



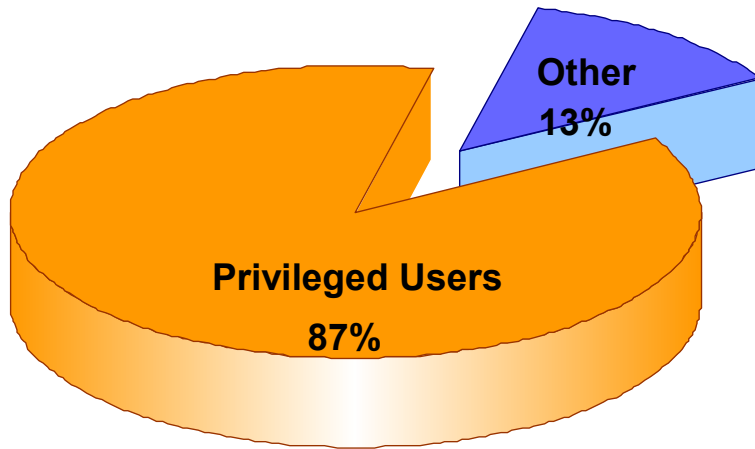
Security, Risk and Compliance

# Security Audit & Compliance

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



# Criticità delle utenze di tipo privilegiato



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

Source: USSS/CET Insider Threat Survey 2005

- 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&amp;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?

# Log management - cosa è necessario rilevare

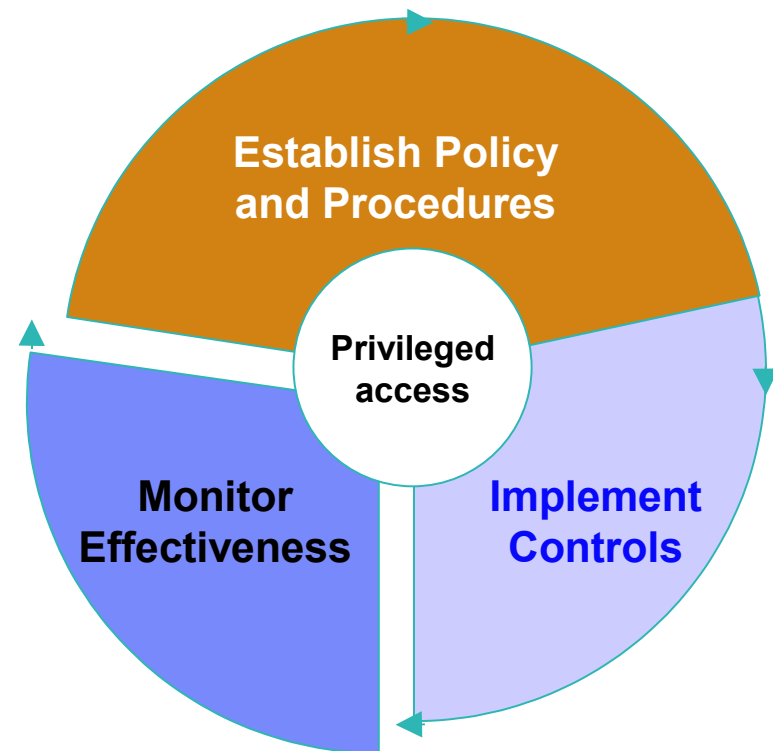
Categoria	Descrizione
<b>Eventi di autenticazione</b>	Eventi di logon / logoff
<b>Eventi di gestione</b>	Start di server, stop, back-up, restore
<b>Change management</b>	Modifiche di configurazione, modifiche sui processi di auditing, modifiche sulla struttura dei database, attività di manutenzione
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

