SECURITY SUMMIT

Security Summit

Napoli 28 maggio 2026

Clusit

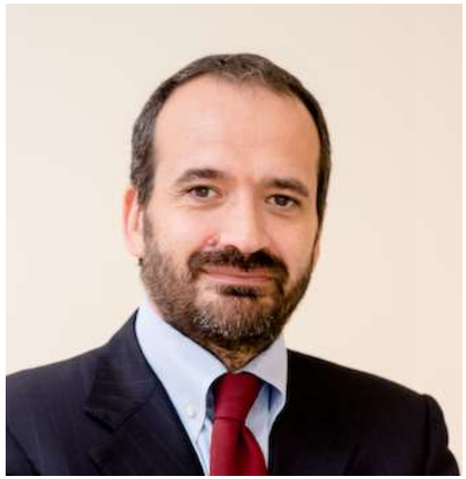
ASTREA

Sessione

Transparent Security:
controllo, sovranità e automazione nel nuovo paradigma cyber

Relatore | Christian Persurich, PhD
Relatore | Ing. Nancy Laurenda

Michele Onorato



Membro del Comitato Scientifico

Partner @P4I – GRUPPO DIGITAL360

Professore – Master CyberSecurity di Experis Academy

bitCorp®

Christian Persurich
CEO - bitCorp

Ing. Nancy Laurenda
Software Architect, Product & Deployment Engineer - bitCorp

Sovranità digitale europea

- Riguarda la capacità di agire autonomamente e di scegliere soluzioni proprie, mantenendo la collaborazione internazionale quando possibile.

- Investire in tecnologie strategiche come calcolo ad alte prestazioni, semiconduttori, reti di nuova generazione, satelliti, quantum, cybersecurity, cloud e AI, favorendo l'adozione pubblica e privata, riducendo dipendenze strategiche e stimolando investimenti privati e appalti pubblici mirati.

- Include la regolamentazione di infrastrutture, dati e tecnologie, garantendo che dati sensibili siano protetti da interferenze esterne e leggi extraeuropee.

Il punto di contatto tra sovranità e Cyber security

SOVRANITA' DIGITALE

Controllo su dati
e infrastrutture

Normative di riferimento e Best Practice di sicurezza ICT
(es: GDPR, NIS 2, Cyber security Act, Data Act, Data Governance Act, EUCS, ISO 27001, ISO 27017/18, CISPE)

PRODOTTI E SERVIZI

INTRODUCONO DIPENDENZE TECNOLOGICHE

TRATTANO DATI CRITICI

OPERANO SU GIURISDIZIONI DIVERSE*

RISCHI DA PRESIDIARE

DATA SOVEREIGNITY RISK
Accesso a dati da paesi terzi

LOCK IN
Difficoltà a migrare verso altri provider

CONTINUITA' OPERATIVA
Interruzioni o degrado dei servizi

RISCHIO DI CONCENTRAZIONE**
Troppa dipendenza da pochi vendor

SECURITY GOVERNANCE DEI PRODOTTI/SERVIZI

CONTRATTO

Clausole critiche:
- Localizzazione e trattamento dei dati
- Diritti di audit
- Gestione subfornitori
- SLA e penali
- Incident & breach notification
- Exit strategy e portabilità

