8 Steps to Holistic Database Security

Nati Shapira
Worldwide Solution Specialist
InfoSphere Guardium

InformationOnDemandIndia2011
The Premier Conference for Information Management
Manage. Analyze. Govern.

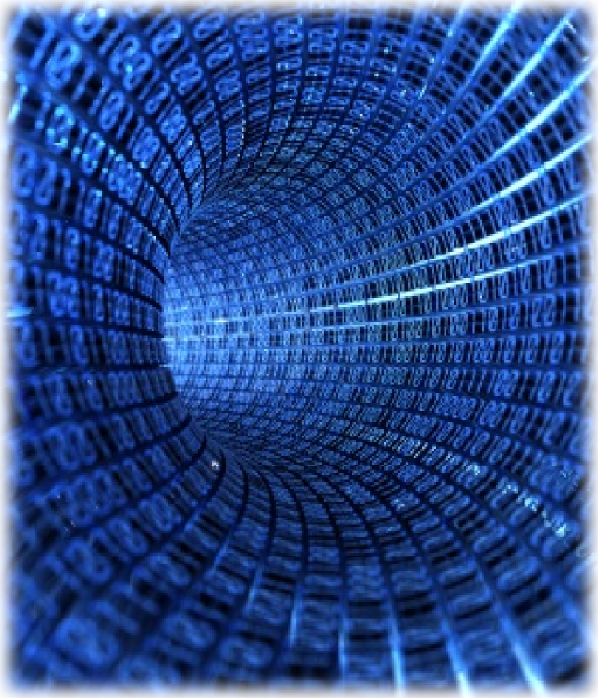
February 2, 2011
Hyatt Regency I Mumbai, India

8 Steps to Database Security

1. Discovery
2. Vulnerability & Configuration Assessment
3. Hardening
4. Change Auditing
5. Database Activity Monitoring (DAM)
6. Auditing
7. Authentication, Access Control & Entitlement Management
8. Encryption

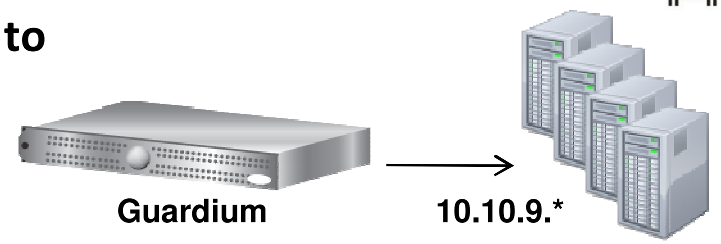
1. Discovery

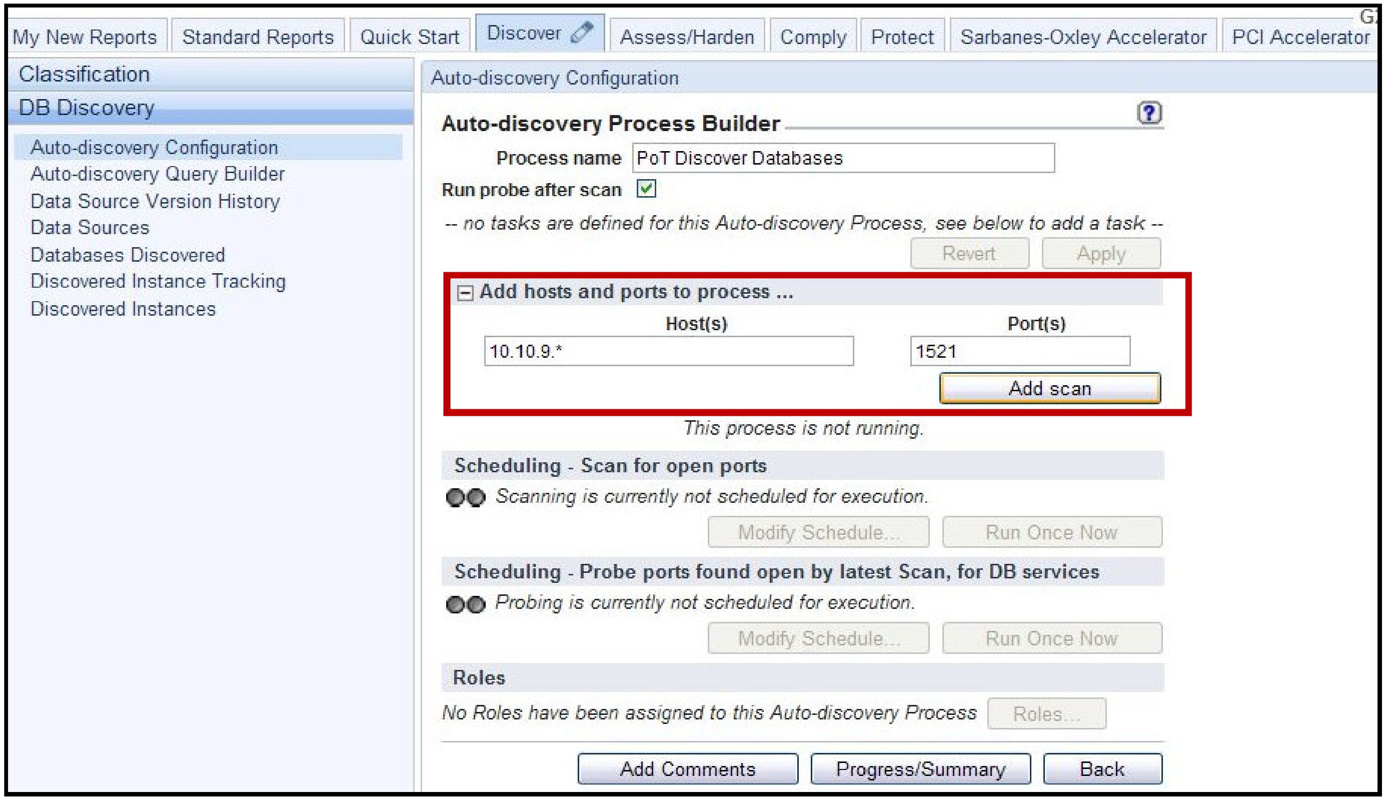
- You can't secure what you don't know.
- You need to have a good mapping of your sensitive assets – both of your database instances and your sensitive data inside the databases.
- You should automate the discovery process since the location of sensitive data is constantly changing due to new or modified applications, mergers and acquisitions, etc.



InfoSphere Guardium Database Discovery

- **You don't need an agent on the database server to discover new databases on the network**





Auto-discovery Configuration

Auto-discovery Process Builder

Process name: PoT Discover Databases

Run probe after scan ☑

-- no tasks are defined for this Auto-discovery Process, see below to add a task --

⊟ Add hosts and ports to process ...

Host(s)	Port(s)
10.10.9.*	1521

This process is not running.

Scheduling - Scan for open ports

Scanning is currently not scheduled for execution.

Scheduling - Probe ports found open by latest Scan, for DB services

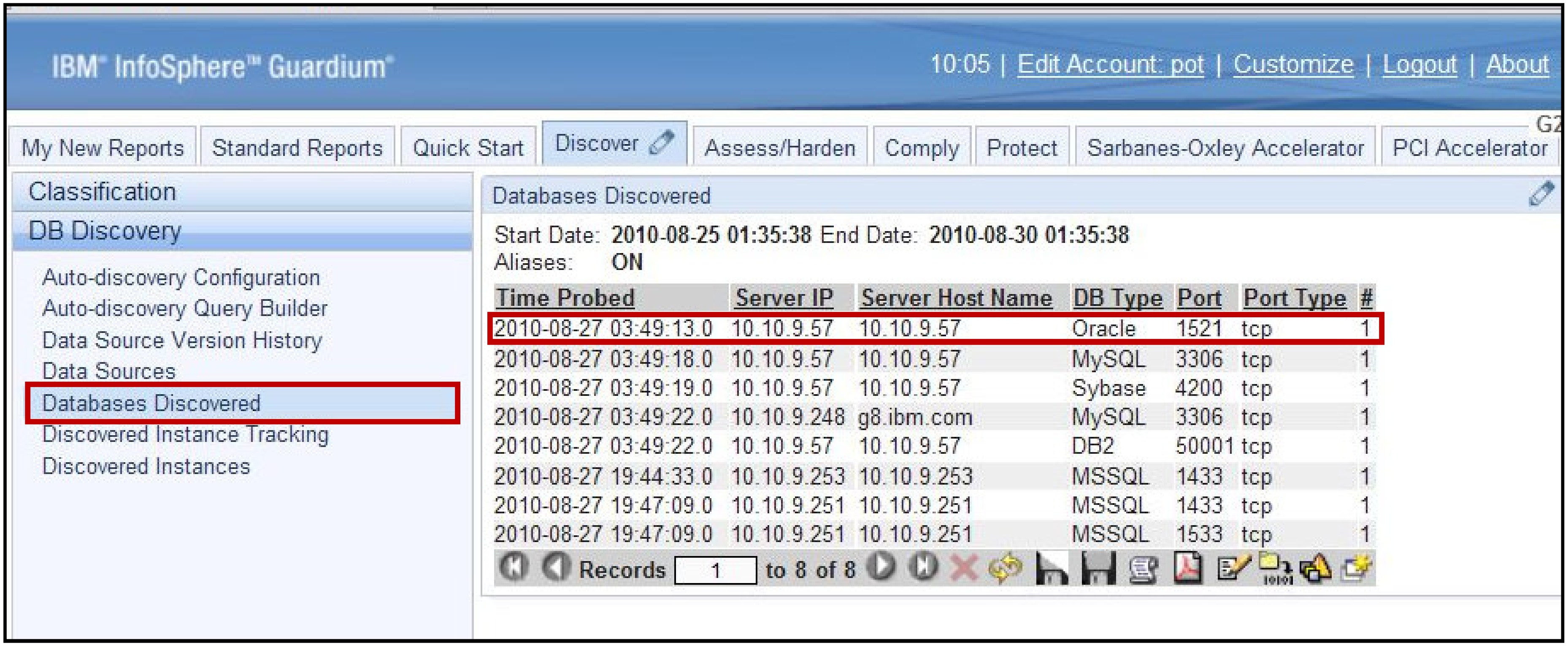
Probing is currently not scheduled for execution.

Roles

No Roles have been assigned to this Auto-discovery Process

Database Discovered Report

- **This is a sample report that shows the results of the DB Discovery process**


IBM® InfoSphere™ Guardium®
10:05 | Edit Account: pot | Customize | Logout | About
My New Reports
Standard Reports
Quick Start
Discover
Assess/Harden
Comply
Protect
Sarbanes-Oxley Accelerator
PCI Accelerator
G2
Classification
DB Discovery
Auto-discovery Configuration
Auto-discovery Query Builder
Data Source Version History
Data Sources
Databases Discovered
Discovered Instance Tracking
Discovered Instances
Records
1
to 8 of 8

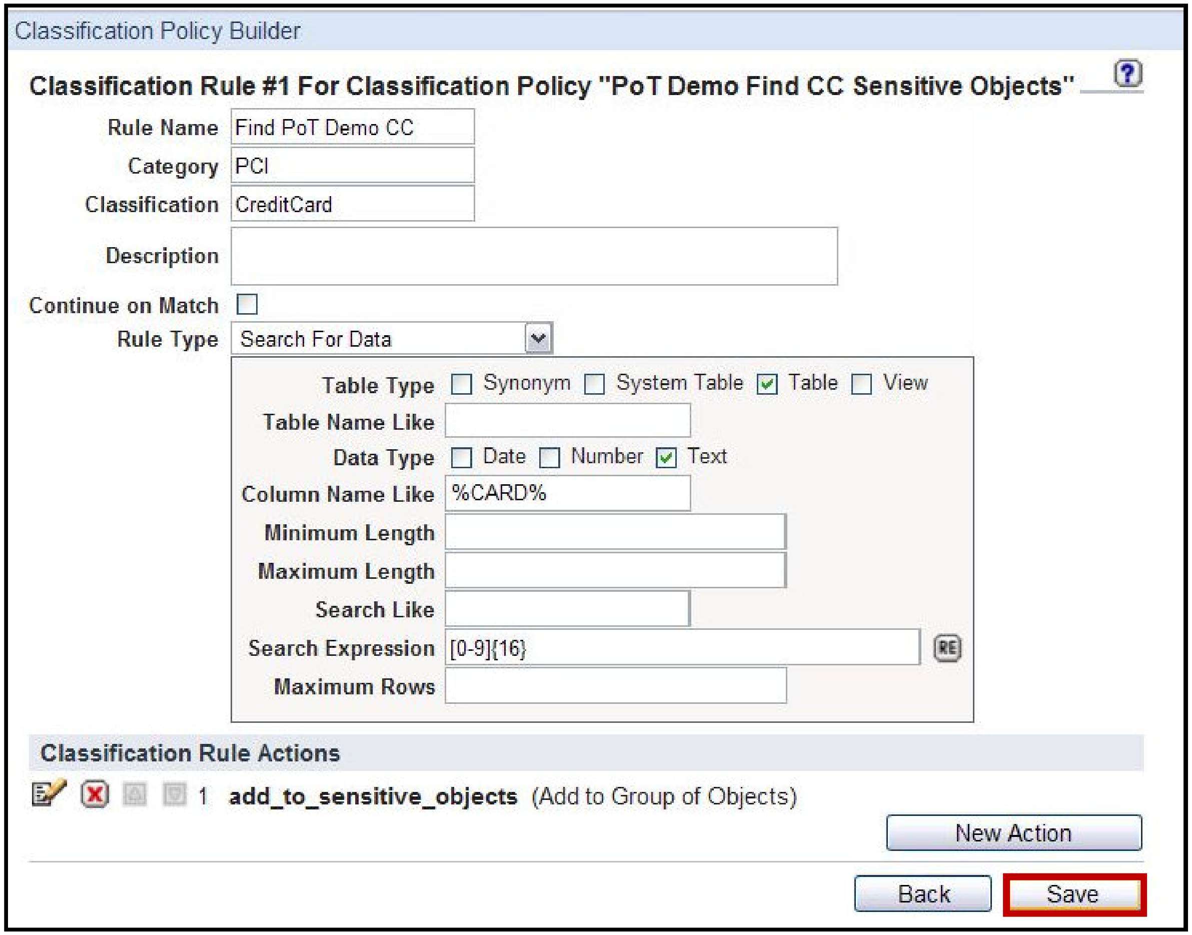
Databases Discovered

Start Date: 2010-08-25 01:35:38 End Date: 2010-08-30 01:35:38
Aliases: ON

Time Probed	Server IP	Server Host Name	DB Type	Port	Port Type	#
2010-08-27 03:49:13.0	10.10.9.57	10.10.9.57	Oracle	1521	tcp	1
2010-08-27 03:49:18.0	10.10.9.57	10.10.9.57	MySQL	3306	tcp	1
2010-08-27 03:49:19.0	10.10.9.57	10.10.9.57	Sybase	4200	tcp	1
2010-08-27 03:49:22.0	10.10.9.248	g8.ibm.com	MySQL	3306	tcp	1
2010-08-27 03:49:22.0	10.10.9.57	10.10.9.57	DB2	50001	tcp	1
2010-08-27 19:44:33.0	10.10.9.253	10.10.9.253	MSSQL	1433	tcp	1
2010-08-27 19:47:09.0	10.10.9.251	10.10.9.251	MSSQL	1433	tcp	1
2010-08-27 19:47:09.0	10.10.9.251	10.10.9.251	MSSQL	1533	tcp	1

Discovering Sensitive Data

- There are many options to discover sensitive data.
- These searches include:
  - **Permission**
  - **Table, view, synonym**
  - **Data (regular expression)**



Classification Policy Builder

Classification Rule #1 For Classification Policy "PoT Demo Find CC Sensitive Objects"