# 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.

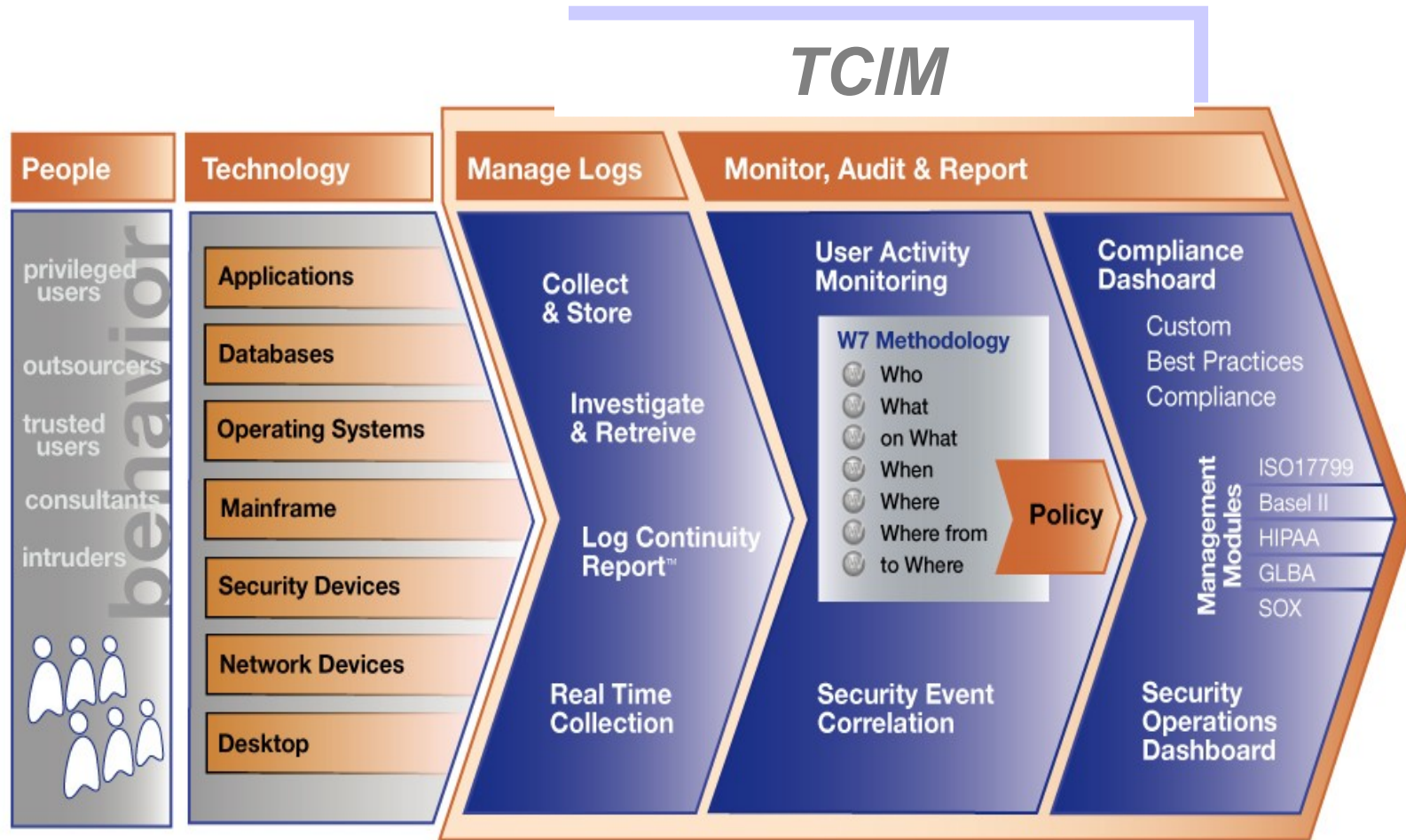
## Quali sono le difficoltà ?

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





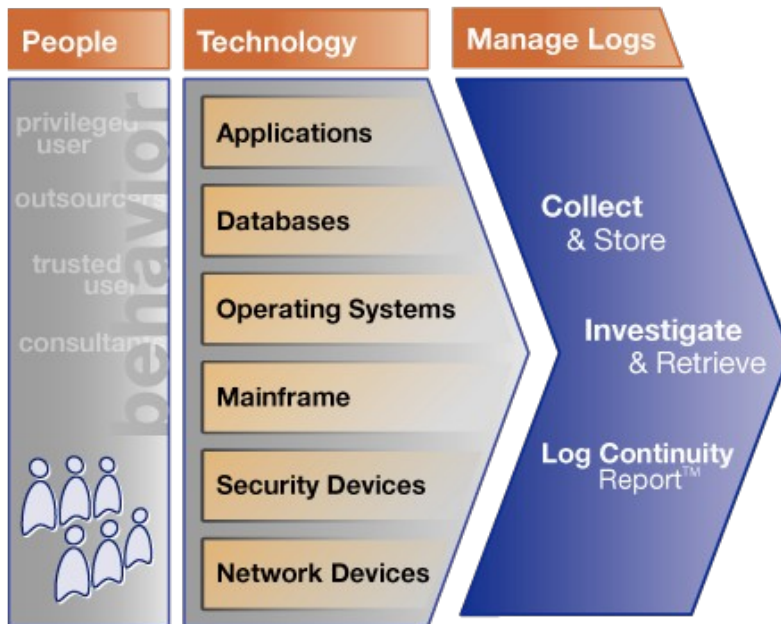
# Le tre C del TCIM: **Cattura**, **Comprende**, **Comunica**





