XIV CONGRESSO NAZIONALE DEGLI ATTUARI

L'ATTUARIO GLOBALE PER UN MONDO SOSTENIBILE TRA TRADIZIONE, INNOVAZIONE E RISCHI EMERGENTI

MILANO
15-17 Novembre 2023
Hotel Quark

Consiglio Ordine Nazionale degli Attuari

CONSIGLIO NAZIONALE DEGLI ATTUARI

La valutazione del rischio cyber

Un modello quantitativo

Valerio Scacco
Ordine degli Attuari

Introduzione

Ottimizzare la cybersecurity

- Per un cyber risk management efficiente, le aziende devono **calibrare oculatamente gli investimenti** in sicurezza informatica
- È essenziale l'allocazione oculata delle risorse finanziarie e l'adozione di **strategie basate su decisioni informate**

Identificare e misurare l'esposizione

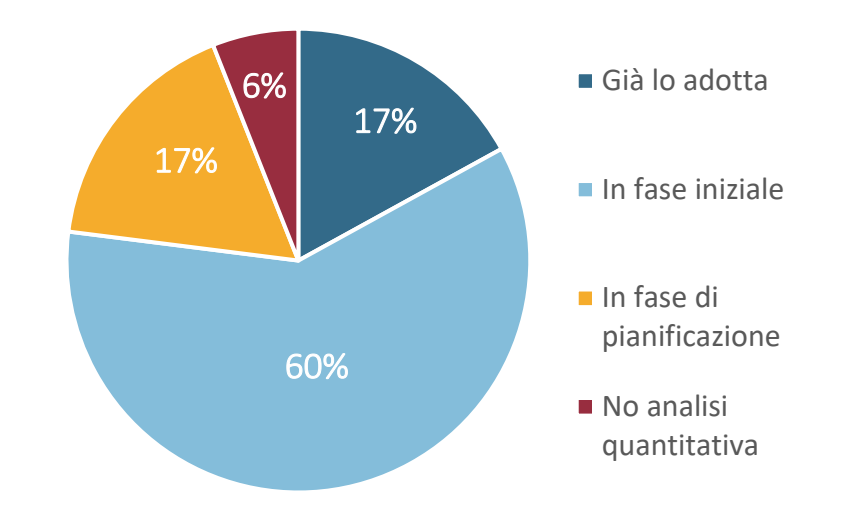
- Questo richiede **competenze nella misurazione del rischio**, i cui benefici sono spesso sottovalutati
- Si rileva **confusione sulle metodologie di misurazione**, la loro utilità e le qualità che le rendono «buone»; soprattutto nei settori diversi dai servizi finanziari
- Nella pratica, l'efficace minimizzazione dell'esposizione al rischio di un asset digitale **richiede il riconoscimento di quali asset necessitino di controlli di sicurezza e contromisure**.

L'evoluzione dei modelli

- **Storicamente**, il cyber security risk management si è basato principalmente sulla **misurazione qualitativa** del del rischio, presumendo che fosse il metodo più adeguato
- Negli ultimi anni, le metodologie di valutazione economica e quantitativa del rischio cyber hanno **raggiunto una maturità simile** a quella delle **metodologie di modelling** su altre categorie di rischio (es. controparte, sottoscrizione assicurativa)
- Questo sta permettendo di **modellizzare quantitativamente i rischi cibernetici**, migliorando le performance delle funzioni di cyber risk management

