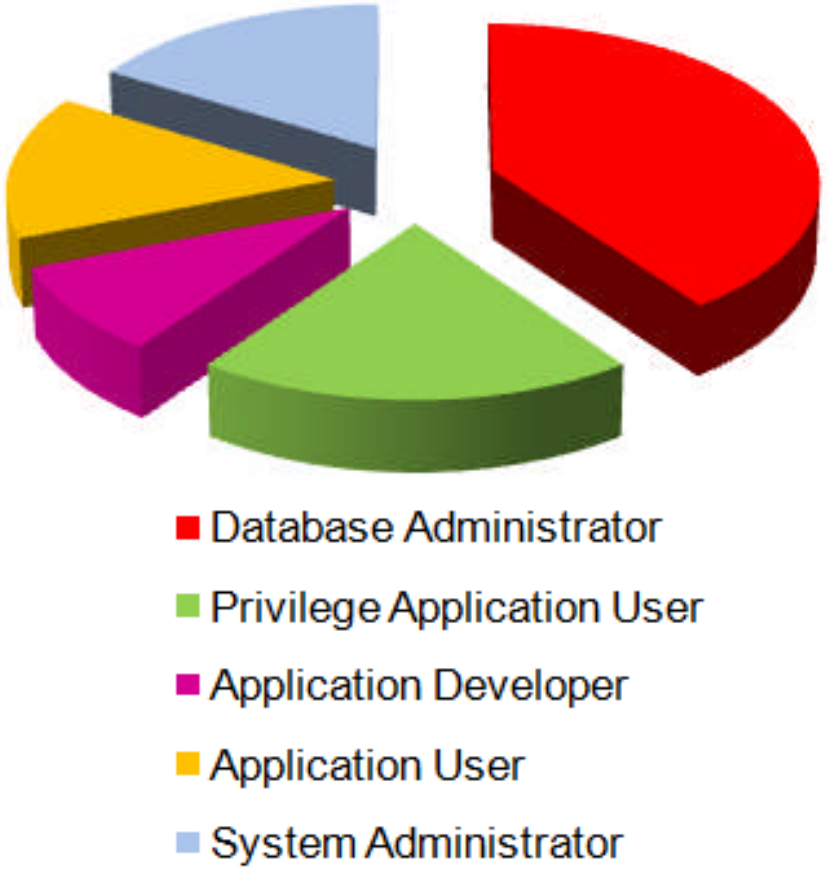


© 2013 IBM Corporation

3 Types of Security Controls Are Required For Applications

1. **Application security controls**
   - Separation of duties for Privilege Application User & Application User access
2. **Database security Controls**
   - Continuously monitor direct access to the database which will bypass the application controls
3. **System administrators security controls**
   - Operating System controls to monitor file access, copy, and modification

Risk By Type of User

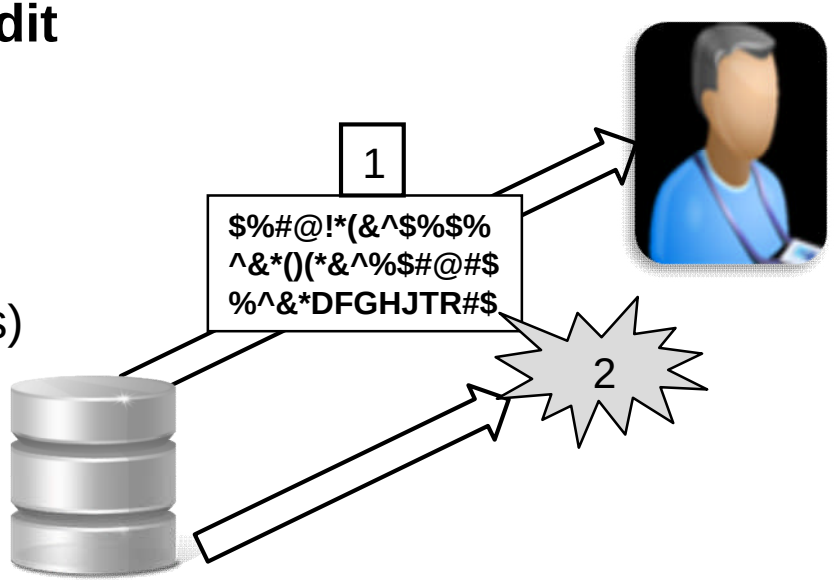


© 2013 IBM Corporation

More Operating System Controls (Deny, Encrypt, Audit, Permit)

- **WHO is attempting to access protected data?**
  - Configure groups, or applications who can access protected data
- **WHAT data is being accessed?**
  - Configure appropriate file and directory access
- **WHEN is the data being accessed?**
  - Configure a range of hours and days of the week for authorized access
- **HOW is the data being accessed?**
  - Configure allowable file system operations allowed to access the data e.g. read, write, delete, rename, application or process, etc.
- **EFFECT: Permit; Deny; Encrypt; Audit**

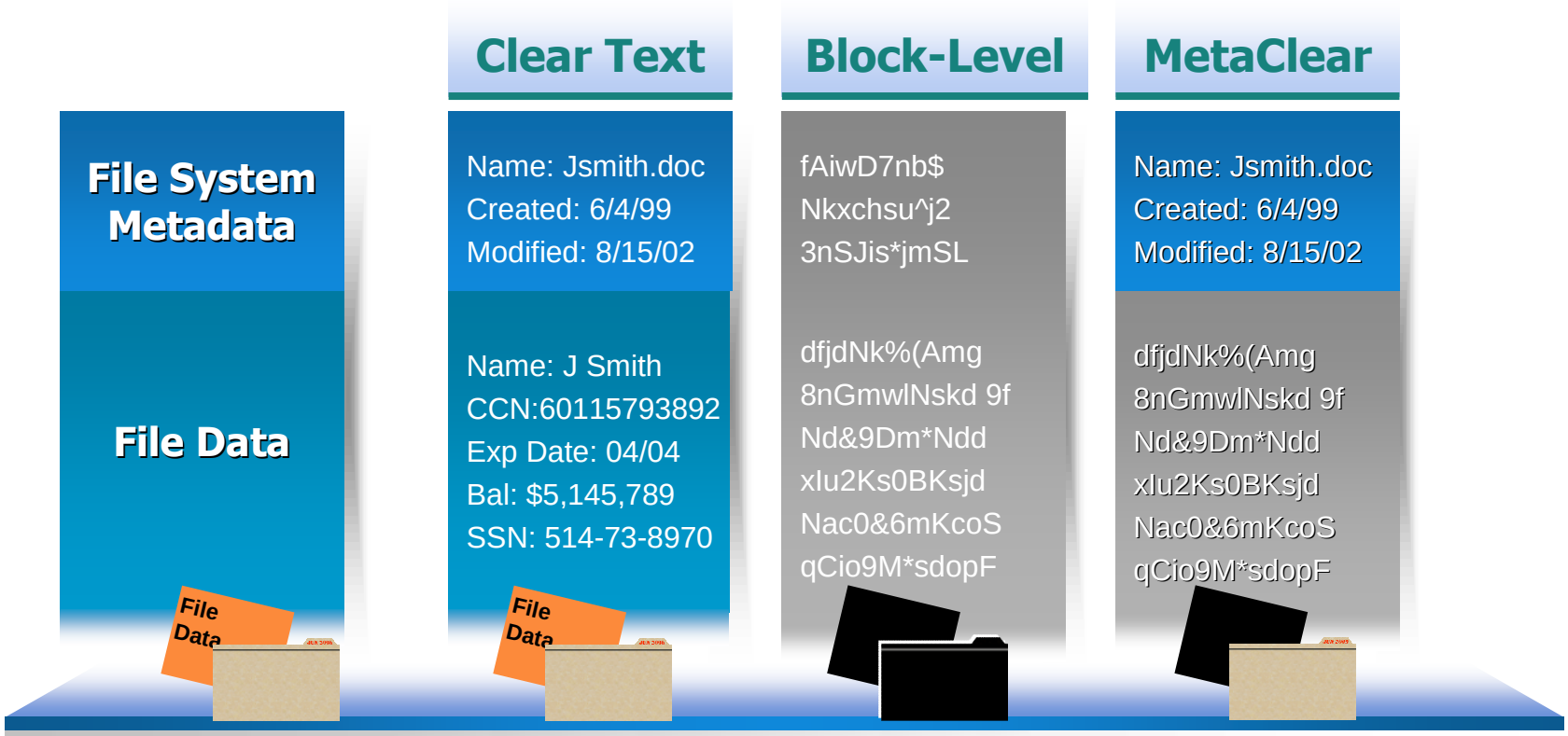
- **Root users can:**
  1. read directory (/SAPDirectory), but it will be encrypted and audited
  2. Blocked access to directory (/NoAccess)



- Database Administrator
- System Administrator

© 2013 IBM Corporation

Guardium Data Encryption Operating System Controls



- Protects Sensitive Information Without Disrupting Data Management
- High-Performance Encryption
- Root Access Control
- Data Access as an Intended Privilege

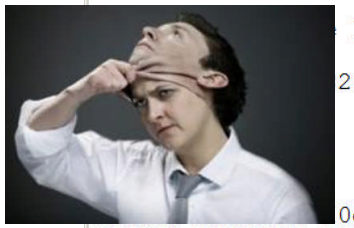
© 2013 IBM Corporation

Operating System Switch User "SU" To Gain Access

Start Date: **2010-03-07 20:53:45** End Date: **2010-03-12 17:53:45**

Timestamp	Client IP	Server IP	Network Protocol	Uid Chain Compressed	OS User	DB User Name	Source Program	Full Sql	Uid Chain
2010-03-11 20:47:40.0	10.10.9.56	10.10.9.56	BEQUEATH	joe	ORACLE	SYSTEM	SQLPLUS@OSPREY	select * from creditcard	(1,root,init [3])->(2267,root,/usr/sbin/sshd)->(20063,root,sshd: joe [priv])->(20065, joe,sshd: joe@pts/3)->(20066,joe,-bash)->(20142,joe,su - oracle)->(20149,oracle,-bash)->(20175, oracle,sqlplus)->(20182,oracle,oracleXE (DESCRIPTION=(LOCAL=YES)(ADDRESS= (PROTOCOL=beq))))

```
joe@osprey:~
Using username "joe".
joe@10.10.9.56's password:
Last login: Fri Sep 25 13:31:39 2009 from j
[joe@osprey ~]$ su - oracle
Password:
-bash-3.00$ sqlplus system

 10.2.0.1.0 - Production o

2, 2005, Oracle.  All righ

0g Express Edition Release 10.2.0.1.0 - Production

SQL> select * from creditcard;

NAME                                               CAR
-------------------------------------------------- ---
Joe D                                              123
Harry S                                            234

ess Edition
```



System Administrators have a lot of power

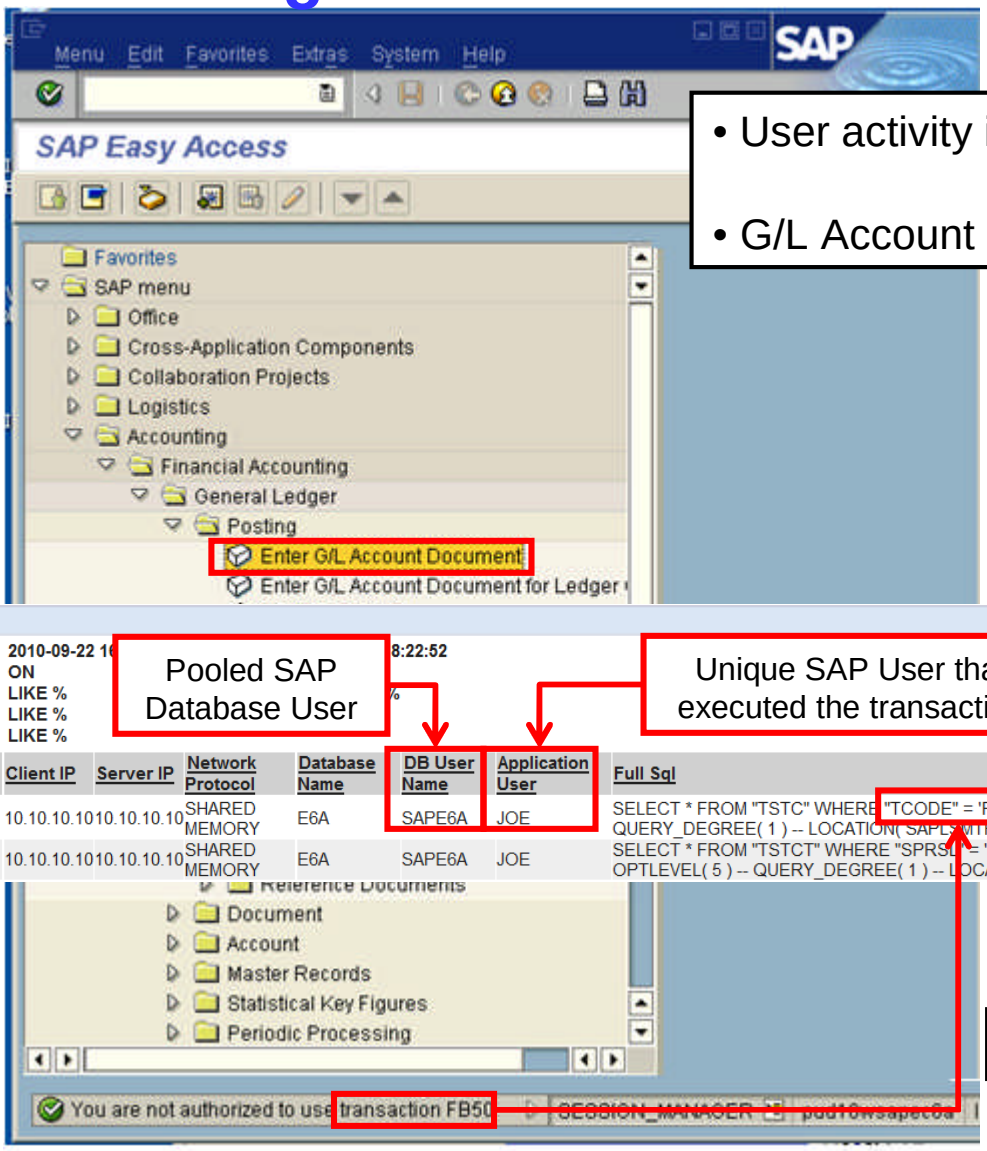
- **Be careful for "SU"**
- **Proactive Policies are required**

- Database Administrator
- System Administrator

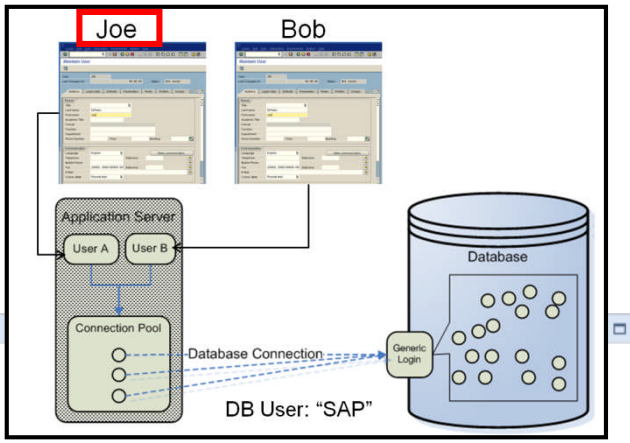
Use Continuous Monitoring to identify high risk users who can switch identity

© 2013 IBM Corporation

SAP Auditing With T-Code



- User activity is based on transactions
- G/L Account Posting = FB50 transaction



- sql trace

Start Date: 2010-09-22 1 8:22:52
Aliases: ON
DBUserLike: LIKE %
NetProtoLike: LIKE %
SourceProgLike: LIKE %

Pooled SAP Database User

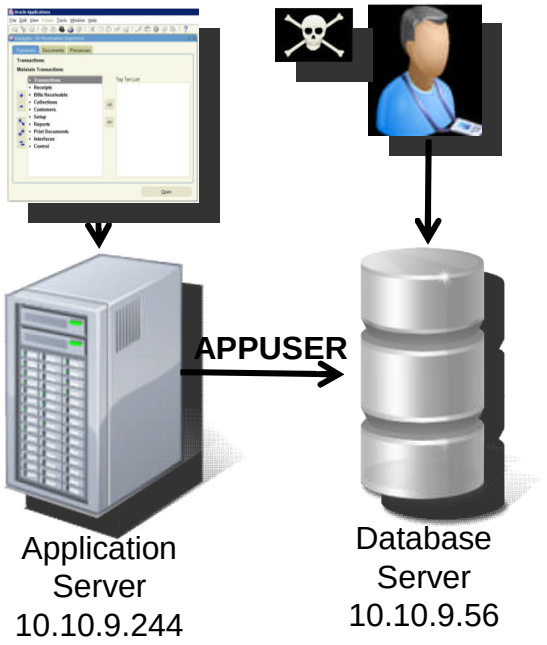
Unique SAP User that executed the transaction

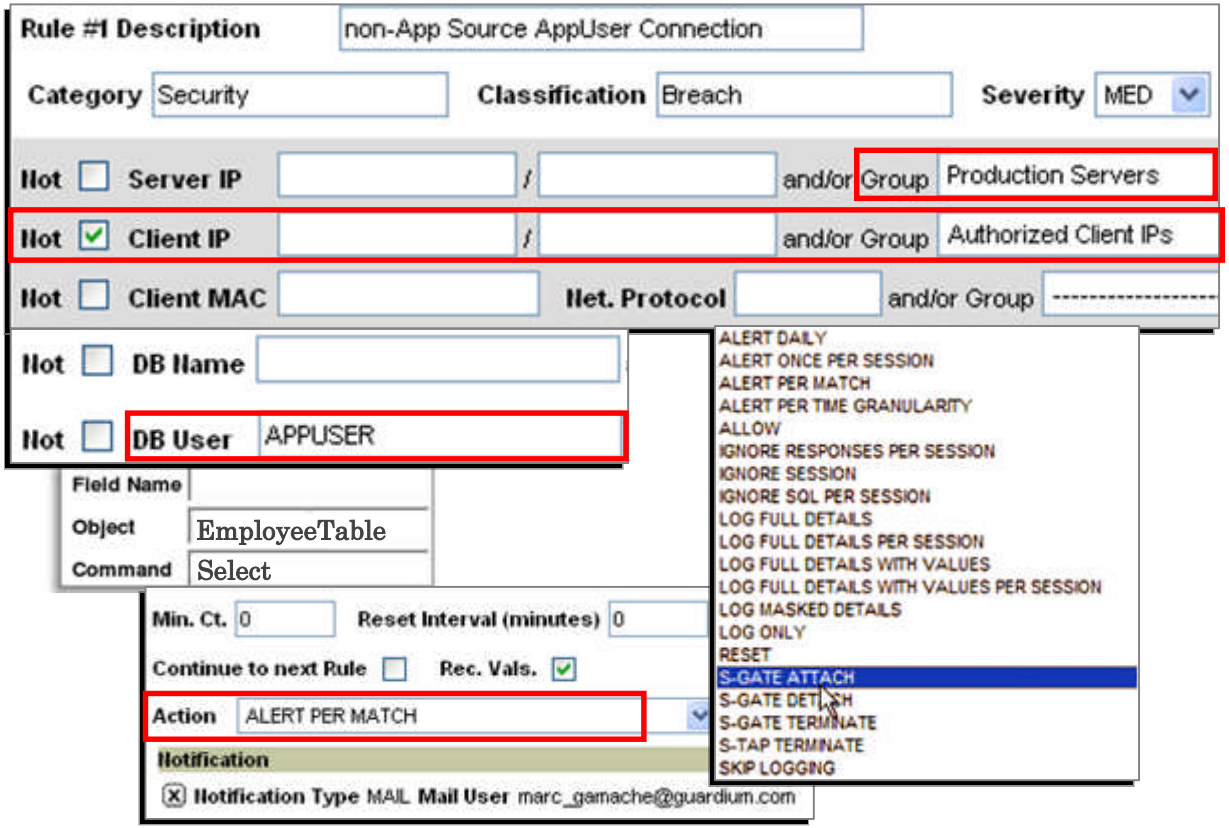
Timestamp	Client IP	Server IP	Network Protocol	Database Name	DB User Name	Application User	Full Sql
2010-09-22 17:24:10.0	10.10.10.10	10.10.10.10	SHARED MEMORY	E6A	SAPE6A	JOE	SELECT * FROM "TSTC" WHERE "TCODE" = 'FB50' FETCH FIRST 1 ROWS ONLY OPTIMIZE FOR 1 ROWS WITH CS -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLSMTR_NAVIGATION_MODULES , 621) -- SYSTEM(E6A , SAPE6A)
2010-09-22 17:24:10.0	10.10.10.10	10.10.10.10	SHARED MEMORY	E6A	SAPE6A	JOE	SELECT * FROM "TSTCT" WHERE "SPRSL" = 'E' AND "TCODE" = 'FB50' FETCH FIRST 1 ROWS ONLY OPTIMIZE FOR 1 ROWS WITH CS -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLSMTR_NAVIGATION_MODULES , 1416) -- SYSTEM(E6A , SAPE6A)

How can we capture this information?