# Cattura – Enterprise Log Management

Compliance &amp; 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

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

Dashboard
History
Continuity
Activity
Investigate
Retrieval

Portal > Log Manager > Continuity Report

## Log Continuity Report

**Continuity Audit**

location

type

January 10, 2007

hour
day
week
month
year

**Log File Detail**

#	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

**Extra Information**

**Help**

**Actions**

- Retrieve selected Logfiles
- Regenerate Report
- Adjust Schedule
- Restore default settings

**View**

- Show Timezone (GMT -6:00)
- By Audited Timezone
- By Browser Timezone
- By Other Timezone

**Filters**

No filtered columns

**Sorting**

- End date
- Start date
- Machine
- Eventsource

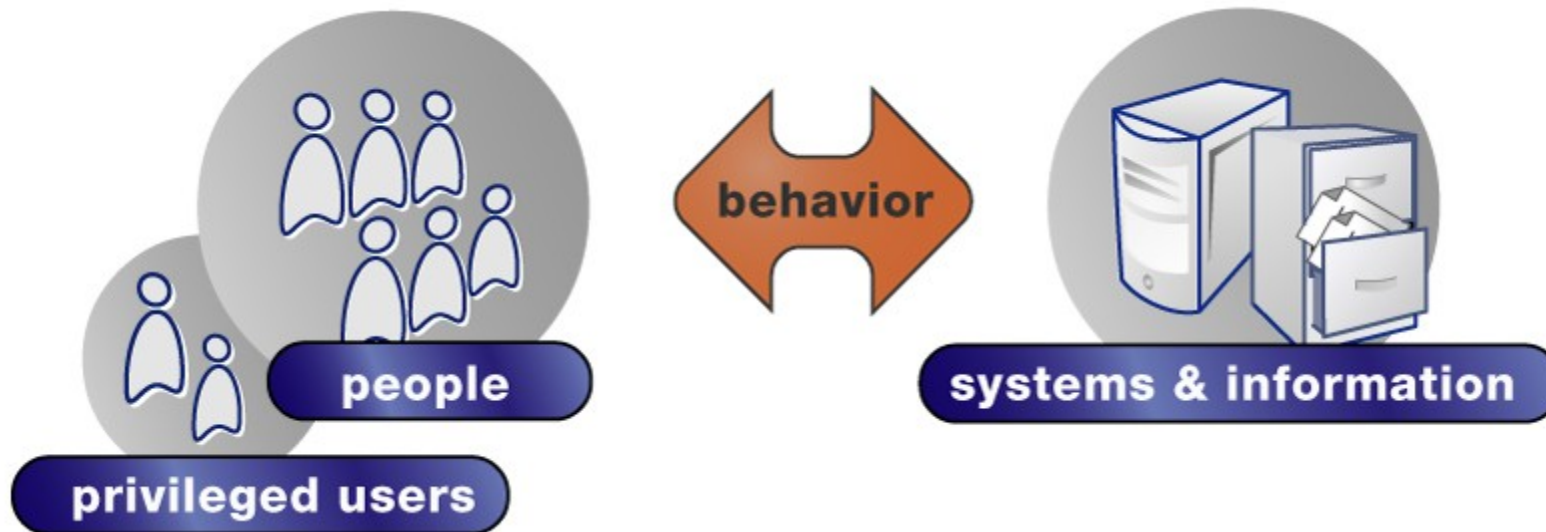
**Legend**

- Complete log set
- Delayed collect, possible data loss
- Failed collect, not collected yet
- Missing log(s)
- Missing log set
- Corrupted log set
- Archived log set(s)

