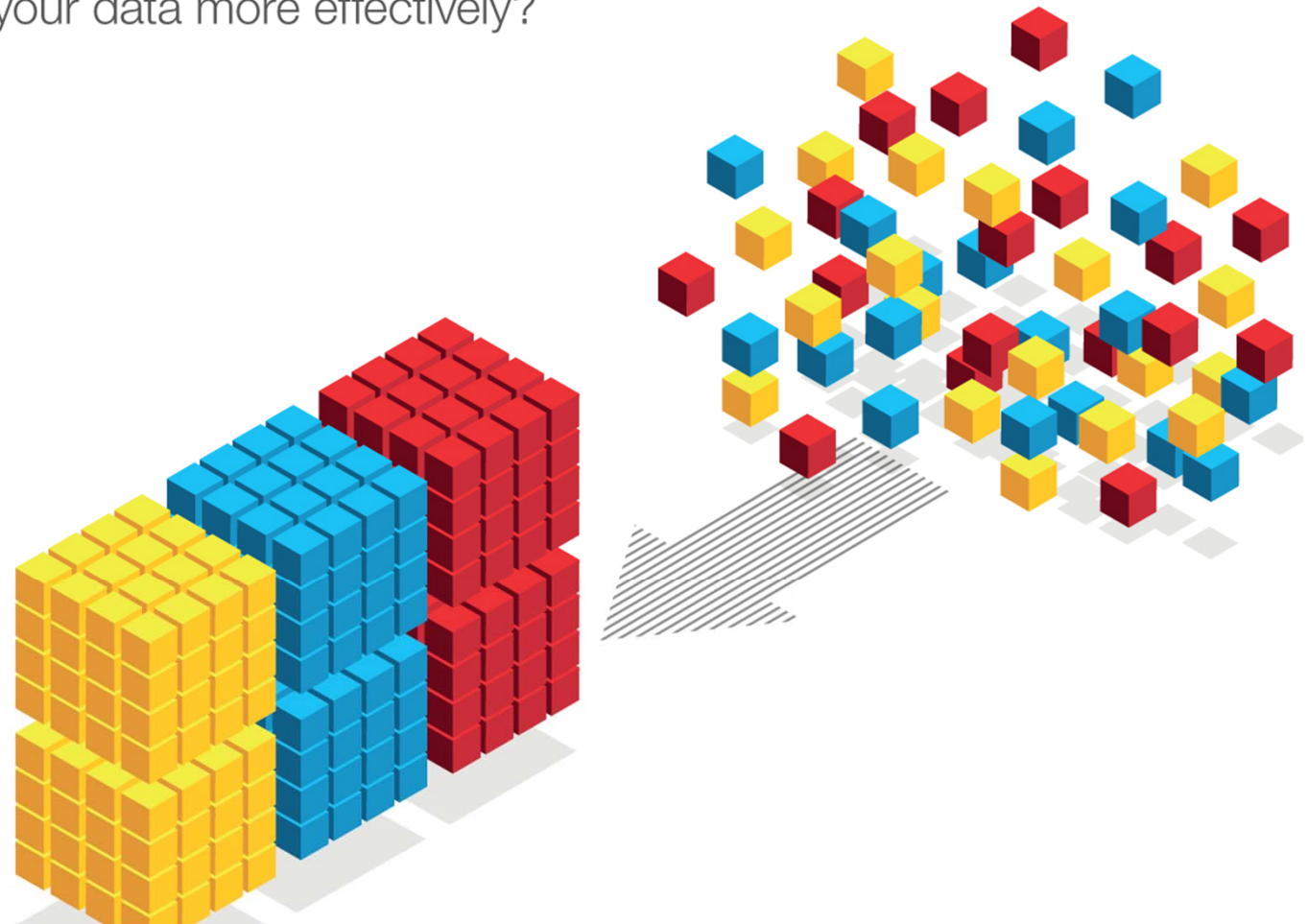


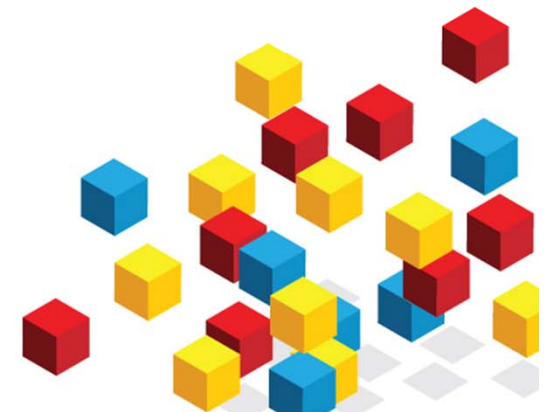
Turn the data you have into the information you need

How will you manage your data more effectively?

