OTORIO

Automotive

Premium Automotive OEM Elevated Cybersecurity and Operational Efficiency

Case Study

Clear Visibility and Operational Exposure Management Extends Global Security Governance

Due to accelerated digitization and interconnectivity, it is paramount for automotive OEMs and Tier 1 with complex multi-vendor, multi-generational environments to achieve resilient and compliant business operations.

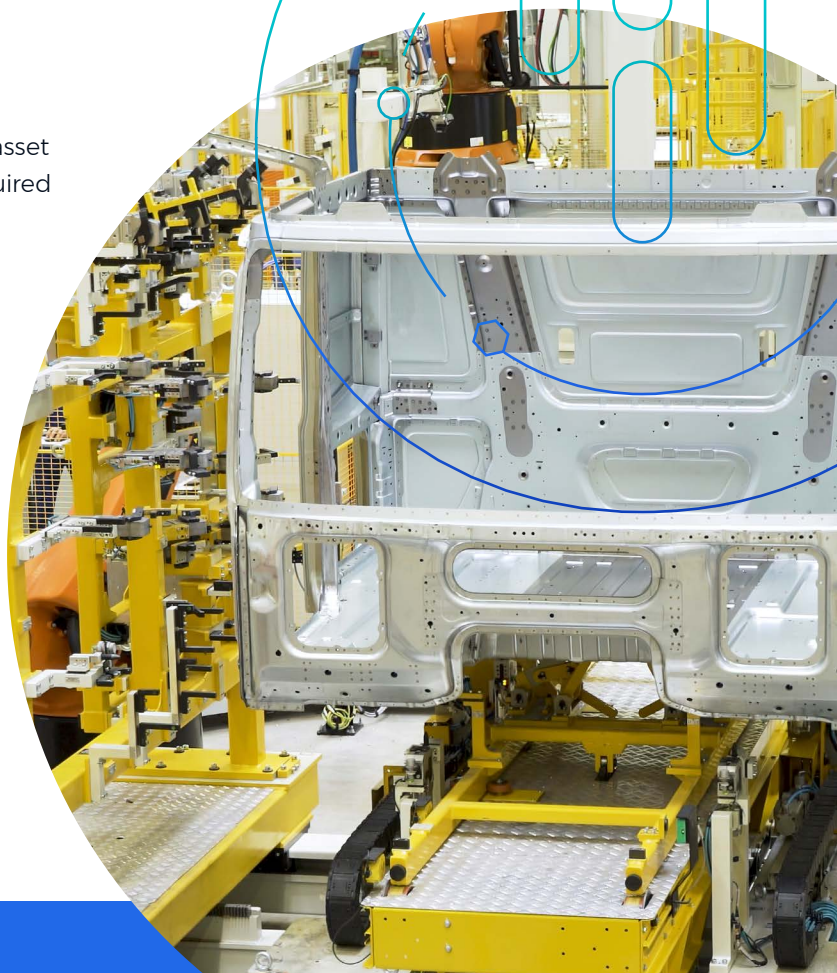
In this case study, the customer implemented an integrated OT security strategy and unified OT governance across geographically dispersed plants for better collaboration and informed business decisions.

The Customer: A Premium automotive OEM

Customer Challenges:
The automotive OEM needed a comprehensive view of asset inventory across its worldwide plants. The customer required that both regional and corporate stakeholders could efficiently track, govern, and report on operational security. This is foundational to making informed decisions based on operational business impact.

The company was looking to address the following main critical challenges:

- Limited visibility into the operational environment.
- Partial and manual mapping of vulnerabilities and security gaps.
- Lack of unified security policies and tools covering IT and OT.



OTORIO

Automotive

OTORIO's Solution

OTORIO's OT Cyber Exposure Management Platform was integrated across the customer's operational environments and connected to the IT infrastructure. The platform used passive network monitoring and non-intrusive active querying, along with integrating with various operational, IT systems and security controls (including EDR, patch management, firewalls, and switch management), to automatically discover, analyze and identify assets in each manufacturing shop. The asset inventory was operationally contextualized by assigning assets to specific manufacturing shops and cells.

Publicly known vulnerabilities in assets and installed applications were pinpointed. Security teams received alerts about misconfigurations and security gaps, such as default vendor credentials, assets that have reached EOL status, and the use of insecure protocols. Segmentation gaps, including overly permissive firewall rules, devices connected to multiple networks (dual-homed devices), and even direct access allowed to external IP addresses were identified. The platform provided actionable, step-by-step mitigation playbooks leveraging existing security controls for each risk.

The platform's patented attack graph analysis engine assessed the exposure of vulnerable assets by simulating potential attack scenarios. Consequently, it offered specific recommendations for effectively hardening the network against ransomware attacks and refined risk prioritization based on exposure and business impact.

