Audit and Compliance Best Practices: A practical guide to winning the war

PulseANZ 2010

Meet the people who can help advance your infrastructure

Trademarks and disclaimers

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries./ Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce. ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office. UNIX is a registered trademark of The Open Group in the United States and other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others. Information is provided "AS IS" without warranty of any kind.

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

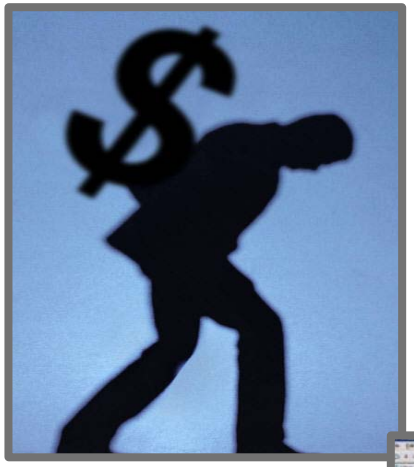
Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Trademarks of International Business Machines Corporation in the United States, other countries, or both can be found on the World Wide Web at http://www.ibm.com/legal/copytrade.shtml.

The Security Challenge: It's a balancing act



Cost of "Effective Security" has been rising faster than our budgets

While Compliance continues to be the hammer with which we can secure funding – spending results in more point products to solve more point problems

The Complexity of the security problem and the solution makes it difficult to know how much security is "good enough"

Meanwhile… Too much security can reduce operating efficiency

Key Regulations Affecting IT Security and Compliance

Privacy Regulations

- Gramm-Leach-Bliley Act (GLBA) US
- PIPEDA Canada
- COPPA and CIPA US
- California Individual Privacy (SB1386) California
- PCI DSS v1.1 Industry
- Computer Security Act US
- EU Data Protection Directive EU
- HIPAA US
- Personal Health Information Act Canada
- Data Protection Act UK

Financial Integrity and Solvency Regulations

- 8th Company Law Directive (Euro SOX) EU
- Financial Instruments and Exchange Law (J-SOX) Japan
- 2012 Solvency II EU
- Sarbanes-Oxley Act US
- Corporate Law Economic Reform Program Australia
- Basel II EU

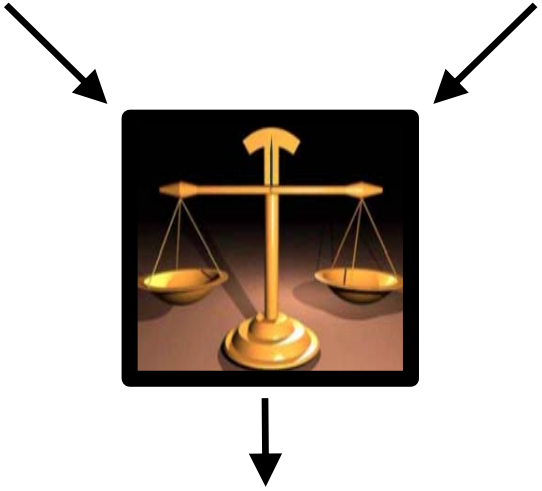
Other Regulations

- Federal Rules of Evidence US
- USA PATRIOT Act US

Security and Compliance –
One does not necessarily lead to the other

Strong IT Security practices do not necessarily lead to a strong Compliance posture.

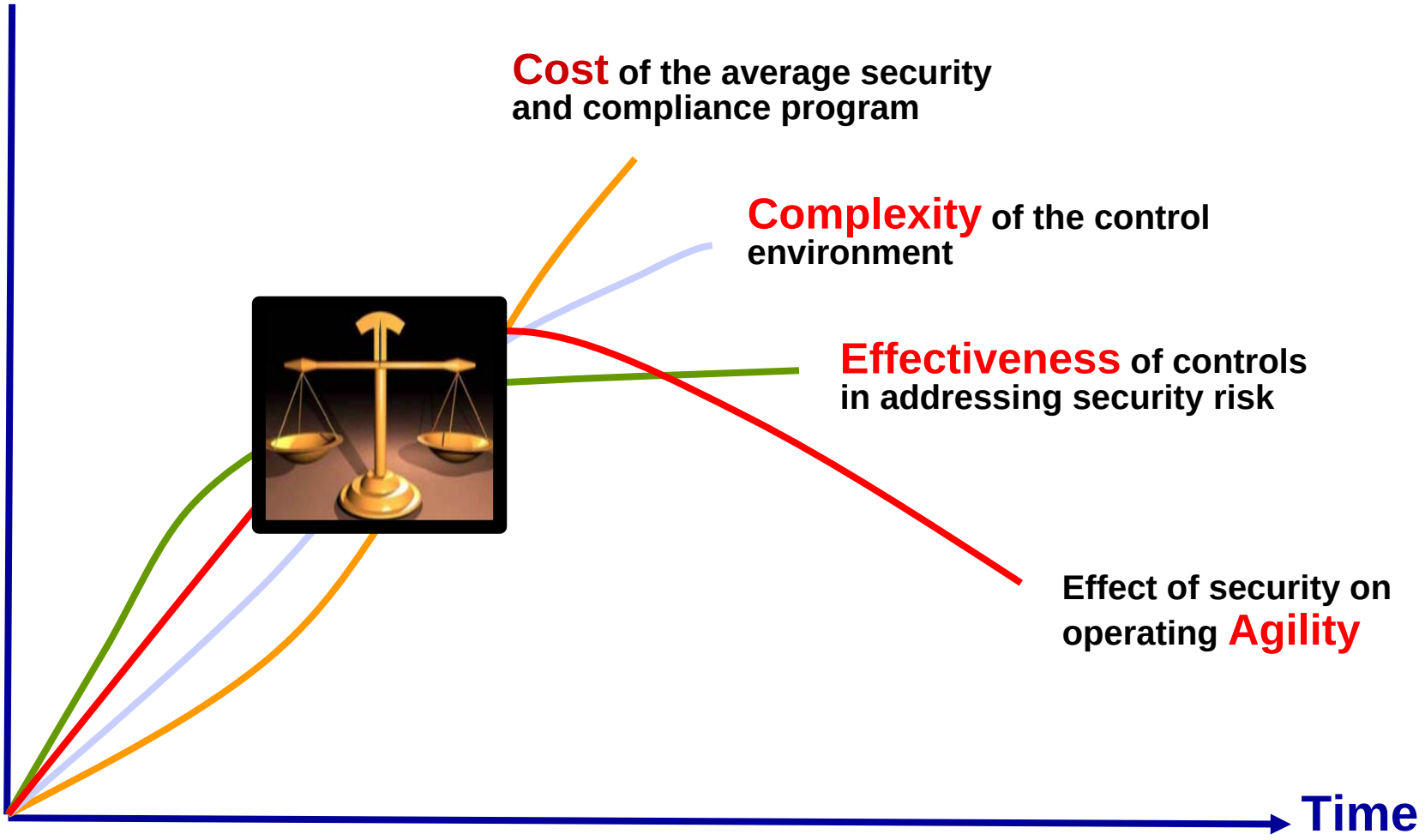
Being "in Compliance" does not necessarily mean you have a strong Security posture.



A balance is needed – Cost, Complexity, Effectiveness and Agility.

The CSO/CISO/CCO Challenge:

Manage Cost, Decrease Complexity, Improve Effectiveness, Assure Agility



Best Practice: Focus on foundational controls

Pareto principle, often referred to as "the 80-20 rule," applies to IT controls.

The Pareto principle states that for many phenomena, 80 percent of the consequences stem from 20 percent of the causes.

After three years of research, ITPI discovered that a small percent of IT controls, also known as *foundational controls*, provide a disproportionately high amount of coverage.

