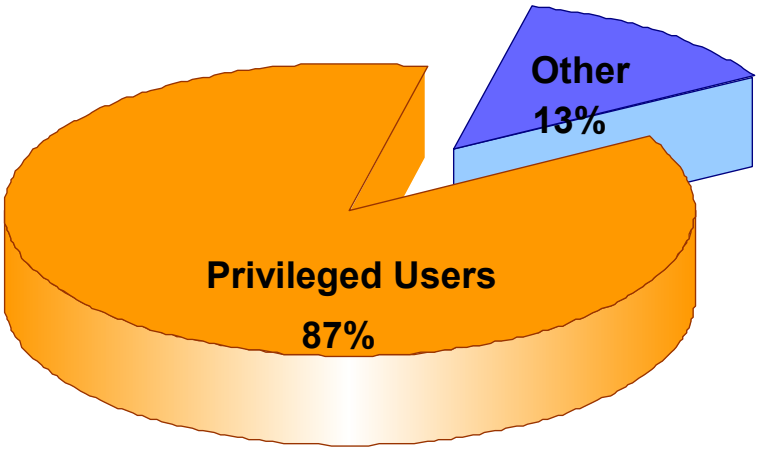
Security Audit & Compliance

Alfonso Ponticelli
Tivoli Security Technical Sales
IBM Italia S.p.A

Compliance&Audit

Criticità delle utenze di tipo privilegiato



Source: USSS/CET Insider Threat Survey 2005

Gli incidenti provocati dalle utenze di tipo privilegiato possono risultare un alto costo per l'azienda e necessitano di una attenta gestione:

- Gli attacchi interni sono costati il 6% del reddito annuo lordo

Verifichiamo se l'effettivo comportamento degli utenti è quello sperato

Richieste relative alla tematica PUMA

Compliance&Audit

Privileged User Monitoring and Audit

Richieste da parte dell'IT e Business management:

- Siamo in grado di controllare se esistono manipolazioni di info sensibili?
- Possiamo verificare le attività degli outsourcers?
- Possiamo ottenere segnalazioni a fronte di attività non autorizzate?

Compliance&Audit

Log management - cosa è necessario rilevare

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

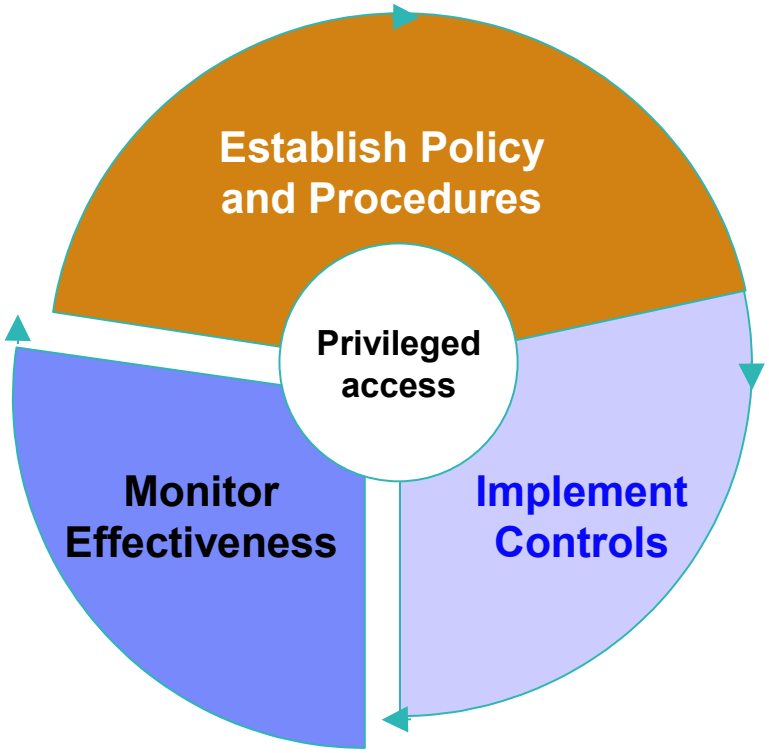
Compliance&Audit

Riuscire ad intervenire in maniera efficace

L'audit è lo strumento più efficace per conoscere e quindi riuscire ad intervenire sui processi di gestione e quindi la salvaguardia del business aziendale.

Quali sono le difficoltà ?

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



IBM Tivoli Compliance Insight Manager Portal

IBM Tivoli Compliance Insight Manager Portal

IBM Tivoli Compliance Portal

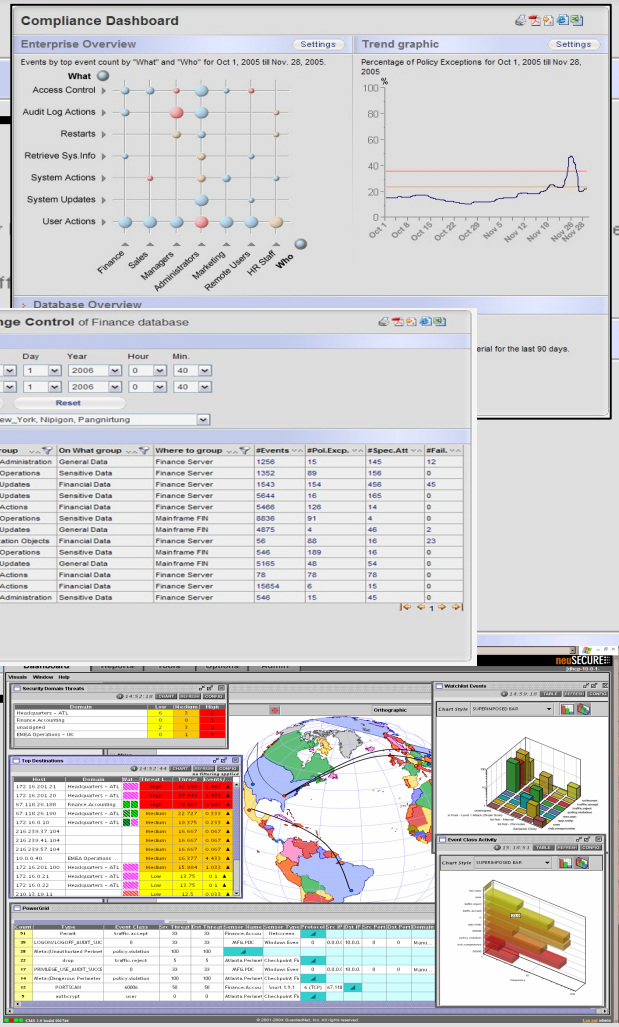
iView	The reporting tool with drill down possibilities
Log Manager	The reporting tool for log management
Policy Generator	A wizard that helps you start using IBM Tivoli Compliance Insight Manager data from your own devices
Scoping	Tool to manage the viewable acces of different users of the system to diff