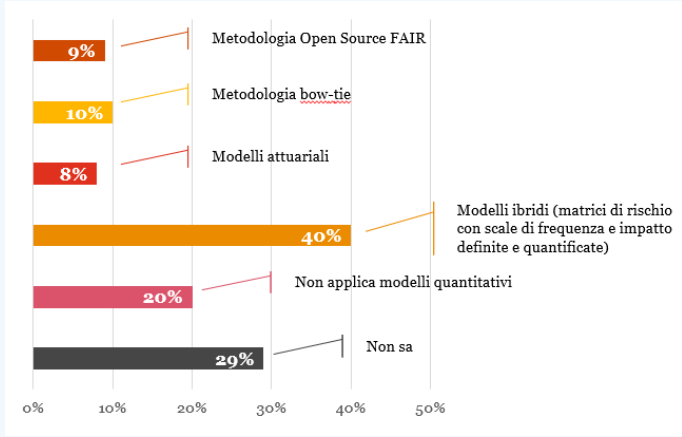
Indagine di Mercato sul Rischio Cyber

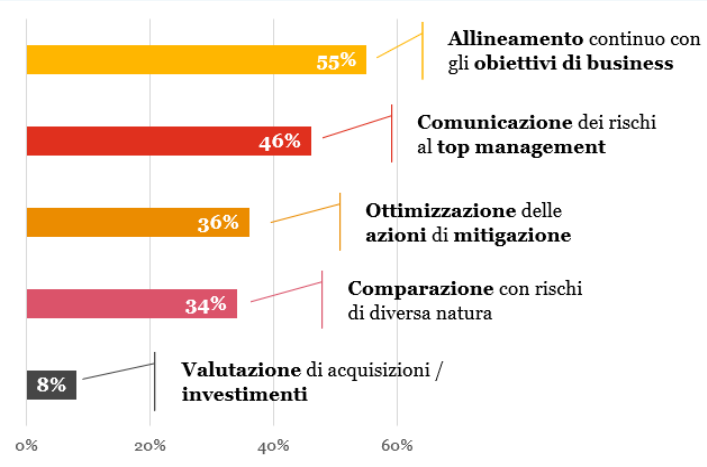
Attraverso i dati ricavati da survey condotte o sponsorizzate da PwC è possibile misurare il **grado di adozione di metodologie di analisi quantitativa del rischio cyber**:



Nella survey "Global Digital Trust Insights 2021[1]", il 17% dei cyber manager intervistati ha dichiarato di svolgere già una quantificazione finanziaria dei rischi cyber, il 60% è in uno stadio iniziale e un ulteriore 17% pianifica di farlo in futuro.

La survey condotta nel 2020[2] dagli Harvard Business Review Analytic Services e sponsorizzata da PwC ha chiesto ai rispondenti **quali metodologie di quantificazione del rischio cyber venissero adottate**.





La medesima survey ha chiesto ai rispondenti di identificare **i principali benefici della quantificazione del rischio.**

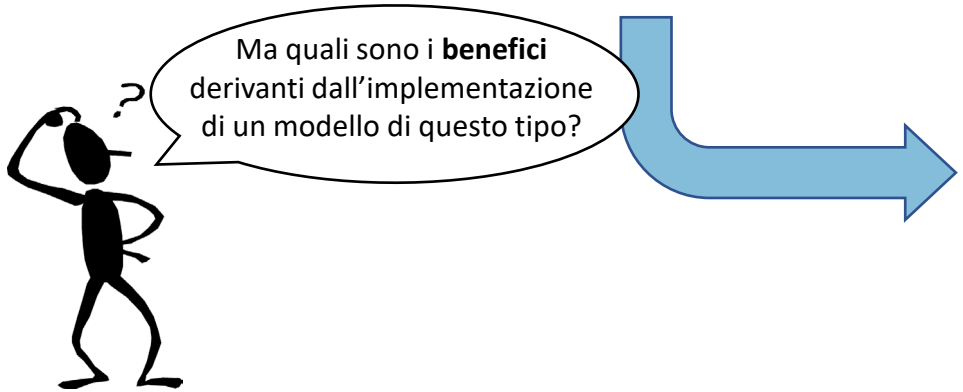
[1] https://www.pwc.com/us/en/services/consulting/cybersecurity/library/cyber-risk-quantification-management.html
[2] https://www.pwc.com/us/en/services/consulting/cybersecurity/library/pwc-covid-19-ciso-pulse-survey.html

Un approccio metodologico

La metodologia che proponiamo si basa sul framework **FAIR (Factor Analysis of Information Risk)** ed è progettata per fornire una valutazione degli impatti economici dei rischi di sicurezza informatica.

