Information Management

企業資料庫安全與監控

Enterprise Database Security & Monitoring

Paul Chang
paulyc@tw.ibm.com

Data Management

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

各行業都的營運秘密資料，如：製程流程與參數、財務資料、員工個人資料、客戶個人資料…。而且從外部入侵或在內部盜取都可能發生

行業別	營運秘密	個人資料
科技及製造業	製程流程與參數、設計資訊、未公開產品規格、軟體原始碼、營運及業務、財務、人事資訊	雇員個人資訊
金融行業	交易資訊、未公開營運資訊、業務、財務、人事資訊	雇員個人資訊、客戶個人資訊、信用卡或帳戶資訊
醫療行業	實驗數據、業務、財務、人事資訊	雇員個人資訊、病患個人資訊、病歷資訊、健康檢查資訊
教育行業	研究報告、業務、財務、人事資訊	教職員資訊、學生及家長個人資訊、學生學習紀錄
政府及軍事	軍事機密資訊、內部調查資料、未公開規劃、稅務資訊、情報資訊	國民、市民資訊、個人稅務及財務資訊、
零售行業	交易資訊、未公開營運資訊、業務、財務、人事資訊	會員資訊、信用卡或帳戶資訊

*客戶負有識別及解釋並遵守和其業務相關的法律或規範之責任.
IBM 並不保證透過其提供之服務或產品即代表其可以符合法律之要求.

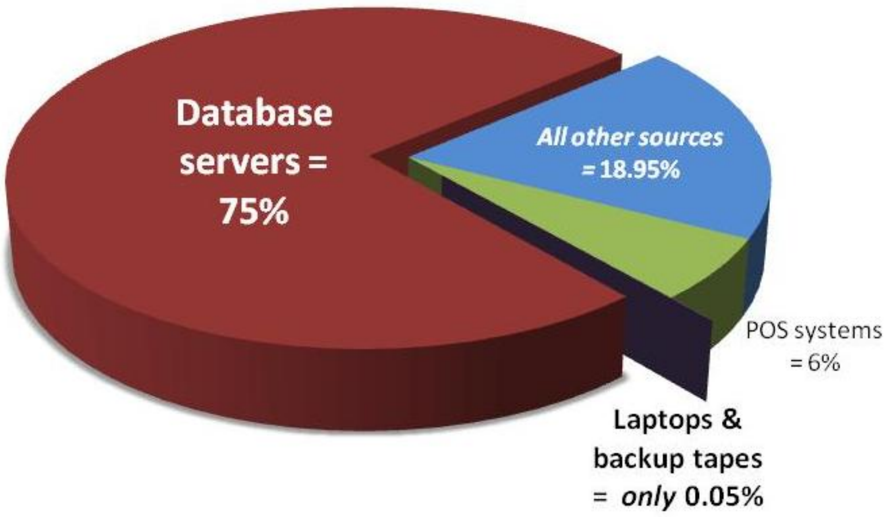
市場調查揭示資料安全最大隱患來自於企業內部!!!

- 59%的受訪者承認離職後會帶走公司的資料；
- 79%的受訪者表示是在未經前雇主允許的情況下帶走公司資訊；
- 64%被員工帶走的資訊來自電子郵件；
- 被帶走的信息中有39%為客戶資訊，例如客戶聯絡方式；而有35%是員工資訊。
- 24%的員工在離職後仍然可以登錄公司的網路存取訊號；其中有35%的人在離職一周後仍然擁有這個許可權。

摘自:賽門鐵克與隱私及資訊管理調查機構(Ponemon Institute)共同發佈了一份以2008年離職員工為研究物件的調查報告

資料外洩的來源...
Database Servers = Vast Majority of Compromised Records

% of Records Breached (2009)

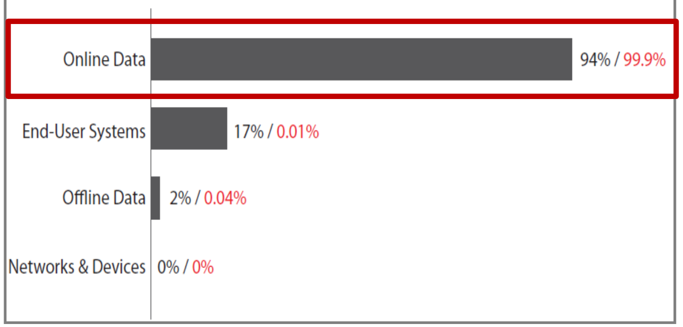


2009 Data Breach Report from Verizon Business RISK Team

http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

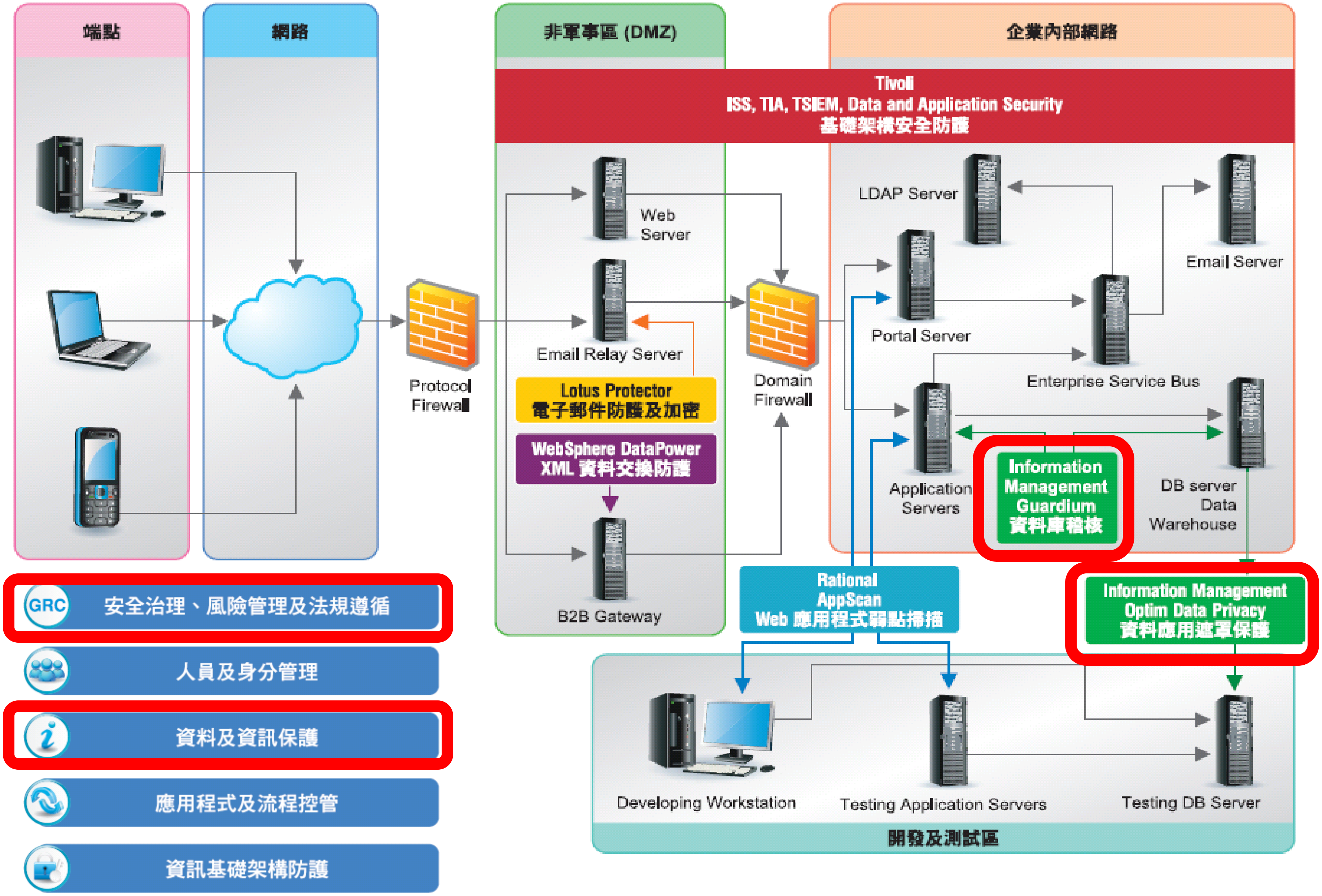
Online data = 99.9% of all compromised records

Figure 25. Asset classes by percent of breaches (black) and records (red)



"Although much angst and security funding is given to **offline data, mobile devices,** and **end-user systems,** these assets are simply **not a major point of compromise.**"

IBM 資訊安全解決方案



端點

網路

非軍事區 (DMZ)

企業內部網路

Tivoli
ISS, TIA, TSIEM, Data and Application Security
基礎架構安全防護

Protocol Firewall

Web Server

Email Relay Server

Lotus Protector
電子郵件防護及加密

WebSphere DataPower
XML 資料交換防護

B2B Gateway

Domain Firewall

LDAP Server

Email Server

Portal Server

Enterprise Service Bus

Application Servers

Information Management Guardium
資料庫稽核

DB server Data Warehouse

Rational AppScan
Web 應用程式弱點掃描

Information Management Optim Data Privacy
資料應用遮罩保護

Developing Workstation

Testing Application Servers

Testing DB Server

開發及測試區

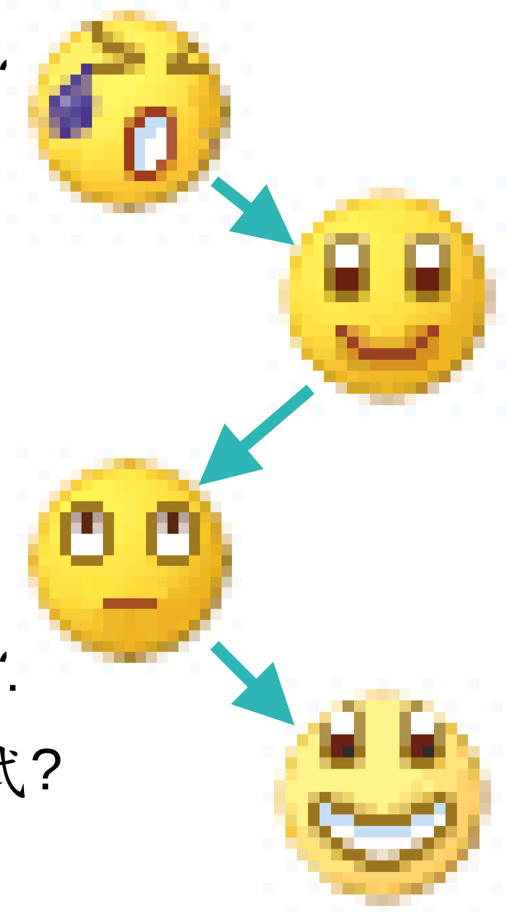
- GRC 安全治理、風險管理及法規遵循
- 人員及身分管理
- 資料及資訊保護
- 應用程式及流程控管
- 資訊基礎架構防護

哪些是我們必須要收集的DAM資料

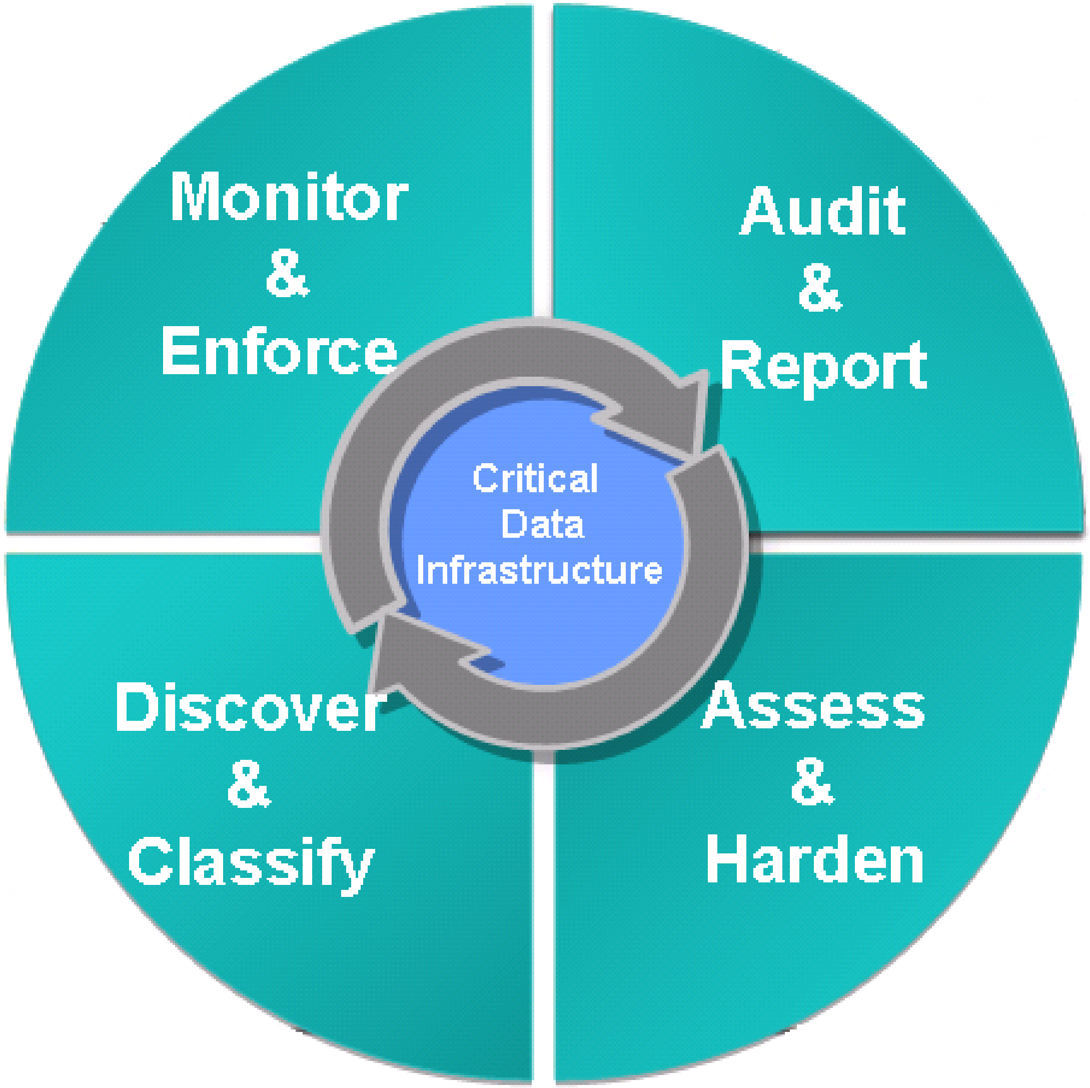
- 80 / 20 法則
- 20% 稽核人員關心的
  - 與身分證ID相關資訊
  - 以身分證ID查詢筆數、內容...等
  - Base line建立後發現得異常Pattern
  - 系統登入、登出資訊
  - 高權限使用者之行為
  - 敏感性資料之存取
  - 對稽核資料Drill down分析
  - 系統資安強化之具體計畫與報告
- 80% 不需監控的資料有哪些?
  - 每日執行的批次作業
  - 每日正常運行且無人為介入之程式作業
  - 由某些特定IP進入資料庫存取且不會有資料外洩疑慮之作業

從DAM系統中可以得到的訊息(與案例說明)

- 誰正在對資料庫進行疑似異常的更動?
- 某些未經過授權的資料變更是在何時進行的?
- DBA或外包廠商對資料庫做了什麼更動?
- 已經發生了多少錯誤的登入紀錄?
- 誰正在擷取敏感性資料?
- 哪些資料正在被哪個網路節點存取?
- 哪些資料正在被哪個應用程式存取?
- 正在進行的資料存取使以什麼方式在進行的?
- 比對資料存取的時間, 是否有哪些可疑的模式?
- 資料庫正在產生什麼錯誤訊息?
- 誰在何時對資料庫進行疑似資料隱碼攻擊?

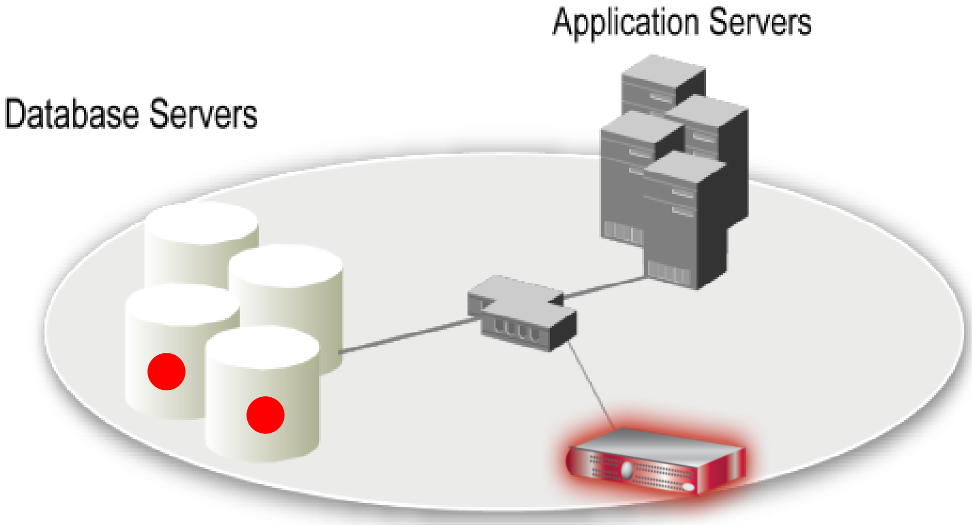


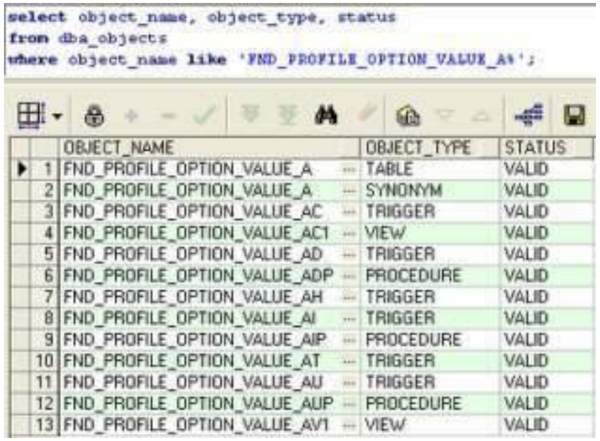
完整的資料庫安全生命週期



資料庫活動監控解決方案類型(與優劣概述)