- Threat and Vulnerability Management
- Identity & Access Management
- Release Management
- Change & Configuration Management
- Security Information and Event Management
- Incident Management

Recommend:

+ automate, monitor, measure and enforce foundational controls

+ Implement a controls-based framework, e.g. CobiT

Stages of Security Practice Evolution -

Know where you are and where you want to be

Traditional approaches to security do not work effectively…

Point Products

Point Problems

Fragmented policy and process

Complexity

Redundant Costs

Resource Inefficiency

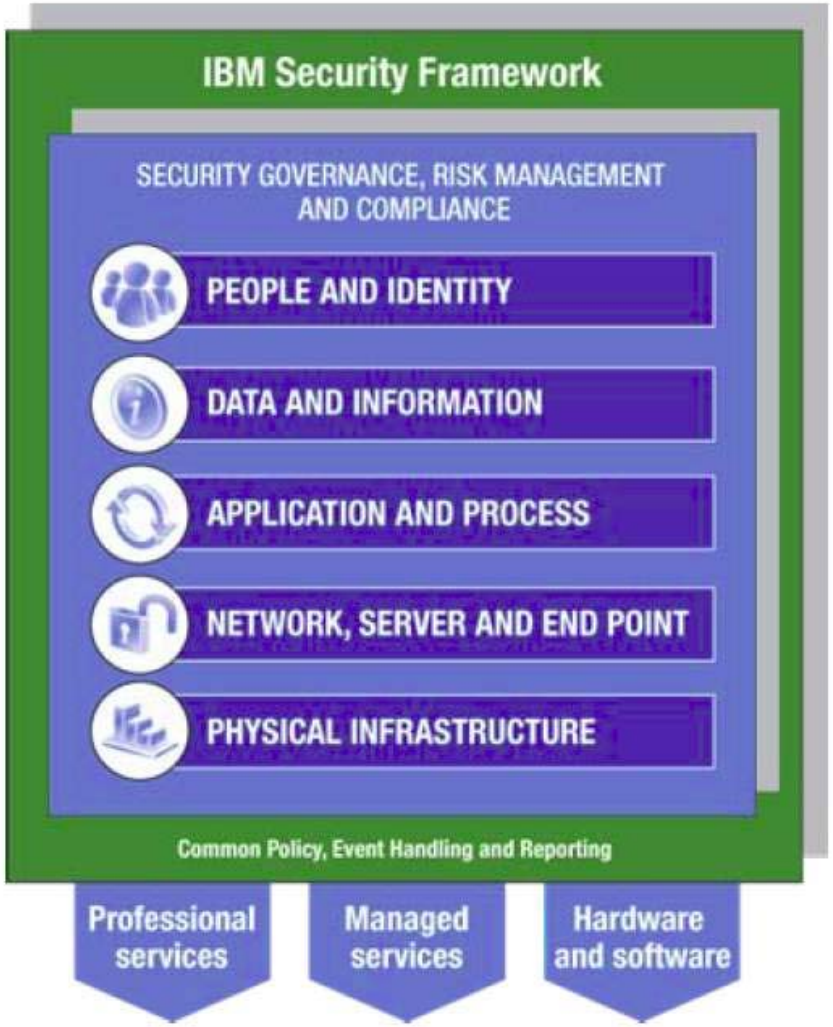
Silos of Data

- An alternative approach is required to solve the security puzzle
- An approach based on delivering business value through integrated solutions built into standard operations

IBM'S integrated approach enables enterprises to:

- **start addressing their most pressing challenge**
- **extend to other focus areas as needed**

A new approach to Security



Designed to….

- Enable innovation through secured infrastructure and platforms
- Reduce number and complexity of required security controls
- Reduce redundant security expenses
- Improve organizational and operational agility and resiliency
- Deliver needed visibility, control and automation

IBM Security Solutions

Identity and Access Assurance

Provide efficient and compliant access for the right people to the right resources at the right time

Data and Application Security

Protect integrity and confidentiality of business data and transactions from browser to disk

Data Center and Operational Security

Optimize service availability by mitigating risks while optimizing expertise, technology and process

SIEM

IBM Security Solutions

Identity and Access

- Identity Manager
- Access Manager for e-business
- Access Manager for Enterprise SSO
- Federated Identity Manager
- Directory Server
- Directory Integrator
- Security Role Manager
- Privileged Identity Manager (component)
- zSecure suite

Data and Application Security

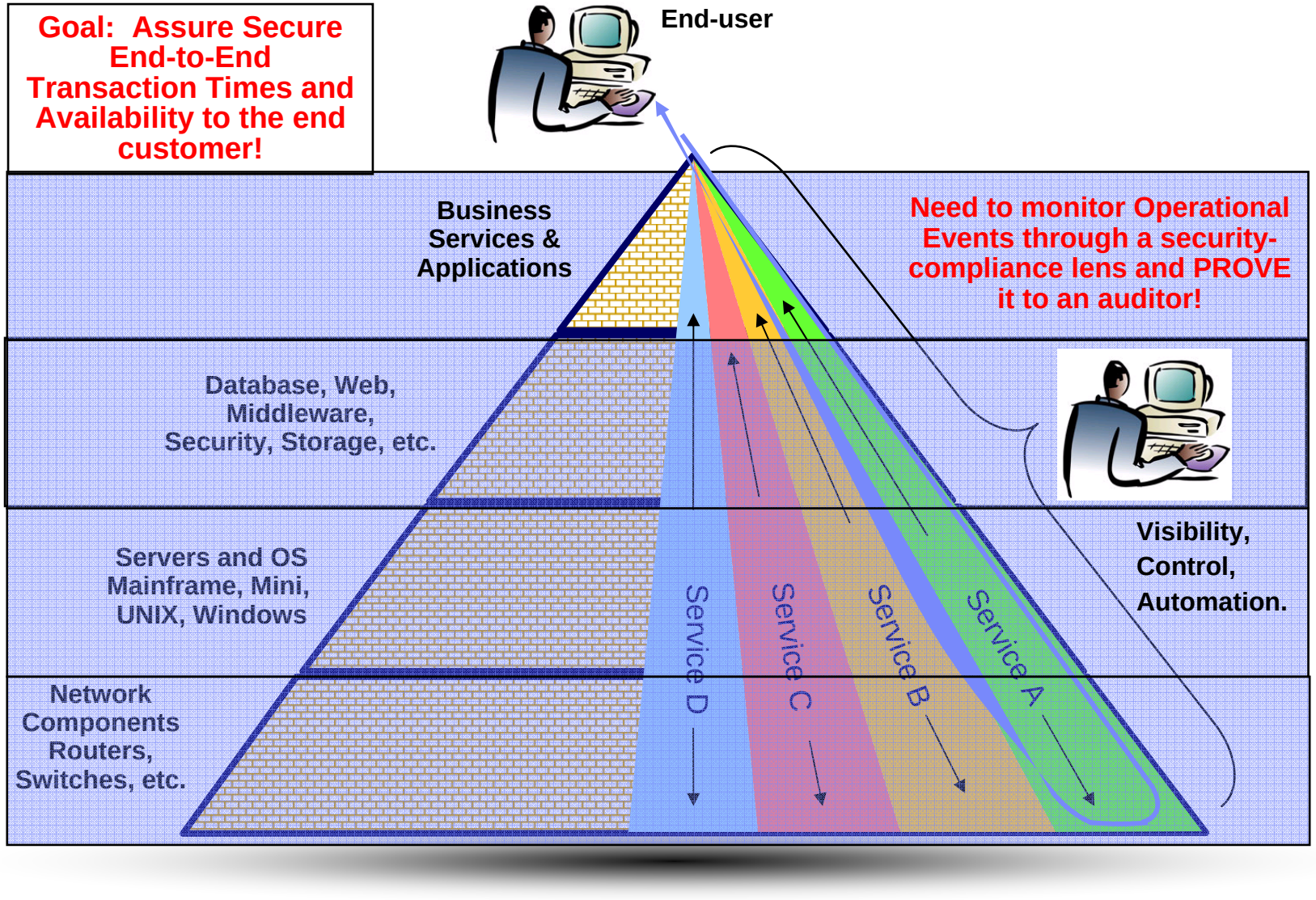
- Security Policy Manager
- Security Web Gateway
- Information Loss Protection
- Key Lifecycle Manager
- Deep Content Analysis SDK
- Multifunction Security

Data Center and Operational Security

- Security Server Protection
- Security SiteProtector System
- Virtual Server Protection
- RealSecure Server Sensor
- Network Intrusion Prevention Appliances
- Network Intrusion Prevention System Virtual Appliance
- Enterprise Scanner
- Desktop Security

TSIEM

Why is compliance so difficult?