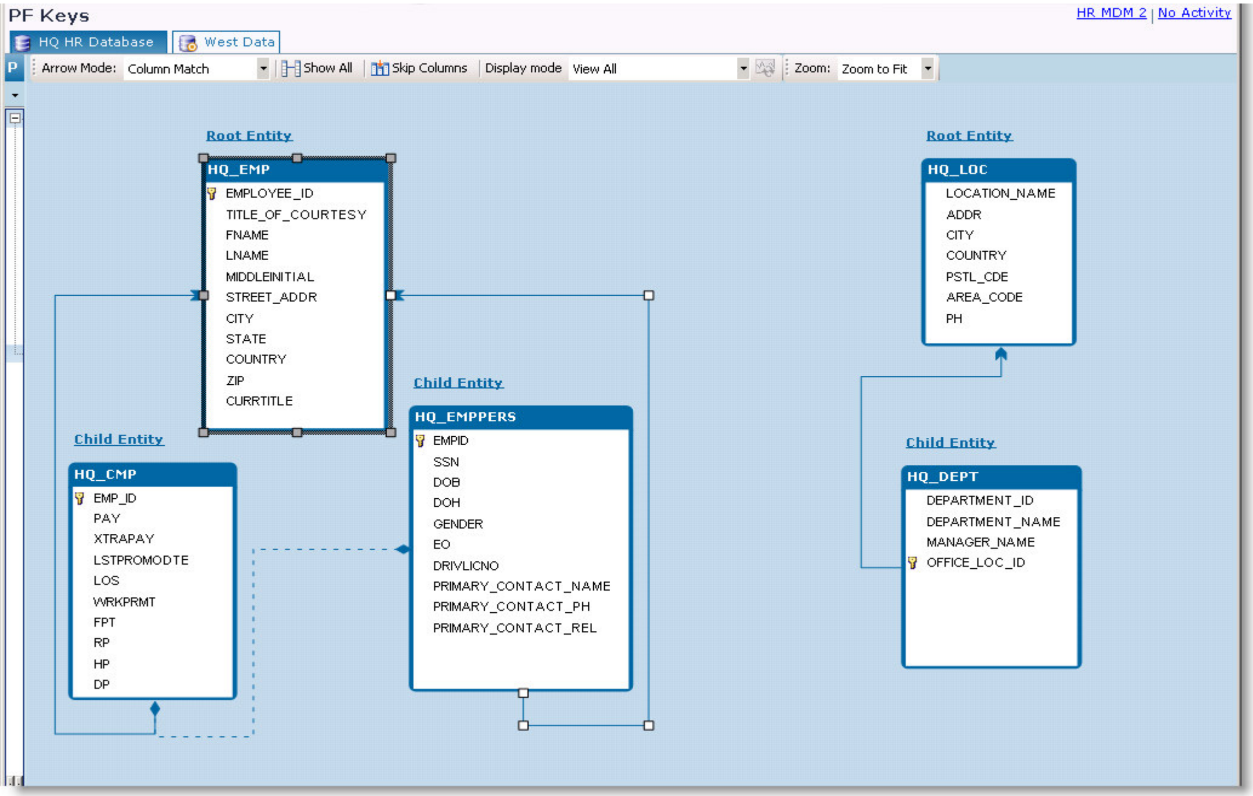
Rule Name	Find PoT Demo CC
Category	PCI
Classification	CreditCard
Description	
Continue on Match	□
Rule Type	Search For Data
Table Type	□ Synonym □ System Table ☑ Table □ View
Table Name Like	
Data Type	□ Date □ Number ☑ Text
Column Name Like	%CARD%
Minimum Length	
Maximum Length	
Search Like	
Search Expression	[0-9]{16}
Maximum Rows	

Classification Rule Actions

1 **add_to_sensitive_objects** (Add to Group of Objects)

InfoSphere Discovery

Accelerate project deployment by automating discovery of your distributed data landscape



PF Keys

Arrow Mode: Column Match

Display mode View All

Zoom: Zoom to Fit

Requirements

- Identify hidden sensitive data requiring protection
- Define business objects for securing sensitive data
- Discover data transformation rules and heterogeneous relationships to secure data

Benefits

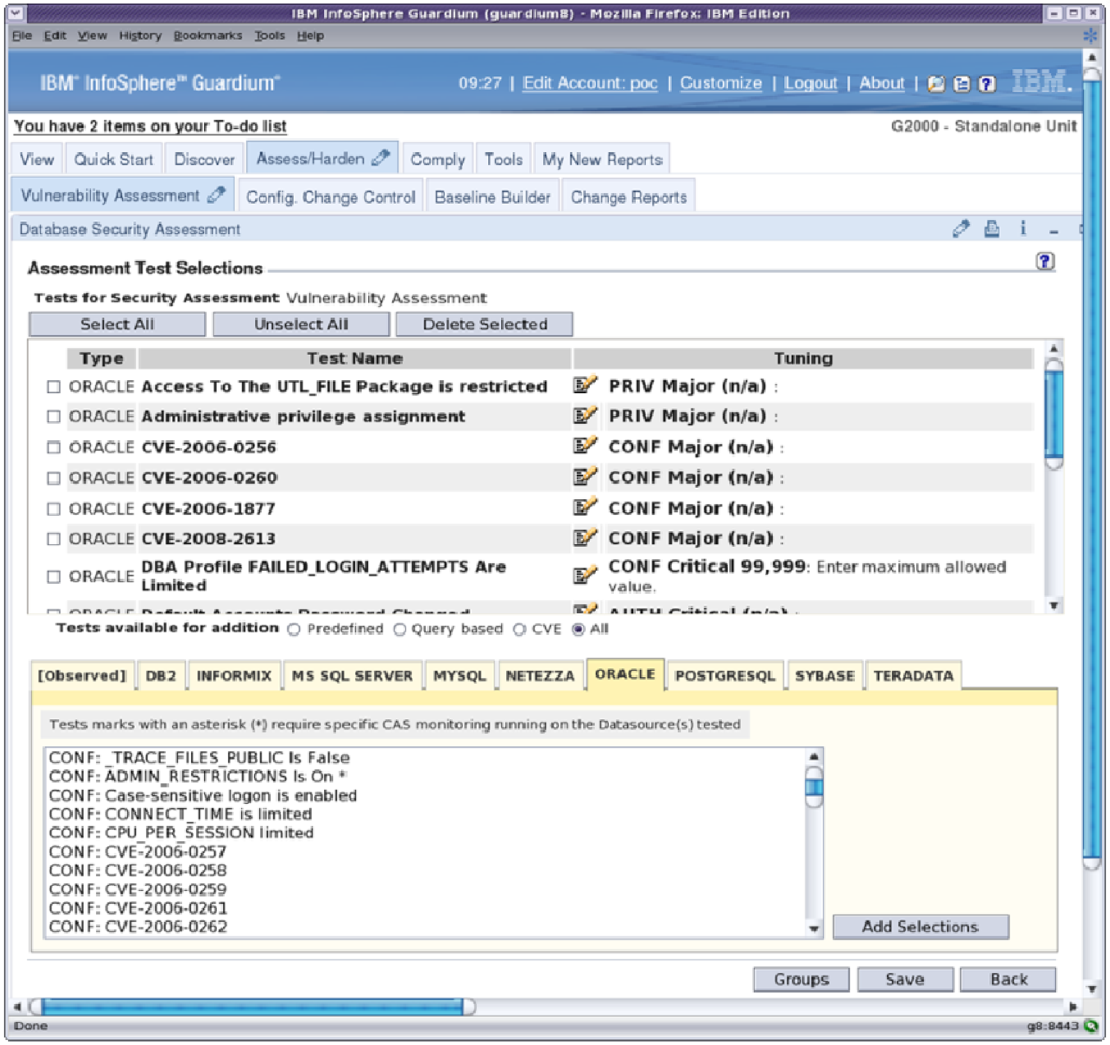
- Minimize risk of breaches by implementing consistent security controls
- Automate manual activities to minimize cost and time while maximizing quality
- Business insight into data relationships reduces project risk

2. Vulnerability and Configuration Assessment

- You need to assess the configuration of your databases to ensure they don't have security holes.
- Verifying the way the database is installed on the operation system.
- Verifying configuration options within the database itself.
- Plus, you need to verify that you're not running database versions with known vulnerabilities.
- Traditional network vulnerability scanners weren't designed for this because they don't have embedded knowledge about database structures and expected behavior, nor can they issue SQL queries (via credentialed access to the database) in order to reveal database configuration information.

InfoSphere Guardium DB Vulnerability Assessment

- Complete suite of VA tests for all nine supported platforms
- Integrated CIS, STIG and CVE identifiers to simplify management and research



You have 2 items on your To-do list

G2000 - Standalone Unit

Database Security Assessment

Assessment Test Selections

Tests for Security Assessment Vulnerability Assessment

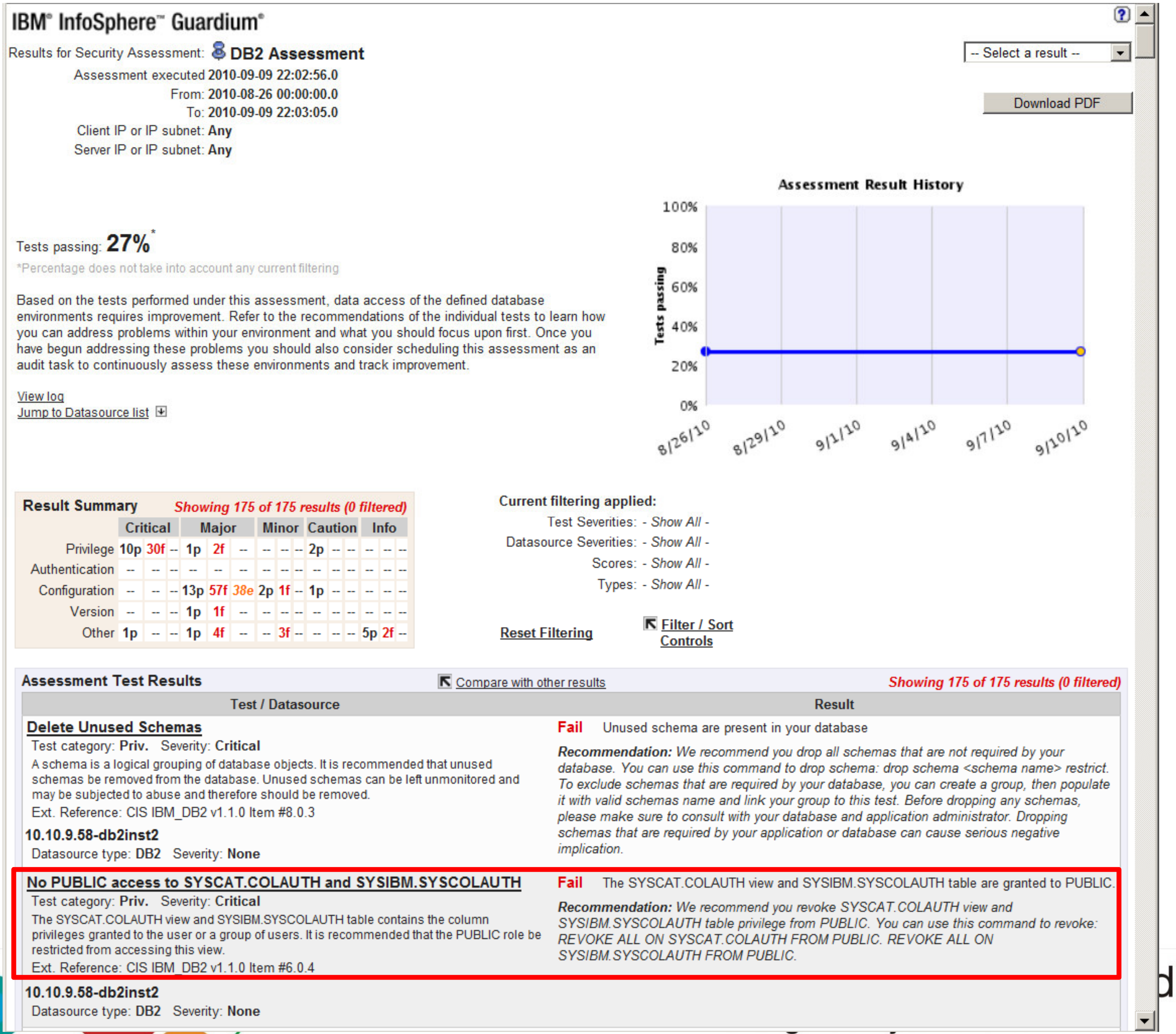
	Type	Test Name	Tuning
□	ORACLE	**Access To The UTL_FILE Package is restricted**	**PRIV Major (n/a)** :
□	ORACLE	**Administrative privilege assignment**	**PRIV Major (n/a)** :
□	ORACLE	**CVE-2006-0256**	**CONF Major (n/a)** :
□	ORACLE	**CVE-2006-0260**	**CONF Major (n/a)** :
□	ORACLE	**CVE-2006-1877**	**CONF Major (n/a)** :
□	ORACLE	**CVE-2008-2613**	**CONF Major (n/a)** :
□	ORACLE	**DBA Profile FAILED_LOGIN_ATTEMPTS Are Limited**	**CONF Critical 99,999**: Enter maximum allowed value.
□	ORACLE	**Default Accounts Password Changed**	**AUTH Critical (n/a)** :

Tests available for addition ○ Predefined ○ Query based ○ CVE ● All

Tests marks with an asterisk (*) require specific CAS monitoring running on the Datasource(s) tested

CONF: _TRACE_FILES_PUBLIC Is False
CONF: ADMIN_RESTRICTIONS Is On *
CONF: Case-sensitive logon is enabled
CONF: CONNECT_TIME is limited
CONF: CPU_PER_SESSION limited
CONF: CVE-2006-0257
CONF: CVE-2006-0258
CONF: CVE-2006-0259
CONF: CVE-2006-0261
CONF: CVE-2006-0262

DB2 Security Assessment



Results for Security Assessment: **DB2 Assessment**

Assessment executed **2010-09-09 22:02:56.0**
From: **2010-08-26 00:00:00.0**
To: **2010-09-09 22:03:05.0**
Client IP or IP subnet: **Any**
Server IP or IP subnet: **Any**

Tests passing: **27%***

*Percentage does not take into account any current filtering

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 175 of 175 results (0 filtered)*

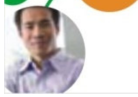
	Critical			Major			Minor			Caution			Info		
Privilege	10p	30f	--	1p	2f	--	--	--	--	2p	--	--	--	--	--
Authentication	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Configuration	--	--	--	13p	57f	38e	2p	1f	--	1p	--	--	--	--	--
Version	--	--	--	1p	1f	--	--	--	--	--	--	--	--	--	--
Other	1p	--	--	1p	4f	--	--	3f	--	--	--	--	5p	2f	--

Current filtering applied:
Test Severities: - *Show All* -
Datasource Severities: - *Show All* -
Scores: - *Show All* -
Types: - *Show All* -

