What makes you special?

IBM/Security

Audit & Compliance

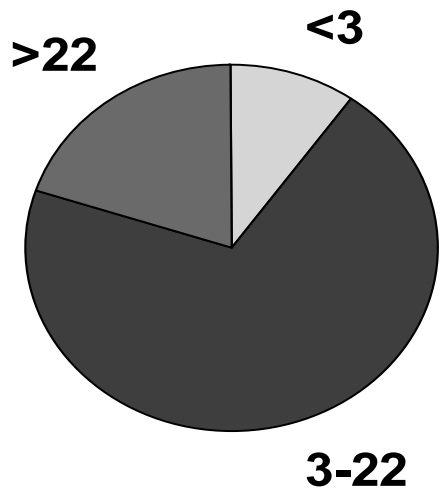
Alfonso Ponticelli
Software Group - Security

IBM Governance and Risk Management
Maximize Value, Manage Risk

IT Policy Compliance Group Study

- **75%** delle aziende ha più di 3 incidenti di sicurezza in un anno riguardanti l'accesso a dati ritenuti importanti
- "Cosa abbiamo trovato attraverso questo studio tuttavia è che **le aziende che hanno avuto i risultati migliori sono quelle che hanno investito di più sulla sicurezza e la conformità alle policy**
- "Le aziende migliori sono quelle che **non solo hanno raggiunto la conformità a regolamentazioni o standard,** ma che **effettivamente verificano e controllano quanto stabilito almeno una volta alla settimana**

Incidenti in 1 anno



Source: "Taking Action to Protect Sensitive Data," IT Policy Compliance Group, March 2007
http://www.itpolicycompliance.com/research_reports/data_protection/read.asp?ID=9

Security e compliance challenges

- **Aumento del numero di standard di Sicurezza**
  - Le normative sono una decina (Basilea II, ISO17799, Dlg. 196/2003, SOX…)
  - Le iniziative di compliance aumentano in ogni settore di industria
  - Migliorare monitoring e controllo, al fine di gestire i rischi e quindi evitare penali e perdita di business
- **Aumento della complessità**
  - Diversità di tecnologie e di infrastrutture complicano il processo di compliance
  - Evoluzione tecnologica (Web 2.0) che trasformano per complessità la compliance in una sfida
- **Aumento dei costi**
  - Difficile sapere a priori il costo di un'attività di audit sulle moderne infrastrutture, eterogenee e distribuite
  - Non risultare compliance e non prevenire gli incidenti di security incide fortemente sui costi aziendali

- **43% dei CFO pensano che migliorare la governance, i controlli e il risk management siano l'obiettivo prioritario**

Sottovalutare la Governance & Risk Management può essere disastroso

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

ComputerWeekly.com

FBI loses 3-4 laptops a month, auditor says

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 Write

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 th onic library.

By: Larry Greeenemeier

EETIMES ONLINE

Head Of Nuclear Agency Leaving Under Pressure Over Security Lapses

AP Press Release, January 5, 2007

USA TODAY

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Massive Insider Breach at DuPont

February 15, 2007 – 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 …

- "Per le aziende il modo migliore per difendersi da incidenti interni è prevedere adeguati processi di monitoraggio sugli accessi alla rete ed ai database e la definizione di apposite soglie oltre le quali identificare un'attività che a secondo dell'utente può classificarsi anomala."

Cosa si è verificato:

- Dipendente passa al competitor
- Ha eseguito accessi al database
- Ha trasfetito 180 documenti sul nuovo laptop

Carnegie Mellon CERT:

- "75% di furti di informazioni riservate, vengono eseguiti dai propri dipendenti"
- "45% aveva gia accettato un lavoro con un'altra azienda"

Source: InformationWeek, Feb. 15, 2007

Gli attacchi interni sono quasi sempre dipendenti dai privilegi

- Il numero di attacchi provenienti dall'interno rispetto all'esterno è approssimativamente uguale (CSI/FBI Survey 2005)
- 87% degli attacchi interni possono essere attribuiti ad utenti privilegiati (USSS/CERT Insider Threat Survey 2005)
- 43.5% del numero globale di incidenti di sicurezza possono essere dipendenti dai privilegi utente.
- Il gruppo di utenti privilegiati rappresentano <5% di una azienda

Cosa vi chiederà un auditor

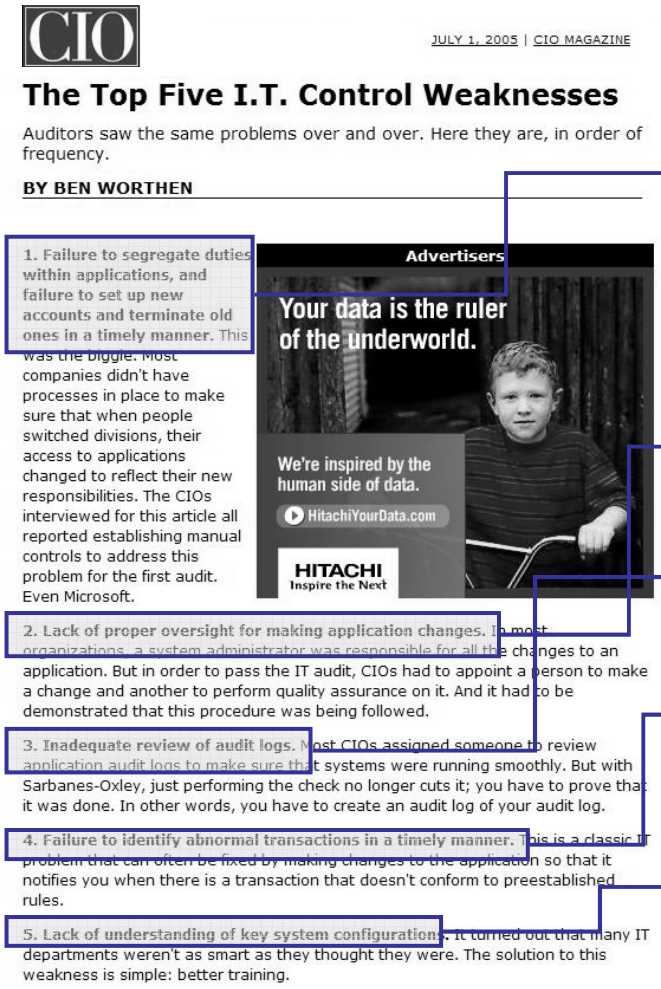
- Violazione di privacy:
  - Esistono DBA che accedono ad informazioni riservate?
  - Esistono usi impropri delle applicazioni HR?
  - Si verificano usi non leggittimi di identità?
- Violazione delle policy di sicurezza:
  - Si verificano delle modifiche all'infrastruttura non autorizzate?
  - Ci sono utenti root che hanno disattivato il tracciamento delle operazioni?
  - Quando sono stati cancellati i log di sistema?
  - Chi ha eseguito uno stop di uno o più processi del sistema?
- Amministratori che violano la segregation of duties:
  - Esistono transazioni che vengono inizializzate ed approvate dalla stessa utenza?
  - Esistono amministratori che creano ed approvano identità ed autorizzazioni sul sistema?

Ma la domanda a cui dovrete rispondere:

Sono in possesso di tutti gli strumenti per collezionare i dati necessari per i report che possano evidenziare violazione di policy?

The Top Five I.T. Control Weaknesses

http://www.cio.com/article/8097/_The_Top_Five_IT_Control_Weaknesses



CIO

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

1. Failure to segregate duties within applications, and failure to set up new accounts and terminate old ones in a timely manner. This was the biggie. 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.

2. Lack of proper oversight for making application changes. In most organizations, a system administrator was responsible for all the 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.

3. Inadequate review of audit logs. Most CIOs assigned someone to review application audit logs to make sure that 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.

4. Failure to identify abnormal transactions in a timely manner. 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.

5. Lack of understanding of key system configurations. 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.

Omissione della segregate duties all'interno delle applicazioni, ed omissione della gestione del ciclo di vita delle utenze con cancellazione dei vecchi account, in tempo reale.

Assenza di adeguata supervisione sui processi di change del sistema.

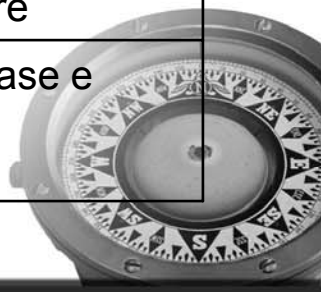
Inadeguati processi per l'analisi dei logs

Difficoltà nell'identificare transazioni anomale in tempo reale

Difficoltà nel comprendere la configurazione del sistema

Cosa è rilevante ?

