OTORIO ANDRITZ

Pulp and Paper

Enabling NIS2 Security Directive Compliance for a Pulp and Paper Company with RAM² platform

Customer Case Study

Pulp and Paper operational cyber security

The company is a global packaging and paper group that develops and manufactures industrial and consumer packaging solutions. Like other industrial manufacturers, it has a complex operational environment with different types of industrial assets. It was obligated to meet the NIS2 security directive and faced challenges with monitoring its OT cybersecurity posture, as well as lacking asset visibility over its entire operational environment.

The company contacted Andritz to ensure operational resilience based on the NIS2 guidelines, to simplify its OT cyber security management, discover and inventory its OT assets, identify risks, and avoid significant financial impact due to lack of compliance.

NIS2 Implication for the Pulp and paper company

The Pulp & Paper company provides essential products and services, such as paper, packaging, and tissue. A disruption to the Pulp and Paper industry would significantly impact the economy and society, as well as potential environmental implications. Therefore, the Pulp and Paper industry now falls under the regulatory obligations set forth by the NIS2 directive. To ensure operational resilience based on the NIS2 guidelines Pulp and Paper mill operators should implement cybersecurity strategy that addresses the following areas:

- Asset and network visibility
- Protection against cyber-attack
- Operational Risk management
- Incident and Crisis management
- Supply chain security and access management
- Response and recovery planning

What is the NIS2 Directive?

The NIS2 Directive is a legislative framework established by the EU to enhance the cybersecurity and resilience of critical infrastructure sectors. It is becoming the baseline for cybersecurity regulations in the EU and applies to both EU and non-EU organizations that provide services within Member States. The NIS2 Directive addresses the following objectives:

- Strengthen the security requirements
- Secure the supply chains
- Streamline reporting obligations
- More stringent supervisory measures
- Stricter enforcement requirements
- Harmonized sanctions across the EU

Customer challenges

The company lacked visibility over different types of OT industrial assets and did not have a complete digital footprint of its operational environment, the basic steps in securing the supply chain according to NIS2 guidelines.
It experienced a high volume of alert noise from an existing IDS solution, often delivering false positive alerts that led to alert fatigue. It also experienced challenges with:

- Unclear and partial asset visibility, with limited details and poor context
- A lack of information about its OT security environment to properly manage risk
- A high volume of false-positive alerts that created alert fatigue
- Limited resources to address each vulnerability alert
- An inability to prioritize risk effectively and efficiently
- Struggling to accurately detect and proactively respond to actual OT security risks.
- An inability to connect and leverage data sources and existing technologies to properly understand and secure its operational environment.

OTORIO Safe Active Query

OTORIO Safe Active Query discovers and identifies assets and security misconfigurations that are not covered by IDS and can increase digital risk to the asset and the operational process to which it belongs.

Andritz and OTORIO's solution

Andritz's service team, in collaboration with OTORIO's technology, supported the Pulp and Paper company in their efforts for NIS2 Directive compliance. To strengthen the security requirements, Andritz's cybersecurity experts utilized OTORIO's RAM^2 solution for OT cyber risk management. This helped reduce compliance costs and expedite the adoption of an integrated OT cybersecurity strategy. The RAM^2 solution established a comprehensive OT asset inventory and overview by integrating with the company's industrial assets and existing security solutions. It identified different types of physical assets and their communication, gathering high-volume data from:

- ABB DCS environment
- IDS
- Existing firewall
- EDRs
- Active directory
- OTORIO Safe Active query

RAM^2 integrated and proactively monitored the DCS environment communication, firewall and host security events with other siloed security and operational systems data. It excluded irrelevant events such as false positives, ghost assets, and analyzed the data considering the operational context, an asset's physical location on the production floor, and the criticality of business impact. This resulted in delivering comprehensive network visibility of the OT environment.

By utilizing OTORIO Secure & Compliant machinery (SCM) to diagnose assets' compliance data and implementing stringent supervisory measures, RAM^2 conducted security configuration audits to ensure compliance with NIS2 guidelines and the IEC 62443-3 industrial security standard. It identified abnormal behavior in the operational environment and provided OT security insights prioritized by severity level, accompanied by clear mitigation steps to address high-priority risks.

Andritz and OTORIO's expertise in deploying safe integrations, extracting meaningful data from existing security controls, and connecting all OT processes together, including the discovery of process paths and associated risk levels, resulted in a unified view of OT cybersecurity risk management detection and response.