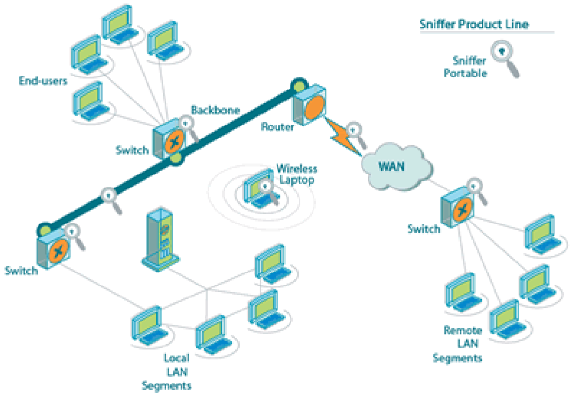
- DB Audit Trial (資料庫原生記錄)
- Port Mirroring (網路封包鏡像)
- Agent/Driver (資料庫本機端程序)





```
select object_name, object_type, status
from dba_objects
where object_name like 'FND_PROFILE_OPTION_VALUE_A%';
```

	OBJECT_NAME	OBJECT_TYPE	STATUS
1	FND_PROFILE_OPTION_VALUE_A	TABLE	VALID
2	FND_PROFILE_OPTION_VALUE_A	SYNONYM	VALID
3	FND_PROFILE_OPTION_VALUE_AC	TRIGGER	VALID
4	FND_PROFILE_OPTION_VALUE_AC1	VIEW	VALID
5	FND_PROFILE_OPTION_VALUE_AD	TRIGGER	VALID
6	FND_PROFILE_OPTION_VALUE_ADP	PROCEDURE	VALID
7	FND_PROFILE_OPTION_VALUE_AH	TRIGGER	VALID
8	FND_PROFILE_OPTION_VALUE_AI	TRIGGER	VALID
9	FND_PROFILE_OPTION_VALUE_AIP	PROCEDURE	VALID
10	FND_PROFILE_OPTION_VALUE_AT	TRIGGER	VALID
11	FND_PROFILE_OPTION_VALUE_AU	TRIGGER	VALID
12	FND_PROFILE_OPTION_VALUE_AUP	PROCEDURE	VALID
13	FND_PROFILE_OPTION_VALUE_AV1	VIEW	VALID



為何資料庫原生記錄(Native Logging)不適用

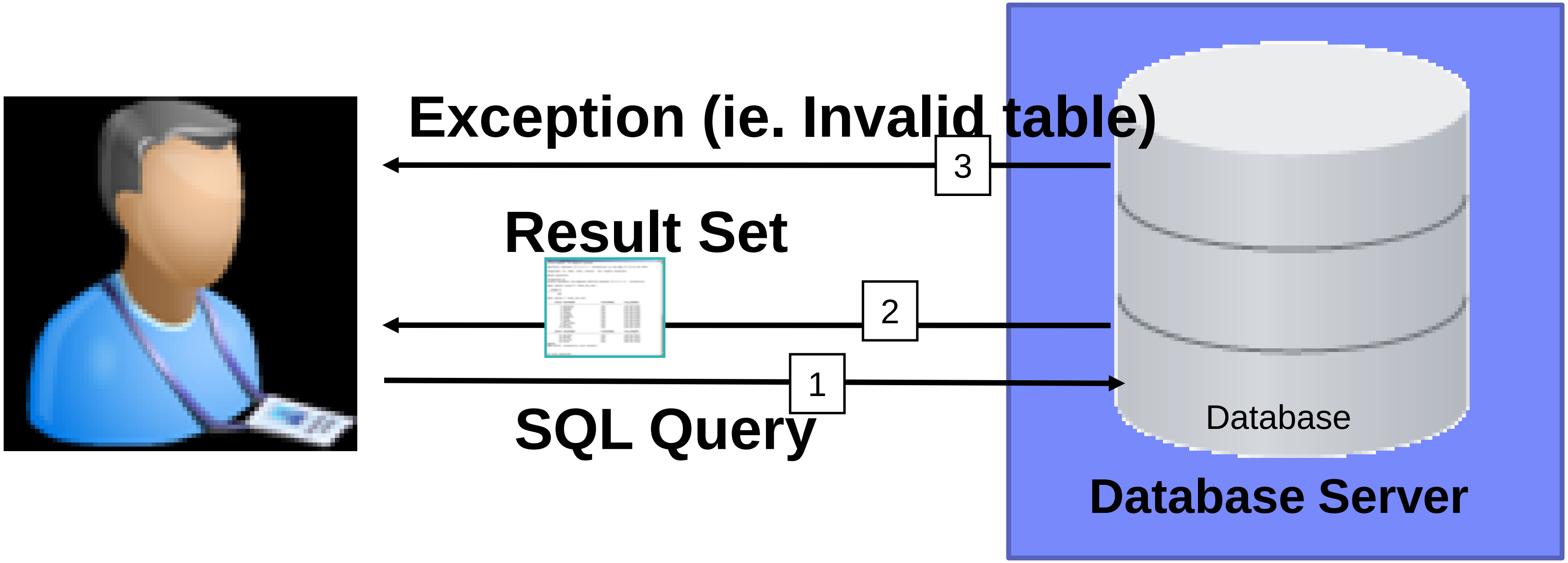
- 影響資料庫效能
  - Which table, from which IP, using which command, which program, …
- 非獨立作業 – 可以很容易被DBA關閉
- 跨資料庫平台會有不一致的稽核策略 (增加複雜度)
- 無法提供主動式的即時安全警示 (review logs every 3 months?)
- 在連接池(connection pooling)的環境無法確認應用程式端的使用者 (PeopleSoft, SAP, Oracle Financials, etc.) – potential fraud
- 須具有大量稽核資料儲存需求
- 在篩選稽核資料時，須撰寫程式
- 在產生符規的稽核報表時，須撰寫程式

成套裝置(Appliance) 與其它的解決方案有何不同之處?

- 即時安全警示與阻絕
  - 主動防護企業資訊
- 安全的稽核資料庫 (獨立作業)
- 詳盡的網路層級資訊
  - Client IP, OS login ID, source application, etc.
- 最小效能影響
- 不須變更資料庫或應用程式設定
- 具跨平台和企業層級的解決方案
  - 具稽核資料的彙總與正規化
  - 集中式的策略定義與執行能力

Guardium
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

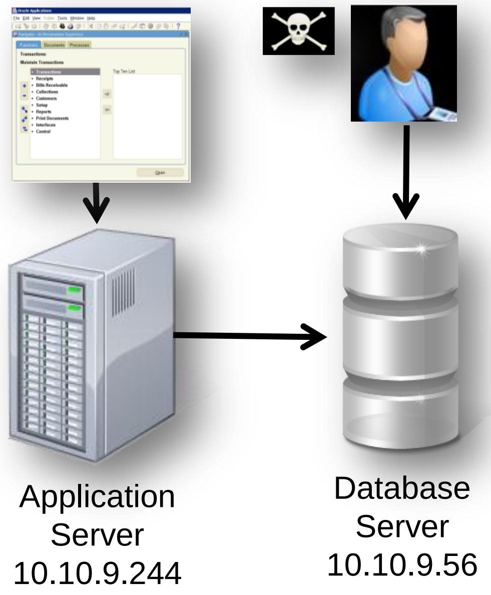
資安政策可以從三種不同的規則去制定

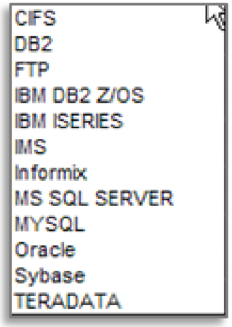


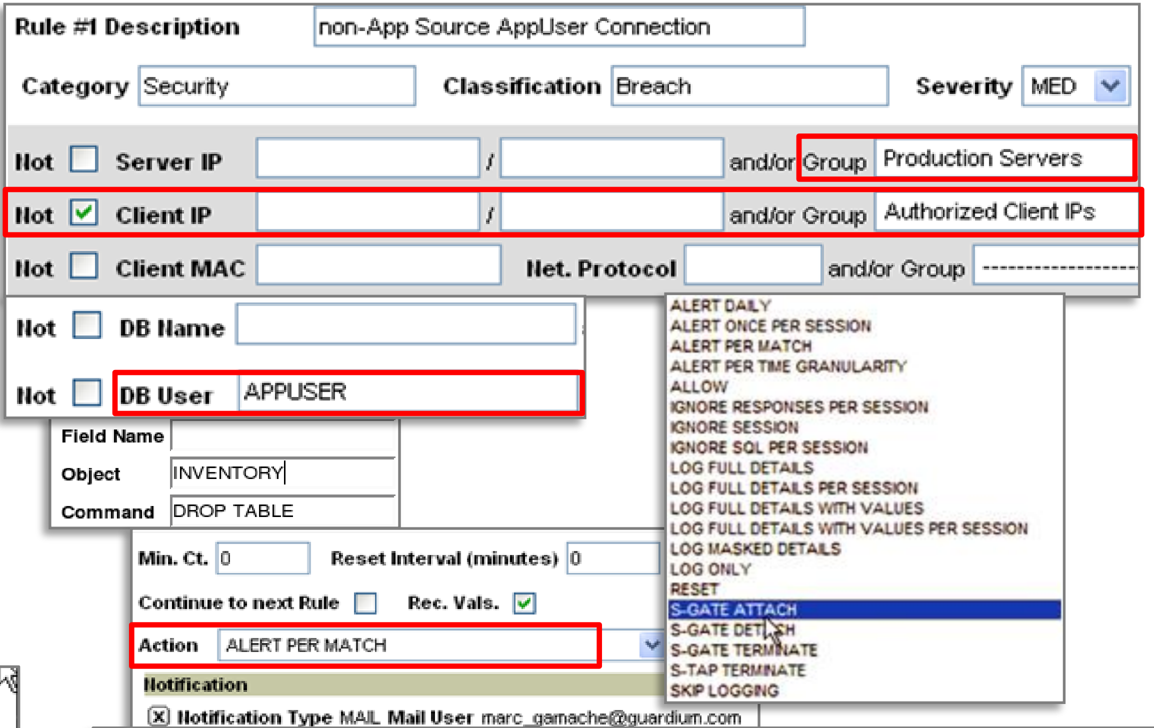
There are three types of rules:

1. An **access rule (存取控制)** applies to client requests
2. An **extrusion rule (產出規則)** evaluates data returned by the server
3. An **exception rule (例外規則)** evaluates exceptions returned by the server

可以細化資安政策之及時性的警示




CIFS
DB2
FTP
IBM DB2 Z/OS
IBM ISERIES
IMS
Informix
MS SQL SERVER
MYSQL
Oracle
Sybase
TERADATA


Rule #1 Description: non-App Source AppUser Connection

Category: Security | Classification: Breach | Severity: MED

Not □ Server IP ___ / ___ and/or Group: Production Servers

Not ☑ Client IP ___ / ___ and/or Group: Authorized Client IPs

Not □ Client MAC ___ Net. Protocol ___ and/or Group: -------------------

Not □ DB Name ___

Not □ DB User: APPUSER

Field Name: ___

Object: INVENTORY

Command: DROP TABLE

Min. Ct.: 0 | Reset Interval (minutes): 0

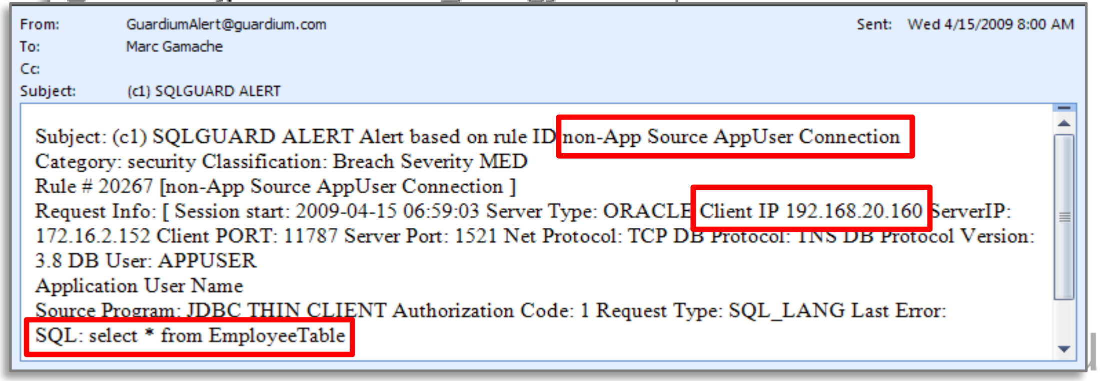
Continue to next Rule □ | Rec. Vals. ☑

Action: ALERT PER MATCH

Notification

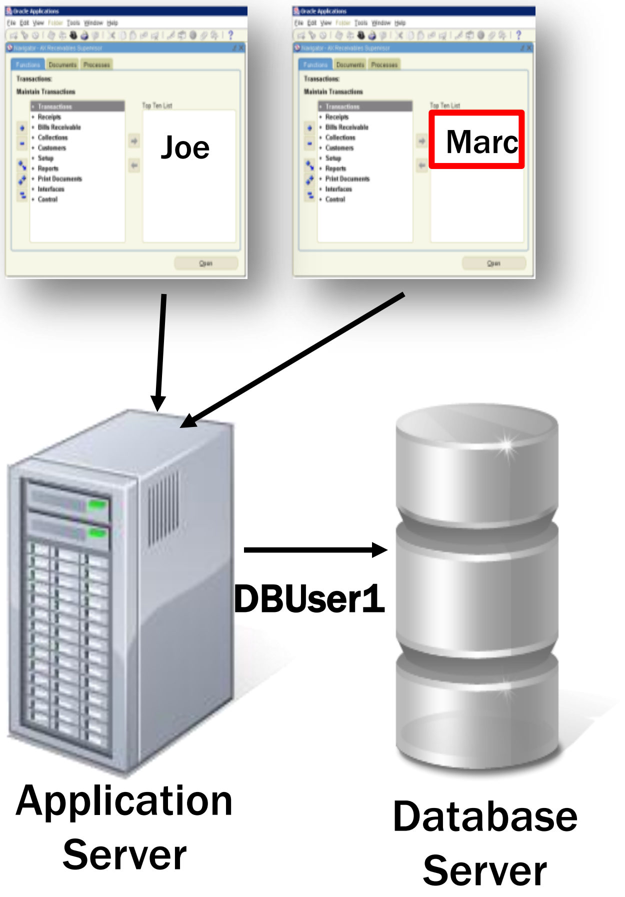
☒ Notification Type MAIL Mail User marc_gamache@guardium.com

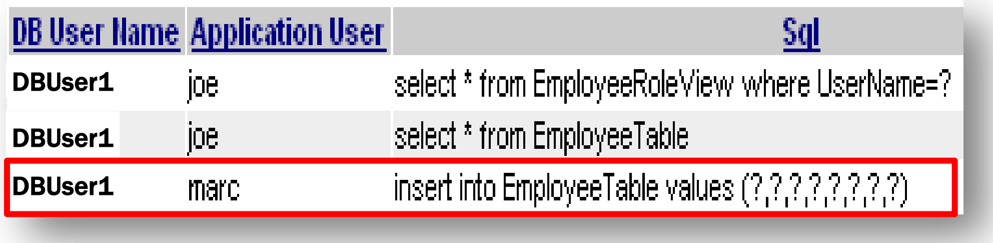
ALERT DAILY
ALERT ONCE PER SESSION
ALERT PER MATCH
ALERT PER TIME GRANULARITY
ALLOW
IGNORE RESPONSES PER SESSION
IGNORE SESSION
IGNORE SQL PER SESSION
LOG FULL DETAILS
LOG FULL DETAILS PER SESSION
LOG FULL DETAILS WITH VALUES
LOG FULL DETAILS WITH VALUES PER SESSION
LOG MASKED DETAILS
LOG ONLY
RESET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


From: GuardiumAlert@guardium.com
To: Marc Gamache
Cc:
Subject: (c1) SQLGUARD ALERT
Sent: Wed 4/15/2009 8:00 AM

Subject: (c1) SQLGUARD ALERT Alert based on rule ID non-App Source AppUser Connection
Category: security Classification: Breach Severity MED
Rule # 20267 [non-App Source AppUser Connection]
Request Info: [Session start: 2009-04-15 06:59:03 Server Type: ORACLE Client IP 192.168.20.160 ServerIP: 172.16.2.152 Client PORT: 11787 Server Port: 1521 Net Protocol: TCP DB Protocol: TNS DB Protocol Version: 3.8 DB User: APPUSER
Application User Name
Source Program: JDBC THIN CLIENT Authorization Code: 1 Request Type: SQL_LANG Last Error:
SQL: select * from EmployeeTable

偵測終端用戶的身份

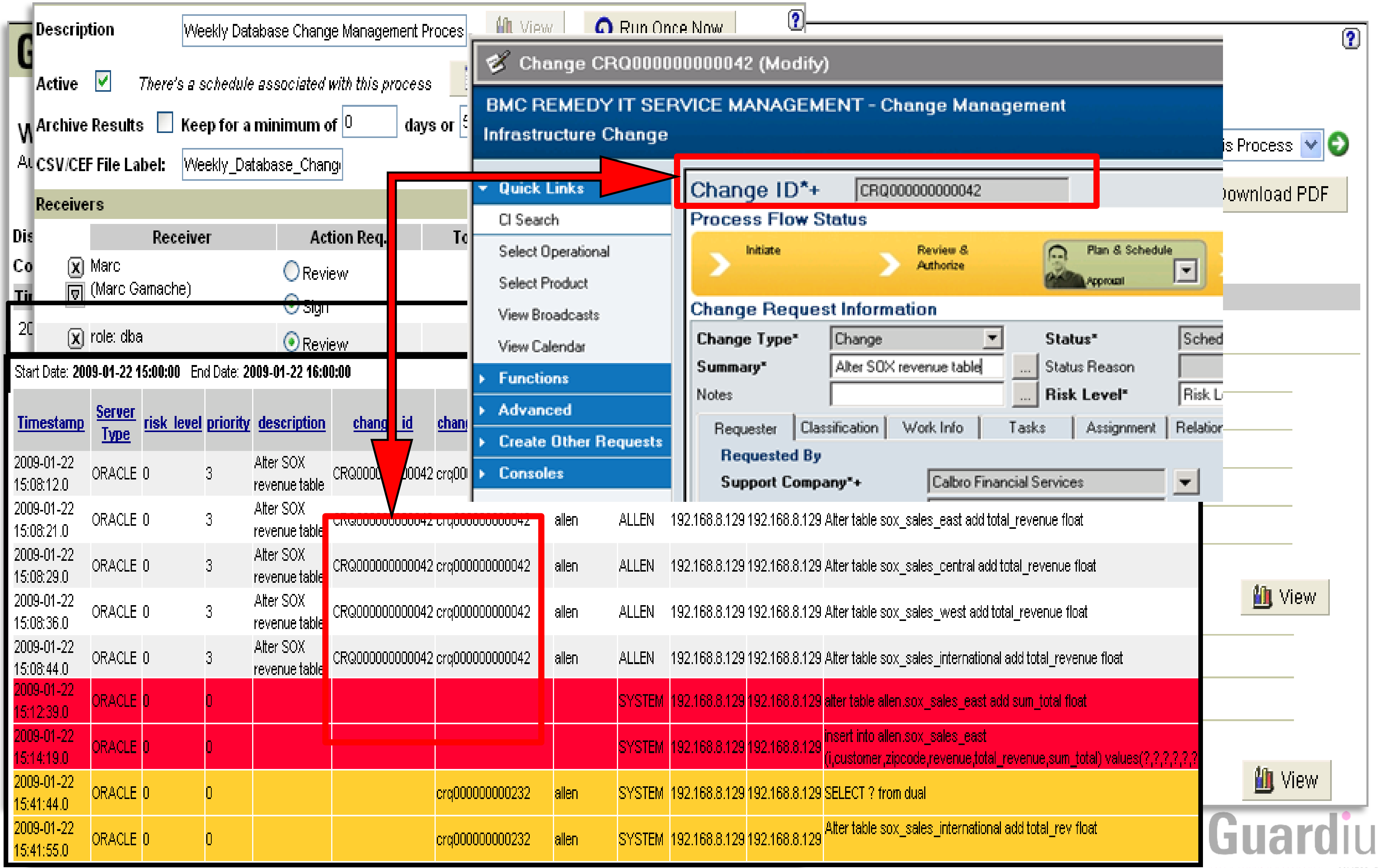




DB User Name	Application User	Sql
DBUser1	joe	select * from EmployeeRoleView where UserName=?
DBUser1	joe	select * from EmployeeTable
DBUser1	marc	insert into EmployeeTable values (?,?,?,?,?,?,?,?)

