OTORIO Enables Safe Digital Growth for a Global Automotive Manufacturer

The customer is a Fortune 1000 manufacturer (OEM) of commercial vehicles with a well-known brand name. With a global presence, the customer has manufacturing facilities on four continents and a large supply chain of Tier 1 and Tier 2 suppliers.

Automated industrial contextual asset visibility

Introduced Continuous compliance monitoring

Reduced alert fatigue via smart business-impact prioritization

THE CHALLENGE

The automotive industry is a prominent target for cyberattackers. The average vehicle contains up to 150 electronic control units and about 100 million lines of software code. That number is projected to reach 300 million lines by 2030.

The increasing digitalization of vehicles introduces many cybersecurity risks. Cars and trucks have become digital platforms in their own rights - with internet access, auto-updating operating systems and physical assets that are vulnerable to attack. New regulations are being devised to ensure consumer safety - notably ISO/SAE 21434, which enters into force in 2024.

The automotive OEM was dealing with a number of issues, including: insufficient visibility into asset inventory, vulnerabilities and risks; gaps in understanding of the operational impact of risks; a shortage of mitigation instructions; and no visibility over converged OT-IT security posture.

Furthermore, the OEM wanted to move beyond the reactive, post-breach detection approach that was offered by their existing cybersecurity tools, since a response after an attack is more costly and less effective than attack prevention. In addition, the OEMs operational teams found it difficult to make sense of mitigation responses proposed by their existing system. As a result, the organization was at risk of being exposed to high-impact cyberattacks.

What They Are Saying

"OTORIO enabled us to see our thousands of assets with a business impact view for the first time. As an OEM who has to follow compliance on multiple continents, OTORIO's compliance tracking is saving us time and money as we are in a constant cycle of compliance preparedness. Within just a few weeks, we made the transformation from threat detection to risk avoidance."
~~ CISO, Automotive OEM

INITIAL FINDINGS

Working closely with the OEM's security teams, OTORIO's experts were able to map several gaps in the organizational management of OT risks, namely:

- Separate systems were handling different security aspects within both the OT and IT environments.
- There was only a partial understanding of the prioritization of risks or security posture.
- Security risks were not assessed in the context of their impact on production processes.
- The risk analysis was focused on incident management and input from the CISO, while decisions regarding security actions were made by operational personnel on the production floor.

THE SOLUTION

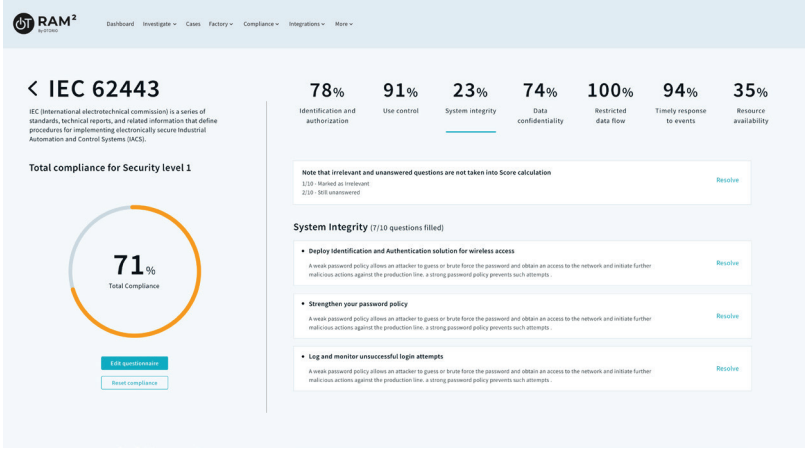
OTORIO RAM² was implemented on the automotive OEM's converged OT-IT network to provide contextual asset inventory management, operational impact, risk prioritization and mitigation, and enhanced compliance governance.

RAM² resolved the asset inventory issue by orchestrating data from multiple sources across the automotive OEM's OT network. This allowed the customer to automatically obtain real-time visibility on all assets within their network (OT, IT and IIot). RAM² automatically organized the OEM's asset inventory in a hierarchical structure based on physical location and operational units (plants, shops, cells). Furthermore, RAM² correlated the assets to vulnerabilities and operational processes. Finally, RAM² calculated risks based on each vulnerability's severity and the associated asset's operational impact - and provided simplified, step-by-step mitigation playbooks.

