

ASSESSMENT CYBERSECURITY OT

Fotografia della maturità cyber degli ambienti industriali

*Risultati del questionario compilato da 75 organizzazioni su
17 aree tematiche di cybersecurity e cybersafety industriale*

28 agosto 2026



Contesto e metodologia

L'assessment ha raccolto le risposte di 75 organizzazioni su 60 domande, organizzate in 17 aree tematiche che ripercorrono l'intero ciclo di vita della cybersecurity industriale: dall'inventario degli asset OT alla governance, passando per accessi, segmentazione di rete, monitoraggio e incident management.

Per alcune domande, applicabili solo a un sottoinsieme delle organizzazioni (es. presenza di asset OT rilevanti o di fornitori con accesso remoto), la base di risposta si riduce a 59 o 54 partecipanti

Scala di risposta utilizzata



Sì

Requisito pienamente soddisfatto



Parzialmente / In corso

Requisito in parte soddisfatto o in fase di definizione



No

Requisito non soddisfatto



Non lo so

Mancanza di visibilità sul tema

17 aree tematiche coperte dal questionario

- 01 · Asset Management
- 02 · Protezione dati e crittografia
- 03 · Configurazione e hardening OT
- 04 · Identity & Access Management
- 05 · Controllo accessi fisici e remoti
- 06 · Vulnerability Management
- 07 · Log Management
- 08 · Protezione da malware
- 09 · Backup & Disaster Recovery
- 10 · Segmentazione di rete
- 11 · Monitoraggio & SOC
- 12 · Formazione
- 13 · Gestione fornitori
- 14 · Incident Management
- 15 · Test & ambienti separati
- 16 · Governance & Policy
- 17 · Sicurezza fisica e ambientale

Executive summary

Maturità in crescita, ma prevalgono controlli isolati rispetto a un sistema organico



L'Assessment evidenzia un livello di attenzione alla cybersecurity OT già significativo, ma caratterizzato da forte variabilità tra le organizzazioni e tra le diverse aree di controllo.

Il dato più rilevante non è tanto la presenza o l'assenza di singoli strumenti, quanto la prevalenza della risposta “parzialmente” in numerosi ambiti: molte aziende hanno avviato percorsi di adeguamento, ma non li hanno ancora trasformati in un sistema organico di gestione della sicurezza OT.

CINQUE EVIDENZE PRINCIPALI

- 1 La conoscenza degli asset OT è ancora incompleta**
Solo 25 aziende su 75 hanno un inventario completo; 42 ne hanno uno parziale.
- 2 Il rischio OT è riconosciuto, ma non ancora integrato**
35 aziende includono l'OT nell'analisi del rischio; 24 sono ancora in fase di definizione.
- 3 I controlli di base sono più maturi di quelli avanzati**
Accessi, ambienti e firewall sono strutturati; VA, logging, SIEM e SOC restano disomogenei.
- 4 La continuità operativa esiste, ma non sempre è OT-aware**
Piani presenti in molte aziende, ma non sempre progettati per le peculiarità OT.
- 5 La cybersecurity OT non è ancora un investimento strutturale**
Budget dedicato solo in 17 aziende su 59; 18 non ne hanno alcuno.

Punti di forza e aree di attenzione



I controlli fisici e perimetrali guidano la maturità, mentre patching e SOC OT rimangono i gap principali

TOP 5 PUNTI DI FORZA

80%

Uso di VPN per gli accessi remoti in ambito OT (11a)

78%

Alimentazioni ridondate, UPS e gruppi di continuità (17d)

76%

Misure minime per l'accesso fisico ai locali (5f)

75%

Misure di sicurezza ambientale (antincendio, condizionamento) (17a)

73%

Segmentazione delle reti degli asset connessi a cloud/web (10a)

TOP 5 AREE DI ATTENZIONE

21%

Aggiornamenti SW/SO validati estesi ai dispositivi OT/SCADA (3c)

25%

Policy di gestione del ciclo di vita degli asset OT (16c)

25%

Test dei nuovi macchinari OT in ambiente separato (15a)

27%

Vulnerability Assessment periodico dei macchinari OT critici (6b)

