OPENINDUSTRIA
OSSERVATORIO DI CULTURA INDUSTRIALE

CISINT
Centro Italiano di Strategia e Intelligence

BLACK PAPER · N. 01 · NOVEMBRE 2026

Dai frigoriferi agli aeroporti: come si difende un sistema cyber-fisico

Architetture, vettori d'attacco, difesa in profondità e risposta all'incidente

a cura di Marco Pugliese

ORCID 0009-0007-7518-4405

TLP:CLEAR

OPENINDUSTRIA × CISINT · RAPPORTO TECNICO
Dati aggiornati al 6 novembre 2026

Premessa

Un banco frigo e un banco check-in sono sistemi cyber-fisici: un comando software produce un effetto materiale. Difenderli significa impedire che un accesso remoto illegittimo arrivi al setpoint, all'attuatore, al processo.

Gli incidenti alla refrigerazione commerciale europea dell'ottobre-novembre 2026 e il ransomware contro la piattaforma MUSE di Collins Aerospace del settembre 2025 mostrano due vie d'ingresso ricorrenti: interfacce di gestione esposte su Internet e fornitori condivisi dotati di accesso privilegiato. Le contromisure più efficaci sono note e verificabili: inventario degli asset, eliminazione dell'esposizione diretta, accesso remoto da un solo punto controllato con autenticazione a più fattori e sessioni registrate, segmentazione per zone e condotti secondo IEC 62443, protezioni di sicurezza indipendenti dal software, backup immutabili e ripristino collaudato. Il failover è la risposta corretta al guasto; quando il sistema è compromesso serve la gestione dell'incidente, altrimenti si replica l'attaccante sul sistema di riserva.

73%
casi di incident response Dragos con credenziali VPN o jump host compromesse

81%
organizzazioni valutate nel 2025 con segmentazione IT/OT inadeguata

42 gg
permanenza media del ransomware in OT; 5 giorni con piena visibilità

+61%
incidenti ransomware industriali, T1 2025 → T2 2026

PARTE I

Come è fatto un sistema cyber-fisico

Il riferimento è l'architettura a livelli derivata dal modello Purdue (ISA-95). Al livello 0 stanno sensori e attuatori: sonde di temperatura, valvole di espansione elettroniche, compressori, nastri bagagli. Al livello 1 i controllori (PLC, regolatori di banco e di centrale frigorifera), che eseguono la regolazione in tempo reale. Al livello 2 la supervisione di sito (SCADA, BMS; nella refrigerazione commerciale i system manager come Danfoss AK-SM o le piattaforme StoreView), che legge le misure, modifica i parametri e gestisce gli allarmi. Al livello 3 i servizi operativi; sopra, la rete aziendale, il cloud del fornitore e Internet. Tra IT e OT va interposta una DMZ industriale con jump host, server di aggiornamento e replica dei dati storici: nessuna sessione deve attraversarla senza terminare su un sistema intermedio controllato.

In ambito OT la triade riservatezza-integrità-disponibilità ha priorità invertite rispetto all'IT: contano prima la disponibilità e l'integrità del processo, poi la riservatezza del dato. Molti protocolli di campo (Modbus/TCP, BACnet/IP, protocolli seriali proprietari) non autenticano i comandi: chi raggiunge la rete del controllore può spesso leggere e scrivere registri, compresi i setpoint. Le varianti sicure (BACnet/SC, Modbus/TCP Security, OPC UA con certificati) richiedono controllori recenti; nel parco installato la prima barriera è quindi il perimetro logico, non il protocollo.

Un aeroporto replica lo schema su scala maggiore: piattaforme common-use (CUTE/CUPPS) per banchi check-in e gate, departure control system delle compagnie, smistamento bagagli (BHS) governato da PLC, controllo accessi e building automation. Molte funzioni sono erogate in modalità condivisa o in cloud

da pochi fornitori: un'efficienza che concentra il rischio, perché un singolo fornitore diventa un punto di guasto comune per decine di scali.

