SECURITY SUMMIT

Security Summit

Napoli 28 maggio 2026

Clusit

ASTREA

Sovranità digitale e prossimità Made in Italy

per gestire il rischio cyber nel 2026

Luca Bonora | CYBEROO

CYBEROO

Luca Bonora

Cybersecurity Evangelist
CYBEROO

Michele Onorato

Membro Comitato Scientifico
CLUSIT

Clusit

SECURITY SUMMIT

ASTREA

Sovranità digitale europea

- Riguarda la **capacità di agire autonomamente** e di **scegliere soluzioni proprie**, mantenendo la **collaborazione internazionale** quando possibile.
- Non equivale a protezionismo o isolamento, ma a **un'azione indipendente** basata sul diritto internazionale, sui propri valori e interessi di sicurezza, favorendo la cooperazione con partner che condividono i valori europei.
- Include la **regolamentazione di infrastrutture, dati e tecnologie**, garantendo che **dati sensibili siano protetti** da interferenze esterne e leggi extraeuropee.

Sovranità digitale europea

- La **sovranità dei dati** è centrale: proteggere i dati sensibili da interferenze esterne, sviluppare strumenti come l'European Digital Identity Wallet e sistemi di dati condivisi.
- 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.

Ruolo Internazionale e Governance

- L’Europa e l’Italia devono assumere un **ruolo attivo nel plasmare politiche globali**, promuovendo infrastrutture sicure, tecnologie emergenti, resilienza delle supply chain, standard digitali e competenze.
- È necessaria una **governance efficace**, integrando strutture esistenti, per garantire trasparenza, inclusività e decisioni condivise tra pubblico, privato, società civile e accademia.
- **Investimenti in educazione, ricerca, competenze digitali e alfabetizzazione** sono fondamentali per rafforzare la **resilienza** e la **competitività europea**.

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.

Puntiamo sull’Italia

Clusit

SECURITY SUMMIT

ASTREA

WE ARE

L'INTERO MAGGIORE DELLA SOMMA DELLE SUE PARTI
Il nostro servizio va oltre le tecnologie eterogenee.

QUOTAZIONE DA RECORD
L'azienda è 1° vendor di cybersecurity quotato in Borsa Italiana.

LA BOUTIQUE DELLA CYBERSECURITY
Cyberoo coniuga tecnologie avanzate e i migliori specialist sul mercato.

RISORSE EUROPEE, CLIENTI INTERNAZIONALI
Siamo italiani in Italia, con un presidio costante e un approccio internazionale.

CYB
EURONEXT
GROWTH

TI

SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI
DNV
ISO/IEC 27001

Sovranità digitale è un concetto vuoto se non lo adatti alla tua struttura produttiva.