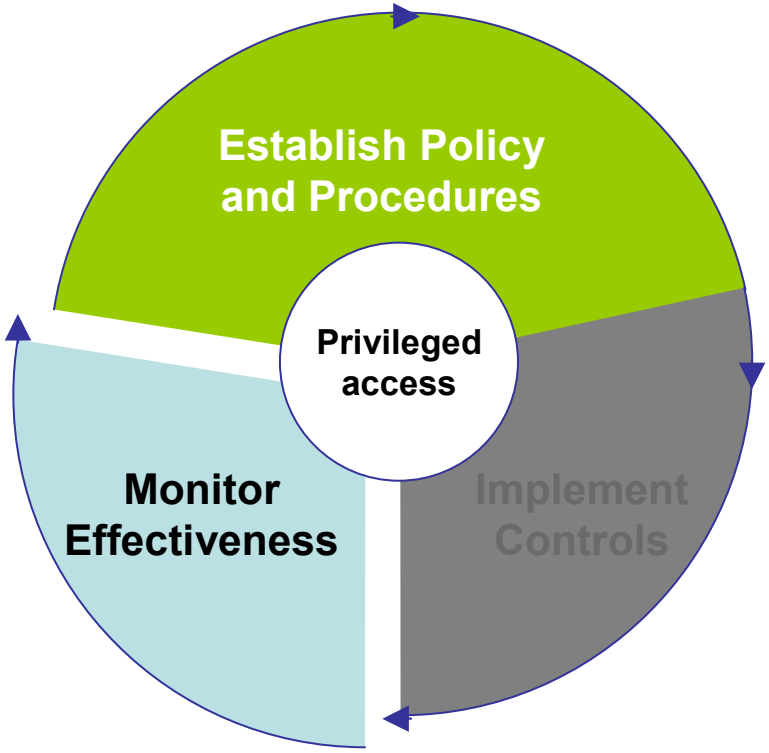
Categoria	Descrizione
Eventi di autenticazione	Eventi di logon / logoff
Eventi di gestione	Start di server, stop, back-up, restore
Change management	Modifiche di configurazione, modifiche sui processi di auditing, modifiche sulla struttura dei database, attività di manutenzione
Gestione utenze	Creazione di nuove utenze, modifica dei privilegi utente, attività di cambio password
Diritti di accesso	Comportamento di tutti i DBA includendo gli accessi ai dati, DBCC (Database Console Command), call a stored procedure
Accesso ai dati sensibili	Tutti gli accessi ai dati sensibili immagazzinati nei database e quindi operazioni di: select, insert, update, delete



La soluzione: la gestione degli utenti

Le difficoltà

- Syslog non sono sufficienti
- Ogni sorgente ha la sua sintassi
- Non basta archiviare ma bisonga poter effettuare interrogazioni
- Enorme quantità di dati

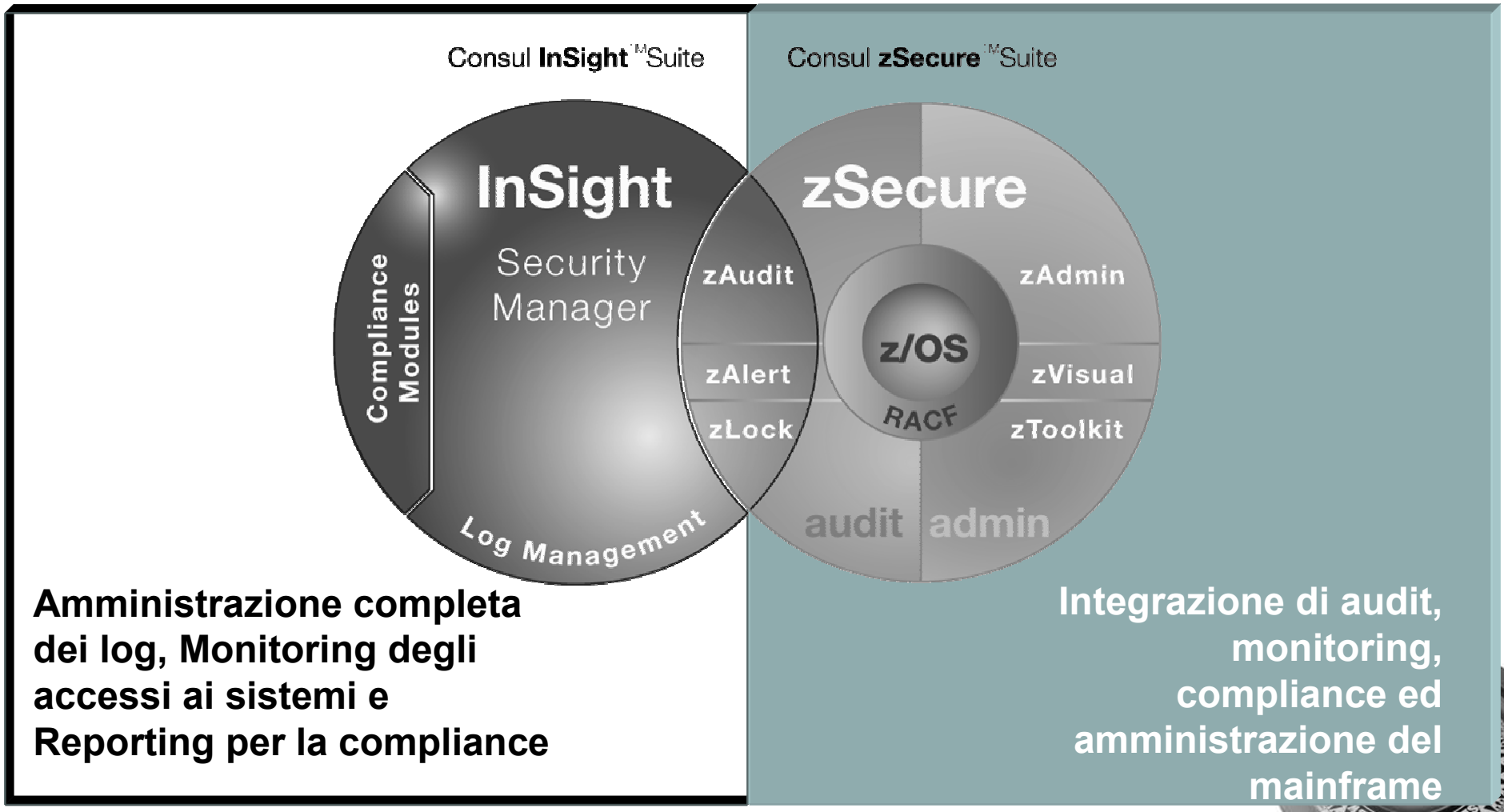


What makes you special?

