SECURITY SUMMIT

Security Summit

Milano 17-18-19 marzo 2026

Clusit

ASTREA

Il puzzle del rischio 2026:

tra sovranità digitale, agenti AI, supply chain e OT, cosa conta davvero

Luca Bonora | CYBEROO

CYBEROO

Luca Bonora

CYBERSECURITY EVANGELIST

Nel 2026 la vera domanda non è se saremo colpiti, ma se **abbiamo davvero capito da cosa dipende oggi il rischio informatico.**

Stiamo davvero investendo dove serve **o ci stiamo illudendo di una sicurezza che non riduce il rischio reale?**

In questo incontro ricostruiamo il **puzzle** del rischio cyber 2026, mostrando con **esempi concreti** dove nasce davvero **l'esposizione**, quali **segnali** anticipano un **incidente** e perché dovresti evitare di mettere il budget nel posto sbagliato.

“

L'essenza della strategia è scegliere cosa non fare

Michael Porter

Gestione del rischio

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

Rischio = Probabilità × Impatto

Minacce

Vulnerabilità

Capacità di risposta

L’obiettivo non è zero attacchi, ma zero incidenti gravi.

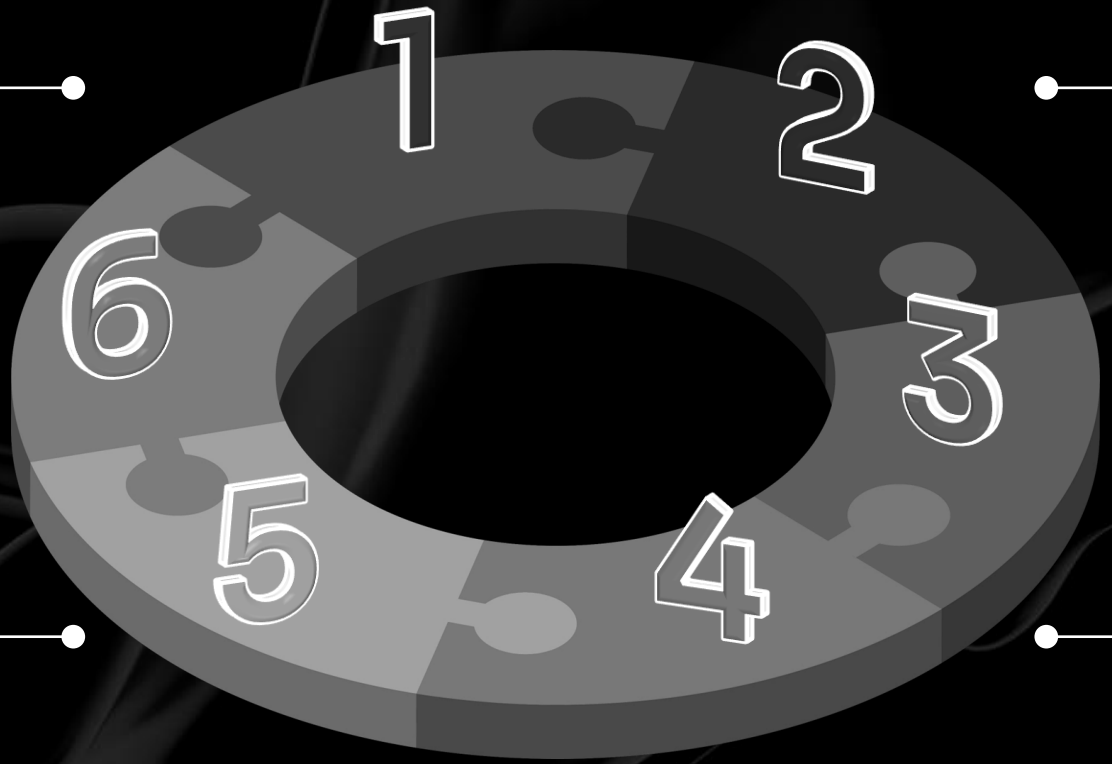
Stai investendo
davvero dove serve
per ridurre **il rischio**?

