Security Summit

Milano 17-18-19 marzo 2026

Sessione

Quando il Cyber diventa Business

Parlare al Board con dati, impatti e simulazioni reali

pikered

Marco Gallina | Managing Director @ Pikered

Diego Lorenzi | Head of Data Science @ Pikered

pikered

Relatori

Marco Gallina
Managing Director @ Pikered

Diego Lorenzi
Head of Data Science @ Pikered

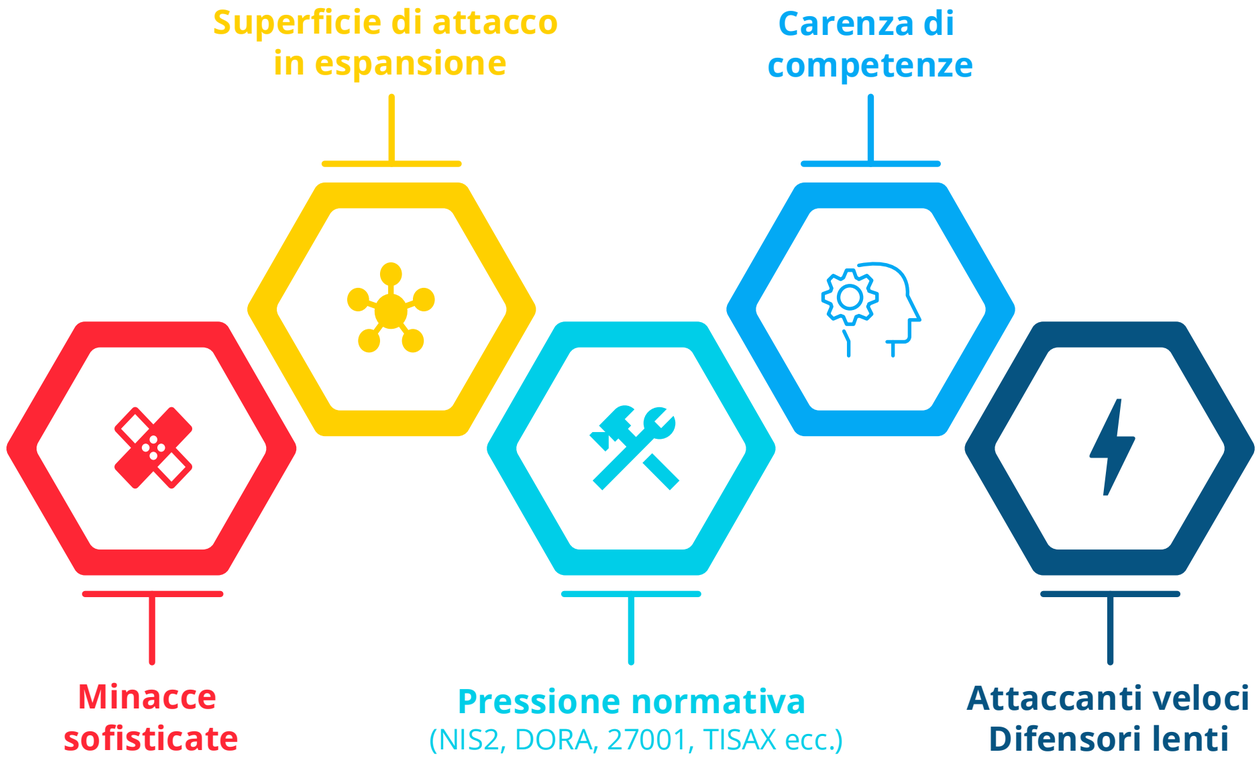
pikered

Ripensare il Cyber Risk nell'era digitale

Il Cyber non è un tema solo IT

... ma di Business Continuity

Il Board vede il Cyber come “tema tecnico”, eppure…



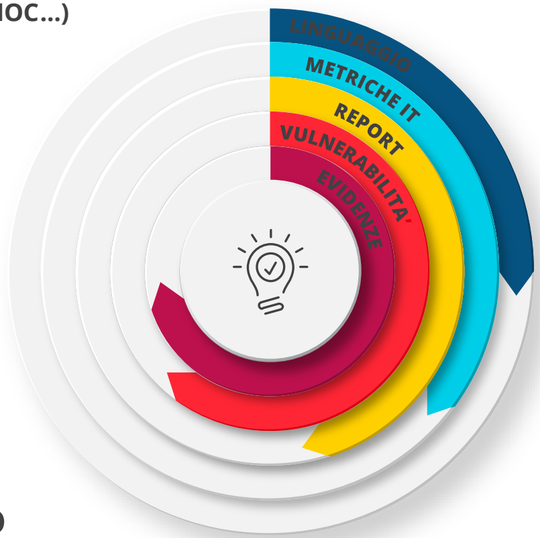
pikered

Perché il Board fatica a comprendere il Cyber Risk?

01 **Linguaggio IT**
(CVSS, CVE, Patch level, IOC...)

