Auditing MySQL for Security and Compliance

Mehlam Shakir

CTO

RippleTech, Inc.

RippleTech

RippleTech

Agenda

- Company Background
- Database Security: Business Drivers
- Product Demonstration

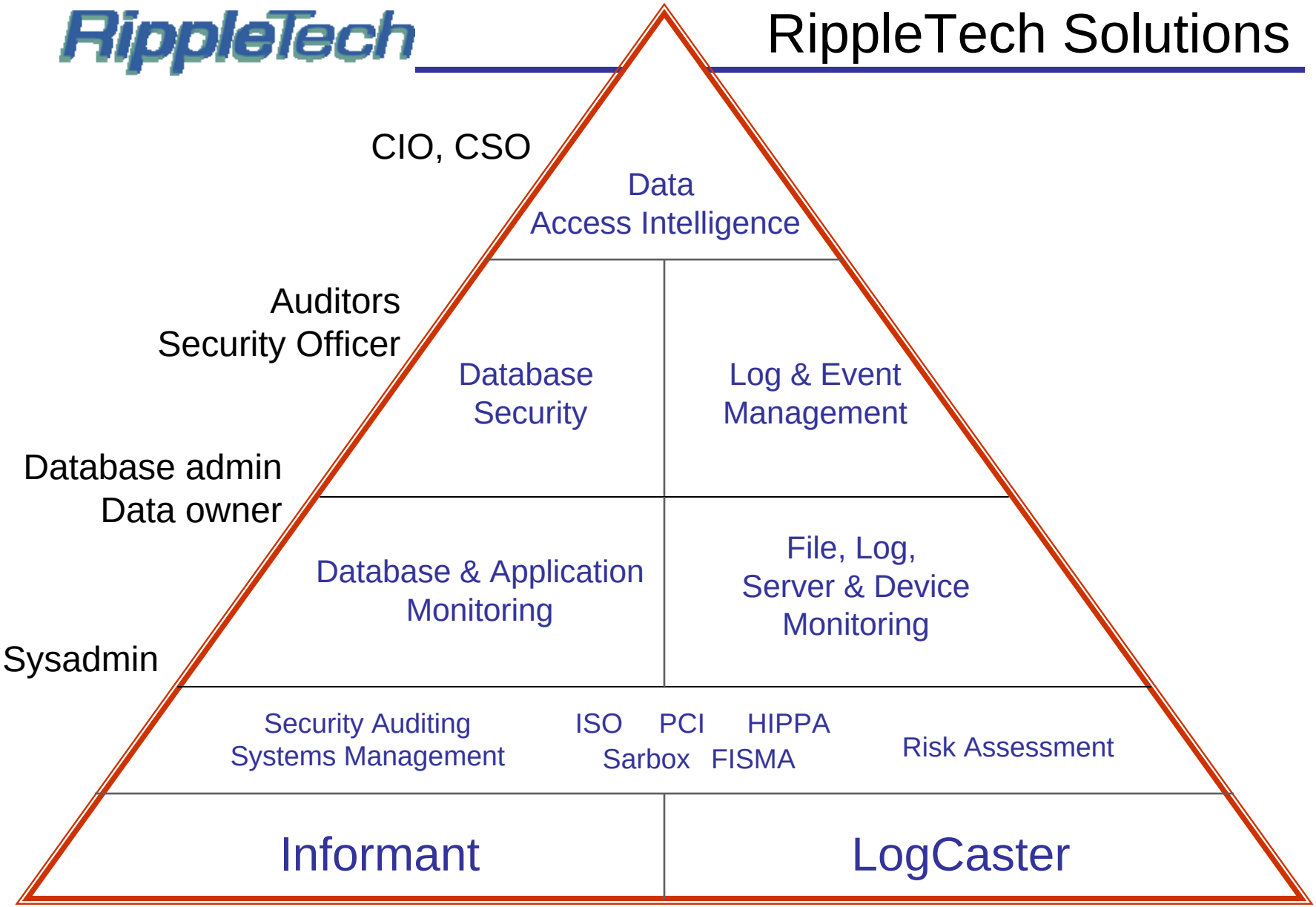
Company Background

RippleTech

RippleTech: Who Are We

- Founded in 1998
- Solutions for Ensuring IT Compliance and Data Security
- Over **650** active customers:
  - Financial Services, Government, Healthcare, Insurance & Manufacturing (30% international)
- Based 10 miles west of Philadelphia, PA
- Venture backed

