REEVO
Cloud & Cyber Security

CYBER SECURITY
ReeVolution

I SERVIZI PER IL MONDO IOT/OT INDUSTRIALE

#BeReeVolution

LE SFIDE CYBER AL MONDO INDUSTRIALE

Ormai è noto che il numero di attacchi informatici ad aziende del settore industriale e manifatturiero è in costante crescita. Secondo l'ultimo rapporto Clusit "*gli incidenti rivolti al Manufacturing rilevati in Italia, in particolare, rappresentano il 27% del totale degli attacchi censiti a livello globale nei confronti di questo settore*"[1]. Se in passato ha inizialmente funzionato il pensare ai sistemi industriali – e in particolare quelli OT (PLC, SCADA, RTU, DCS) - come isolati, e di conseguenza sganciati dalle problematiche di sicurezza dei sistemi IT, oggi nessuno è più immune dai rischi. L'Industry-Of-Things, la crescente interconnessione dei sistemi e la convergenza IT/OT fanno sì che un **approccio integrato alla cybersicurezza** si renda necessario.

1 *Rapporto Clusit 2023*

COME RISPONDE REEVO?

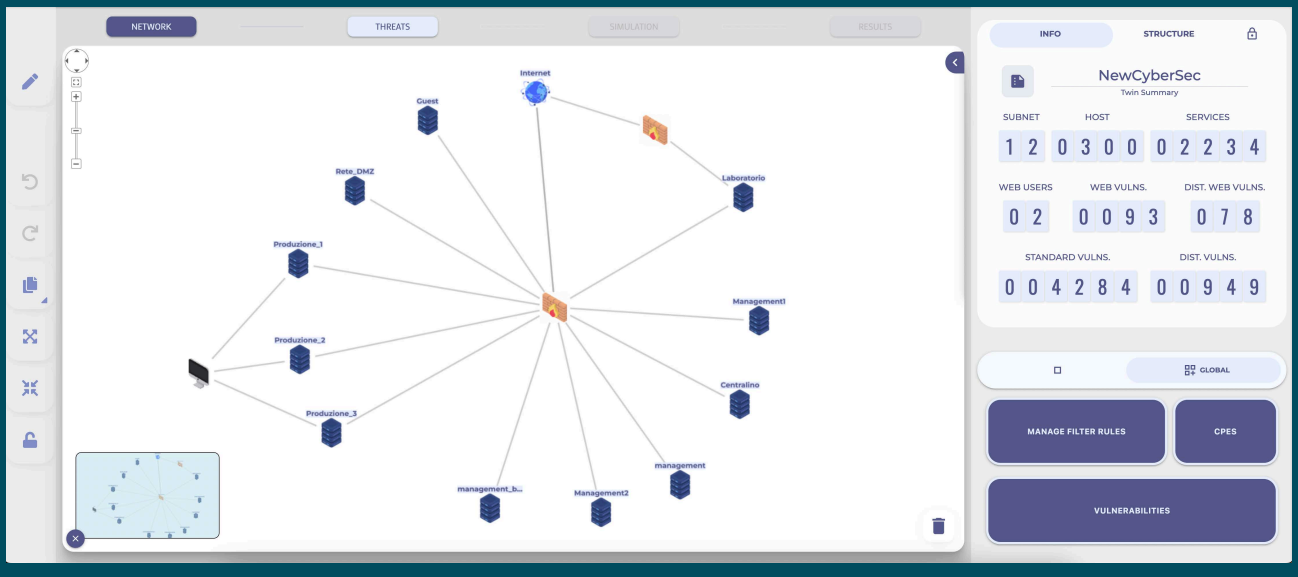
ReeVo risponde alle necessità di protezione degli ambienti produttivi o dei macchinari OEM con servizi basati sullo standard ISO/IEC 62443 e EU Cyber Resilience Act.