SECURITY BY DESIGN

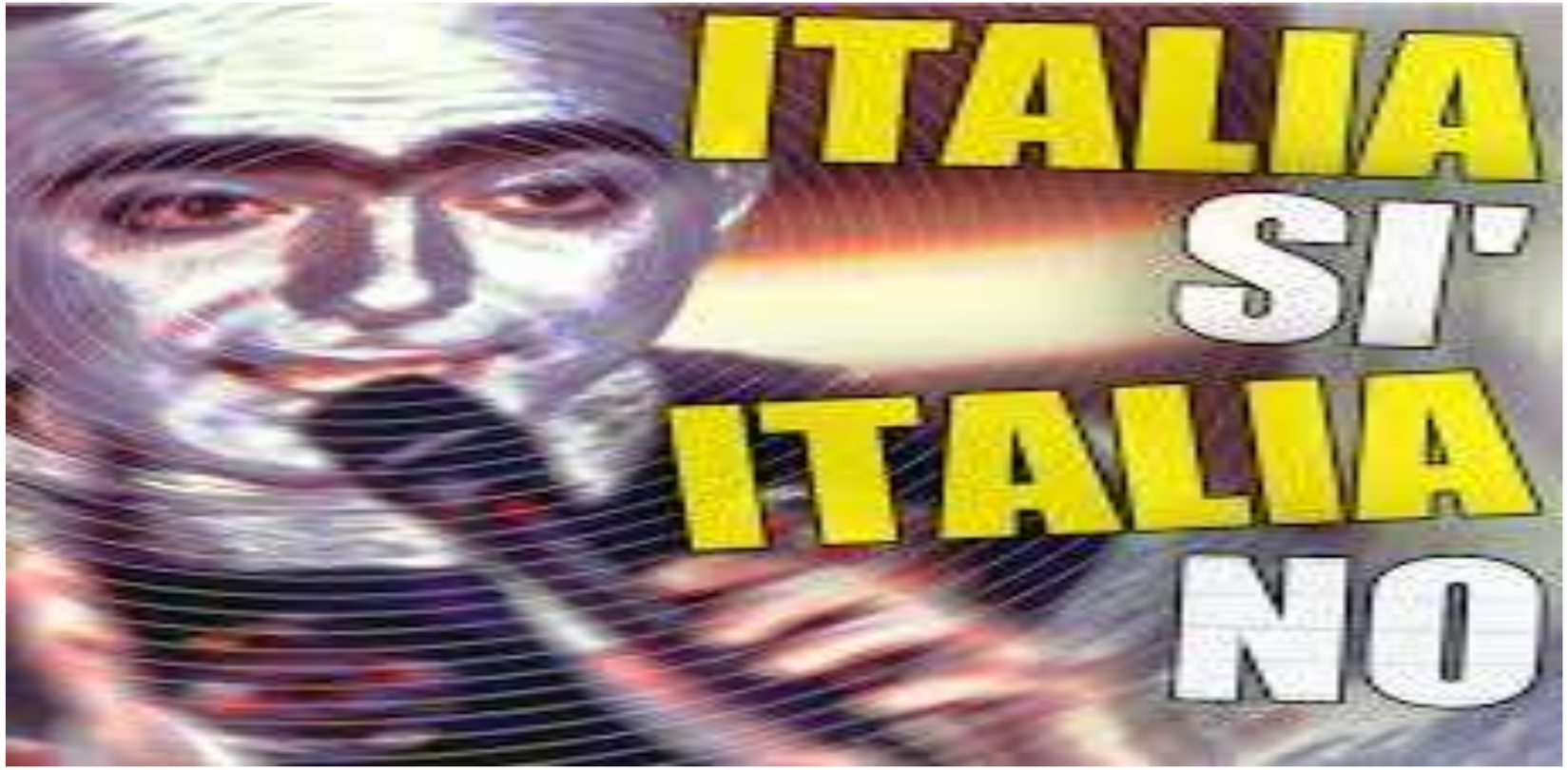
- **Selezione:** Due diligence su sicurezza e data location
- **Onboarding:** Definizione contratti e controlli
- **Monitoraggio:** KPI, SLA, audit periodici
- **Exit:** Piano di uscita e migrazione

**Esempio concreto: Uso di servizi cloud di Amazon Web Services o Microsoft Azure con dati potenzialmente soggetti a normative extra-UE*
***Esempio concreto: Un'azienda che utilizza un unico provider cloud per tutti i sistemi core è esposta a rischio sistemico in caso di outage*

Impegno principale

- La dichiarazione rappresenta un impegno politico condiviso per ridurre le dipendenze strategiche, rafforzare capacità tecnologiche e preservare la democrazia, posizionando l'Europa come partner affidabile e innovativo nel contesto globale digitale.