02 **Metriche IT non collegate al business**

03 **Report troppo dettagliati**



04 **Vulnerabilità da validare**

05 **Assenza di evidenze misurabili**

Conseguenza: infodemia!

pikered

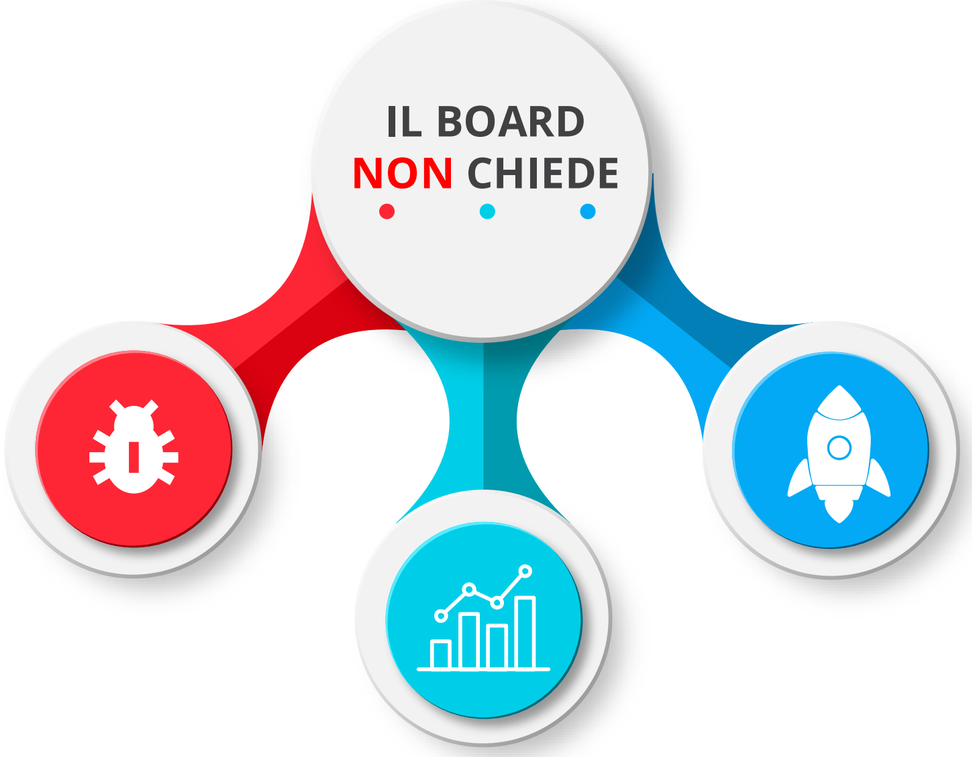
Il Board non finanzia CVSS, piuttosto…

pikered

Le sfide del CISO come «traduttore» strategico

pikered

Cosa non vuole il Board?



Quante vulnerabilità abbiamo?

Quanti alert gestiamo?

Quali Remediations applichiamo?

pikered

Cosa vuole davvero il Board?

Quanto rischio stiamo correndo?

Si conoscono le probabilità in % di subire un attacco?
Si conoscono gli economical di un fermo operativo o di un danno reputazionale?

Quanto ci costerebbe un attacco?

