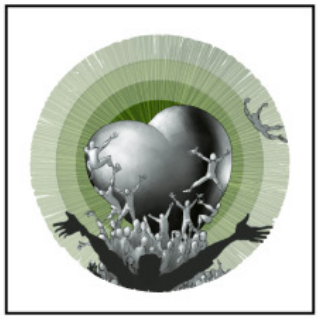
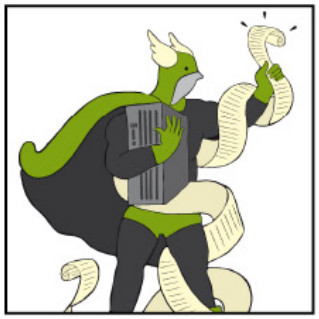
IBM SOFTWARELAND 2009.
SOLUZIONI INTELLIGENTI PER PROSPETTIVE CHE CAMBIANO.




Alfonso Ponticelli

Soluzioni Tivoli di Security Information and Event Management

Compliance and Security secondo IBM

Gestione delle identità e controllo degli accessi alle risorse aziendali: le soluzioni TIVOLI

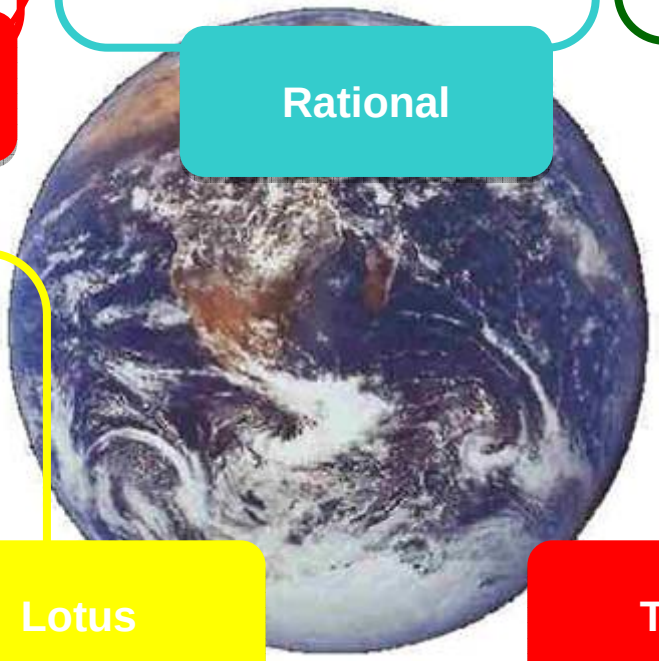
Tivoli

Le soluzioni Rational a garanzia della sicurezza delle applicazioni e il rispetto della compliance

Rational

Il rispetto delle normative legali e di settore per la privacy dei dati e il records management

Information Management



Protezione preventiva e controllo dello spam, virus e contenuto delle email per il tuo ambiente di posta Domino, con Lotus Protector

Lotus

Gestione del rischio, rispetto delle leggi e delle policy aziendali, report standard conformi alle normative

Tivoli

La sfida per la sicurezza è quella di trovare un punto di equilibrio fra la necessità di crescita e di innovazione e i rischi per il business …

- Crescente **complessità** delle problematiche di sicurezza nello scenario odierno
- Alti costi per la **gestione** e il supporto della sicurezza
- **Conformità** con i requisiti di legge e le esigenze **di audit**
- **Limitare** e **tracciare l'accesso** alle informazioni e agli asset sensibili
- Stabilire una **relazione di fiducia** con i clienti e i partner
- Proteggersi contro **le intrusioni e il furto di informazioni confidenziali**
- Difficile **realizzare** la sicurezza in ogni nuova applicazione e processo
- Le problematiche di Sicurezza stanno colpendo il **cuore dell'operatività**!

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

Cosa ci si aspetta da un sistema SIEM

- **Collezione dei log e Gestione dei log** in formato nativo
- **Correlazione degli eventi** con Allarmi e Notifiche
- **Monitoraggio degli utenti privilegiati** con verifica dei comportamenti anomali
- **Identificare** e prioritizzare le più serie **minacce di sicurezza** che necessitano un'immediata risposta
- **Dashboard** che supportano ed assistano l'investigazione
- Necessità di viste differenziate per **analizzare la postura di compliance**
- Una piattaforma per il **tracking degli incidenti** e per la loro gestione
- **Visibility** - Necessità di report che possano essere facilmente capiti da utenti non-tecnici inclusi il business management e gli auditor

