txOne networks

Customer Story

Schutz Kritischer Infrastrukturen: Wie Valmet die Sicherheit industrieller Steuerungssysteme mit TXOne Networks stärkt

Angesichts strenger Anforderungen bei der Cybersicherheit und komplexer Industrieumgebungen benötigte Valmet eine robuste Lösung, die den laufenden Betrieb nicht beeinträchtigt. Mit TXOne Networks konnte Valmet OT-native Cybersicherheit nahtlos in seine Automatisierungslösungen integrieren – das stärkt das Vertrauen der Kunden, vereinfacht die Einhaltung regulatorischer Vorgaben und setzt neue Maßstäbe für die Sicherheit industrieller Steuerungssysteme.

Die Ausgangssituation

Valmet ist ein in Finnland ansässiger, weltweit führender Anbieter von Industrieautomatisierung und Maschinenbau – insbesondere in den Bereichen Zellstoff- und Papierproduktion, Energieerzeugung und Prozessindustrie. Das Unternehmen beschäftigt rund 19.000 Mitarbeitende weltweit und verfügt über eine starke Präsenz in Deutschland, wo viele Kunden zur kritischen nationalen Infrastruktur zählen.

Valmets Automatisierungstechnologie – darunter das Flaggschiff-System **Valmet DNAe** – bildet das operative Rückgrat zahlreicher Industrieanlagen, von Papierfabriken bis hin zu Kraftwerken, und gewährleistet stabile, kontinuierliche Produktionsprozesse.

In den letzten Jahren ist Cybersicherheit zu einer zentralen Herausforderung geworden. Kunden von Valmet, insbesondere Betreiber kritischer Infrastrukturen, unterliegen zunehmend strengen Anforderungen wie

Valmet

"Mit TXOne können wir OT-native Cybersicherheit bereitstellen, die auf die speziellen Anforderungen industrieller Umgebungen zugeschnitten ist."

Teemu Kiviniemi
Solution Manager OT Cybersecurity bei Valmet

der **EU-Richtlinie NIS2**, die von Anbietern verlangt, Automatisierungssysteme mit integrierten, fortschrittlichen Sicherheitsfunktionen zu liefern und das Ermitteln und Abstellen von Schwachstellen zu dokumentieren.

„Unsere Kunden betreiben Maschinen, die für ganze Länder essenziell sind – beispielsweise Kraftwerke. Sie vertrauen darauf, dass wir diese Systeme absichern", erklärt **Teemu Kiviniemi**, Solution Manager OT Cybersecurity bei Valmet. „Mit TXOne können wir OT-native Cybersicherheit bereitstellen, die auf die speziellen Anforderungen industrieller Umgebungen zugeschnitten ist."

Industrielle Steuerungssysteme unterscheiden sich stark von IT-Systemen: Updates oder Neustarts sind nur mit sorgfältiger Planung möglich. Viele Kunden betreiben ältere Anlagen, die nicht regelmäßig gepatcht werden können – ein erhebliches Sicherheitsrisiko. Kiviniemi bezeichnet das Patch-Management daher als „das größte Einzelproblem in der OT-Cybersicherheit". Ungeeignete Sicherheitsmaßnahmen – etwa IT-Lösungen, die unerwartete Neustarts erzwingen – könnten katastrophale Ausfälle verursachen.

„Stellen Sie sich vor, eine Sicherheitslösung startet zur falschen Zeit neu: Ein Kraftwerk könnte ausfallen, und große Teile Deutschlands wären ohne Strom", warnt Kiviniemi.

Valmet suchte daher eine Lösung, die speziell für industrielle Umgebungen entwickelt wurde – mit zuverlässigem Schutz auch für Legacy-Systeme und kontinuierlicher, automatischer Absicherung ohne Betriebsunterbrechungen.

Die Umsetzung

Mit diesen Anforderungen begann Valmet, potenzielle Cybersicherheitspartner zu evaluieren. Frühere IT-basierte Sicherheitsprodukte erwiesen sich als unzureichend. „Es gibt einen klaren Unterschied zwischen IT- und OT-Sicherheit. IT-Tools erkennen Bedrohungen meist nur – wir brauchten etwas, das speziell für operative Technologie entwickelt wurde und Angriffe in Echtzeit aktiv verhindert", so Kiviniemi.

Die passende Partnerschaft ergab sich, als **TXOne Networks** direkt auf Valmet zukam. Von Anfang an erkannte Valmet, dass TXOne anders war als andere Anbieter: Die Lösungen wurden explizit für OT-Umgebungen konzipiert und adressierten genau die Herausforderungen, mit denen Valmet konfrontiert war. Nach ersten Gesprächen entschied sich Valmet für eine umfassende Evaluierung des gesamten TXOne-Portfolios.