IBM Tivoli Regulatory Compliance Reports

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

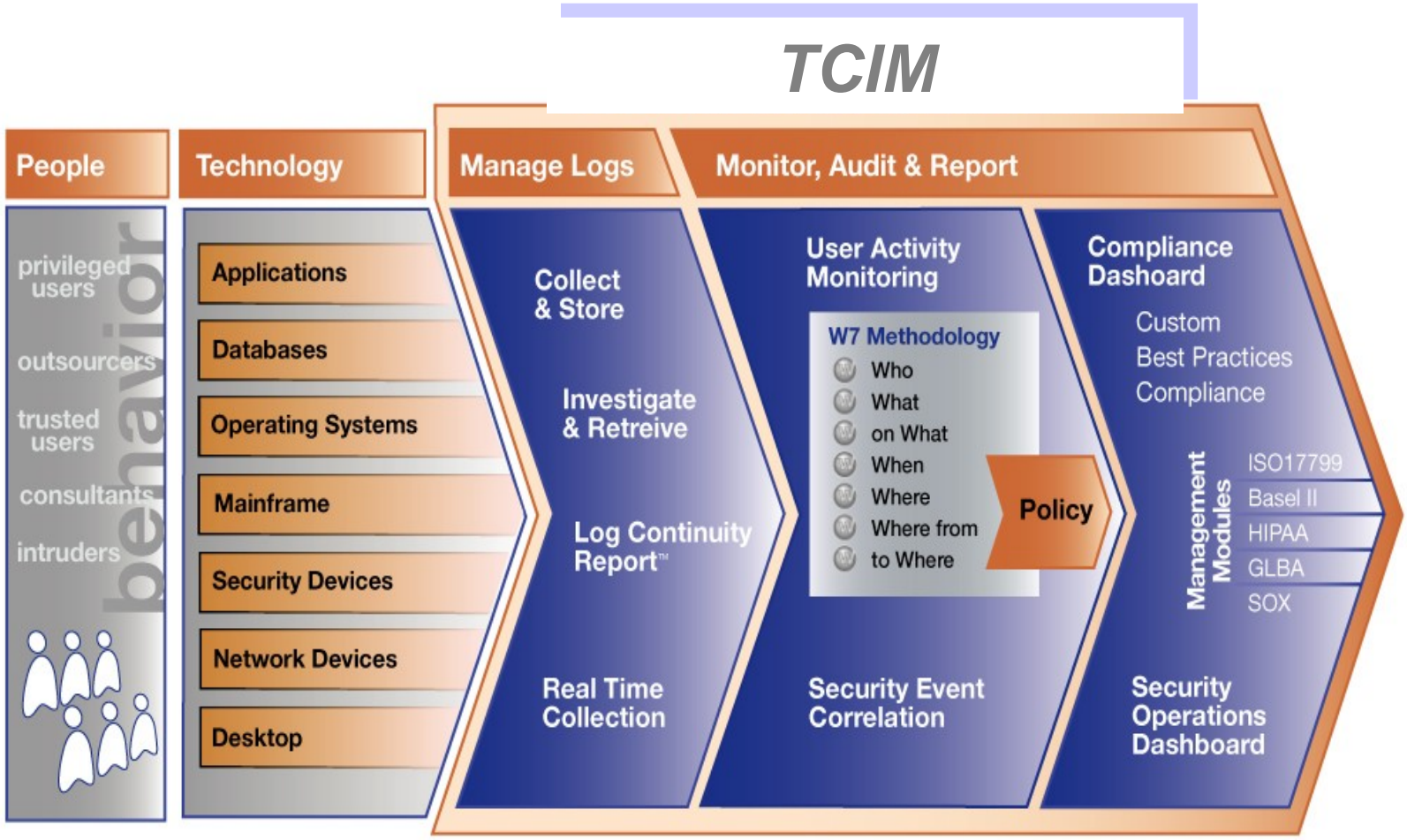
IBM Tivoli Security Operations Portal

Realtime Portal	Open Security Operations Realtime Event Portal
Realtime Reporting Portal	Open Security Operations Realtime Reporting Portal



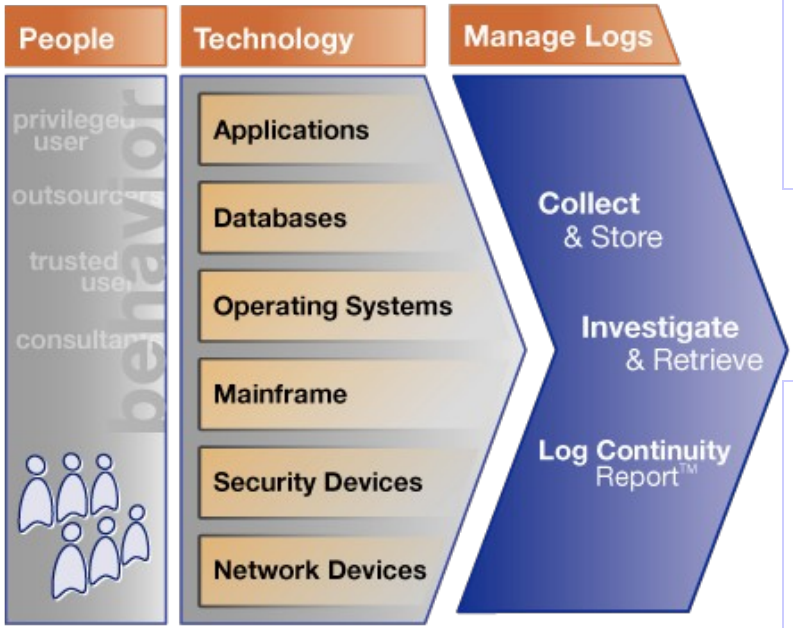
Tivoli Compliance Insight Manager

Le tre C del TCIM: **Cattura**, **Comprende**, **Comunica**



Cattura – Enterprise Log Management

Compliance&Audit



Funzionalità:

- Centralizzazione sicura ed affidabile di log da numerose piattaforme
- Raccolta automatica dei syslogs
- Supporto su attività di raccolta di eventi da log nativi
- Memorizzazione efficiente ed in modalità compressa dei dati
- Possibilità di query e definizione di report custom oltre a quelli offerti nativamente

Benefici:

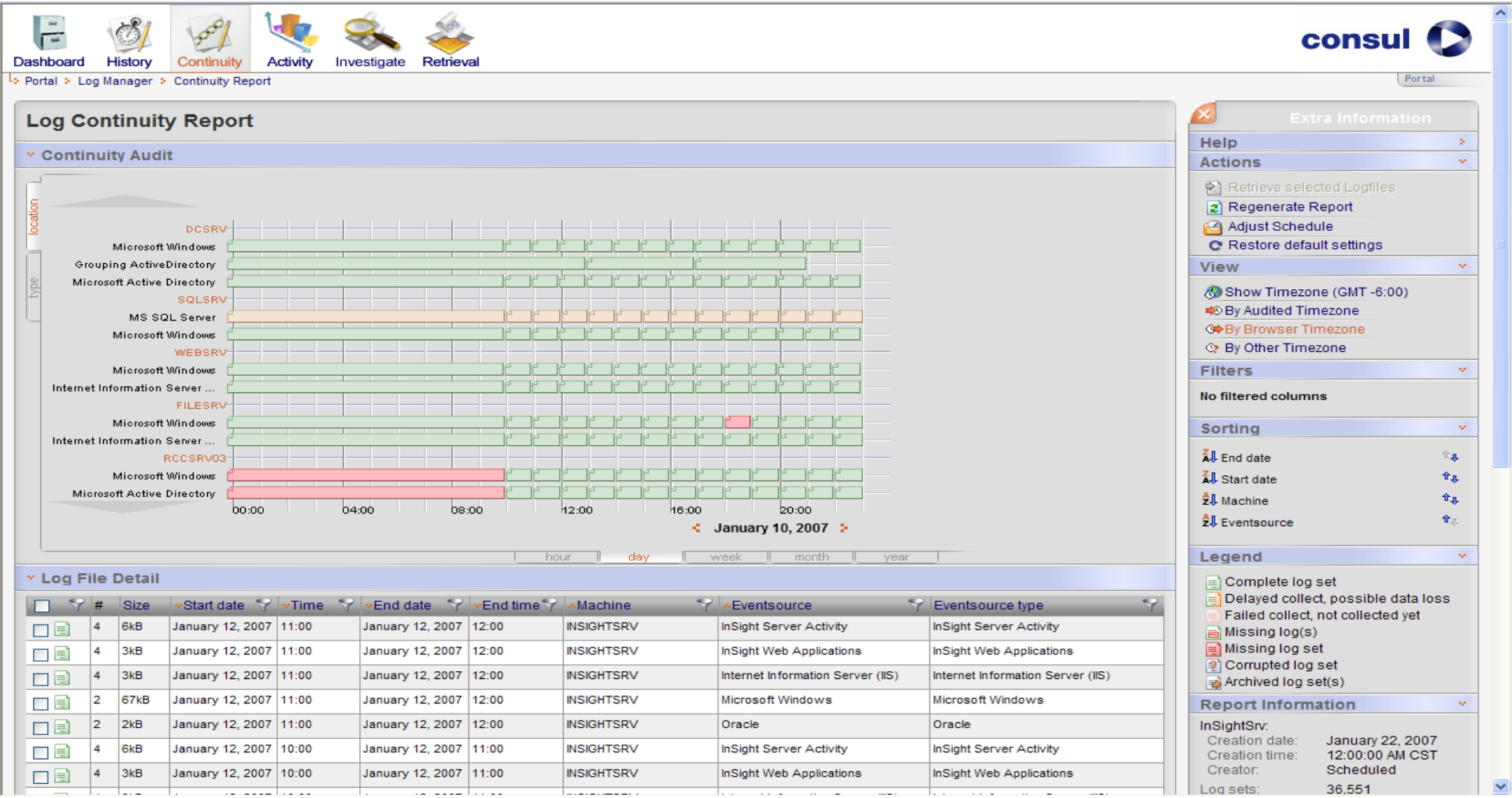
- Riduzione dei costi grazie all'automatizzazione e centralizzazione delle attività di raccolta dei dati
- Garanzia di una costante condizione di "audit ready"

Implementation time: plug and play.