Autonomia strategica europea

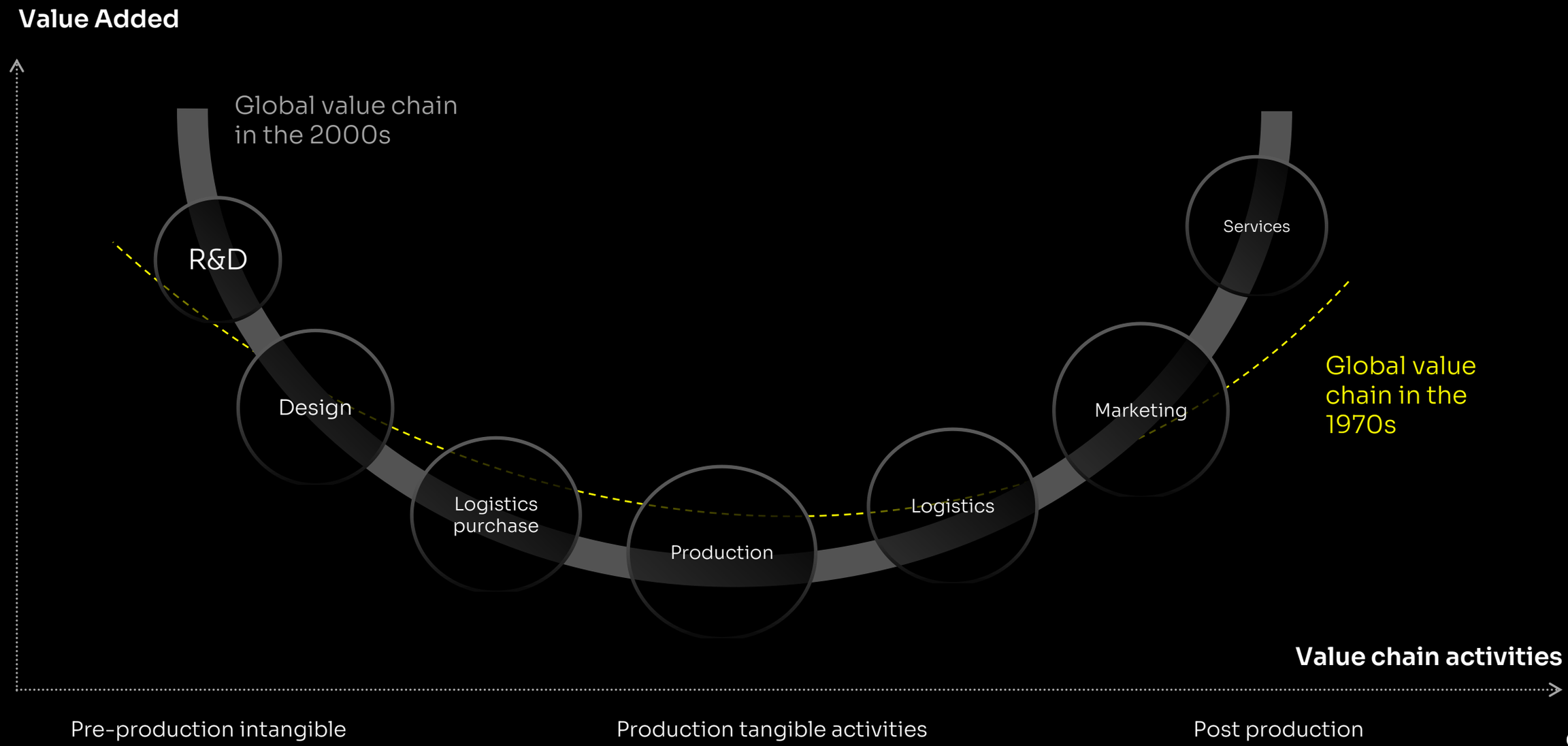
La capacità di un Paese di restare competitivo nel tempo passa attraverso la continua evoluzione delle sue imprese