RippleTech Solutions



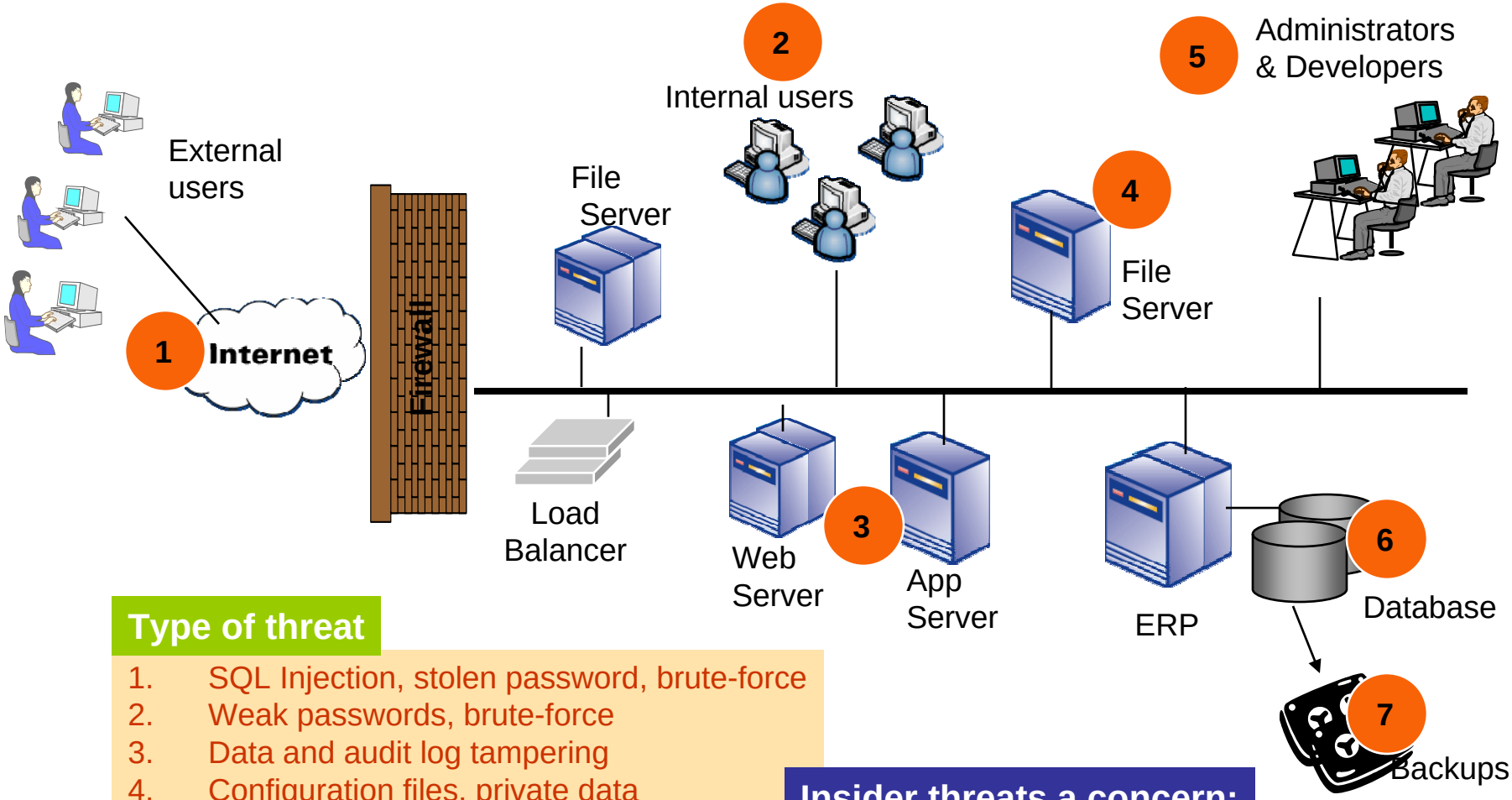
Database Security:
Business Drivers

RippleTech

RippleTech

FORRESTER®

Database Security Threats



Type of threat

1. SQL Injection, stolen password, brute-force
2. Weak passwords, brute-force
3. Data and audit log tampering
4. Configuration files, private data
5. Vulnerabilities, password exposed
6. Weak database security
7. Tapes stolen/lost

Insider threats a concern:

80% of threats come from insiders
65% of internal threats are undetected
25% of enterprises detected security breaches
60% of data loss/corruption caused by human error

RippleTech

Database Attacks

+ Hacking
  - SQL Injection, Password & Brute Force, Database Vulnerability Exploit, Denial of Service, Malware
+ Malicious Intent
  - Confidential Information/Identity Theft, Data Destruction/Sabotage, Unauthorized Access, Data compromise/Fraud

80%

+ Inappropriate Access
  - Policy violation, Illegal Database Backup, Privilege Abuse, Inappropriate Data Access e.g. Unauthorized Application
+ User Error
  - Accidental deletion

RippleTech Visibility into Database Access

+ HR Server
  + Account Added
  + Failed Logon
  + Failed Database Backup
    + arcserver
      + backup table employee to
        "c:\take_it_home.bak"
  + Prohibited Command Issued
    + john
    + mel
      + select * from credit_data

Report

Significant Event

Repeat Failures

Policy Violation

Malicious Intent

Real-time alert

RippleTech Visibility into Database Access

- Alert and report if any “user account” was added, deleted and or modified
- Alert and report if production database was modified during business hours

RippleTech

Hacking

- Alert on repeat logon failures by a user
- Alert on repeat access denied errors

RippleTech

Inappropriate Access

+ Alert and report on data access policy violation

  “root user accessed server from Untrusted network”

RippleTech

SOX, PCI, HIPAA

Business Drivers: Use Cases

+ Customer Case Study
  - Layer I – Monitor Network Perimeter & Hosts
  - Layer II – Monitor Databases and Applications
    - Visibility into application access
    - Privilege abuse by staff
    - Attempts to gain unauthorized access
    - SQL Injection attempts
    - Track administrator's changes
    - Forensic analysis – what was compromised?

