

Integrare MITRE ATT&CK nel processo
NIST 800-30 per una difesa
proattiva e di precisione.



Un briefing strategico per la
governance della sicurezza IT.

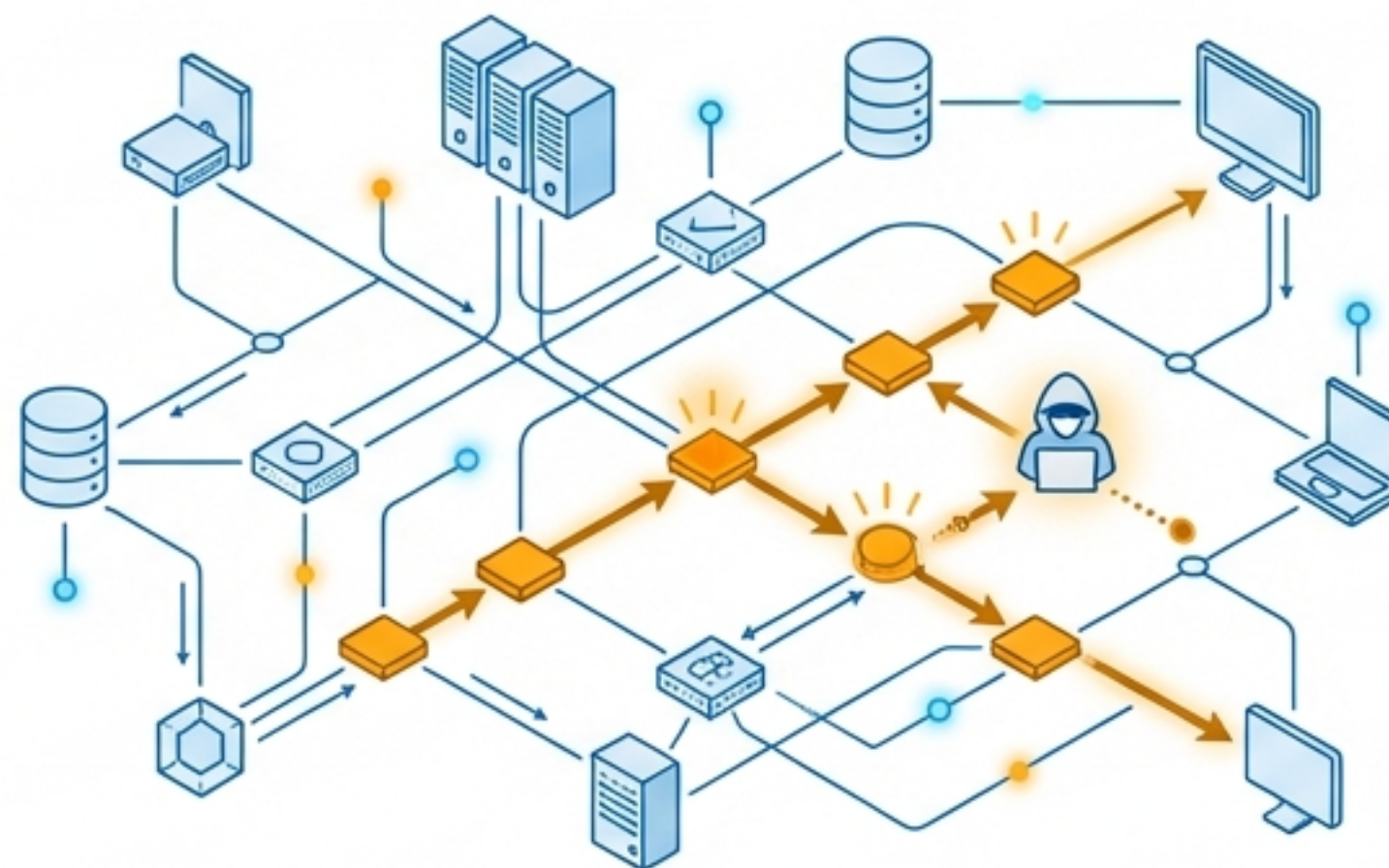
Il Limite delle Valutazioni Tradizionali

L'Approccio Basato sulla Conformità



- Le valutazioni tradizionali del rischio IT si concentrano su elenchi di controllo teorici.
- Trascurano il comportamento reale degli avversari.
- **Risultato:** Una conformità su carta che lascia l'organizzazione cieca di fronte alle minacce emergenti.