L’impulso della normativa Europa

Governare il cambiamento:
da efficienza a sicurezza

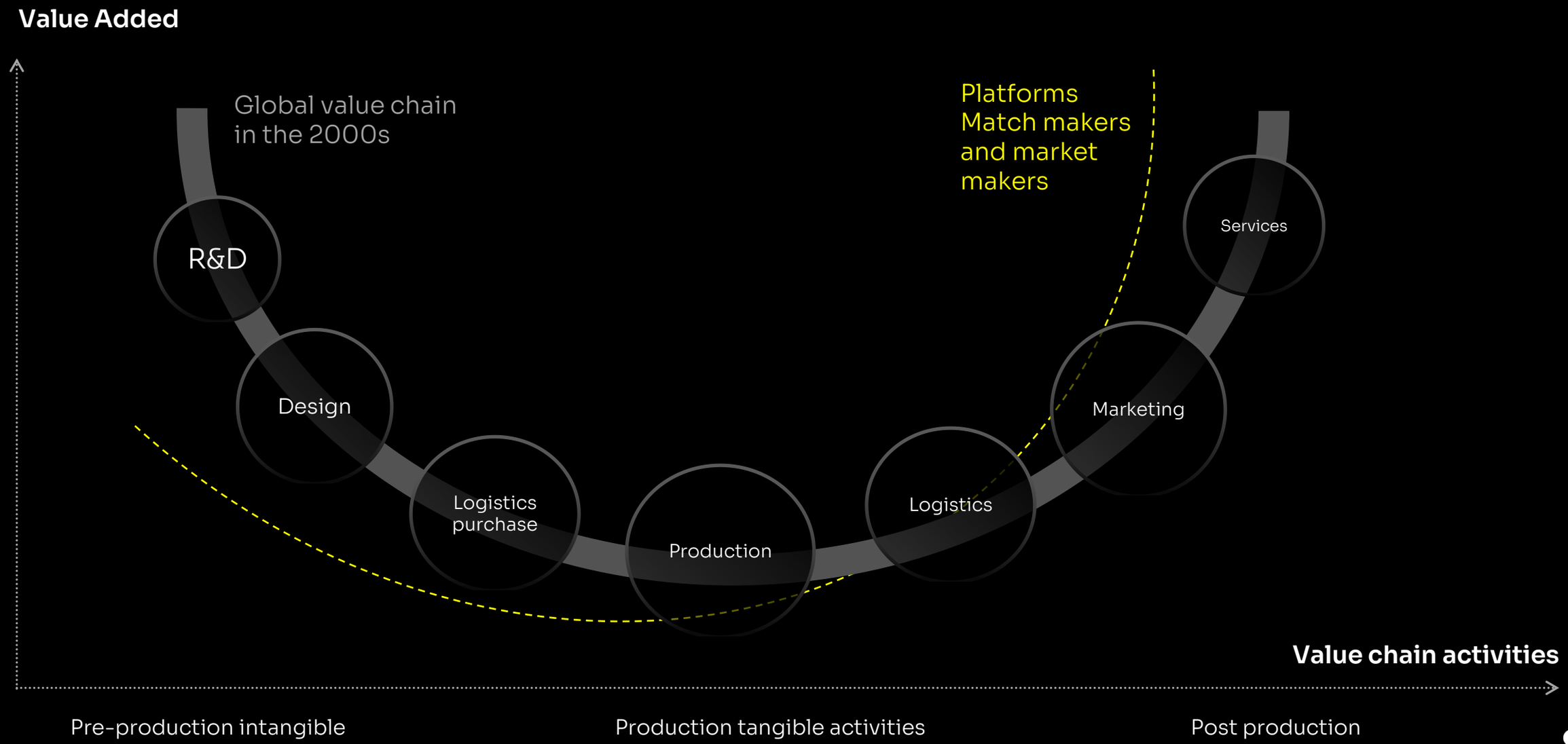
Source: Chu, H. et al. (2026). From smile curve to wicked smile? Regional Studies, 60(1).

La smiling curve in passato



Source: Chu, H. et al. (2026). From smile curve to wicked smile? Regional Studies, 60(1).

La smiling curve oggi



Sovranità digitale

Conoscenza

Made in Italy digitale

Prossimità

Continuità operativa

Indipendenza

Governance

Prossimità e Made in Italy

Presidio costante

Supporto vicino e rapido

Stessa lingua, stesso contesto

La **sovranità digitale**
non è un tema tecnologico,
è una **scelta di responsabilità**.

La sovranità digitale è un elemento
che si lega al rischio cyber.
Come approcciarlo?

