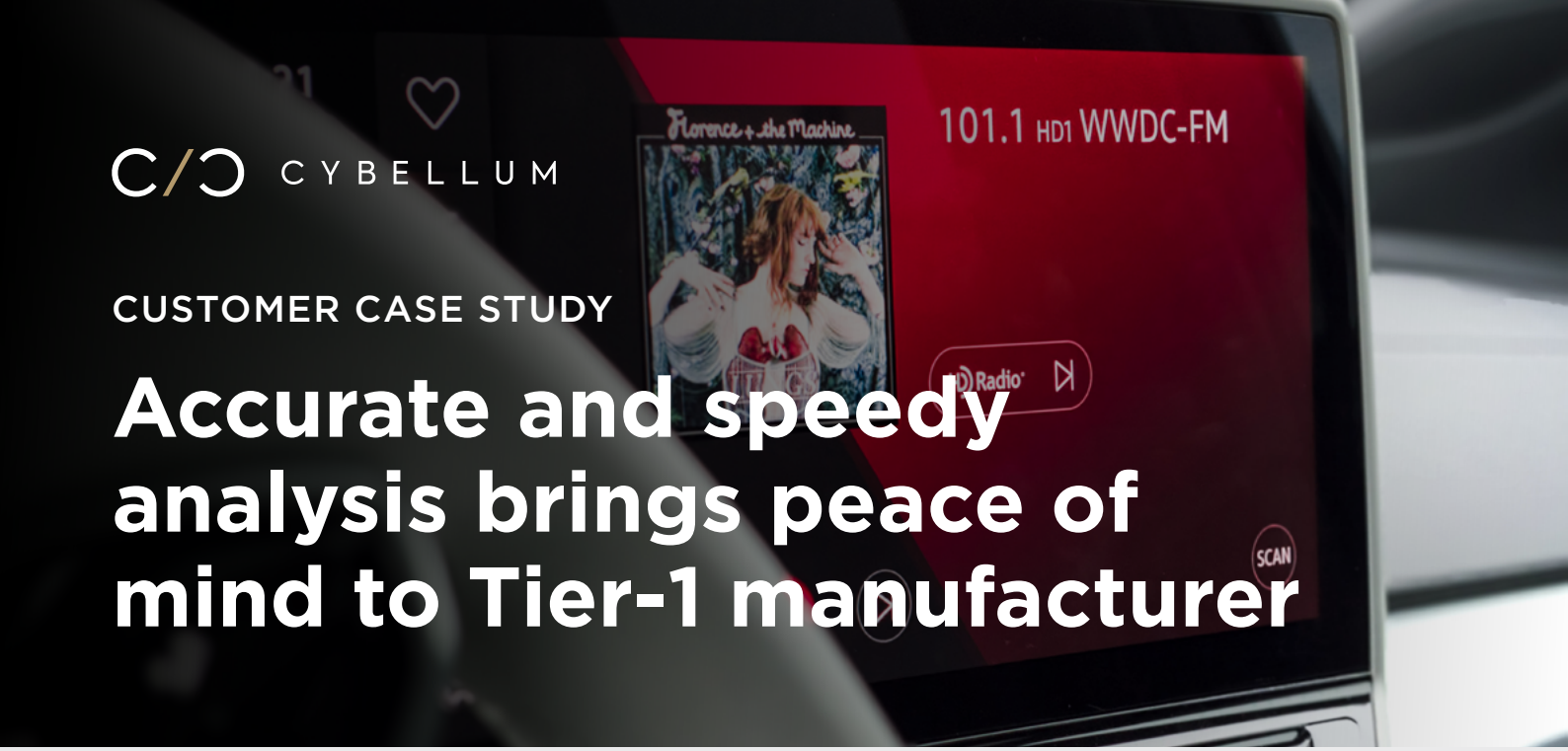

CYBELLUM

CUSTOMER CASE STUDY

Accurate and speedy analysis brings peace of mind to Tier-1 manufacturer

About the Customer: Headquartered in APAC, the Tier-1 supplier caters to global OEMs with an extensive product portfolio ranging from power-train and cockpit systems to air conditioning and safety solutions.

THE CHALLENGE

Scale vulnerability management processes for CVEs and zero-days and prepare for ISO 21434

THE OUTCOME

15x
faster assessments

-60%
false positives

EXPOSED
false negatives

ISO 21434
ready

"Cybellum's highly accurate assessments and automation enable us to meet OEM deadlines and regain control over our own supply chain. **Security Manager, Automotive Tier-1 Manufacturer**

THE NEED

As a global player with a diverse portfolio of automotive products, the manufacturer was struggling to consistently and efficiently manage cyber risks using a mix of inaccurate source-code analysis tools and manual assessments (including black-box pen-testing). On top of that, the aggregation and analysis of all results required considerable manual effort.

THE REQUIREMENTS

- Automate legacy vulnerability management processes covering CVEs and Zero-Day coding weaknesses
- Reduce false positives and false negatives
- Drive a consistent security validation processes for rich-OS systems and RTOS based AUTOSAR components
- Support multiple microcontroller architectures
- Enhance visibility into the security status of engineering programs
- Minimize supply chain cyber risks
- Validate adherence to internal policies

THE SOLUTION

Following a competitive evaluation process and a successful trial project, the Cybellum Cyber Digital Twins™ platform was deployed as the centralized vulnerability management solution:

- Tens of Cyber Digital Twins generated from binary ECU files
- Automatic security validation of 1st party software and Tier-2 deliverables
- Context-based prioritization and remediation guidelines
- Threat intelligence feed enhanced with a private vulnerability database
- Support for ARM, Renesas and TriCore architectures
- Compliance validation of internal policies (coding standards, privacy leaks etc.)
- Dashboards track the security status of different programs
- All activities are documented for future regulatory certification

THE RESULTS

Cybellum enabled the manufacturer's product security team to consistently analyze all automotive products including rich ECUs and mission-critical, resource limited MCU-based components. Results were quick to come:

- **15x faster vulnerability management process compared to legacy methods**
- **False positives reduced by 60% and the team was able to focus on real risks**
- **Exposed "false negatives" - zero-days that were previously undetected**
- **Enhanced organizational adherence to internal security policies**
- **Improved visibility into the security status of all development programs**
- **Enhanced collaboration between product security, engineering and Tier-2 suppliers**
- **ISO 21434 readiness ahead of regulations impacting OEM customers**

KEY BENEFITS

COMPLETE COVERAGE

Manage vulnerabilities and security gaps in vehicle components and companion apps, protecting them from CVEs and zero-days. All via binary analysis. No source code needed.

SHIFT TO AUTOMATIC

Scale up vulnerability management across development programs with minimal manual effort, so you can meet and beat deadlines and prevent security risks.

ACTIONABLE INSIGHTS

Bring context to chaos and eliminate irrelevant vulnerabilities, so you can prioritize your team's efforts and quickly resolve security gaps, aided by our remediation recommendations.

About Cybellum

Cybellum empowers OEMs and their suppliers to develop and maintain secure automotive products at scale. Our Cyber Digital Twins™ platform unifies pre-SOP Product Security Assessments with post-development Product Security Operations, providing you the visibility, context and agility needed to secure vehicles across their lifespan.