Forti della nostra esperienza ventennale come fornitore di servizi integrati di cloud e cybersecurity, abbiamo sviluppato un framework di protezione per tutte le fasi del ciclo di un processo industriale.
E lo facciamo aiutando le aziende al rispetto di direttive o normative in ambito cybersecurity industriale (quali ad esempio **ISO/IEC 62443, EU Cyber Resiliency Act**, solo per citarne alcune)
In estrema sintesi: **prevenzione <-> difesa <-> integrazione, secondo gli standard internazionali.**

LA FASE DI PREVENZIONE

Che sia a beneficio di un **OEM per tutelarsi dall'immissione sul mercato di apparecchiature vulnerabili**, o per un'industria che ha macchinari e impianti in produzione e vuole agire in difesa dei propri asset dagli attacchi cyber, **la fase di "prevenzione" è irrinunciabile**. ReeVo è in grado di fornire strumenti e servizi per prevenire in modo costante i problemi, prima che possano costituire un rischio. L'accento è sul garantire un "processo continuo" di prevenzione, anziché limitarsi a offrire tecnologie o servizi che danno delle prese di coscienza sporadiche (ad esempio tramite vulnerability assessment o penetration test effettuati una tantum).

Tramite la costruzione di un **Digital Twin (gemello digitale)**, in una modalità completamente **non invasiva**, nei datacenter ReeVo è possibile creare **la copia digitale di qualunque infrastruttura IT/OT** e sottoporla costantemente a milioni di attacchi al fine di **poter quantificare il rischio cyber sia in fase di progettazione per i produttori OEM sia all'interno della fabbrica**



LA FASE DI DIFESA: OT E RETI

È possibile rendere sicuri gli ambienti OT mutuando logiche e practice della sicurezza IT?

Sì, ma soddisfacendo alcuni requisiti importanti tra i quali:

- avere una rete *software-defined* con traffico dati OT segmentabile.
- soddisfare la normativa **ISO/IEC 62443** e garantire la sicurezza della **rete** di telecomunicazioni OT e dei dispositivi.
- delegare al **reparto IT monitoraggio e gestione centralizzata della sicurezza**, ma garantire sempre la possibilità di **manutenzione manuale OT da parte degli operatori**, che possono intervenire - in autonomia e su necessità - sul controllo del sistema (ad esempio con dispositivi mobile).

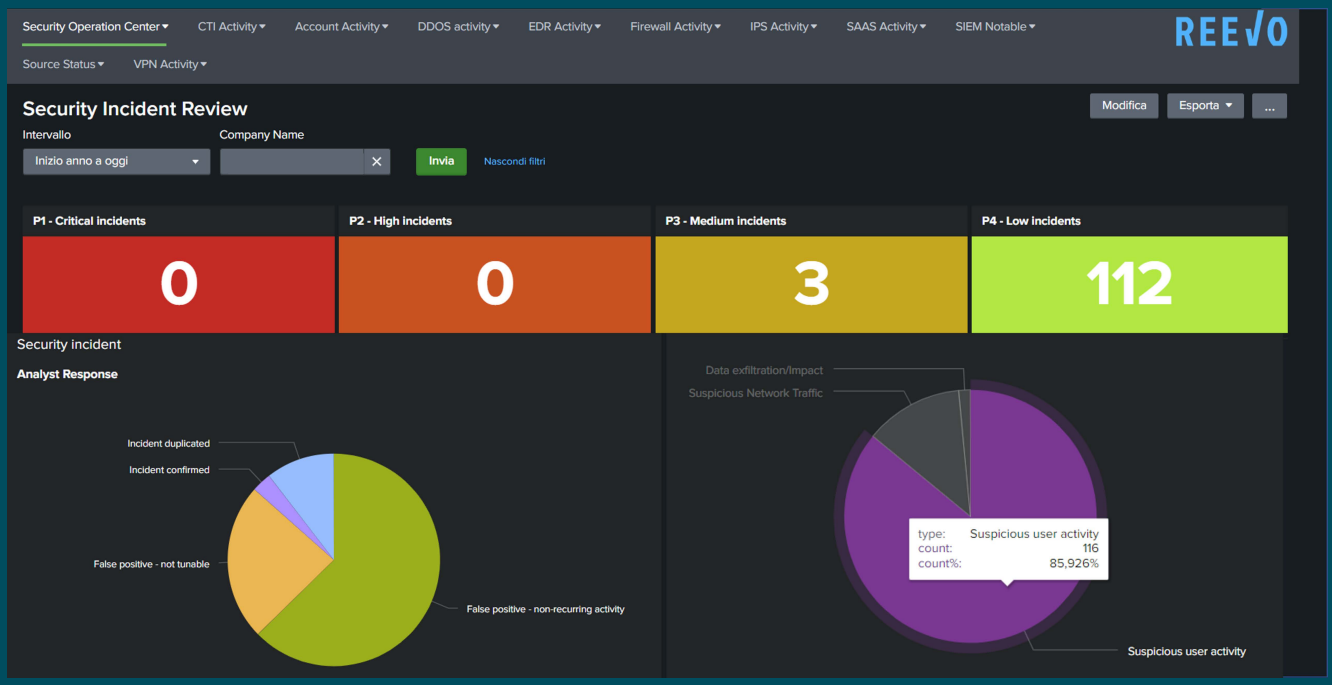
Un ulteriore punto di vantaggio, per velocità di implementazione e protezione degli investimenti, è poi ottenibile cercando soluzioni che si adattano alle configurazioni di rete OT esistenti, non richiedendo una modifica degli apparati.