**Report Information**

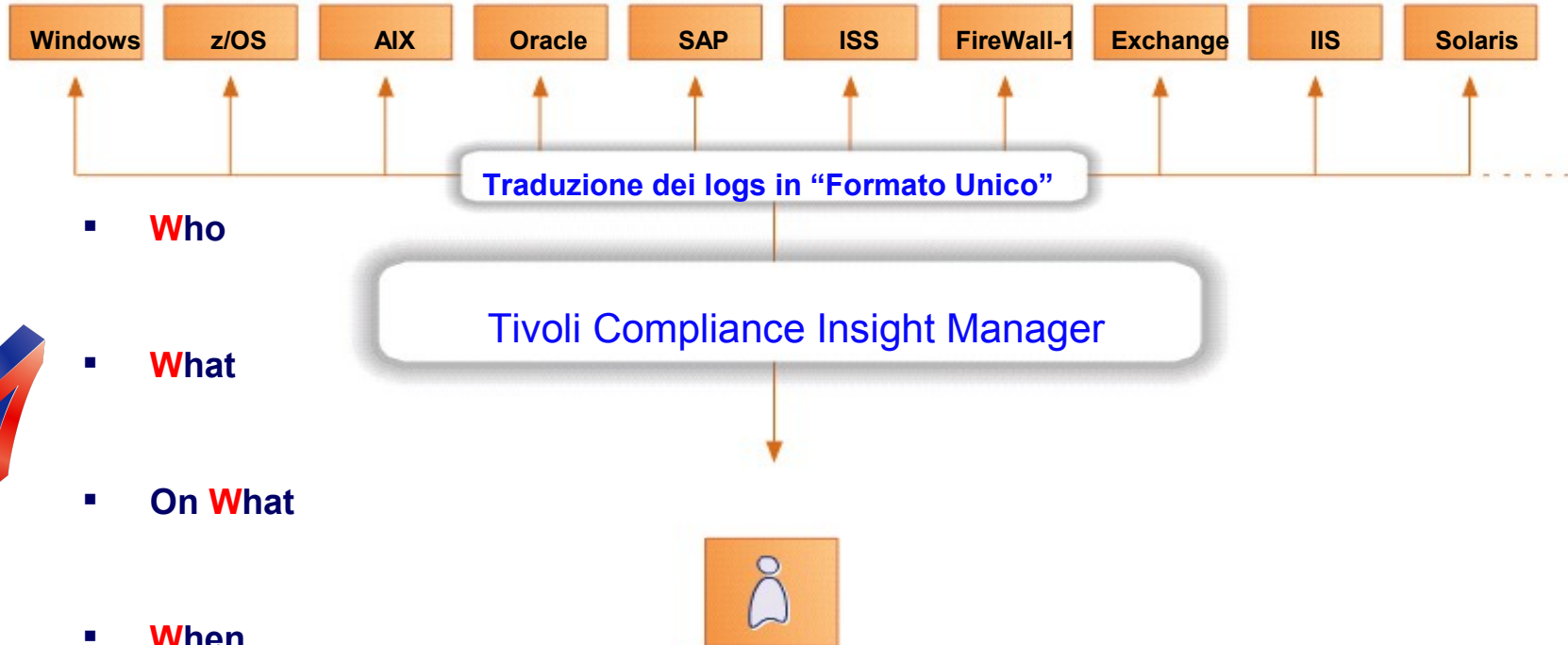
InSightSrv:  
 Creation date: January 22, 2007  
 Creation time: 12:00:00 AM CST  
 Creator: Scheduled  
 Log sets: 36.551

