



 What makes you special?

Tivoli Security Information & Event Management

Martin Borrett
Lead Security Architect
Technical Staff Member
NE Europe
IBM SWG

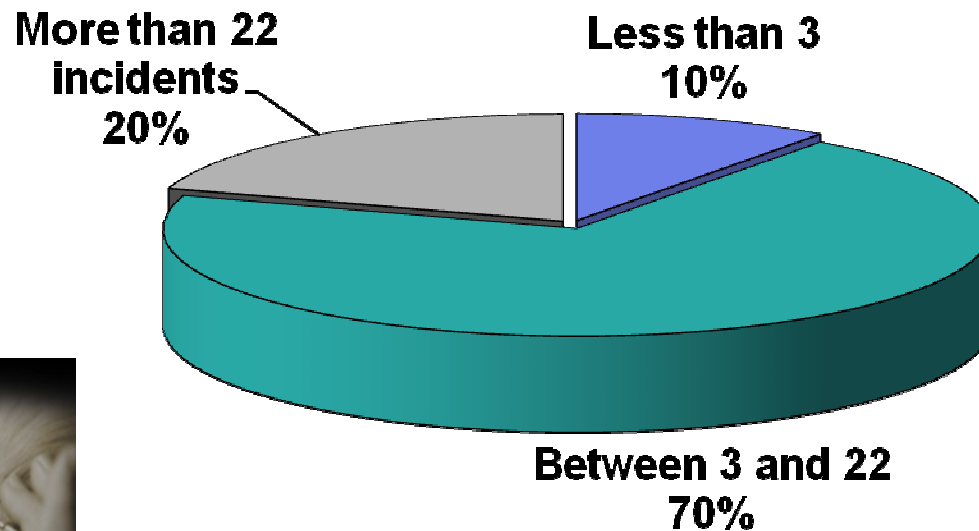


IBM Governance and Risk Management 
Business alignment, visibility and control



Security Requirements

Breaches of sensitive business data in past year:



Source: 2006 survey by the IT Policy Compliance Group





Known People (un) Intentionally Do Great Harm

87% of insider incidents are caused by privileged or technical users

Many are inadvertent violations of:

- Change management process
- Acceptable use policy

Others are deliberate, due to:

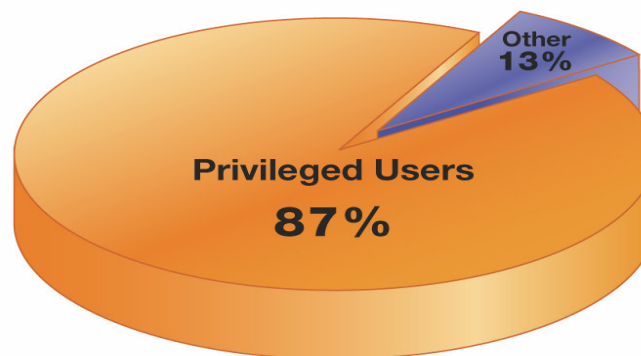
- Revenge (84%)
- "Negative events" (92%)

Regardless, too costly to ignore:

- Internal attacks cost 6% of gross annual revenue
- Costing \$400 billion in the US alone

Who Causes Internal Incidents?

Who Causes Internal Incidents?



Source: USSS/CERT Insider Threat Survey 2005

Who are they?

- Male
- 17-60 Years Old
- 87% technical positions
- About half married
- Variety of racial and ethnic backgrounds



Challenges to address

Increasing
Requirements

Increasing
Complexity

Increasing
Cost

**Security Compliance
Dashboard and Reporting**

**Privileged User Monitoring
and Audit (PUMA)**

**Database Monitoring and
Audit**

**Log and Audit Trail
Management**

Solutions In





Regulators & Auditors Make It Urgent

[ISO17799:2005]

10.10.1 Audit logging

Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.





The Problems We Help to Solve

“I need to provide reports to my auditors and regulators”

“I need to prove that I have effective IT security controls”

“My staff lacks the time, expertise, and desire to scan logs”

“I’m concerned about privileged actions”

“I need to store logs for forensics”

“I have no idea which logs to collect or how”





Agenda

Problems

Solution: TSIEM -- The 3 C's

1. Capture – Enterprise Log Management
2. Comprehend – Sophisticated Log Interpretation
3. Communicate – Full Audit and Compliance Reporting

Technology

Proven Results

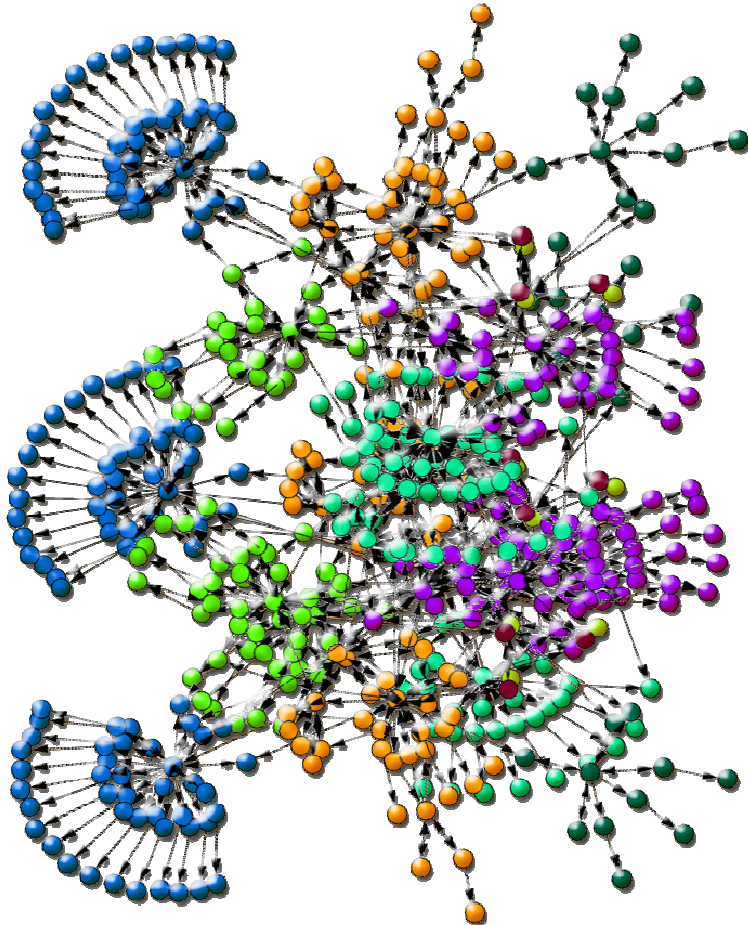




I Need to Collect Logs but it's Too Hard

Your enterprise

How to collect the logs?



