



# Security Summit OT

Milano 24 settembre 2026



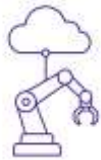
## **Chi comanda in fabbrica? Governare gli accessi OEM tra attacchi OT e continuità operativa**

**Vincenzo Marrone** | Cyber Security Senior Consultant @Deda Tech

**deda.tech**

# L'illusione dell'Air-Gap e la fabbrica iperconnessa

Per vent'anni, una frase ha fatto dormire sonni tranquilli a generazioni di direttori di stabilimento: *"I nostri macchinari non sono su Internet."* Oggi dobbiamo dircelo con franchezza: **l'Air-Gap è morto.**



## La trasformazione silenziosa

Con **Industria 4.0** e la spinta all'efficienza post-Covid, robot, PLC, azionamenti, HMI e quadri elettrici comunicano oggi con l'esterno per manutenzione predittiva e teleassistenza remota.



## La fabbrica nel Cyberspazio

Lo stabilimento non è più un'isola d'acciaio recintata: è diventata un'**estensione del cyberspazio aziendale**, connessa a fornitori, OEM e reti IT aziendali.



## La differenza fondamentale dall'IT

Se salta una casella di posta, l'impiegato aspetta. Se salta un controllore in fabbrica, si ferma il fatturato, si perde il prodotto e si mette a rischio l'**incolumità fisica** delle persone.



## Chi ha davvero il controllo?

Accessi di teleassistenza permanenti, responsabilità poco definite e canali paralleli nascosti aumentano il rischio anziché ridurlo. La domanda centrale: **chi governa gli accessi alle macchine?**

# Dalla teoria alla cronaca: quando il Cyberattacco spegne gli stabilimenti

Non stiamo parlando di rischi teorici o scenari da film di spionaggio. Guardiamo la cronaca recente del manifatturiero italiano tra fine 2024 e i primi mesi del 2025.

| Settore                                 | Impatto Operativo Reale                                                                |
|-----------------------------------------|----------------------------------------------------------------------------------------|
| Azienda di arredo di design             | Impianti completamente paralizzati; linee robotizzate spente per oltre una settimana.  |
| Impianto di meccanica di precisione     | Commesse bloccate, penali salatissime verso i clienti della filiera Just-in-Time.      |
| Fabbrica di componentistica industriale | Centinaia di operai in cassa integrazione forzata; milioni di euro di danni operativi. |

Quando un ransomware o un sabotaggio colpisce la produzione, la sicurezza logica diventa all'istante un **problema sociale, economico e contrattuale**. Chi risponde di queste perdite?



# La tempesta normativa alle porte: NIS2, CRA e Regolamento Macchine

Nel 2026 le normative europee segnano un cambio di paradigma definitivo: la responsabilità legale della sicurezza dello stabilimento e della supply chain ricade esplicitamente su **CISO e organi di vertice**.

## NIS2

Sposta la responsabilità legale della resilienza e della sicurezza dell'intera **Supply Chain** sul **CISO** e sugli organi di vertice aziendale.

## IEC 62443

Framework internazionale di riferimento per la **cybersecurity industriale**: Zones, Conduits e Security Levels per gli impianti OT.

## Cyber Resilience Act

Impone standard stringenti di sicurezza **"by design"** e supporto continuo lungo **tutto il ciclo di vita** dei dispositivi OT hardware e software connessi.

## Reg. Macchine UE 2023/1230

La cybersecurity diventa un **requisito essenziale di salute e sicurezza funzionale** della macchina stessa, non un'opzione aggiuntiva.

La legge dice chiaramente: *"Sei tu il responsabile legale della sicurezza del tuo stabilimento e dei terzi che vi accedono."* Ma qui esplode il primo vero paradosso di fabbrica...

# Il Ricatto dell'OEM: Chi comanda davvero sui macchinari?

Mentre la legge assegna la responsabilità al CISO, in reparto si consuma ogni giorno **il ricatto dell'OEM**. Il costruttore del macchinario milionario impone la sua regola contrattuale: *"Se tocchi le impostazioni di rete o non mi lasci la teleassistenza aperta H24, decade la garanzia."*

| Il Nodo                         | Il Problema Operativo                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------|
| Accesso Just-in-Time            | Canali permanenti (AnyDesk, TeamViewer, modem 4G) nascosti nelle canaline dei quadri elettrici                |
| Session Recording e Audit Trail | Nessuna tracciabilità su cosa il manutentore esterno ha fatto durante la sessione remota e chi si è collegato |
| Zero Impatto sulla Macchina     | Qualsiasi agente installato a bordo rischia di far decadere la garanzia del costruttore                       |



# Soluzione Deda Tech: Remote access & PAM industriale

Trasformiamo la teleassistenza da un rischio incontrollato a un vantaggio di governance, restituendo all'azienda la piena sovranità sugli accessi ai propri asset produttivi.



