



IBM Software Group

Consul InSight Overview

Evento Audit & Risk Management
Hotel Flora, Roma, 10 Maggio 2007



Monica Galiano
Tivoli Security Pre-Sales
Monica_galiano@it.ibm.com
IBM Software Group

Security and compliance challenges

- **Increasing Requirements**
 - Hundreds of compliance initiatives
 - Compliance requirements are increasing in many industries
 - Improved monitoring and control are needed to manage risks and avoid penalties, and lost business
- **Increasing Complexity**
 - Disparate technologies and infrastructures fragment and hamper compliance efforts
 - Linking infrastructure-level to business-level compliance is desirable, but challenging
- **Increasing Cost**
 - Lack of predictability and visibility across complex infrastructures drives rapid cost inflation
 - Failure to achieve compliance or to prevent security breaches can impose enormous costs



- **43% of CFOs think that improving governance, controls and risk management is their top challenge.**

*CFO Survey: Current state & future direction,
IBM Business Consulting Services*

The Business Cost Of Poor Governance & Risk Management Can Be Staggering

January 29, 2007 03:00 PM

TJX Stored Customer Data, Violated Visa Payment Rules The company held on too long to cardholder data... **InformationWeek**
By: Larry Greenemeier

Bacs system failure hits 400,000 salary payments Up to 400,000 people will receive their salary three days late because the Bacs payment processing system - used by every bank in the UK - experienced a failure on Wednesday. By Will Hadfield Friday 20 March 2007

ComputerWeekly.com

FBI loses 3-4 laptops a month, auditor says

AP Associated Press

February 12, 2007

BusinessWeek Sidestepping Disaster; Raynor argues for a governance structure that will allow for safer growth by Dean Foust March 19, 2007

CIO

Telstra's \$11M Network and IT Overhaul in Trouble February 14, 2007 — **CIO** — Australian telecommunications giant Telstra is struggling to successfully upgrade its IT infrastructure...

IT glitch 'could hit elections' Burnley Council says problems could be nationwide IT problems could cause disruption for more than 100 councils at May's local elections, the BBC has learned.
March 27, 2007, BBC Staff Writer

BBC NEWS

Bill Would Punish Retailers For Leaks of Personal Data by Joseph Pereira (February 22, 2007)

THE WALL STREET JOURNAL

February 15, 2007
Massive Insider Breach At DuPont A research chemist who worked for DuPont for 10 years before accepting a job with a competitor downloaded 22,000 sensitive documents and viewed 16,706 more in the company's electronic library.
By: Larry Greenemeier

EETIMES ONLINE

Head Of Nuclear Agency Leaving Under Pressure Over Security Lapses

AP Press Release, January 5, 2007

USA TODAY

abc NEWS

iTunes back to normal after holiday traffic quadruples
ABC News: December 28, 2006

The Top Five I.T. Control Weaknesses



JULY 1, 2005 | CIO MAGAZINE

The Top Five I.T. Control Weaknesses

Auditors saw the same problems over and over. Here they are, in order of frequency.

BY BEN WORTHEN

The screenshot shows an advertisement for Hitachi with the text "Your data is the ruler of the underworld." and "We're inspired by the human side of data." Below the ad, the article text is partially visible and redacted with grey boxes. Arrows point from these redactions to callout boxes on the right.

was the biggest. Most companies didn't have processes in place to make sure that when people switched divisions, their access to applications changed to reflect their new responsibilities. The CIOs interviewed for this article all reported establishing manual controls to address this problem for the first audit. Even Microsoft.

most changes to an application. But in order to pass the IT audit, CIOs had to appoint a person to make a change and another to perform quality assurance on it. And it had to be demonstrated that this procedure was being followed.

most CIOs assigned someone to review their systems were running smoothly. But with Sarbanes-Oxley, just performing the check no longer cuts it; you have to prove that it was done. In other words, you have to create an audit log of your audit log.

this is a classic IT problem that can often be fixed by making changes to the application so that it notifies you when there is a transaction that doesn't conform to preestablished rules.

it turned out that many IT departments weren't as smart as they thought they were. The solution to this weakness is simple: better training.

Failure to segregate duties within applications, and failure to set up new accounts and terminate old ones in a timely manner

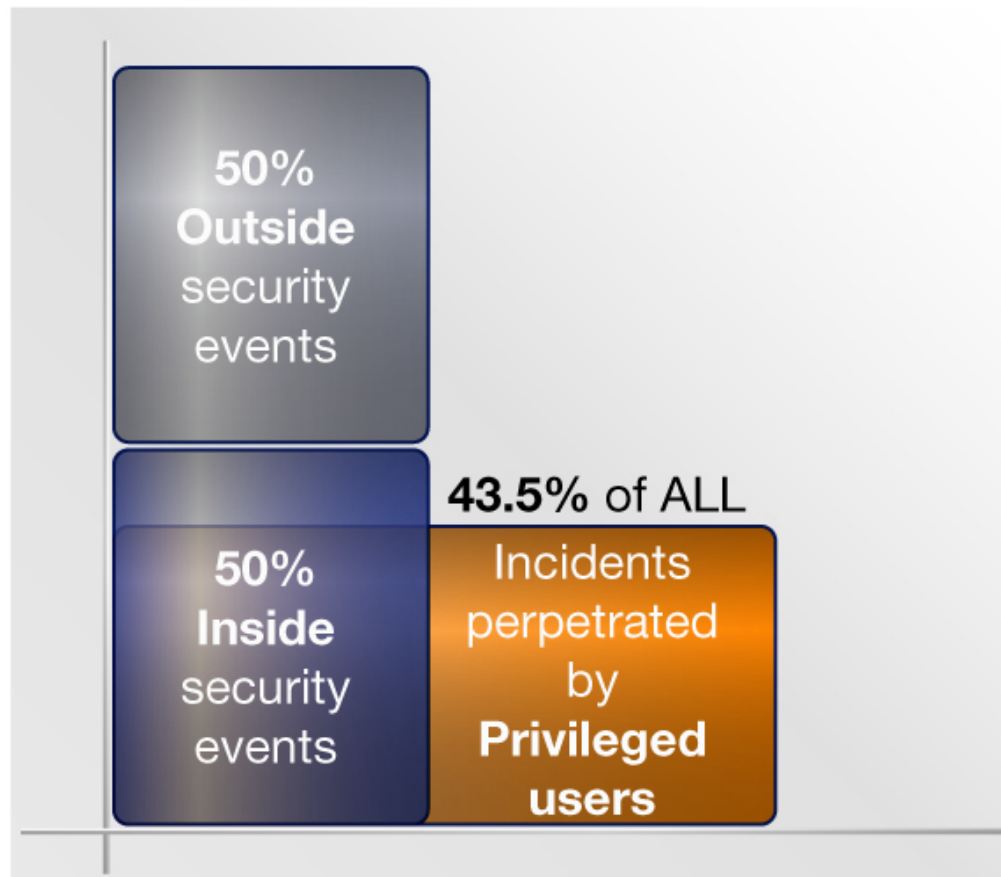
Lack of proper oversight for making application changes