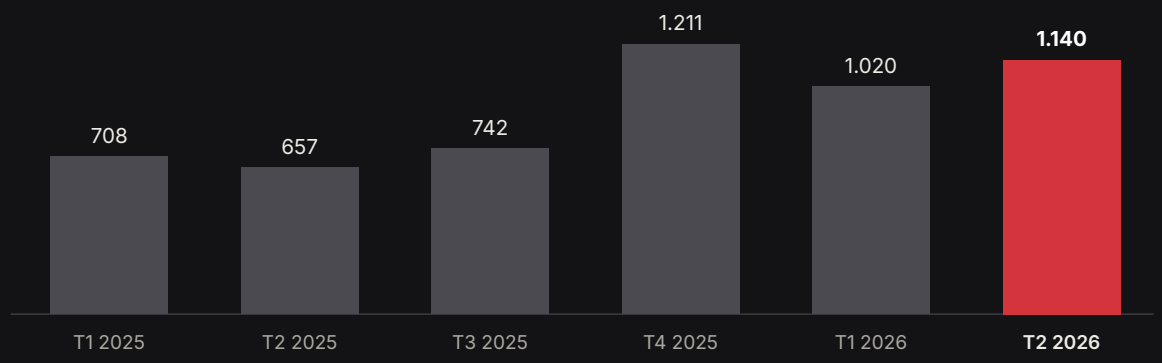
PARTE II

Superficie d'attacco e vettori

La minaccia cresce in volume e si concentra sugli accessi. Nei casi di incident response di Dragos il 73% ha coinvolto credenziali compromesse di VPN o jump host; nelle valutazioni del 2025 l'81% delle organizzazioni aveva una segmentazione IT/OT inadeguata e solo il 46% un monitoraggio adeguato della rete OT. Il tempo medio di permanenza del ransomware negli ambienti OT è stato di 42 giorni, contro 5 nelle organizzazioni con piena visibilità.

Il ransomware contro organizzazioni industriali cresce del 61% in sei trimestri

Incidenti per trimestre, vittime rivendicate o divulgate



Conteggi minimi: vittime pubblicate sui siti di leak o divulgate, non il totale degli attacchi.

Fonte: Dragos, Industrial Ransomware Analysis, T1 2025 – T2 2026 (somme trimestrali riportate da Stingrai).

Un dato tecnico pesa più del volume: nel secondo trimestre 2026 Dragos non ha osservato operatori ransomware capaci di manipolare direttamente un sistema di controllo. Il fermo della produzione è derivato dalla cifratura, o dallo spegnimento precauzionale, di sistemi IT e di virtualizzazione da cui l'OT dipende. Difendere l'OT significa quindi anche conoscere e ridurre queste dipendenze.

VETTORE	MECCANISMO TECNICO	CONTROMISURA PRIMARIA
Interfaccia di gestione esposta	Pannello web del supervisore raggiungibile da Internet, individuabile con scanner come Censys o Shodan	Rimozione dell'esposizione; accesso solo via VPN o gateway controllato
Credenziali predefinite o condivise	Account di fabbrica, password comuni a più siti o a più tecnici	Account individuali, MFA, rotazione, divieto di riuso tra siti
Vulnerabilità del firmware	Ad esempio CVE-2025-41450/41451/41452 sui Danfoss AK-SM 800A: bypass dell'autenticazione ed esecuzione di comandi	Aggiornamento (R4.3.1), livello di sicurezza più restrittivo, dismissione dei modelli fuori supporto
Accesso remoto del manutentore	VPN permanenti, strumenti RMM (AnyDesk, TeamViewer), account legacy senza MFA	Accesso just-in-time, sessioni registrate, revoca immediata

Fornitore condiviso o cloud	Compromissione a monte che si propaga a tutti i clienti	Clausole contrattuali, SBOM, monitoraggio dei condotti verso il fornitore, piano manuale
Pivot IT→OT	Ransomware su Active Directory, hypervisor o ERP da cui dipendono le operazioni	Segmentazione, identità OT separate, DMZ industriale
Ingegneria sociale e supporti rimovibili	Finto supporto IT su Teams, chiavette USB, phishing di credenziali e codici MFA	MFA resistente al phishing (FIDO2), controllo dei supporti, formazione

