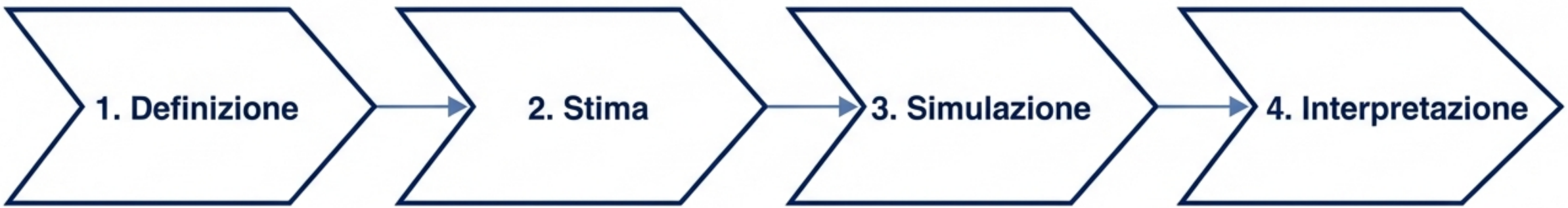
Metodologia Quantitativa per la Valutazione del Rischio Cyber

Il Metodo HTMA (How to Measure Anything in Cybersecurity Risk)

Modulo 7: Framework di Analisi del Rischio

Introduzione al Framework HTMA

Sviluppato nel 2016 da Douglas Hubbard e Richard Seiersen, il metodo HTMA propone un approccio scientifico per ridurre l'incertezza nel rischio informatico, passando da stime qualitative a misurazioni quantitative probabilistiche.



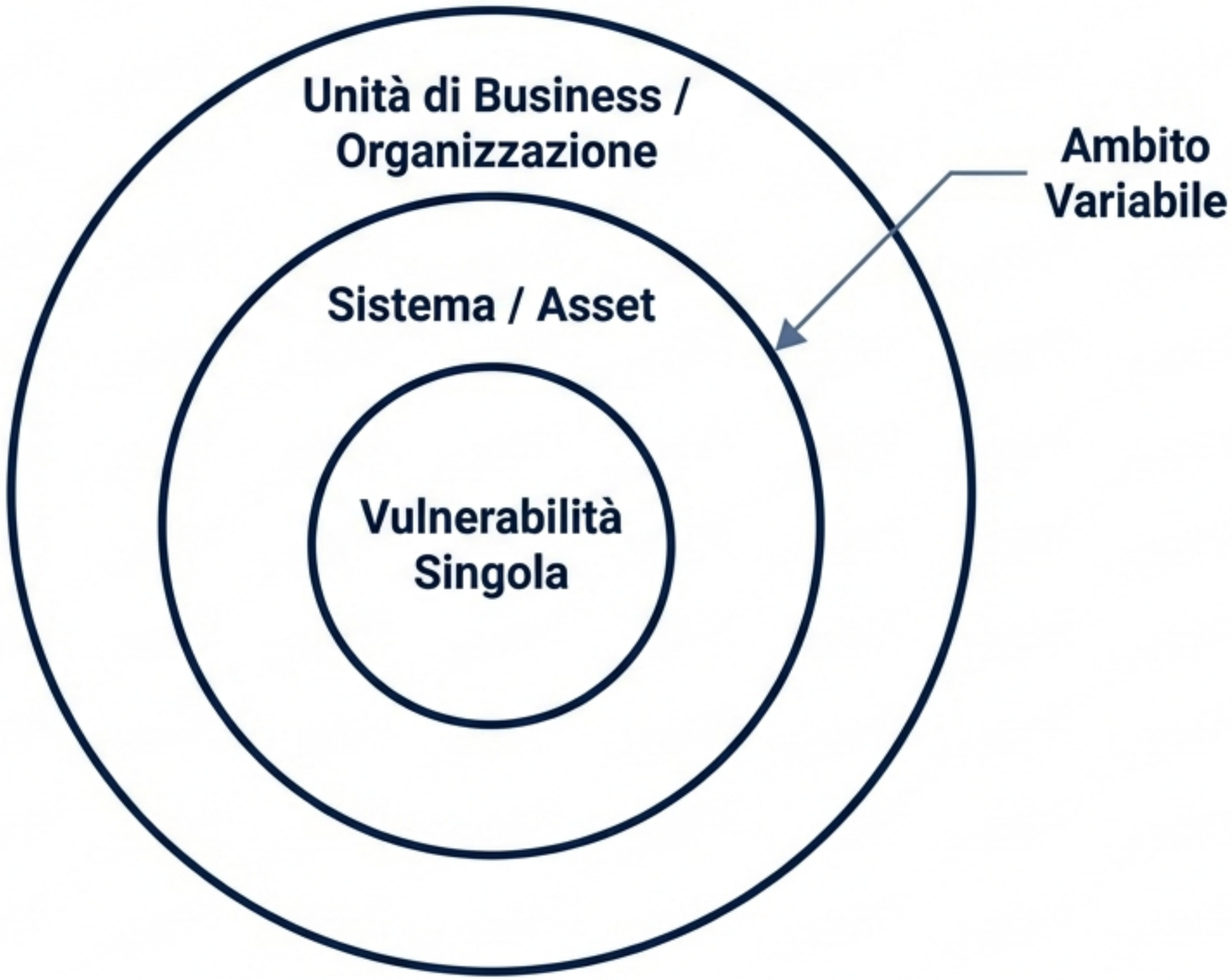
Step 1: Definizione dello Scenario di Minaccia