Inadequate review of audit logs

Failure to identify abnormal transactions in a timely manner

Lack of understanding of key system configurations

Insider attacks are almost always privileged



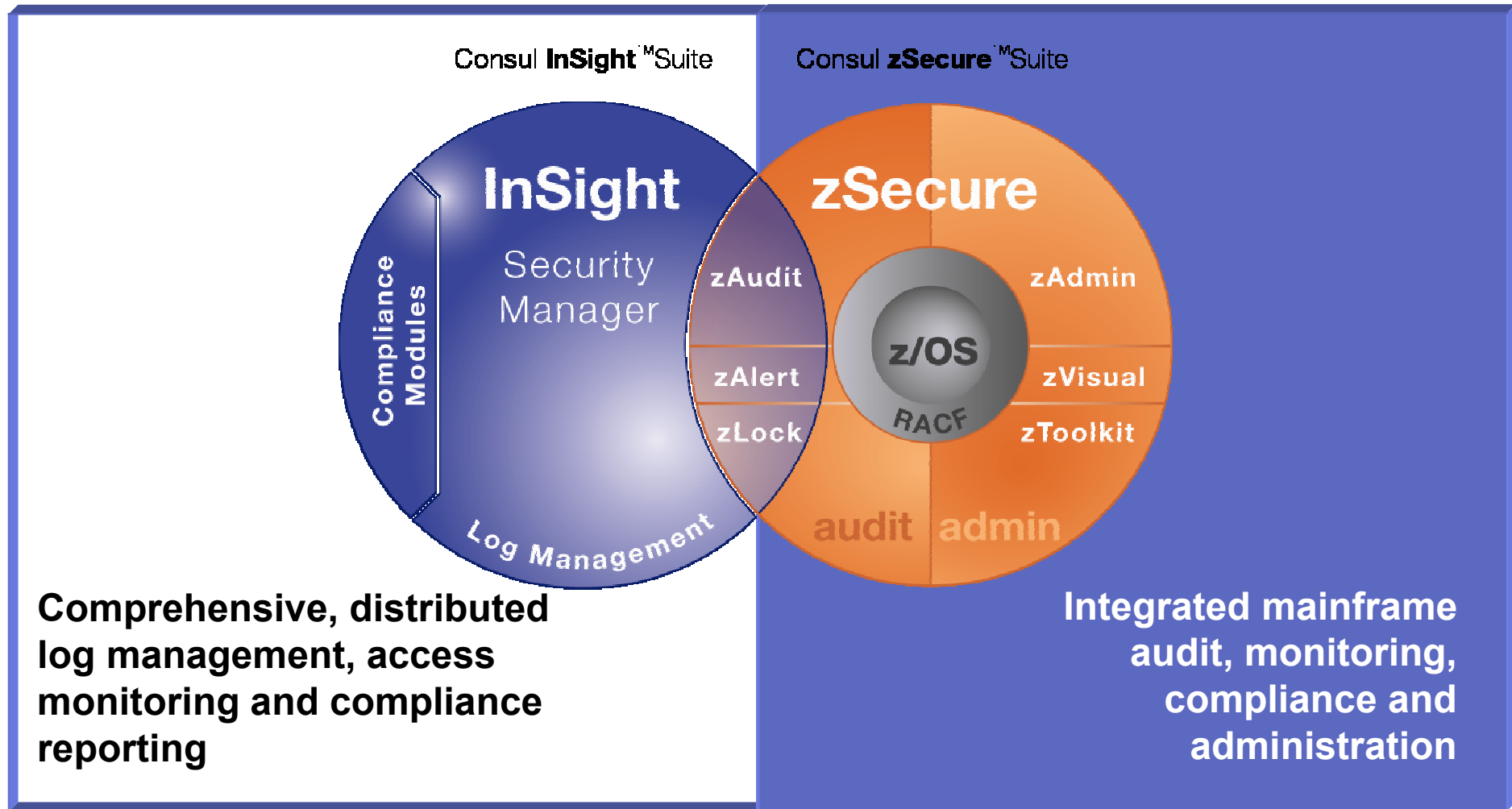
SUMMARY:

- The number of attacks attributed to the inside vs. outside is approximately equal (Source: CSI/FBI Survey 2005)
- 87% of all “insider attacks” can be attributed to the privileged user (Source: USSS/CERT Insider Threat Survey 2005)
- Therefore, 43.5% of the total number of security incidents experienced globally can be attributed directly to the privileged user group.
- *The privileged user group generally represents < 5% of any given organization.*

What is relevant ?

Category	Description
Authentication events	Includes logon / logoff events
Operational events	Server start, stop, back-up, restore
Change management	Configuration changes, audit settings changes, database structure changes, maintenance activities
User and privilege mgt	New users, changes to user privileges, password changes
Privileged user access	All DBA behavior, including data access, DBCC, stored procedure calls
Sensitive data access	Includes all user access to sensitive data stored in the database: selects, inserts, updates, deletes

Consul's Portfolio: Consul InSight Suite

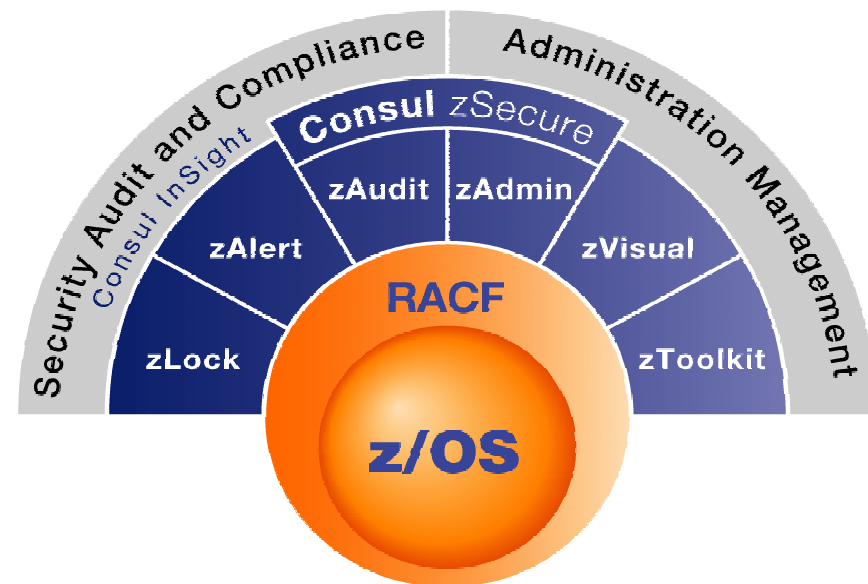


zSecure Suite

The Consul zSecure Suite adds a user-friendly layer onto the mainframe that enables superior administration coupled with audit, alert and monitoring capabilities for z/OS Resource Access Control Facility (RACF)

Key Features

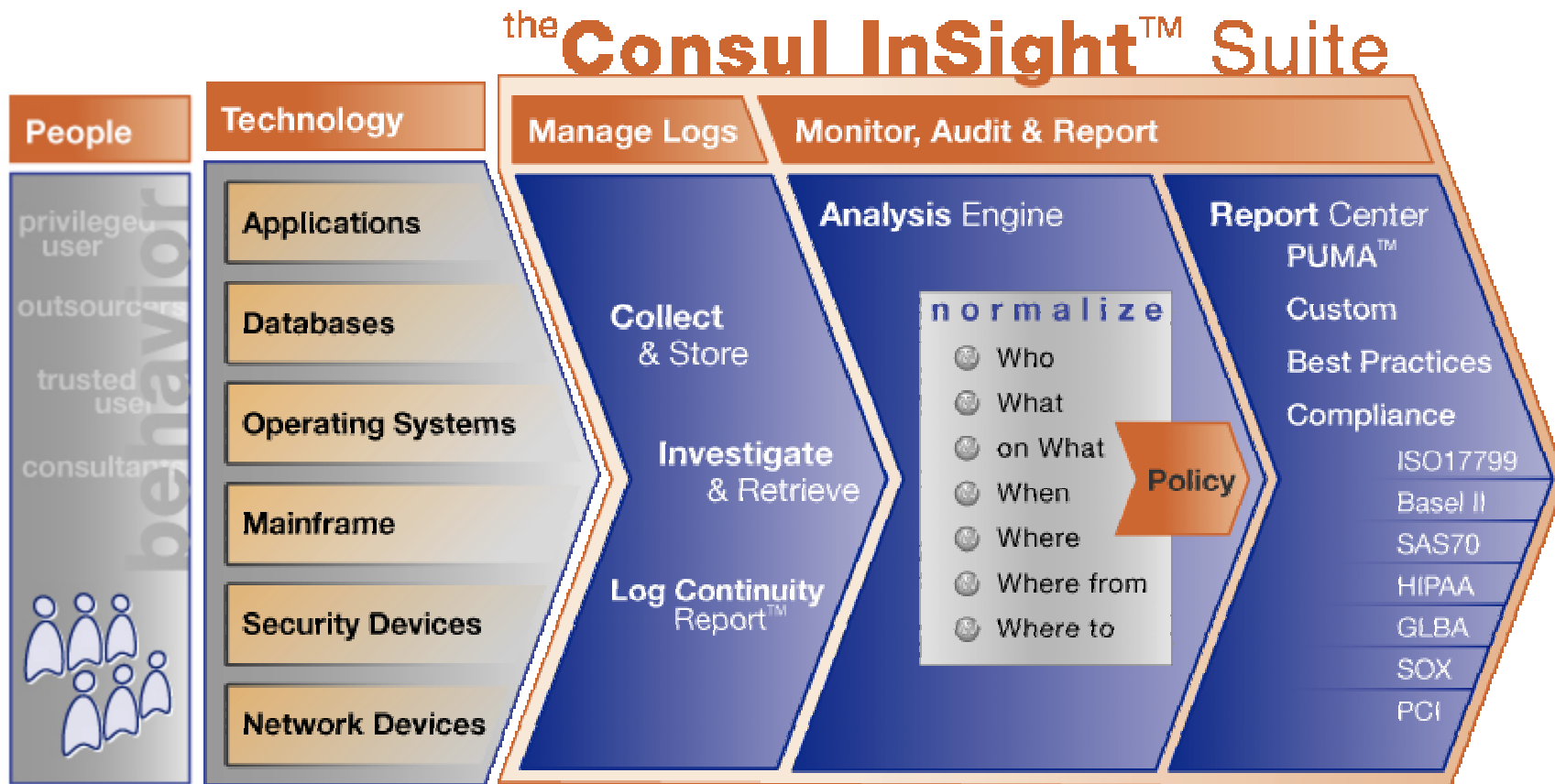
- The zSecure suite improves mainframe security, improves the efficiency of administration and enhances the ability for the mainframe to be the hub of enterprise security.
- **Administration and provisioning:**
 - zAdmin enhances security administration and user management for RACF
 - zVisual offers a Windows GUI to RACF
 - zToolkit for Extensibility with CICS support
- **Audit, monitoring and compliance:**
 - zLock offers automated security monitoring, protection
 - zAlert provides intrusion detection and alerting.
 - zAudit provides event detection, analysis & reporting and system integrity audit & analysis