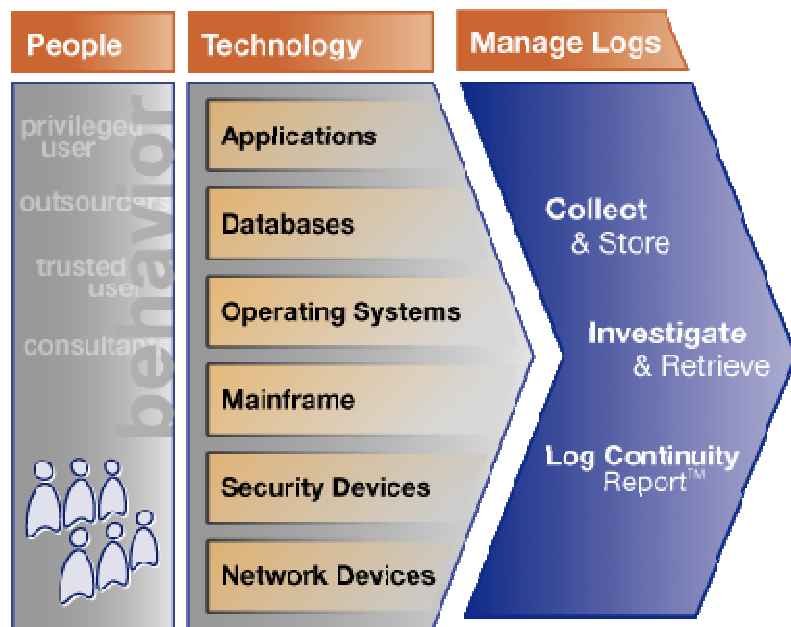
- Thousands of points across the enterprise generating event logs
- Regulators and auditors require you to capture and retain these log files
- Internal and external threats mean you need to investigate activities
- Time and cost constraints means it must be fast and affordable

Capture





Enterprise Log Management



Capabilities:

- Secure, reliable log capture from any platform
- Auto collection of syslogs
- Full support for native log collection
- Store in an efficient, compressed depot
- Access data when needed
- Search across all logs
- Reports to prove complete collection

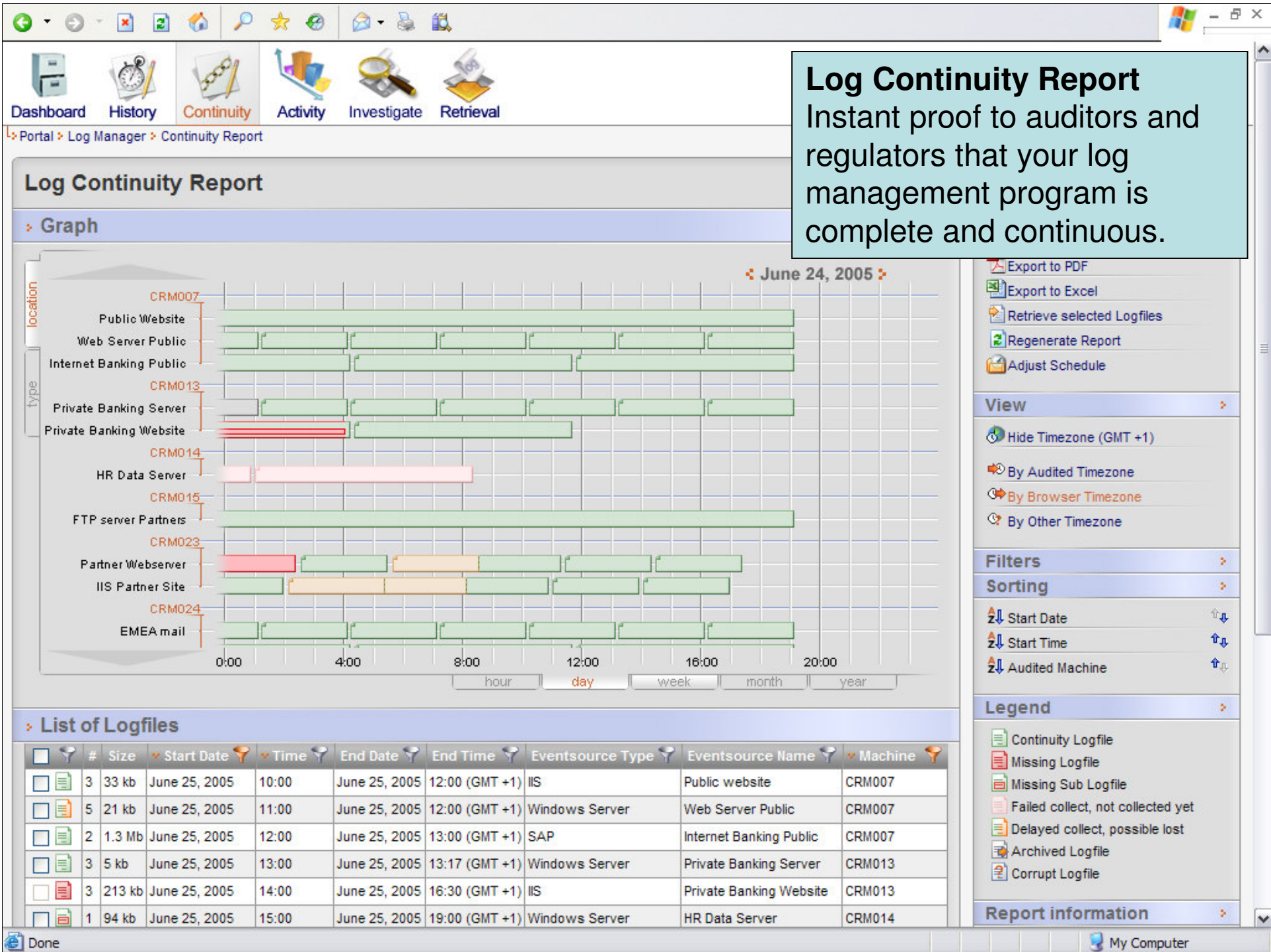
Benefits:

- Reduce costs by automating and centralizing collection
- Be “audit ready” at any time!

Implementation time: plug and play.



Capture



Log Continuity Report
Instant proof to auditors and regulators that your log management program is complete and continuous.

Export to PDF
Export to Excel
Retrieve selected Logfiles
Regenerate Report
Adjust Schedule

View

Hide Timezone (GMT +1)
By Audited Timezone
By Browser Timezone
By Other Timezone

Filters

Sorting

Start Date
Start Time
Audited Machine

Legend

Continuity Logfile
Missing Logfile
Missing Sub Logfile
Failed collect, not collected yet
Delayed collect, possible lost
Archived Logfile
Corrupt Logfile

Report information

Portal > Log Manager > Investigation Tool

Depot Investigation Tool

Query builder

Step 1. Time period

from: month: April, day: 1, year: 2001 till: month: April, day: 21, year: 2006

Step 2. Event Source

InSight server	Point of presence	Audited machine name	Event source type	Event source name
all	all	all	all	all
server-01	SERVER-05	SERVER-05	InSight Server Activit	InSight Server Activit
server-05		STYX	InSight Web Applica	Internet Information S
			Microsoft Windows	Oracle
			Oracle	

Step 3. Select Fieldnames

You changed your selection in the eventsources, this may cause missing fields in this list. Refresh the list to see all relevant fieldnames

Refresh Fieldname list

Select All Fields

<input checked="" type="checkbox"/> date	<input type="checkbox"/> s_port	<input type="checkbox"/> service
<input checked="" type="checkbox"/> dst	<input checked="" type="checkbox"/> number	<input type="checkbox"/> action
<input checked="" type="checkbox"/> type	<input type="checkbox"/> granularity	<input checked="" type="checkbox"/> scr
<input type="checkbox"/> eventclass	<input type="checkbox"/> resource	<input type="checkbox"/> sublogtype

Step 4. Content Search

clearlog*

Start Search Stop Search

Depot Investigation Tool
 Information at your fingertips,
 with easy to use search

Help

Actions

- Refresh Fieldname List
- Start Search
- Stop Search
- Retrieve selected Logfiles
- Restore default settings

View

- Show Timezone (GMT)
- By Browser Timezone
- By Other Timezone

Search information

Status: 0%

Creation Time: 0

Logfiles: 0

Events: 0

Support



Agenda

Problems

Solution: TSIEM -- The 3 C's

1. Capture – Enterprise Log Management
2. Comprehend – Sophisticated Log Interpretation
3. Communicate – Full Audit and Compliance Reporting