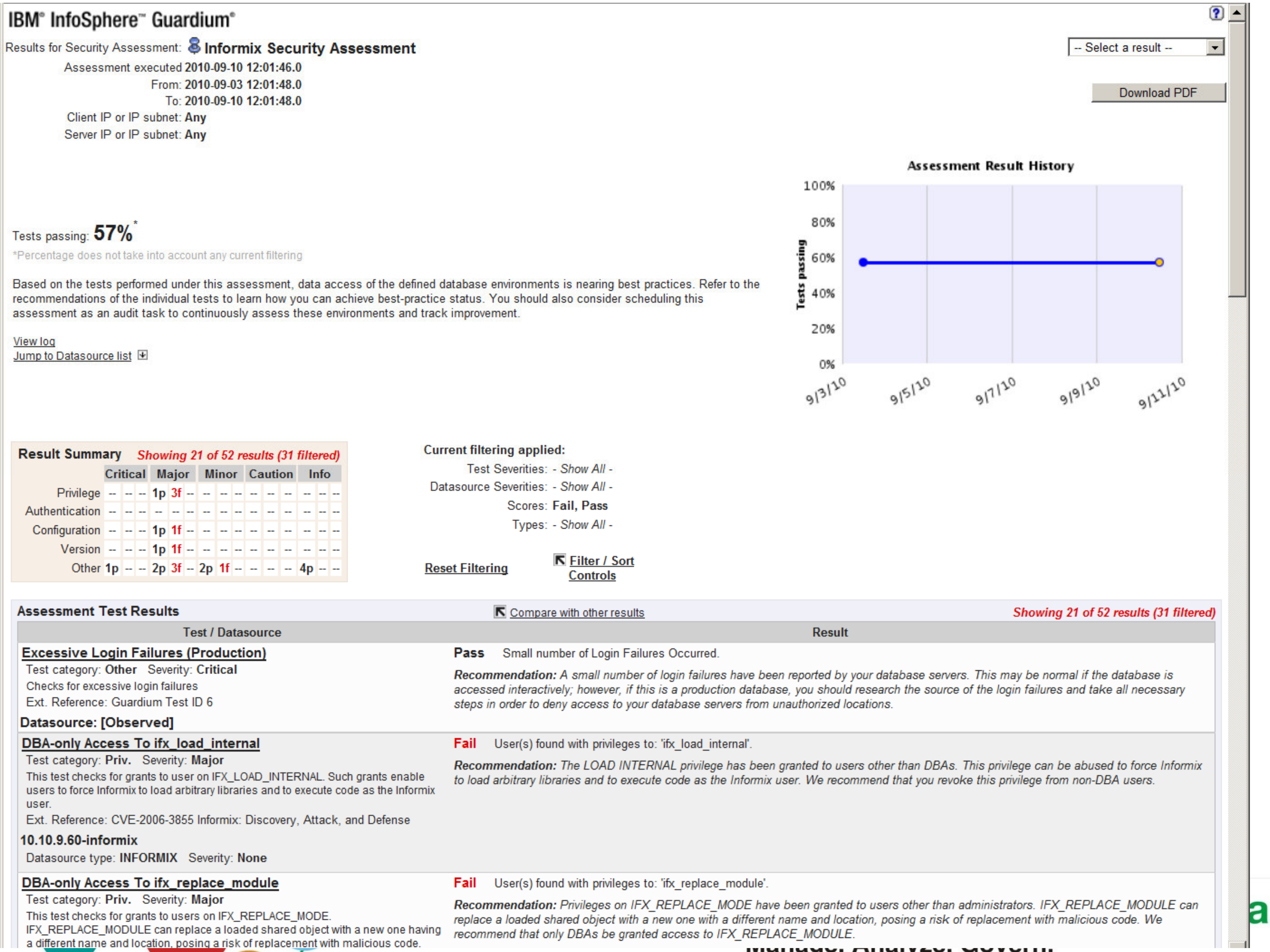
Reset Filtering
Filter / Sort Controls

Assessment Test Results Compare with other results *Showing 175 of 175 results (0 filtered)*

Test / Datasource	Result
Delete Unused Schemas Test category: **Priv.** Severity: **Critical** A schema is a logical grouping of database objects. It is recommended that unused schemas be removed from the database. Unused schemas can be left unmonitored and may be subject to abuse and therefore should be removed. Ext. Reference: CIS IBM_DB2 v1.1.0 Item #8.0.3 **10.10.9.58-db2inst2** Datasource type: **DB2** Severity: **None**	**Fail** Unused schema are present in your database ***Recommendation:*** *We recommend you drop all schemas that are not required by your database. You can use this command to drop schema: drop schema <schema name> restrict. To exclude schemas that are required by your database, you can create a group, then populate it with valid schemas name and link your group to this test. Before dropping any schemas, please make sure to consult with your database and application administrator. Dropping schemas that are required by your application or database can cause serious negative implication.*
No PUBLIC access to SYSCAT.COLAUTH and SYSIBM.SYSCOLAUTH Test category: **Priv.** Severity: **Critical** The SYSCAT.COLAUTH view and SYSIBM.SYSCOLAUTH table contains the column privileges granted to the user or a group of users. It is recommended that the PUBLIC role be restricted from accessing this view. Ext. Reference: CIS IBM_DB2 v1.1.0 Item #6.0.4 **10.10.9.58-db2inst2** Datasource type: **DB2** Severity: **None**	**Fail** The SYSCAT.COLAUTH view and SYSIBM.SYSCOLAUTH table are granted to PUBLIC. ***Recommendation:*** *We recommend you revoke SYSCAT.COLAUTH view and SYSIBM.SYSCOLAUTH table privilege from PUBLIC. You can use this command to revoke: REVOKE ALL ON SYSCAT.COLAUTH FROM PUBLIC. REVOKE ALL ON SYSIBM.SYSCOLAUTH FROM PUBLIC.*



IBM Informix® Security Assessment



Results for Security Assessment: **Informix Security Assessment**

Assessment executed 2010-09-10 12:01:46.0
From: 2010-09-03 12:01:48.0
To: 2010-09-10 12:01:48.0
Client IP or IP subnet: Any
Server IP or IP subnet: Any

Tests passing: **57%***

*Percentage does not take into account any current filtering

Based on the tests performed under this assessment, data access of the defined database environments is nearing best practices. Refer to the recommendations of the individual tests to learn how you can achieve best-practice status. 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 21 of 52 results (31 filtered)*

	Critical			Major			Minor			Caution			Info		
Privilege	--	--	--	1p	3f	--	--	--	--	--	--	--	--	--	--
Authentication	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Configuration	--	--	--	1p	1f	--	--	--	--	--	--	--	--	--	--
Version	--	--	--	1p	1f	--	--	--	--	--	--	--	--	--	--
Other	1p	--	--	2p	3f	--	2p	1f	--	--	--	--	4p	--	--

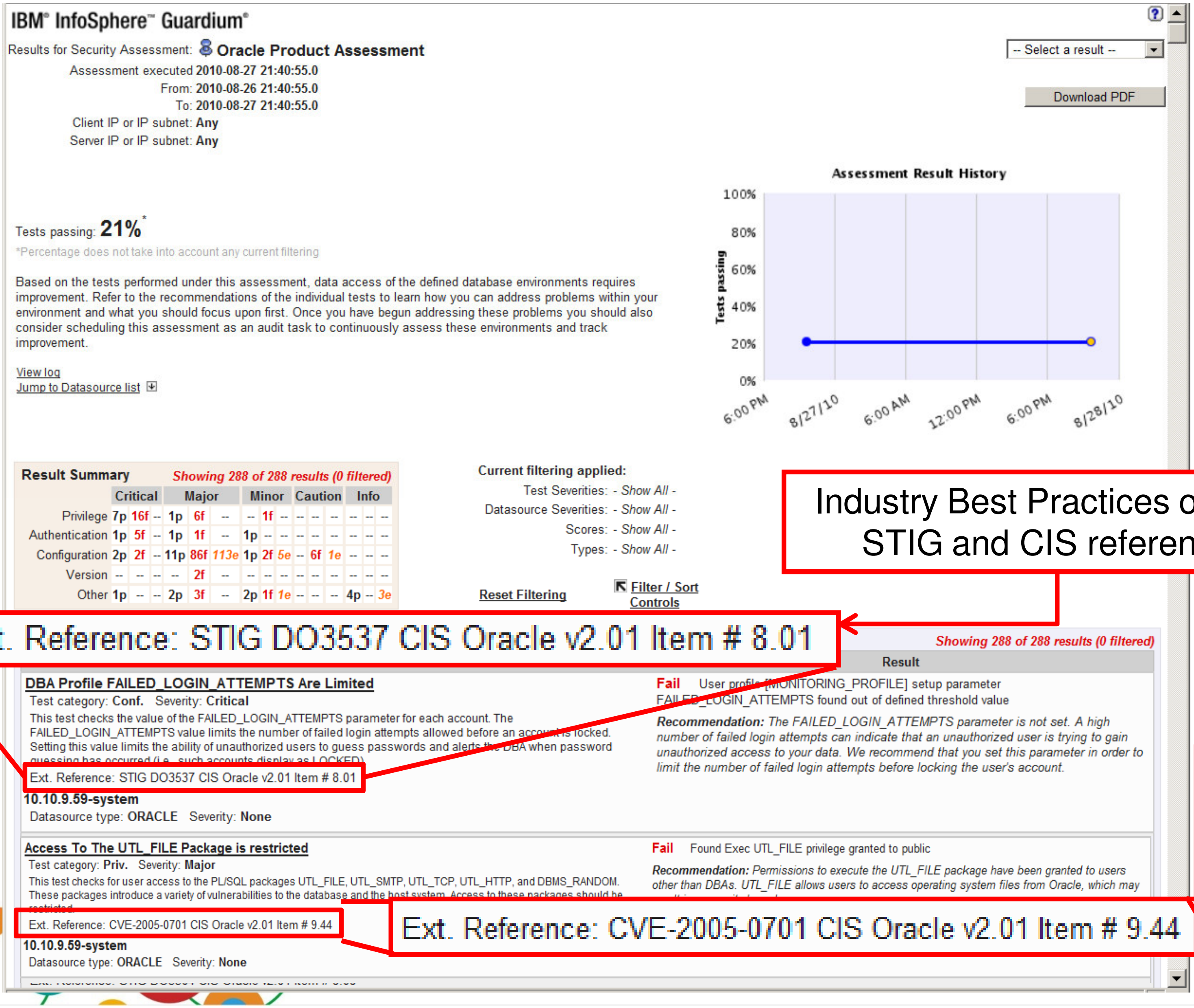
Current filtering applied:
Test Severities: *- Show All -*
Datasource Severities: *- Show All -*
Scores: **Fail, Pass**
Types: *- Show All -*

Reset Filtering Filter / Sort Controls

Assessment Test Results Compare with other results *Showing 21 of 52 results (31 filtered)*

Test / Datasource	Result
Excessive Login Failures (Production) Test category: Other Severity: **Critical** Checks for excessive login failures Ext. Reference: Guardium Test ID 6 **Datasource: [Observed]**	**Pass** Small number of Login Failures Occurred. ***Recommendation:*** *A small number of login failures have been reported by your database servers. This may be normal if the database is accessed interactively; however, if this is a production database, you should research the source of the login failures and take all necessary steps in order to deny access to your database servers from unauthorized locations.*
DBA-only Access To ifx_load_internal Test category: **Priv.** Severity: **Major** This test checks for grants to user on IFX_LOAD_INTERNAL. Such grants enable users to force Informix to load arbitrary libraries and to execute code as the Informix user. Ext. Reference: CVE-2006-3855 Informix: Discovery, Attack, and Defense **10.10.9.60-informix** Datasource type: **INFORMIX** Severity: **None**	**Fail** User(s) found with privileges to: 'ifx_load_internal'. ***Recommendation:*** *The LOAD INTERNAL privilege has been granted to users other than DBAs. This privilege can be abused to force Informix to load arbitrary libraries and to execute code as the Informix user. We recommend that you revoke this privilege from non-DBA users.*
DBA-only Access To ifx_replace_module Test category: **Priv.** Severity: **Major** This test checks for grants to users on IFX_REPLACE_MODE. IFX_REPLACE_MODULE can replace a loaded shared object with a new one having a different name and location, posing a risk of replacement with malicious code.	**Fail** User(s) found with privileges to: 'ifx_replace_module'. ***Recommendation:*** *Privileges on IFX_REPLACE_MODE have been granted to users other than administrators. IFX_REPLACE_MODULE can replace a loaded shared object with a new one with a different name and location, posing a risk of replacement with malicious code. We recommend that only DBAs be granted access to IFX_REPLACE_MODULE.*

Oracle Security Assessment



Results for Security Assessment: **Oracle Product Assessment**

Assessment executed **2010-08-27 21:40:55.0**
From: **2010-08-26 21:40:55.0**
To: **2010-08-27 21:40:55.0**
Client IP or IP subnet: **Any**
Server IP or IP subnet: **Any**

Tests passing: **21%***

*Percentage does not take into account any current filtering

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 288 of 288 results (0 filtered)*

	Critical			Major			Minor			Caution			Info		
Privilege	7p	16f	--	1p	6f	--	--	1f	--	--	--	--	--	--	--
Authentication	1p	5f	--	1p	1f	--	1p	--	--	--	--	--	--	--	--
Configuration	2p	2f	--	11p	86f	*113e*	1p	2f	*5e*	--	6f	*1e*	--	--	--
Version	--	--	--	--	2f	--	--	--	--	--	--	--	--	--	--
Other	1p	--	--	2p	3f	--	2p	1f	*1e*	--	--	--	4p	--	*3e*

Current filtering applied:
Test Severities: - *Show All* -
Datasource Severities: - *Show All* -
Scores: - *Show All* -
Types: - *Show All* -

Reset Filtering
Filter / Sort Controls

Showing 288 of 288 results (0 filtered)

Result

DBA Profile FAILED_LOGIN_ATTEMPTS Are Limited
Test category: **Conf.** Severity: **Critical**
This test checks the value of the FAILED_LOGIN_ATTEMPTS parameter for each account. The FAILED_LOGIN_ATTEMPTS value limits the number of failed login attempts allowed before an account is locked. Setting this value limits the ability of unauthorized users to guess passwords and alerts the DBA when password guessing has occurred (i.e., such accounts display as LOCKED).
Ext. Reference: STIG DO3537 CIS Oracle v2.01 Item # 8.01
10.10.9.59-system
Datasource type: **ORACLE** Severity: **None**

Fail User profile [MONITORING_PROFILE] setup parameter FAILED_LOGIN_ATTEMPTS found out of defined threshold value

Recommendation: *The FAILED_LOGIN_ATTEMPTS parameter is not set. A high number of failed login attempts can indicate that an unauthorized user is trying to gain unauthorized access to your data. We recommend that you set this parameter in order to limit the number of failed login attempts before locking the user's account.*

Access To The UTL_FILE Package is restricted
Test category: **Priv.** Severity: **Major**
This test checks for user access to the PL/SQL packages UTL_FILE, UTL_SMTP, UTL_TCP, UTL_HTTP, and DBMS_RANDOM. These packages introduce a variety of vulnerabilities to the database and the host system. Access to these packages should be restricted.
Ext. Reference: CVE-2005-0701 CIS Oracle v2.01 Item # 9.44
10.10.9.59-system
Datasource type: **ORACLE** Severity: **None**

