OTORIO

Pulp and Paper

Extended Asset Visibility for a Pulp & Paper Company

How OTORIO Delivered Actionable OT Security Risk Insights

Case Study

Industrial-native risk management

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 a variety of industrial assets. It faced challenges with monitoring its Operational Technology (OT) cyber security posture and lacked asset visibility over its entire operational environment.

The company contacted OTORIO for a solution to simplify its OT cyber security management, discover and inventory its OT assets, identify risks, and reduce security-notification volume for improved risk management and operational efficiency.

OTORIO RAM² delivered comprehensive OT assets visibility with a unified view of risk for OT, IT, and IIoT-aligned network security systems and industrial systems in the OT environment

Customer Challenges

The company lacked visibility over all of its OT industrial assets and lacked a complete digital footprint of its operational environment. The pulp and paper manufacturer 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:

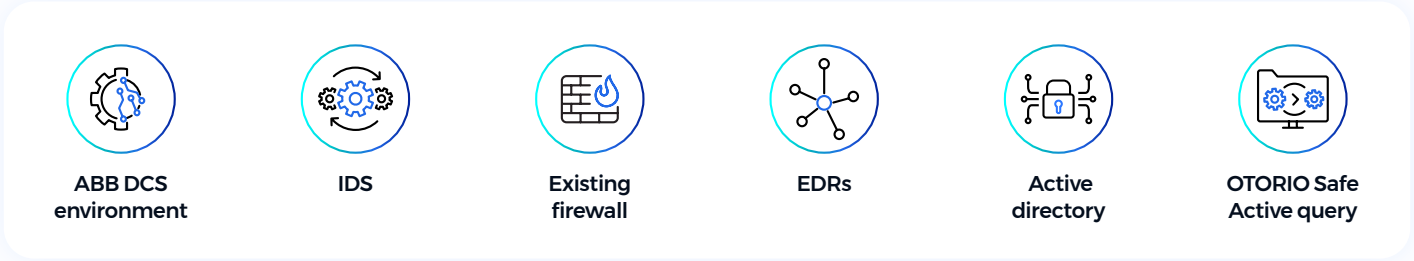
- Unclear and partial asset visibility, with limited details and poor context
- Limited resources to address each vulnerability and alert
- An inability to prioritize risk mitigation actions effectively and efficiently
- OT Security skill gap
- Lacking a good understanding of the company's network security posture and the potential business consequences of security gaps

OTORIO's Solution

OTORIO's RAM² (risk assessment, monitoring and management) solution built a rich OT asset inventory and overview by integrating with the company's industrial assets and existing security solutions. RAM² successfully integrated with the company's ABB 800xA Distributed Control System (DCS) delivering valuable insights beyond the data gathered from the existing IDS:

- **Aspect directory** integration delivers details about machine controllers, identifying the OT logic of each one
- **Logs of ABB's 800xA Redundant Network Routing Protocol (RNRP)**
  - RAM² monitors RNRP logs to deliver alerts about errors and abnormal events, and indications of attacks on the DCS network
- **OPC protocol** integration delivered live system events
  - RAM² provides detailed operational context for the DCS assets , such as DCS object, user, node name and values before and after operators change a specific process parameter.

To create comprehensive network visibility in the OT environment, RAM² expanded integrations, identified all types of physical assets and the communication among them. RAM² gathered high-volume data from the manufacturer's:



RAM² integrated and proactively monitored DCS environment communication, firewall and host security events with other siloed security and operational systems data. The risk management platform then excludesd irrelevant events (e.g., false positives, ghost assets) and analyzesd the data, taking into consideration the operational context, an asset's physical location on the production floor, and business impact criticality. Using OTORIO's Secure & Compliant machinery (SCM) to diagnose assets compliance data, RAM² audited the security configurations to verify their compliance with IEC 62443-3 industrial security standards. It enabled the the pulp and paper manufacturer to identify abnormal behavior in the operational environment, and generated OT security insights prioritized by their severity level, with clear, practical steps on how to mitigate the critical risks.