Technology

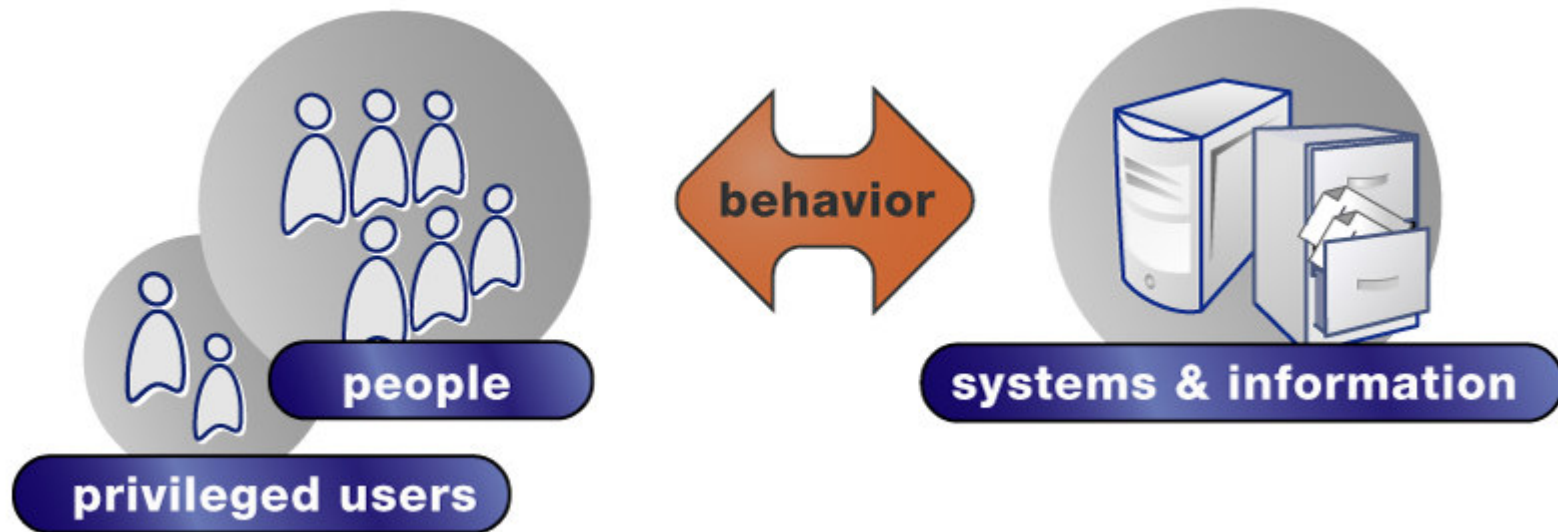
Proven Results





What are People Doing on My Network?

Comprehend



87% of insider incidents are caused by privileged and technical users.





How do I make sense of all this?

Comprehend

The screenshot shows a security audit log viewer with three audit events. Red boxes highlight key fields in each event, and red arrows point from these boxes to a central area where the fields are listed together for clarity.

System	Event	Process Name	Username	Remote Node ID	Remote Node Fullname
APPLES (system id: 2074)	Batch process login	BATCH_440	SYSTEM		
CYGNUS (system id: 2073)	Network login	MQMTC_P2_BG164	MQM	241859594	xyzz.bananajunior.com
CYGNUS (system id: 2073)	Batch process login	BATCH_443	SYSTEM		

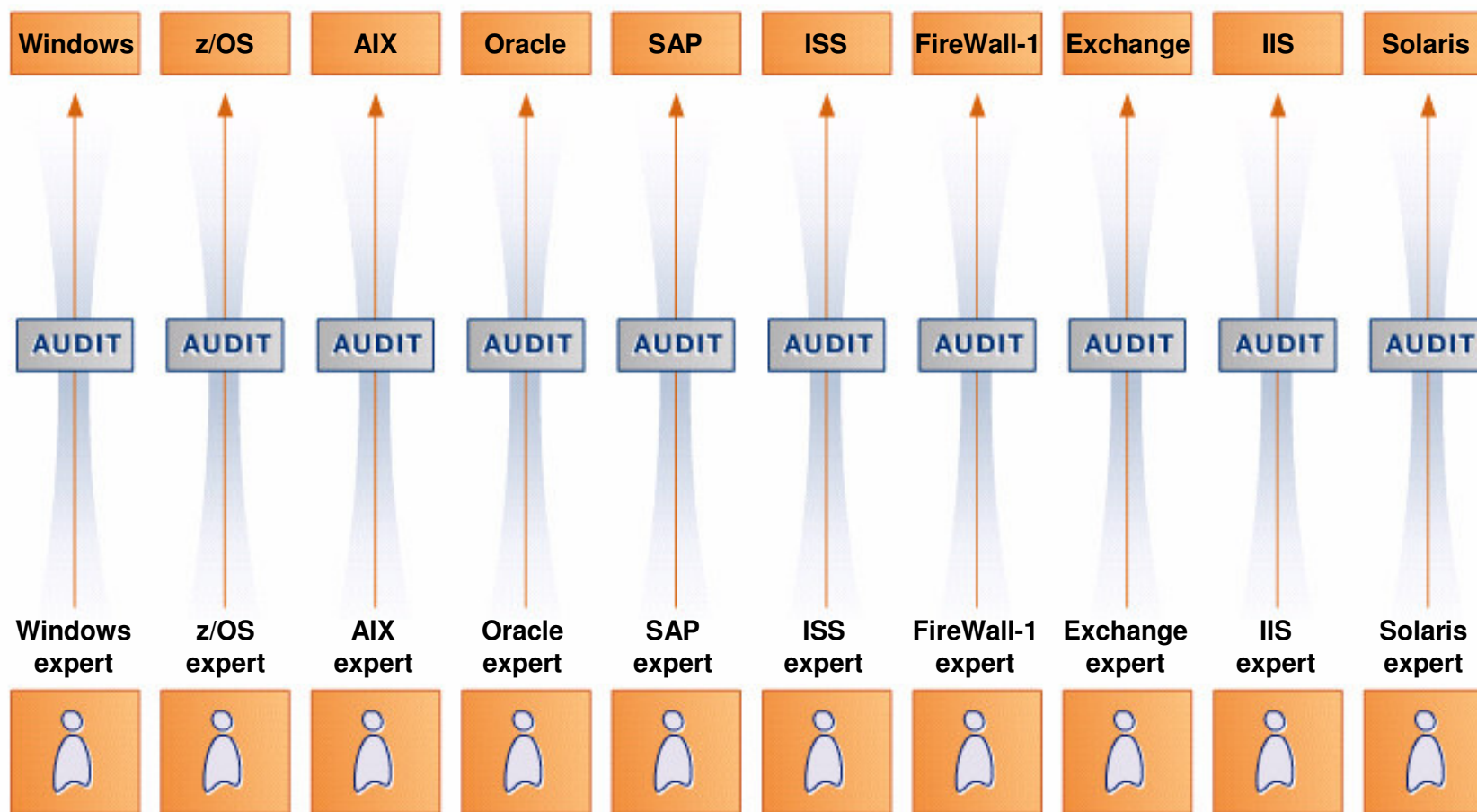
The log viewer also shows a list of system log entries (syslog) for pam_unix, including session closures for user MQM and session openings for user ebarrios.





