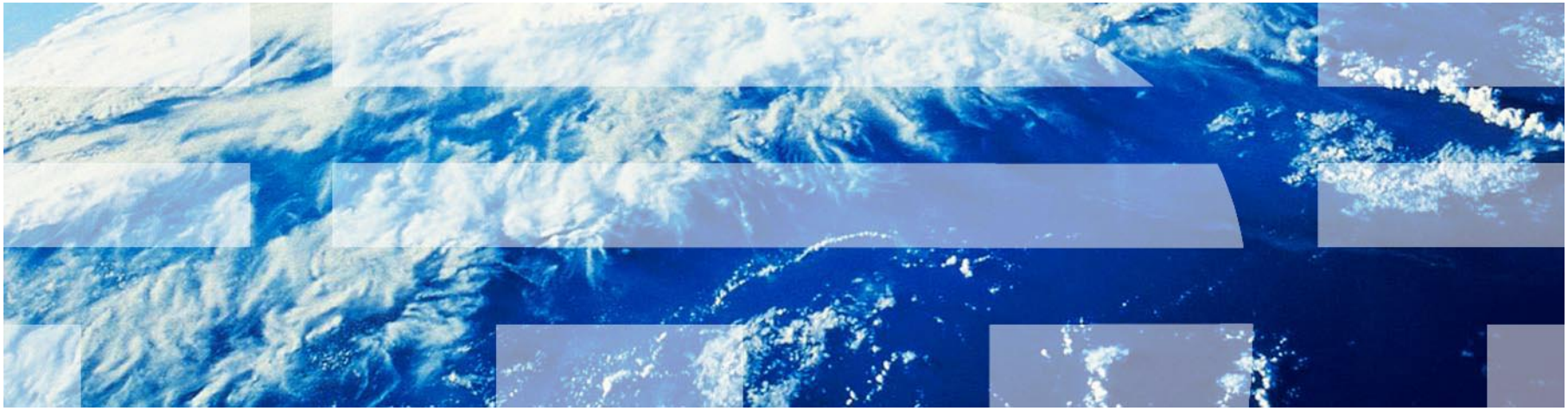
Introduction

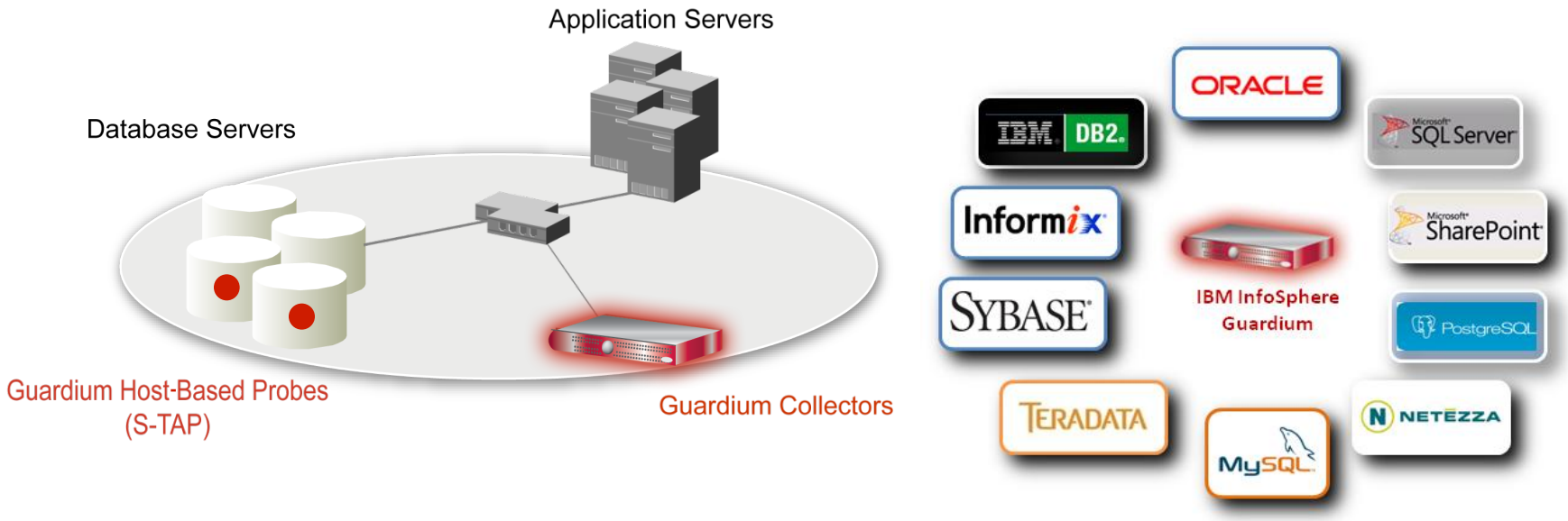
IBM InfoSphere Guardium



Fakhreddine EL Mourabiti
Guardium Technical Sales
Sout West Europe

fmourabiti@be.ibm.com

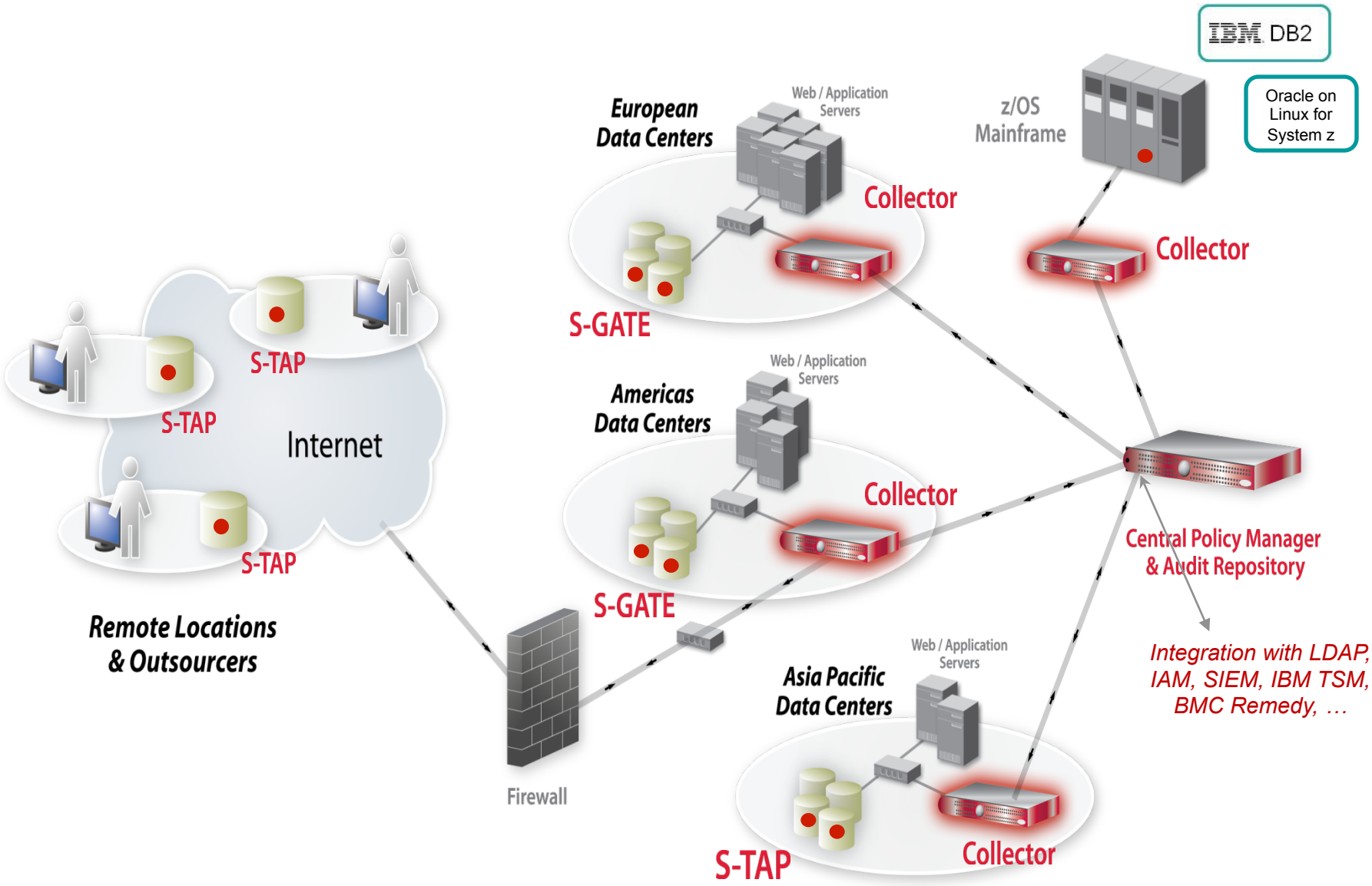
Non-Invasive, Real-Time Database Security & Monitoring



- 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***

Scalable Multi-Tier Architecture



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

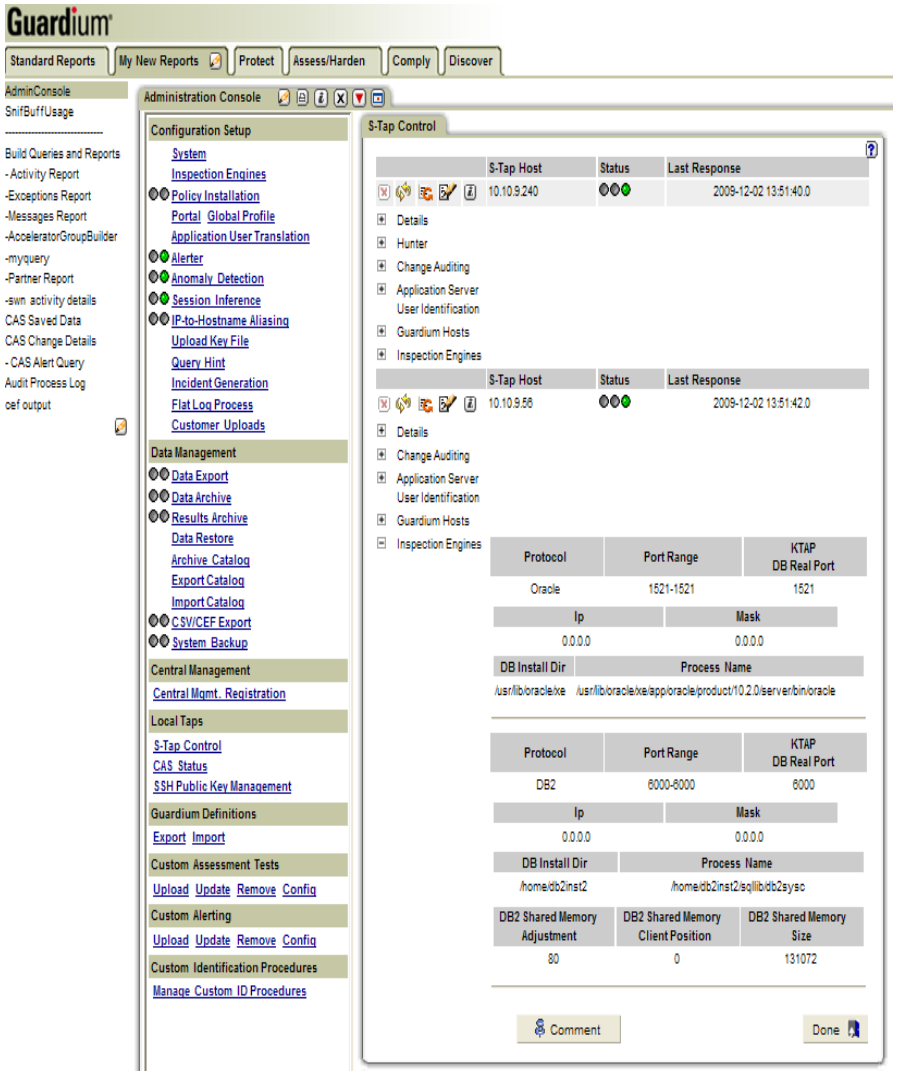
S-TAP – Design Goals

- 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?