PARTE III

Caso 1: la refrigerazione commerciale europea

Tra metà ottobre e i primi di novembre 2026 i sistemi di refrigerazione di supermercati e operatori alimentari sono stati manomessi in dodici Paesi europei, Italia compresa: otto casi risultano intrusioni informatiche confermate, gli altri sono manomissioni segnalate o anomalie di causa non accertata. In diversi casi, ad esempio in Svezia, i setpoint sono stati portati a 50 °C e oltre. Nessuno ha rivendicato gli attacchi e la Commissione ha dichiarato che non attribuirà responsabilità prima della conclusione delle indagini nazionali; la somiglianza tra episodi non prova un unico attore.

DATA	EVENTO	RILIEVO TECNICO
3 nov 2026	La Commissione riunisce task force interistituzionale, ENISA ed Europol, poi le autorità nazionali in EU-CyCLONe; ACN aggiorna il bollettino (v1.1)	Gestione di crisi a livello UE
2 nov 2026	Seconda ondata: Belgio (Delhaize, alcune decine di negozi), Lussemburgo, Svezia, Estonia, Paesi Bassi, Italia (quattro punti vendita in Sicilia)	Interfacce StoreView esposte in Francia scese a 220
14 ott 2026	Nuova scansione Censys	Interfacce esposte in Francia: 537
13 ott 2026	CSIRT Italia (ACN) pubblica un bollettino per GDO, logistica del freddo e manutentori	Verifica e mitigazione urgenti
12 ott 2026	CERT-FR emette l'allerta CERTFR-2026-ALE-012 su supervisori Danfoss, Copeland e Dixell (aggiornata al 16 ottobre)	Rimuovere l'esposizione, aggiornare il firmware, cambiare le password di fabbrica
11 ott 2026	Primi incidenti in Francia; Censys conta 1.825 interfacce Danfoss StoreView esposte nel Paese	Superficie d'attacco misurabile da chiunque

La catena d'attacco plausibile è breve. L'attaccante individua il pannello web del supervisore, lo raggiunge sfruttando credenziali deboli o una vulnerabilità di autenticazione (come quelle note sugli AK-SM 800A, non dimostrate come vettore di questi incidenti), poi modifica setpoint, cicli di sbrinamento e soglie di allarme. Il fornitore belga Sabcobel ha confermato che gli evaporatori sono stati forzati in modalità sbrinamento. I regolatori eseguono il nuovo valore come un comando legittimo e la temperatura del prodotto sale in poche ore. In Portogallo il gruppo Mosqueteiros ha indicato come possibile bersaglio un prestatore esterno che gestiva gli impianti: il manutentore è un condotto privilegiato verso decine di siti. Il calo delle interfacce esposte in Francia (circa −88% in tre settimane) indica che la superficie si riduce in fretta quando gli avvisi arrivano agli installatori, ma un dispositivo sparito dalle scansioni non è necessariamente aggiornato.

La difesa dell'impianto procede su quattro piani. **Esposizione**: nessuna interfaccia di gestione su Internet, accesso remoto solo tramite VPN o gateway con MFA, firmware aggiornato, livello di sicurezza del controllore al massimo, password di fabbrica sostituite. **Configurazione**: limiti di setpoint bloccati nel regolatore (un banco latticini non deve accettare valori sopra +8 °C), revisione dei programmi di sbrinamento, export periodico dei parametri come configurazione di riferimento. **Fisico**: sonde e datalogger indipendenti con allarme su canale separato (GSM o rete dedicata), termostati e pressostati di sicurezza elettromeccanici che il software non può scavalcare. **Procedure**: per i dispositivi compromessi riavvio o reset di fabbrica e riconfigurazione prima del rientro in servizio, sapendo che un modello fuori supporto resta vulnerabile anche dopo il reset; scenario di manomissione nei piani HACCP (Reg. CE 852/2004), perché il ritorno alla temperatura corretta non prova che il prodotto sia rimasto sicuro.