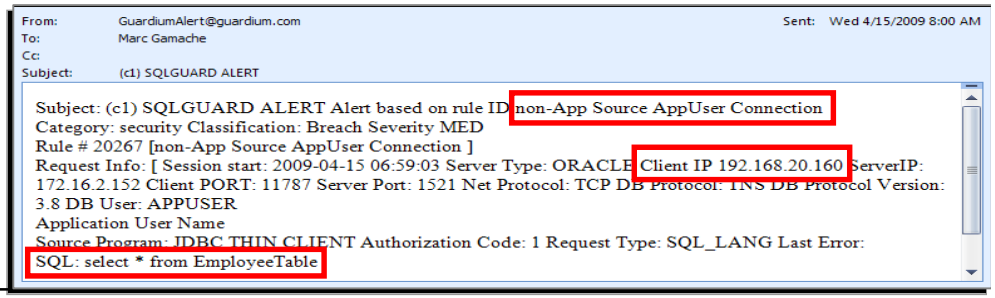
© 2013 IBM Corporation

Granular Policies with Detective & Preventive Controls





Sample Alert



© 2013 IBM Corporation

Guardium SAP monitoring Options

1. SAP DB Method

- Requires application user translation configuration
- Requires database connection
- Populate SAP APP Serves and SAP DB Servers groups
- SAP audit logs must be preserved
- Runs only as scheduled

No “Selects”

2. SAP Observed Method

- Requires application user translation configuration
- Populate SAP APP Servers and SAP DB Servers groups
- Requires inspection engine restart
- Must be scheduled

3. Out of box Method

- Populate SAP APP Servers and SAP DB Servers groups
- Requires inspection engine restart
- Minimum SAP kernel version requirements

© 2013 IBM Corporation

SAP-DB Method Report Example

SAP Application Access

Start Date: **2011-04-02 19:44:09** End Date: **2011-10-02 20:44:09**
Aliases: OFF

Application Type	Application Code	Item Name	User	Operation Type	Transaction Code	System Id	Change Date	Record Detail 1
SAP-DB	SAPs	ADRESSE	DDIC	U	XD01	000	2011-07-28 14:39:35.0	BP 0000023809
SAP-DB	SAPs	ADRESSE3	JOE	U	SU01	800	2011-07-28 22:32:51.0	BC010000057353000000008322
SAP-DB	SAPs	ADRESSE3	LARRY	U	SU01	001	2011-09-30 14:18:29.0	BC010000024069000000941
SAP-DB	SAPs	DEBI	DDIC	I	XD01	000	2011-07-28 14:39:35.0	A1111Z
SAP-DB	SAPs	NRINTERVAL	JOE	U	SU01	800	2011-07-28 22:32:51.0	SO_OBJ_FOL
SAP-DB	SAPs	NRINTERVAL	JOE	U	SU01	800	2011-07-28 22:32:51.0	SO_OBJ_USR

Records 1 to 6 of 6

Entity List
- Client/Server
- Session
- Application Data

SAP Application Access

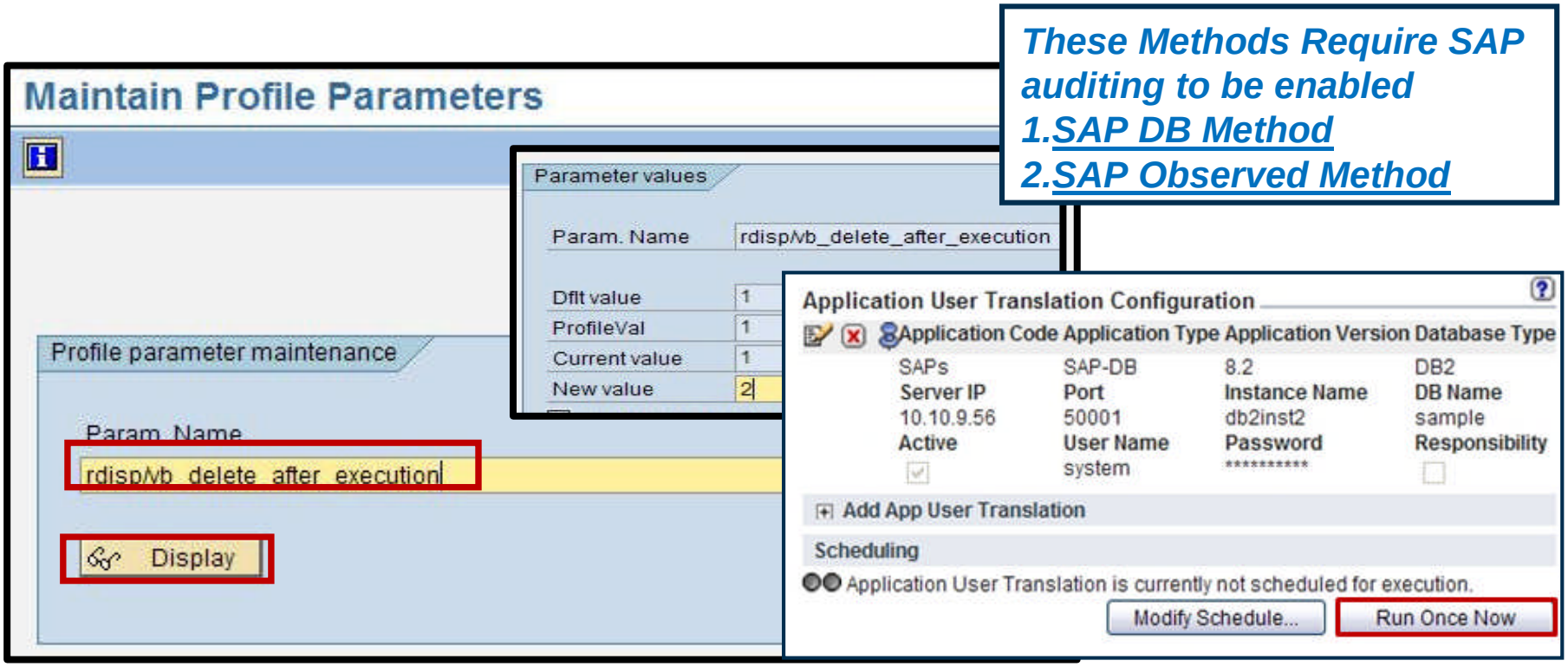
Main Entity: **Application Data**

Query Fields

Seq.	Entity	Attribute	Field Mode
1	Application Data	Application Type	Value
2	Application Data	Application Code	Value
3	Application Data	Item Name	Value
4	Application Data	User	Value
5	Application Data	Operation Type	Value
6	Application Data	Transaction Code	Value
7	Application Data	System Id	Value
8	Application Data	Change Date	Value
9	Application Data	Record Detail 1	Value

© 2013 IBM Corporation

Verify That SAP Logging is Activated



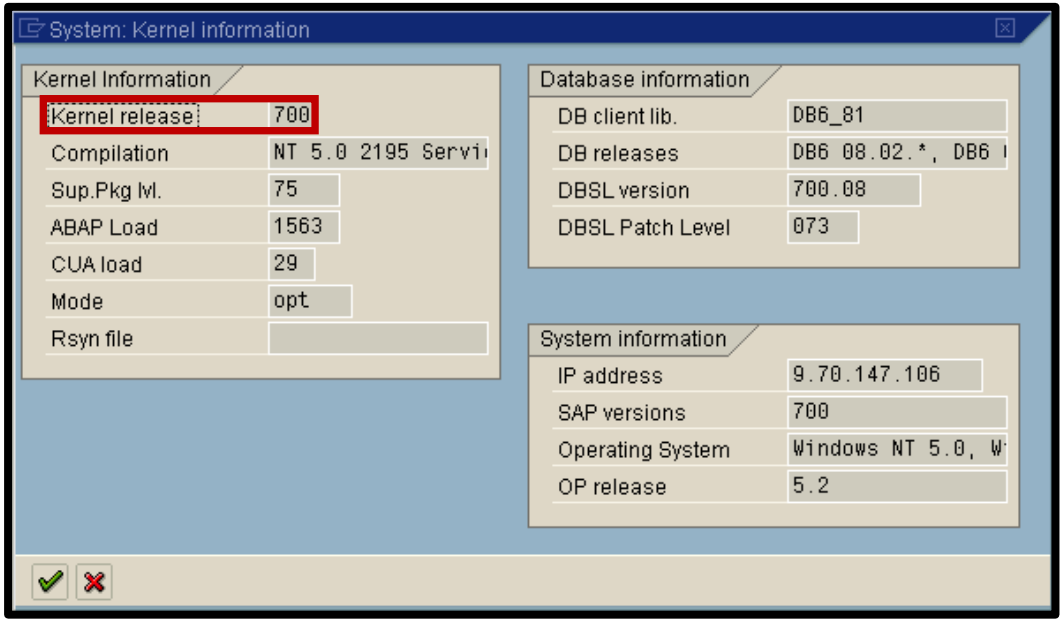
- **SAP Transaction RZ11 rdisp/vb_delete_after_execution**
- **SAP Basis/Staff member with proper authority**
- **Current value must be set to 2 so that logs will not be deleted after execution**

Note: When set to 2 automatic deletion is deactivated. This value can be used to get the update and database performance. In this case, the **report rsm 13002 with the parameter DELETE = X** should run in the background at least once a day to prevent the update tables from becoming excessively large.

Note: These settings will revert back to default each time the system restarted. **This can be overriden via SAP Transaction RZ10.**

© 2013 IBM Corporation

Out of box Method - System Kernel Information (ABAP Stack)



In this example, the kernel is 700.

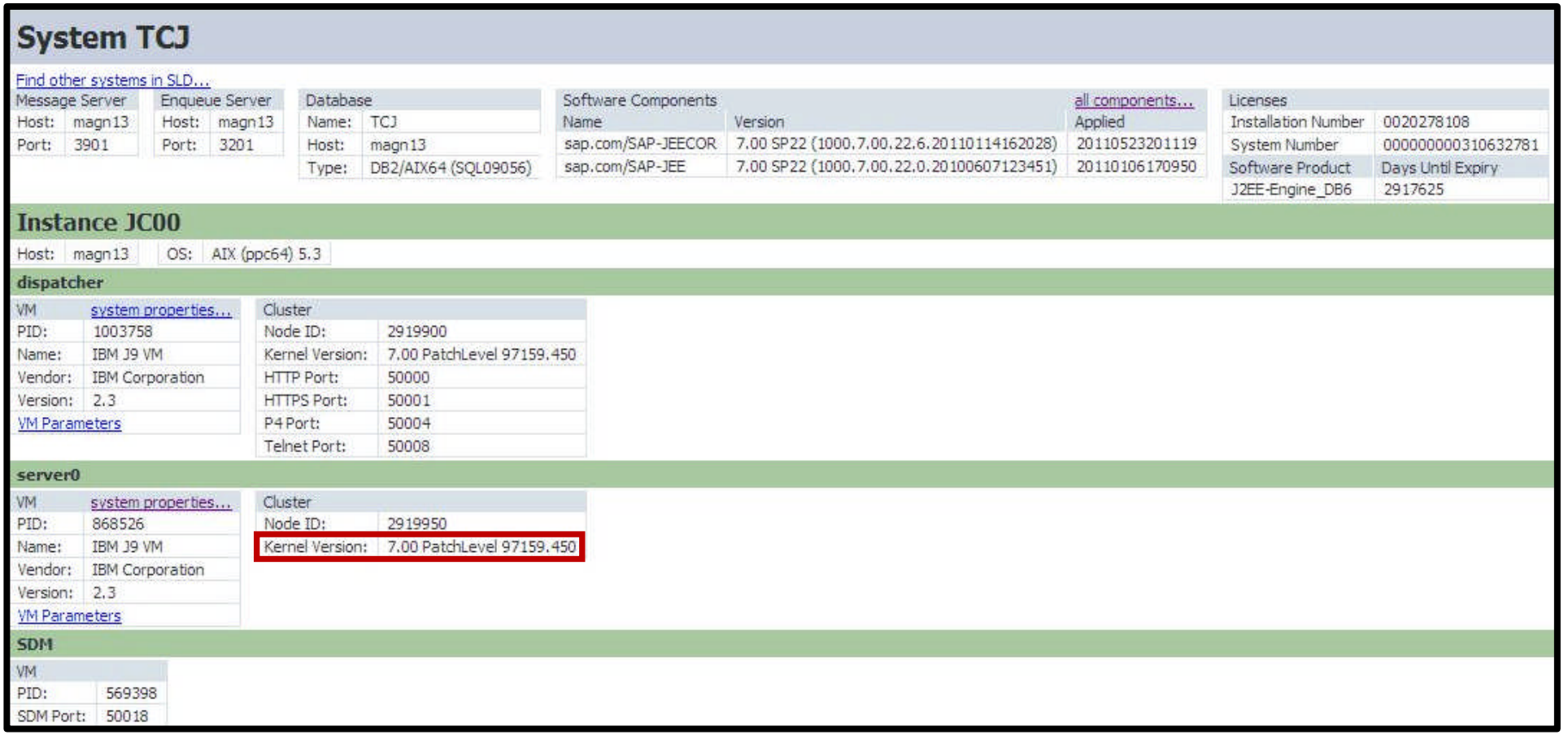
SAP with DB2 backend database requires a kernel of 700 or higher to support Application User Translation out of the box

SAP with Oracle database backend requires a kernel of 710 or higher to support Application User Translation out of the box

Data gets put into the app user field and the app event string.

© 2013 IBM Corporation

Out of box Method – Java Stack



System TCJ

Find other systems in SLD...

Message Server	
Host:	magn13
Port:	3901

Enqueue Server	
Host:	magn13
Port:	3201

Database	
Name:	TCJ
Host:	magn13
Type:	DB2/AIX64 (SQL09056)

Software Components — all components...

Name	Version	Applied
sap.com/SAP-JEECOR	7.00 SP22 (1000.7.00.22.6.20110114162028)	20110523201119
sap.com/SAP-JEE	7.00 SP22 (1000.7.00.22.0.20100607123451)	20110106170950

Licenses	
Installation Number	0020278108
System Number	0000000310632781
Software Product	Days Until Expiry
J2EE-Engine_DB6	2917625

Instance JC00

Host:	magn13	OS:	AIX (ppc64) 5.3

dispatcher

VM	system properties...
PID:	1003758
Name:	IBM J9 VM
Vendor:	IBM Corporation
Version:	2.3
VM Parameters	

Cluster	
Node ID:	2919900
Kernel Version:	7.00 PatchLevel 97159.450
HTTP Port:	50000
HTTPS Port:	50001
P4 Port:	50004
Telnet Port:	50008

server0

VM	system properties...
PID:	868526
Name:	IBM J9 VM
Vendor:	IBM Corporation
Version:	2.3
VM Parameters	

Cluster	
Node ID:	2919950
Kernel Version:	7.00 PatchLevel 97159.450

SDM

VM	
PID:	569398
SDM Port:	50018

SAP for either DB2 or Oracle requires a kernel of 7.02 or higher for Java Stack
SAP sets similar client properties in the Java Stack as it did for ABAP Stack

© 2013 IBM Corporation

Populate SAP Pre-Defined Application Groups

Application	Pre-Defined Group	Group Type
EBS	EBS App Servers	Client IP
EBS	EBS DB Servers	Server IP
PeopleSoft	PSFT App Servers	Client IP
PeopleSoft	PSFT DB Servers	Server IP
People Soft	PeopleSoft Objects	Objects
Siebel	SIEBEL App Servers	Client IP
Siebel	SIEBEL DB Servers	Server IP
SAP	SAP App Servers	Client IP
SAP	SAP DB Servers	Server IP
SAP	SAP - PCI	Objects

© 2013 IBM Corporation

SAP Auditing Example

- **Reports can be easily customized**
- **Details of what SAP tables are being accessed with T-Codes**
- **Color code by command (insert, update, delete, select, etc)**
- **Doesn't SAP use a "pooled" database user connection?**

SAP OBJECT TRACKING

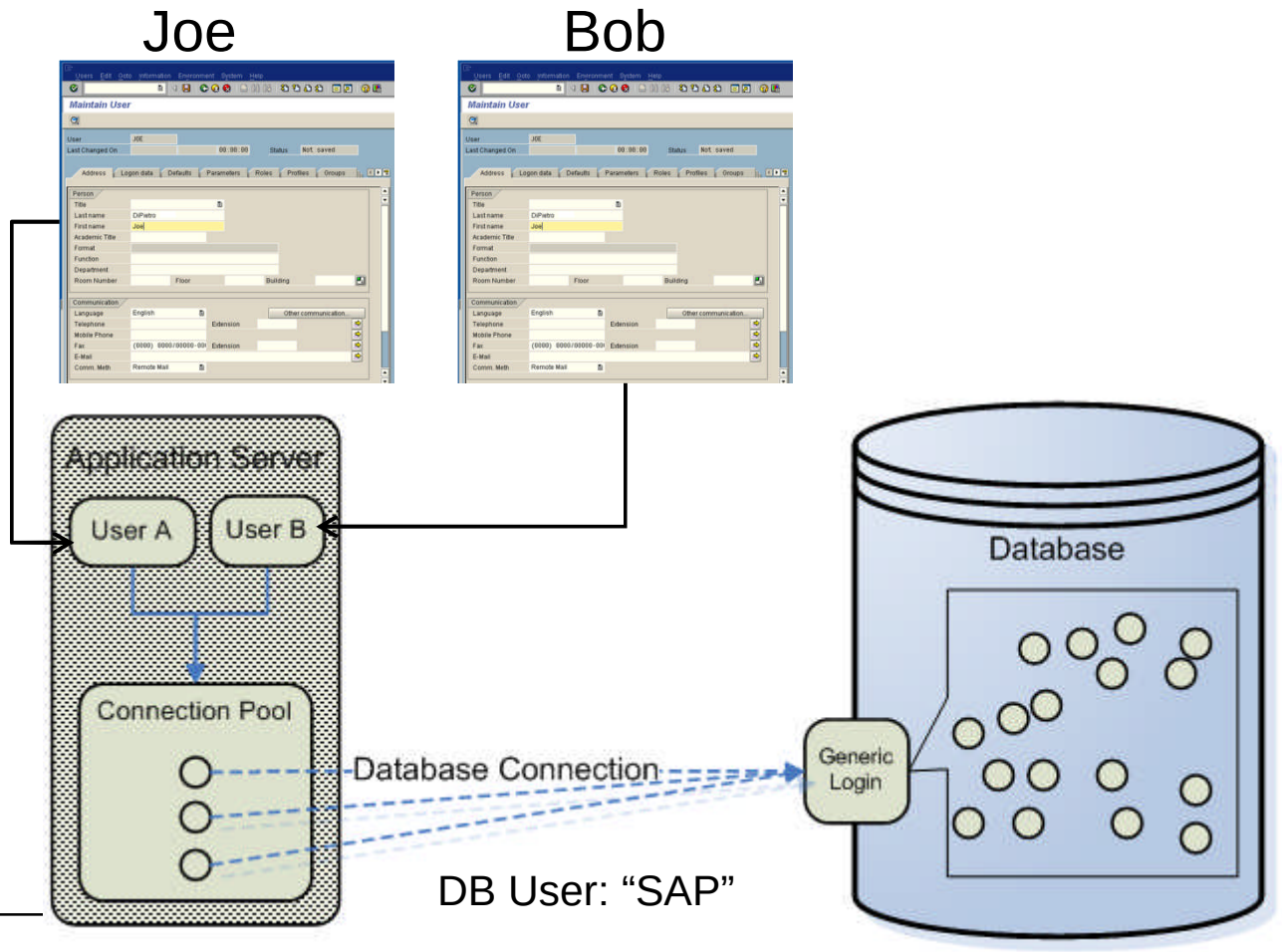
Start Date: 2012-07-23 12:54:32 End Date: 2012-07-23 13:54:32
Aliases: OFF DBUsernameLike: LIKE %
ObjectNameLike: LIKE % SAPID3: LIKE %
ServerIPLike: LIKE %

Client IP	SQL Verb	Object Name	Transaction	Total access
9.70.147.107	SELECT	UST10S	SU01	1
9.70.147.107	SELECT	UST10C	SU01	25
9.70.147.107	SELECT	UST04	SU01	0
9.70.147.107	INSERT	UST04	SU01	3
9.70.147.107	UPDATE	USRSTAMP	SU01	3
9.70.147.107	UPDATE	USREFUS	SU01	3
9.70.147.107	UPDATE	USREFUS	PA40	0
9.70.147.107	SELECT	USRBF2	SU01	9
9.70.147.107	SELECT	USRBF2	PA40	0
9.70.147.107	INSERT	USRBF2	SU01	4
9.70.147.107	UPDATE	USR41_MLD	PA40	1
9.70.147.107	UPDATE	USR41_MLD	SU01	7
9.70.147.107	DELETE	USR41	SU01	6
9.70.147.107	DELETE	USR41	PA40	0
9.70.147.107	UPDATE	USR21	SU01	8
9.70.147.107	SELECT	USR21	SU01	1
9.70.147.107	SELECT	USR21	PA40	0
9.70.147.107	SELECT	USR10	SU01	0
9.70.147.107	SELECT	USR05	PA40	0
9.70.147.107	SELECT	USR05	SU01	4
9.70.147.107	INSERT	USR05	SU01	0
9.70.147.107	DELETE	USR05	SU01	3
9.70.147.107	UPDATE	USR04	SU01	3
9.70.147.107	SELECT	USR02	SU01	2
9.70.147.107	SELECT	USR02	PA40	0
9.70.147.107	UPDATE	USR01	SU01	7
9.70.147.107	INSERT	USH04	SU01	3
9.70.147.107	UPDATE	USH02	SU01	2
9.70.147.107	SELECT	USERS_SSM	SU01	2

© 2013 IBM Corporation

SAP Architecture –
Why Is It Difficult To Non-Intrusively Audit SAP?