Fail Found Exec UTL_FILE privilege granted to public

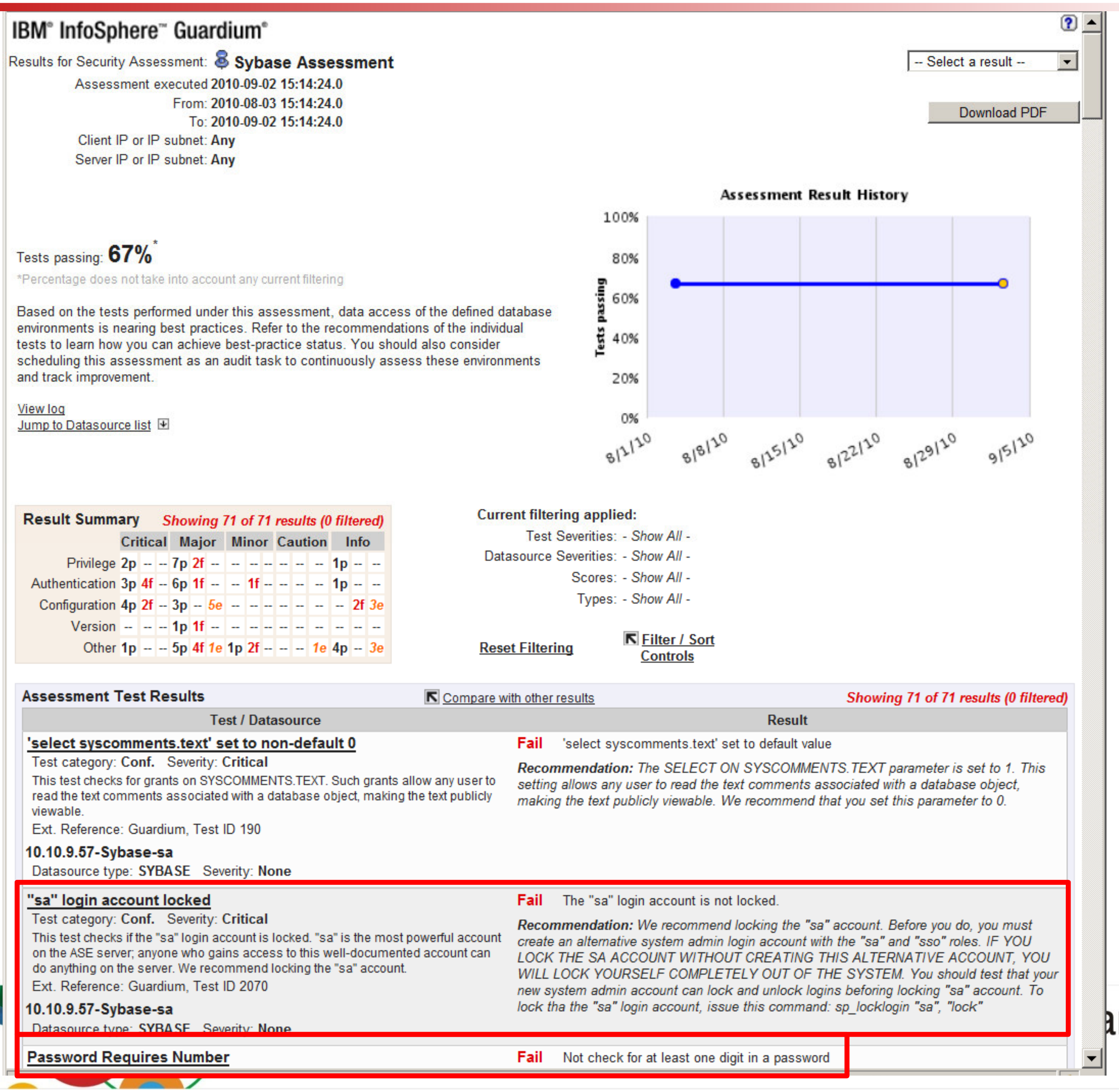
Recommendation: *Permissions to execute the UTL_FILE package have been granted to users other than DBAs. UTL_FILE allows users to access operating system files from Oracle, which may*

Industry Best Practices of CVE, STIG and CIS references

Ext. Reference: STIG DO3537 CIS Oracle v2.01 Item # 8.01

Ext. Reference: CVE-2005-0701 CIS Oracle v2.01 Item # 9.44

Sybase Security Assessment



Results for Security Assessment: **Sybase Assessment**

Assessment executed 2010-09-02 15:14:24.0
From: 2010-08-03 15:14:24.0
To: 2010-09-02 15:14:24.0
Client IP or IP subnet: **Any**
Server IP or IP subnet: **Any**

Tests passing: **67%***

*Percentage does not take into account any current filtering

Based on the tests performed under this assessment, data access of the defined database environments is nearing best practices. Refer to the recommendations of the individual tests to learn how you can achieve best-practice status. 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 71 of 71 results (0 filtered)*

	Critical			Major			Minor			Caution			Info		
Privilege	2p	--	--	7p	2f	--	--	--	--	--	--	--	1p	--	--
Authentication	3p	4f	--	6p	1f	--	--	1f	--	--	--	--	1p	--	--
Configuration	4p	2f	--	3p	--	5e	--	--	--	--	--	--	--	2f	3e
Version	--	--	--	1p	1f	--	--	--	--	--	--	--	--	--	--
Other	1p	--	--	5p	4f	1e	1p	2f	--	--	--	1e	4p	--	3e

Current filtering applied:
Test Severities: *- Show All -*
Datasource Severities: *- Show All -*
Scores: *- Show All -*
Types: *- Show All -*

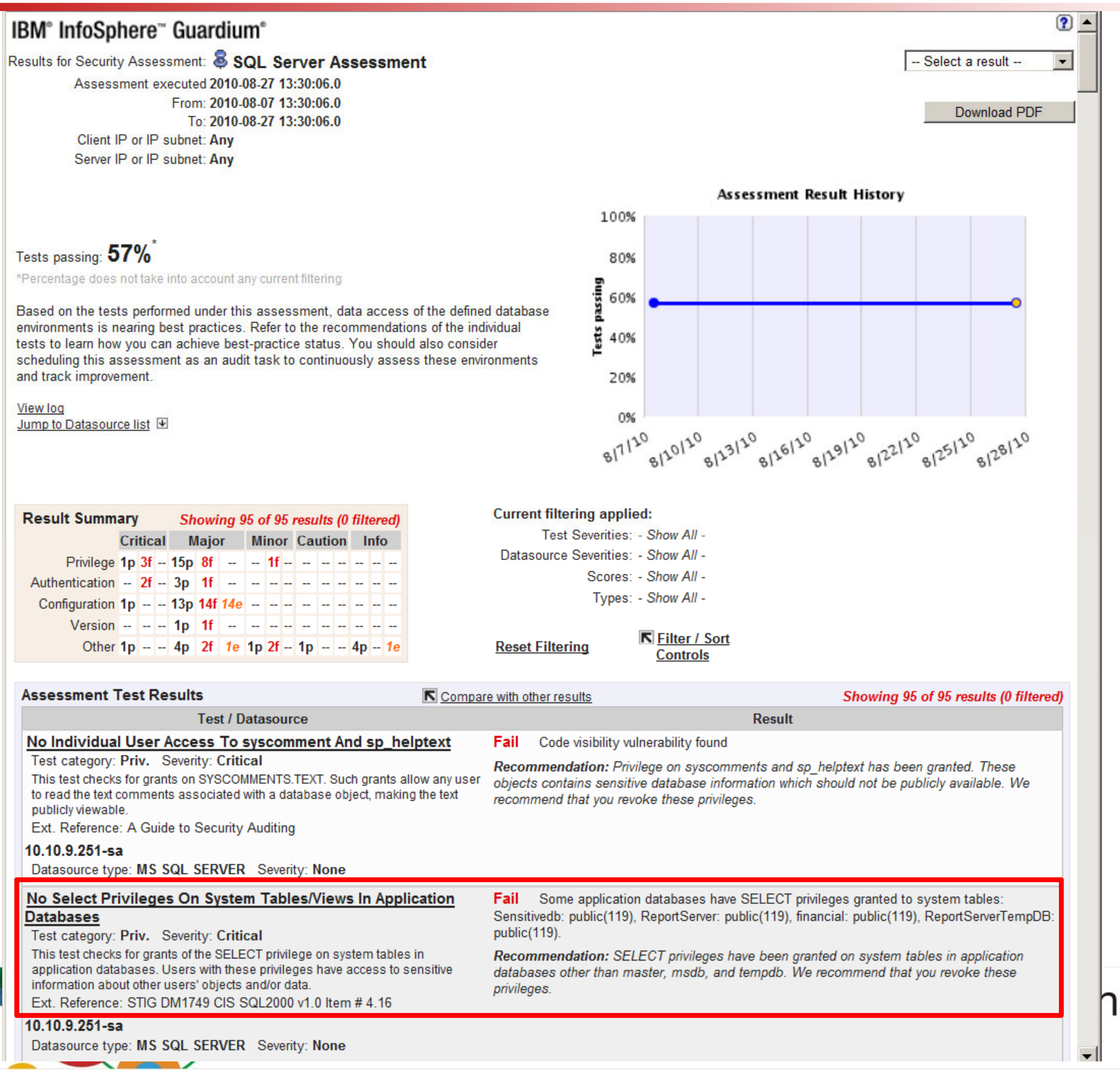
Reset Filtering   Filter / Sort Controls

Assessment Test Results   Compare with other results   *Showing 71 of 71 results (0 filtered)*

Test / Datasource	Result
'select syscomments.text' set to non-default 0 Test category: **Conf.** Severity: **Critical** This test checks for grants on SYSCOMMENTS.TEXT. Such grants allow any user to read the text comments associated with a database object, making the text publicly viewable. Ext. Reference: Guardium, Test ID 190 **10.10.9.57-Sybase-sa** Datasource type: **SYBASE** Severity: **None**	**Fail** 'select syscomments.text' set to default value ***Recommendation:*** *The SELECT ON SYSCOMMENTS.TEXT parameter is set to 1. This setting allows any user to read the text comments associated with a database object, making the text publicly viewable. We recommend that you set this parameter to 0.*
"sa" login account locked Test category: **Conf.** Severity: **Critical** This test checks if the "sa" login account is locked. "sa" is the most powerful account on the ASE server; anyone who gains access to this well-documented account can do anything on the server. We recommend locking the "sa" account. Ext. Reference: Guardium, Test ID 2070 **10.10.9.57-Sybase-sa** Datasource type: **SYBASE** Severity: **None**	**Fail** The "sa" login account is not locked. ***Recommendation:*** *We recommend locking the "sa" account. Before you do, you must create an alternative system admin login account with the "sa" and "sso" roles. IF YOU LOCK THE SA ACCOUNT WITHOUT CREATING THIS ALTERNATIVE ACCOUNT, YOU WILL LOCK YOURSELF COMPLETELY OUT OF THE SYSTEM. You should test that your new system admin account can lock and unlock logins beforing locking "sa" account. To lock tha the "sa" login account, issue this command: sp_locklogin "sa", "lock"*
Password Requires Number	**Fail** Not check for at least one digit in a password

andIndia2011

Microsoft SQL Server™ Security Assessment



IBM® InfoSphere™ Guardium®

Results for Security Assessment: **SQL Server Assessment**

Assessment executed **2010-08-27 13:30:06.0**
From: **2010-08-07 13:30:06.0**
To: **2010-08-27 13:30:06.0**
Client IP or IP subnet: **Any**
Server IP or IP subnet: **Any**

Tests passing: **57%***

*Percentage does not take into account any current filtering

Based on the tests performed under this assessment, data access of the defined database environments is nearing best practices. Refer to the recommendations of the individual tests to learn how you can achieve best-practice status. 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 95 of 95 results (0 filtered)*

	Critical			Major			Minor			Caution			Info		
Privilege	1p	3f	--	15p	8f	--	--	1f	--	--	--	--	--	--	--
Authentication	--	2f	--	3p	1f	--	--	--	--	--	--	--	--	--	--
Configuration	1p	--	--	13p	14f	14e	--	--	--	--	--	--	--	--	--
Version	--	--	--	1p	1f	--	--	--	--	--	--	--	--	--	--
Other	1p	--	--	4p	2f	1e	1p	2f	--	1p	--	--	4p	--	1e

Current filtering applied:
Test Severities: *- Show All -*
Datasource Severities: *- Show All -*
Scores: *- Show All -*
Types: *- Show All -*

Reset Filtering
Filter / Sort Controls

Assessment Test Results Compare with other results *Showing 95 of 95 results (0 filtered)*

Test / Datasource	Result
No Individual User Access To syscomment And sp_helptext Test category: **Priv.** Severity: **Critical** This test checks for grants on SYSCOMMENTS.TEXT. Such grants allow any user to read the text comments associated with a database object, making the text publicly viewable. Ext. Reference: A Guide to Security Auditing **10.10.9.251-sa** Datasource type: **MS SQL SERVER** Severity: **None**	**Fail** Code visibility vulnerability found ***Recommendation:*** *Privilege on syscomments and sp_helptext has been granted. These objects contains sensitive database information which should not be publicly available. We recommend that you revoke these privileges.*
No Select Privileges On System Tables/Views In Application Databases Test category: **Priv.** Severity: **Critical** This test checks for grants of the SELECT privilege on system tables in application databases. Users with these privileges have access to sensitive information about other users' objects and/or data. Ext. Reference: STIG DM1749 CIS SQL2000 v1.0 Item # 4.16 **10.10.9.251-sa** Datasource type: **MS SQL SERVER** Severity: **None**	**Fail** Some application databases have SELECT privileges granted to system tables: Sensitivedb: public(119), ReportServer: public(119), financial: public(119), ReportServerTempDB: public(119). ***Recommendation:*** *SELECT privileges have been granted on system tables in application databases other than master, msdb, and tempdb. We recommend that you revoke these privileges.*

3. Hardening

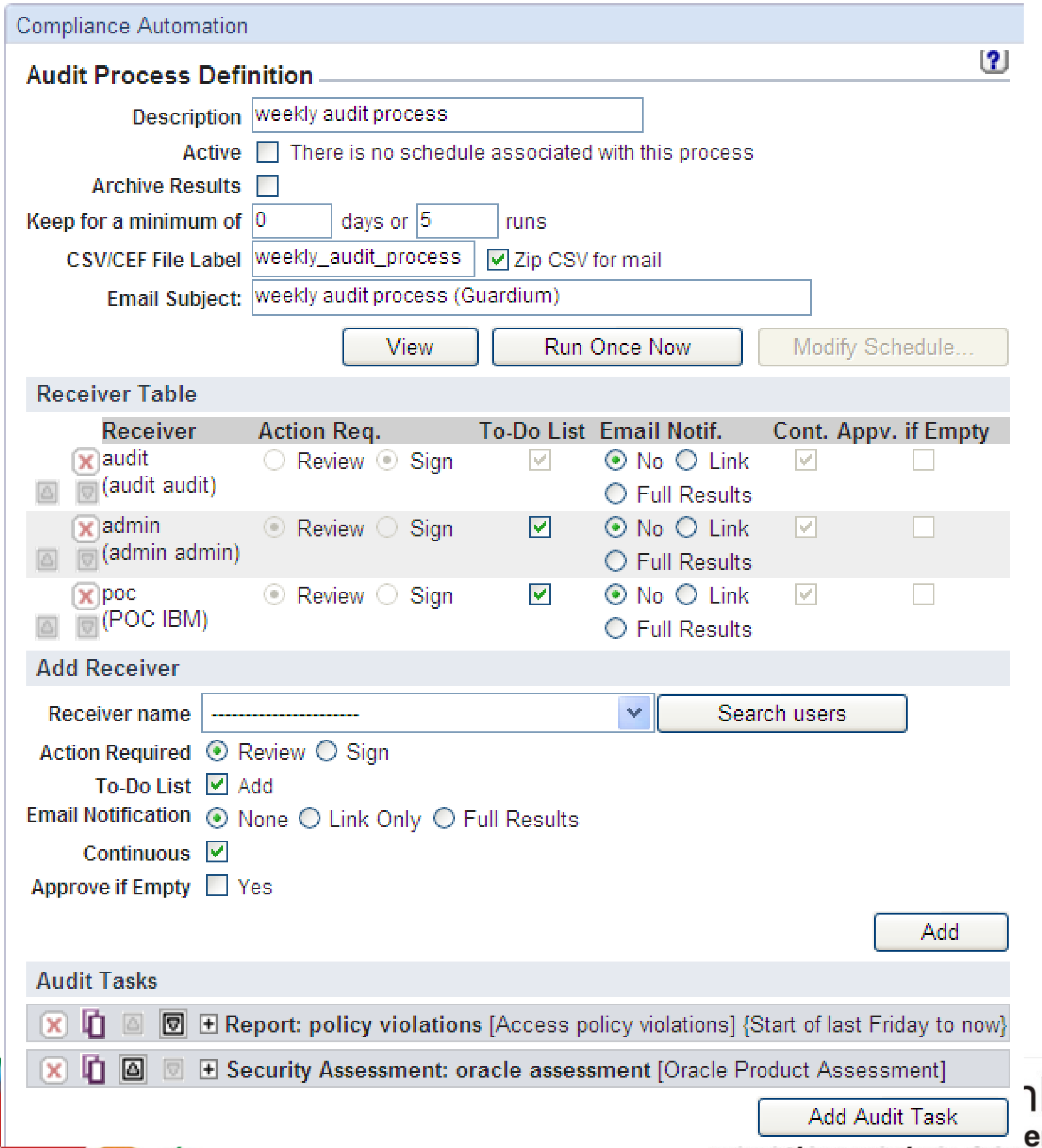
- The result of a vulnerability assessment is often a set of specific recommendations. This is the first step in hardening the database. Other elements of hardening involve removing all functions and options that you do not use.

4. Change Auditing

- Once you’ve created a hardened configuration, you must continually track it to ensure that you don’t digress from your “gold” (secure) configuration.