Approccio metodologico supportati dalle soluzioni tecnologiche

Phase 5: Education

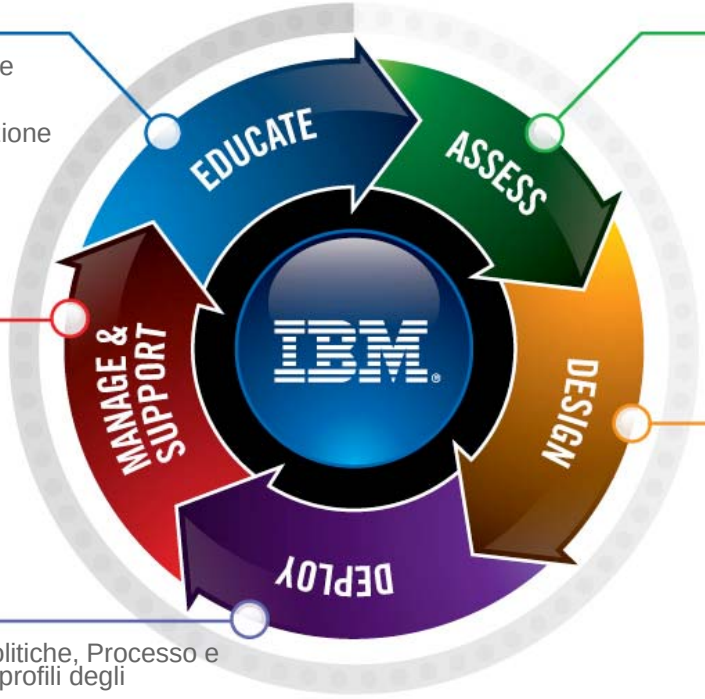
- Training specifico per le piattaforme tecnologiche
- Corsi di sensibilizzazione e formazione in materia di Audit & Compliance

Phase 4: Management and Support

- Affiancamento per la gestione ed il controllo delle piattaforme tecnologiche
- Servizi di assistenza alla gestione

Phase 3: Deployment

- Supporto alla implementazione di Politiche, Processo e Procedure per la gestione dei ruoli e profili degli amministratori
- Supporto alla implementazione della soluzione tecnologica e procedurale per il monitoraggio delle attività



Phase 1: Assessment

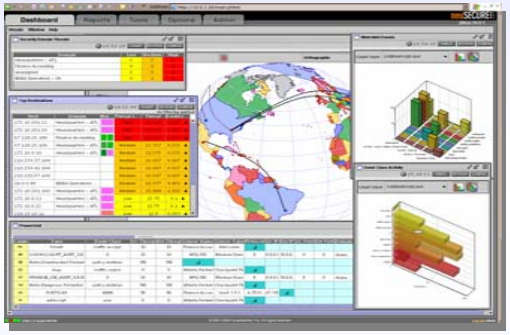
- Rilevazione ed analisi delle piattaforme tecnologiche e della gestione degli amministratori e dei relativi profili
- Gap Analysis rispetto ai requisiti delle normative aziendali
- Piano degli Interventi di miglioramento organizzativi e tecnologici

Phase 2: Design

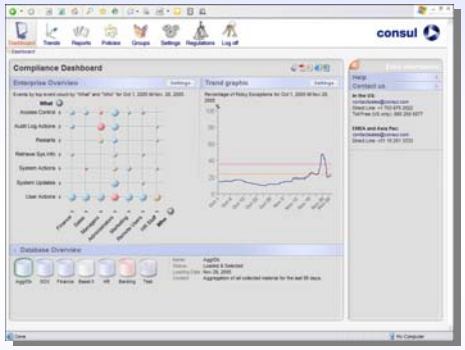
- Sviluppo Politiche, Processo e Procedure per la gestione dei ruoli e profili degli amministratori
- Sviluppo specifiche per la soluzione tecnologica e procedurale per il monitoraggio delle attività
- Piano di implementazione

Tivoli Security Information and Event Manager

TSOM correla eventi verso Report e Dashboard TCIM
TCIM ruota violazioni di Policy alla console operativa del TSOM



- Violazioni delle Network Security Policy
- Accessi utente ed eventi amministrativi dall'infrastruttura
- Asset compromessi o minacciati



Tivoli Security Operations Manager (TSOM)

Tivoli Compliance InSight Manager (TCIM)

Allarmi per Violazioni di Policy
-Fornisce la conoscenza della violazione sull'host o sull'applicazione da parte di uno specifico
- Apre un Ticket per un nuovo incidente

IBM SOFTWARELAND 2009.