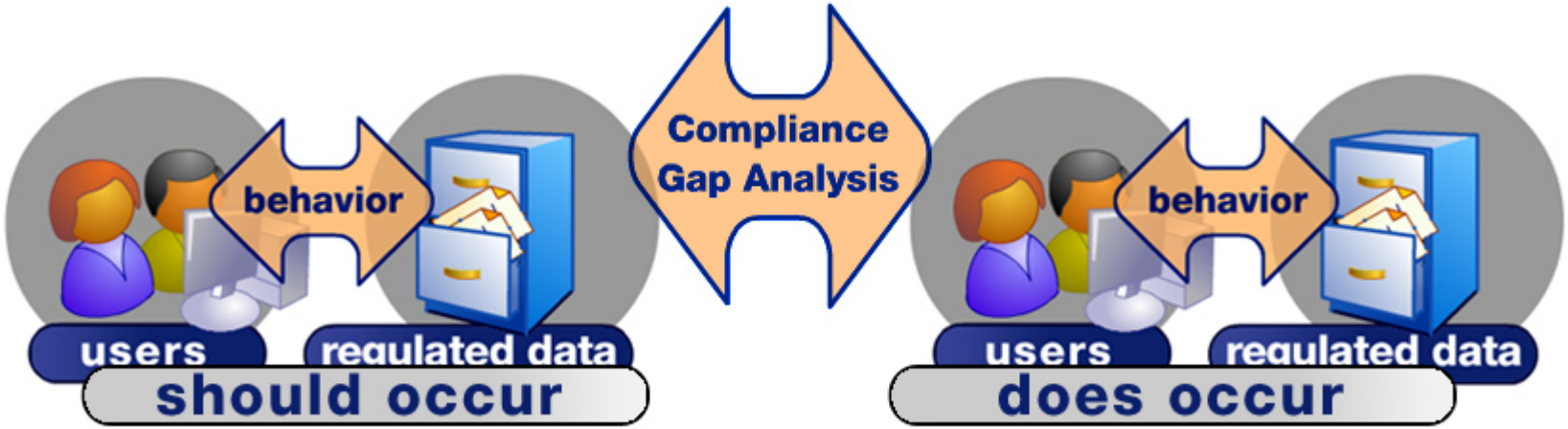


Can you answer these questions?

- Did anyone touch or modify sensitive data inappropriately? **(acceptable use)**
- Are outsourcers managing systems and data responsibly? **(change management)**
- Were there any unauthorized changes to the operating environment? **(change management)**
- Are we alerted when rogue administrative accounts are created? **(account management)**
- Are system administrator and system operator activities logged and reviewed on a regular basis?
- Is all access to sensitive data – including root/administration and DBA access – logged and monitored?
- Are security incidents and suspicious activity analyzed, investigated and remedial actions taken?

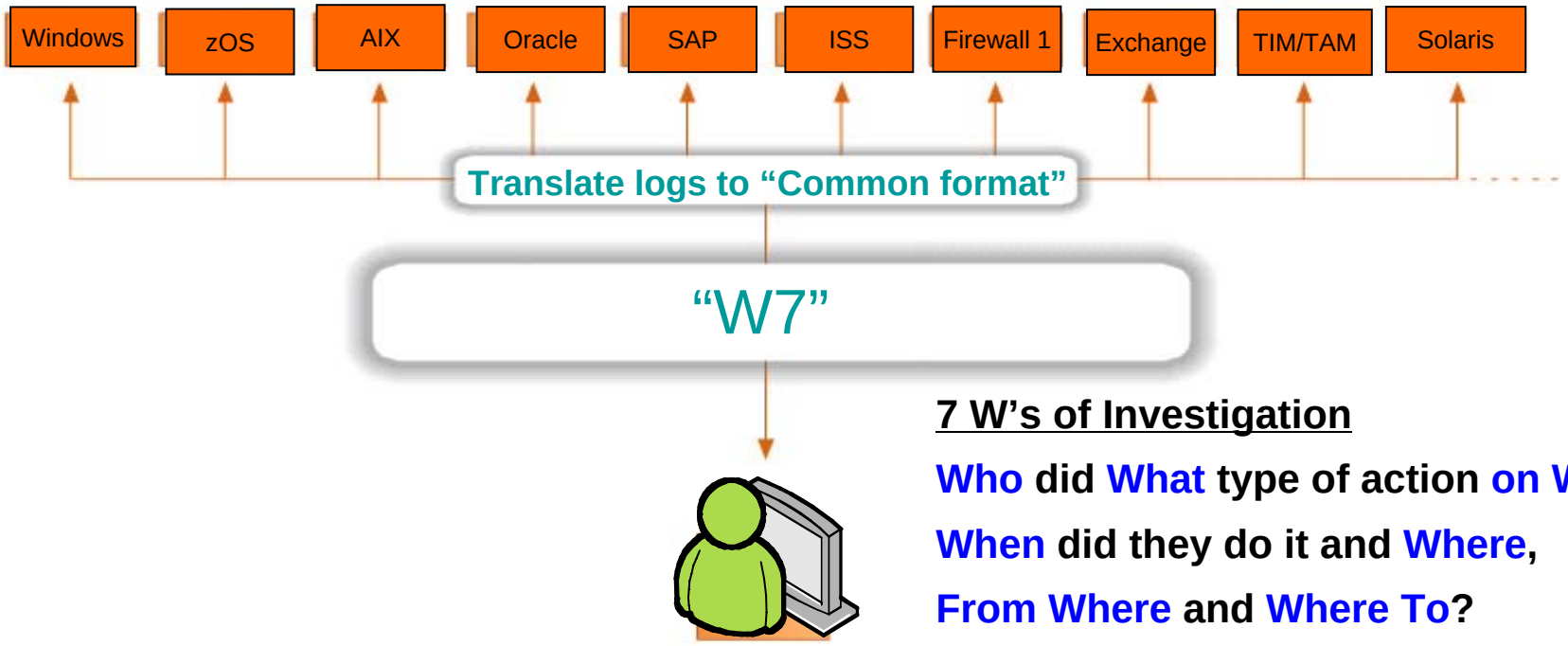
TSIEM enables governance

Compares desired versus actual behavior...



... like an auditor does.

All Logs in Your Enterprise in a Single Language



7 W's of Investigation

Who did What type of action on What?