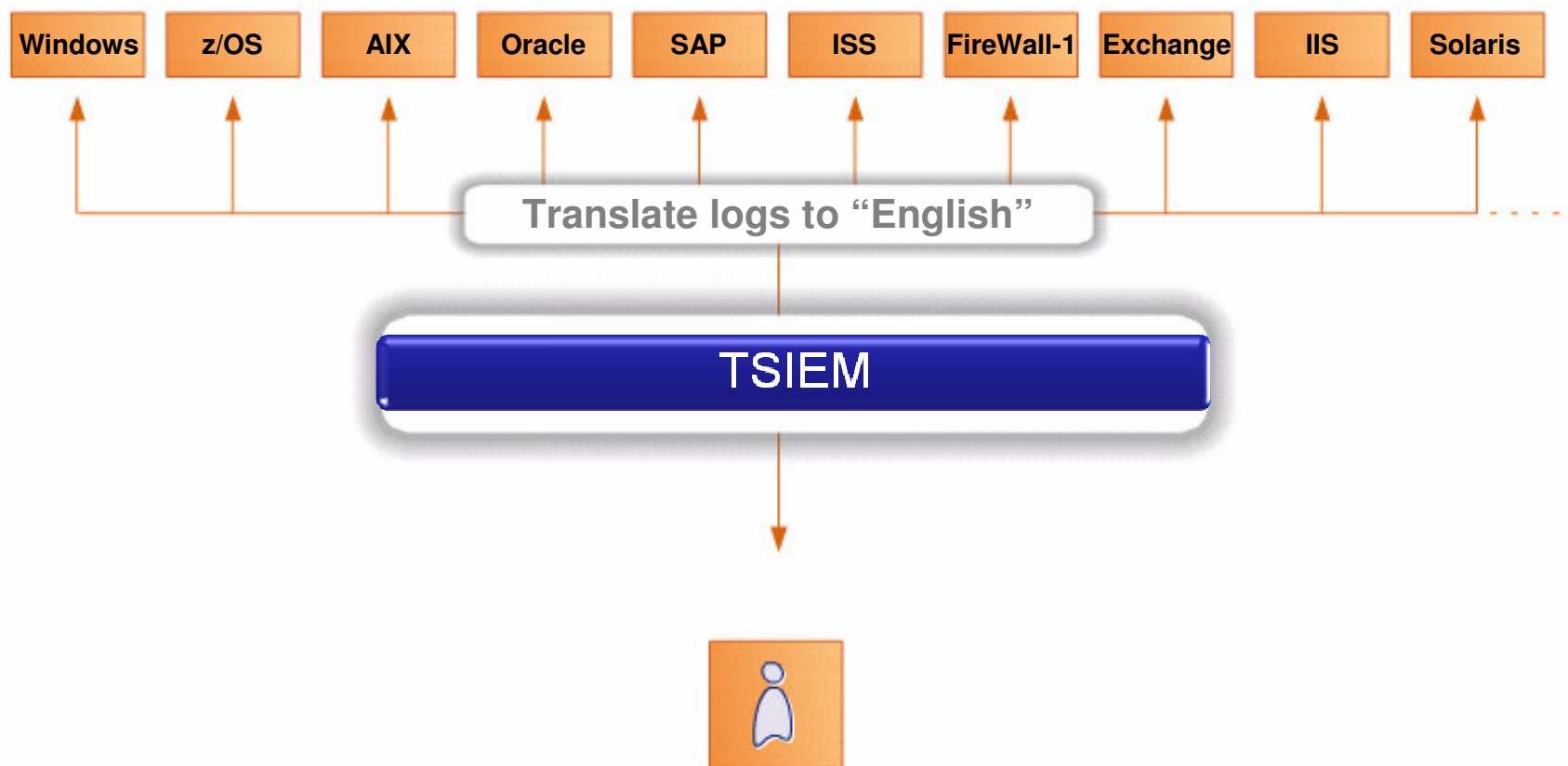
After Log Capture, Translation is Next

Comprehend





Now all Logs in Your Enterprise in a Single Language



Comprehend

TSIEM saves your information security and compliance staff time and money by automating monitoring across the enterprise.



Translate Logs into English IBM Tivoli's W7 Methodology

Comprehend

Who did **What** type of action **on What**?

When did he do it and **Where**, **From Where** and **Where To**?

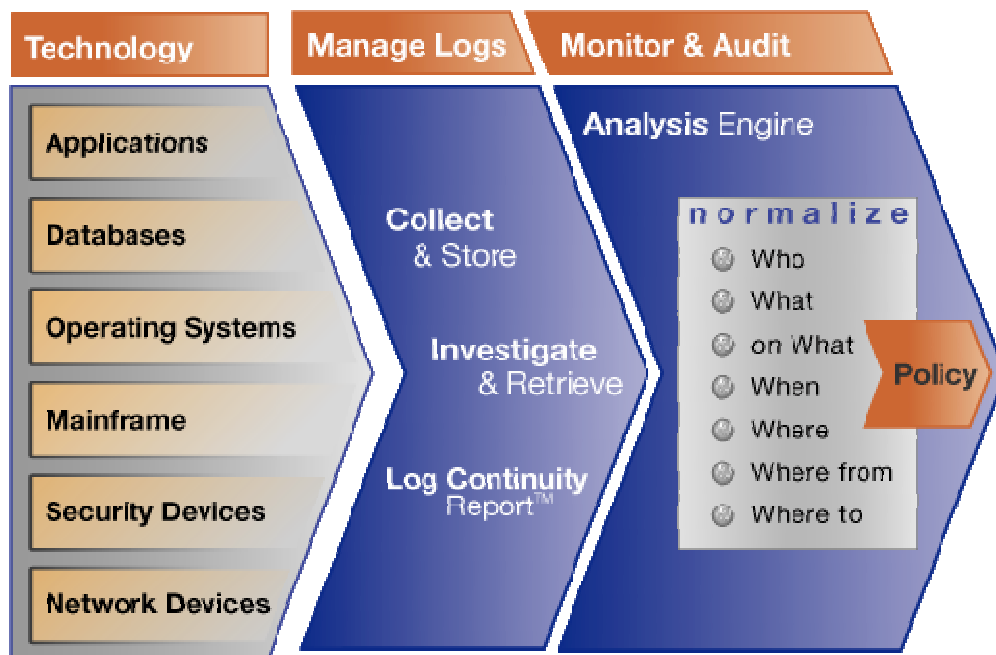
We do the hard work, so you don't have to!!





Sophisticated Log Interpretation and Correlation

Comprehend



Capabilities:

- W7 normalization
- Interpret EVERY log (Syslog and native logs) into English
- Compare billions of log entries to baseline policy

Benefits:

- Interpret and monitor all logs with fewer and less expensive resources
- More quickly detect and solve security problems



Out of the box log normalization!



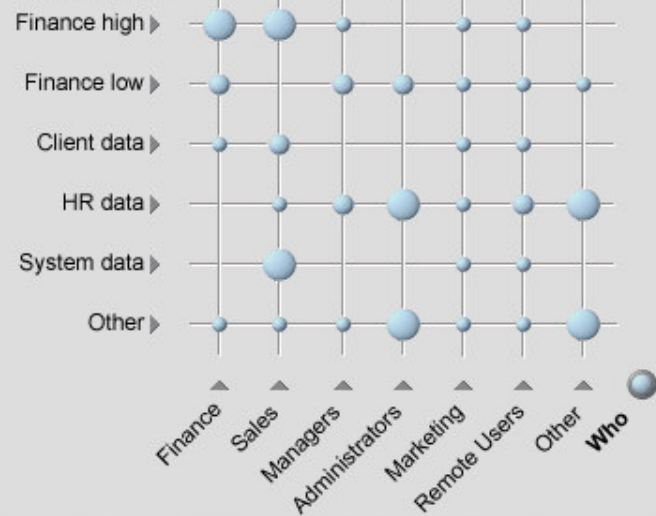
Compliance Dashboard
 Logs after W7 – Billions of log files summarized on one overview graphic!