“

L'essenza della strategia
è scegliere cosa non fare

MICHAEL PORTER

Gestione del rischio

Definire cosa **proteggere** davvero,
perché e con quale **priorità.**

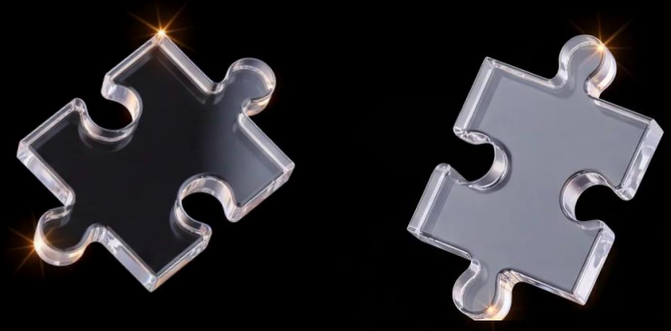
Stai investendo dove serve
davvero per ridurre **il rischio**?

Conoscere il rischio per ridurlo

the Rumsfeld Matrix

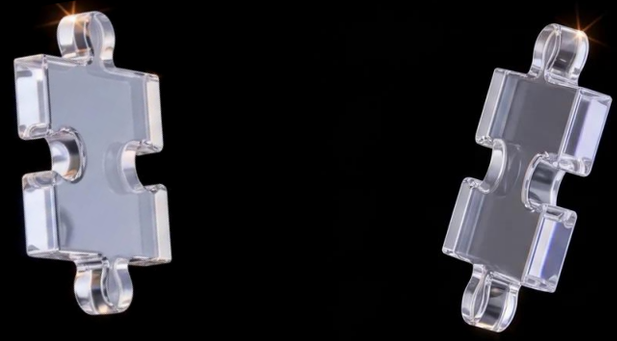
Gli elementi del rischio 2026

Sovranità digitale



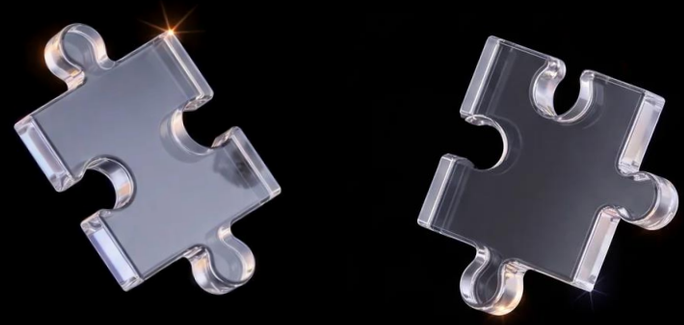
Industrial OT

IT systems



Intelligenza artificiale

Supply chain



Persone e awareness

Operational Technology

L’OT non lascia margine di errori:
una debolezza può generare
impatti fisici, fermi produttivi
e recovery complesse.

Tre pillar fondamentali

Asset Discovery

OT Monitoring

Vulnerability Assessement

Roadmap di implementazione

- Comprendere gli interlocutori
- Segmentazione reti
- Modello Purdue 3.0
- Monitoraggio avanzato
- Aggiornamento firmware continuo

Regolamentazione

Cyber Resilience Act

Regolamento Macchine

Attacchi e agenti AI

La minaccia non è solo l’AI che **potenzia** gli attacchi, ma anche gli agenti che operano in **autonomia**.