- **問題**：在三層式的架構下，應用系統伺服器是使用“連接池”中的 DB User 來使用資料庫中的資料。所以從DBA的角度上，無法得知真正的使用者 AP User。
- **需求**：可以得到 AP User 與所執行的SQL指令間的關聯
  - Major enterprise applications (Oracle EBS, PeopleSoft, SAP, Siebel, Business Objects, Cognos…) and
  - Custom applications (WebSphere….)

自動化的簽核與請示流程以滿足合規需求



Description: Weekly Database Change Management Proces

Active ☑ *There's a schedule associated with this process*

Archive Results □ Keep for a minimum of 0 days or

CSV/CEF File Label: Weekly_Database_Chang

Receivers

Receiver	Action Req.
☒ Marc (Marc Gamache)	○ Review ○ Sign
☒ role: dba	● Review

Change CRQ000000000042 (Modify)

BMC REMEDY IT SERVICE MANAGEMENT - Change Management

Infrastructure Change

Change ID*+ CRQ000000000042

Process Flow Status

Change Request Information

Change Type*	Change	Status*	Sched
Summary*	Alter SOX revenue table	Status Reason	
Notes		Risk Level*	Risk L

Requested By

Support Company*+ Calbro Financial Services

Start Date: **2009-01-22 15:00:00** End Date: **2009-01-22 16:00:00**

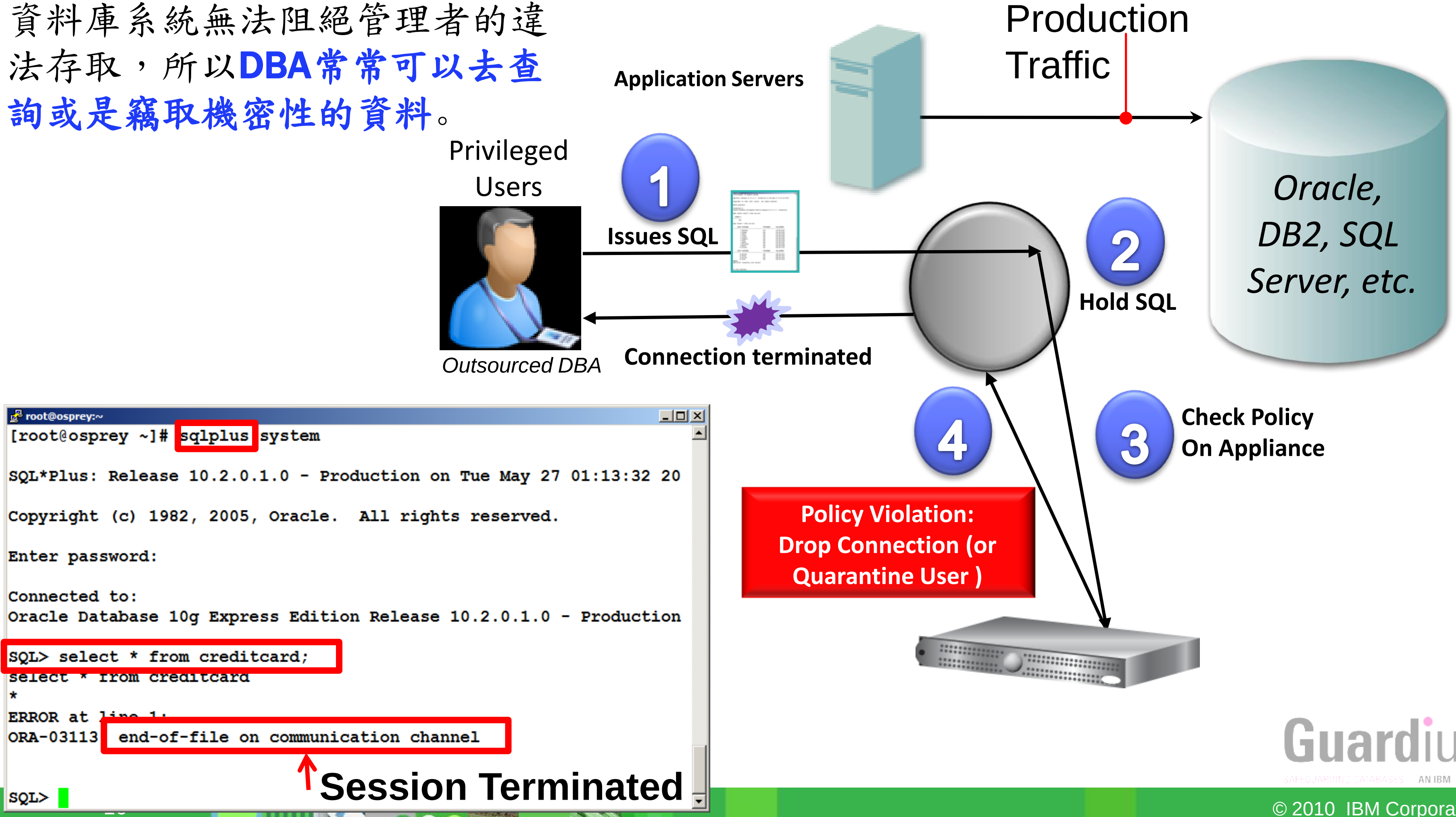
Timestamp	Server Type	risk_level	priority	description	chang_id	chan					
2009-01-22 15:08:12.0	ORACLE	0	3	Alter SOX revenue table	CRQ0000 00042	crq00					
2009-01-22 15:08:21.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_east add total_revenue float
2009-01-22 15:08:29.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_central add total_revenue float
2009-01-22 15:08:36.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_west add total_revenue float
2009-01-22 15:08:44.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_international add total_revenue float
2009-01-22 15:12:39.0	ORACLE	0	0					SYSTEM	192.168.8.129	192.168.8.129	alter table allen.sox_sales_east add sum_total float
2009-01-22 15:14:19.0	ORACLE	0	0					SYSTEM	192.168.8.129	192.168.8.129	insert into allen.sox_sales_east (i,customer,zipcode,revenue,total_revenue,sum_total) values(?,?,?,?,?,?
2009-01-22 15:41:44.0	ORACLE	0	0			crq000000000232	allen	SYSTEM	192.168.8.129	192.168.8.129	SELECT ? from dual
2009-01-22 15:41:55.0	ORACLE	0	0			crq000000000232	allen	SYSTEM	192.168.8.129	192.168.8.129	Alter table sox_sales_international add total_rev float

Guardium
SAFEGUARDING DATABASES · AN IBM COMPANY

阻斷不被授權的存取

"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

資料庫系統無法阻絕管理者的違法存取，所以**DBA常常可以去查詢或是竊取機密性的資料**。



```
[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> 
```

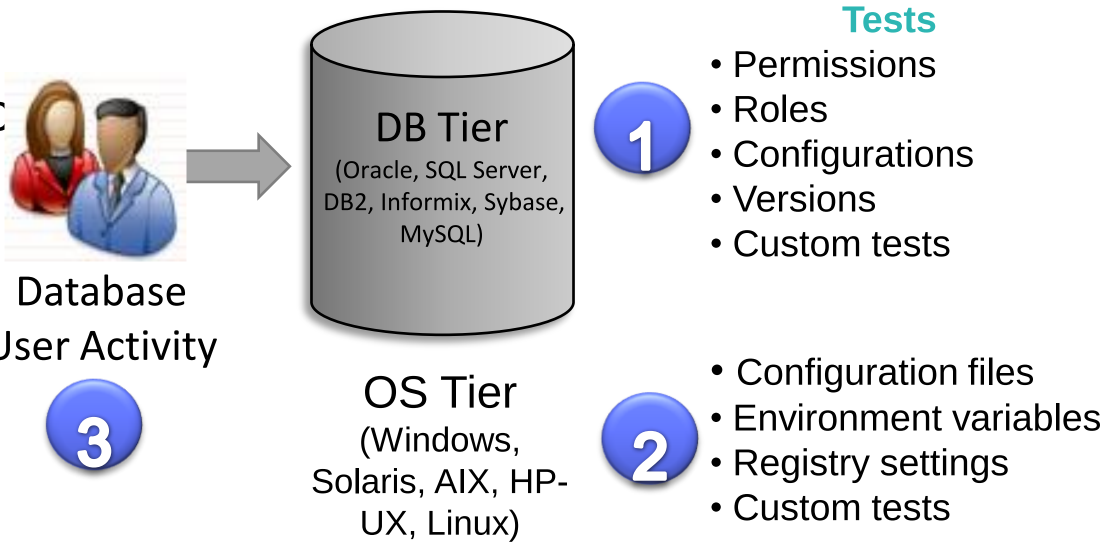
異質資料庫系統的支援

Supported Platforms	Supported Versions
Oracle	8i, 9i, 10g (r1, r2), 11g, 11gR2
Oracle (ASO, SSL)	9i,10g (r1,r2), 11g
Microsoft SQL Server	2000, 2003, 2008
Microsoft SharePoint	2007, 2010
IBM DB2 (Linux, Unix, Linux for System z)	9.1, 9.5, 9.7
IBM DB2 for z/OS	7, 8, 9
IBM DB2 (Windows)	9.1, 9.2, 9.5, 9.7
IBM DB2 for iSeries	V5R2, V5R3, V5R4, V6R1
IBM Informix	7, 9, 10,11, 11.5
Oracle MySQL and MySQL Cluster	4.1, 5.0, 5.1
Sybase ASE	12, 15, 15.5
Sybase IQ	12.6, 15
Teradata	6.x, 12,13
Netezza	4.5
PostgreSQL	8

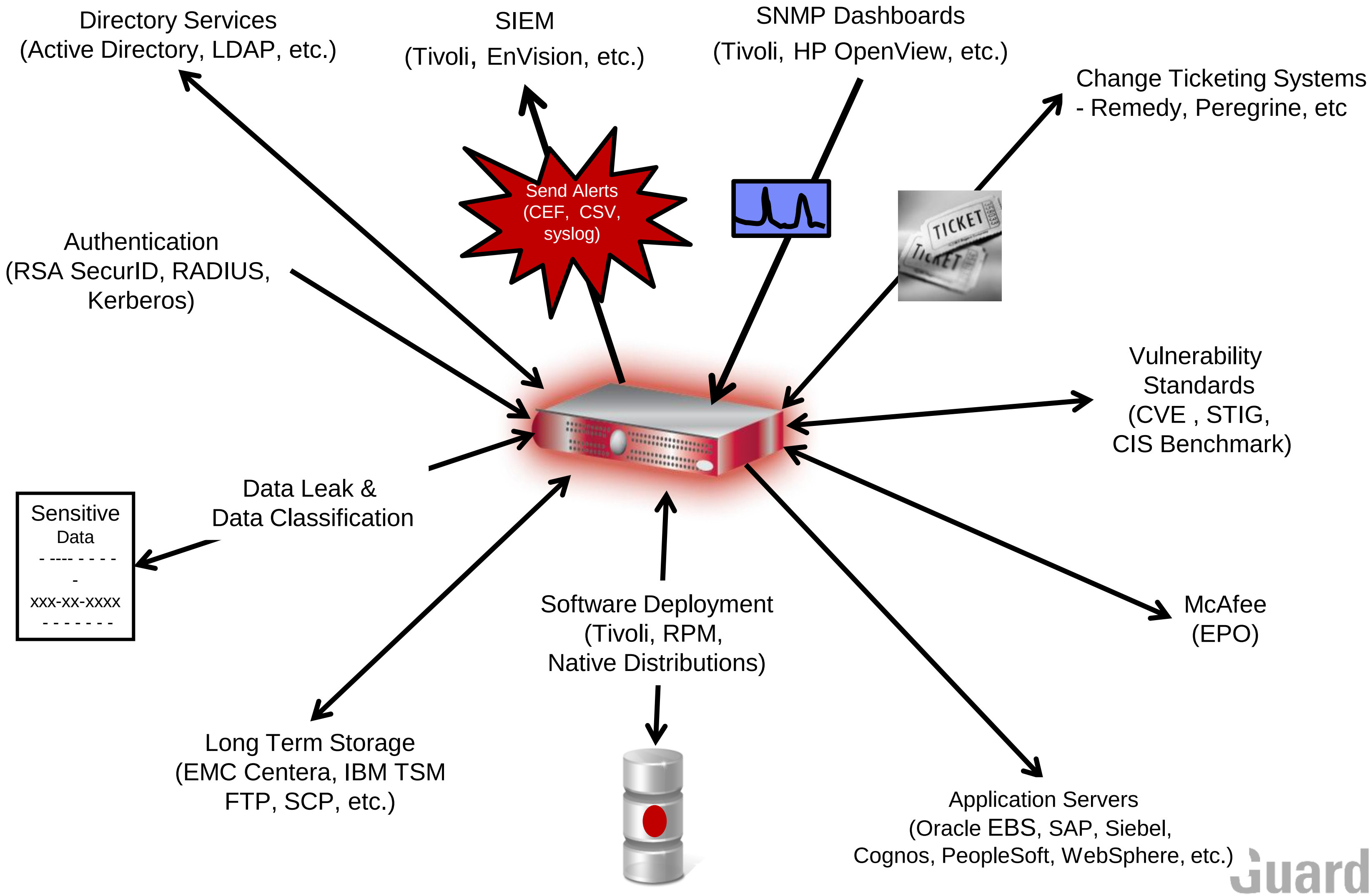
rdium
SAFEGUARDING DATABASES AN IBM COMPANY

弱點評估與配置變更管理

- 基於產業的測試標準 (DISA STIG & CIS Benchmark)
- 可以進行客制化
  – Via custom scripts, SQL queries, environment variables, etc.
- 整合性的測試以確保能涵蓋完整的使用環境
  – Database settings
  – Operating system
  – Observed behavic



與您現有的系統架構完全整合



Directory Services
(Active Directory, LDAP, etc.)

SIEM
(Tivoli, EnVision, etc.)

SNMP Dashboards
(Tivoli, HP OpenView, etc.)

Change Ticketing Systems
- Remedy, Peregrine, etc

Send Alerts
(CEF, CSV,
syslog)

Authentication
(RSA SecurID, RADIUS,
Kerberos)

Vulnerability
Standards
(CVE , STIG,
CIS Benchmark)

Data Leak &
Data Classification

Sensitive
Data
- ---- - - - -
-
xxx-xx-xxxx
- - - - - - -

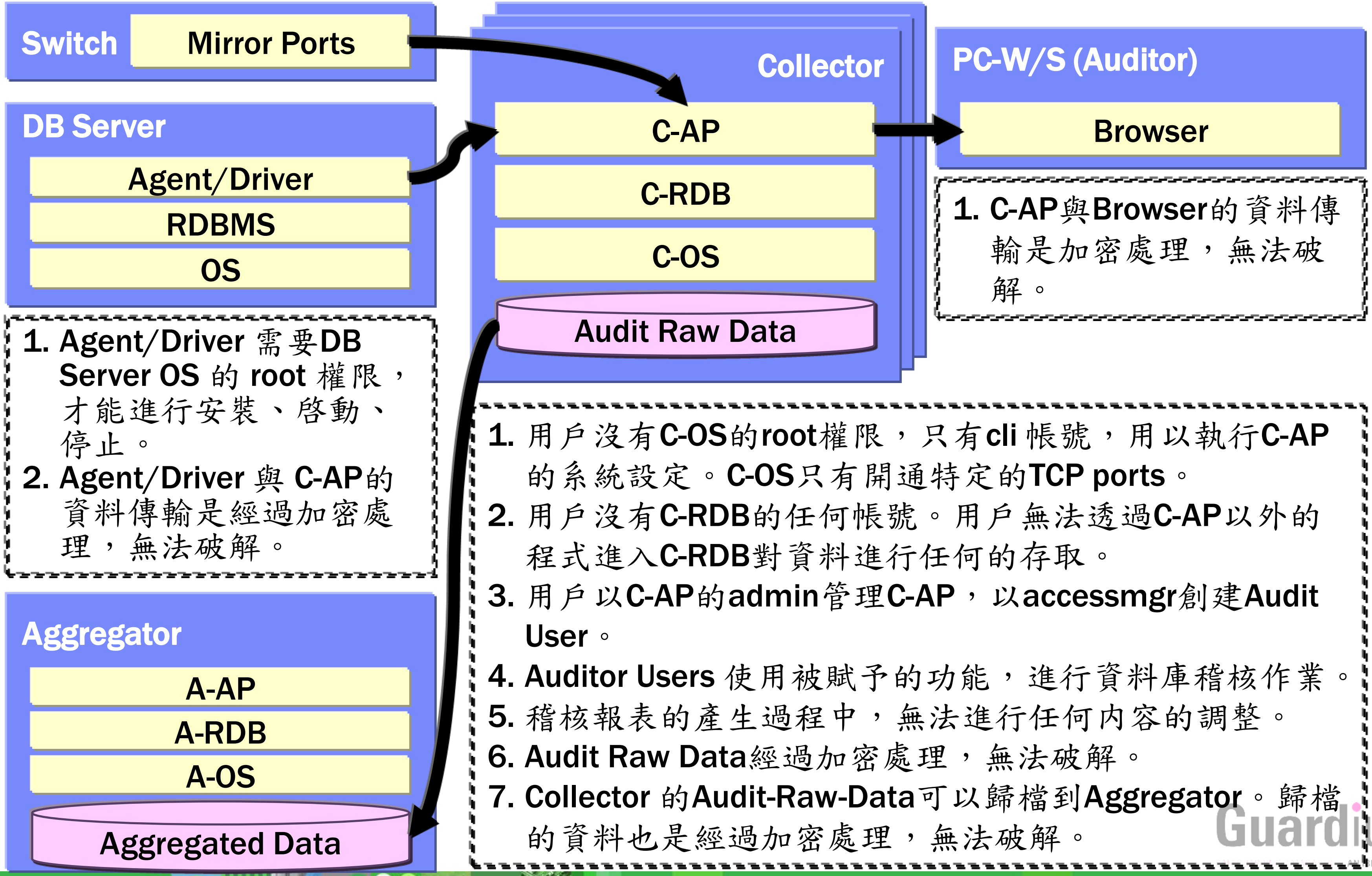
Software Deployment
(Tivoli, RPM,
Native Distributions)

McAfee
(EPO)

Long Term Storage
(EMC Centera, IBM TSM
FTP, SCP, etc.)