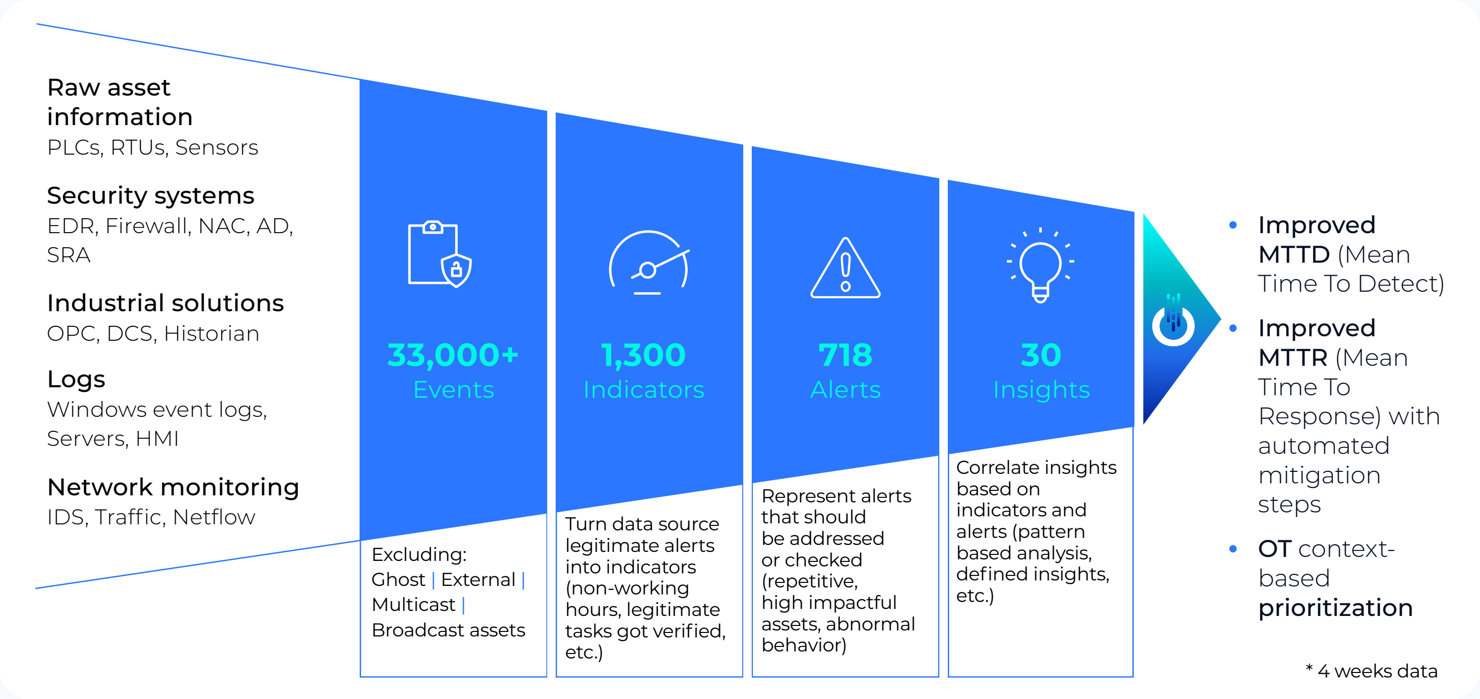
Results

Andritz has a proven track record of providing professional services and possessing extensive knowledge of OT cybersecurity. The combination of OTORIO's technical solutions with the expert team resulted in a seamless integration with the company's industrial assets and existing security controls in the OT environment, delivering a comprehensive asset inventory. RAM^2 strengthens compliance with the NIS2 security directive by enhancing asset attribution with the operational context of OT processes and paths. It assessed the impact level of assets, identified known vulnerabilities, and conducted a thorough assessment of security posture controls and compliance.

The correlation between security posture events and asset inventory provided operational cybersecurity risk identification and noise suppression, enabling the company security team to focus their efforts on what matters most.

The integration of RAM^2 with IDS (Intrusion Detection System) reduced the number of noisy alerts and eliminated assets that were not relevant (e.g., ghost assets) based on rules and pattern configurations. This integration connected all siloed events into a unified view, simplifying the management of OT cybersecurity detection and response processes.

Less noise. More context



Raw asset information
PLCs, RTUs, Sensors

Security systems
EDR, Firewall, NAC, AD, SRA

Industrial solutions
OPC, DCS, Historian

Logs
Windows event logs, Servers, HMI

Network monitoring
IDS, Traffic, Netflow

33,000+ Events

Excluding: Ghost | External | Multicast | Broadcast assets

1,300 Indicators

Turn data source legitimate alerts into indicators (non-working hours, legitimate tasks got verified, etc.)

718 Alerts

Represent alerts that should be addressed or checked (repetitive, high impactful assets, abnormal behavior)

30 Insights

Correlate insights based on indicators and alerts (pattern based analysis, defined insights, etc.)

