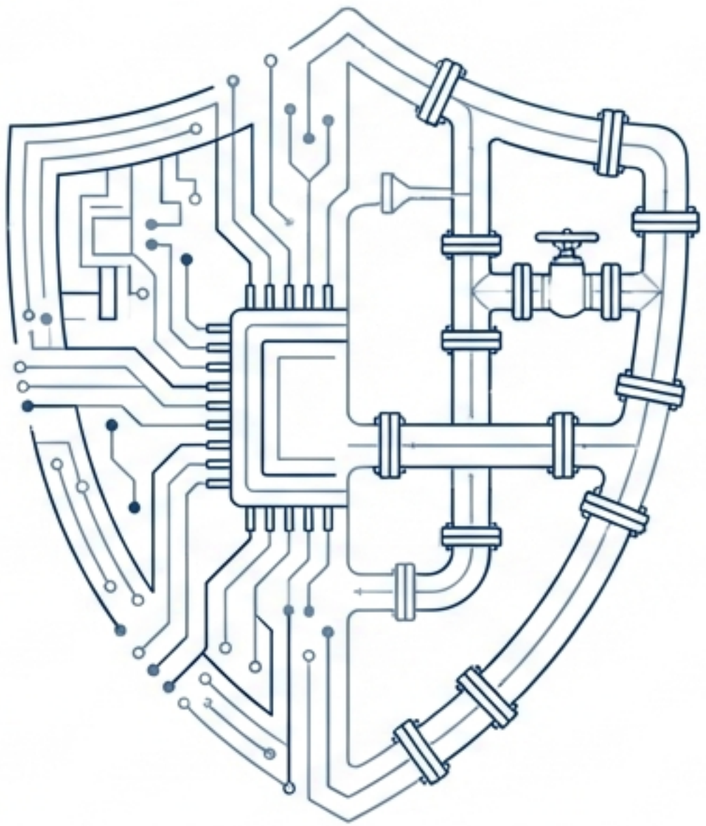
ISA/IEC 62443: Standard Globale per la Cybersecurity Industriale

Sicurezza dei Sistemi di Automazione e Controllo (IACS) – Struttura, Requisiti e Applicazioni

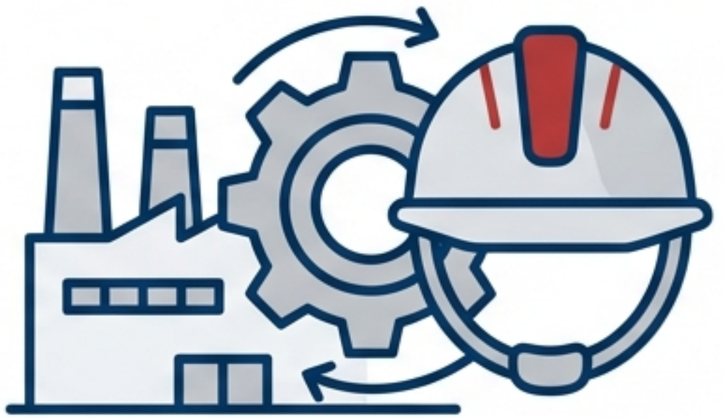


La Convergenza IT/OT e la Priorità della Sicurezza Fisica

IT - Enterprise

- **Focus**: Riservatezza (Confidentiality)
- **Protezione**: Dati e Proprietà Intellettuale
- **Conseguenza**: Perdita Finanziaria / Reputazione

OT - Industrial



- **Focus**: Disponibilità e Incolumità (HSE)
- **Protezione**: Processi Fisici, Persone, Ambiente
- **Conseguenza**: Danni Fisici, Stop Produzione, Impatto Ambientale

Mentre la **ISA/IEC 62443** protegge il **processo fisico** e le **persone**.

Definizione e Scopo: Cosa è un IACS?

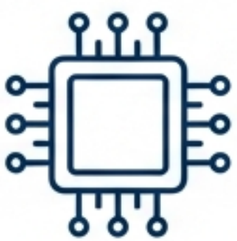
Un Industrial Automation and Control System (IACS) è una collezione di:

- **Persone:** Operatori, manutentori, fornitori
- **Processi:** Politiche, procedure, gestione del rischio
- **Tecnologia**: Hardware, software, reti (PLC, SCADA, DCS)

L’Ecosistema dei Ruoli: Una Responsabilità Condivisa

Asset Owner
Responsabile del rischio (CSMS) e dell’operatività.

System Integrator
Progettazione e integrazione della soluzione.



