La protezione delle Basi Dati, l'integrazione con i sistemi di Sicurezza aziendali, nel rispetto delle Normative internazionali.

Business Case:

UniCredit Business Integrated Solutions

5 giugno 2012

Reply
spike

Agenda

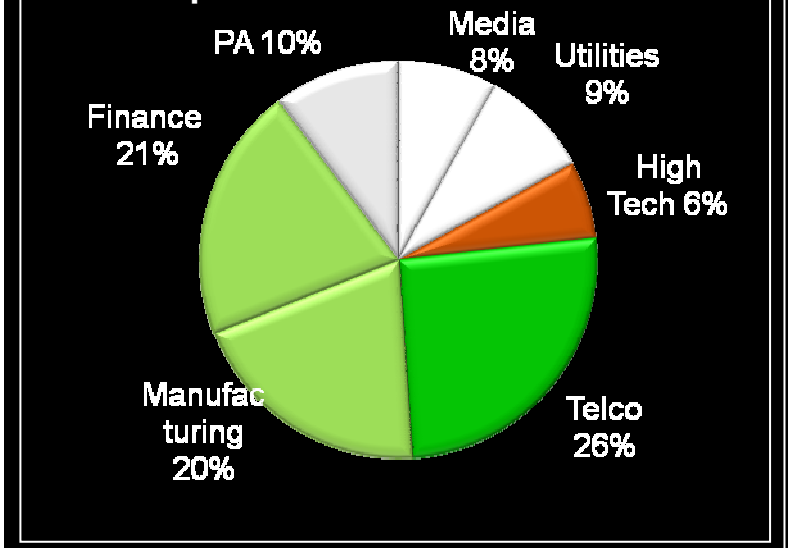
- Presentazione del Gruppo Reply:
  Business Security & Fraud Management

- Enterprise Security Intelligence:
  Le nuove strategie per l'integrazione, la gestione ed il governo della Business Security

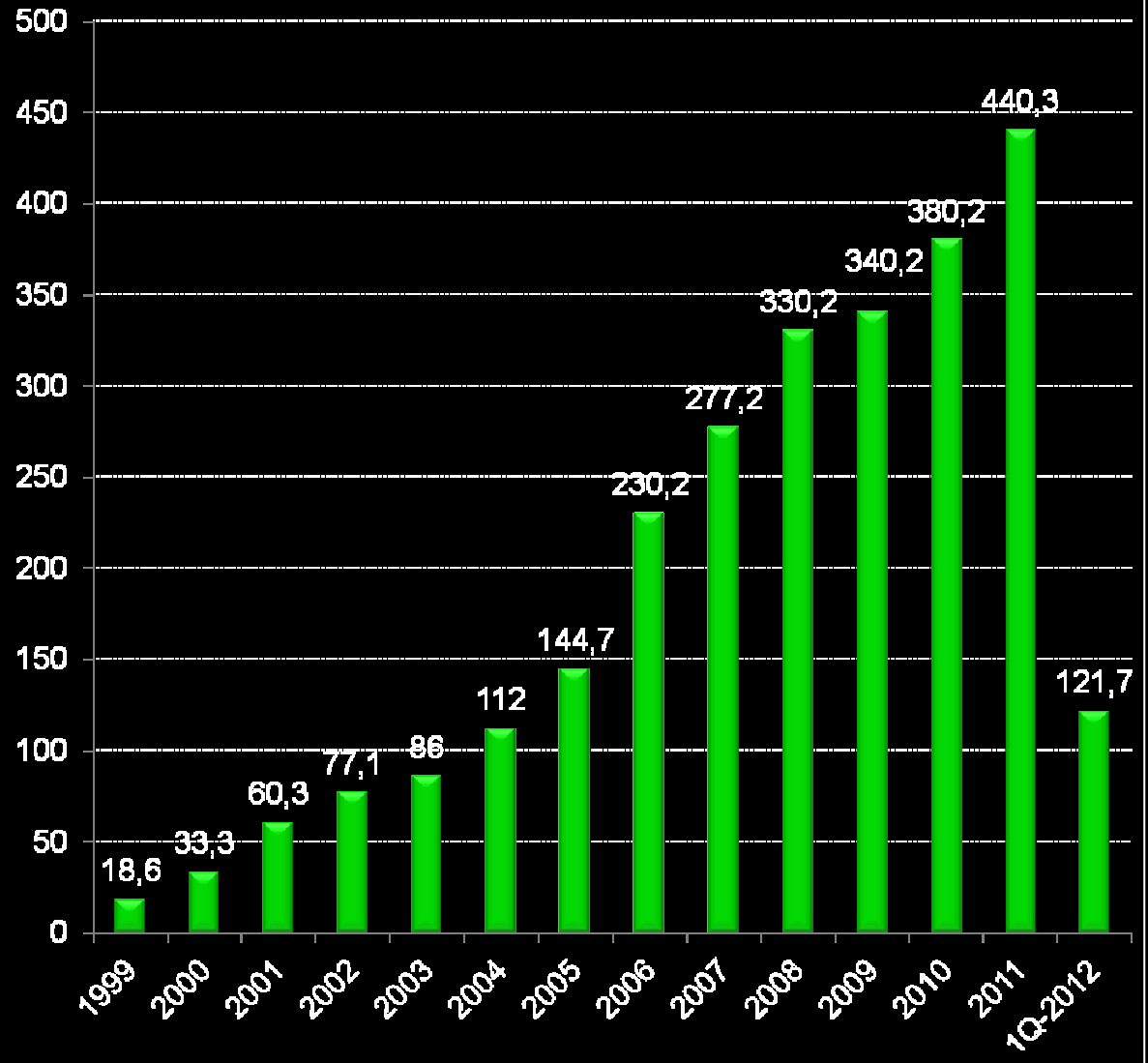
- Business Case:
  La soluzione di Data Protection in UniCredit Business Integrated Solutions

Reply – Facts & Figures

Market Split



Reply Main Offices



People: 3.000+

Security Service Provider con eccellenze riconosciute

ca 200 professionisti
+200 certificazioni

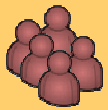
- **Attivi presso i principali enti, organismi, istituti nazionali ed intl: ABILab, AIPSA, AIPSI-ISSA, BCManagers, CLUSIT, CEPAS, …**
- **Partnerships con "tutti" Technology / Products Vendor**

Security Operation Center

24x7 Operations
Service Level Agreements
Security Intelligence
Security Labs

Data Center

Control Room



War Room

Consulting & Professional Svcs

Professional Training and Tools for Security Specialists. OFFENSIVE security

PMI

ACFE Association of Certified Fraud Examiners

BSI

(ISC)²

C|EH Certified Ethical Hacker Hackers are here. Where are you?