Ipotesi di attribuzione: IA fuori controllo o prova?

Nessuna ipotesi è dimostrata: le autorità non hanno identificato i responsabili, nessuno ha rivendicato e non è confermato alcun collegamento tra l'ondata di ottobre e quella di novembre. La procura federale belga ha aperto un'indagine penale. Le ipotesi hanno però un peso molto diverso.

IPOTESI	ELEMENTI A FAVORE	ELEMENTI CONTRO	VALUTAZIONE
Agente IA autonomo sfuggito al controllo	Nessuno specifico	Due ondate a tre settimane di distanza, la seconda sincronizzata nella stessa notte in più Paesi; azione mirata (sbrinamento forzato, setpoint a 50 °C)	Poco plausibile
Attaccanti umani assistiti da IA	L'IA accelera ricognizione e riproduzione di vulnerabilità note sui controllori	Per individuare migliaia di pannelli esposti basta uno scanner	Possibile, non distinguibile dai dati pubblici
Prova o sabotaggio dimostrativo	Nessuna richiesta di riscatto; danno reale ma recuperabile; bersaglio visibile; misura dei tempi di reazione e del coordinamento UE	Gli stessi tratti si adattano ad altri attori	Ipotesi seria
Hacktivisti o imitatori	Avvisi pubblici e dati di esposizione facilmente accessibili dopo ottobre	Coordinamento transnazionale nella stessa notte	Possibile

Tre indicatori aiuteranno a distinguere le ipotesi: la continuità tecnica tra le ondate (strumenti, infrastruttura, sequenza dei comandi), la comparsa di rivendicazioni con prove verificabili e l'evoluzione dei bersagli. Il passaggio dalla grande distribuzione a catene del freddo critiche, come farmaci, ospedali e logistica sanitaria, rafforzerebbe in modo netto l'ipotesi della prova di capacità.

PARTE IV

Caso 2: MUSE e la supply chain aeroportuale

Poco prima della mezzanotte del 19 settembre 2025 un ransomware ha colpito MUSE, la piattaforma common-use di Collins Aerospace (gruppo RTX) che consente a più compagnie di condividere banchi check-in e gate. Da sabato 20 Heathrow, Bruxelles, Berlino Brandeburgo e Dublino sono passati al check-in manuale con laptop, tablet, carte d'imbarco ed etichette bagagli scritte a mano. ENISA ha confermato il ransomware il 22 settembre; quel giorno l'aeroporto di Bruxelles ha chiesto alle compagnie di cancellare

circa 140 dei 276 voli in partenza, perché il fornitore non aveva ancora consegnato una versione sicura del sistema. Il 24 settembre la polizia britannica ha arrestato un sospettato.

Tre elementi tecnici rendono il caso esemplare. Il primo è il **guasto di modo comune**: aeroporti indipendenti sono caduti insieme perché condividevano lo stesso fornitore, e l'impatto si è concentrato proprio sugli scali che usavano MUSE. Il secondo è la **reinfezione**: secondo Heathrow i computer coinvolti erano oltre mille, e il fornitore, tentando di ricostruire il sistema, ha trovato gli attaccanti ancora presenti. Ripristinare prima di aver eradicato la persistenza (account creati, task pianificati, chiavi rubate) significa riconsegnare all'attaccante un ambiente pulito. Il terzo è la **dipendenza nascosta**: banchi e gate erano integri, ma senza il servizio centrale non potevano emettere carte d'imbarco né riconciliare passeggeri e bagagli.