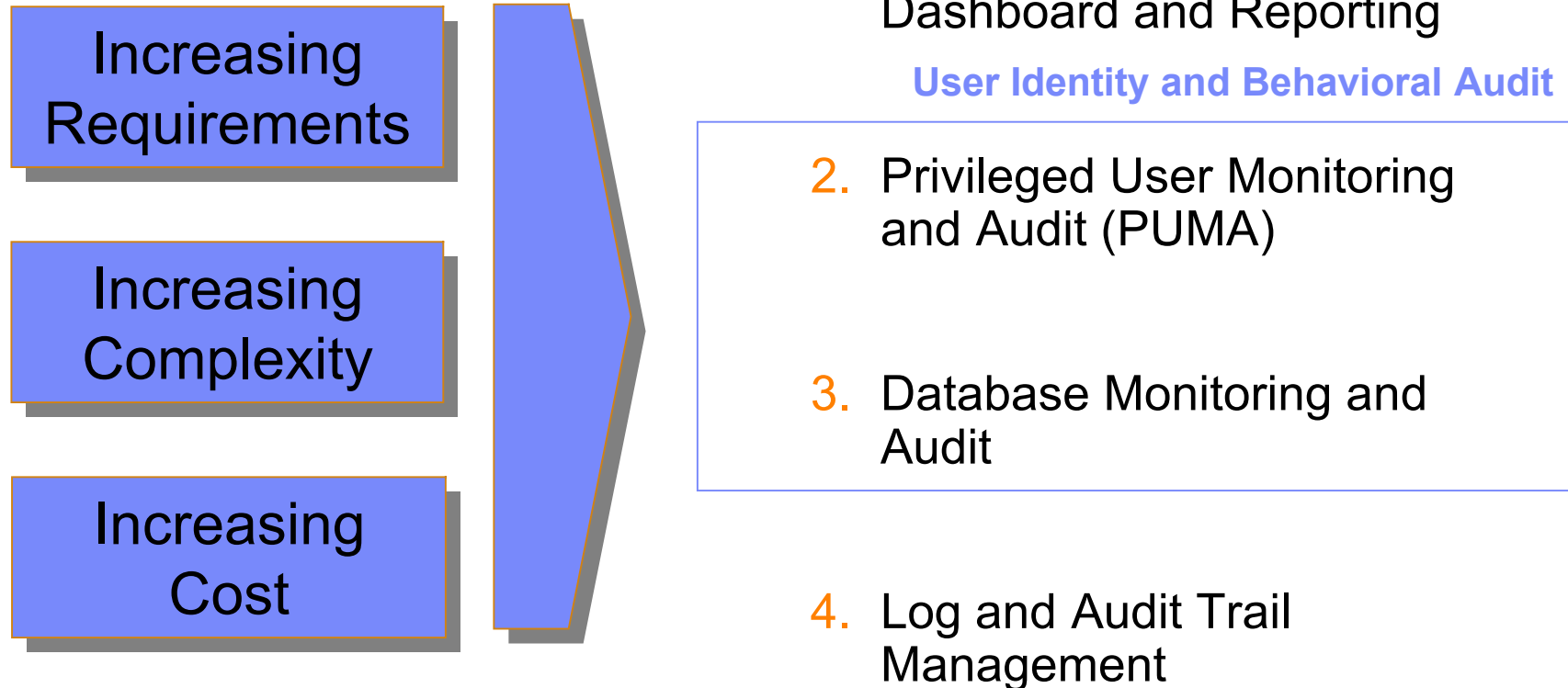
Benefits Summary

- **Administration and provisioning:**
 - Reduce administration time, effort and cost
 - Enable de-central administration
 - Quick response time, enabling business
 - Reduce training time needed for new administrators
- **Audit, monitoring and compliance:**
 - Pass audits more easily, improve security posture
 - Save time and costs through improved security and incident handling
 - Increase operational effectiveness

Consul InSight Suite



More Specifically, Challenges InSight can Help



Questions the auditor will ask

- **Breach of privacy:**

- Are DBAs accessing confidential information?
- Are trusted users abusing HR data?
- Did a disgruntled administrator engage in identity theft?

- **Violation of system policies:**

- Were unauthorized system changes made?
- Did any root users turn off auditing?
- When did OS administrators clear the audit logs?
- Who stopped key system processes without permission?

- **Administrators violating segregation of duties:**

- Did anyone initiate and approve transactions on applications?
- Did an admin create and approve identity/privileges in system?

InSight – Portal Access



Portal

Log Off 0m

Consul InSight™ Suite Portal

Consul InSight™ Security Manager

	iView	The reporting tool with drill down possibilities
	Log Manager	The reporting tool for log management
	Policy Generator	A wizard that will help you start using Consul InSight Security Manager by creating a policy (= policy-rules and grouping) by using collected data from your own devices
	Scoping	Tool to manage the viewable acces of different users of the system to different sets of data

Consul InSight™ Compliance Management Modules

	Basel II	The compliance entrance for Basel II
	GLBA	The compliance entrance for GLBA
	HIPAA	The compliance entrance for HIPAA
	ISO17799	The compliance entrance for ISO17799
	Sarbanes-Oxley	The compliance entrance for Sarbanes Oxley

Consul InSight™ Suite
version 7.0

Extra Information

Help ▾

This page is a single sign-on entrance to installed InSight™ components.

