

La trasmissione inizierà a breve

Connetti il tuo **audio** 



Chiama tramite PC



Audio



Connessione
audio e video



Chiama tramite computer

oppure



Chiama via telefono



02 87103980



ID Evento 926 017 872# e poi ancora #

Informazioni sul meeting



Il meeting verrà registrato e sarà disponibile dopo l'evento per il riascolto



Tutte le linee sono silenziose per garantire un buon ascolto



Potete sottoporre i vostri commenti durante l'evento usando l'apposita funzione **“Chat”**



Se avete domande, potete sottoporle in qualsiasi momento nel box **“Q&A”** – le risposte verranno fornite alla fine

Relatori



Eugenio Nicotra

*Digital Marketing Manager
Cybertech*

eugenio.nicotra@cybertech.eu



Gabriele Ventura

*Security Specialist
Cybertech*

gabriele.ventura@cybertech.eu



Andrea Polverino

*Security Specialist
Cybertech*

andrea.polverino@cybertech.eu

WEBINAR - 17 Settembre ore 12.00

DATA SECURITY & PRIVACY

*Tecnologie e soluzioni
per la sicurezza data-centric*



IL GRUPPO CYBERTECH

Eugenio Nicotra
Digital Marketing Manager Cybertech



THE CYBERSECURITY EXPERTS OF THE **ENGINEERING** GROUP

**Enabling Digital Transformation
with a Holistic Vision of IT Security
and Asset Management**

People

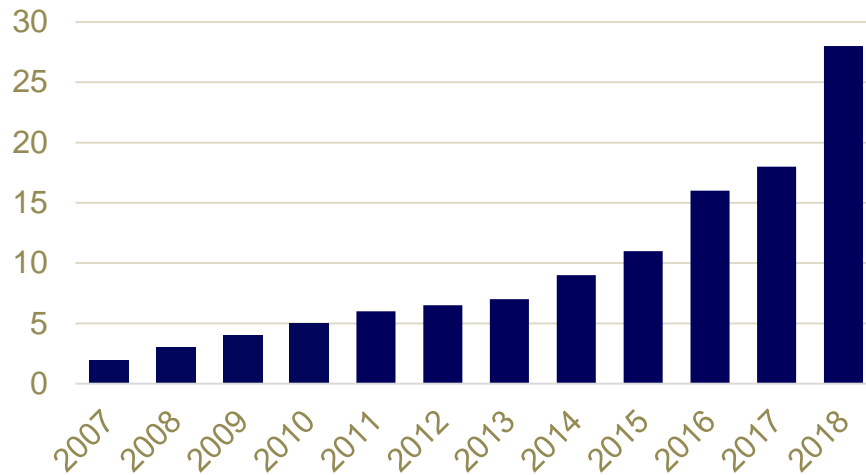
 **300 Employees**

15%  Methodology & Consulting

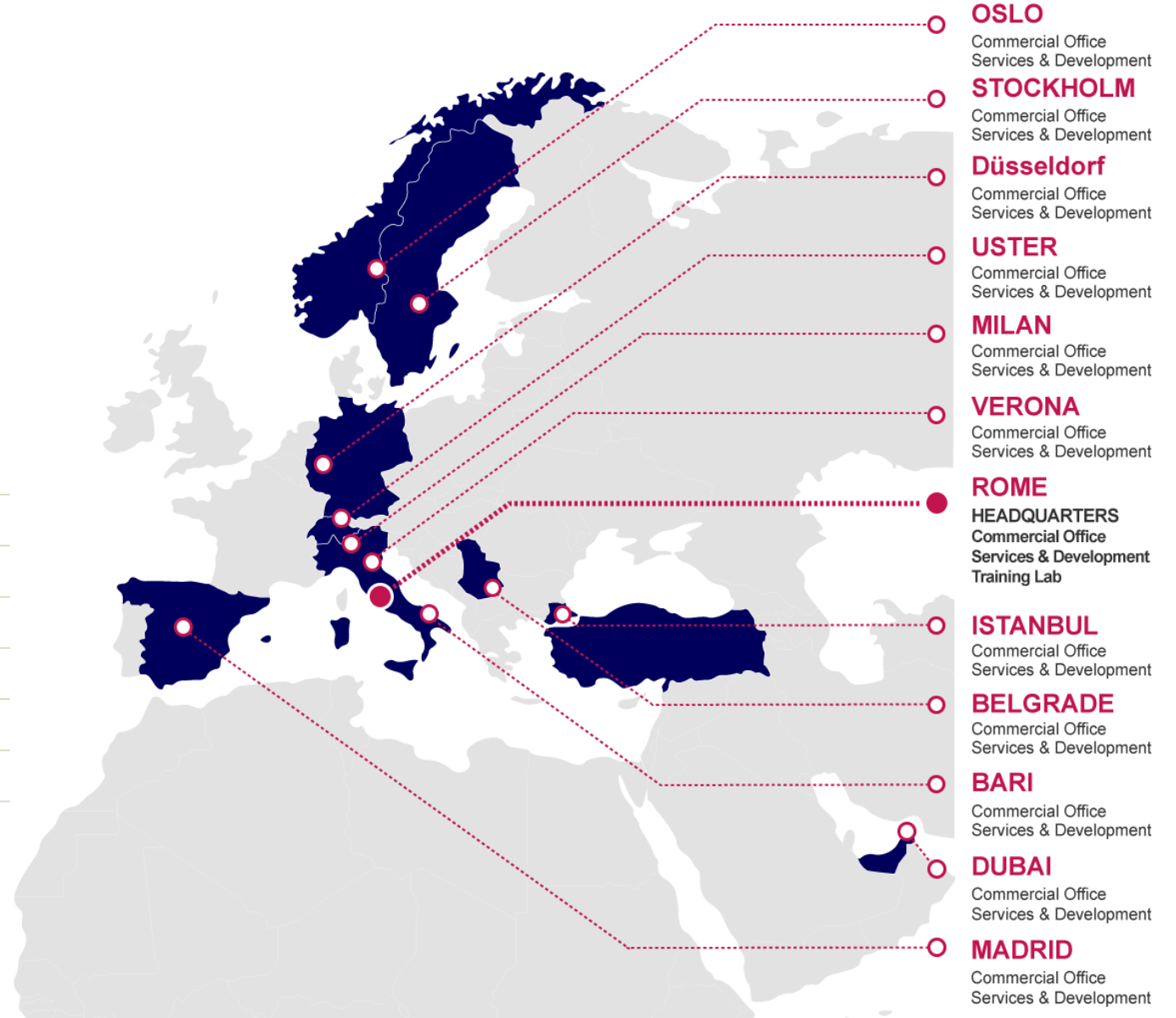
35%  Senior Technical Professionals

50%  Product Specialist

Turnover



International Coverage



OUR VALUE PROPOSITION

The "new balance" of security

Securely enable digital business



CLOUD



MOBILITY



SOCIAL
MEDIA



BIG DATA



INTERNET
OF THINGS



TARGETED
ATTACKS



INSIDER
THREAT

INCREASED THREAT SURFACE



ENABLE THE BUSINESS

PROTECT THE BUSINESS

**DELIVER SECURE
NEW BUSINESS
SERVICES**