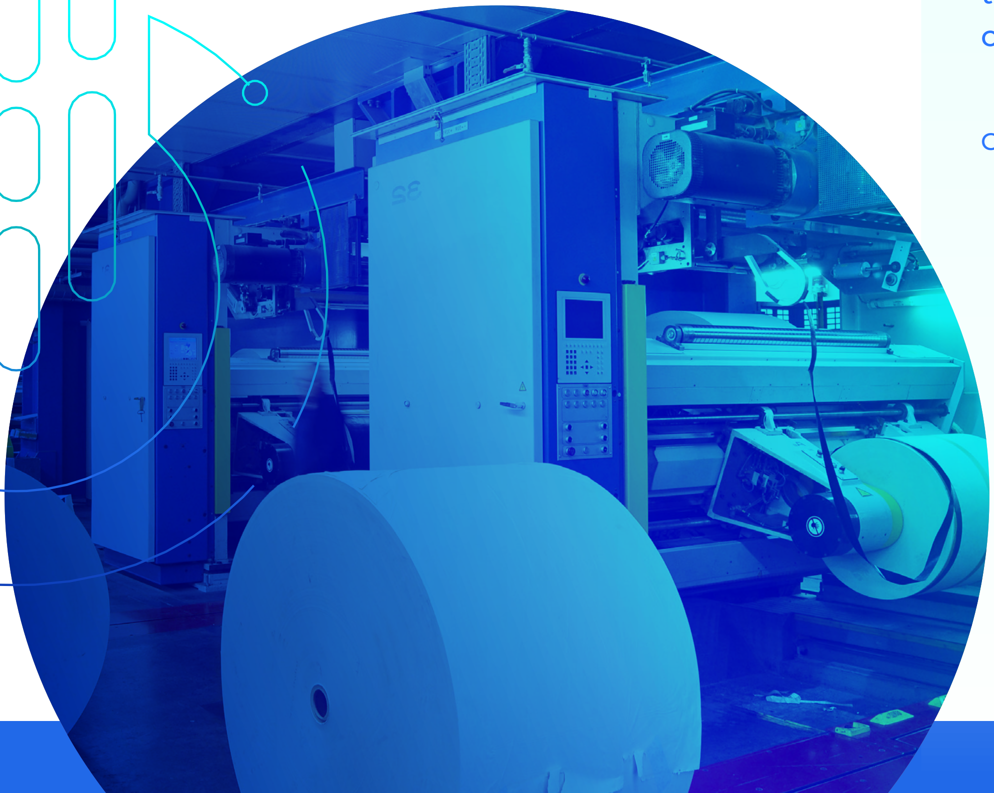
- **Improved MTTD** (Mean Time To Detect)
- **Improved MTTR** (Mean Time To Response) with automated mitigation steps
- OT context-based **prioritization**

* 4 weeks data

Benefits for the Pulp and Paper company

Andritz and OTORIO improved the company preparedness for the NIS2 Directive, safely, efficiently, and effectively with:

- A comprehensive OT assets visibility with a unified view of risk for converged IT-OT-IIoT network security systems and industrial systems in the OT environment.
- The company's security teams have operational context and impact analysis of an asset or process-level for OT risk-based management.
- Exposures identifications based on correlation between security posture and asset inventory.
- OTORIO's RAM^2 provides the company with insights that improved their MTTD and MTTR, while reducing noise and highlighting which risks and vulnerabilities to prioritize.
- The company receives safe operational security posture assessments that don't disturb its ongoing operations.
- The company improved ROI, leveraging existing security controls and solutions by integrating them with OTORIO's RAM^2 platform.
- Maintenance teams now have quick risk mitigation playbooks with clear instructions to harden site-specific OT network risks and vulnerabilities.



> "Our partnership with Andritz and OTORIO helped us to define our operations security policies, and provided the needed tools for continuous governance of their implementation. With the RAM^2 platform we have comprehensive visibility into the OT/ICS and Operations Supporting Systems networks. The platform enables us to get a clear view regarding the risk level of different regions, and allocate proper resources while focusing on the most critical risks. OTORIO's solution is an important enabler for increased operational efficiency through automation and connectivity."

CIO, Pulp & Paper company

OTORIO ANDRITZ

Pulp and Paper

> "With OTORIO's solution we gained full transparency into our asset inventory and network. We are using OTORIO as an overlay on existing controls to create a single source of truth and improve our ROI. OTORIO's RAM^2 improves our team's efficiency through standard processes, automated data collection and vulnerability management, reducing noise, and feasible risk mitigation guidance. OTORIO's platform supports our preparation for compliance with the NIS2 Directive and enables governance and policy enforcement from the single asset and mill levels, up to the regional levels. With OTORIO and Andritz, we can scale the solution to additional sites, without compromising on safety, efficiency and reliability."

OT security global manager, Pulp & Paper company

About ANDRITZ

ANDRITZ is an international technology group providing plants, systems, equipment, and services for various industries. The company is one of the technology and global market leaders in the hydropower business, the pulp and paper industry, the metal working and steel industries, and in solid/liquid separation in the municipal and industrial segments. The listed Group is headquartered in Graz, Austria. Since its foundation 170 years ago, ANDRITZ has developed into a Group with approximately 27,400 employees, and more than 280 locations in over 40 countries worldwide. As a reliable and competent partner, ANDRITZ supports its customers in achieving corporate and sustainability goals.

www.andritz.com

About OTORIO

OTORIO has pioneered an industrial-native OT security platform that enables its customers to achieve an integrated, holistic security strategy for industrial control systems (ICS) and cyber-physical systems (CPS).

Together with its partners, OTORIO empowers operational security practitioners to proactively manage cyber risks and ensure resilient operations. The company's platform provides automated and consolidated visibility of the entire operational network, enabling companies to take control of their security posture, eliminate critical risks, and deliver immediate business value across the organization.

OTORIO's global team combines the extensive mission-critical experience of top nation-state cyber security experts with deep operational and industrial domain expertise.

CN 060723