Conoscere il rischio per ridurlo: the Rumsfeld Matrix

	Known	**Unknown**
Known	Rischi e informazioni già identificati e misurabili	Rischi riconosciuti ma non ancora quantificati
Unknown	Informazioni disponibili ma non utilizzate nei processi decisionali	Rischi fuori dal modello mentale o dal perimetro di osservazione

Gli elementi del rischio 2026

1. Sovranità digitale
2. Intelligenza Artificiale
3. Persone e awareness
4. Industrial OT
5. Supply Chain
6. Consumo Energetico



1

Sovranità digitale

Il vero rischio è perdere il controllo operativo di identità, dati e servizi, anche in cloud.

2

Agenti e attacchi AI

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

3

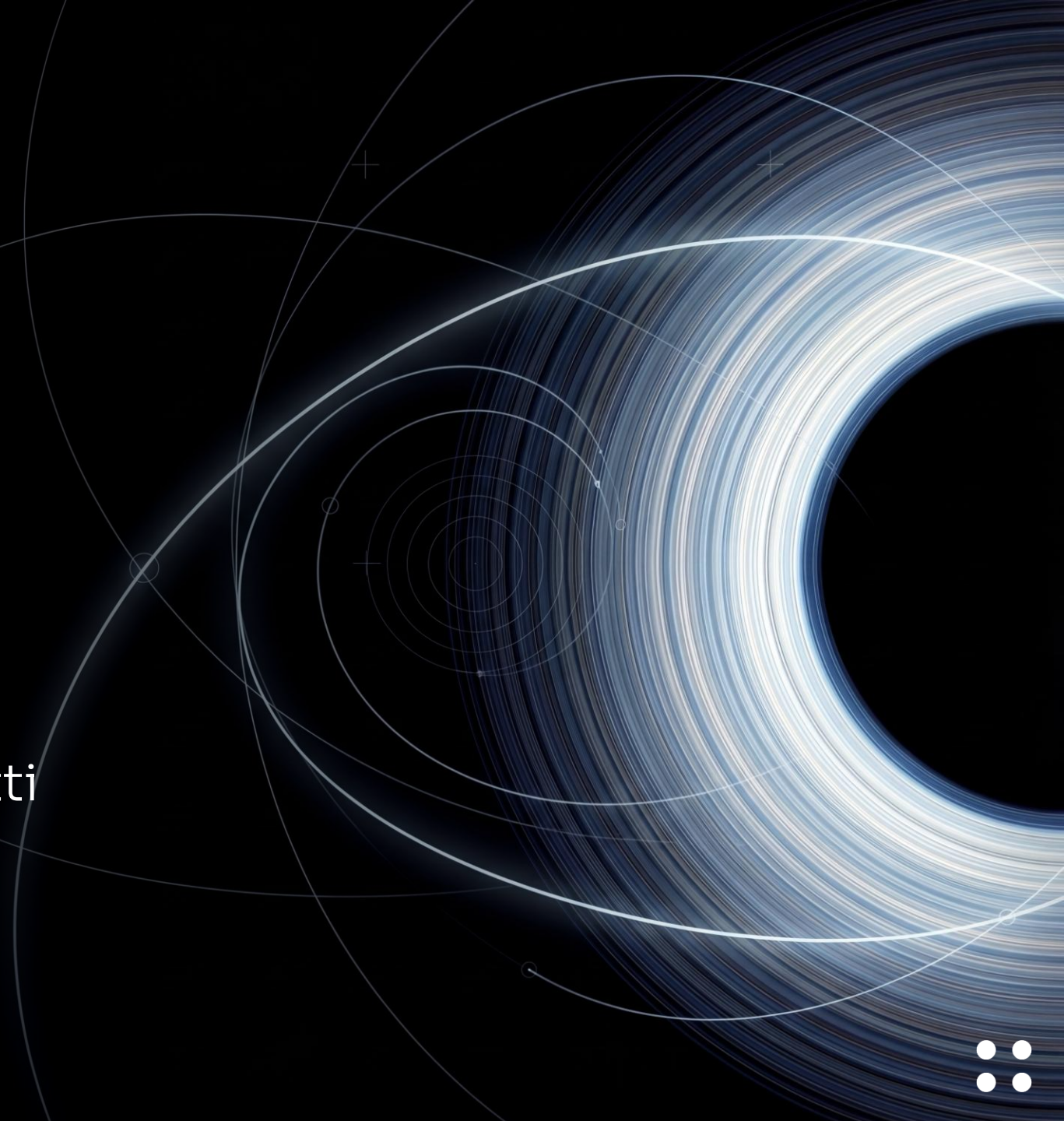
Persone e awareness

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

4

Industrial OT

L’OT non ha margini: una debolezza può generare impatti fisici, fermi produttivi e recovery complesse.