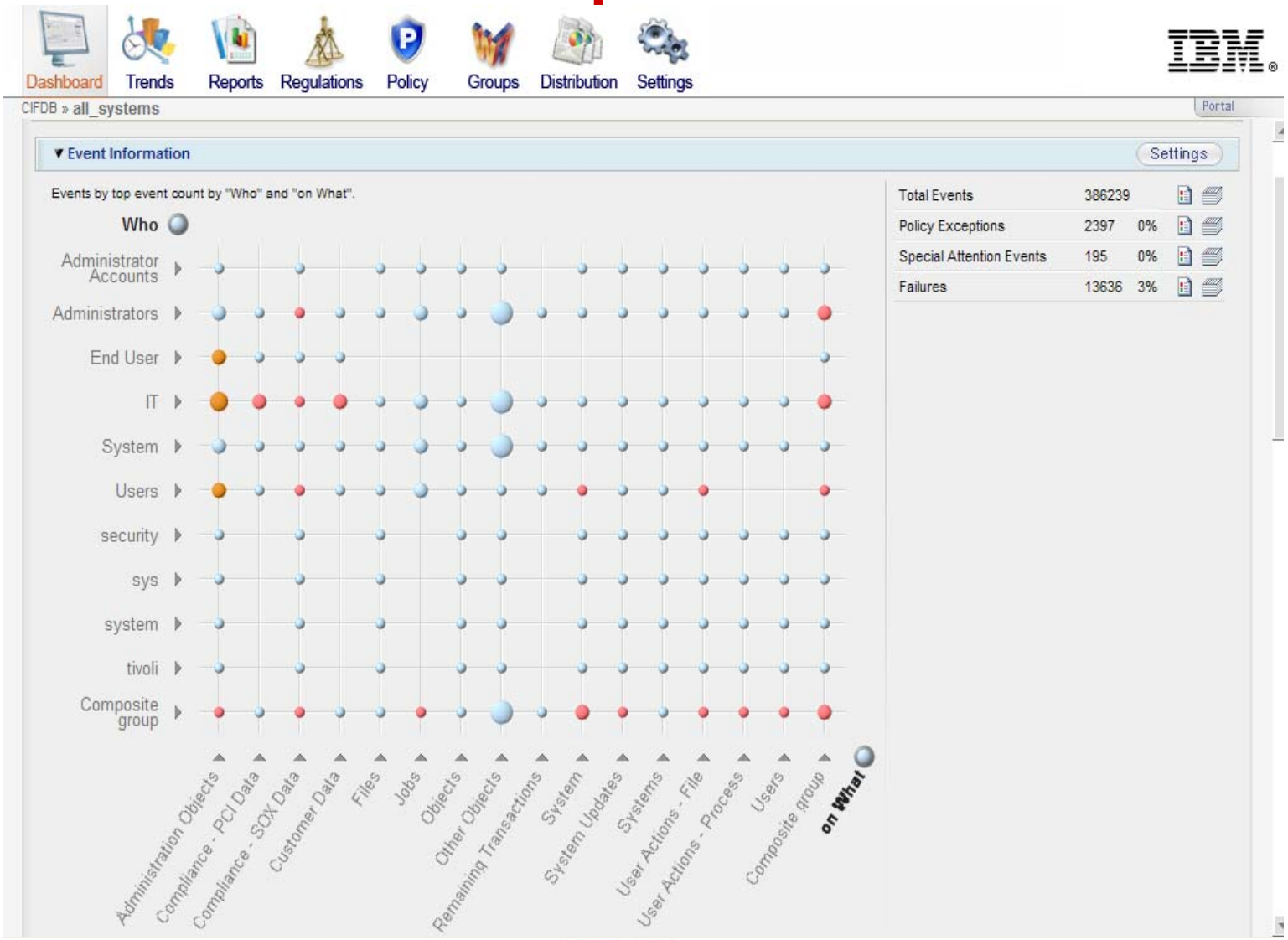
When did they do it and Where,

From Where and Where To?

TSIEM's W7 saves your information security and compliance staff time and money.

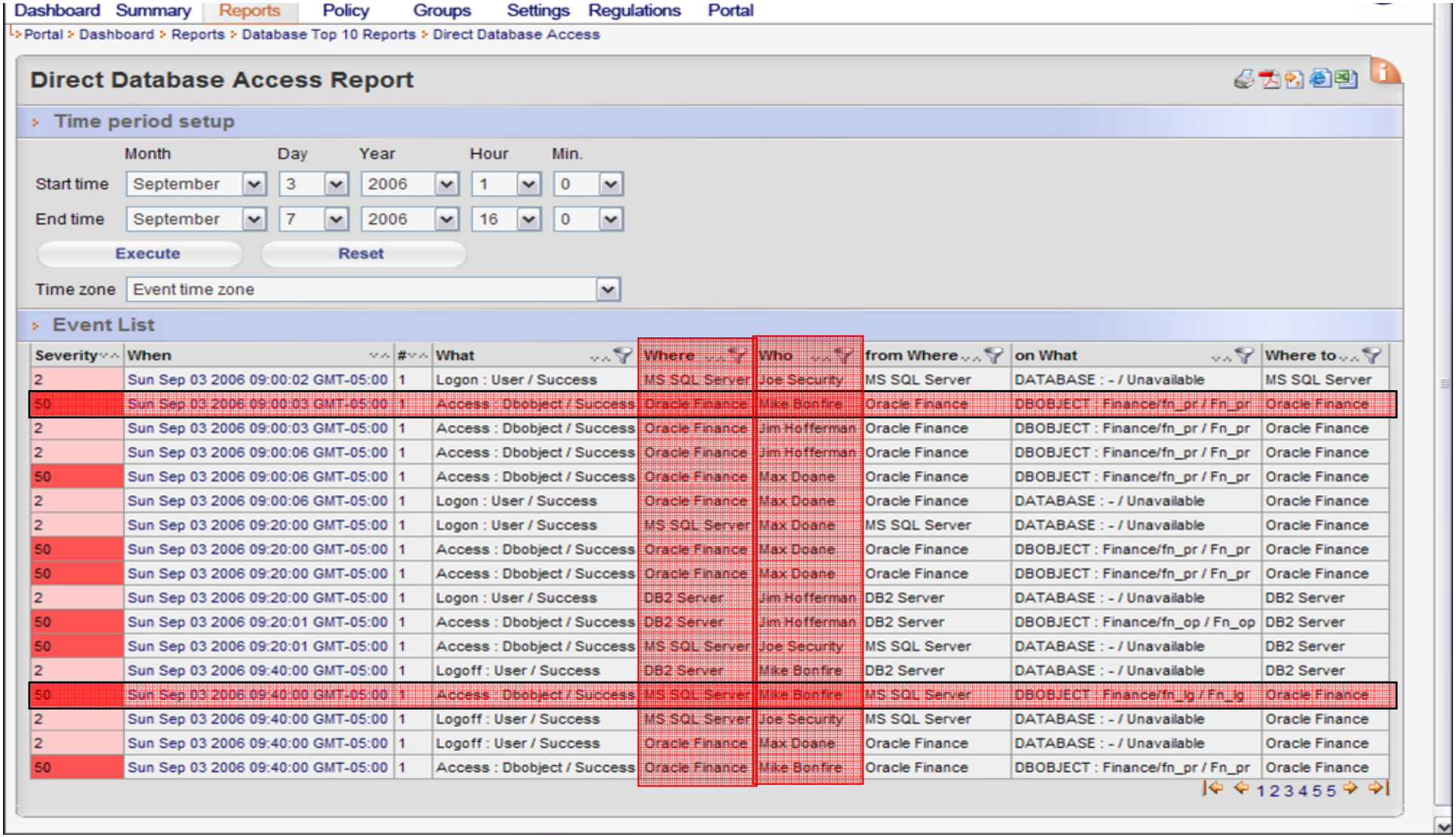
- **reduces the need for skilled staff**
- **produces reports auditors can understand**
- **automates monitoring across the enterprise.**

Demonstrate Compliance



- Quick Drill-down
- Policy Exceptions
- Special Attentions
- Failures
- Trends
- Reporting DBs
- Aggregation DBs
- Enterprise Overview
- Reports Distribution
- Self-audit

Example: Database Activity Monitoring with TSIEM



Severity	When	#	What	Where	Who	from Where	on What	Where to
2	Sun Sep 03 2006 09:00:02 GMT-05:00	1	Logon : User / Success	MS SQL Server	Joe Security	MS SQL Server	DATABASE : - / Unavailable	MS SQL Server
50	Sun Sep 03 2006 09:00:03 GMT-05:00	1	Access : Dbobject / Success	Oracle Finance	Mike Bonfire	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
2	Sun Sep 03 2006 09:00:03 GMT-05:00	1	Access : Dbobject / Success	Oracle Finance	Jim Hofferman	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
2	Sun Sep 03 2006 09:00:06 GMT-05:00	1	Access : Dbobject / Success	Oracle Finance	Jim Hofferman	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
50	Sun Sep 03 2006 09:00:06 GMT-05:00	1	Access : Dbobject / Success	Oracle Finance	Max Doane	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
2	Sun Sep 03 2006 09:00:06 GMT-05:00	1	Logon : User / Success	Oracle Finance	Max Doane	Oracle Finance	DATABASE : - / Unavailable	Oracle Finance
2	Sun Sep 03 2006 09:20:00 GMT-05:00	1	Logon : User / Success	MS SQL Server	Max Doane	MS SQL Server	DATABASE : - / Unavailable	Oracle Finance
50	Sun Sep 03 2006 09:20:00 GMT-05:00	1	Access : Dbobject / Success	Oracle Finance	Max Doane	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
50	Sun Sep 03 2006 09:20:00 GMT-05:00	1	Access : Dbobject / Success	Oracle Finance	Max Doane	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance
2	Sun Sep 03 2006 09:20:00 GMT-05:00	1	Logon : User / Success	DB2 Server	Jim Hofferman	DB2 Server	DATABASE : - / Unavailable	DB2 Server
50	Sun Sep 03 2006 09:20:01 GMT-05:00	1	Access : Dbobject / Success	DB2 Server	Jim Hofferman	DB2 Server	DBOBJECT : Finance/fn_op / Fn_op	DB2 Server
50	Sun Sep 03 2006 09:20:01 GMT-05:00	1	Access : Dbobject / Success	MS SQL Server	Joe Security	MS SQL Server	DATABASE : - / Unavailable	DB2 Server
2	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Logoff : User / Success	DB2 Server	Mike Bonfire	DB2 Server	DATABASE : - / Unavailable	DB2 Server
50	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Access : Dbobject / Success	MS SQL Server	Mike Bonfire	MS SQL Server	DBOBJECT : Finance/fn_lg / Fn_lg	Oracle Finance
2	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Logoff : User / Success	MS SQL Server	Joe Security	MS SQL Server	DATABASE : - / Unavailable	Oracle Finance
2	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Logoff : User / Success	Oracle Finance	Max Doane	Oracle Finance	DATABASE : - / Unavailable	Oracle Finance
50	Sun Sep 03 2006 09:40:00 GMT-05:00	1	Access : Dbobject / Success	Oracle Finance	Mike Bonfire	Oracle Finance	DBOBJECT : Finance/fn_pr / Fn_pr	Oracle Finance