**SECURE THE MOBILE,
CLOUD-CONNECTED
ENTERPRISE**



**PROTECT AGAINST
INSIDER THREATS &
EXTERNAL ATTACKS**

WEBINAR - 17 Settembre ore 12.00

DATA SECURITY & PRIVACY

*Tecnologie e soluzioni
per la sicurezza data-centric*



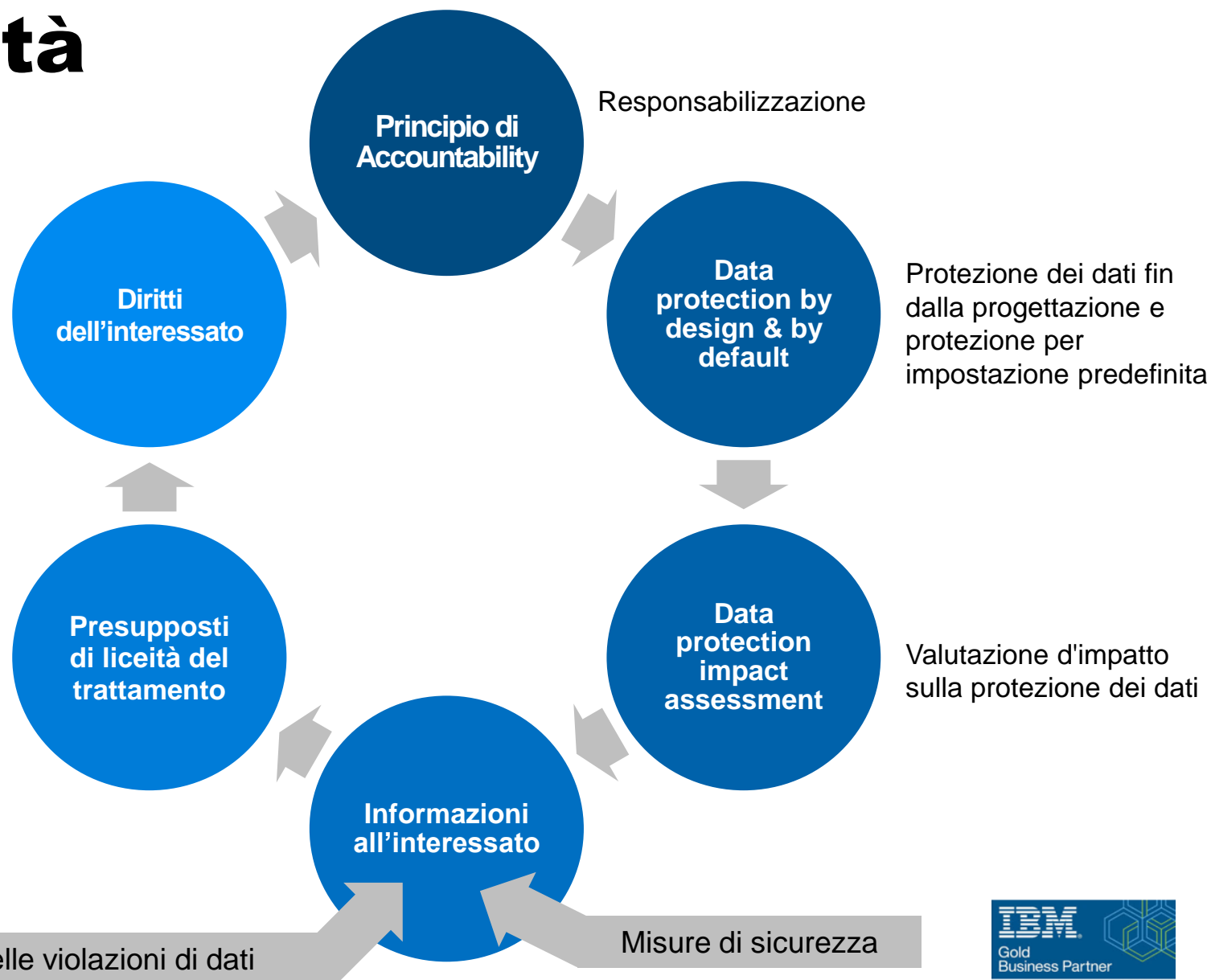
Sicurezza Dati (data security)

La sicurezza dei dati consiste nel proteggere i dati digitali, come quelli contenuti in una banca dati, da forze distruttive e dalle azioni indesiderate di utenti non autorizzati, come ad esempio un **cyberattack** o una violazione dei dati.

- I dati sono qualsiasi tipo di informazione digitale memorizzata.
- Ogni azienda ha bisogno di luoghi in cui conservare conoscenze e dati istituzionali.
- Spesso i dati contengono informazioni proprietarie:
 - Dati Personali
 - Dati HR dei dipendenti
 - Dati finanziari
- **La sicurezza e la riservatezza di questi dati è di fondamentale importanza.**