Tivoli Compliance Insight Manager

IBM Governance and Risk Management
Maximize Value, Manage Risk

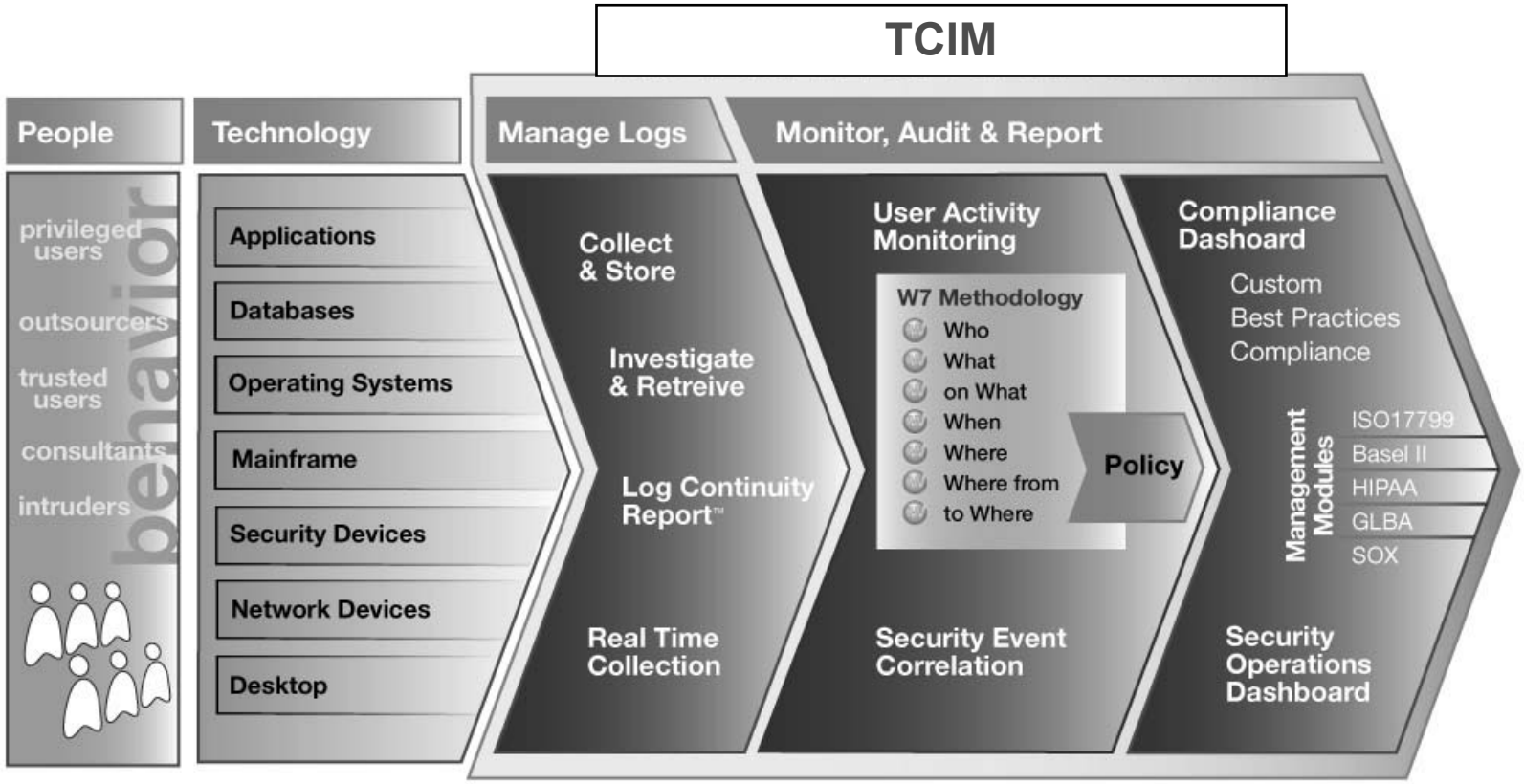
Tivoli Compliance: soluzione



Amministrazione completa dei log, Monitoring degli accessi ai sistemi e Reporting per la compliance

Integrazione di audit, monitoring, compliance ed amministrazione del mainframe

Introduzione... IBM Tivoli Security and Compliance Insight



TCIM: i problemi che aiutiamo a risolvere

"Ho bisogno di produrre report per i miei auditor"

"Ho bisogno di dimostrare di possedere una struttura di IT security controls"

"Il mio staf non possiede tempo ed esperienza ma necessita di eseguire la scansione dei logs"

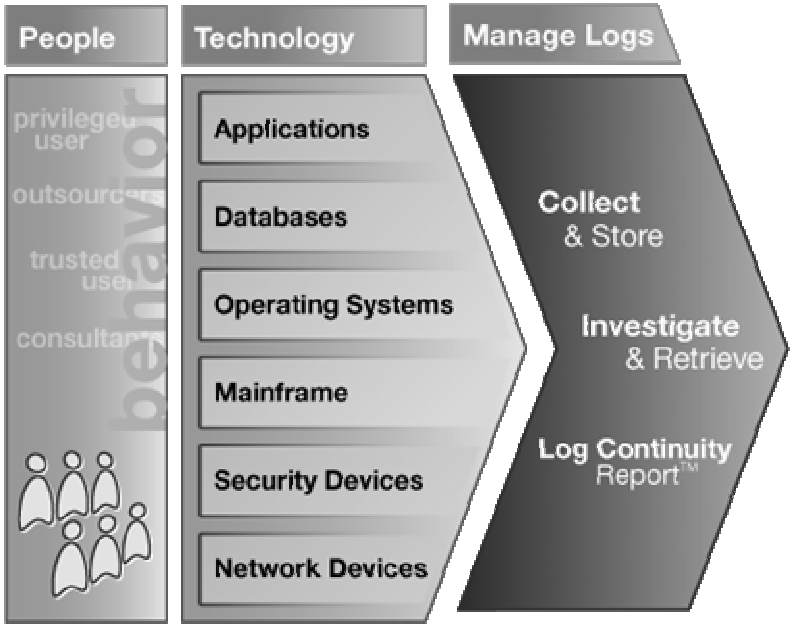
"Sono interessato ad individuare i privilegi che permettono determinate azioni"

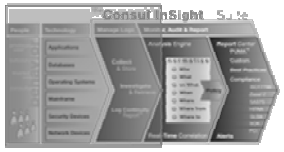
"Ho bisogno di storicizzare i log per analisi forense"

"Non ho idea di quale log collezionare e come farlo"

Enterprise Log Management

Capture





Funzionalità:

- Sicuro, affidabile accentratore di log da qualunque piattaforma
- Cattura in automatico i syslogs
- Pieno supporto su attività di collect di eventi da log nativi
- Immagazzina in modo efficiente e compresso i dati in un depot
- Accesso ai dati quando necessario
- Ricerca su tutti i log
- Reports sui dati raccolti

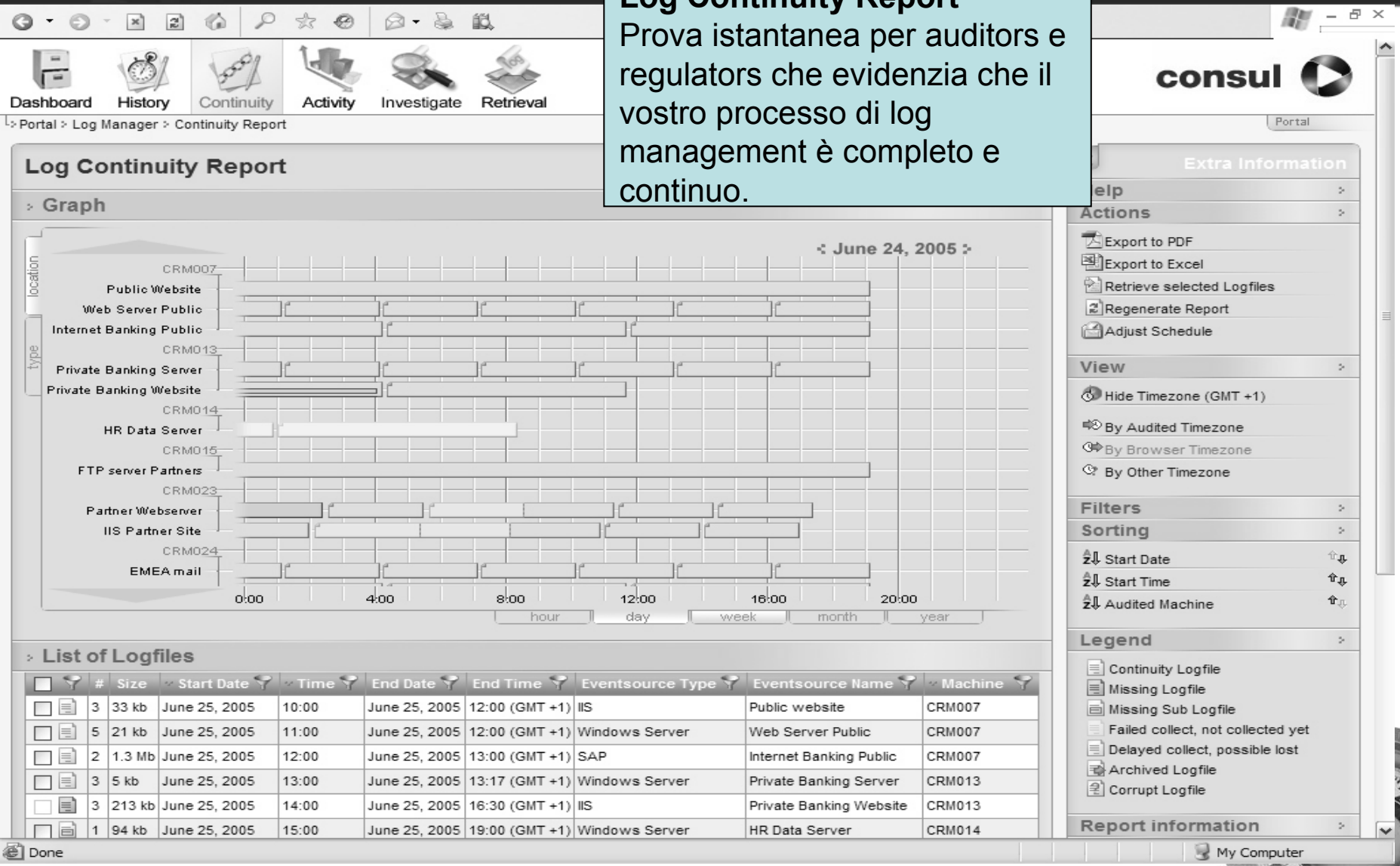
Benefici:

- Riduzione dei costi grazie all'automatizzazione e centralizzazione del collect dei dati
- Essere sempre "audit ready"!