La Realtà Operativa



- Gli avversari operano attraverso **tattiche, tecniche e procedure (TTP)** specifiche.
- I sistemi difensivi richiedono dati basati sull'osservazione empirica degli attacchi.
- **Soluzione:** Un'evoluzione strategica verso una sicurezza **Threat-Informed**.

Sinergia Strategica: Governance e Tattica

[Dimensione]	 [NIST Cybersecurity Framework]	 [MITRE ATT&CK]
Obiettivo Principale:	Gestione macroscopica del rischio (Identify, Protect, Detect, Respond, Recover).	Comprensione dettagliata dei comportamenti degli avversari (TTP).
Prospettiva:	Livello strategico e di governance.	Livello tattico e operativo.
Applicazione:	Stabilire policy e best practice.	Informare le difese contro vettori di attacco specifici.
Valore Primario:	Struttura e conformità aziendale.	Precisione e intelligence sulle minacce reali.

La governance stabilisce le regole d'ingaggio; l'intelligence tattica fornisce il mirino.

L'Anatomia di un Attacco: Le 14 Tattiche MITRE



L'Evoluzione della Metodologia NIST 800-30

L'integrazione di MITRE ATT&CK eleva ogni singola fase del processo di valutazione, trasformando le congetture in analisi basate sui dati.



Fase 1: Identificazione delle Minacce

Sostituire le ipotesi con le tattiche avversarie reali.

