OTORIO

Manufacturing

OTORIO's RAM²: Profound Asset Visibility Across Global Manufacturing Sites

Case Study

Unified worldwide security operations

The company is a global manufacturer and distributor of medical devices, with manufacturing sites situated across Europe, Asia, and the Americas. The company's recent expansion through multiple factory acquisitions worldwide resulted in limited asset visibility across various locations. To address this issue, the company's security team sought a single solution that could provide global asset visibility and vulnerability assessment, enabling them to manage cyber security risk more effectively. The team required a unified solution capable of identifying assets, detecting vulnerabilities, assigning international team members to specific cases, and tracking the progress of risk mitigation efforts to enhance the organization's operational security posture.

OTORIO was selected by the manufacturing company to identify and inventory all of its OT-IT-IIoT assets according to their operational hierarchy and manufacturing site location. This solution enabled the company to detect and assess risks, as well as simplify its OT cyber security management using impact-driven prioritization and prescriptive mitigation playbooks. By monitoring the mitigation activities globally, across different sites, the security team was empowered to manage risks more effectively on a single platform, covering all operational security activities.

> "RAM² performed significantly better in our key criteria; GUI ease of use, logical overview for operation staff & management, ease of customization, risk-based approach, supplier's OT security expertise, supporting vulnerabilities mitigation and reporting."
>
> Director OTS,
> Manufacturing company

Customer Challenges

The company's security team manages security for various manufacturing sites scattered worldwide and has experienced issues with incomplete asset visibility, asset duplication, and lack of information about the global manufacturing sites. Despite investing in cyber security, the team still faced several challenges:

- Unclear and partial asset visibility, with limited details and poor context.
- The absence of adequate information about the company's operational environment makes it difficult to manage risks effectively.
- Globally and at each manufacturing site, there is a deficiency in security posture information.
- Unknown relationship of assets to the operational hierarchy makes it difficult to identify the risk score per business process and country.
- Lack of vulnerability assessment and determining which alerts require immediate attention.

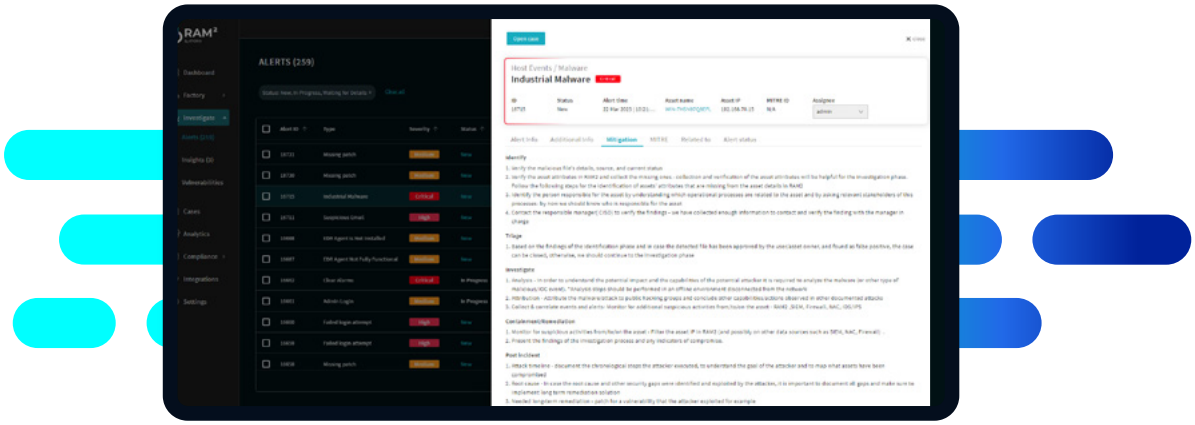
OTORIO's Solution

OTORIO's RAM² OT cyber risk management solution helped the manufacturing company with building a rich, in-depth OT asset inventory and visibility with OTORIO's proprietary Secured and Compliant Machinery endpoint security analysis tool, Safe Active Querying, and integrations with the company's Firewall, EDR and operational network in every manufacturing location, mapping the asset name, IP, MAC and firewall versions based on the operational hierarchy and site location. RAM²'s consolidated asset visibility provided operational context with the ability to identify and classify assets by their type, role, physical location, owner, risk level, and impact on operations in every manufacturing site worldwide.