Open Source Security Testing Methodology Manual OSSTMM www.osstmm.org

cloud CSA security alliance

ISECOM INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

HO/P **The Honeynet Project**

SUPPORTS PCI DSS

OWASP The Open Web Application Security Project

Business Security & Fraud Mgmt: copertura funzionale

Economico
- Analisi Costi / Benefici
- Valutazione Impatti

Legale
- Leggi
- Normative
- Standard di Sicurezza

Strategico
- Obiettivi Aziendali
- Analisi dei Rischi
- Piano di Business Continuity

Organizzativo
- Definizione Ruoli e Responsabilità
- Impianto Documentale / Policy e Procedure
- Formazione Risorse Umane

Tecnologico
- Verifica strumenti di Protezione e livelli di Sicurezza
- Progettazione delle Contromisure contro le Minacce e le Frodi
- Implementazione, Gestione, Monitoraggio delle Soluzioni

Agenda

- Presentazione del Gruppo Reply:
  Business Security & Fraud Management

- Enterprise Security Intelligence:
  Le nuove strategie per l'integrazione, la gestione ed il governo della Business Security

- Business Case:
  La soluzione di Data Protection in UniCredit Business Integrated Solutions

La visione degli analisti

ICTSecurity Silos						
User Security	Client Security	System & Network Security	Data Security	Application Security	Security Monitoring	Security Assessment

- Poca interazione, integrazione e correlazione tra questi diversi mondi
- Problematico definire un contesto o fare una ricerca lineare condivisa
- Secondo Gartner le aziende non “vedono” il problema nella sua interezza

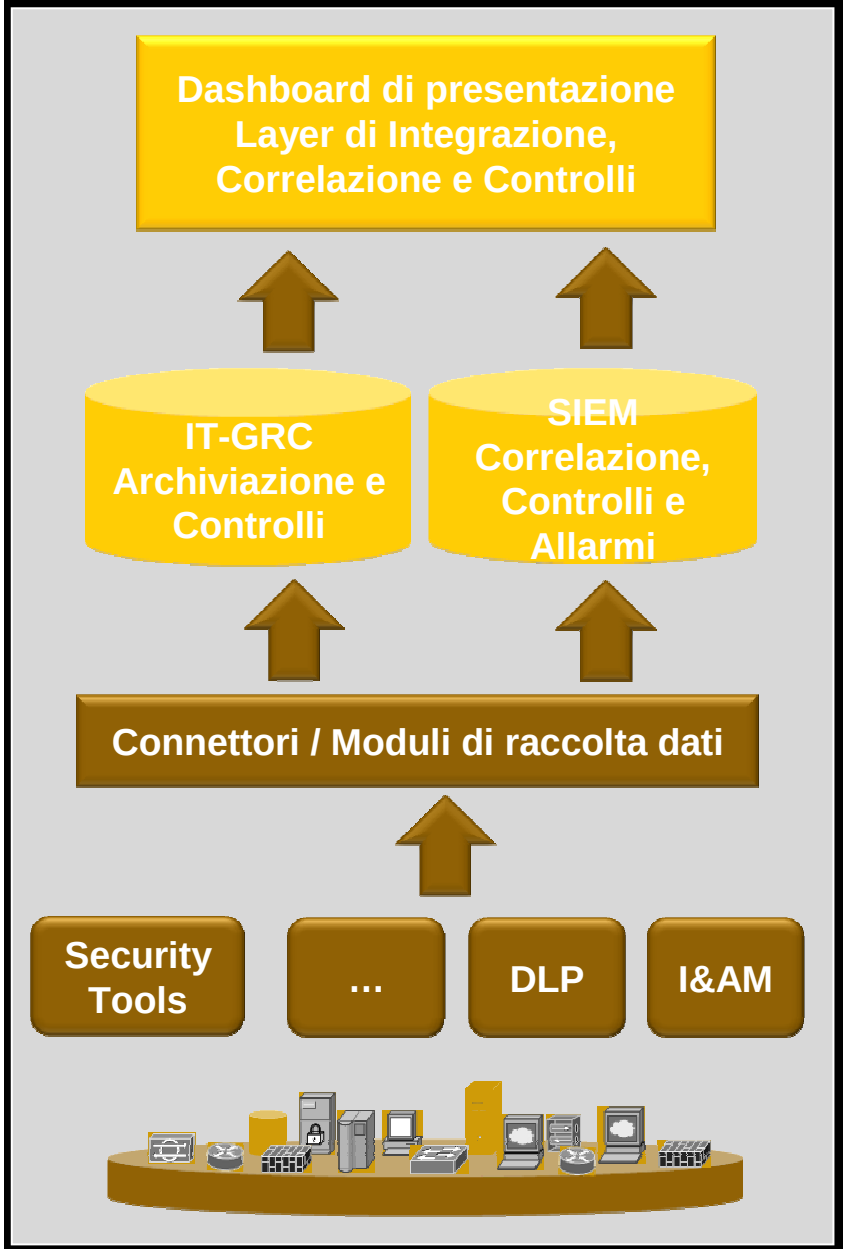
- Il termine Enterprise Security Intelligence (ESI - introdotto da Gartner) definisce una prospettiva olistica nel processo di gestione dei Rischi che consente una vista integrata e quindi una gestione più efficace della Business Security
- Abilita la “sicurezza avanzata”; la capacità di analisi e di sintesi al fine di prendere decisioni consistenti

Fonte: Gartner - Prepare for the Emergence of Enterprise Security Intelligence, Giugno 2010

Enterprise Security Intelligence: il nuovo paradigma

- L’applicazione di contromisure di sicurezza verticali (introdotte da richieste di “information protection” o di “compliance”) ha portato una proliferazione di soluzioni; poche volte si e’ pensato ad una gestione centralizzata e coordinata
- L’ESI è un nuovo paradigma per cui la capacità di intelligence è un deliverable che va posto come obiettivo strategico per la Security e per il Risk Management
- Occorre raccogliere le informazioni e gli eventi di rilevanza per la Security dai singoli componenti dell’IT, dai diversi tools di sicurezza e dalle diverse persone/organizzazioni che interagiscono con il Sistema di Gestione della Sicurezza Aziendale e analizzarle applicando tecniche di Intelligence (aggregazione, correlazione, analisi e sintesi)
- L’impatto atteso è analogo a quelli avuti dalle architetture SOA per il mondo applicativo e dalla BI per l’analisi dei dati aziendali

ESI: gli elementi abilitanti



Skill – Metodhologies – Best Practises

Security Dashboard
- integrazione e correlazione tra fonti dis-omogee
- sintesi ed analisi (grafica) per la Governance

IT-GRC
- controlli di GRC-Security sugli asset IT
- centralizza i controlli svolti sui diversi Silos di Security

Security Information & Event Mgmt
- abilita la raccolta, la correlazione e l'analisi real-time
- devono essere integrati i layer applicativi ed il sistema di Identity Management per il controllo sulle identità digitali

Consulting Services
- capacità di realizzazione

IBM e Reply: portfolio Security a 360°

Governance, Risk and Compliance

Servizi di Consulenza	Reply Security Dashboard	Identity Intelligence	Risk Assessment

IBM Security Products Portfolio

QRadar SIEM	QRadar Log Manager	QRadar Risk Manager

People	Data	Applications	Infrastructure	
			Network	Endpoint
Identity & Access Management Suite	Guardium Database Security	AppScan Source Edition	Network Intrusion Prevention	Endpoint Manager (BigFix)
Federated Identity Manager	Optim Data Masking	AppScan Standard Edition	DataPower Security Gateway	zSecure, Server and Virtualization Security
Enterprise Single Sign-On	Key Lifecycle Manager	Security Policy Manager	QRadar Anomaly Detection / QFlow	Native Server Security (RACF, IBM Systems)
Identity Assessment, Deployment and Hosting Services	Data Security Assessment Service	Application Assessment Service	Managed Firewall, Unified Threat and Intrusion Prevention Services	Penetration Testing Services
	Encryption and DLP Deployment	AppScan OnDemand Software as a Service		