Cattura – Log Continuity Report

Compliance&Audit

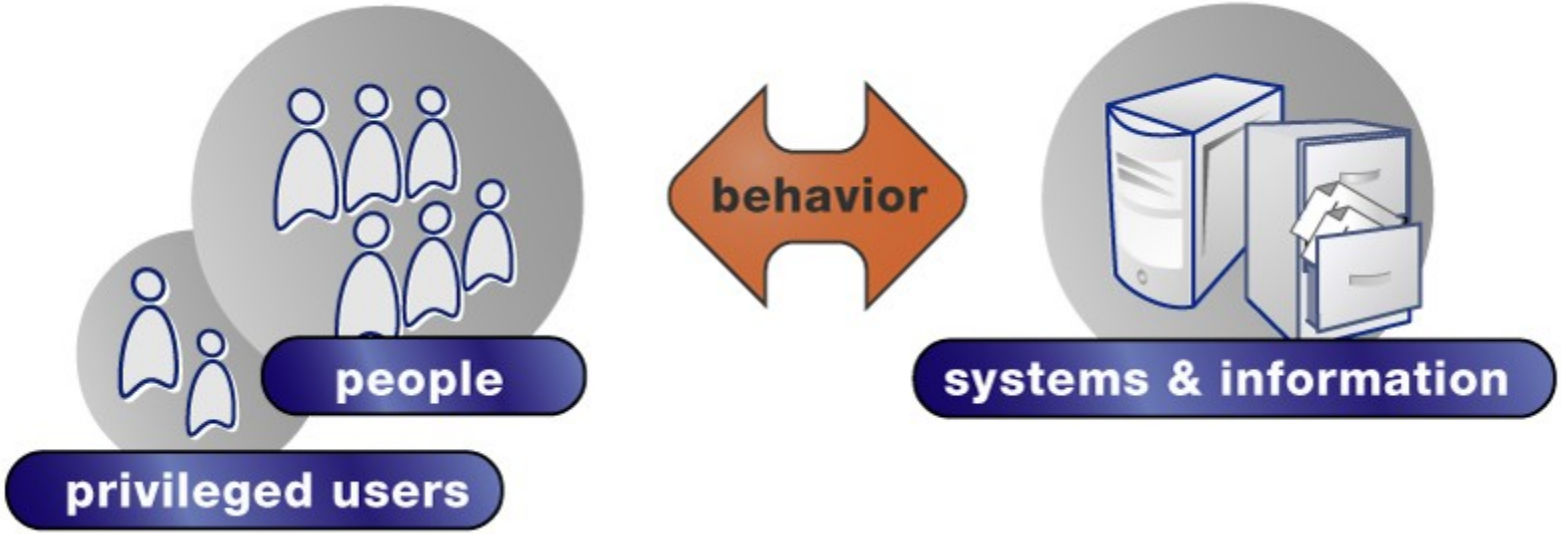
Controllo automatico che evidenzia la continuità e la completezza del processo di log management



#	Size	Start date	Time	End date	End time	Machine	Eventsource	Eventsource type
4	6kB	January 12, 2007	11:00	January 12, 2007	12:00	INSIGHTSRV	InSight Server Activity	InSight Server Activity
4	3kB	January 12, 2007	11:00	January 12, 2007	12:00	INSIGHTSRV	InSight Web Applications	InSight Web Applications
4	3kB	January 12, 2007	11:00	January 12, 2007	12:00	INSIGHTSRV	Internet Information Server (IIS)	Internet Information Server (IIS)
2	67kB	January 12, 2007	11:00	January 12, 2007	12:00	INSIGHTSRV	Microsoft Windows	Microsoft Windows
2	2kB	January 12, 2007	11:00	January 12, 2007	12:00	INSIGHTSRV	Oracle	Oracle
4	6kB	January 12, 2007	10:00	January 12, 2007	11:00	INSIGHTSRV	InSight Server Activity	InSight Server Activity
4	3kB	January 12, 2007	10:00	January 12, 2007	11:00	INSIGHTSRV	InSight Web Applications	InSight Web Applications

Compliance&Audit

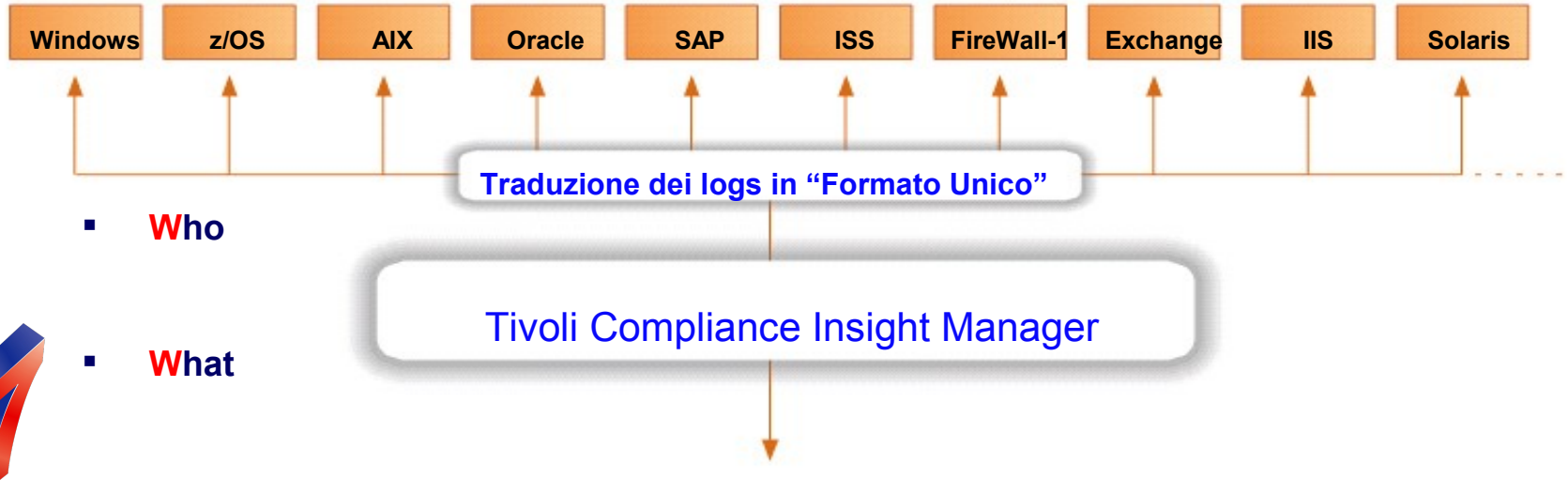
Comprende – Verifica delle attività degli utenti



87% degli incidenti interni sono causati da utenti privilegiati.

Compliance&Audit

Comprende – Centralizzazione dei log



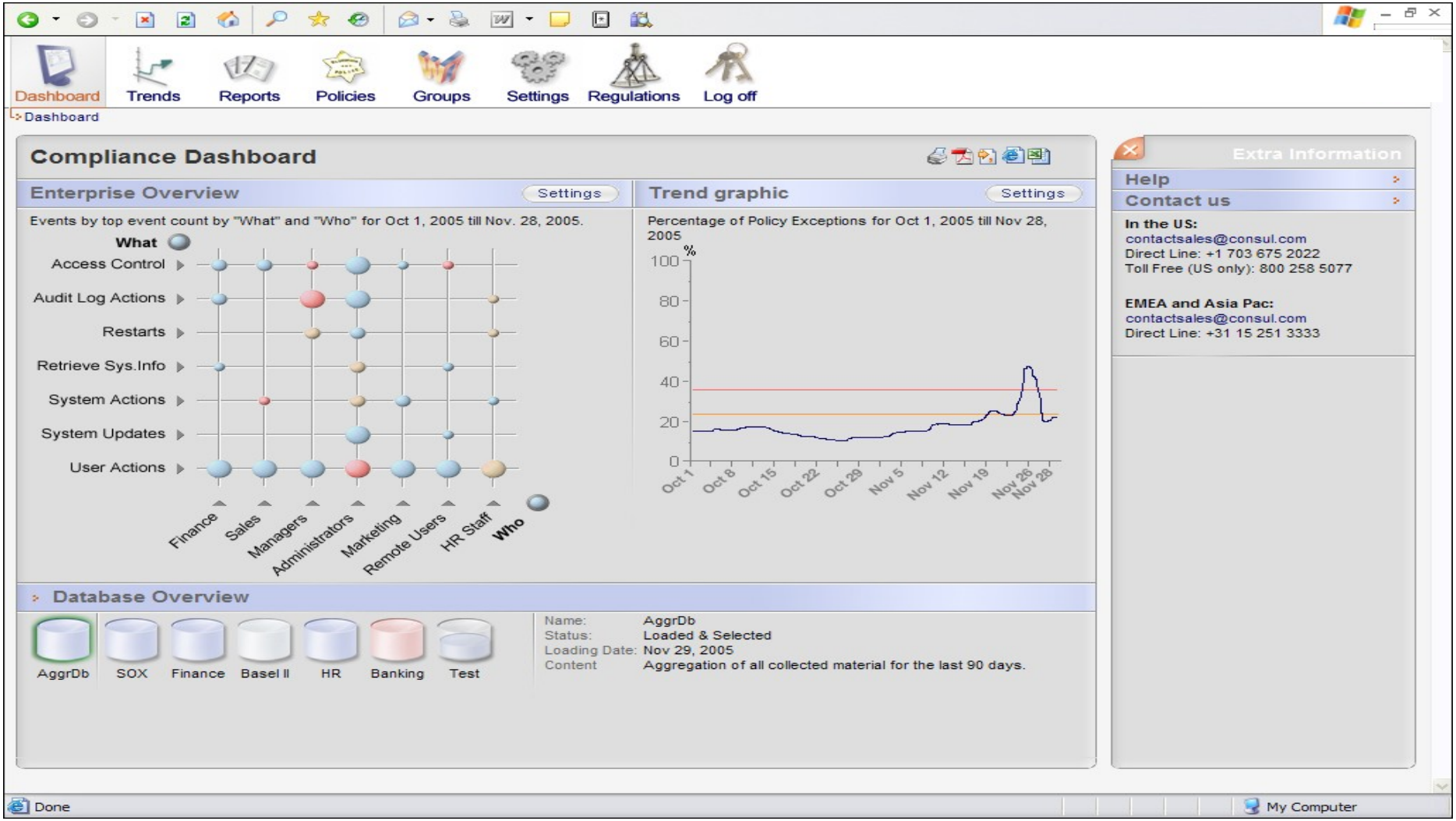
- **Who**
- **What**
- **On What**
- **When**
- **Where**
- **Where From**