RippleTech

Security, Compliance, & Systems Management

More Use Cases

- Forensics - Which records were compromised, if any?
- Monitor Database Backdoors
- Audit Trail of Employee Prior To Termination
- Reconcile Database Change Control Activity
- Log Service Provider Activity
- Data Utilization Trends (Most & Least Used, By Who?)
- Recurring Problem Identification - Slow SQL, Errors

Product Demonstration:

Monitoring Databases with ZERO Impact using RippleTech Informant

RippleTech

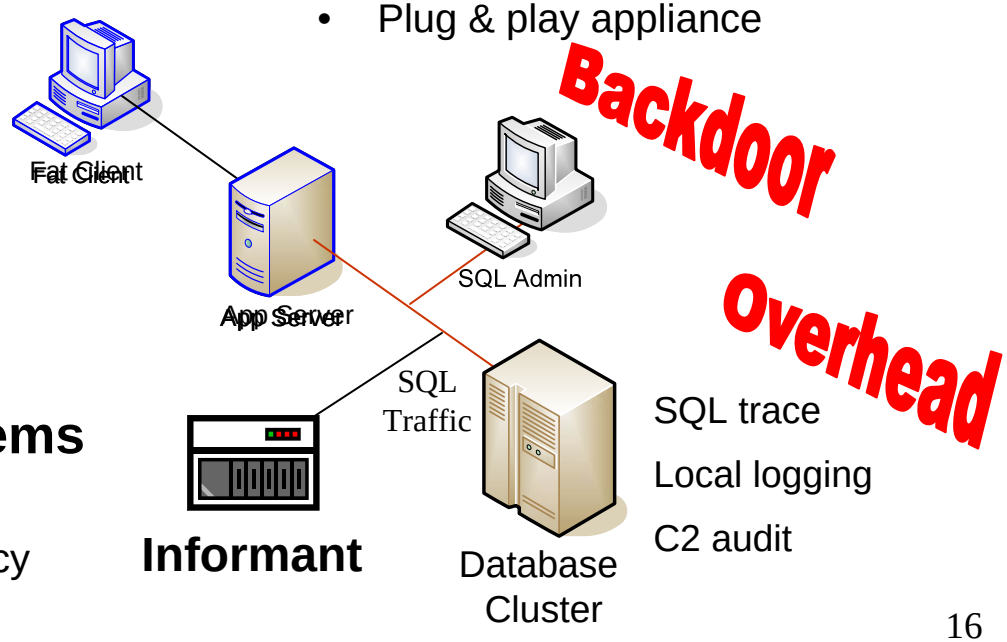
DB Monitoring Approaches

Traditional Approach
(Limited Value)

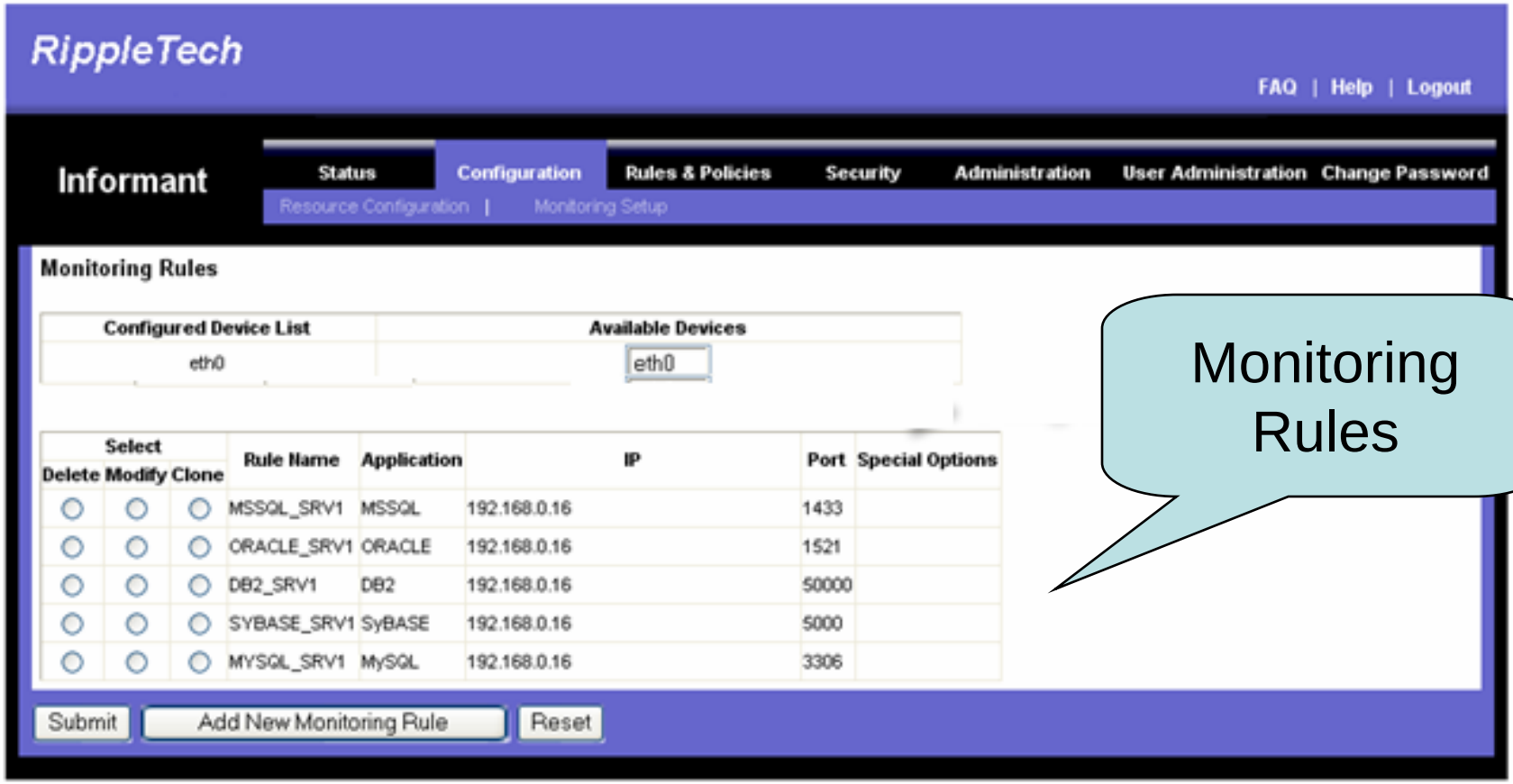
+ **Native Database Auditing**
  - Unacceptable performance
  - No management & reporting
  - No support for competing vendor tools
  - Cannot segregate security administration from DBA's
+ **Application Controls**
  - Insufficient information
  - No logging standard
  - No log of backdoor entries
+ **Intrusion Detection Systems**
  - Not session aware
  - Not suitable for monitoring policy violations