Soluzioni italiane



bitCorp®

01

TRASPARENZA E SOVRANITÀ DEL DATO

Controllo, visibilità e protezione del tuo patrimonio più critico

VISIBILITÀ TOTALE
Sai sempre dove sono i tuoi dati e chi vi accede

CONTROLLO SULLA PRIVACY
Decidi tu dove risiedono i dati e chi può utilizzarli

PROTEZIONE CONTINUA
Sicurezza by design, verificabile e auditabile

CONTROLLO DEI FLUSSI INFORMATIVI
Monitora e governa ogni spostamento dei dati

TRASPARENZA NEI PROCESSI DI DETECTION & RESPONSE
Processi chiari, log completi, decisioni tracciabili

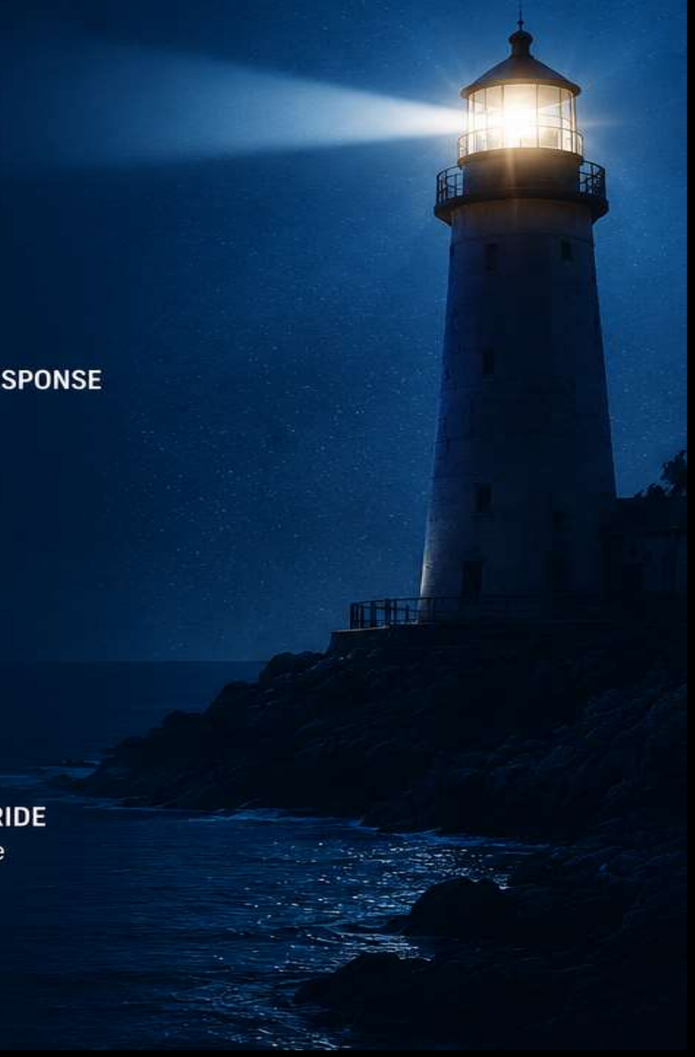
LOCALIZZAZIONE DEL DATO
Scegli dove i dati vengono archiviati e trattati

SEGMENTAZIONE INFRASTRUTTURALE
Isola i dati critici e riduci la superficie di attacco

RIDUZIONE DELLE DIPENDENZE CRITICHE
Meno lock-in, più controllo, maggiore resilienza

APPROCCIO SELF-HOSTED E ARCHITETTURE IBRIDE
Combina flessibilità del cloud e controllo on-premise

AUDITABILITÀ E COMPRENSIONE
Audit completi e comprensione profonda dei processi di sicurezza



02
AUTOMAZIONE INTELLIGENTE

Governare il controllo senza rinunciare all'innovazione

IL SUBSTRATO: LO STANDARD DI MERCATO

Microsoft
Sistema Nervoso Centrale

Identità · Produttività · Collaborazione · Cloud · Sicurezza

Massima integrazione con Microsoft.
Ma il controllo resta all'azienda.

LA NOSTRA DIFFERENZIAZIONE: 9 LEVE PER GOVERNARE E LIMITARE LA DELEGA

VPN E ACCESSI SICURI
Connessioni protette e zero trust

SEGMENTAZIONE DI RETE
Isola i dati critici e riduce il rischio di lateral movement

AUTOMAZIONE DELLE POLICY
Policy coerenti, applicate e aggiornate in automatico

ORCHESTRAZIONE CENTRALIZZATA
Gestione unificata di sistemi, identità e policy

MONITORAGGIO DISTRIBUITO
Controllo continuo e correlazione degli eventi

STORAGE E RETENTION CONTROLLATA
Dati protetti, classificati e conservati solo il tempo necessario