TCIM ottimizza le informazioni di security e compliance ottimizzando I tempi ed I costi attraverso l'automatizzazione dei processi di monitoraggio aziendale

Comprende – Security Compliance Dashboard

Compliance&Audit

Dopo la normalizzazione W7 tutti i dati di log sono riassunti in un unico grafico



Comprende – Policy Exception

Compliance&Audit

Definizione di policy che regolamentano cosa è permesso sui sistemi

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

Verifica se gli utenti eseguono attività consentite

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

Comprende – Special Attention

Compliance&Audit

Verifica delle variabili che caratterizzano l'attività sui sistemi

Attention Rules:

Who	What	When	Where	OnWhat	WhereFrom
Database Admin	Delete Data	Out of Office Hours		Financial Data	
Database Admin	Delete Data	Out of Office Hours		HR Data	
	Collect Failure				
				Sensitive Groups	
IT				Non-Public Data	
IT				Organizational Data	
Administrators				Non-Public Data	
Administrators				Organizational Data	
IT				Sensitive Data	
IT				Proprietary Data	
Administrators				Sensitive Data	
Administrators				Proprietary Data	
MailAdmins	Logon - Unavlbl			Mailboxes	

Policy | Attention

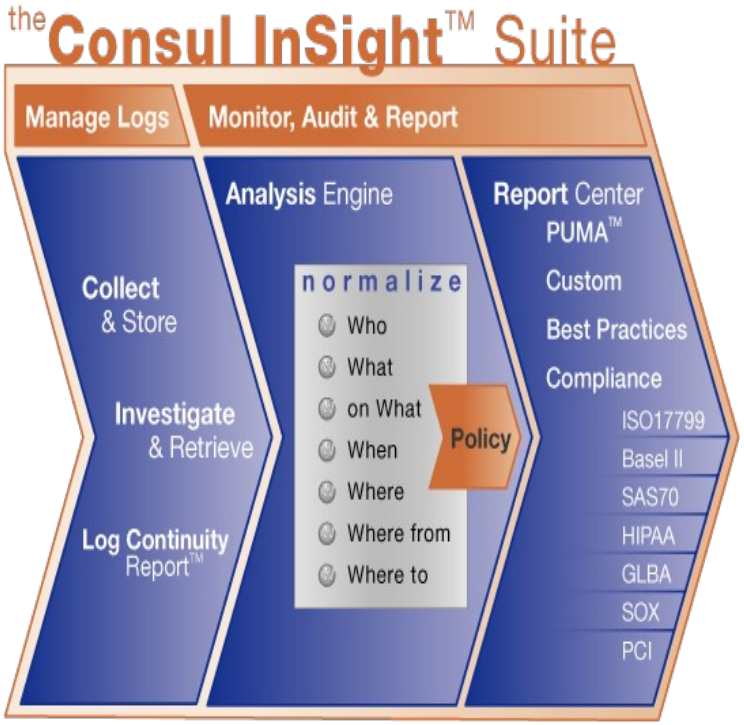
SMTP

SNMP

Script

Comunica – Funzionalità di Reporting

Compliance&Audit



Funzionalità:

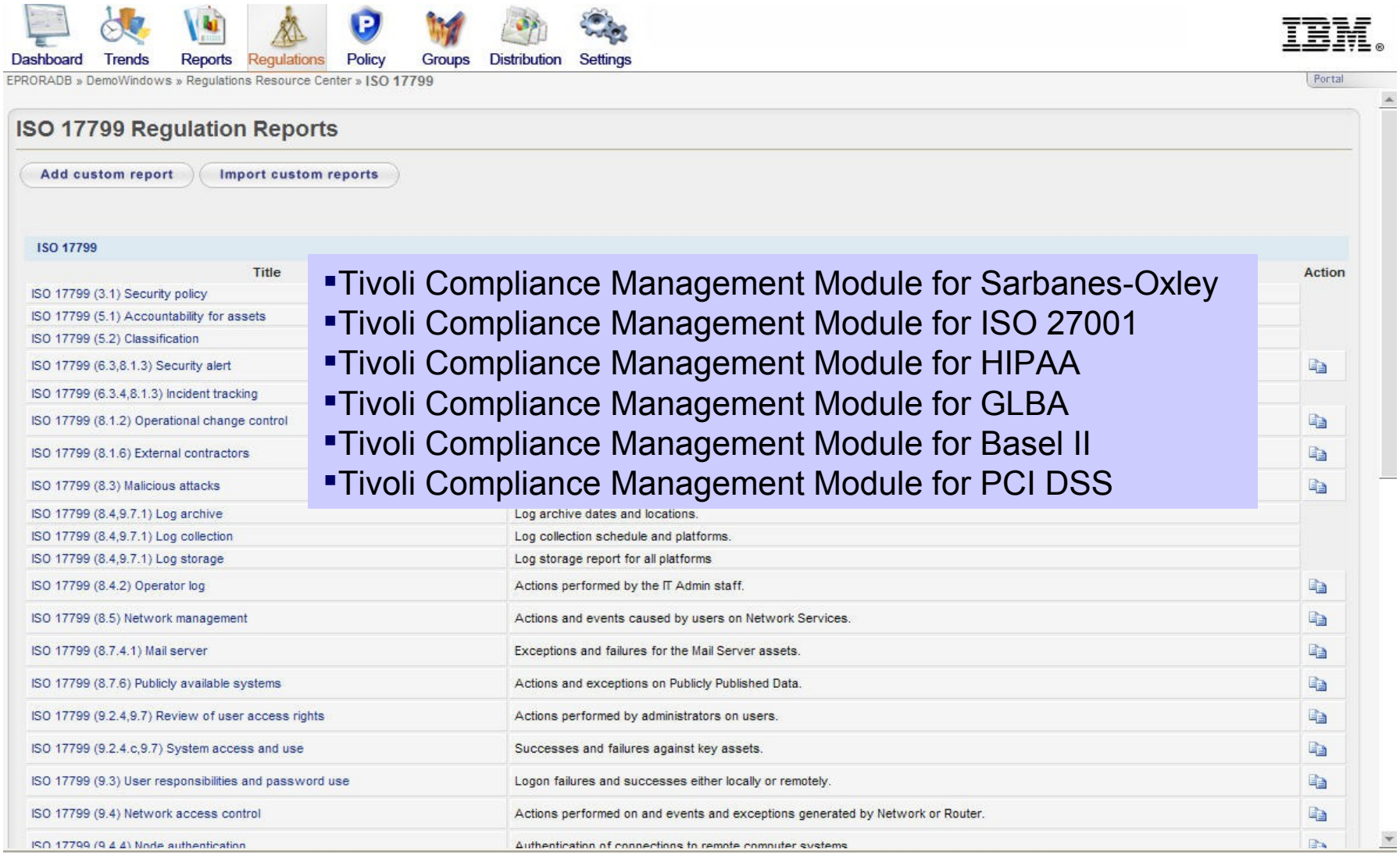
- Centinaia di reports
- Moduli di Compliance
- Alert di Special attention
- Reports Custom