New Approach
(High Value)

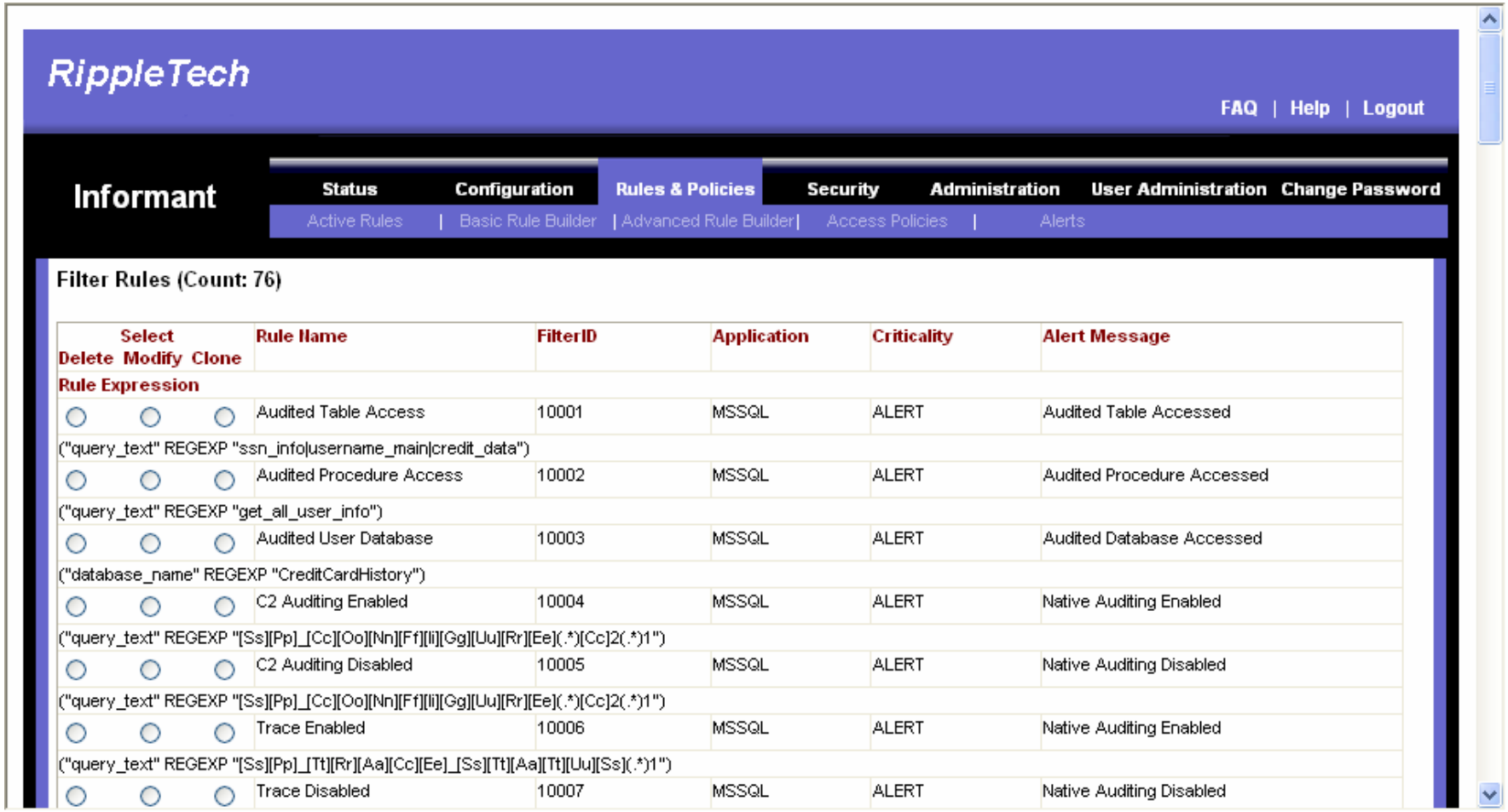
+ **Use a parallel process to create a log of ALL database activity**
  - No impact on production databases
  - Complete user session audit-trail
  - Plug & play appliance



