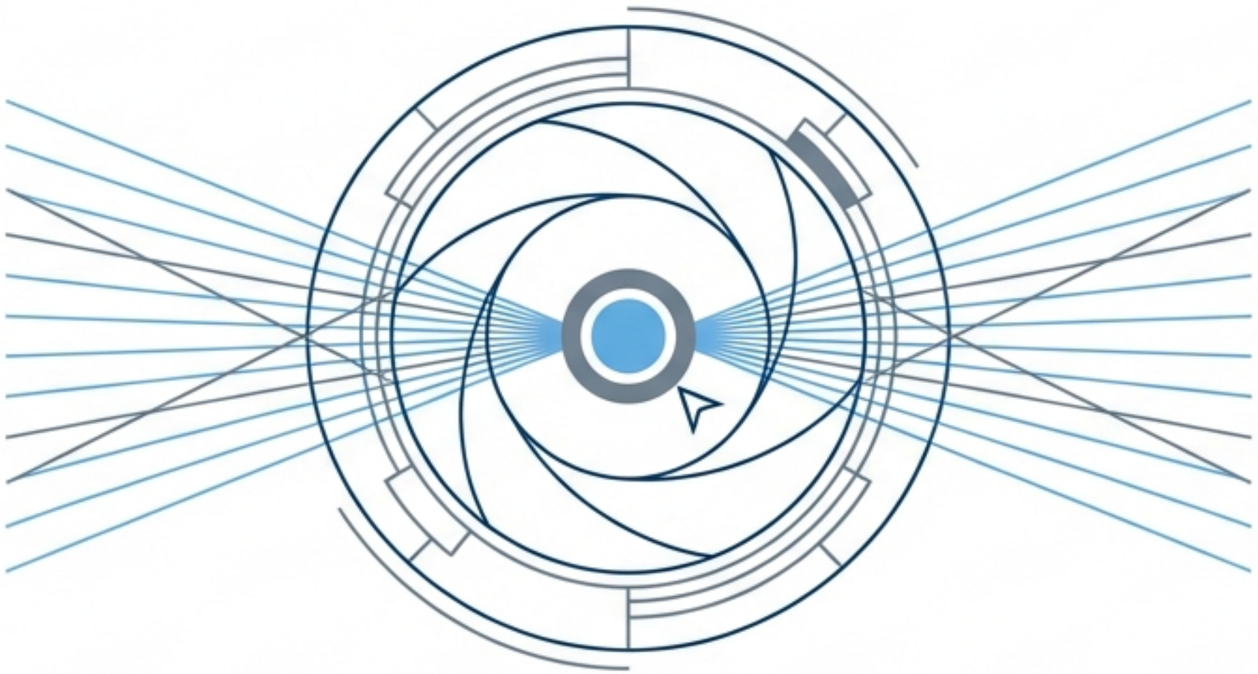
ISO/IEC 27004:2016



Tecnologie informatiche — Tecniche di sicurezza — Gestione della sicurezza delle informazioni — Monitoraggio, misurazione, analisi e valutazione