Compliance Dashboard

Enterprise Overview Settings

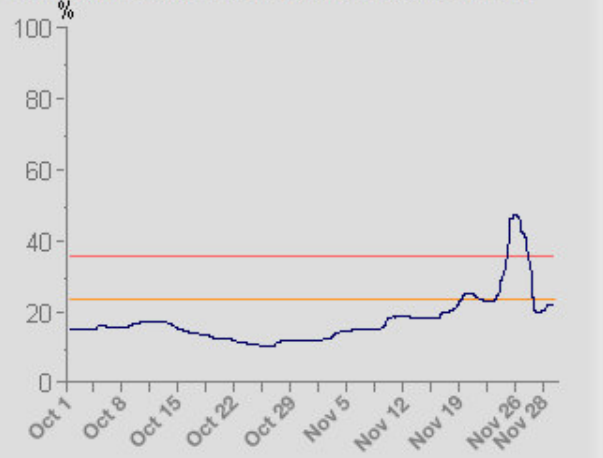
Events by top event count by "on What" and "Who" for Oct 1, 2005 till Nov. 28, 2005.

on What



Trend graphic Settings

Percentage of Exceptions for Oct 1, 2005 till Nov 28, 2005

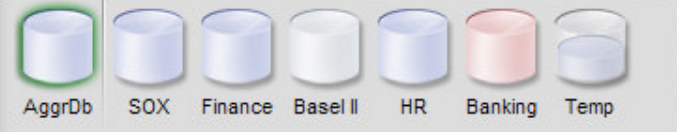


Contact us

In the US:
contactsales@consul.com
 Direct Line: +1 703 675 2022
 Toll Free (US only): 800 258 5077

EMEA and Asia Pac:
contactsales@consul.com
 Direct Line: +31 15 251 3333

Database Overview



Name: AggrDb
 Status: Loaded & Selected
 Loading Date: Nov 29, 2005
 Content: Aggregation of all collected material for the last 90 days.

[Dashboard](#)
[Summary](#)
[Reports](#)
[Policy](#)
[Groups](#)
[Settings](#)
[Regulations](#)
[Portal](#)

[Portal](#) > [Dashboard](#) > [Reports](#) > [Database Top 10 Reports](#) > [Direct Database Access](#)

Direct Database Access Report

> Time period setup

Start time: Month: September, Day: 3, Year: 2006, Hour: 1, Min.: 0
 End time: Month: September, Day: 7, Year: 2006, Hour: 16, Min.: 0
 Execute Reset
 Time zone: Event time zone

> Event List

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 Hofferan	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 Hofferan	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 Hofferan	DB2 Server	DATABASE : - / Unavailable	DB2 Server
50	Sun Sep 03 2006 09:20:01 GMT-05:00	1	Access : Dbobject / Success	DB2 Server	Jim Hofferan	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](#)

W7 Eventlist
 Note!: Mike Bonfire, a DBA,
 is reading the payroll



Agenda

Problems

Solution: TSIEM -- The 3 C's

1. Capture – Enterprise Log Management
2. Comprehend – Sophisticated Log Interpretation
3. Communicate – Full Audit and Compliance Reporting

Technology

Proven Results





You Need Reports to Communicate

Communicate

NetworkWorld 2/7/05

activity

time

The Sarbanes-Oxley Act imposes a heavy burden on IT, but innovative execs are complying with the law and bolstering network security.

Thinking outside the Sarbox





Full Audit and Compliance Reporting

The IBM Tivoli SIEM Solution



Communicate

- Hundreds of reports
- Compliance modules
- Special attention alerts
- Custom reports

- Reduce length and effort required for audits
- Reports in an instant, saving time
- Reduce risk of insider threat:

- Info protection
- Change control
- User management



Compliance Modules

Basel II

[Introduction](#)
[Classification Template](#)
[Policy Template](#)
[Reports](#)
[Documentation](#)

Gramm-Leach-Bliley Act (GLBA)

Health Insurance Portability and Accountability Act (HIPAA)

ISO 17799

[Introduction](#)
[Classification Template](#)
[Policy Template](#)
[Reports](#)
[Documentation](#)

Sarbanes Oxley (SOX)

[Introduction](#)
[Classification Template](#)
[Policy Template](#)
[Reports](#)
[Documentation](#)

consul

Dashboard Summary Reports Policies Groups Settings Regulations Log off

Dashboard > Regulations > Classification Template

Classification Template

Download this template to use in the management Console

Who

What

Group Name	Description
Alerts	Alerts generated by system devices resources
Alerts - High	Alerts generated by system devices resources - High
Alerts - Low	Alerts generated by system devices resources - Low
Alerts - Medium	Alerts generated by system devices resources - Medium
Exposure - High	description of Exposure - High
Exposure - Low	description of Exposure - Low
Exposure - Medium	description of Exposure - Medium
Intrusion - High	description of Intrusion - High
Intrusion - Low	description of Intrusion - Low
Intrusion - Medium	description of Intrusion - Medium
Intrusions	Intrusions reported by IDS devices

on What

When

Group Name	Description
Office Hours	Normal working hours for staff
Out of Office Hours	Out of normal working hours

Extra Information

Help

Contact us

In the US:
contact@consul.com
Direct Line: +1 703 876 2022
Toll Free (US only): 800 258 5077

EMEA and Asia Pac:
contact@consul.com
Direct Line: +31 15 251 3333

consul

Dashboard Summary Reports Policies Groups Settings Regulations Log off

Dashboard > Regulations > Policy Template

Policy Template

Download this template to use in the management Console

Policy Rules

Attention Rules

Who group	What group	When group	Where group	Entity group	From/To group	Where To Group	ID	Severity	Description
HR Management	Intrusion - Medium	Office Hours						30	Review
			Customer Information Systems					50	Requires attention
Administrators				HR - Medium				40	
Administrators				Financial - Medium				50	Requires attention
Administrators				Customer Data - High				50	Requires attention
Administrators				Financial - Low				70	Requires immediate attention
IT				Sensitive				20	Review
Unknown			Customer					25	Review

Extra Information

Help

Please login into the Consul InSight Suite. This will give you access to all the products available with the specific username.

If you forgot your username and/or password please contact your administrator.

Contact us

In the US:
contact@consul.com
Direct Line: +1 703 876 2022
Toll Free (US only): 800 258 5077

EMEA and Asia Pac:
contact@consul.com
Direct Line: +31 15 251 3333

consul

Dashboard Summary Reports Policies Groups Settings Regulations Log off

Dashboard > Regulations > Sarbanes Oxley Regulation Reports

Sarbanes Oxley Regulation Reports

ID	Title	Description
Sarbanes Oxley (FFEC 1.1.4)	Security Policy report	No description given
Sarbanes Oxley (FFEC 1.3.1)	Classification report	No description supplied
Sarbanes Oxley (8.3.8.1.3)	Security alert	Alerts sent in response to policy exceptions or special attention exceptions
Sarbanes Oxley (8.1.2)	Operational change control	Changes to the operating environment such as system updates, O&A activity etc.
Sarbanes Oxley (8.1.6)	External contractors	Exceptions and failures caused by External Contractors
Sarbanes Oxley (8.3)	Malicious attacks	Exceptions and failures due to Malicious attacks
Sarbanes Oxley (8.4.2)	Operator log	Actions performed by the IT Admin staff
Sarbanes Oxley (8.5)	Network management	Actions and events caused by users on Network Services
Sarbanes Oxley (8.7.4.1)	Mail server	Exceptions and failures for the Mail Server assets
Sarbanes Oxley (8.7.6)	Policy available systems	Actions and exceptions on Policy Filtered Data
Sarbanes Oxley (8.2.4.8.7)	Review of user access rights	Actions performed by administrators on users
Sarbanes Oxley (8.2.4.6.9.7)	System access and use	Successes and failures against key assets
Sarbanes Oxley (8.3)	User responsibilities and password use	Login failures and successes either locally or remotely
Sarbanes Oxley (8.4)	Network access control	Actions performed on and events and exceptions generated by Network or Router
Sarbanes Oxley (8.4.4)	Node authentication	Authentication of connections to remote computer systems
Sarbanes Oxley (8.4.5)	Remote diagnostic port access	Detection of accesses to the diagnostic ports on servers
Sarbanes Oxley (8.5.3)	User identification and authentication	Login/Logout successes and failures
Sarbanes Oxley (8.5.5)	System utilities	Usage of system utilities
Sarbanes Oxley (8.6)	Application access control	Actions, Exceptions and events on HR Data, Sensitive Data, User Sensitive Data, System, Financial Data, Proprietary Data and General Data
Sarbanes Oxley (8.6.1)	Information access restrictions	Who accessed sensitive or private data successfully or unsuccessfully
Sarbanes Oxley (8.6.2)	Sensitive system isolation	Exceptions and failures against sensitive systems data in asset groups
Sarbanes Oxley (8.7.3)	Logging and reviewing events	Exceptions and failures recorded by the InSight system
Sarbanes Oxley (8.8.1)	Mobile worker	Exceptions and failures for mobile workers

Extra Information

Help

Please login into the Consul InSight Suite. This will give you access to all the products available with the specific username.