Application Servers
(Oracle EBS, SAP, Siebel,
Cognos, PeopleSoft, WebSphere, etc.)

獨立性、安全性與不可否認性

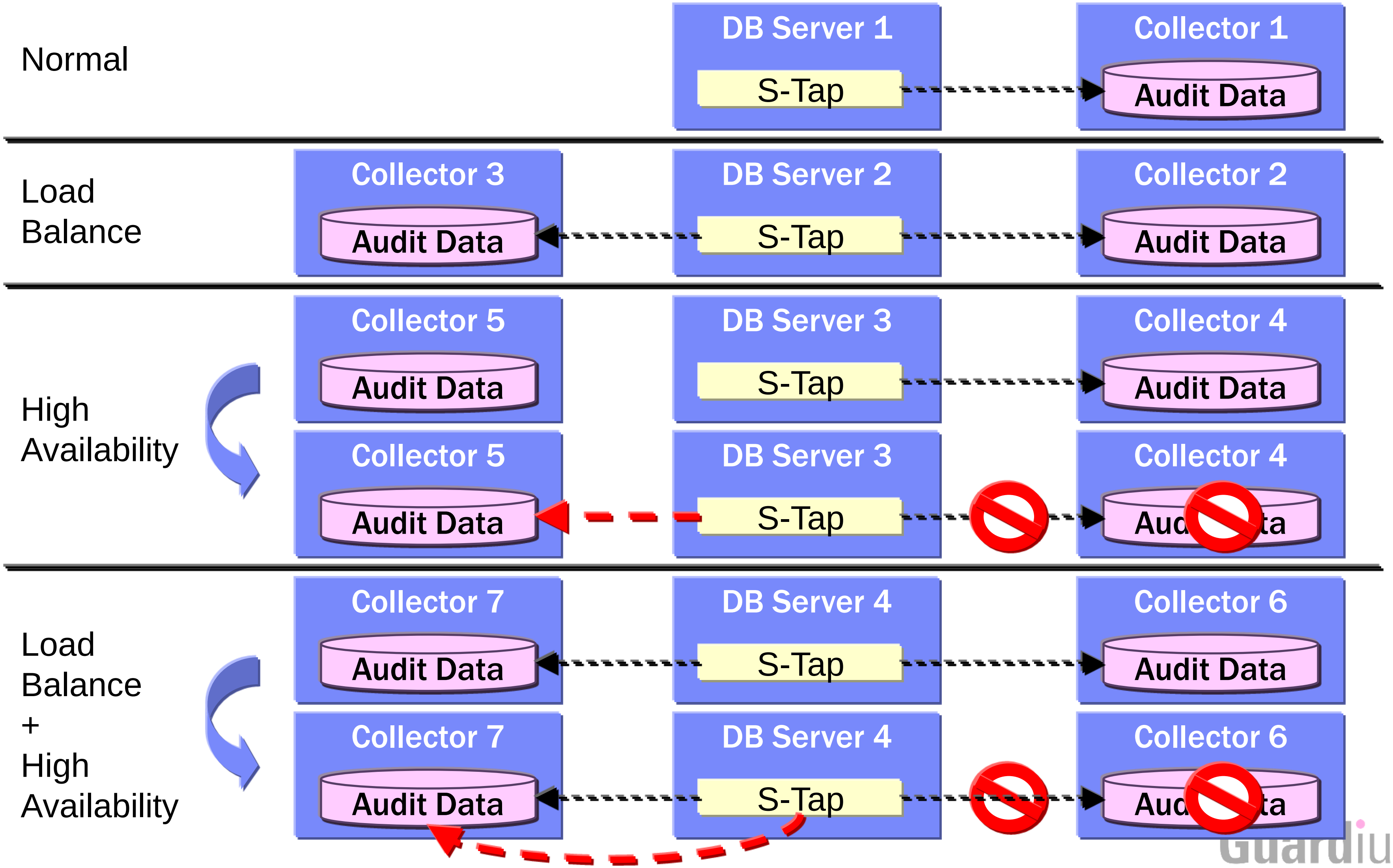


1. Agent/Driver 需要DB Server OS 的 root 權限，才能進行安裝、啓動、停止。
2. Agent/Driver 與 C-AP的資料傳輸是經過加密處理，無法破解。

1. C-AP與Browser的資料傳輸是加密處理，無法破解。

1. 用戶沒有C-OS的root權限，只有cli帳號，用以執行C-AP的系統設定。C-OS只有開通特定的TCP ports。
2. 用戶沒有C-RDB的任何帳號。用戶無法透過C-AP以外的程式進入C-RDB對資料進行任何的存取。
3. 用戶以C-AP的admin管理C-AP，以accessmgr創建Audit User。
4. Auditor Users 使用被賦予的功能，進行資料庫稽核作業。
5. 稽核報表的產生過程中，無法進行任何內容的調整。
6. Audit Raw Data經過加密處理，無法破解。
7. Collector 的Audit-Raw-Data可以歸檔到Aggregator。歸檔的資料也是經過加密處理，無法破解。

DAM 之負載平衡與高可用度



Guardium
AN IBM COMPANY

Guardium通過行業專家的驗證

Validated by Industry Experts

FORRESTER®

"Dominance in this space"
#1 Scores for Current Offering, Architecture & Product Strategy

ChannelWeb

"Most Powerful
Compliance Regulations

the 451 group

SC MAGAZINE

"*5-Star Ratings*: Easy installation, sophisticated reporting, strong policy-based security."

the 451 group

"Guardium is ahead of the pack and gaining speed."

"Guardium is ahead of the pack and gaining speed."

InformationWeek

Top of DBEP Class"

"Practically every feature you'll need to lock down sensitive data."

RED HERRING WINNER 100 N. AMERICA

SQL SERVER magazine

2007 Editor's Choice Award in "Auditing and Compliance"

INFORMATION SECURITY MAGAZINE

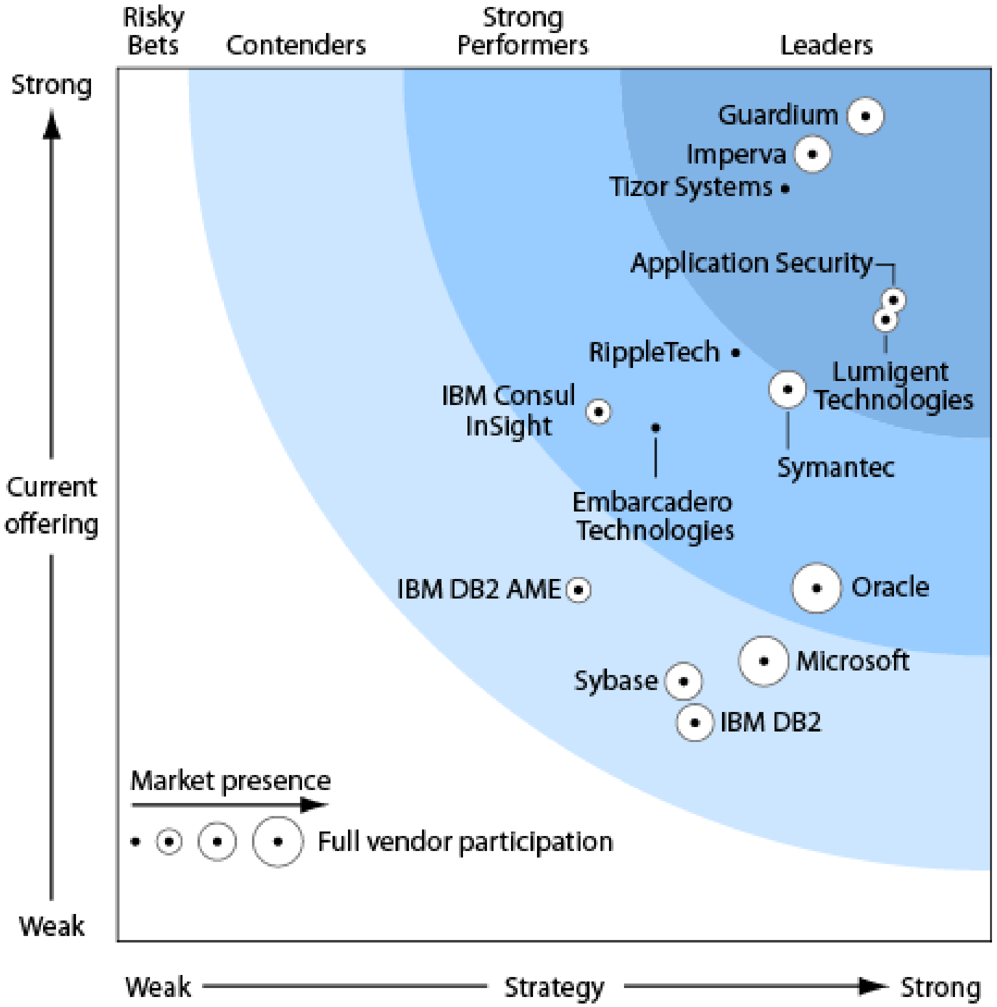
"Enterprise-class data security product that should be on every organization's radar."

INFORMATION SECURITY Hotpick

Guardium AN IBM COMPANY

Highest Overall Score for Current Offering, Corporate & Product Strategy

- “Dominance in this space.”
- “A Leader across the board.”
- “Leadership in supporting large heterogeneous environments,… high performance and scalability, simplifying administration …and real-time database protection."
- “Strong road map ahead with more innovation and features.”



The Forrester Wave is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Source: “The Forrester Wave™: Enterprise Database Auditing and Real-Time Protection

Guardium AN IBM COMPANY

全球領導企業均採用Guardium

- 5 of the top 5 global banks
- 2 of the top 3 global retailers
- 3 of the top 5 global insurers
- 2 of the world’s favorite beverage brands
- The most recognized name in PCs
- 15 of the world’s leading telcos

- Top government agencies
- Top 3 auto maker
- #1 dedicated security company
- Leading energy suppliers
- Major health care providers
- Media & entertainment brands

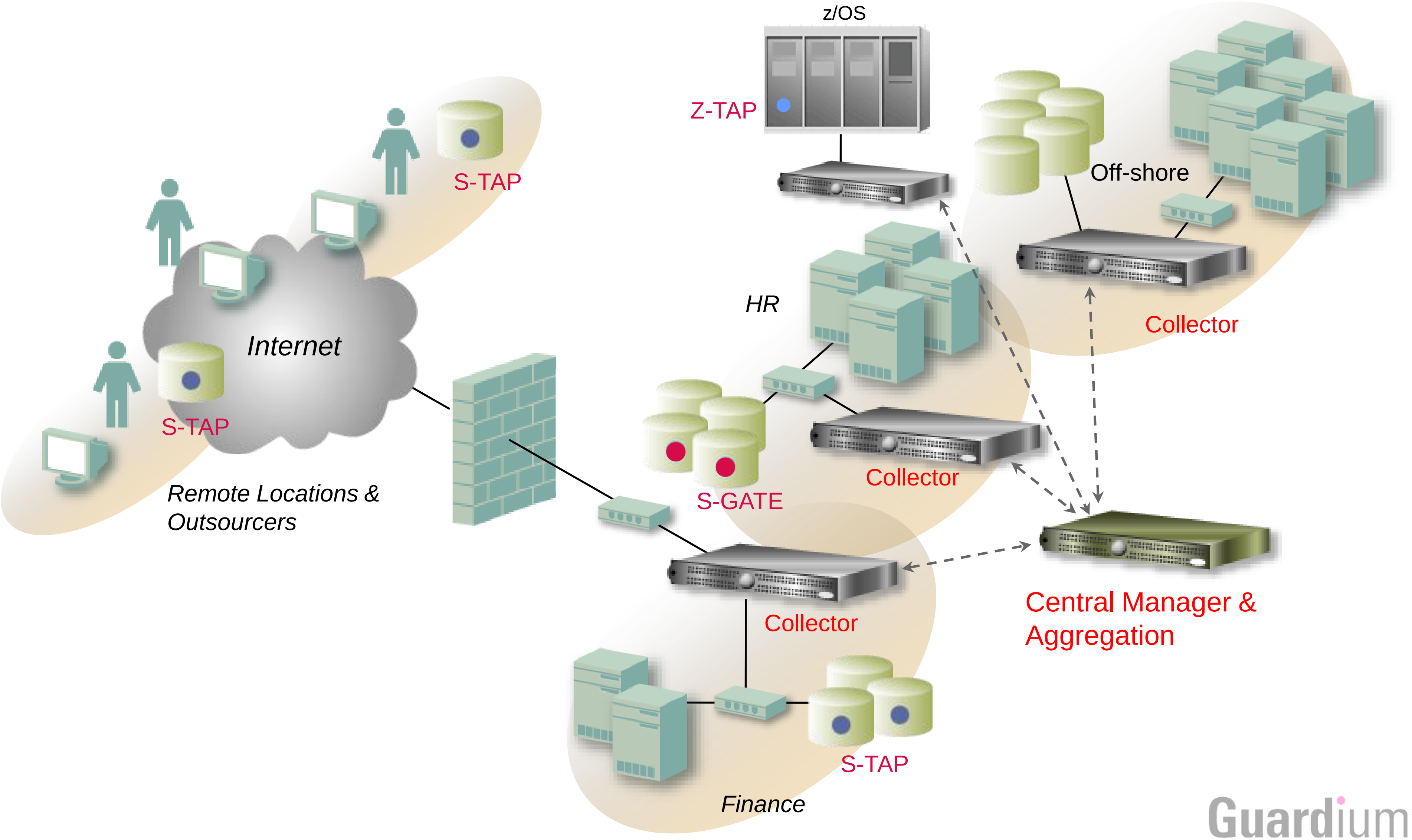
合規的工作

The Compliance Mandate

規定要求	CobiT (SOX)	PCI DSS	HIPAA	CMS ARS	GLBA	ISO 27002	NERC	NIST 800-53 (FISMA)
1.查詢敏感性資料 **(Successful/Failed SELECTs)**		✓	✓	✓	✓	✓		✓
2.改變表定義(DDL) **(Create/Drop/Alter Tables, etc.)**	✓	✓	✓		✓	✓	✓	✓
3.資料操作 (DML) **(Insert, Update, Delete)**	✓			✓		✓		
4.例外操作 **(Failed logins, SQL errors, etc.)**	✓	✓	✓	✓	✓	✓	✓	✓
5.授權變更(DCL) **(GRANT, REVOKE)**	✓	✓	✓	✓	✓	✓	✓	✓

DDL = Data Definition Language (aka schema changes)
DML = Data Manipulation Language (data value changes)
DCL = Data Control Language

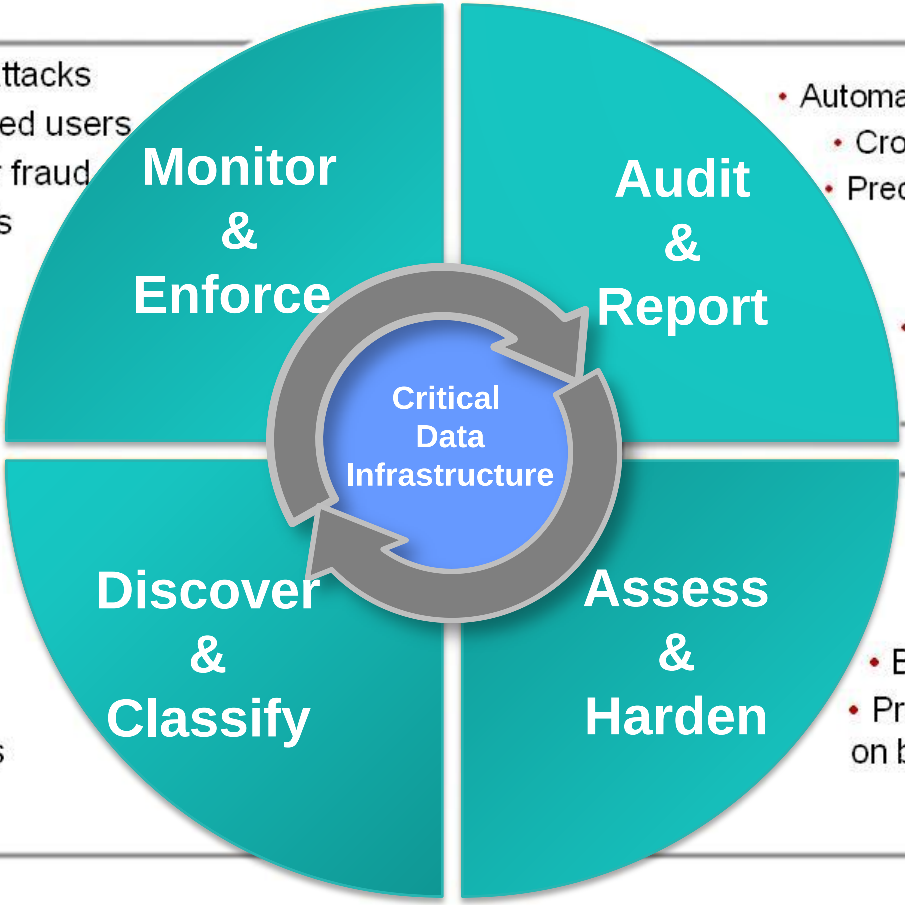
可擴展的多層次架構


z/OS
Z-TAP
Off-shore
Collector
S-TAP
HR
Internet
S-TAP
Collector
S-GATE
Remote Locations &
Outsourcers
Collector
Central Manager &
Aggregation
S-TAP
Finance

Guardium支援完整的資料庫安全生命週期

- Prevent SQL injection attacks
- Monitor & block privileged users
- Detect application-layer fraud
- Enforce change controls
- Real-time alerts
- Forensics data mining
- SIEM integration

- Automated & centralized controls
- Cross-DBMS audit repository
- Preconfigured policies/reports
- Sign-off management
- Long-term retention
- No database changes or performance impact



- Discover & classify sensitive data
- Continuously update security policies
- Discover embedded malware & logic bombs

- Assess database vulnerabilities
- Configuration auditing
- Behavioral vulnerabilities
- Preconfigured tests based on best practices standards (STIG, CIS)

Thank You!