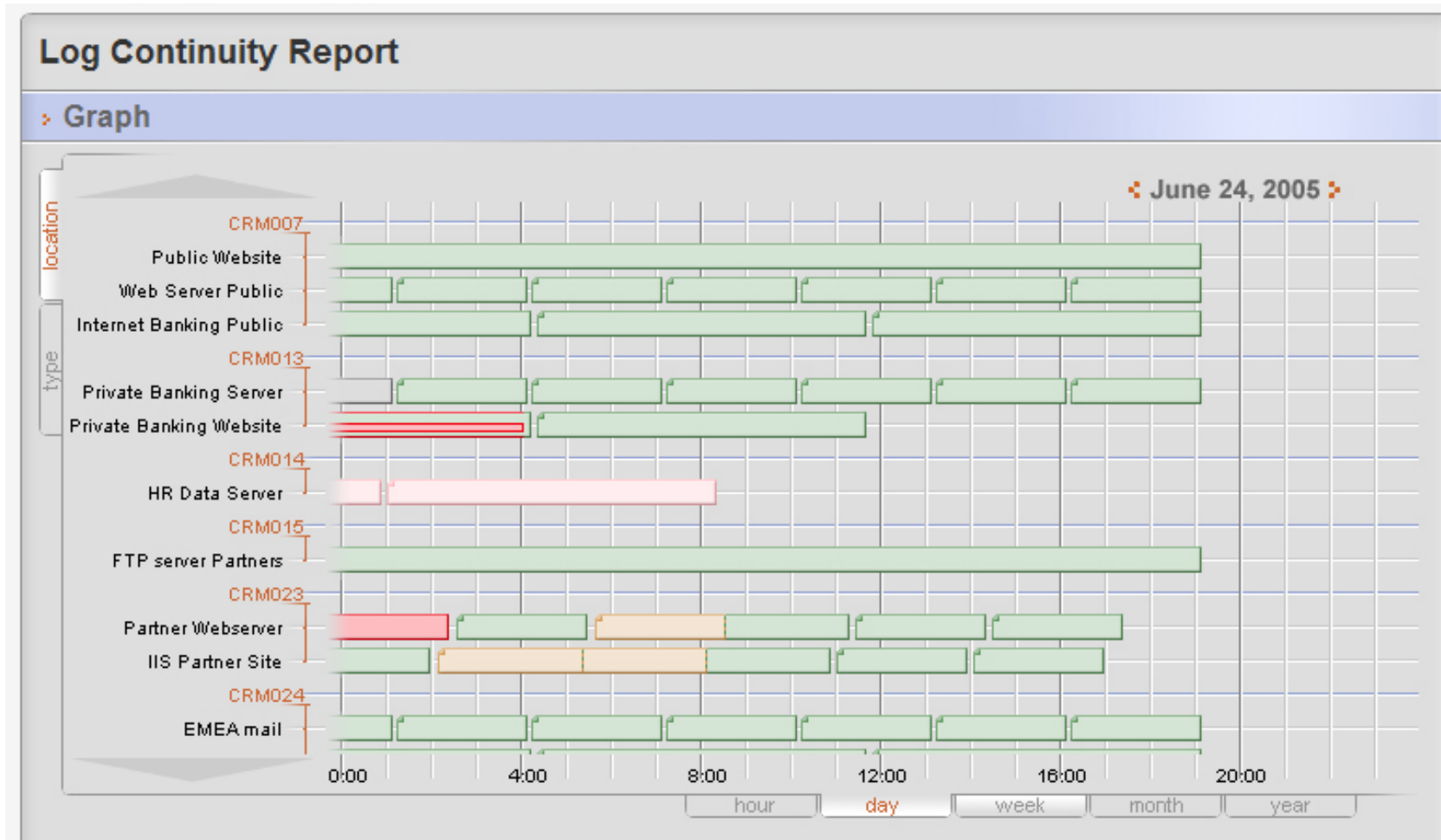
Section Consul InSight™ Security Manager contains links to the principal components of the InSight Suite.

Section Consul InSight™ Compliance Management Modules contains links to the InSight Suite Compliance Management Modules, tailored to help you meet SOX, GLBA, HIPAA and ISO 17799 requirements.

Click the corresponding link to login to a component. InSight™ components can be protected by InSight™ roles.

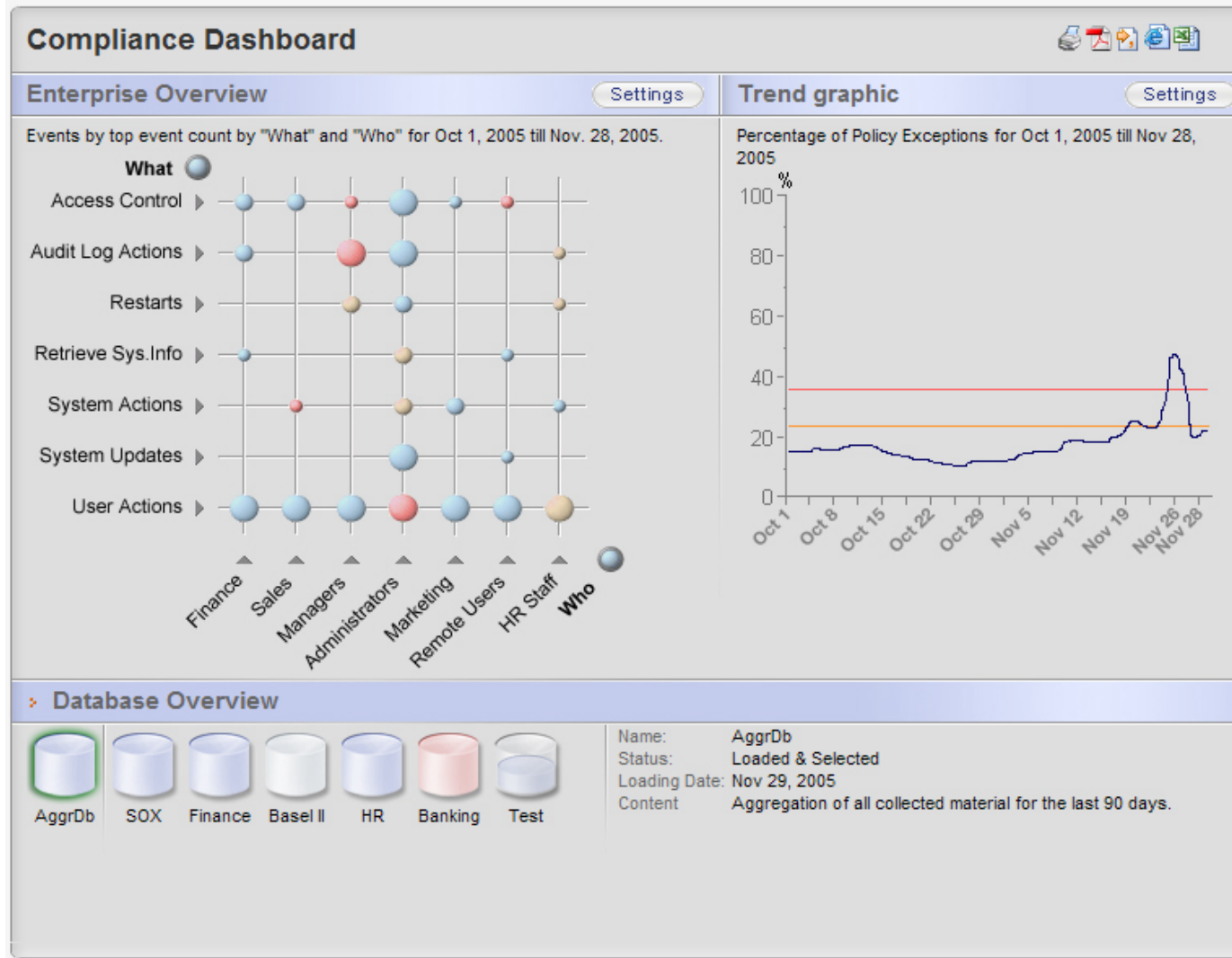
Support ▸

InSight - Log Management



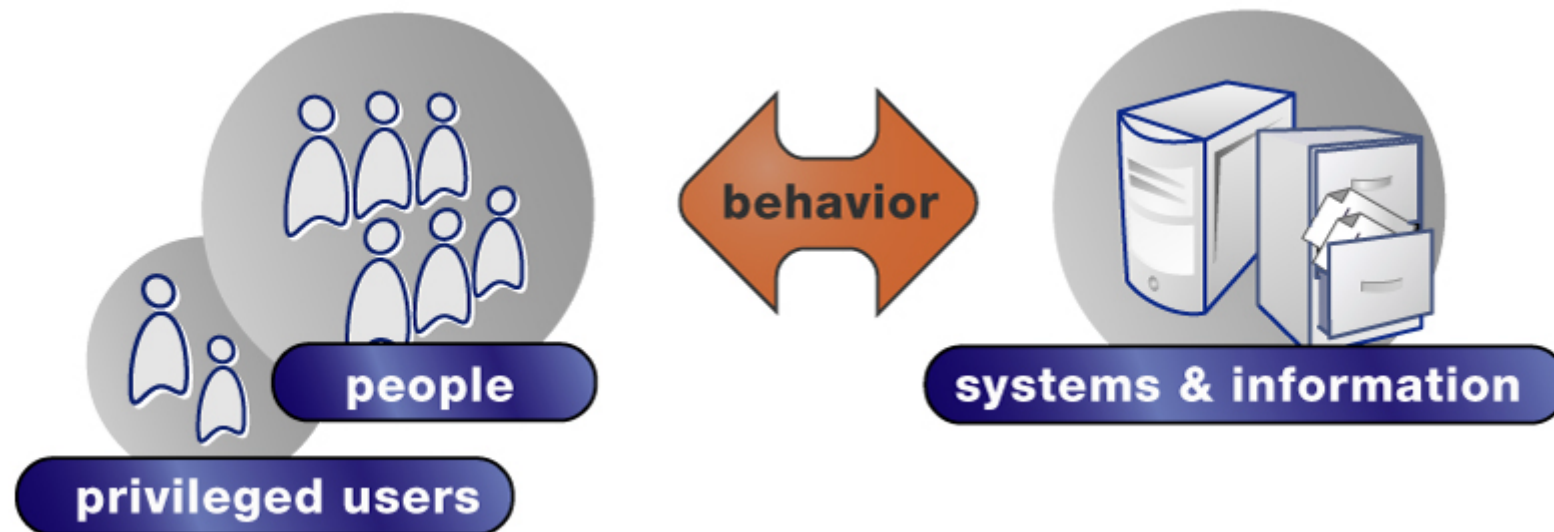
“Prove continuous collection from all monitored event sources”

InSight - Monitor/Report using Compliance Dashboard



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

What are People Doing on My Network?