- You can do this with change auditing tools that compare snapshots of the configurations (at both the operating system level and at the database level) and immediately alert you whenever a change is made that could affect the security of the database.

InfoSphere Guardium Compliance Workflow Automation



Compliance Automation

Audit Process Definition

Description	weekly audit process
Active	□ There is no schedule associated with this process
Archive Results	□
Keep for a minimum of	0 days or 5 runs
CSV/CEF File Label	weekly_audit_process ☑ Zip CSV for mail
Email Subject:	weekly audit process (Guardium)

Receiver Table

Receiver	Action Req.	To-Do List	Email Notif.	Cont.	Appv. if Empty
audit (audit audit)	○ Review ● Sign	☑	● No ○ Link ○ Full Results	☑	□
admin (admin admin)	● Review ○ Sign	☑	● No ○ Link ○ Full Results	☑	□
poc (POC IBM)	● Review ○ Sign	☑	● No ○ Link ○ Full Results	☑	□

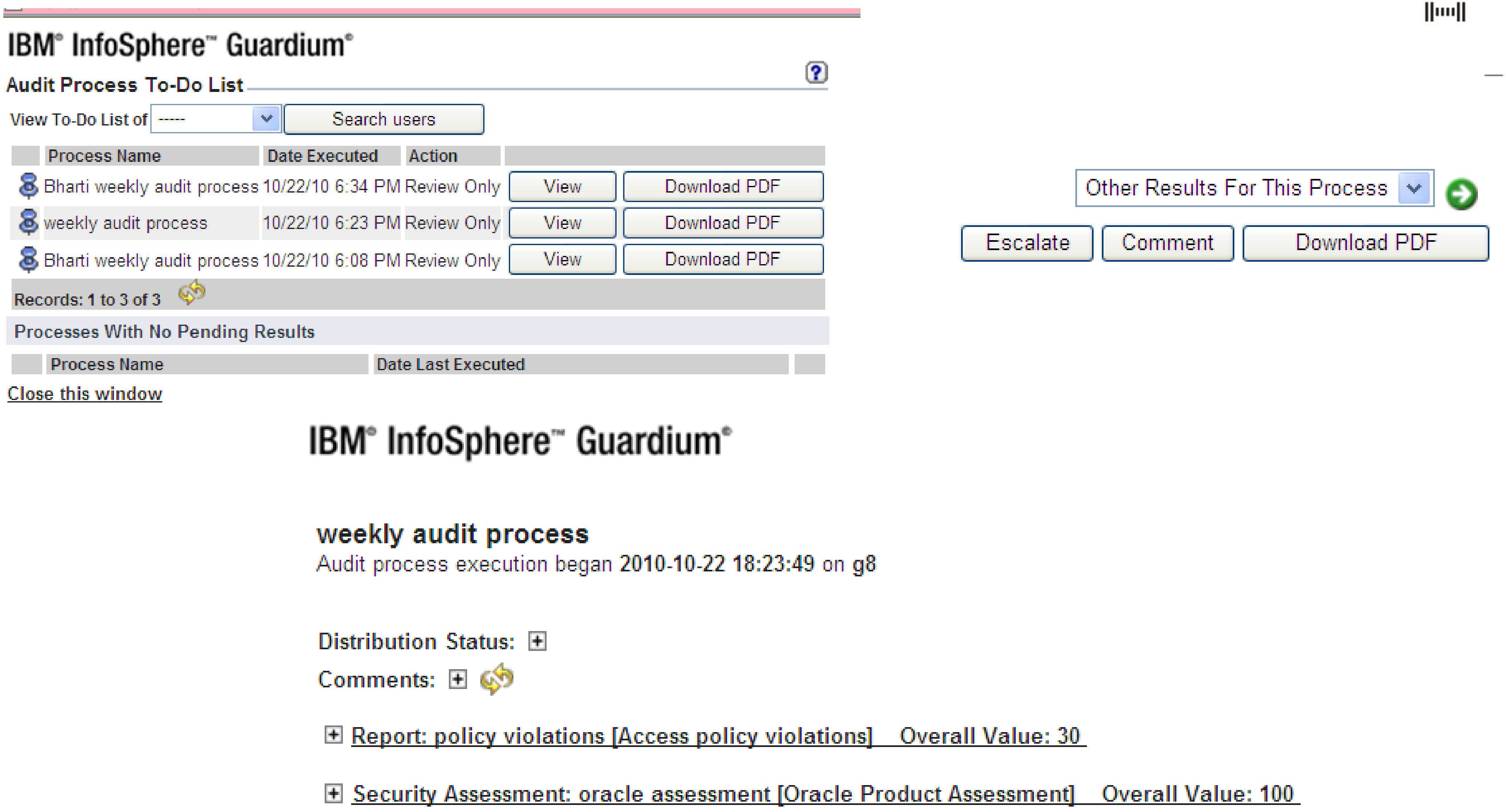
Add Receiver

Receiver name	-----------------------
Action Required	● Review ○ Sign
To-Do List	☑ Add
Email Notification	● None ○ Link Only ○ Full Results
Continuous	☑
Approve if Empty	□ Yes

Audit Tasks

- **Report: policy violations** [Access policy violations] {Start of last Friday to now}
- **Security Assessment: oracle assessment** [Oracle Product Assessment]

InfoSphere Guardium Compliance Workflow Automation



IBM® InfoSphere™ Guardium®

Audit Process To-Do List

View To-Do List of ----- Search users

	Process Name	Date Executed	Action		
	Bharti weekly audit process	10/22/10 6:34 PM	Review Only	View	Download PDF
	weekly audit process	10/22/10 6:23 PM	Review Only	View	Download PDF
	Bharti weekly audit process	10/22/10 6:08 PM	Review Only	View	Download PDF

Records: 1 to 3 of 3

Processes With No Pending Results

	Process Name	Date Last Executed	

Close this window

IBM® InfoSphere™ Guardium®

weekly audit process

Audit process execution began 2010-10-22 18:23:49 on g8

Distribution Status: ⊞

Comments: ⊞

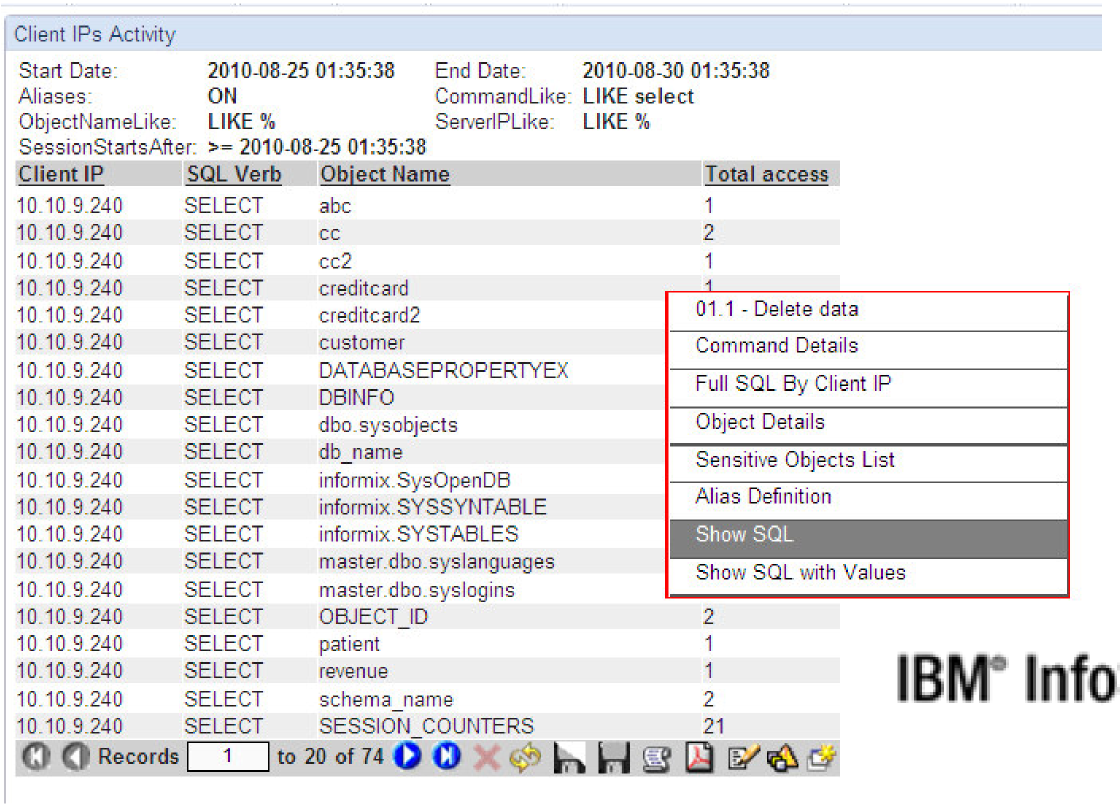
⊞ Report: policy violations [Access policy violations]   Overall Value: 30

⊞ Security Assessment: oracle assessment [Oracle Product Assessment]   Overall Value: 100

5. Database Activity Monitoring (DAM)

- Real-time monitoring of database activity is key to limiting your exposure by immediately detecting intrusions and misuse.
- For example, DAM can alert on unusual access patterns indicating a SQL injection attack, unauthorized changes to financial data, elevation of account privileges, and configuration changes executed via SQL commands.
- Monitoring privileged users is also a requirement for data governance regulations such as SOX and data privacy regulations such as PCI DSS.
- Finally, some DAM technologies offer application-layer monitoring, allowing you to detect fraud conducted via multi-tier applications such as PeopleSoft, SAP and Oracle e-Business Suite, rather than via direct connections to the database.

InfoSphere Guardium Report Builder – Visibility



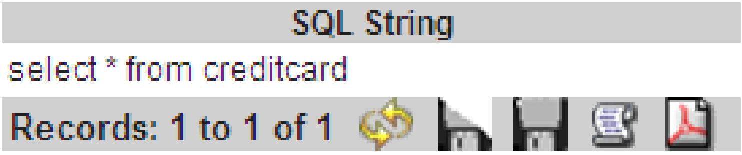
Client IPs Activity

Start Date: 2010-08-25 01:35:38 End Date: 2010-08-30 01:35:38
Aliases: ON CommandLike: LIKE select
ObjectNameLike: LIKE % ServerIPLike: LIKE %
SessionStartsAfter: >= 2010-08-25 01:35:38

Client IP	SQL Verb	Object Name	Total access
10.10.9.240	SELECT	abc	1
10.10.9.240	SELECT	cc	2
10.10.9.240	SELECT	cc2	1
10.10.9.240	SELECT	creditcard	1
10.10.9.240	SELECT	creditcard2	
10.10.9.240	SELECT	customer	
10.10.9.240	SELECT	DATABASEPROPERTYEX	
10.10.9.240	SELECT	DBINFO	
10.10.9.240	SELECT	dbo.sysobjects	
10.10.9.240	SELECT	db_name	
10.10.9.240	SELECT	informix.SysOpenDB	
10.10.9.240	SELECT	informix.SYSSYNTABLE	
10.10.9.240	SELECT	informix.SYSTABLES	
10.10.9.240	SELECT	master.dbo.syslanguages	
10.10.9.240	SELECT	master.dbo.syslogins	
10.10.9.240	SELECT	OBJECT_ID	2
10.10.9.240	SELECT	patient	1
10.10.9.240	SELECT	revenue	1
10.10.9.240	SELECT	schema_name	2
10.10.9.240	SELECT	SESSION_COUNTERS	21

Records 1 to 20 of 74

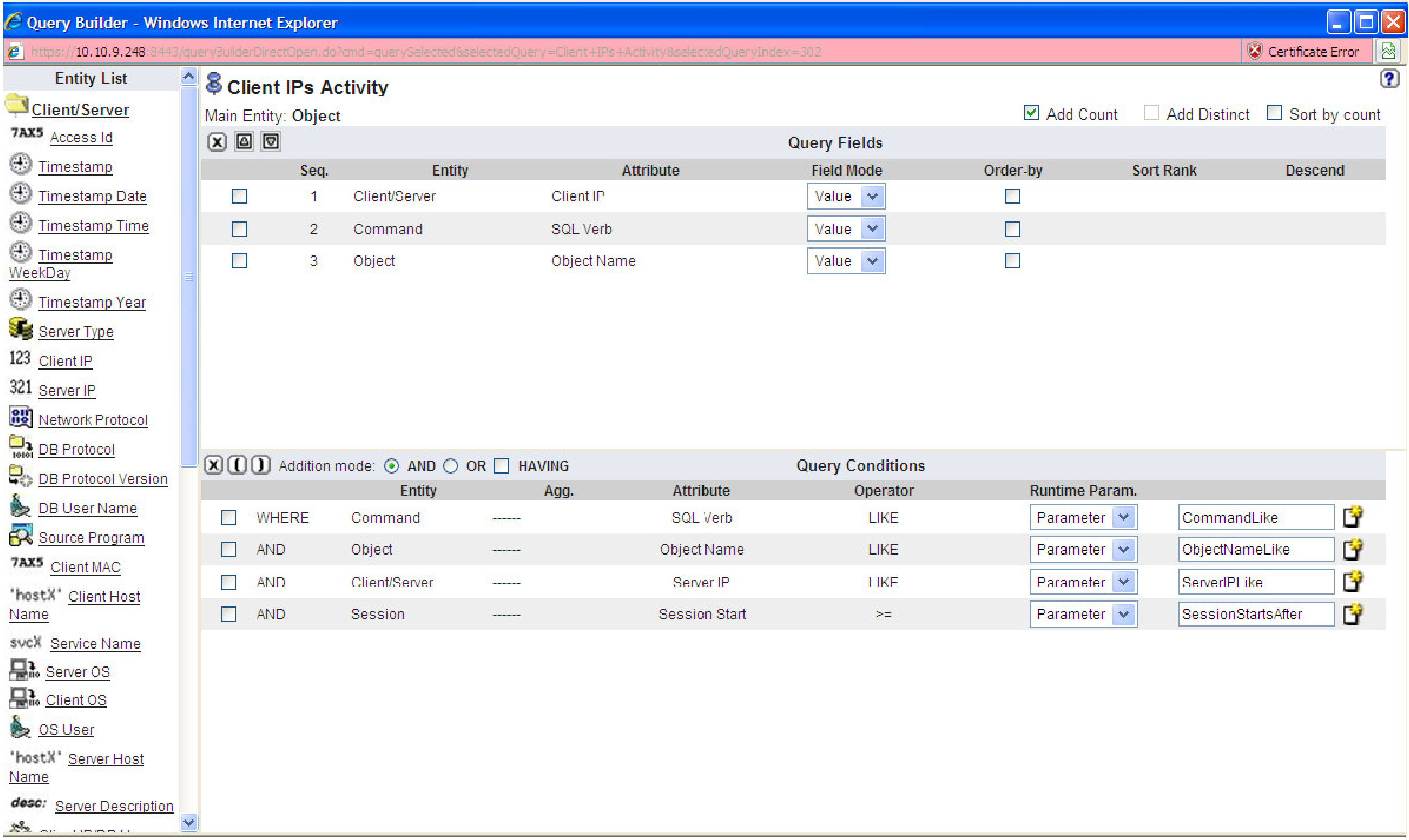
IBM® InfoSphere™ Guardium®



SQL String
select * from creditcard

Records: 1 to 1 of 1

Report Builder – Visibility



Query Builder - Windows Internet Explorer
https://10.10.9.248:8443/queryBuilderDirectOpen.do?cmd=querySelected&selectedQuery=Client+IPs+Activity&selectedQueryIndex=302
Certificate Error

Entity List

- Client/Server
- Access Id
- Timestamp
- Timestamp Date
- Timestamp Time
- Timestamp WeekDay
- Timestamp Year
- Server Type
- Client IP
- Server IP
- Network Protocol
- DB Protocol
- DB Protocol Version
- DB User Name
- Source Program
- Client MAC
- Client Host Name
- Service Name
- Server OS
- Client OS
- OS User
- Server Host Name
- Server Description