If you forgot your username and/or password please contact your administrator.

Contact us

In the US:
contact@consul.com
Direct Line: +1 703 876 2022
Toll Free (US only): 800 258 5077

EMEA and Asia Pac:
contact@consul.com
Direct Line: +31 15 251 3333

Regulation specific modules with tailored reports to jumpstart your compliance efforts – saving you staff time and reducing audit costs

Sarbanes Oxley Regulation Reports

Title	Description
Sarbanes Oxley (FFIEC 1.1.1.4) Security Policy report	No description given
Sarbanes Oxley (FFIEC 1.3.1.1) Classification report	No description supplied
Sarbanes Oxley (6.3, 8.1.3) Security alert	Alerts sent in response to policy exceptions or special attention exceptions.
Sarbanes Oxley (8.1.2) Operational change control	Changes to the operating environment such as system updates, DBA activity etc.
Sarbanes Oxley (8.1.6) External contractors	Exceptions and failures caused by External Contractors.
Sarbanes Oxley (8.3) Malicious attacks	Exceptions and failures due to Malicious attacks.
Sarbanes Oxley (8.4.2) Operator log	Actions performed by the IT Admin staff.
Sarbanes Oxley (8.5) Network management	Actions and events caused by users on Network Services.
Sarbanes Oxley (8.7.4.1) Mail server	Exceptions and failures for the Mail Server assets.
Sarbanes Oxley (8.7.6) Publicly available systems	Actions and exceptions on Publicly Published Data.
Sarbanes Oxley (9.2.4, 9.7) Review of user access rights	Actions performed by administrators on users.
Sarbanes Oxley (9.2.4.c, 9.7) System access and use	Successes and failures against key assets
Sarbanes Oxley (9.3) User responsibilities and password use	Logon failures and successes either locally or remotely.
Sarbanes Oxley (9.4) Network access control	Actions performed on and events and exceptions generated by Network or Router.
Sarbanes Oxley (9.4.4) Node authentication	Authentication of connections to remote computer systems
Sarbanes Oxley (9.4.5) Remote diagnostic port access	Detection of accesses to the diagnostic ports on servers.
Sarbanes Oxley (9.5.3) User identification and authentication	Logon/Logoff successes and failures.
Sarbanes Oxley (9.5.5) System utilities	Usage of system utilities
Sarbanes Oxley (9.6) Application access control	Actions, Exceptions and events on HR Data, Sensitive Data, User Sensitive Data, System, Financial Data, Proprietary Data and General Data.
Sarbanes Oxley (9.6.1) Information access restrictions	Who accessed sensitive or private data successfully or unsuccessfully.
Sarbanes Oxley (9.6.2) Sensitive system isolation	Exceptions and failures against sensitive systems data in asset groups User, HR Data, Source Code, and Financial Data
Sarbanes Oxley (9.7.2.3) Logging and reviewing events	Exceptions and failures recorded by the InSight system.
Sarbanes Oxley (9.8.1) Mobile worker	Exceptions and failures for mobile workers.

Please login into the Consul InSight Suite. This will give you access to all the products available with this specific username.

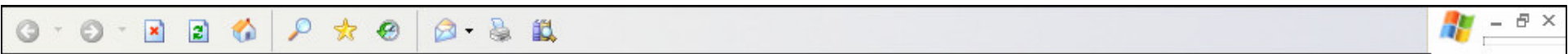
If you forgot your username and/or password please contact your administrator.

Contact us

In the US:
contactsales@consul.com
 Direct Line: +1 703 675 2022
 Toll Free (US only): 800 258 5077

EMEA and Asia Pac:
contactsales@consul.com
 Direct Line: +31 15 251 3333

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



Dashboard > Regulations > Sarbanes Oxley Regulation Reports > Operational Change Control

Operational Change Control of Finance database

Time period setup

Start time: Month: October, Day: 1, Year: 2006, Hour: 0, Min.: 40
 End time: Month: November, Day: 1, Year: 2006, Hour: 0, Min.: 40

Execute Reset

Time zone: GMT-05:00 New_York, Nipigon, Pangnirtung

Summary report

Who group	What group	On What group	Where to group	#Events	#Pol.Excp.	#Spec.Att	#Fail.
Administrators	System Administration	General Data	Finance Server	1256	15	145	12
Administrators	System Operations	Sensitive Data	Finance Server	1352	89	156	0
Administrators	System Updates	Financial Data	Finance Server	1543	154	456	45
FinAdmin Staff	System Updates	Sensitive Data	Finance Server	5644	16	165	0
IT	System Actions	Financial Data	Finance Server	5466	126	14	0
IT	System Operations	Sensitive Data	Mainframe FIN	8836	91	4	0
IT	System Updates	General Data	Mainframe FIN	4875	4	46	2
IT Admin	Authorization Objects	Financial Data	Finance Server	56	88	16	23
IT Admin	System Operations	Sensitive Data	Mainframe FIN	546	189	16	0
IT Admin	System Updates	General Data	Mainframe FIN	5165	48	54	0
Sales	System Actions	Financial Data	Finance Server	78	78	78	0
System	System Actions	Financial Data	Finance Server	15654	6	15	0
System	System Administration	Sensitive Data	Finance Server	546	15	45	0

Usage Help

The system update report shows changes to key system components. This report when used with the incident tracking report allows changes to be monitored and recorded and tracked via an external incident tracking system.

Regulation

Paragraph 8.1.2

Data Selection

This report is based on the following groups:

What DBA Actions,

- System Actions,
- System Administration,
- System Operations,
- System Updates

Contact us

In the US:
contactsales@consul.com
 Direct Line: +1 703 675 2022
 Toll Free (US only): 800 258 5077

EMEA and Asia Pac:
contactsales@consul.com
 Direct Line: +31 15 251 3333

Severity	When	#	What	Where	Who			
2	Tue Oct 24 2006 14:32:44 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	WS_03442 (Windows)	USER : David088 / David088	SRV_DC_034 (Windows)
2	Tue Oct 24 2006 16:09:39 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	WS_03442 (Windows)	USER : David088 / David088	SRV_DC_034 (Windows)
2	Tue Oct 24 2006 16:20:49 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Jim Hofferman	WS_03442 (Windows)	USER : Administrator / Administrator	SRV_DC_034 (Windows)
2	Tue Oct 24 2006 16:20:52 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Jim Hofferman	WS_03442 (Windows)	USER : Administrator / Administrator	SRV_DC_034 (Windows)
2	Sat Oct 28 2006 11:21:26 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Jim Hofferman	SRV_DC_034 (Windows)	USER : Administrator / Administrator	SRV_DC_034 (Windows)
2	Sat Oct 28 2006 11:21:49 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	SRV_DC_034 (Windows)	USER : Unavailable / Unavailable	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:03:02 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Max Doane	SRV_DC_034 (Windows)	USER : Richard019 / Richard019	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:03:02 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Max Doane	SRV_DC_034 (Windows)	USER : Richard019 / Richard019	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:05:01 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Jim Hofferman	SRV_DC_034 (Windows)	USER : Chin055 / Chin055	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:05:01 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Jim Hofferman	SRV_DC_034 (Windows)	USER : Chin055 / Chin055	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:05:01 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Joe Security	SRV_DC_034 (Windows)	USER : Sean031 / Sean031	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:05:01 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Joe Security	SRV_DC_034 (Windows)	USER : Sean031 / Sean031	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:10:00 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	SRV_DC_034 (Windows)	USER : Rick053 / Rick053	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:10:00 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	SRV_DC_034 (Windows)	USER : Rick053 / Rick053	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:30:00 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	SRV_DC_034 (Windows)	USER : Ralph037 / Ralph037	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:30:00 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	SRV_DC_034	USER : Ralph037 /	SRV_DC_034

Event List
 Zoom in into the all actions that IT admin did on the financial Server and see the creation of the user account of Chin055

[Dashboard](#)
[Summary](#)
[Reports](#)
[Policy](#)
[Groups](#)
[Settings](#)
[Regulations](#)
[Portal](#)

Portal > Dashboard > Regulations > Sarbanes Oxley > Operational Change Report > Eventlist > Event-detail

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 Hofferan	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 (+/-)

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

Filter by Platform: SRV_DC_034 (Windows)

Filter by User: Jim Hofferan

Investigate

Logrecords...

