

La tecnologia come alleato strategico nella protezione degli ambienti produttivi

Ansaldo Energia sceglie le soluzioni TXOne Networks per proteggere gli impianti critici senza impattare sulla continuità operativa.

Introduzione

Nata a Genova nel 1853, Ansaldo ha contribuito nei decenni successivi all'industrializzazione dell'Italia. Profondamente radicata nel territorio, l'azienda ha costruito nel tempo un patrimonio di competenze industriali e tecnologiche di primo piano, diventando un punto di riferimento nella progettazione e realizzazione di soluzioni per la produzione di energia.

Nel 1991 nasce Ansaldo Energia, che ha intrapreso un percorso di progressiva specializzazione nel settore della generazione elettrica, affermandosi come uno dei principali player a livello internazionale. Il quartier generale è tuttora a Genova, mentre il Gruppo è oggi presente in oltre 30 Paesi nel mondo, con più di 3.500 dipendenti.

Il core business di Ansaldo Energia comprende la progettazione e la produzione di turbine a gas, turbine a vapore e generatori, oltre alla realizzazione di impianti completi per la produzione di energia. A queste attività si affianca un'ampia offerta di servizi ad alto valore aggiunto che include manutenzione, upgrade tecnologici, monitoraggio delle prestazioni degli impianti e soluzioni avanzate di manutenzione predittiva.

txone.com

TXOne Networks | Cybersecurity OT. Semplificata.

ansaldo | energia

"TXOne Networks si è affermata come partner tecnologico ideale in grado di rispondere in modo puntuale alle esigenze di Ansaldo Energia"



Diego Lusso

Cyber Security
OT Manager,
Ansaldo Energia.

L'azienda opera inoltre nel settore nucleare ed è fortemente impegnata nello sviluppo di tecnologie sostenibili attraverso Ansaldo Green Tech, con l'obiettivo di supportare la transizione energetica e i processi di decarbonizzazione dell'industria.

Il contesto

Storicamente, nel settore industriale, la cybersecurity è sempre stata subordinata alle esigenze operative – racconta Diego Lusso, Cyber Security OT Manager presso Ansaldo Energia. La priorità assoluta era garantire la continuità del processo produttivo: tutto doveva funzionare senza interruzioni. In questa prospettiva, la sicurezza informatica era spesso vista come un elemento da integrare con attenzione, per garantire protezione senza compromettere l'efficienza operativa

Per molto tempo, inoltre, la protezione degli ambienti industriali è stata affidata a presunti fattori di sicurezza, come l'isolamento dei sistemi OT o l'utilizzo di protocolli proprietari poco diffusi. Con il progressivo evolversi degli scenari di minaccia, questi approcci si sono però rivelati insufficienti, trasformandosi in veri e propri falsi miti.

La crescente integrazione tra mondo IT e OT, insieme alla digitalizzazione degli impianti, ha definitivamente superato l'idea di un ambiente industriale chiuso e intrinsecamente sicuro. Di conseguenza, la superficie di attacco si è ampliata e le vulnerabilità sono diventate più evidenti.

“In questo scenario, la sfida non è solo tecnologica, ma anche culturale - prosegue Lusso. È necessario superare una visione che considera la cybersecurity come un problema, vedendola invece come un fattore abilitante della continuità operativa e del business. Fortunatamente – ci spiega Lusso – in Ansaldo Energia il management ha sempre dimostrato una forte sensibilità su questi temi, non solo per rispondere agli obblighi normativi, ma proprio per una scelta strategica consapevole orientata alla protezione degli impianti e del valore aziendale”.

Sfide e soluzioni

“L'adozione delle soluzioni TXOne nasce da un'iniziativa del top management di Ansaldo Energia, che ha promosso un assessment strutturato con l'obiettivo di individuare criticità e vulnerabilità in ambito cybersecurity, con un focus specifico sugli asset OT più sensibili dal punto di vista operativo” – spiega Lusso.

Seguendo anche le indicazioni dello standard internazionale IEC 62443, riferimento per la sicurezza degli ambienti industriali, è stata condotta pertanto un'analisi approfondita su impianti e fabbriche di Ansaldo Energia che ha evidenziato la necessità di proteggere sistemi OT spesso basati su piattaforme legacy, caratterizzate da risorse di calcolo e memoria limitate, attraverso soluzioni progettate nativamente per il contesto industriale.

In questo quadro, TXOne Networks si è affermata come partner tecnologico ideale in grado di rispondere in modo puntuale alle esigenze di Ansaldo Energia.

Il primo passo è stato l'adozione di **Stellar**, la soluzione di endpoint protection basata su approccio AllowList, particolarmente indicata per gli ambienti OT. “Stellar è un software estremamente leggero, compatibile anche con sistemi operativi datati, che ci ha permesso di sostituire antivirus IT tradizionali non più aggiornabili e poco adatti a contesti in cui anche un falso positivo può avere un impatto diretto sulla produzione” - spiega Lusso.

“Nel mondo OT, infatti, anche un'interruzione di pochi minuti può generare conseguenze rilevanti. La tecnologia whitelist di Stellar, basata su certificati e sull'identificazione puntuale delle applicazioni legittime – inclusi quelli rilasciati dai vendor delle macchine – consente di distinguere con precisione le attività autorizzate da quelle potenzialmente malevoli. In questo modo si riducono drasticamente i falsi positivi, garantendo al contempo la continuità operativa. Un ulteriore elemento distintivo è la possibilità di operare anche in assenza di connessione diretta a Internet, requisito fondamentale in ambienti industriali sensibili”.