Inspection Engine Overview

- 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

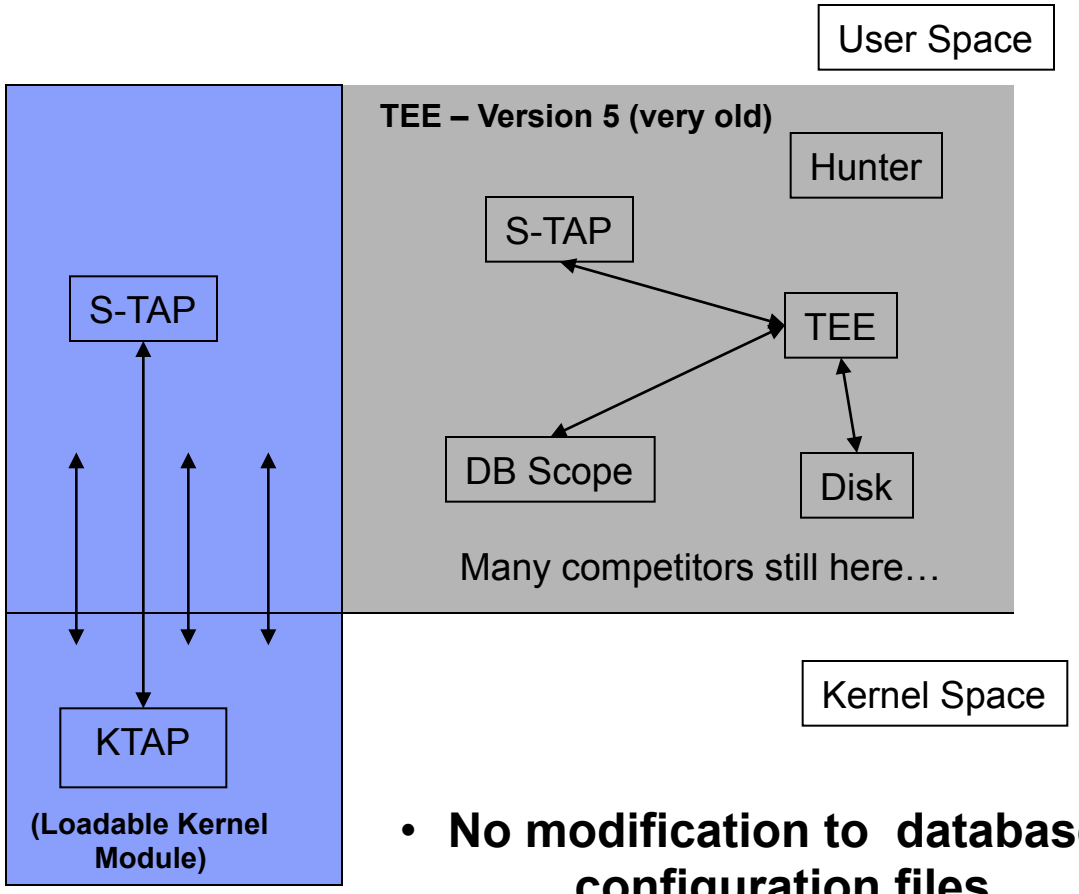


Kernel Modules…It's not easy…

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	9, 10	Both
Enterprise		
Solaris - SPARC	6, 8, 9, 10	Both
Solaris - Intel/AMD	10	Both
Windows	NT	32-Bit
	2000, 2003, 2008	Both

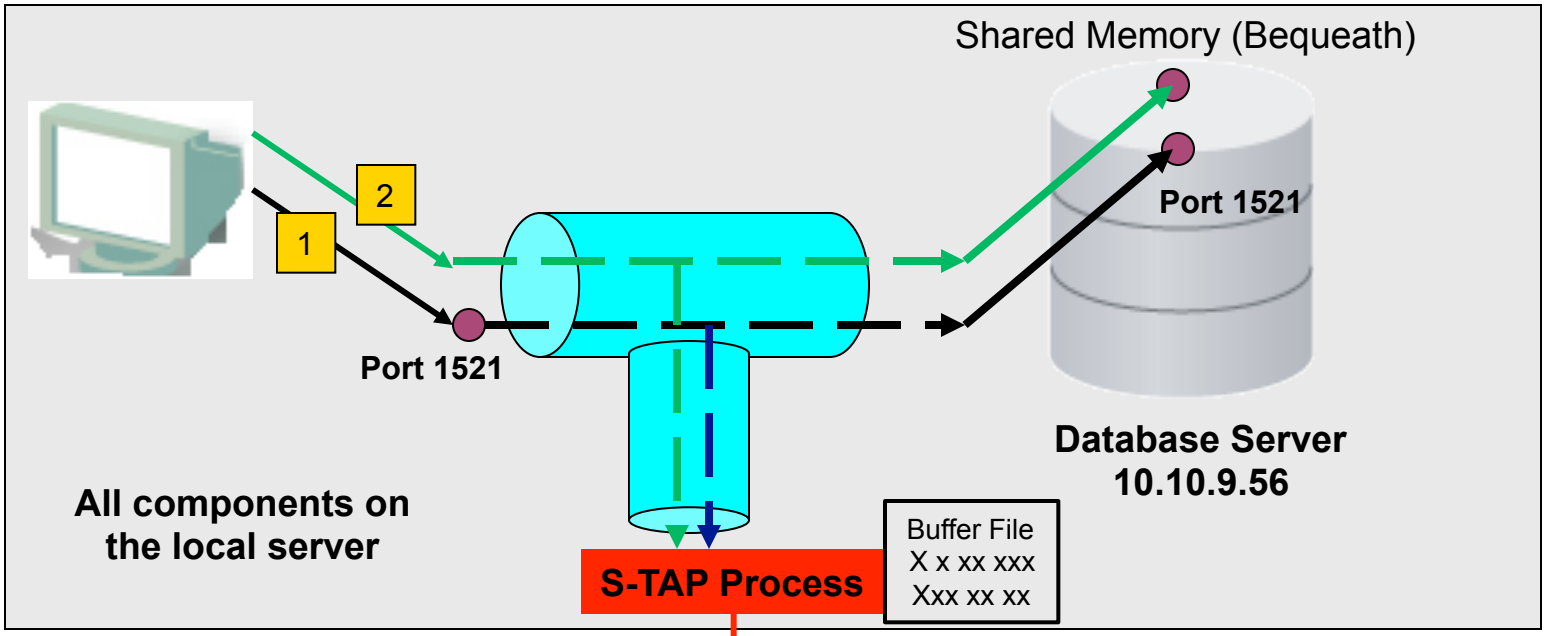
Supported Platform	Supported Versions
Oracle	8i, 9i, 10g (r1, r2), 11g, 11i
Microsoft SQL Server	2000, 2005, 2008
IBM DB2 UDB (Windows, Linux, Unix, z/Linux)	8, 8.2, 9.1, 9.5
IBM DB2 for z/OS	7, 8, 9, 9.5
IBM DB2 UDB for iSeries (AS/400)	V5R2, V5R3, V5R4, V6R1
IBM Informix	7, 8, 9, 10, 11
Sun MySQL	4.1,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