- **SAP uses “Pooled” database user connections**
- **This means the user Joe and Bob can’t uniquely be identified at the database level**
- **They share the “SAP” database user account, which does their transactions for them**



© 2013 IBM Corporation

Securing SAP Trivia Quiz…

- **What do two important users in the SAP system have in common?**
- **The default password for SAP* is 06071992.**
- **The default password for DDIC is 19920706**

- This is the initial date when R/3 was officially launched (6 July 1992)
- Make sure you change these passwords!!!

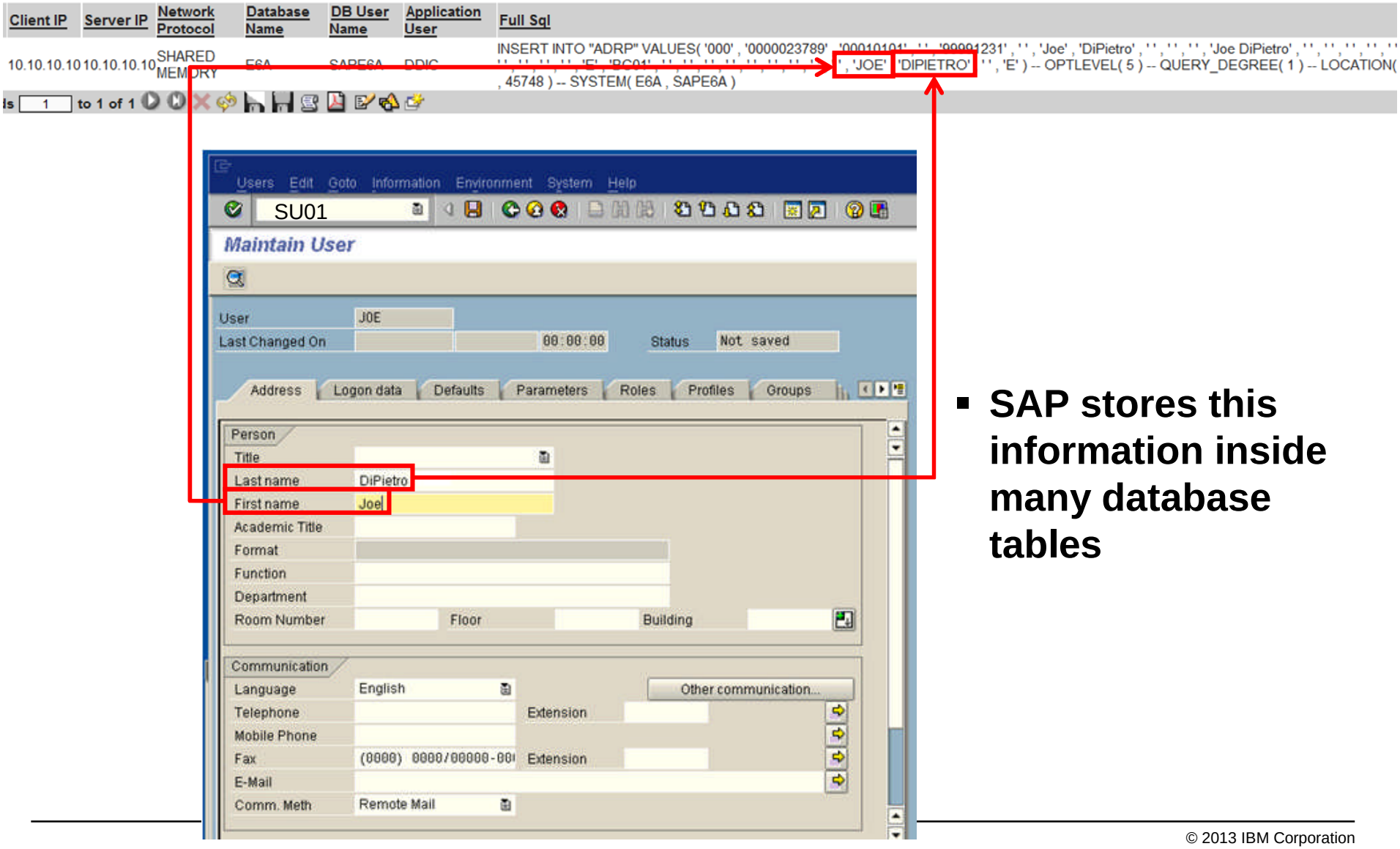
© 2013 IBM Corporation

Monitoring SAP Users

- Good security starts with monitoring users and privileges
- What is the process to add a user to the system?
- Transaction codes…
- SU01 is a transaction code that allows you to add users
- How can we monitor this action?

© 2013 IBM Corporation

“SU01” - Adding Users within SAP



- **SAP stores this information inside many database tables**

© 2013 IBM Corporation

SAP Database Tables Relating to User Information…

Client IP	Server IP	Network Protocol	Database Name	DB User Name	Application User	Full Sql
10.10.10.10	10.10.10.10	SHARED MEMORY	E6A	SAPE6A	DDIC	INSERT INTO 'ADRP' VALUES('000' , '0000023789' , '00010101' , ' ' , '99991231' , ' ' , 'Joe' , 'DiPietro' , ' ' , ' ' , ' ' , 'Joe DiPietro' , ' ' , ' ' , ' ' , ' ' , ' ' , ' ' , ' ' , ' ' , ' ' , 'E' , 'BC01' , ' ' , ' ' , ' ' , ' ' , ' ' , ' ' , ' ' , ' ' , ' ' , 'JOE' , 'DIPIETRO' , ' ' , 'E') -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(, 45748) -- SYSTEM(E6A , SAPE6A)

ls 1 to 1 of 1

- **ADRP = Personal Data like First and Lastname**

- **USR01 = User master record**

Client IP	Server IP	Network Protocol	Database Name	DB User Name	Application User	Full Sql
10.10.10.10	10.10.10.10	SHARED MEMORY	E6A	SAPE6A	DDIC	INSERT INTO "USR01" VALUES('000' , 'JOE' , ' ' , ' ' , ' ' ... 5) -- QUERY_DEG -- LOCATION(SAPLSUU1 , 8486) -- SYSTEM(E6A , SA

- **USR02 = Logon Data**

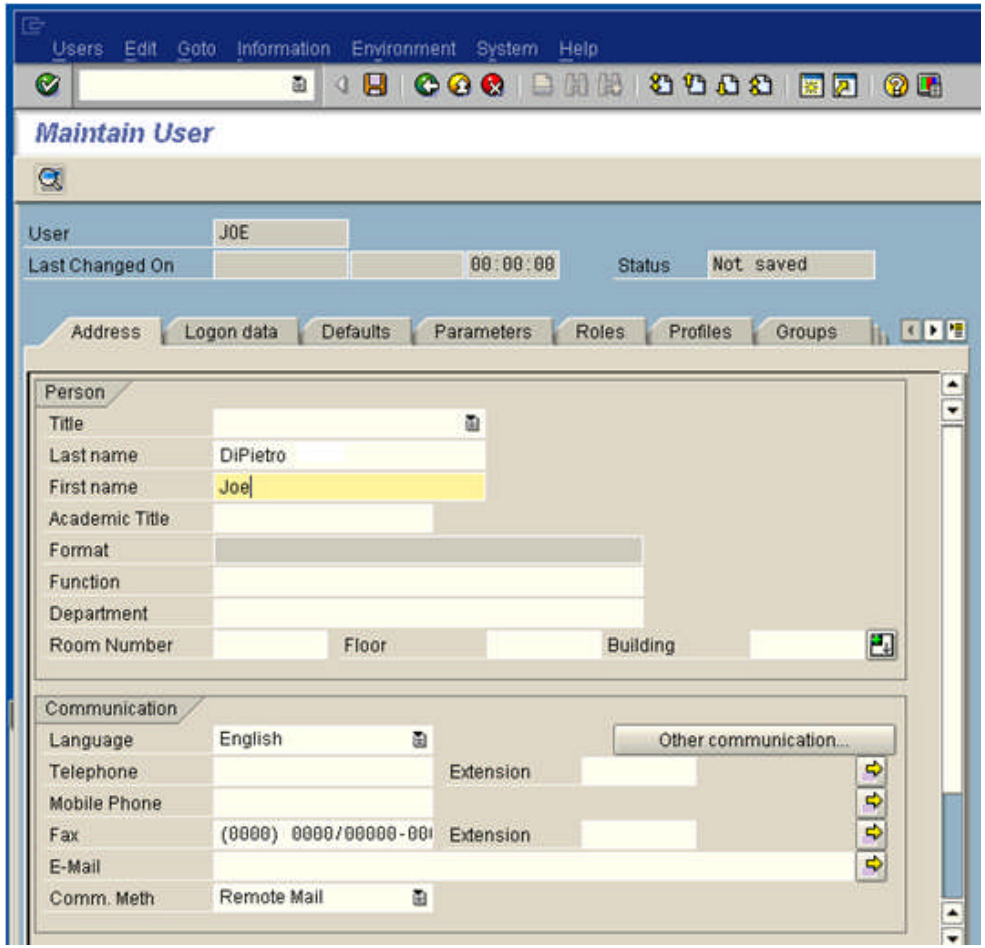
Timestamp	Client IP	Server IP	Network Protocol	Database Name	DB User Name	Application User	Full Sql
2010-09-22 17:16:41.0	10.10.10.10	10.10.10.10	SHARED MEMORY	E6A	SAPE6A	DDIC	INSERT INTO "USR02" VALUES('000' , 'JOE' , null , '00000000' , '00000000' , 'A' , ' ' , 0 , 0 , ' ' , 'DDIC' , '20100922' , '00000000' , ' ' , null , '00000000' , ' ' , null , '00000000' , ' ' , null , '00000000' , ' ' , null , '00000000' , ' ' , ' ' , 'G' , ' ' , ' ' , null , '20100922' , 0 , 0 , 0 , OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLSUU1 , 8654) -- SYSTEM(E6A , SAPE6A)

- **USR04 = Master Authorization**

Timestamp	Client IP	Server IP	Network Protocol	Database Name	DB User Name	Application User	Full Sql
2010-09-22 17:16:44.0	10.10.10.10	10.10.10.10	SHARED MEMORY	E6A	SAPE6A	DDIC	INSERT INTO "USR04" VALUES('000' , 'JOE' , '20100922' , '171641' , 'DDIC' , 2 , 'C') -- OPTLEVEL(5) -- QUERY_DE SAPLSUU2 , 1292) -- SYSTEM(E6A , SAPE6A)

Defining One User Touches Many Different Database Tables

- **It's important to understand how to easily get at this information when monitoring and auditing an SAP System….**



© 2013 IBM Corporation

Drill Down Capability Is Critical To Understanding SAP Transactions

estamp	Client IP	Server IP	Network Protocol	Database Name	DB User Name	Application User	Full Sql
-09-22 :44.0	10.10.10.10	10.10.10.10	SHARED MEMORY	E6A	SAPE6A	DDIC	INSERT INTO "USR04" VALUES('000' , 'JOE' , SAPLSUU2 , 1292) -- SYSTEM(E6A , SAPE6A

- 0FullDetails
- 0OpenStapSessions
- 0ShowSQLs
- Admin Users Sessions
- Basel II - DDL Distribution
- Basel II - DML Distribution
- Client IP Activity Summary
- DB Predefined Users Sessions
- DB Server Throughput-Chart
- Detailed Sessions List
- Exceptions Type Distribution
- Full SQL By Client IP
- Full SQL By DB User
- SOX - DDL Distribution
- SOX - DML Distribution
- Throughput-Chart
- **User Activity Summary**
- Alias Definition
- Show SQL
- Show SQL with Values

- **Identify user activity based on table**

IBM® InfoSphere™ Guardium®

Client IP	Source Program	SQL Verb	Depth	Object Name	Total access
10.10.10.10	DISP+WORK.EXE	SELECT	0	ADCNTRYQU	2
10.10.10.10	DISP+WORK.EXE	INSERT	0	ADCP	2
10.10.10.10	DISP+WORK.EXE	SELECT	0	ADCP	9
10.10.10.10	DISP+WORK.EXE	SELECT	0	ADR3	25
10.10.10.10	DISP+WORK.EXE	INSERT	0	ADR3	2
10.10.10.10	DISP+WORK.EXE	SELECT	0	ADR7	2
10.10.10.10	DISP+WORK.EXE	INSERT	0	ADR7	2
10.10.10.10	DISP+WORK.EXE	SELECT	0	ADRC	18
10.10.10.10	DISP+WORK.EXE	INSERT	0	ADRCOMC	3
10.10.10.10	DISP+WORK.EXE	SELECT	0	ADRCT	4
10.10.10.10	DISP+WORK.EXE	SELECT	0	ADRG	5
10.10.10.10	DISP+WORK.EXE	SELECT	0	ADRGP	5
10.10.10.10	DISP+WORK.EXE	INSERT	0	ADRP	6
10.10.10.10	DISP+WORK.EXE	SELECT	0	ADRP	5
10.10.10.10	DISP+WORK.EXE	SELECT	0	ADRT	30
10.10.10.10	DISP+WORK.EXE	SELECT	0	ADRU	25
10.10.10.10	DISP+WORK.EXE	INSERT	0	ADRU	5
10.10.10.10	DISP+WORK.EXE	SELECT	0	ADRVP	15
10.10.10.10	DISP+WORK.EXE	INSERT	0	ADRVP	4
10.10.10.10	DISP+WORK.EXE	SELECT	0	AGR_AGRS	144

Records: 1 to 20 of 394

ADRP = Personal Data like First and Lastname

Who accessed this?

© 2013 IBM Corporation

Drill Down Capability – What Table Are You Interested

IBM® InfoSphere™ Guardium®

Client IP	Source Program	SQL Verb	Depth	Object Name	Total access
10.10.10.10	DISP+WORK.EXE	INSERT	0	TUCON	48
10.10.10.10	DISP+WORK.EXE	SELECT	0	T_01	1458
10.10.10.10	DISP+WORK.EXE	INSERT	0	UCMP000	4
10.10.10.10	DISP+WORK.EXE	SELECT	0	URL_EXITS	1
10.10.10.10	DISP+WORK.EXE	SET CLIENT APPLNAME	0	US01	2
10.10.10.10	DISP+WORK.EXE	SELECT	0	USERS_SSM	6
10.10.10.10	DISP+WORK.EXE	SELECT	0	USGRP_USER	4
10.10.10.10	DISP+WORK.EXE	INSERT	0	USH02	5
10.10.10.10	DISP+WORK.EXE	SELECT	0	USH02	6
10.10.10.10	DISP+WORK.EXE	UPDATE	0	USH02	4
10.10.10.10	DISP+WORK.EXE	SELECT	0	USOBX_C	21
10.10.10.10	DISP+WORK.EXE	SELECT	0	USR01	2
10.10.10.10	DISP+WORK.EXE	UPDATE	0	USR01	5
10.10.10.10	DISP+WORK.EXE	INSERT	0	USR01	2
10.10.10.10	DISP+WORK.EXE	UPDATE	0	USR02	9
10.10.10.10	DISP+WORK.EXE	SELECT	0	USR02	24
10.10.10.10	DISP+WORK.EXE	INSERT	0	USR02	1
10.10.10.10	DISP+WORK.EXE	SELECT	0	USR04	104
10.10.10.10	DISP+WORK.EXE	INSERT	0	USR04	1
10.10.10.10	DISP+WORK.EXE	SELECT	0	USR05	6

Records: 328 to 347 of 394

- Client IP Activity Summary
- Command Details
- Full SQL By Client IP
- Object Activity Summary
- Object Details
- Sensitive Objects List
- Alias Definition
- Show SQL
- Show SQL with Values