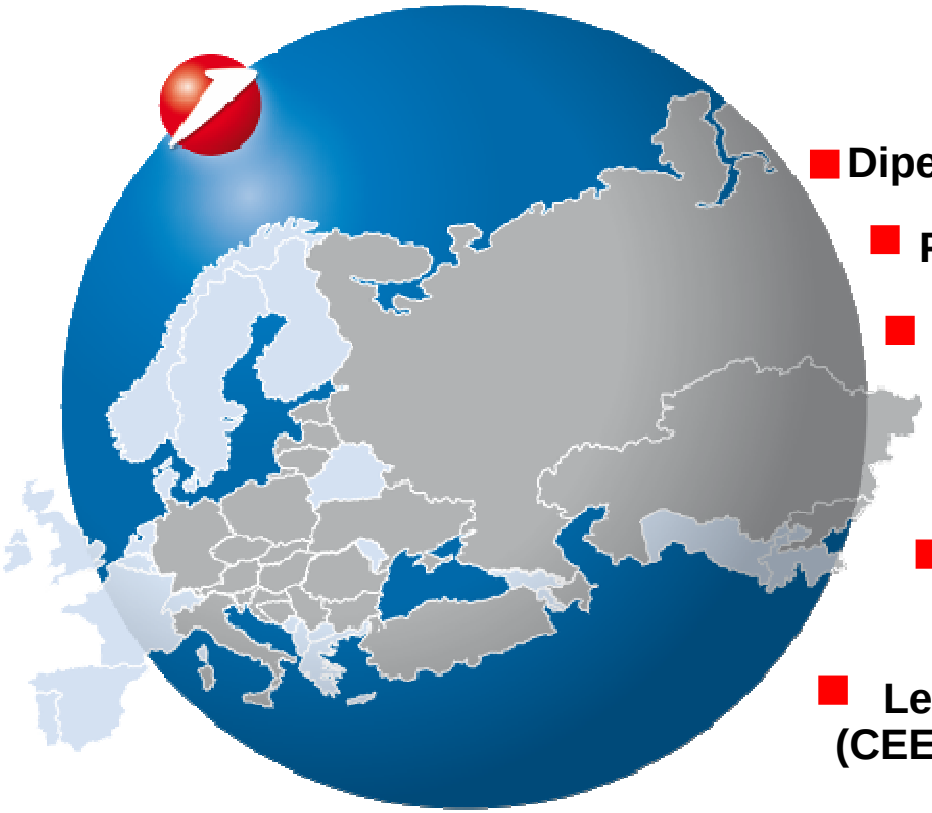
Agenda

- Presentazione del Gruppo Reply:
  Business Security & Fraud Management

- Enterprise Security Intelligence:
  Le nuove strategie per l'integrazione, la gestione ed il governo della Business Security

- Business Case:
  La soluzione di Data Protection in UniCredit Business Integrated Solutions

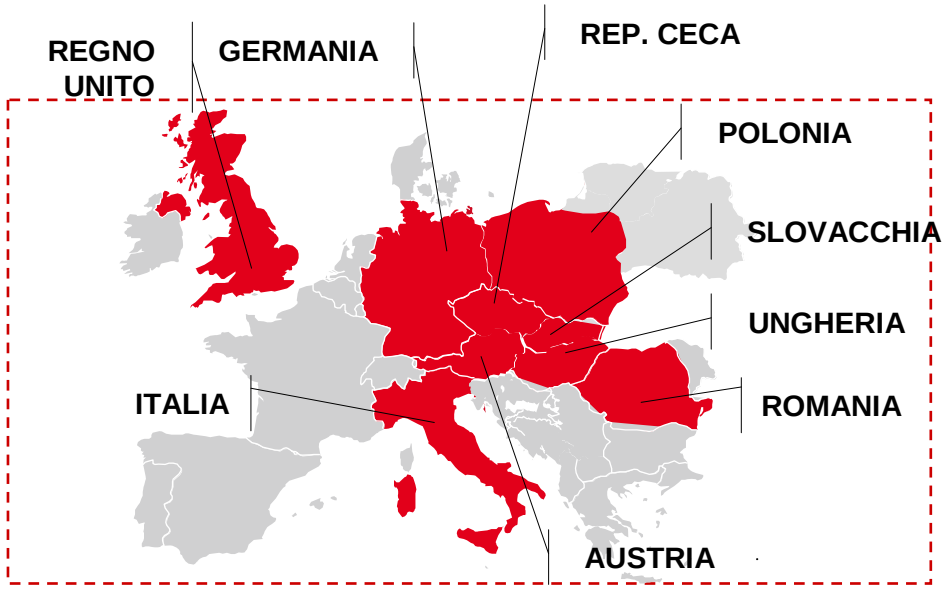
UniCredit – Dati principali



- **Dipendenti: oltre 159.000***
- **Filiali: 9.466***
- **Operazioni bancarie in 22 paesi**
- **Rete internazionale distribuita in:**
  ~ 50 paesi
- **Operatore globale nell'asset management:**
  €156,2 miliardi di attività gestite*
- **Leader di mercato nell'Europa centro-orientale (CEE) facendo leva sulle forze strutturali dell'area**

* Fonte: UniCredit Company Profile, dati al 31 marzo 2012

UniCredit Business Integrated Solutions: carta di identità



- ~ 11.300 Fte's (y/y pro forma)
- 11 Paesi*
- 4 Legal Entity

1Q – 2012 **

- **~ 662 mln di saving entro il 2015**
- **~ 450 mln in investimenti IT** ***

UniCredit Business Integrated Solutions è il primo traguardo tangibile del piano strategico annunciato a novembre 2011. Fornisce servizi operativi e di supporto alla rete Commerciale di UniCredit.

Detenuta da UniCredit, nasce dall'integrazione e consolidamento di 16 società del Gruppo (tra cui UCBP, URE, UC) è dedicata all'erogazione dei servizi di Information e Communication Tecnology (ICT), Back Office e Middle Office, Real Estate, Security e Procurement .

Un nuovo modello di business, unico nel panorama bancario europeo, basato sui reali bisogni del Business (es. Commercial Banking, Global Markets, CEE) non soltanto sull'erogazione dei servizi.

* UniCredit Business Integrated Solutions coordina le attività anche in 2 branch, una a New York e una a Singapore
** Dati al 31 marzo, 2012 *** Nel 2012, 450 mln sono stati destinati a ICT, Application e Infrastructure, di questi 408 mln saranno riservati al Software. Circa il 50% dei progetti sono già stati approvati.