# Comprende – Verifica delle attività degli utenti



*87% degli incidenti interni sono causati da utenti privilegiati.*

# Comprende – Centralizzazione dei log



- **Who**
- **What**
- **On What**
- **When**



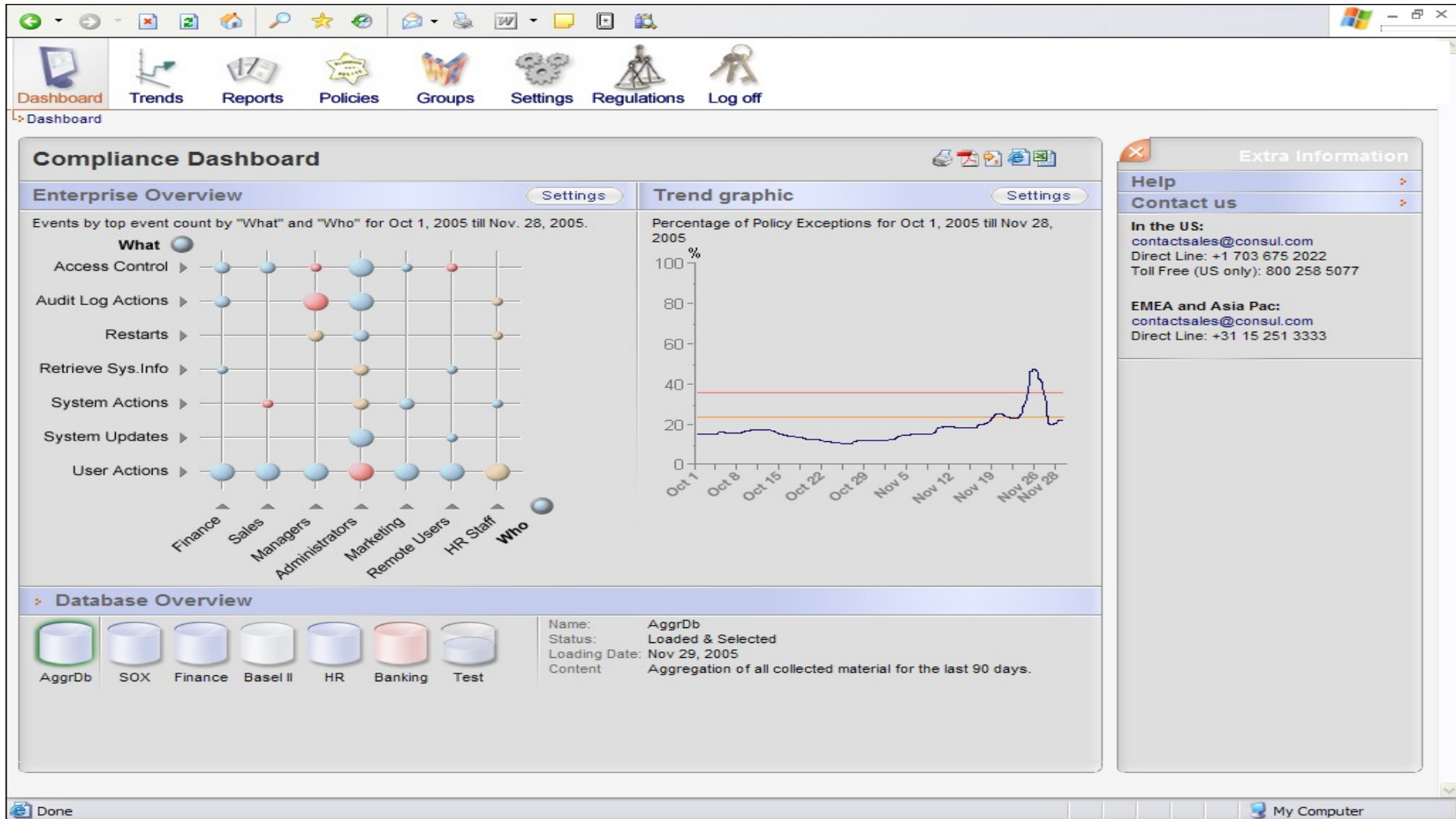
**TCIM** ~~work~~ *centralizza le informazioni di security e compliance ottimizzando i tempi ed i costi attraverso l'automatizzazione dei processi di monitoraggio aziendale*

- **Where From**

# Comprende – Security Compliance Dashboard

Compliance & Audit

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



# Comprende – Policy Exception

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

► Incident Tracking

▼ Additional information

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



# Comprende – Special Attention

*Verifica delle variabili che caratterizzano l'attività sui sistemi*

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				
IT				Sensitive Groups	
IT				Non-Public Data	
Administrators				Organizational Data	
Administrators				Non-Public Data	
IT				Organizational Data	
IT				Sensitive Data	
Administrators				Proprietary Data	
Administrators				Sensitive Data	
Administrators				Proprietary Data	
MailAdmins	Logon - Unavlbl			Mailboxes	