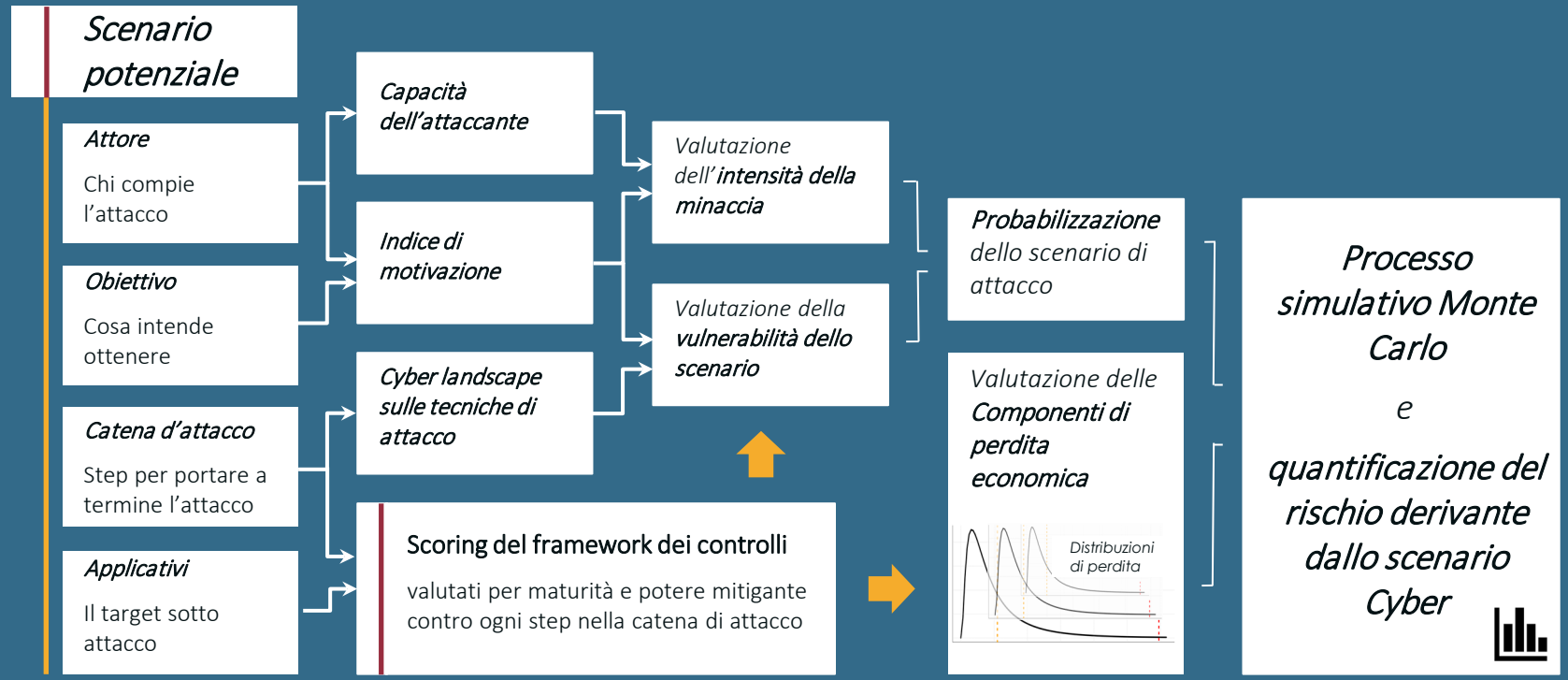
Factor Analysis of Information Risk

- Scomposizione del rischio in fattori misurabili
- Utilizzo di tecniche attuariali
- Misurazione probabilistica delle minacce e dei loro impatti



- ❑ Analisi di **scenari specifici**, rilevanti per l'impresa
- ❑ **Misurazione quantitativa e probabilizzata** dell'esposizione cyber
- ❑ Parametrizzazione sensibile alle **informazioni** sulle minacce e all'efficacia dei controlli
- ❑ Approccio **implementato e testato su apposito tool**
- ❑ L'utilizzo del modello:
  - ❑ **potenzia l'autoconsapevolezza sul framework dei controlli**
  - ❑ aumenta la **capacità di identificare e prioritizzare** correttamente le management action, grazie alla possibilità di valutare in anticipo gli impatti di mitigazione
  - ❑ permette una **razionalizzazione strutturata delle relazioni tra i controlli e le minacce**.