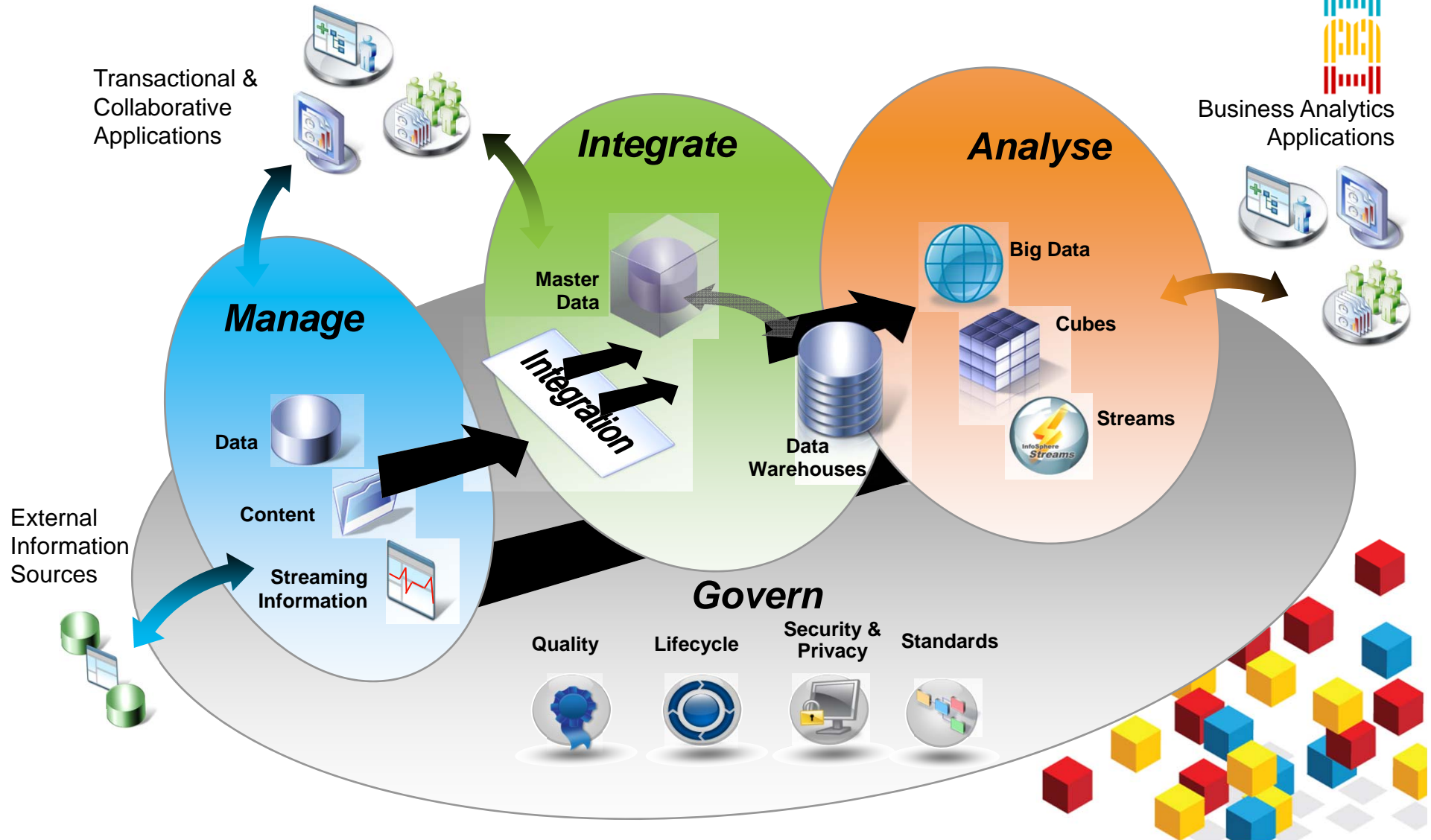


IBM Data Governance

1.30 – 3.00 pm



Delivering trusted information for smarter business decisions across your entire information supply chain



Can today's organisations successfully protect their information?



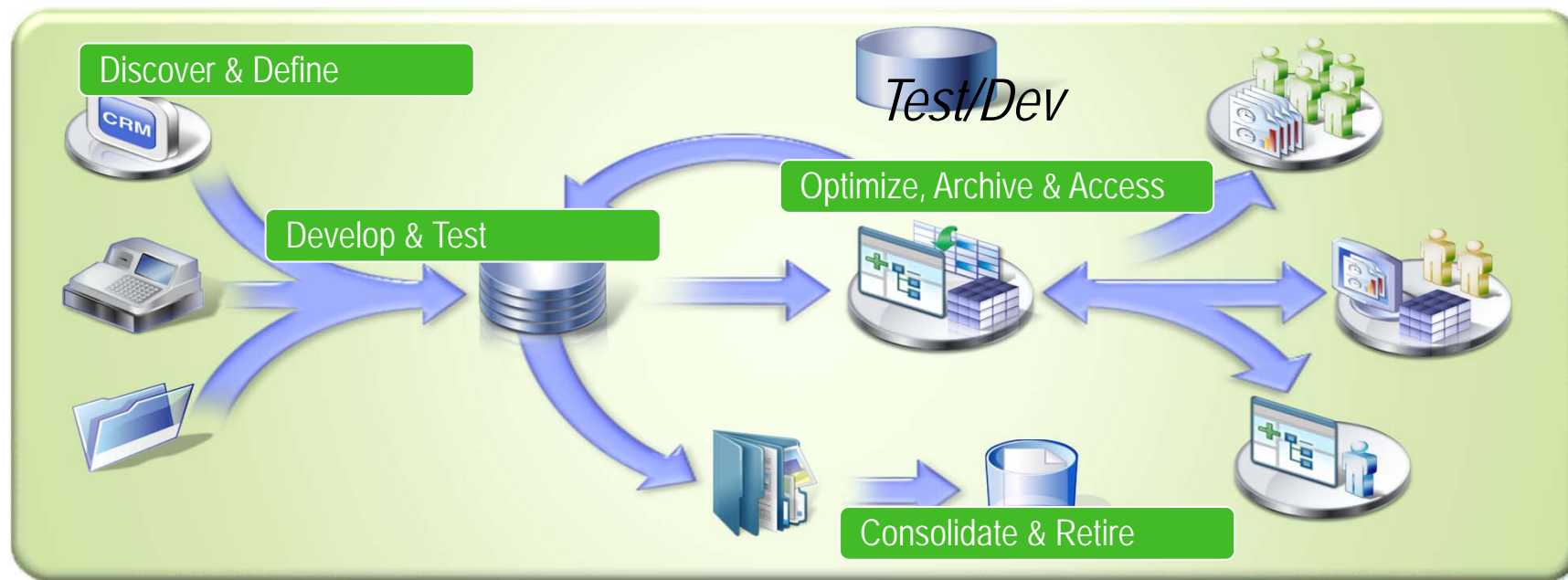
- Where does your sensitive data reside?
- Can you protect from both authorized and unauthorized access?
- Is confidential data in documents safeguarded?
- How can access to your enterprise databases be protected, monitored and audited?
- Can data in your non-production environments be protected, yet still be usable?

Larry Ponemon, founder of the group that bears his name, said that survey shows a shift in the way C-level executives think about security software. Investing in data protection, he said, is now seen as less expensive than recovering from a data breach.

Managing the Lifecycle of Data in the Information Supply Chain



- Understanding the “what and where” of enterprise data
- Developing models and code to store and access enterprise data including configuration of data for test environments
- Optimizing the performance of applications through identification of bottlenecks and building the right strategy for managing data growth
- Implementing a consistent process for retiring or consolidating applications as their usage expires



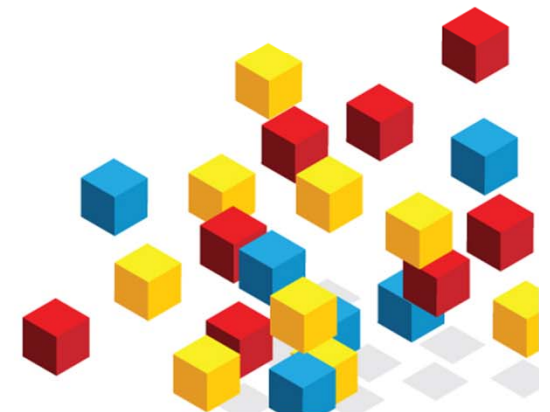
Guardium Data Security Audit, Access Control and Alerting



Steve Gibson

Data Security & Compliance

13th July 2011



An Insider Tale



- Certegy – US Public Company
 - Cheque verification & Credit Card services
- Senior DBA sold 8.5 million customer records to data broker
 - Names, addresses, birth dates, bank account & credit card info – was paid \$580K
- Data theft came to light after retailer reported correlation between transactions and receipt of external marketing offers by its customers
 - U.S. Secret Service found data came from separate company owned by the DBA
 - “Why did it take Certegy **more than five years to find out** that confidential consumer information was being sucked out of its database?” (*St. Petersburg Times*)
- Settled class-action suit for \$4 million
 - Plus \$975,000 in fines from Attorney General
 - Plus mandatory security audit every year
 - Plus 2 years of credit monitoring services (\$180 per customer)
- Rogue DBA sentenced to over five years in prison



Protecting and securing data is no longer optional



42%

of all cases involved third-party mistakes and flubs ... magnitude of breach events ranged from about 5,000 to 101,000 lost or stolen customer records

Fifth Annual U.S. Cost of Data Breach Study", Ponemon Institute, Jan 2010

73%

of security professionals anticipate the volume of database security attacks will continue to increase

Enterprise Strategy Group, Databases at Risk, September 2009

\$90 to \$305

cost per lost record per security breach

Forrester Research, 2007

92%

of compromised records originated in database servers

Data Breach Investigations Report, Verizon Business, 2010

Over 82%

of firms surveyed have had more than one data breach in the past year involving loss or theft of 1,000+ records with personal information

2009 Annual Study: Cost of a Data Breach, Ponemon Institute LLC., January 2010



The Real Cost of Doing Nothing

Bloomberg Anywhere | Professional | Solutions | About



Related News: [U.S.](#) · [Technology](#)