- User space – you need to modify database configuration files



- **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

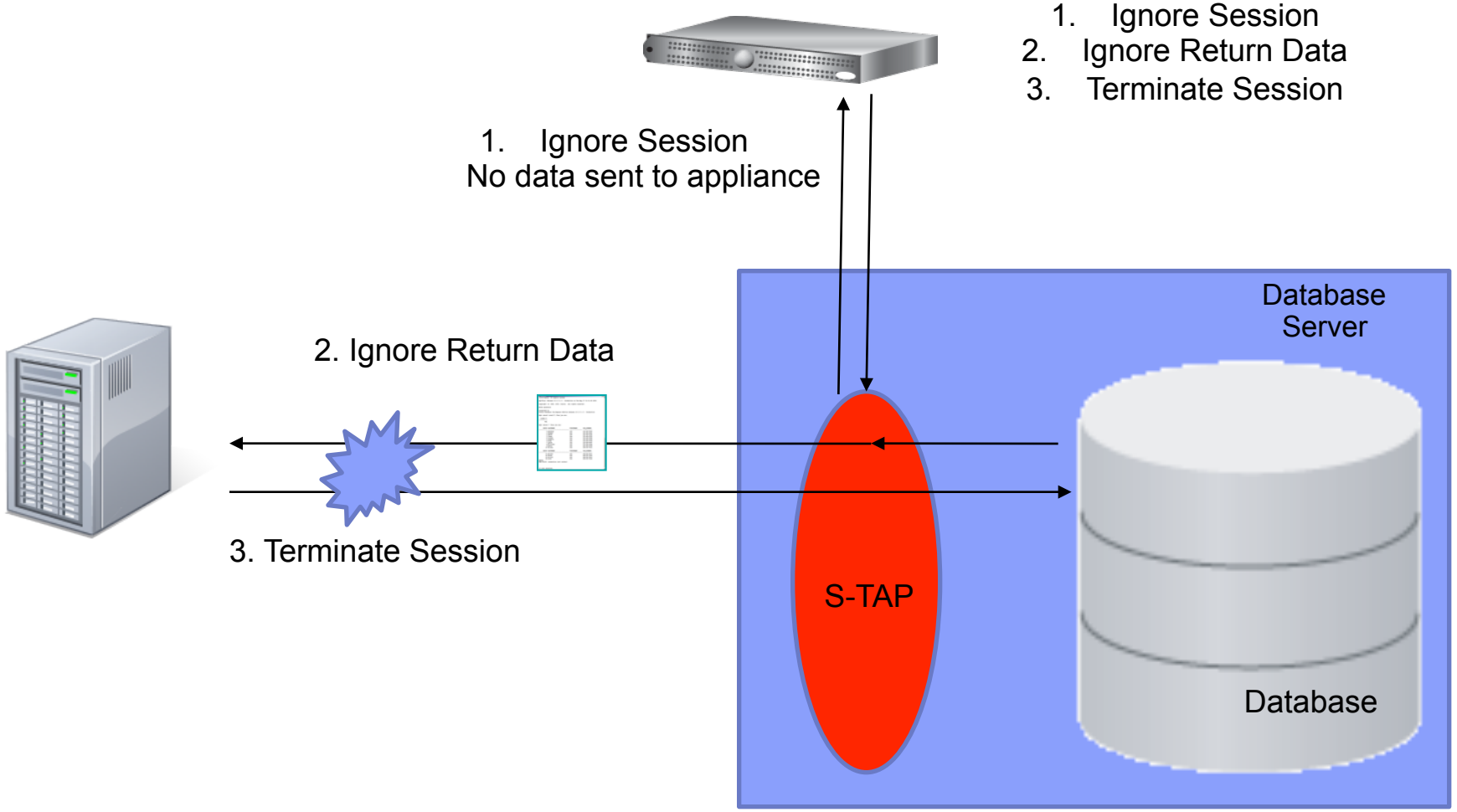
```
Shared Memory Access - Bequeath
```

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

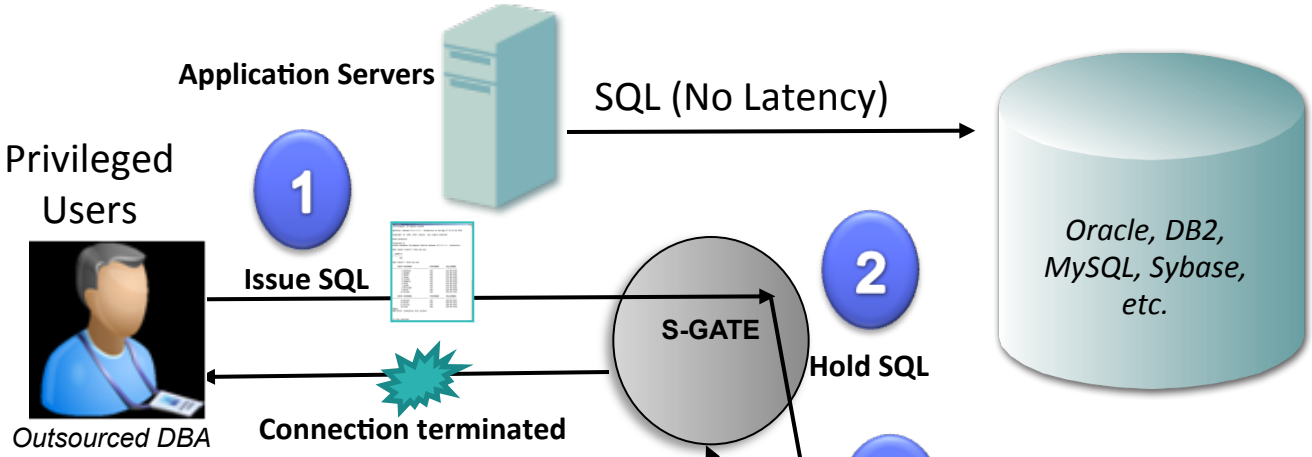
Guardium Appliance
10.10.9.245

S-TAP Architecture



S-GATE: Blocking Access Without Inline Appliances

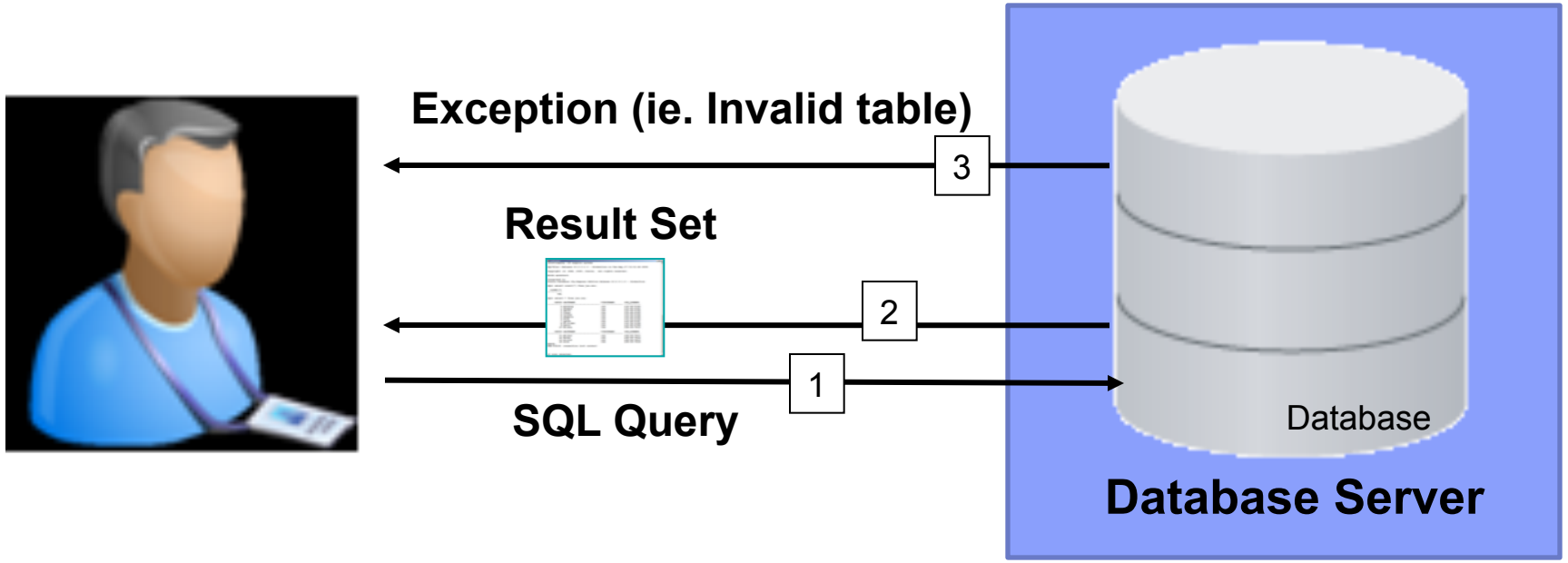
"DBMS software does not protect data from administrators, so DBAs today have the ability to view or steal confidential data stored in a database." Forrester, "Database Security: Market Overview," Feb. 2009




```
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

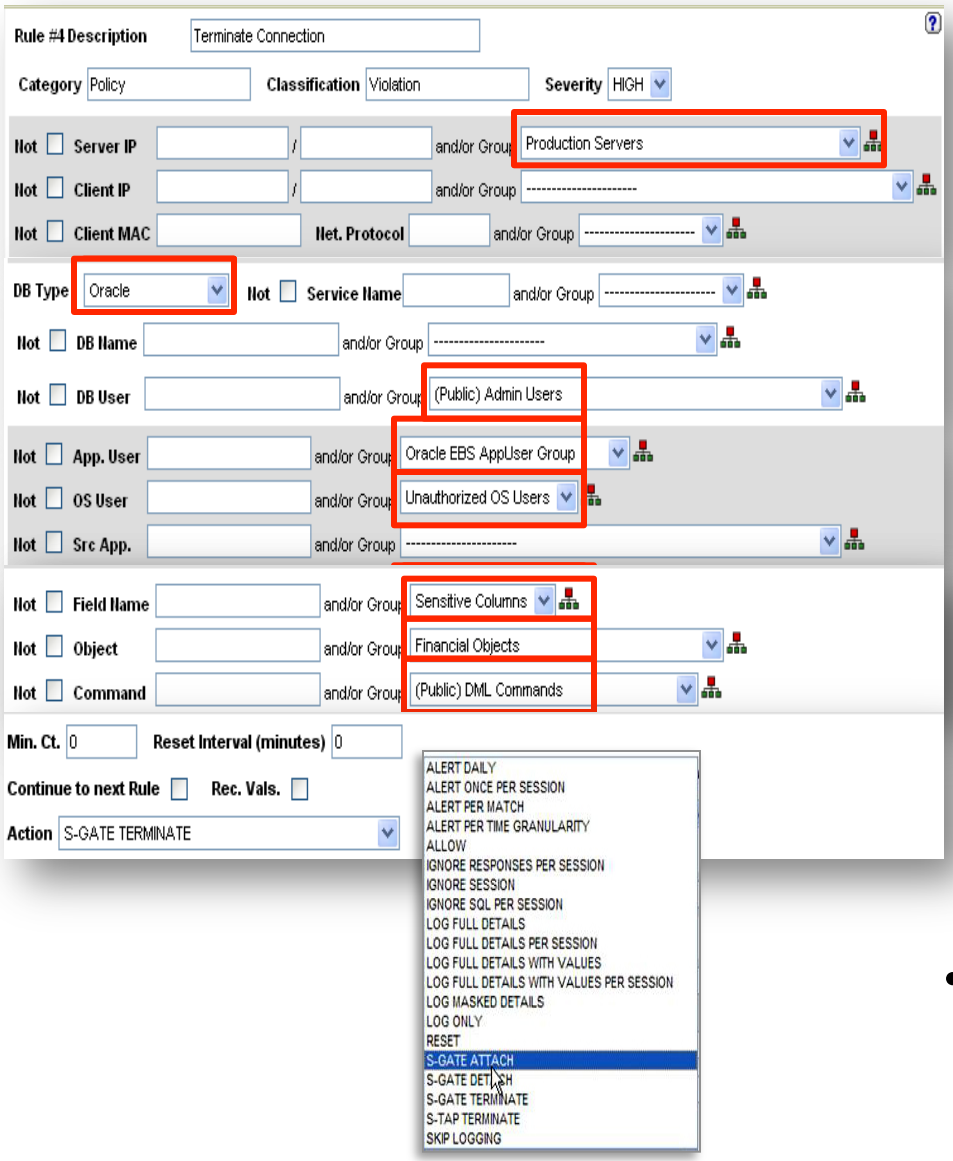
Object Name	Field Name	Value	Object-Field	DB User Name	Object-Command	Full Sql	Sql
Payroll	Salary	50000	Payroll+Salary	HARRY	Payroll+INSERT	Insert into Payroll(NAME,ID, Salary) VALUES('TOM JONES',2,50000)	Insert into Payroll(NAME,ID, Salary) VALUES(?,?,?)
payroll	salary	55000	payroll+salary	HARRY	payroll+UPDATE	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

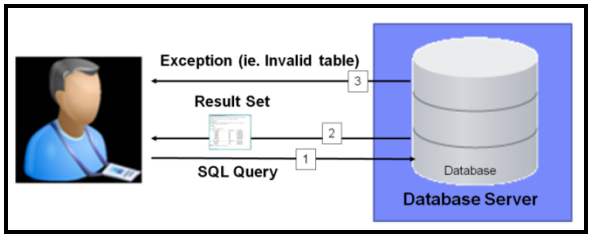
Each level of detail will store more information

- 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



Which Servers



Which Databases

Which Users

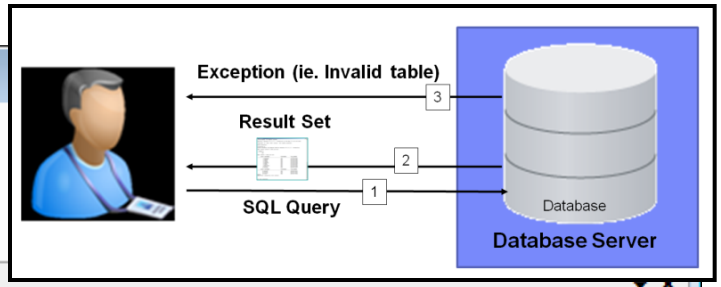
Which Fields

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



Microsoft SQL Server Management Studio

File Edit View Query Project Tools Window Community Help

New Query | Privacy | Execute

Object Explorer

Connect

10.10.9.248 (SQL Server 9.0.1399 - joe)
- Databases
- Security
- Server Objects
- Replication
- Management
- Notification Services
- SQL Server Agent (Agent XPs disa

10.10.9.248.Privacy - SQLQuery3.sql* | Summary