33%

SOC con competenze specifiche per l'ambiente OT (11d) (58% No)

La fotografia complessiva

Dall'incrocio delle risposte emerge una struttura a tre livelli di maturità



RELATIVAMENTE PIÙ MATURE

- Physical Security: Controllo accessi, ambienti, videosorveglianza, UPS
- Network Protection: Firewall, VPN e segregazione reti IT/OT
- Basic Access Control: Password di default, ruoli e credenziali
- Risk Awareness: Consapevolezza e integrazione iniziale dell'OT nel risk management

MATURITÀ INTERMEDIA

- Backup & Disaster Recovery: Backup presenti, ma scarsi test specifici per OT
- Incident Management: Procedure presenti ma con forte divario di formalizzazione
- Supplier Security: Attenzione contrattuale crescente ma non omogenea
- Compliance & Regulatory: Presenza di policy senza monitoraggio strutturato

PRINCIPALI GAP

- OT Asset Inventory: Conoscenza parziale o incompleta degli asset reali
- OT Vulnerability Assessment: Scansioni non generalizzate né ricorrenti per l'OT
- Continuous Monitoring & OT SOC: Carenza di presidio SOC OT specialistico
- Lifecycle Management & Budget: Mancanza di investimenti e budget strutturali dedicati

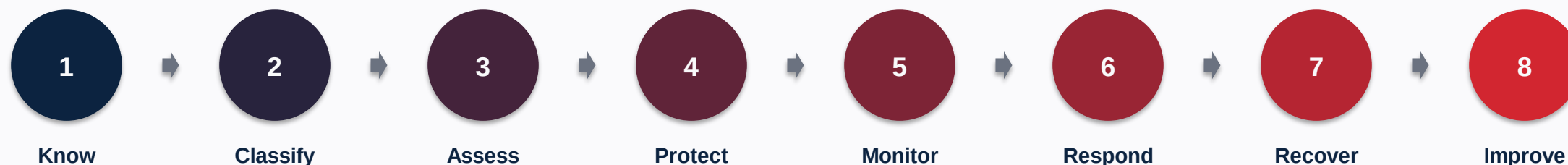
La considerazione più importante

Evolgere da una sicurezza orientata ai controlli singoli a una governance strutturata



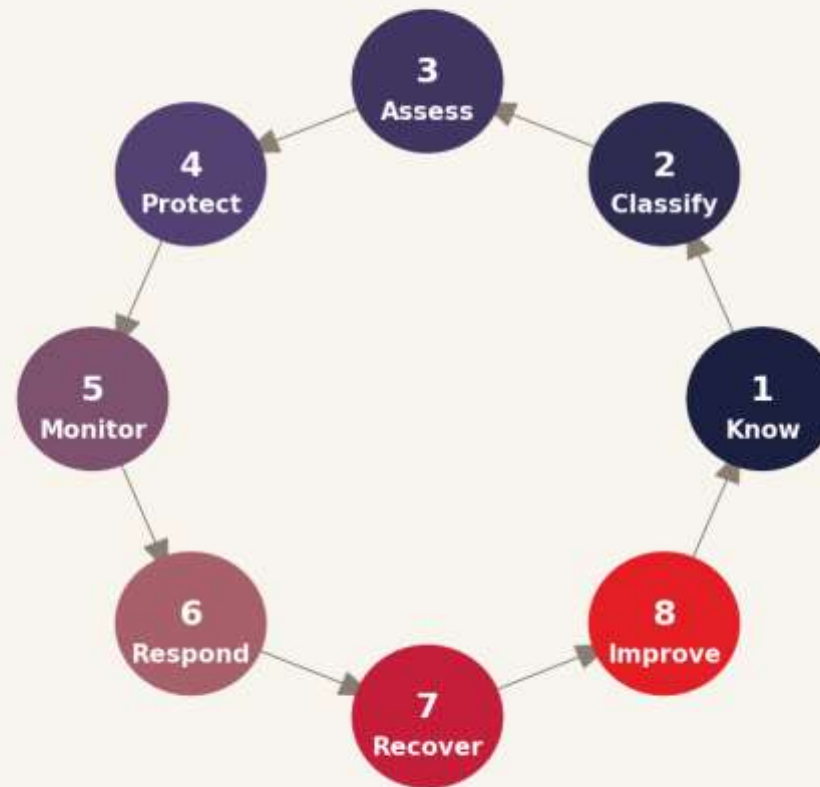
“Le aziende non partono da zero. Il problema è trasformare una serie di controlli già presenti in un modello organico di Cybersecurity OT.”

