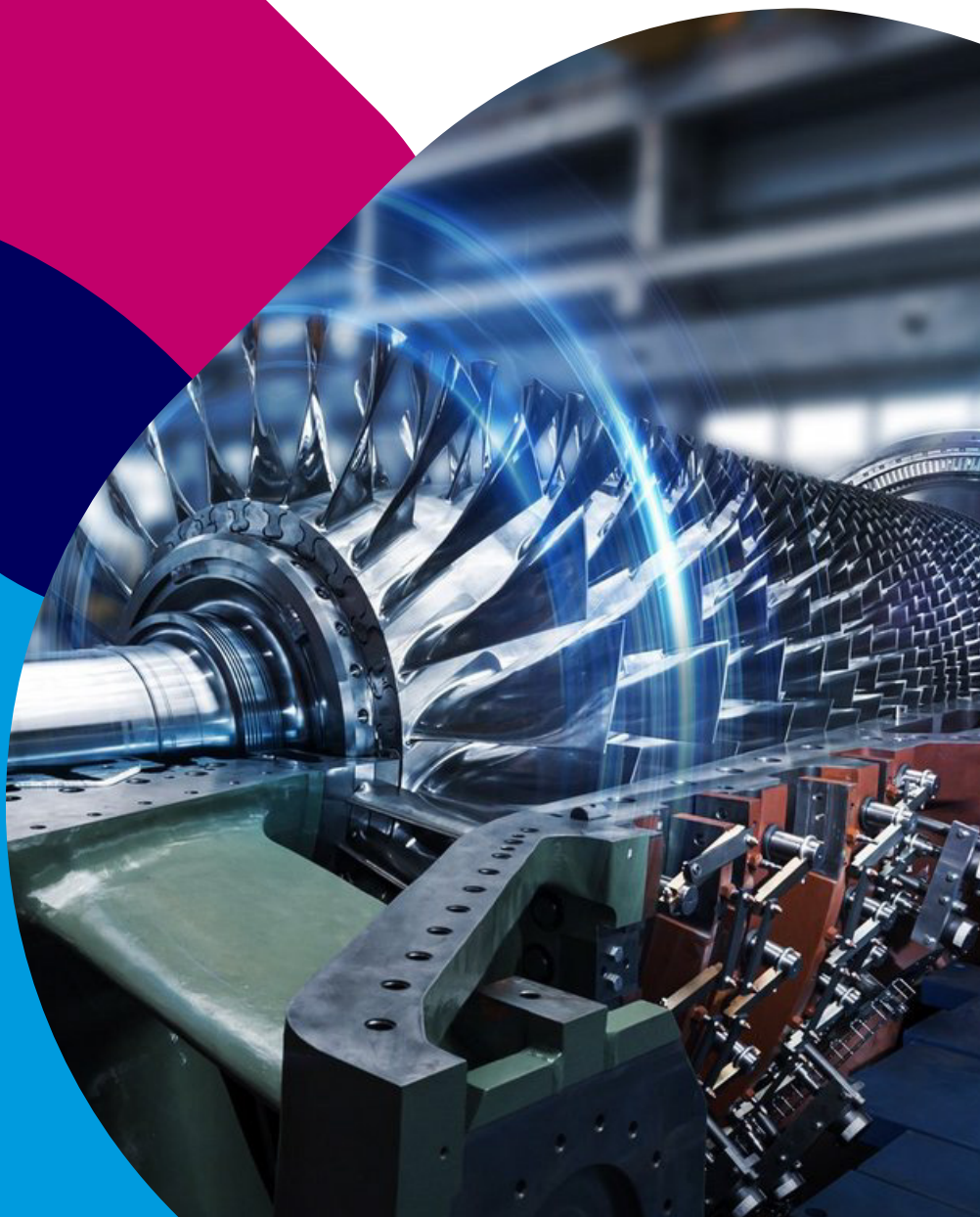
Proteggere le infrastrutture energetiche: L'approccio multi-step di Ansaldo Energia all'industrial cybersecurity



HWG Sababa

ansaldo | energia

Ansaldo Energia

- **170 anni di esperienza con la partecipazione a centinaia di progetti internazionali**
- **Presenza in più di 35 Paesi in tutto il mondo**
- **Attualmente ha un organico di oltre 3.300 persone**

Introduzione

L'evoluzione dei requisiti di sicurezza è un processo naturale per qualsiasi operatore del settore energetico con una lunga storia alle spalle. Nel corso di un secolo, queste aziende sperimentano un'interazione dinamica tra progressi tecnologici, cambiamenti normativi e rivoluzioni sociali che modellano il loro approccio alla salvaguardia delle operazioni, degli asset e del personale.