Definizione di Rischio

Lo stato di incertezza in cui alcune possibilità comportano una perdita o un esito indesiderato.

Flessibilità dell'Ambito (Scope)

A differenza di altri metodi (es. FAIR), HTMA permette discrezionalità totale sull'unità di analisi.
L'analista seleziona solo le minacce pertinenti.



Fonti Dati: Superare la “Sindrome del Foglio Bianco”

Non è necessario iniziare l'analisi da zero. L'identificazione delle minacce si basa su repository standardizzati.

CVE (Common Vulnerabilities and Exposures)

Database pubblico di falle di sicurezza che permette di coordinare le priorità di risoluzione.

225.772+

Record disponibili al Marzo 2024

CVE ID	DESCRIPTION	SEVERITY	STATUS
CVE-2024-XXXX	Remote Code Execution in…	HIGH	PUBLISHED
CVE-2024-YYYY	SQL Injection vulnerability…	CRITICAL	PUBLISHED
CVE-2024-ZZZZ	Cross-Site Scripting (XSS)…	MEDIUM	PUBLISHED

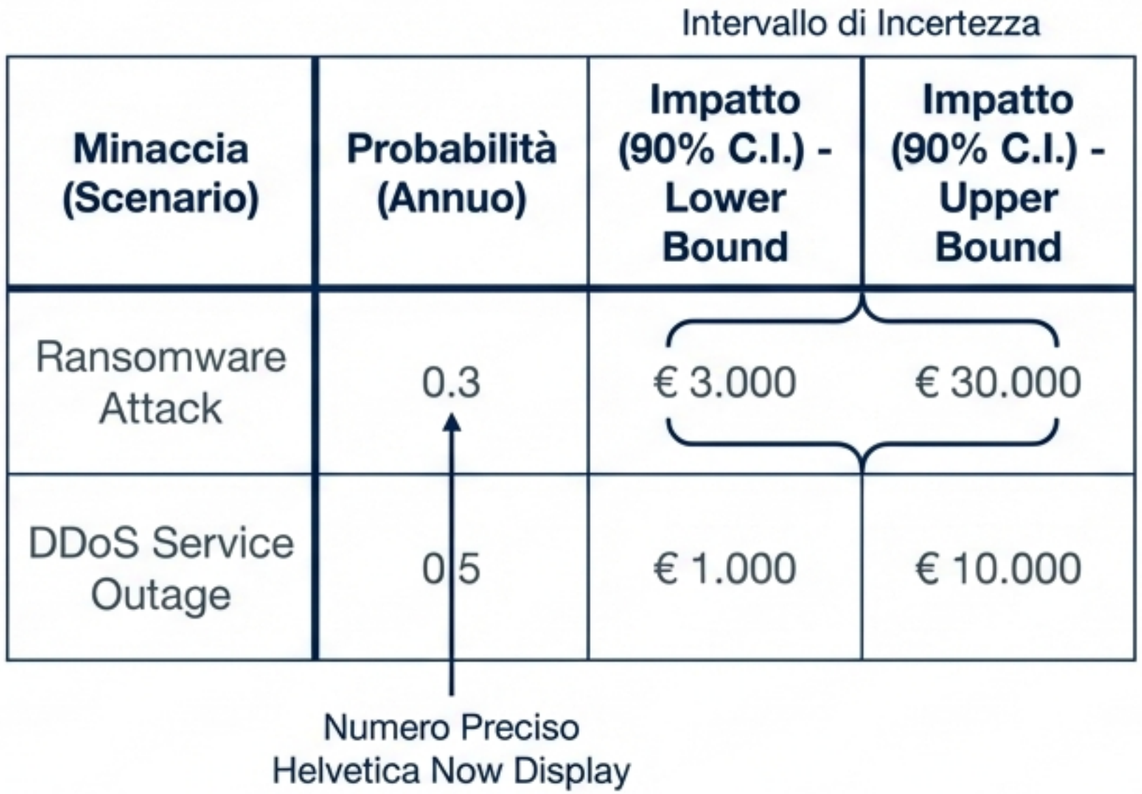
Step 2: Il Ruolo dell'Esperto Calibrato

La stima non è un processo automatico. Richiede l'input di un "Esperto Calibrato" capace di tradurre la conoscenza tecnica in parametri numerici probabilistici.

Step 2: Parametrizzazione degli Input

Per ogni minaccia identificata, l'esperto deve fornire due metriche critiche:

- **Probabilità**: La possibilità che l'evento accada in un anno (valore puntuale).
- **Impatto**: Un intervallo di confidenza al 90% (da minimo a massimo).



Step 3: Fondamenti della Simulazione Monte Carlo

Definizione

Studio di una variabile aleatoria attraverso la generazione di numerosi scenari casuali.

L’Analogia del Dado

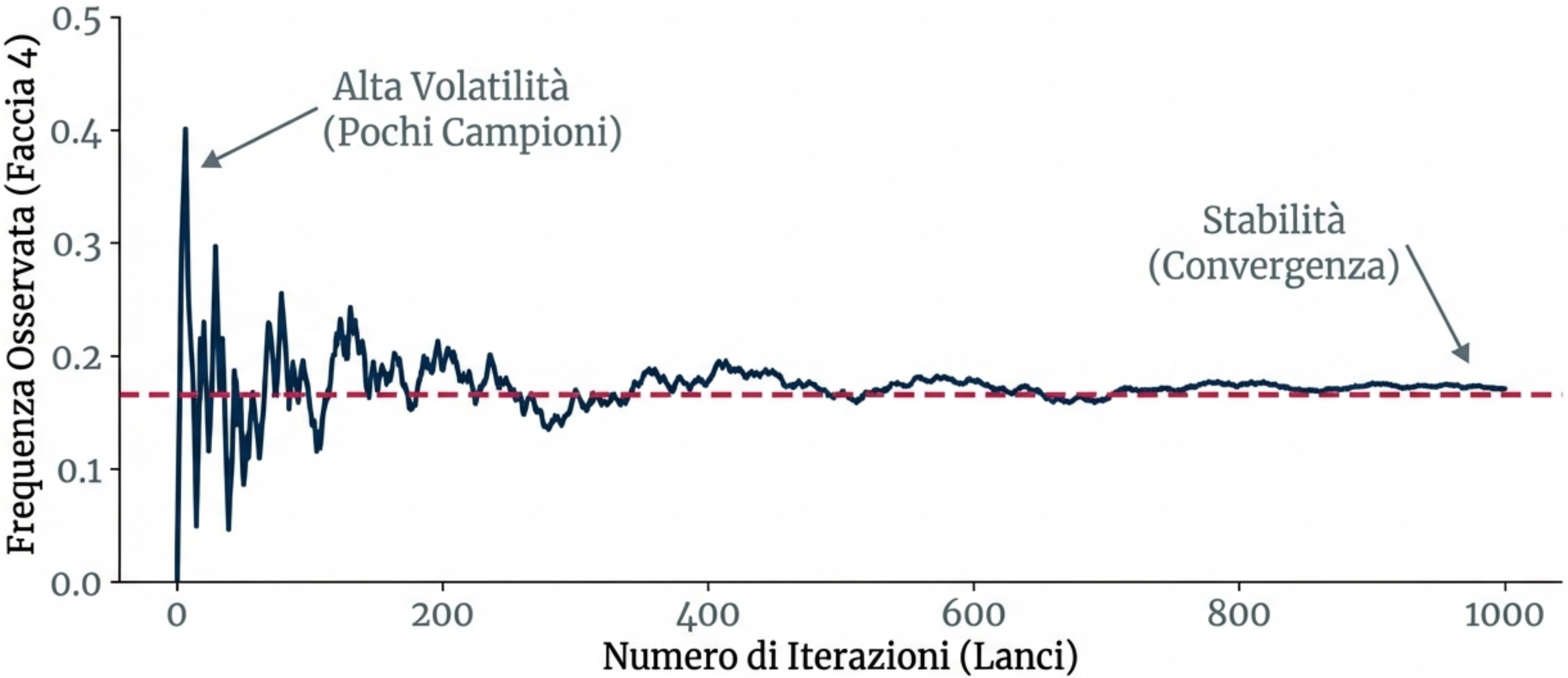
La frequenza (esperienza empirica) coincide con la probabilità teorica (calcolo matematico) solo se l'esperimento viene eseguito infinite volte.