```
Select * from customer where customerID < 9
```

Results | Messages

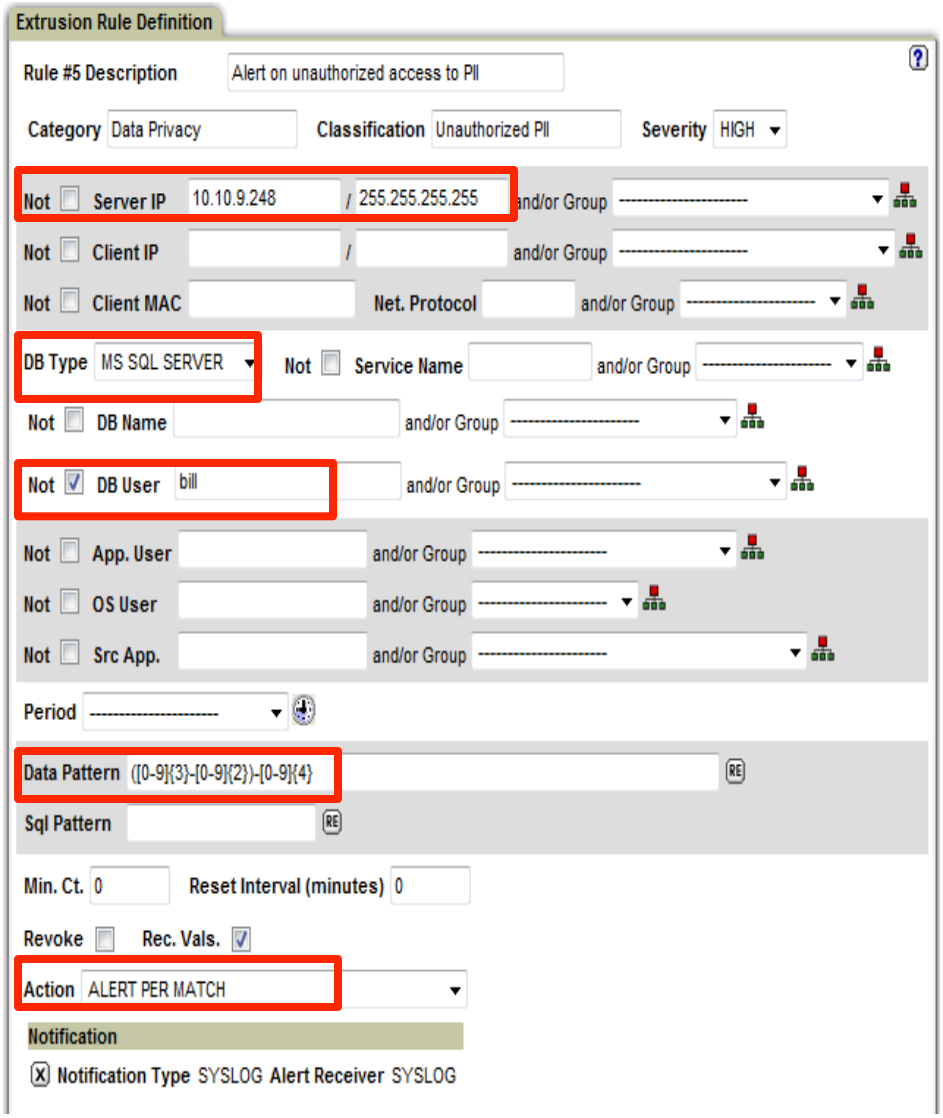
	CustomerID	FirstName	LastName	CardNumber	Name_on_Card	ssn	birthdate	address	zipcode	amount
1	0	Joe	Anthony	6011884338876676	Joe Anthony	123-45-6789	4/4/62	123 Main Street, New York, NY	02345	126.76
2	1	Joe	Thomas	6011516565028858	Joe Thomas	234-56-7890	4/4/82	32 South Street, Boston, MA	54321	231.22
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, Seatle, 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

Query executed successfully. | joe (52) | Privacy | 00:00:00 | 9 rows

Ready | Ch 1 | INS

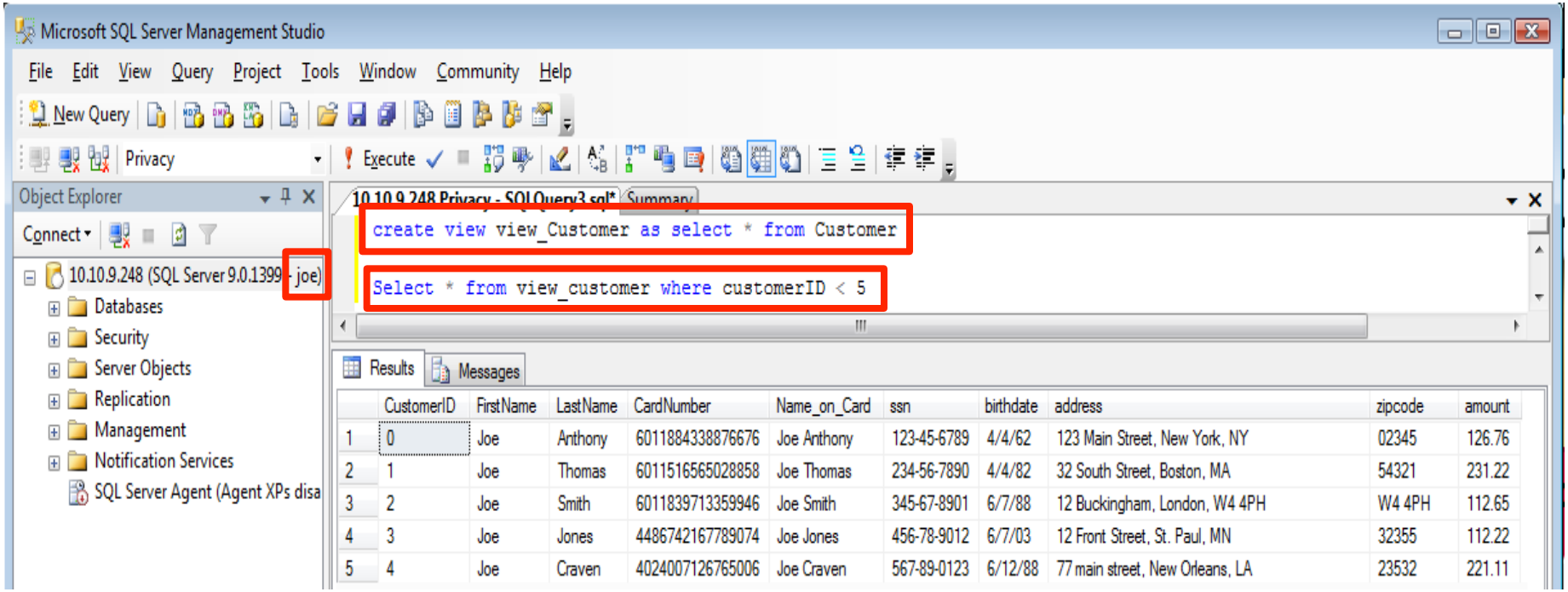
This is the results set to the query "select * from customer where customerID < 9"

2. Extrusion Definition to Alert on Unauthorized Results Set



- 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



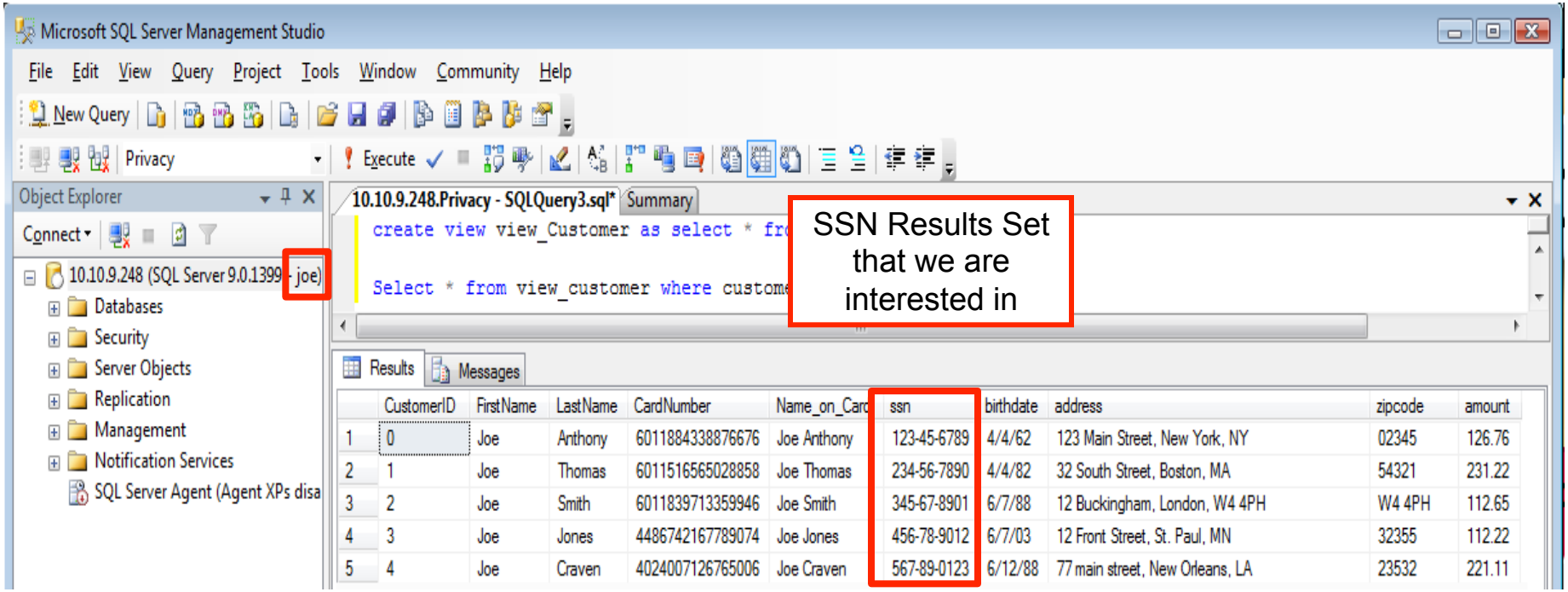
	CustomerID	FirstName	LastName	CardNumber	Name_on_Card	ssn	birthdate	address	zipcode	amount
1	0	Joe	Anthony	6011884338876676	Joe Anthony	123-45-6789	4/4/62	123 Main Street, New York, NY	02345	126.76
2	1	Joe	Thomas	6011516565028858	Joe Thomas	234-56-7890	4/4/82	32 South Street, Boston, MA	54321	231.22