L'architettura del modello

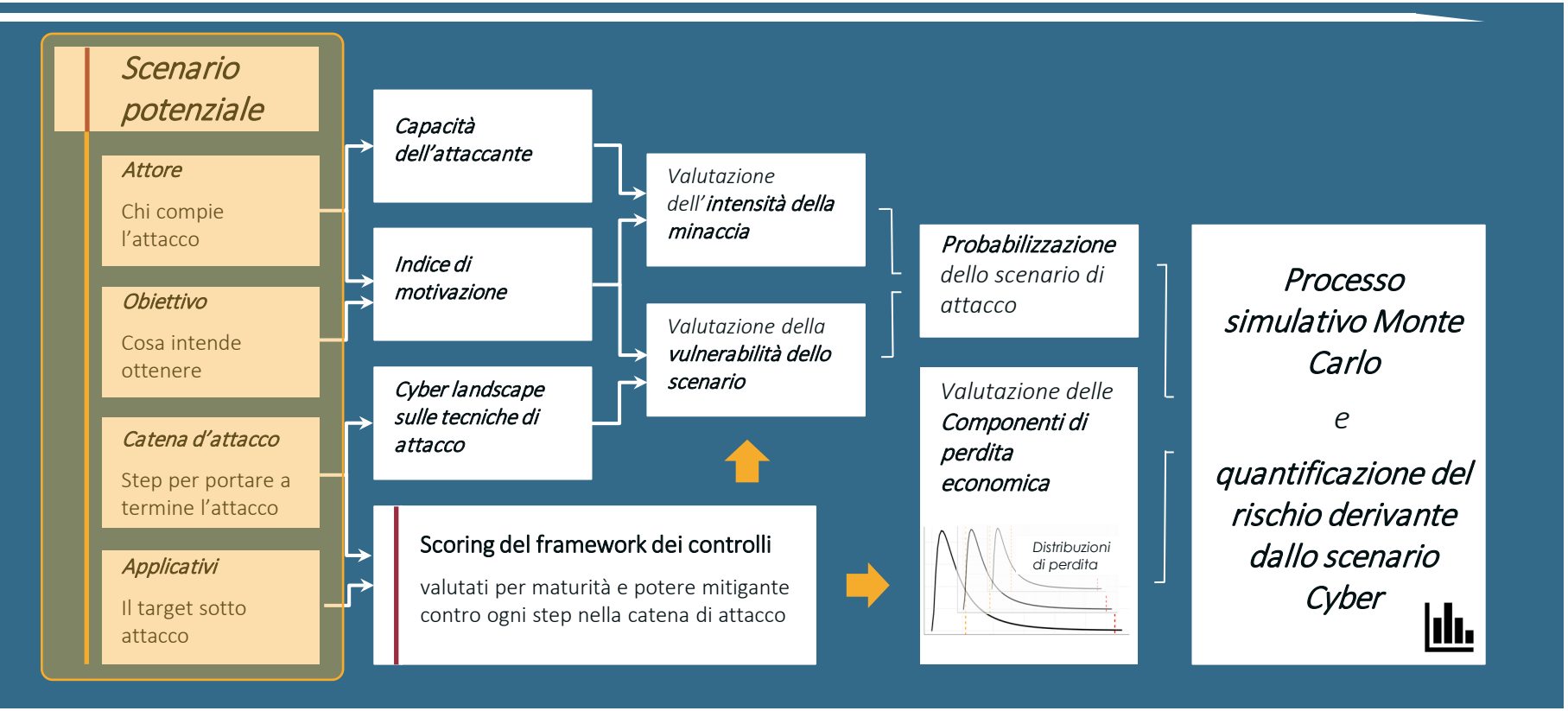


- **Approccio modulare flessibile**

  Ogni modulo è un micro-modello, che produce uno **specifico output intermedio**, fornendo preziose indicazioni sulle vulnerabilità dell'azienda e sulle **esigenze di prioritizzazione**.

- **Dati di alimentazione**
  - **Serie storiche** derivanti da incidenti di cyber security
  - Report specifici di settore
  - **Informazioni e dati specifici** della realtà aziendale
  - **Expert judgment**

