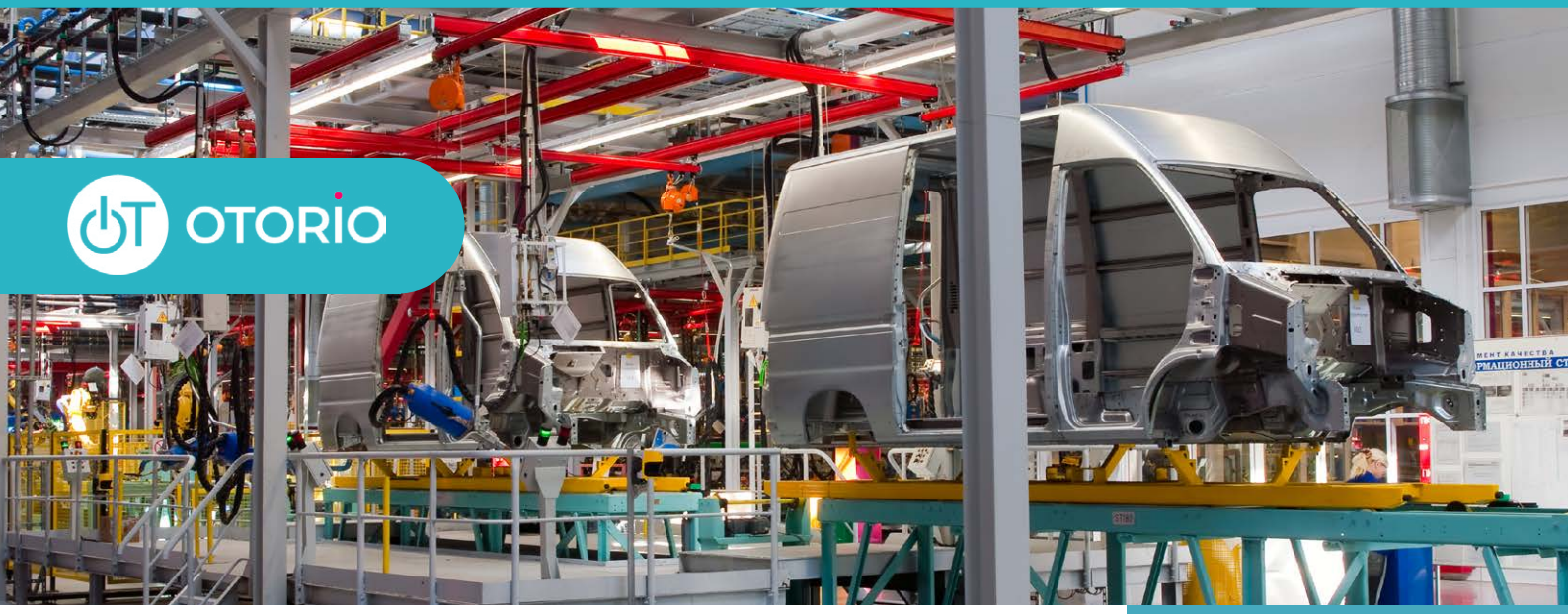


OTORIO Enables Safe Digital Growth For an Automotive Client

A global automotive manufacturer approached OTORIO to help them manage continuous security risk assessment to enable their safe digital growth.

OTORIO's Objectives

- Identifying security risks that could impact production
- Detect and correlate data OT/IT/IOT assets, such as data from multiple sources within the customer's industrial network
- Monitor and track changes in assets and configurations on the production floor in real-time
- Reducing the complexity and improving the efficiency of SecOp activities
- Standardizing the security efforts across operational processes
- Evaluating the company's security posture and its vulnerabilities and suggest mitigation and improvement measures

Securing a Converged OT/IT/IOT Network

OTORIO's team worked closely with the customer and identified conflicts within internal systems as well as inconsistencies in the data provided for the same assets. This generated an incorrect and incomplete picture of the converged OT/IT/IOT asset inventory, which could lead to making poor operational decisions.

In addition, the team discovered that critical actions to reduce the risk to the production floor were neglected, due to the inability to track changes in assets and configurations. Other tasks were neglected as well, such as monitoring thousands of assets to identify those using the default (not secured) credentials.

Lastly, the team found that 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 have to be made by operational personnel on the production floor.