VISIBILITÀ OPERATIVA
Vedi tutto, in tempo reale, per decidere meglio

RIDUZIONE DELL'EFFORT IT
Meno attività ripetitive, più focus sul valore

RAPIDITÀ DI ADEGUAMENTO NORMATIVO
Rispondi rapidamente ai cambiamenti normativi

I RISULTATI

LIMITAZIONE DELLA DELEGA TOTALE A MICROSOFT
- Dati sotto controllo
- Processi trasparenti e auditabili
- Sovranità del dato preservata

→

VANTAGGI OPERATIVI E DI BUSINESS
- Riduzione dell'effort IT
- Processi più rapidi ed efficienti
- Orchestrazione centralizzata ottimizzata

→

CONFORMITÀ E RESILIENZA
- Rapidità di adeguamento normativo
- Auditability e compliance garantite
- Maggiore resilienza e continuità operativa

CONTROLLO DOVE SERVE · INTEGRAZIONE SENZA FRENI · TRASPARENZA END-TO-END · SICUREZZA BY DESIGN · AGILITÀ CONTINUA

bitCorp®

03

AI CONTROL LAYER

Governo, identità e responsabilità per l'AI in azienda

L'AI è già qui.
Agisce, decide, influenza.
Ma spesso nessuno sa chi sia, cosa faccia e chi risponda.

IL PROBLEMA: UN DIPENDENTE INVISIBILE

L'AI si comporta come un dipendente: accede ai dati, elabora informazioni, prende decisioni, interagisce con sistemi e persone.
Ma senza identità, ruoli, responsabilità e supervisione.

I RISCHI DI UNA GOVERNANCE ASSENTE

IDENTITÀ
Nessuna identità definita per le AI e gli agenti utilizzati

RUOLI
Assenza di ruoli e privilegi chiari: chi fa cosa?

RESPONSABILITÀ
Nessun owner responsabile delle azioni dell'AI

ACCOUNTABILITY
Impossibile risalire a chi ha autorizzato, usato o deciso

SUPERVISIONE
Assenza di controllo e supervisione continua

RISCHIO REALE: delega inconsapevole di decisioni critiche, data leakage, bias, violazioni normative, danni reputazionali.

LA SOLUZIONE: UN APPROCCIO DUPLICE

1. APPROCCIO PREVENTIVO

Definire regole prima dell'uso

- **Assegnazione di ruoli e permessi**
  Ogni utente può usare l'AI secondo il proprio ruolo
- **Policy di utilizzo chiare**
  Cosa è consentito, cosa no, con quali dati
- **Controlli e guardrail automatici**
  Filtri, blocchi, limitazioni in base al contesto
- **Valutazione del rischio e classificazione**
  Dati, modelli e casi d'uso sotto controllo

2. APPROCCIO DI ACCOUNTABILITY

Tracciare e rispondere dopo l'uso

- **Tracciabilità completa delle interazioni**
  Chi ha usato quale AI, quando, con quali input
- **Logging e audit immutabili**
  Ogni azione è registrata e verificabile
- **Attribution e responsabilità**
  Individuazione del responsabile in caso di errore o abuso
- **Monitoraggio continuo e alerting**
  Rilevazione di comportamenti anomali o rischiosi

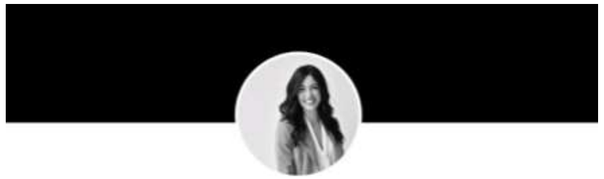
USO SICURO E CONSAPEVOLE dell'AI in azienda
PROTEZIONE DEL DATO e della reputazione
CONFORMITÀ NORMATIVA e riduzione del rischio legale
INNOVAZIONE SOSTENIBILE con controllo e fiducia

Q&A

Contatti:

Christian Persurich, PhD
bitCorp CEO

https://www.linkedin.com/in/christianpersurich



Nancy Laurenda
Product & Corporate Deployment Engineer
presso bitCorp - Secured by Professional...

https://www.linkedin.com/in/nancylaurenda

Antonio Glorioso
Sales System Engineer
Bludis

https://www.linkedin.com/in/antonio-glorioso-a77465278/

Vi aspettiamo al nostro Stand!