**SMTP**



**SNMP**

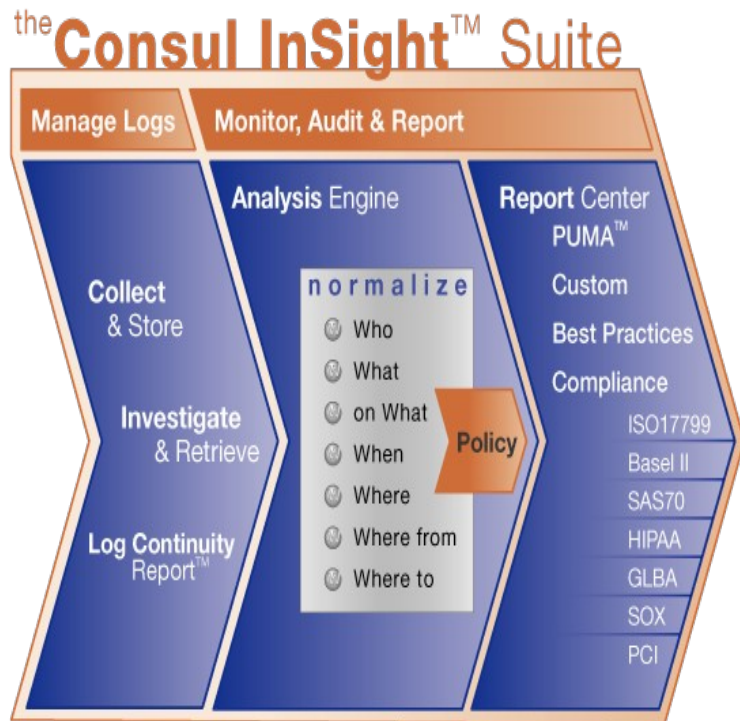


**Script**



# 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 &amp; Audit



EPRORADB » DemoWindows » Regulations Resource Center » ISO 17799

Portal

## ISO 17799 Regulation Reports

Add custom report

Import custom reports

ISO 17799

Title		Action
ISO 17799 (3.1) Security policy	■ Tivoli Compliance Management Module for Sarbanes-Oxley	
ISO 17799 (5.1) Accountability for assets	■ Tivoli Compliance Management Module for ISO 27001	
ISO 17799 (5.2) Classification	■ Tivoli Compliance Management Module for HIPAA	
ISO 17799 (6.3,8.1.3) Security alert	■ Tivoli Compliance Management Module for GLBA	
ISO 17799 (6.3.4,8.1.3) Incident tracking	■ Tivoli Compliance Management Module for Basel II	
ISO 17799 (8.1.2) Operational change control	■ Tivoli Compliance Management Module for PCI DSS	
ISO 17799 (8.1.6) External contractors		
ISO 17799 (8.3) Malicious attacks		
ISO 17799 (8.4,9.7.1) Log archive	Log archive dates and locations.	
ISO 17799 (8.4,9.7.1) Log collection	Log collection schedule and platforms.	
ISO 17799 (8.4,9.7.1) Log storage	Log storage report for all platforms	
ISO 17799 (8.4.2) Operator log	Actions performed by the IT Admin staff.	
ISO 17799 (8.5) Network management	Actions and events caused by users on Network Services.	
ISO 17799 (8.7.4.1) Mail server	Exceptions and failures for the Mail Server assets.	
ISO 17799 (8.7.6) Publicly available systems	Actions and exceptions on Publicly Published Data.	
ISO 17799 (9.2.4,9.7) Review of user access rights	Actions performed by administrators on users.	
ISO 17799 (9.2.4.c,9.7) System access and use	Successes and failures against key assets.	
ISO 17799 (9.3) User responsibilities and password use	Logon failures and successes either locally or remotely.	
ISO 17799 (9.4) Network access control	Actions performed on and events and exceptions generated by Network or Router.	
ISO 17799 (9.4.4) Node authentication	Authentication of connections to remote computer systems.	