L'architettura del modello – Definizione degli scenari



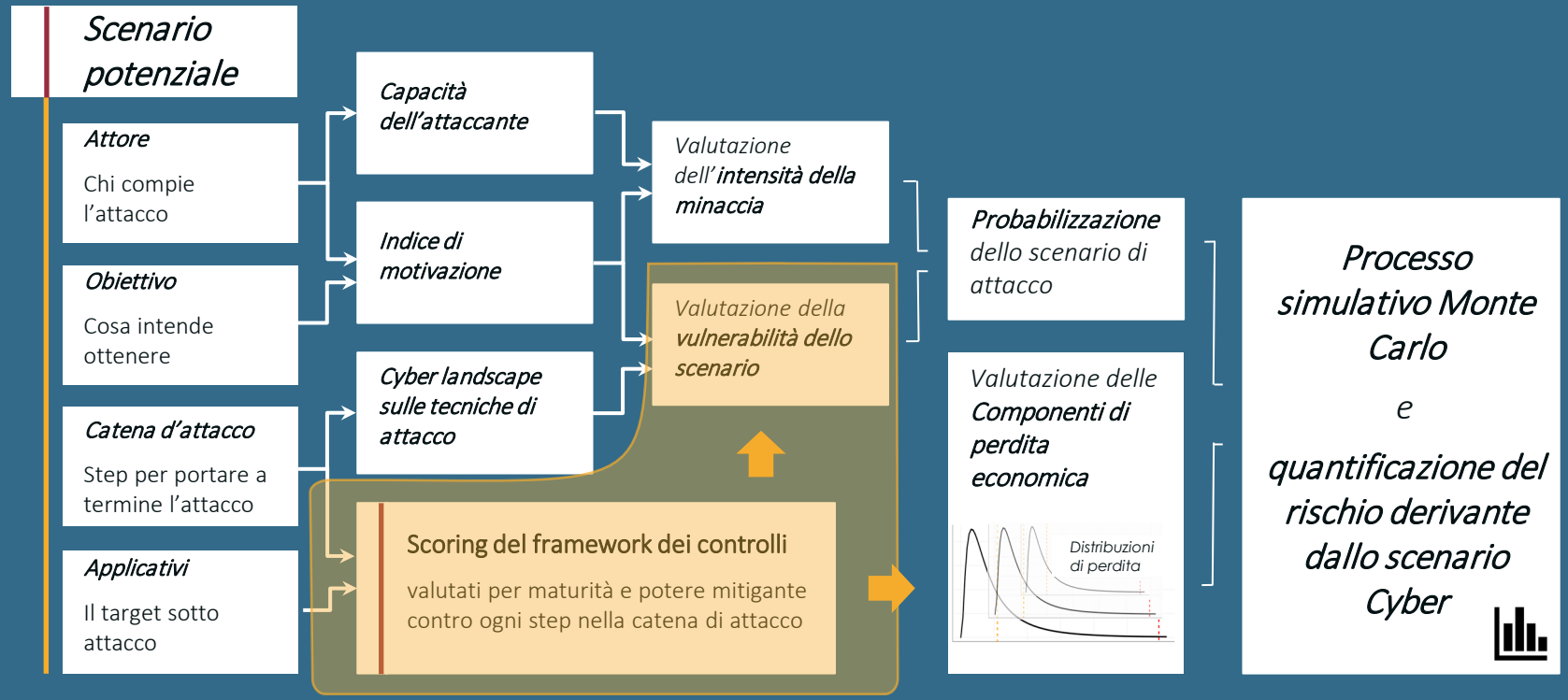
- Componenti dello Scenario

  Il modello è sviluppato in modo da poter **costruire gli scenari di interesse** per la propria esposizione al rischio

  Quattro "librerie" vengono utilizzate come "ingredienti" di base per definire lo scenario di rischio da quantificare:

  - **Attore, Obiettivo e Catena d'Attacco:** Rappresentano fattori di rischio (reperibili anche da fonti esogene) utilizzati dal modello per calibrare le metriche funzionali alla fase simulativa
  - **Applicativi:** Sono specifici dell'impresa e rappresentano l'asset da includere nel perimetro e le informazioni ad essi relative (es.: interazione tra applicativi, numero/tipo di record esposti al rischio, tempi/costi di ripristino, etc.)