OTORIO's safe integrations with security controls and industrial systems, as well as the integration with the IDS in the environment, extended the customer's visibility into the asset inventory, enabled contextualized security posture assessment, and improved the customer's ability to detect and respond to suspicious events.

OTORIO Safe Active Query

OTORIO's Safe Active Query discovers and identifies assets and security misconfigurations, occasionally-overlooked misconfigurations can increase risk to the asset and the operations process to which it belongs.

RAM²'s ability to communicate with industrial assets provided the company with a clear, contextual view of operational security risks based on their potential business impact, including:

- High-fidelity asset detail with a richer understanding of its role, potential risk impact, and vulnerabilities
- Broader network coverage of security and industrial systems that effectively demonstrated risk
- Improved MTTD (Mean Time To Detect) and MTTR (Mean Time To Respond)

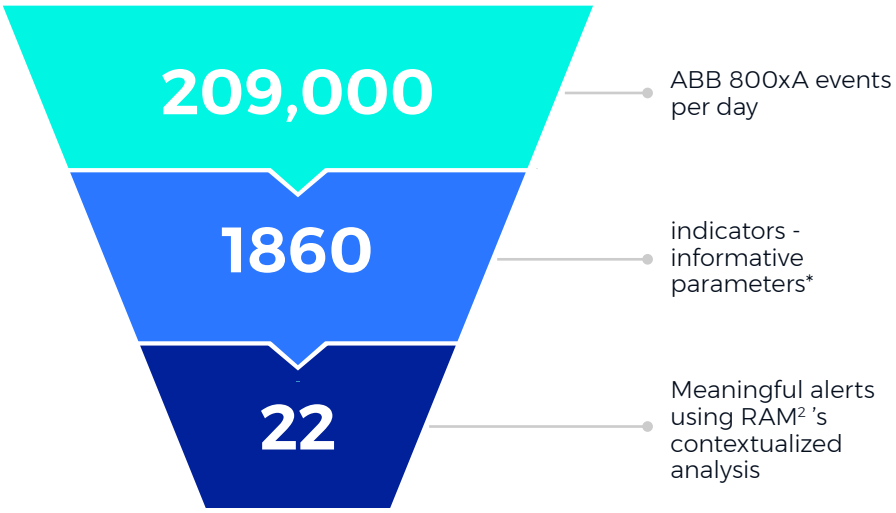
Results

OTORIO's RAM² solution integrated smoothly with ABB 800xA DCS and existing security controls in the pulp and paper manufacturer's OT environment providing it with a comprehensive asset inventory.

RAM² enriched asset attribution with the operational context of OT process and paths, assets impact level, known vulnerabilities, and a comprehensive 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's security team to focus its efforts on what matters most.

RAM²'s integration with ABB 800xA DCS reduced alert notification dramatically from ~209K unfiltered OPC events to 22 alerts total per day. The noise reduction includes 1,860~ "indicators"* per day, because RAM² demonstrates "indicators" as insights only when it identifies a contextualized risk pattern within the operational environment.

