CASE STUDY

# Enabling Safe Digital Growth For an Automotive Client

## The Challenge

- Identifying cyber exposure risks that could impact production.
- Standardizing the security efforts for full visibility, security and control across all assets and operational processes.
- Detecting threats and correlating security findings across OT/IT/IOT assets.

## The Solution

**Armis Centrix™ for OT/IoT Security (On-prem)** delivered comprehensive visibility, security and control across all connected assets—enabling continuous asset discovery, change detection, and vulnerability management.

Real-time, contextualized and prioritized alerts on emerging cybersecurity threats and CVEs, along with actionable mitigation guidance to proactively reduce risk.

## The Results

- Automated the previous need for manual mapping of new vulnerabilities to the thousands of assets in the plant by automatic analysis.
- Promoted smart identification and analysis of CVE information, which only triggers alerts on items that are relevant to the specific assets, models, and versions.

**Industry:** Automotive

**Location:** N/A

**Size:** N/A

Armis Centrix™ for OT/IoT Security (On-prem)

## Background

A leading global manufacturer of commercial vehicles faced growing security challenges due to limited visibility into its industrial asset inventory. As the company expanded its digital footprint, it needed a way to continuously assess and manage cybersecurity risks across its converged OT/IT/IoT environments. To support this effort, the manufacturer turned to Armis to help enable secure, scalable digital transformation.

## The Challenge

**The organization sought to address several key cybersecurity and operational issues, including:**

- Identifying and mitigating security risks that could disrupt production operations
- Gaining unified visibility across diverse OT, IT, and IoT assets from multiple data sources
- Monitoring real-time changes in asset configurations on the factory floor

- Streamlining and enhancing the efficiency of Security Operations (SecOps)
- Standardizing security practices across all operational processes
- Continuously evaluating the organization's security posture and recommending actionable improvements

## The Solution

The 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 the production environment. 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.

## The Results

Through a close partnership and continuous collaboration, Armis helped the automotive manufacturer transform its approach to cyber risk management by streamlining operations, improving threat detection, and prioritizing mitigation efforts without disrupting production.

**Key outcomes included:**

- **Speed**: Armis Centrix™ for OT/IoT Security (On-prem) eliminated the need for time-consuming manual mapping of vulnerabilities to thousands of plant assets. Asset intelligence and threat analysis enabled rapid identification of relevant risks, accelerating response times and ensuring vulnerabilities and other potential threats weren't overlooked due to scale or complexity.
- **Accuracy**: Leveraging Armis' proprietary asset intelligence engine, the solution contextualized CVE and other threat data with specific asset models and firmware versions. This smart filtering significantly reduced noise and ensured security teams prioritized the most relevant and impactful threats.
- **Prioritization**: A customized risk calculation model was introduced, combining the severity and likelihood of cyber threats with their potential operational impact. Using attack graph analysis, the solution identified the most critical vulnerabilities, attack proliferation pathways and estimated risk reduction after mitigation.
- **Feasibility**: In environments where patching was not viable, Armis provided alternative segmentation-based mitigation strategies that accounted for existing network architecture and operational constraints.

Mitigation actions were clearly communicated to the customer, prioritized from the factory level down to individual devices and assets. A phased implementation plan was established and as a result, the manufacturer can now continuously track changes to assets and configurations across its production floors; automating what were once manual, time-intensive tasks. This has significantly improved operational efficiency while maintaining a strong cybersecurity posture.

## Outcomes

**Improved Operational Uptime**
Avoidance of costly unplanned downtime and disruptions to vehicle manufacturing lines.

**Increased Security Efficiency and Scale**
Eliminated manual asset inventory mapping, allowing the security team to manage thousands of assets across global production sites without scaling headcount.

**Faster Incident Response and Risk Mitigation**
Automated risk correlation and asset analysis enabled the security team to react to emerging threats in minutes,not days, thereby reducing exposure windows.

**Enhanced Risk-Based Decision Making**
Prioritization models tailored to operational impact empowered leaders to focus mitigation efforts where they would deliver the greatest risk reduction and business value.

**Regulatory Readiness and Compliance Support**
Improved visibility and documentation of asset inventory, changes, and security controls helped streamline audit preparation and align with industry regulations.

**Reduced Alert Fatigue and Focused Resources**
By filtering out irrelevant CVEs and surfacing only actionable alerts, Armis enabled security teams to focus on real threats boosting productivity and improving the overall organizational security posture.

**Secure Digital Transformation**
The company laid a strong cybersecurity foundation to support ongoing automation and Industry 4.0 initiatives, with confidence that new technologies could be safely integrated into its operations at scale.