Probabilità Teorica
(Faccia 4) = 1/6 ≈ 16.7%

Frequenza (dopo 6 lanci) =
Variabile (es. 0%, 16%, 33%)

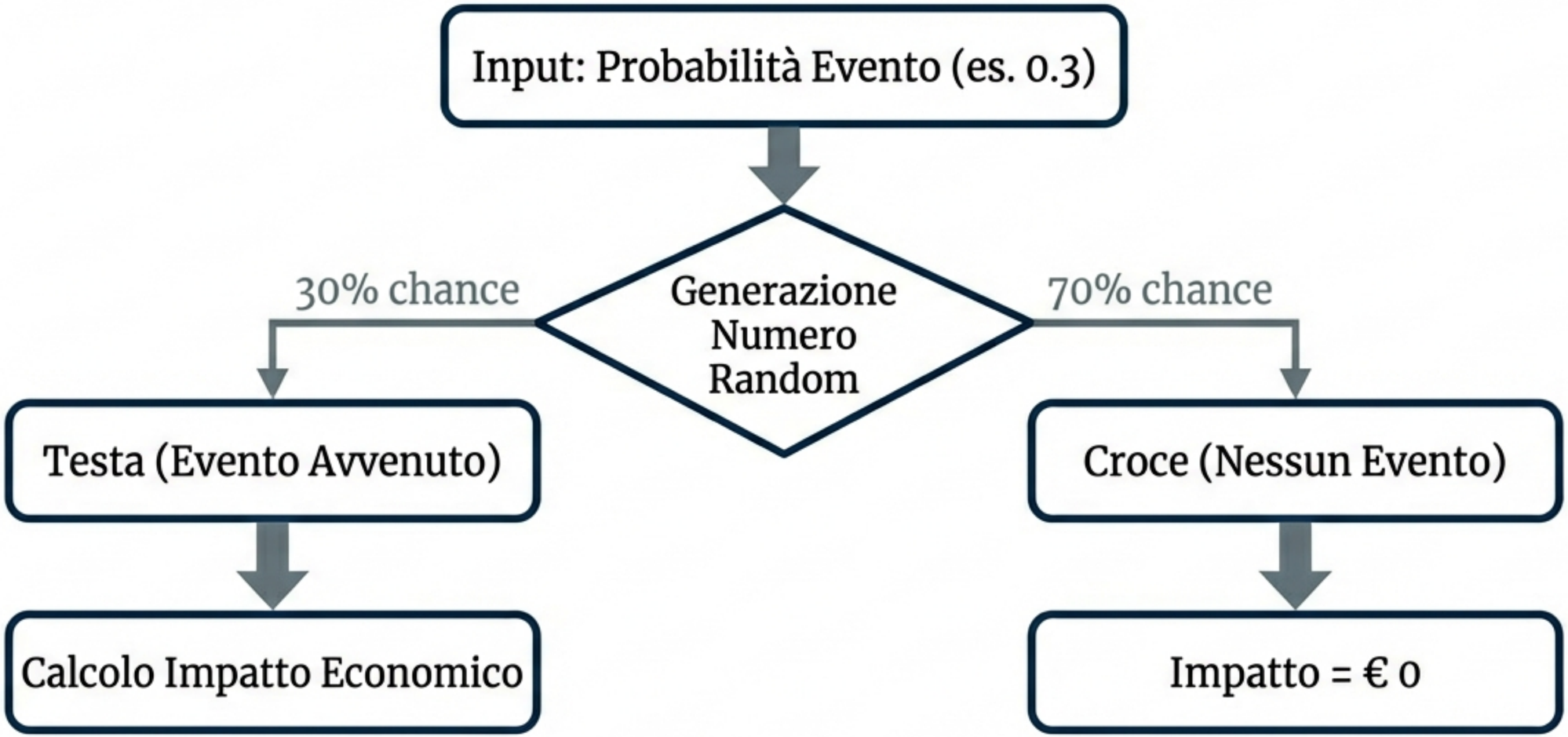
Frequenza (dopo ∞ lanci)
= 16.7%

Convergenza: Dalla Frequenza alla Probabilità



Step 3: Modellazione dell’Evento

La Logica della ‘Moneta Truccata’