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



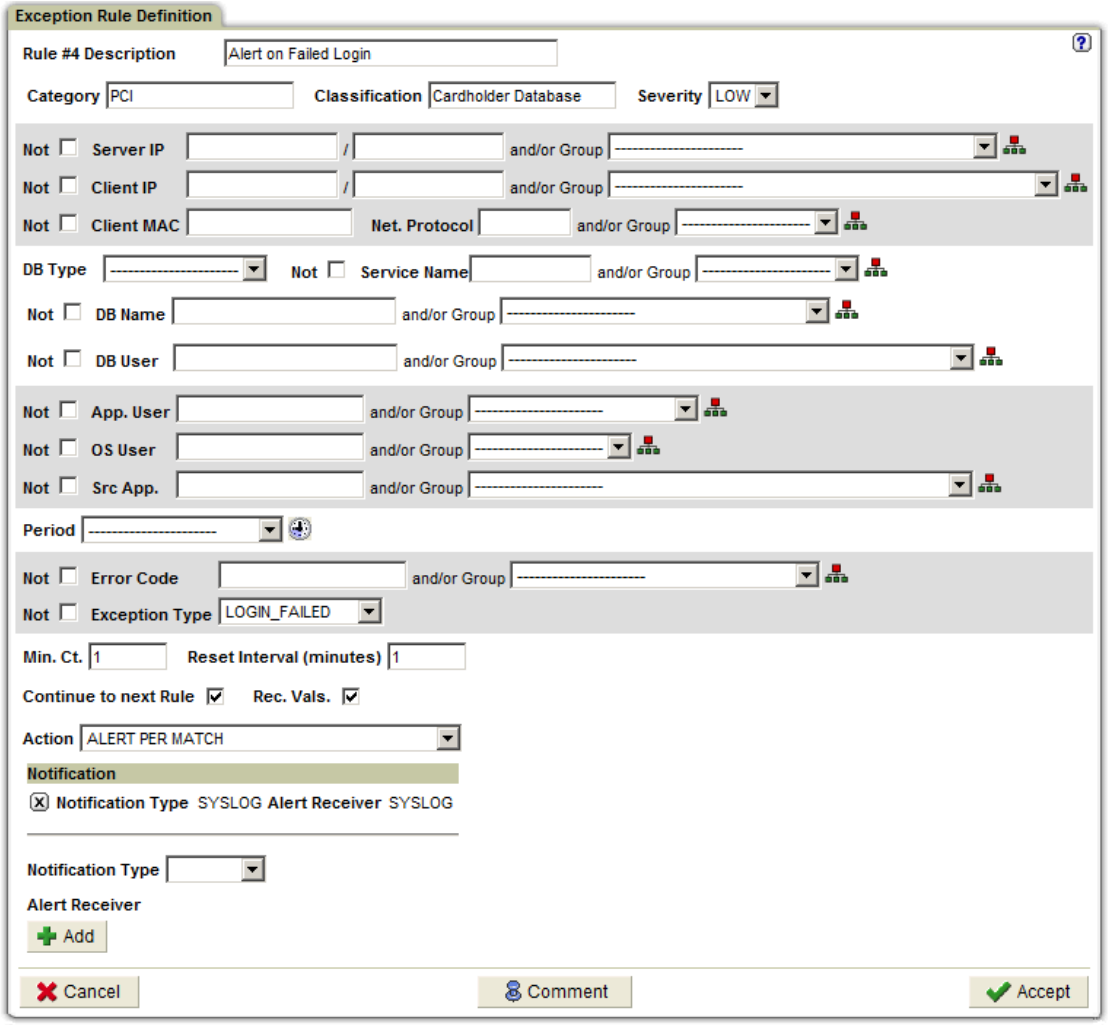
Policy Violations Details

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

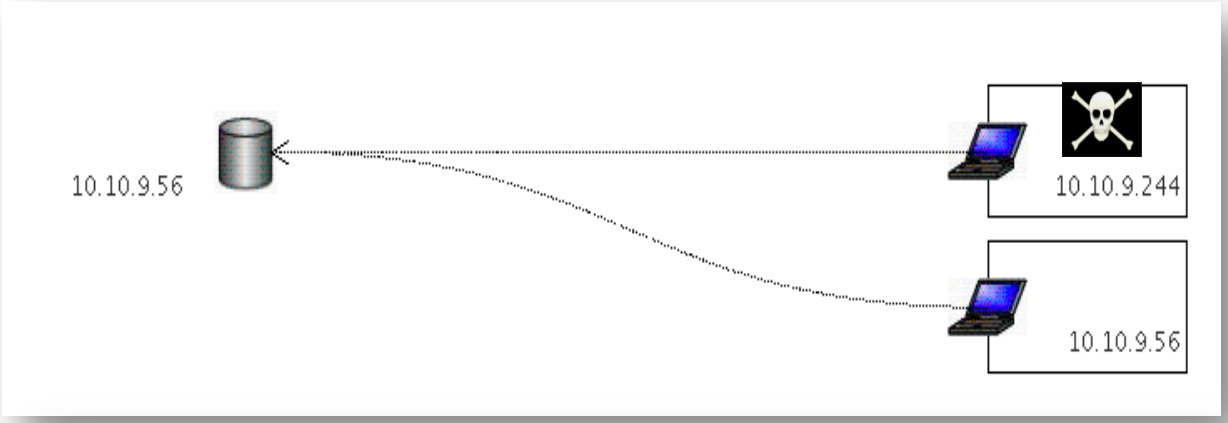
Masked Extrusion Values ([0-9]{3}-[0-9]{2})-[0-9]{4}

3. Policy Exception Rule



- 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	APPLSYSPUB	ORA-00942: table or view does not exist

SQL injection leads to **SQL errors**!

Failed Login Attempts

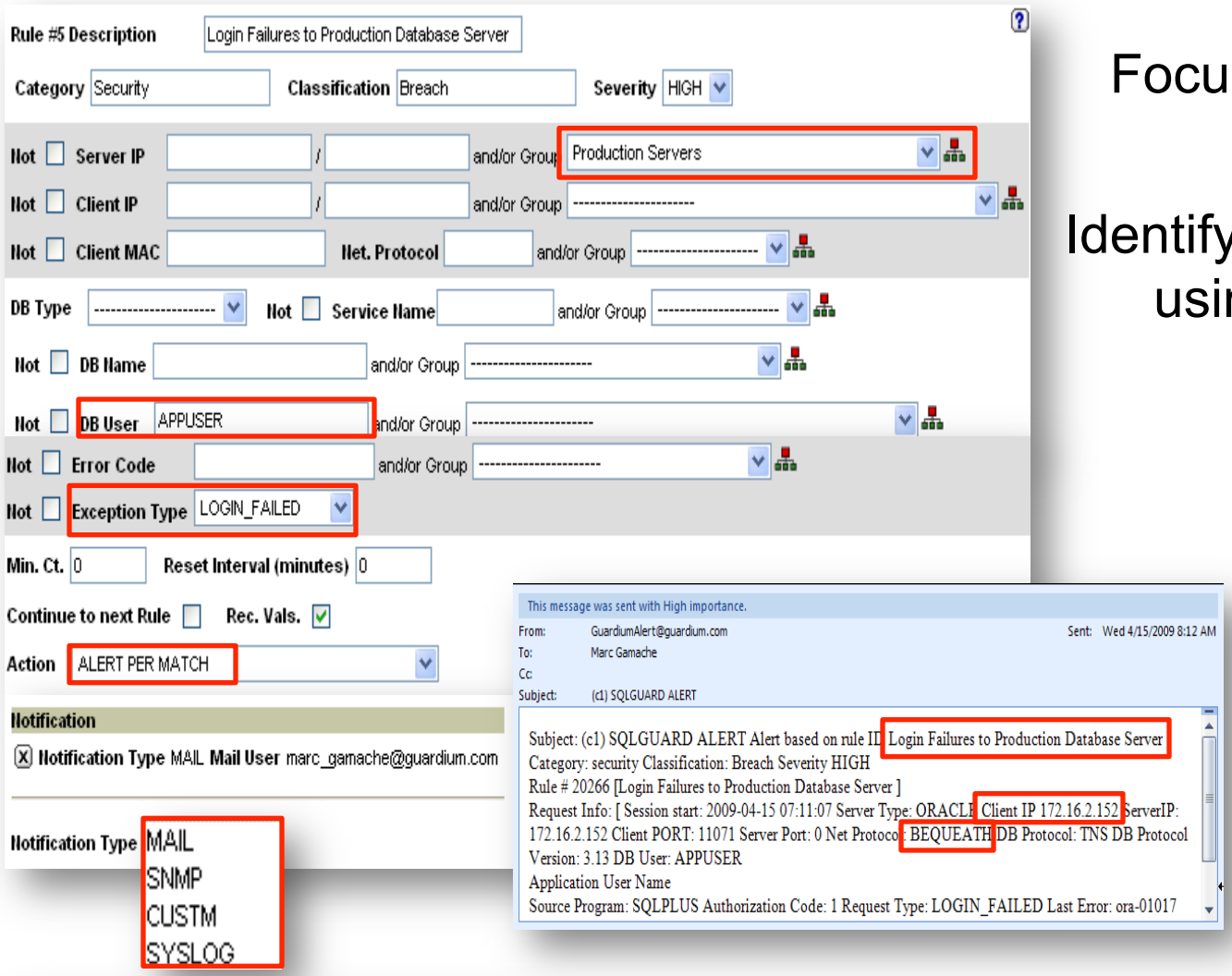
Start Date: **2007-03-01 00:00:00** End Date: **2007-05-01 00:00:00**

User Name	Source Address	Destination Address	Database
MarcG	192.168.20.107	10.10.9.56	ORACLE
APPLSYSPUB	10.10.9.244	10.10.9.56	ORACLE
APPLSYSPUB	10.10.9.56	10.10.9.56	ORACLE

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

Guardium: 100% visibility with real-time alerts …

Exception Policies With Real-Time Alerts



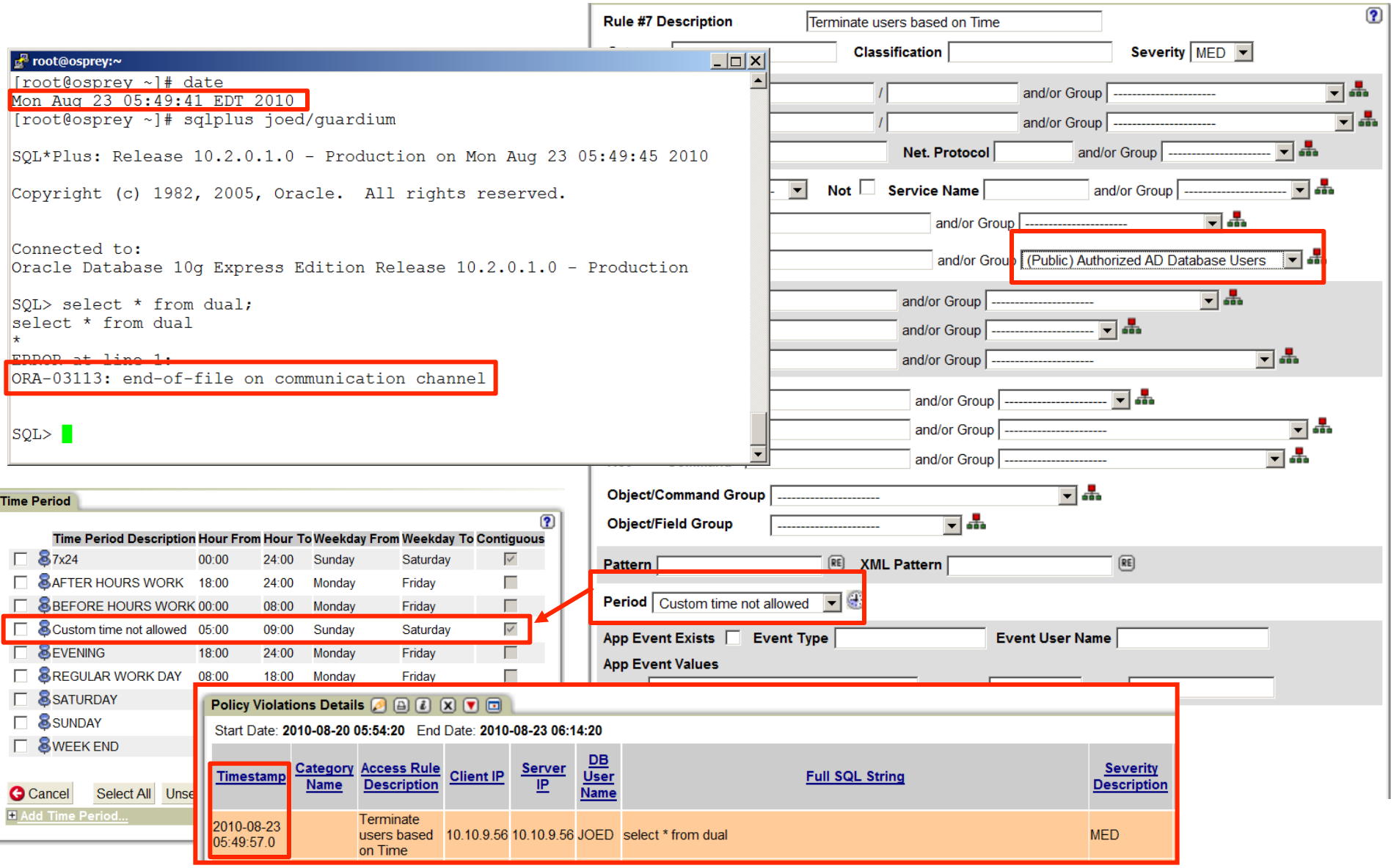
Focus on production DB servers

Identify failed login attempts using the application account!

Take Action:
Send alert via email, SYSLOG, SNMP or custom Java class

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

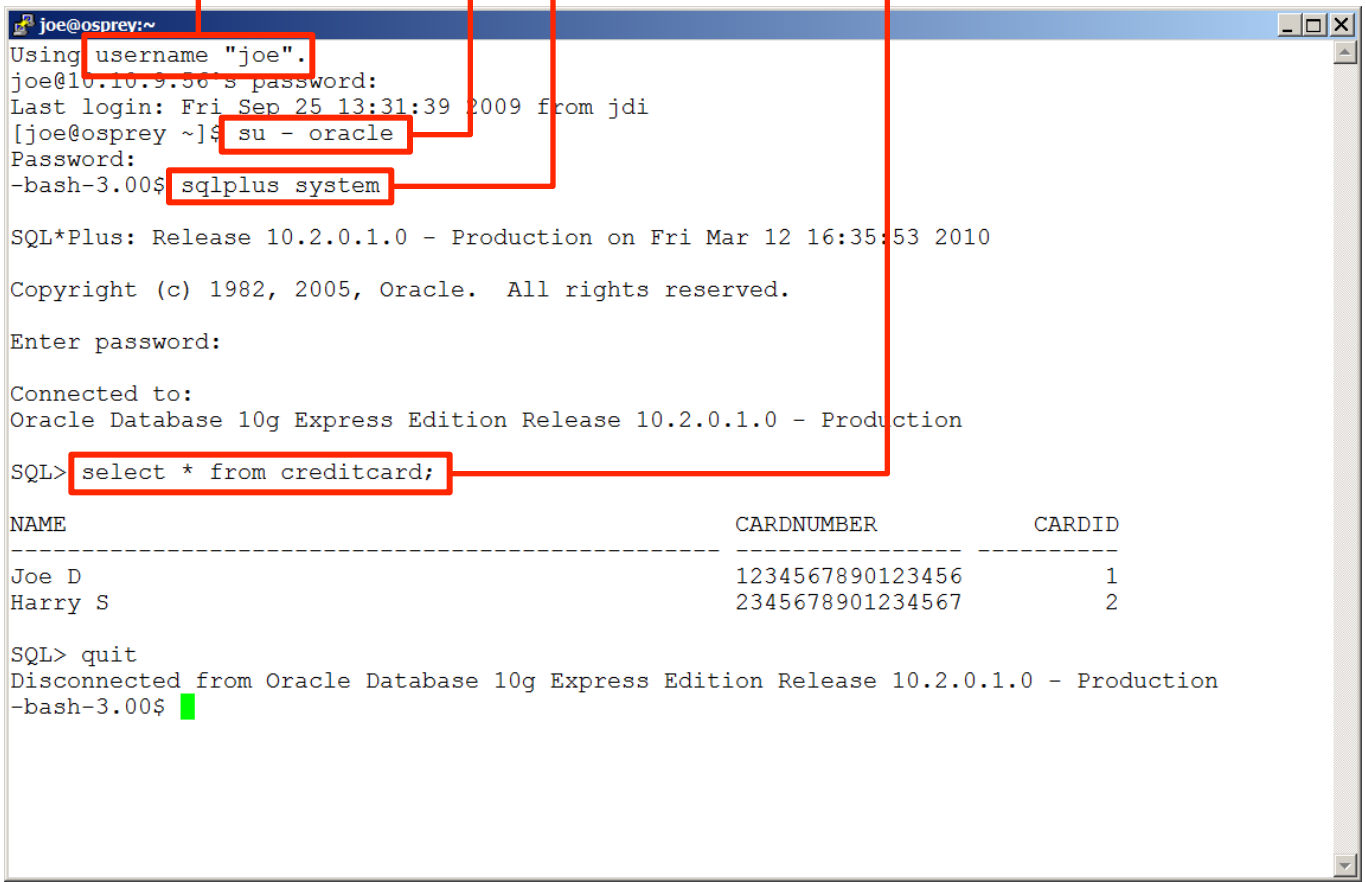
Example: Deny User Based on Time