# SOX 1.4.1.1

## System utilities usage summary Database DemoWindows on Server EPRORADB



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

Setup:

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

### 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:

Start time: Month: September, Day: 12, Year: 2006, Hour: 22, Min: 0

End time: Month: July, Day: 6, Year: 2007, Hour: 9, Min: 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 legittimati 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:

Start time: Month:  Day:  Year:  Hour:  Min:   
 End time: Month:  Day:  Year:  Hour:  Min:

Time zone:

**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

Dashboard Summary Reports Policies Groups Settings Regulations Log off

Dashboard > Reports > User by Event type

### User by Event type

Parameter Setup

What (event type)

<input checked="" type="checkbox"/> Add : Privilege / Success	<input type="checkbox"/> Load : Module / Success	<input type="checkbox"/> Read : File / Success	<input type="checkbox"/> Stop : Service / Success
<input type="checkbox"/> Authenticate : User / Failure	<input type="checkbox"/> Logoff : User / Success	<input type="checkbox"/> Receive : Message / Success	<input type="checkbox"/> Update : Parameter / Failure
<input checked="" type="checkbox"/> Clear : Auditlog / Success	<input type="checkbox"/> Logon : User / Failure	<input type="checkbox"/> Restart : System / Success	<input type="checkbox"/> Use : Service / Success
<input type="checkbox"/> Complete : Process / Success	<input type="checkbox"/> Logon : User / Success	<input checked="" type="checkbox"/> Start : Process / Success	<input type="checkbox"/> Use : Service / Success
<input checked="" type="checkbox"/> Grant : Privilege / Failure	<input type="checkbox"/> Read : Access / Success	<input type="checkbox"/> Start : Service / Success	<input checked="" type="checkbox"/> Write : Config / Success
<input checked="" type="checkbox"/> Grant : Privilege / Success	<input type="checkbox"/> Read : Config / Success	<input checked="" type="checkbox"/> Start : System / Success	<input type="checkbox"/> Write : Log / Success

Submit Reset

### Summary report

Who (Name)	Logonname	What (Event type)	#Events
Administrator	WINDOWS_NT01\Administrator	Add: Privilege / Success	294
Administrator	WINDOWS_NT01\Administrator	Clear: Auditlog / Success	1150
Administrator	WINDOWS_NT01\Administrator	Grant: Privilege / Success	334
Administrator	WINDOWS_NT01\Administrator	Start: System / Success	7
ROOT	LIN_SERVROOT	Add: Privilege / Success	5
ROOT	LIN_SERVROOT	Grant: Privilege / Success	7
ROOT	LIN_SERVROOT	Start: Process / Success	42
ROOT	LIN_SERVROOT	Start: System / Success	306
ROOT	LIN_SERVROOT	Write: Config / Success	42
System	NT AUTHORITY\SYSTEM	Start: Process / Success	494
System	NT AUTHORITY\SYSTEM	Start: System / Success	178
Michael Myers	WINDOWS_NT01\Managers\Michael076	Clear: Auditlog / Success	2
Michael Myers	WINDOWS_NT01\Managers\Michael076	Grant: Privilege / Failure	1
Eric Sanders	WINDOWS_NT01\Sales\Eric887	Start: Process / Success	18

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

# Query e viste dedicate (2/3)



Portal > iView > Automated Report Distribution > Edit Automated Report Distribution

Portal

## Edit Automated Report Distribution Task

### General Information

#### Email

Title\*:

Body\*:

\* Required field

Report Format:

PDF

CSV

Also send reports when they contain no data:

#### Schedule

Start date: month:  day:  year:

Run time: hour:  minutes:

Recurrence:

Inactive

Daily

Weekly

Monthly

Daily recurrence pattern:

Every  day(s)

Every weekday

### Reports

Report	Database	Load Schedule	Action
PCI (10.1) Access to System Components	DemoWindows	Never	
<input type="text" value="Select a report..."/>			

### Addressees

**Extra Information**

- [Help](#) >
- [Support](#) >





# Tool di ricerca sui dati originali

Compliance & Audit

**Depot Investigation Tool**

Portal > Log Manager > 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
			Internet Information S	Oracle
			Microsoft Windows	
			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