ABB events per day

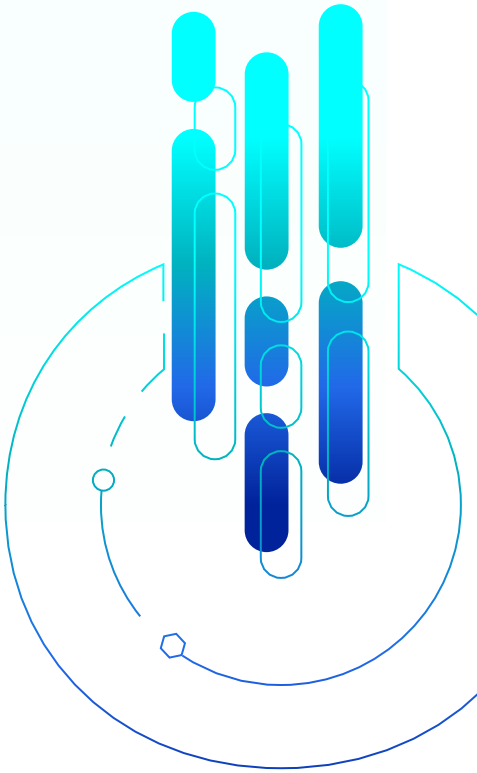


* Indicators are managed in RAM² background and used for future risk scenarios.

RAM²'s integration with IDS reduced above 90% noisy alerts and assets (e.g., ghost assets) based on rules and patterns configurations, connecting all siloed events into an holistic unified view to simplify the process of managing the OT cybersecurity detection and response processes.

"What is OT security context?"

OT security context refers to the totality of circumstances that affect an asset or a group of assets (e.g., vulnerabilities, communication paths, asset relationships, exposure, and discovery). Information is gathered and assessed together with any potential business and operational impact on processes (i.e., production, safety, financial, environmental, and regulatory matters). To provide necessary context for risk-based OT security situational awareness, these elements are analyzed using a rich set of security and industrial data sources that are backed by deep domain research.

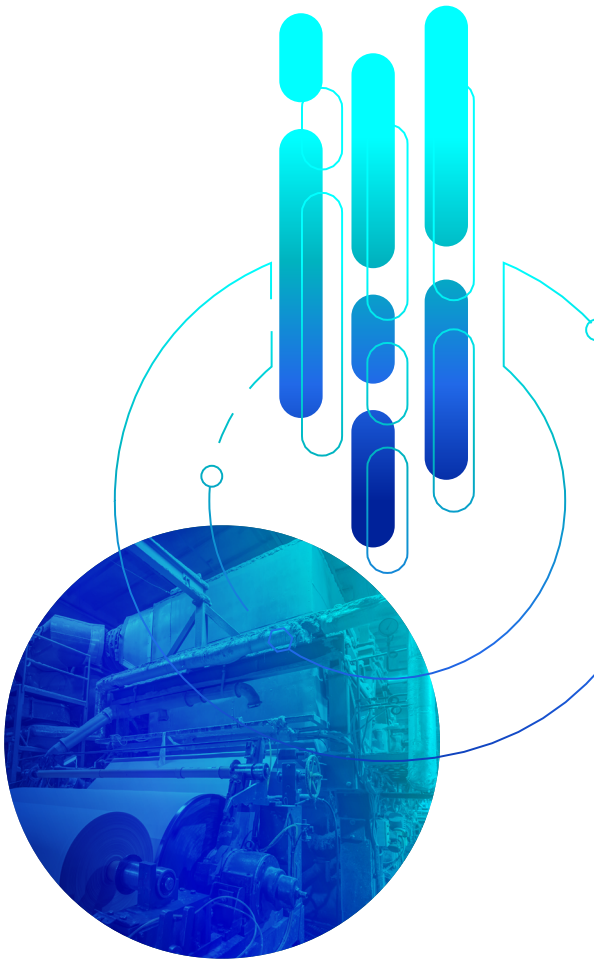


OTORIO

Pulp and Paper

Benefits for the Pulp and Paper company

- Comprehensive OT assets visibility with a unified view of risk for OT, IT, and IIoT-aligned 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
- OTORIO's RAM² insights improved the company's MTTD and MTTR, reduced noice, and highlight which risks and vulnerabilities to prioritize
- It receives safe operational security posture assessments that don't disrupt its ongoing operations.
- The company improved ROI by leveraging and integrating its existing security controls and tools with OTORIO's RAM² platform
- Teams have risk mitigation playbooks with clear instructions to harden site-specific OT network risks and vulnerabilities



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 071222