RTO (Recovery Time Objective) e RPO (Recovery Point Objectives) sono noti?
Si conoscono i tempi di ripristino parziali o totali dopo un attacco?

Stiamo investendo nel modo corretto?

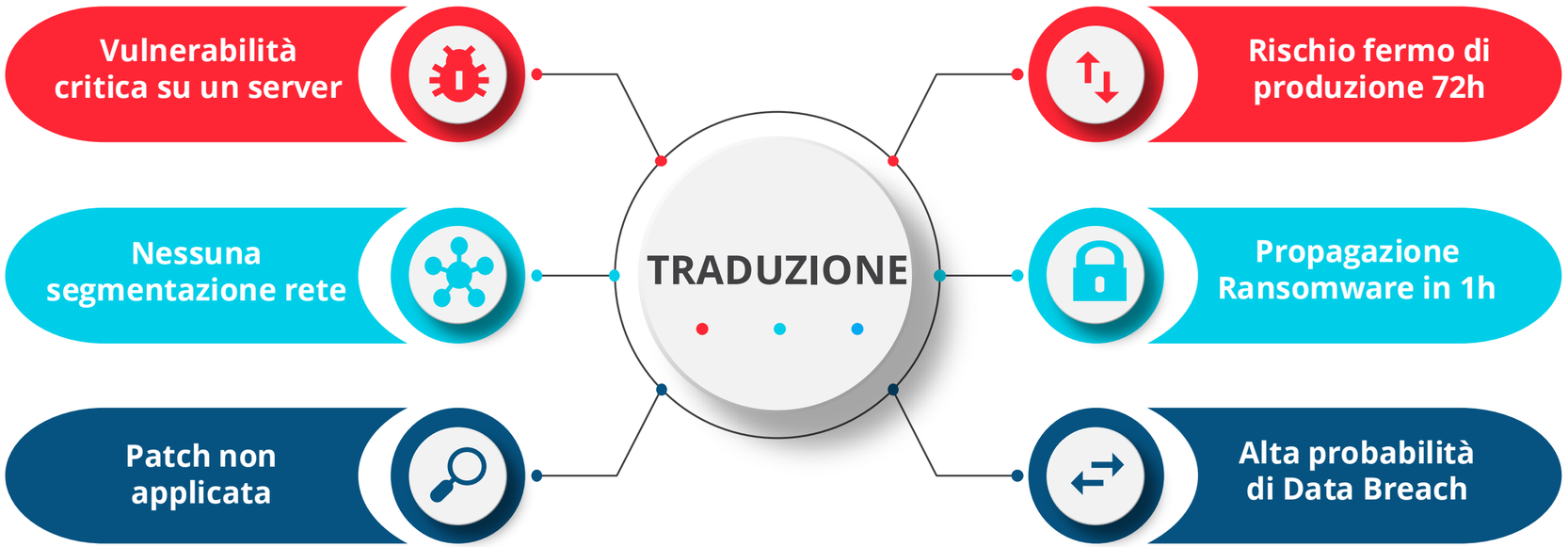
Budget previsionali, Adozione di Tecnologie adeguate,
Adeguare le risorse umane in ambito Cyber (non solo IT)

Siamo compliant?