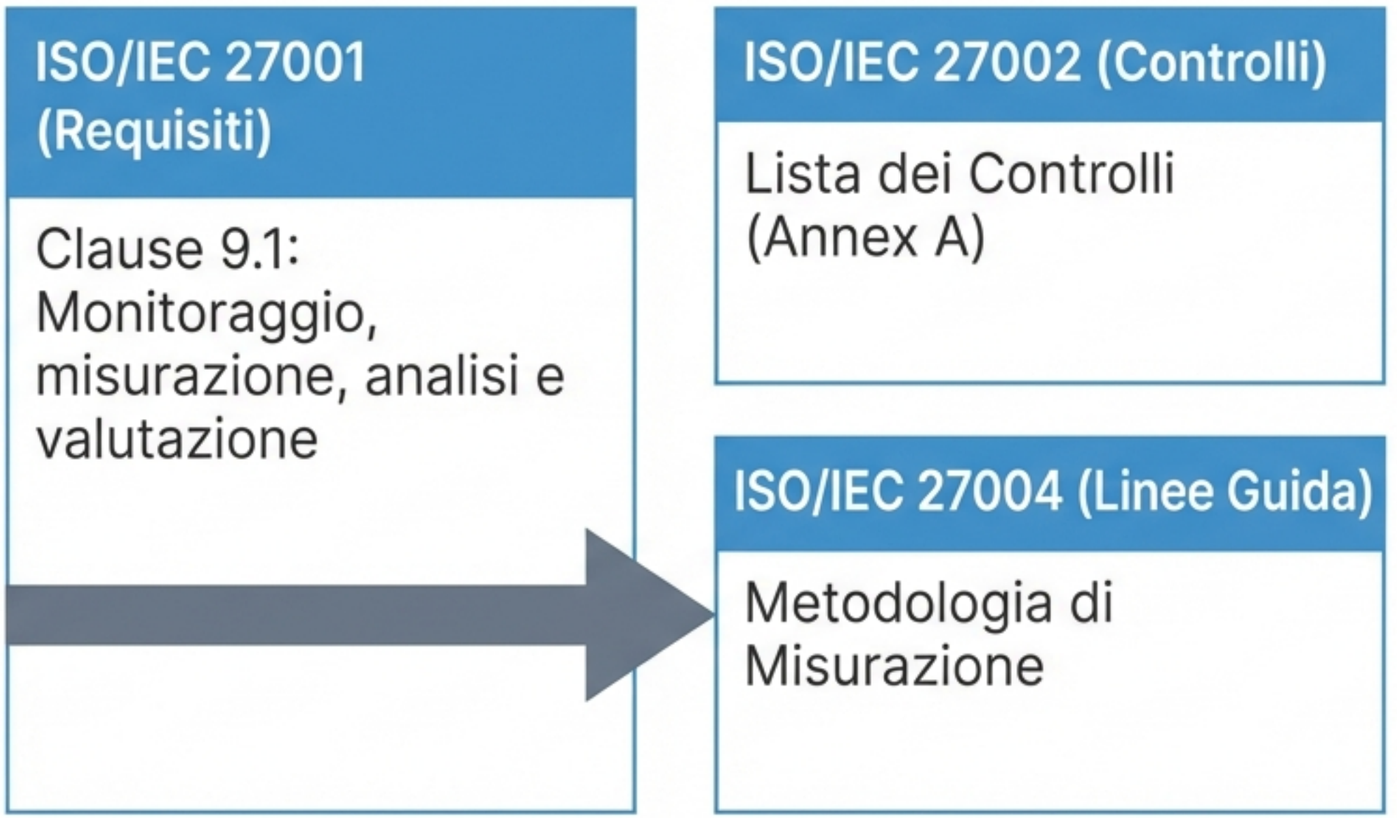
---

Metrologia della Sicurezza: Un approccio accademico alla misurazione dell'ISMS

Il Contesto Normativo: La Famiglia ISO 27000

ISO 27001 richiede CHE si misuri.

ISO 27004 spiega COME misurare.



Scopo e Razionale (Clause 5)

“Non si può gestire ciò che non si si può misurare.”

- **Validazione:** Confermare che i controlli siano implementati ed efficaci.
- **Responsabilità (Accountability):** Dimostrare la conformità agli stakeholder.
- **Decisioni informate:** Spostamento da opinioni soggettive a dati oggettivi per l’allocazione delle risorse.
- **Miglioramento continuo:** Identificare trend negativi prima che diventino incidenti.

Tassonomia e Definizioni Chiave (Clause 3)

Monitoraggio

Determinare lo stato di un sistema, processo o attività (processo continuo).

Misurazione

Processo per determinare un valore (fotografia puntuale).