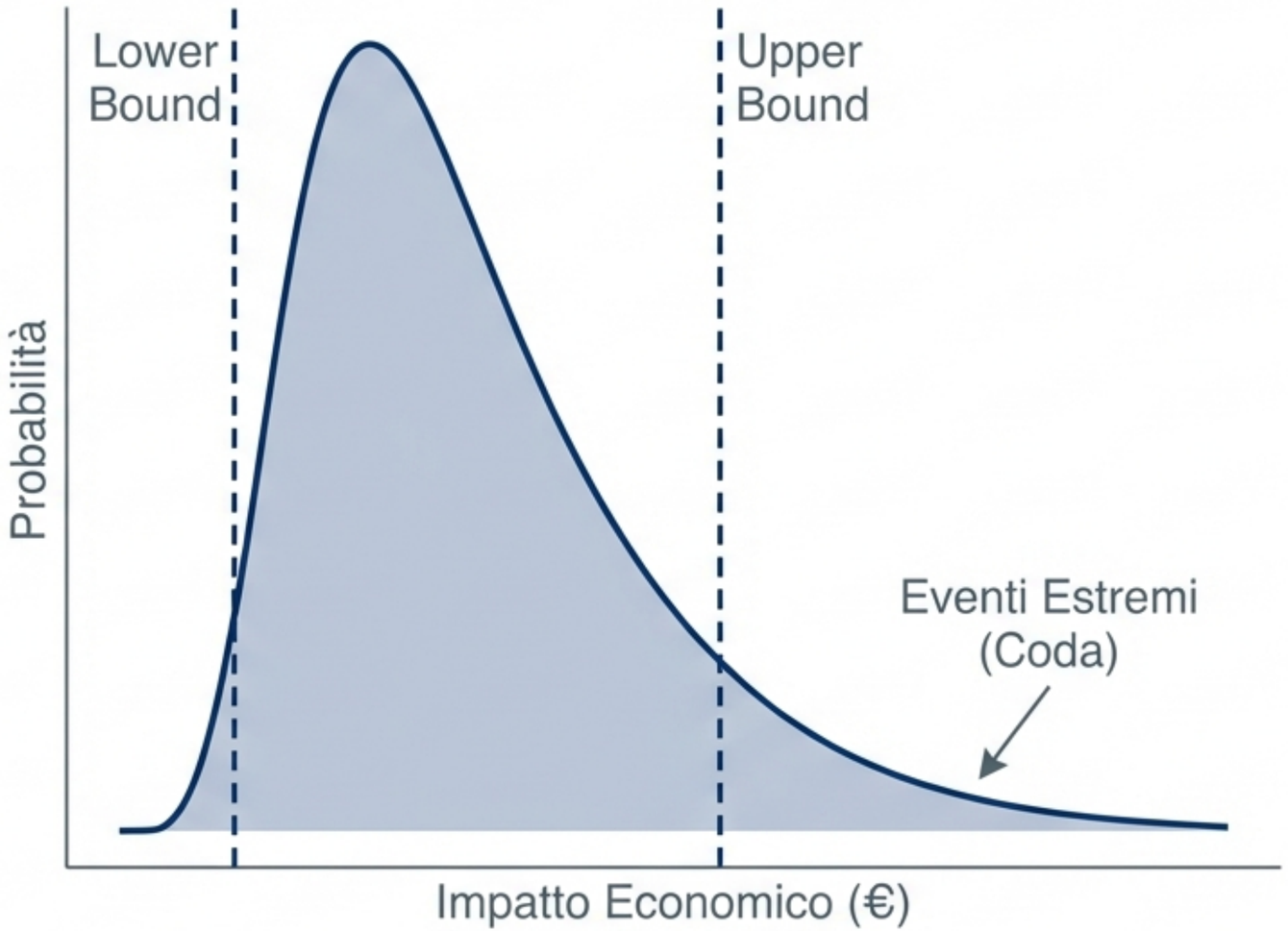


Questo processo determina se l’attacco ha successo nell’anno simulato.

Step 3: Modellazione dell'Impatto Economico

Se l'evento si verifica, il costo non è uniforme. I valori tendono a concentrarsi, con la possibilità di "code" estreme.