Product Supplier
Sviluppo sicuro (SDL) di hardware e software.

Ogni attore deve rispettare specifici documenti della normativa (es. 2-4 per i Service Provider, 4-1 per i Supplier)

L’Architettura della Normativa: I 4 Pilastri

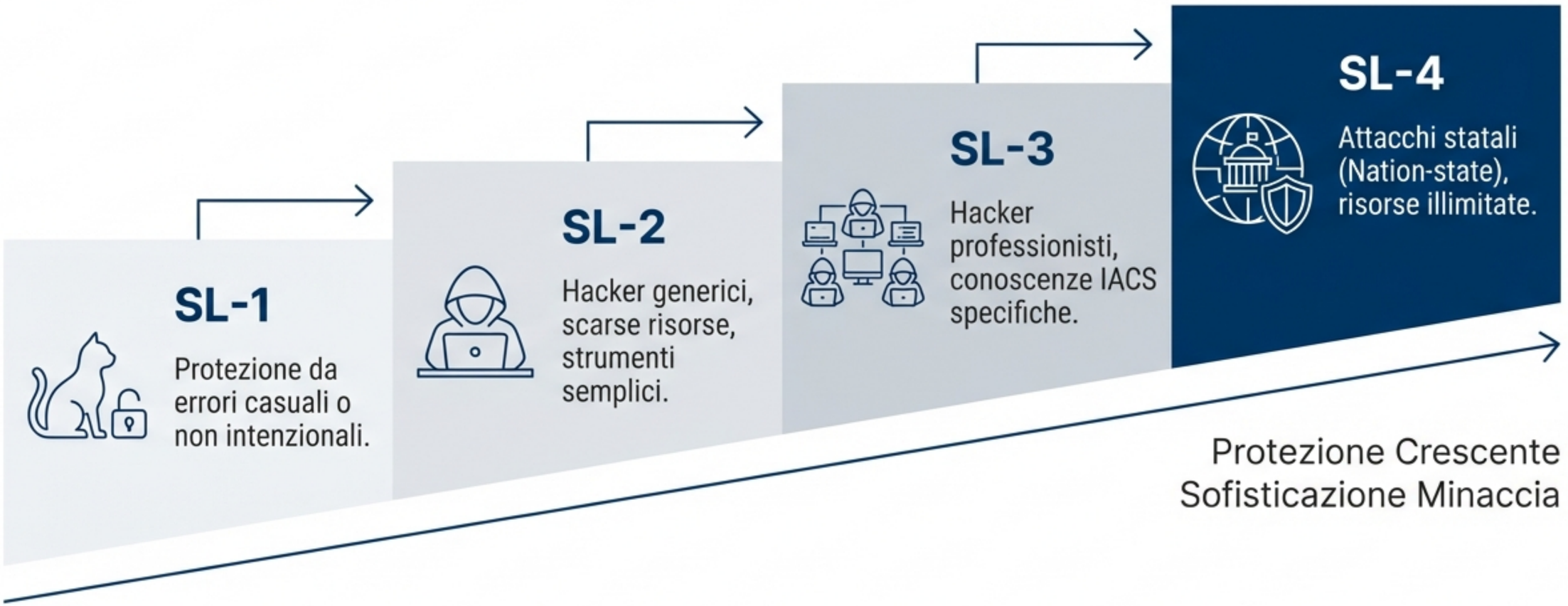
Component (4-X)
Ciclo di vita sviluppo prodotto (SDL) e specifiche componenti

System (3-X)
Requisiti di sistema, Risk Assessment e Security Levels

Policies & Procedures (2-X)
Programmi di sicurezza per Asset Owner e Service Provider

General (1-X)
Concetti, Modelli, Terminologia

Security Levels (SL): Lo Spettro della Protezione



"La protezione scala in base alla sofisticazione della minaccia."

La Matematica della Sicurezza: SL-T, SL-C, SL-A

$SL\text{-}A \geq SL\text{-}T$

SL-T (Target)

Il livello desiderato definito dal Risk Assessment.