## 1. Accesso JIT e minimo privilegio

Nessun fornitore mantiene accessi permanenti. L'apertura avviene solo su richiesta esplicita, con autorizzazione del Plant Manager limitato al singolo asset coinvolto o per un periodo pre-concordato.



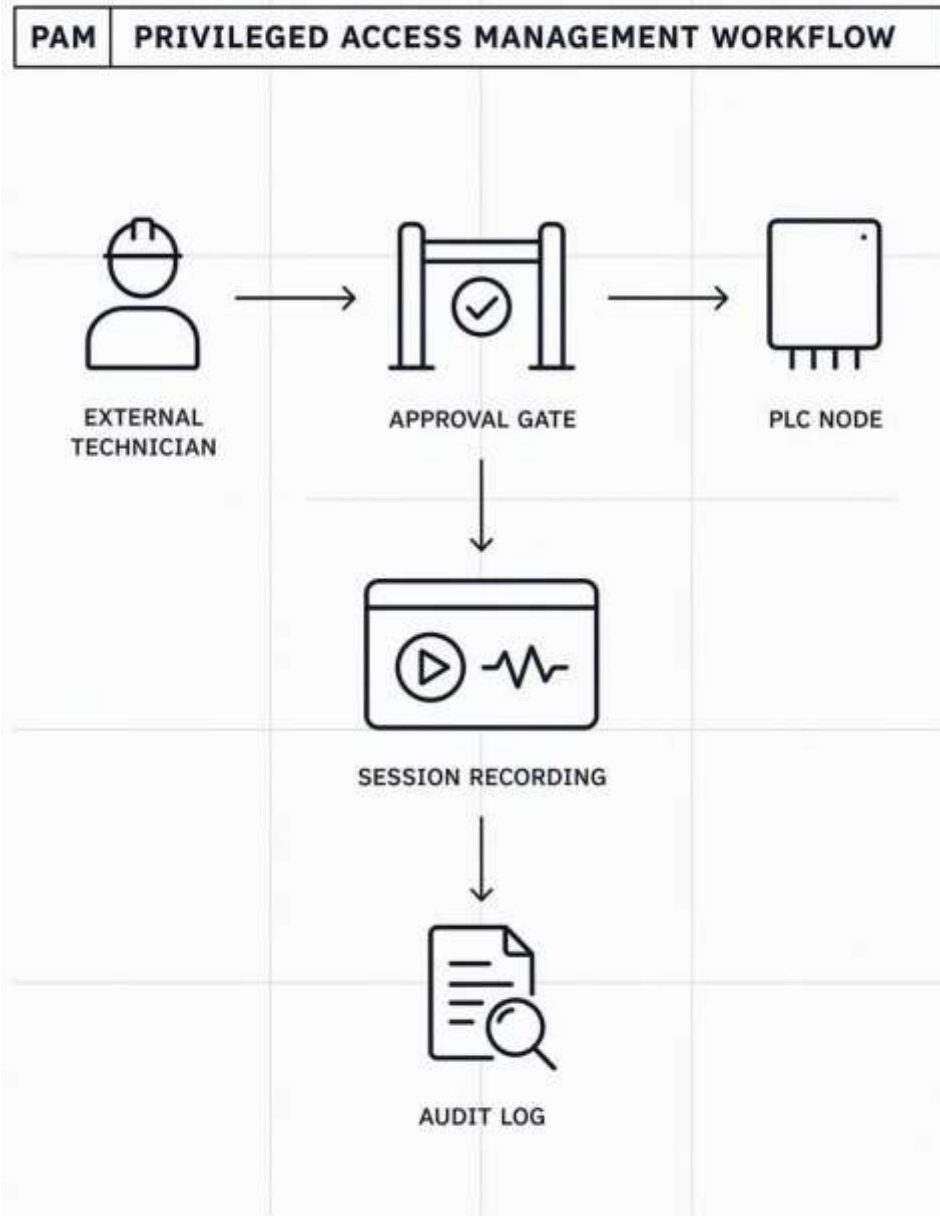
## 2. Session recording e revoca immediata

Ogni sessione è registrata integralmente (video + comandi). L'accesso è revocabile in tempo reale. Il log è immutabile e disponibile per audit di compliance NIS2 e CRA.



## 3. Garanzia OEM preservata

Il portale opera a livello di canale di rete, senza installare software invasivo a bordo macchina. Abbiamo dimostrato sul campo che soddisfa sia l'OEM sia il CISO, azzerando il rischio di decadenza della garanzia.



# Visibilità e rischio reale: cosa rischia davvero l'imprenditore?

## ⚠ Il Problema

**Non si può proteggere ciò che non si conosce.**

Quando chiediamo quanti asset industriali possiede un'azienda, la risposta tiene conto solo dei grandi macchinari a catalogo.