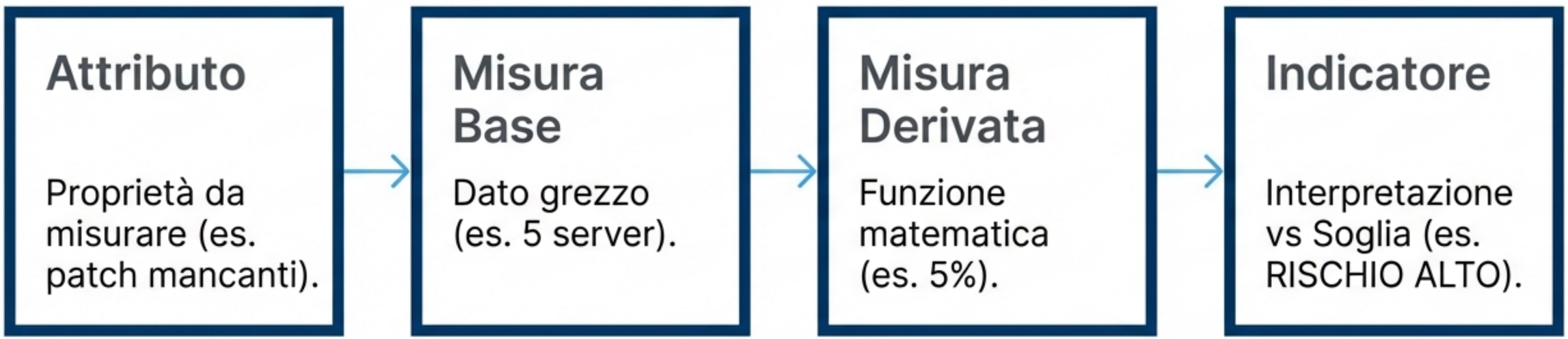
Analisi

Esame dei dati per individuare relazioni, tendenze e cause.

Valutazione

Confronto dei risultati con i criteri di rischio per determinare se gli obiettivi sono raggiunti.

Il Modello di Misurazione (Annex A)



Tipi di Misure (Clause 7)

Misure di Prestazione

Focus: Efficienza dell'implementazione.

Domanda: Stiamo facendo ciò che abbiamo pianificato?

Esempio: % di audit completati rispetto al piano.

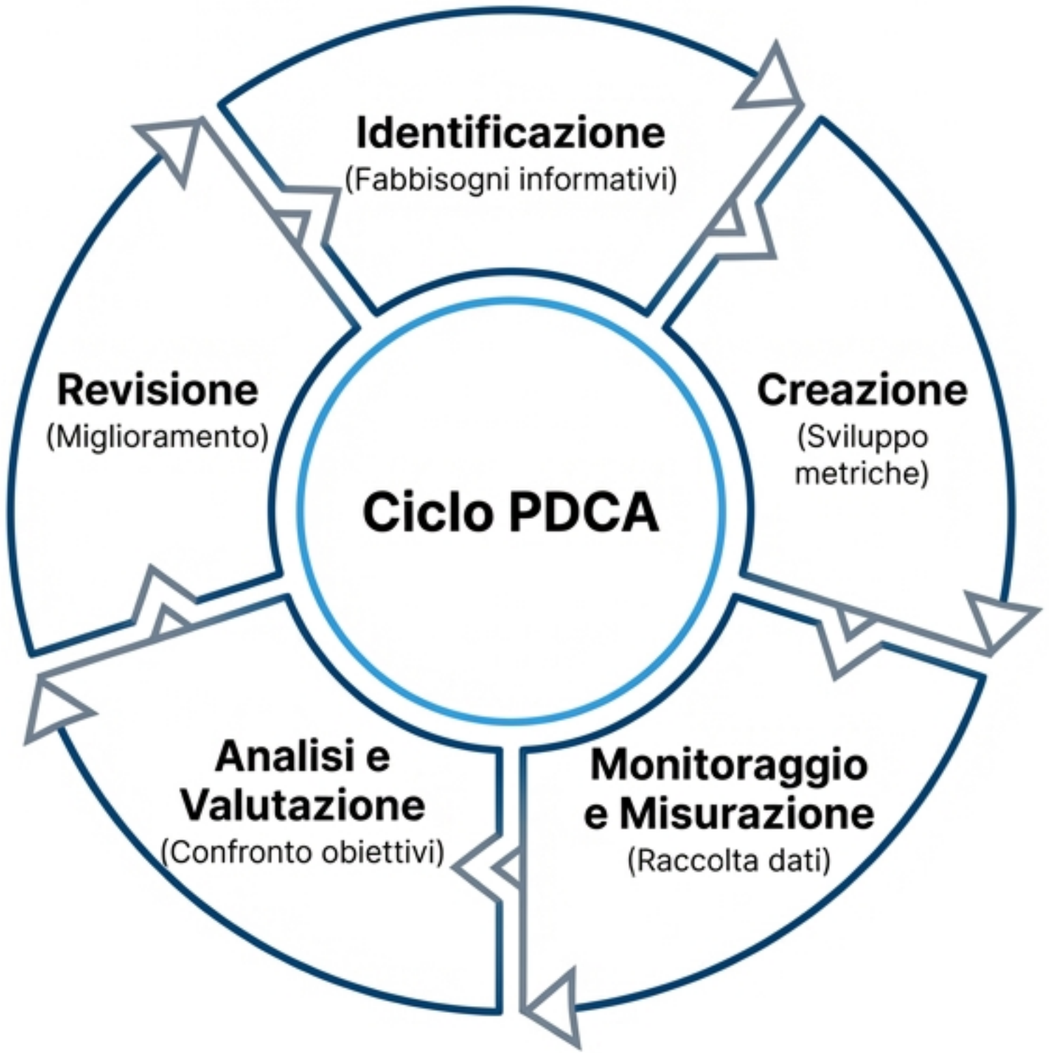
Misure di Efficacia

Focus: Risultato e riduzione del rischio.