1 2 3 4 5 5

Example: Privileged User Monitoring with TSIEM

Event Detail

Event information

	Field	Group	
Severity	2 (1x)	-	
When	Fri Oct 31, 2006 08:05:01 GMT +02:00	Office Hours (10)	10
What	Grant - Privilege / Success	Security Changes Administration	50 40
Where	SRV_DC_034 (Windows)	Finance Server	50
Who	Jim Hofferman	Administrators Database Admin Finance Admin	30 30 20
From Where	XPWKST03 (Windows)	Workstation	10
On What	USER - Chin055 / Chin055	Authorization Objects	30 20
Where To	SRV_DC_034 (Windows)	Finance Server	50

Incident Tracking

Additional information

Investigate

Time: Fri Oct 31, 2006 08:05:01 GMT +02:00 (+/-) 1 minute

Selected time zone: GMT+01:00 Rome, San_Marino, Sarajevo

Filter by Platform: SRV_DC_034 (Windows)

Filter by User: Jim Hofferman

Investigate

Logrecords...

```
. .......?VGIBSMF      ..K.....              ..M
.........?VGIBJES2     ..P.....              ...
.........?VGIBSMFDUMPS.......?               ...
.....D...?VGIBSMFDUMPS.......?               ...
.....E...?VGIBDFHSM    ..Y.....              ...
. .......?VGIBDFHSM    ..Y.....              ..C
. .......?VGIBDFHSM    ..Y.....              . C
.1.......?VGIBHSM      ........**HSM***..O
.........?VGIBDFHSM    ..Y.....              ..D
.1.......?VGIBHSM      ........**HSM***..O
.1.......?VGIBHSM      ........**HSM***..O
.0.......?VGIB...VSRTEST01..?
.1.......?VGIBHSM      ........**HSM***..O
. ...b...?VGIBSMFDUMPS.......?               ..M
.....w...?VGIBSMFDUMPS.......?               ...
.........?VGIBSMFDUMPS.......?               ...
```

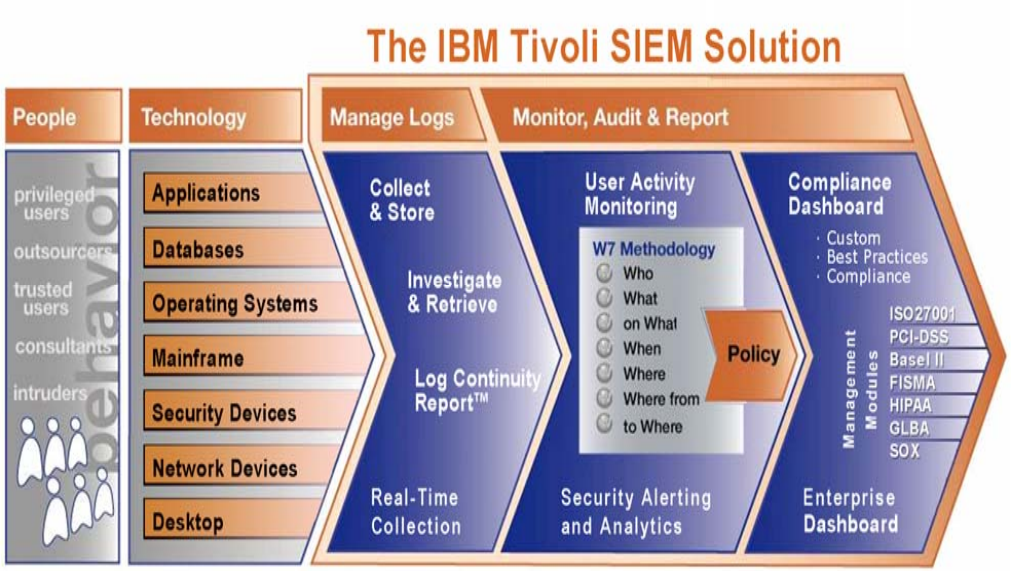
Assessing compliance: Tivoli Security Information and Event Manager

Manage logs and monitor privileged users for insider threat and compliance initiatives

Tivoli Security Information and Event Manager provides a single, integrated product for insider threat, audit and compliance

Highlights

- Single, integrated product
- Log Management Reporting
- Unique ability to monitor user behaviour
- Enterprise compliance dashboard
- Compliance management modules and regulation-specific reports
- Broadest, most complete log and audit trail capture capability
- W7 log normalisation translates your logs into business terms
- Makes it easy to compare behaviour to regulatory and company policies



Multinational Financial and Travel Services Provider protects intellectual property and complies with regulations

Company profile:

- Major diversified financial and travel services provider
- S&P 500

Issues:

- Protect intellectual property across global operations while outsourcing significant IT functions
- Need to monitor privileged users:
  - Significant audit finding
  - Concern for customer data
  - Major concerns about outsourcers
- Prove compliance in regulated environment (**SOX, PCI**)

IBM TSIEM fills the gap:

- Activity auditing across various systems:
  - **AS400**
  - **Mainframe**
  - **Windows**
  - **UNIX (Solaris, AIX)**
  - **Databases (Oracle, SQL Server, UDB)**
  - **Stratus**
- SOX and customized outsourcer reports
- Multi-million dollar investment with plans to monitor 20,000 systems at full deployment

Benefits:

- Monitor outsourcers for compliance
- Audit behavior of privileged users
- Meet audit concern
- Fulfill regulatory requirements
- Improve operational efficiency

Major Automotive Manufacturer is at the forefront of Compliance Management Implementations

Company profile:

- Major automotive manufacturer
  - Finance Division
- S&P 500 – $2B Company
- Worldwide operations
- 10,000 employees

Issues:

- Compliance with **GLBA, PCI and SOX**
- Mgmt of insider threats and reduction of risk from privileged users
- Monitoring of external perimeter threats
- Monitoring the effectiveness of the identity and access management process

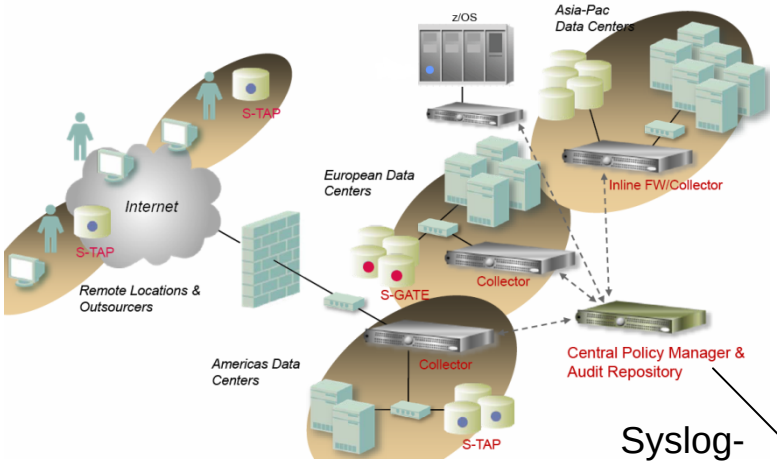
TSIEM fills the gap:

- Monitor privileged user activity, provide forensic evidence and consolidate data for compliance reporting in IAM environment:
  - Automate on and off boarding of users
  - Control access to sensitive information
  - Provide visibility into WHO accessed sensitive information
  - Flag abnormal activities
  - Report on compliance posture
- Provide security threat and activity auditing across various systems:
  - Network nodes
  - Web Servers
  - ISS SiteProtector (consolidate Network Security Devices & CISCO security information)
  - Mainframe
  - Windows, UNIX, Databases
  - Legacy financial systems on iSeries
- SOX, GLBA, and PCI reports