Solo nel XX secolo si è passati da misure di sicurezza fisica - tra cui il controllo degli accessi, la sorveglianza, la protezione del perimetro - e una formazione basilare in materia di safety, a sistemi di sicurezza elettronici avanzati e a norme standardizzate sulla salute e la sicurezza dei lavoratori e dell'ambiente. Il secolo corrente ha inaugurato l'era digitale, portando alla luce il tema della sicurezza informatica: la protezione contro le minacce, le violazioni dei dati e i cyber-attacchi è emersa come priorità fondamentale. Allo stesso tempo, la formazione in materia di safety ha raggiunto livelli più avanzati, sono state integrate pratiche ergonomiche e si è registrata una maggiore conformità a normative stringenti.

Con centinaia di centrali elettriche dall'inaugurazione della prima nel lontano 1923, anche **Ansaldo Energia** ha esplorato i panorami dinamici di security, safety e cybersecurity, adattando costantemente le proprie strategie per soddisfare le esigenze in continua evoluzione di un mondo sempre più moderno.

Oggi, l'integrazione della digitalizzazione e della connettività negli ambienti industriali impone un approccio olistico alla sicurezza, che comprenda misure di sicurezza fisica, adeguati protocolli, iniziative di formazione continua, conformità a standard normativi, nonché soluzioni di cybersecurity specifiche per il settore.

"Il settore industriale sta abbracciando fortemente la trasformazione digitale e il concetto di Industria 4.0, portando ad una crescente connettività e convergenza tra IT e OT. Fino a poco tempo fa, erano pochissimi i sistemi OT connessi, oggi lo sono quasi tutti" **ha commentato Stefano Santucci, CIO di Ansaldo Energia**, *"Gestire efficacemente la sicurezza in un ambiente OT richiede conoscenze mirate ed un approccio di tipo olistico che consentano di affrontare sfide, vulnerabilità e rischi specifici".*

Il progetto

Quando si tratta di grandi imprese con anni di storia alle spalle ed un ambiente complesso, la definizione di un'efficace strategia di cybersecurity non si limita all'implementazione di tecnologie, ma richiede l'attenta formulazione di un piano d'azione composto da molteplici fasi. Forte di una partnership consolidata e proficua, Ansaldo Energia si è rivolta ad **HWG Sababa** per la realizzazione di questo progetto multi-step.

Step 1. Industrial Cybersecurity Training per gli Ingegneri d'Impianto

Nella fase finale della prima collaborazione con Sababa Security per la messa in sicurezza della propria infrastruttura IT, Ansaldo Energia aveva ritenuto fondamentale integrare nel progetto una formazione specifica in materia di industrial cybersecurity, finalizzata a fornire agli ingegneri tutti gli strumenti necessari per sviluppare, gestire e integrare i prodotti in modo sicuro e conforme. Tra i quasi 100 partecipanti, alcuni sono diventati un vero e proprio punto di riferimento in azienda per la sicurezza OT.

"Questa formazione in ambito OT è stata un vero successo, e non solo per l'alta qualità dei contenuti e la grande competenza degli esperti che li hanno erogati, ma anche perché ha fatto sì che tutti gli operatori iniziassero a considerare il team di Cyber Security Operation (CSO) come un centro di competenza per la sicurezza industriale", **ha spiegato Marco Grillo, Deputy General Manager di Ansaldo Energia** *"Visti i risultati, la nostra intenzione è quella di svolgere questo tipo di training su base regolare, soprattutto dopo l'introduzione della Direttiva NIS 2. I clienti, infatti, ci chiedono quotidianamente di rispettare determinati requisiti di cybersecurity, quindi vorrei che la formazione fosse un processo continuo, soprattutto per coloro che lavorano negli impianti".*

Step 2. Micro-Segmentazione per Mitigare i Rischi

Il secondo passo di Ansaldo Energia verso il rafforzamento della propria security posture è stato **l'implementazione della micro-segmentazione**. Il processo - durato circa 3 mesi - ha avuto come obiettivo finale la suddivisione della rete in segmenti più piccoli e isolati, ciascuno contenente uno specifico macchinario di produzione, che non poteva comunicare con altri sulla stessa rete. Questa fase ha visto un ottimo lavoro di squadra tra Ansaldo Energia, HWG Sababa e digipoint; la parte più complicata è stata la valutazione del traffico di rete che poteva essere consentito ad ogni singola macchina.

"Questo approccio proattivo è estremamente importante per Ansaldo Energia. Infatti, come molti altri operatori del settore energetico, Ansaldo dispone anche di sistemi legacy che non possono essere facilmente aggiornati a causa di problemi di compatibilità. L'isolamento fornisce un livello di sicurezza anche per i sistemi più vecchi, salvaguardandoli dalle moderne minacce informatiche", **ha commentato Diego Lusso Cybersecurity Analyst di HWG Sababa**, *"Inoltre, con la micro-segmentazione, eventuali movimenti laterali sono drasticamente ridotti, impedendo la diffusione di potenziali attacchi ad altre parti della rete e riducendo al minimo i rischi".*

Step 3. ISA/IEC 62443 Assessment

La sicurezza non è solo una questione di tecnologie, ma riguarda anche i processi organizzativi, i comportamenti degli utenti, le policy e le procedure. Per questo motivo, Ansaldo Energia e HWG Sababa non hanno esitato ad includere l'**assessment** nel loro progetto.