Domanda: Le misure di sicurezza stanno funzionando?

Esempio: % di riduzione degli incidenti.

Il Processo di Misurazione (Clause 8)



Costrutto di Misurazione (Measurement Construct)

> La validità richiede riproducibilità: chiunque esegua la misura deve ottenere lo stesso risultato.

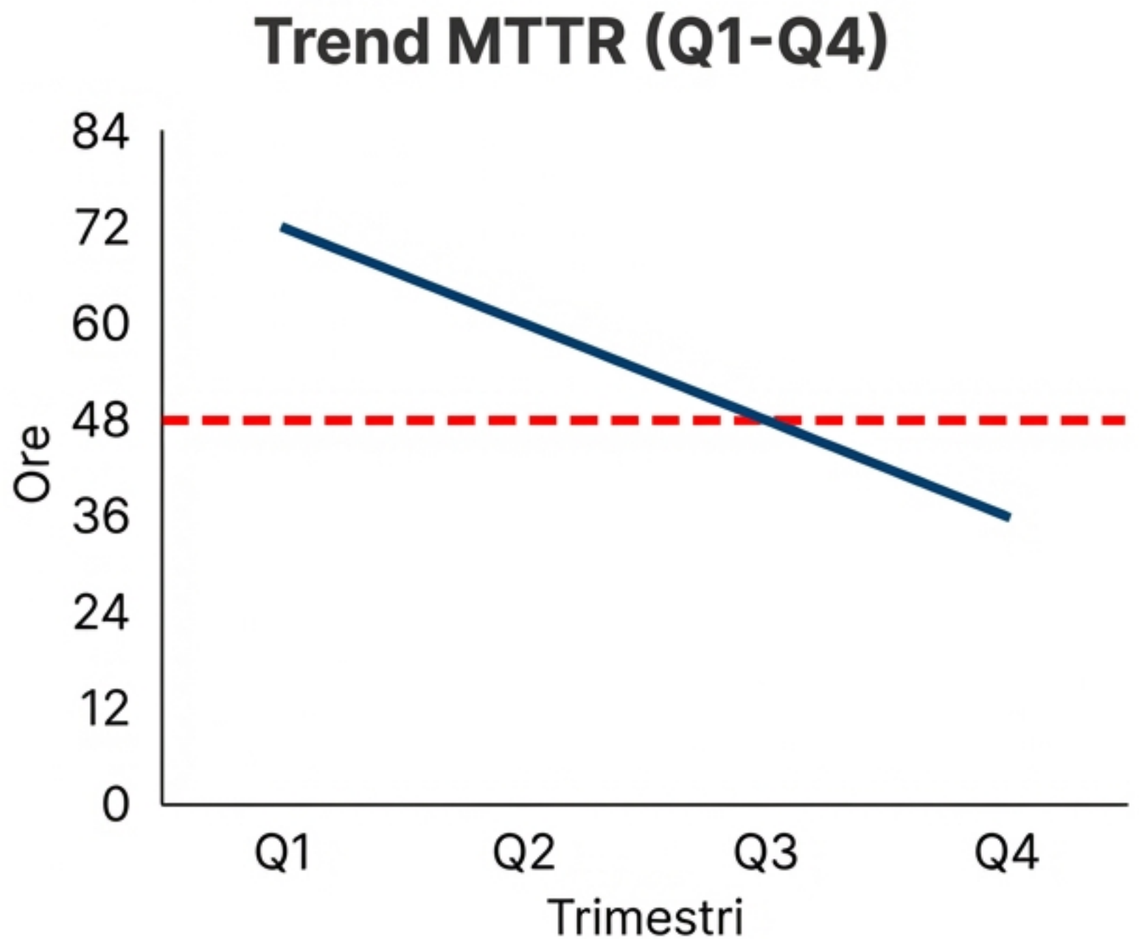
ID Misura:	M-042
Fabbisogno Informativo:	Cosa vogliamo sapere?
Oggetto della Misura:	Sistema Firewall
Formula:	Algoritmo di calcolo
Frequenza:	Mensile
Fonte Dati:	Log del SIEM
Soglia (Threshold):	< 99% = Allarme