USR04 = Master Authorization

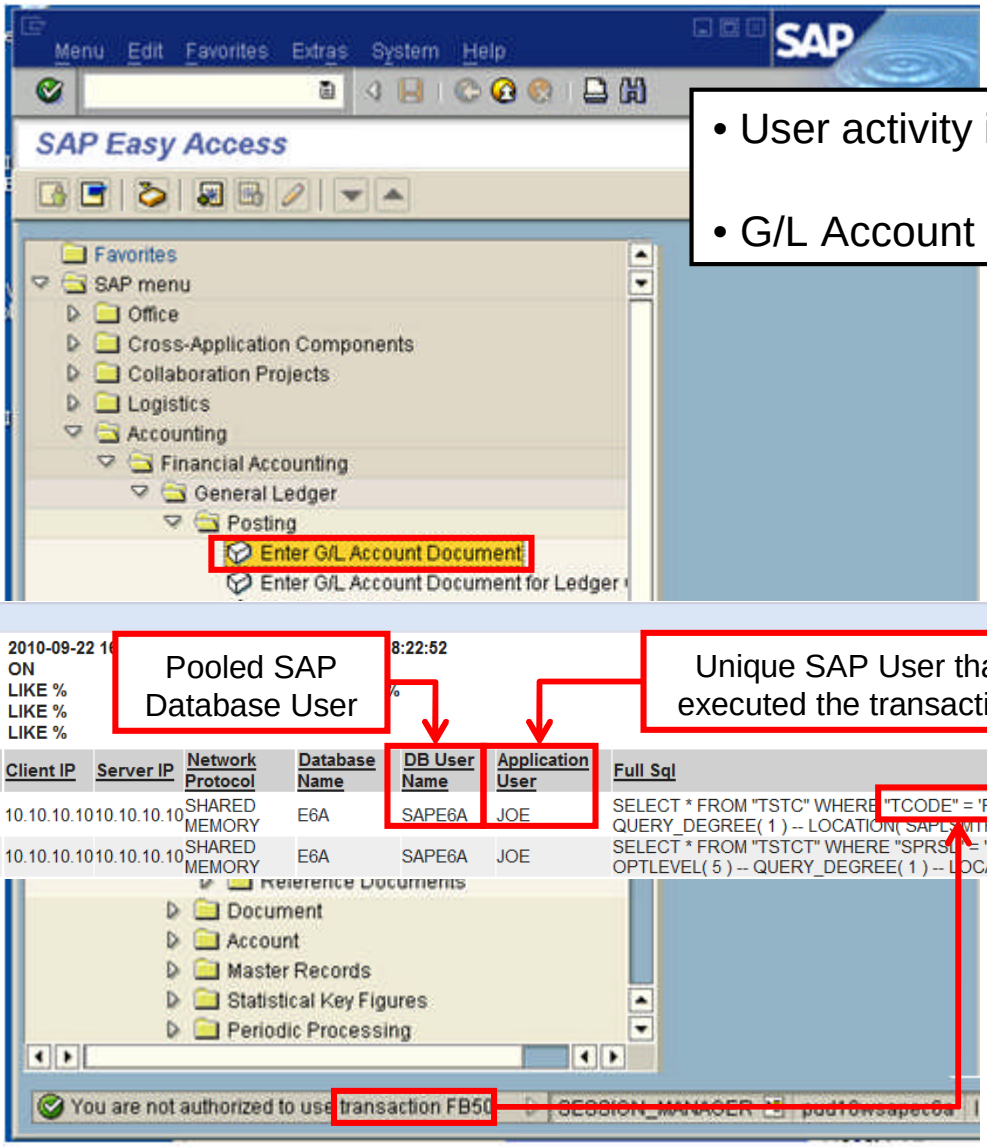
IBM® InfoSphere™ Guardium®

SQL String
INSERT INTO "USR04" VALUES('000' , 'JOE' , '20100922' , '171641' , 'DDIC' , 2 , 'C') -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLSUU2 , 1292) -- SYSTEM(E6A , SAPE6A)

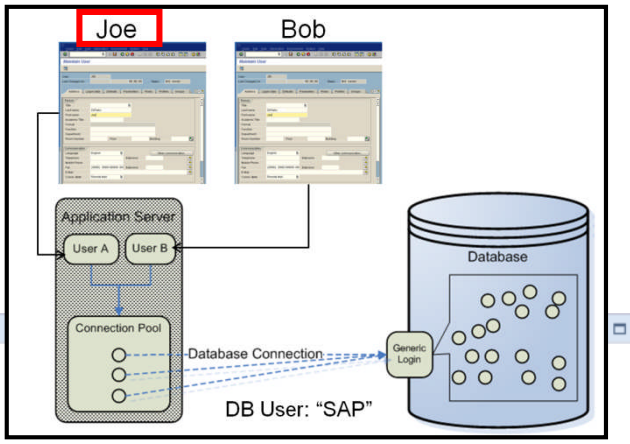
JOE's authorizations were added to the USR04 database table

© 2013 IBM Corporation

SAP Transactions to G/L Account



- User activity is based on transactions
- G/L Account Posting = FB50 transaction



- sql trace

Start Date: 2010-09-22 1 8:22:52
Aliases: ON
DBUserLike: LIKE %
NetProtoLike: LIKE %
SourceProgLike: LIKE %

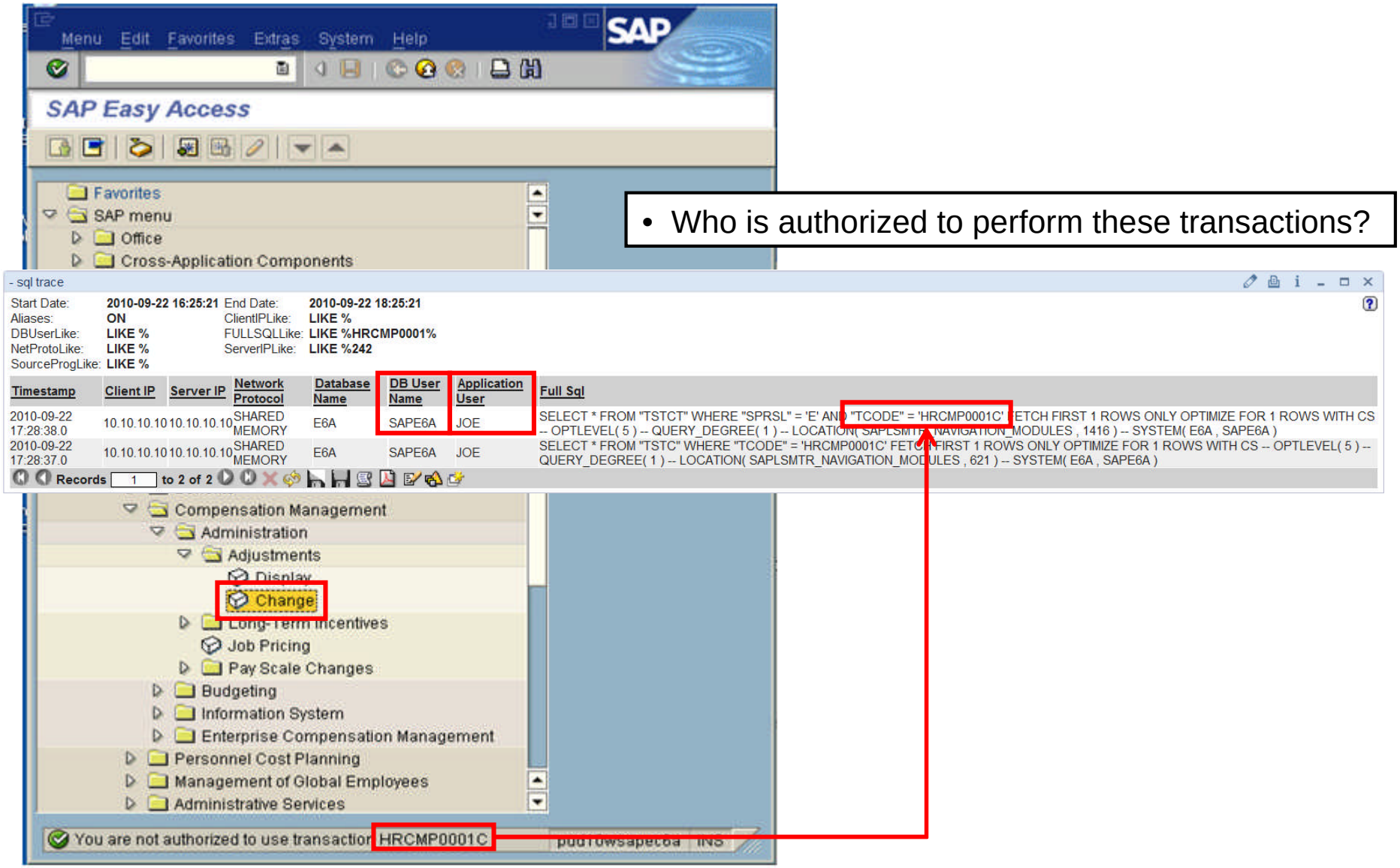
Pooled SAP Database User

Unique SAP User that executed the transaction

Timestamp	Client IP	Server IP	Network Protocol	Database Name	DB User Name	Application User	Full Sql
2010-09-22 17:24:10.0	10.10.10.10	10.10.10.10	SHARED MEMORY	E6A	SAPE6A	JOE	SELECT * FROM "TSTC" WHERE "TCODE" = 'FB50' FETCH FIRST 1 ROWS ONLY OPTIMIZE FOR 1 ROWS WITH CS -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLSMTR_NAVIGATION_MODULES , 621) -- SYSTEM(E6A , SAPE6A)
2010-09-22 17:24:10.0	10.10.10.10	10.10.10.10	SHARED MEMORY	E6A	SAPE6A	JOE	SELECT * FROM "TSTCT" WHERE "SPRSL" = 'E' AND "TCODE" = 'FB50' FETCH FIRST 1 ROWS ONLY OPTIMIZE FOR 1 ROWS WITH CS -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLSMTR_NAVIGATION_MODULES , 1416) -- SYSTEM(E6A , SAPE6A)

© 2013 IBM Corporation

SAP HR Compensation Adjustments

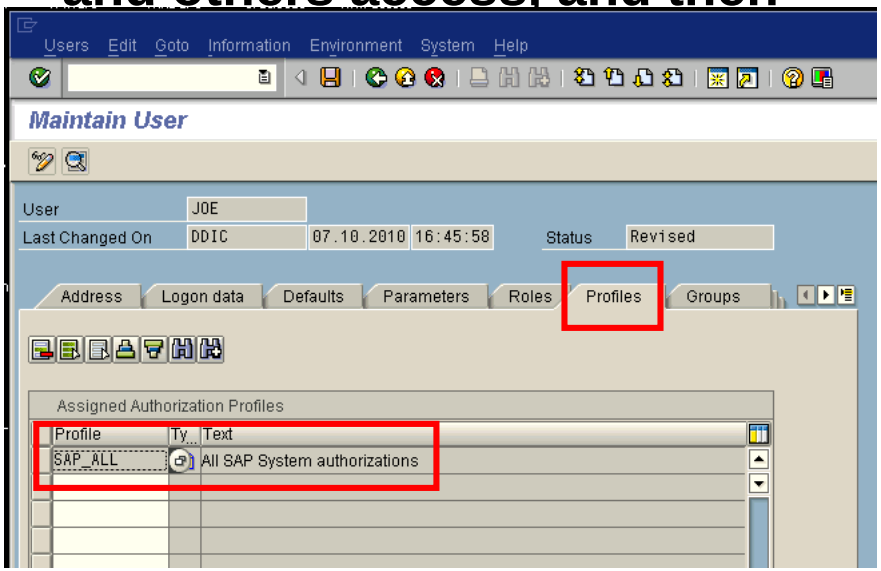


- Who is authorized to perform these transactions?

© 2013 IBM Corporation

Security Issue With “SAP_ALL”

- **SAP_ALL allows the user to perform all transactions which bypasses all of the profile security of SAP**
- **Consultants that have access to systems can grant themselves and others access, and then**



Hello All.

I have a Security issue in the Company I work.
A consultant included unauthorized access to himself and to other 2 employees.
When I identified that, I checked at USH04 table, that the user inserted the profile SAP_ALL in SAP to him. After that, I removed the access and these two changes in the user´s profile were registred at the USH04 table. I took a print screen of the table in that day, with the evidence of this issue.

Yesterday, I was checking the system and saw that the registries that identiry these changes (insert and remove SAP_ALL permission) was deleted from USH04 from these 3 users.

Do you guys know how to recover that information? Or how can I know who was responsible for the deletion? Is there any log?

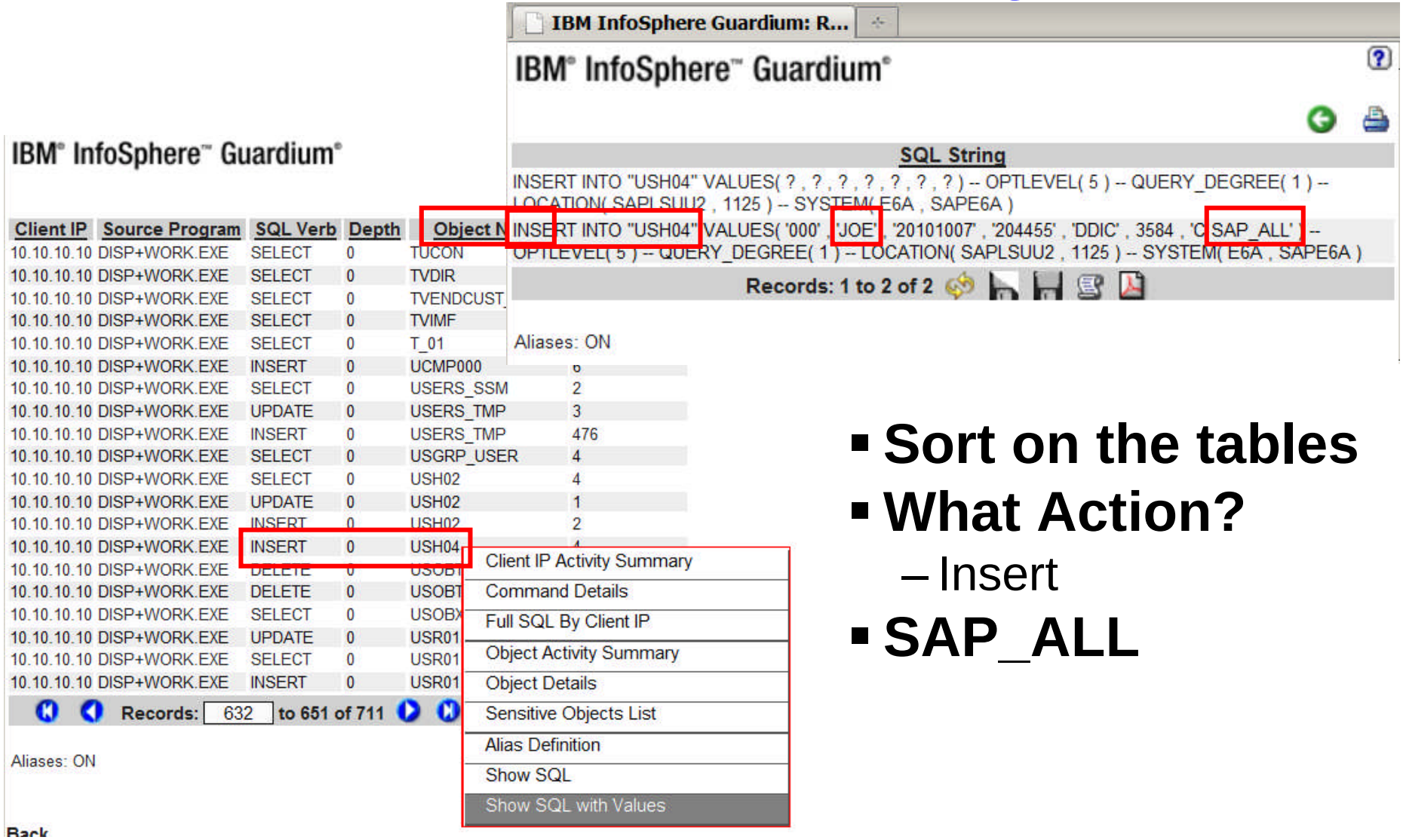
I believe the deletion was made in SE16, is most likely that. Is there any way I know who did it?

I really need some help about it.

Thank you.
Regards

© 2013 IBM Corporation

Drill Down Control For Forensic Investigations…



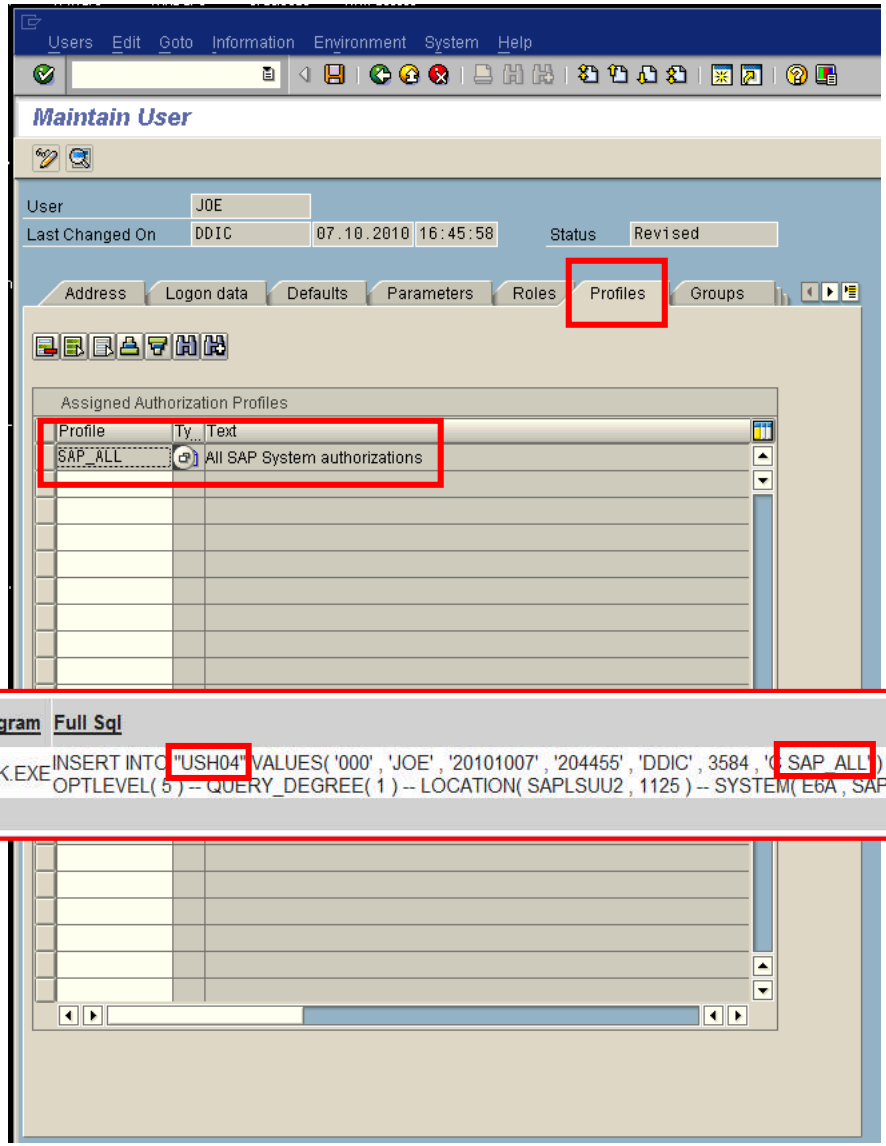
Drill Down Capability

- **Sort on the tables**
- **What Action?**
  - Insert
- **SAP_ALL**

© 2013 IBM Corporation

Auditing SAP_ALL Transactions

- **Can't delete SAP transaction logs if they are not on the application or database server!**
- **Tells you specifically what user gave them SAP_ALL privileges in the USH04 table…**
- **Automate Reports & Alerts for SAP_ALL**



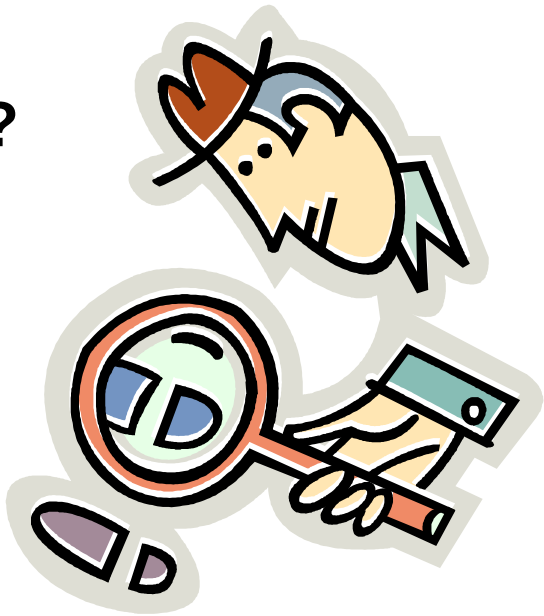
Timestamp	Client IP	Server IP	Network Protocol	Server Type	DB User Name	Application User	Source Program	Full Sql
2010-10-07 22:34:10.0	10.10.10.10	10.10.10.10	SHARED MEMORY	DB2	SAPSERVICEE6A	JOE	DISP+WORK.EXE	INSERT INTO "USH04" VALUES('000' , 'JOE' , '20101007' , '204455' , 'DDIC' , 3584 , 'SAP_ALL') -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLSUU2 , 1125) -- SYSTEM(E6A , SAPE6A)

Records 1 to 1 of 1

© 2013 IBM Corporation

How Can You Identify Who Accessed Sensitive Information?