Benefici:

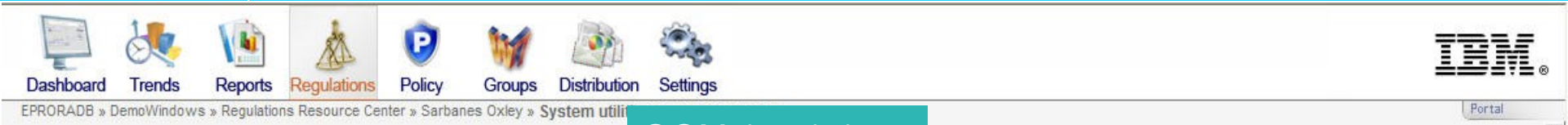
- Riduce l'impegno e del tempo richiesto per l'audit e per la definizione dei Reports
- Riduzione dei rischi di minacce a dati sensibili:
  - Protezione dei dati
  - Controllo sui change

Moduli come baseline per la compliance

Compliance&Audit



- Tivoli Compliance Management Module for Sarbanes-Oxley
- Tivoli Compliance Management Module for ISO 27001
- Tivoli Compliance Management Module for HIPAA
- Tivoli Compliance Management Module for GLBA
- Tivoli Compliance Management Module for Basel II
- Tivoli Compliance Management Module for PCI DSS



SOX 1.4.1.1

System utilities usage summary
Database DemoWindows on Server EPRORADB

Setup:

	Month	Day	Year	Hour	Min.
Start time	September	12	2006	22	0
End time	July	6	2007	9	49

Execute Reset

Time zone: GMT-06:00 Cancun, Chicago, Knox

Who group	What group	When group	#Events	#Pol. Excp.	#Spec. Att	#Fail.
Oracle.DBA	InSight Maintenance	Office Hours	1	0	0	0
Oracle.DBA	User Actions	Office Hours	1	0	0	0
SysAdmin.R	Administration	Office Hours	1	0	0	0
SysAdmin.R	Security Changes	Office Hours	26	0	0	0
SysAdmin.R	User Actions - File	Office Hours	1	0	0	0
SysAdmin.R	InSight Maintenance	Office Hours	1	0	0	0
SysAdmin.R	User Actions	Office Hours	1	0	0	0
Finance.MSSQL.RW	Administration	Office Hours	1	0	0	0
Finance.MSSQL.RW	Security Changes	Office Hours	63	0	0	0
Finance.MSSQL.RW	User Actions - File	Office Hours	1	0	0	0
Finance.MSSQL.RW	InSight Maintenance	Office Hours	1	0	0	0
Finance.MSSQL.RW	User Actions	Office Hours	1	0	0	0
Finance.Oracle.RW	Administration	Office Hours	1	0	0	0
Finance.Oracle.RW	Security Changes	Office Hours	63	0	0	0
Finance.Oracle.RW	User Actions - File	Office Hours	1	0	0	0
Finance.Oracle.RW	InSight Maintenance	Office Hours	1	0	0	0
Finance.Oracle.RW	User Actions	Office Hours	1	0	0	0
Finance.R	Administration	Office Hours	1	0	0	0
Finance.R	Security Changes	Office Hours	77	0	0	0
Finance.R	User Actions - File	Office Hours	1	0	0	0
Finance.R	InSight Maintenance	Office Hours	1	0	0	0
Finance.R	User Actions	Office Hours	1	0	0	0
Finance.RW	Administration	Office Hours	1	0	0	0
Finance.RW	Security Changes	Office Hours	63	0	0	0

Le Utility di sistema devono essere usate esclusivamente da staff specializzato in determinate finestre temporali. Gli eventi che non rispondono a tale regola vengono evidenziate come exceptions.

Extra Information

Help

System utilities should only be used by appropriate staff at appropriate times. This is defined in the policy and exceptions to this are reported as policy exceptions. Additionally you should put in place special attention events for key systems.

Background

Paragraph FFIEC 1.4.1.1

Filters

Support:

To contact IBM Support:

Electronically: IBM Tivoli Software Support website

Telephone: Refer to the IBM Software Support Handbook for Phone Numbers Worldwide

SOX 9.2.4

EPRORADB » DemoWindows » Regulations Resource Center » Sarbanes Oxley » System access and use

Portal

System access and use
Database DemoWindows on Server EPRORADB

Setup:

	Month	Day	Year	Hour	Min.
Start time	September	12	2006	22	0
End time	July	6	2007	9	49

Execute Reset

Time zone: GMT-06:00 Cancun, Chicago, Knox

Who group	What group	On What group	#Fail.	#Succ.
Enterprise Admins	Security Changes	InSight Objects	0	471
Enterprise Admins	Security Changes	Databases	21	0
Enterprise Admins	Security Changes	Exchange Components	49	88
Enterprise Admins	Security Changes	Servers	2	0
Enterprise Admins	Security Changes	Financial Data - Sensitive	0	47
Enterprise Admins	User Actions - File	Administration Objects	0	1352
Enterprise Admins	User Actions - File	Not Finance or HR data	28	1338
Enterprise Admins	User Actions - File	Administration	0	44
Enterprise Admins	User Actions - File	HR Data	0	109
Enterprise Admins	User Actions - File	HR Data - Low	0	109
Enterprise Admins	User Actions - File	System Utilities	0	7
Enterprise Admins	User Actions - File	User Actions - File	0	1308
Enterprise Admins	User Actions - File	Connections	28	88
Enterprise Admins	User Actions - File	InSight Maintenance	0	1352
Enterprise Admins	User Actions - File	User Actions	0	1308
Enterprise Admins	User Actions - File	InSight Objects	0	332
Enterprise Admins	User Actions - File	Databases	21	0
Enterprise Admins	User Actions - File	Exchange Components	49	88
Enterprise Admins	User Actions - File	Servers	2	0
Enterprise Admins	User Actions - File	Financial Data - Sensitive	0	44
Enterprise Admins	Alerts	Administration Objects	2	0
Enterprise Admins	Alerts	Not Finance or HR data	2	0
Enterprise Admins	Alerts	System Updates	2	0
Enterprise Admins	Alerts	Servers	5	0

Evidenza degli accessi a risorse aziendali, con indicazione del numero di success e failure. Gli accessi in failure indicano che i diritti di accesso attribuiti agli utenti potrebbero non essere sufficienti e quindi bisognosi di ricertificazione. Nel contempo la possibilità di verificare se gli utenti che hanno acceduto a specifiche risorse critiche, erano e sono leggittimati a tali attività

Extra Information

Help

This report shows accesses by users to key resources and shows success and failures. Failures indicate that the user rights are not sufficient to access the resource. These failures need to be reviewed to determine if this user does have legitimate needs to access this data. Similarly, successful accesses must be reviewed on a regular basis to determine if these users should still have rights to access this resource and if not have the access revoked changed.

Background

Paragraph 9.2.4.c
Paragraph 9.7

Support:

To contact IBM Support:

Electronically: IBM Tivoli Software Support website

Telephone: Refer to the IBM Software Support Handbook for Phone Numbers Worldwide

SOX 9.3

EPRORADB » DemoWindows » Regulations Resource Center » Sarbanes Oxley » User responsibilities and password use

Portal

User responsibilities and password use
Database DemoWindows on Server EPRORADB

Setup:

	Month	Day	Year	Hour	Min.
Start time	September	12	2006	22	0
End time	July	6	2007	9	49

Execute Reset

Time zone: GMT-06:00 Cancun, Chicago, Knox

Evidenza dei login in failure a sistemi ed a servizi di rete, in modo da poter verificare se trattasi di dimenticanza di password oppure un tentativo di violazione. Punto di partenza per verificare l'esistenza di eventuali furti di identità.