UniCredit Business Integrated Solutions

Data Protection: Obiettivi del progetto

Banca Austria

- Compliance verso leggi e normative locali
- Segregation of Duties

UniCredit

- Integrazione SIEM
- Rispondenza a requisiti del Garante Privacy
- Soluzione globale di Gruppo

Key Points del progetto per UniCredit Business Integrated Solutions

GUARDIUM

- Adottare un **approccio centralizzato** alla tematica della Data Protection
- Garantire la **Segregation of duties**: l'attività dei privileged user è rilevata in modo conforme alle normative (es. PCI)
- Svolgere il **monitoring** in real-time di accessi e attività senza necessità di abilitare database logging nativo
- Garantire la granularità di azioni di **auditing** e la capacità di **rispetto delle policy** (es.: real-time blocking)
- Garantire **conformità ai requisiti di compliance** (es. Garante, PCI, SOX, etc.) con particolare riferimento all'implementazione del **Provvedimento del Garante** del 12 Maggio 2011 in merito ai tracciamenti bancari
- Incrementare la capacità di **intercettare minacce e prevenire attacchi**
- Integrarsi con soluzioni SIEM per una **reportistica integrata** e per la gestione di **allarmi**

UniCredit Business Integrated Solutions

Laws and Regulations Compliance Requirements

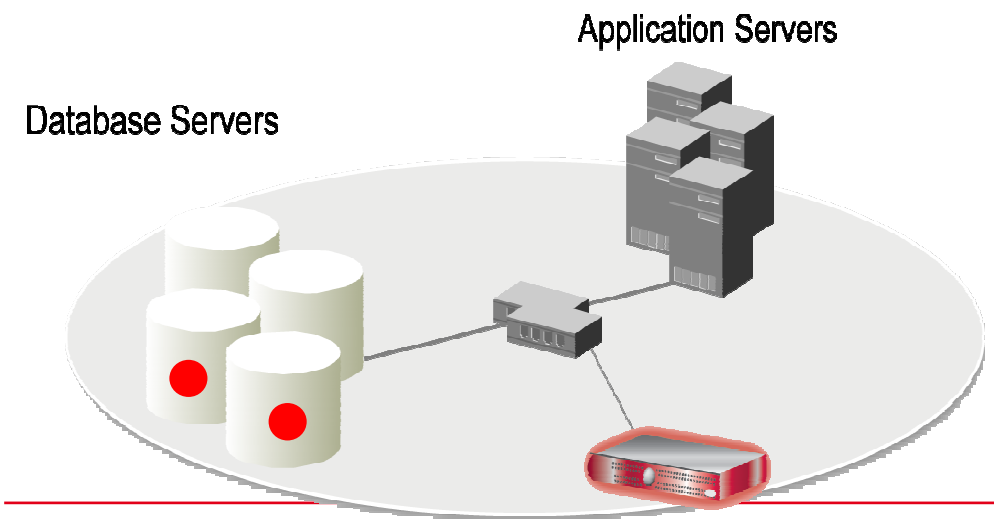
Audit Requirements	COBIT (SOX)	PCI-DSS	ISO 27002	Data Privacy & Protection Laws	NIST SP 800-53 (FISMA)
1. Access to Sensitive Data (Successful/Failed SELECTs)		✓	✓	✓	✓
2. Schema Changes (DDL) (Create/Drop/Alter Tables, etc.)	✓	✓	✓	✓	✓
3. Data Changes (DML) (Insert, Update, Delete)	✓		✓		
4. Security Exceptions (Failed logins, SQL errors, etc.)	✓	✓	✓	✓	✓
5. Accounts, Roles & Permissions (DCL) (GRANT, REVOKE)	✓	✓	✓	✓	✓

Sistemi di Sicurazza tradizionali: soluzioni inefficienti

- IDS / IPS mancano di consapevolezza specializzata relativamente ai protocolli di comunicazione dei database e, soprattutto, delle attività codotte.
- La crittografia del database richiede importanti modifiche alle applicazioni e ai database e non fornisce protezione contro gli utenti privilegiati.
- Le tecnologie DLP non riescono a proteggere i dati aziendali nel data center stesso.
- I sistemi SIEM si basano sui dati di log nativi piuttosto che raccogliere i log del database autonomamente. Sono inoltre carenti per le capacità di analisi mirate sui database.

DAM Pro and Cons analysis

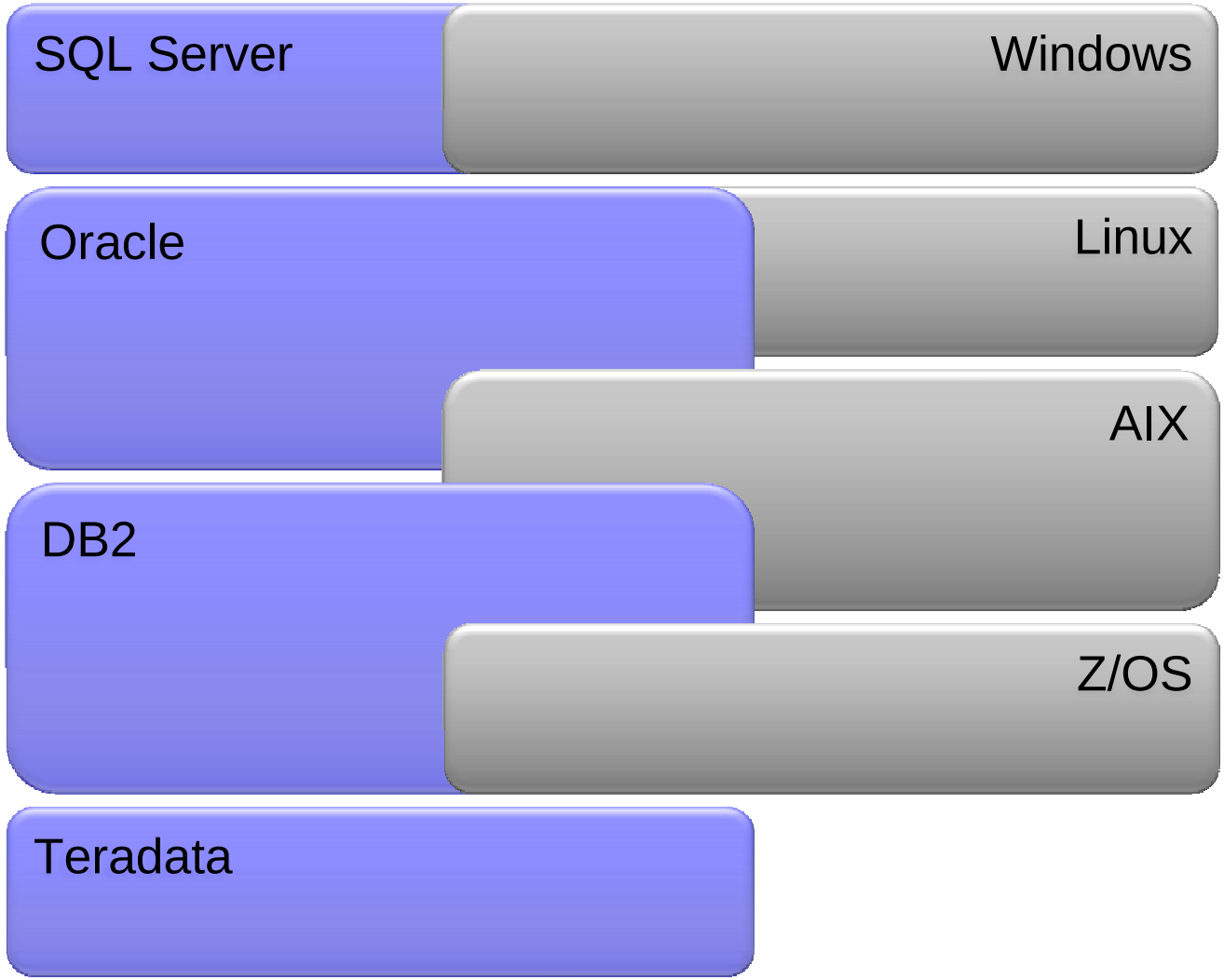
SOLUZIONI	PRO	CONTRO	TEMPI
Abilitazione Log delle tabelle	Implementabile immediatamente	Impatti sulle prestazioni del servizio; controllabile dal DBA	Rapidi per il deployment, se il sistema e' potente Lunghi per l'analisi
Uso di tool per ogni DB (DB2 Query Monitor)	Implementabile immediatamente	Limitato ad alcuni DB, della medesima tipologia; controllabile dal DBA	Rapidi per il deployment Medi - Lunghi per l'analisi
Uso di tool adatti a diversi DB **DAM (**Database Activity Monitoring) **& Control**	**Unico sistema per monitorare e prevenire. Gestione diretta in carico alla security**	**Necessita di una figura responsabile della sicurezza; Necessita di investimento HW/SW**	**Medi per il deployment** **Rapidi per l'analisi** **(Report di compliance and assessment preinpostati)**



