SECURITY SUMMIT

Security Summit

Verona 28 ottobre 2026

Clusit

ASTREA

I perimetri da (ri)definire per governare il rischio IT/OT

Moderano:
Luca Bechelli, CD, Clusit
Cinzia Ercolano, Fondatrice Women For Security

Presentazione della survey Women For Security sulla maturità della cybersecurity OT nelle aziende manifatturiere, a cura di **Georgia Cesarone**, Comitato Direttivo WFS.

Segue una tavola rotonda con i protagonisti della giornata:
- Mauro Cicognini
- Matteo Colella
- Alessio Pennasilico
- Anna Vaccarelli

WOMEN for Security

28 ottobre, 17 – 18.00

CYBERSECURITY OT

Cosa ci raccontano 75 organizzazioni sulla maturità degli ambienti industriali?



PROTEGGERE ≠ ESSERE RESILIENTI

Dai controlli isolati ad un modello integrato di sicurezza industriale

La fotografia del campione

Un assessment trasversale

75

organizzazioni coinvolte

60

domande di assessment

17

aree di cybersecurity e cybersafety

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.

Scala di risposta utilizzata

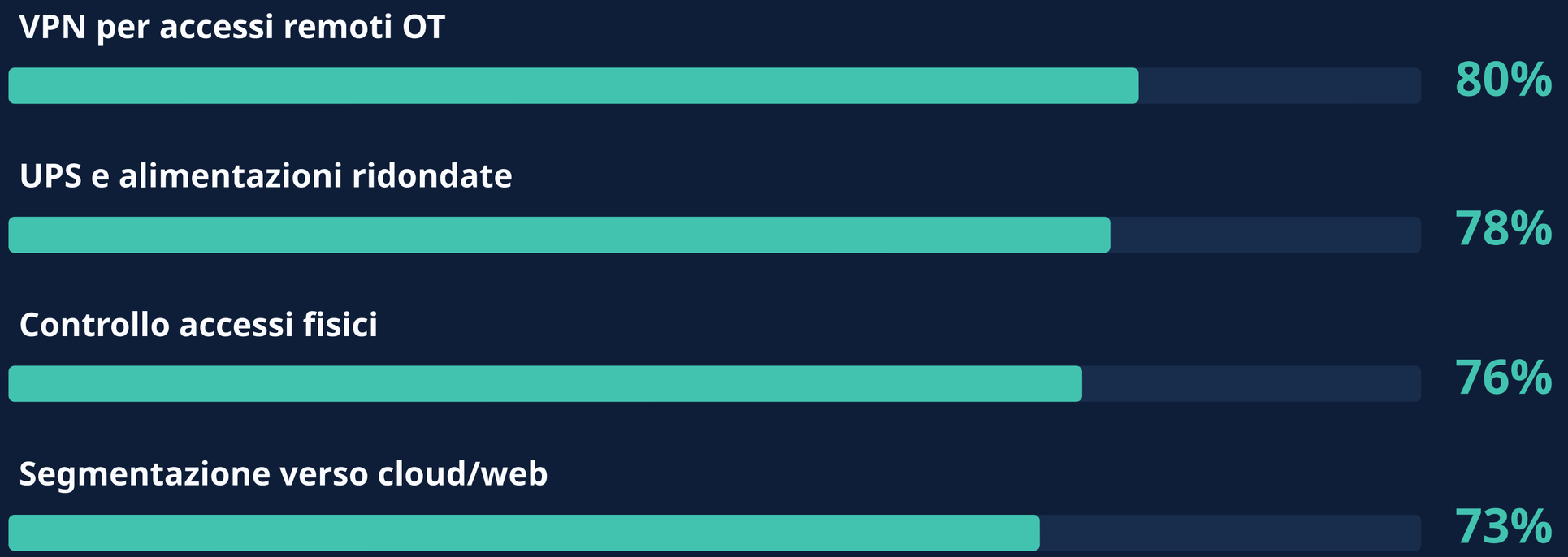
- **Sì** — Requisito pienamente soddisfatto
- **No** — Requisito non soddisfatto
- **Parzialmente / In corso** — Requisito in parte soddisfatto o in fase di definizione
- **Non lo so** — Mancanza di visibilità sul tema

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.

