How ARTC Leverages Cybellum's Product Security Platform to Secure the Future of Automotive R&D in Taiwan

Background

Founded in 1990, The Automotive Research & Testing Center (ARTC) was established with one goal in mind- the improvement of automotive development in Taiwan.

As vehicles have gone from simple electronic systems, such as lights, radio, and windows, to the software-defined vehicles we see rolling off production lines today, ARTC has been evolving alongside the automotive industry. This not only means ensuring the development of reliable components but also aligning testing and certification services with government standards and regulations.

ARTC oversees mechatronics control, lighting, image recognition, and vehicle-to-vehicle communications. These include:

- **Safety enhancement systems,** including image type adaptive front-lighting system (IAFS), blind-spot detection and door opening warning system (BDS), lane departure warning system (LDW), lane keeping system(LKS), driver surveillance system (DSS), and forward collision warning system (FCW)
- **Driving convenience systems,** such as fingerprint recognition keyless system(FRKS), parking assistance system(PAS), automatic parking guidance system (APGS);
- **Energy-saving systems,** consisting of LED headlamps and others
- **Intelligent chassis systems,** which consist of an electric parking brake system (EPB) and electric power steering system(EPS).

Moreover, they are actively addressing global issues surrounding energy saving and environmental changes such as energy-conserving LED headlamps, developing electric vehicles and green systems, and the study of improving efficiency. They also focus on in-vehicle convenience systems and reducing traffic accidents by means of electronics and communication technologies.

Meeting market demand for compliance services

As new cybersecurity standards and regulations, such as WP.29 R155 & R156 and ISO/SAE21434 came into effect, there has been increased demand from ARTC's customers to meet compliance standards. As the organization received the government mandate to help the industry keep its products in line with the latest requirements, it has become critical to have visibility into each component's product security exposure and license standing.

This is when ARTC decided to seek out a product that could help them identify the posture of each software-driven embedded component- even if hidden within the AUTOSAR architecture. **As software complexity continues to increase year over year, ARTC recognized the need to manage and automate various aspects of their product security capabilities to keep up with market realities.** They included:

- **CWE (Common Weakness Enumeration) Detection -** Needed support for identifying unknown weaknesses in the software, and enhancing vulnerability detection capabilities.
- **Version Management -** Product security teams need to track and manage component software versions so they can focus their efforts on identifying and mitigating risks.
- **Unlimited Capacity -** As automotive projects become larger and lines of code increase, ARTC must be able to scan new files regardless of their size.
- **System-Level Security Analysis -** It has become challenging to analyze a full system manually since untangling the complex development process is resource-intensive. Bringing order to this process was critical to finding solutions.

ARTC's main platform use cases

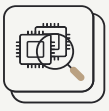
- Support the Taiwanese automotive market in the adoption of new regulation
- Validating WP.29 & ISO/SAE 21434 compliance
- Limitless assessment capacity of products and components
- Broad integration support with existing product lifecycle tools
- Thorough CVE & CWE detection and vulnerability management

Less effort with greater impact with the Product Security Platform

As pressure continued to grow from regulators and customers to meet these new standards, Cybellum worked with ARTC, along with a local partner FIC (First International Computer), to implement an ADAS POC in just two weeks. The POC proved the helpfulness of the Product Security Platform, allowing ARTC to move ahead with Cybellum and FIC to deliver cybersecurity testing services to automotive companies.

> ***Through product security efforts, we are committed to supporting ARTC's R&D of related technology and the improvement of product quality for both them and their customers. This includes helping ARTC to leverage Cybellum's product security technology to identify and address security issues more effectively, reducing the time and effort required for industry compliance.***
>
> *Eddie Lazebnik, VP Asia-Pacific Activities at Cybellum*

Reaching new levels of productivity was possible by recognizing:



Immediate access to product status - real-time access to open source software (OSS), CVE, and CWE data. This real-time visibility allows them to swiftly identify potential vulnerabilities and security issues in software components.

Effortless Customer Reporting - Easily generate comprehensive reports for 50+ standards and regulations as well as internal processes.

Better visibility - Gained visibility into components within the AUTOSAR architecture and third-party binary code security status, without requesting such information from suppliers.

Greater control over supply chain security- Better product security visibility from upstream suppliers.

About us

CYBELLUM IS WHERE TEAMS DO PRODUCT SECURITY.

Top Automotive manufacturers such as Jaguar Land Rover, Nissan, Audi, and Faurecia 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.

Experience what product security can be. Book a demo.