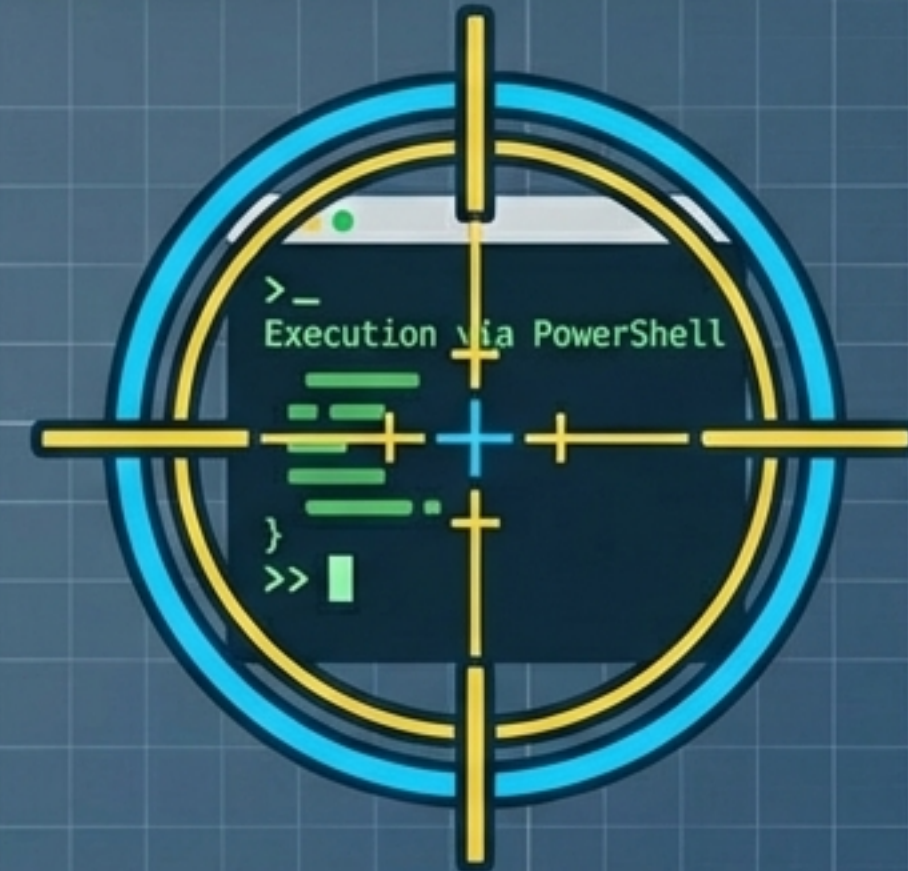
Approccio Tradizionale



Malware

- Affidamento a dati storici e scenari ipotetici.
- Elenchi di minacce generiche (es. Infezione da Malware).