Principali novità

**Necessità di un
Modello Organizzativo
Privacy
...e dunque di un DPO
(Responsabile della
protezione dei dati)**



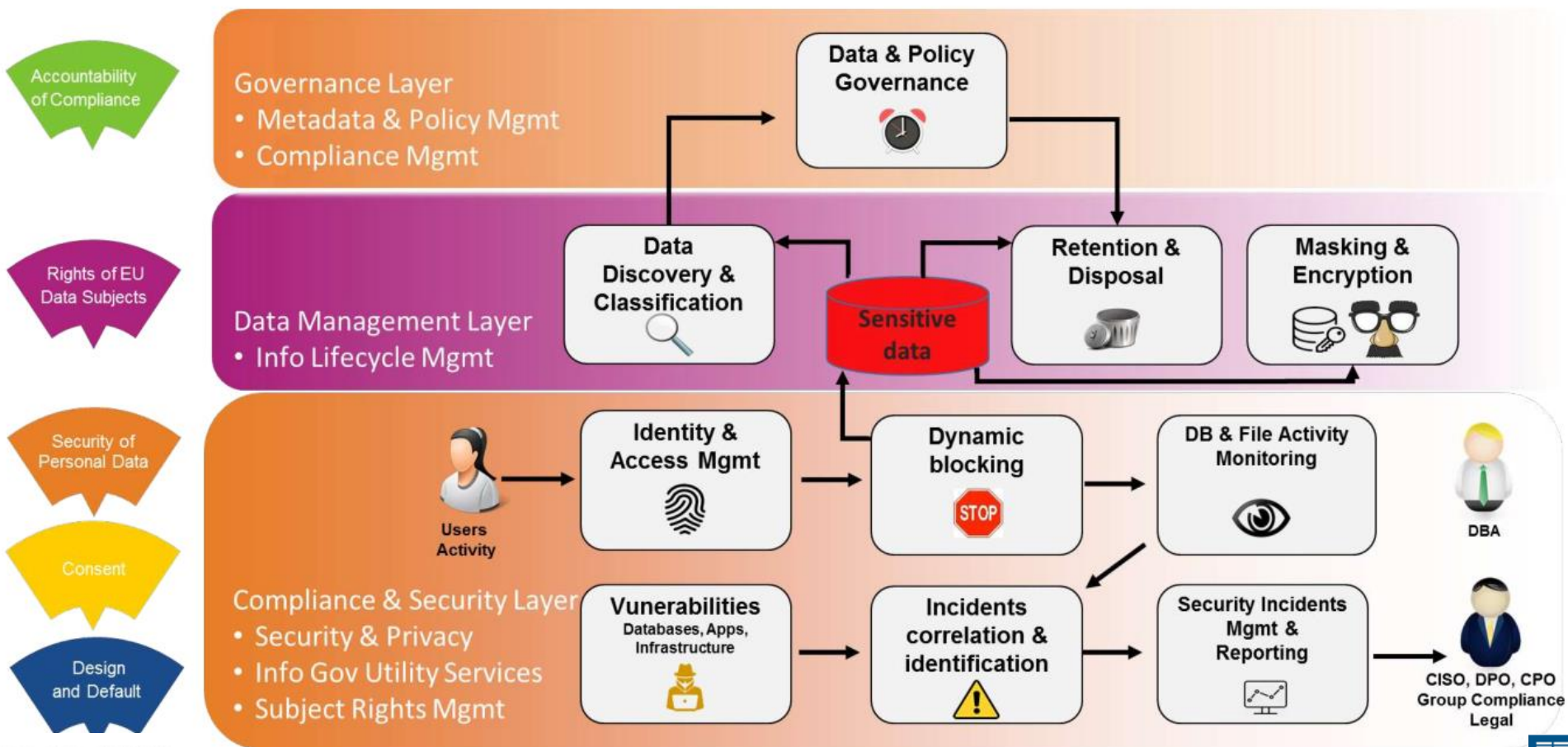
Le quattro questioni chiave per la sicurezza dei dati

Ci sono quattro questioni chiave nella sicurezza delle banche dati, proprio come per tutti i sistemi di sicurezza:

- **Disponibilità**
- **Autenticità**
- **Integrità**
- **Riservatezza**



Cosa possono fare le aziende per mettere al sicuro i dati in termini di compliance?



Cosa bisogna fare da ora per garantire la sicurezza dei dati critici aziendali?

RACCOMANDAZIONI	APPLICABILITÀ
Analisi Dati Non Strutturati	Non risiedono in banche dati o storage di dati tradizionali. Possono avere una struttura interna, ma non si adattano ad un modello di dati relazionale.
Analisi Dati Strutturati	Sono i dati conservati in database, organizzati secondo schemi e tabelle rigide. Questa è la tipologia di dati più indicata per i <i>modelli di gestione relazionale</i> delle informazioni.
Data Breach	Il GDPR definisce una violazione dati come un'azione che porta alla distruzione, perdita, alterazione o accesso a dati personali trasmessi, immagazzinati o processati in altro modo.
Data Masking	Applicazione di maschere «intelligenti» in modo da ottenere dei dati totalmente non riconducibili a quelli reali e quindi utilizzabili in ambienti di test (pseudonimizzazione).
Auditing e Report	<ul style="list-style-type: none">• Reports: Compliance Report, Data Assessment Report, Data Topology Report.• Auditing: Event logs, harvest e action audit trails
Vulnerability Assessment periodico	Il Database Vulnerability Assessment viene utilizzato per scansionare l'infrastruttura del database alla ricerca di vulnerabilità e fornire una valutazione dello stato di salute della sicurezza del database e dei dati, con misurazioni in tempo reale e storiche.
Monitorare le operazioni e le minacce	Trova automaticamente i database sulla rete, li protegge con una serie di difese preconfigurate e aiuta a creare policy di sicurezza personalizzate per l'ambiente di lavoro.