Piattaforme supportate

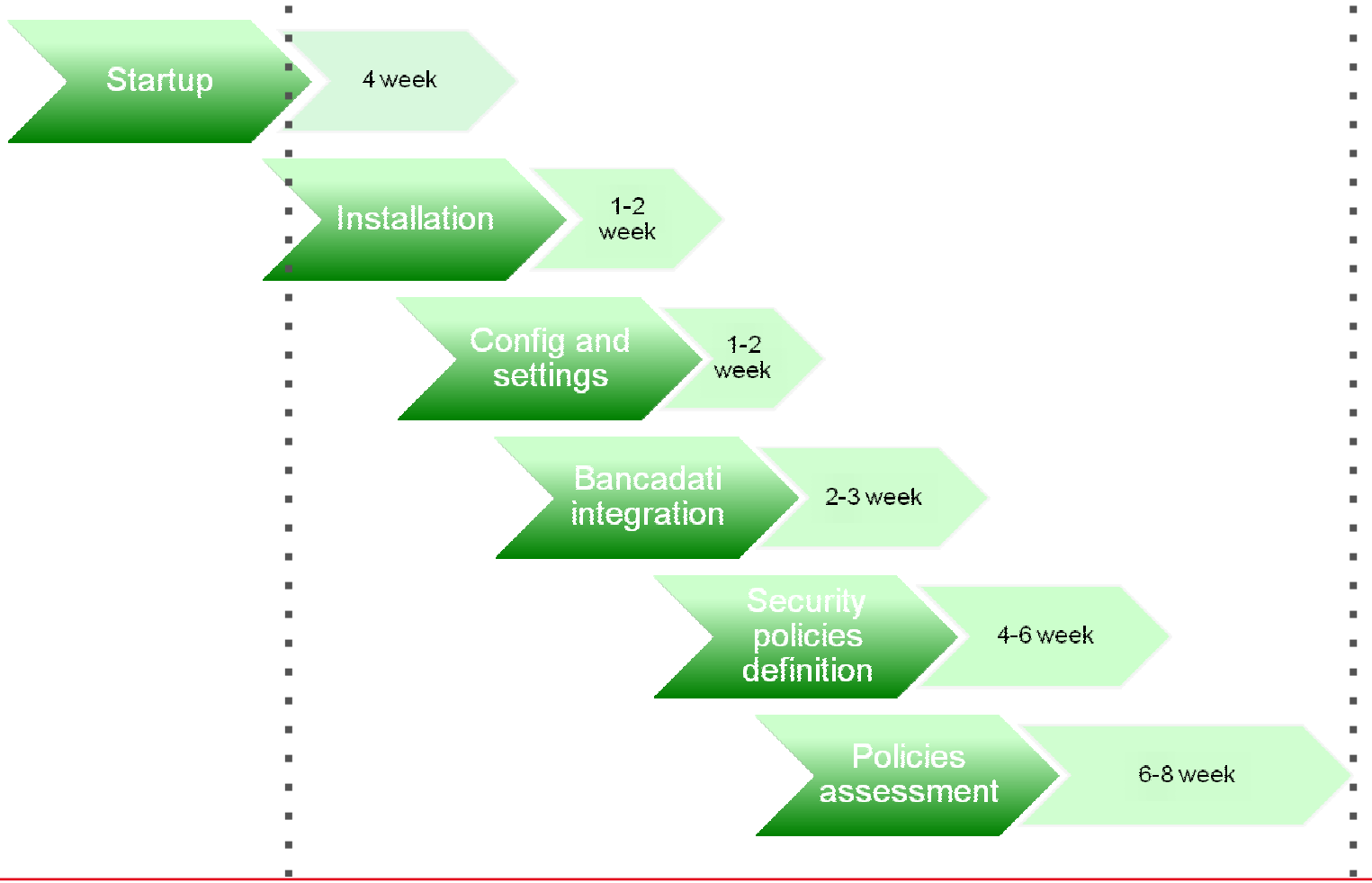
ORACLE
IBM DB2
SQL Server
TERADATA
SYBASE
MySQL
Informix

Attuale copertura delle piattaforme IT implementate



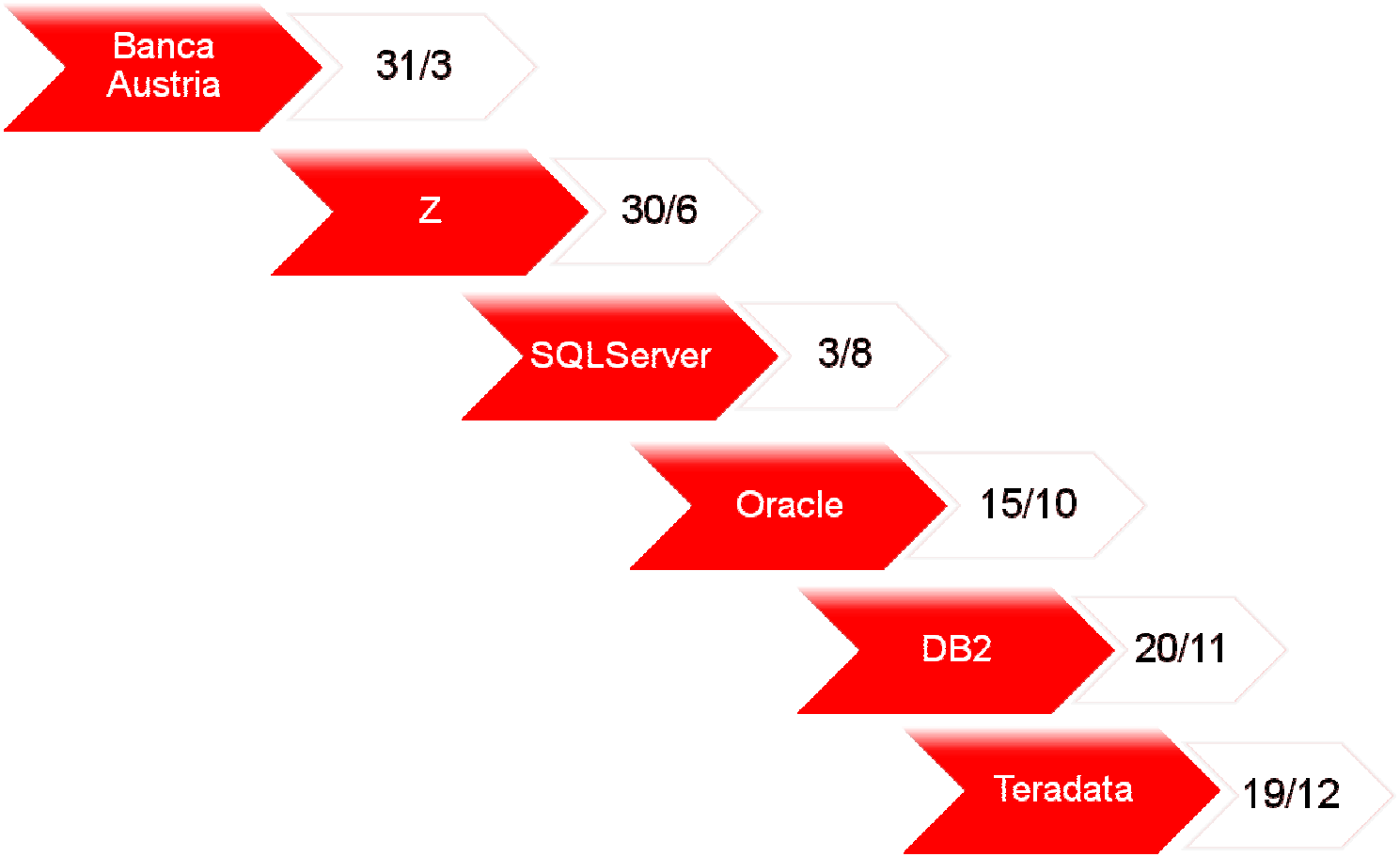
Primo Progetto: Protezione di Bancadati con Guardium