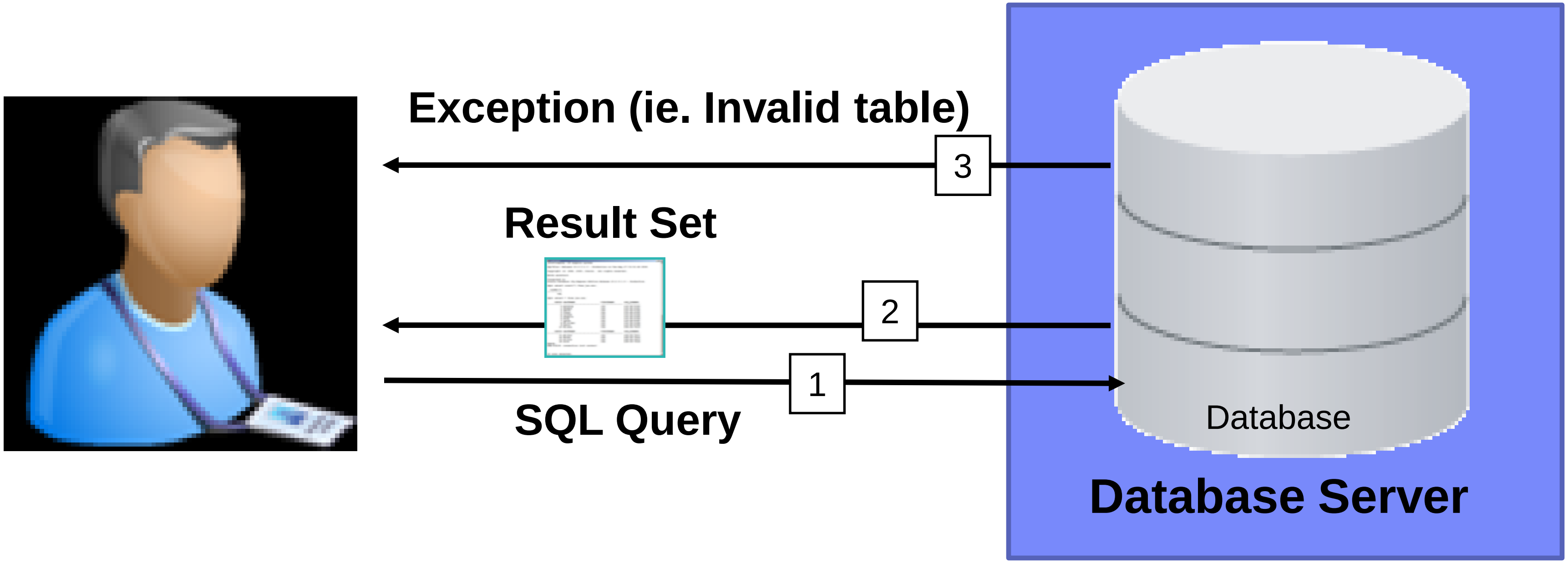
Data Management

Guardium®

SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Backup Slide

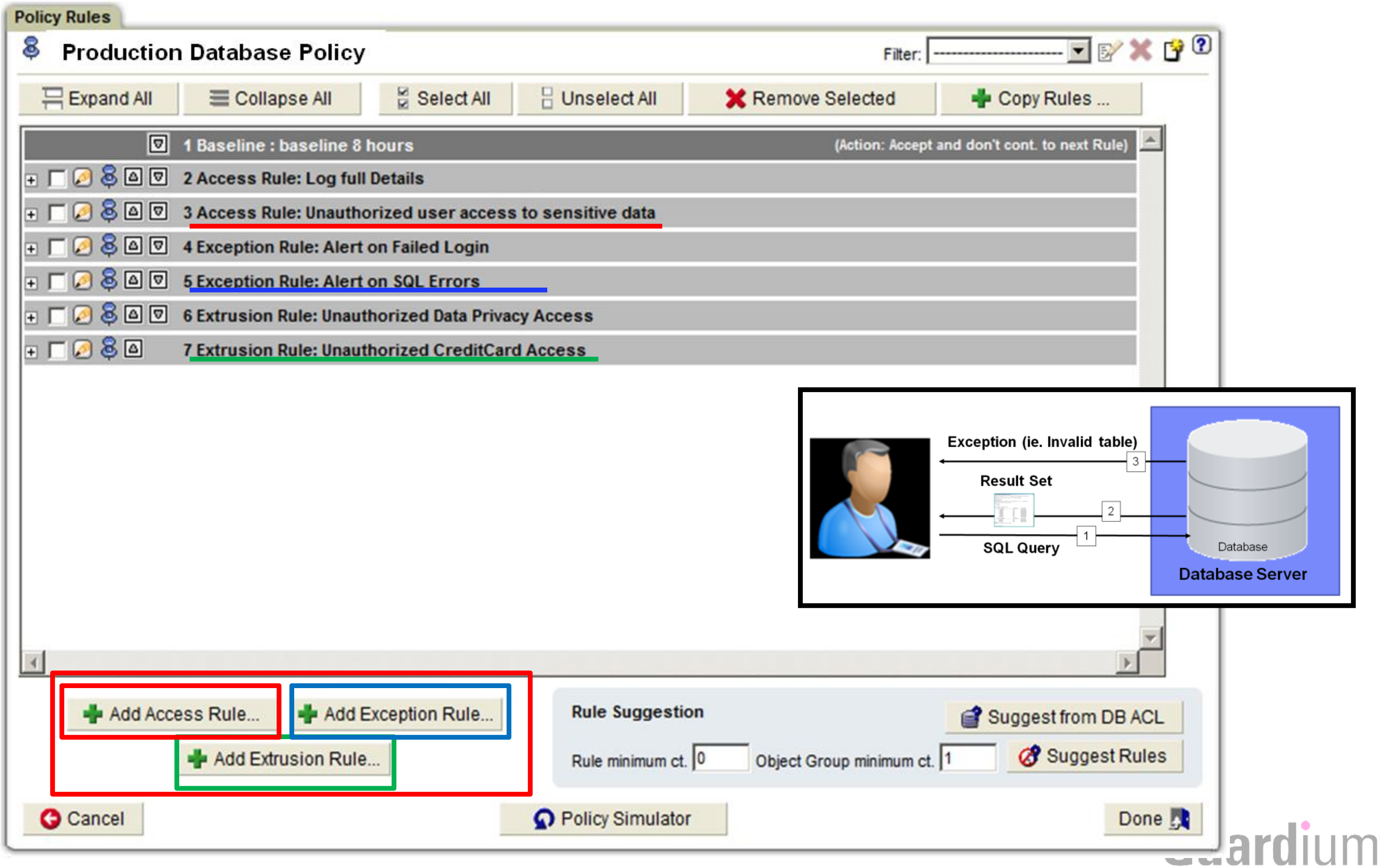
3 Types of Rules



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

Policies



Policy Rules

Production Database Policy

Filter: --------------------

Expand All | Collapse All | Select All | Unselect All | Remove Selected | Copy Rules ...

1 Baseline : baseline 8 hours (Action: Accept and don't cont. to next Rule)

- ☐ 2 Access Rule: Log full Details
- ☐ 3 Access Rule: Unauthorized user access to sensitive data
- ☐ 4 Exception Rule: Alert on Failed Login
- ☐ 5 Exception Rule: Alert on SQL Errors
- ☐ 6 Extrusion Rule: Unauthorized Data Privacy Access
- ☐ 7 Extrusion Rule: Unauthorized CreditCard Access

Add Access Rule... | Add Exception Rule... | Add Extrusion Rule...

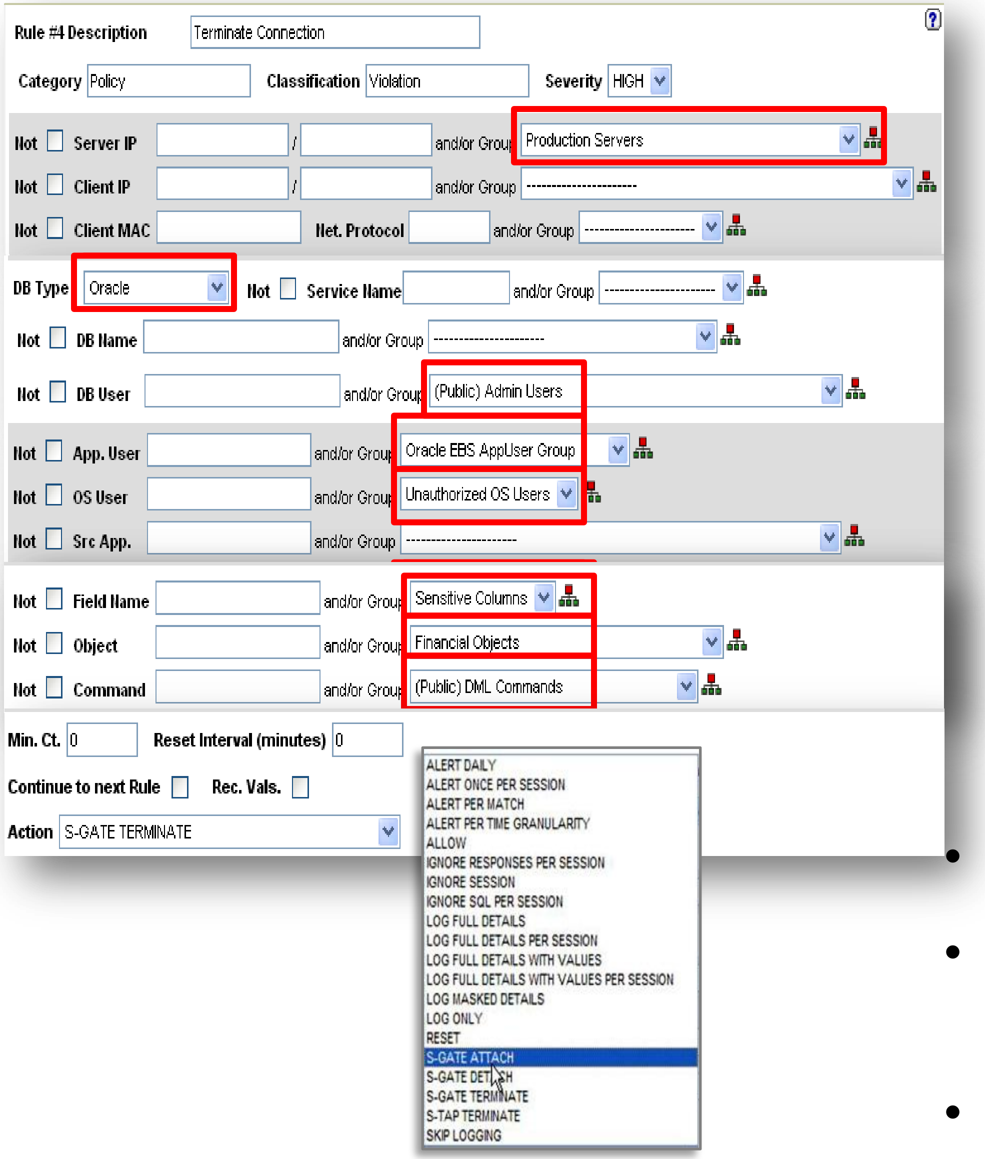
Rule Suggestion

Suggest from DB ACL

Rule minimum ct. 0 Object Group minimum ct. 1 Suggest Rules

Cancel | Policy Simulator | Done

1. Access Policy – Very Granular to Meet Customer Requirements



Rule #4 Description: Terminate Connection

Category: Policy | Classification: Violation | Severity: HIGH

Not □ Server IP / and/or Group: Production Servers

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

Not □ Client MAC | Net. Protocol | and/or Group: ---------------------

DB Type: Oracle | Not □ Service Name | and/or Group: ---------------------

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

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

Not □ App. User | and/or Group: Oracle EBS AppUser Group

Not □ OS User | and/or Group: Unauthorized OS Users

Not □ Src App. | and/or Group: ---------------------

Not □ Field Name | and/or Group: Sensitive Columns

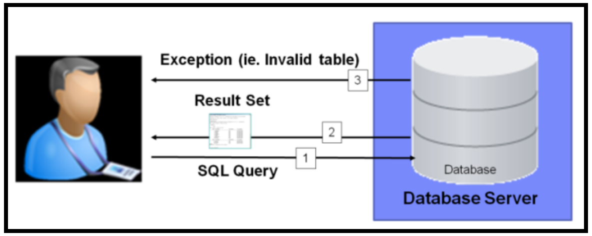
Not □ Object | and/or Group: Financial Objects

Not □ Command | and/or Group: (Public) DML Commands

Min. Ct. 0 | Reset Interval (minutes) 0

Continue to next Rule □ | Rec. Vals. □

Action: S-GATE TERMINATE



Which Servers

Which Databases

Which Users

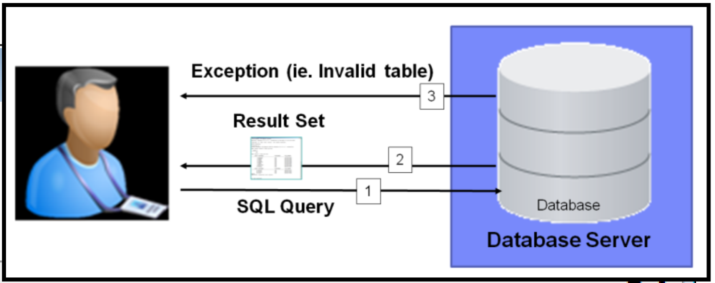
Which Fields

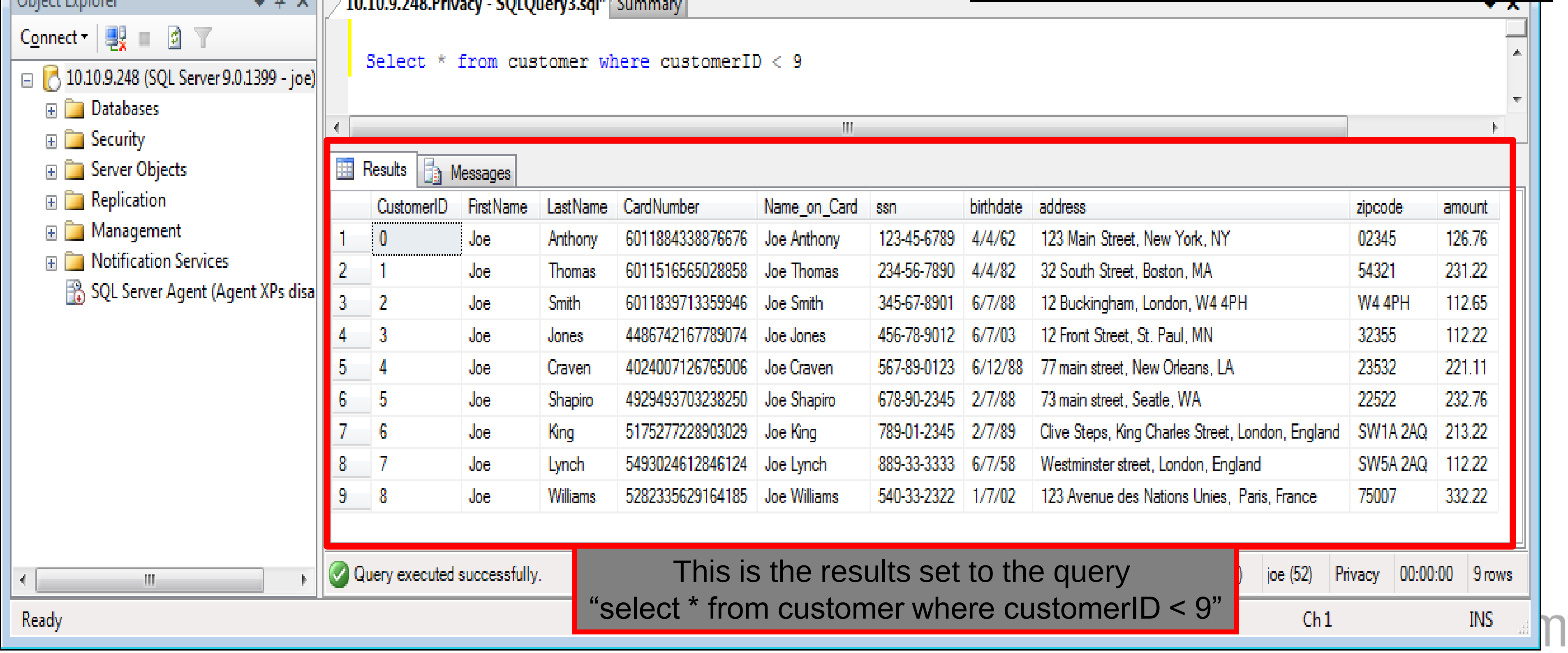
Which Tables

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
Results
Messages
joe (52)
Privacy
00:00:00
9 rows
Ready
Ch 1
INS

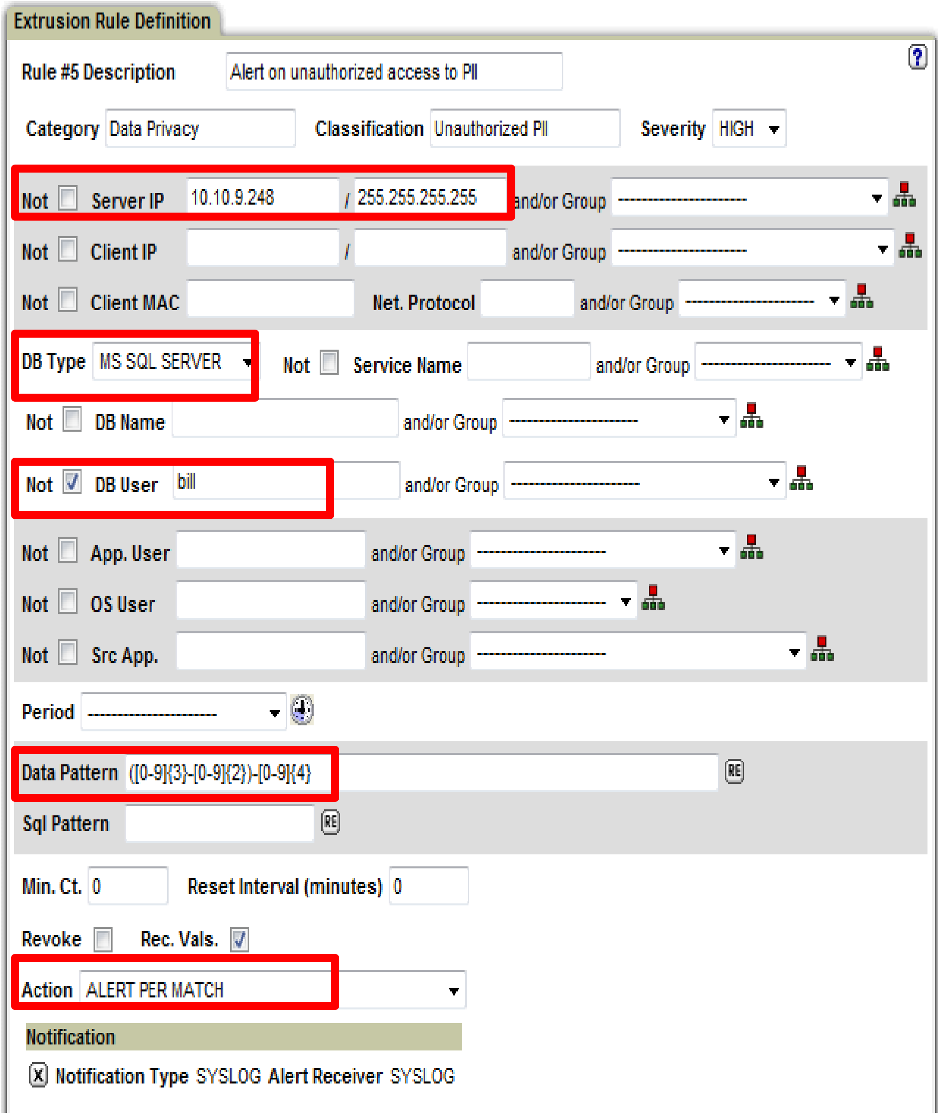
```
Select * from customer where customerID < 9
```

	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.