Informant Appliance Setup

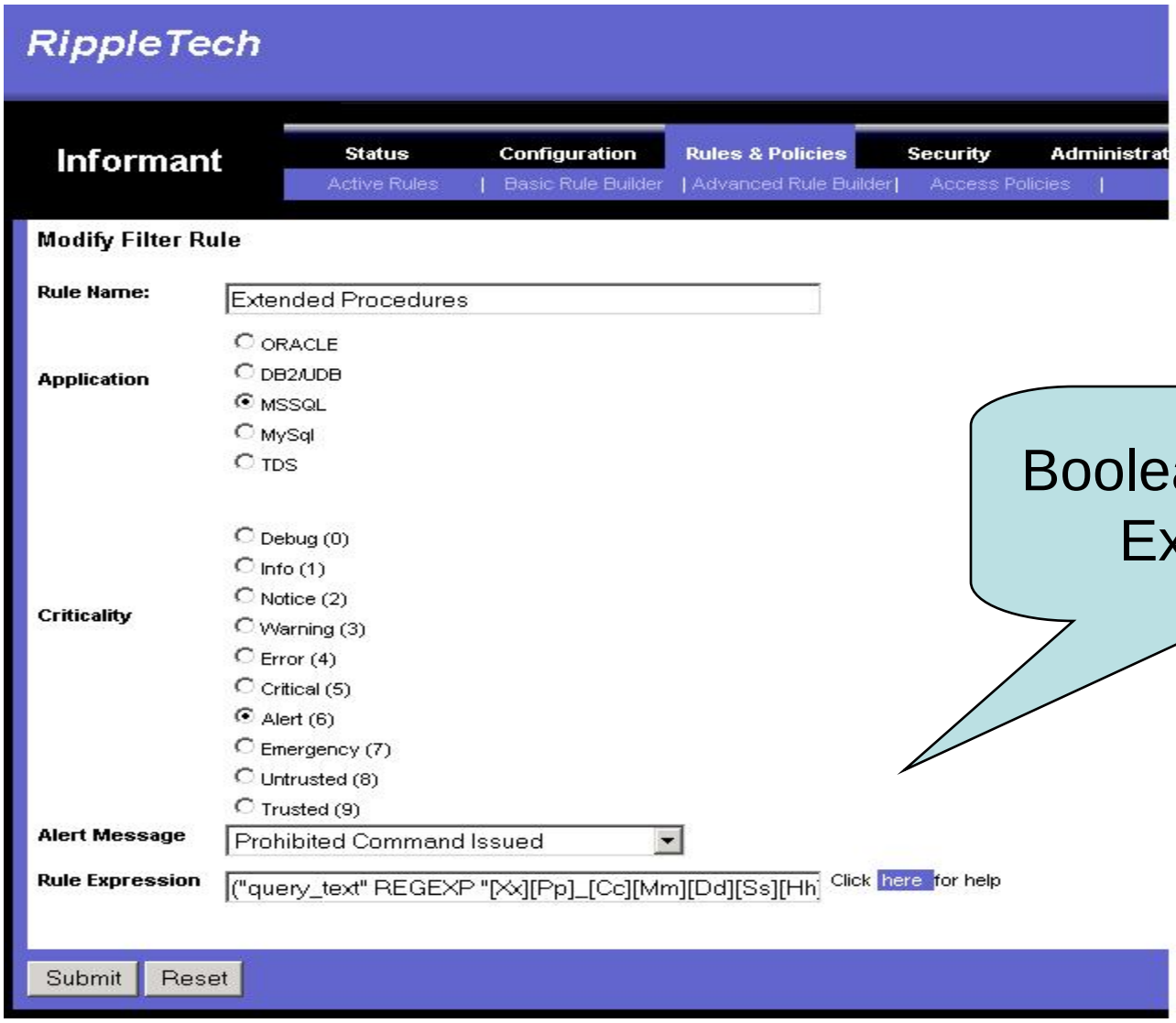


Informant Rules & Policies



Select Delete Modify Clone	Rule Name	FilterID	Application	Criticality	Alert Message
Rule Expression					
○ ○ ○	Audited Table Access	10001	MSSQL	ALERT	Audited Table Accessed
("query_text" REGEXP "ssn_info|username_main|credit_data")					
○ ○ ○	Audited Procedure Access	10002	MSSQL	ALERT	Audited Procedure Accessed
("query_text" REGEXP "get_all_user_info")					
○ ○ ○	Audited User Database	10003	MSSQL	ALERT	Audited Database Accessed
("database_name" REGEXP "CreditCardHistory")					
○ ○ ○	C2 Auditing Enabled	10004	MSSQL	ALERT	Native Auditing Enabled
("query_text" REGEXP "[Ss][Pp]_[Cc][Oo][Nn][Ff][Ii][Gg][Uu][Rr][Ee](.*)[Cc]2(.*)1")					
○ ○ ○	C2 Auditing Disabled	10005	MSSQL	ALERT	Native Auditing Disabled
("query_text" REGEXP "[Ss][Pp]_[Cc][Oo][Nn][Ff][Ii][Gg][Uu][Rr][Ee](.*)[Cc]2(.*)1")					
○ ○ ○	Trace Enabled	10006	MSSQL	ALERT	Native Auditing Enabled
("query_text" REGEXP "[Ss][Pp]_[Tt][Rr][Aa][Cc][Ee]_[Ss][Tt][Aa][Tt][Uu][Ss](.*)1")					
○ ○ ○	Trace Disabled	10007	MSSQL	ALERT	Native Auditing Disabled