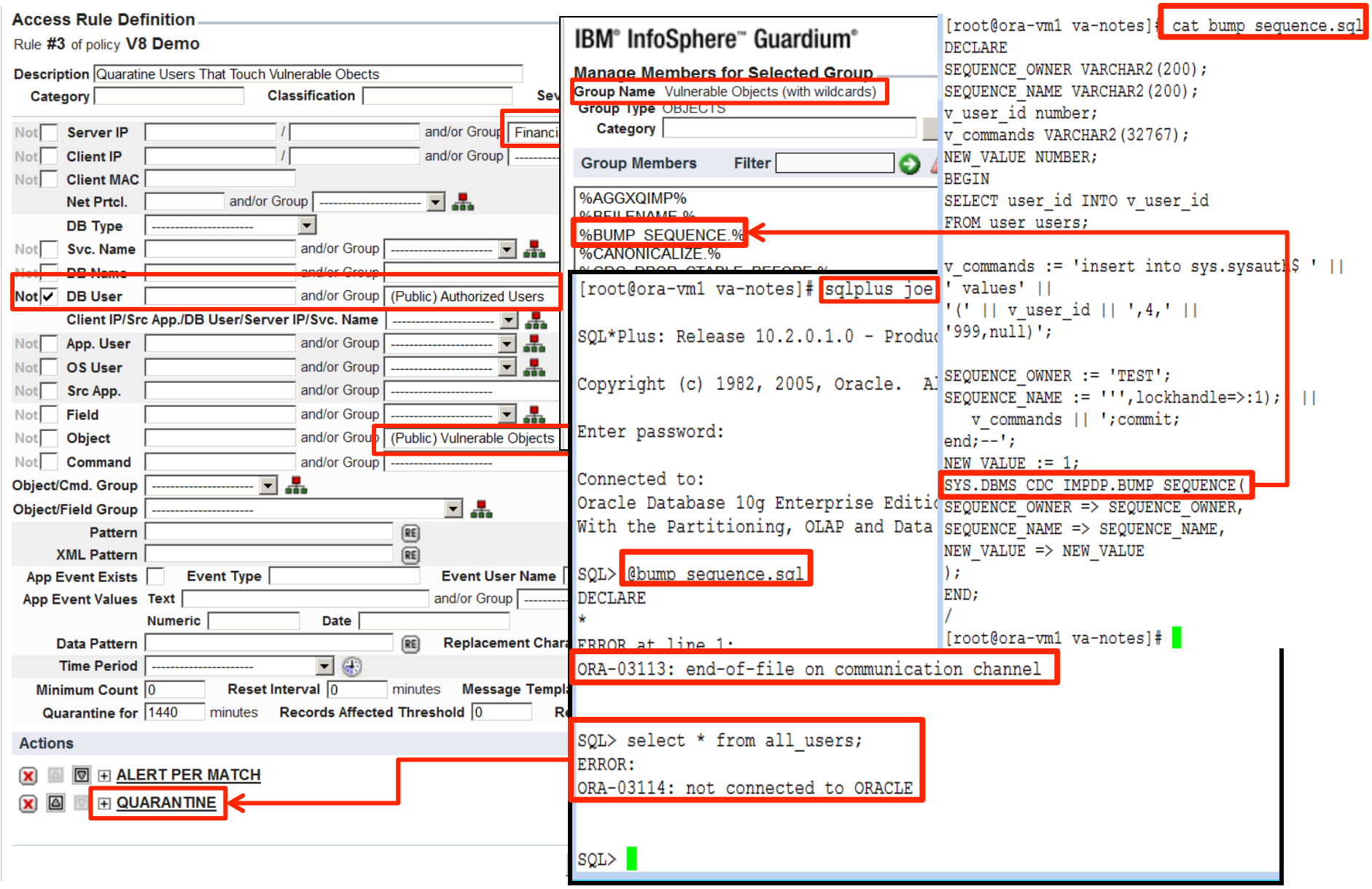
Example: “SU” To Different Users Accounts

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

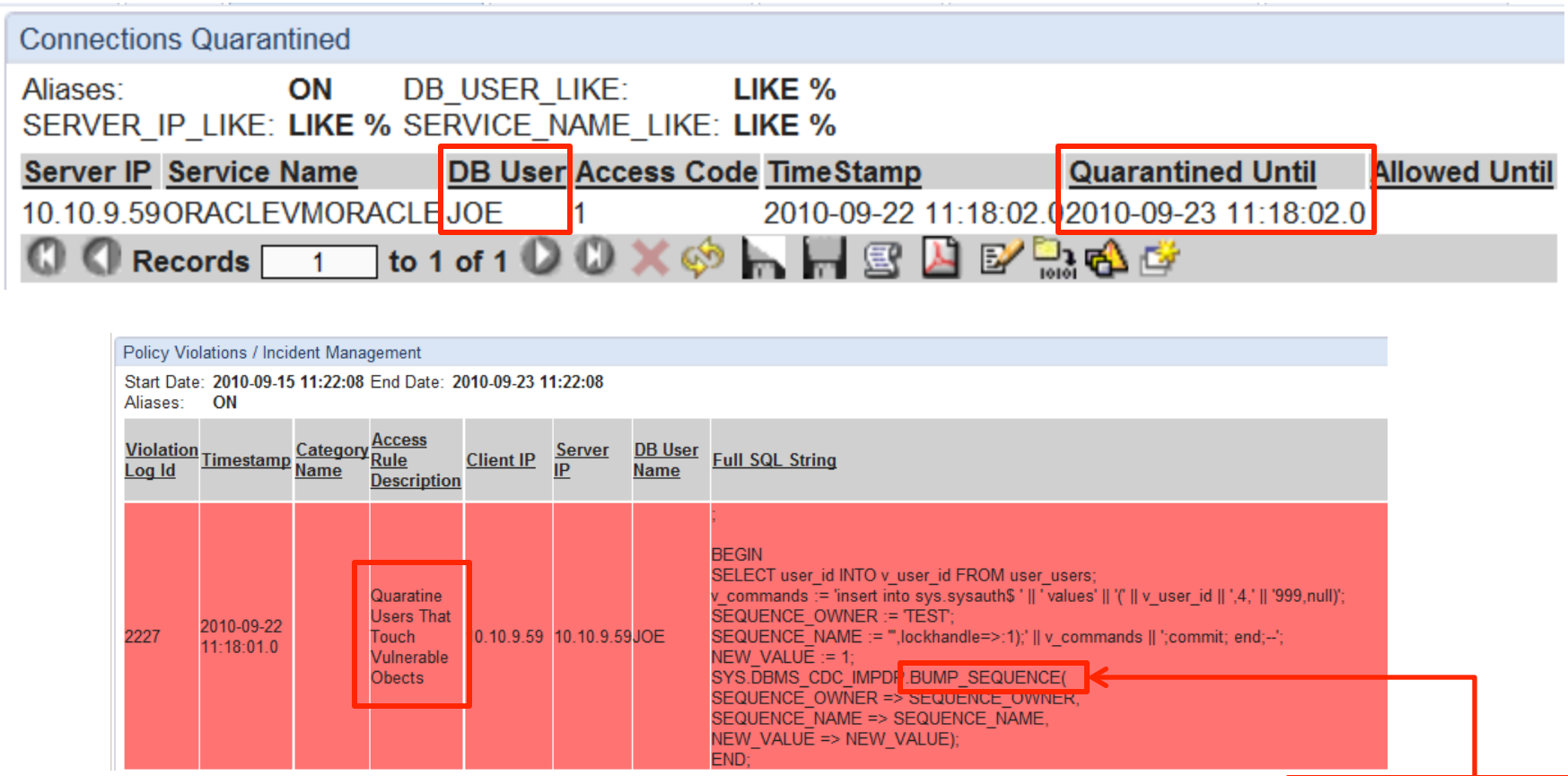
Timestamp	Client IP	Server IP	Network Protocol	Uid Chain Compressed	OS User	DB User Name	Source Program	Full Sql	Uid Chain
2010-03-11 20:47:40.0	10.10.9.56	10.10.9.56	BEQUEATH	joe	ORACLE	SYSTEM	SQLPLUS@OSPREY	select * from creditcard	(1,root,init [3])->(2267,root,/usr/sbin/sshd)->(20063,root,sshd: joe [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))))



Quarantine Unauthorized Access to Vulnerable Objects



Quarantine Unauthorized Access to Vulnerable Objects



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

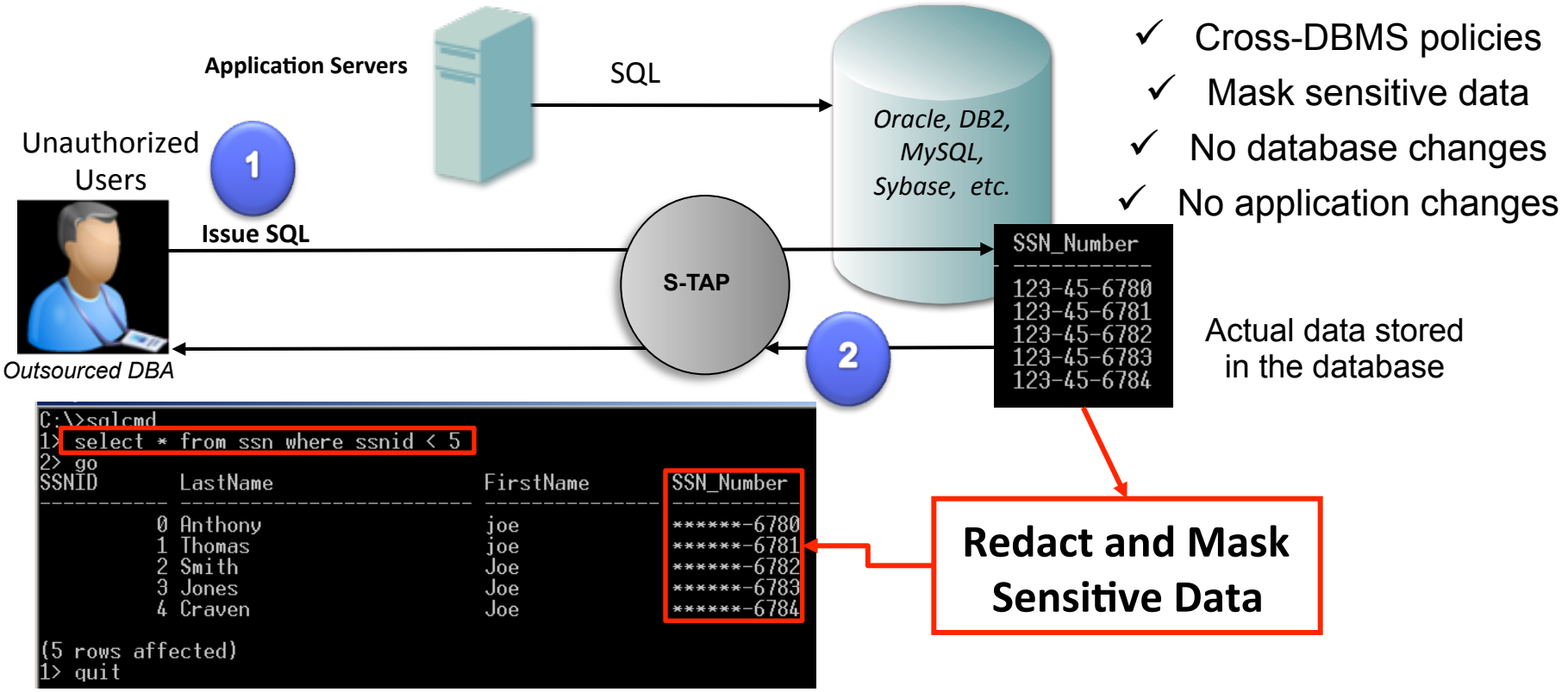
2227	2010-09-22 11:18:01.0		Quaratine Users That Touch Vulnerable Obects	0.10.9.59	10.10.9.59	JOE	;
							BEGIN
							SELECT user_id INTO v_user_id FROM user_users;
							v_commands := 'insert into sys.sysauth$ ' || ' values' || '(' || v_user_id || ',4,' || '999,null)';
							SEQUENCE_OWNER := 'TEST';
							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;

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

Redact Action for Live Data Masking