Who group	When group	Where group	#Events	#Pol. Excp.	#Spec. Att	#Fail.	#Succ.
Domain Users	Office Hours	Mail	62	0	13	5	57
Domain Users	Office Hours	Production Systems	1630	0	13	7	1623
Domain Users	Office Hours	Systems with non-segregated administration	1630	0	13	7	1623
Domain Users	Office Hours	crmlab.info	62	0	13	5	57
Domain Users	Out of Office Hours	Production Systems	1	0	0	0	1
Domain Users	Out of Office Hours	Systems with non-segregated administration	1	0	0	0	1
Enterprise Administrators	Office Hours	Mail	44	0	13	5	39
Enterprise Administrators	Office Hours	Production Systems	1179	0	13	7	1172
Enterprise Administrators	Office Hours	Systems with non-segregated administration	1179	0	13	7	1172
Enterprise Administrators	Office Hours	crmlab.info	44	0	13	5	39
Enterprise Administrators	Out of Office Hours	Production Systems	1	0	0	0	1
Enterprise Administrators	Out of Office Hours	Systems with non-segregated administration	1	0	0	0	1
Enterprise Admins	Office Hours	Mail	44	0	13	5	39
Enterprise Admins	Office Hours	Production Systems	1179	0	13	7	1172
Enterprise Admins	Office Hours	Systems with non-segregated administration	1179	0	13	7	1172
Enterprise Admins	Office Hours	crmlab.info	44	0	13	5	39
Enterprise Admins	Out of Office Hours	Production Systems	1	0	0	0	1
Enterprise Admins	Out of Office Hours	Systems with non-segregated administration	1	0	0	0	1
Exchange Domain Servers	Office Hours	Mail	44	0	13	5	39
Exchange Domain Servers	Office Hours	Production Systems	1179	0	13	7	1172
Exchange Domain Servers	Office Hours	Systems with non-segregated administration	1179	0	13	7	1172
Exchange Domain Servers	Office Hours	crmlab.info	44	0	13	5	39
Exchange Domain Servers	Out of Office Hours	Production Systems	1	0	0	0	1
Exchange Domain Servers	Out of Office Hours	Systems with non-segregated administration	1	0	0	0	1

Extra Information

Help

This report shows failed attempts to log in to the systems and services in the network. Failed logons can be as simple as someone having forgotten a password or an attempted breach of security. This report is an excellent starting point for someone looking to determine in appropriate use of user information or identity theft.

Background

Paragraph 9.3

Filters

This report is based on the following equality:

What group	Logon, Logon Failures, Remote Logon, Remote Logon Failures

Support:

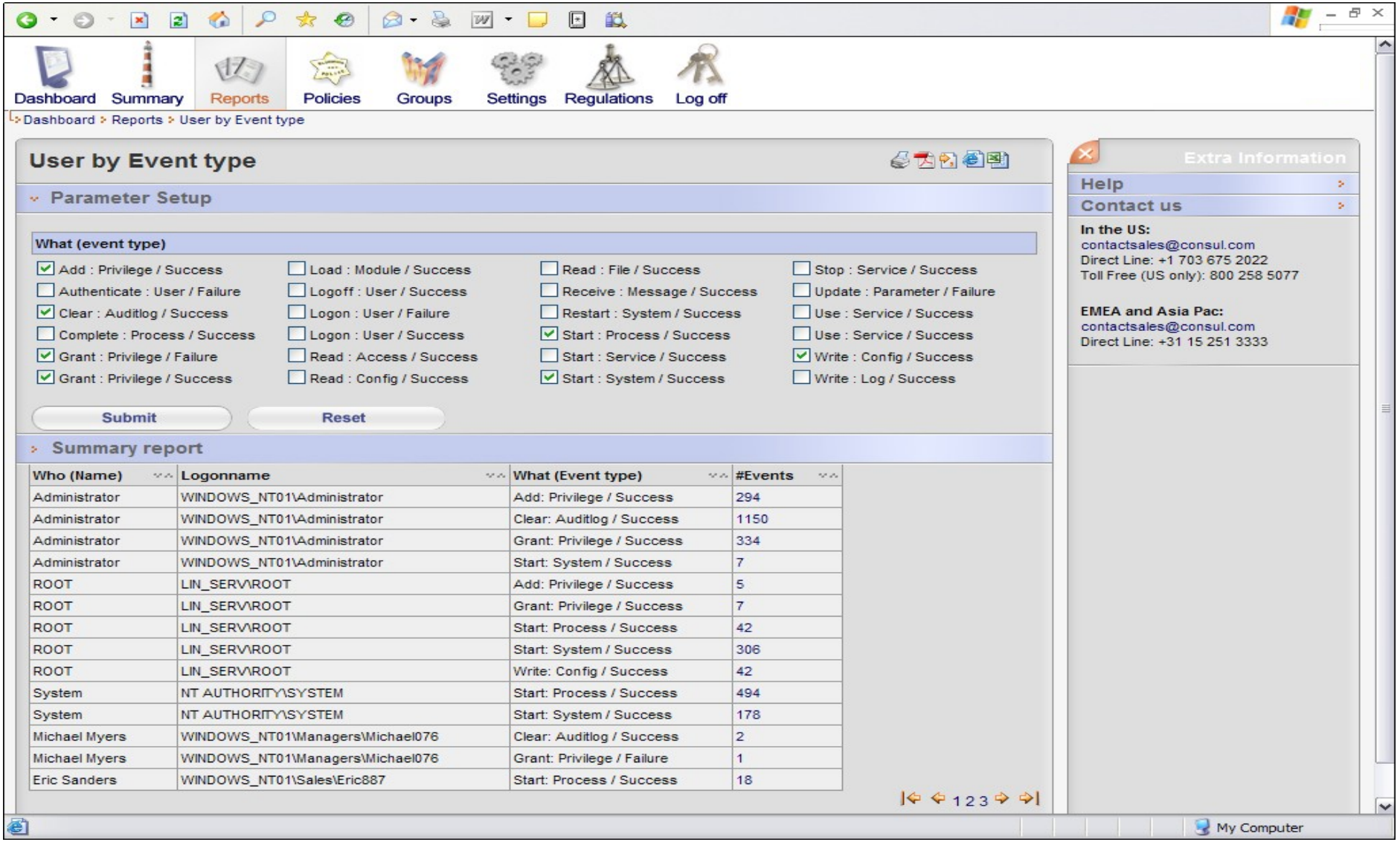
To contact IBM Support:

Electronically: IBM Tivoli Software Support website

Telephone: Refer to the IBM Software Support Handbook for Phone Numbers Worldwide

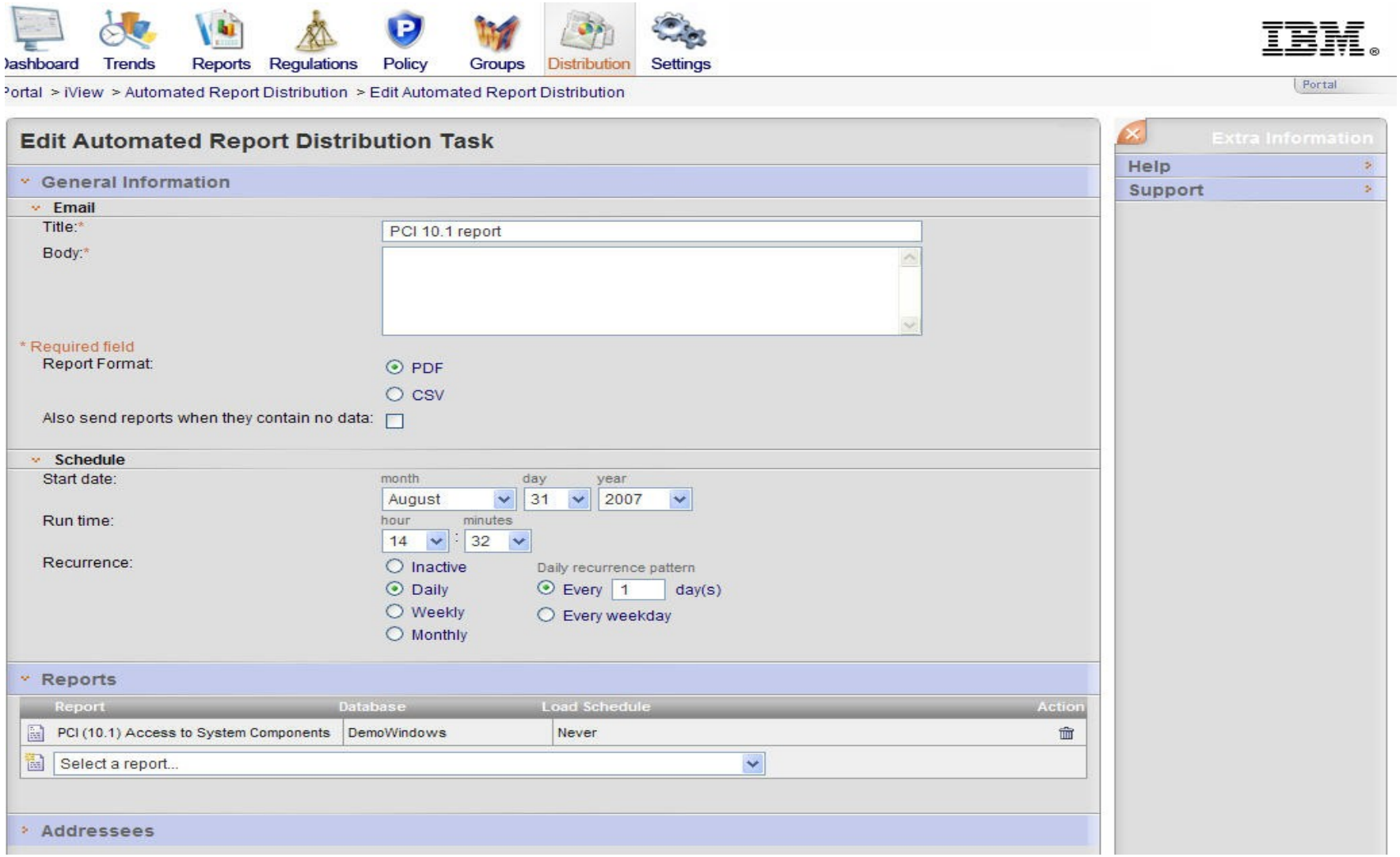
Query e viste dedicate (1/3)