Implementation time: plug and play.

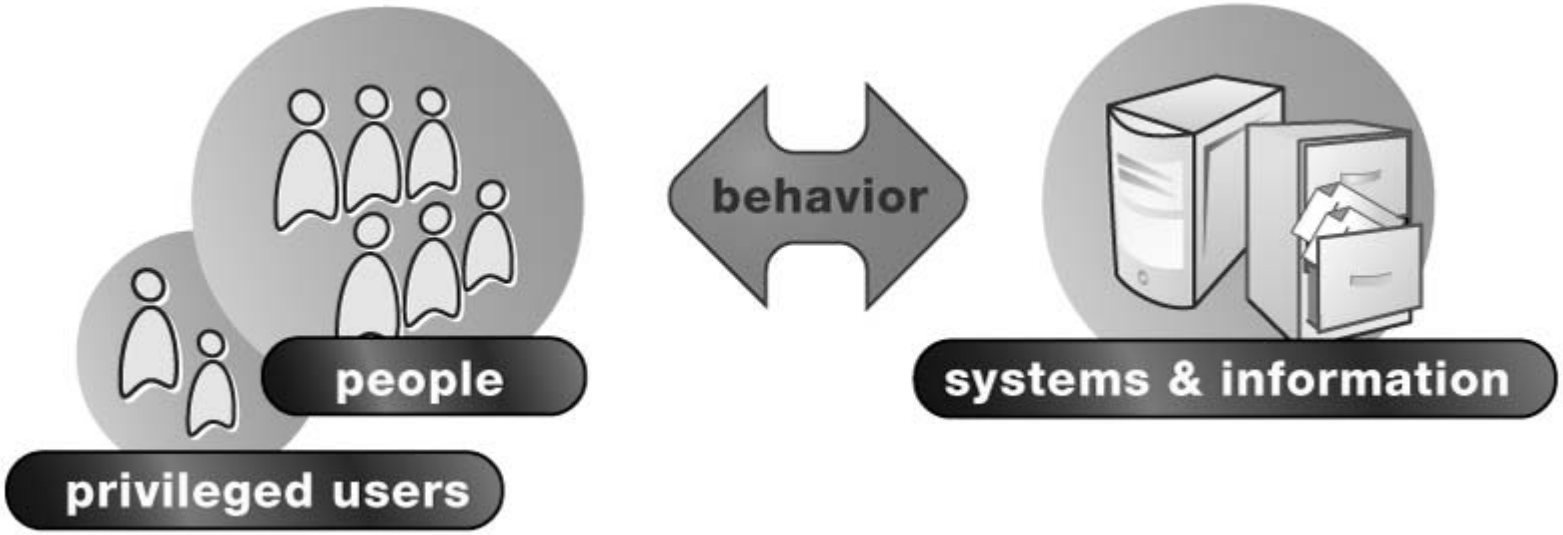
Log Continuity Report

Prova istantanea per auditors e regulators che evidenzia che il vostro processo di log management è completo e continuo.



Cosa stanno facendo gli utenti sulla mia rete?

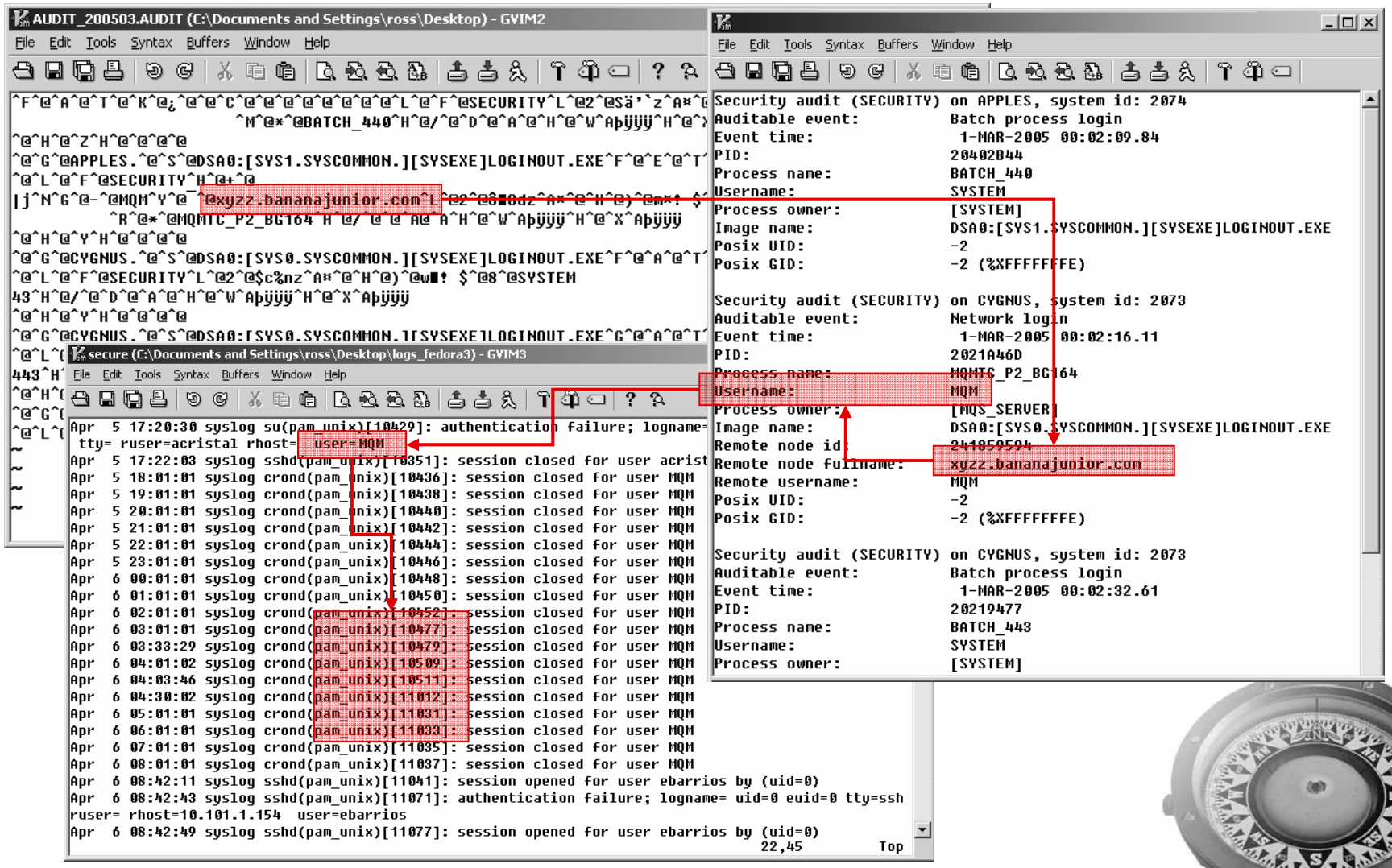
Comprehend



87% degli incidenti interni sono causati da utenti privilegiati.