L'Iniezione di Precisione MITRE

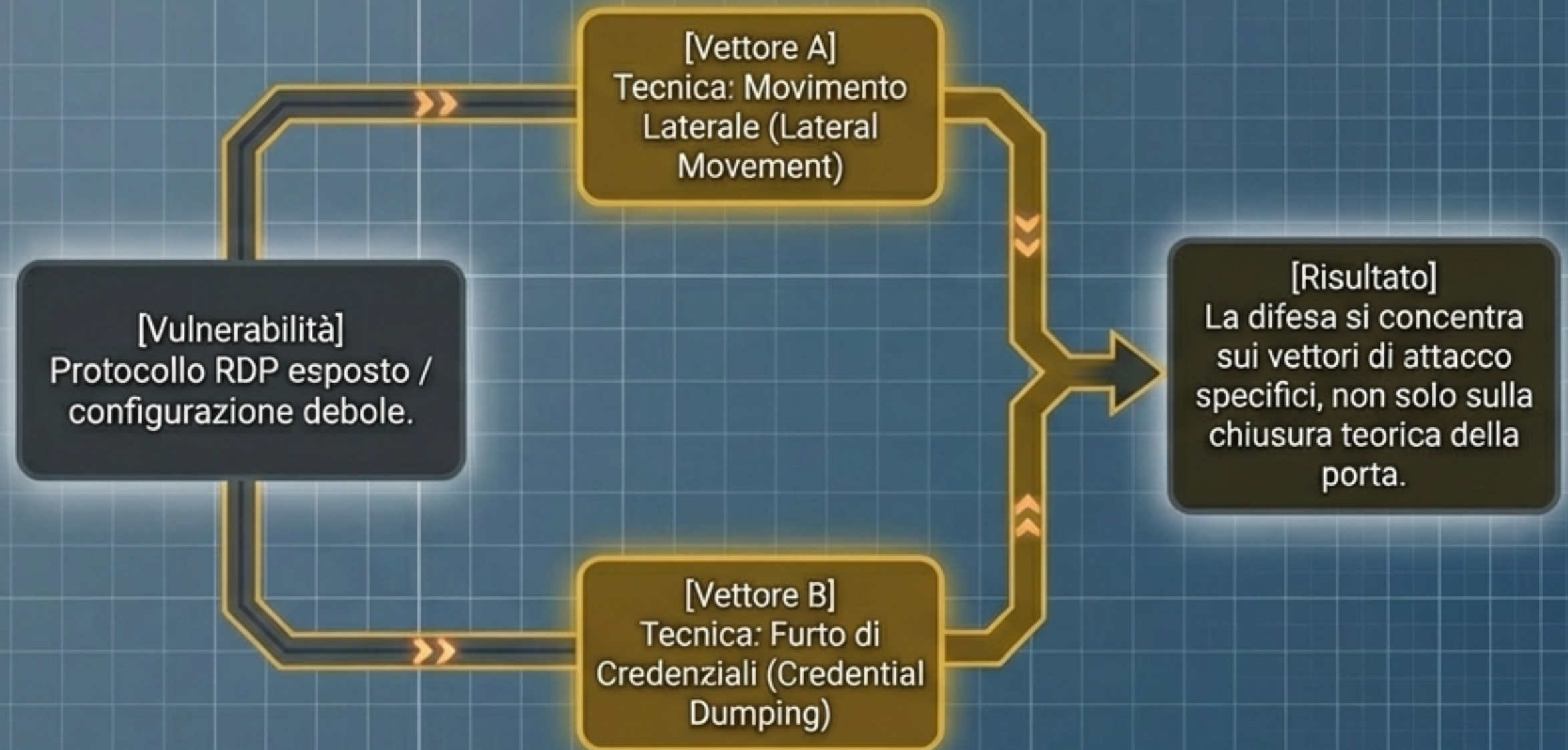


- Catalogo dettagliato di TTP reali.
- Identificazione mirata in base a settore e infrastruttura.
- Esempio Pratico: Invece di "Malware", identificazione della tecnica specifica Execution (es. script dannosi o PowerShell), fornendo un contesto immediato per la difesa.

Fase 2: Identificazione delle Vulnerabilità

Mappare le debolezze architetturali alle tecniche di sfruttamento.

- Le vulnerabilità isolate non descrivono il rischio completo.
- MITRE ATT&CK collega software non patchati o configurazioni errate direttamente ai metodi di sfruttamento.



Fase 3: Determinazione della Probabilità