EMC's RSA Security Breach May Cost Bank Customers \$100 Million

By Rachael King - Jun 9, 2011 3:35 AM ET

 Recommend

 Tweet 14

 Share 19

 +1 1

 More

 Print

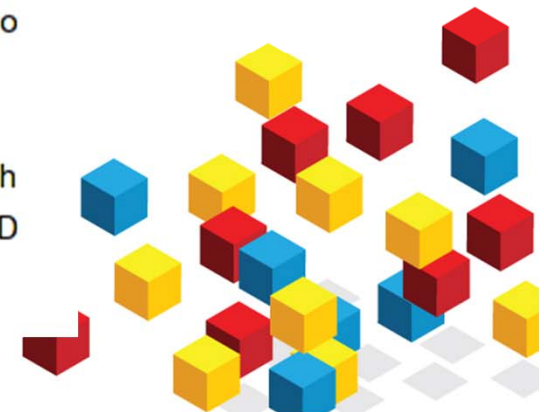
 Email

The security breach at EMC Corp.'s RSA unit may cost the banking industry as much as \$100 million to replace identification tokens that left their computers vulnerable to spying.

Banks may be forced to pay \$50 million to \$100 million to distribute new RSA SecurID devices that employees use to securely log onto corporate networks, according to a Gartner Inc. research analyst.

RSA clients include [Wells Fargo & Co. \(WFC\)](#) and [Northwest](#)

[Bancshares Inc. \(NWBI\)](#) as well as defense contractor [Lockheed Martin Corp. \(LMT\)](#), which said a May 21 cyberattack on its computers is linked to the March breach of RSA's SecurID database.



Won't Happen To Me? Think Again...



Data Breach Threat to Businesses Rises to Statistical Certainty: Survey

By: Fahmida Y. Rashid

2011-06-23

Article Rating: ☆☆☆☆☆ / 0



12 [Share](#) 4 [Share](#) 33 [tweets](#) [retweet](#)

The latest Ponemon Institute study called the chances of an organization being hacked in a 12-month period a "statistical certainty."

Cyber-attacks are becoming more frequent and severe with the vast majority of businesses suffering as least one data breach in the past year, according to a new Ponemon Institute survey.

Businesses of all sizes are being hit by cyber-attacks, as 90 percent of surveyed businesses reported at least one IT security breach in the past 12 months, the Ponemon Institute found in its latest report, published June 22. More than half of those respondents, or 90 percent, claimed two or more breaches over the same period. Nine percent reported five or more network intrusions in the past year.

More than half of the respondents had little confidence of being able to prevent another cyber-attack over the next 12 months, according to the survey. About 43 percent of the respondents in the study said there was a significant rise in the frequency of cyber-attacks during the past year and 77 percent said the attacks had become more severe or difficult, to contain, the study found.

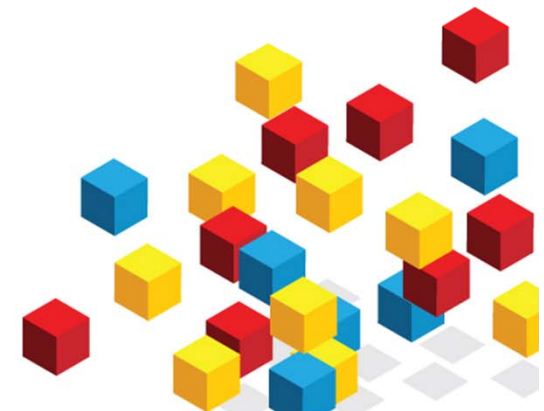
Rate This Article:

Poor Best

[Rate](#)

[E-mail](#) [PDF Version](#)

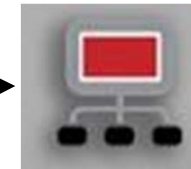
[Print](#)



What Solutions are in use today?



**Manual
remediation,
dispatch
and tracking**



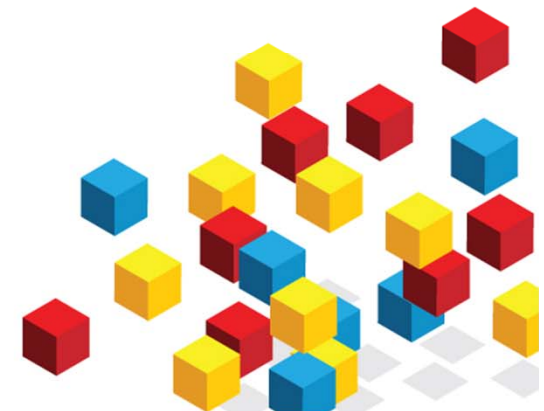
**Manual
review**



**Create
reports**



- Native database logging
- Homegrown scripts
- Scrape and parse the data
- Fill repositories with log data
- Stove-piped approach



What are the Challenges with this Approach?



Expense

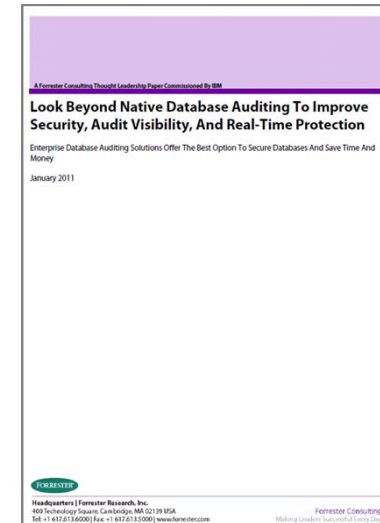
- Performance impact of native logging on the DBMS
- Another data store to secure and manage (\$\$\$)
- Lack of DBMS expertise on security teams
- Significant complexity & labor cost to analyze audit data, maintain homegrown scripts as compliance audit requirements change

Weak Security Controls

- No separation of duties -- DBAs & hackers can easily modify logs
- Not real-time
- No preventive controls

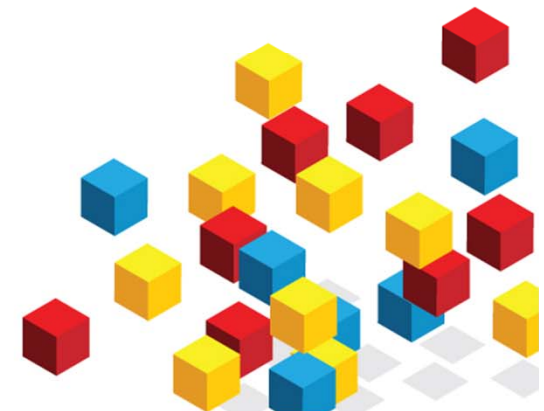
Compliance Audit Failures

- Limited scope & granularity of log data
- Inconsistent policies across applications, DBMS platforms, compliance initiatives
- Can't identify end-user fraud for connection-pooled applications that use generic service accounts (SAP, etc.)