Strumenti per proteggere i dati – Come gestire la complessità

- In base alle politiche di sicurezza i dati devono essere classificati secondo la loro «sensibilità».
- Una volta che ciò è avvenuto, i dati più sensibili sono oggetto di misure supplementari per salvaguardare e garantire la loro integrità e disponibilità.
- Tutti gli accessi a questi dati sensibili devono essere registrati.
- Controllo dell'accesso fisico alla banca dati o all'area in cui i dati sono memorizzati.
- **Active** o **Open Directory** sono sistemi di gestione dell'autenticazione centralizzata per controllare e registrare gli accessi a tutti i dati del sistema.
- La crittografia dei dati sensibili è fondamentale se accediamo da reti pubbliche.

Database activity monitoring

La sfida quotidiana riguarda la protezione dei dati alla sorgente

- Il perimetro puo' essere oltrepassato.
- Gli endpoints sono vulnerabili
- Gli utenti interni sono un potenziale rischio
- Gli account degli utenti privilegiati sono pozzi di dati 'rilevanti' in attesa di essere intercettati.



**Proteggere i dati è una
necessità a livello aziendale**

IBM Guardium

Protegge i dati critici da **accessi** non autorizzati e consente alle aziende di conformarsi alle normative e gli standard del settore.

Prevent data breaches

Impedire la divulgazione o la perdita di dati sensibili

Privacy assicurata

Prevenire modifiche non autorizzate ai dati (integrità)

Ridurre il costo della compliance

Automatizza e centralizza i controlli attraverso normative diverse ed ambienti eterogenei

Identify data risks

Rileva le informazioni sensibili, identifica i dati inattivi, valuta le lacune e le vulnerabilità di configurazione

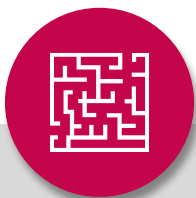


Le sfide dei dati di oggi...



Compliance

- Regolamenti in espansione
- Volumi di dati in costante crescita
- Alto rischio Data Breach



Complessità

- Migliaia di potenziali vulnerabilità
- Ambienti dati eterogenei
- Mancanza di competenze interne all'organizzazione



Comunicazione

- Prove di conformità
- Dimostrazione dei progressi/KPIs
- Ruoli & Responsabilità funzionali



Costi

- Sanzioni rilevanti in caso di inadempienza
- Le soluzioni tradizionali sono costose e non danno certezze

IBM Security Guardium Analyzer: *Casi d'uso*

Identificare in modo efficiente e semplice le informazioni personali e sensibili, comprendere i rischi associati a tali dati e intraprendere azioni.

Risk-scoring: applicato ai risultati di vulnerabilità e ai dati classificati

Quali dati avete e dove sono?

Find Sensitive Data



Next-generation: motore di classificazione per trovare e classificare i dati regolamentati

Uncover Risk



I tuoi dati sono al sicuro in questi archivi?

Take Action

Come faccio a dare la priorità alle azioni da intraprendere?