Agenti AI
investimento corretto

Esterno

AI anche nella difesa

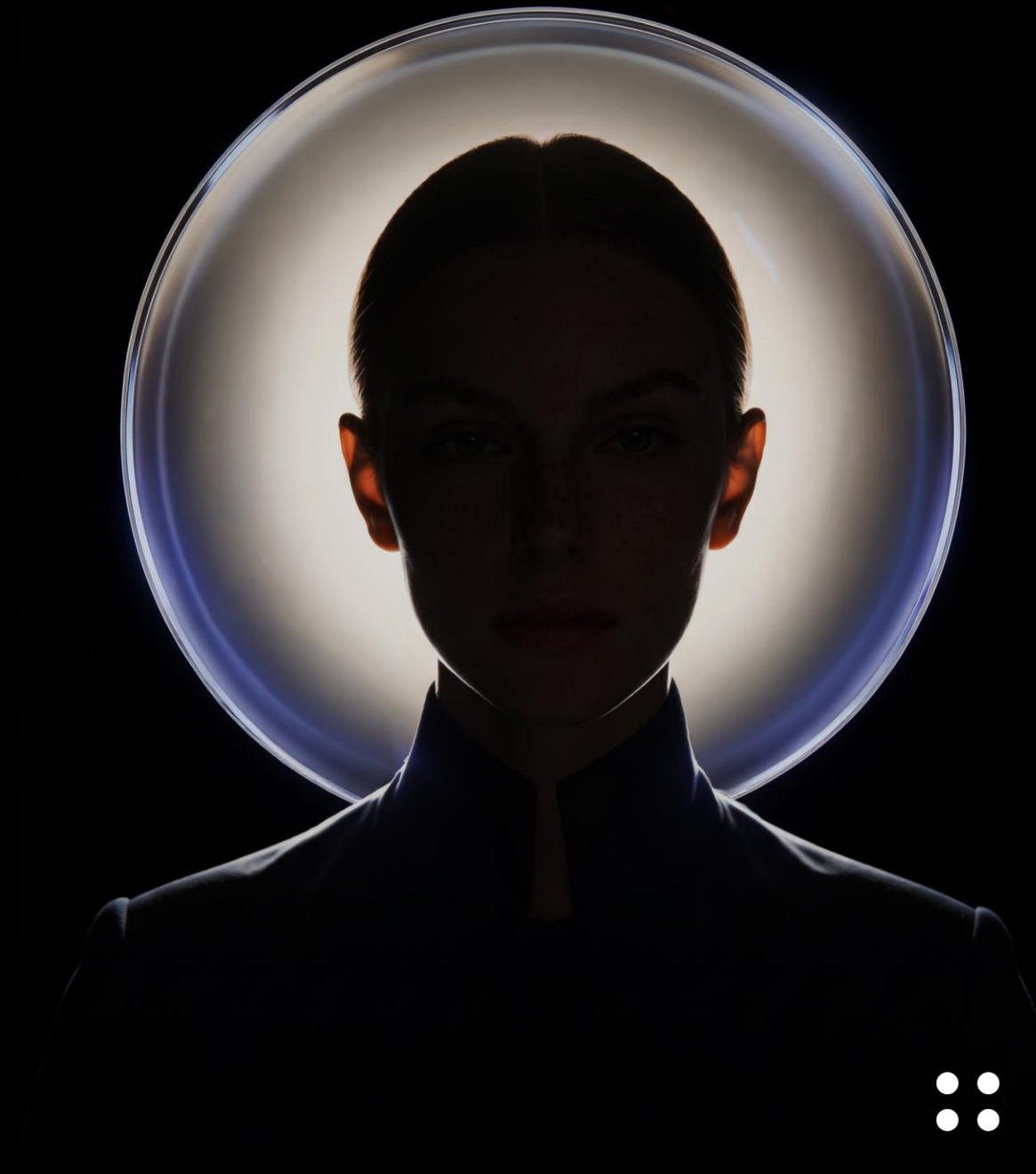
CYPEER **AI-driven**

Interno

- Human-in-the-loop
- Adozione framework UE
- Regolamenti e policy AI interne
- Agenti AI come identità
- Test di robustness e human oversight
- Wrapper AI