SL-C (Capability)

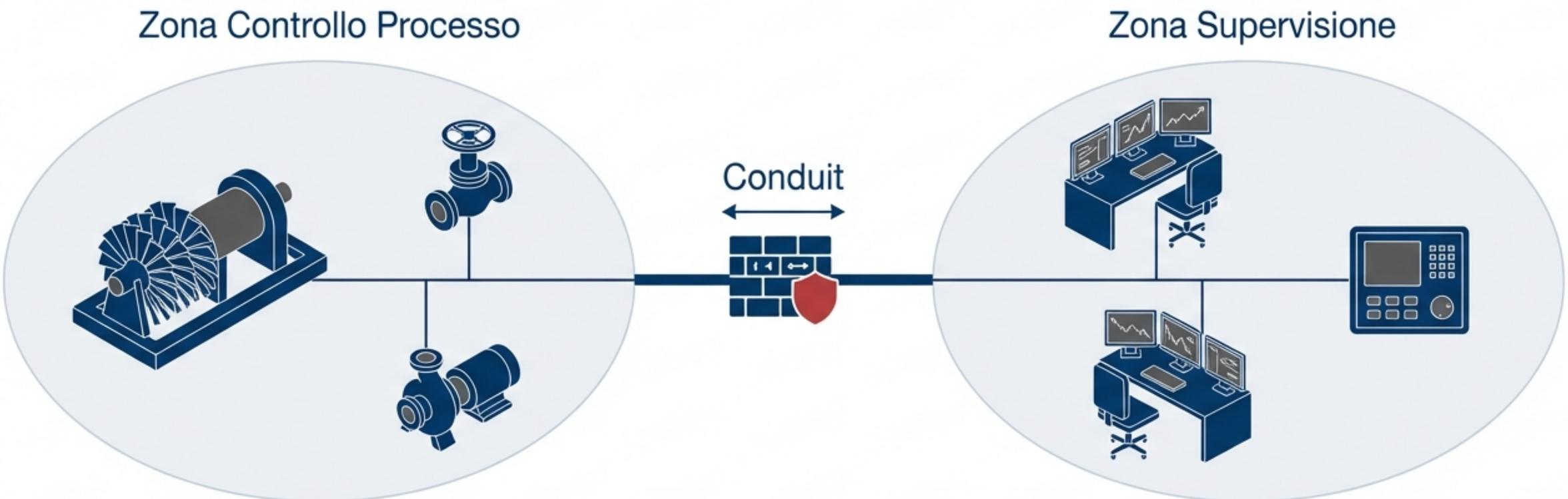
Il livello di sicurezza nativo del componente (offerto dal fornitore).

Misure Compensative (es. Firewall esterno)

SL-A (Achieved)

Il livello reale misurato post-installazione (incluse misure compensative).

Segmentazione Architetturale: Zones & Conduits



Zone: Raggruppamento di asset con requisiti di sicurezza simili.

Conduit: Canale di comunicazione controllato per il flusso dati.

I 7 Requisiti Fondamentali (Foundational Requirements)

FR 1 (IAC)

Identification & Authentication Control

FR 2 (UC)

Use Control

FR 3 (SI)

System Integrity

FR 4 (DC)

Data Confidentiality

FR 5 (RDF)

Restricted Data Flow

FR 6 (TRE)