Informant Rules & Policies



Boolean and Regex Expressions

Informant Reports (1 of 3)

All Database Activity

Description

A summary of all database activity events for the specified time period

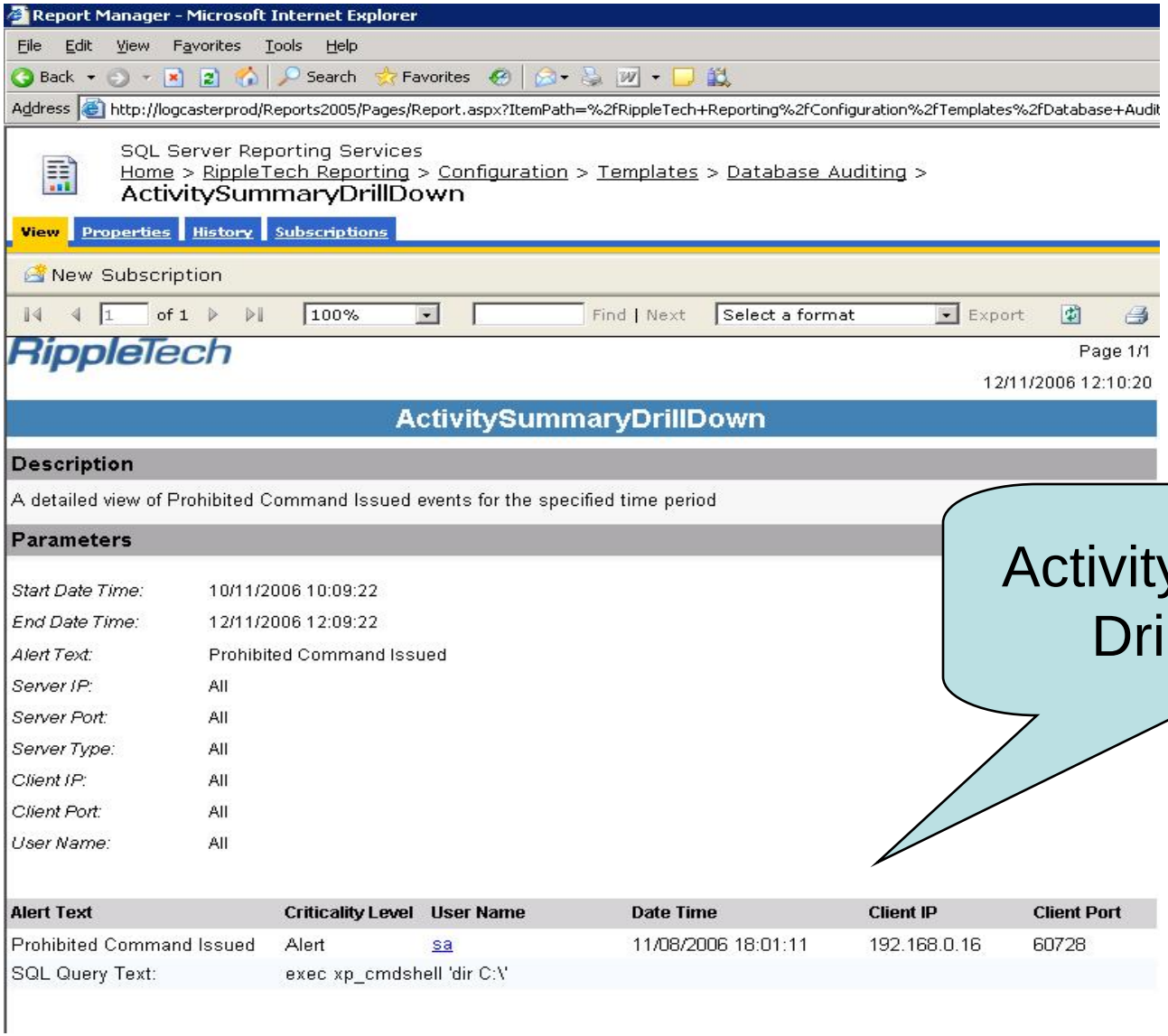
Parameters

Start Date Time:	10/01/2006 19:40:24	*Violation Type:*	All
End Date Time:	01/01/2007 21:40:24	*Client IP:*	All
Server IP:	All	*User Name:*	All
Server Port:	All		
Server Type:	All		
Category:	All		
Criticality Level:	All		