LA FASE DI DIFESA: INDUSTRIAL SOC

Il punto centrale della proposizione ReeVo è rappresentato dal **SOC H24**.

Indipendentemente dal numero e dalla tipologia di tecnologie utili a proteggersi dalle minacce informatiche, per esperienza sappiamo che l'investimento in esse non copre dai rischi, in assenza di un servizio rapido e intelligente in grado di integrare i segnali da esse provenienti e a mettere in campo le risposte più rapide ed appropriate.

E questo è proprio quello che l'**Industrial SOC di ReeVo** – a **risposta automatica** - è in grado di fare.

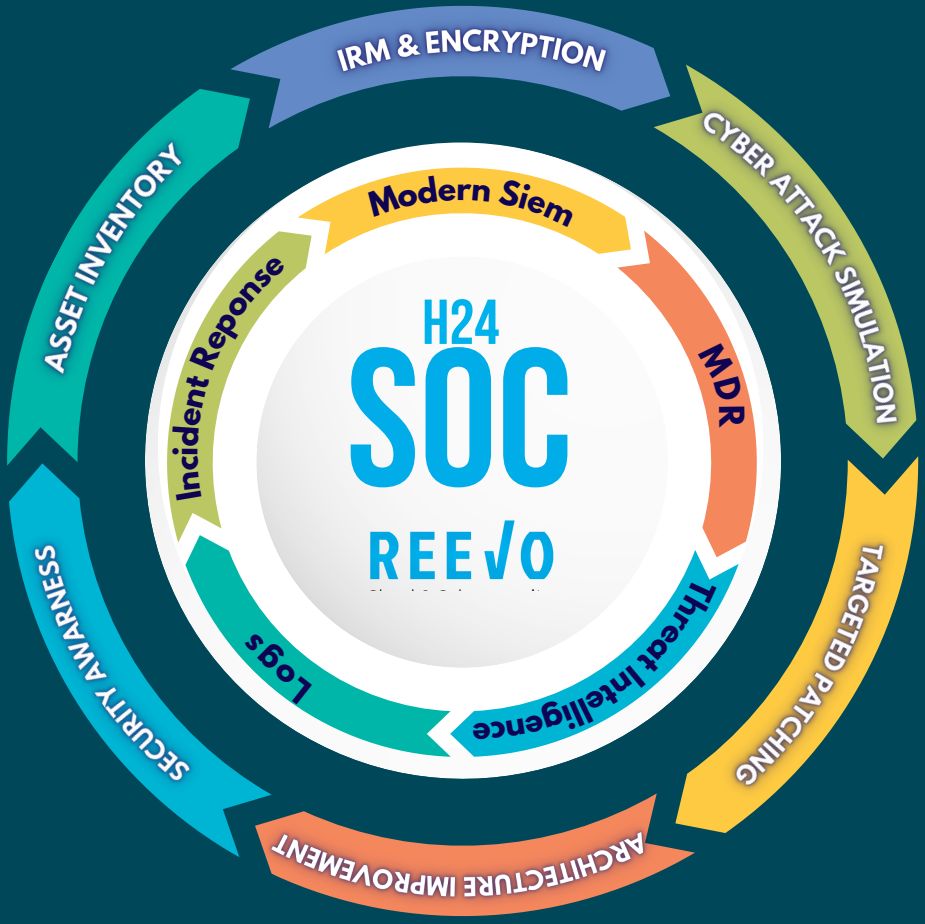


Va sottolineato come l'aspetto di **"automazione" nella risposta** sia **un fattore cruciale**. Rispondere in modo istantaneo a potenziali minacce evita problemi ben più seri. Questo **non è possibile nei SOC di tipo tradizionale** dove viene sostanzialmente gestita un'allarmistica dai sistemi in modo reattivo.

Il SOC di ReeVo interviene subito in automatico a fronte dell'insorgere di un potenziale problema, evitando che abbia effetti dannosi o che si propaghi all'interno dell'azienda.

Al potenziale insorgere di una minaccia, l'interazione con la **Cyber Threat Intelligence** da parte di una componente di **SOAR** (Security Orchestration, Automation and Response) consente la **corretta classificazione del rischio** e la più veloce azione di risposta.

Successivamente l'interazione da parte degli esperti SOC, consente di prolungare l'**isolamento** della minaccia, in attesa di una **remediation**, o il **ripristino** di una corretta operatività, nel caso di falsi positivi.



#BeReeVolution

SERVIZI CYBER SECURITY

SECURITY OPERATION CENTER (SOC) AS A SERVICE