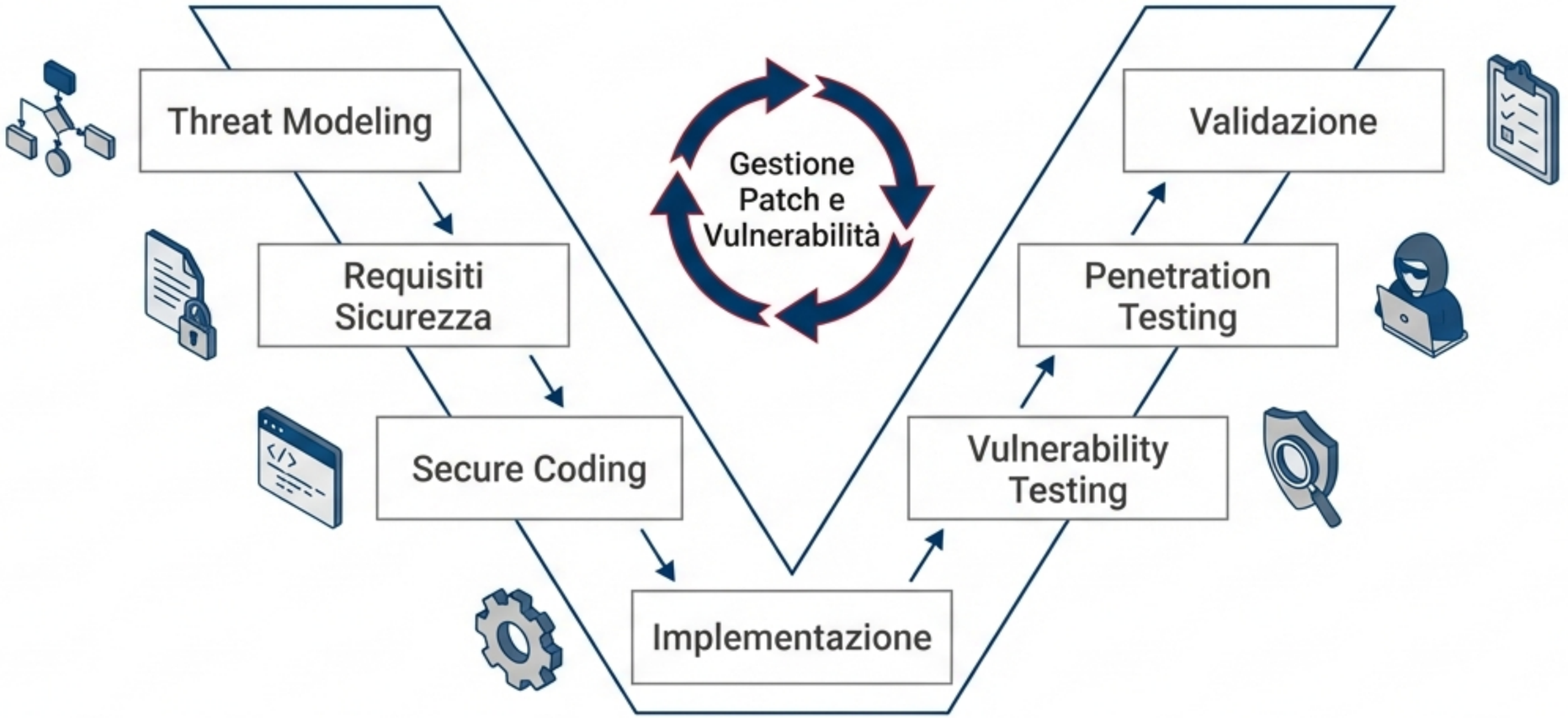
Timely Response to Events

FR 7 (RA)

Resource Availability

Focus Produttori: Secure Product Development Lifecycle (SDL)

Normativa di riferimento: ISA/IEC 62443-4-1



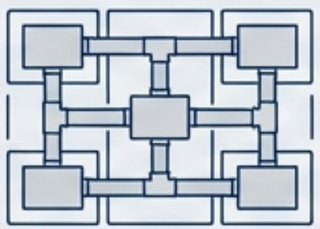
Secure by Design: La sicurezza integrata dal concepimento al ritiro.

Focus Asset Owner: Gestione del Rischio e CSMS

Normativa di riferimento: ISA/IEC 62443-2-1 e 3-2

High-Level Risk Assessment

Identificazione macro rischi



Partitioning

Divisione in Zone e Conduits

Detailed Risk Assessment

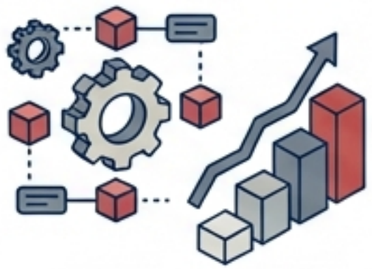
Assegnazione SL-T per zona

Cybersecurity Requirements (CRS)

Specifica requisiti ai fornitori

Evoluzione 2024-2026: I Nuovi Aggiornamenti

NEW



Nuova Edizione 2-1 (2024)

Introduzione dei “Security Program Elements” (SPE) e modelli di maturità per una gestione più flessibile.

NEW

Accesso Remoto e MFA

Requisiti obbligatori di Multi-Factor Authentication e monitoraggio live delle sessioni remote.

NEW

Gestione Sistemi Legacy

Uso formale di misure compensative per sistemi con ciclo di vita >20 anni.

Allineamento Normativo Europeo: CRA & NIS-2

La 62443 fornisce il framework tecnico per rispettare gli obblighi di legge europei.

Sfide Implementative e Best Practices

Ostacoli Principali

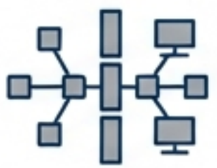
- Sistemi Legacy (20+ anni)

- Carenza di competenze OT

- Vincoli di budget e risorse

Best Practices

- Formazione continua del personale



- Segmentazione di rete aggressiva

- Monitoraggio continuo (non solo audit puntuali)

- Secure by Design nei nuovi acquisti

Conclusione: Un Viaggio Continuo

La sicurezza non è un prodotto, è un processo.