- Planning



Estensione del perimetro Guardium su Bank of Austria, MainFrame e mondo Open

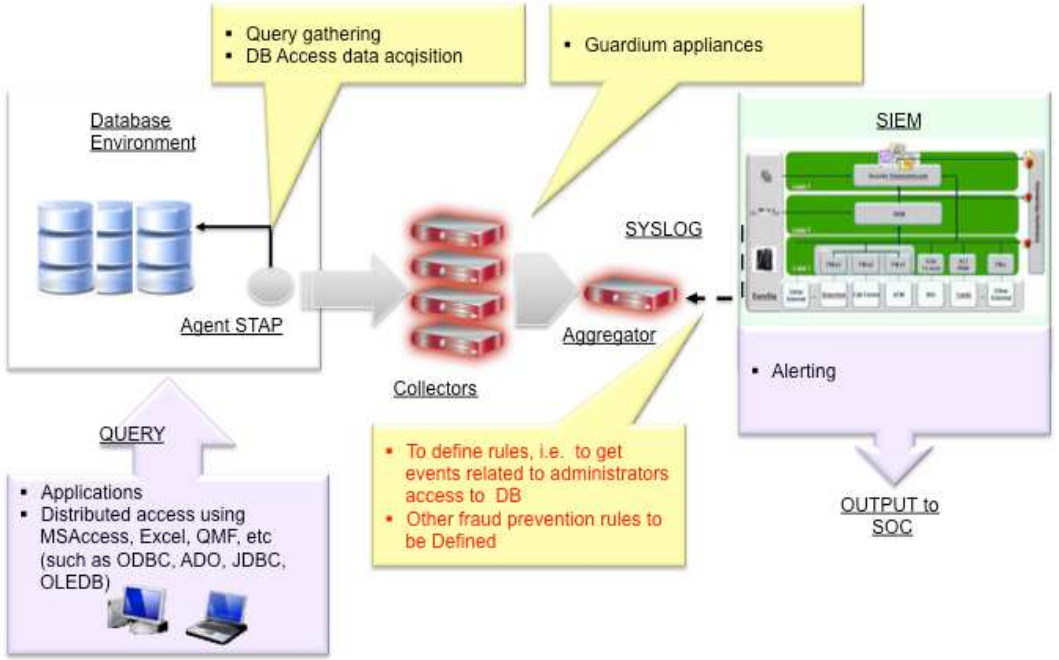
- Planning



IBM GUARDIUM

- **LOG MANAGEMENT**: Guardium opera a livello applicativo, monitorando gli accessi e le attività su oggetti sensibili effettuate da DBA e utenti del database. Le informazioni sono acquisite da agenti e sono costituite da 'query-text', non vengono acquisiti i risultati del query, evitando di gestire dati sensibili o bancari.

- **ALERTING**: i dati collezionati dagli agenti sono inviati agli appliance che verificano la rispondenza delle regole e producono i report in accordo con le policy configurate. I report prodotti ed eventuali allarmi sono inviati al SIEM possono contente solo dati statistici riassuntivi o gli statement delle query, in funzione della configurazione



Alerting – Proposta di Policy e regole

1. Timing criteria
   - Accessed table by non “system” and “batch” user from 18 pm to 8 am
   - Accessed table by non “system” and “batch” user week end and bank holiday time
2. User Management criteria
   - GRANT, REVOKE USER
   - PERMISSION CHANGE
3. Disruptive commands criteria
   - DROP, TRUNCATE, executed by Administrators
4. Write criteria
   - UPDATE, DELETE, INSERT executed directly on DB by DBA
5. Read criteria
   - EXPORT, queries (SELECT *)
   - Users executing queries which return more than x records (1000?)
   - Queries with high number of JOIN (>20?)
   - Similar queries ran with slightly different parameters
6. Sensible Data access criteria
   - CRITERIA TO BE DEFINED BY “BUSINESS USERS” (i.e. Bank, Audit, Internal Controls, ecc.)

Log Management – Opzioni di integrazione ad un SIEM

Sottoinsieme delle attività tracciate e invio al SIEM

La soluzione consiste nel configurare policy che monitorino solo le attività più significative sul database e quindi l'invio al SIEM dei report collegati alle attività tracciate.

- Pro: migliori performance in entrambi gli ambienti
- Contro: difficoltà nella correlazione del 100% degli eventi sul SIEM, rischio di non avere tutte le attvità e gli accessi al DB traccaiti

Log Completi su Guardium e invio parziale al SIEM

La seconda soluzione consiste nel configurare policy che monitorino tutte le attività effettuate sul database, ma solo una parte delle informazioni tracciate vengono inviate al SIEM mediante report personalizzati.

- Pro: migliori prestazioni con minori richieste di hardware per il SIEM (dischi, CPU,…)
- Contro: difficoltà nella correlazione del 100% degli eventi sul SIEM (es. Correlazione tra Active Directory e attività sul DB non integrate nel SIEM)

Log Completo su Guardium, tutti i log inviati al SIEM

Soluzione scelta, consiste nel configurare policy che monitorino tutte le attività effettuate sul database, quindi configurare i report corrispondenti per l'invio al SIEM.