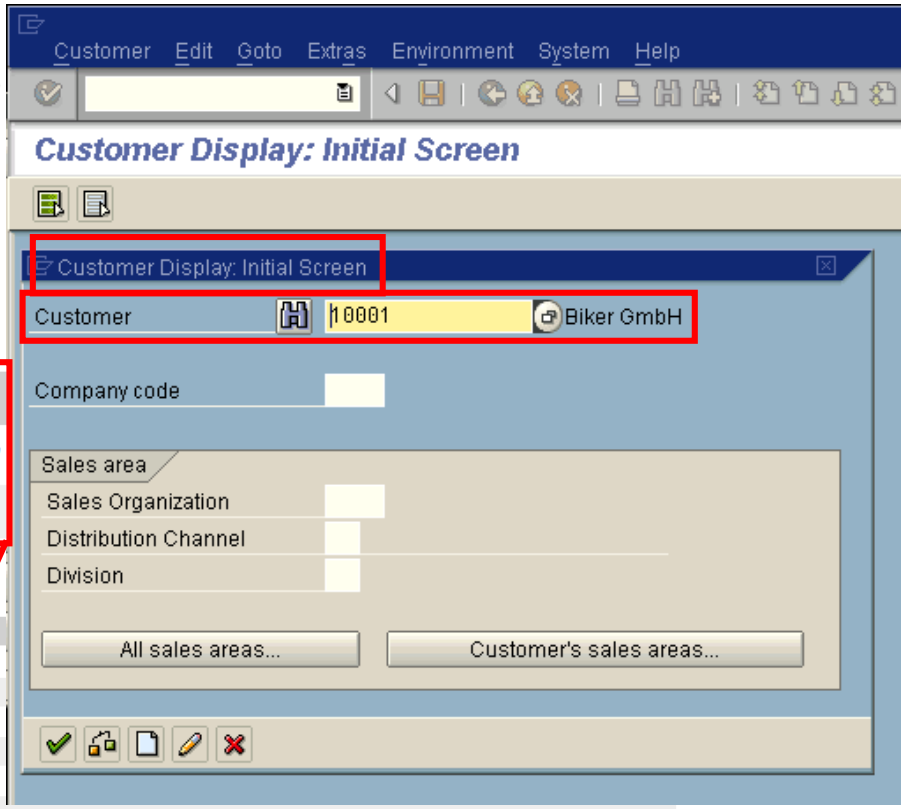
- **Who accessed your customer records?**
- **Who changed your customer records?**



© 2013 IBM Corporation

SAP Transaction Code XD03 = Display Customer Records

- **Log and audit anytime someone looks at this customer record “Biker GmbH”**
- **The transaction code for this is XD03**
- **Here’s the audit data**



Application User	Source Program	Full Sql
JOE	DISP+WORK.EXE	SET CLIENT ACCTNG 'SQL09010NT XD03 JOE ',X'08','SAPLVS01'
JOE	DISP+WORK.EXE	SET CLIENT APPLNAME 'XD03'

Timestamp	Client IP	Server IP	Network Protocol	Server Type	DB User Name	Application User	Source Program	Full Sql
2010-10-08 14:47:54.0	10.10.10.10	10.10.10.10	SHARED MEMORY	DB2	SAPSERVICEE6A	JOE	DISP+WORK.EXE	SET CLIENT ACCTNG 'SQL09010NT XD03 JOE ',X'08','SAPLVS01'
2010-10-08 14:47:54.0	10.10.10.10	10.10.10.10	SHARED MEMORY	DB2	SAPSERVICEE6A	JOE	DISP+WORK.EXE	SET CLIENT APPLNAME 'XD03'
2010-10-08 14:47:54.0	10.10.10.10	10.10.10.10	SHARED MEMORY	DB2	SAPSERVICEE6A	JOE	DISP+WORK.EXE	SET CLIENT ACCTNG 'SQL09010NT XD03 JOE ',X'08','SAPMF02D'
2010-10-08 14:47:54.0	10.10.10.10	10.10.10.10	SHARED MEMORY	DB2	SAPSERVICEE6A	JOE	DISP+WORK.EXE	SET CLIENT APPLNAME 'XD03'
2010-10-08 14:47:54.0	10.10.10.10	10.10.10.10	SHARED MEMORY	DB2	SAPSERVICEE6A	JOE	DISP+WORK.EXE	SET CLIENT ACCTNG 'SQL09010NT XD03 JOE ',X'08','SAPLPHOD'
2010-10-08 14:47:53.0	10.10.10.10	10.10.10.10	SHARED MEMORY	DB2	SAPSERVICEE6A	JOE	DISP+WORK.EXE	SET CLIENT APPLNAME 'XD03'
2010-10-08 14:47:43.0	10.10.10.10	10.10.10.10	SHARED MEMORY	DB2	SAPSERVICEE6A	JOE	DISP+WORK.EXE	SET CLIENT APPLNAME 'XD03'
2010-10-08 14:47:43.0	10.10.10.10	10.10.10.10	SHARED MEMORY	DB2	SAPSERVICEE6A	JOE	DISP+WORK.EXE	SET CLIENT ACCTNG 'SQL09010NT XD03 JOE ',X'08','SAPLVS01'
2010-10-08 14:46:31.0	10.10.10.10	10.10.10.10	SHARED MEMORY	DB2	SAPSERVICEE6A	JOE	DISP+WORK.EXE	UPDATE "ARFCSSTATE" SET "ARFCSTATE" = 'RECORDED' , "ARFCFNAM" = 'BAPI_CRM_SAVE' , "ARFCRETURN" = 'I' , "ARFCUZEIT" = '144536' , "ARFCDATUM" = '20101008' , "ARFCUSER" = 'JOE' , "ARFCRETRYS" = '0021' , "ARFCTCODE" = 'XD03' , "ARFCRHOST" = 'pud10wsa' , "ARFCMSG" = ' ' , "ARFCRESERV" = 'SAPMF02D 800 IR3AD_CUSTOME10001 00001286554023000001000 0 pud10wsapec6a_E6A_00 20101008120702 00000002 E' , "HASH" = null WHERE "ARFCIPID" = '0946936A' AND "ARFCPID" = '0B00' AND "ARFCTIME" = '4CAF41A6' AND "ARFCTIDCNT" = '0192' AND "ARFCDEST" = 'DTZ_800' AND "ARFCLUWCNT" = '00000002' -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(RSARFCSE , 236) -- SYSTEM(E6A , SAPE6A)

JOE

Joe looked at “Biker GmbH” customer number 10001

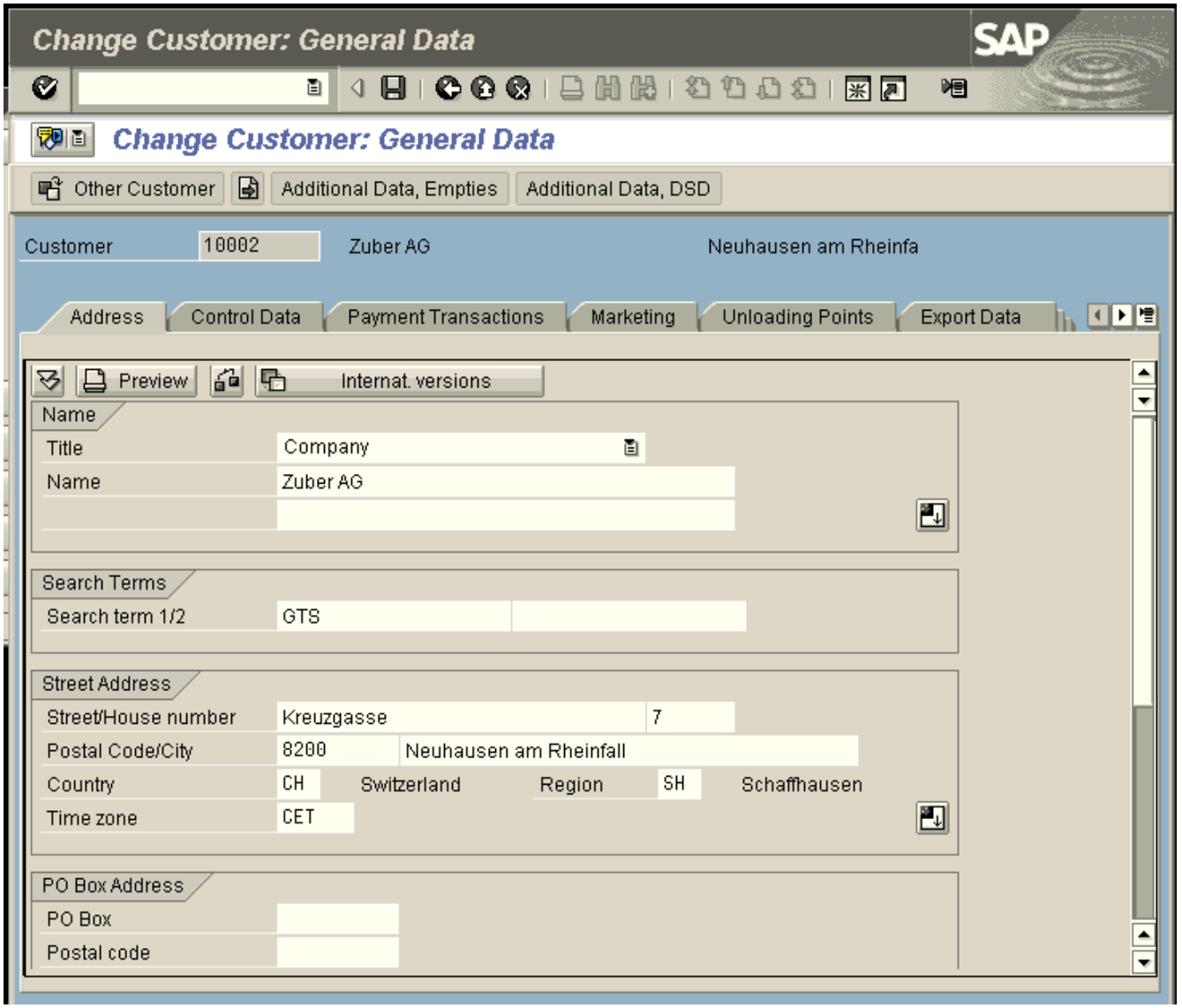
UPDATE "ARFCSSTATE" SET "ARFCSTATE" = 'RECORDED' , "ARFCFNAM" = 'BAPI_CRM_SAVE' , "ARFCUZEIT" = '144536' , "ARFCDATUM" = '20101008' , "ARFCUSER" = 'JOE' , "ARFCTCODE" = 'XD03' , "ARFCRHOST" = 'pud10wsa' , "ARFCMSG" = ' ' , 800 IR3AD_CUSTOME10001 00001286554023000001000 008120702 00000002 E' , "HASH" = null WHERE "ARFCIPID" = '0946936A' AND "ARFCPID" = '0B00' AND "ARFCTIME" = '4CAF41A6' AND "ARFCTIDCNT" = '0192' AND "ARFCDEST" = 'DTZ_800' AND "ARFCLUWCNT" = '00000002' -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(RSARFCSE , 236) -- SYSTEM(E6A , SAPE6A)

© 2013 IBM Corporation

Deleting a User…

© 2013 IBM Corporation

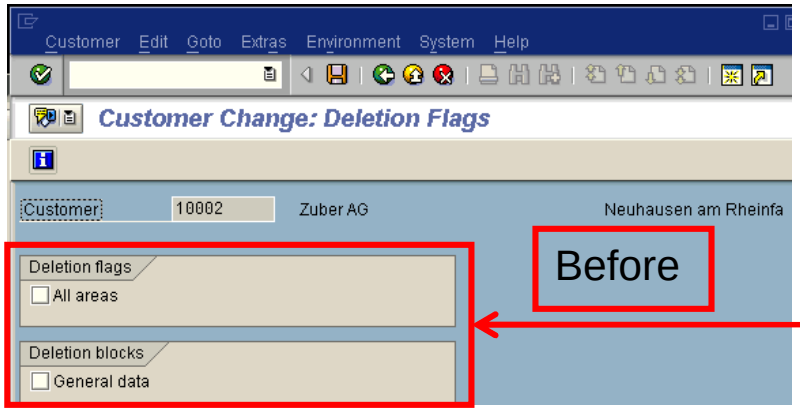
SAP Transaction Code XD02 = Change Customer Records

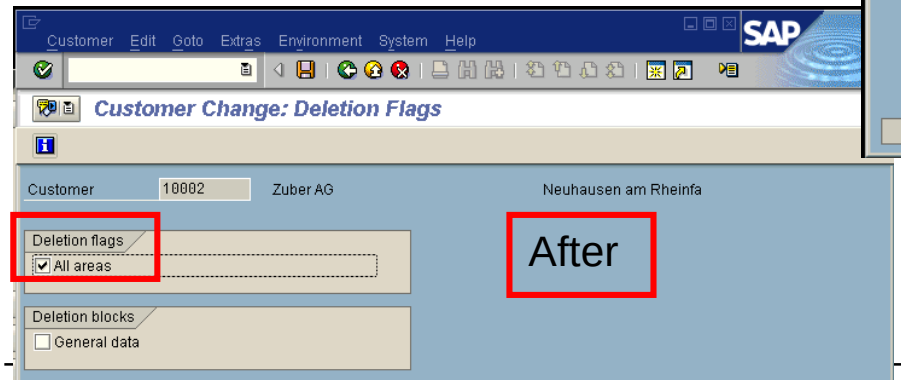


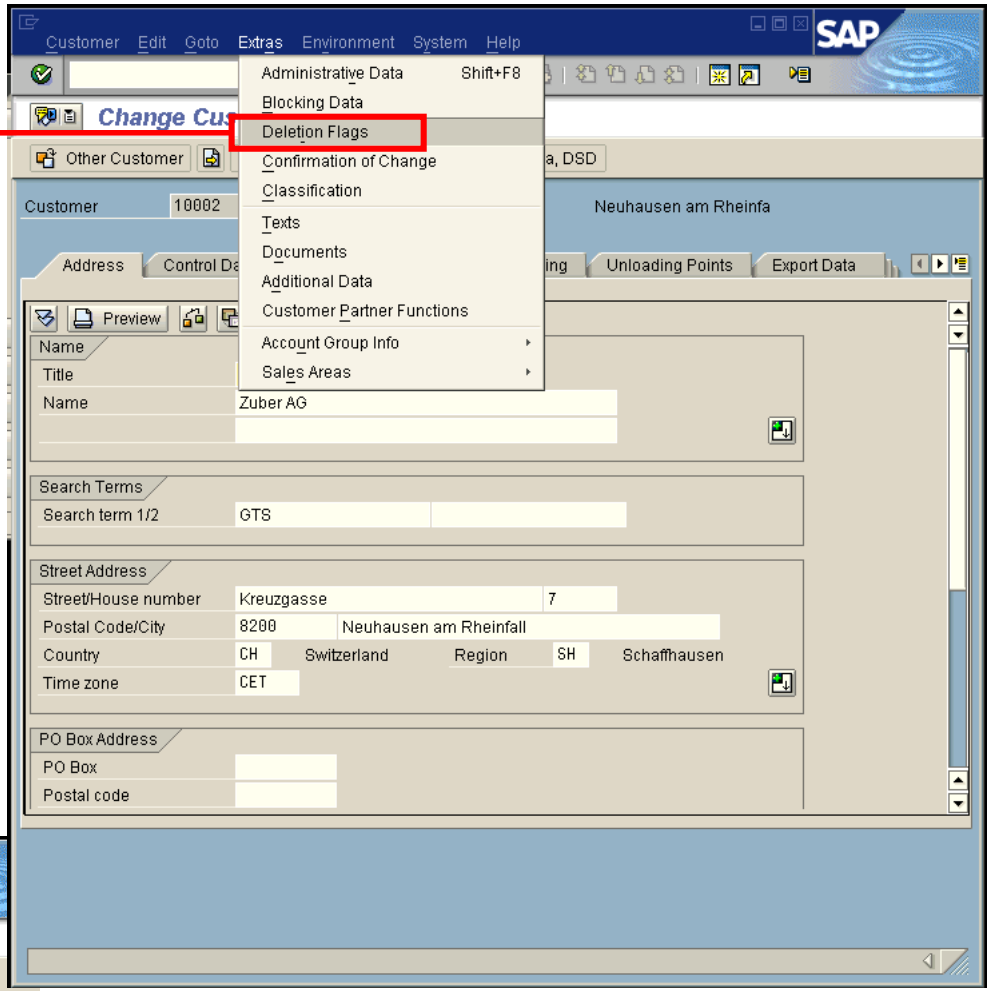
© 2013 IBM Corporation

Deleting a customer…

- If someone deletes a customer record, it ripples through the entire SAP system
- This could prevent you from closing your financials at the end of the quarter







© 2013 IBM Corporation

SAP Ripple Effect…Many Tables Are Affected By “Delete” Flag

- **52 Items…**

TRFCQOUT = tRFC Queue
ARFCSSTATE and ARFCSSDATA tables are used for outbound Transactional Remote Function Calls (tRFC)

SAP Auditing can be useful in troubleshooting SAP transactions, since you have the full history available…

Start Date:	2010-10-08 06:26:15	End Date:	2010-10-08 17:26:15
Aliases:	ON	ApplicationUserLike:	LIKE %
ClientIPLike:	LIKE %	DBuserLike:	LIKE %
FULLSQLLike:	LIKE %10002%	NetProtoLike:	LIKE %
ServerIPLike:	LIKE %106	ServerTypeLike:	LIKE %
SourceProgLike:	LIKE %		