L'architettura del modello – La valutazione del sistema dei controlli



- **Framework dei Controlli**

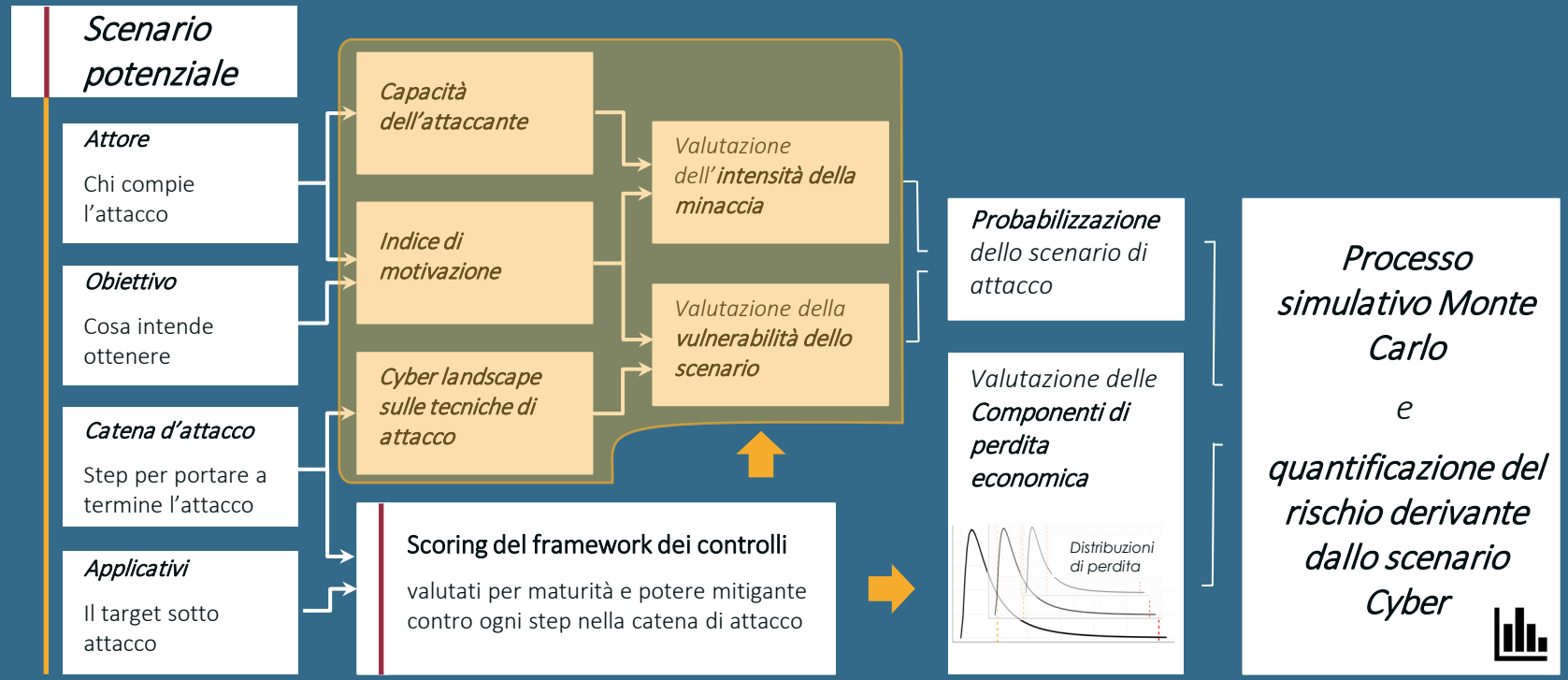
Il framework dei controlli rappresenta la **maggiore difesa da parte delle unità** che subiscono il tentativo di attacco.

Al fine di definire la bontà del sistema dei controlli, considerando il loro effettivo potere di mitigazione, è prevista la loro **declinazione in una «tassonomia incrociata»**, che combina ogni forma di difesa con ogni step di attacco della libreria scenari.

La tassonomia definita servirà a valutare il sistema dei controlli secondo due dimensioni con scopi distinti:

- **Maturità:** Descrive in termini quantitativi il livello assoluto dei controlli.
- **Efficacia**: Rappresenta il potere di mitigazione di ogni controllo classificato verso ogni possibile tecnica presente nella libreria degli step d'attacco.