Benefits:

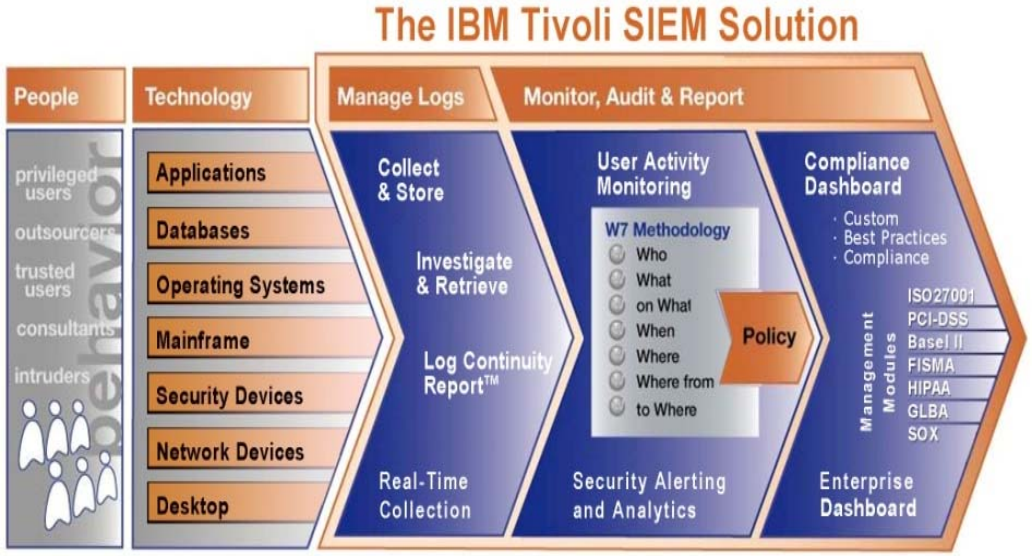
- Got ROI from the 1st day
  - SIM →Peoplesoft login/logoff reports
  - SEM → Detected internal customers affected by malicious email and executed a 0-day worm/trojan. Addressed affected machines on real-time
- Closed the loop on user access provisioning
- Audit behavior of privileged users
- Meet audit concern
- Lock down all critical resources
- Fulfill regulatory requirements
- Improve operational efficiency and reduced costs

TSIEM with Guardium: Database monitoring
Low overhead with no reliance on native logging



- Granular database monitoring and protection
- Low overhead; no reliance on native logging
- Database location and classification
- Database assessment and hardening
- Automated compliance reporting and workflow
- Export alerts and key data to TSIEM

Syslog-CEF Feed



- Integrate Guardium alerts and data
- Enterprise compliance and audit
- Forensics
- Log management
- Compliance management modules for ISO27001, GLBA, SOX, HIPAA, etc.

TSIEM 2.0 Log Management server features

- Reliable and scalable log collection and archiving
- Flexible integration, able to collect any type of log located on any type of machine in a tcp/ip network.
- Out-of-the-box log management reports
- Out-of-the-box best practice log analysis reports.
- Customizable search tool for advanced log analysis.
- Includes TDI 7.0: The ultimate information transformation swiss army knife!

TDI 7.0

The ultimate information transformation swiss army knife.

Axis Easy Web Service Server Connector
Axis Easy Web Service Invoke
Axis Java-to-Soap
Invoke Soap Web Service
Axis Soap-to-Java

LDAP Connector
LDAP Server Connector
Tivoli Access Manager Connector
TSIEM Connector
Windows Users and Groups Connector

Active Directory Changelog Connector v2
IBM Directory Server Changelog Connector
Netscape/iPlanet Changelog Connector
zOS LDAP Changelog Connector

JDBC Connector
Properties Connector
SystemStore Connector
RDBMS Changelog Connector

AssemblyLine Connector
Server Notifications Connector
AssemblyLine Function Component

Domino Change Detection Connector
Domino Users Connector
Lotus Notes Connector

Exchange Changelog Connector
Mailbox Connector
SendEMail Function Component

TIM DSMLv2 Connector
DSMLv2 SOAP Connector
DSML v2 SOAP Server Connector
Generic JNDI Connector
ITIM Agent Connector

EMF SDOToXML Function Component
EMF XMLToSDO Function Component

Timer Connector

AssemblyLines

Add new TSIEM event sources easily.

Generic Log Adapter Connector
RAC Connector
CBE (Common Base Event) components

JMX Connector
SNMP Connector
SNMP Server Connector
TCP Connector
TCP Server Connector

Remedy/Peregrine /CCMDB tickets
Maximo MEA / IF
Many custom Components on
OPAL, tdi-users.org or on request

PeopleSoft Connector
Siebel Connector
SAP ALE IDoc Connector
SAP R/3 Business Object Repository
SAP R/3 User Registry
SAP R/3 RFC Component

Script Connector
Generic Java Method
Parser FC

Remote secure command Line
z/OS TSO/E Command Line
Command Line Connector
MemQueue Connector

Memory Stream Connector

HTTP/REST Connector
File System Connector
FTP Client Connector
URL Connector
HTTP Client
HTTP Server Connector

IBM MQ Series Connector
JMS Pub/Sub Connector
MQe Password Store Connector

CCMDB

Netcool

RSS

Google

<u>Parsers</u>
CSV
DSML v1 & v2
Fixed Record
HTTP
LDIF
Line reader/writer
SOAP
Script
XML
XML Sax
XSL

As of June 26,2010

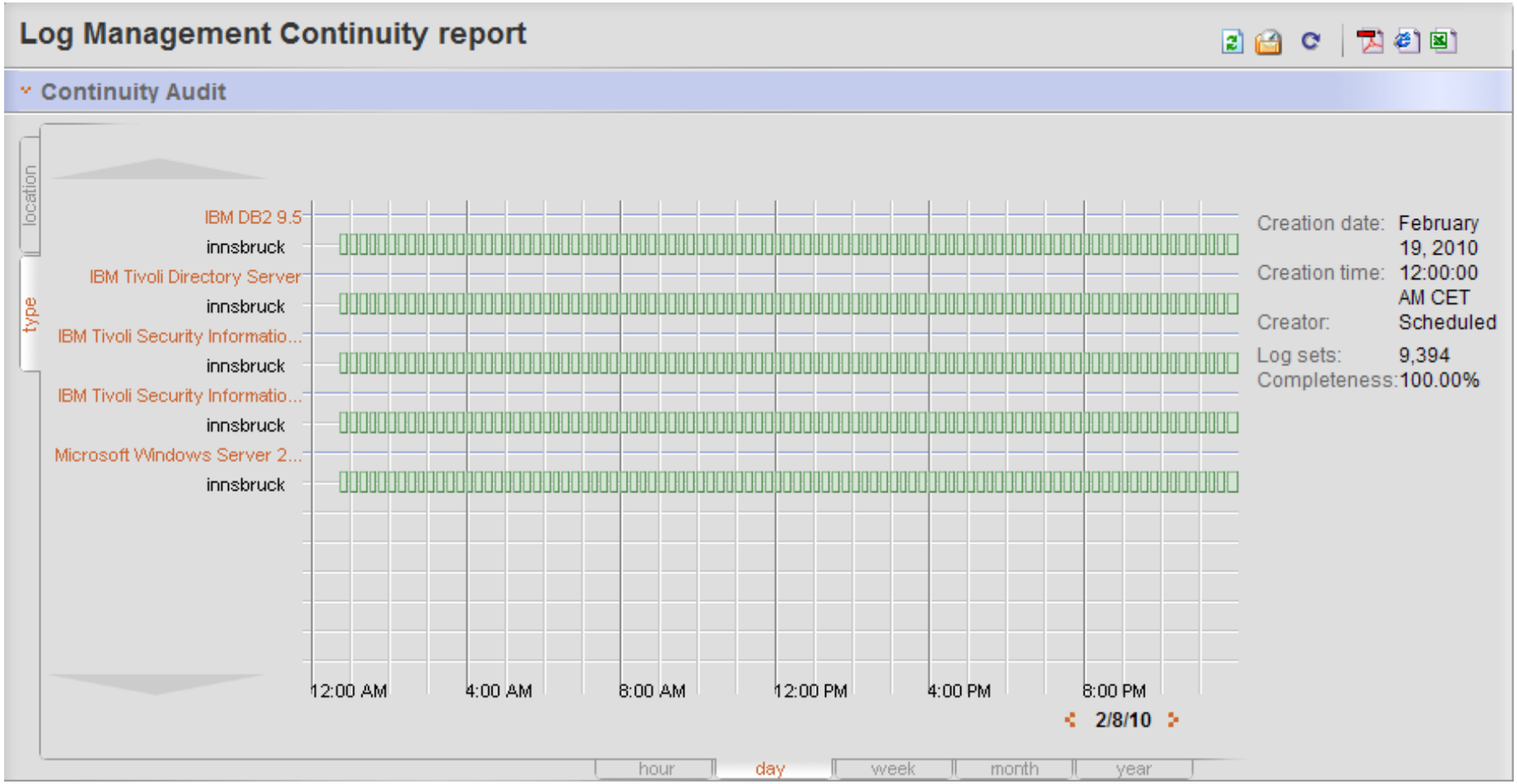
Log Management features: reliable and scalable