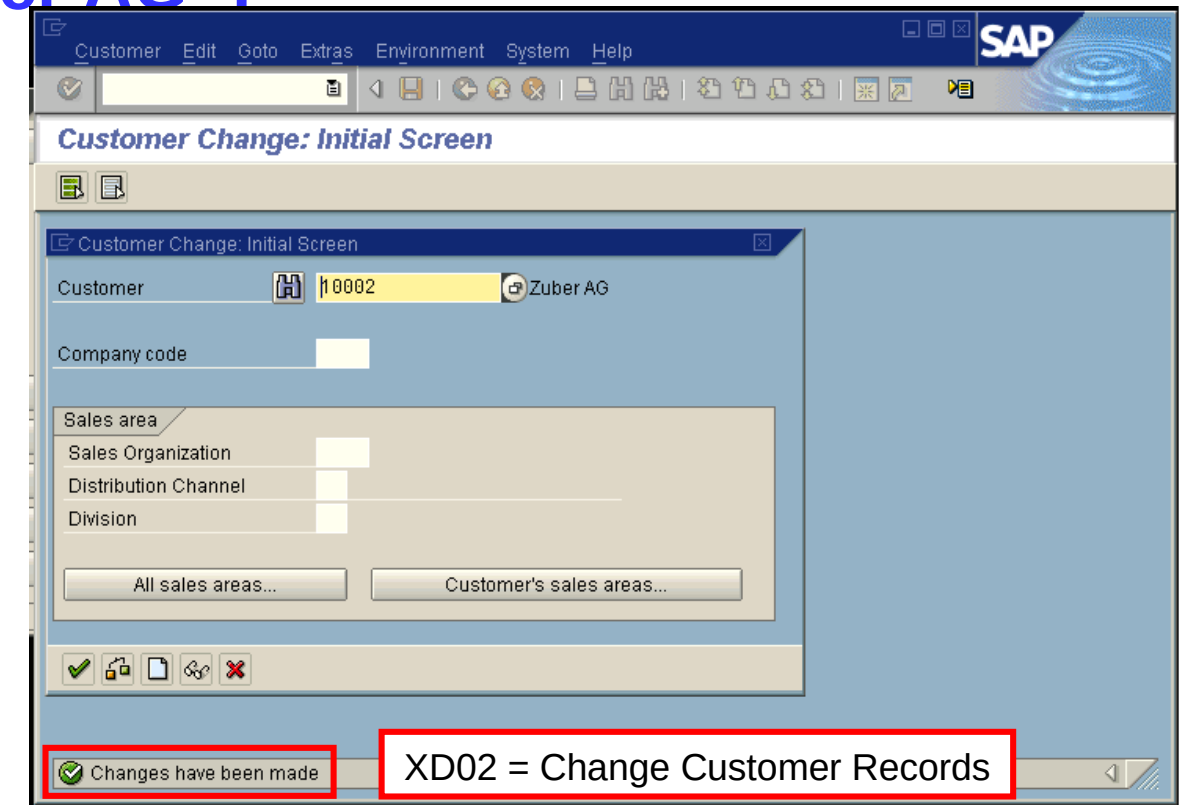
Timestamp	Client IP	Server IP	Network Protocol	Server Type	DB User Name	Application User	Source Program	Full Sql
2010-10-08 17:11:31.0	10.10.10.10	10.10.10.10	SHARED MEMORY	DB2	SAPSERVICEE6A	JOE	DISP+WORK.EXE	UPDATE "TRFCQOUT" SET "HPQNAME" = ' ' , "NOSEND" = ' ' , "QSTATE" = 'READY' , "QLOCKCNT" = '00000000000000000000000' , "QRFCUSER" = 'JOE' , "QRFCFNAM" = 'BAPI_CRM_SAVE' , "QRFCDATUM" = '20101008' , "QRFCUZEIT" = '153842' , "QLUWCNT" = '00000001' , "QMAILED" = ' ' , "ERRMESS" = 'Error when opening an RFC connection' WHERE "MANDT" = '800' AND "ARFCIPID" = '0946936A' AND "ARFCPID" = '0B00' AND "ARFCTIME" = '4CAF7342' AND "ARFCTIDCNT" = '0193' AND "QNAME" = 'R3AD_CUSTOME10002' AND "DEST" = 'DTZ_800' AND "QCOUNT" = '000012865667220000010000' -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(RSARFCSE , 180) -- SYSTEM(E6A , SAPE6A)
2010-10-08 17:11:31.0	10.10.10.10	10.10.10.10	SHARED MEMORY	DB2	SAPSERVICEE6A	JOE	DISP+WORK.EXE	UPDATE "ARFCSSTATE" SET "ARFCSTATE" = 'RECORDED' , "ARFCFNAM" = 'BAPI_CRM_SAVE' , "ARFCRETURN" = 'I' , "ARFCUZEIT" = '171131' , "ARFCDATUM" = '20101008' , "ARFCUSER" = 'JOE' , "ARFCRETRYS" = '0025' , "ARFCTCODE" = 'XD02' , "ARFCRHOST" = 'pud10wsa' , "ARFCMSG" = ' ' , "ARFCRESERV" = 'SAPMF02D 800 IR3AD_CUSTOME10002 000012865667220000010000 pud10wsapec6a_E6A_00 20101008153842 00000003 E' , "HASH" = null WHERE "ARFCIPID" = '0946936A' AND "ARFCPID" = '0B00' AND "ARFCTIME" = '4CAF7342' AND "ARFCTIDCNT" = '0193' AND "ARFCDEST" = 'DTZ_800' AND "ARFCLUWCNT" = '00000001' -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(RSARFCSE , 236) -- SYSTEM(E6A , SAPE6A)
2010-10-08 17:11:31.0	10.10.10.10	10.10.10.10	SHARED MEMORY	DB2	SAPSERVICEE6A	JOE	DISP+WORK.EXE	SELECT "ARFCIPID" , "ARFCPID" , "ARFCTIME" , "ARFCTIDCNT" , "QNAME" , "DEST" , "QCOUNT" , "QSTATE" FROM "TRFCQOUT" WHERE "MANDT" = '800' AND "QNAME" = 'R3AD_CUSTOME10002' AND "DEST" = 'DTZ_800' WITH UR -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLSQCWK , 3243) -- SYSTEM(E6A , SAPE6A)
2010-10-08 17:11:31.0	10.10.10.10	10.10.10.10	SHARED MEMORY	DB2	SAPSERVICEE6A	JOE	DISP+WORK.EXE	SELECT MIN("QCOUNT") FROM "TRFCQOUT" WHERE "MANDT" = '800' AND "QNAME" = 'R3AD_CUSTOME10002' AND "DEST" = 'DTZ_800' WITH UR -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLQRFC , 18174) -- SYSTEM(E6A , SAPE6A)

Records 1 to 4 of 52

© 2013 IBM Corporation

Who Changed “Zuber AG”?

- **Simplify auditing…**
- **Can you identify who changed data in your SAP system?**
- **Was it authorized?**
- **Do you have appropriate documentation?**



Start Date: **2010-10-08 04:42:17** End Date: **2010-10-08 15:42:17**
Aliases: **ON** ApplicationUserLike: **LIKE %**
ClientIPLike: **LIKE %** DBuserLike: **LIKE %**
FULLSQLLike: **LIKE %xd02%** NetProtoLike: **LIKE %**
ServerIPLike: **LIKE %106** ServerTypeLike: **LIKE %**
SourceProgLike: **LIKE %**

Joe changed at “Zuber AG” customer number 10002

Timestamp	Client IP	Server IP	Network Protocol	Server Type	DB User Name	Application User	Source Program	Full Sql
2010-10-08 15:38:43.0	10.10.10.10	10.10.10.10	SHARED MEMORY	DB2	SAPSERVICEE6A	JOE	DISP+WORK.EXE	UPDATE "ARFCSSTATE" SET "ARFCSTATE" = 'CPICERR' , "ARFCFNAM" = 'BAPI_CRM_SAVE' , "ARFCRETURN" = 'I' , "ARFCUZEIT" = '155343' , "ARFCDATUM" = '20101008' , "ARFCUSER" = 'JOE' , "ARFCRETRYS" = '0030' "ARFCTCODE" = 'XD02' "ARFCRHOST" = 'pud10wsa' "ARFCMSG" = 'Error when opening an RFC connection' , "ARFCRESERV" = 'SAPMF02D 800XIR3AD CUSTOME10002 00001286566722000001000 pud10wsapec6a_E6A_00 20101008153842 00000003 E' , "HASH" = null WHERE "ARFCIPID" = '0946936A' AND "ARFCPID" = '0B00' AND "ARFCTIME" = '4CAF7342' AND "ARFCTIDCNT" = '0193' AND "ARFCDEST" = 'DTZ_800' AND "ARFCLUWCNT" = '00000001' -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLARFC , 5955) -- SYSTEM(E6A , SAPE6A)

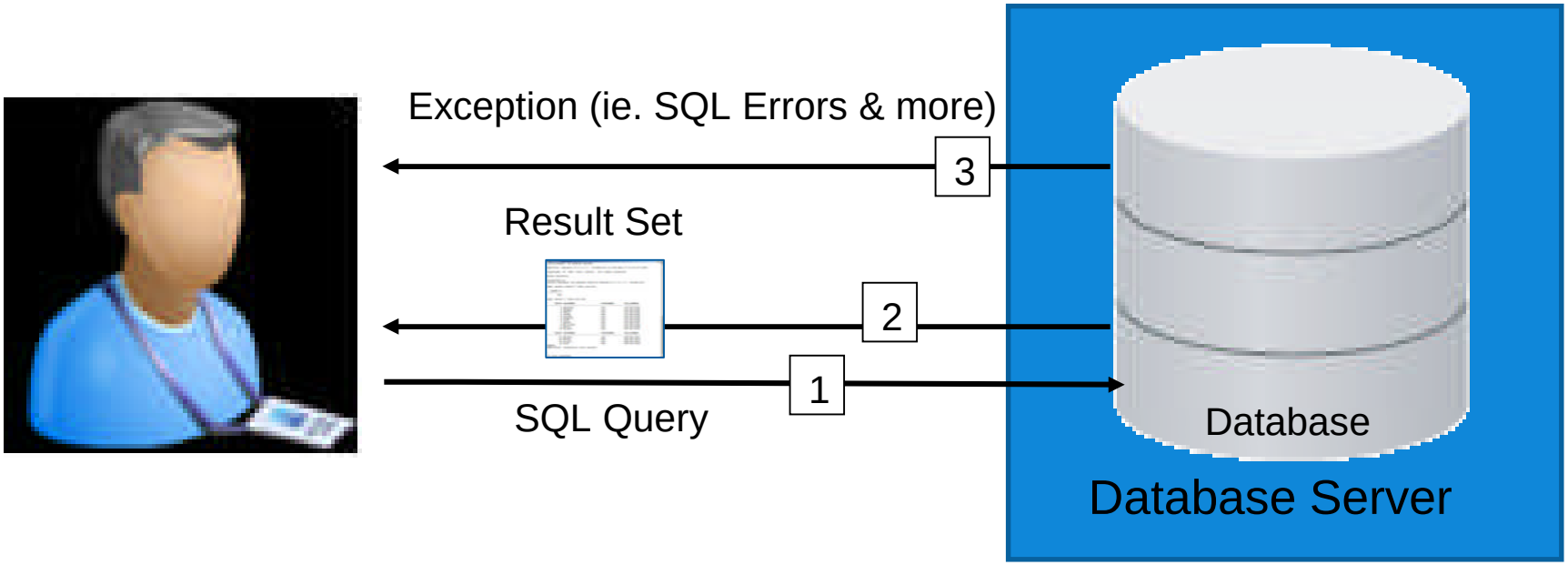
© 2013 IBM Corporation

InfoSphere Guardium - PCI SAP Protection

- Guardium has predefined PCI Policies for SAP systems
- These policies help protect against a variety of security issues
- Rules can be customized
- InfoSphere Guardium “Database Protection Knowledge Base” automatically populates policies for relevant SAP PCI tables (“we’ve done the work for you”)
- There are three components in the policies

© 2013 IBM Corporation

Good SAP Policies Cover 3 Types of Rules

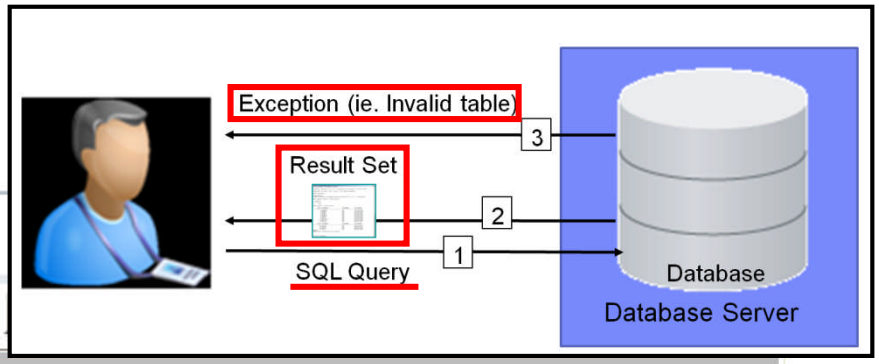


There are three types of rules:

1. An access rule applies to client requests
2. An extrusion rule evaluates data returned by the server
3. An exception rule evaluates exceptions returned by the server

© 2013 IBM Corporation

SAP PCI Policy Overview



Policy Rules

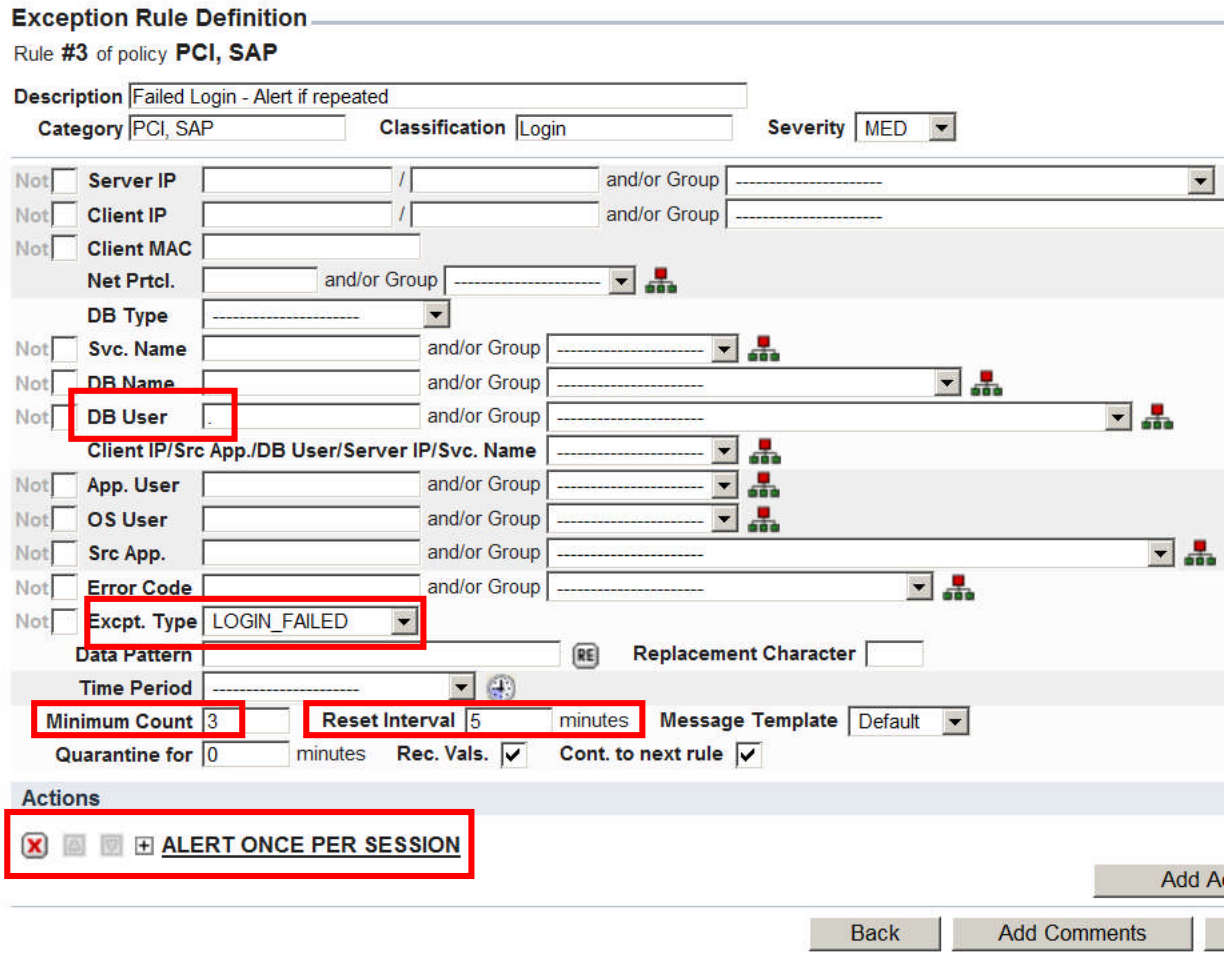
- PCI, SAP Production

Expand All | Collapse All | Select All

1	Access Rule: Non SAP DB Server - Ignore
2	Exception Rule: Failed Login - Log Violation
3	Exception Rule: Failed Login - Alert if repeated
4	Exception Rule: SQL Error - Log
5	Exception Rule: SQL Error - Alert on Risk Indicative errors
6	Access Rule: Selects Commands, Not APP Users, Cardholder SAP Objects - Log Full Details
7	Access Rule: DDL Commands, Cardholder SAP Objects - Log Full Details
8	Access Rule: Suspicious Users - Log Full Details
9	Access Rule: Suspicious Users, Cardholder SAP Objects - Log Info
10	Access Rule: Grant Commands, Cardholder SAP Objects - Log INFO
11	Access Rule: DDL Commands, Cardholder SAP Objects - Log INFO
12	Access Rule: DML Commands - Allow
13	Access Rule: guardium://CREDIT_CARD , Unauthorized - Violation
14	Access Rule: guardium://PCI_TRACK_DATA , Unauthorized Users - Violation
15	Access Rule: Unauthorized Clients access Cardholder SAP Objects - Alert
16	Access Rule: Unauthorized Users on Cardholder SAP Objects - Alert
17	Extrusion Rule: Credit Card Numbers, Unauthorized Users - Log Violation
18	Extrusion Rule: PCI Track Data, Unauthorized Users - Log Violation

© 2013 IBM Corporation

Alert On Failed Login (Exception Rule)

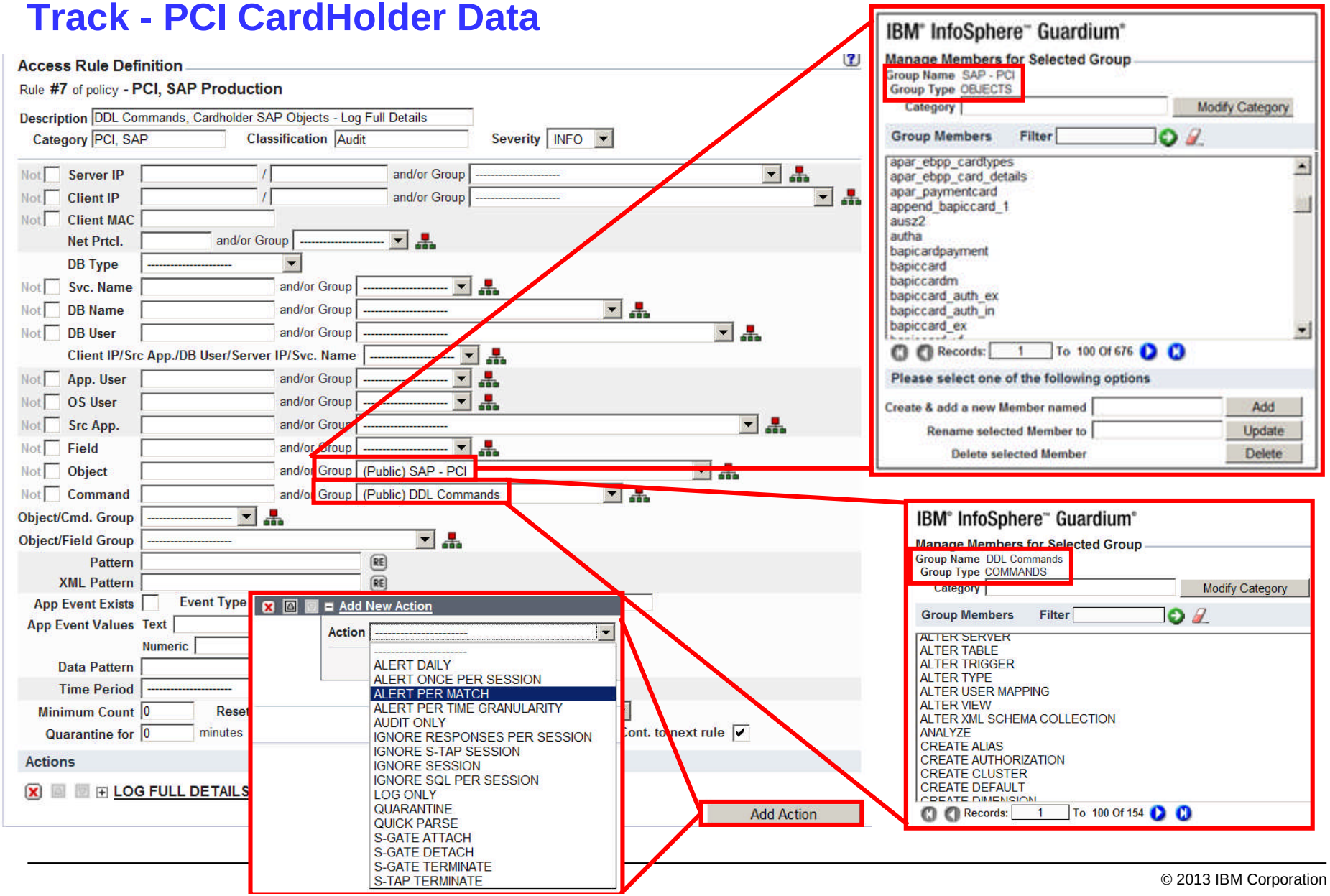


- **DB User = “.”**
  - This means the same database user
- **Excpt Type = Failed Logins**
- **Min Count = How often**
- **Reset Interval = Between what time period**
- **Action = Alert**
- **So…Alert on 3 Failed Login attempts from the same user if they occur 3 times within a 5 minute interval**

You should not have 3 failed logins on a production system!