L'architettura del modello – Elaborazione delle metriche e reporting intermedio



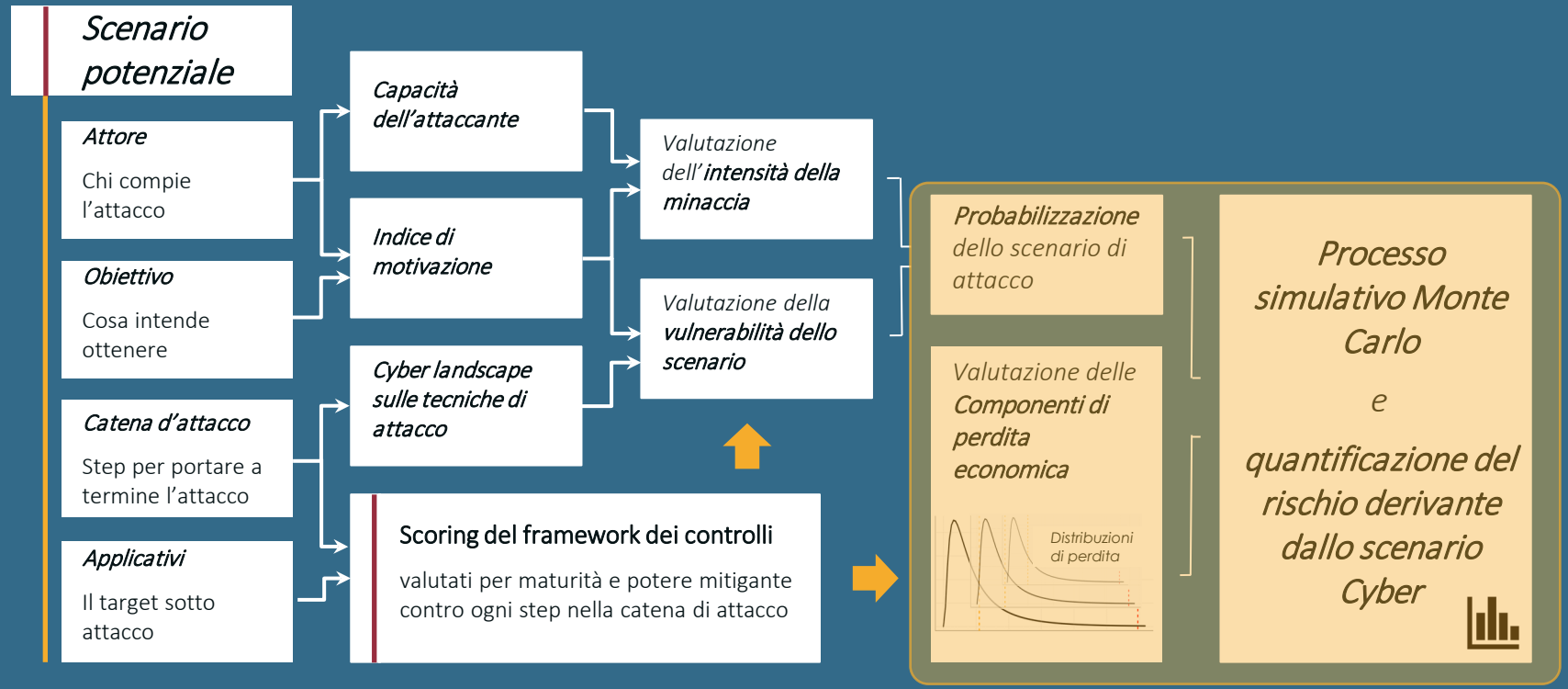
- **Input di probabilizzazione**

  A partire dalle librerie definite nella prima fase e integrando la valutazione del sistema dei controlli di cui alla fase precedente, il modello calcola una serie di **metriche intermedie** che dipendono dalle scelte effettuate in sede di definizione dello scenario.

  Vengono valutate **l'intensità della minaccia e la vulnerabilità del soggetto attaccato**:

  - **Intensità:** Score che ha la funzione di esprimere il livello della minaccia dal punto di vista dell'attaccante e dipende dalla sua motivazione e dalle sue capacità.
  - **Vulnerabilità:** Disponibile sia per ogni singolo step che compone l'attacco, sia per l'intero scenario. Descrive il livello della minaccia dal punto di vista del difensore, con riferimento ad informazioni di settore sulle tecniche di attacco e al livello degli specifici controlli aziendali che su di esse agiscono.

L'architettura del modello – Processo simulativo e report



- Processo Simulativo & Quantificazione del Rischio di Scenario

Per ogni scenario elaborato, il processo simulativo utilizza **due distribuzioni** che, **combinate** opportunamente, permetteranno di ottenere **l'intera distribuzione** associata alla perdita economica derivante dallo **scenario**, su una base temporale prefissata:

- **Distribuzione della Probabilità di Accadimento e di Riuscita**: Calcolata tramite funzioni matematiche a partire dalle metriche ottenute precedentemente (intensità e vulnerabilità);
- **Distribuzione dell'Impatto Economico**: Elaborata a partire dalle distribuzioni delle diverse componenti di perdita associate allo scenario.