Forrester Consulting –
Commissioned Report

“If we didn’t have [our enterprise database auditing and monitoring solution], we would need an army of additional IT people.” (CISO)



The Objectives of Database Activity Monitoring



1. Prevent data breaches & fraud

- Mitigate external & internal threats
- Secure customer & credit card data, sales pipeline, strategic plans & IP



2. Assure data governance

- Prevent unauthorized changes to financial & ERP data



3. Reduce cost of compliance

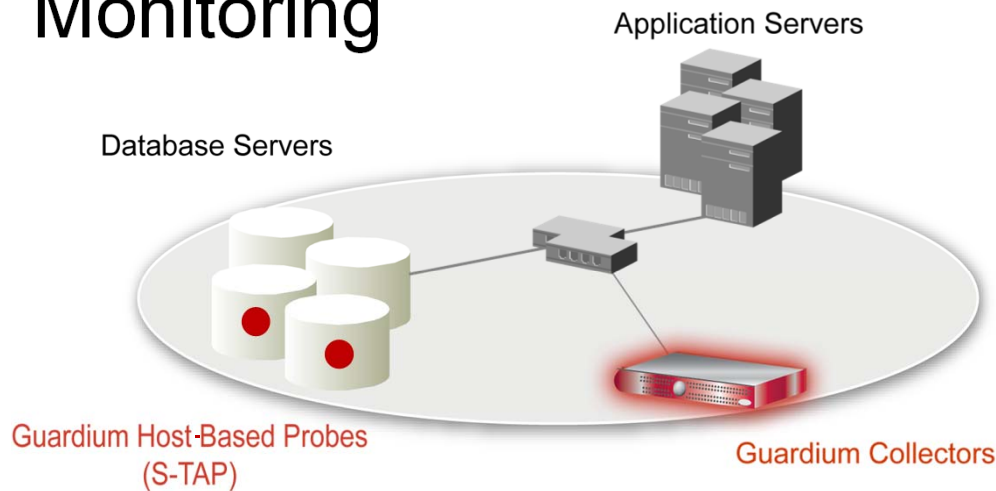
- Automate & centralize controls
- Simplify processes



...Without performance impact or changes to databases & applications!



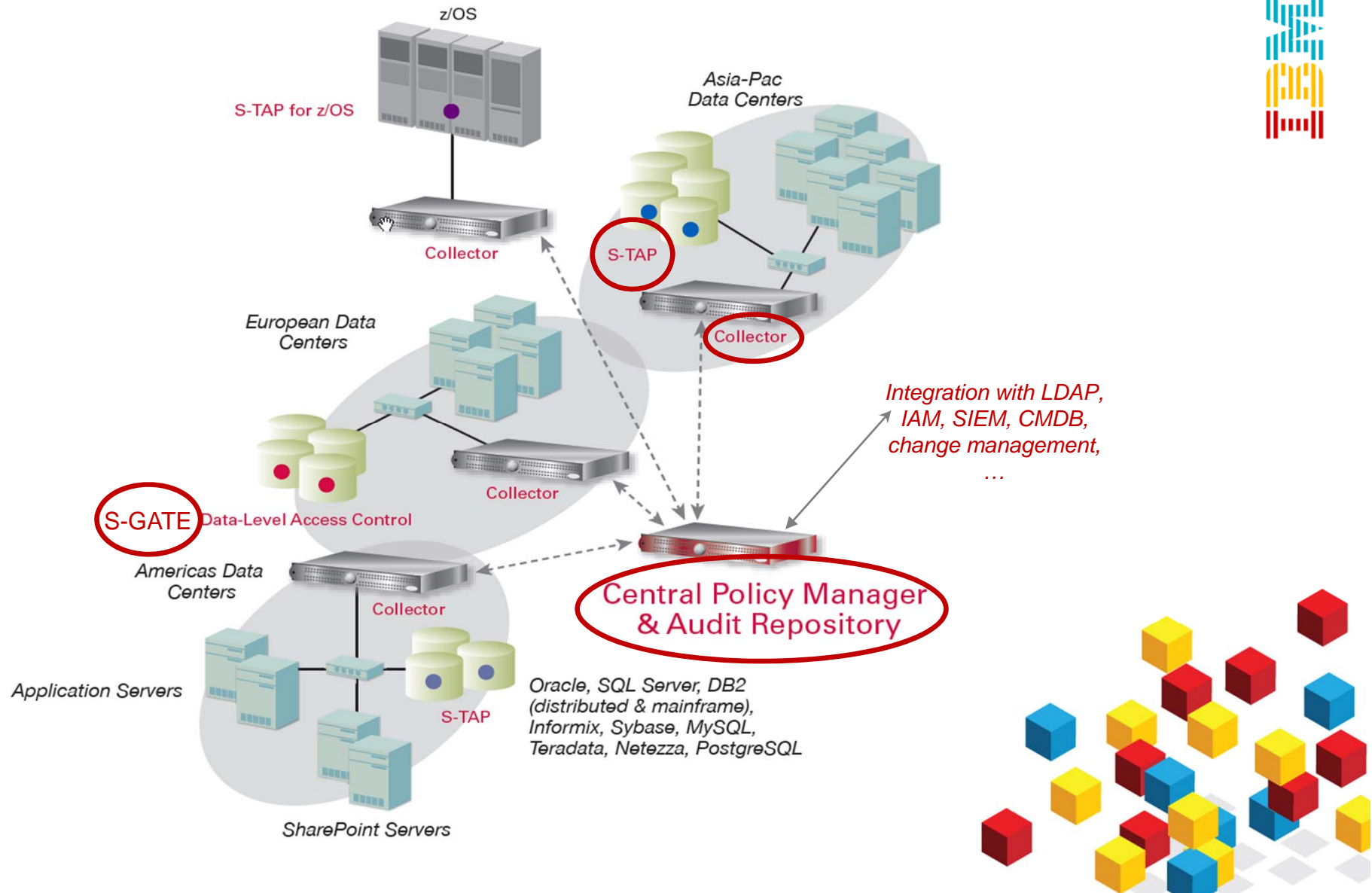
Non-Invasive, Real-Time Database Security & Monitoring



- 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
- 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



Scalable Multi-Tier Architecture



Addressing the Full Lifecycle of Database Security

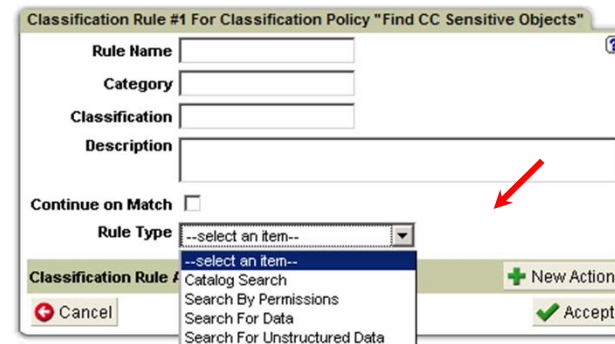


Real-time Database Security & Monitoring



Discovering Sensitive Data in Databases

- *Discover database instances on network*
- *Catalog Search*: Search the database catalog for table or column name
 - Example: Search for tables where column name is like “%card%”
- *Search by Permission*: Search for the types of access that have been granted to users or roles
- *Search for Data*: Match specific values or patterns in the data
 - Example: Search for objects matching *guardium://CREDIT_CARD* (a built-in pattern defining various credit card patterns)
- *Search for Unstructured Data*: Match specific values or patterns in an unstructured data file (CSV, Text, HTTP, HTTPS, Samba)



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

Rule Name:

Category:

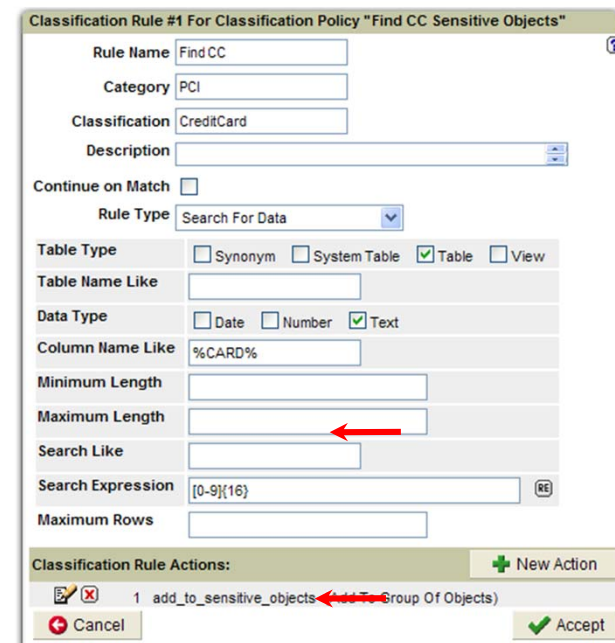
Classification:

Description:

Continue on Match:

Rule Type: --select an item--

Classification Rule Actions:



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

Rule Name: Find 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:

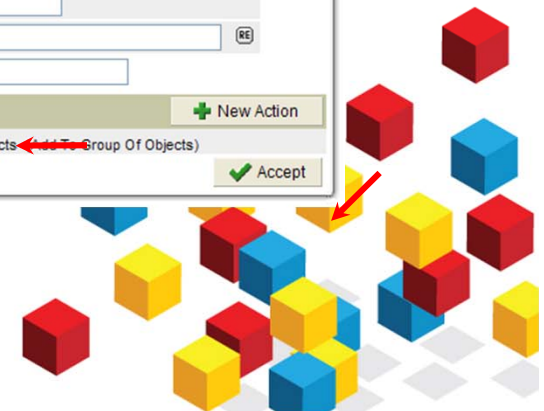
Search Like:

Search Expression: [0-9]{16}

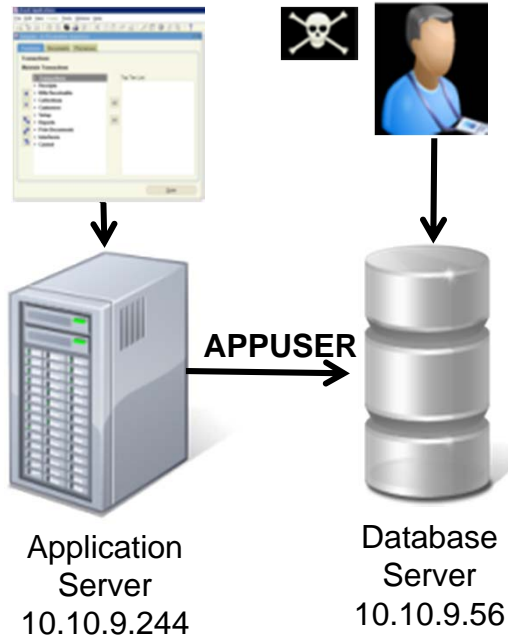
Maximum Rows:

Classification Rule Actions:

1 add_to_sensitive_objects (Group Of Objects)



Granular Policies with Detective & Preventive Controls



Rule #1 Description non-App Source AppUser Connection

Category Security **Classification** Breach **Severity** MED

Hot **Server IP** / and/or **Group** Production Servers

Hot **Client IP** / and/or **Group** Authorized Client IPs

Hot **Client MAC** and/or **Group** -----

Hot **DB Name**

Hot **DB User** APPUSER

Field Name **Object** EmployeeTable **Command** Select

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

Sample Alert

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

Reporting & Forensic Drill-Down Info



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

IBM® InfoSphere™ Guardium®

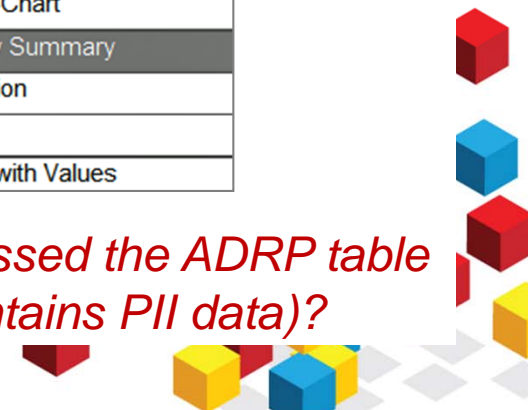
Drill down: show all tables that were accessed by this user

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

Records: 1 to 20 of 394

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

Who accessed the ADRP table (which contains PII data)?



Advanced Compliance Workflow Automation



Event Type

Existing Task Event Types

Event Type	First Status	Allowed Status
NA Store Daily PCI DSS Incident Workflo	Open	Approved, Not Approved, Open, Review state

Edit Event Type Definition NA Store Daily PCI DSS Incident Workflo

Description: NA Store Daily PCI DSS Incident Workflo

First Status: Open

Allowed Status

Available Status: Closed (Final)

Allowed Status: Approved (Final), Not Approved (Final), Open, Review state

Defined Event Actions

Event Action Description	Prior Status	Next Status	Sign-off
Under review	Open	Review state	<input type="checkbox"/>
Approved state	Review state	Approved	<input checked="" type="checkbox"/>
Not approved	Review state	Not Approved	<input checked="" type="checkbox"/>

Roles

Roles have been assigned to this event type with status: Approved

Roles have been assigned to this event type with status: Open

Roles have been assigned to this event type with status: Not Approved

No roles have been assigned to this event type with status: Review state

Buttons: Cancel, Apply, New Event Type, Event Status

- Easily create custom processes by specifying unique combination of workflow steps, actions and users
 - Use case: Different oversight processes for financial servers than PCI servers. Different workflows in NA vs. EU.
 - Enables cost benefits of automation to be realized in large, complex organizations
- Supports automated execution of oversight processes on a report line item basis, maximizing efficiency without sacrificing security
 - Use case: Daily exception report contains 4 items I know about and have resolved, but one that needs detailed investigation. Send 4 on for sign-off; hold one
 - Increases efficiency of overall oversight process, and each individual

Compliance Automation

Audit Process Definition

Description: Daily PCI DSS Incident Review

Active: There is no schedule associated with this process

Archive Results:

Keep for a minimum of: 365 days or 0 runs

CSV/CEF File Label: Daily_PCI_DSS_Incident_ Zip CSV for mail

Email Subject: Daily PCI DSS Incidents for Remediation and Sign-off

Buttons: View, Run Once Now, Modify Schedule...

Receiver Table

Receiver	Action Req.	To-Do List	Email Notif.	Cont. Appv. if Empty
Payment Card DB Admin (Ernst Potlherfeldt)	<input type="radio"/> Review <input checked="" type="radio"/> Sign	<input checked="" type="checkbox"/>	<input type="radio"/> No <input checked="" type="radio"/> Link <input type="radio"/> Full Results	<input checked="" type="checkbox"/>
Retail InfoSec (Max Dufresne)	<input type="radio"/> Review <input checked="" type="radio"/> Sign	<input checked="" type="checkbox"/>	<input type="radio"/> No <input checked="" type="radio"/> Link <input type="radio"/> Full Results	<input type="checkbox"/>

Add Receiver

Receiver name: [Search users]

Action Required: Review Sign

To-Do List: Add

Email Notification: None Link Only Full Results

Continuous:

Approve if Empty: Yes

Add

Audit Tasks

Report: Daily PCI DSS Incident Report [Policy Violations Details] (NOW -1 DAY to NOW)