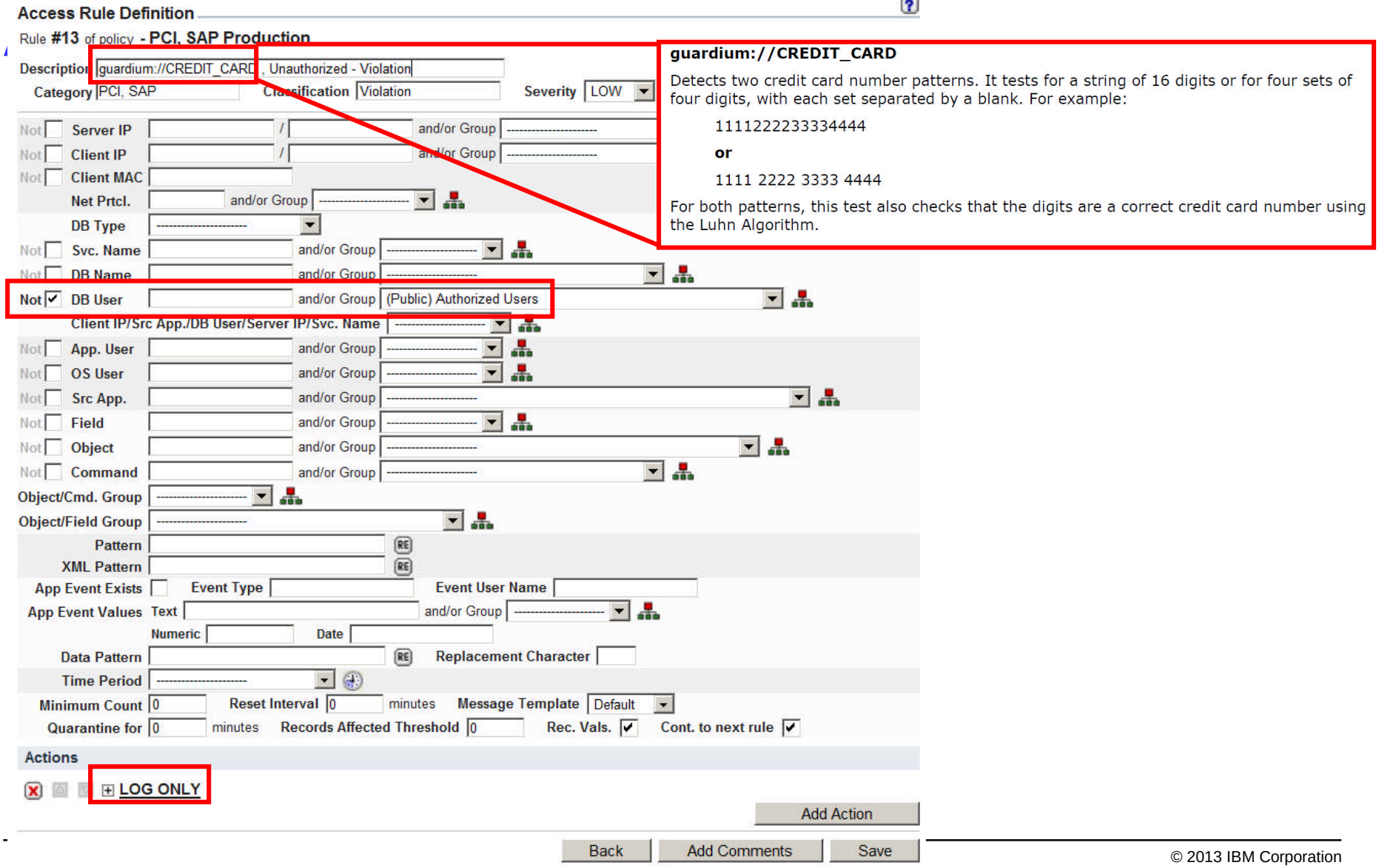
© 2013 IBM Corporation

SAP PreDefined PCI Policy Rule (Access Rule) Track - PCI CardHolder Data



© 2013 IBM Corporation

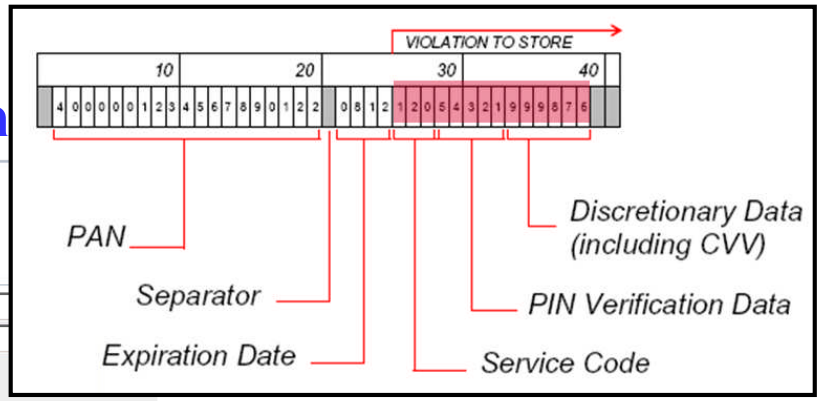
Unauthorized Users Accessing Credit Cards
Guardium Will Verifv Credit Card Validity With Luhn



© 2013 IBM Corporation

PCI Track Data…

Guardium Tracks PCI “Track Data



guardium://PCI_TRACK_DATA

Detects two patterns of magnetic stripe data. The first pattern consists of a semi-colon (;), 16 digits, an equal sign (=), 20 digits, and a question mark (?). For example:

;1111222233334444=11112222333344445555?

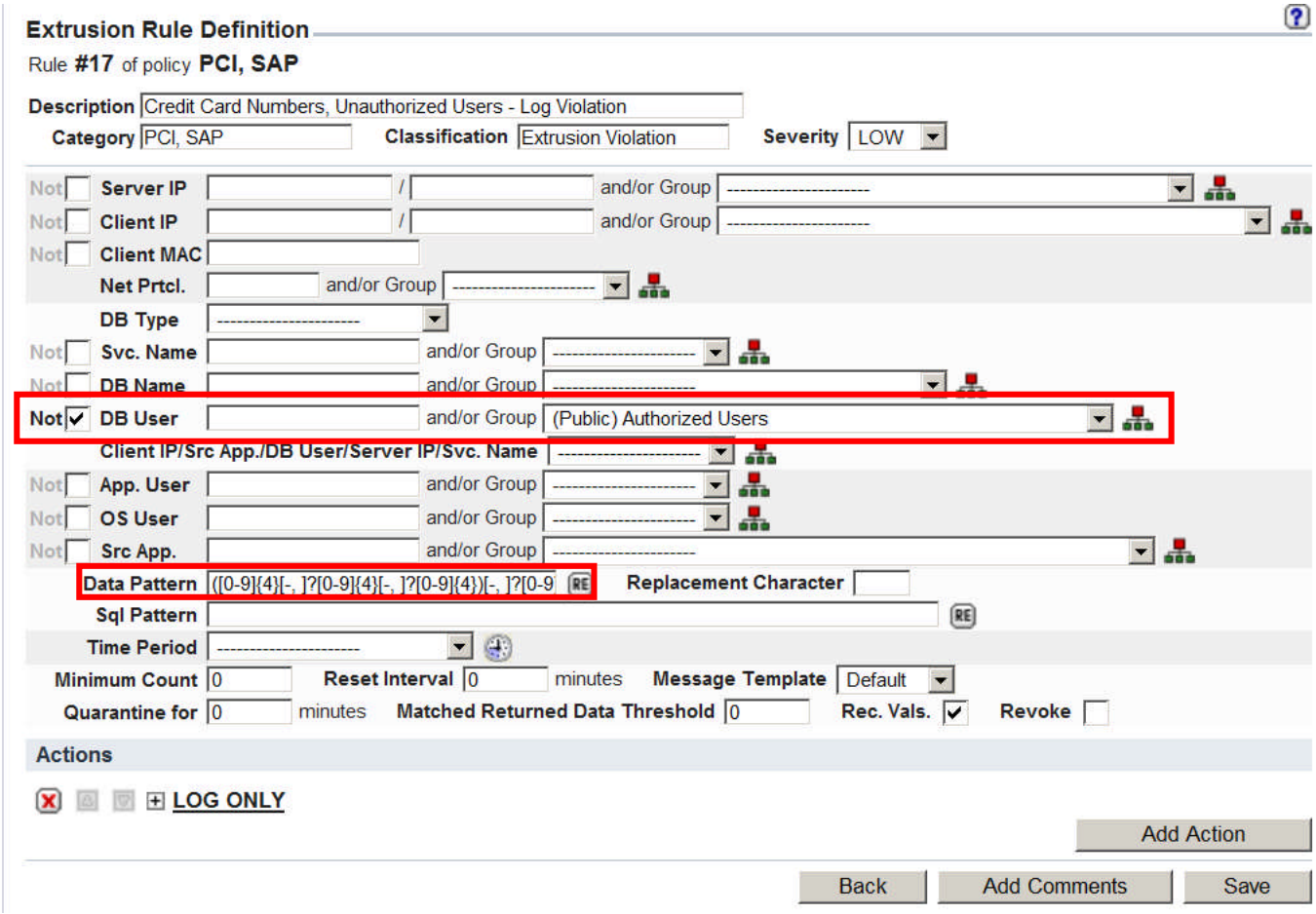
The second pattern consists of a percent sign (%), the character B, 16 digits, a carat (^), a variable-length character string terminated by a forward slash (/), a second variable-length character string terminated by a carat (^), 31 digits, and a question mark (?). For example:

%B1111222233334444^xxx/xxxx x^11112222333344445555666677778888?

- ***DO NOT store the full contents of any track from the magnetic stripe***
- ***DO NOT store the card-validation code (three-digit or four-digit value printed on the front or back of a payment card (e.g., CVV2 and CVC2 data))***
- ***DO NOT store the PIN Verification Value (PVV)***

© 2013 IBM Corporation

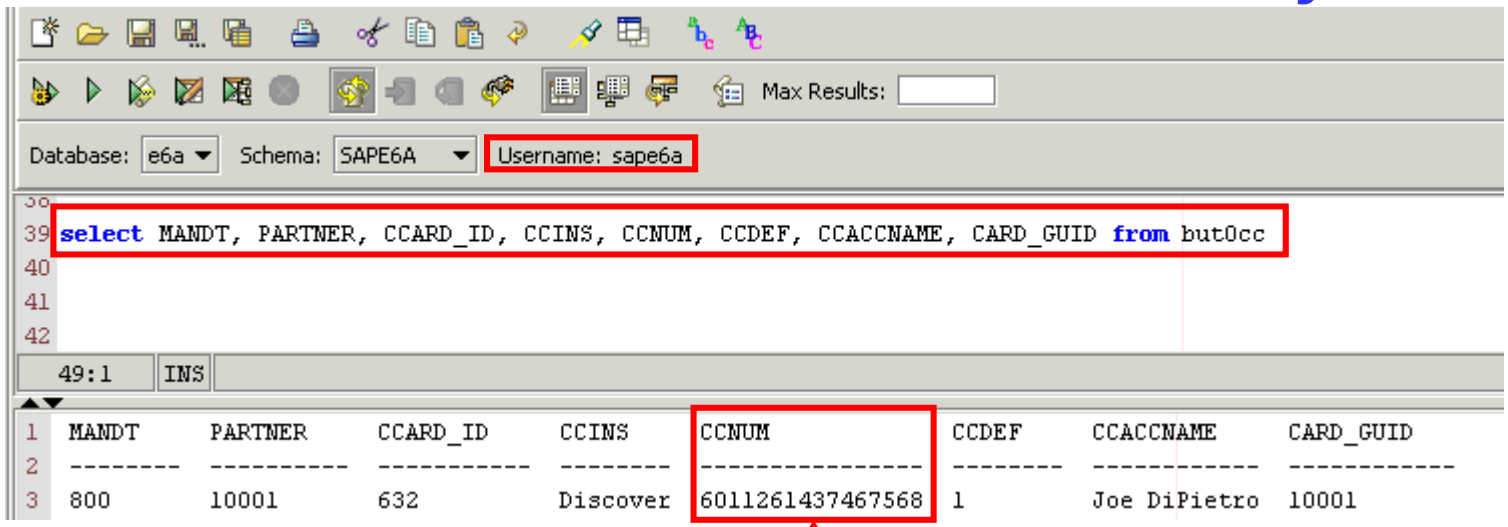
Unauthorized Creditcard Access (Extrusion Rule)



- **If you are not an authorized user accessing creditcard information, log a policy violation**

© 2013 IBM Corporation

One Unauthorized Access Violates 4 Security Rules



guardium://CREDIT_CARD

Detects two credit card number patterns. It tests for a string of 16 digits or for four sets of four digits, with each set separated by a blank. For example:

1111222233334444

or

1111 2222 3333 4444

For both patterns, this test also checks that the digits are a correct credit card number using the Luhn Algorithm.

Policy Violations Details

Start Date: **2010-10-13 16:48:07** End Date: **2010-10-13 21:48:07**
Aliases: **ON** ServerIPLike: **LIKE %**

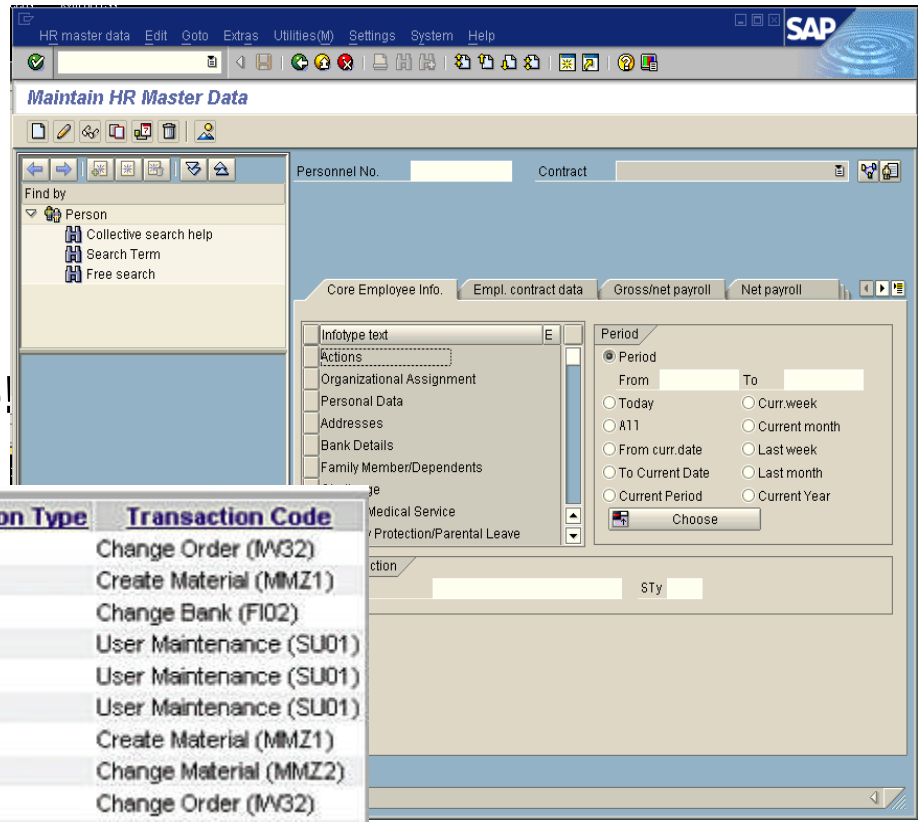
Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description
2010-10-13 21:44:14.0	PCI, SAP	Credit Card Numbers, Unauthorized Users - Log Violation	10.24.131.133	10.10.10.10	SAPE6A	select MANDT, PARTNER, CCARD_ID, CCINS, CCNUM, CCDEF, CCACCNAME, CARD_GUID from but0cc Extrusion Values: **********7568	LOW
2010-10-13 21:44:14.0	PCI, SAP	guardium://CREDIT_CARD , Unauthorized - Violation	10.24.131.133	10.10.10.10	SAPE6A	select MANDT, PARTNER, CCARD_ID, CCINS, CCNUM, CCDEF, CCACCNAME, CARD_GUID from but0cc	LOW
2010-10-13 21:44:14.0	PCI, SAP	Unauthorized Users on Cardholder SAP Objects - Alert	10.24.131.133	10.10.10.10	SAPE6A	select MANDT, PARTNER, CCARD_ID, CCINS, CCNUM, CCDEF, CCACCNAME, CARD_GUID from but0cc	MED
2010-10-13 21:44:14.0	PCI, SAP	Unauthorized Clients access Cardholder SAP Objects - Alert	10.24.131.133	10.10.10.10	SAPE6A	select MANDT, PARTNER, CCARD_ID, CCINS, CCNUM, CCDEF, CCACCNAME, CARD_GUID from but0cc	MED

© 2013 IBM Corporation

SAP Highlights

- **SAP is a very complicated system with very good documentation**
- **From an audit perspective there is good information to help identify some of the basic information you need to secure your SAP systems**
- **More detailed information now available about SAP users**
  - Goes beyond SAP transaction logs
- **Easier to detect fraud**
- **No application changes required**

- **IBM InfoSphere Guardium can help!**



Application Type	User	Item Name	Operation Type	Transaction Code
SAP	HANSSCHMIDT	HFPT_COEJA_PP_ORDER_RPSCO_V2	Query	Change Order (MV32)
SAP	HANSSCHMIDT	MATERIAL	Update	Create Material (MMZ1)
SAP	VOLKERHIESTERMANN	BANK	Update	Change Bank (FI02)
SAP	HANSSCHMIDT	ADRESSE3	Update	User Maintenance (SU01)
SAP	GEORGHELD	ADRESSE3	Update	User Maintenance (SU01)
SAP	GEORGHELD	ADRESSE3	Update	User Maintenance (SU01)
SAP	HANSSCHMIDT	MATERIAL	Update	Create Material (MMZ1)
SAP	HANSSCHMIDT	MATERIAL	Update	Change Material (MMZ2)
SAP	HANSSCHMIDT	ORDER	Update	Change Order (MV32)

© 2013 IBM Corporation

Case Study: Securing SAP & Siebel with 239% ROI & <6 Months Payback

- **Who: F500 consumer food manufacturer ($15B revenue)**
- **Need: Secure SAP & Siebel data for SOX**
  - Enforce change controls & implement consistent auditing across platforms
- **Environment**
  - SAP, Siebel, Manugistics, IT2 + 21 other Key Financial Systems (KFS)
  - Oracle & IBM DB2 on AIX; SQL Server on Windows
- **Results: 239% ROI & 5.9 months payback, plus:**
  - **Proactive security:** Real-time alert when changes made to critical tables
  - **Simplified compliance**: Passed 4 audits (internal & external)
    - *"The ability to associate changes with a ticket number makes our job a lot easier … which is something the auditors ask about."* [Lead Security Analyst]
  - **Strategic focus on data security**
    - *"There's a new and sharper focus on database security within the IT organization. Security is more top-of-mind among IT operations people and other staff such as developers."*