IBM SIEM Portal

IBM Tivoli Compliance Insight Manager Portal

IBM Tivoli Compliance Portal

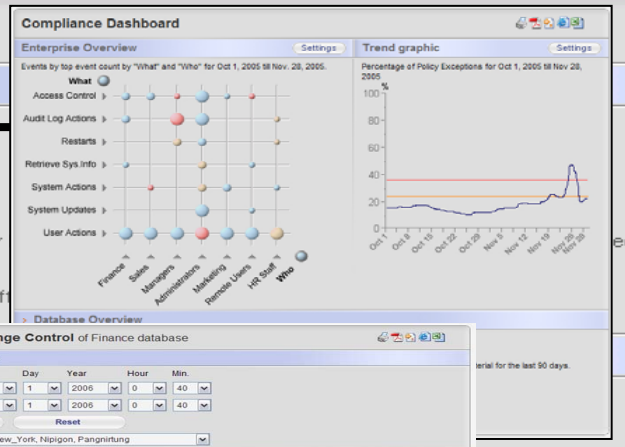
iView	The reporting tool with drill down possibilities
Log Manager	The reporting tool for log management
Policy Generator	A wizard that helps you start using IBM Tivoli Compliance Insight Manager data from your own devices
Scoping	Tool to manage the viewable acces of different users of the system to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

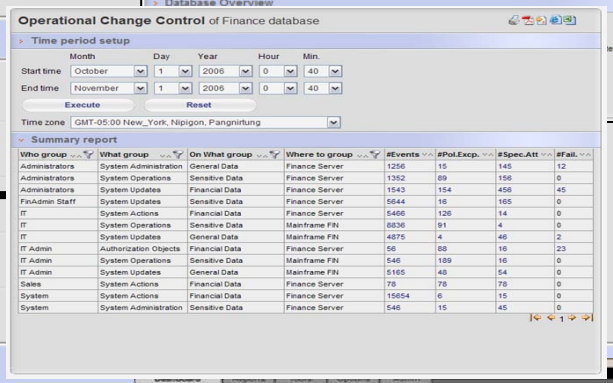
IBM Tivoli Regulatory Compliance Reports

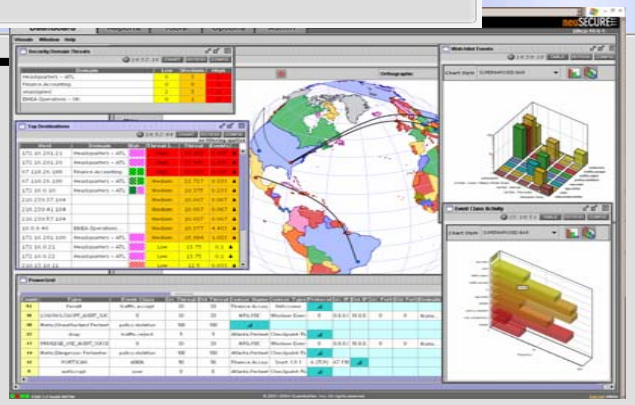
Basel II	The compliance entrance for Basel II
GLBA	The compliance entrance for GLBA
HIPAA	The compliance entrance for HIPAA
ISO17799	The compliance entrance for ISO17799
Sarbanes-Oxley	The compliance entrance for Sarbanes Oxley

