



CYBERFERO

Vulnerability assessment continuativo OT



- ✓ **Visibilità completa degli asset ot**
- ✓ **Rilevamento vulnerabilità con priorità per rischio**
- ✓ **Monitoraggio in tempo reale e alert**

www.cyberfero.com

CHE COS'È?

Proteggi il tuo impianto dalle minacce OT, senza fermare la produzione. Un servizio gestito continuativo che individua asset, vulnerabilità e comportamenti anomali nel mondo OT: sensori (temperatura, pressione, livello, vibrazione, portata), plc, hmi/scada, reti industriali, attuatori, valvole e componenti di campo.



Negli ambienti OT il problema non è solo “se” esiste una vulnerabilità, ma quanto può impattare sul processo: fermo linea, degrado qualità, rischio safety, inefficienze, blocco impianto. In più, l’eterogeneità (macchine nuove e legacy, fornitori diversi, protocolli industriali, accessi remoti) rende impossibile affidarsi a controlli spot.

Serve un controllo continuo, progettato per l’operatività industriale.





Vulnerability assessment continuativo ot è l'equivalente del vulnerability assessment continuativo it, applicato al mondo operativo:

- 01 Scansiona e osserva l'ecosistema ot in modo continuativo
- 02 Identifica vulnerabilità e criticità di configurazione
- 03 Rileva variazioni non autorizzate e anomalie di rete/processo
- 04 Produce priorità e azioni consigliate, orientate alla continuità operativa

COSA MONITORIAMO?

asset OT e IoT

- ✓ Plc, hmi, scada, gateway, switch e segmenti di rete industriale
- ✓ Sensori: temperatura, pressione, livello, vibrazione, portata
- ✓ Attuatori e componenti di campo: valvole, chiuse idrauliche, sistemi ausiliari
- ✓ Interconnessioni it/ot e accessi remoti
- ✓ Apparati ip connessi, anche non gestiti



COME FUNZIONA ?



1) Visibilità

Inventario e mappatura dell'impianto: cosa è connesso, dove si trova, che ruolo ha e cosa cambia nel tempo.



3) Risposta

Priorità basata sul rischio e supporto all'azione: cosa correggere prima, cosa pianificare in fermo impianto, cosa mitigare subito.



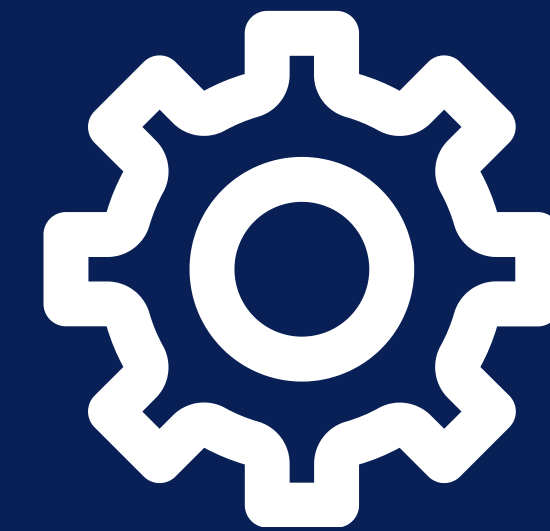
2) Rilevamento

Monitoraggio continuo per intercettare:

- ✓ Vulnerabilità note e nuove esposizioni
- ✓ Comportamenti anomali
- ✓ Variazioni rispetto a configurazioni autorizzate

APPROCCIO TECNICO

per garantire efficacia in ambiente industriale, il servizio combina:



- ✓ Sonde on site posizionate in punti strategici della rete impianto
- ✓ Gestione centralizzata e correlazione degli eventi
- ✓ Monitoraggio ibrido: passivo (osserva il traffico senza interferire) e attivo (interrogazioni mirate quando necessario)

Obiettivo: aumentare sicurezza e resilienza senza introdurre complessità inutile.

BENEFICI:

- ✓ Dashboard con inventario asset, criticità e stato sicurezza
- ✓ Report periodico (mensile o secondo esigenza) con:
 - Vulnerabilità rilevate e priorità
 - Evidenze, impatto e raccomandazioni tecniche
 - Piano di azione per mitigazione e correzione
- ✓ Alert su anomalie, nuove connessioni e variazioni non autorizzate
- ✓ Possibilità di affiancamento al team interno e ai fornitori per la remediation (su richiesta)



A CHI E' CONSIGLIATO?

Ideale per aziende che:

- 01 Gestiscono impianti con continuità operativa critica
- 02 Hanno ambienti misti legacy/moderni e vendor differenti
- 03 Devono ridurre downtime e rischio operativo
- 04 Vogliono costruire una base solida per audit, policy di gruppo e compliance





CYBERFERO

Da oltre 10 anni leader nel settore Cybersecurity e Sicurezza

CYBERFERO è un Managed Security Service Provider (MSSP) specializzato nella fornitura di soluzioni di sicurezza complete per aziende di tutte le dimensioni. In qualità di partner di fiducia, offriamo un'ampia gamma di servizi di sicurezza progettati per proteggere la tua organizzazione da minacce informatiche, violazioni dei dati e altri rischi per la sicurezza.

[Visita il sito web](#)

Contatti



+39 0522 1685330



<https://www.cyberfero.com>



info@cyberfero.com



Via Statuto 3, 42123 – Reggio nell'Emilia (RE)