Utilizing RAM², the automotive OEM was able to significantly reduce the number of alerts. Disparate alerts from a variety of cybersecurity tools were now aggregated into clear, contextualized insights - allowing security teams to identify and mitigate security risks with the highest impact on production.

RAM²'s intuitive dashboards allowed the OEM to significantly improve asset inventory management, and become aware of minor production floor changes.

Moreover, RAM²'s automated compliance governance capability enabled the OEM to accurately measure their compliance with relevant industry cybersecurity standards. Now, the production floor team is made aware of their state of compliance. If compliance scores fall below the required threshold, RAM² provides simple playbooks, allowing the automotive OEM's operational teams to quickly resolve the issues. This also enabled the teams to focus on complying with future automotive cybersecurity standards, as well.



OTORIO was tasked to:

- Identify security risks that could impact production
- Evaluate the company's security posture and vulnerabilities, suggesting mitigation and improvement measures
- Detect and correlate data from OT/IT/IOT assets from multiple sources within the customer's industrial network
- Monitor and track changes in assets and configurations on the production floor in real-time
- Reduce the complexity and improving the efficiency of SecOp activities
- Standardize the security efforts across operational processes
- Identify compliance gaps and suggest resolutions steps

THE BENEFITS

By implementing OTORIO RAM², the automotive OEM reaped immediate benefits, including:

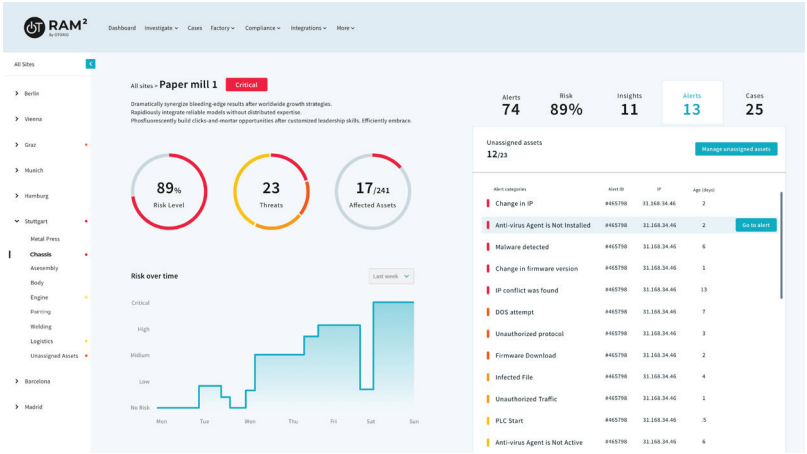
- **Risk reduction** - By attaining asset visibility and mapping assets to vulnerabilities and operational processes, the OEM was able to quickly understand its organizational risk posture and proactively remove risks before they could become breaches.

- **Eliminate alert fatigue** – By orchestrating data from multiple sources and correlating them into meaningful insights that are contextualized with operational process, RAM² helps the OEM reduce the number of alerts and focus only on the most critical risks.

- **Visibility** - OTORIO's unmatched asset inventory capability automatically tailors the OEM's industrial environment - creating a hierarchical view of assets in different plants, shops and cells, with a risk calculation and dashboards for every business level. As a result, the OEM was able to better understand their security posture and map areas that required more attention.

- **Speed** - By eliminating the need for manual mapping of new vulnerabilities to the thousands of assets in the plant and automating the triage and correlation of tens of thousands of alerts, RAM² made a massive task feasible. In addition, by providing easy-to-use playbooks, RAM² made the OEM's risk mitigation processes faster and more efficient.

- **Prioritization** - RAM² enabled smarter analysis of CVE information based on OTORIO's OT industrial vulnerabilities database, only triggering alerts on items that are relevant to the specific assets, models, and versions. RAM² also calculated risk based on a combination of the cybersecurity threat severity and probability with the potential impact on operations – enabling the OEM to prioritize risks according to their operational impact.



About OTORIO

OTORIO delivers next-generation OT security and digital risk management solutions that ensure reliable, safe and efficient industrial digitalization. The company combines the professional experience of top nation-state industrial cybersecurity experts with cutting edge digital risk management technology to provide the highest level of protection to the manufacturing industry.