Calibrare il rischio attraverso il contesto dell'avversario.

Metodo Classico



- Basato su giudizi qualitativi o trend storici generici.
- Valutazione piatta e soggettiva.

Integrazione MITRE



- Analisi dei modelli di attacco osservati.
- Caso Studio: Nel settore finanziario, l'analisi ATT&CK rivela che gli avversari utilizzano prevalentemente tecniche di Accesso Iniziale come lo spear-phishing o lo sfruttamento degli accessi dei dipendenti.
- Il calcolo della probabilità diventa un dato empirico e focalizzato.

Fase 4: Determinazione dell'Impatto

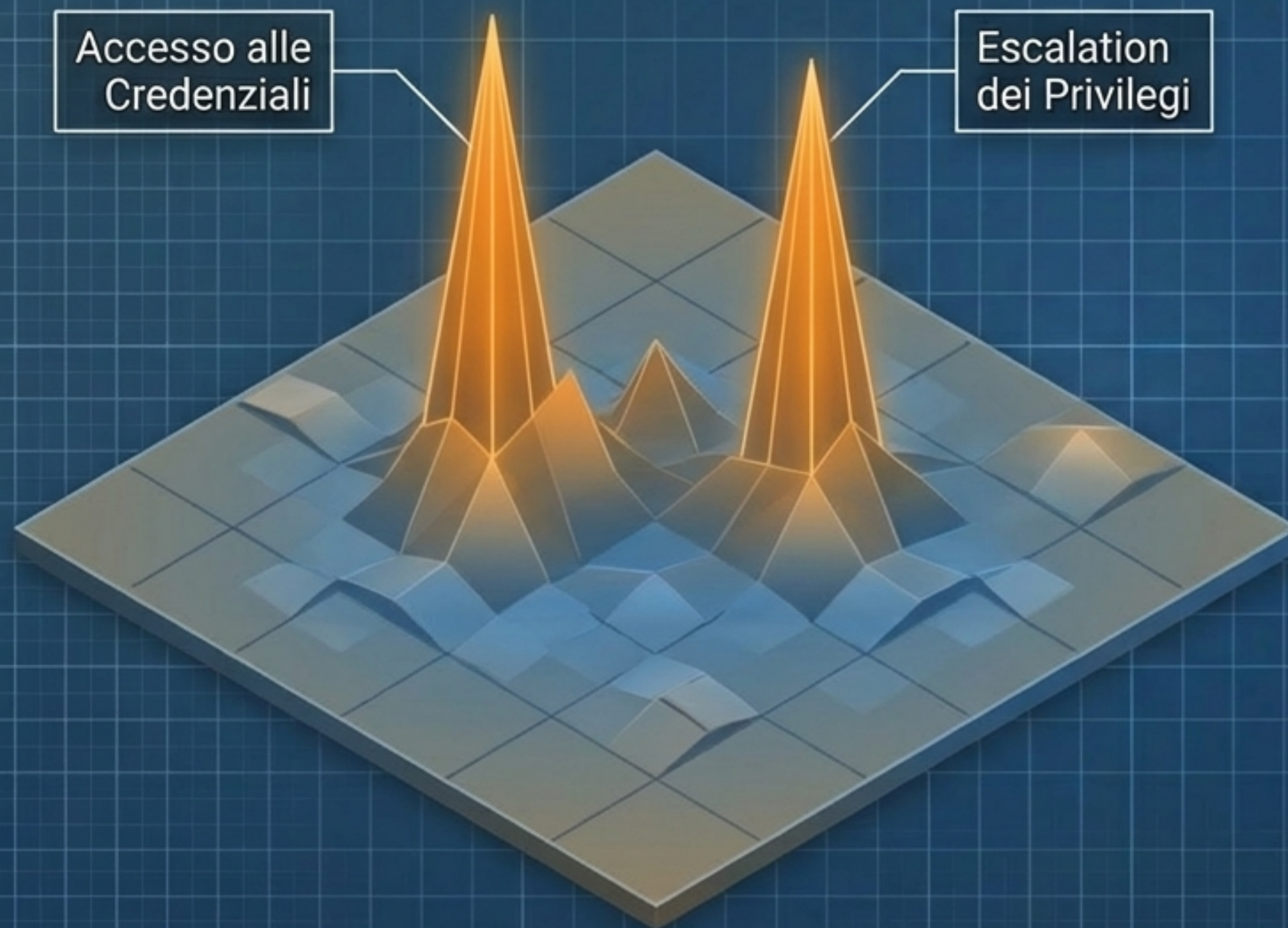
Collegare le tecniche tattiche all'impatto sul business.



