OTORIO Enables Safe Digital Growth For an Automotive Client

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

OTORIO was tasked with

- Identifying security risks that could impact production
- Finding a way to detect and correlate OT assets, such as data from many sources within the customer's industrial network
- Discovering a way to monitor and track changes in assets and
- configurations on the production floor
- Reducing the complexity and improving the efficiency of secOp activities
- Standardizing the security efforts across operational processes
- Understanding the company's security posture and its vulnerabilities

OTORIO was tasked with

We worked closely with the customer and identified conflicts within their internal systems and inconsistencies in the data they provided for the same assets. This generated an incorrect and incomplete picture of their inventory, which could lead to making poor operational decisions.

We 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. In addition, time consuming, tedious tasks, such as monitoring thousands of assets to identify those which are using the default credentials, were neglected as well.

We saw that separate systems were handling different security aspects in the OT network. 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

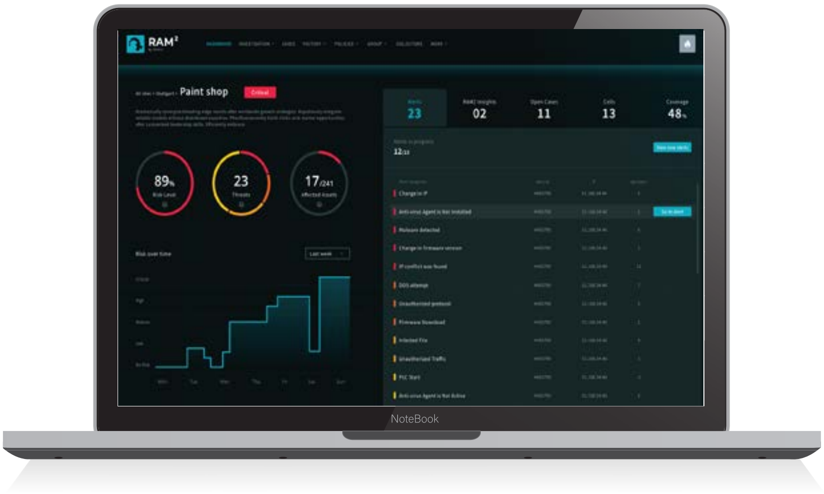
The customer, a manufacturer of commercial vehicles, was dealing with a number of security issues, such as a lack of visibility into asset inventory

Moving forward

Our close relationship with the client enabled us to partner with them and address their concerns effectively.

We improved their risk prioritization strategies that had a positive impact on their production processes as follows:

- **Speed:** We 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 our proprietary OT threat intelligence module and automatic analysis of asset information. Because they are dealing with tens of thousands of assets, this would have taken a tremendous amount of time or would have been neglected.
- **Accuracy:** We 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 and the solution's ability to analyze the asset information and match them accurately to the CVEs, while reducing noise and only providing the most relevant matches.
- **Prioritization** - We were able to calculate risk as the combination of potential impact on operations with the cyber security threat severity and probability. This included attack graph analysis that provides information about the expected risk reduction once implemented within the operational context, taking into account the potential impact.



- **Feasibility** - We consider the operational constraints and provide segmentation alternatives to patching. We verify 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.

Recommendations

Some of our suggestions included:

Deploy RAM² within their OT network for asset, change, and vulnerability management

Receive OTORIO's Threat intelligence alerts for cyber security vulnerabilities (CVEs) and the appropriate mitigation steps.

Implement our segmentation recommendations

Re-evaluate using our ongoing monitoring services

Conduct segmen tation planning, based on attack graph simulations and when necessary, offering alternatives to patching that take into account their specific industrial context

Extend the scope of RAM² integrations to include additional data sources and thereby leverage additional value from the platform

Continue working together to improve their asset management and configuration for better visibility and order

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

We created a plan for gradual implementation of recommended mitigation steps at the cell level, by order of risk priority. We work according to a mitigation plan to implement mitigation steps and reduce the risk level. We can reevaluate recommendations and priorities based on changes in the network as they are reflected in the RAM² 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.

Their new orchestration takes disparate data sources and places them into a unified view, providing visibility of gaps and conflicts between different systems. Their operational personnel can manage the system, take immediate action when necessary, and track the status without the help of security experts. They can now focus on the most important tasks that have the greatest impact on their production lines.

The client was able to leverage the value of RAM² and improve their operational processes management. Their focus is now on proactive, risk management, rather than just reacting to incidents after they occur.
This is another step to enable their safe digitalization of their production processes. With this platform in place, the company can now manage their security risk assessment in a more efficient way.