Client IPs Activity

Main Entity: Object

☑ Add Count □ Add Distinct □ Sort by count

Query Fields

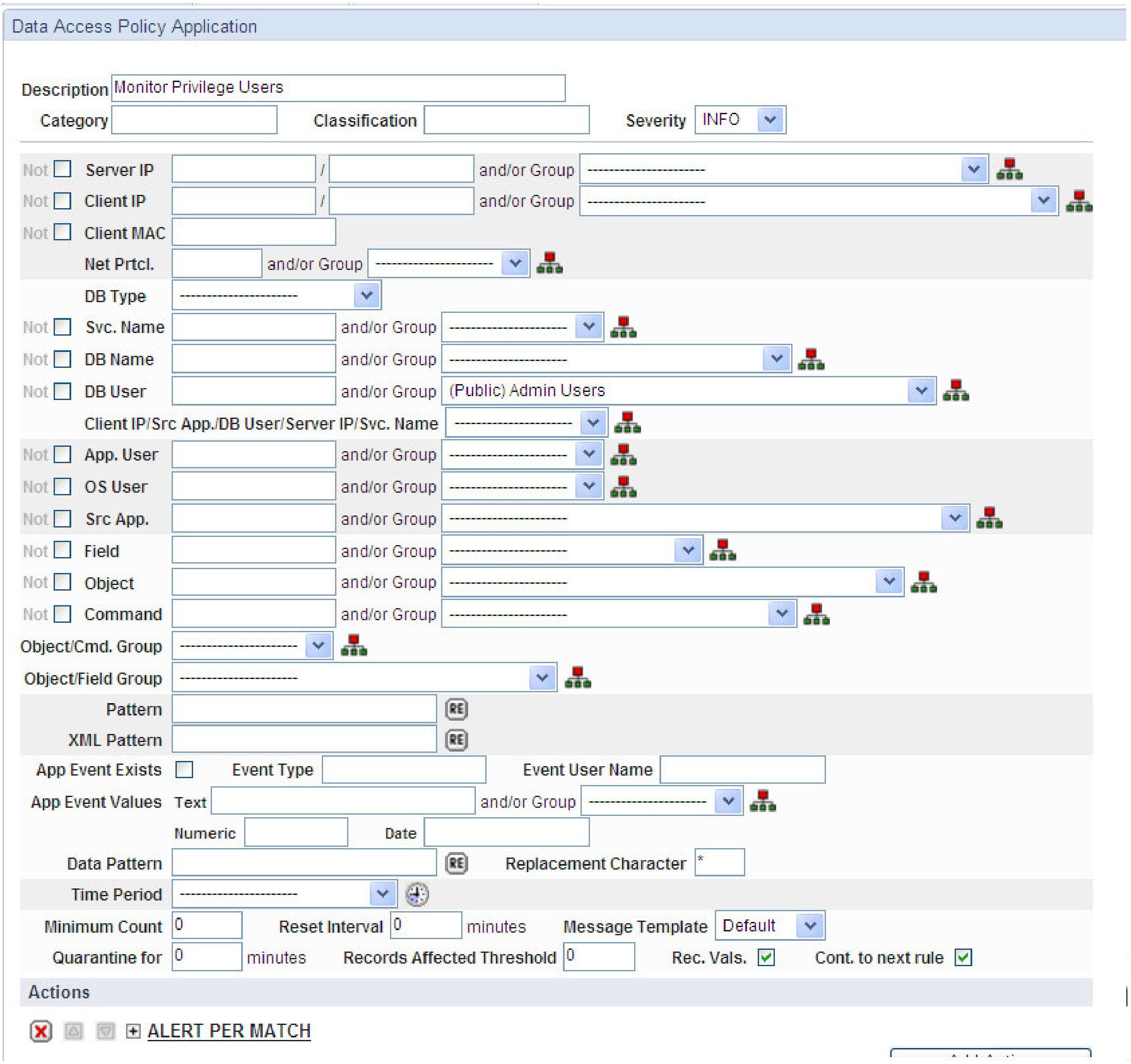
	Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
□	1	Client/Server	Client IP	Value	□		
□	2	Command	SQL Verb	Value	□		
□	3	Object	Object Name	Value	□		

Addition mode: ● AND ○ OR □ HAVING

Query Conditions

		Entity	Agg.	Attribute	Operator	Runtime Param.	
□	WHERE	Command	------	SQL Verb	LIKE	Parameter	CommandLike
□	AND	Object	------	Object Name	LIKE	Parameter	ObjectNameLike
□	AND	Client/Server	------	Server IP	LIKE	Parameter	ServerIPLike
□	AND	Session	------	Session Start	>=	Parameter	SessionStartsAfter

InfoSphere Guardium Policy – Detection – Real time alert



Data Access Policy Application

Description: Monitor Privilege Users

Category: | Classification: | Severity: INFO

Not □ Server IP: / | and/or Group: ---------------------

Not □ Client IP: / | and/or Group: ---------------------

Not □ Client MAC:

Net Prtcl.: | and/or Group: ---------------------

DB Type: ---------------------

Not □ Svc. Name: | and/or Group: ---------------------

Not □ DB Name: | and/or Group: ---------------------

Not □ DB User: | and/or Group: (Public) Admin 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: ---------------------

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 Character: *

Time Period: ---------------------

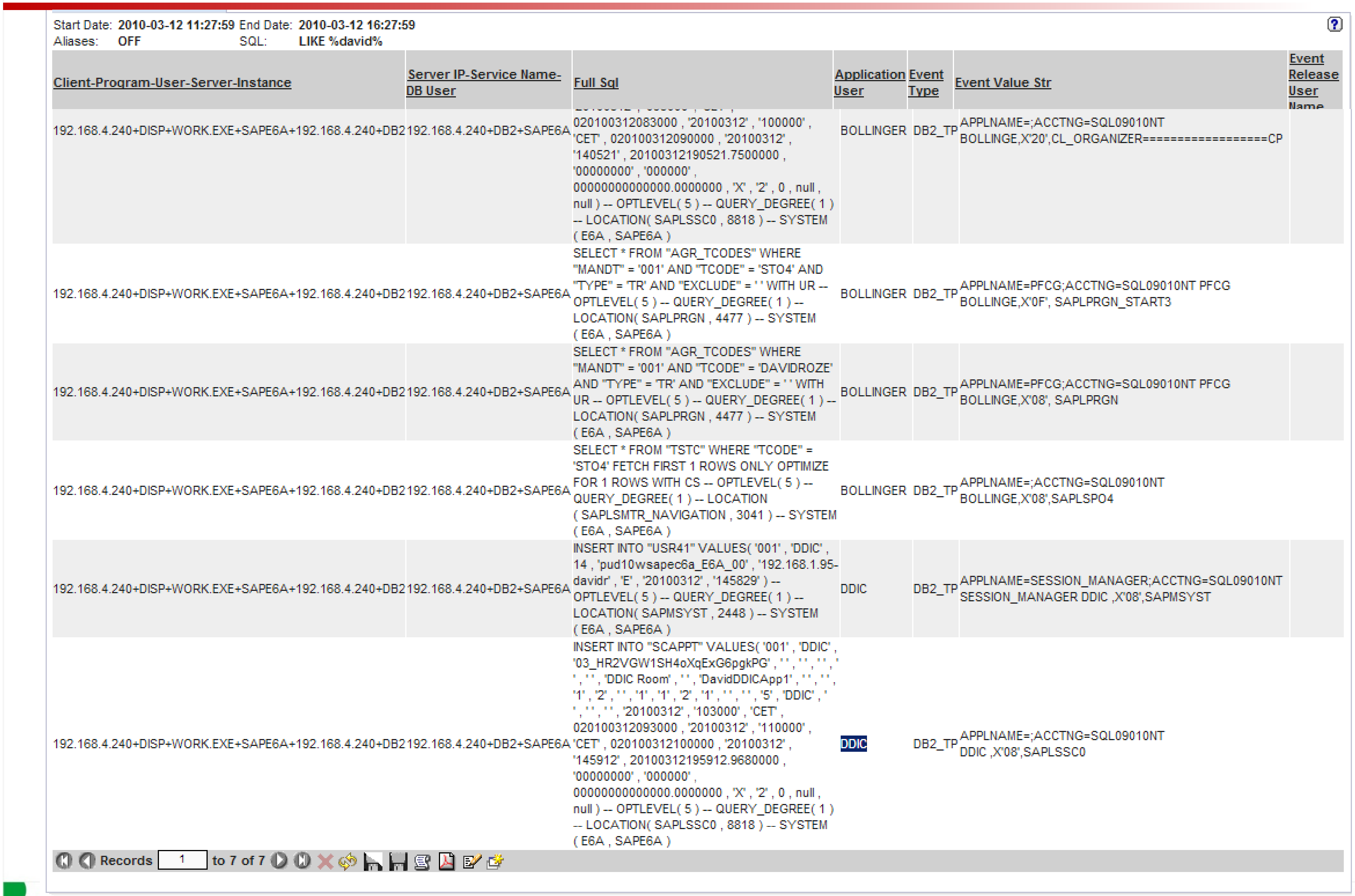
Minimum Count: 0 | Reset Interval: 0 minutes | Message Template: Default

Quarantine for: 0 minutes | Records Affected Threshold: 0 | Rec. Vals. ☑ | Cont. to next rule ☑

Actions

☒ ⊞ ALERT PER MATCH

Application-layer monitoring



Start Date: **2010-03-12 11:27:59** End Date: **2010-03-12 16:27:59**
Aliases: **OFF** SQL: **LIKE %david%**

Client-Program-User-Server-Instance	Server IP-Service Name-DB User	Full Sql	Application User	Event Type	Event Value Str	Event Release User Name
192.168.4.240+DISP+WORK.EXE+SAPE6A+192.168.4.240+DB2	192.168.4.240+DB2+SAPE6A	020100312083000 , '20100312' , '100000' , 'CET' , 020100312090000 , '20100312' , '140521' , 20100312190521.7500000 , '00000000' , '000000' , 0000000000000.0000000 , 'X' , '2' , 0 , null , null) -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLSSC0 , 8818) -- SYSTEM (E6A , SAPE6A)	BOLLINGER	DB2_TP	APPLNAME=;ACCTNG=SQL09010NT BOLLINGE,X'20',CL_ORGANIZER===================CP	
192.168.4.240+DISP+WORK.EXE+SAPE6A+192.168.4.240+DB2	192.168.4.240+DB2+SAPE6A	SELECT * FROM "AGR_TCODES" WHERE "MANDT" = '001' AND "TCODE" = 'STO4' AND "TYPE" = 'TR' AND "EXCLUDE" = ' ' WITH UR -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLPRGN , 4477) -- SYSTEM (E6A , SAPE6A)	BOLLINGER	DB2_TP	APPLNAME=PFCG;ACCTNG=SQL09010NT PFCG BOLLINGE,X'0F', SAPLPRGN_START3	
192.168.4.240+DISP+WORK.EXE+SAPE6A+192.168.4.240+DB2	192.168.4.240+DB2+SAPE6A	SELECT * FROM "AGR_TCODES" WHERE "MANDT" = '001' AND "TCODE" = 'DAVIDROZE' AND "TYPE" = 'TR' AND "EXCLUDE" = ' ' WITH UR -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLPRGN , 4477) -- SYSTEM (E6A , SAPE6A)	BOLLINGER	DB2_TP	APPLNAME=PFCG;ACCTNG=SQL09010NT PFCG BOLLINGE,X'08', SAPLPRGN	
192.168.4.240+DISP+WORK.EXE+SAPE6A+192.168.4.240+DB2	192.168.4.240+DB2+SAPE6A	SELECT * FROM "TSTC" WHERE "TCODE" = 'STO4' FETCH FIRST 1 ROWS ONLY OPTIMIZE FOR 1 ROWS WITH CS -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION (SAPLSMTR_NAVIGATION , 3041) -- SYSTEM (E6A , SAPE6A)	BOLLINGER	DB2_TP	APPLNAME=;ACCTNG=SQL09010NT BOLLINGE,X'08',SAPLSPO4	
192.168.4.240+DISP+WORK.EXE+SAPE6A+192.168.4.240+DB2	192.168.4.240+DB2+SAPE6A	INSERT INTO "USR41" VALUES('001' , 'DDIC' , 14 , 'pud10wsapec6a_E6A_00' , '192.168.1.95-davidr' , 'E' , '20100312' , '145829') -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPMSYST , 2448) -- SYSTEM (E6A , SAPE6A)	DDIC	DB2_TP	APPLNAME=SESSION_MANAGER;ACCTNG=SQL09010NT SESSION_MANAGER DDIC ,X'08',SAPMSYST	
192.168.4.240+DISP+WORK.EXE+SAPE6A+192.168.4.240+DB2	192.168.4.240+DB2+SAPE6A	INSERT INTO "SCAPPT" VALUES('001' , 'DDIC' , '03_HR2VGW1SH4oXqExG6pgkPG' , ' ' , ' ' , ' ' , ' ' , ' ' , 'DDIC Room' , ' ' , 'DavidDDICApp1' , ' ' , ' ' , '1' , '2' , ' ' , '1' , '1' , '2' , '1' , ' ' , ' ' , '5' , 'DDIC' , ' ' , ' ' , ' ' , '20100312' , '103000' , 'CET' , 020100312093000 , '20100312' , '110000' , 'CET' , 020100312100000 , '20100312' , '145912' , 20100312195912.9680000 , '00000000' , '000000' , 0000000000000.0000000 , 'X' , '2' , 0 , null , null) -- OPTLEVEL(5) -- QUERY_DEGREE(1) -- LOCATION(SAPLSSC0 , 8818) -- SYSTEM (E6A , SAPE6A)	DDIC	DB2_TP	APPLNAME=;ACCTNG=SQL09010NT DDIC ,X'08',SAPLSSC0	

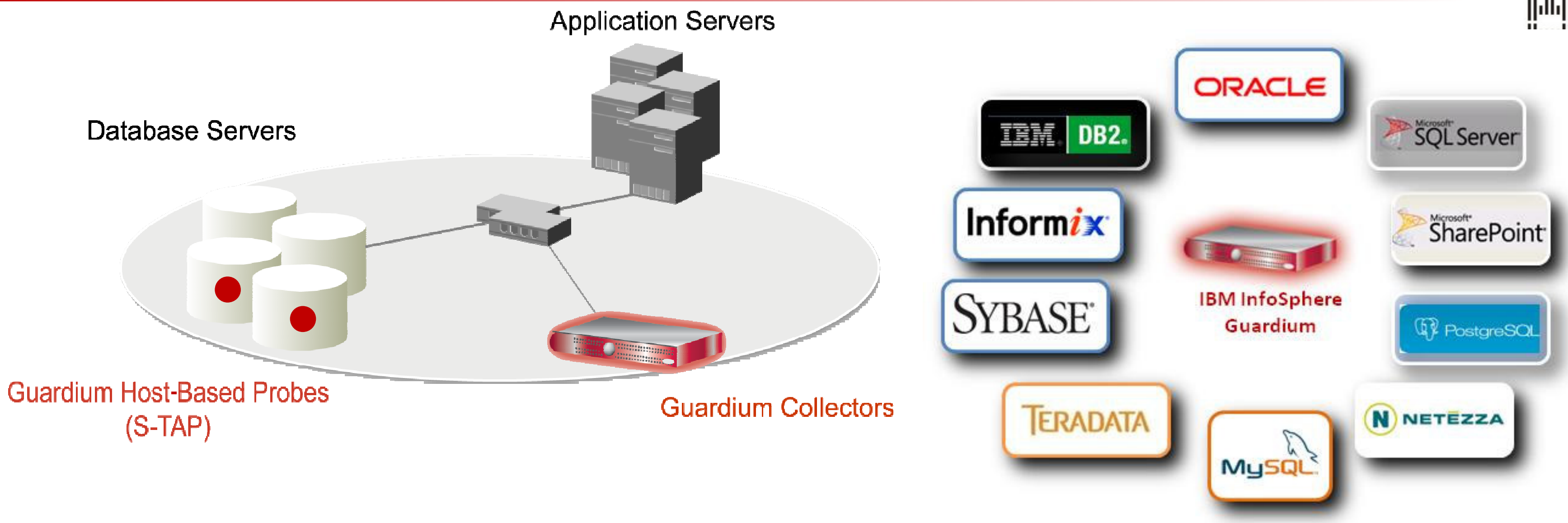
6. Auditing

- Secure, non-repudiable audit trails must be generated and maintained for any database activities that impact security posture, data integrity or viewing sensitive data.