Superare le stime generalizzate: quantificare l'impatto legando le azioni tecniche alla severity aziendale.

Fase 5: Determinazione del Rischio

Prioritizzazione chirurgica basata sulla frequenza e sull'impatto delle TTP.



- Non tutti i rischi hanno lo stesso peso operativo.
- Unendo le probabilità contestualizzate e l'impatto di business, MITRE ATT&CK filtra il "rumore di fondo".
- **Risultato Operativo:** Consente ai team di sicurezza di concentrare gli investimenti sulle tecniche prioritarie più frequentemente utilizzate contro architetture simili.

Fase 6: Risposta al Rischio

Progettare contromisure specifiche per bloccare comportamenti reali.

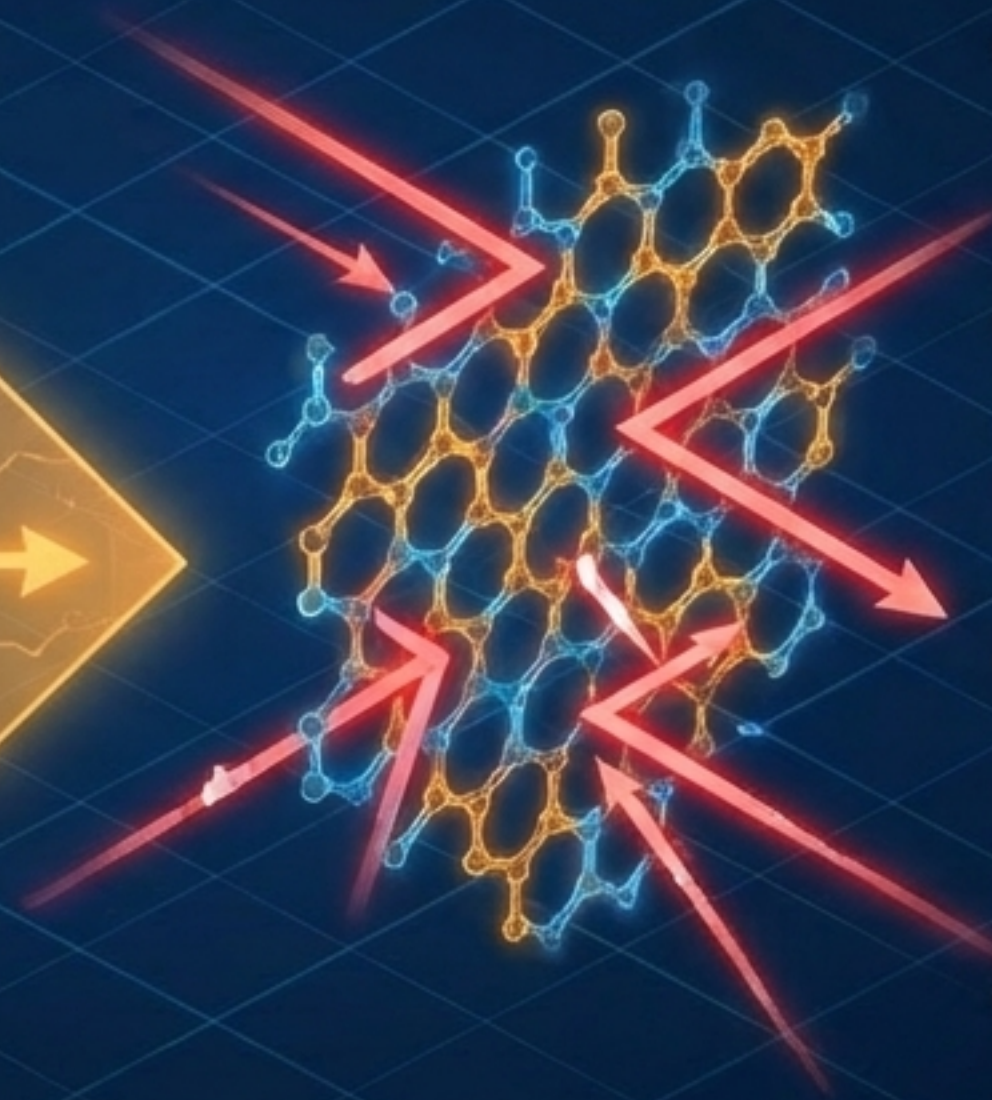
Risposta Generica



- Difese ampie e non ottimizzate.
- **Esempio:** "Migliorare la sicurezza della rete".



Risposta Mirata MITRE



- Contromisure progettate per intercettare l'avversario nella catena di attacco.
- **Esempio 1:** Tecnica Persistenza -> Monitoraggio specifico delle modifiche insolite al registro di sistema.
- **Esempio 2:** Tecnica Esfiltrazione -> Rilevamento di trasferimenti dati non autorizzati su canali anomali.
- **Esempio 3:** Tecnica Esecuzione -> Restrizione severa degli script PowerShell solo agli utenti autorizzati.

I Benefici Strategici

Il valore della transizione verso valutazioni Threat-Informed.



Difesa Informata sulle Minacce

- Passaggio dalla conformità teorica alla difesa contro gli attacchi del mondo reale.
- Identificazione granulare e azionabile delle vulnerabilità.



Prioritizzazione Basata sui Dati

- Allocazione efficiente delle risorse di sicurezza verso i vettori di attacco più probabili e distruttivi, riducendo lo spreco su rischi teorici.