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

The Consul InSight Suite: Audit users as they access systems and information



People:

- Privileged users
- Outsourcers
- Consultants

Behavior:

- Mistakes, human error
- Sabotage of data or systems
- Theft/release of information assets
- Introduction of bad code
- Installation of unauthorized software

Systems and Information:

- Applications
- Databases
- OS's
- Mainframes
- Devices
- Customer data
- Patient files
- Financial info
- HR record

These actions may result in lengthy outages, lost business, lost customers, legal liability or audit deficiencies – at cost of 6% of annual revenue.

How do I make sense of all this?

The image displays two windows from a security audit tool. The left window shows a log of system events, including authentication failures and session closures for various users. The right window shows detailed security audit information for three different systems: APPLES, CYGNUS, and another instance of CYGNUS. Red boxes and arrows highlight specific fields like 'Process name' and 'Image name' across different entries.

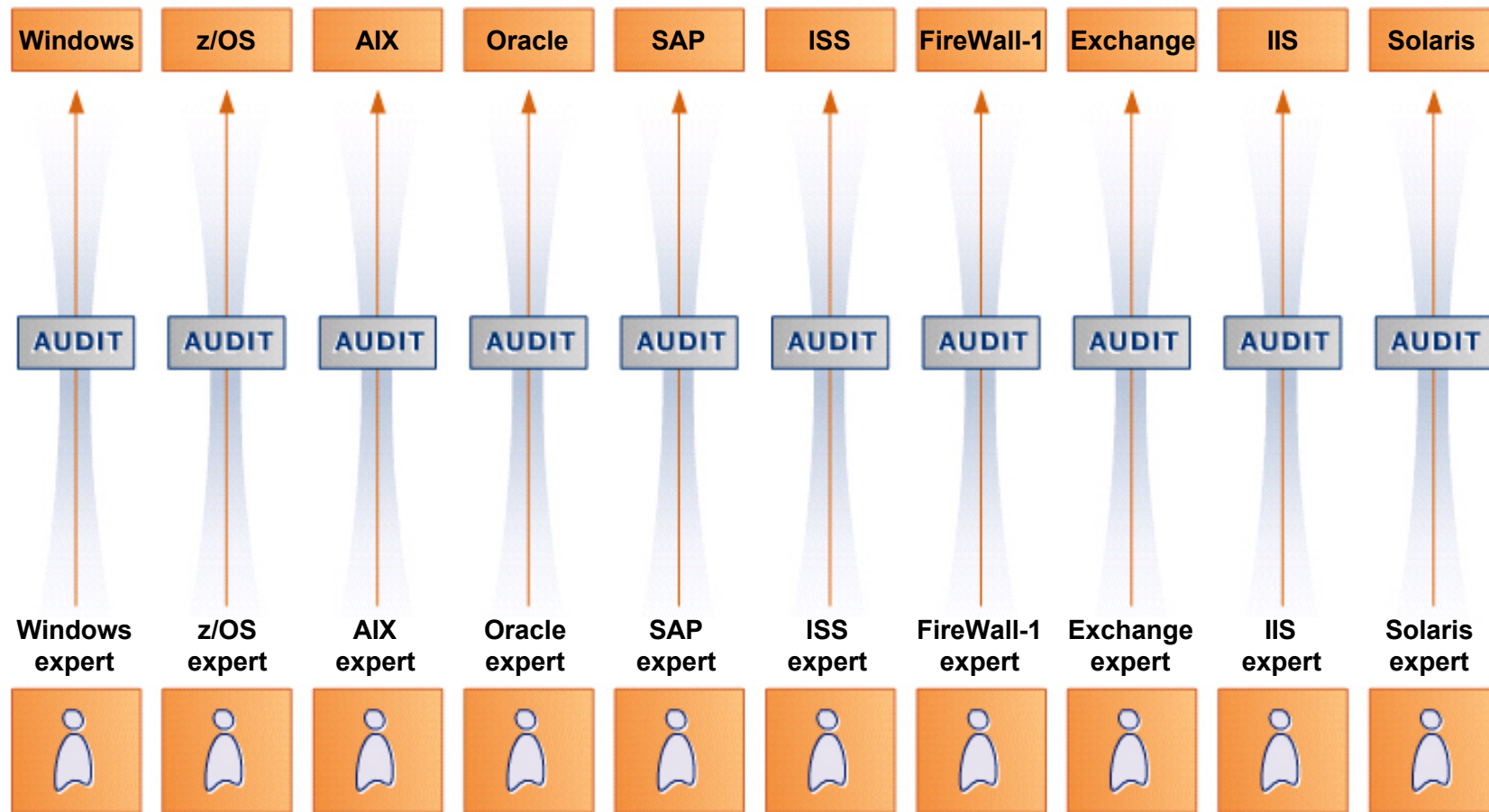
Security audit (SECURITY) on APPLES, system id: 2074
Auditable event: Batch process login
Event time: 1-MAR-2005 00:02:09.84
PID: 20402B44
Process name: BATCH_440
Username: SYSTEM
Process owner: [SYSTEM]
Image name: DSA0:[SYS1.SYSCOMMON.][SYSEXE]LOGINOUT.EXE
Posix UID: -2
Posix GID: -2 (%XFFFFFFFFE)

Security audit (SECURITY) on CYGNUS, system id: 2073
Auditable event: Network login
Event time: 1-MAR-2005 00:02:16.11
PID: 2021A46D
Process name: MQMTC_P2_BG164
Process owner: [MQMTC_P2_BG164]
Image name: DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE
Remote node id: 21480504
Remote node fullname: [REDACTED]
Remote username: MQM
Posix UID: -2
Posix GID: -2 (%XFFFFFFFFE)