- Reliable Log collection using FIPS certified protocol.
  - Encrypted data transfer (AES128)
  - Secure channel (1024-bit DSA)
  - Compression rate 0.15
- Secure Log archive
  - Log archive storage on IBM DR550 ensures log integrity
  - Log Manager continuity report monitors quality of the log archive
- Scalable Log Management servers
  - High performance syslog/SNMP collector capable of processing up to **30.000 events per second**
  - One Log Management server manages around **5000 event sources**
  - One Log Management server collects and archives up to **180 GB per day**. (equal around 200.000.000 events per day)
  - Once a log has been archived its contents is always available for log analysis. The log can be exported from the archive to save disk space.

Best practice Log Analysis reports can be customised

Reports can be generated in many formats

Log Management: Continuity Report



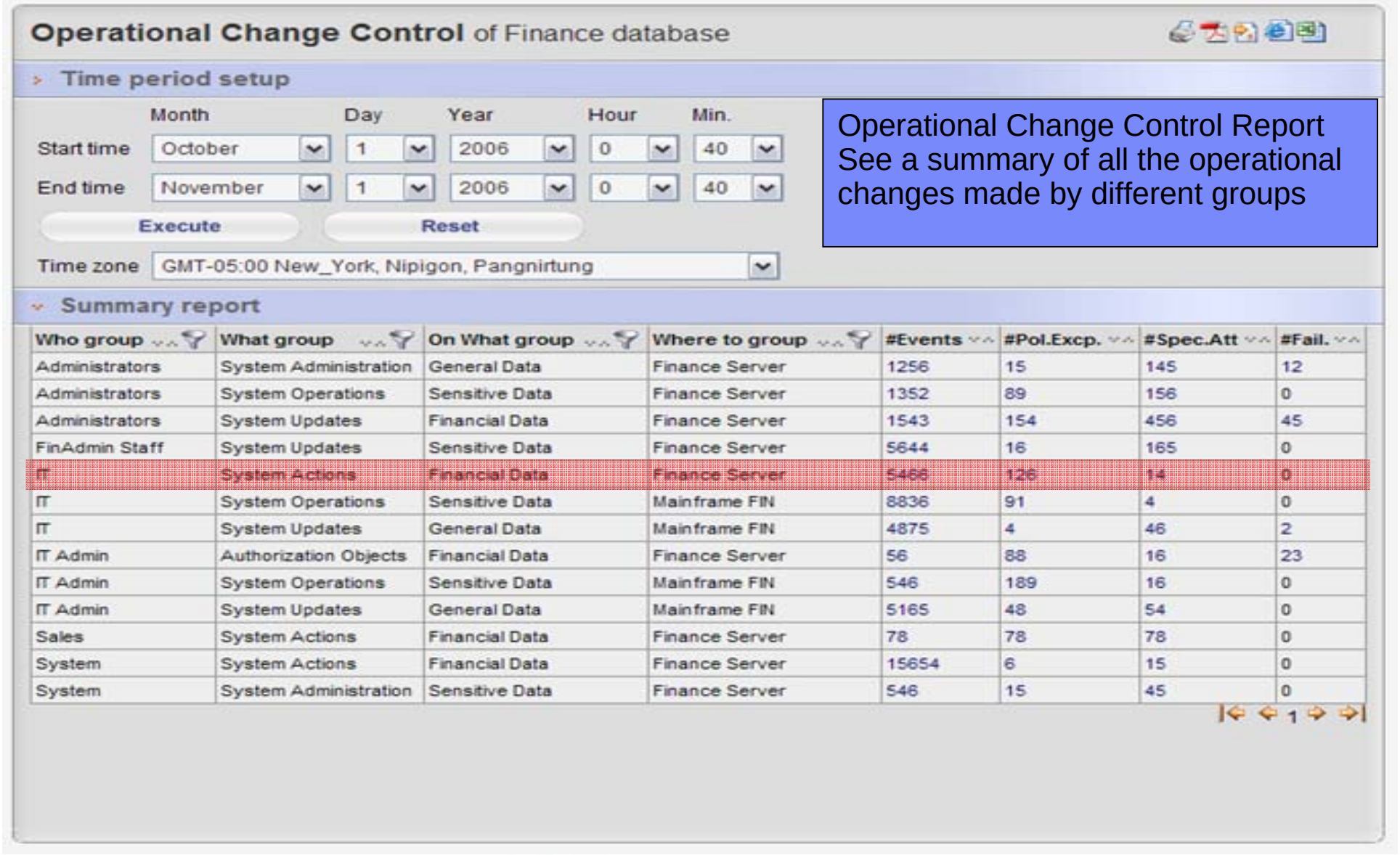
- Color codes are used to show the quality of the log archive
- Notifications can be sent to alert when gaps are found

PCI-DSS Regulation Reports

Add custom report | Import custom reports

PCI-DSS

Title	Description
PCI-DSS (1.2) Network intrusions	Unauthorized network access events
PCI-DSS (1.3) Network exposures	Exposures resulting from network misconfiguration
PCI-DSS (1.4) Network access violations	Exceptions and failures on network access
PCI-DSS (2.1,2.2) Configuration exposures	Exposures resulting from systems misconfiguration
PCI-DSS (2.3) Remote diagnostic port access	Detection of accesses to the diagnostic ports on servers.
PCI-DSS (5.1,5.2) Anti-virus configuration exposures	Exposures resulting from misconfiguration of anti-virus software
PCI-DSS (5.1,5.2) Covert channels and trojan code	Exceptions found from anti-virus software
PCI-DSS (6.1) Security patches	Exceptions and failures caused by insufficient security patch levels
PCI-DSS (6.3.3,6.3.4) Source code access	Exceptions and failures caused by accessing source code.
PCI-DSS (6.3.3,6.3.4) System test data	Controlled access to System test data.
PCI-DSS (7.1) Information access restrictions	Who accessed sensitive or private data successfully or unsuccessfully.
PCI-DSS (7.1) Sensitive system isolation	Exceptions and failures against sensitive systems data in asset groups Cardholder data, User, HR Data, Source Code, and Financial Data
PCI-DSS (8.5) Access Enforcement	Logon successes and failures, both locally and remotely
PCI-DSS (8.5) Account Management	System account management activity
PCI-DSS (8.5) System account policies	Exceptions and failures caused by systems account policy violations
PCI-DSS (10.2.1) Cardholder data access	Successful and failed cardholder data access
PCI-DSS (10.2.2) Operational change control	Changes to the operating environment such as system updates, DBA activity etc.