Contact us

In the US:
contactsales@consul.com
 Direct Line: +1 703 675 2022
 Toll Free (US only): 800 258 5077

EMEA and Asia Pac:
contactsales@consul.com
 Direct Line: +31 15 251 3333

An Event Detail Report
 Even drill down into that specific event and see all the event details, and we can even go to the raw log-file



IBM TSOM – Real-Time Correlation and Monitoring

IBM Tivoli Security Operations Manager (TSOM) is a real-time security information and event management (SIEM) platform designed to improve the effectiveness and efficiency of security operations and information risk management. TSOM centralizes and stores security data from throughout the heterogeneous technology infrastructure so that security analysts can:

Key Features

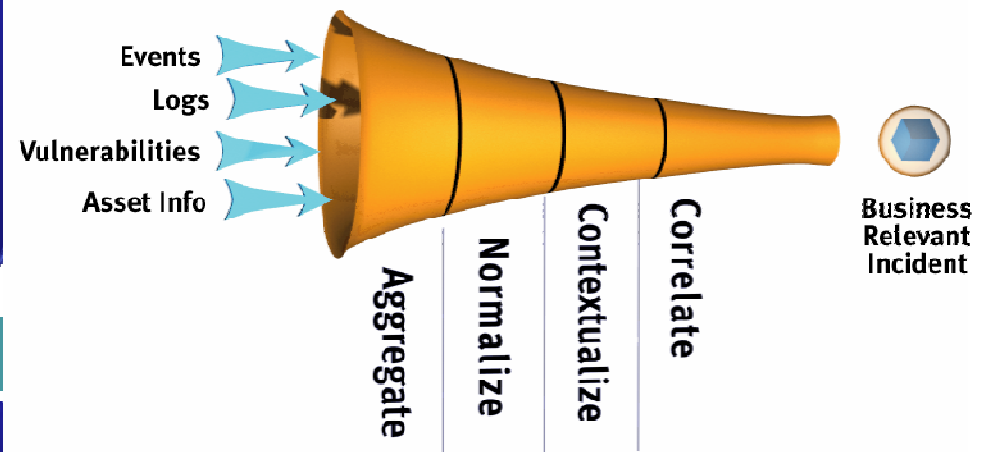
Log Management - automated aggregation of security events and audit logs

Correlation - Real-time, cross-device event correlation for incident management and investigation

Regulatory Compliance – reporting and policy monitoring to support regulatory compliance initiatives

Maximize and amplify security operations resources through automation

Integrates Security Operations with other IT Operations groups via Netcool and TEC



"TSOM automates the aggregation and correlation process. It mitigates false positives and alerts my team to real threats in a timely manner. The product is more or less what I would have designed and built myself, given four years and a pool of developers." ~ Communications User of TSOM



Consolidated View via TSOM Customizable Dashboard

Address: http://10.0.1.28/main.phtml

neUSECURE [dhcp-10-0-1-]

Dashboard Reports Tools Options Admin

Visuals Window Help

Security Domain Threats

Domain	Low	Medium	High
Headquarters - ATL	6	3	2
Finance, Accounting	0	0	1
unassigned	2	3	0
EMEA Operations - UK	0	1	0

Top Destinations

Host	Domain	Wat...	Threat L...	Threat	Events / ...
172.16.201.21	Headquarters - ATL	[Pattern]	High	42,189	1,467 ▲
172.16.201.20	Headquarters - ATL	[Pattern]	High	37,443	1,433 ▲
67.118.26.188	Finance, Accounting	[Pattern]	High	29,167	0,167 ▲
67.118.26.190	Headquarters - ATL	[Pattern]	Medium	22,727	0,333 ▲
172.16.0.10	Headquarters - ATL	[Pattern]	Medium	19,375	0,233 ▲
216.239.37.104			Medium	16,667	0,067 ▲
216.239.41.104			Medium	16,667	0,067 ▲
216.239.57.104			Medium	16,667	0,067 ▲
10.0.0.40	EMEA Operations ...		Medium	16,377	4,433 ▲
172.16.201.100	Headquarters - ATL	[Pattern]	Medium	15,984	1,033 ▲
172.16.0.21	Headquarters - ATL	[Pattern]	Low	13,75	0,1 ▲
172.16.0.22	Headquarters - ATL	[Pattern]	Low	13,75	0,1 ▲
210.13.19.11		[Pattern]	Low	12,5	0,033 ▲

Orthographic

Watchlist Events

Chart Style: SUPERIMPOSED BAR

PowerGrid

Count	Type	Event Class	Src Threat	Dst Threat	Sensor Name	Sensor Type	Protocol	Src IP	Dst IP	Src Port	Dst Port	Domain
51	Permit	traffic.accept	33	33	Finance.Accou	Netscreen	▲					
35	LOGON/LOGOFF_AUDIT_SUC	0	33	33	MFG.PDC	Windows Even	0	0.0.0.0	10.0.0.0	0	0	Manu...
28	Meta:(Unauthorized Perimet	policy.violation	100	100								
22	drop	traffic.reject	5	5	Atlanta.Perimet	Checkpoint Fi	▲					
17	PRIVILEGE_USE_AUDIT_SUCCE	0	33	33	MFG.PDC	Windows Even	0	0.0.0.0	10.0.0.0	0	0	Manu...
14	Meta:(Dangerous Perimeter	policy.violation	100	100	Atlanta.Perimet	Checkpoint Fi	▲					
12	PORTSCAN	60006	50	50	Finance.Accou	Snort 1.9.1	6 (TCP)	67.118				
5	authcrypt	user	0	0	Atlanta.Perimet	Checkpoint Fi	▲					

Event Class Activity

Chart Style: SUPERIMPOSED BAR



Agenda

Problems

Solution: TSIEM-- The 3 C's

1. Capture – Enterprise Log Management
2. Comprehend – Sophisticated Log Interpretation
3. Communicate – Full Audit and Compliance Reporting

