How CATARC Data Center Secures Automotive Data with Cybellum's Product Security Platform

Background

China Automotive Technology & Research Center (CATARC) Data Center (中汽数据有限公司) is a science research institute that was founded in 1985 to meet China's need to manage the automotive industry and now belongs to SASAC (State-owned Assets Supervision and Administration Commission of the State Council). Their work includes collecting automotive data to research forward-thinking technologies in the fields of energy conservation, carbon emissions reduction, green ecology, market research, and beyond.

The Data Center is working on properly developing a secure system for new infrastructure. This includes strengthening the automotive industry cloud, intelligent connected vehicles, smart cabins, and industrial internet (industrial software) within China. It aims to drive industry transformation with data and lead the future of the automotive industry in a way that is secure and intelligent.

CATARC's Data Center's greater mission is to build China's automotive industry data infrastructure along with the national automotive industry data system by creating a:

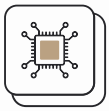
- National Automotive Industry Data Center
- National Automotive Supply Chain Visibility
- National Automotive Industry Digitalization Support Institution

Protecting Automotive Deep Data

The China Automotive Cyber Security Team focuses on driving safety and aligns with China's two major national strategies– cyber security and security control including failsafes.

Bolstering these strategies will allow for more secure technological development throughout the Chinese automotive ecosystem. For example, CATARC may work to develop a secure method for vehicles to communicate with one another over the internet. A vehicle with secure connectivity must be able to recognize other vehicles that are meeting the same standard. This is only possible by analyzing data and understanding the most secure method for communication.

To achieve the desired level of cybersecurity, CATARC Data Center needed a product-security solution that could allow them to:



Automate product security

Automation of product security tasks helps achieve the desired level of security while also generating compliance-ready reports in the process, something crucial for meeting client work requirements.

Manage SBOMs

As in-house or open-source components are added, removed, or patched, product security workflows automatically update the SBOM to reflect the current state of each product.

Vulnerability Detection & Management

With an always up-to-date SBOM, product security teams can run vulnerability scans against each embedded component to ensure no weak points exist.

> ***We are securing vehicle networks by identifying and patching any problems. This way, we can offer services that protect cars from attacks, share data securely, and build safe systems for the whole car network. This helps keep cars and their data safe online.***
>
> Security Manager at CATARC Data Center

Securing vehicle data with Cybellum

CATARC's goal was to shorten the certification process time-to-market while ensuring the highest security standards CATARC has always been committed to.

Upon implementing Cybellum's Product Security Platform, CATARC Data Center began streamlining processes and reducing the burden put on team members. This includes working with their customers to increase visibility into component risk and ensure they are ready for new and existing regulations in China, Europe, and beyond.

Today, CATARC uses Cybellum's platform to identify and manage risk for many types of embedded devices used in the Automotive sector. Once scanned, the Cybellum platform automatically generates a detailed replica of the component including its SBOMs, interfaces, operating systems configuration, encryption mechanism, hardening and mitigation mechanism, API calls and more, all with no access to its source code. With this critical information, customers are able to manage their Software Bill of Materials repository and deliver the most up to date information needed to conduct vulnerability management and risk assessment activities, which are necessary to remain compliant.

> ***Through their groundbreaking research, CATARC is shaping the future of Automotive data and innovation, and it's been an honor working with their team to keep embedded devices and data secure.***
>
> Eddie Lazebnik, VP Channel Sales, Cybellum

> *Our work with Cybellum over the last few years has enabled us to streamline our customer's security tasks so they can comply with regulations– whether it be R155, ISO/SAE21434, or upcoming automotive regulations here in China. In practice this means shortening time to discovery and resolution, increasing the accuracy of our cyber reporting, and improving our customer's compliance reporting.*

Security Manager at CATARC Data Center

According to CATARC Data Center, they've experienced:

- ✓ A 30% increase in efficiencies with automated workflows
- ✓ Unparalleled support across architecture and OS types
- ✓ Impressive Zero-day detections
- ✓ Accurate and contextualized vulnerability insights
- ✓ More focus on high-priority tasks with fewer distractions from false positives

About Cybellum

Cybellum is where teams do product security.

Top Automotive manufacturers such as Jaguar Land Rover, Nissan, Audi, McLaren as well as numerous testing institutes in China, and 5 of the country's top 13 OEMs use Cybellum's Product Security Platform and services to manage the main aspects of their cybersecurity operations across business units and lifecycle stages. From SBOM to Vulnerability Management, Compliance Validation, and Incident Response, teams ensure their connected products are fundamentally secure and compliant – and stay that way.

With multi-language support, including Mandarin, as well as significant local presence, Cybellum is the focal point for Automotive manufacturers and testing facilities all across China.