Add Audit Task



Identifying Unpatched & Misconfigured Systems



Results for Security Assessment: **Guardium Oracle** -- Select another result --

Assessment executed **2009-09-29 21:38:18.0**

From: 2009-09-01 00:00:00.0 Client IP or IP subnet: Any
 To: 2009-09-25 00:00:00.0 Server IP or IP subnet: Any Download PDF

Tests passing: **45%**

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](#)
[lump to Datasource list](#)

Result Summary Showing 104 of 104 results (0 filtered)

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

Assessment Result History

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 104 of 104 results (0 filtered)

Cat.	Test Name	Datasource	P/F	Sev.	Reason
Auth:	Default Accounts Password Changed	ORACLE: Oracle Local	Fail	Critical	5 active pre-defined users have default passwords. <i>Recommendation: Some predefined Oracle user accounts are still enabled and still have the Oracle default password. These predefined Oracle users and passwords are well-known to anyone familiar with Oracle, and represent one of the easiest entry points for attacks and data theft/damage. We recommend that you remove any predefined Oracle user accounts that are not absolutely required, and we strongly recommend that you change the passwords for any of these users who are required.</i>
Priv:	No Access To 'Users' Catalog Tables	ORACLE: Oracle Local	Fail	Critical	Some users or roles without 'SELECT_CATALOG_ROLE' authority have access to 'DBA_USERS' or 'ALL_USERS': CTXSYS, PUBLIC. <i>Recommendation: Access to the DBA_USERS or ALL_USERS tables has been granted to users other than</i>

Summary
Outlining
Results

Result History

Filters and Sort
Controls

Detailed Test
Results

Detailed
Descriptions of
Fixes



Audit Policies

A Detailed Look



IBM InfoSphere™ Guardium 15:46 | Edit Account: poc | Customize | Logout | About | IBM.

You have 8 items on your To-do list You have been assigned 1 Incident G2000 - Standalone Unit

Standard Reports Quick Start My New Reports Monitor/Audit Discover Assess/Harden Protect Comply Sarbanes-Oxley Accelerator PCI Accelerator Data Privacy Accelerator

Overview Plan & Organize PCI Req. 10 Track & Monitor PCI Req. 11 Ongoing Validation PCI Policy Monitoring

Overview

- 10.2 and 10.3 Automation
- 10.2.1 Data Access
- 10.2.2 Admin Activity
- 10.2.3 Audit Trail Access
- 10.2.4 Invalid Access
- 10.2.6 Initialization Log
- 10.5 Secure audit trails
- 10.6 Access Auditing

PCI - Activity by Root / Admin

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

Aliases: ON

DB User Name	Client IP	Server IP	Database Name	Server Type	SQL Verb	Count of Object Name	Total access
BILL	10.10.9.57	10.10.9.57	Customer	ORACLE	CALL	2	3
BILL	10.10.9.57	10.10.9.57	Customer	ORACLE	SELECT	6	9
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	Customer	DB2	CALL	1	11
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	Customer	DB2	SELECT	2	14
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	CustomerDB	DB2	ALTER TABLE	1	1
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	CustomerDB	DB2	CALL	2	16
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	CustomerDB	DB2	CREATE FUNCTION1	1	1
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	CustomerDB	DB2	CREATE TABLE	5	7
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	CustomerDB	DB2	DROP TABLE	2	2
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	CustomerDB	DB2	INSERT	5	96

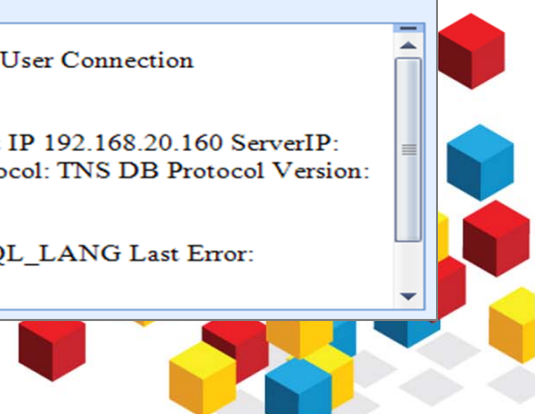
From: GuardiumAlert@guardium.com Sent: Wed 4/15/2009 8:00 AM

To: Marc Gamache

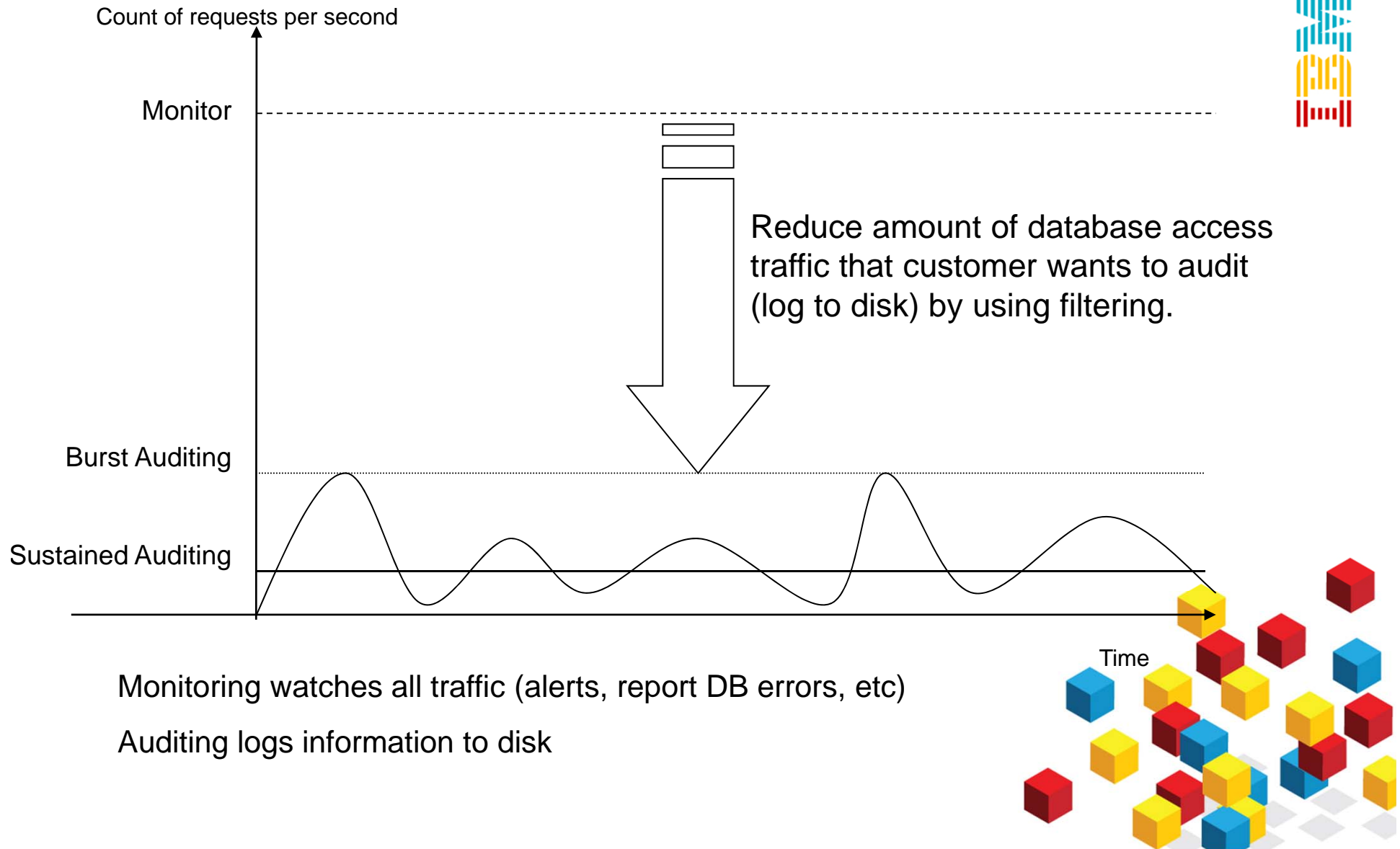
Cc:

Subject: (c1) SQLGUARD ALERT

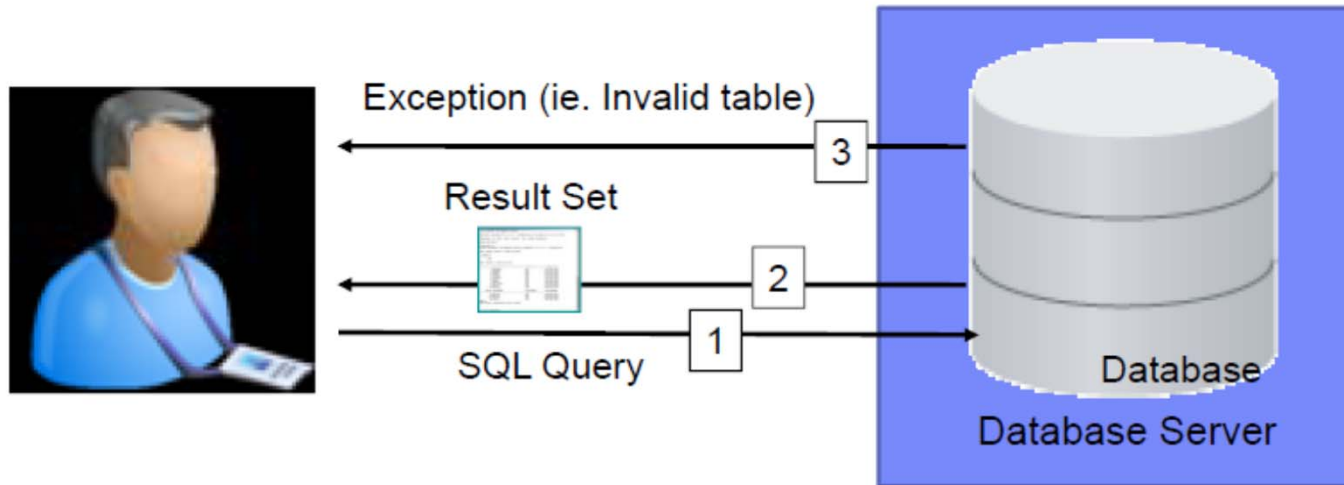
Subject: (c1) SQLGUARD ALERT Alert based on rule ID non-App Source AppUser Connection
 Category: security Classification: Breach Severity MED
 Rule # 20267 [non-App Source AppUser Connection]
 Request Info: [Session start: 2009-04-15 06:59:03 Server Type: ORACLE Client IP 192.168.20.160 ServerIP: 172.16.2.152 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



Monitoring or Auditing?



Policy - Identify and Audit Significant Activity



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

Add Access Rule...

Add Extrusion Rule...

Add Exception Rule...



Access Rule



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 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

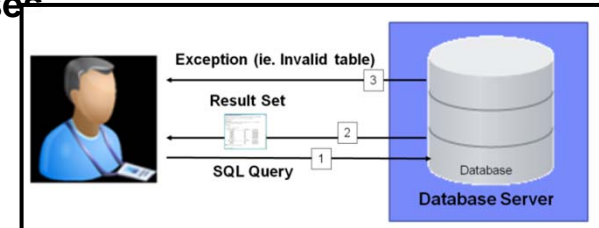
Continue to next Rule Rec. Vals.

Action: S-GATE TERMINATE

Which Servers

Which Databases

Which Users



Which Fields

Which Tables

Which SQL Commands

- 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

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



Access Rule Actions



Log Full Details with Values

Log Full Details

Allow

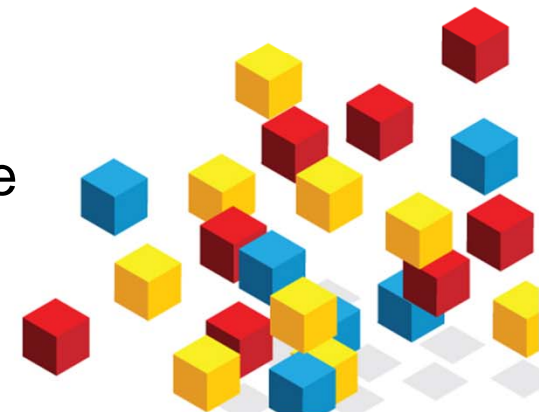
Start Date: 2009-08-11 09:39:36 End Date: 2009-08-11 10:39:36

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

Records: 1 to 3 of 3

Each level of detail will store more information

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



Extrusion Rule - Monitor the Results Set For Sensitive Data



The screenshot shows Microsoft SQL Server Management Studio with a query window containing the following SQL query:

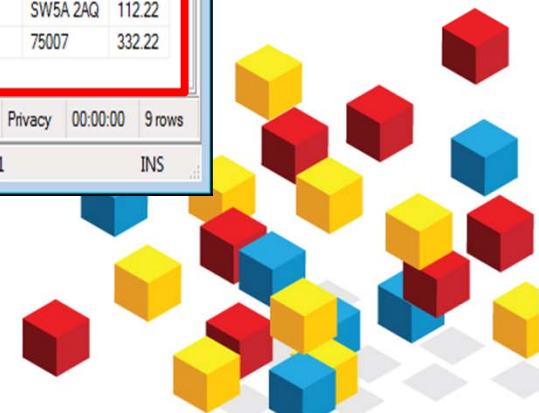
```
Select * from customer where customerID < 9
```

The Results pane displays the following data:

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

An inset diagram shows a person on the left, a 'Database Server' on the right, and a 'Result Set' in the middle. Arrows indicate the flow: 'SQL Query' (1) from the person to the database, 'Result Set' (2) from the database to the person, and 'Exception (ie. Invalid table)' (3) from the database to the person.

Below the results table, a text box states: "This is the results set to the query 'select * from customer where customerID < 9'"



Extrusion Definition to Alert on Suspect Results



Extrusion Rule Definition

Rule #5 Description ?

Category Classification Severity

Not Server IP / and/or Group

Not Client IP / and/or Group

Not Client MAC Net. Protocol and/or Group

Not DB Type and/or Group

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 Data Pattern RE

Not Sql Pattern RE

Min. Ct. Reset Interval (minutes)

Revoke Rec. Vals.