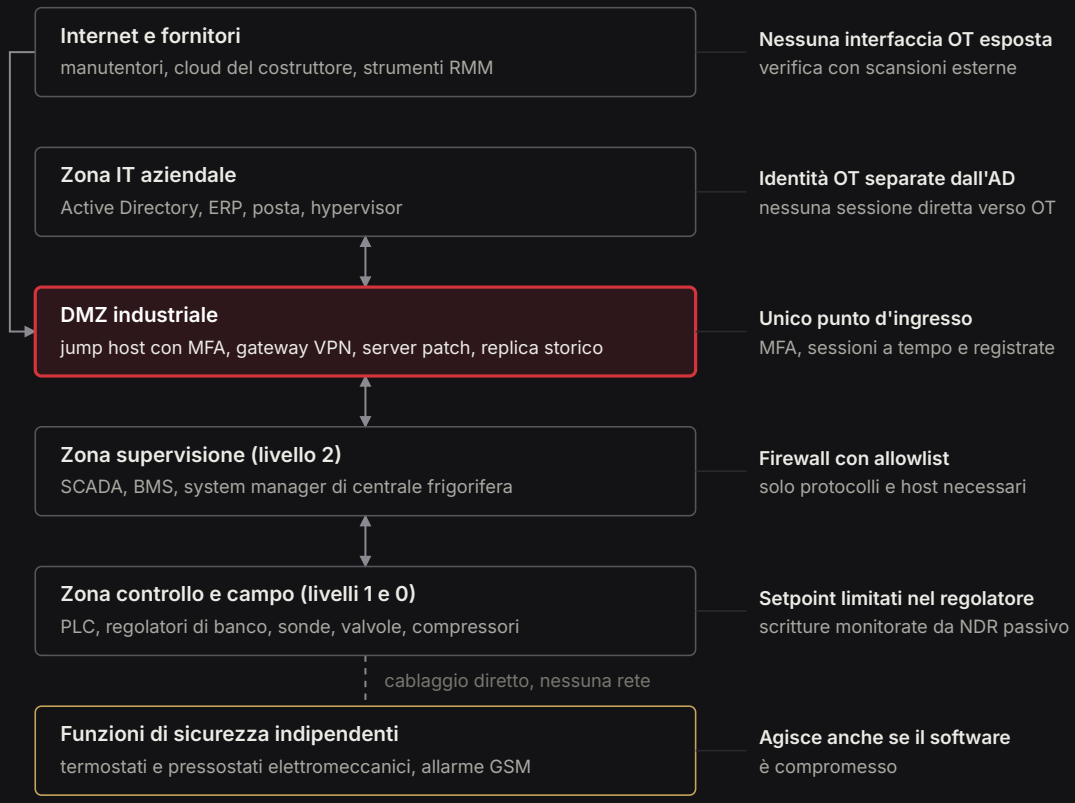
Per un gestore aeroportuale la difesa parte dalla mappa delle dipendenze: per ogni funzione critica (check-in, imbarco, bagagli, informativa voli) quali fornitori, quali connessioni, quale modalità degradata. Seguono il trattamento dei collegamenti con i fornitori come condotti a fiducia limitata (terminati in DMZ, filtrati, registrati, interrompibili in pochi minuti), requisiti contrattuali su notifica degli incidenti, SBOM e tempi di ripristino, e un piano manuale già pronto: liste passeggeri esportate offline a intervalli regolari, etichette bagagli prestampate, postazioni di riserva non collegate al sistema compromesso, esercitazioni periodiche con le compagnie.

PARTE V

Come si difende: architettura in profondità

La difesa efficace non affida la sicurezza a un solo strato. La norma IEC 62443 divide il sistema in zone con requisiti omogenei e ammette il traffico tra zone solo attraverso condotti definiti, ciascuno con un livello di sicurezza obiettivo (SL 1-4) e controlli propri; la parte 3-3 fissa i requisiti di sistema, la parte 2-4 quelli per integratori e manutentori, utile per scrivere i contratti.

Ogni accesso ai controllori passa dalla DMZ industriale



Architettura di riferimento per zone e condotti (IEC 62443): sei zone, quattro condotti di rete, una funzione di sicurezza fuori rete.