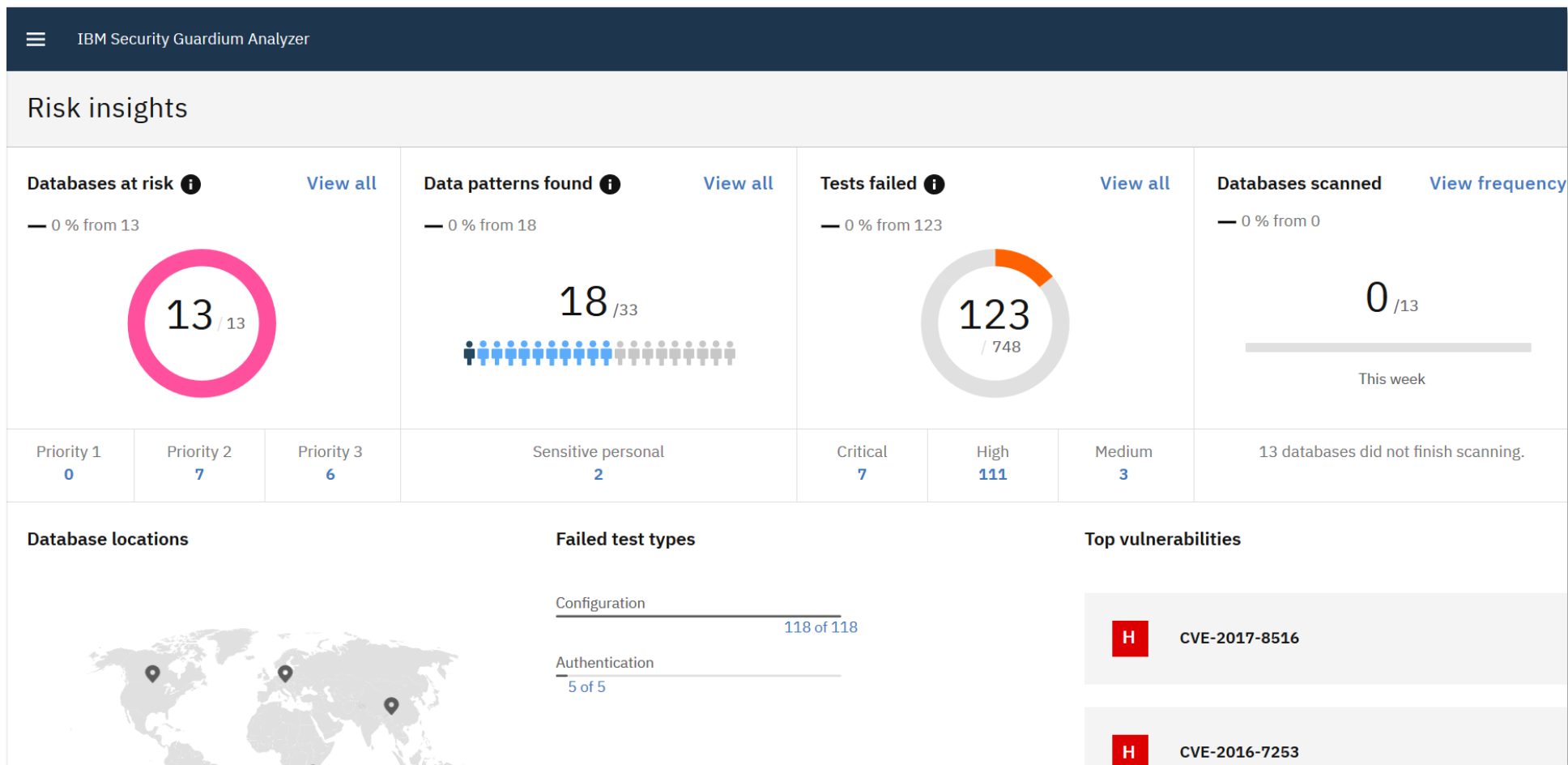


Raccomandazioni di bonifica e relazioni per affrontare i rischi legati ai dati

IBM Security Guardium Analyzer

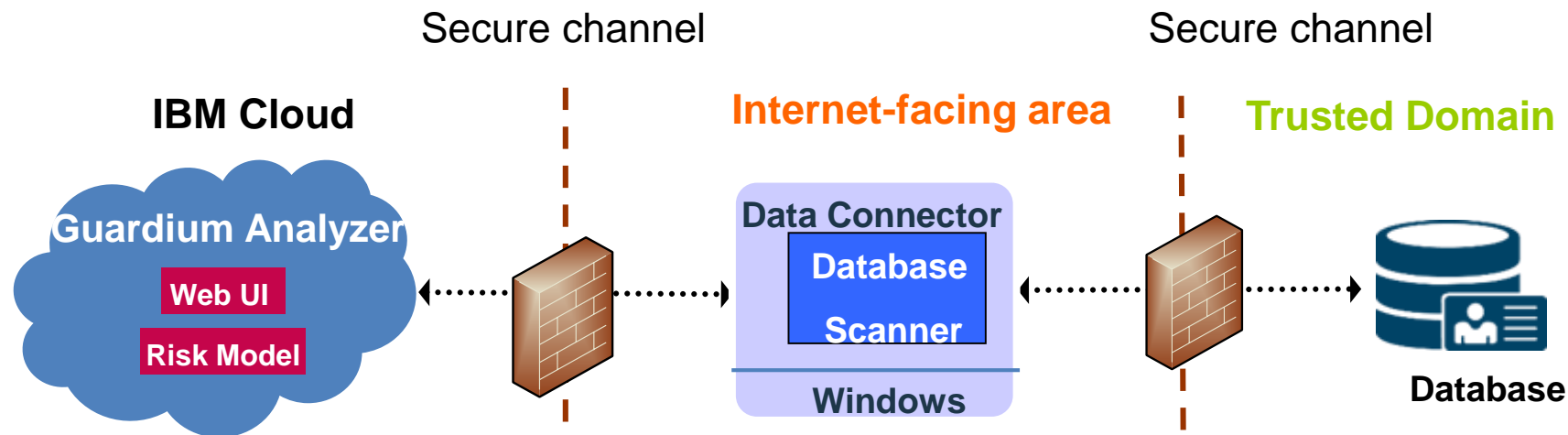
Tutto sotto controllo!