Activity Summary

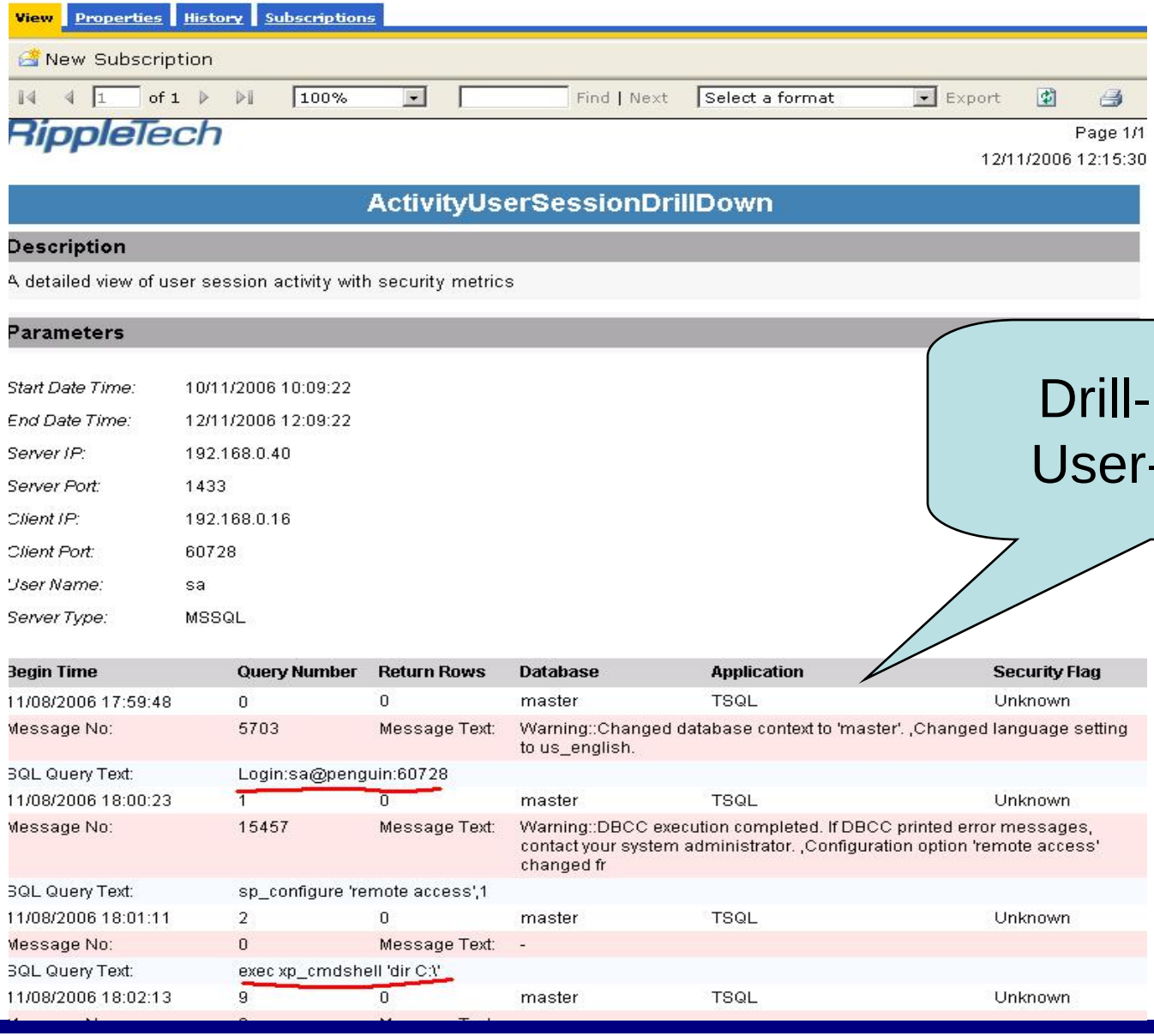
Alert	Criticality Level	Count
Untrusted Session	Untrusted	11
System Table Change	Alert	1
Process Killed	Alert	1
Prohibited Command Issued	Alert	1
Server Configuration Change	Alert	2

Informant Reports (2 of 3)



Activity Summary Drill-Down

RippleTech Informant Reports (3 of 3)



View | Properties | History | Subscriptions

New Subscription

1 of 1 | 100% | Find | Next | Select a format | Export

RippleTech

Page 1/1

12/11/2006 12:15:30

ActivityUserSessionDrillDown

Description

A detailed view of user session activity with security metrics

Parameters

Start Date Time:	10/11/2006 10:09:22
End Date Time:	12/11/2006 12:09:22
Server IP:	192.168.0.40
Server Port:	1433
Client IP:	192.168.0.16
Client Port:	60728
User Name:	sa
Server Type:	MSSQL

Begin Time	Query Number	Return Rows	Database	Application	Security Flag
11/08/2006 17:59:48	0	0	master	TSQL	Unknown
Message No:	5703	Message Text:	Warning::Changed database context to 'master'. ,Changed language setting to us_english.		
SQL Query Text:	Login:sa@penguin:60728				
11/08/2006 18:00:23	1	0	master	TSQL	Unknown
Message No:	15457	Message Text:	Warning::DBCC execution completed. If DBCC printed error messages, contact your system administrator. ,Configuration option 'remote access' changed fr		
SQL Query Text:	sp_configure 'remote access',1				
11/08/2006 18:01:11	2	0	master	TSQL	Unknown
Message No:	0	Message Text:	-		
SQL Query Text:	exec xp_cmdshell 'dir C:\'				
11/08/2006 18:02:13	9	0	master	TSQL	Unknown

Drill-Down to User-Session

RippleTech

Popular Reports

1. **Access Policy Violations**
   - Access to database from Untrusted sources (Users, IP Address)
2. **Audited Object Access**
   - Access or change to sensitive tables, procedures by all users & apps
3. **Database Schema Changes**
   - Reports on all DDL changes on all audited databases
4. **Failed Logins**
   - Failed Logins Attempts
5. **Logon Logoff**
   - Reports on all successful and failed logon & logoff attempts
6. **User Accounts and Privilege Changes**
   - Reports on all user account additions, modifications, deletions and privilege changes
7. **Privileged User Session/Audit Trail**
   - Audit-trail of all database activity performed by privileged users