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

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

Not ☐ Server IP 10.10.9.248 / 255.255.255.255 and/or Group ------------------

Not ☐ Client IP / and/or Group ------------------

Not ☐ Client MAC — Net. Protocol — and/or Group ------------------

DB Type: MS SQL SERVER — Not ☐ Service Name — and/or Group ------------------

Not ☐ DB Name — and/or Group ------------------

Not ☑ DB User bill — and/or Group ------------------

Not ☐ App. User — and/or Group ------------------

Not ☐ OS User — and/or Group ------------------

Not ☐ Src App. — and/or Group ------------------

Period ------------------

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

Sql Pattern

Min. Ct. 0 — Reset Interval (minutes) 0

Revoke ☐ Rec. Vals. ☑

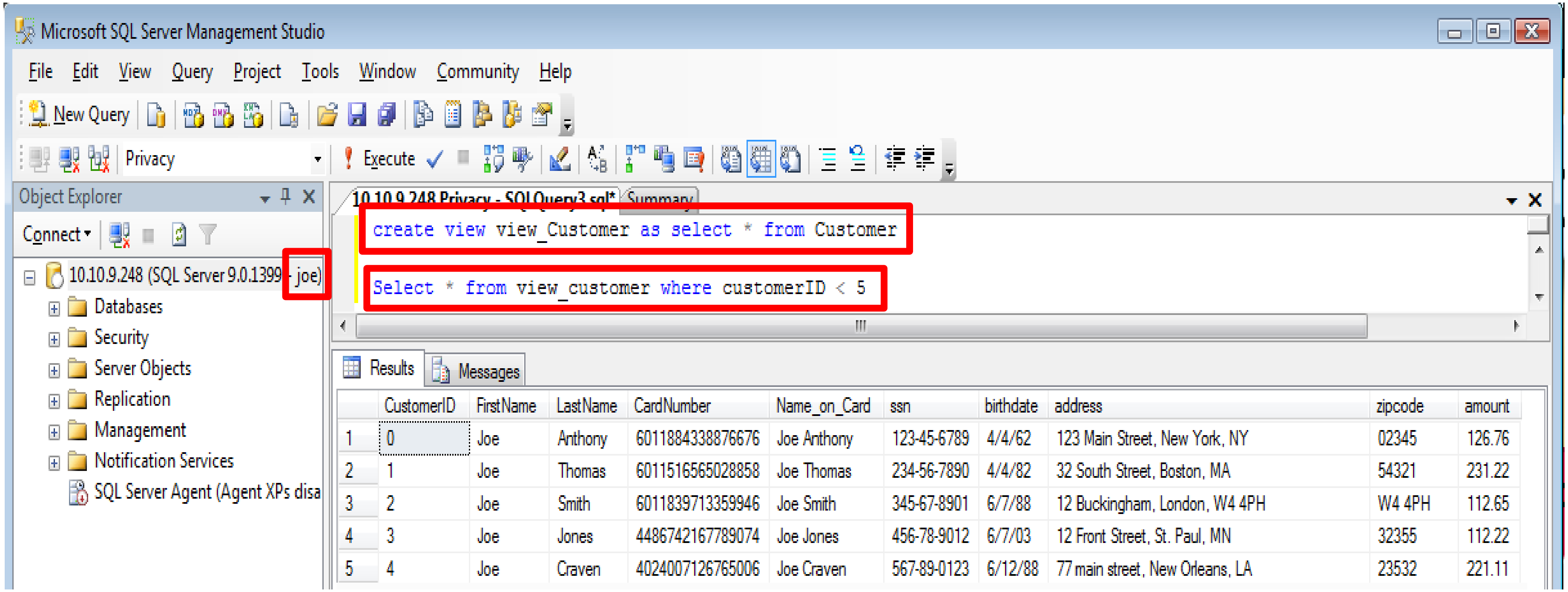
Action: ALERT PER MATCH

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

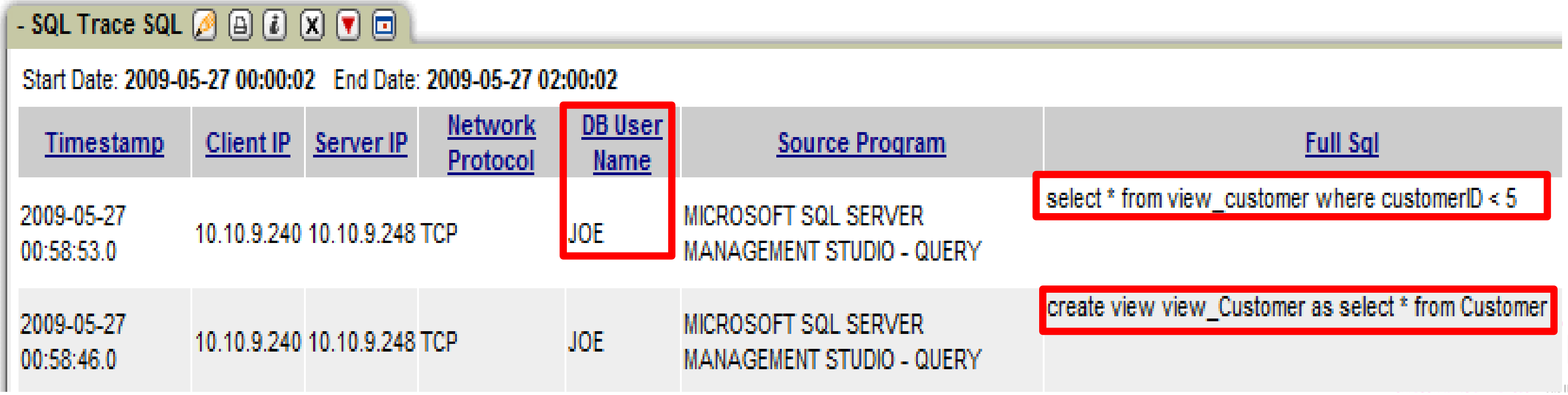
Joe Created a View and Then Tried to Extract Data


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
Results
Messages

```
create view view_Customer as select * from Customer

Select * from view_customer where customerID < 5
```

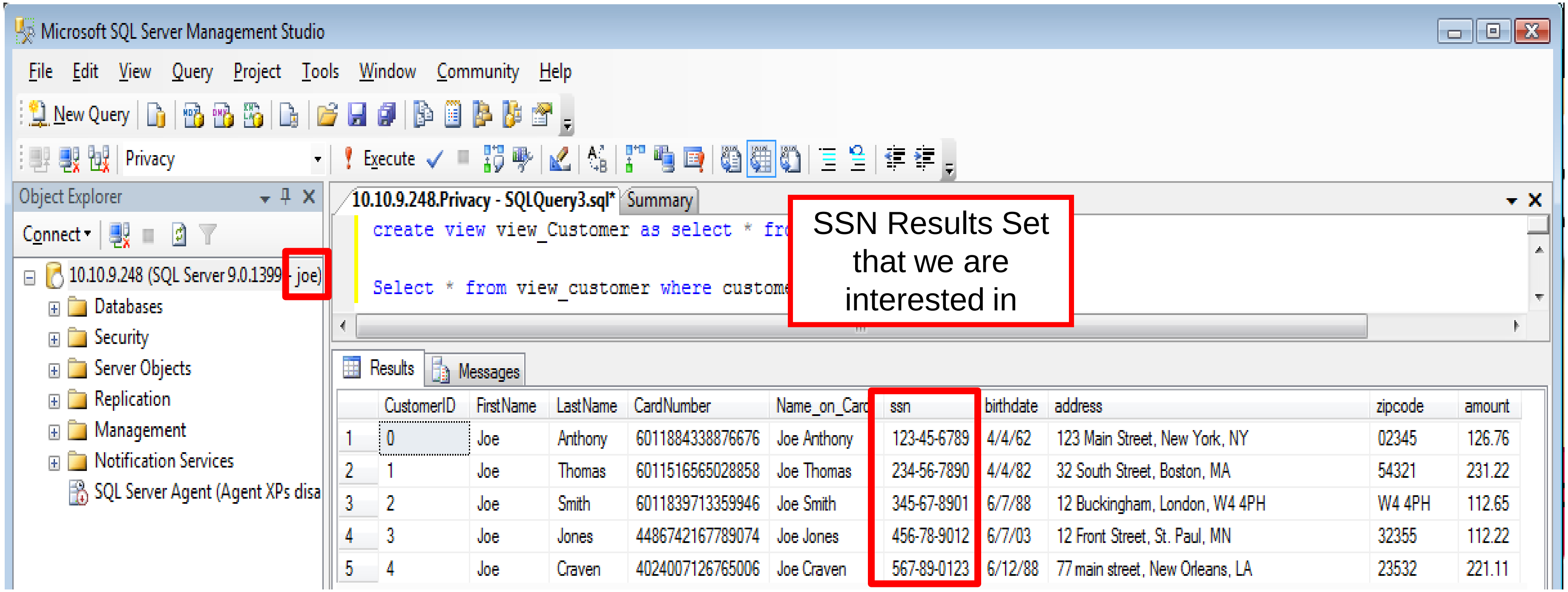
	CustomerID	FirstName	LastName	CardNumber	Name_on_Card	ssn	birthdate	address	zipcode	amount
1	0	Joe	Anthony	6011884338876676	Joe Anthony	123-45-6789	4/4/62	123 Main Street, New York, NY	02345	126.76
2	1	Joe	Thomas	6011516565028858	Joe Thomas	234-56-7890	4/4/82	32 South Street, Boston, MA	54321	231.22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



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
New Query
Privacy
Execute
Object Explorer
Connect
10.10.9.248.Privacy - SQLQuery3.sql*
Summary
Results
Messages

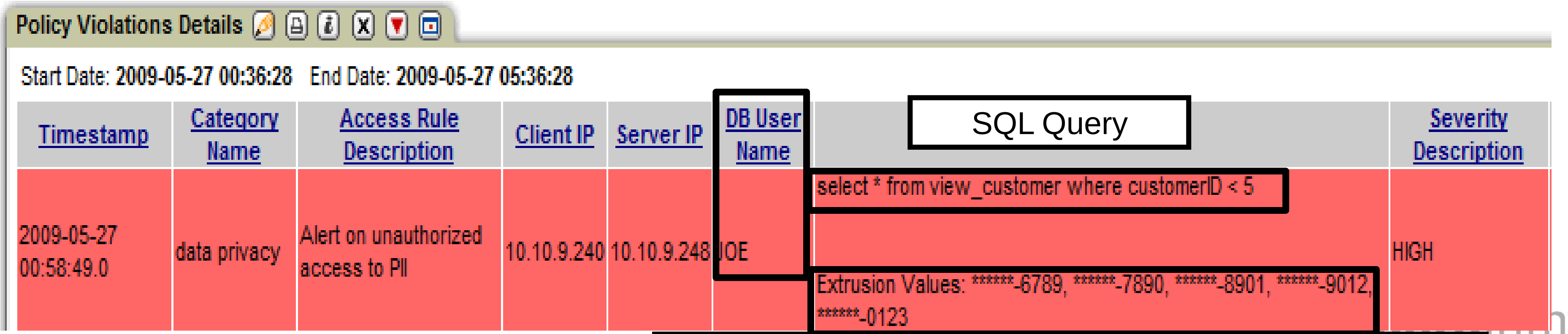
- 10.10.9.248 (SQL Server 9.0.1399 - joe)
  - Databases
  - Security
  - Server Objects
  - Replication
  - Management
  - Notification Services
  - SQL Server Agent (Agent XPs disa

```
create view view_Customer as select * fr

Select * from view_customer where custome
```

SSN Results Set that we are interested in

	CustomerID	FirstName	LastName	CardNumber	Name_on_Carc	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

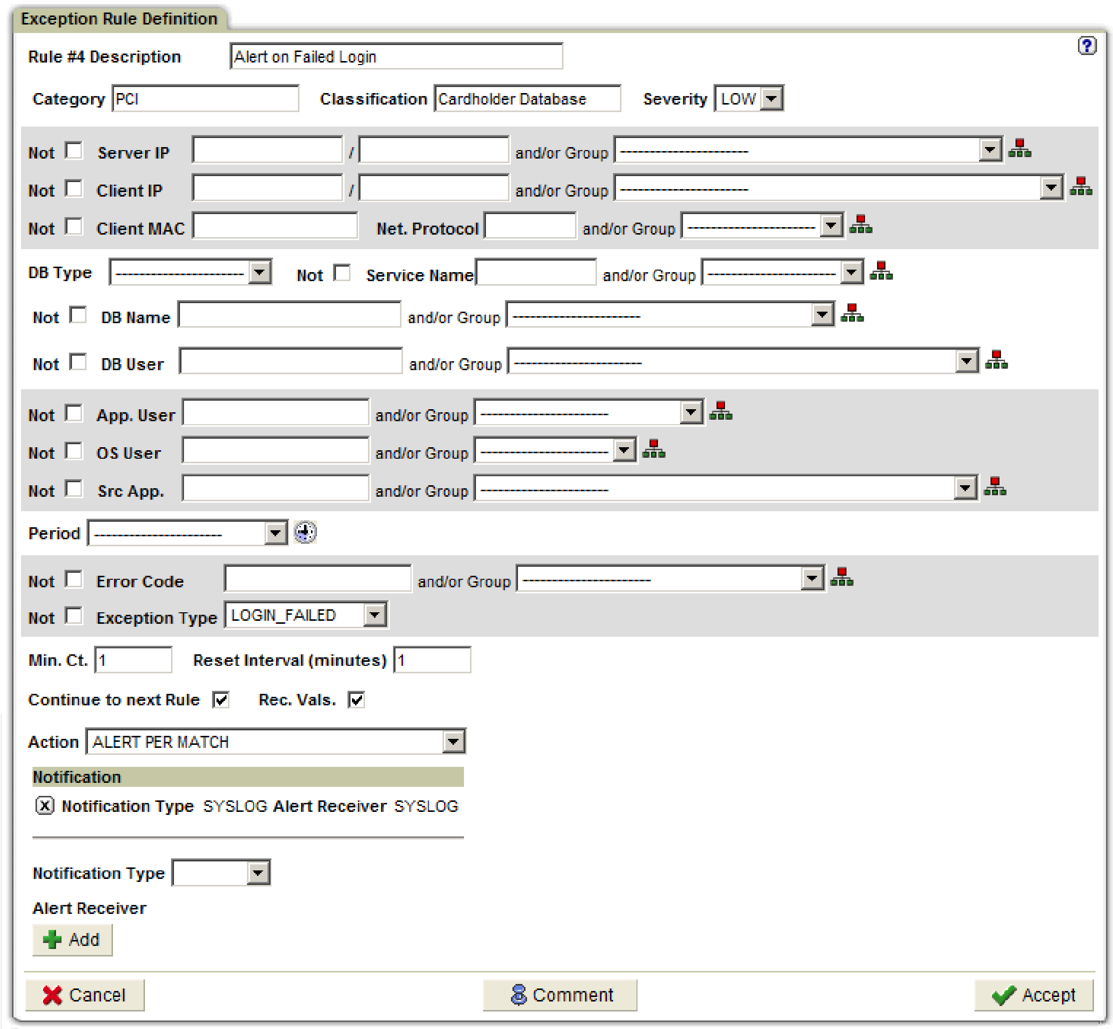

Policy Violations Details

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: Alert on Failed Login

Category: PCI | Classification: Cardholder Database | Severity: LOW

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: LOGIN_FAILED

Min. Ct.: 1 | Reset Interval (minutes): 1

Continue to next Rule ☑ | Rec. Vals. ☑

Action: ALERT PER MATCH

Notification

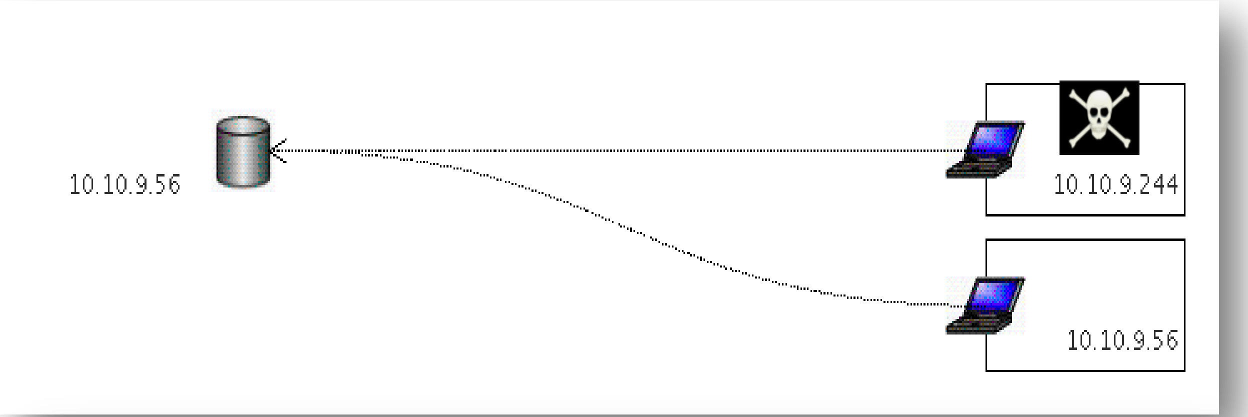
☒ Notification Type SYSLOG Alert Receiver SYSLOG