Gli output del modello

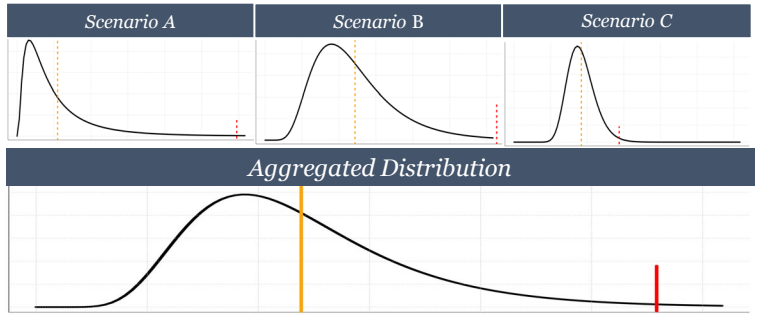
Reporting

Per ogni scenario è possibile ottenere tabelle di output e report grafici.

Tutti gli input e output dei moduli possono essere elaborati attraverso **strumenti di risk intelligence** al fine di **identificare «chirurgicamente» le vulnerabilità che guidano l'esposizione**.

Aggregazione & Dipendenze

Il modello fornisce la distribuzione della probabilità di perdita per ciascun scenario e per i diversi step di aggregazione, tenendo conto delle dipendenze tra le diverse componenti dello scenario stesso (Attaccanti, Obiettivi,…)



Allocazioni

L'esposizione complessiva al rischio **può essere allocata sulle librerie** definite, funzionando come **strumento di intelligence sulle fonti di rischio**.

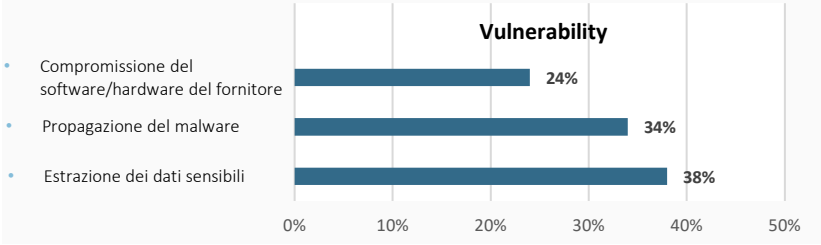
Un esempio di «scheda scenario»

Quali sono i controlli più impattanti nel modello e da quali potremmo ottenere una maggiore mitigazione del rischio?

Scenario di Data Breach: Classificazione dei Controlli più significativi

Rank	Perimetro del Controllo	Obiettivo del Controllo	Stima di Riduzione del Rischio a fronte di un miglioramento
#1	Rilevamento Minacce	Valutazione dell'implementazione ed efficacia dei test interni per il rilevamento di minacce	1,50
#2	Risorse Interne	Valutazione della sensibilità delle risorse interne in materia di cyber sicurezza	1,43
#3	Risorse Interne	Valutazione dell'efficacia dei corsi interni somministrati agli sviluppatori in merito ai tool aziendali	1,41
#4	Correzione delle minacce	Valutazione delle simulazioni condotte in caso di attacco cyber completato con successo	1,19

In relazione a quale step della catena di attacco l'entità legale risulta essere più vulnerabile?



Qual è l'esposizione finanziaria?

Probabilità	Impatto	Esposizione
0.17 *1 ogni 6 anni*	34 €M *1 volta ogni 100 attacchi*	**3.7 €M**

I «key take-away»

Il modello di *cyber risk quantification* permette di simulare una libreria completa di scenari di minaccia informatica e produrre statistiche dettagliate (oltre a KPI riepilogativi) sulle potenziali perdite, con particolare attenzione ai vari elementi delle fonti di vulnerabilità

Il processo di parametrizzazione del modello integra in modo efficace l'intelligence sulle minacce, le competenze informatiche e le peculiarità aziendali attraverso l'utilizzo di input specifici

Consente l'implementazione di un efficace sistema di misurazione e reporting, supportando un allineamento continuo con gli obiettivi aziendali, attraverso una chiara e tempestiva comunicazione dei rischi e delle vulnerabilità aziendali al management

Consente di adottare con maggiore consapevolezza ed efficienza azioni manageriali e progetti di investimento sulla cybersecurity, grazie alla preliminare valutazione degli impatti di mitigazione sull'esposizione

Grazie!

Valerio Scacco
Ordine degli Attuari