- Pro: una unica interfaccia/sistema per l'analisi dei log ed il reporting
- Contro: prestazioni complessive inferiori (carico su hardware e network) nel caso di elevate quantità di dati (ma da verificare)

Esempi di report di Guardium e log su SIEM

<u>Caratteristiche peculiari e fondamentali di Guardium per la compliance normativa</u>

- Elevato dettaglio nell'acquisitzione delle informazioni
- Anonimizzazione nativa nel trattamento dei dati
- Possibilità di selezionare il dettaglio delle informazioni tracciate

Record Affected >500

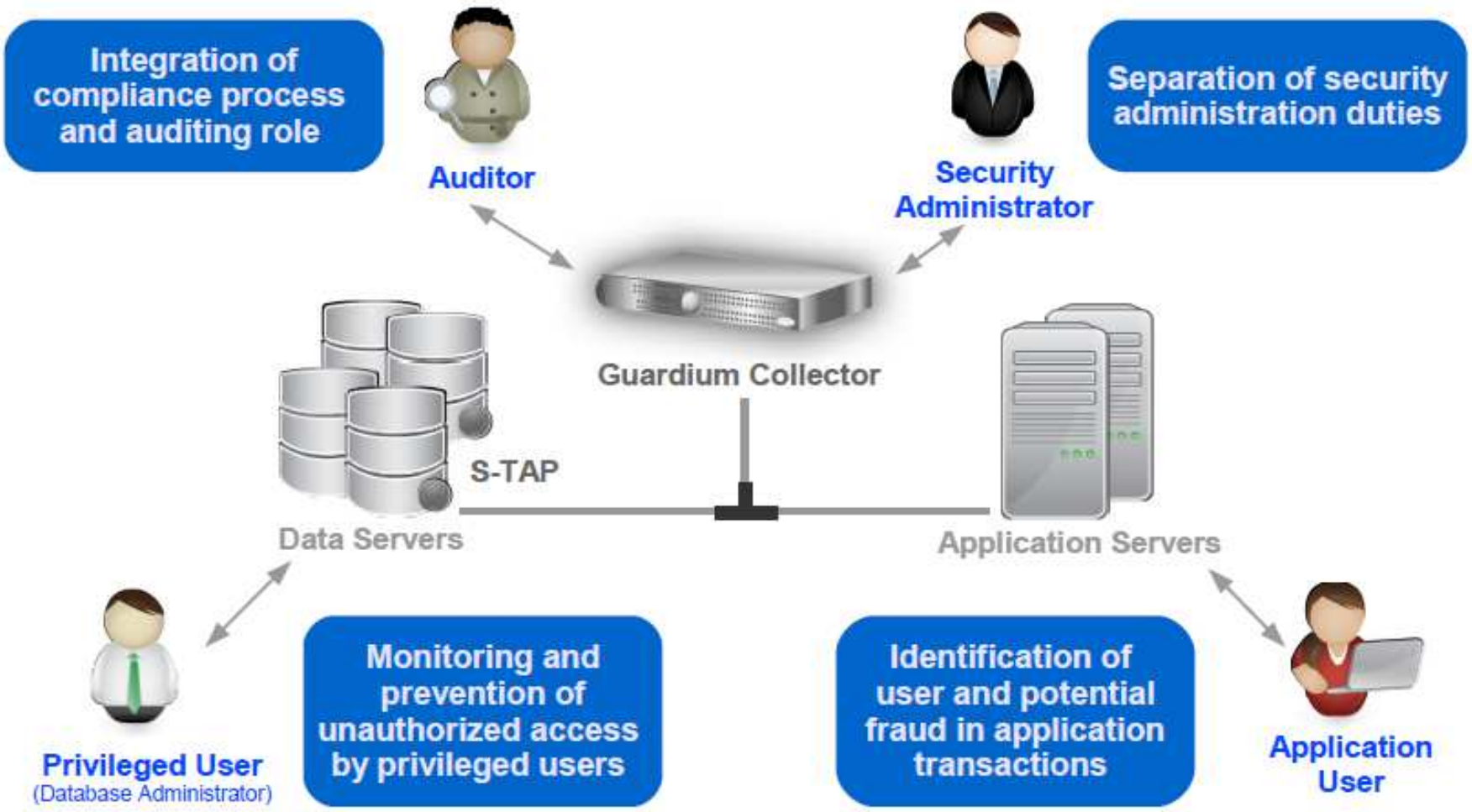
Start Date: **2012-02-24 08:00:00** End Date: **2012-02-24 08:20:00**
Using Merge Period Between 2012-02-10 and 2012-02-24.
Aliases: OFF Remote Source: usdbspl004.hd00.unicreditgroup.eu

Session Start	Client IP	Server Type	Server IP	Database Name	Network Protocol	DB Protocol	Client Port	Server Port	DB User Name	Source Program	Sql
2012-02-24 07:59:26.0	10.248.8.250	DB2	10.113.3.40	[redacted]	TCP	DRDA	1391	12153		MSACCESS.EXE	SELECT ?.?.? ,?.?.? ,?.?.? ,?.?.? ,SUM(?.?.?) FROM ?.?,?.?,?.?,?.? WHERE (((((?.?.? = ?.?.?) AND (?.?.? = ?)) AND (?.?.? = ?.?.?)) AND (?.?.? IN (?))) AND (?.?.? = ?.?.?)) AND (?.?.? = ?)) GROUP BY ?.?.? ,?.?.? ,?.?.? ,?.?.?
2012-02-24 07:59:26.0	10.248.8.250	DB2	10.113.3.40	[redacted]	TCP	DRDA	1391	12153		MSACCESS.EXE	SELECT ?.?.? ,?.?.? ,?.?.? ,?.?.? ,SUM(?.?.?) ,SUM(?.?.?) ,SUM(?.?.?) ,SUM(?.?.?) ,SUM(?.?.?) ,SUM(?.?.?) ,SUM(?.?.?) ,SUM(?.?.?) ,SUM(?.?.?) ,SUM(?.?.?) ,SUM(?.?.?) ,SUM(?.?.?) ,SUM(?.?.?) FROM ?.?,?.?,?.?,?.? WHERE (((((?.?.? = ?.?.?) AND (?.?.? = ?)) AND (?.?.? = ?.?.?)) AND (?.?.? IN (?))) AND (?.?.? = ?.?.?)) AND (?.?.? = ?)) GROUP BY ?.?.? ,?.?.? ,?.?.? ,?.?.?
2012-02-24 07:59:26.0	10.248.8.250	DB2	10.113.3.40	[redacted]	TCP	DRDA	1391	12153		MSACCESS.EXE	CONNECT TO [redacted] USING ?????????????????????