Il tuo alleato, attivo 24/7, che monitora la "superficie di attacco" e scopre le vulnerabilità sfruttabili da cyber criminali per l'accesso ai tuoi sistemi.

CYBER ATTACK SIMULATION

Crea il gemello digitale della tua infrastruttura IT/OT e lo colpisce con migliaia di simulazioni di attacco per scoprire i percorsi utilizzati, le patch mirate su cui intervenire e quelle che fondamentali per la tua sicurezza. Agisce anche in fase di pianificazione di risorse con logiche "What-If".

IRM & DOCUMENT ENCRYPTION

Offre controllo e la protezione dei dati, sempre e ovunque. Massima granularità su accessi e autorizzazioni e rischi interni ed esterni di sicurezza, estorsione e data breach, ridotti al minimo.

INCIDENT RESPONSE

Un "pronto intervento" 24/7 che ti supporta in caso di attacco informatico e la migliore Task Force di Cyber Analyst, System Engineer e staff per gli adempimenti legali.

#CybersecReeVolution

FATTORI DI UNICITÀ REEVO:

PERCHÉ PENSIAMO DI AVERE LA PROPOSIZIONE CHE CERCHI

- **SOC H24**
- **Valutazione preventiva** del rischio cyber (**senza fermi macchine**)
- **Cyber Threat Intelligence**
- Processo di **Incident Response** a risposta automatica
- **Supporto** localizzato **in Italia e madrelingua**
- Solo **Datacenter Tier4 /ANSI TIA 942** dislocati sul territorio nazionale
- **18 certificazioni** (tra le quali ISO 27001, 27017, 27018, 27035, Cybersecurity Made in Europe)
- **Alleanze tecnologiche** “solo” con vendor **leader di mercato**

ENTRIAMO IN CONTATTO

+39 039 2873925
+34 910 48 85 69

staff@reevo.it
staff@reevo.es

www.reevo.it
www.reevo.es

ReeVo Cloud and Cybersecurity

Foro Buonaparte, 57
20121 Milano (MI)
Av. De Bruselas 7 28108 Alcobendas, Madrid

REEVO

Cloud & Cyber Security