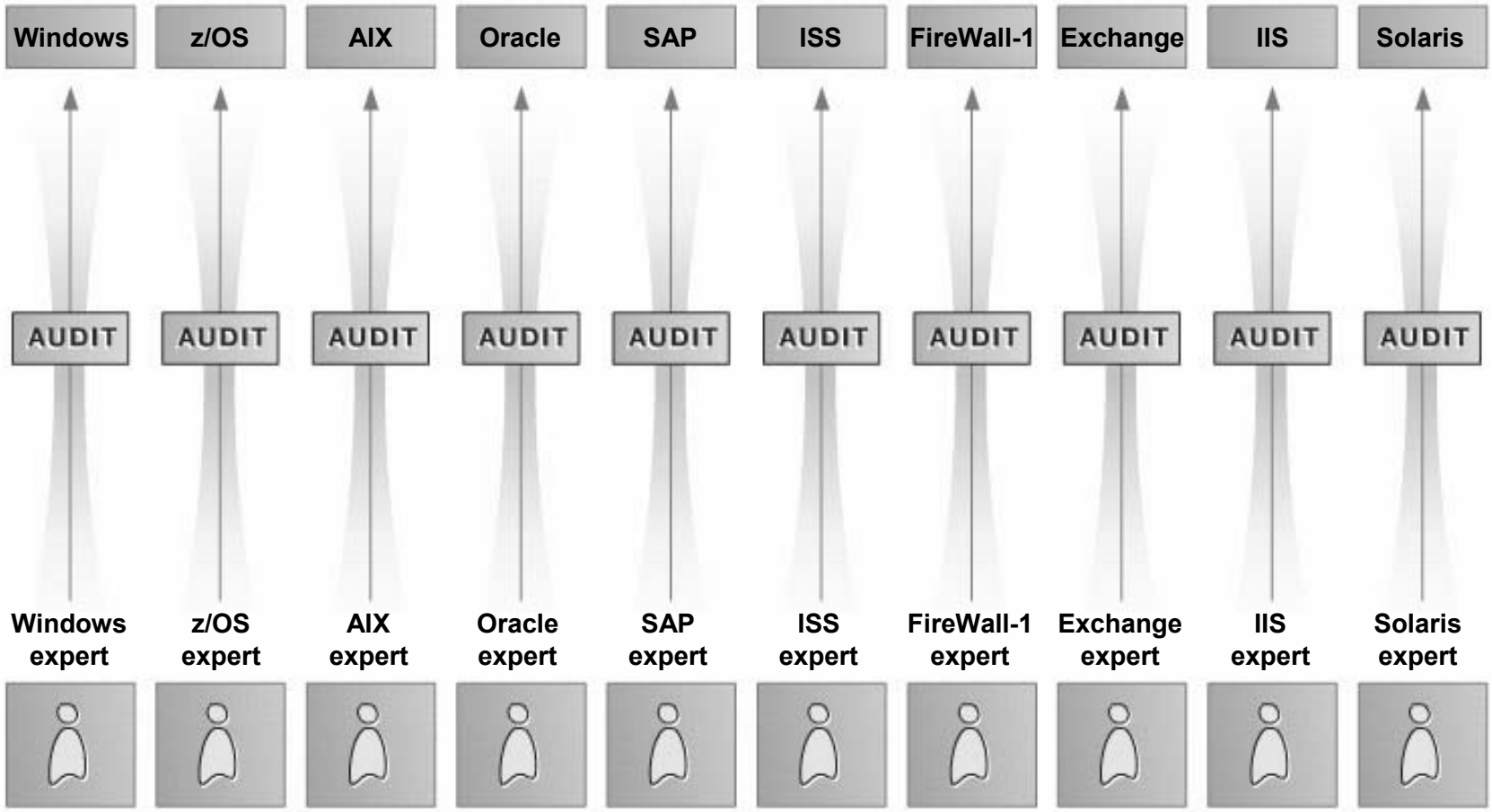
Come faccio a capire il senso di tutto questo?

Comprehend



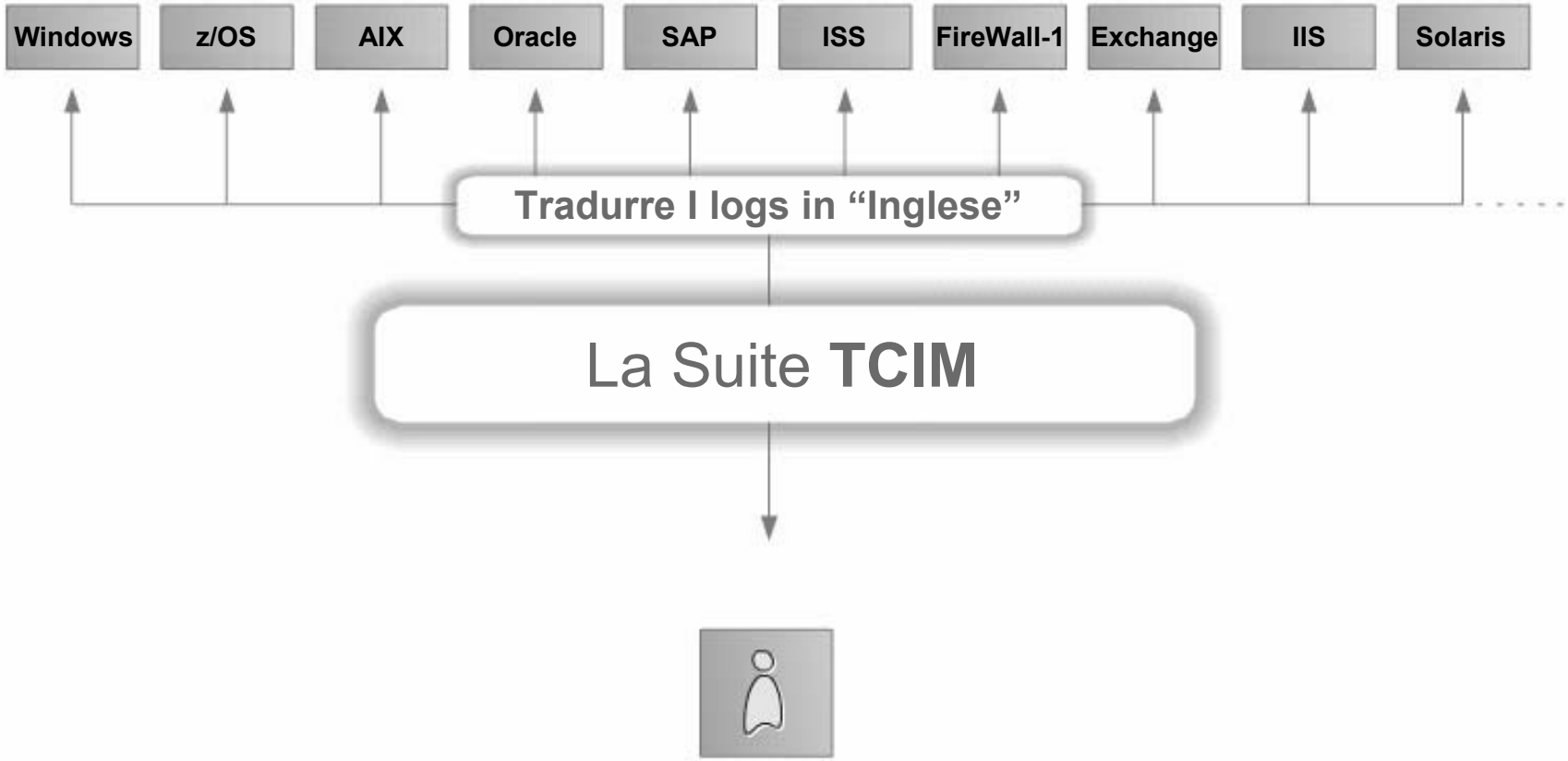
Dopo aver catturato i dati, Tradurli è il prossimo passo

Comprehend



Ora tutti i log della vostra azienda in un unico linguaggio

Comprehend



Consul InSight storicizza le vostre informazioni di security e compliance risparmiando tempo e soldi attraverso l’automatizzazione di processi di monitoring sull’azienda.

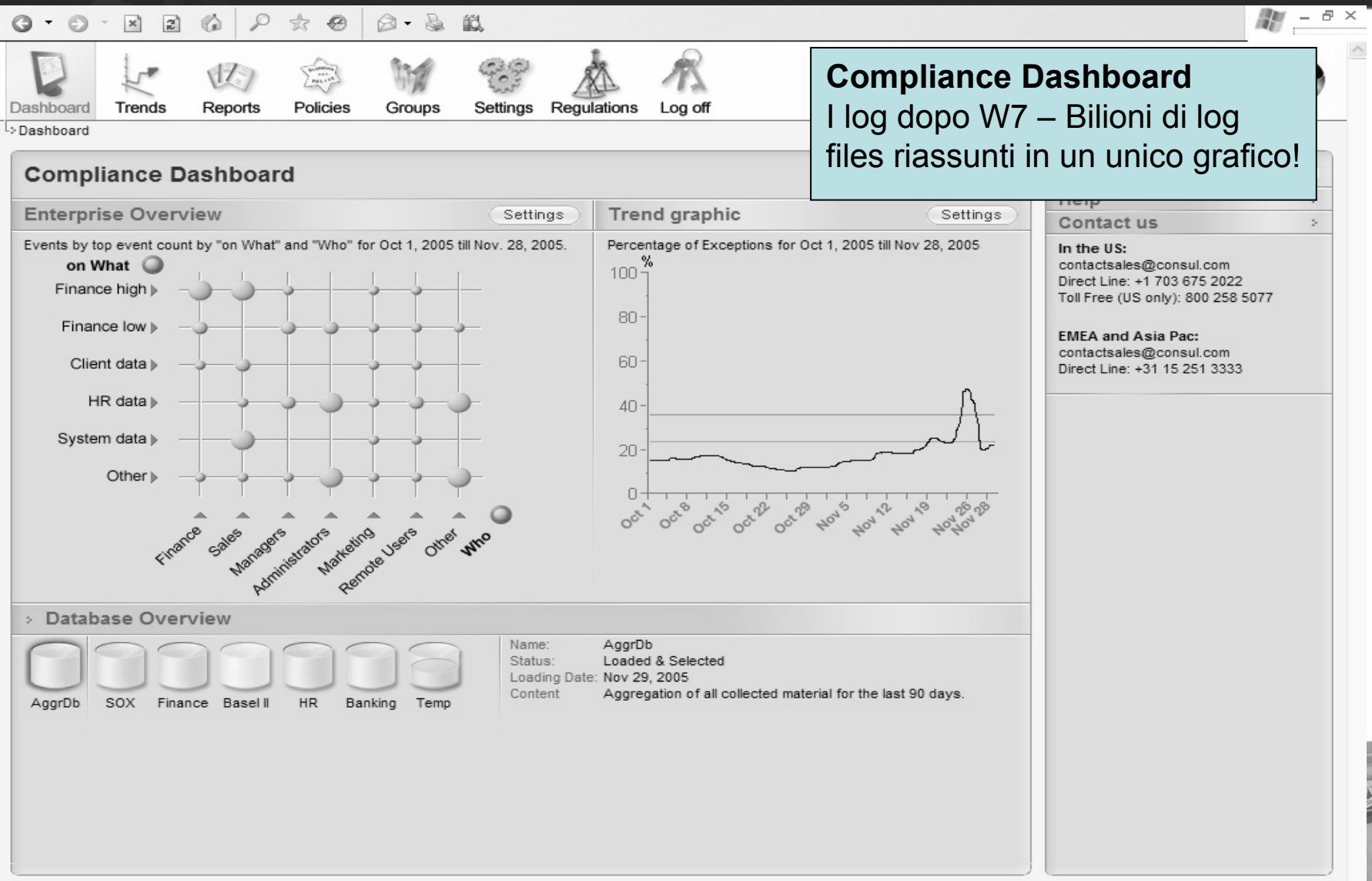
Tradurre i Log in Inglese – con la metodologia Consul W7