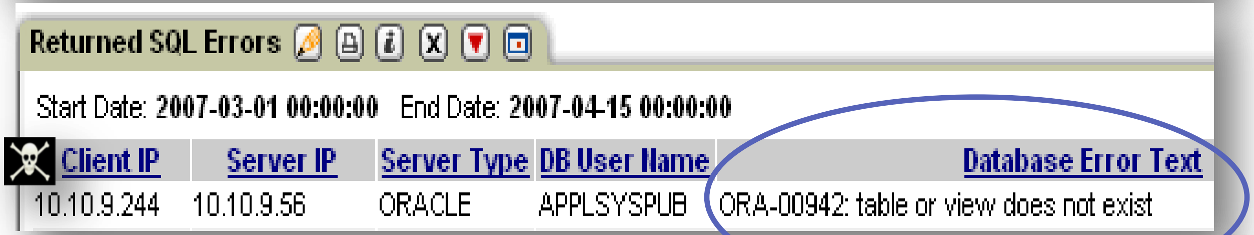
Notification Type

Alert Receiver

- Policy Exceptions
  - Failed logins
  - SQL Errors
  - etc

3. Policy Exception Rule - Preventing Attacks

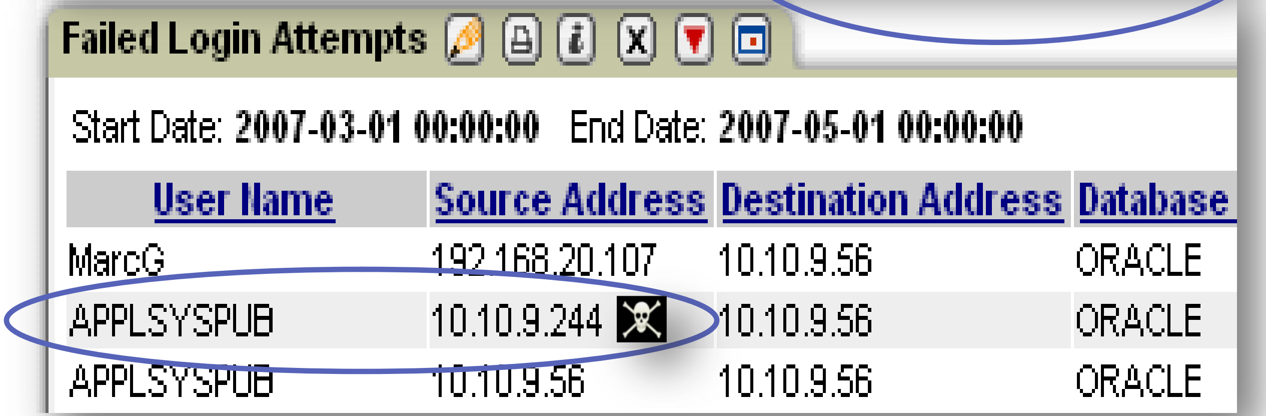




Returned SQL Errors

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



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

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

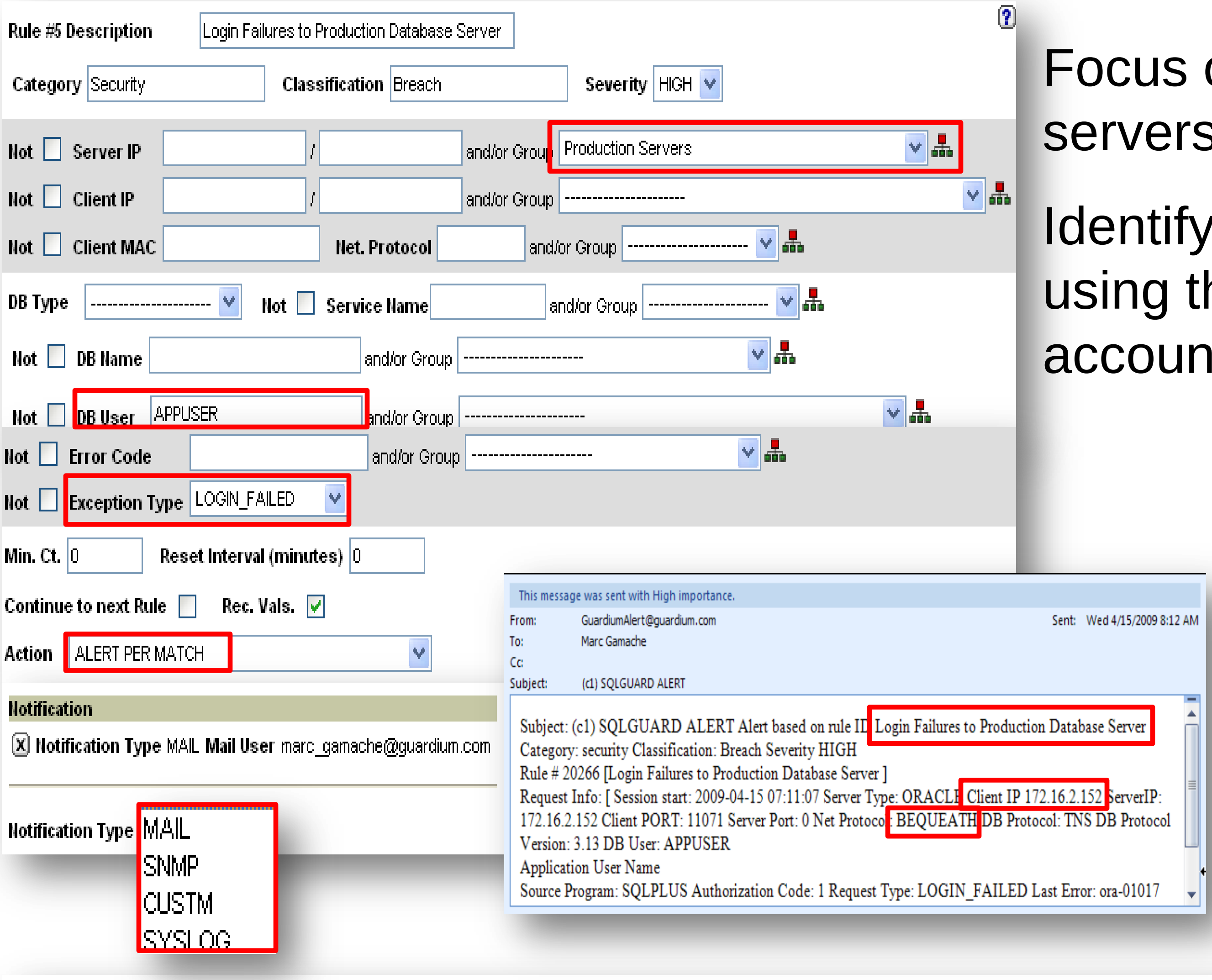
SQL injection leads to **SQL errors**!

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

Guardium: 100% visibility with real-time alerts …

Guardium
AN IBM COMPANY

Exception Policies With Real-Time Alerts



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 Net. Protocol 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.

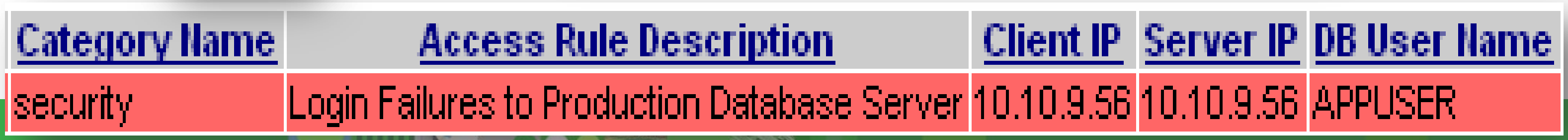
From: GuardiumAlert@guardium.com Sent: Wed 4/15/2009 8:12 AM
To: Marc Gamache
Cc:
Subject: (c1) SQLGUARD ALERT

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

Focus on production DB servers

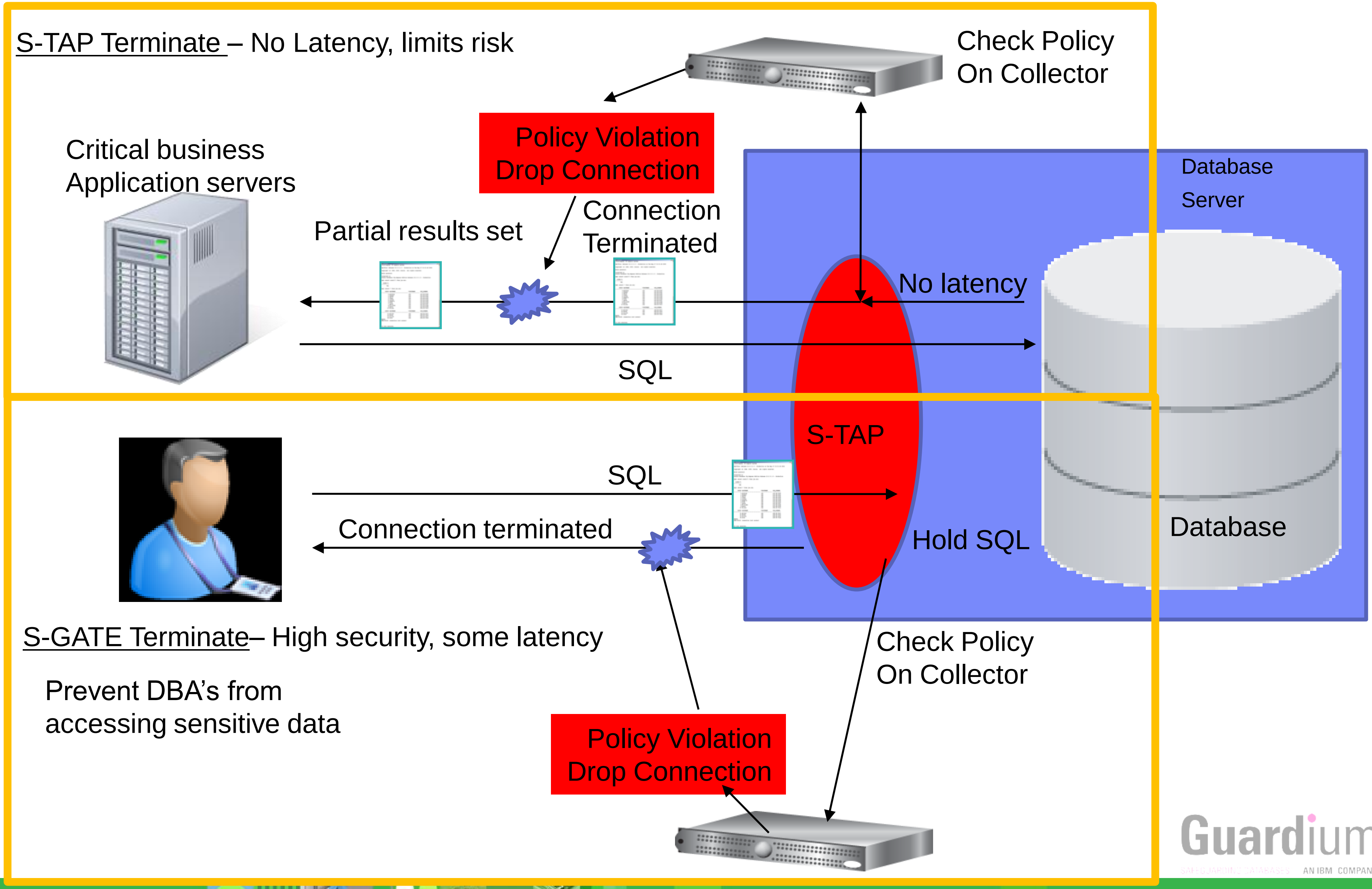
Identify failed login attempts using the application account!

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

Enforcement Configuration Options



S-TAP Terminate – No Latency, limits risk

Check Policy On Collector

Critical business Application servers

Policy Violation Drop Connection

Partial results set

Connection Terminated

Database Server

No latency

SQL

S-TAP

Hold SQL

Database

SQL

Connection terminated

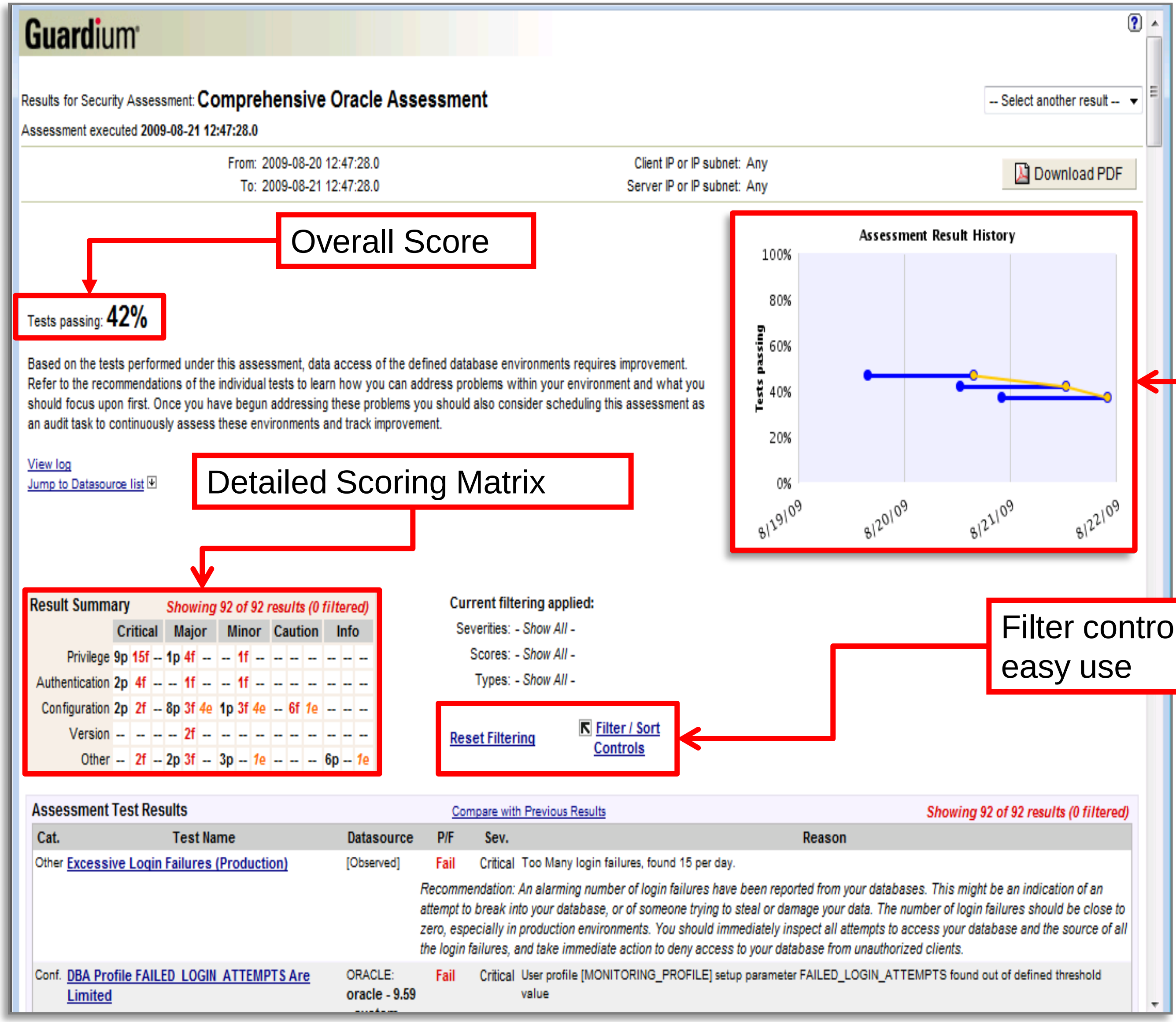
S-GATE Terminate– High security, some latency

Prevent DBA’s from accessing sensitive data

Check Policy On Collector

Policy Violation Drop Connection

Vulnerability Assessment Report



Guardium

Results for Security Assessment: **Comprehensive Oracle Assessment**

-- Select another result --

Assessment executed **2009-08-21 12:47:28.0**

From: 2009-08-20 12:47:28.0
To: 2009-08-21 12:47:28.0

Client IP or IP subnet: Any
Server IP or IP subnet: Any

Download PDF

Tests passing: **42%**

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 92 of 92 results (0 filtered)*

	Critical			Major			Minor			Caution			Info		
Privilege	9p	15f	--	1p	4f	--	--	1f	--	--	--	--	--	--	--
Authentication	2p	4f	--	--	1f	--	--	1f	--	--	--	--	--	--	--
Configuration	2p	2f	--	8p	3f	4e	1p	3f	4e	--	6f	1e	--	--	--
Version	--	--	--	--	2f	--	--	--	--	--	--	--	--	--	--
Other	--	2f	--	2p	3f	--	3p	--	1e	--	--	--	6p	--	1e

Current filtering applied:

Severities: - *Show All* -
Scores: - *Show All* -
Types: - *Show All* -

Reset Filtering
Filter / Sort Controls

Assessment Test Results Compare with Previous Results *Showing 92 of 92 results (0 filtered)*

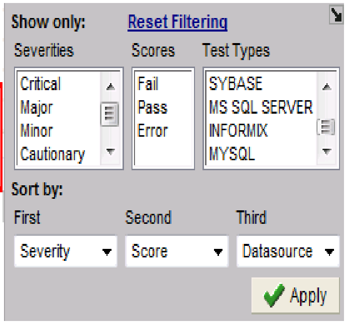
Cat.	Test Name	Datasource	P/F	Sev.	Reason
Other	Excessive Login Failures (Production)	[Observed]	Fail	Critical	Too Many login failures, found 15 per day.
					Recommendation: An alarming number of login failures have been reported from your databases. This might be an indication of an attempt to break into your database, or of someone trying to steal or damage your data. The number of login failures should be close to zero, especially in production environments. You should immediately inspect all attempts to access your database and the source of all the login failures, and take immediate action to deny access to your database from unauthorized clients.
Conf.	DBA Profile FAILED_LOGIN_ATTEMPTS Are Limited	ORACLE: oracle - 9.59	Fail	Critical	User profile [MONITORING_PROFILE] setup parameter FAILED_LOGIN_ATTEMPTS found out of defined threshold value