*Trovare i dati
regolamentati.
Scoprire i rischi.
Agire.*



IBM Security Guardium Analyzer

Ma come funziona?



La Dashboard di Guardium Analyzer:

- Fornisce una visione centralizzata e prioritaria basata sul rischio
- Visione di come i dati sono distribuiti geograficamente
- **Reporting centralizzato** per gli auditors in caso di Audit

Il Data Connector:

- Scansiona i database alla ricerca di dati personali e sensibili
- Scansione delle vulnerabilità del database
- **Non memorizza e non sposta i dati personali sensibili**
- Invia solo i **metadati** nel Cloud
- Supporto Db2, Oracle, MySQL, SQL Server... e molto altro nel futuro (**flessibilità**)

Principali benefici in sintesi

IBM Security Guardium Analyzer

Trovare i dati

Scoprire i rischi

Agire!

- ✓ **Definisce un processo di valutazione** a sostegno dei «mandati di conformità» (e.g. GDPR) locali o globali.
- ✓ Puoi ottenere una visione degli asset **incentrata su rischio e priorità**.
- ✓ Utilizza una dashboard **intuitiva e facile**.
- ✓ **Focalizza l'attenzione sul supporto al proprio business** senza investire in risorse IT o hardware.
- ✓ **Soluzione flessibile e facilmente personalizzabile**.

IBM Security Guardium Analyzer

Piano costi per livello di servizio

Piano Gratuito

Prova questa versione di prova gratuita per scoprire come Guardium Analyzer può aiutarti a ricercare dati regolamentati, valutare vulnerabilità e rischi e intraprendere azioni.

Piano Standard

Con il piano standard, si paga a scansione e il servizio consente di trovare dati regolamentati, valutare vulnerabilità e rischi e intraprendere azioni.

Piano Professionale

Con il piano professionale, si paga per connessione al database, per facilitare la ricerca di dati regolamentati, la valutazione di vulnerabilità e rischi e l'attuazione di azioni.

Da
€27.98*

a scansione (attività) al mese

- Connettersi a un massimo di 3 database
- Supporta database on-prem e su cloud, che includono: Oracle, IBM db2, Microsoft SQL Server e MySQL
- Sistema operativo Windows necessario per il connettore dati
- Supporto: IBM Support Community
- Personalizzazione, dashboard di avanzamento

Da
€48.25*

a scansione (attività) al mese

- Abbonamento mensile senza alcuna soglia minima mensile
- Pagamento mensile a scansione e connessione a database su cloud e on-premise, singoli o multipli.
- Supporta database on-prem e su cloud, che includono: Oracle, IBM db2, Microsoft SQL Server e MySQL
- Sistema operativo Windows necessario per il connettore dati
- Supporto: IBM Support Community

- Abbonamento mensile con un termine minimo di 12 mesi
- Pagamento per connessione al database al mese, con scansioni illimitate per ogni database connesso
- Supporta database on-prem e su cloud, che includono: Oracle, IBM db2, Microsoft SQL Server e MySQL
- Sistema operativo Windows necessario per il connettore dati
- Supporto: Supporto per il prodotto IBM standard
- Personalizzazione, dashboard di avanzamento

**Prezzo mostrato ad esclusione delle tasse applicabili*

Session Q&A

Webinar's Take-aways

Take-aways Gabriele Ventura

- Identificazione e protezione delle informazioni critiche.
- Controllo per limitare il rischio.
- Monitoraggio in real time (IBM Guardium)
- Salvaguardia della reputazione del Brand.