Con l'obiettivo di avere un quadro accurato della postura della sicurezza e di identificare le aree di miglioramento, il team di HWG Sababa ha condotto un audit sulla base dell'ISA/IEC 62443, uno standard ampiamente riconosciuto dedicato alla sicurezza per i sistemi di automazione e controllo industriale.

"Dopo aver identificato gli obiettivi e lo scopo dell'attività, abbiamo stabilito i criteri di audit sulla base dei requisiti dell'ISA/IEC 62443" **ha spiegato Irene Parodi, Cybersecurity Analyst di HWG Sababa** *"Abbiamo intervistato molti degli stakeholder di Ansaldo Energia, ispezionato ogni angolo degli impianti, verificato l'applicazione di policy e procedure, identificato le vulnerabilità e dato loro una priorità in base al potenziale impatto e rischio. L'intero audit è durato circa 2 mesi".*

Al termine dell'attività, il team di HWG Sababa ha elaborato un report dettagliato, comprensivo di risultati, osservazioni e suggerimenti per il miglioramento. Sulla base di questo, insieme agli stakeholder di Ansaldo Energia, hanno poi sviluppato una roadmap di azioni correttive da implementare, che riguardavano principalmente aspetti organizzativi, di policy e procedurali.

Step 4. Scouting di Soluzioni Tecniche

Parallelamente alla messa a punto delle azioni correttive individuate nell'ambito dell'assessment, il colosso energetico ha rivolto il suo sguardo al mercato per individuare le soluzioni di sicurezza che potessero proteggere al meglio i propri impianti produttivi e garantire una maggiore prevenzione e rilevazione delle minacce.

Dopo approfondite ricerche e test - con il supporto di HWG Sababa - la scelta di Ansaldo Energia è ricaduta su due importanti player del settore industriale, **Radiflow** e **TXOne Networks**. Mentre i prodotti del primo sono stati implementati per l'analisi del traffico OT e il risk assessment, le soluzioni del secondo sono state scelte per aumentare la sicurezza di postazioni obsolete e non aggiornabili, oltre che per proteggere le comunicazioni critiche con IPS industriali. Tutte le soluzioni implementate sono sottoposte ad un monitoraggio continuo tramite il Security Operations Center di HWG Sababa.

Bilanciare la continuità operativa con una fluida integrazione delle misure di cybersecurity si è rivelata una sfida su più fronti che ha richiesto un'attenta pianificazione ed esecuzione.

"La parte più difficile è stata trasmettere internamente il messaggio che l'implementazione di queste soluzioni non avrebbe influito sull'operatività. La chiave è vedere la sicurezza, la safety, la compliance e la continuità operativa come componenti interconnesse che insieme contribuiscono alla resilienza e al successo dell'organizzazione", **ha commentato Ivan Monti, CISO & Head of IT Infrastructure Operations di Ansaldo Energia** *"Fortunatamente, la cybersecurity è un concetto ben consolidato tra i nostri operatori OT, soprattutto dopo il training a cui hanno preso parte, e questo ci ha aiutato a superare in breve tempo l'apprensione iniziale".*

Risultati e prossimi step

Nonostante l'ambizione e la complessità del progetto, gli obiettivi inizialmente fissati sono stati raggiunti con successo, consolidando ulteriormente il rapporto tra il colosso energetico ed HWG Sababa.

Inoltre, avendo bene a mente che la cybersecurity non è una procedura una tantum, ma un processo continuo che si evolve di pari passo con le minacce e le tecnologie, Ansaldo Energia ha già le idee ben chiare su quali saranno le prossime mosse.

“Con HWG Sababa, ci siamo concentrati finora sulla sicurezza dei nostri impianti di produzione, ma ora stiamo lavorando attivamente per monitorare anche le centrali elettriche e le turbine che forniamo ai nostri clienti in tutto il mondo", **ha spiegato Ivan Monti, CISO & Head of IT Infrastructure Operations di Ansaldo Energia** *“Il prossimo passo sarà quello di portare la sicurezza delle centrali elettriche e delle turbine più vecchie allo stesso livello di maturità di quelle più recenti, soprattutto in vista delle nuove normative e dei nuovi requisiti del settore”.*

Un ulteriore obiettivo è quello di allestire una cyber demo room all'interno della Sala Prove Generatori di Ansaldo Energia, dove viene testata la qualità dei generatori usciti dalle linee di produzione interne. Poiché la sua struttura e automazione presentano molte similarità con gli impianti dei clienti di Ansaldo, è stata scelta come banco di prova adatto a mostrare - attraverso dashboard dedicate - le contromisure di sicurezza che possono essere adottate per proteggere i sistemi di produzione di energia.

HWG Sababa

ansaldo | energia

Follow us on:

www.hwgsababa.com
contacts@hwgsababa.com