Operational Change Control Report
See a summary of all the operational changes made by different groups

“Acceptable Use” Policy -> Policy Violation, White List

Event Detail

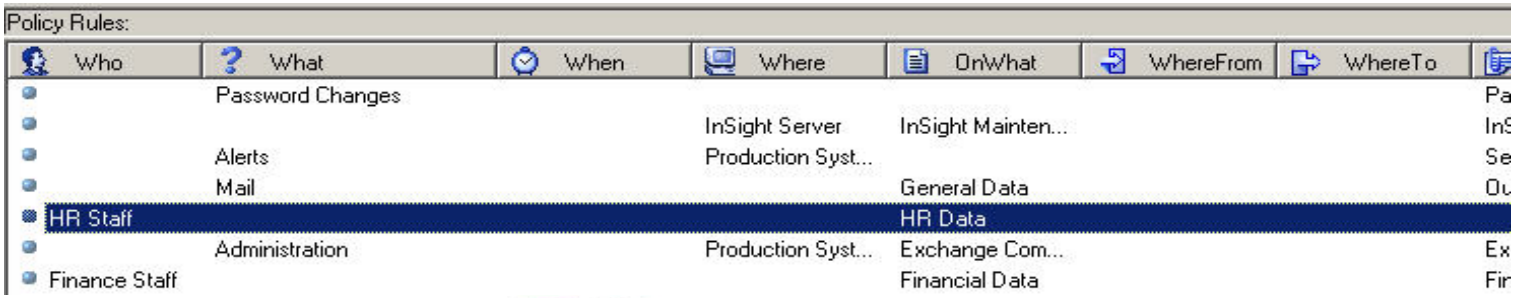
	Field	Group
Severity	50	This is a policy exception.
When	Fri Sep 15 2006 13:02:44 GMT-05:00	Office Hours (10)
What	Delete : Dbobject / Success	Configuration Changes (50) DBA Actions (20)
Where	XPWKST04 (MS SQL Server)	Systems with non-segregated administration (10)
Who	RHC\bfivozinshy	Unknown (10) Not System (10)
From Where	XPWKST04 (MS SQL Server)	Systems with non-segregated administration (10)
On What	DBOBJECT : Humanresources/hr_ben / Hr_ben	HR Data (30) HR Data - Medium (20)
Where To	XPWKST04 (MS SQL Server)	Systems with non-segregated administration (10)

► Incident Tracking

▼ Additional information

Aspect	Value
Event :: description	Delete [hr_ben] where [ssn]=@1

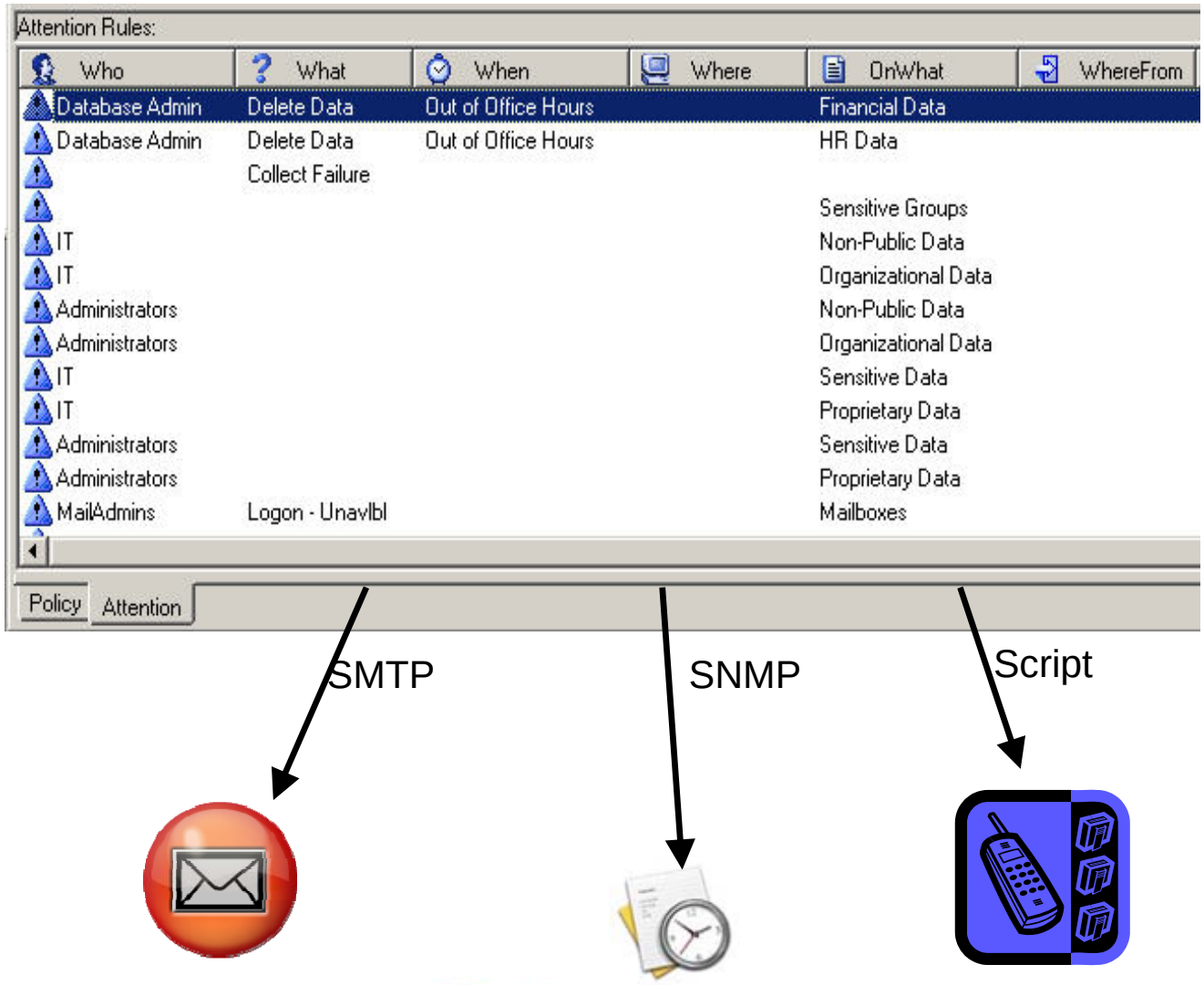
Define what is acceptable in your environment



Policy Rules:

Who	What	When	Where	OnWhat	WhereFrom	WhereTo	
	Password Changes						Pa
			InSight Server	InSight Mainten...			InS
	Alerts		Production Syst...				Se
	Mail			General Data			Ou
HR Staff				HR Data			
	Administration		Production Syst...	Exchange Com...			Ex
Finance Staff				Financial Data			Fir

Tell me when "**that**" happens. (Special Attention, Black List)



Audit and Compliance: Best Practices

- Apply the 80-20 rule
  - *Focus on foundational controls*
  - Implement a controls-based framework, e.g., CobiT
- Engage Business level management
- Start with an immediate use case & build on incremental success
- Select an integrated security solution with depth and breadth of event source support that **fuses** security across your enterprise and enables you to:
  - Audit as transparently as possible to minimize impact to the business
  - demonstrate reliable and verifiable log collection
  - identify and monitor sensitive information assets and privileged users
  - integrate with user provisioning solution (“closed loop” to IAM)
  - compare activity against “acceptable use” policy
  - Distribute policy exception reports/alerts to stakeholders
  - Take action: improve policy and improve process

TSIEM helps you win the Audit and Compliance war

- **W7 Reporting:** *"Who did What type of action on What?, When did they do it, and Where, From Where and Where To?"* - reduces audit costs. Out-of-the-box dashboards and reports are drill-down enabled and can be easily customised or combined using a user-friendly report wizard.
- **Privileged User Monitoring:** PUMA is part of the DNA of TSIEM and not a bolt on - as it is with competing solutions. Gartner has recognised our user and resource monitoring solution as the market leader.
- **Database Security:** Integration of SIEM with the Guardium database monitoring sets IBM apart from the competition uniquely providing customers with a complete database security solution.
- **Closed Loop Compliance:** Only a SIEM-IAM integrated solution offers true closed loop compliance capabilities. And only IBM offers an integrated in-house solution.
- **The Threat Monitoring Factor:** Integration of TSIEM with both ISS and Guardium easily differentiates IBM from the competition. An effective security framework requires a broader scope of relational solutions.
- **Mainframe / AS400 Support:** Unlike the competition, TSIEM offers full support for mainframe environments including integration with IBM's market leading zSecure solution. Superior for mainframe auditing. More SMF types collected, more detail.
- **Custom Event Sources & TDI:** Tivoli Directory Integrator (TDI) is the ultimate integration and information transformation swiss knife. Using TDI based methods, IBM can **quickly and easily build custom event collectors**. The competition has nothing like TD!.