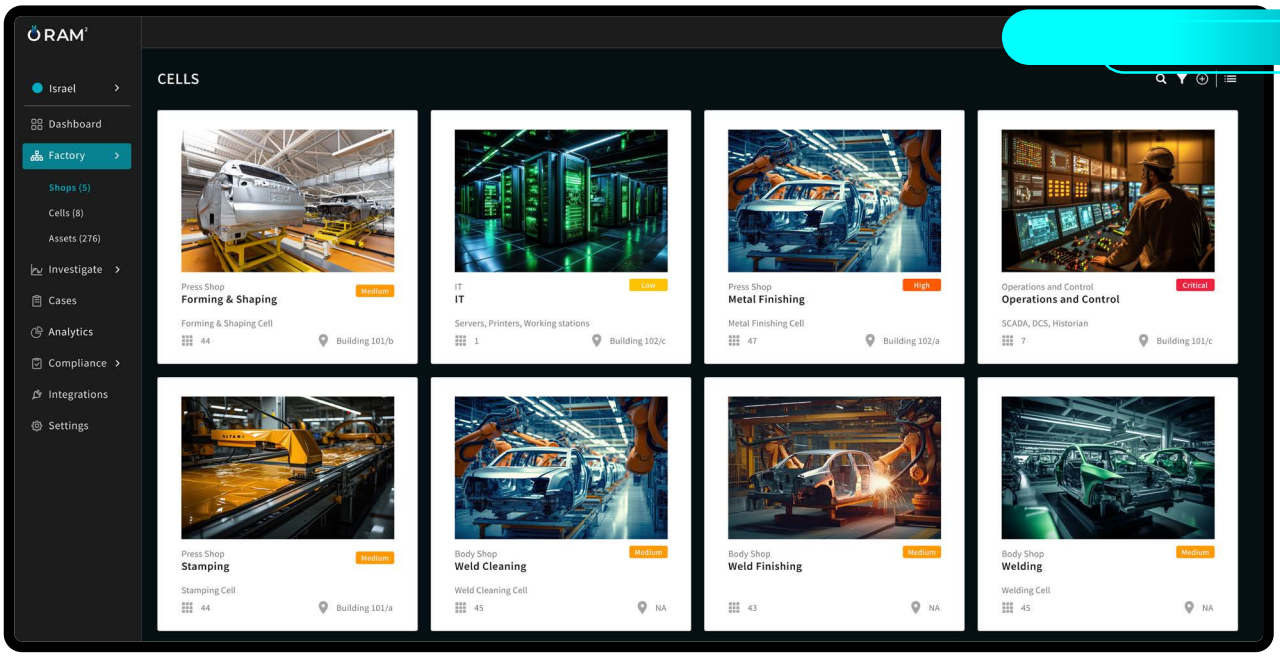


Image: Operational hierarchy with contextualized asset inventory.

The efficient deployment successfully unified OT visibility and security governance into the IT infrastructure, yielding a return on investment within a short time frame.

Integration with ServiceNow provided the IT and OT security teams with streamlined workflows by extending the governance view from IT to OT, streamlining asset management, and accelerating incident resolution by mitigating the most critical risks to achieve operational efficiency.

OTORIO

Automotive

Customer Results

OTORIO's OT Cyber Exposure Management Platform provided the automotive OEM:

- **Asset inventory transparency:** OTORIO's asset discovery capabilities provided unmatched visibility down to level 0 assets to build a comprehensive asset inventory.
- **Identified Vulnerability and Security Misconfigurations:** OTORIO's analysis discovered default credentials in existing industrial controls, identified firewall segmentation gaps and misconfiguration, and provided detailed mitigation guidance for each finding.
- **Continuous OT assessment:** Automating assessment and monitoring processes proactively identify risk exposures, reducing the likelihood of exploitability.
- **Streamlined asset management:** OTORIO's open platform and plugin integrations import data from different sources and export inventory, alerts and insights to other systems, such as ServiceNow and industrial systems.
- **Proactive risk reduction:** OTORIO's exposure assessment with patented Attack Graph provides focus on the highest business impact findings, prioritizing mitigation actions to reduce risk.
- **Improved resource allocation:** OTORIO's governance dashboards and actionable mitigation playbooks enable IT-OT collaboration and extend IT security governance and policies to the OT environment.

Summary

OTORIO's platform provided the automotive OEM with unified OT governance across geographically dispersed manufacturing plants and facilitated OT cyber exposure management. Security teams gained accurate visibility of all operational assets, processes, vulnerabilities, and actionable mitigation playbooks, empowering IT-OT teams to collaborate more effectively in making informed decisions that strengthen security posture and develop a robust risk management strategy.

About OTORIO

OTORIO is a provider of OT security solutions, delivering a cyber exposure management platform that leverages operational context to seamlessly protect ICS-CPS environments and proactively achieve resilient and compliant business operations. **Visit OTORIO.com**

CN 01042024