Take-aways Andrea Polverino

- Trovare i dati «sensibili» (*Database activity monitoring*)
- Reporting e interfaccia intuitiva.
- Piani di costo adattabili alle diverse esigenze.

Contatta gli esperti tecnici Cybertech

Gabriele Ventura

Security Specialist Cybertech

Mobile +39 345 8812451

Email gabriele.ventura@cybertech.eu

Andrea Polverino

Security Specialist Cybertech

Mobile +39 392 1653635

Email andrea.polverino@cybertech.eu

Contatta il Marketing Cybertech Group & DBG IBM

Sales IBM Digital Sales

Piero Stanco

Mobile +39 349 2779058

pietrostanco@it.ibm.com

Marketing Cybertech

Eugenio Nicotra

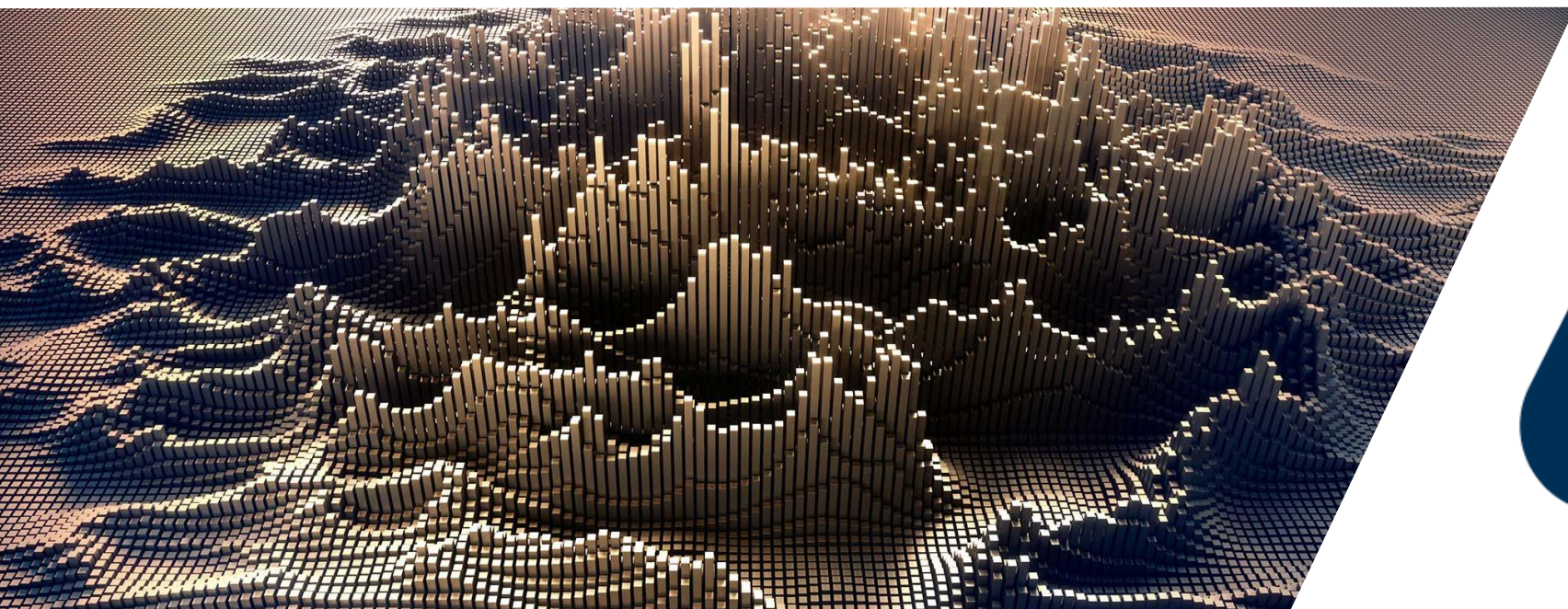
Mobile +39 335 7693716

eugenio_nicotra@it.ibm.com

eugenio.nicotra@cybertech.eu



Grazie



Proteggere le informazioni critiche

Tecniche

- Sostituzione
- Rimescolamento
- Numero e varianza dati
- Crittografia
- Eliminazione
- Mascheramento

Tipologie

- Mascheramento statico dei dati
- Oscuramento statistico dei dati
- Mascheramento dei dati al volo
- Mascheramento dinamico dei dati

IBM GUARDIUM

Protegge i dati critici da **accessi** non autorizzati e consente alle aziende di conformarsi alle normative e gli standard del settore.