- **Who** l'ha fatto **What** tipo di azione **on What**?
- **When** l'ha fatto e **Where**, **From Where** e **Where To**?

Comprehend

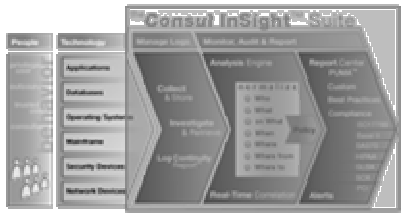
We do the hard work, so you don't have to!!

Compliance Dashboard
I log dopo W7 – Bilioni di log files riassunti in un unico grafico!



Full Audit and Compliance Reporting

Communicate



Capabilities:

- Centinaia di reports
- Moduli di Compliance
- Alert di Special attention
- Reports Custom

Benefits:

- Riduce l'impegno richiesto per l'audit
- Reports istantanei, salva tempo
- Riduce i rischi di minacce a dati sensibili:
  - Protezione dei dati
  - Controllo sui change
  - User management

Moduli di compliance predisposti – con riduzione dei tempi del proprio staff e riduzione dei costi di audit

Dashboard | Summary | Reports | Policies | Groups | Settings | Regulations | Log off

Dashboard > Regulations > Sarbanes Oxley Regulation Reports

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.

Help

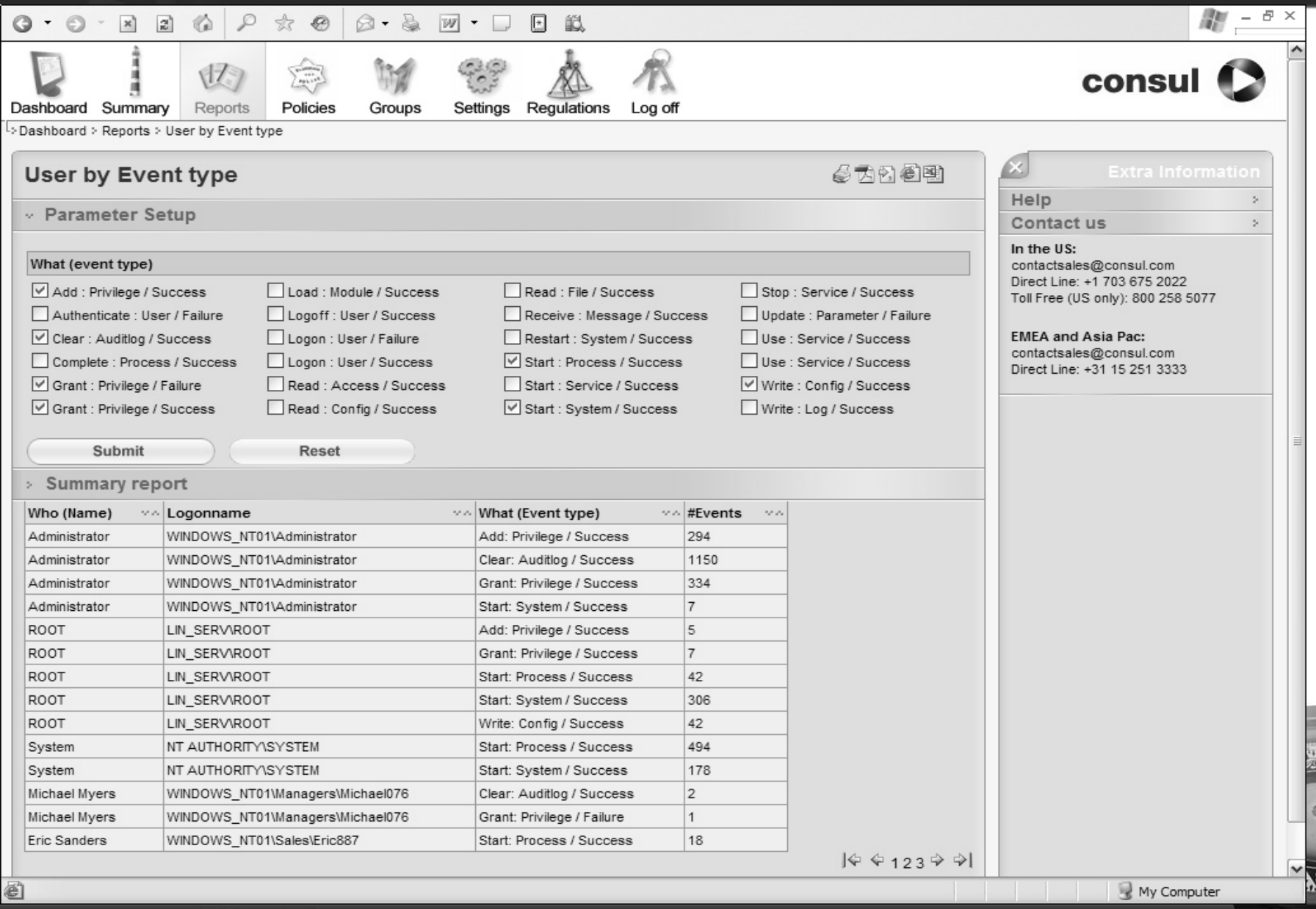
Please login into the Consul InSight Suite. This will give you access to all the products available with this specific username.