Compliance&Audit



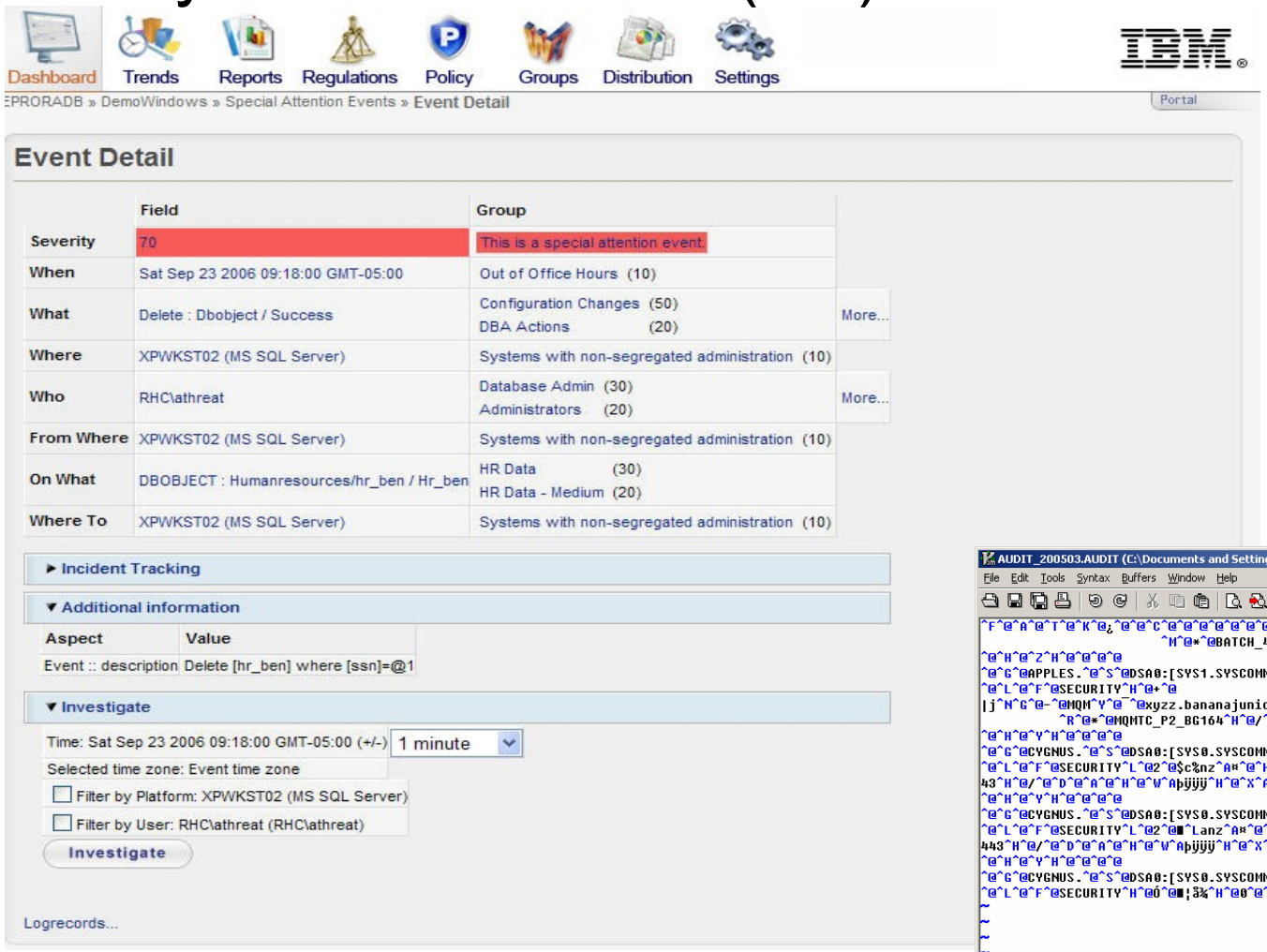
Query e viste dedicate (2/3)

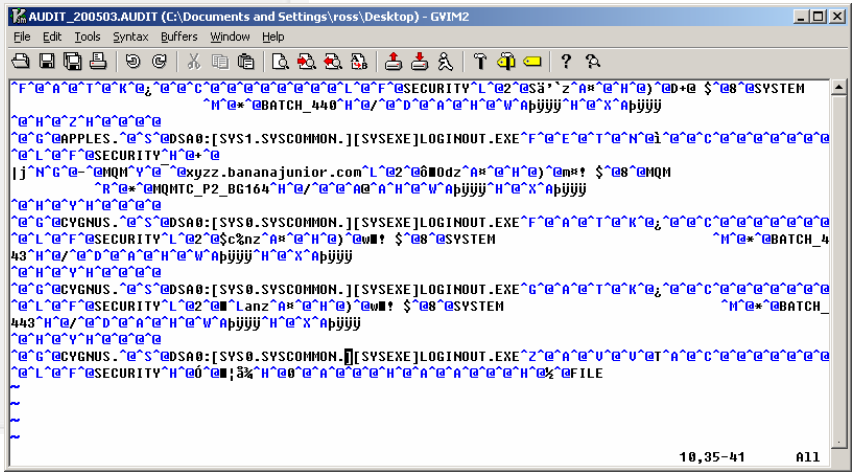
Compliance&Audit



Compliance&Audit

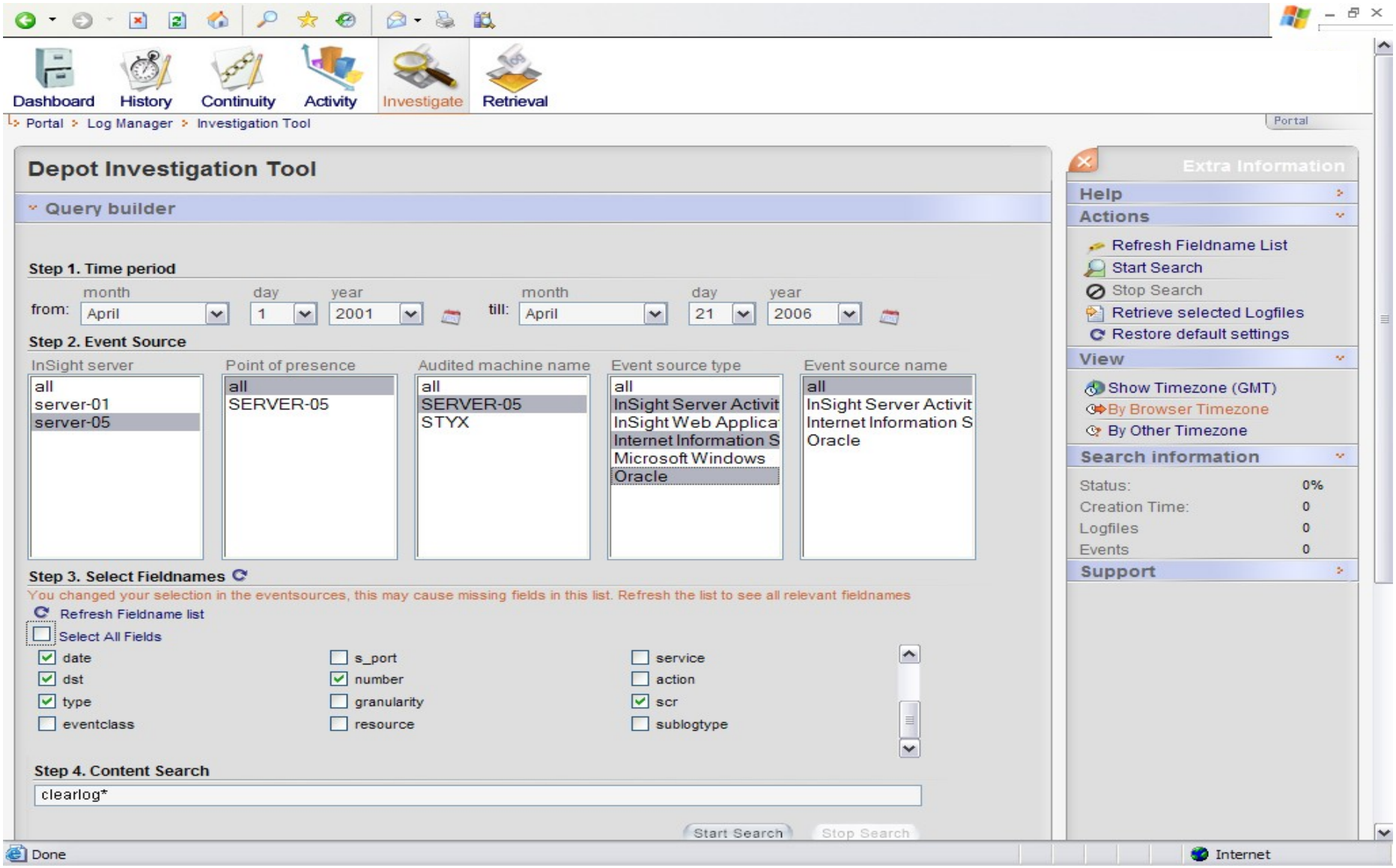
Query e viste dedicate (3/3)