Die Tests dauerten fast zwei Jahre und waren äußerst gründlich. Ingenieurteams beider Unternehmen arbeiteten eng zusammen, um die Sicherheitslösungen in Valmets Automatisierungssysteme zu integrieren. Technische Anpassungen waren erforderlich, doch TXOne reagierte schnell und proaktiv.

„Wir hatten typische Integrationsherausforderungen, aber TXOne unterstützte uns in jeder Phase und nahm Anpassungen umgehend vor", erklärt Kiviniemi. „Wir behandeln TXOne-Produkte, als wären es unsere eigenen – wenn etwas nicht sofort funktioniert, lösen wir es gemeinsam."

Valmet integrierte schließlich mehrere TXOne-Lösungen, darunter die **Stellar Endpoint Protection Suite, EdgeIPS**-Netzwerkschutzlösungen und Tools für **virtuelles Patching**. Letzteres war besonders entscheidend: Virtuelles Patching schützt Systeme auf Netzwerkebene vor Schwachstellen, bis reguläre Wartungsarbeiten stattfinden. So bleiben auch ungepatchte Systeme sicher.

Ebenso wichtig war, dass Valmet Cybersicherheit fest in seine bestehende Serviceinfrastruktur einbettete. Das Unternehmen schulte sein weltweites Serviceteam in der Implementierung und Verwaltung der TXOne-Technologien. „Wir benötigen kein separates Cybersecurity-Team", so Kiviniemi. „Unsere Servicetechniker, die die Steuerungssysteme installieren und warten, können auch die Sicherheitslösungen managen – alles ist integriert, transparent und effizient."

Das Ergebnis

Heute verfügen viele Valmet-Automatisierungssysteme über integrierte, OT-native Cybersicherheitsfunktionen von TXOne Networks. Das Ergebnis: Kunden müssen sich keine Sorgen mehr über ungeschützte Schwachstellen oder IT-Sicherheitsupdates machen, die den Betrieb stören oder gar lahmlegen können. Kontinuierliche Cybersicherheit ist nun Standardbestandteil der Valmet-Lösungen.

Die **Ausfallsicherheit**, oberste Priorität für Betreiber kritischer Infrastrukturen, wird durch Lösungen sichergestellt, die auch ältere Systeme vor Bedrohungen schützen – selbst bei längeren Patch-Intervallen.

„Wenn eine Schwachstelle auftaucht, wissen unsere Kunden: Ihr System bleibt sicher bis zur nächsten Wartung. Das ist echte Sicherheit", sagt Kiviniemi.

Diese strategische Entscheidung hat Valmets Marktposition erheblich gestärkt. Kunden sehen Valmet zunehmend nicht nur als Maschinenlieferanten, sondern als **verlässlichen Cybersicherheitspartner**. Die Einhaltung gesetzlicher Vorgaben – etwa der NIS2 – wurde vereinfacht. Valmet bietet nun Systeme an, die bereits alle Sicherheitsanforderungen erfüllen. Die Compliance ist integraler Bestandteil der Lösung – kein nachträgliches Add-on sind erforderlich.

Darüber hinaus eröffnete die Integration von TXOne neue Geschäftsmöglichkeiten: Valmet bietet heute umfassende **Cybersecurity-Services** – von Risikoanalysen und Fernüberwachung bis hin zu Incident-Response-Leistungen. Dies unterstreicht die proaktive Rolle des Unternehmens in der industriellen Cybersicherheit.

Valmets Ansatz gilt als wegweisend: Die vorausschauende Integration von TXOne-Technologien hebt den Sicherheitsstandard der gesamten Branche.

„Cybersicherheit ist Teamsport", resümiert Kiviniemi. „Gemeinsam mit TXOne zeigen wir, dass der Schutz kritischer Infrastrukturen proaktiv, umfassend und nahtlos möglich ist – ohne Kompromisse bei der Verfügbarkeit."

Über TXOne Networks

TXOne Networks bietet Cybersicherheits-Lösungen, die mithilfe der OT Zero Trust-Methode die Zuverlässigkeit und Sicherheit von industriellen Steuerungssystemen und OT-basierten Produktionsumgebungen gewährleisten. TXOne Networks arbeitet sowohl mit führenden Produktionsunternehmen als auch mit Betreibern kritischer Infrastrukturen zusammen, um praktische, betriebsfreundliche Ansätze für die Cyberabwehr zu entwickeln. TXOne Networks bietet dank seiner Defense-in-Depth-Methode sowohl netzwerk- als auch endpunktbasierte Produkte zur Absicherung von OT-Netzwerken und betriebskritischen Endgeräten in Echtzeit. Mehr erfahren über www.txone.com.