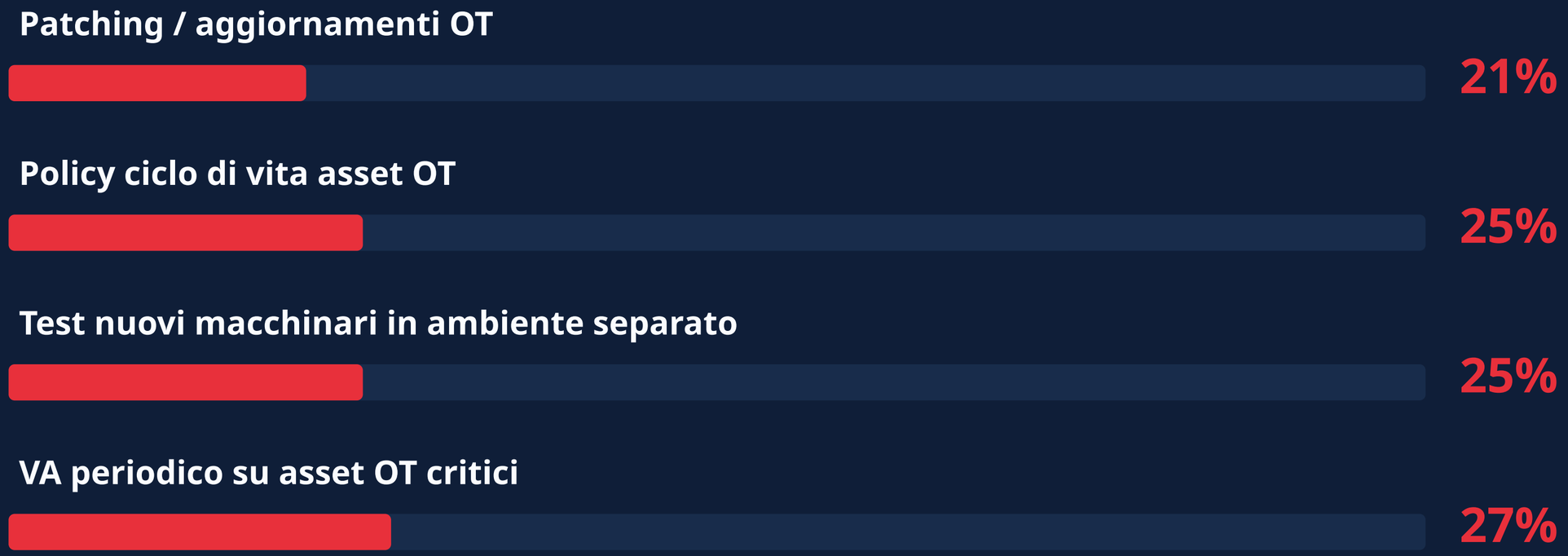
Dove siamo più forti

I controlli fisici e perimetrali sono già diffusi



Dove si concentrano i gap

Le capacità OT-specifiche avanzate sono ancora fragili



Il divario più evidente

Accesso protetto non significa capacità di rilevare un attacco

80%

utilizza VPN per gli accessi remoti OT

32%

dispone di un SOC con competenze OT

48 punti percentuali di distanza

La sfida: passare dalla protezione al monitoraggio e alla risposta.

Prima di proteggere, conoscere

L’inventario OT è spesso presente, ma incompleto

25/75

inventario OT completo

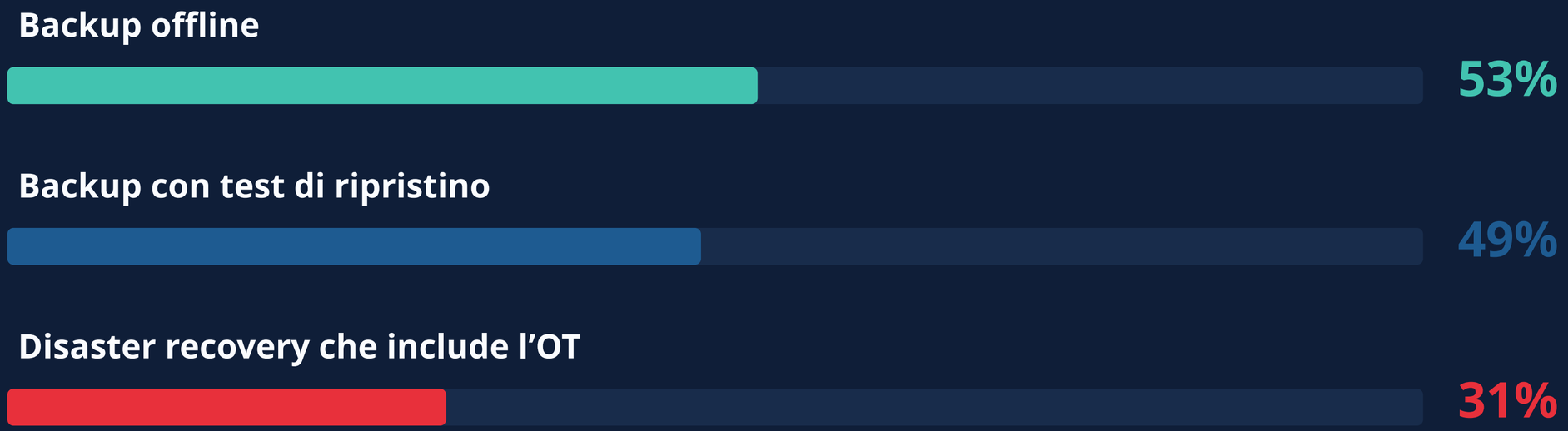
42/75

inventario OT solo parziale

Un inventario utile alla sicurezza deve descrivere criticità, dipendenze, owner e accessi.

La resilienza non si improvvisa

Backup e procedure esistono, ma il ripristino OT resta un punto debole



Un impianto non si ripristina come un server.

La governance è il vero acceleratore

Senza responsabilità e investimenti, i controlli restano frammentati

17/59

organizzazioni con budget OT dedicato

35/75

includono l’OT nell’analisi del rischio

Cybersecurity OT = cyber + safety + continuità + ambiente + produzione

Quattro priorità per i prossimi passi

Dalla fotografia dell’assessment all’impostazione di una roadmap concreta

01 **CONOSCERE**

Inventario e mappatura degli asset critici

02 **PROTEGGERE**

Patching, accessi, segmentazione e test

03 **RILEVARE**

Logging, monitoraggio e risposta OT

04 **GOVERNARE**

Ruoli, fornitori, investimenti e recovery