IBM Tivoli Security Operations Portal

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







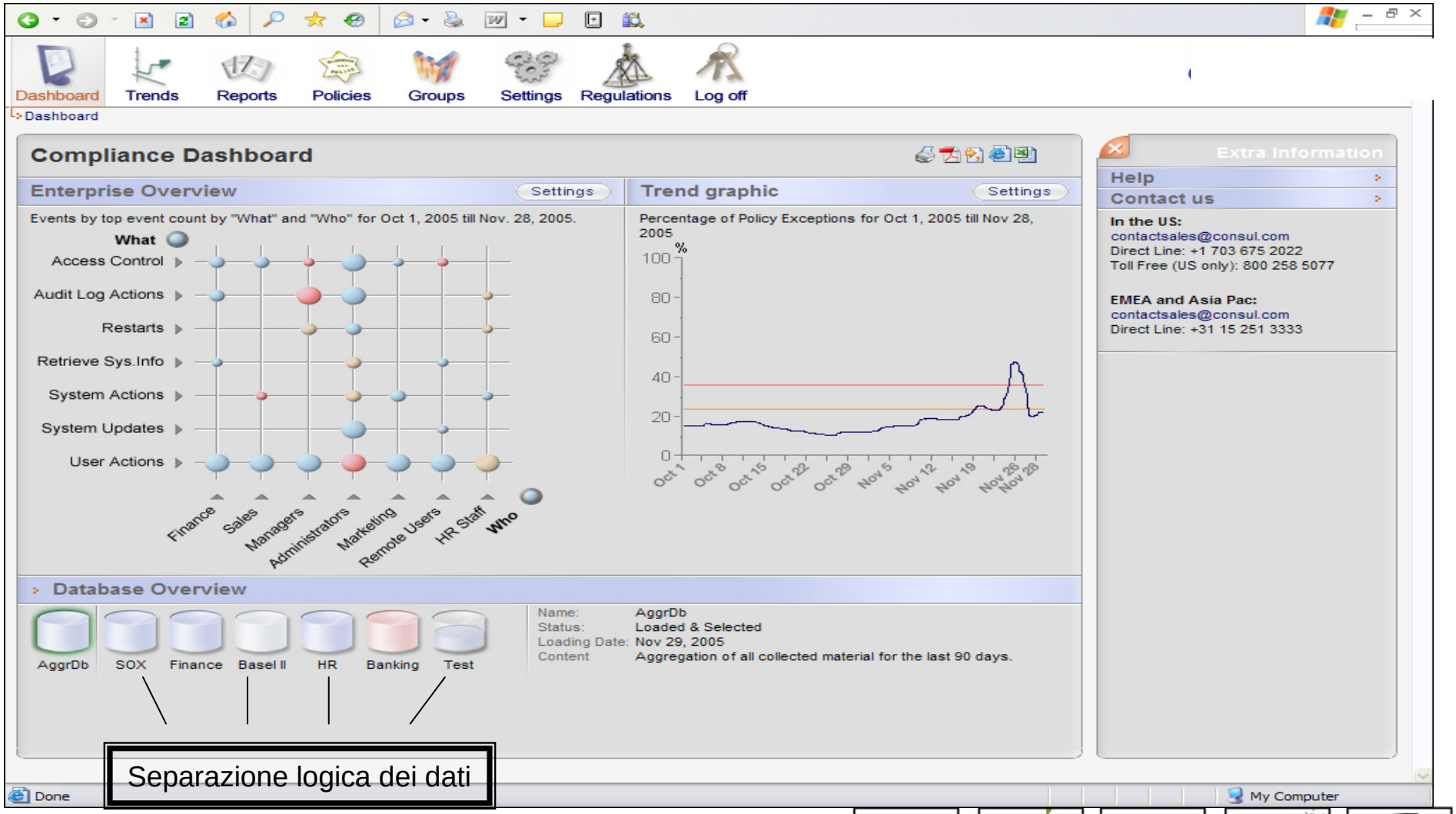
Tivoli

Le tre C del TCIM: Capture, Comprehend, Communicate

SIM

TCIM

Dopo la normalizzazione W7 gli eventi sono riassunti in un unico grafico



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

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

Gli eventi che non corrispondono alle politiche definite