**Extra Information**

**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%

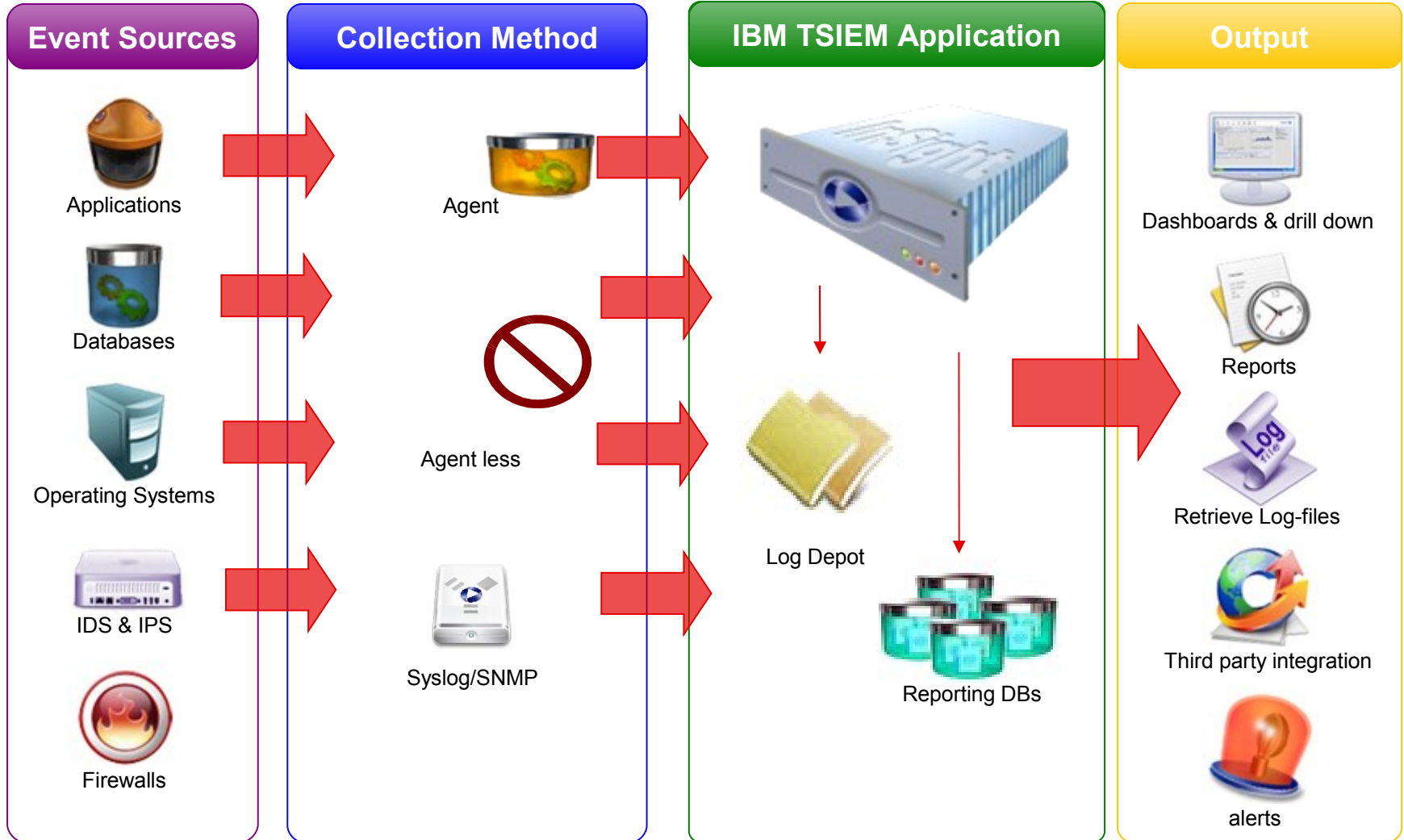
Creation Time: 0

Logfiles: 0

Events: 0

**Support**

# 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:  $1.5 * (\text{total GB of daily logs} / 10 \text{ compression factor}) * \text{number of days to keep in repository} + 25\text{GB}$

# 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

## Supported MAINFRAME:

- Novell NSure Audit
- IBM z/OS + RACF
- Novell Suse Linux
- IBM z/OS + CA ACF2
- RedHat Linux
- IBM z/OS + CA Top Secret

## 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

## Supported DATABASES:

- IBM DB2 on z/OS
- IBM DB2 on Windows
- IBM DB2 UDB on Windows, Solaris, AIX
- Microsoft Exchange
- Microsoft Internet Information Server
- 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)