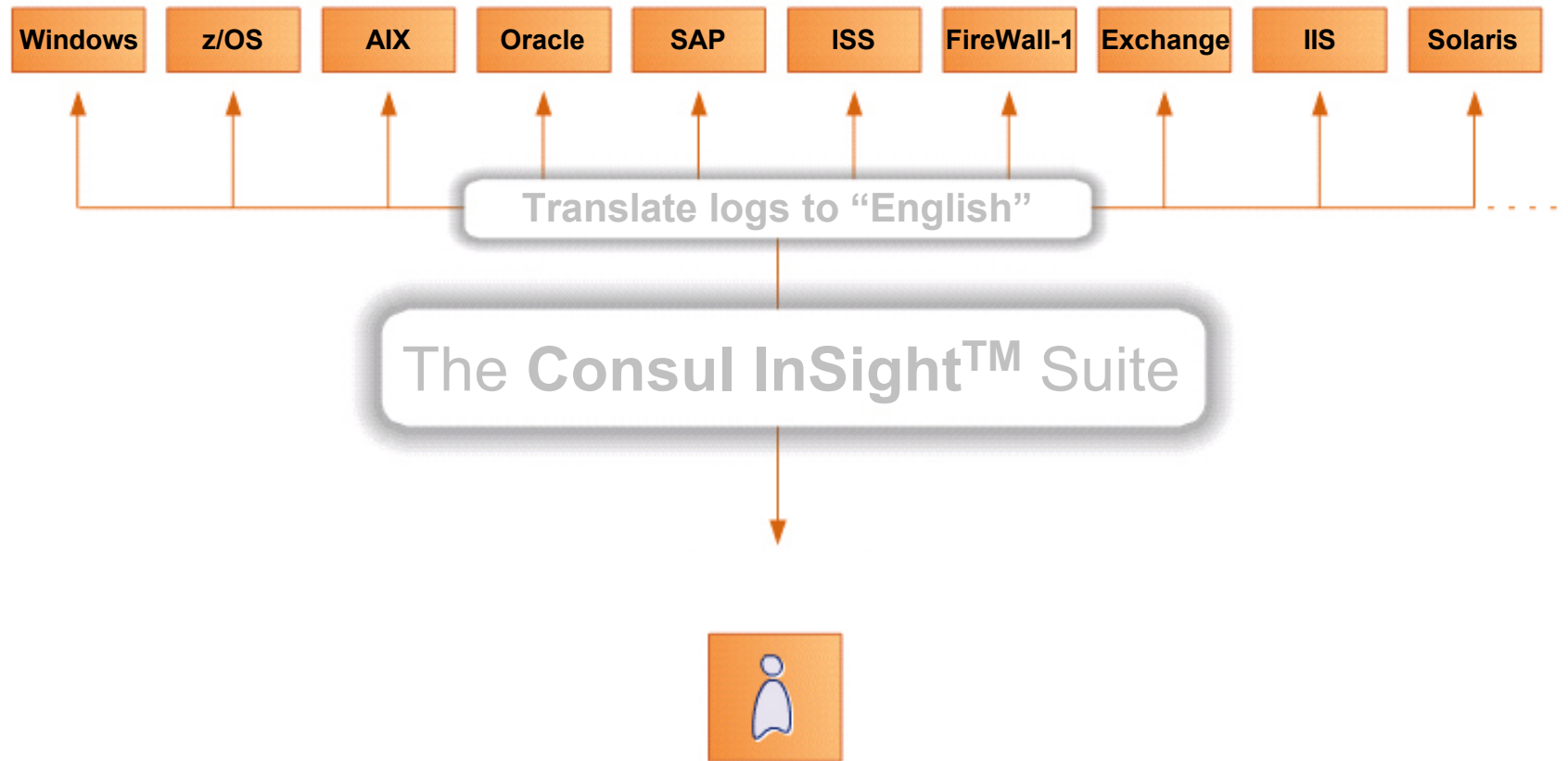
Security audit (SECURITY) on CYGNUS, system id: 2073
Auditable event: Batch process login
Event time: 1-MAR-2005 00:02:32.61
PID: 20219477
Process name: BATCH_443
Username: SYSTEM
Process owner: [SYSTEM]

Log entries (Left Window):
Apr 5 17:20:30 syslog su(pam_unix)[10429]: authentication failure; logname= ruser=acrystal rhost=[REDACTED] tty=
Apr 5 17:22:03 syslog sshd(pam_unix)[10351]: session closed for user acristal
Apr 5 18:01:01 syslog crond(pam_unix)[10436]: session closed for user MQM
Apr 5 19:01:01 syslog crond(pam_unix)[10438]: session closed for user MQM
Apr 5 20:01:01 syslog crond(pam_unix)[10440]: session closed for user MQM
Apr 5 21:01:01 syslog crond(pam_unix)[10442]: session closed for user MQM
Apr 5 22:01:01 syslog crond(pam_unix)[10444]: session closed for user MQM
Apr 5 23:01:01 syslog crond(pam_unix)[10446]: session closed for user MQM
Apr 6 00:01:01 syslog crond(pam_unix)[10448]: session closed for user MQM
Apr 6 01:01:01 syslog crond(pam_unix)[10450]: session closed for user MQM
Apr 6 02:01:01 syslog crond(pam_unix)[10452]: session closed for user MQM
Apr 6 03:01:01 syslog crond(pam_unix)[10454]: session closed for user MQM
Apr 6 03:33:29 syslog crond(pam_unix)[10456]: session closed for user MQM
Apr 6 04:01:02 syslog crond(pam_unix)[10458]: session closed for user MQM
Apr 6 04:03:46 syslog crond(pam_unix)[10460]: session closed for user MQM
Apr 6 04:30:02 syslog crond(pam_unix)[10462]: session closed for user MQM
Apr 6 05:01:01 syslog crond(pam_unix)[10464]: session closed for user MQM
Apr 6 06:01:01 syslog crond(pam_unix)[10466]: session closed for user MQM
Apr 6 07:01:01 syslog crond(pam_unix)[11035]: session closed for user MQM
Apr 6 08:01:01 syslog crond(pam_unix)[11037]: session closed for user MQM
Apr 6 08:42:11 syslog sshd(pam_unix)[11041]: session opened for user ebarrios by (uid=0)
Apr 6 08:42:43 syslog sshd(pam_unix)[11071]: authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.101.1.154 user=ebarrios
Apr 6 08:42:49 syslog sshd(pam_unix)[11077]: session opened for user ebarrios by (uid=0)

After Log Capture, Translation is Next



Now all Logs in Your Enterprise in a Single Language



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

Translate Logs into English - Consul's W7 Methodology

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!!



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

Direct Database Access Report

Time period setup

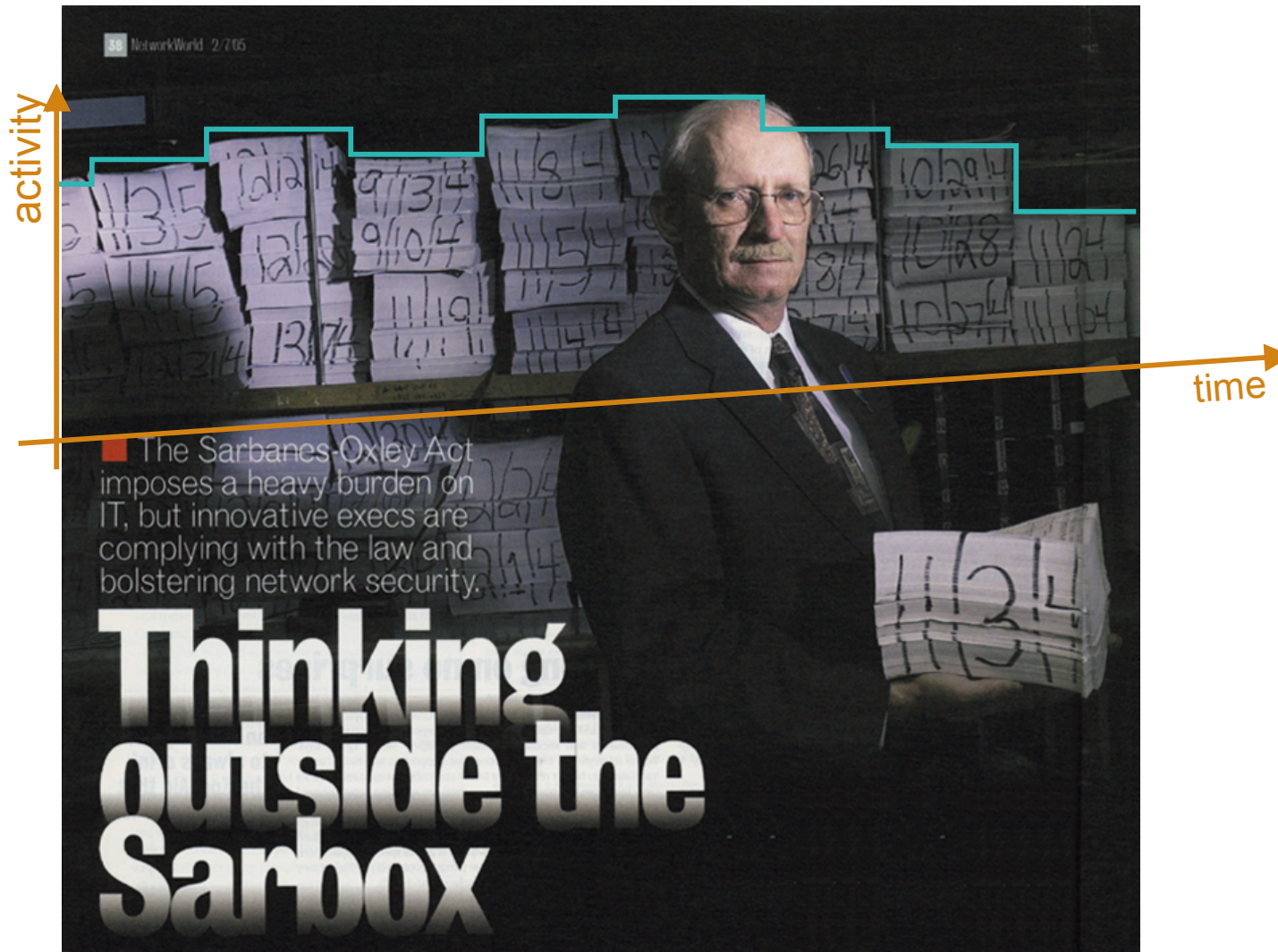
Month: September | Day: 3 | Year: 2006 | Hour: 1 | Min: 0
 Start time: September 3 2006 1:00
 End time: September 7 2006 16:00
 Execute Reset
 Time zone: Event time zone

