SECURITY SUMMIT

Security Summit

Roma 23 giugno 2026

Clusit

ASTREA

OLTRE LA TECNOLOGIA

Governare il rischio Cyber nell'era della complessità.

Luca Benatti| CYBEROO

CYBEROO

RELATORE

Luca Benatti

PRODUCT MANAGER

TITAAN & CYBER SECURITY SUITE

Clusit

SECURITY SUMMIT

ASTREA

CYBEROO

GESTIONE DEL RISCHIO

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

CYBEROO

L'essenza della strategia
è scegliere **cosa non fare**.

MICHAEL PORTER

CYBEROO

GESTIONE DEL RISCHIO

In ambito cyber, la **gestione del rischio** è il processo sistemico per: **identificare, valutare, trattare e monitorare** i rischi che possono compromettere **confidenzialità, integrità e disponibilità** delle informazioni.

CYBEROO

LA MATEMATICA DEL RISCHIO

Probabilità × Impatto = **Rischio**

MINACCE

RISPOSTA

VULNERABILITÀ

L'OBIETTIVO NON È ZERO ATTACCHI,
MA ZERO INCIDENTI GRAVI.

CYBEROO

SOLUTION SPRAWL

83 STRUMENTI DI IT

29 VENDOR DIVERSI

52%

Degli executive considera la complessità il principale problema cyber

45%

Ritiene di non avere skill interne sufficienti per la cyber security

+84

Giorni di containment in stack frammentato

Il rischio cyber risente direttamente del numero di **strumenti** e **vendor** coinvolti.

Fonte: IBM, 2025 · Eurobarometer, European Commission, 2024

CYBEROO

QUANDO L'AZIENDA CRESCE

Il rischio cyber diventa ancora più complesso da gestire quando la complessità dell'azienda aumenta.

CYBEROO

LA COMPLESSITÀ HA UN COSTO

La **gestione della complessità assorbe risorse** dedicate alla riduzione del rischio.