- In addition to being a key compliance requirement, having granular audit trails is also important for forensic investigations.

- A new class of DAM solutions are now available that provide granular, DBMS-independent auditing with minimal impact on performance, while reducing operational costs via automation, centralized cross-DBMS policies and audit repositories, filtering and compression.

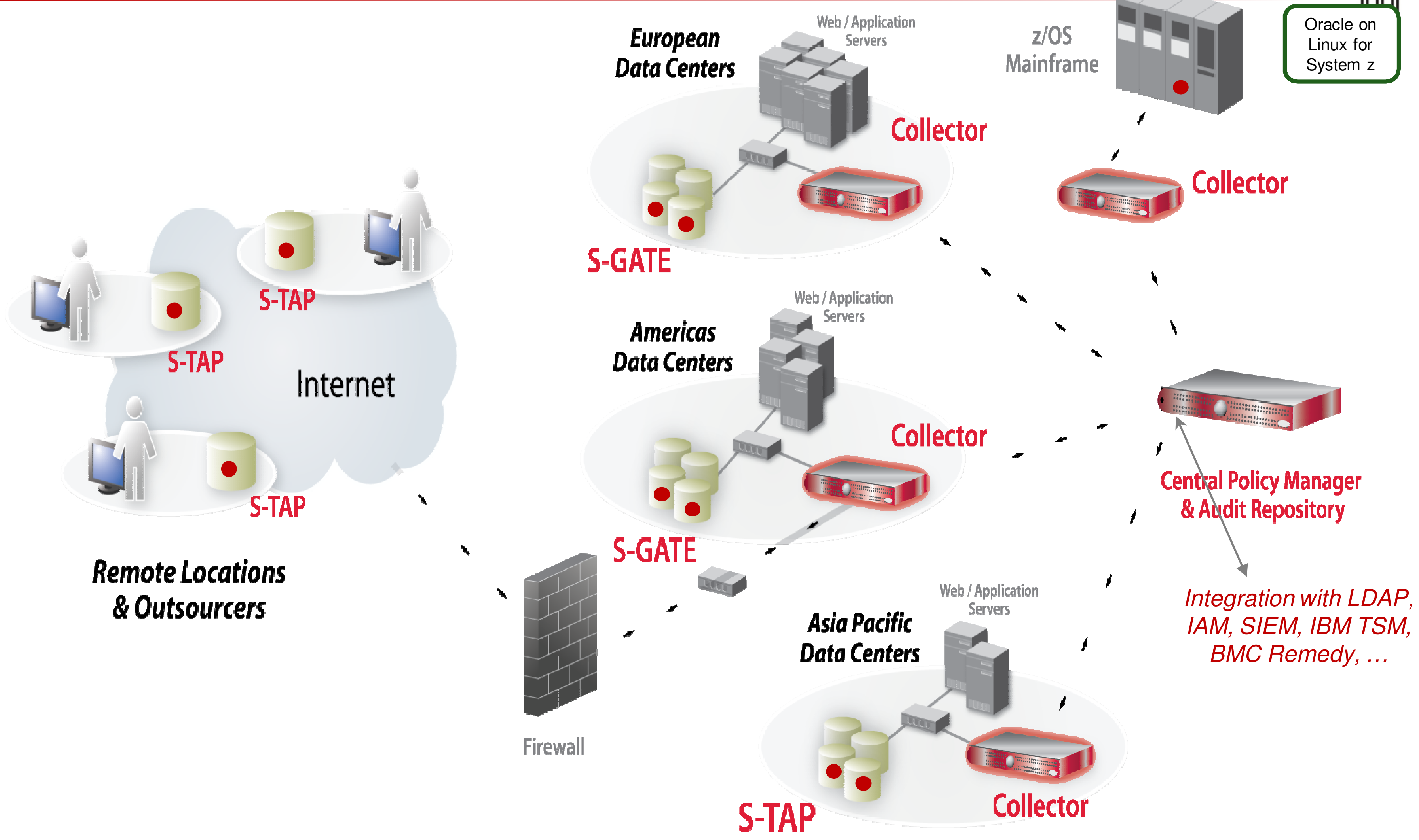
Non-Invasive, Real-Time Database Security & Monitoring



- 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***

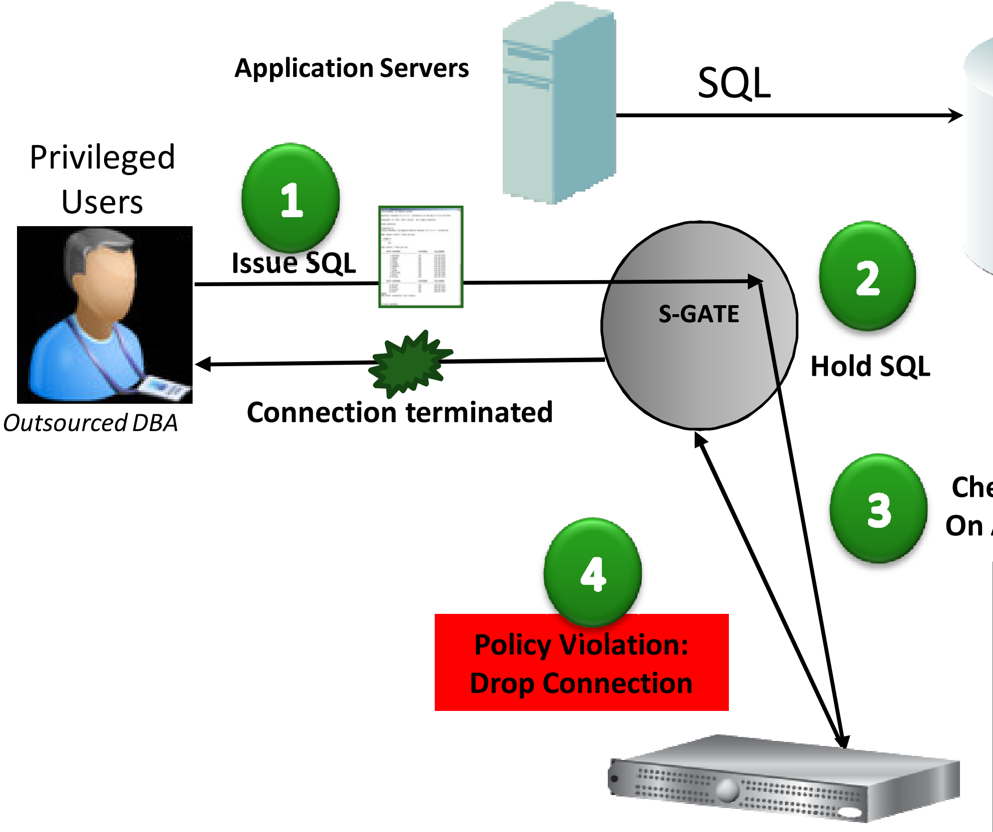
Scalable Multi-Tier Architecture


IBM DB2
Oracle on Linux for System z
European Data Centers
Web / Application Servers
z/OS Mainframe
Collector
Collector
S-GATE
S-TAP
S-TAP
Internet
S-TAP
Remote Locations & Outsourcers
Americas Data Centers
Web / Application Servers
Collector
S-GATE
Central Policy Manager & Audit Repository
Firewall
Asia Pacific Data Centers
Web / Application Servers
Integration with LDAP, IAM, SIEM, IBM TSM, BMC Remedy, …
S-TAP
Collector

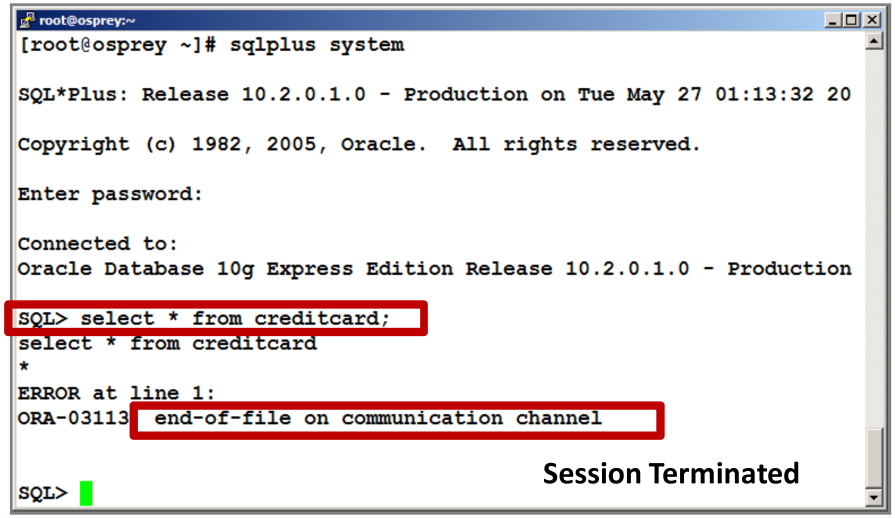
7. Authentication, Access Control & Entitlement Management

- Not all data and not all users are created equally.
- You must authenticate users, ensure full accountability per user, and manage privileges to limit access to data.
- You should enforce these privileges – even for the most privileged database users.
- You also need to periodically review entitlement reports (also called User Right Attestation reports) as part of a formal audit process.

InfoSphere Guardium Data-Level Access Control (S-GATE)

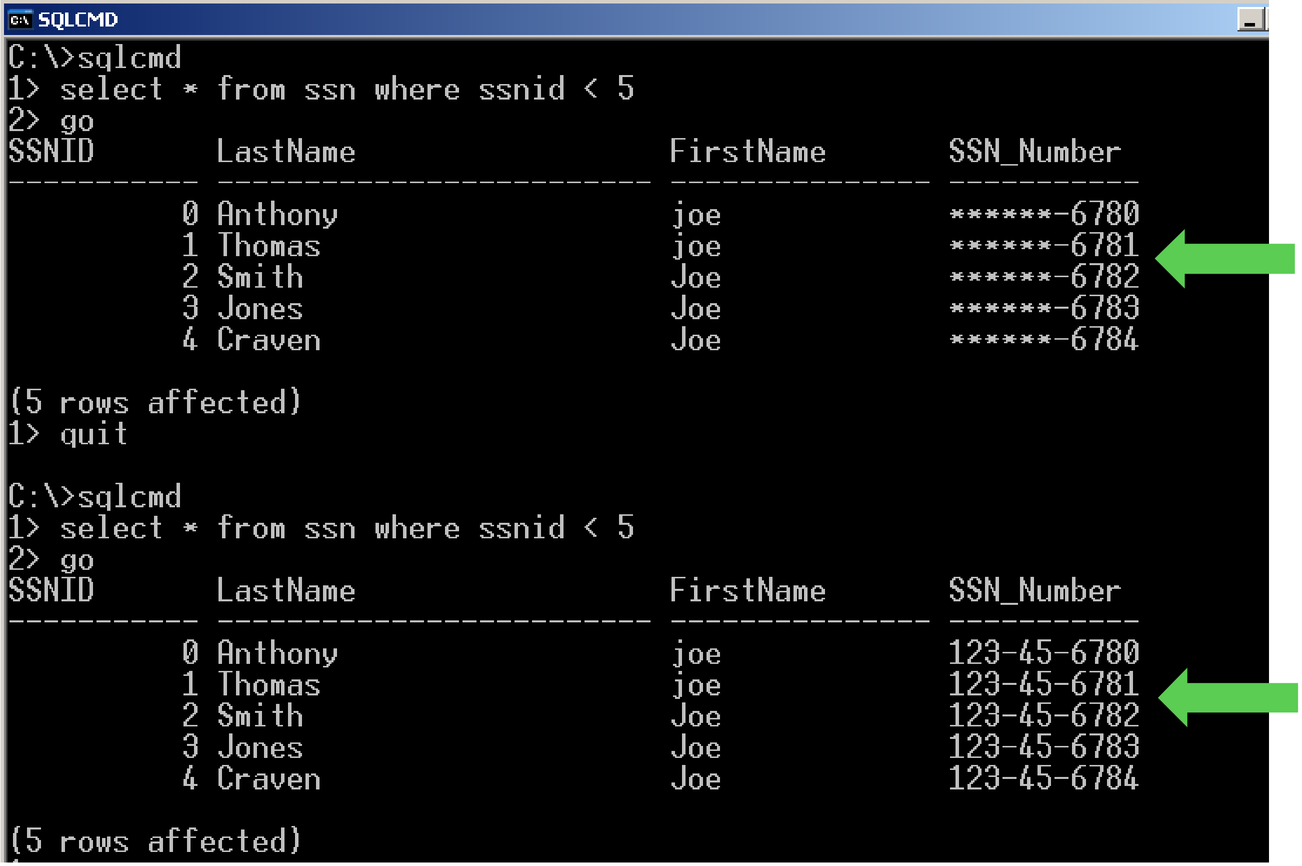


- ✓ Cross-DBMS policies
- ✓ Block privileged user actions
- ✓ No database changes
- ✓ No application changes
- ✓ Without risk of inline appliances that can interfere with application traffic



```
[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>
```

Mask Sensitive Information From Unauthorized Users



```
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)
```

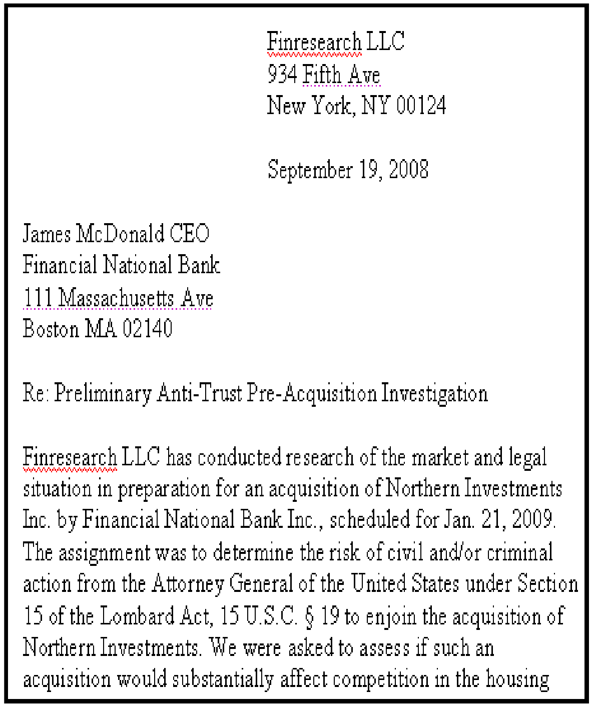
Masked values to database client

Actual Values in the database server

- Mask data on the fly for production database servers

InfoSphere Guardium Data Redaction

Protect sensitive unstructured data in documents and forms



Finresearch LLC
934 Fifth Ave
New York, NY 00124

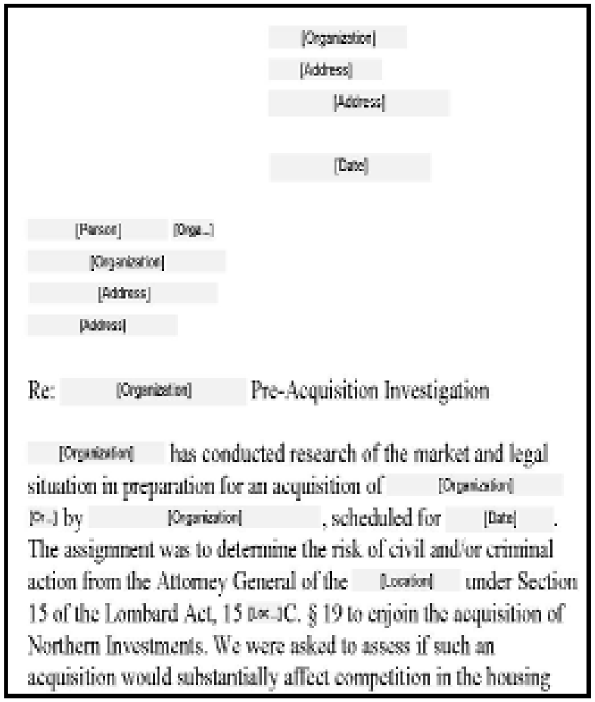
September 19, 2008

James McDonald CEO
Financial National Bank
111 Massachusetts Ave
Boston MA 02140

Re: Preliminary Anti-Trust Pre-Acquisition Investigation

Finresearch LLC has conducted research of the market and legal situation in preparation for an acquisition of Northern Investments Inc. by Financial National Bank Inc., scheduled for Jan. 21, 2009. The assignment was to determine the risk of civil and/or criminal action from the Attorney General of the United States under Section 15 of the Lombard Act, 15 U.S.C. § 19 to enjoin the acquisition of Northern Investments. We were asked to assess if such an acquisition would substantially affect competition in the housing