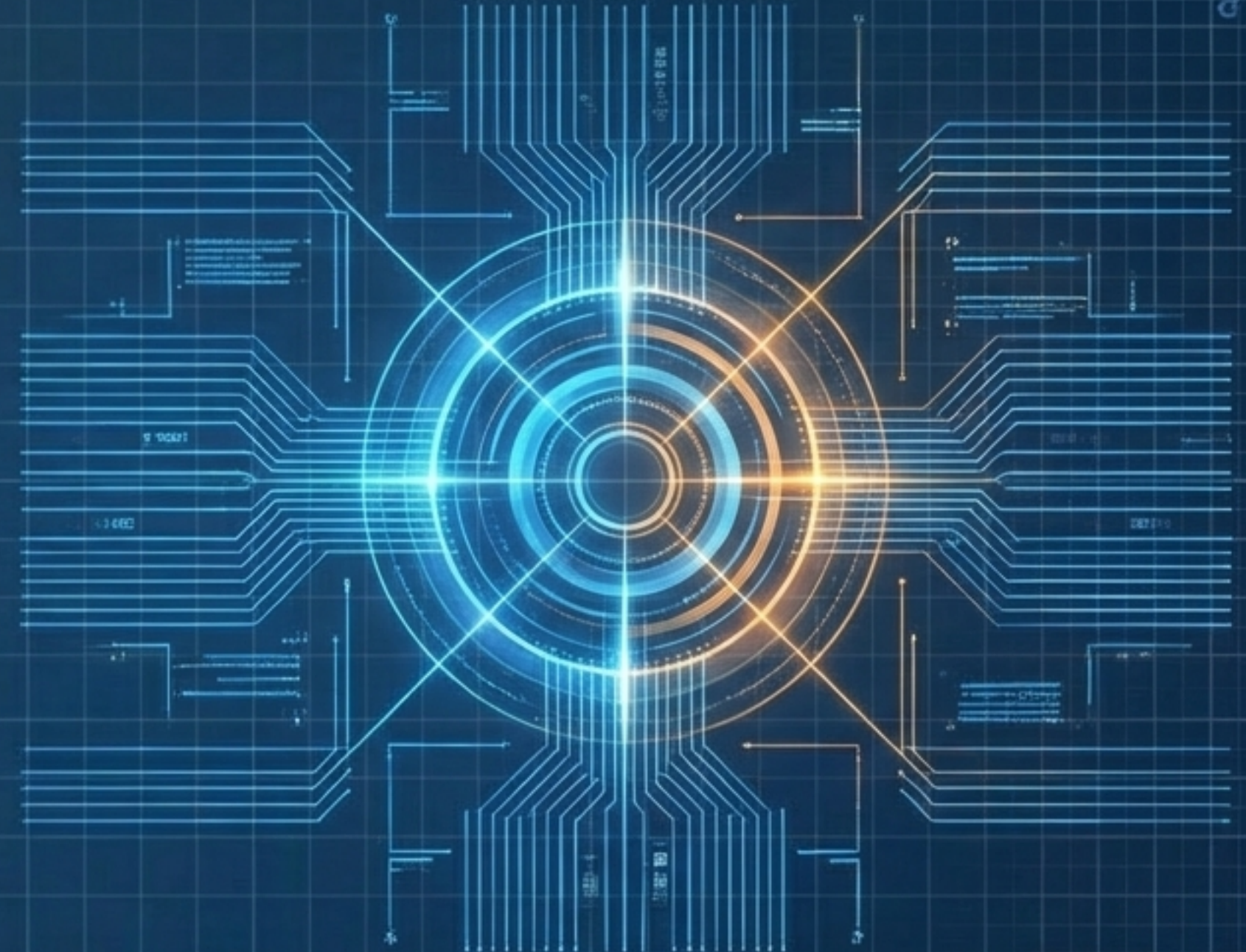


Allineamento al Business

- Traduzione diretta delle minacce tattiche in impatto finanziario e operativo, facilitando la comunicazione del rischio con il Board of Directors.

L'Acceleratore: Automazione su Scala

- Integrare l'intero framework MITRE ATT&CK in valutazioni dinamiche richiede enormi risorse manuali. L'automazione è la chiave.
- La Piattaforma Rivial automatizza l'integrazione di MITRE ATT&CK nel processo di valutazione del rischio.
- Vantaggio Competitivo: Elabora in pochi minuti il collegamento tra il comportamento dell'attaccante e l'impatto finanziario quantificato.
- Consente decisioni più intelligenti e rapide per proteggere i sistemi informativi aziendali.



La precisione tattica incontra l'efficienza automatizzata. (Rivial Data Security)