NIS 2, ISO 27001, ACN (QCx), TISAX, DORA

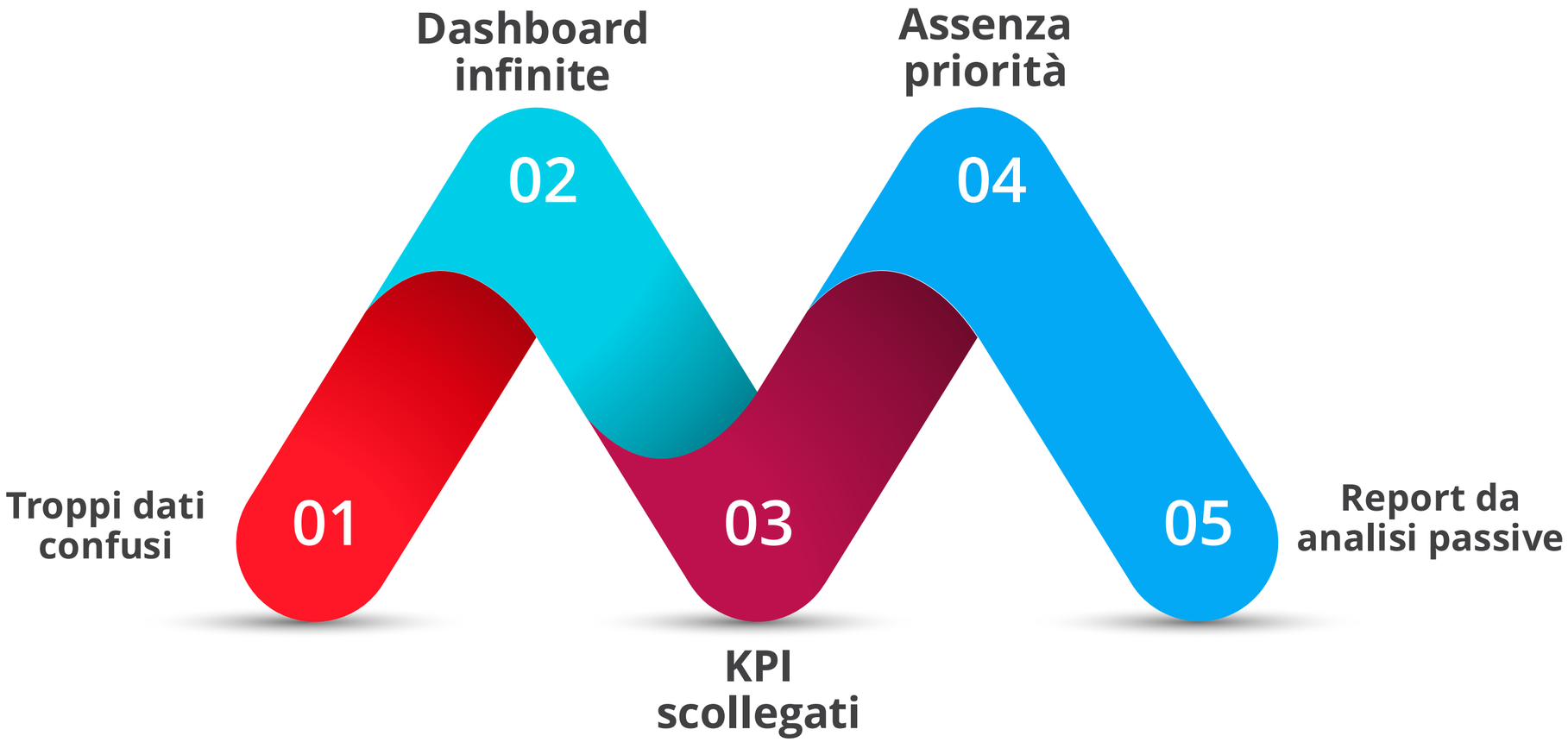
pikered

Traduzioni dal Tecnico al Business



pikered

La Cyber infodemia è:



pikered

La Cyber infodemia provoca:

01 Decisione lente

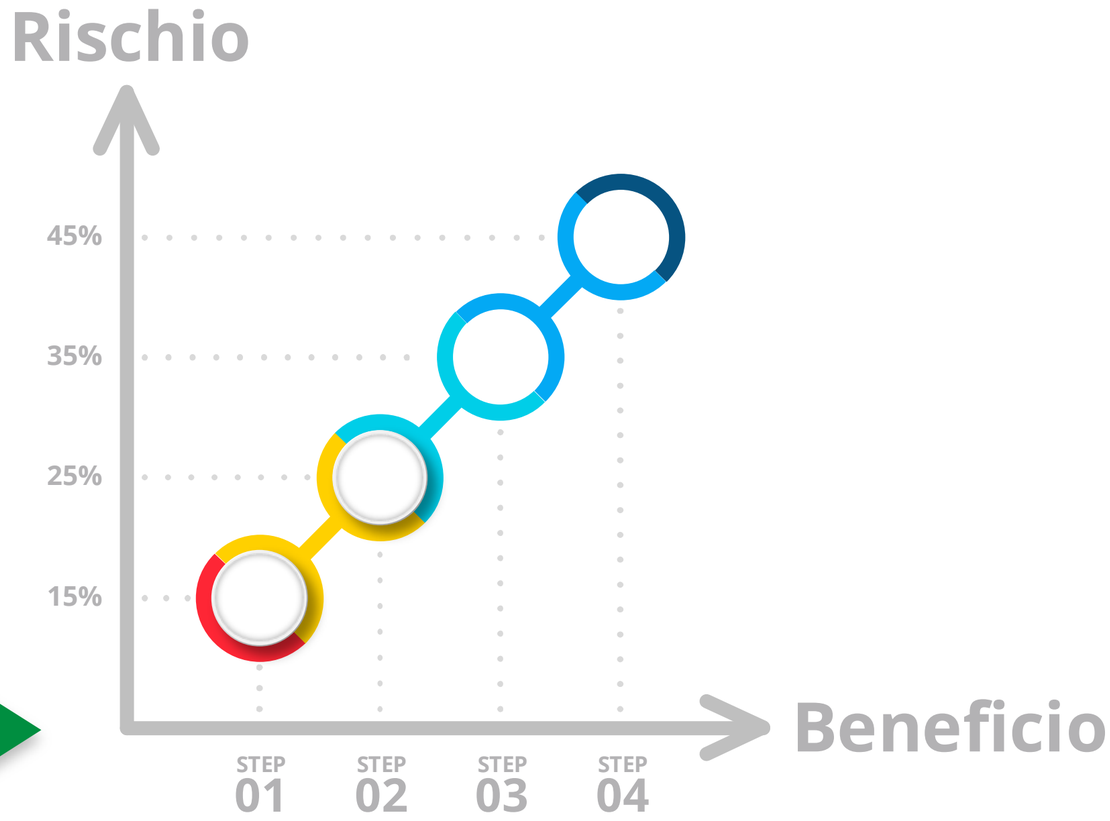
02 Budget mal allocati

03 False sensazioni di sicurezza

pikered

Servono evidenze, non opinioni!

Cosa accadrebbe davvero se un attaccante ci colpisse oggi? Sarebbe utile potersi mettere alla prova, in sicurezza?



La risposta c'è
e si chiama: **AEV**

pikered

Adversarial Exposure Validation (AEV)

Simulazioni realistiche di attacco

Emulazione dei threat actor

Validazione continua delle difese

Misurazione oggettiva dell’esposizione

pikered

Verso una gestione proattiva

Liste di vulnerabilità

Severity teorica

Nessun contesto

Percorsi di attacco

Evidenza dimostrabile

Impatto concreto

pikered

AEV in azione

01. Accesso iniziale realistico

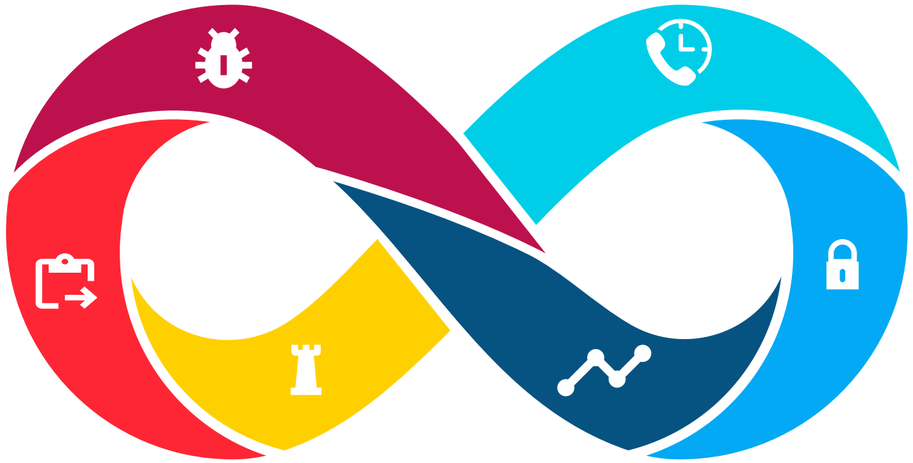
Valuta la capacità di un potenziale attaccante di ottenere un accesso tramite vettori comunemente utilizzati per stabilire connessioni C2.