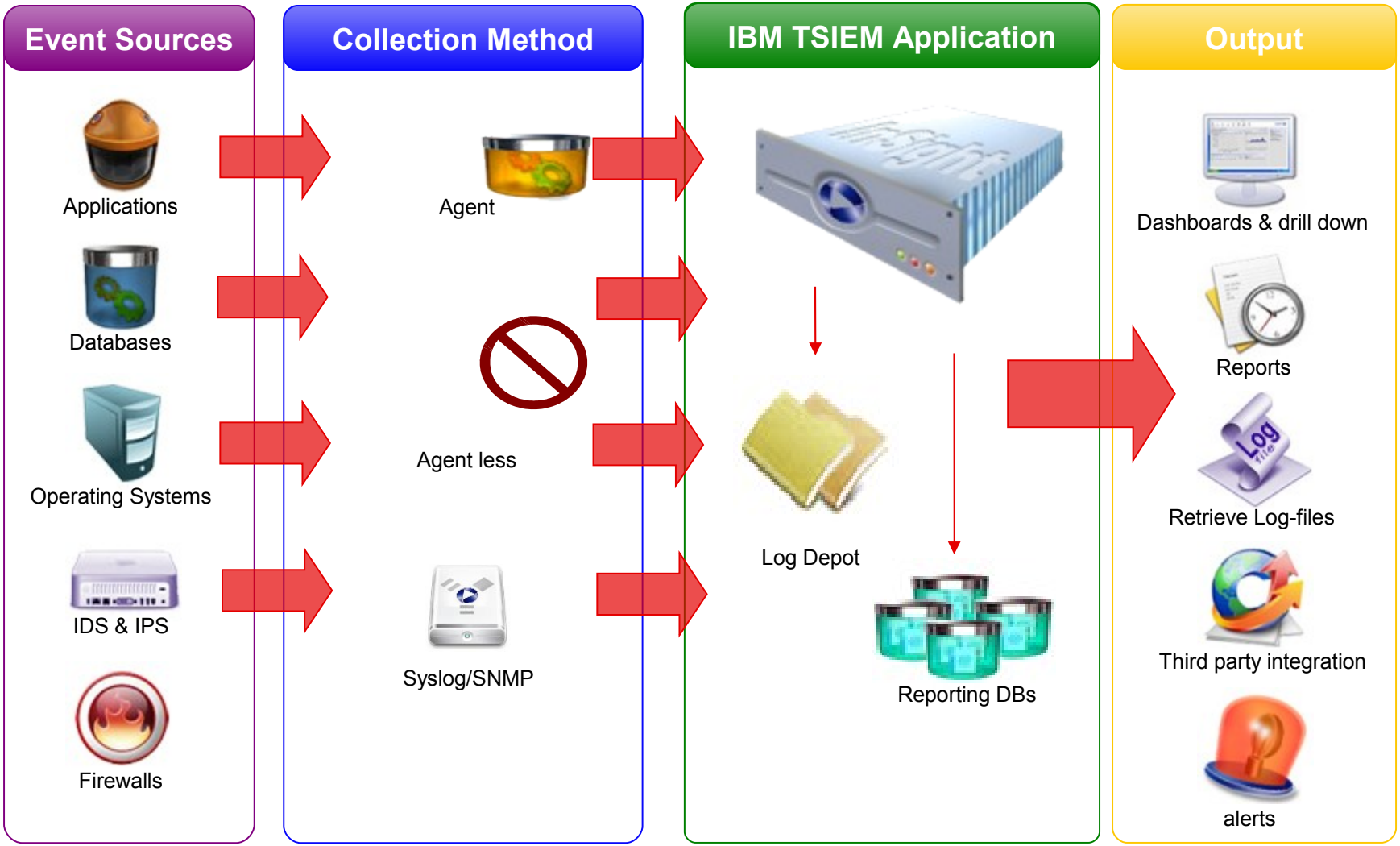


Tool di ricerca sui dati originali

Compliance&Audit



Architettura



Platform Requirements

- **Standard Server (minimum requirements)**
  - 2 x Xeon 3.0Ghz CPU
  - 6 GB RAM
  - Disk storage depends on log volume and retention policy*
    - Guideline: *1.5 * (total GB of daily logs / 10 compression factor) * number of days to keep in repository + 25GB*

Log source supportate dal TCIM

Compliance&Audit

Supported SERVERS:

- IBM AIX Audit logs
- IBM AIX syslog
- IBM OS/400 & i5/OS journals
- Hewlett-Packard HP-UX Audit logs
- Hewlett-Packard HP-UX syslog
- Hewlett-Packard NonStop (Tandem)
- Hewlett-Packard OpenVMS
- Hewlett-Packard Tru64
- Microsoft Windows
- Novell Netware
- Novell NSure Audit
- Novell Audit
- Novell Suse Linux
- RedHat Linux
- Stratus VOS
- SUN Solaris BSM Audit logs

Supported MAINFRAME:

- IBM z/OS + RACF
- IBM z/OS + CA ACF2
- IBM z/OS + CA Top Secret
- CA Top Secret for VSE/ESA

Supported APPLICATIONS:

- Tivoli Identity Manager
- Tivoli Access Manager for OS and for e-Business
- FUTURE (in engineering pipeline): TFIM, TDS, TDI, TSOM
- SAP R/3 on Windows, Solaris, AIX, HP-UX
- Misys OPICS
- BMC Identity Manager
- CA eTrust (Netegrity) SiteMinder
- RSA Authentication Server
- Microsoft Exchange
- IBM Lotus Domino Server on Windows
- Microsoft Internet Information server
- SUN iPlanet Web Server on Solaris

Supported DATABASES:

- IBM DB2 on z/OS
- IBM DB2 / UDB on Windows, Solaris, AIX
- Microsoft SQL Server application logs
- Microsoft SQL Server trace files
- Oracle DBMS on Windows, AIX, Solaris, HP-UX
- Oracle DBMS FGA on Windows, AIX, Solaris, HP-UX
- Sybase ASE on Windows, AIX, Solaris, HP-UX

Supported DEVICES:

- Cisco Router
- Hewlett-Packard ProCurve Switch
- Blue Coat Systems ProxySG Series
- Check Point Firewall-1
- Cisco PIX
- Cisco VPN Concentrator (3000 series)
- Symantec (Raptor) Enterprise Firewall
- ISS RealSecure
- ISS System Scanner
- McAfee IntruShield IPS Manager
- McAfee ePolicy Orchestrator
- Snort IDS
- Symantec Antivirus
- TrendMicro ScanMail for Domino
- TrendMicro ScanMail for MS Exchange
- TrendMicro ServerProtect for Windows

La soluzione IBM Tivoli Security Information and Event Manager (TSIEM v1.0)