Esempio Pratico: Gestione delle Vulnerabilità

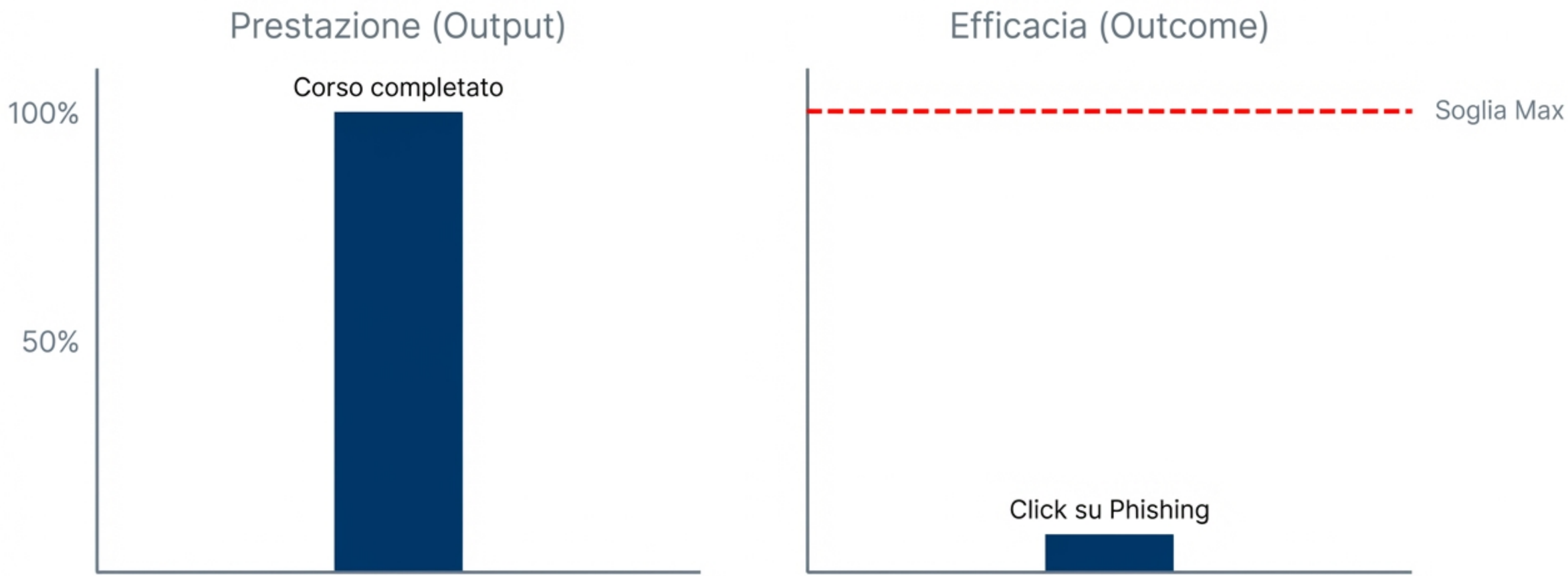
Misura Base: Numero di vulnerabilità critiche aperte.

Misura Derivata: Mean Time to Remediate (MTTR).

Soglia: Target < 48 ore.



Esempio Pratico: Consapevolezza (Awareness)



L'efficacia misura il comportamento reale, non solo la partecipazione.

Analisi e Valutazione dei Dati

Executive Dashboard

Patching	Incidenti	Training
		
In target	Fuori soglia (Azione Richiesta)	Attenzione

- Identificazione dei Trend: Il rischio aumenta o diminuisce?
- Analisi degli Outlier: Cause delle anomalie.
- Processo Decisionale: I dati rossi innescano azioni correttive (ISO 27001 Clause 10.1).

Ruoli e Responsabilità (Clause 9.1)

Sfide Comuni e 'Vanity Metrics'

Metriche di Vanità

Numeri positivi ma senza significato reale (es. '1M di attacchi bloccati').

Costo vs Valore

Il costo della misurazione non deve superare il valore dell'insight.

