Caso di successo

Proteggere le infrastrutture critiche: come Valmet migliora la sicurezza dei sistemi di controllo industriale con TXOne Networks

Di fronte a rigide esigenze di cybersecurity e ad ambienti industriali complessi, Valmet aveva bisogno di una protezione robusta che non compromettesse la continuità operativa. La scelta di TXOne Networks ha permesso a Valmet di integrare in modo fluido la cybersecurity nativa OT nelle proprie soluzioni di automazione – rafforzando la fiducia dei clienti, semplificando la conformità normativa e stabilendo nuovi standard per la sicurezza dei sistemi di controllo industriale.

La situazione

Valmet è un'azienda globale con sede in Finlandia, leader nell'automazione industriale e nella produzione di macchinari, che serve settori critici come la produzione di cellulosa e carta, la generazione di energia e le industrie di processo. L'azienda impiega circa 19.000 professionisti in tutto il mondo e mantiene una forte presenza in Germania, dove molti dei suoi clienti operano infrastrutture nazionali essenziali. La tecnologia di automazione di Valmet – inclusi i suoi sistemi di controllo distribuito di punta, come Valmet DNAe – rappresenta la spina dorsale operativa di grandi impianti industriali, dalle cartiere alle centrali elettriche, garantendo processi produttivi stabili e continui.

Negli ultimi anni, la cybersecurity è emersa come una sfida cruciale. I clienti di Valmet, soprattutto quelli classificati come operatori di infrastrutture critiche, si trovano ad affrontare normative sempre più stringenti, come la direttiva europea NIS2. Queste normative richiedono ai fornitori come Valmet di

"Con TXOne, siamo in grado di fornire una sicurezza informatica nativa OT su misura per le esigenze specifiche degli ambienti industriali."

Teemu Kiviniemi
Solution Manager OT Cybersecurity, Valmet

offrire sistemi di automazione con funzionalità di sicurezza informatica avanzate e integrate.

"I nostri clienti gestiscono macchine critiche per interi Paesi – come le centrali elettriche. Si fidano di noi per garantire che questi sistemi siano sicuri," spiega **Teemu Kiviniemi**, Solution Manager, OT Cybersecurity di Valmet, e aggiunge: "Con TXOne, possiamo fornire una cybersecurity nativa OT in grado di affrontare le particolarità degli ambienti industriali."

A differenza dei sistemi IT, i sistemi di controllo industriale non possono essere aggiornati o riavviati liberamente. Alcuni clienti di Valmet utilizzano apparecchiature datate che non possono ricevere patch regolarmente, lasciando potenziali falle di sicurezza. Per questo motivo, Kiviniemi definisce la gestione delle patch "il problema più grande della cybersecurity OT". Se le misure di sicurezza sono inadeguate – per esempio soluzioni IT che impongono riavvii imprevisti – si rischiano fermi impianto catastrofici.

"Immaginate una soluzione di sicurezza che si riavvia nel momento sbagliato: una centrale elettrica potrebbe spegnersi, causando blackout diffusi e lasciando gran parte della Germania senza energia," sottolinea Kiviniemi.

Valmet aveva bisogno di una soluzione progettata specificamente per l'ambiente industriale – capace di proteggere in modo affidabile i sistemi legacy e offrire protezione continua e automatica senza rischiare interruzioni operative.

La transizione

Riconoscendo questi requisiti fondamentali, Valmet ha iniziato a valutare potenziali partner di cybersecurity. In passato, si era affidata a prodotti di sicurezza basati su IT tradizionale, ma è stato chiaro fin da subito che tali strumenti non erano più adeguati agli ambienti OT.

"C'è una netta differenza tra sicurezza IT e OT. Gli strumenti IT utilizzati in OT di solito si limitano a rilevare le minacce, ma noi avevamo bisogno di qualcosa progettato per la tecnologia operativa, che prevenisse attivamente gli attacchi in tempo reale," afferma Kiviniemi.

Il partner giusto è emerso quando TXOne Networks ha contattato direttamente Valmet. Fin dal primo incontro, Valmet ha percepito TXOne come diversa dai concorrenti: offriva soluzioni sviluppate appositamente per ambienti OT, in grado di affrontare esattamente i vincoli e i rischi riscontrati. Dopo i primi colloqui, Valmet ha deciso di valutare in profondità l'intero portafoglio di prodotti TXOne.

I test sono stati rigorosi e approfonditi, durando quasi due anni. I team di ingegneria di Valmet e TXOne hanno collaborato strettamente per integrare la tecnologia di sicurezza informatica nei sistemi di automazione Valmet. Le sfide tecniche non sono mancate, ma il team di TXOne ha risposto in modo rapido e proattivo.

"Abbiamo incontrato i tipici problemi di integrazione, ma TXOne ci ha supportati passo dopo passo, effettuando gli aggiustamenti necessari tempestivamente," spiega Kiviniemi. "Trattiamo i prodotti TXOne come se fossero nostri; se qualcosa non funziona subito, la risolviamo insieme."

Valmet ha infine integrato diverse soluzioni TXOne, tra cui la suite di protezione degli endpoint **Stellar**, le difese di rete **EdgeIPS**, e strumenti di **virtual patching**. Quest'ultima funzionalità si è rivelata cruciale: il patching virtuale consente di proteggere i sistemi a livello di rete fino alla successiva manutenzione programmata, mantenendo i sistemi sicuri anche quando non è possibile applicare patch immediate.

Valmet ha inoltre garantito che la cybersecurity fosse pienamente integrata nella propria infrastruttura di servizi. Ha formato la propria rete globale di ingegneri per distribuire e gestire le tecnologie TXOne.

"Gli stessi ingegneri che installano e mantengono i sistemi di controllo possono gestire anche la cybersecurity. È tutto integrato, trasparente e semplice," afferma Kiviniemi.

Il risultato

Oggi molte soluzioni di automazione Valmet includono di serie la cybersecurity nativa OT fornita da TXOne Networks. L'impatto è stato notevole: i clienti non devono più preoccuparsi di vulnerabilità non protette o di interruzioni operative causate da aggiornamenti IT. La protezione continua è ora parte integrante dell'offerta Valmet.

La continuità operativa – priorità assoluta per gli operatori di infrastrutture critiche – è garantita da soluzioni che proteggono anche i sistemi legacy durante lunghi ritardi di patching.

"Se emerge una vulnerabilità, i nostri clienti sanno che i loro sistemi restano protetti fino alla prossima manutenzione programmata. È tranquillità," dice Kiviniemi.

Questa strategia ha rafforzato la posizione di mercato di Valmet. I clienti vedono ora Valmet non solo come un fornitore di macchinari, ma come un partner affidabile in materia di cybersecurity. La conformità normativa, in particolare con la NIS2, è diventata più semplice grazie a soluzioni già conformi ai più alti standard di sicurezza.

L'integrazione delle tecnologie TXOne ha aperto nuove opportunità: Valmet offre oggi servizi dedicati di cybersecurity, dalle valutazioni di rischio al monitoraggio remoto fino alla risposta agli incidenti, creando nuove opportunità di business.

L'approccio di Valmet rappresenta un passo decisivo per il settore dell'automazione industriale.

"La cybersecurity è uno sport di squadra," conclude Kiviniemi. "Con TXOne, abbiamo dimostrato che proteggere le infrastrutture critiche può essere fatto in modo proattivo, completo e fluido – senza compromettere le prestazioni operative."

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.