RippleTech

Popular Alerts

1. Repeat logon failures by super user
2. Repeat logon failures by same user
3. Repeat query failures by same user
4. Successful logon after repeat failures
5. Successful logon by client on watch list
6. Successful logon by user on watch list

Database Events & Alarms

Alarms Groups

Audited Application Access	Large Result Set
Audited User Access	Logon-logoff
Audited Data Changes	Object Changes (DDL)
Audited Object Access	Privileges Changes
Audited Schema Changes	Prohibited Activity
Connection Changes	Server Startup & Shutdown
Data Changes (DML)	Slow Queries
Database Config Changes	Successful Logons
Database Maintenance	Suspicious Activity
Database Server Changes	System Table Changes
Failed Logons	Untrusted Access
Failed Transactions	Users Changes

Alert Options

SNMP	SCRIPT
SMTP	3rd Party Tools
SYSLOGS	

Criticality Levels

DEBUG	0
INFO	1
NOTICE	2
WARNING	3
ERROR	4
CRIT	5
ALERT	6
EMERG	7
UNTRUSTED	8
TRUSTED	9
CUSTOM	>= 10

Sample Raw Data

Exhaustive metrics normalized for reporting and analysis

sec_flag	begin_time	end_time	response_time	server_response_time	begin_time_skew	client_ip	server_ip	
	client_port	server_port	query_number	query_exit_status	data_in	data_out	packets_in	
	packets_out	network_time	client_name	user_name	application_name	server_name	nt_client_Name	
	nt_user_Name	nt_domain_Name	query_type	error_code	error_severity	error_message	client_pid	return_rows
	query_text	database_name	spid					
2	9/6/2005 12:17	9/6/2005 12:17	0.008	0.004	5	192.168.1.5	192.168.1.100	55870
	1433	0	0	615	168	3	2	0.004
	roman	sa	TSQL	192.168.1.100	-	-	-	2 0
	0	-	14131	0	Login:sa@roman:55870		master	51
2	9/6/2005 12:17	9/6/2005 12:17	0.003	0.001	5	192.168.1.5	192.168.1.100	55870
	1433	1	4096	50	193	2	2	0.002
	roman	sa	TSQL	192.168.1.100	-	-	-	1 0
	0	-	14131	0	USE Northwind	Northwind	51	
2	9/6/2005 12:17	9/6/2005 12:17	0.002	0.002	5	192.168.1.5	192.168.1.100	55870
	1433	4	4096	50	17	1	1	0.000
	roman	sa	TSQL	192.168.1.100	-	-	-	1 0
	0	-	14131	0	INSERT INTO test1 values (123,1,'test 1')			Northwind 51
10248	Northwind	51						
2	9/6/2005 12:17	9/6/2005 12:17	0.001	0.001	5	192.168.1.5	192.168.1.100	55870
	1433	15	4608	65	264	1	1	0.000
	roman	sa	TSQL	192.168.1.100	-	-	-	1
	587333632	16	Error::DELETE statement conflicted with COLUMN REFERENCE constraint 'FK_Order_Details_Orders'.					
The conflict occurred in database 'Northwind', table 'Order Details', column 'OrderID'.			CROW	14131	0	DELETE FROM		
Orders WHERE OrderId IN ('11072', '11076')			Northwind	51				
2	9/6/2005 12:17	9/6/2005 12:17	0.000	0.000	5	192.168.1.5	192.168.1.100	55870
	1433	16	0	0	0	0	0	0.000
	roman	sa	TSQL	192.168.1.100	-	-	-	0 0
	0	-	14131	0	Logout:sa@roman:55870		Northwind	51

RippleTech

Enterprise Requirements

+ Minimal impact to applications and servers
+ Support high-volume transactions
+ Support for heterogeneous environment
+ Separation of roles – DBA/security
+ Self-auditing tamper-proof audit repository
+ Centralized control of all audit information and mgmt
+ Long-term data archival
+ Customizable rules, reports and audit procedure
+ Role-based access to audit-data & reports
+ Granular auditing – who accessed what & when
+ Seamless integration into the enterprise SIM framework

Breaches in the News

- **(VISA) Credit card breach exposes 40 million accounts**

  MasterCard International announced information on more than 40 million credit cards **may have** been stolen.

- **US Air Force scrambles after privacy breach**

  The US Air Force has been forced to notify more than 33,000 airmen that their personal details **might** have been exposed ... on one account into a careers database

- **Database Breach at Computer Forensics Company**

  Guidance Software Inc stated **that it believed** that the compromised database contained names, addresses, credit card numbers and expiration dates of some 3,800 people

- **Honeywell Data Breach-** Reported January 26, 2006 - personal information of **19,000 employees compromised**.

RippleTech

Financial Impact

The list of companies with '*possible*' breaches that 'MAY' have, 'MIGHT' have, 'BELIEVED' to have had a breach goes on and on.....

And the cost per **'possible' breach** is significant....over **$182** per record compromised, *3 notifications required*

We can't afford to guess

Enterprises need to actively monitor and report on exactly who is accessing data, what they are doing with it, and alert when in-appropriate use is detected.

Questions

RippleTech

RippleTech

Thank you

For more information:

Go to: www.rippletech.com

Email: results@rippletech.com

Call: 610-862-4000