CYBEROO

Cybersecurity tradizionale

- CENTRATA SUGLI STRUMENTI
- CENTRATA SULLA DETECTION
- GUIDATA DALLA TECNOLOGIA
- REATTIVA
- FRAMMENTATA

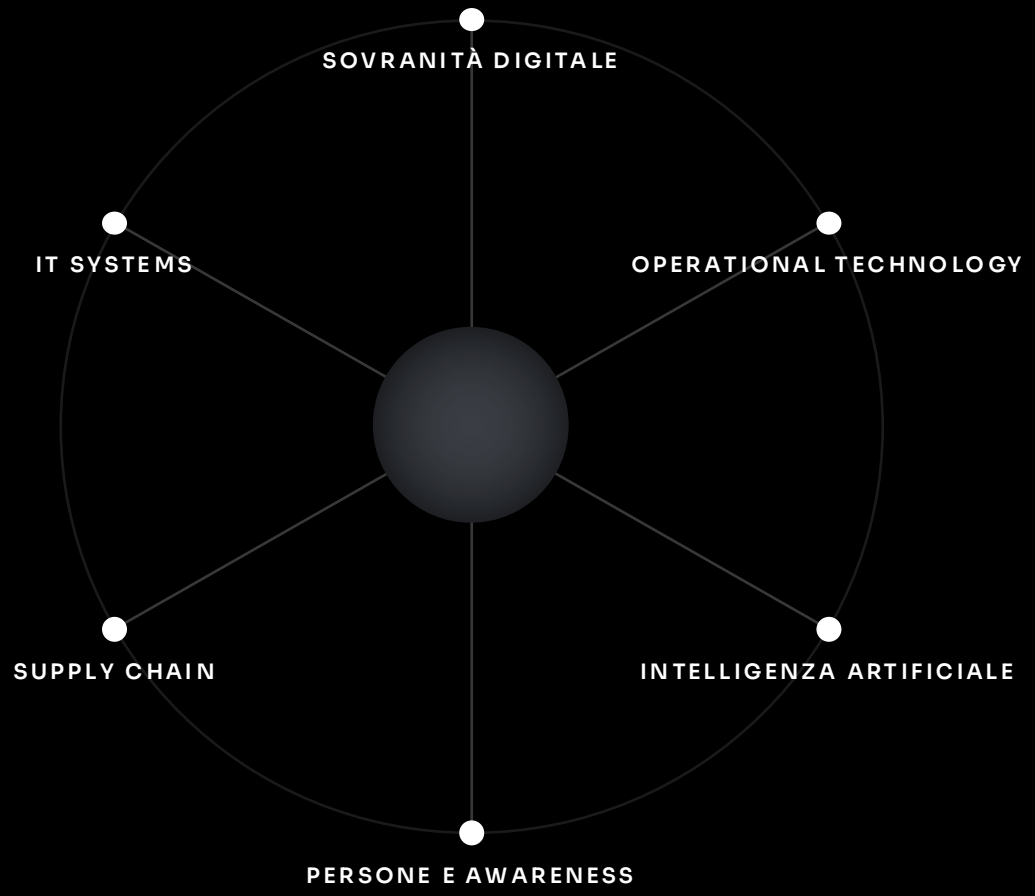
Gestione del rischio

- CENTRATA SUL BUSINESS
- OPERATIVA
- CONTINUA
- INTEGRATA
- ORIENTATA AI RISULTATI

CYBEROO

2026

Gli elementi del rischio



CYBEROO

1. SOVRANITÀ DIGITALE

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

CYBEROO

UNA SCELTA STRATEGICA

Non è isolamento, è controllo consapevole del rischio

ADOTTARE CLOUD SOVRANI

POLITICHE DI DATA LOCALIZATION

INDIPENDENZA

COMPETITIVITÀ

INNOVAZIONE

CYBEROO

2. OPERATIONAL TECHNOLOGY

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

CYBEROO

Tre pillar fondamentali

1. ASSET DISCOVERY
2. OT MONITORING
3. VULNERABILITY ASSESSMENT

CYBEROO

- COMPRENDERE GLI INTERLOCUTORI
- CISO COME PONTE TRA IT & OT
- COLLABORAZIONE ATTIVA CON I VENDOR
- ADOZIONE ZERO TRUST
- SEGMENTAZIONE RETI
- AGGIORNAMENTO FIRMWARE CONTINUO
- MONITORAGGIO AVANZATO