Lo schema si traduce in sei controlli tecnici. **Inventario**: elenco di controllori, supervisori, gateway e servizi di teleassistenza con modello, firmware, proprietario e stato di supporto, alimentato anche da discovery passiva per non disturbare dispositivi fragili. **Esposizione**: nessun pannello di gestione raggiungibile da Internet, verificato con scansioni esterne periodiche dello spazio di indirizzi aziendale. **Accesso remoto**: un solo punto d'ingresso nella DMZ, account nominativi, MFA resistente al phishing, abilitazione just-in-time su richiesta del manutentore, registrazione delle sessioni, nessuna VPN permanente e revoca dell'accesso di un fornitore in pochi minuti. **Segmentazione**: firewall industriali con regole in allowlist per host, porta e, dove possibile, funzione del protocollo (lettura sì, scrittura solo da host autorizzati); per l'esportazione dei dati verso l'IT, diodi di rete o gateway unidirezionali. **Hardening**: password di fabbrica sostituite, servizi inutili disattivati, firmware aggiornato secondo priorità di rischio e, dove la patch non è possibile, controlli compensativi come l'isolamento o la sostituzione programmata. **Monitoraggio**: sensori NDR passivi su porta SPAN o TAP che apprendono il traffico normale e allertano su nuove connessioni, comandi di scrittura fuori finestra di manutenzione, cambi di firmware o di configurazione, con log correlati nel SOC.

Sotto tutto questo restano le protezioni che non dipendono dal software: limiti di setpoint impostati nel controllore e non modificabili da remoto, termostati e pressostati di sicurezza elettromeccanici, datalogger con alimentazione e canale d'allarme propri. Sono l'ultima barriera, quella che limita il danno fisico quando tutte le altre hanno ceduto.

PARTE VI

Guasto o attacco: failover e risposta all'incidente

La ridondanza protegge dal guasto, non dalla compromissione. Contro un guasto hardware o software il failover commuta il servizio su un nodo di riserva (cluster attivo-passivo, controllori ridondati, link duplicati), dimensionato su due parametri: RTO, il tempo massimo di indisponibilità accettabile, e RPO, la quantità massima di dati che si può perdere. In un attacco lo stesso meccanismo lavora contro il difensore: la replica sincrona copia sulla riserva file cifrati e configurazioni alterate, gli account dell'attaccante restano validi su entrambi i nodi, la commutazione automatica riporta in servizio un ambiente ancora controllato da altri. La domanda iniziale non è come ripartire, ma se il sistema è integro.

Un sistema compromesso non va commutato sulla riserva: prima si contiene



Flusso decisionale guasto / incidente: una decisione, due percorsi.

Se ci sono indicatori di compromissione si segue il ciclo di risposta all'incidente descritto da NIST SP 800-61 (rev. 3, allineata al Cybersecurity Framework 2.0). Il contenimento isola le zone coinvolte agendo sui condotti, revoca le credenziali usate, compresi gli account di servizio e quelli dei fornitori, e sospende le sessioni remote. L'analisi forense acquisisce memoria, log e immagini dei sistemi prima di qualsiasi reinstallazione e ricerca i meccanismi di persistenza. L'eradicazione ricostruisce server, postazioni di supervisione e, se serve, firmware dei controllori da immagini verificate. Il ripristino riporta i servizi nell'ordine dato dalla mappa delle dipendenze, sotto monitoraggio rafforzato. Il caso MUSE mostra il costo di invertire le fasi: un ripristino eseguito con l'attaccante ancora presente.

I backup sono utili solo se sopravvivono all'attacco e si sa ripristinarli. La regola 3-2-1-1-0 è un buon riferimento: tre copie, su due supporti diversi, una fuori sede, una offline o immutabile, zero errori nelle prove di ripristino. In ambito OT il perimetro del backup è più ampio dell'IT: programmi dei PLC, parametri e setpoint dei regolatori, progetti SCADA, immagini delle postazioni di supervisione, licenze e chiavi, documentazione di rete. Ogni copia va conservata con un'impronta crittografica per verificarne l'integrità e provata in esercitazioni periodiche con tempi misurati.