PLC legacy, switch industriali, sensori, inverter e HMI rimangono invisibili — e quindi non aggiornati, non monitorati e vulnerabili a movimenti laterali in caso di intrusione.

## ✓ La Risposta

**Servizi di OT Security Startup e Asset Management di Deda Tech:** mappatura passiva e automatica dell'intero perimetro OT, senza impattare la disponibilità degli impianti.

L'output non è un elenco informe di CVE: è un **Assessment Report e Remediation Plan** che traduce il gergo tecnico in priorità di business — cosa può fermare la produzione oggi e cosa è già protetto da misure compensative.

# Fare leva sui fornitori: dalla subalternità agli SLA di sicurezza

Una volta ottenuta la visibilità delle vulnerabilità, l'azienda smette di subire i fornitori e acquisisce **potere negoziale concreto** sulla propria supply chain OT con il fine di diminuire il rischio.



## SLA di manutenzione e patching

Grazie ai vincoli NIS2 e CRA, possiamo pretendere contrattualmente dai costruttori finestre di rilascio di patch testate e certificate per il software di controllo, con SLA definiti e verificabili.



## Responsabilità e rischio residuo condivisi

Definiamo contrattualmente ruoli, autorizzazioni, procedure di escalation e ownership del rischio residuo tra azienda, OEM e manutentori terzi, rendendo esplicito chi risponde di cosa.



## Micro-segmentazione e misure compensative

Se un PLC legacy non è aggiornabile dall'OEM, interveniamo con il modulo **Network Guarding** di Deda Tech con particolare attenzione all'isolamento in zone di sicurezza (IEC 62443: Conduits & Zones) per rilveare movimenti laterali.

# Il SOC che capisce la fabbrica: monitorare l'OT senza fermare la produzione

Collegare i log e i pacchetti di rete industriale a un SOC IT generico crea il **caos operativo e tanto rumore**. Un normale pacchetto PROFINET o Modbus viene etichettato come "tentativo di attacco DDoS", e l'analista SOC chiama i responsabili di impianto alle 3 di notte per una routine di backup del PLC.

## La differenza chiave

Non cerchiamo il virus da computer, ma l'anomalia di processo e la perdita di integrità operativa.

## Il modello Deda Tech

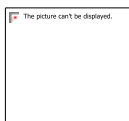
Figure specializzate (OT Security Architect e OT Security Expert) con contesto produttivo reale.

## La prima domanda del SOC

"Qual è l'impatto sul processo produttivo se blocchiamo questo flusso di traffico anomalo?" — non l'isolamento distruttivo dell'host.

# Playbook Deda Tech: monitoraggio ibrido IT/OT

Interveniamo solo quando la minaccia è reale, con procedure concordate con i responsabili di stabilimento, salvaguardando la continuità operativa e la sicurezza delle persone.



## 1. Correlazione con il contesto produttivo

Sappiamo distinguere una variazione di parametri in turno di produzione da un comando anomalo inviato fuori orario. Il monitoraggio è calibrato sul processo, non su firme antivirus generiche.



## 2. Playbook di triage OT

Avendo piena visibilità sul contesto dell'asset il SOC non effettua interventi al buio. Prima di qualsiasi azione, concorda con il referente di stabilimento la strategia di mitigazione: es. escalare l'ingaggio verso il fornitore/OEM oppure applicare misure di hardening compensativo non bloccanti per la produzione.



## 3. Procedure concordate con lo stabilimento

Ogni piano di risposta agli incidenti è definito preventivamente con i responsabili di produzione. Nessuna azione viene eseguita senza validazione dell'impatto operativo e sulla sicurezza fisica.

# Conclusione: riprendere il controllo della fabbrica

La convergenza tra IT e OT non è un pericolo da evitare, ma un'opportunità da governare. Proteggere la fabbrica moderna non significa blindare le macchine fino a renderle inservibili, né accettare passivamente contratti di teleassistenza insicuri.

| Il Nodo Critico             | La Risposta Deda Tech                                                                                                                       |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Accessi OEM incontrollati   | PAM Industriale Just-in-Time con session recording, accesso minimo e revoca immediata — senza toccare il software a bordo macchina.         |
| Invisibilità degli asset OT | Mappatura passiva automatica, Assessment Report e Remediation Plan prioritizzato per impatto sul processo produttivo.                       |
| Supply chain non governata  | SLA di manutenzione e patching negoziati con leva normativa (NIS2/CRA); micro-segmentazione IEC 62443 per i legacy non aggiornabili.        |
| SOC IT cieco al processo OT | Monitoraggio ibrido IT/OT process-aware con playbook di triage che valuta sempre prima l'impatto sulla produzione e sulla sicurezza fisica. |





# Grazie

**Venite a trovarci al desk!**

**deda.tech**