CYBEROO

Regolamentazione

1. CYBER RESILIENCE ACT
2. REGOLAMENTO MACCHINE

CYBEROO

03. ATTACCHI E AGENTI AI

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

CYBEROO

INVESTIMENTO CORRETTO

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

Esterno

- AI ANCHE NELLA DIFESA

CYBEROO

04. PERSONE E AWARNESS

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

CYBEROO

PERSONE · BEHAVIORAL SECURITY

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

Compliance NIS2

- FORMAZIONE CONTINUA
- AUDIT E REGISTRI
- RESPONSABILITÀ NIS2
- SANZIONI

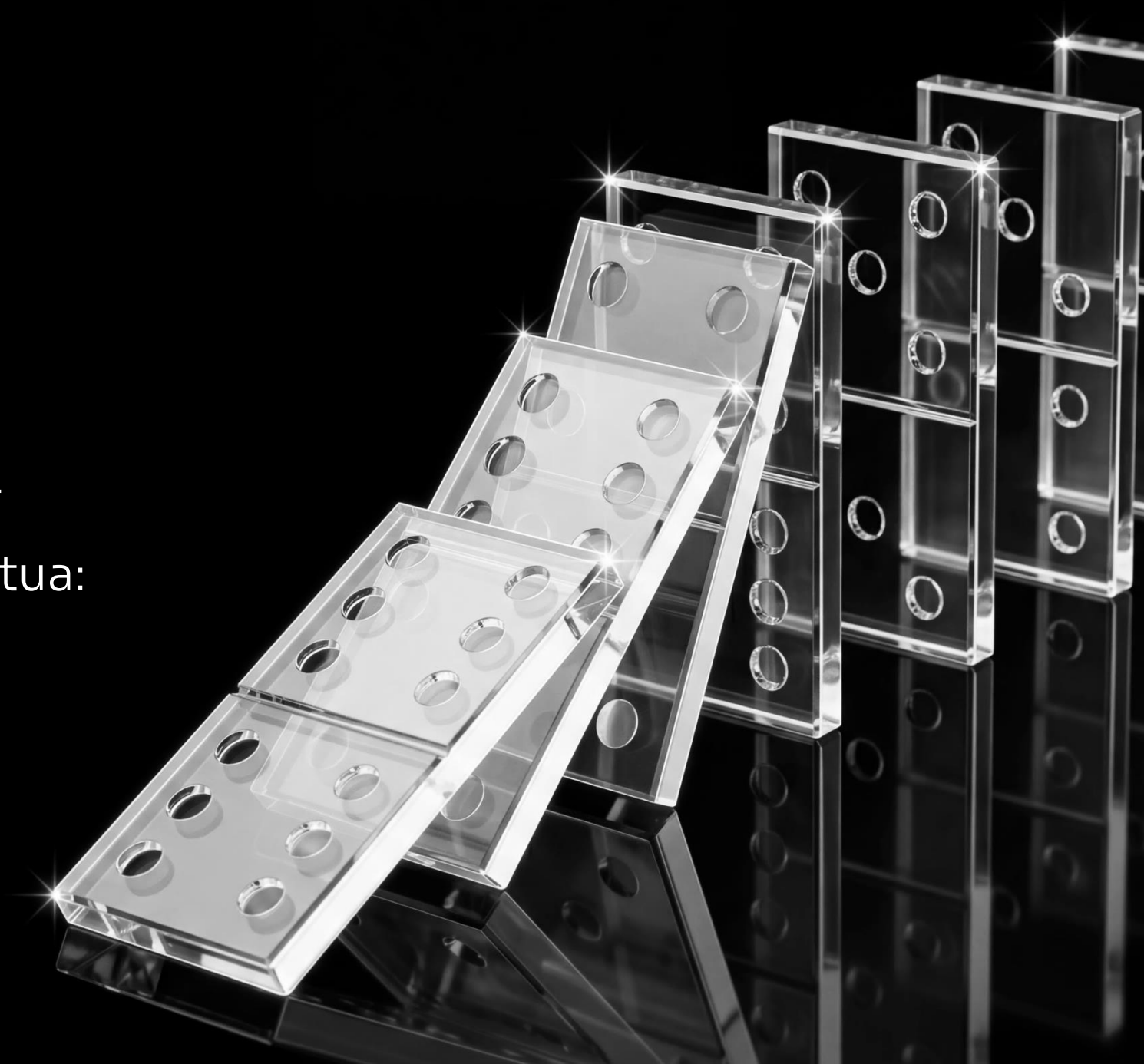
Coinvolge

- BOARD
- PERSONALE TECNICO
- RISORSE AZIENDALI

CYBEROO

05. SUPPLY CHAIN

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



CYBEROO

ROADMAP DI IMPLEMENTAZIONE

- MAPPATURA DELLA SUPPLY CHAIN
- RICHIESTA SBOM
- DIVERSIFICAZIONE DEI FORNITORI
- MONITORAGGIO DELLE VULNERABILITÀ
- VISIBILITÀ CONTINUA SULLA SUPPLY CHAIN
- CONTRATTI CON GESTIONE DEL RISCHIO E PENALI

CYBEROO

06. SISTEMI IT

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

CYBEROO

NUOVE SFIDE PER L'IT

COMPLESSITÀ CRESCENTE DEGLI AMBIENTI

CARENZA DI TEMPO E RISORSE

SUPERFICIE DI ATTACCO IN ESPANSIONE

ATTACCHI SEMPRE PIÙ VELOCI

CYBEROO

LA VERA GESTIONE DEL RISCHIO

01

La matematica del rischio

Probabilità × Impatto, amplificata dalla complessità intrinseca.

02

Sei elementi, sei rischi

Ogni elemento fondamentale genera un rischio distinto da gestire.