- 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

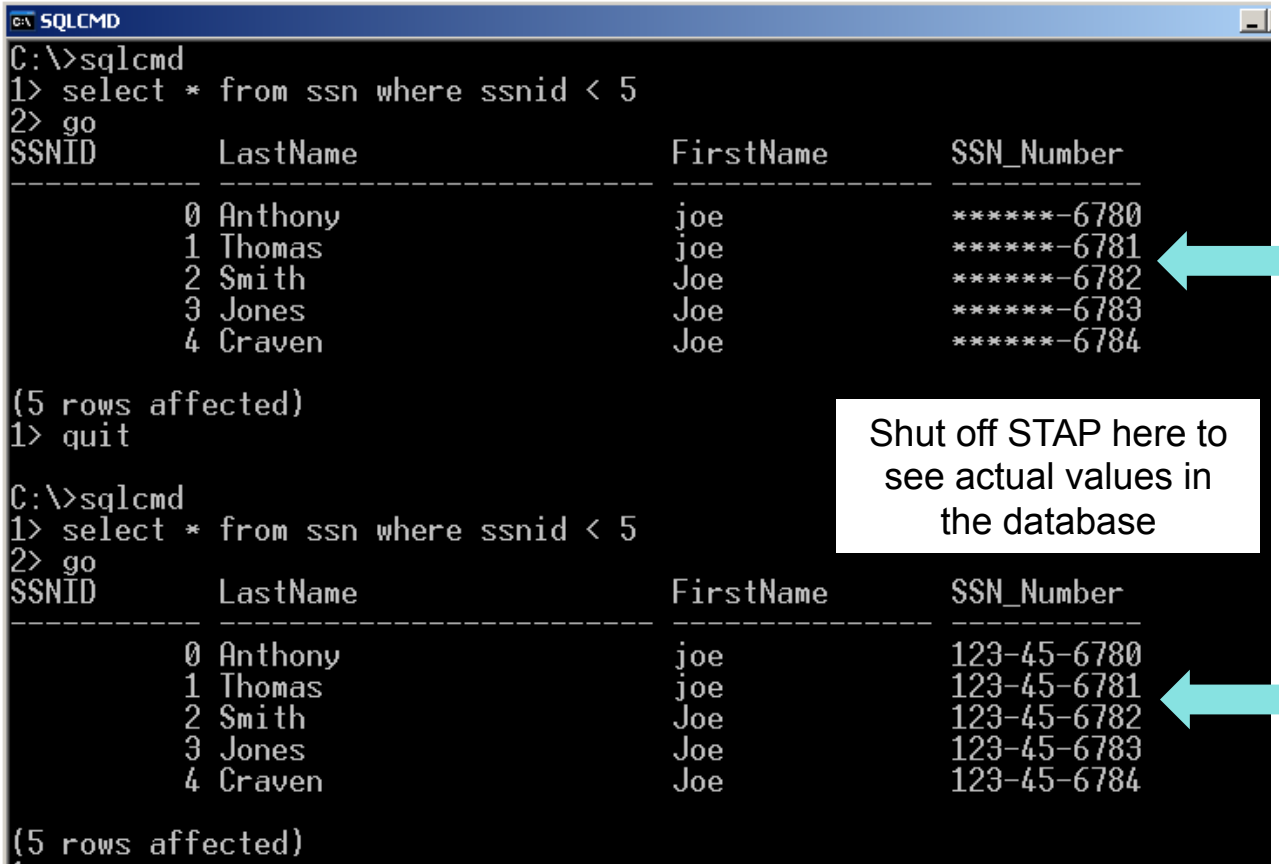
Data-Level Access Control



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

User view of the data in the database

Mask Sensitive Information From Unauthorized Users



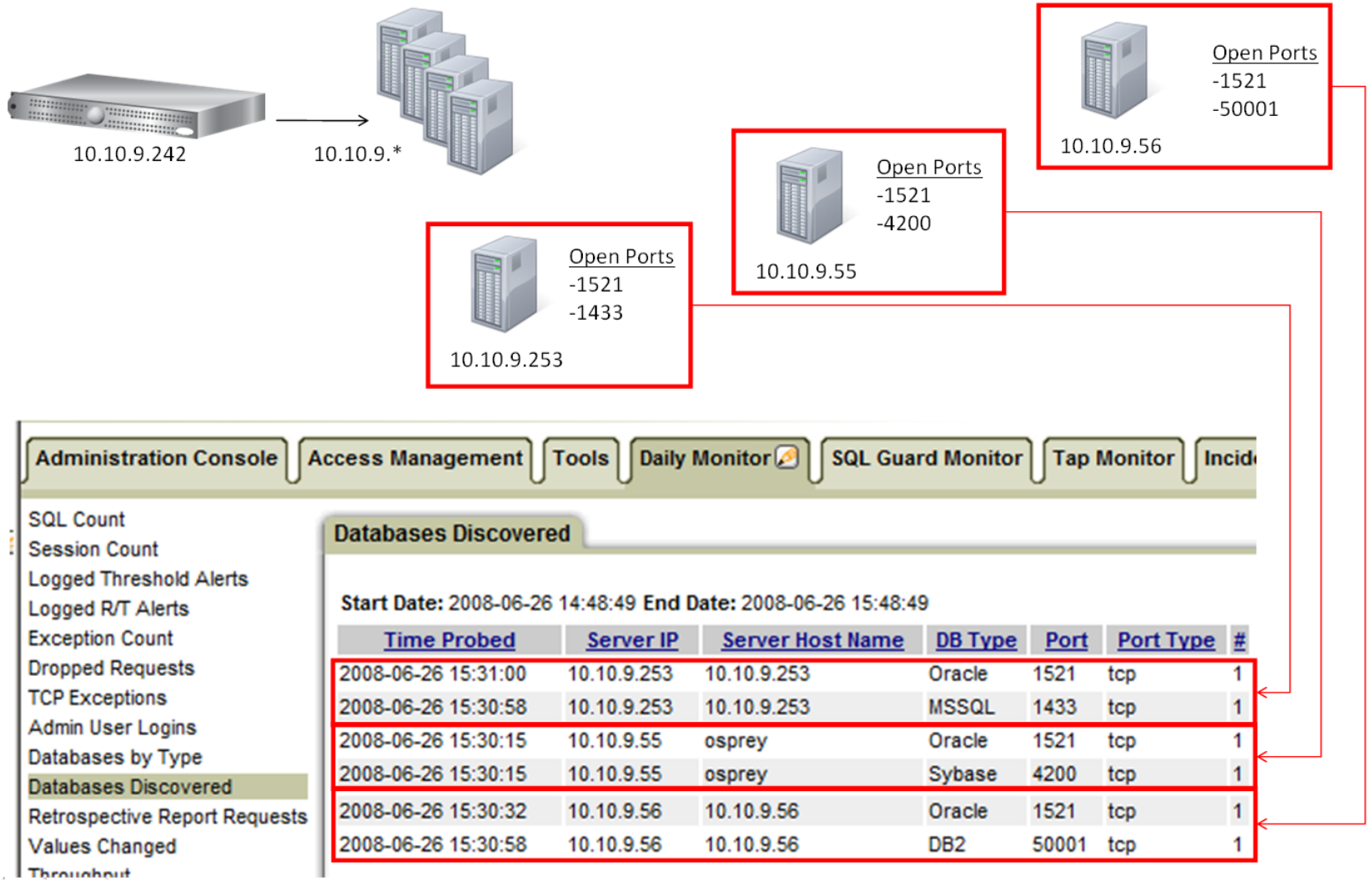
Masked values to database client

Shut off STAP here to see actual values in the database

Actual Values in the database server

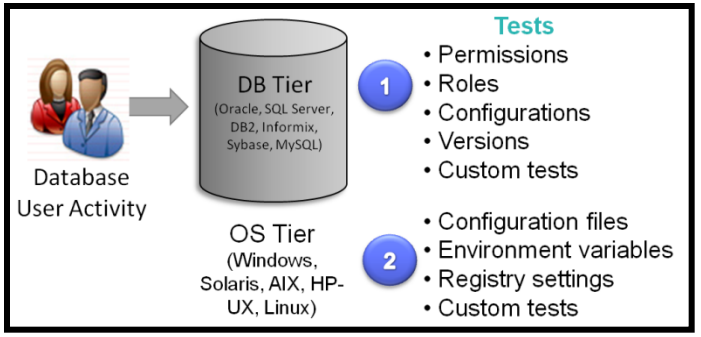
- Mask data on the fly for production database servers
- Use Optim Test Data Management for development and test environments

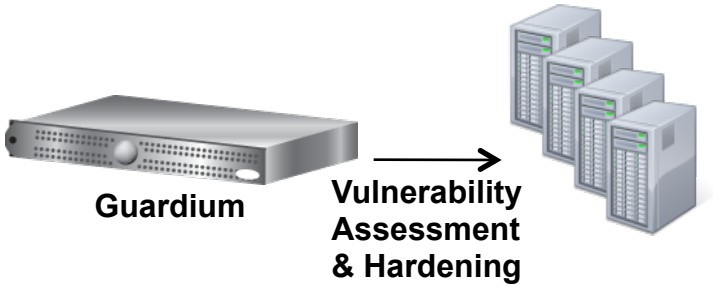
Database Automatic Discovery



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	--

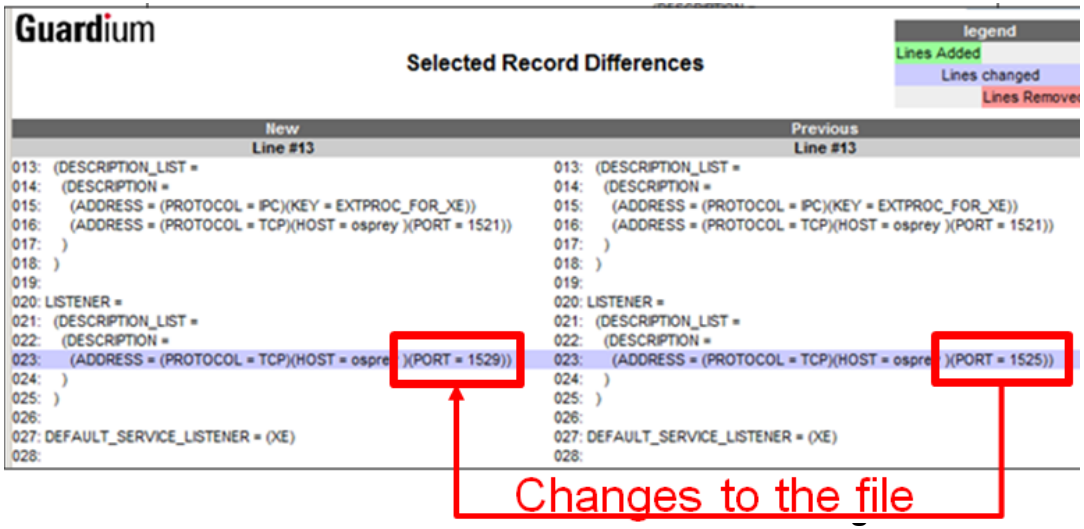
2. Identify Risk

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
					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 ar likely to become known to unauthorized users. We recommend that you set this parameter in order to limit the lifetime of users' passwords.
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
					Recommendation: No Password Verification Routine has been implemented. We recommend that you implement a password function to prevent the use of weak passwords.