Before



[Organization]
[Address]
[Address]

[Date]

[Person] [Orga...]
[Organization]
[Address]
[Address]

Re: [Organization] Pre-Acquisition Investigation

[Organization] has conducted research of the market and legal situation in preparation for an acquisition of [Organization] [Or...] by [Organization], scheduled for [Date]. The assignment was to determine the risk of civil and/or criminal action from the Attorney General of the [Location] under Section 15 of the Lombard Act, 15 [Lo...]C. § 19 to enjoin the acquisition of Northern Investments. We were asked to assess if such an acquisition would substantially affect competition in the housing

After

Requirements

- Protect unstructured data in textual, graphical and form based documents
- Control data views with user role policies
- Automate batch workflow process with optional human review

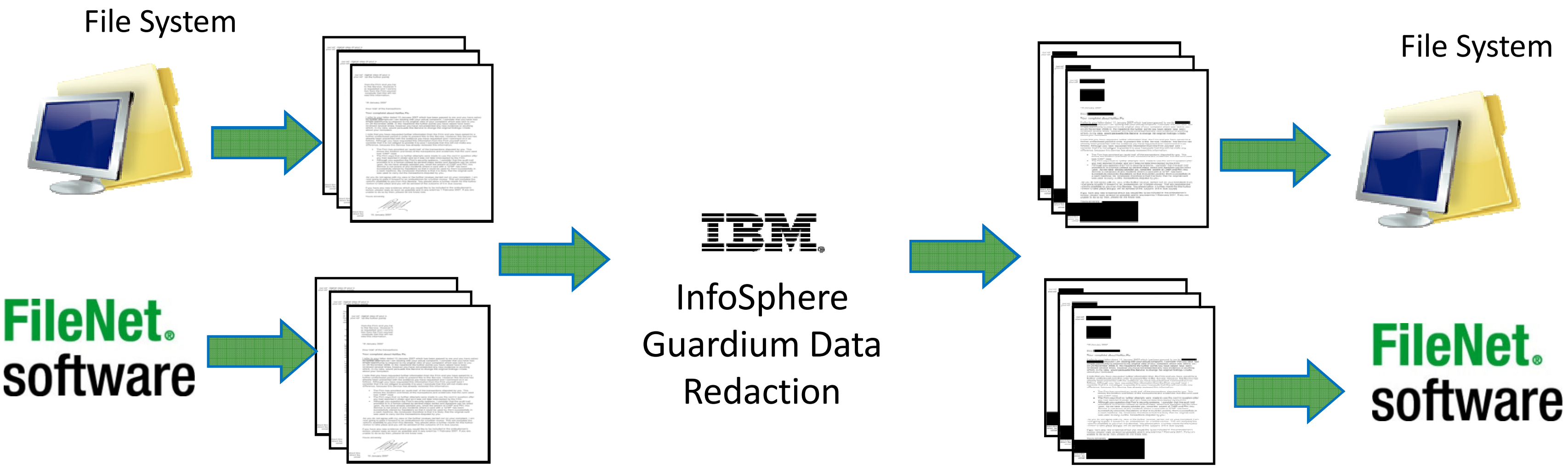
Benefits

- Prevent unintentional data disclosure
- Comply with regulatory and corporate compliance standards
- Increase efficiency and reduce risk via automation

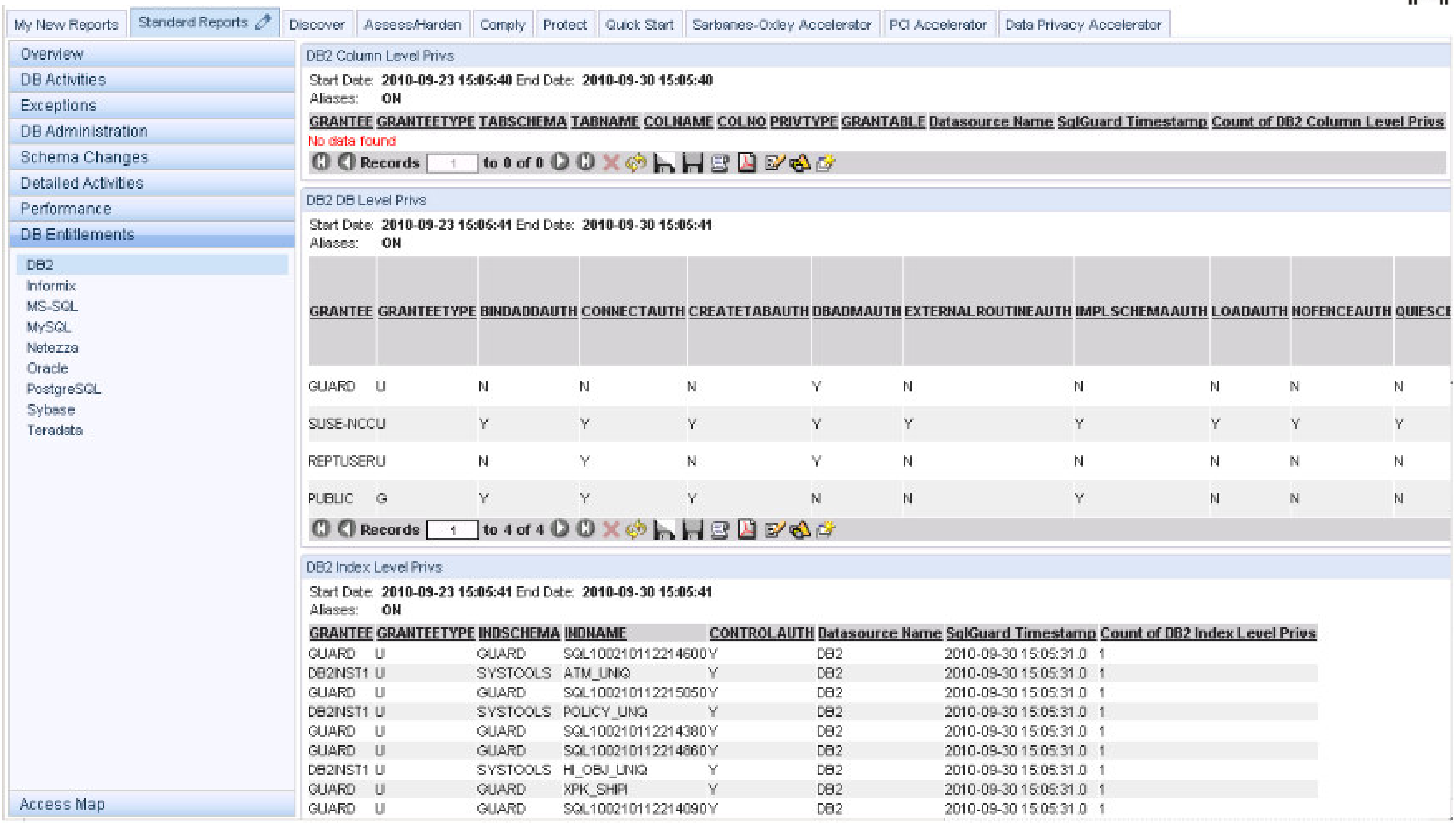
InfoSphere Guardium Data Redaction

✓ Now integrated with ECM FileNet!

- Out of the box support for P8 (v 4.5.1) ensures protection of sensitive unstructured documents part of enterprise repository



InfoSphere Guardium Entitlement Report



DB2 Column Level Privs

Start Date: **2010-09-23 15:05:40** End Date: **2010-09-30 15:05:40**
Aliases: **ON**

GRANTEE	GRANTEETYPE	TABSCHEMA	TABNAME	COLNAME	COLNO	PRIVTYPE	GRANTABLE	Datasource Name	SqlGuard Timestamp	Count of DB2 Column Level Privs

No data found

Records 1 to 0 of 0

DB2 DB Level Privs

Start Date: **2010-09-23 15:05:41** End Date: **2010-09-30 15:05:41**
Aliases: **ON**

GRANTEE	GRANTEETYPE	BINDADDAUTH	CONNECTAUTH	CREATETABAUTH	DBADMAUTH	EXTERNALROUTINEAUTH	IMPLSCHEMAAUTH	LOADAUTH	NOFENCEAUTH	QUIESCE
GUARD	U	N	N	N	Y	N	N	N	N	N
SUSE-NCCU	U	Y	Y	Y	Y	Y	Y	Y	Y	Y
REPTUSER	U	N	Y	N	Y	N	N	N	N	N
PUBLIC	G	Y	Y	Y	N	N	Y	N	N	N

Records 1 to 4 of 4

DB2 Index Level Privs

Start Date: **2010-09-23 15:05:41** End Date: **2010-09-30 15:05:41**
Aliases: **ON**

GRANTEE	GRANTEETYPE	INDSCHEMA	INDNAME	CONTROLAUTH	Datasource Name	SqlGuard Timestamp	Count of DB2 Index Level Privs
GUARD	U	GUARD	SQL100210112214600	Y	DB2	2010-09-30 15:05:31.0	1
DB2INST1	U	SYSTOOLS	ATM_UNIQ	Y	DB2	2010-09-30 15:05:31.0	1
GUARD	U	GUARD	SQL100210112215050	Y	DB2	2010-09-30 15:05:31.0	1
DB2INST1	U	SYSTOOLS	POLICY_UNQ	Y	DB2	2010-09-30 15:05:31.0	1
GUARD	U	GUARD	SQL100210112214380	Y	DB2	2010-09-30 15:05:31.0	1
GUARD	U	GUARD	SQL100210112214860	Y	DB2	2010-09-30 15:05:31.0	1
DB2INST1	U	SYSTOOLS	H_OBJ_UNIQ	Y	DB2	2010-09-30 15:05:31.0	1
GUARD	U	GUARD	XPK_SHIPI	Y	DB2	2010-09-30 15:05:31.0	1
GUARD	U	GUARD	SQL100210112214090	Y	DB2	2010-09-30 15:05:31.0	1

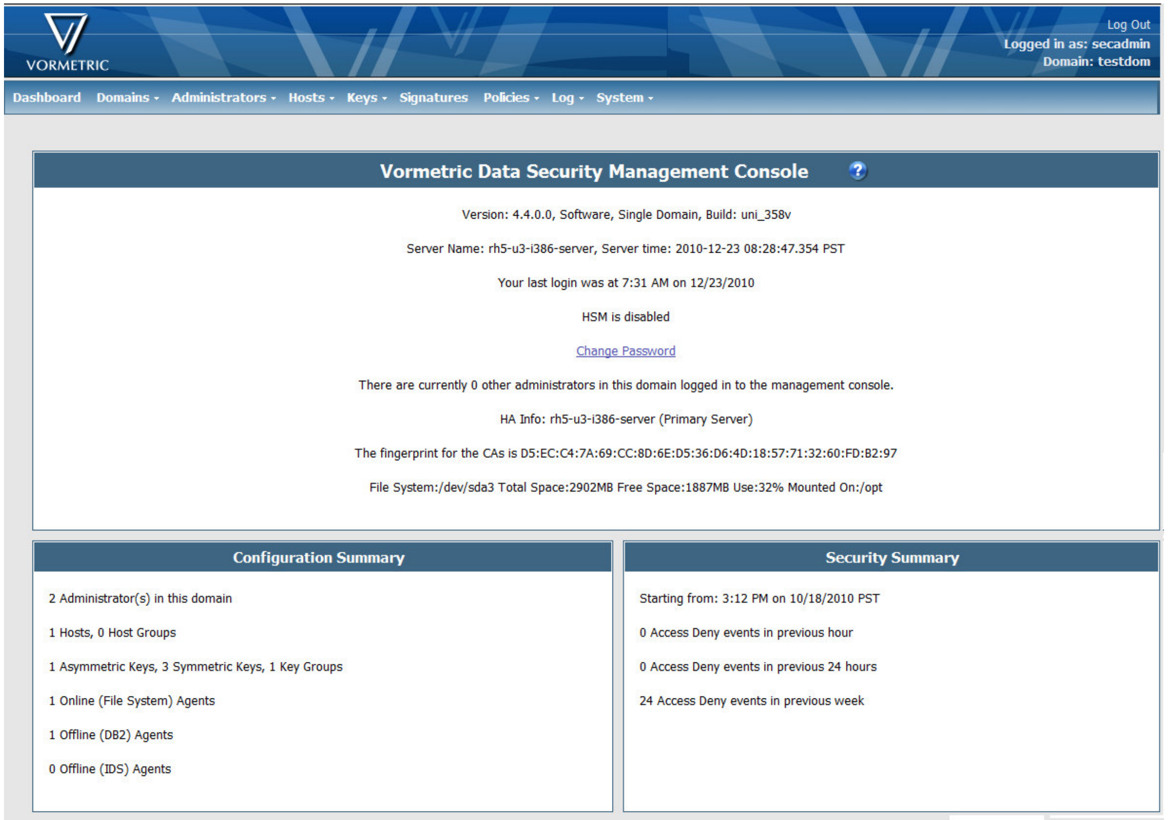
8. Encryption

- Use encryption to render sensitive data unreadable, so that an attacker cannot gain unauthorized access to data from outside the database.

- This includes both encryption of data-in-transit, so that an attacker cannot eavesdrop at the networking layer and gain access to the data when it is sent to the database client, as well as encryption of data-at-rest, so that an attacker cannot extract the data even with access to the media files.

IBM InfoSphere Guardium Encryption Expert

Ensure compliance and protect enterprise data with encryption



Logged in as: secadmin
Domain: testdom

Vormetric Data Security Management Console

Version: 4.4.0.0, Software, Single Domain, Build: uni_358v

Server Name: rh5-u3-i386-server, Server time: 2010-12-23 08:28:47.354 PST

Your last login was at 7:31 AM on 12/23/2010

HSM is disabled

Change Password

There are currently 0 other administrators in this domain logged in to the management console.

HA Info: rh5-u3-i386-server (Primary Server)

The fingerprint for the CAs is D5:EC:C4:7A:69:CC:8D:6E:D5:36:D6:4D:18:57:71:32:60:FD:B2:97

File System:/dev/sda3 Total Space:2902MB Free Space:1887MB Use:32% Mounted On:/opt

Configuration Summary

2 Administrator(s) in this domain

1 Hosts, 0 Host Groups

1 Asymmetric Keys, 3 Symmetric Keys, 1 Key Groups

1 Online (File System) Agents

1 Offline (DB2) Agents

0 Offline (IDS) Agents

Security Summary

Starting from: 3:12 PM on 10/18/2010 PST

0 Access Deny events in previous hour

0 Access Deny events in previous 24 hours

24 Access Deny events in previous week

Requirements

- Encrypt data without making any application changes
- Protect data in both online and offline environments (ie backup, database extracts, portable devices)
- Establish separation of duties

Benefits

- Protect enterprise data with no-down time to implement and no missed SLAs
- Ensure environment is audit ready
- Satisfy industry and government regulations and

Thank You

InformationOnDemand**India2011**

The Premier Conference for Information Management

Manage. Analyze. Govern.

February 2, 2011

Hyatt Regency I Mumbai, India