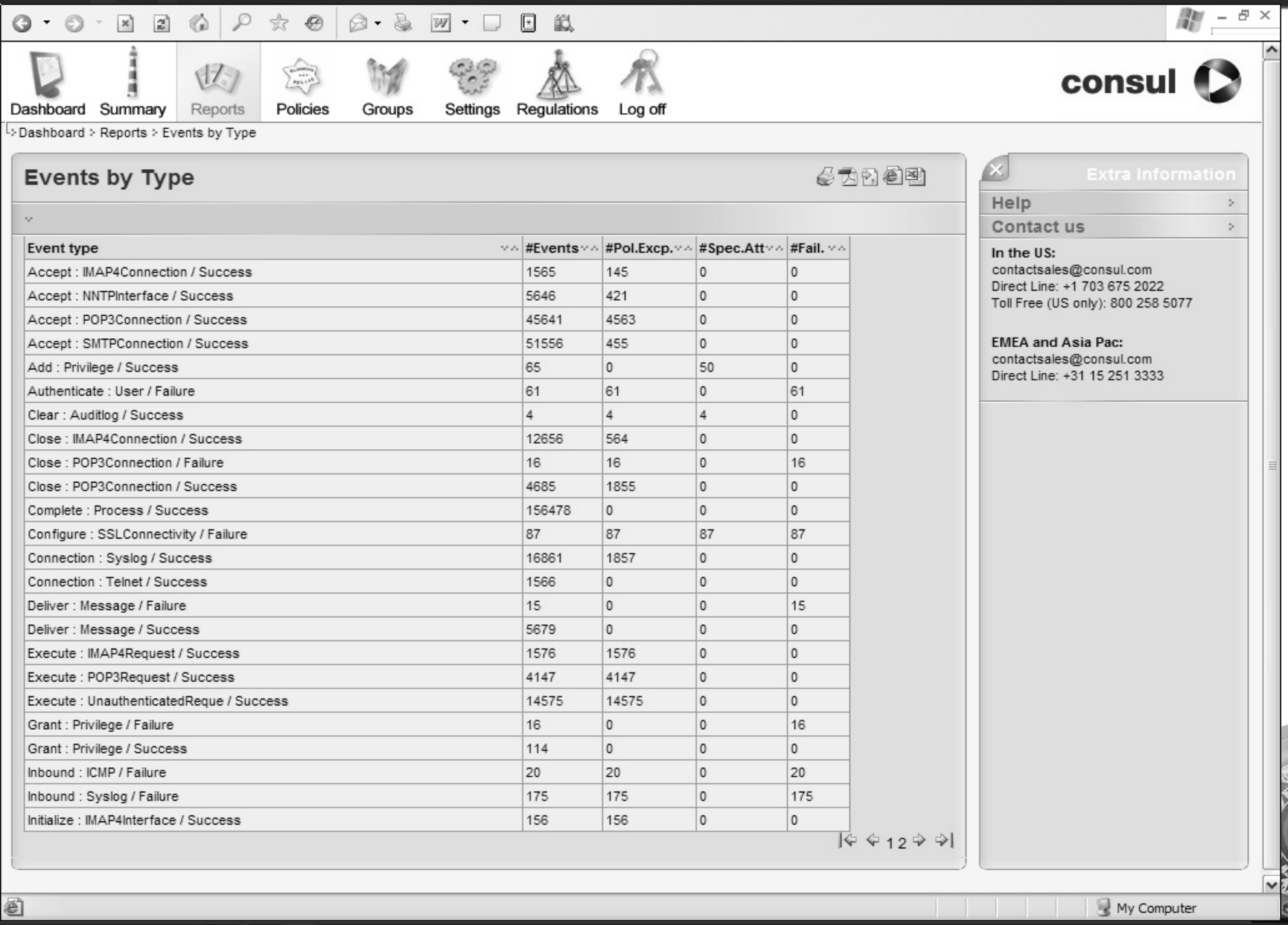
If you forgot your username and/or password please contact your administrator.

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





Dashboard Summary Reports Policies Groups Settings Regulations Log off

consul

Dashboard > Reports > Events by Type

Events by Type

Event type	#Events	#Pol.Excp.	#Spec.Att	#Fail.
Accept : IMAP4Connection / Success	1565	145	0	0
Accept : NNTPInterface / Success	5646	421	0	0
Accept : POP3Connection / Success	45641	4563	0	0
Accept : SMTPConnection / Success	51556	455	0	0
Add : Privilege / Success	65	0	50	0
Authenticate : User / Failure	61	61	0	61
Clear : Auditlog / Success	4	4	4	0
Close : IMAP4Connection / Success	12656	564	0	0
Close : POP3Connection / Failure	16	16	0	16
Close : POP3Connection / Success	4685	1855	0	0
Complete : Process / Success	156478	0	0	0
Configure : SSLConnectivity / Failure	87	87	87	87
Connection : Syslog / Success	16861	1857	0	0
Connection : Telnet / Success	1566	0	0	0
Deliver : Message / Failure	15	0	0	15
Deliver : Message / Success	5679	0	0	0
Execute : IMAP4Request / Success	1576	1576	0	0
Execute : POP3Request / Success	4147	4147	0	0
Execute : UnauthenticatedReque / Success	14575	14575	0	0
Grant : Privilege / Failure	16	0	0	16
Grant : Privilege / Success	114	0	0	0
Inbound : ICMP / Failure	20	20	0	20
Inbound : Syslog / Failure	175	175	0	175
Initialize : IMAP4Interface / Success	156	156	0	0

1 2

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 15 251 3333

My Computer

Drill down
visualizzare i dettagli di uno specifico evento, con la possibilità di andare in view sul log originale

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 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...

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 15 251 3333

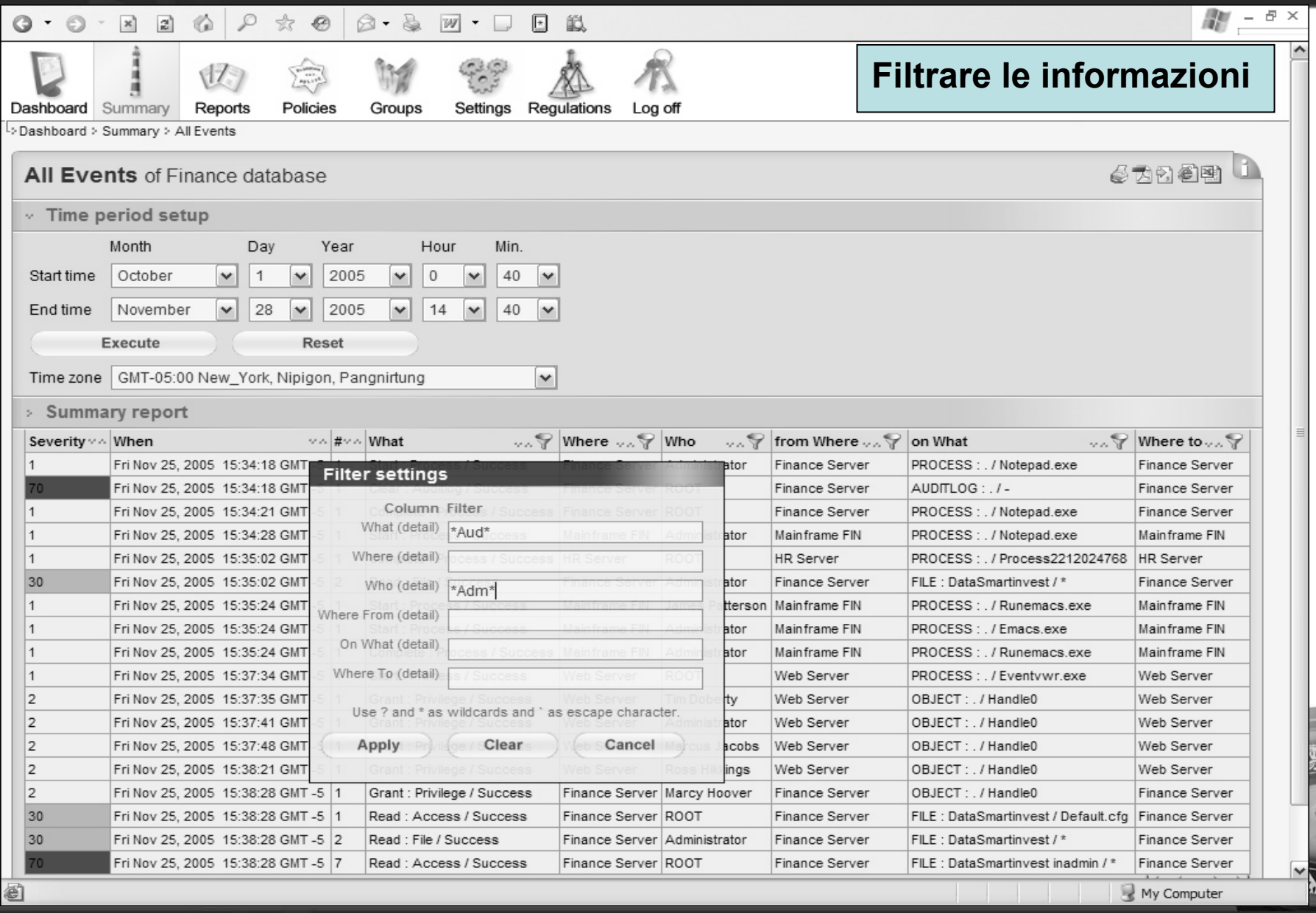
AUDIT_200503.AUDIT (C:\Documents and Settings\ross\Desktop) - GVIM2

