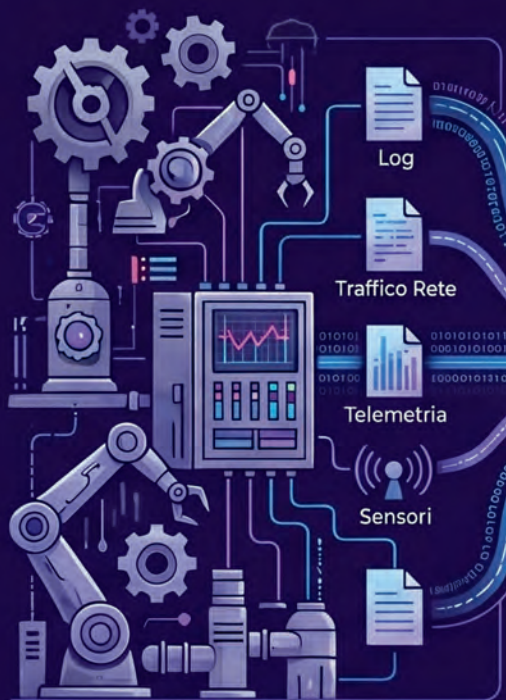


L'Intelligenza Artificiale nella Sicurezza OT: Dal Rilevamento alla Risposta

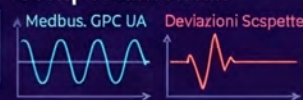
Acquisizione Dati e Segnali



Elaborazione IA: Rilevamento Intelligente e Correlazione



Rilevamento Anomalie Comportamentali



L'IA apprende il comportamento normale dei protocolli industriali (Modbus, OPC UA) per segnalare deviazioni sospette.



Correlazione Eventi Multi-Sorgente

Analisi in tempo reale di log, traffico di rete e telemetria per identificare attacchi multi-stadio complessi.



Riduzione dei Falsi Positivi

90% L'IA filtra fino al 90% degli alert irrilevanti, eliminando l'affaticamento da alert degli analisti.

Supporto al SOC e Risposta agli Incidenti



Triage e Investigazione Accelerata

Uso di assistenti AI (LLM) riduce i tempi di investigazione della causa radice del 67%.



Risposta Autonoma e Coordinata (SOAR)

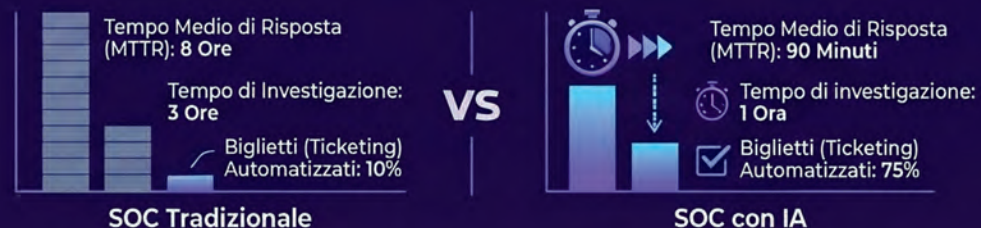
Esecuzione di playbook automatizzati per isolare asset compromessi e bloccare IP malevoli in pochi secondi.



Collaborazione Human-in-the-Loop

L'IA fornisce spiegazioni trasparenti (XAI) per permettere all'uomo di validare azioni critiche con fiducia.

Efficienza Operativa: SOC Tradizionale vs. SOC con IA



OT Fast Path: La Via Strategica alla Cybersecurity Industriale

Il **programma OT Fast Path** di Relatech trasforma la sicurezza tecnologica in valore industriale misurabile, integrando valutazione tecnica, formazione del personale e governance continua.

Fase 1: Valutazione e Competenze



OT Cybersecurity Evaluation

Un framework in quattro fasi: mappatura rete, assessment, valutazione del rischio e piani di remediation.



OT Security Training

Percorsi formativi (Essential e Advanced) per rendere il personale tecnico un livello di difesa fondamentale.



Secure Programming & AI

Laboratori pratici sulla programmazione sicura del PLC con supporto di logiche AI.

RELATECH®

Fase 2: Resilienza e Governance Continua



Incident Readiness

Esercitazioni tabletop e analisi forense per ridurre i tempi di risposta e i fermi impianto.