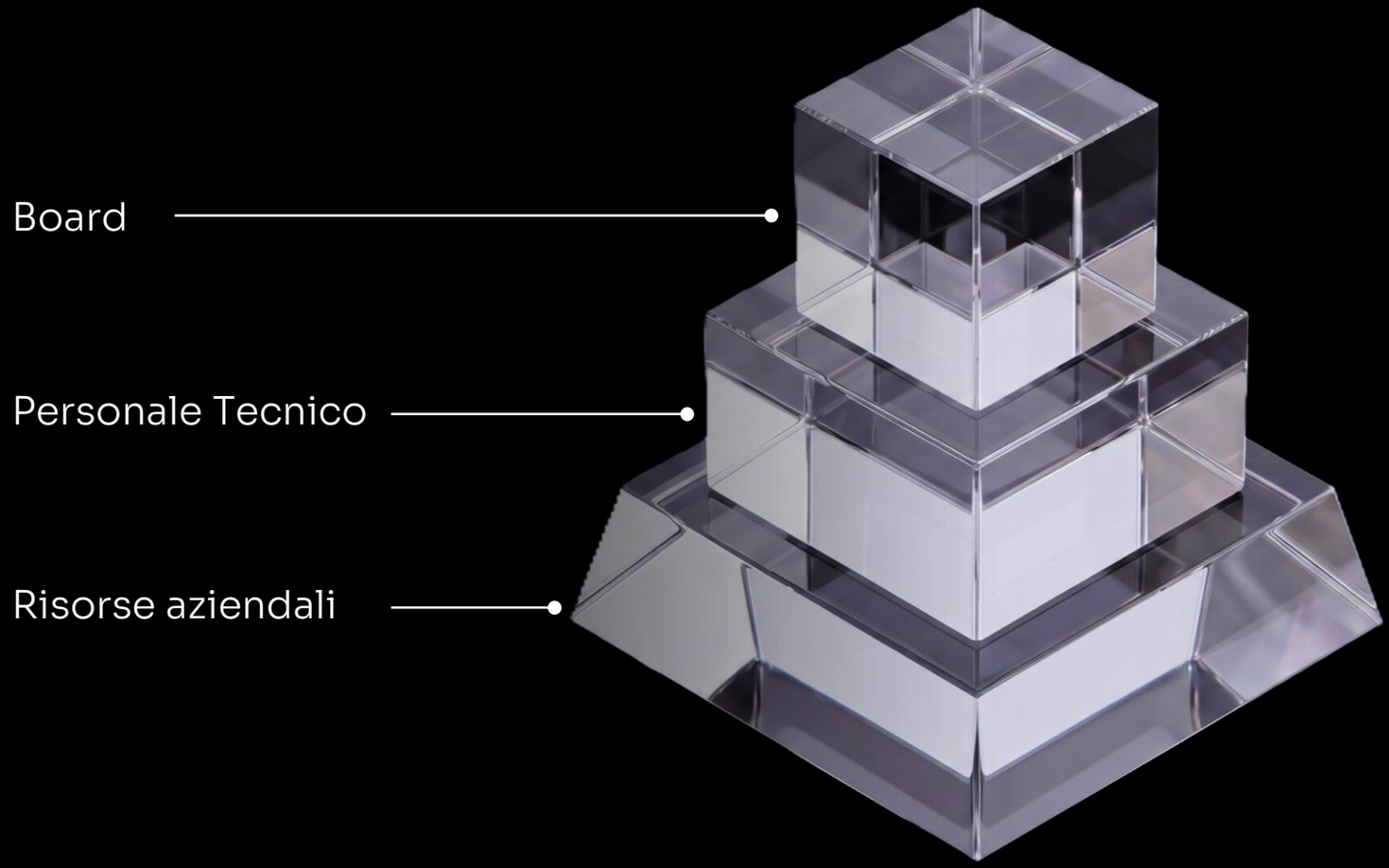
Persone e awareness

Il **rischio** non è l’utente, ma **comportamenti** non allenati: sotto pressione il cervello semplifica, si affida e sbaglia.