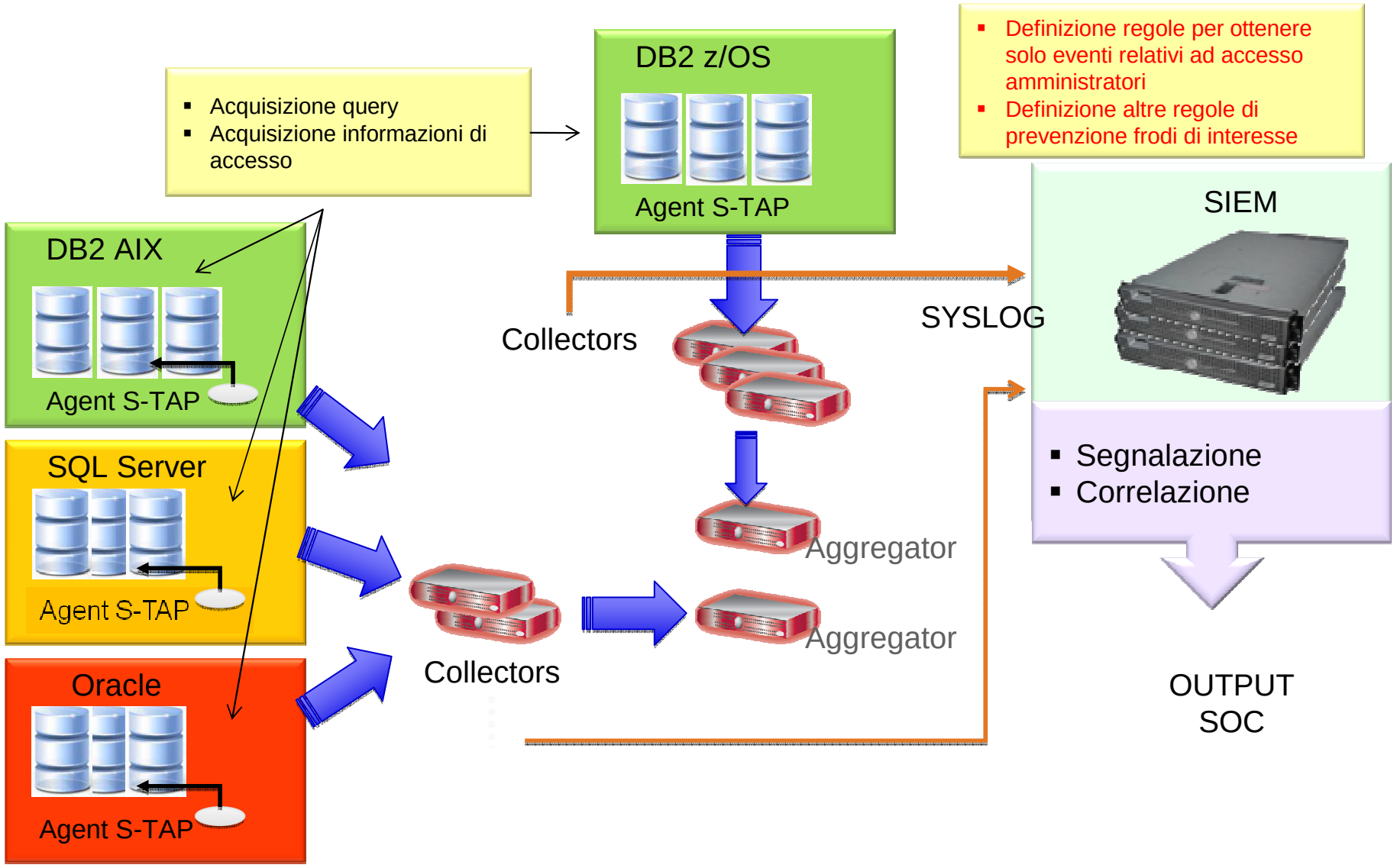
10.113.115.186 Feb 24 07:41:23 us[redacted] guard_sender[3382]: Alert based on rule ID Alert - Records Affected > 500#012Category: Classification: Severity LOW #012Rule # 20120 [Alert - Records Affected > 500]#012Request Info: [Session start: 2012-02-24 07:39:45 Server Type: DB2 Client: 10.248.8.250 (F0064411) Server: 10.113.3.40 () Client PORT: 4724 Server Port: 12137 Service Name: USUDB Net Protocol: TCP DB Protocol: DRDA DB Protocol Version: 3.0 DB User: [redacted]#012Application User Name #012Source Program: MSACCESS.EXE Authorization Code: 0 Request Type: ROW_COUNT Last Error: #012SQL: SELECT "R[redacted]" ,"NDG" ,"F[redacted]" ,"TP_CAT_CC" ,"TP_[redacted]" ,"SPORT" ,"IM[redacted]NT_CTV" ,"I[redacted]Q_CTV" ,"DT_RIF" FROM "F0".[redacted]LG" WHERE ("FL_EST_RAPP" = '?')#012 To add to baseline:

UniCredit Business Integrated Solutions

Segregation of Duties



Modello Architetturale Implementato



Strategia delle Security Policy

FASE 1: Monitoraggio Passivo'

FASE 2: Attivazione funzionalità di blocco

Identification of each transaction

- **Who:** database user, application user, OS user
- **What:** database, object, field
- **When:** timestamp, time period
- **Where:** client IP, server IP
- **How:** access, exception, data extrusion

Logging

- Reporting on critical activity
- Establishing baseline of known use patterns
- Finding anomalies in observed data

Alerting

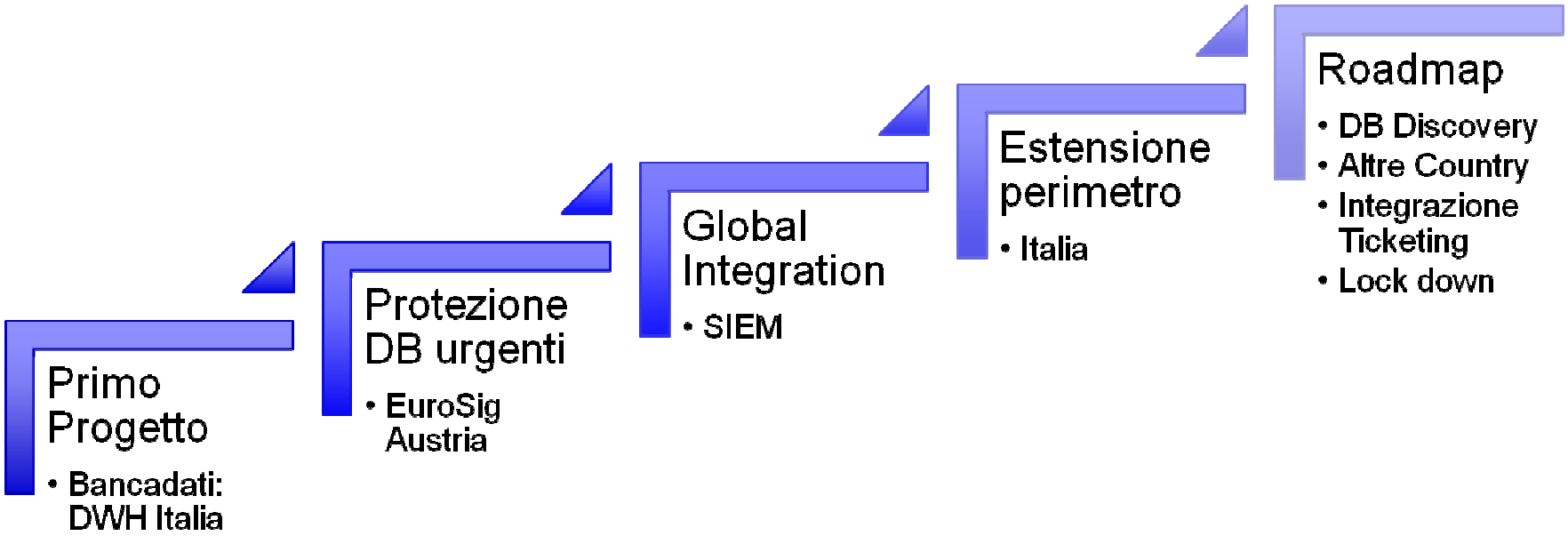
- Email messages
- Enterprise events management

Access Control

- Termination
- Quarantine
- Redact

Fase 2

Roadmap implementazione complessiva



Grazie

Giacomo Segalli
g.segalli@reply.eu

Giovanni Papa
giovanni.papa@unicreditgroup.eu