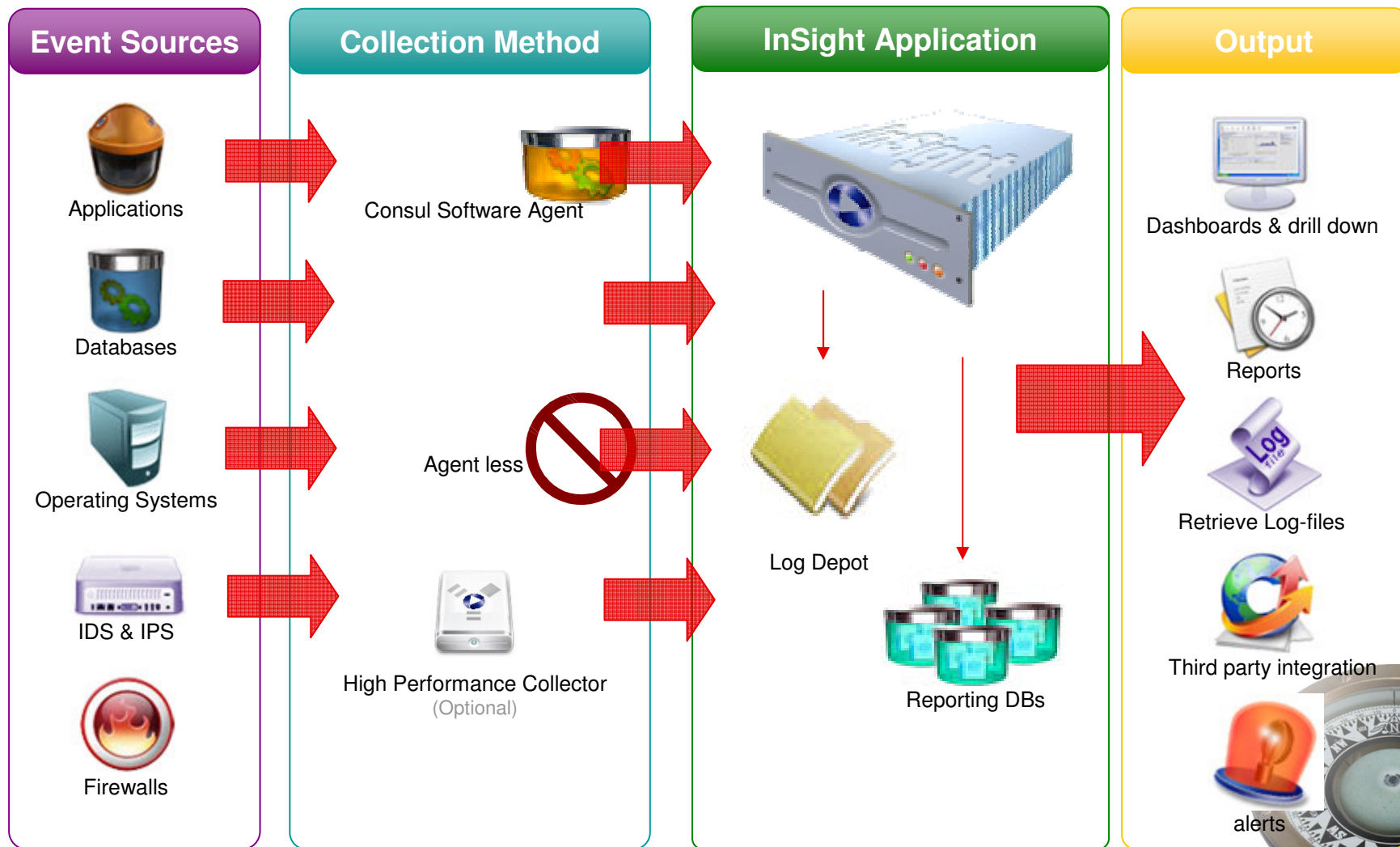
Technology

Proven Results





Architecture





Agenda

Problems

Solution: TSIEM

1. Capture – Enterprise Log Management
2. Comprehend – Sophisticated Log Interpretation
3. Communicate – Full Audit and Compliance Reporting

Technology

Proven Results





Customers Turn to TSIEM

Multinational Insurance Company

To close compliance gaps for SOX; centralize collection, monitoring, and reporting of millions of log files; and provide transparency into the activities of privileged users across a heterogeneous network.

Major US Payment Processor

To prepare for federal regulations and to meet the requirements of the VISA CISP, this large payment processor brought Consul onboard to help audit enterprise IT.

Major Office Supplies Store

The Manager of Data Security began looking for a solution to audit their entire enterprise IT environment.

Large US Grocery Chain

Needed IT audit solution they could roll-out across the corporate network to audit AIX, mainframe, UNIX, Windows and OS/400, and then to 2,500 stores.

Industrial Cleaning Firm

In order to meet SOX requirements and IT Security best practices, the Director of IT Security began looking for a product that could help them manage their log data.

Major Office Equipment Manufacturer

Company received a mandate from their CEO to comply with federal regulatory requirements, specifically Sarbanes-Oxley

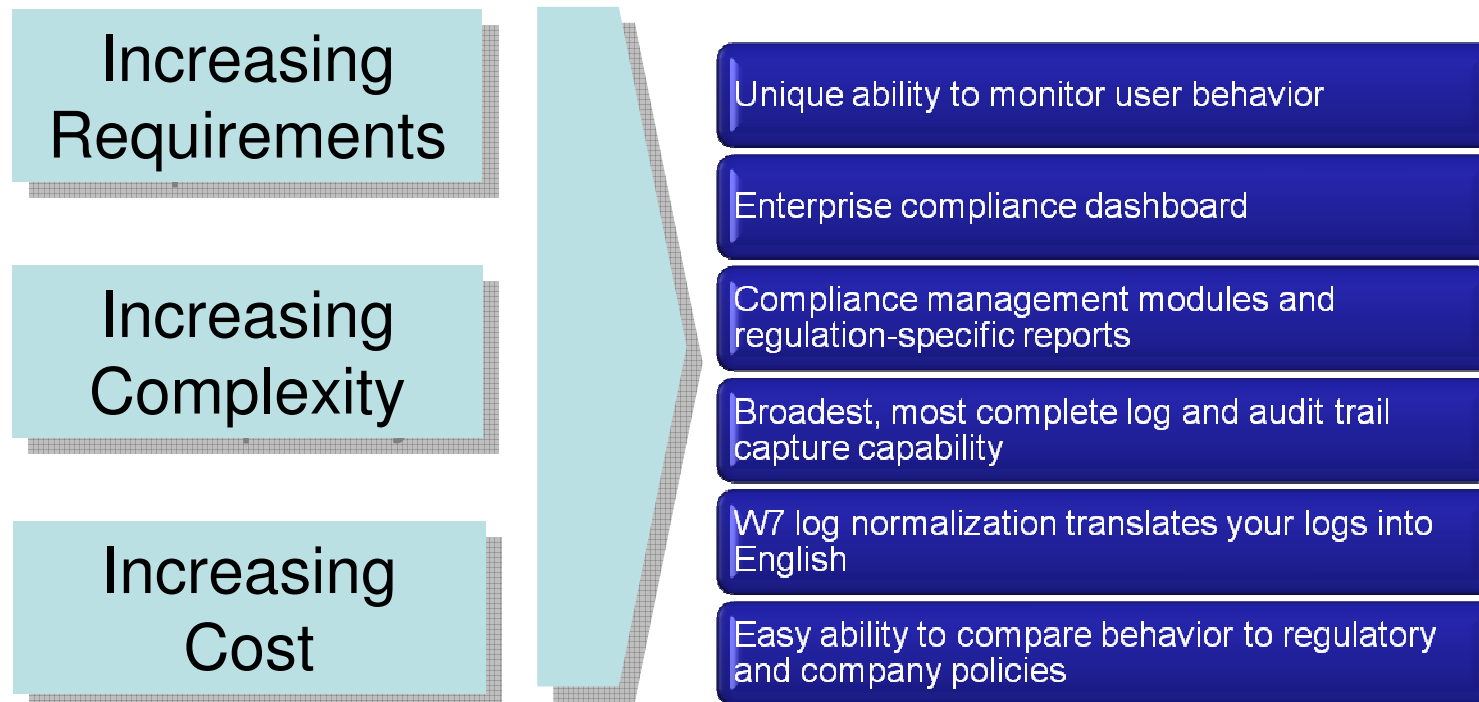
Global Food Manufacturer

IT Security team driven by requirements given to them by Internal Auditors to meet Sarbanes-Oxley requirements





The TSIEM Difference





 What makes you special?

Tivoli Security Information & Event Management



IBM Governance and Risk Management 
Business alignment, visibility and control