KEATRIX

Un cambio **radicale** verso il training del **comportamento**

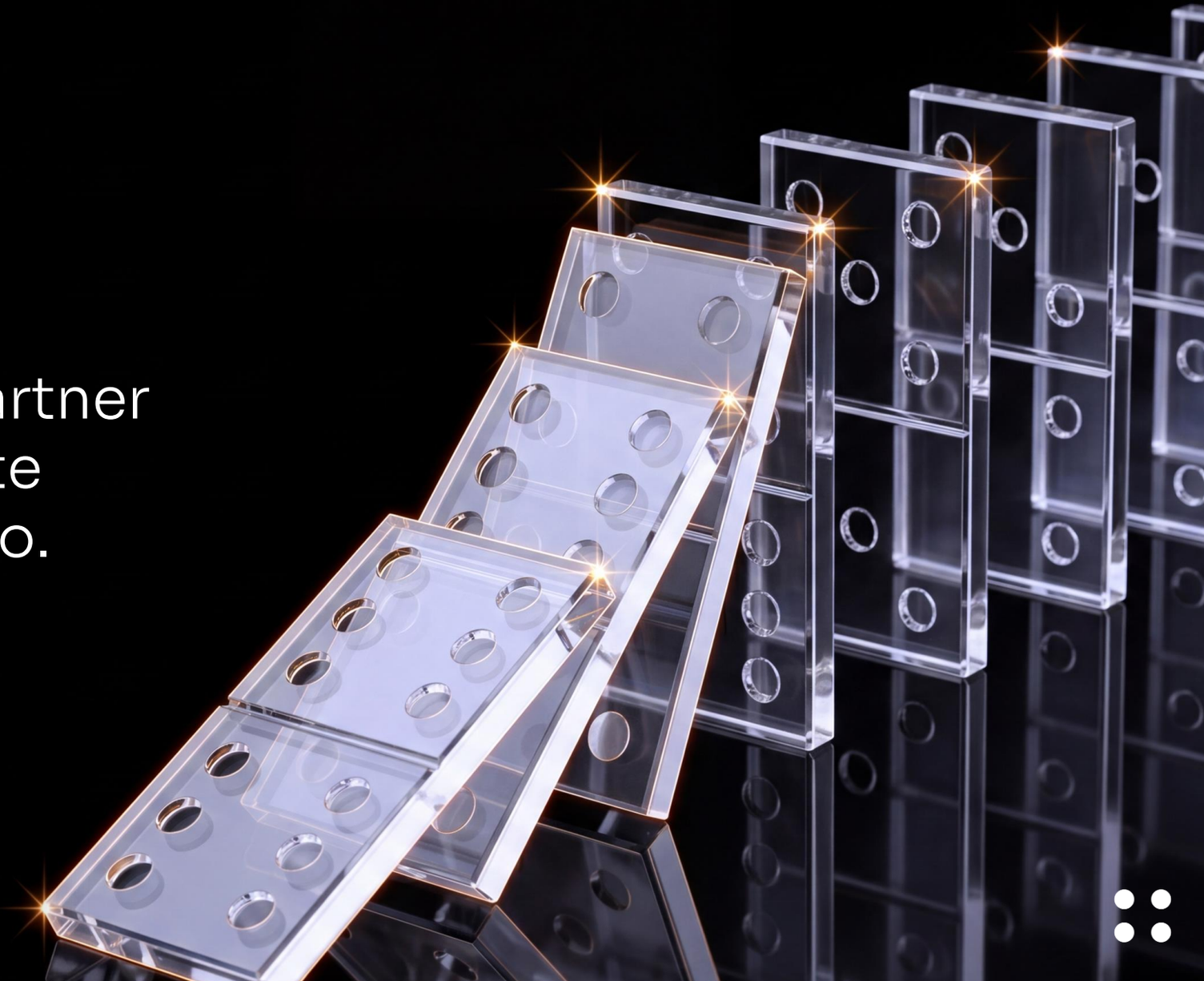


Compliance NIS2

- Formazione continua
- Audit e registri
- Responsabilità NIS2
- Sanzioni
- Behavioral Security

Supply chain

La **vulnerabilità** di un partner diventa immediatamente la tua: è **rischio** ereditato.




