

# Schneider Electric a Cybertech Europe: dall'integrazione di competenze OT e innovazione IT l'arma vincente per difendere in profondità la trasformazione digitale.

---

*L'azienda è fra gli sponsor dell'evento per proporre un approccio alla cybersecurity di industria e infrastrutture che fa leva su EcoStruxure, una piattaforma nata per la digitalizzazione del mondo operativo.*

Schneider Electric, il leader nella trasformazione digitale dell'industria e della gestione dell'energia, è tra gli sponsor di Cybertech Europe, la più importante conferenza europea di tecnologie cyber, che si terrà a Roma il 26 e 27 settembre prossimi al Centro Congressi La Nuvola.

La connettività sempre più ricca e pervasiva, accompagnata dall'emergere continuo di nuove tecnologie e opportunità, costringe le imprese a ridefinire sempre più spesso le coordinate e i confini del loro business: impianti produttivi, infrastrutture, utility operano in uno scenario in cui sistemi, persone, processi, oggetti esistono e agiscono in modo sempre più interdipendente.

Controllare il perimetro fisico dei sistemi aziendali è necessario ma non certamente sufficiente a difendersi dalla velocissima evoluzione del cybercrime che come già si è potuto sperimentare è oggi in grado di scatenare attacchi con un impatto potenzialmente catastrofico, capaci di creare centinaia di milioni di euro di danni e di bloccare l'erogazione di servizi essenziali come: energia, trasporti, infrastrutture.

*“Per un'industria investire in cybersecurity, sia dal punto di vista delle tecnologie sia da quello delle procedure e delle competenze, è essenziale; in diversi casi – pensiamo ad esempio ai settori interessati dalla direttiva NIS - è anche obbligatorio”* spiega **Umberto Cattaneo, Cybersecurity Technical Sales Consultant di Schneider Electric**. *“Siamo a Cybertech Europe per dare un segnale al nostro mercato: è il momento che oltre agli attori dell'IT entrino in campo direttamente gli attori che vengono dal mondo delle tecnologie operative, perché questo porta un valore aggiunto importante per assicurarsi capacità di difesa senza scendere in alcun modo a compromessi in termini di fluidità operativa, agilità, flessibilità produttiva”.*

*“Ci proponiamo come partner nell'ecosistema della cybersecurity partendo dal nostro punto di forza: abbiamo abbracciato a 360 gradi la digitalizzazione con investimenti ingenti in ricerca e sviluppo ma nasciamo nel mondo delle tecnologie operative e quindi conosciamo meglio di chiunque altro ciò che potrebbe rendere vulnerabile ogni tipo di componente e sistema di controllo industriale, nei più diversi settori”.*

## **Defence in depth: difendersi in profondità supportati da una piattaforma intrinsecamente sicura**

L'integrazione di expertise e competenze IT e OT realizzata da Schneider Electric consente di collaborare con i dipartimenti IT ed altri provider di soluzioni di sicurezza per sviluppare soluzioni efficaci e adeguate alle caratteristiche operative di ogni azienda, sulla base di una conoscenza approfondita che permette di adottare scelte del tutto mirate.

Piuttosto che combattere ogni volta una singola battaglia, Schneider Electric propone alle aziende di adottare strategie che consentano di prevenire o minimizzare l'effetto di attacchi: un sistema di difesa che aderisce ai principali standard di riferimento in ambito industriale (come: IEC62443, IEC62351, NIST, ISO27019) e si realizza con un approccio che prevede più livelli e l'utilizzo di più tecnologie per proteggere i sistemi critici.

E' una strategia di "difesa in profondità" per definizione olistica, che si basa su una metodologia collaudata di gestione del ciclo di vita della cyber security : dall'assessment alla definizione delle idonee architetture di sistema per l'implementazione di soluzioni intrinsecamente sicure, dalla gestione al monitoraggio, fino alla manutenzione e all'offerta di servizi di consulenza e di formazione dedicati.

In questo senso Schneider Electric ha la capacità di offrire risposte anche alle richieste più difficili. Ad esempio, è in grado di offrire alle industrie critiche del settore oil & gas, energia ed infrastrutture interessate dalla direttiva NIS soluzioni che le aiutano a rispettare i complessi requisiti operativi e di processo richiesti.

### **L'ecosistema della sicurezza: trasparenza, fiducia, innovazione ed EcoStruxure, una piattaforma intrinsecamente sicura**

Lo scenario del cybercrime è talmente complesso che nessuna azienda può dire di avere in mano, da sola, l'arma per vincere definitivamente la battaglia. La collaborazione anche pre-competitiva in un ecosistema dinamico di partnership, piattaforme, istituzioni e il coinvolgimento di tutta la supply chain sono fondamentali per stimolare la ricerca, la creazione di nuove policy, la trasparenza e la fiducia.

Schneider Electric dispone, oltre che di un team di esperti cybersecurity che lavorano direttamente con i clienti, di un Global Threat Intelligence Center che si occupa di un monitoraggio attivo del cyberspazio per individuare potenziali rischi e sviluppare le adeguate contromisure da implementare sulle proprie soluzioni.

Accanto a tutto questo, l'azienda offre oltre centinaia di prodotti certificati secondo standard di cybersecurity per applicazioni in ambito industriale ed elettrico. Si tratta di componenti connessi che fanno parte di EcoStruxure, la piattaforma e architettura aperta, interoperabile e basata su IoT su cui si fonda la capacità di innovazione e trasformazione digitale di Schneider Electric nelle industrie, nelle infrastrutture, nel mondo building, nell'energia e nell'IT.

I prodotti incorporano componenti sicuri, al livello di controllo la security è integrata nella progettazione e sviluppo dei sistemi, che sono sottoposti a rigorose procedure di Test e Validazione, così come nello sviluppo di tutte le applicazioni che consentono alle imprese di cogliere appieno i vantaggi della digitalizzazione usufruendo di servizi innovativi, analytics e cloud. In questo modo aziende, gestori di infrastrutture e servizi adottando la piattaforma ottengono, nativamente, soluzioni sicure.

Per ulteriori informazioni: <https://www.schneider-electric.com/en/work/solutions/cybersecurity/>