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

You Need Reports to Communicate

Communicate





EPRORADB » DemoData » Reports

My reports

Add custom report

Export custom reports

▼ Configuration tools

Type	Title	Description	Action
	Admin Exceptions		
	Events by rule	List of events that comply with a W7 rule	
	Events by type	Summary of audited event types	
	Policy Settings	List of events that comply with the Policy rules	
	Policy Wizard	Tool to help defining a policy and to verify the existing policy	
	W7 Summary	Summary of all events	

▼ Custom Report

Type	Title	Description	Action
	Database System Events	Database System Startup, Shutdown and Other Utility Events	
	Finance & HR Access	Finance & HR Access	
	Privileged Operations	Database Privileged Operations	
	Stored Procedures	List of Stored Procedures and results	

▼ Daily verification

Type	Title	Description	Action
	Alerts	List of Alerts by Priority	
	All Exposures	List of Exposures by Priority	
	DBA Activity	List of changes to databases	
	Events by type	Summary of audited event types	
	Failed System Operations	List of failed operator and configuration commands	
	Failed System Services	List of system processes that ended with (security) error condition	
	Failed Transactions	List of failed transactions (SAP, Oracle)	
	Impersonation	List of Users who caused events under another name	
	Logon Failure Summary	Summary of logon failures	
	Reconnaissance	List of actions to retrieve system information	
	Restarts	List of system starts and restarts	
	System Operations	Operator and system configuration activity	
	System Update	List of modifications to the system	
	Users	List of users	

▼ Detailed investigation

Type	Title	Description	Action
------	-------	-------------	--------

Dashboard > Regulations

Compliance Modules

- Basel II
 - Introduction
 - Classification Template
 - Policy Template
 - Reports
 - Documentation
- Gramm-Leach-Bliley Act (GLBA)
 - Introduction
 - Classification Template
 - Policy Template
 - Reports
 - Documentation
- Health Insurance Portability and Accountability Act (HIPAA)
 - Introduction
 - Classification Template
 - Policy Template
 - Reports
 - Documentation
- ISO 17799
 - Introduction
 - Classification Template
 - Policy Template
 - Reports
 - Documentation
- Sarbanes Oxley (SOX)
 - Introduction
 - Classification Template
 - Policy Template
 - Reports
 - Documentation

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
Exposure	description of Exposure
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
Weekend	Non-working days

Where

Extra Information

Help

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 15 261 3333

@consul.com
 1 703 675 2022

Policy Template

Download this template to use in the management Console.

Policy Rules

Attention Rules

Who group	What group	When group	Where group	on/that group	From/where group	Where To Group ID	Severity	Description
HR Management	Intrusion - Medium	Office Hours			Remote Workstation		30	Review
Administrators			Customer Information Systems	HR - Medium			40	Requires attention
Administrators			Financial - Medium				access medium	50
Administrators			Customer Data - High				access medium	50
Administrators			Financial - Low				access high	70
IT			Sensitive				access low	20
Unknown	Customer							25

Sarbanes Oxley Regulation Reports

Title	Description
Sarbanes Oxley (FFEC 1.1.1.4) Security Policy report	No description given
Sarbanes Oxley (FFEC 1.3.1.1) 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, 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 (8.4.5) 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 (9.2.4.6.7) System access and use	Successes and failures against key assets.
Sarbanes Oxley (9.3) User responsibilities and password use	Login 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	Login/Logout 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 group 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.

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.
[Redacted]	
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.

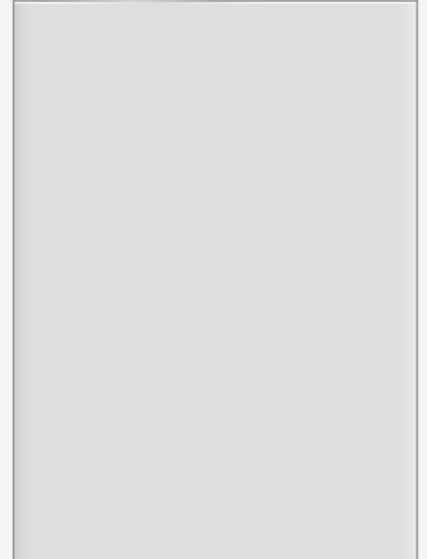
Please login into the Consul InSight Suite. This will give you access to all the products available with this specific username.

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

Operational Change Control of Finance database

Time period setup

Month Day Year Hour Min.

Start time: October 1 2006 0 40

End time: November 1 2006 0 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	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:

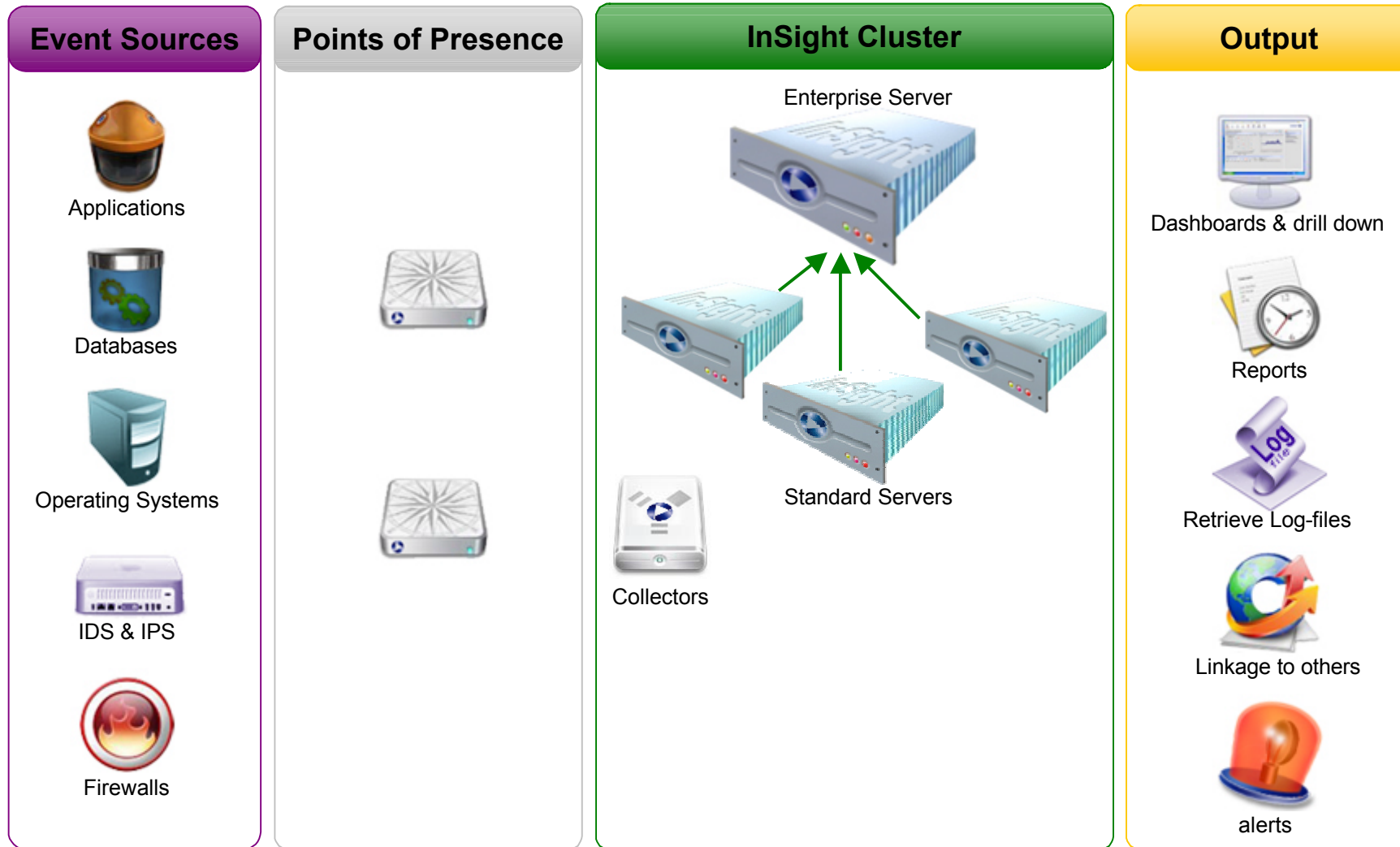
- What DBA Actions,**
- System Actions,
 - System Administration,
 - System Operations,
 - System Updates