02. Simulazione di infiltrazione

Ricerca di account ed asset critici, escalation di privilegi, movimenti laterali e compromissione dei Crown Jewels.

03. Simulazione di impatto

Simulazione di cifratura ed esfiltrazione, furto di credenziali, accesso alle e-mail...



04. Validazione di Detection & Response

Misura i tempi di reazione e contenimento del SOC e valida l'efficacia degli EDR/XDR contro tecniche d'attacco moderne.

05. Remediation e Hardening

Migliora i playbook di risposta, risolvi le misconfigurazioni, migliora il logging ed effettua fine-tuning dei prodotti di difesa.

06. Deliverable per i decision maker

Individua i controlli che hanno fallito, i sistemi critici impattati e il tempo impiegato per comprometterli, e stima il potenziale impatto.

pikered

Continuous Threat Exposure Management (CTEM)

01. Scoping

Determina gli asset nello scope e la loro criticità per l'organizzazione.

02. Discovery

Identifica tutte le vulnerabilità (CVE, misconfigurazioni...) nello scope, sia on-premises che in cloud.

03. Prioritization

Valuta i rischi secondo la facilità di sfruttamento e il potenziale impatto, e prioritizza le minacce a cui porre rimedio.

04. Validation

Valuta il reale impatto di potenziali attacchi all'organizzazione, identifica gli elementi critici, e misura l'efficacia di controlli, team e soluzioni di sicurezza.

05. Mobilization

Abilita i team di sicurezza, migliorandone la collaborazione per velocizzare le mitigazioni e rafforzare la protezione.

pikered

AEV come pilastro del CTEM

05. Mobilization

Fornisci ai team di sicurezza una reportistica chiara, una mappatura dei punti ciechi dell'EDR e strumenti facilitati per la creazione di ticket.

04. Validation

Valuta il miglioramento della postura difensiva nel tempo.

01. Scoping

Individua asset nascosti con esposizioni critiche.

02. Discovery

Identifica misconfigurazioni e vulnerabilità più profonde di quelle individuabili da tool che sfruttano scansioni massive o semplice esecuzione di exploit.

03. Prioritization

Riconosci i rischi concreti con una vista istantanea del potenziale impatto.

pikered

La reportistica per il Board deve:

Essere sintetica

Mostrare i trend

Evidenziare i rischi

Quantificare l’impatto economico

Supportare decisioni di investimento

pikered

I deliverable dell'AEV per il Board

05. Stato delle attività

Vulnerabilità critiche residue, priorità di mitigazione, aree di miglioramento

01. Scoring

Punteggi riassuntivi sul livello di protezione delle principali aree.

02. Trend

Andamento del livello di protezione negli ultimi 6/12 mesi.

04. Impatto finanziario

Fermi produttivi, pubblicazione di know-how, perdita di accesso a dati e sistemi critici

03. Impatto tecnico

Facilità di movimento laterale, numero di credenziali esfiltrate, possibilità di esecuzione di un ransomware.

pikered

AEV: vantaggi per il CISO

pikered

AEV: benefici per il Board

pikered

Quando il Cyber diventa Business?

Discussione a livello strategico

Integrazione nei processi decisionali

Supporto di evidenze

Gestione orientata all’impatto

pikered

E adesso?

CISO

1. Non riportate solo vulnerabilità
2. Raccontate scenari
3. Portate evidenze

Board

1. Chiedete simulazioni
2. Ragionate sull'impatto
3. Investite in ottica strategica

pikered

Se oggi doveste dimostrare che il rischio è sotto controllo o, al contrario, giustificare un budget milionario per ridurre esposizioni critiche, che evidenze portereste al Board?

Q&A

pikered

www.pikered.com

Connect with us on LinkedIn

Parliamo delle vostre sfide: ci trovate al nostro Stand!