Not Action

Notification

Notification Type SYSLOG Alert Receiver SYSLOG

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



Exception Rule - Alert On Failed Login



Rule #5 Description Login Failures to Production Database Server

Category Security **Classification** Breach **Severity** HIGH

Hot **Server IP** / and/or Group Production Servers

Hot **Client IP** / and/or Group

Hot **Client MAC** **Net. Protocol** and/or Group

DB Type **Hot** **Service Name** and/or Group

Hot **DB Name** and/or Group

Hot **DB User** APPUSER and/or Group

Hot **Error Code** and/or Group

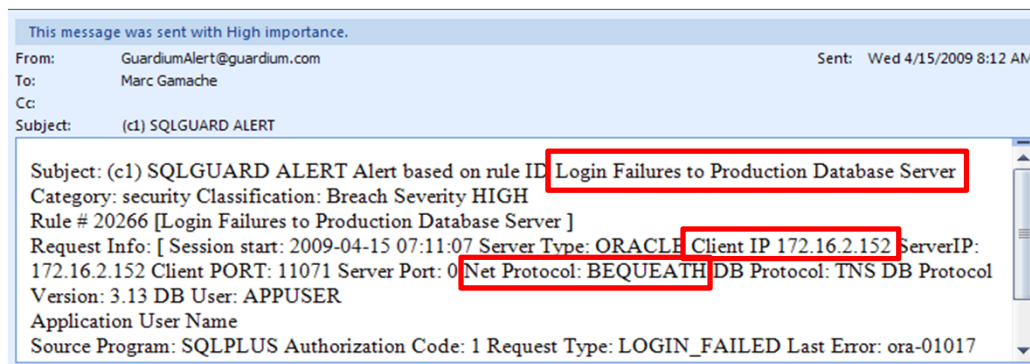
Hot **Exception Type** LOGIN_FAILED

Minimum Count 3 **Reset Interval** 5 minutes

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

Action ALERT PER MATCH MAIL
SNMP
CUSTM
SYSLOG

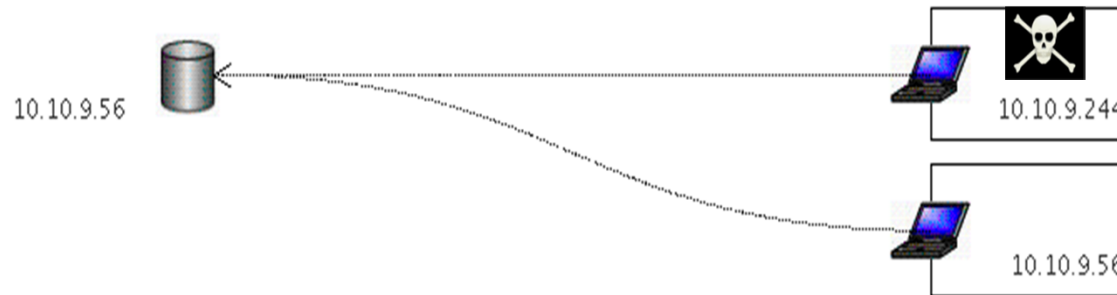
- APPUSER is generic DB service account (connection pooling)
- Exception Type = Failed Login
- Min Count = How often
- Reset Interval = Time period for count
- Action = Alert
- So ... Alert on 3 Failed Login attempts from the same user if they occur 3 times within a 5 minute interval



Actual SMTP Alert

You should not see three failed logins from a production application

Exception Rule - Preventing Attacks



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

Returned SQL Errors

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

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

SQL injection leads to **SQL errors!**

Failed Login Attempts

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

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

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

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

Exception Rules 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 / 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.

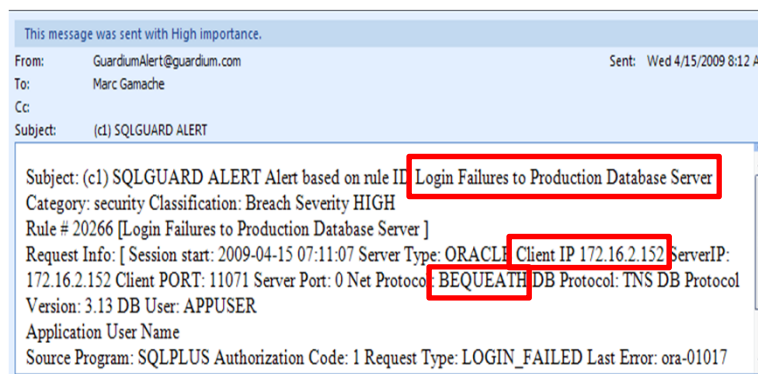
Action ALERT PER MATCH

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

Demonstration

Activity Monitoring, Auditing & Alerting



IBM InfoSphere™ Guardium® 15:46 | Edit Account: poc | Customize | Logout | About | IBM.

You have 8 items on your To-do list You have been assigned 1 Incident G2000 - Standalone Unit

Standard Reports Quick Start My New Reports Monitor/Audit Discover Assess/Harden Protect Comply Sarbanes-Oxley Accelerator PCI Accelerator Data Privacy Accelerator

Overview Plan & Organize PCI Req. 10 Track & Monitor PCI Req. 11 Ongoing Validation PCI Policy Monitoring

Overview
10.2 and 10.3 Automation
10.2.1 Data Access
10.2.2 Admin Activity
10.2.3 Audit Trail Access
10.2.4 Invalid Access
10.2.6 Initialization Log
10.5 Secure audit trails
10.6 Access Auditing

PCI - Activity by Root / Admin
Start Date: 2010-08-25 01:35:38 End Date: 2010-08-30 01:35:38
Aliases: ON

DB User Name	Client IP	Server IP	Database Name	Server Type	SQL Verb	Count of Object Name	Total access
BILL	10.10.9.57	10.10.9.57	Customer	ORACLE	CALL	2	3
BILL	10.10.9.57	10.10.9.57	Customer	ORACLE	SELECT	6	9
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	Customer	DB2	CALL	1	11
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	Customer	DB2	SELECT	2	14
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	CustomerDB	DB2	ALTER TABLE	1	1
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	CustomerDB	DB2	CALL	2	16
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	CustomerDB	DB2	CREATE FUNCTION	1	1

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

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



Thank you



IBM InfoSphere™ Guardium 15:46 | Edit Account: poc | Customize | Logout | About | IBM.

You have 8 items on your To-do list You have been assigned 1 Incident G2000 - Standalone Unit

Standard Reports Quick Start My New Reports Monitor/Audit Discover Assess/Harden Protect Comply Sarbanes-Oxley Accelerator PCI Accelerator Data Privacy Accelerator

Overview Plan & Organize PCI Req, 10 Track & Monitor PCI Req, 11 Ongoing Validation PCI Policy Monitoring

Overview
10.2 and 10.3 Automation
10.2.1 Data Access
10.2.2 Admin Activity
10.2.3 Audit Trail Access
10.2.4 Invalid Access
10.2.6 Initialization Log
10.5 Secure audit trails
10.6 Access Auditing

PCI - Activity by Root / Admin
Start Date: 2010-08-25 01:35:38 End Date: 2010-08-30 01:35:38
Aliases: ON

DB User Name	Client IP	Server IP	Database Name	Server Type	SQL Verb	Count of Object Name	Total access
BILL	10.10.9.57	10.10.9.57	Customer	ORACLE	CALL	2	3
BILL	10.10.9.57	10.10.9.57	Customer	ORACLE	SELECT	6	9
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	Customer	DB2	CALL	1	11
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	Customer	DB2	SELECT	2	14
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	CustomerDB	DB2	ALTER TABLE	1	1
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	CustomerDB	DB2	CALL	2	16
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	CustomerDB	DB2	CREATE FUNCTION1	1	1
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	CustomerDB	DB2	CREATE TABLE	5	7
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	CustomerDB	DB2	DROP TABLE	2	2
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	CustomerDB	DB2	INSERT	5	96
DB2INST2	10.10.9.56	Oracle @ 10.10.9.56	CustomerDB	DB2	SELECT	8	48
JOE	10.10.9.57	10.10.9.57	Customer	ORACLE	CALL	2	18

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

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