Commissioned Forrester Consulting Case Study

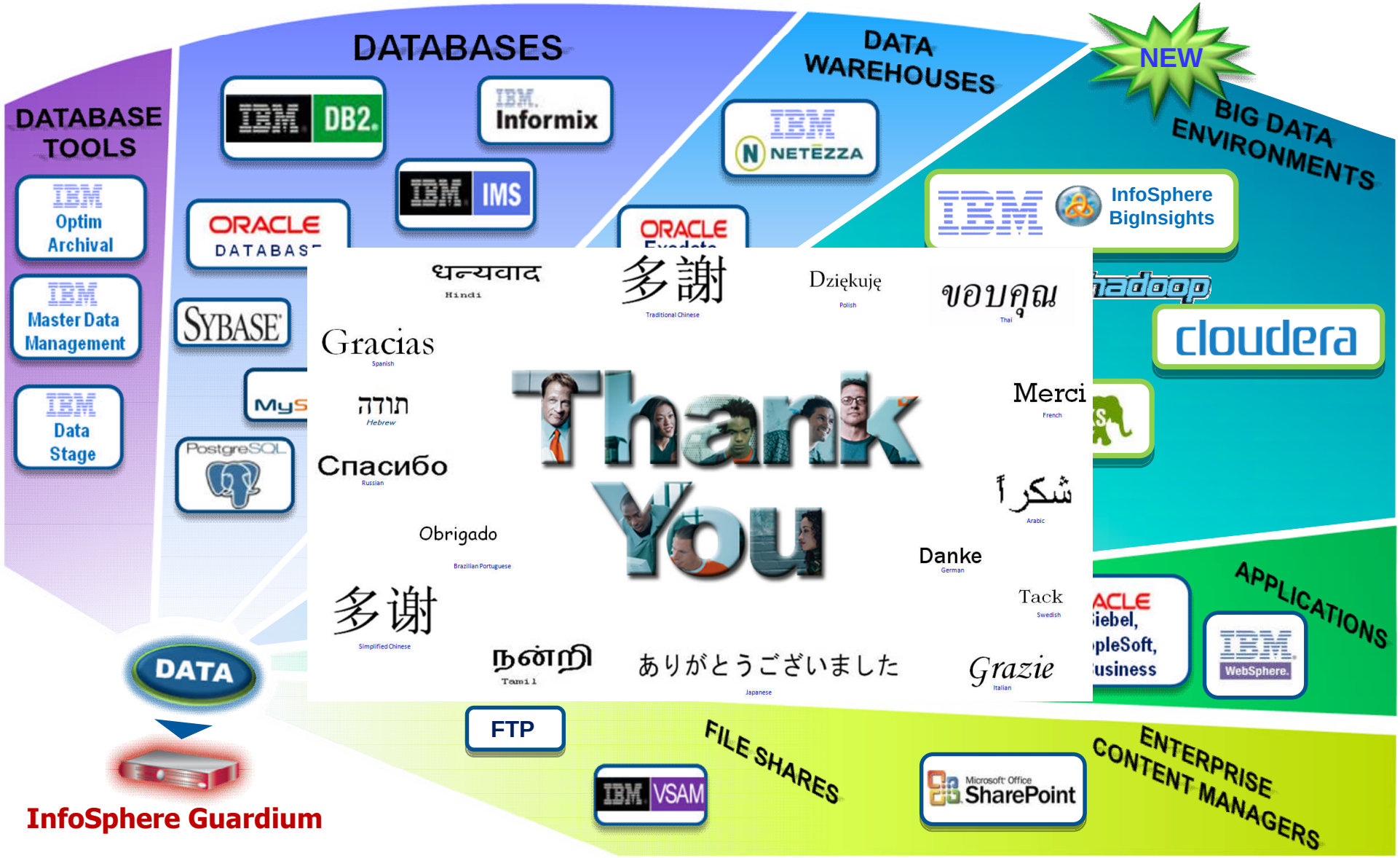
© 2013 IBM Corporation

Summary & Conclusions

- **Basic database security is insufficient to secure high-value databases**
  - Ineffective against privileged users or end-users violating corporate policies
  - No real-time monitoring to immediately detect or block unauthorized access
  - Inability to detect fraud at application layer (SAP, PeopleSoft, etc.)
  - No VA, data discovery, leakage detection, file integrity monitoring, …
  - No data masking to de-identify data in test/dev environments
  - Requires unique policies for each DBMS platform
- **IBM/Guardium is the most widely-deployed solution, with ongoing feedback from the most demanding data center environments worldwide**
  - Scalable enterprise architecture
  - Broad heterogeneous support
  - Deep automation to reduce workload
  - Holistic (comprehensive) approach
  - Available as virtual appliance for cloud environments

© 2013 IBM Corporation

Real-Time Application & Data Activity Monitoring…



© 2013 IBM Corporation

धन्यवाद
Hindi

多謝
Traditional Chinese

Dziękuję
Polish

ขอบคุณ
Thai

Gracias
Spanish

תודה
Hebrew

Merci
French

Спасибо
Russian

شكراً
Arabic

Obrigado
Brazilian Portuguese

Danke
German

多谢
Simplified Chinese

Tack
Swedish

நன்றி
Tamil

ありがとうございました
Japanese

Grazie
Italian

© 2013 IBM Corporation

Information, training, and community

- InfoSphere Guardium Tech Talks – at least one per month. Suggestions welcome!
- InfoSphere Guardium YouTube Channel – includes overviews, technical demos, tech talk replays
- InfoSphere Guardium newsletter
- developerWorks forum (very active)
- Guardium DAM User Group on Linked-In (very active)
- Community on developerWorks (includes discussion forum, content and links to a myriad of sources, developerWorks articles, tech talk materials and schedules)
- Guardium Info Center (Installation, System Z S-TAPs, how-tos, more to come)
- Technical training courses (classroom and self-paced)

InfoSphere Guardium Virtual User Group. Open, technical discussions with other users. Not recorded!

Send a note to **bamealm@us.ibm.com** if interested.

@2013 IBM Corporation

Reminder: Guardium Tech Talks

Next tech talk: How to audit and protect SAP systems with InfoSphere Guardium Data Activity Monitor

Speakers: Peter Mandel and Ernie Mancill

Date &Time: Thursday, October 17, 2013

11:30 AM Eastern (75 minutes)

Register here: http://bit.ly/156DCVX

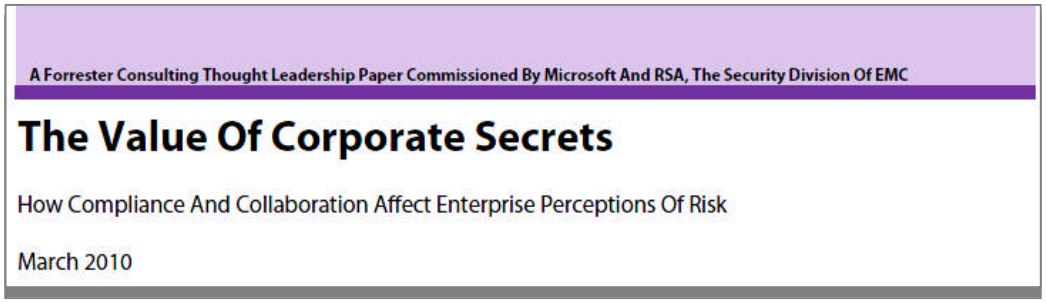
- Link to more information about this and upcoming tech talks can be found on the InfoSpere Guardium developerWorks community: http://ibm.co/Wh9x0o
- Please submit a comment on this page for ideas for tech talk topics.

© 2013 IBM Corporation

Background Slides

© 2013 IBM Corporation

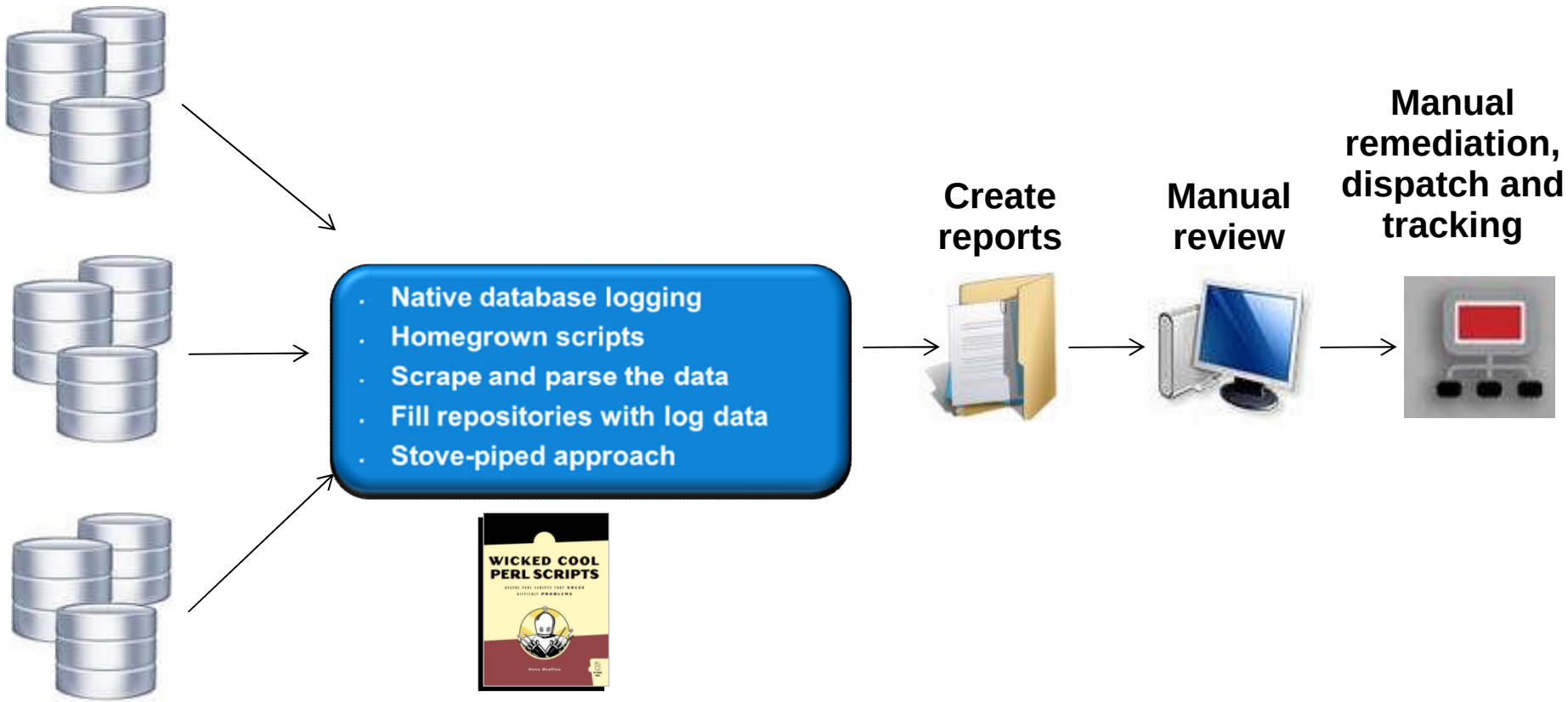
Cost of a Data Breach



- **Forrester survey of 305 IT decision makers**
- **Secrets (e.g., strategic plans) are twice as valuable as custodial data (personal information, credit card data, etc.)**
  - 2/3 of value in corporate information portfolio from non-regulated data (secrets)
- **Companies focus mainly on preventing accidents (email, etc.)**
  - But deliberate theft of information by employees is much more costly
  - Damage caused by rogue IT administrator = $482K (average)
  - Average cost of accidental leakage = $12K
- **Most CISOs don't really know if their controls really work**
- **Note: Survey does not address other costs such as fines**
  - Australian bank was fined $500K by VISA
  - Heartland breach cost = $140M

© 2013 IBM Corporation

What Database Audit Tools are Enterprises Using Today?



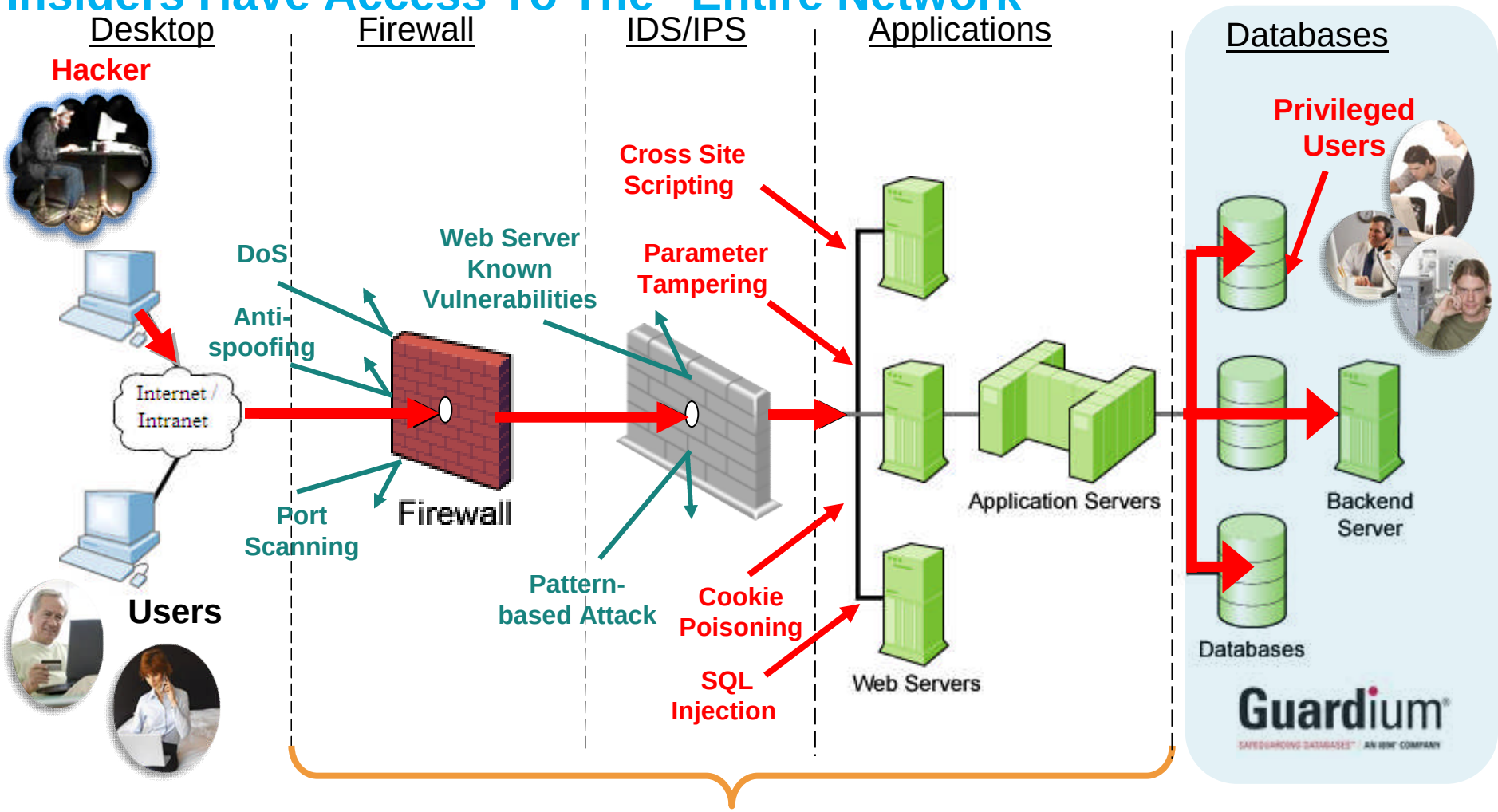
© 2013 IBM Corporation

What Are the Challenges with Current Approaches?

- No separation of duties -- DBAs & hackers can easily tamper with logs to cover their tracks
- Performance impact of native logging on the DBMS
- Limited scope & granularity of log data
- Not real-time
- No preventive controls
- Another data store to secure and manage ($$$)
- Inconsistent policies across apps, DBMS platforms, compliance initiatives
- Can’t identify end-user fraud for connection-pooled applications that use generic service accounts (SAP, PeopleSoft, etc.)
- Lack of DBMS expertise on security teams
- Last-minute audit scrambles -- significant labor cost to clean & review data, create reports, maintain oversight processes

© 2013 IBM Corporation

Defense in Depth, but…
Insiders Have Access To The "Entire Network"



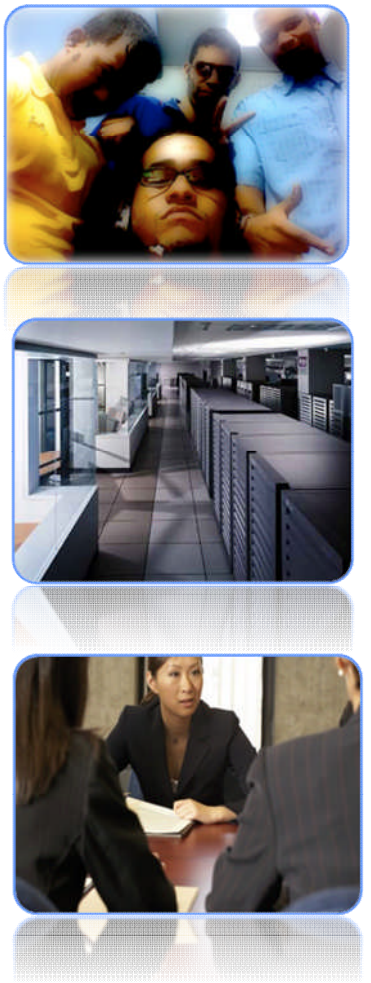
Reality: Most of the front end security layer protection cannot stop all the threat vectors ➔
Need the last layer of protection at the data level for Privilege Users!!

© 2013 IBM Corporation

Key Business Drivers for Database Activity Monitoring (DAM)

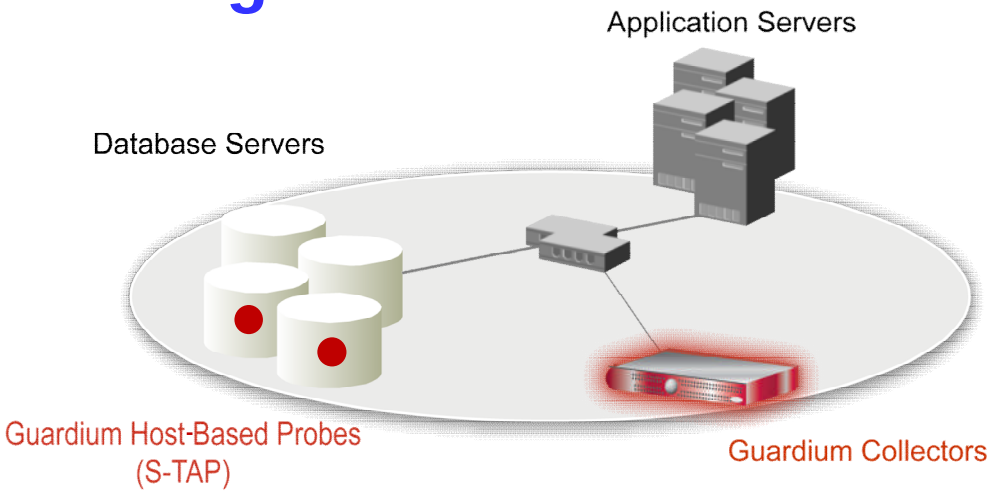
Continuously Monitor All Access to Sensitive Data:

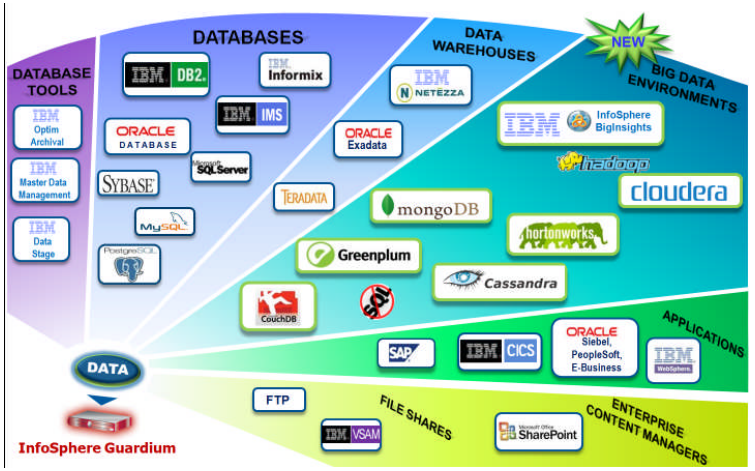
1. **Prevent data breaches**
   - Cybercriminals & rogue insiders
   - Protect customer data & corporate secrets (IP)
2. **Minimize risk & assure data governance**
   - Prevent unauthorized changes to sensitive data by privileged users
3. **Reduce audit costs**
   - Automated, continuous controls
   - Simplified audit & security processes
   - *… without performance impact or changes to databases or applications*



© 2013 IBM Corporation

Non-Invasive, Real-Time Database Security & Monitoring





- Continuously monitors all database activities (including local access by superusers)
- Heterogeneous, cross-DBMS solution
- Does not rely on native DBMS logs
- Minimal performance impact
- No DBMS or application changes
- Supports Separation of Duties
- Activity logs can't be erased by attackers or DBAs
- Automated compliance reporting, sign-offs & escalations (SOX, PCI, NIST, etc.)
- Granular, real-time policies & auditing
  - *Who, what, when, where, how*

© 2013 IBM Corporation