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

Attività sui sistemi da evidenziare indifferentemente dalle politiche

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	

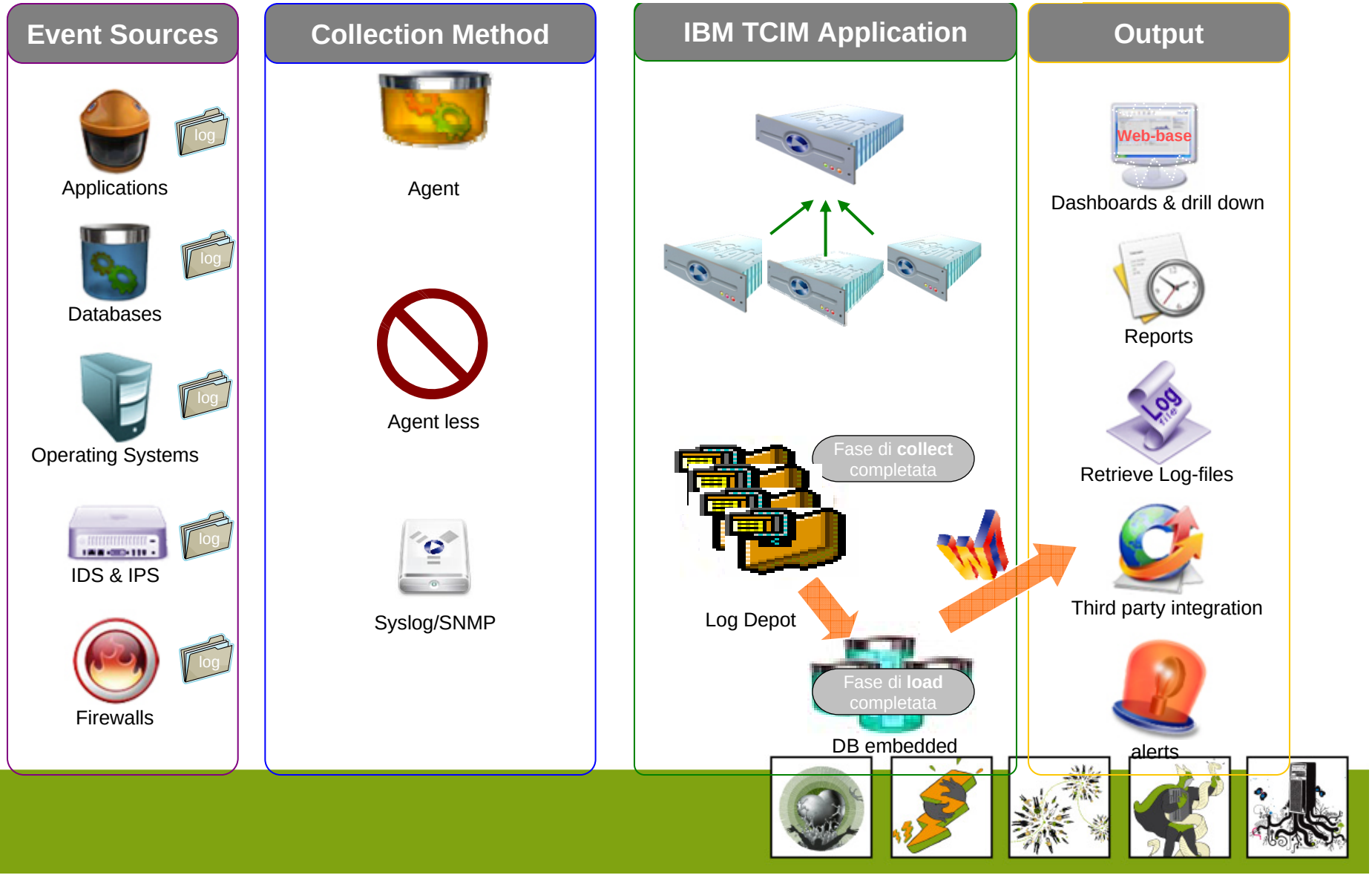
Policy | Attention

Non è una policy

Ma una attention

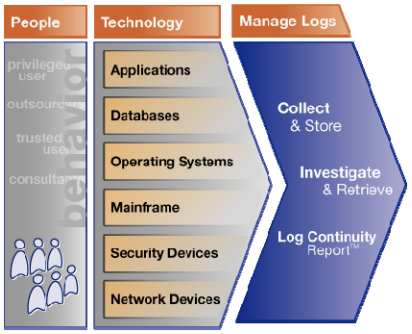
SMTP **SNMP** **Script**

TCIM - Architettura

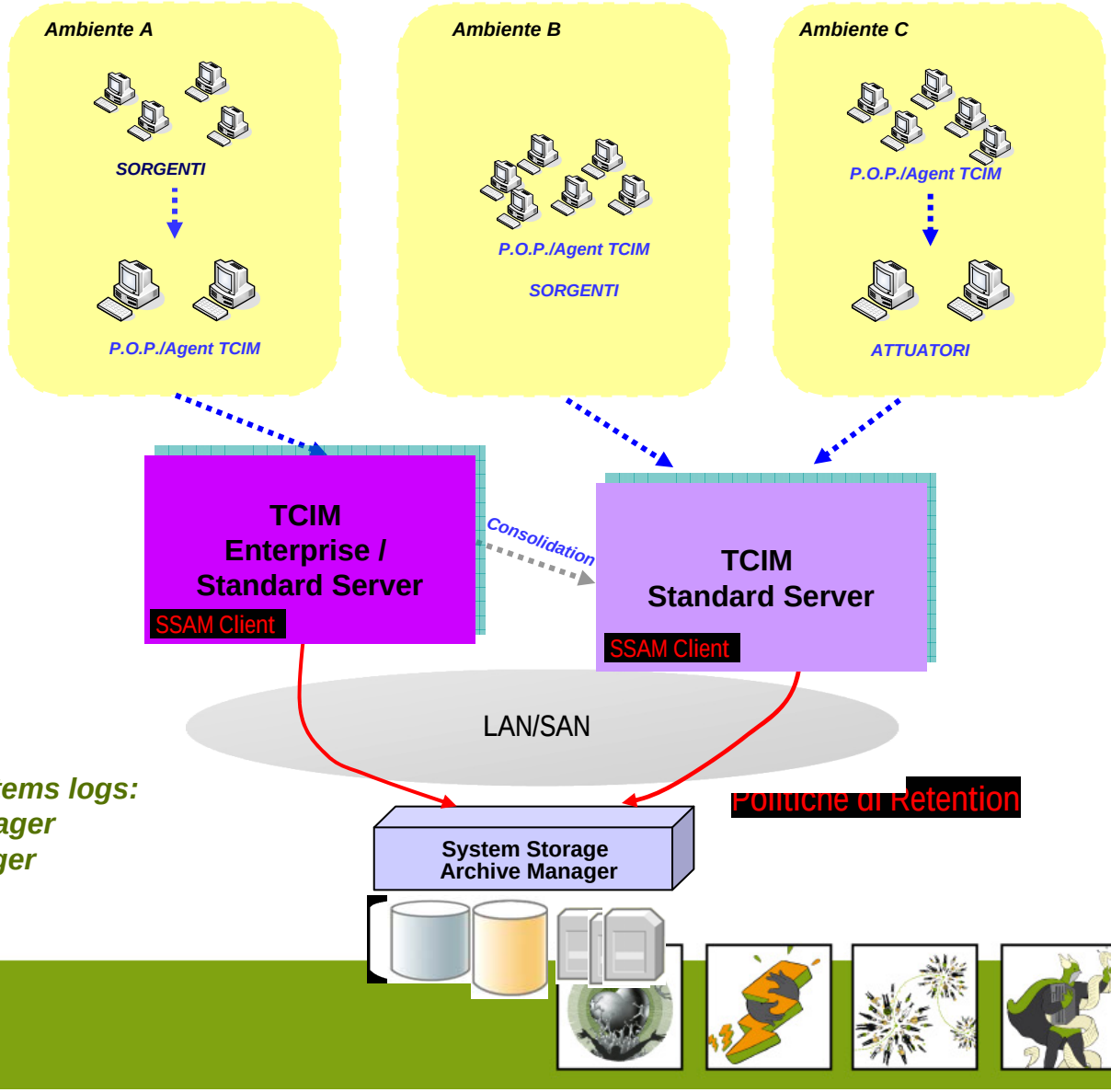


TCIM risponde agli obblighi previsti dal provvedimento del Garante del 27/11/08