5

Supply chain

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

+2.700 CVE univoche individuate
nel 2025 sui **fornitori** monitorati.

CYBEROO

6

Consumo energetico

Più potenza digitale richiede più energia: il rischio è restare senza capacità quando serve.

Obblighi normativi 2026

2 AGO 2026

AI Act
Sistemi ad alto rischio
Obbligo requisiti e trasparenza.

11 SET 2026

Cyber Resilience Act
Notifica vulnerabilità
Entro 24h, anche su prodotti esistenti.

31 OTT 2026

Direttiva NIS2
Misure di sicurezza minime
Governance, risk management e controlli.

2026

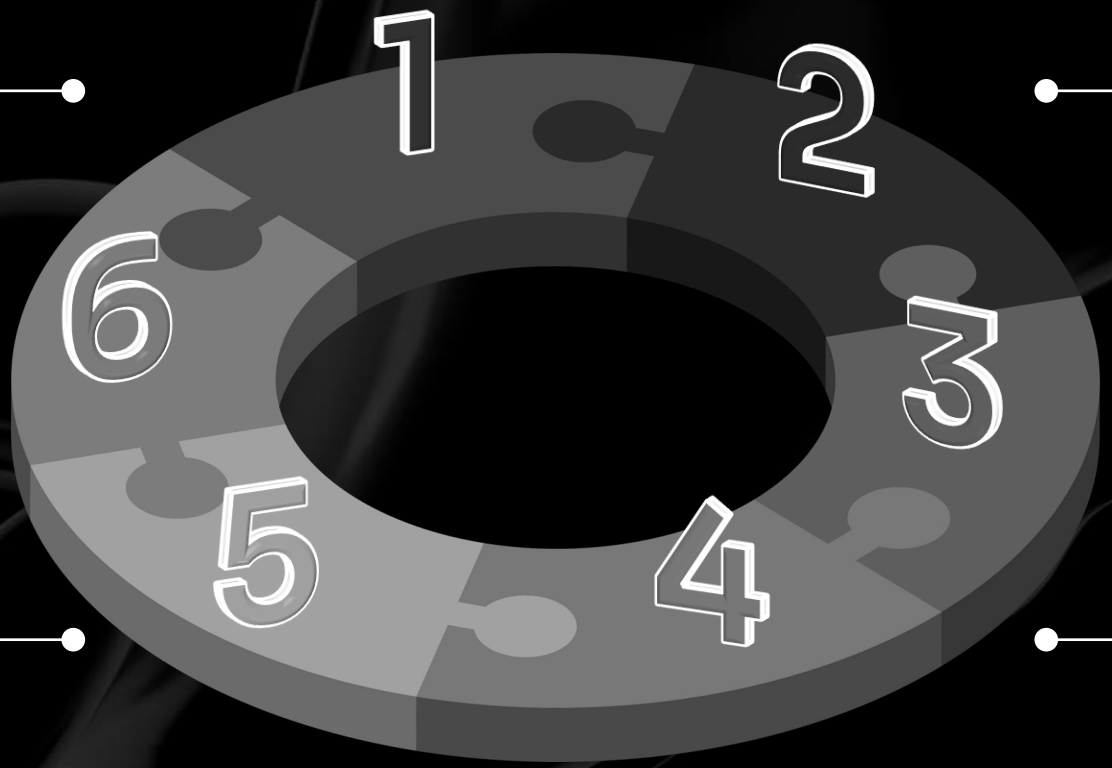
Regolamento DORA
Testing e controlli ICT
Ai fornitori critici e reporting rafforzato.

Ridurre il rischio 2026

Autonomia e indipendenza europea

Ottimizzazione consumi digitali

Trasparenze e audit di terze parti



Agenti e regolamenti interni e definiti

Training sui comportamenti di sicurezza

Isolamento e controllo

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