Il livello di maturità rilevato è quello di una “security by controls”, nella quale sono presenti diversi strumenti e procedure, ma non sempre una vera “security by design and governance”. La priorità non è aggiungere nuovi strumenti: è costruire un percorso.



Ciclo Continuo di Sicurezza OT | Approccio Olistico in 8 Fasi

Ciclo Continuo di Cybersecurity OT



Proposta di roadmap in 4 step

Un percorso strutturato per elevare la maturità cyber degli asset industriali



STEP 1

Know your OT

Creazione dell'OT Asset Inventory e mappatura dei sistemi critici.

Conoscere asset, connessioni, dipendenze, owner e criticità.

STEP 2

Secure your OT

Risk assessment, network segmentation, identity & access management, vulnerability assessment, patching e hardening.

Ridurre la superficie di attacco senza compromettere la produzione.

STEP 3

Monitor & Respond

OT monitoring, NIDS, SIEM, EDR/XDR, SOC e incident response

Passare dalla prevenzione alla capacità di rilevare e rispondere.

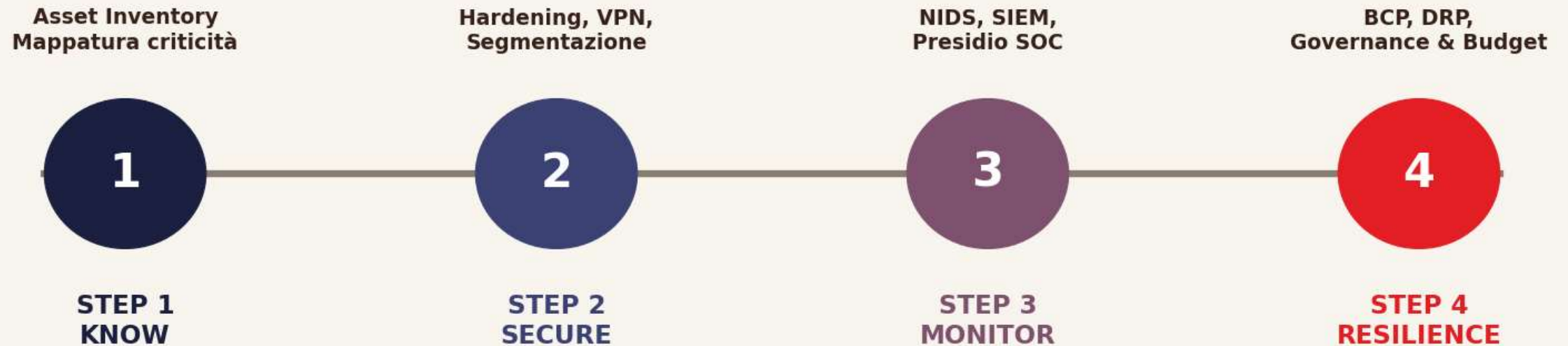
STEP 4

Resilience & Gov.

BCP, DR, crisis management, supply chain security, formazione, KPI e budget.

Trasformare la cybersecurity OT in una capacità permanente.

La Timeline Strategica | Quattro Step Incrementali



Conclusioni

Il consolidamento delle pratiche di cybersecurity e la misurazione della maturità



L'Assessment evidenzia un mercato che ha già sviluppato consapevolezza sulla cybersecurity OT, ma che si trova in una fase di consolidamento.

La domanda non è più “dobbiamo proteggere l'OT?": sta diventando “come rendiamo la sicurezza OT misurabile, continua e integrata nella gestione industriale e nella cybersecurity governance complessiva dell'azienda?”.

È in questo spazio che si colloca l'opportunità di un percorso strutturato di assessment, remediation e accompagnamento alla maturità nella governance integrata dell'OT.