OTORIO

Automotive

Automotive Manufacturing Resilience: OTORIO's Cybersecurity Solution

Ensuring the integrity of Automotive Tier 1 and 2 supply chains is essential for adhering to demanding manufacturing schedules, enhancing productivity, improving resiliency and maintaining the functional safety of employees and vehicles — effectively safeguarding lives.

Automotive manufacturers are a prime target for cybercriminals because they face unique, industry-specific risks. Automotive supply chains are inherently complex, with automotive OEMs relying on globally-distributed networks of third party manufacturers for a vast array of parts - including software and electronic hardware components. This expansion of the attack surface heightens risks for both manufacturers and consumers.

$22,000 per minute. That's the cost for a car manufacturer when production comes to a standstill*

These kinds of financial consequences emphasize the need for cyber resilience in the automotive sector. The growing interconnectivity and data sharing between systems and networks broadens the potential attack surface for manufacturers and third-party vendors, which could lead to production disruptions - and ultimately profit losses. Strict adherence to security compliance standards like the NIS2 Directive and IEC 62443 not only strengthens the industry against evolving threats but also instills consumer confidence in the safety and privacy of modern vehicles.

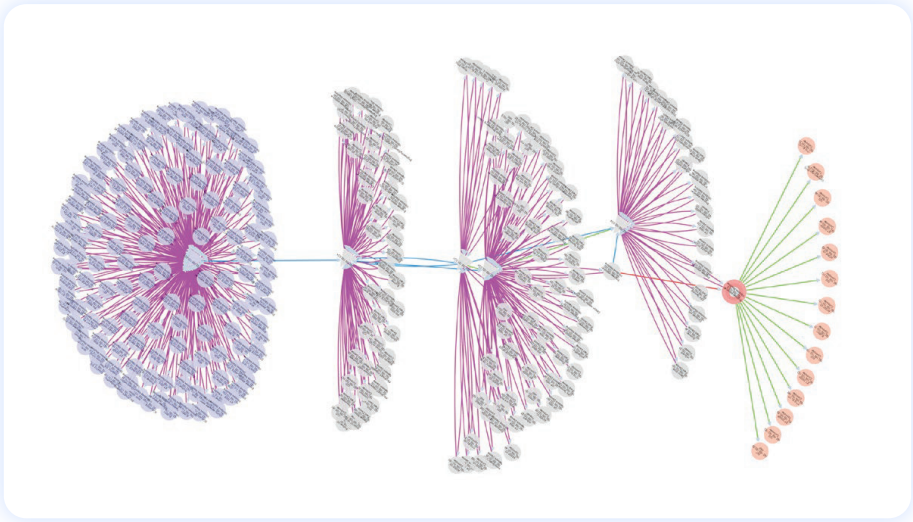
Proactively manage operational risk with OTORIO's OT cybersecurity technology

OTORIO's industrial-native OT cyber risk management platform empowers Automotive operational security practitioners to proactively manage cyber risks. Take control of your security posture and eliminate critical risks, wherever you are in your OT security journey. OTORIOTitan provides you:

- **Unparalleled consolidated visibility** of your Firewall, EDR, IDS, PLC, SCADA, DCS, Historians, Engineering systems, and more across assembly lines, paint shops and all the operational environment.
- All devices, networks, and systems in the operational environment can be **seen and monitored in near real-time**, so practitioners can efficiently address potential risks with a proactive approach.
- **OTORIO's Attack Graph** Analysis **identifies security posture gaps and risks within the production environment**. By mapping out the interconnectedness of devices, networks, and vulnerabilities, this solution generates visual representations of attack paths. Manufacturers can anticipate potential breach points, understand attack vectors, and prioritize mitigation strategies of most critical risks.
- **Impact-driven risk assessment** based on operational context, focuses on risks that matter most to your business.
- **Continuous monitoring** of the environment delivers ongoing assessment of the security posture, with alerts regarding any new vulnerability and security gap, to be addressed before they are exploited, ensuring the robustness and resilience of the environment.
- **Ransomware ready assessments** identifying critical assets and network configuration for hardening against ransomware.
- **Rich, granular reports** that proactively identify the most critical vulnerabilities.
- **A prescriptive expert defined risk mitigation guidance**. Best practice and tailored practical playbooks provide step-by-step instructions to help teams mitigate vulnerabilities, demonstrate compliance and ensure operational resilience.
- **Immediate business value** across your organization, maximizes ROI from your operational security controls and processes.

* Forbes, 2022

OTORIO



Full network topology with asset vulnerabilities

Key Benefits

- Improve **central visibility** and transparency across the organization
- Ensure a **ransomware-ready** environment
- Increase **collaboration** between OT-IT practitioners
- Free up cyber security expert **resources**
- Shorten exposure **time** from months to days
- Achieve **compliance** and standardization across the organization
- Save up to **75%** of overall time and resources spent on assessments, data collection, analysis, and reporting
- Optimize **risk mitigation** resource allocation according to criticality and business impact
- Avoid **regulatory** penalties
- Improve operational **insurability**

Ensure Compliance and Standardizations

Align with the NIS2 Cybersecurity Framework to protect networks and individual devices against external threats. Easily conduct compliance assessments - from the single asset to the entire operational network - so you can adhere to the necessary compliance and standardizations requirements. OTORIO's out-of-the-box automated compliance, enables you to enforce and govern industry required regulations to safeguard the production ecosystem and minimizes legal and financial risks. OTORIO does this with:

- Automated compliance assessments from the single asset to the entire operational network, ensuring manufacturers adhere to the necessary compliance requirements.
- Compliance audit for manufacturing regulations such as NIST2, IEC 62443, NERC CIP Cybersecurity Framework, and other sector-specific standards.
- Clear and detailed reports on any deviation, with compliance scores and the required remediation instructions.

Summary

By mapping attack paths, protecting complex supply chains, and auditing regulatory adherence, you can fortify your systems, strengthen stakeholder trust, and ensure the seamless operation of your automotive production ecosystem. With OTORIO, you can safeguard both productivity and the lives of vehicle occupants.

About OTORIO

OTORIO is a leader in OT security solutions, dedicated to safeguarding enterprise IoT and OT environments for enhanced safety, productivity, compliance and resilience. Its flagship platform, OTORIO Titan, provides an all-encompassing suite of applications that brokers IIoT, OT, and CPS security controls into IT workflows, ensuring proactive protection and efficient risk management.

otorio.com