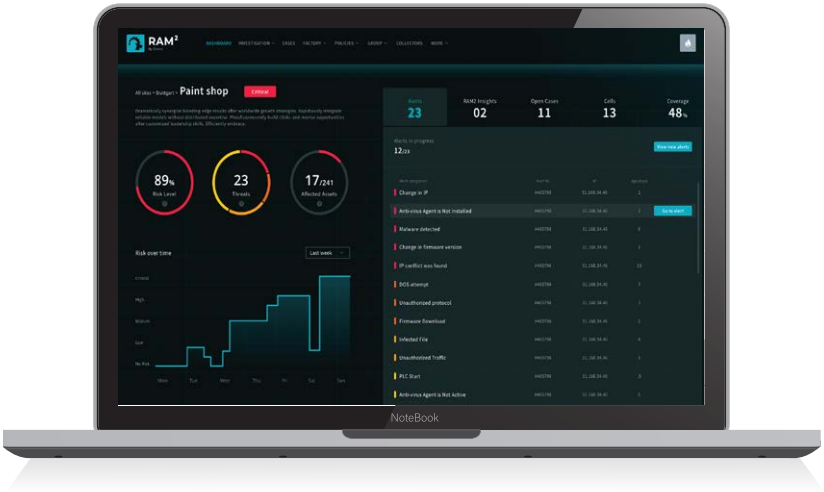
Background

The customer, a manufacturer of commercial vehicles, was dealing with a number of security issues, such as a lack of visibility into asset inventory.

Moving Forward

OTORIO's close relationship with the client enabled us to partner with them and address their concerns effectively. Together, the teams improved the client's risk prioritization strategies, providing a positive impact on the production processes. This included:

- **Speed:** Eliminated the need for manual mapping of new vulnerabilities to the thousands of assets in the plant by automatic analysis by RAM². This is based on OTORIO's proprietary OT threat intelligence module and automatic analysis of asset information. It would have taken a tremendous amount of time to deal with a huge number of assets, or the task would have been neglected altogether.
- **Accuracy:** Promoted smart analysis of CVE information, which only triggers alerts on items that are relevant to the specific assets, models, and versions. This is based on OTORIO's OT vulnerabilities database. The solution analyzes the asset information and matches it accurately to the CVEs. This reduces noise and only provides the most relevant matches.
- **Prioritization**: OTORIO developed a risk calculation model using the combination of the potential impact on operations with the cybersecurity threat severity and probability. This included an attack graph analysis and provides information about the expected risk reduction after it is implemented within the operational context and considers the potential impact on the system.



- **Feasibility:** Considering the operational constraints to provide segmentation alternatives to patching. OTORIO staff verifies if the suggestions can be implemented with respect to the current configuration and network characteristics. If the suggested mitigation steps are not feasible, we can look for an alternative solution with the help of OTORIO's security research team.

Outcomes

- Deploy RAM² within a converged OT/IT/IOT network for asset, change, and vulnerability management
- Integrate OTORIO's Threat Intelligence alerts for cybersecurity vulnerabilities and exploits (CVEs) and the appropriate mitigation steps
- Apply ongoing monitoring services
- Conduct segmentation planning based on attack graph simulations
- Consider alternatives to patching that consider specific industrial contexts
- Continue our work to improve asset management and configuration for better visibility

OTORIO made sure our client understood the suggestions for practical mitigation actions and the risks they are designed to reduce. This was done in order of priority, from the level of factory to cell and asset level.

A plan for gradual implementation of recommended mitigation steps was developed starting at the cell level, by order of risk priority. These steps are constantly and automatically evaluated by RAM^2 and priorities based on changes in the network as reflected in the RAM^2 reports.

The client was able to continuously monitor changes in assets and configurations on the production floor. With the automated monitoring of assets, the company saves time and can now handle simple, yet critical, tasks.

An orchestration platform, RAM^2 takes disparate data sources from across the OT/IT/IOT network, and places them into a unified view, providing visibility of gaps and conflicts between different systems. Operational personnel can manage the system, take immediate action when necessary, and track the status without the help of security experts. This allows the client to focus on the most important tasks that have the greatest impact on their production lines.

About OTORIO

OTORIO designs and markets the next generation of OT security and digital risk management solutions. The company combines the experience of top nation-state cybersecurity experts with cutting edge digital risk management technologies to provide the highest level of protection for the manufacturing industry.