PARTE VII

Quadro normativo e checklist operativa

Tre strumenti europei fissano gli obblighi. La direttiva **NIS2**, recepita in Italia con il D.Lgs. 138/2024, include il trasporto aereo (aeroporti, vettori, controllo del traffico) tra i settori ad alta criticità e la produzione e distribuzione alimentare tra gli altri settori critici, limitatamente all'ingrosso e alla produzione industriale: il dettaglio non è nell'allegato II. Per i soggetti coperti impone misure di gestione del rischio, compresa la sicurezza della catena di approvvigionamento, e la notifica degli incidenti significativi in tre tempi: preallarme entro 24 ore, notifica entro 72 ore, relazione finale entro un mese. Il **Cyber Resilience Act** (Reg. UE 2024/2847) sposta l'onere sui produttori: dall'11 settembre 2026 devono segnalare entro 24 ore le vulnerabilità attivamente sfruttate, anche nei prodotti già sul mercato; i requisiti essenziali di sicurezza dei prodotti si applicano dall'11 dicembre 2027. La serie **IEC 62443** resta il riferimento tecnico per progettare e verificare le misure e per esigerle contrattualmente da integratori e manutentori.

Le azioni seguenti sono ordinate per rapporto tra riduzione del rischio e costo.

30 GIORNI	☐ Scansione esterna degli indirizzi aziendali e chiusura di ogni interfaccia di gestione OT esposta
30 GIORNI	☐ Sostituzione delle password di fabbrica e disattivazione degli account condivisi o non nominativi
30 GIORNI	☐ Censimento degli accessi remoti dei fornitori; revoca delle VPN permanenti e degli strumenti RMM non autorizzati
90 GIORNI	☐ Inventario completo degli asset OT con firmware e stato di supporto; piano di aggiornamento o dismissione
90 GIORNI	☐ Jump host unico in DMZ con MFA, accesso just-in-time e registrazione delle sessioni
90 GIORNI	☐ Limiti di setpoint bloccati nei regolatori e allarmi indipendenti su canale separato
90 GIORNI	☐ Backup offline o immutabili di programmi, parametri e immagini, con prova di ripristino cronometrata
12 MESI	☐ Segmentazione per zone e condotti con firewall industriali in allowlist
12 MESI	☐ Monitoraggio passivo del traffico OT integrato nel SOC, con casi d'uso su scritture e cambi di configurazione
12 MESI	☐ Clausole con i fornitori su notifica degli incidenti, patch, SBOM e revoca degli accessi; esercitazione congiunta con operatività manuale

RIFERIMENTI

Fonti

1. Agenda Digitale, attacchi alla refrigerazione e contromisure (3 novembre 2026) — cronologia, allerta CERT-FR, dati Censys, CVE, risposta UE, NIS2 e CRA
2. Euronews, attacco informatico ai frigoriferi dei supermercati (2 novembre 2026)
3. Tech Princess, attacchi anche in Italia (3 novembre 2026)
4. Beinsure, meccanismo dello sbrinamento forzato (novembre 2026)
5. Dim Sum Daily, ipotesi di sabotaggio in assenza di riscatto (2 novembre 2026)
6. Al Jazeera, indagine penale in Belgio (3 novembre 2026)
7. Quotidiano.net, rischi dei sistemi di refrigerazione connessi secondo Claroty (3 novembre 2026)
8. Dragos, Industrial Ransomware Analysis Q2 2026
9. Stingrai, statistiche OT/ICS 2026 su dati Dragos, SANS e CISA
10. TechRepublic, ransomware sugli aeroporti europei confermato da ENISA (23 settembre 2025)
11. Computing, ENISA e il ransomware su MUSE (22 settembre 2025)
12. Airport Technology, cronologia dell'attacco a Collins Aerospace
13. BlackFog, cronologia e impatti del caso Collins Aerospace

Black Paper OpenIndustria × CISINT · N. 01 · Novembre 2026 · a cura di Marco Pugliese

Le valutazioni di attribuzione riflettono le informazioni pubbliche disponibili al 6 novembre 2026 e possono cambiare con l'avanzare delle indagini.