RAM² as a single source of truth for the operational environment inventory and security posture, provided the security team new actionable insights into their existing systems. They uncovered critical vulnerabilities that were previously unknown and were able to address numerous alerts through RAM²'s case management system.

Leveraging the integration with existing data sources provided valuable, in-depth information about the manufacturing OT environment. RAM² also identified security gaps such as a significant number of assets with default SMB1 credentials, which could potentially lead to unauthorized access of remote computers.

RAM² empowered the team to manage and track open cases and efficiently mitigate the risk in collaboration with the local teams.



OTORIO's RAM² provided the manufacturing company with a holistic solution, including contextual OT security risk management. This gave the client a unified organizational view of risk, including:

- Broader coverage of security and industrial systems for each manufacturing site by analyzing users' environment to demonstrate risk to the organization.
- High-fidelity asset detail with a deeper and richer understanding of its role, impact, vulnerabilities, organizational structure and physical location.
- Central visibility into the inventory and security posture of geographically spread manufacturing sites, including dormant devices.
- Contextualized impact-driven prioritization of mitigation efforts.
- Improved MTTD (Mean Time To Detect) and MTTR (Mean Time To Respond) while reducing noise and highlighting what needs focus.
- An assessment of existing security controls and best practices to harden security configurations and network interfaces.
- Actionable mitigation steps for each risk, presented in a simple, practical way that is tailored to the operational environment.
- Security team has the capability to handle cases (tickets) and keep track of the mitigation process.

OTORIO

Manufacturing

Results

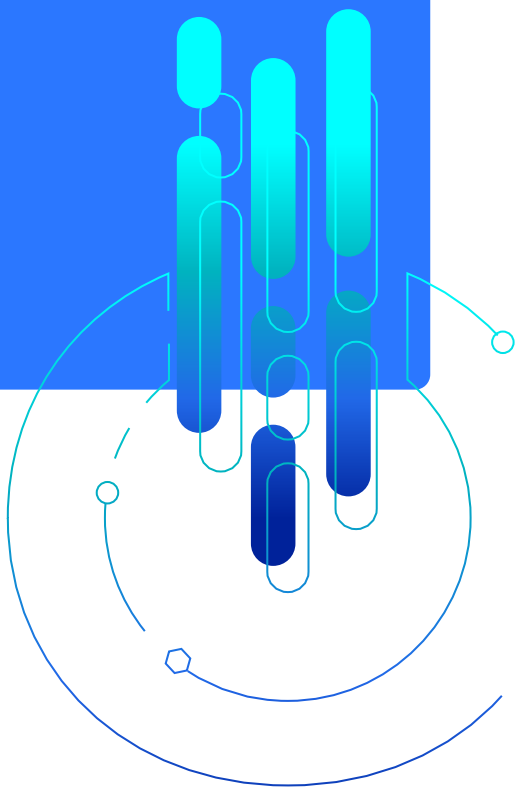
RAM² provides security teams with a comprehensive solution that enables them to discover, identify and classify assets across sites, detect and prioritize vulnerabilities and threats by business context, and collaboratively manage the process of risk mitigation. The solution allows teams to assign cases to specific team members, monitor the progress until completion, and perform all of these tasks in a unified platform. By consolidating the entire risk management process, RAM² improves the robustness and resilience of the operational environment.

Manufacturing Company Benefits

- RAM² provides the global cybersecurity team with a single platform 'single source of truth' to effectively manage operational environment security from any operational site across the world.
- It now has a unified risk view of worldwide manufacturing sites' operational environment.
- The security teams have OT operational context and impact analysis of an asset or process-level for OT risk-based management.
- OTORIO's RAM² provides them with actionable insights that improve the company's Mean-Time-To-Detect and Mean-Time-To-Respond, while reducing noise and highlighting what risks and vulnerabilities should be prioritized.
- The OT security platform enables the manufacturing company to conduct safe operational security posture assessments without disturbing ongoing operations.
- Collaborative management of the risk mitigation process, security teams manage the entire security process within RAM² case management, assigning owners and monitoring the mitigation progress.
- Teams utilize prescriptive mitigation playbooks with clear instructions, to harden site-specific OT network risks and vulnerabilities.
- The manufacturing company is becoming "ransomware ready" by automating gaps and exposure analysis to reduce OT security risks.

Summary

The manufacturing company tested several security solutions but ultimately decided on OTORIO for its scalable and adaptable industrial-native security solution, extensive expertise and ability to provide a unified view of operational systems worldwide.



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 040523