Virtual CISO & Resilient Platform

Governance del rischio in tempo reale e conformità semplificata alle normative NIS2 e IEC 62443.

Cybersecurity Investment Planning

Ottimizzazione del budget tramite analisi "what-if" per prioritizzare gli investimenti ad alto impatto.

Trust Indicators del Gruppo Relatech



Professionisti:
700+



Volume d'affari:
100 M€

•  **14 Sedi**
•  **9 Italia**
•  **5 Estero**

Cybersecurity OT: Da Opzione a Requisito Legale

Il Nuovo Quadro e i Rischi per il Management

La Security è un Requisito Fisico (CE)



Senza cybersecurity, un macchinario non è più considerato sicuro secondo il nuovo Regolamento Macchine.

Responsabilità Diretta e Sanzioni



Multe fino a **10 milioni** di euro o al **2%** del fatturato mondiale annuo.

La cybersecurity è soggetta a obblighi diretti di conformità, con sanzioni fino al 2% del fatturato mondiale annuo.

Rischio di Fermo Macchina Fisico



In ambito OT, un attacco informatico può causare downtime prolungati e la potenziale alterazione dei lotti produttivi.

Tre Pilastri Normativi Europei

		Impatto Chiave
NIS2		Obbligo di resilienza della supply chain e continuità
Regolamento Macchine		La Cybersecurity diventa requisito per la conformità CE
CRA		Obbligo di "Security by Design" per l'intero ciclo di vita

"Quick Wins" per la Resilienza OT



Cybersecurity Industriale: Dalla Conformità alla Resilienza Operativa

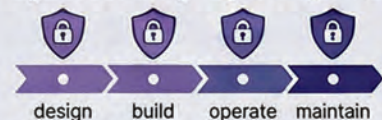
Il Nuovo Paradigma Normativo (MR & CRA)



Sicurezza Intrinseca e Obbligatoria

Il Regolamento 2023/1230 rende la cybersecurity un requisito di sicurezza essenziale per le macchine.

Cybersecurity "By Design" (CRA)

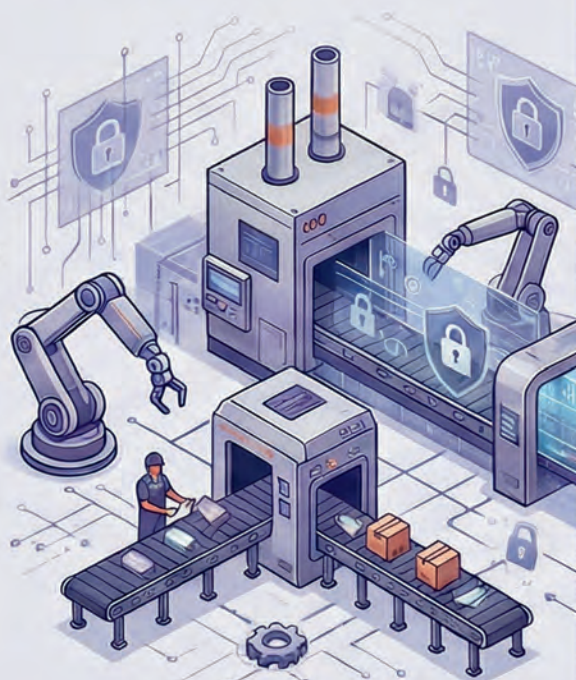


I prodotti devono essere sicuri lungo l'intero ciclo di vita, dalla progettazione alla manutenzione.



Responsabilità Condivisa OEM & Asset Owner

Produttori e utilizzatori devono collaborare per garantire la continuità operativa e la conformità.



OT Cybersecurity Evaluation & Risk Assessment



Mappatura reti e valutazione del rischio basata sugli standard IEC 62443 e NIS2.

Panoramica dell'impatto industriale di Relatech Cloudsecurity.

Professionisti



>100
Esperti in Cybersecurity

Esperienza SOC

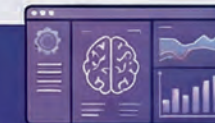


>150
Clienti MDR gestiti

Certificazioni



>200
Certificazioni Individuali



Virtual CISO & Resilient Platform

Piattaforma GRC per il controllo del rischio in tempo reale e pianificazione investimenti.



Incident Readiness & Training

Formazione specialistica (PLC, Cyber Hygiene) ed esercitazioni tabletop per una risposta rapida agli incidenti.