- Cattura → Gestisce i Log a livello Enterprise
- li centralizza per periodi anche superiori ai 6 mesi
- li conserva in formato originale
- Comprende → normalizza ed intepreta i LOG utilizzando un motore brevettato
- Comunica → Produce Report ad uso e consumo degli auditor per provare la compliance a specifiche politiche



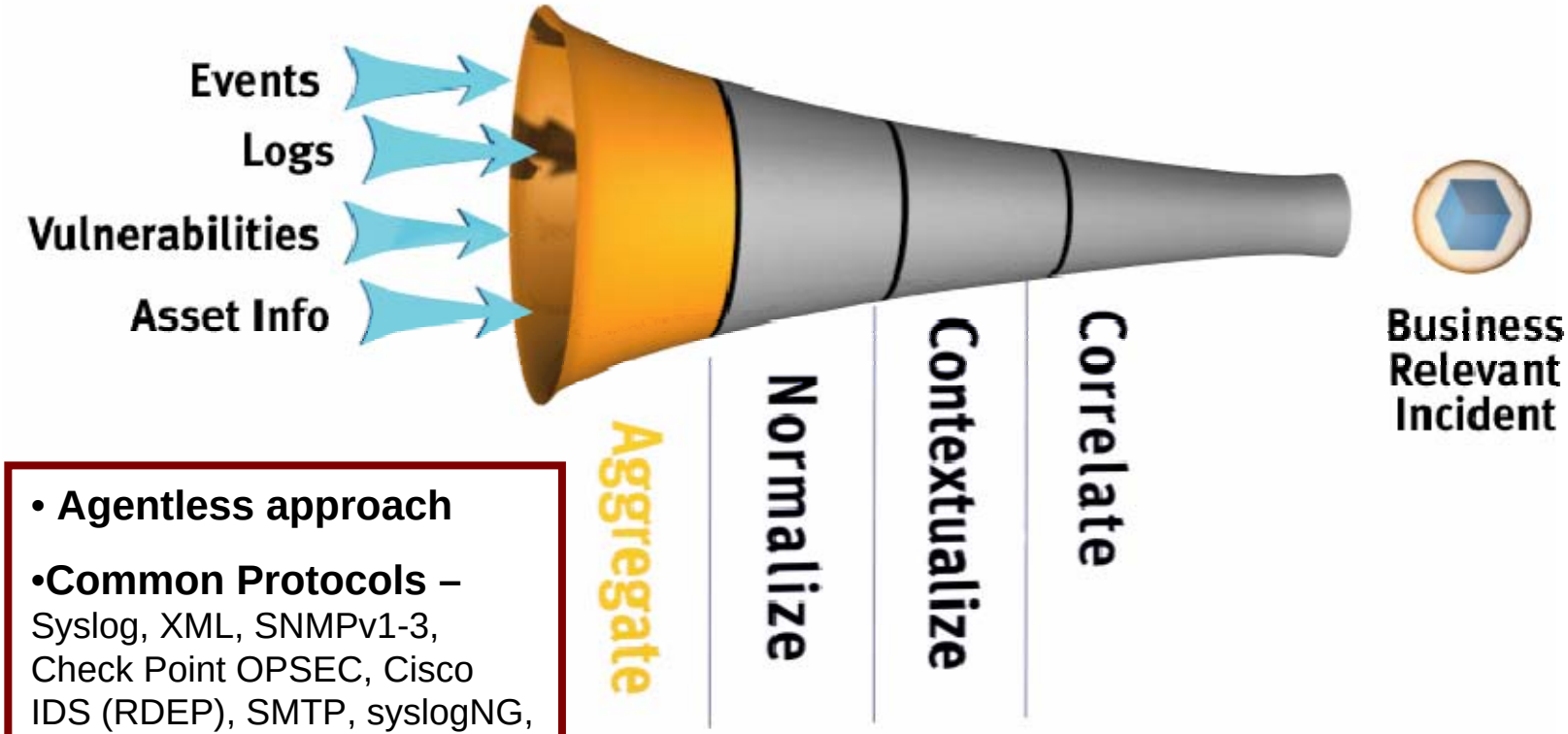
Architettura Tivoli Compliance Insight Manager e System Storage Archive Manager per rispondere al provvedimento del Garante