Auth.	Default Accounts Password Changed	ORACLE: Oracle on Ocean	Fail	Critical	2 active pre-defined users have default passwords.
					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 your 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.
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.
					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.

- 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



- 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

Change Control Reconciliation

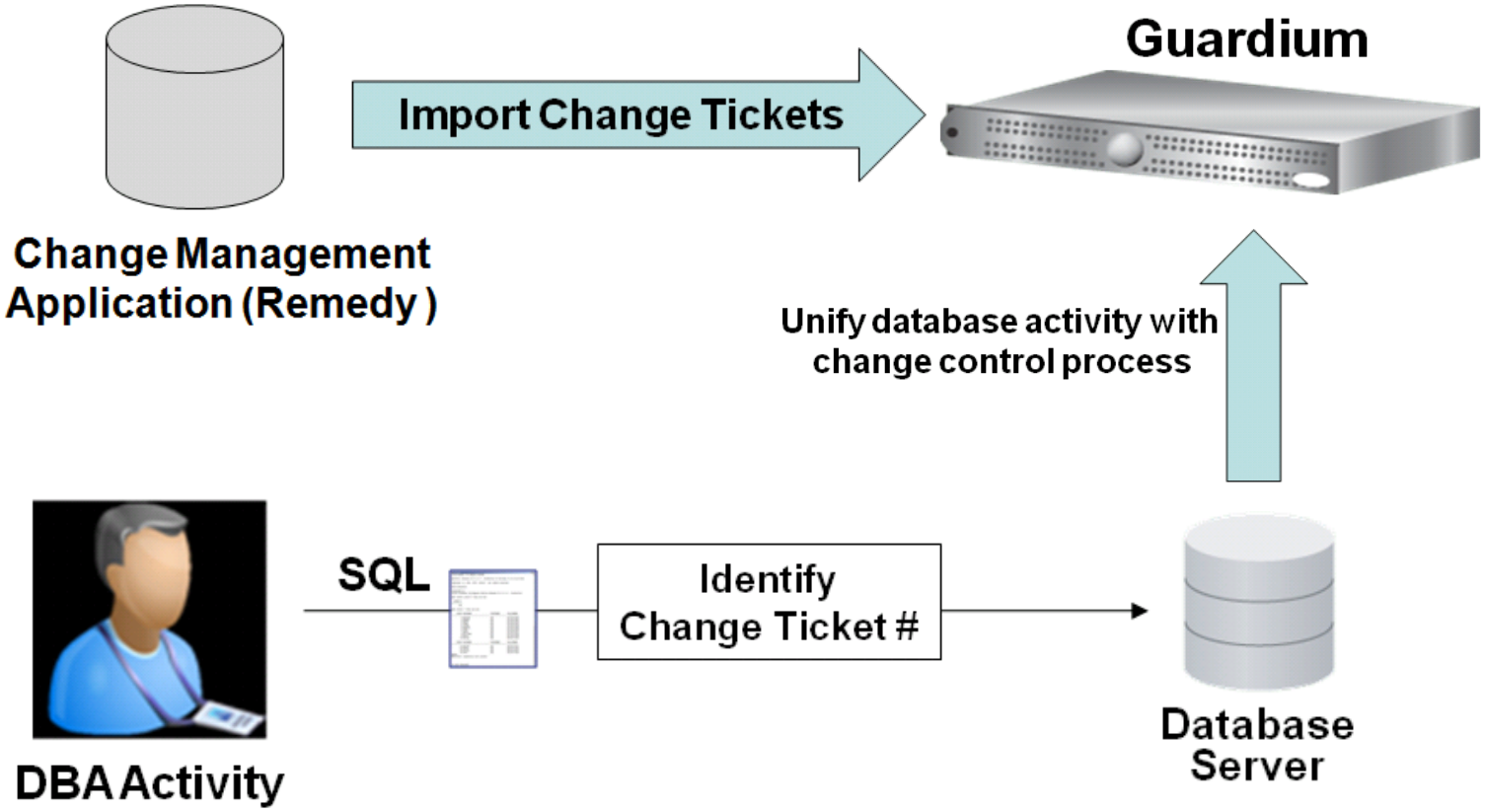
BMC Remedy Change Control - Reconciliation

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	Plase create a table called PCI_data
2008-09-22 17:34:02.0			drop table pci_data		

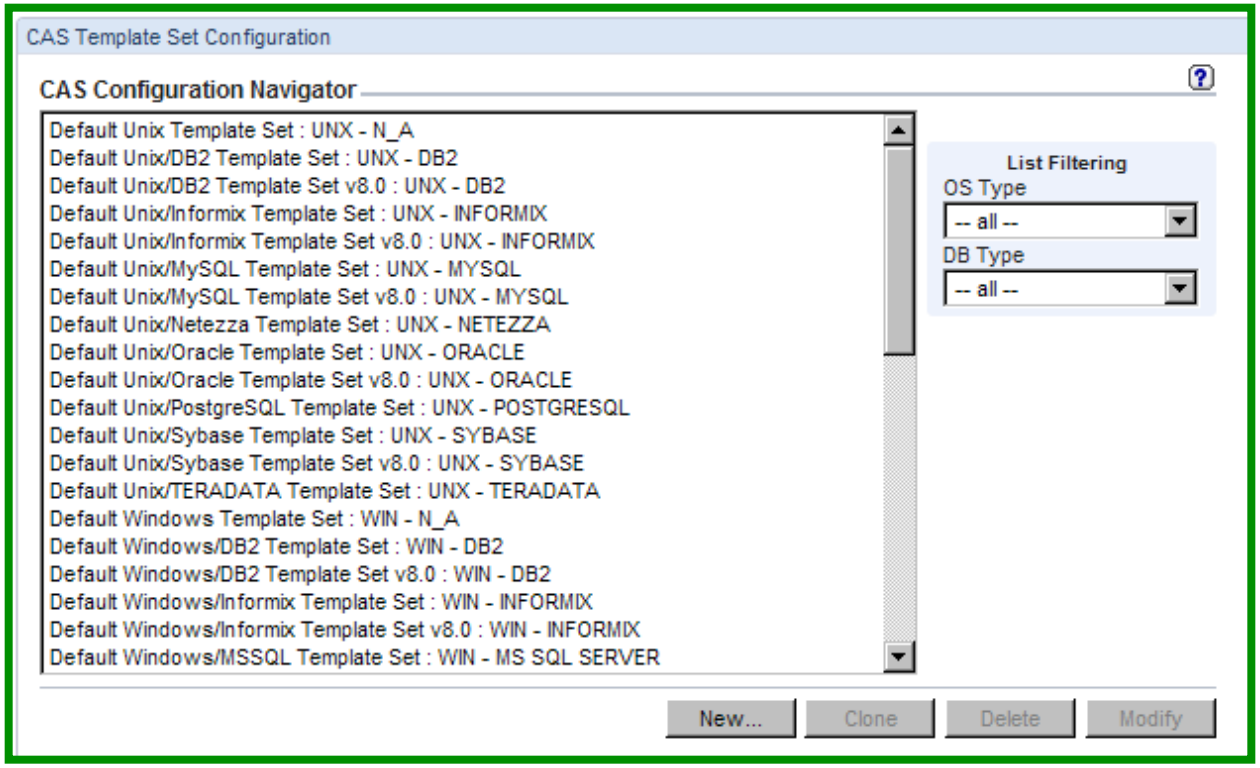
Records: 1 to 2 of 2

Ticketed
Unticketed

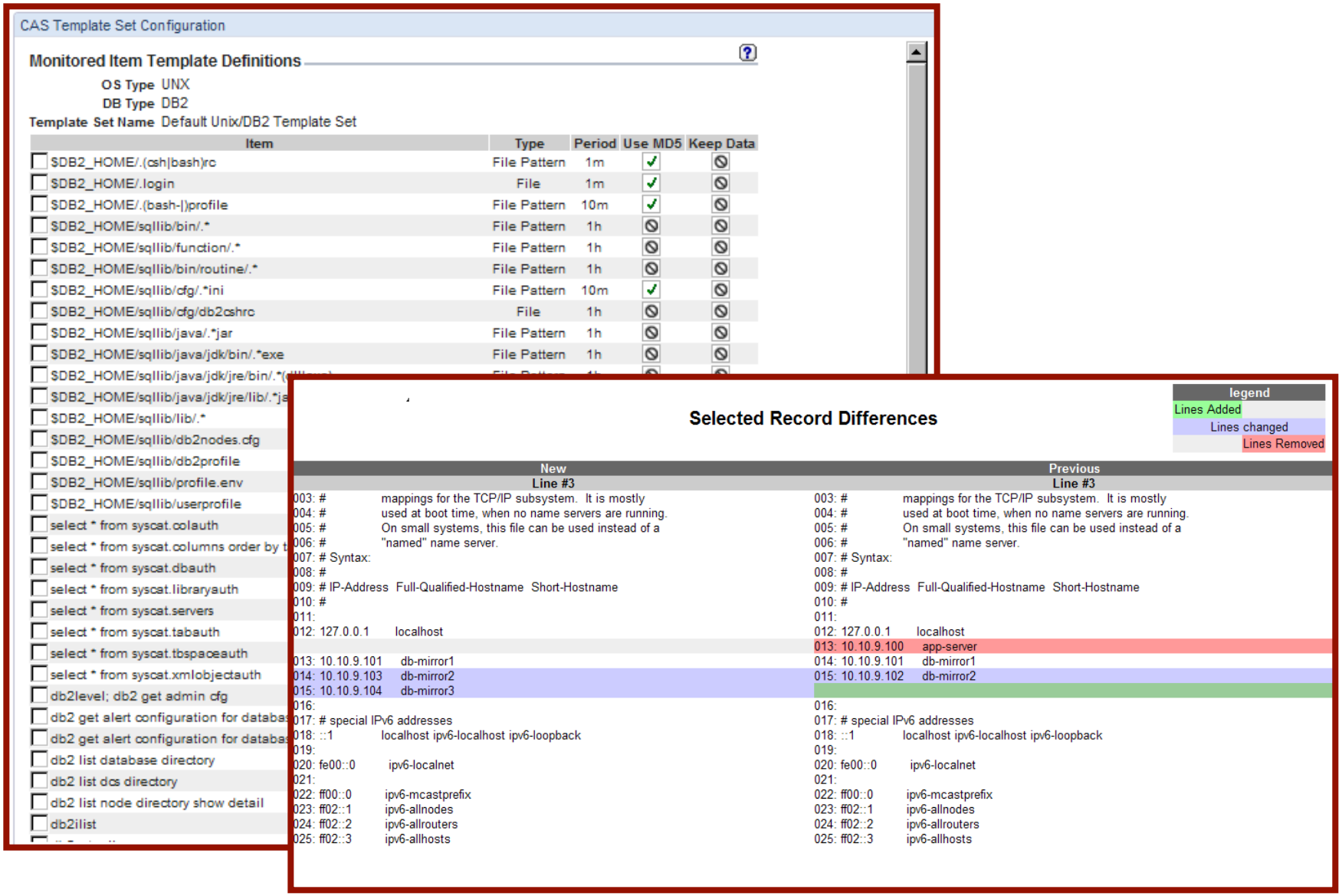


Configuration Auditing

- Database configuration auditing for Guardium occurs through it's 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



Configuration Auditing

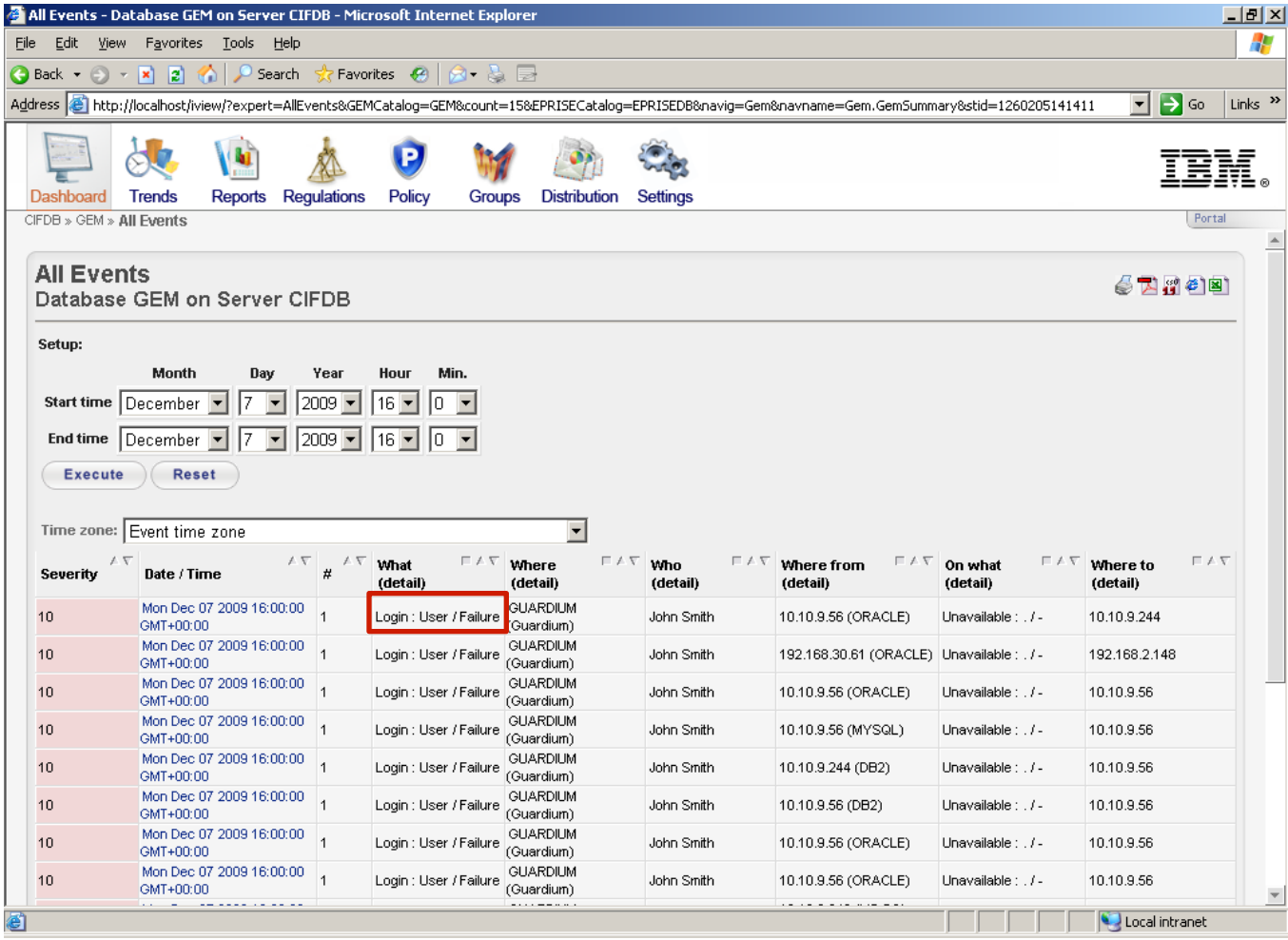


Integrating with IBM TSIEM

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

Events in IBM SIEM



Questions