Contact us

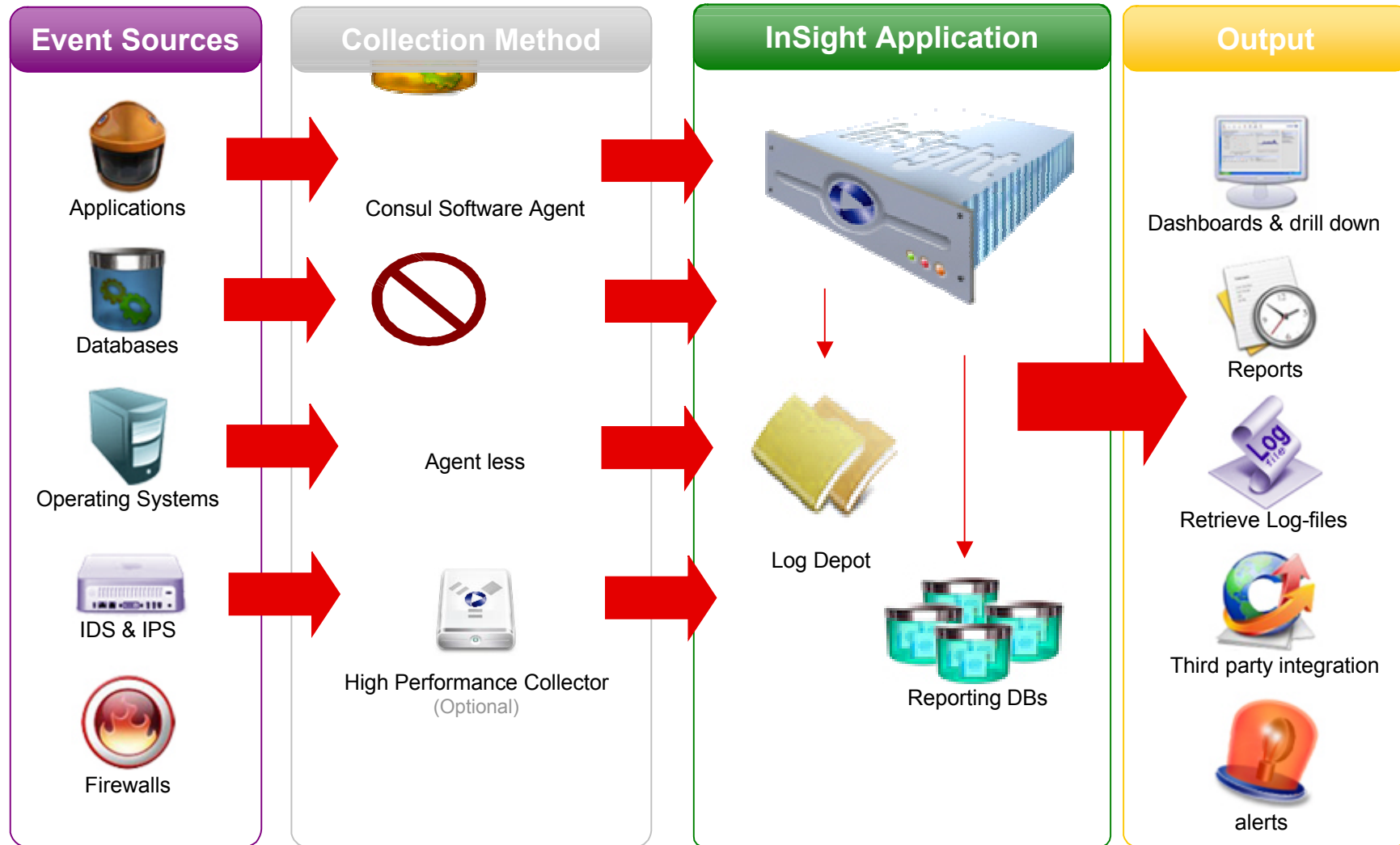
In the US:
contactsales@consul.com
 Direct Line: +1 703 675 2022
 Toll Free (US only): 800 258 5077

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

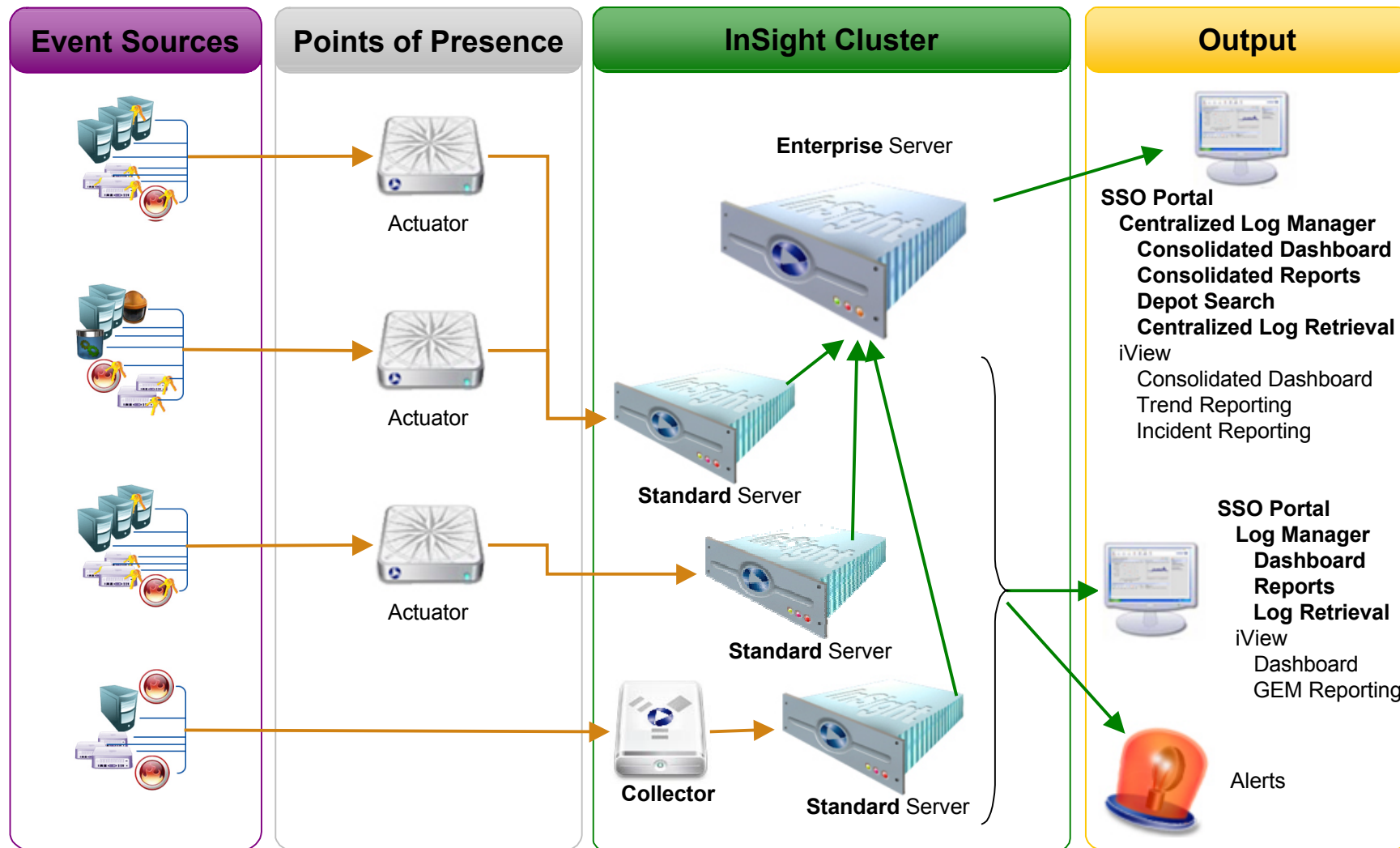
InSight – Functional Component Overview



Architecture



Single Cluster



IBM's security management vision and strategy:

Integrated capabilities from Tivoli, Consul, ISS, STG and IGS