Monitoring and retention of systems logs:
-Tivoli Compliance Insight Manager
- System Storage Archive Manager

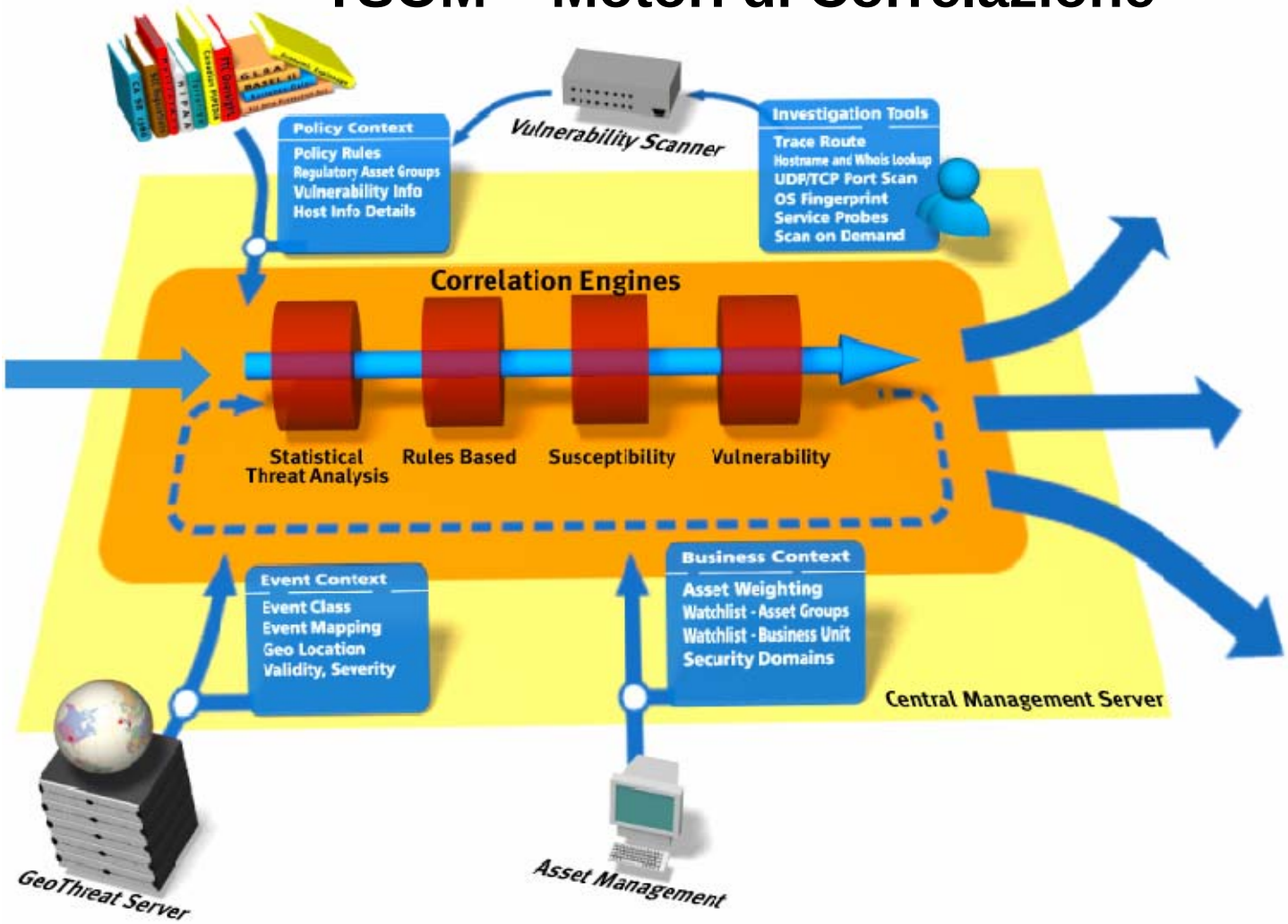
SEM

TSOM

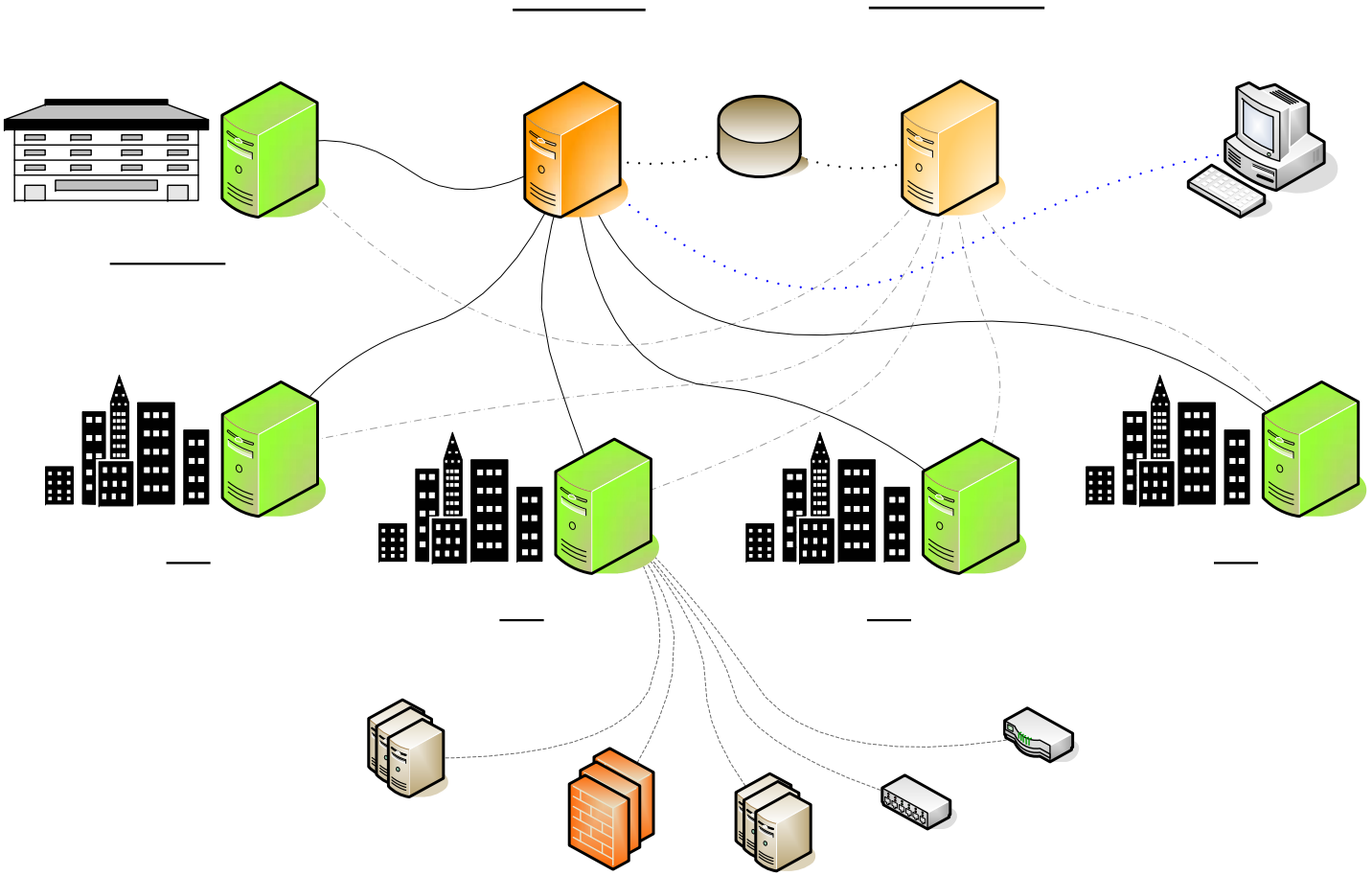


- **Agentless approach**
- **Common Protocols –** Syslog, XML, SNMPv1-3, Check Point OPSEC, Cisco IDS (RDEP), SMTP, syslogNG, AVDL
- **Low-Impact Agents –** Small footprint, customizable for files, DB's, etc

TSOM – Motori di Correlazione



TSOM - Architettura



Domande