A partire da questa prima implementazione, Ansaldo Energia ha progressivamente esteso l'adozione delle soluzioni TXOne Networks lungo diversi livelli di protezione.

“Le **Portable Inspector** sono state introdotte per la scansione di macchine particolarmente delicate, sulle quali non è possibile installare software di sicurezza”- continua Lusso. Questi dispositivi consentono di effettuare controlli antimalware in modo non invasivo e di raccogliere informazioni utili anche su asset non connessi alla rete, supportando le attività di asset inventory in contesti complessi”.

Le Portable Inspector integrano inoltre una memoria cifrata per il trasferimento sicuro dei file, con scansione automatica dei contenuti. Questa funzionalità garantisce che nessun malware venga introdotto nei sistemi produttivi, rispondendo anche alle crescenti richieste dei clienti di Ansaldo Energia in tema di sicurezza dei software installati sugli impianti.

Per rafforzare ulteriormente il controllo sugli storage rimovibili, Ansaldo Energia ha adottato anche **SafePort**, una soluzione che permette di verificare e mettere in sicurezza i dispositivi USB utilizzati dal personale di manutenzione. “SafePort consente di superare definitivamente il falso mito della sicurezza garantita dal semplice isolamento degli impianti, introducendo un controllo strutturato e centralizzato dei supporti rimovibili” – puntualizza Lusso.

Infine, è in corso l'implementazione delle soluzioni **EDGEIPS**, dedicate alla protezione del traffico di rete verso gli asset più critici. Questi dispositivi consentono sia il monitoraggio delle comunicazioni (funzione IDS), sia il blocco del traffico potenzialmente pericoloso (funzione IPS), con un'elevata flessibilità di configurazione. Questo approccio permette di privilegiare inizialmente la visibilità e la rilevazione, riducendo il rischio di falsi positivi. Grazie a EDGEIPS, Ansaldo Energia ha ottenuto una maggiore visibilità sui flussi di dati provenienti dai computer dei manutentori, sia in loco sia da remoto, verso i sistemi OT critici.

Nel complesso, l'adozione delle soluzioni TXOne Networks ha consentito ad Ansaldo Energia di costruire una difesa multilivello, migliorando significativamente il livello di sicurezza degli ambienti OT senza compromettere l'efficienza e la continuità operativa.

La fiducia

La cybersecurity non rappresenta mai uno stato definitivo. Non esiste una condizione in cui si possa dire di essere completamente al sicuro: alla crescita delle difese corrisponde infatti un'evoluzione continua delle capacità degli attaccanti e il numero di minacce è in costante aumento.

“Dal punto di vista operativo, rafforzare la sicurezza senza incidere sulla produttività è un percorso continuo, che va oltre la semplice implementazione delle tecnologie. È stato fondamentale costruire nel tempo la fiducia delle persone che operano quotidianamente nelle fabbriche e negli impianti, superando le iniziali resistenze” – precisa Lusso.

“Questo percorso è stato agevolato da un approccio fortemente collaborativo con gli esperti TXOne. Le soluzioni adottate si sono evolute anche grazie al confronto costante del nostro team di Ansaldo Energia con il team di TXOne Networks con un'attenzione puntuale alle specificità delle singole macchine: un lavoro congiunto – sottolinea Lusso – che ci ha permesso di introdurre la sicurezza in modo graduale e consapevole, senza impatti sui processi produttivi e favorendo l'accettazione da parte di chi lavora direttamente sulle macchine”.

“Questo percorso è stato agevolato da un approccio fortemente collaborativo con gli esperti TXOne”

Caso di successo

Scenari futuri

Guardando al futuro, la cybersecurity industriale si troverà sempre più al centro di un equilibrio complesso tra nuove minacce e opportunità tecnologiche, in particolare legate all'intelligenza artificiale. Se da un lato strumenti di calcolo avanzati e algoritmi sofisticati possono aumentare il livello di rischio per gli impianti industriali, dall'altro offrono nuove possibilità di difesa.

“In ambito OT, una delle criticità principali resta la gestione dei falsi positivi, che possono compromettere la fiducia degli operatori nelle piattaforme di sicurezza. In questo contesto, l'IA può giocare un ruolo chiave, migliorando l'analisi dei dati e consentendo interventi più rapidi e mirati. Il futuro della cybersecurity industriale sarà quindi sempre più una sfida condivisa, in cui l'innovazione tecnologica diventa un alleato strategico nella protezione degli ambienti produttivi” – conclude Lusso.

Informazioni su TXOne Networks

TXOne Networks fornisce soluzioni di cybersecurity che assicurano l'affidabilità e la sicurezza dei sistemi di controllo industriale e degli ambienti di tecnologia operativa. L'azienda collabora con i principali produttori e operatori di infrastrutture critiche per sviluppare approcci pratici e operativi alla difesa informatica. TXOne Networks propone prodotti sia per la rete che per gli endpoint, proteggendo la rete OT e i dispositivi mission-critical attraverso un approccio di difesa in profondità in tempo reale. Per ulteriori informazioni, visitate www.txone.com.

txone.com

TXOne Networks | Cybersecurity OT. Semplificata.