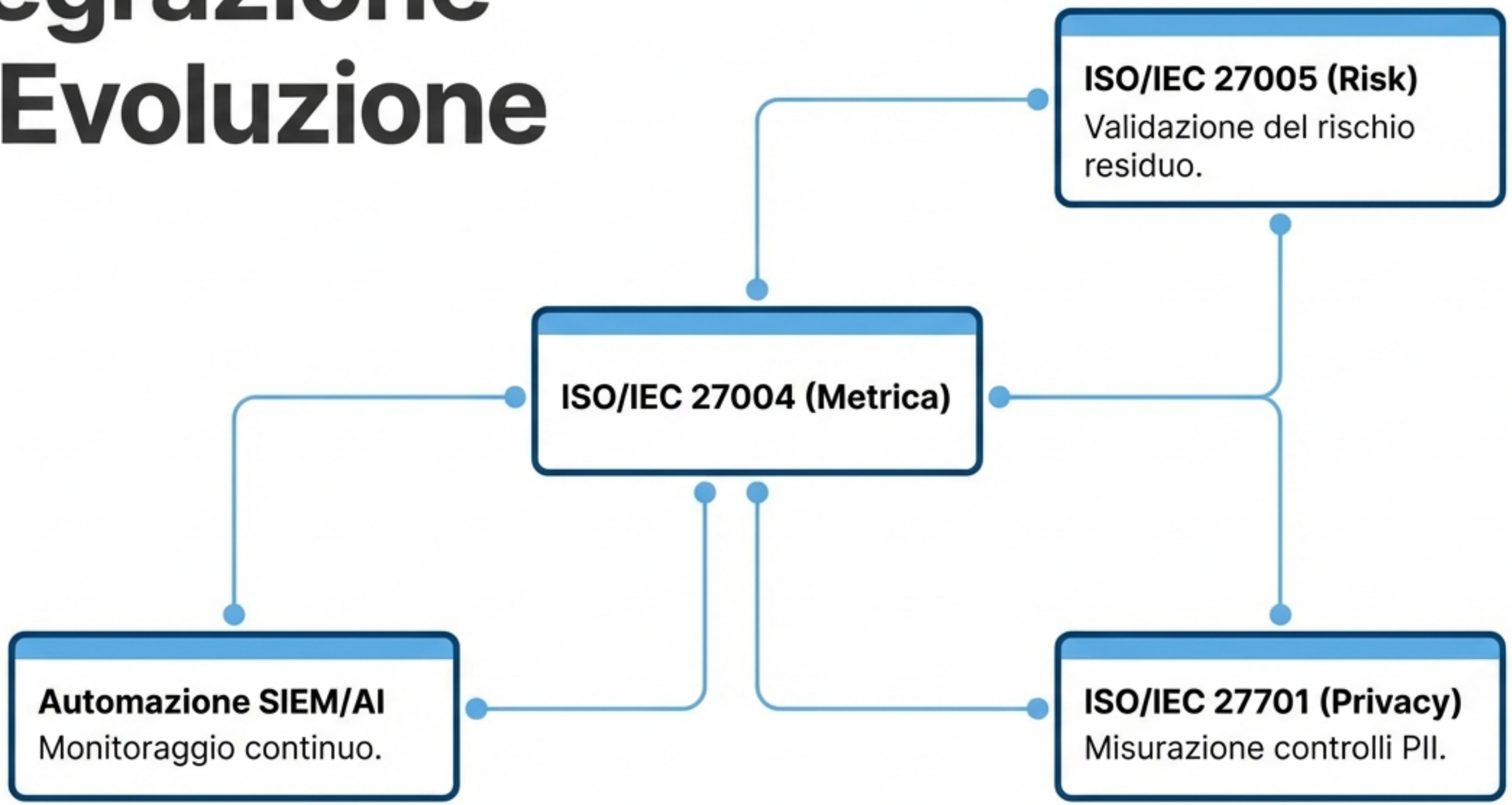
Soggettività

Evitare 'feeling' di sicurezza. Usare dati.

Integrità dei Dati

Garbage in, Garbage out.

Integrazione ed Evoluzione



Conclusione: Dall'Arte alla Scienza

1. ISO 27004 trasforma la sicurezza da arte soggettiva a scienza ingegneristica.

2. Fornisce l’evidenza oggettiva per la certificazione ISO 27001.

3. Passaggio dalla conformità alla resilienza.