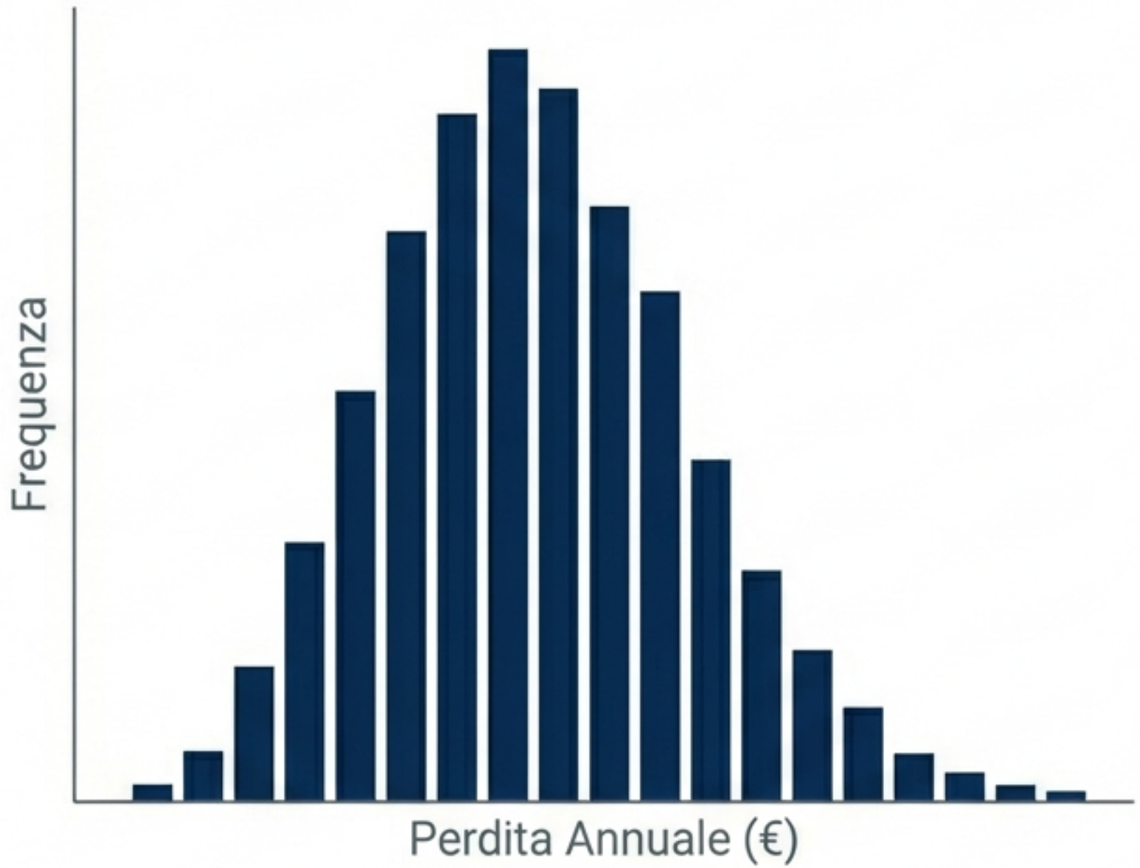
Distribuzione Log-Normale



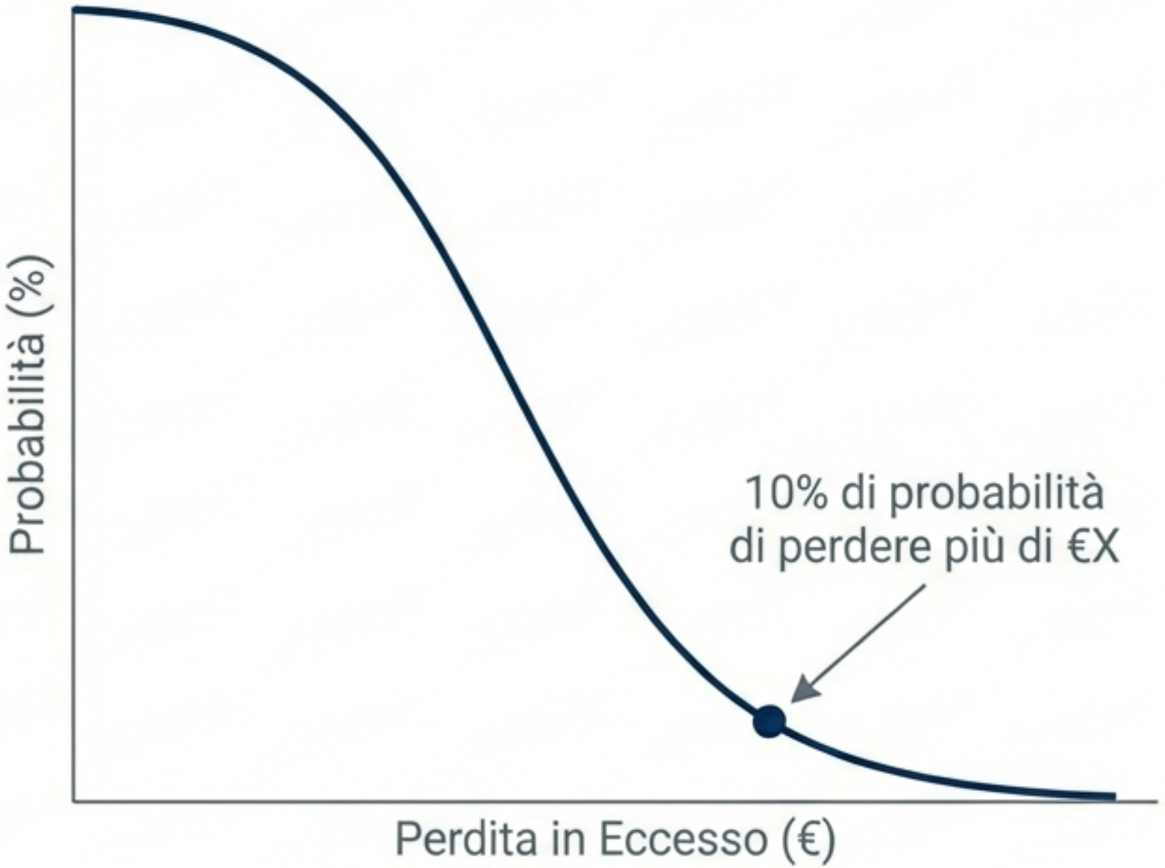
Il Motore di Calcolo: Rischio Totale Annuo

Step 4: Interpretazione dei Risultati (Output)

Istogramma delle Frequenze



Curva LEC (Loss Exceedance Curve)



Sintesi e Riferimenti Bibliografici

Il metodo HTMA trasforma l'opinione soggettiva in dati probabilistici, permettendo decisioni di business basate su scenari simulati e non su percezioni. L'approccio combina dati storici (CVE) con la calibrazione degli esperti e la potenza statistica della simulazione Monte Carlo.

Hubbard, D. W., & Seiersen, R. (2016). How to Measure Anything in Cybersecurity Risk. Wiley.

The MITRE Corporation (2024). CVE (Common *Vulnerabilities and Exposures*) Database. cve.mitre.org

[Nome Università]. Modulo 7: *Metodi Quantitativi per la Valutazione del Rischio.*