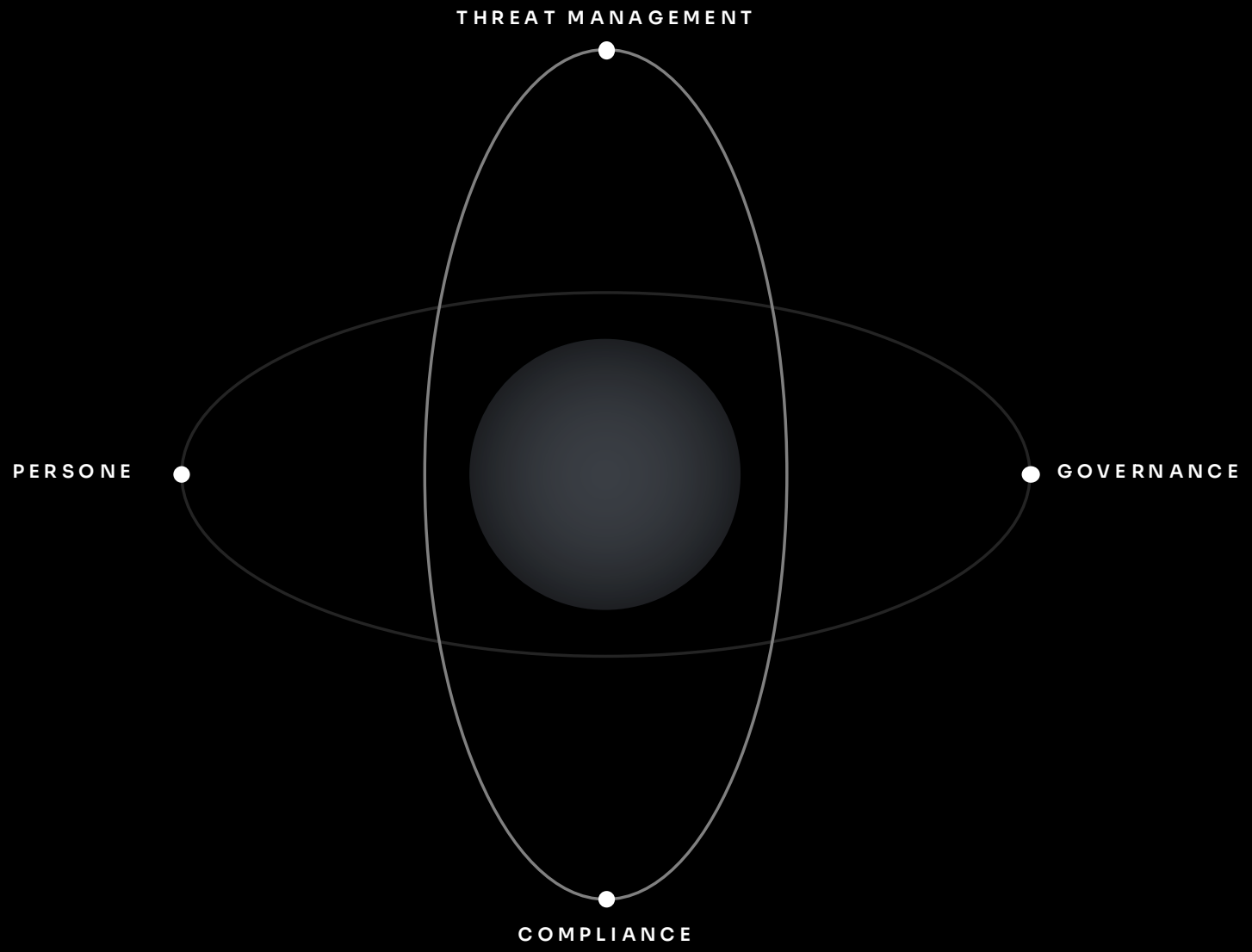
03

Visione sistemica

La risposta non è un altro software, ma una regia d'insieme.

CYBEROO

I 4 pilastri del modello operativo



CYBEROO

NON UN PRODOTTO

NON UNA PIATTAFORMA

NON UN SERVIZIO ISOLATO

MA UN MODELLO OPERATIVO

CYBEROO

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

It’s your turn.

Q&A

CONTATTACI

SITO

www.cyberoo.com

NUMERO VERDE

800 608 086

SOCIAL

LinkedIn · YouTube · Instagram

TELEFONO

0522 388111