File Edit Tools Syntax Buffers Window Help

```
^F^@^A^@^T^@^K^@¿^@^@^C^@^@^@^@^@^@^@^@^@^L^@^F^@SECURITY^L^@2^@S¾'`z^A¤^@^H^@)^@D+@ $^@8^@SYSTEM
                              ^M^@*^@BATCH_440^H^@/^@^D^@^A^@^H^@^W^Aþÿÿÿÿ^H^@^X^Aþÿÿÿÿ
^@^H^@^Z^H^@^@^@^@
^@^G^@APPLES.^@^S^@DSA0:[SYS1.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^F^@^E^@^T^@^N^@ì^@^@^C^@^@^@^@^@^@^@
^@^L^@^F^@SECURITY^H^@+^@
|j^N^G^@-^@MQM^Y^@ ^@xyzz.bananajunior.com^L^@2^@ô■Odz^A¤^@^H^@)^@m¤! $^@8^@MQM
          ^R^@*^@MQMTC_P2_BG164^H^@/^@^@^A@^A^H^@^W^Aþÿÿÿ^H^@^X^Aþÿÿÿ
^@^H^@^Y^H^@^@^@^@
^@^G^@CYGNUS.^@^S^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^F^@^A^@^T^@^K^@¿^@^@^C^@^@^@^@^@^@^@
^@^L^@^F^@SECURITY^L^@2^@$c%nz^A¤^@^H^@)^@w■! $^@8^@SYSTEM                              ^M^@*^@BATCH_4
43^H^@/^@^D^@^A^@^H^@^W^Aþÿÿÿ^H^@^X^Aþÿÿÿ
^@^H^@^Y^H^@^@^@^@
^@^G^@CYGNUS.^@^S^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^G^@^A^@^T^@^K^@¿^@^@^C^@^@^@^@^@^@^@
^@^L^@^F^@SECURITY^L^@2^@■^Lanz^A¤^@^H^@)^@w■! $^@8^@SYSTEM                              ^M^@*^@BATCH_
443^H^@/^@^D^@^A^@^H^@^W^Aþÿÿÿ^H^@^X^Aþÿÿÿ
^@^H^@^Y^H^@^@^@^@
^@^G^@CYGNUS.^@^S^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^Z^@^A^@^V^@^V^@T^A^@^C^@^@^@^@^@^@^@
^@^L^@^F^@SECURITY^H^@Ó^@■¦3¾^H^@0^@^A^@^@^@^H^@^A^@^A^@^@^@^H^@½^@FILE
~
~
~
~
                                                                    10,35-41      All
```

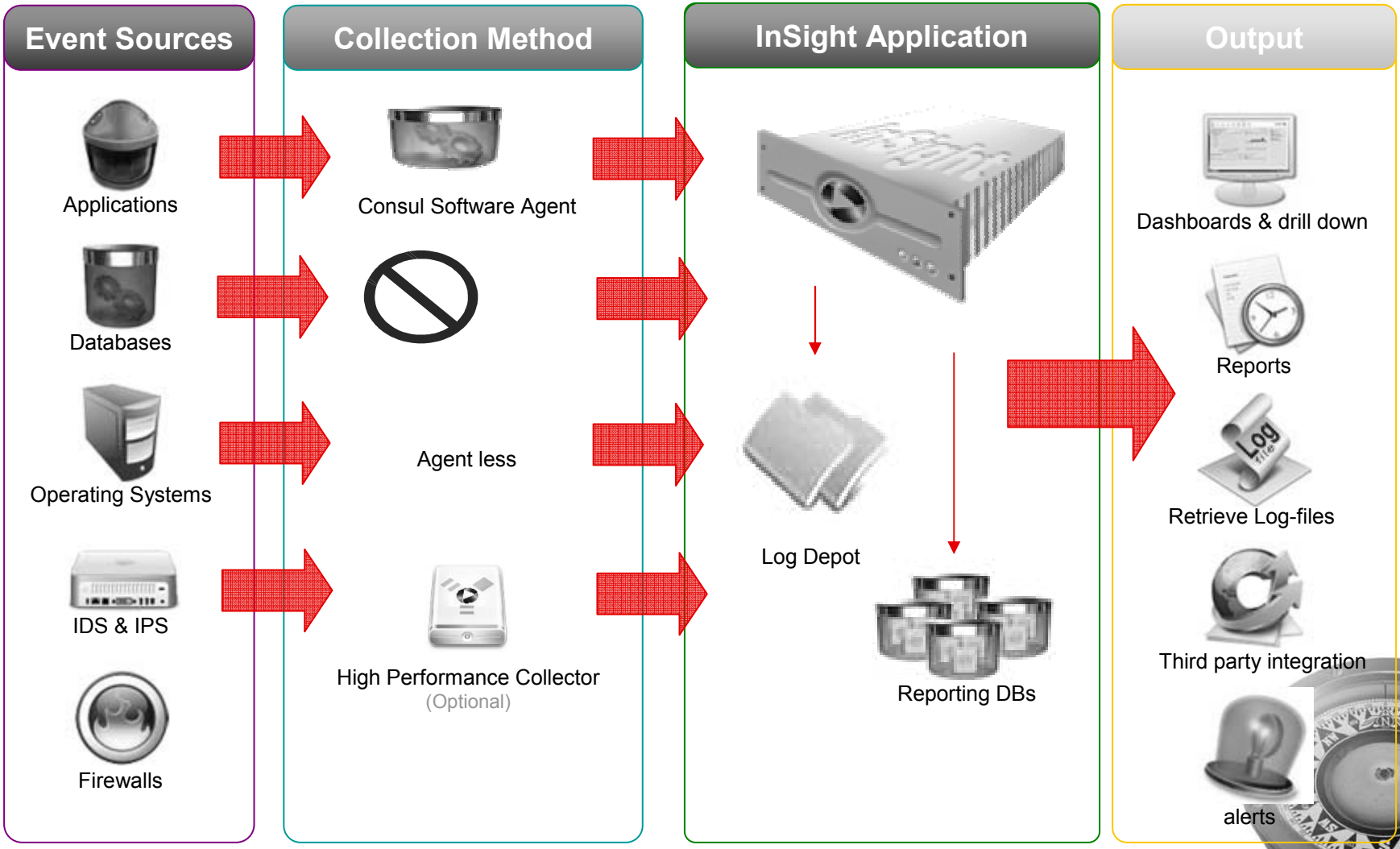
My Computer

Filtrare le informazioni



Severity	When	#	What	Where	Who	from Where	on What	Where to
1	Fri Nov 25, 2005 15:34:18 GMT				ator	Finance Server	PROCESS : . / Notepad.exe	Finance Server
70	Fri Nov 25, 2005 15:34:18 GMT					Finance Server	AUDITLOG : . / -	Finance Server
1	Fri Nov 25, 2005 15:34:21 GMT					Finance Server	PROCESS : . / Notepad.exe	Finance Server
1	Fri Nov 25, 2005 15:34:28 GMT				ator	Mainframe FIN	PROCESS : . / Notepad.exe	Mainframe FIN
1	Fri Nov 25, 2005 15:35:02 GMT					HR Server	PROCESS : . / Process2212024768	HR Server
30	Fri Nov 25, 2005 15:35:02 GMT				ator	Finance Server	FILE : DataSmartinvest / *	Finance Server
1	Fri Nov 25, 2005 15:35:24 GMT				tterson	Mainframe FIN	PROCESS : . / Runemacs.exe	Mainframe FIN
1	Fri Nov 25, 2005 15:35:24 GMT				ator	Mainframe FIN	PROCESS : . / Emacs.exe	Mainframe FIN
1	Fri Nov 25, 2005 15:35:24 GMT				ator	Mainframe FIN	PROCESS : . / Runemacs.exe	Mainframe FIN
1	Fri Nov 25, 2005 15:37:34 GMT					Web Server	PROCESS : . / Eventvwr.exe	Web Server
2	Fri Nov 25, 2005 15:37:35 GMT				ty	Web Server	OBJECT : . / Handle0	Web Server
2	Fri Nov 25, 2005 15:37:41 GMT				ator	Web Server	OBJECT : . / Handle0	Web Server
2	Fri Nov 25, 2005 15:37:48 GMT				acobs	Web Server	OBJECT : . / Handle0	Web Server
2	Fri Nov 25, 2005 15:38:21 GMT				ings	Web Server	OBJECT : . / Handle0	Web Server
2	Fri Nov 25, 2005 15:38:28 GMT -5	1	Grant : Privilege / Success	Finance Server	Marcy Hoover	Finance Server	OBJECT : . / Handle0	Finance Server
30	Fri Nov 25, 2005 15:38:28 GMT -5	1	Read : Access / Success	Finance Server	ROOT	Finance Server	FILE : DataSmartinvest / Default.cfg	Finance Server
30	Fri Nov 25, 2005 15:38:28 GMT -5	2	Read : File / Success	Finance Server	Administrator	Finance Server	FILE : DataSmartinvest / *	Finance Server
70	Fri Nov 25, 2005 15:38:28 GMT -5	7	Read : Access / Success	Finance Server	ROOT	Finance Server	FILE : DataSmartinvest inadmin / *	Finance Server

Architecture



What makes you special?

LA SICUREZZA ALLA A ALLO Z

Le nuove soluzioni per IBM System z

Milano, 25 settembre 2007 - IBM Forum – Segrate

Roma, 3 ottobre 2007 - Sala Convegni Elveno Pastorelli, Comando Provinciale Vigili del Fuoco - Via Genova 3

IBM Governance and Risk Management
Maximize Value, Manage Risk