+2.700 CVE
univoche individuate
nel 2025 sui
fornitori monitorati

Roadmap di implementazione

- Mappatura della supply chain
- Richiesta SBOM
- Diversificazione dei fornitori
- Monitoraggio delle vulnerabilità
- Contratti con gestione del rischio e penali

Sistemi IT

Infrastrutture, sicurezza e continuità operativa dipendono dall’efficienza dei sistemi IT.

Nuove sfide per l’IT

Complessità crescente degli ambienti

Superficie di attacco in espansione

Carenza di tempo e risorse

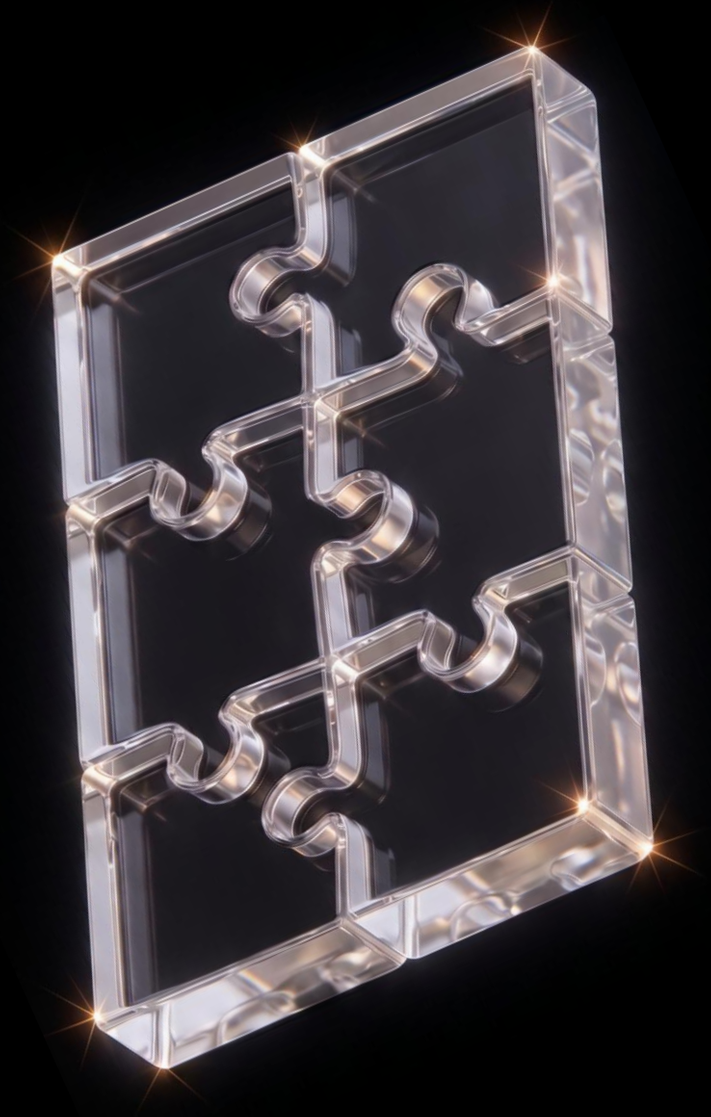
Attacchi sempre più veloci

Ridurre il rischio 2026

Autonomia e indipendenza europea

Governare l’IT in modo unificato

Trasparenze e audit di terze parti



Isolamento e controllo

Agenti e regolamenti interni e definiti

Training sui comportamenti

Oggi **non vince** chi aggiunge strati,
ma chi sa ricomporre il puzzle del **rischio**
riducendo davvero l’esposizione.

OSSERVATORIO 2026

SCARICALO ORA.


It’s your turn.
Q&A

CONTACT US

Cyberoo S.p.A.
Via Brigata Reggio, 37
42124 Reggio Emilia

Tel. 0522.388111

Mail: info@cyberoo.com

Web: www.cyberoo.com

LinkedIn: CYBEROO

YouTube: CYBEROO

X: CYBEROO

Instagram:
@cyberoo_official