Overall Score

Detailed Scoring Matrix

Historical Progress or Regression

Filter control for easy use



Show only: Reset Filtering

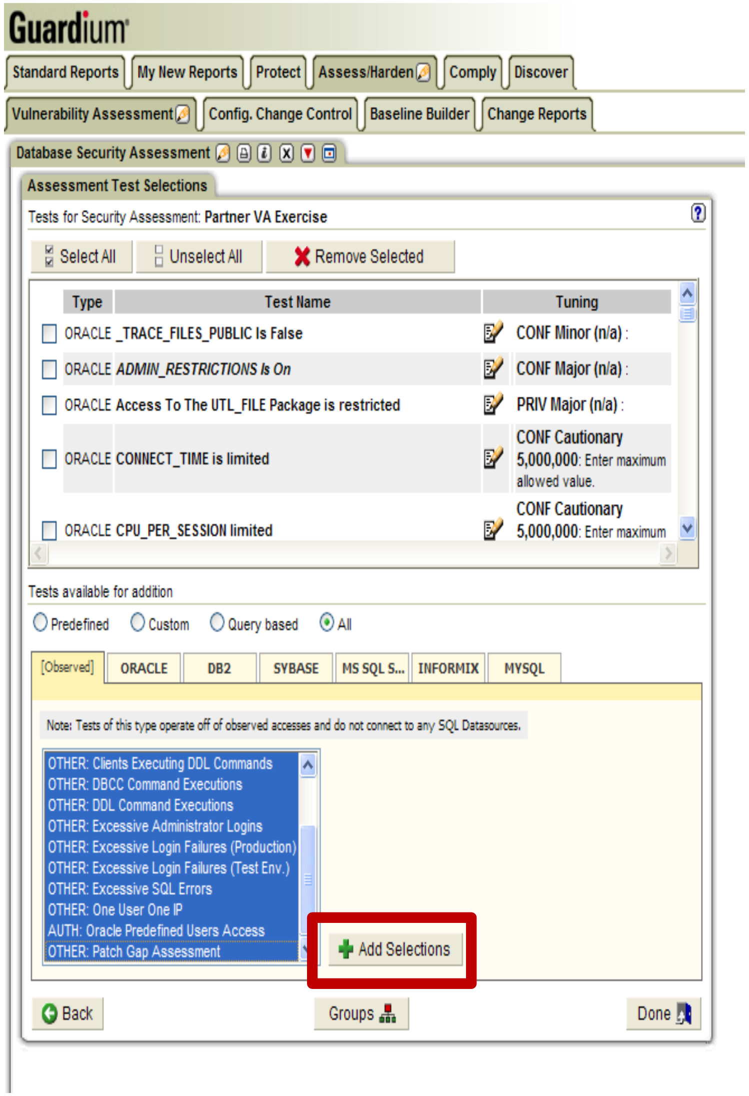
Severities	Scores	Test Types
Critical Major Minor Cautionary	Fail Pass Error	SYBASE MS SQL SERVER INFORMIX MYSQL

Sort by:

First	Second	Third
Severity	Score	Datasource

Apply

Vulnerability Assessment Example



Tests for Security Assessment: Partner VA Exercise

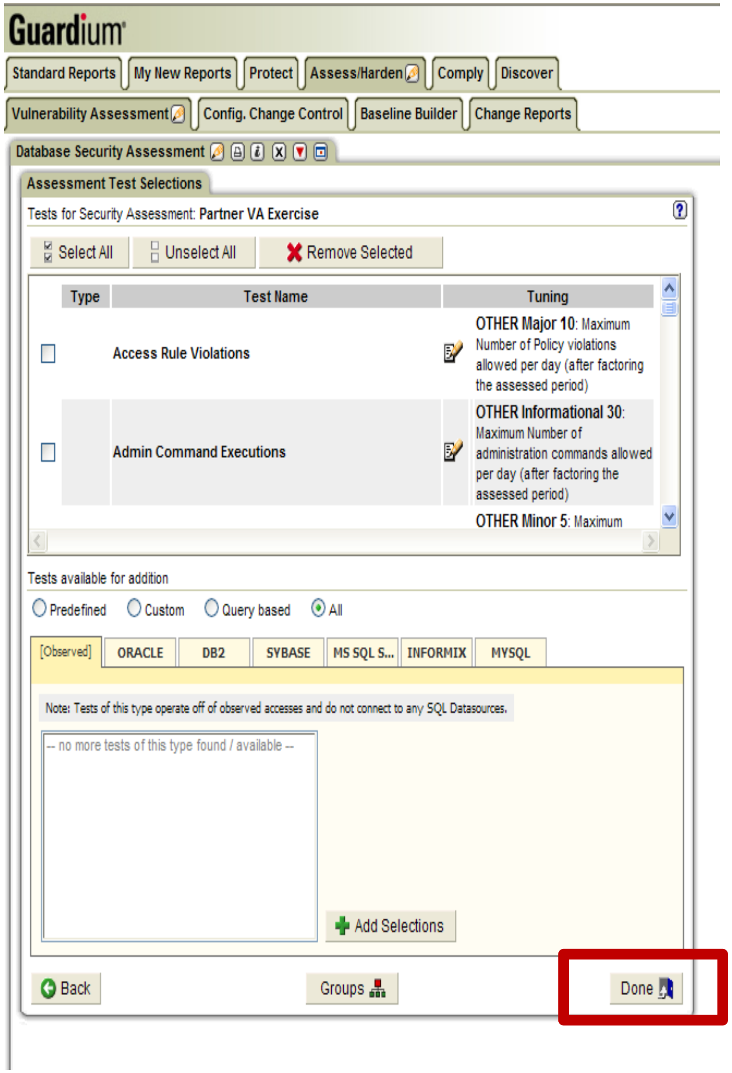
	Type	Test Name	Tuning
□	ORACLE	_TRACE_FILES_PUBLIC Is False	CONF Minor (n/a) :
□	ORACLE	*ADMIN_RESTRICTIONS Is On*	CONF Major (n/a) :
□	ORACLE	Access To The UTL_FILE Package is restricted	PRIV Major (n/a) :
□	ORACLE	CONNECT_TIME is limited	CONF Cautionary 5,000,000: Enter maximum allowed value.
□	ORACLE	CPU_PER_SESSION limited	CONF Cautionary 5,000,000: Enter maximum

Tests available for addition

○ Predefined ○ Custom ○ Query based ● All

Note: Tests of this type operate off of observed accesses and do not connect to any SQL Datasources.

- OTHER: Clients Executing DDL Commands
- OTHER: DBCC Command Executions
- OTHER: DDL Command Executions
- OTHER: Excessive Administrator Logins
- OTHER: Excessive Login Failures (Production)
- OTHER: Excessive Login Failures (Test Env.)
- OTHER: Excessive SQL Errors
- OTHER: One User One IP
- AUTH: Oracle Predefined Users Access
- OTHER: Patch Gap Assessment



Tests for Security Assessment: Partner VA Exercise

	Type	Test Name	Tuning
□		Access Rule Violations	OTHER Major 10: Maximum Number of Policy violations allowed per day (after factoring the assessed period)
□		Admin Command Executions	OTHER Informational 30: Maximum Number of administration commands allowed per day (after factoring the assessed period)
			OTHER Minor 5: Maximum

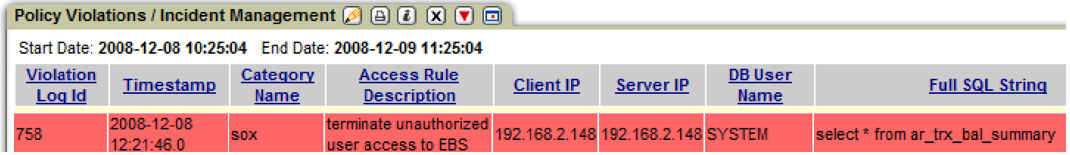
Tests available for addition

○ Predefined ○ Custom ○ Query based ● All

Note: Tests of this type operate off of observed accesses and do not connect to any SQL Datasources.

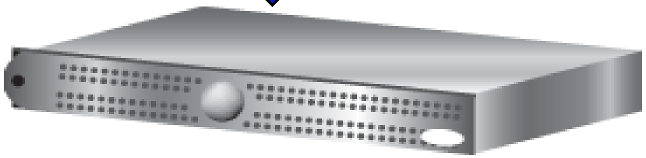
-- no more tests of this type found / available --

Integration with Security Infrastructure
Send Policy Violation to SIEM



Start Date: 2008-12-08 10:25:04 End Date: 2008-12-09 11:25:04

Violation Log Id	Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String
758	2008-12-08 12:21:46.0	sox	terminate unauthorized user access to EBS	192.168.2.148	192.168.2.148	SYSTEM	select * from ar_trx_bal_summary



Guardium

SIEM Vendors
Tivoli, ArcSight, CA, EnVision, LogLogic, SenSage, etc
-FW
-Windows
-Unix
-Cisco
-AV
-IDS
-Etc

Transport - Syslog, CEF, SNMP, csv,etc

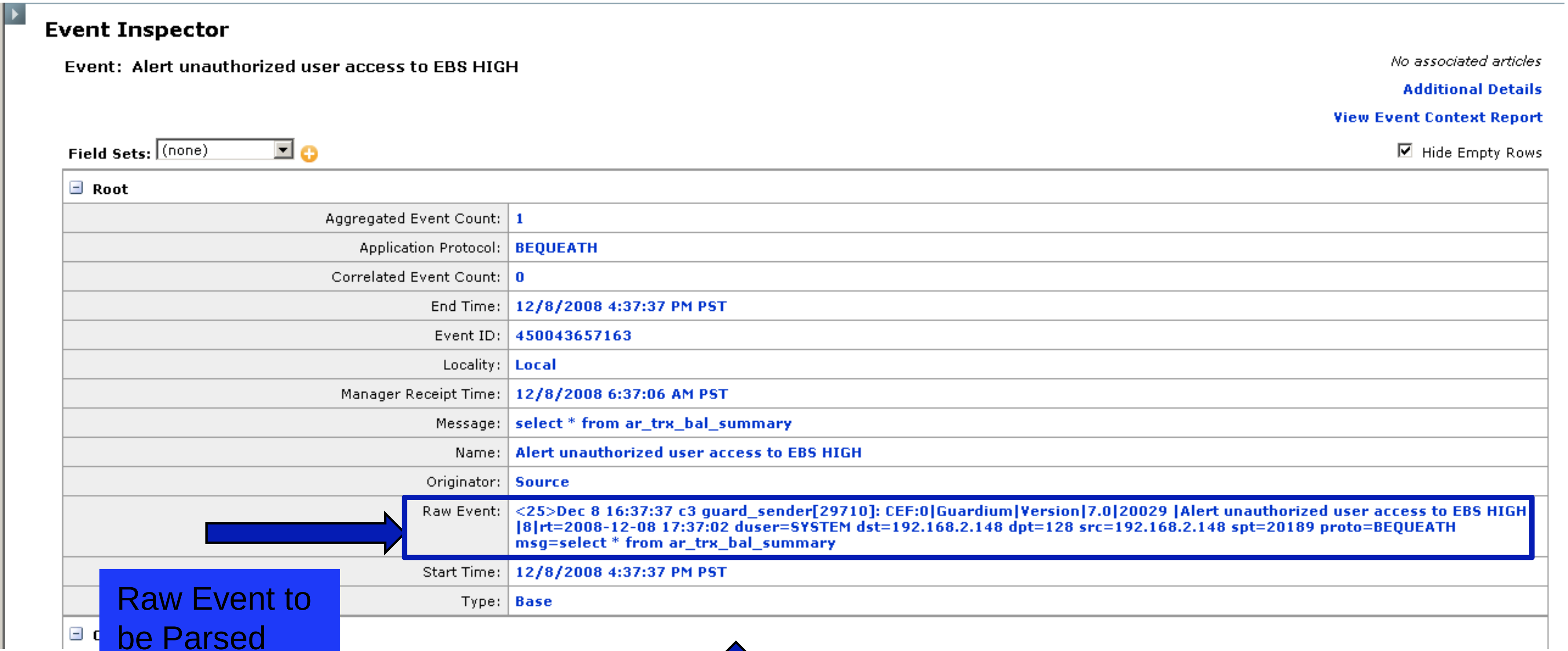
Send Security Event to SIEM

SIEM Vendor Schema
Src, Dst, log field, action, vulnerability level, priority

Mapping

Guardium
SIEM Templates for mapping
Src, Dst, log field, action, vulnerability level, priority

TCIM Raw Event



Event Inspector

Event: Alert unauthorized user access to EBS HIGH

No associated articles

Additional Details

View Event Context Report

Field Sets: (none)

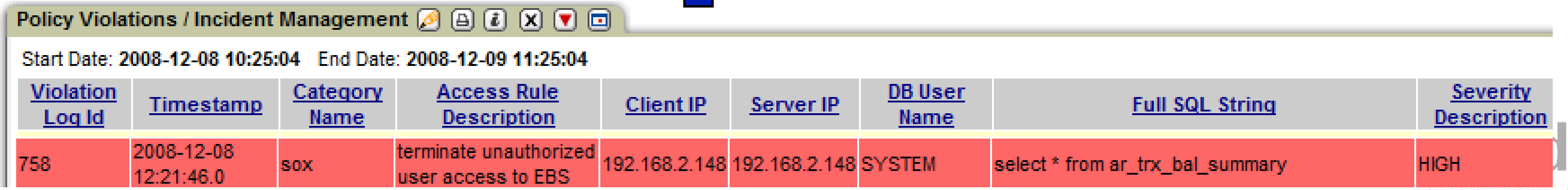
☑ Hide Empty Rows

⊟ Root

Aggregated Event Count:	1
Application Protocol:	BEQUEATH
Correlated Event Count:	0
End Time:	12/8/2008 4:37:37 PM PST
Event ID:	450043657163
Locality:	Local
Manager Receipt Time:	12/8/2008 6:37:06 AM PST
Message:	select * from ar_trx_bal_summary
Name:	Alert unauthorized user access to EBS HIGH
Originator:	Source
Raw Event:	<25>Dec 8 16:37:37 c3 guard_sender[29710]: CEF:0|Guardium|Version|7.0|20029 |Alert unauthorized user access to EBS HIGH |8|rt=2008-12-08 17:37:02 duser=SYSTEM dst=192.168.2.148 dpt=128 src=192.168.2.148 spt=20189 proto=BEQUEATH msg=select * from ar_trx_bal_summary
Start Time:	12/8/2008 4:37:37 PM PST
Type:	Base

Raw Event to be Parsed

Policy Violation Sent to ArcSight

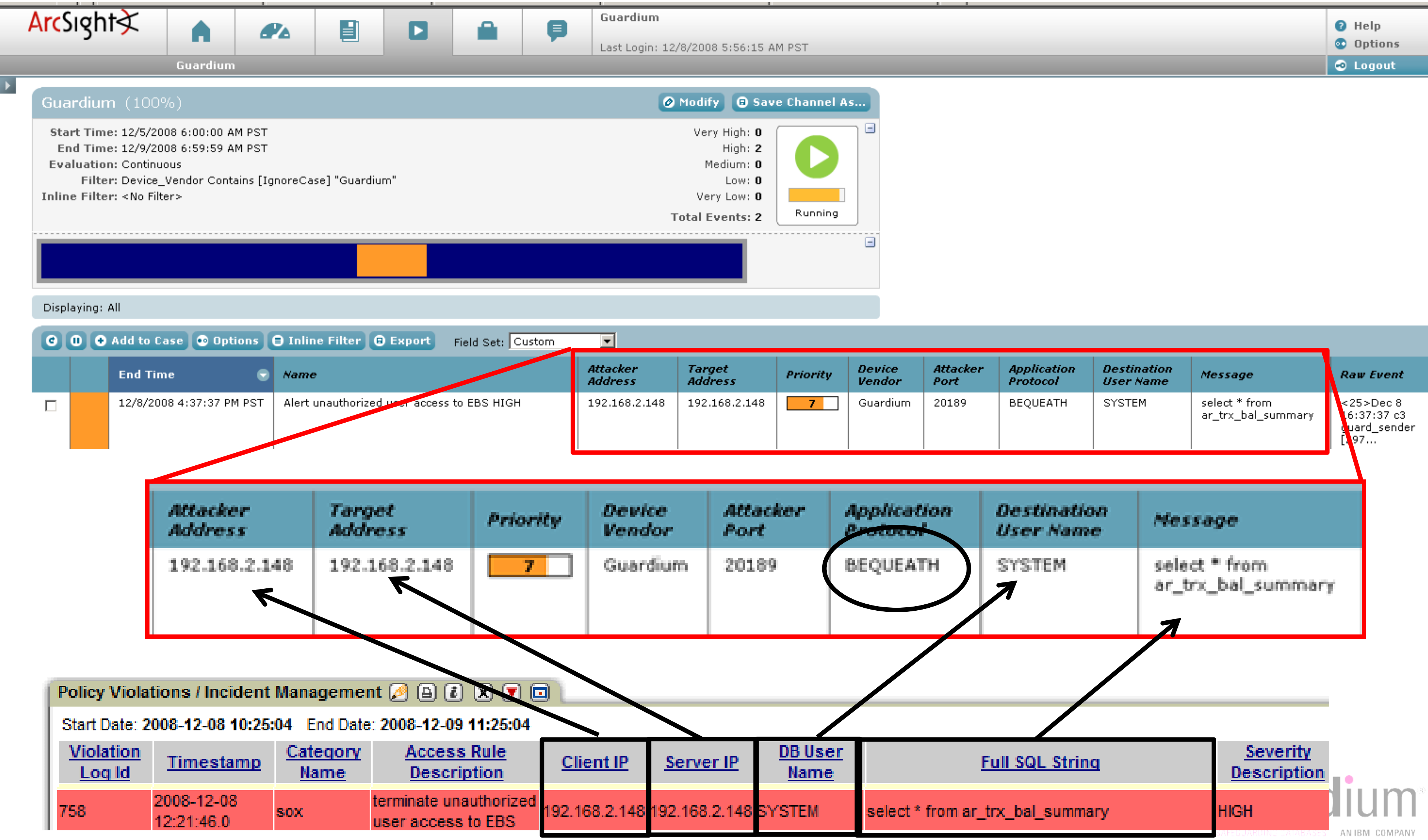


Policy Violations / Incident Management

Start Date: 2008-12-08 10:25:04 End Date: 2008-12-09 11:25:04

Violation Log Id	Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description
758	2008-12-08 12:21:46.0	sox	terminate unauthorized user access to EBS	192.168.2.148	192.168.2.148	SYSTEM	select * from ar_trx_bal_summary	HIGH

Connection Terminated – Sent Event to SIEM



Guardium

Last Login: 12/8/2008 5:56:15 AM PST

Guardium (100%)

Start Time: 12/5/2008 6:00:00 AM PST
End Time: 12/9/2008 6:59:59 AM PST
Evaluation: Continuous
Filter: Device_Vendor Contains [IgnoreCase] "Guardium"
Inline Filter: <No Filter>

Very High: **0**
High: **2**
Medium: **0**
Low: **0**
Very Low: **0**
Total Events: 2

Displaying: All

Field Set: Custom

		End Time	Name	Attacker Address	Target Address	Priority	Device Vendor	Attacker Port	Application Protocol	Destination User Name	Message	Raw Event
□		12/8/2008 4:37:37 PM PST	Alert unauthorized user access to EBS HIGH	192.168.2.148	192.168.2.148	7	Guardium	20189	BEQUEATH	SYSTEM	select * from ar_trx_bal_summary	<25>Dec 8 16:37:37 c3 guard_sender [297...

Attacker Address	Target Address	Priority	Device Vendor	Attacker Port	Application Protocol	Destination User Name	Message
192.168.2.148	192.168.2.148	7	Guardium	20189	BEQUEATH	SYSTEM	select * from ar_trx_bal_summary

Policy Violations / Incident Management

Start Date: **2008-12-08 10:25:04** End Date: **2008-12-09 11:25:04**

Violation Log Id	Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description
758	2008-12-08 12:21:46.0	sox	terminate unauthorized user access to EBS	192.168.2.148	192.168.2.148	SYSTEM	select * from ar_trx_bal_summary	HIGH