CYMOTIVE
TRUSTED SMART MOBILITY

Automated Vulnerability Management

for the Full Vehicle Lifecycle

Solution Brief

The 2024 Cyber Challenge
and Beyond

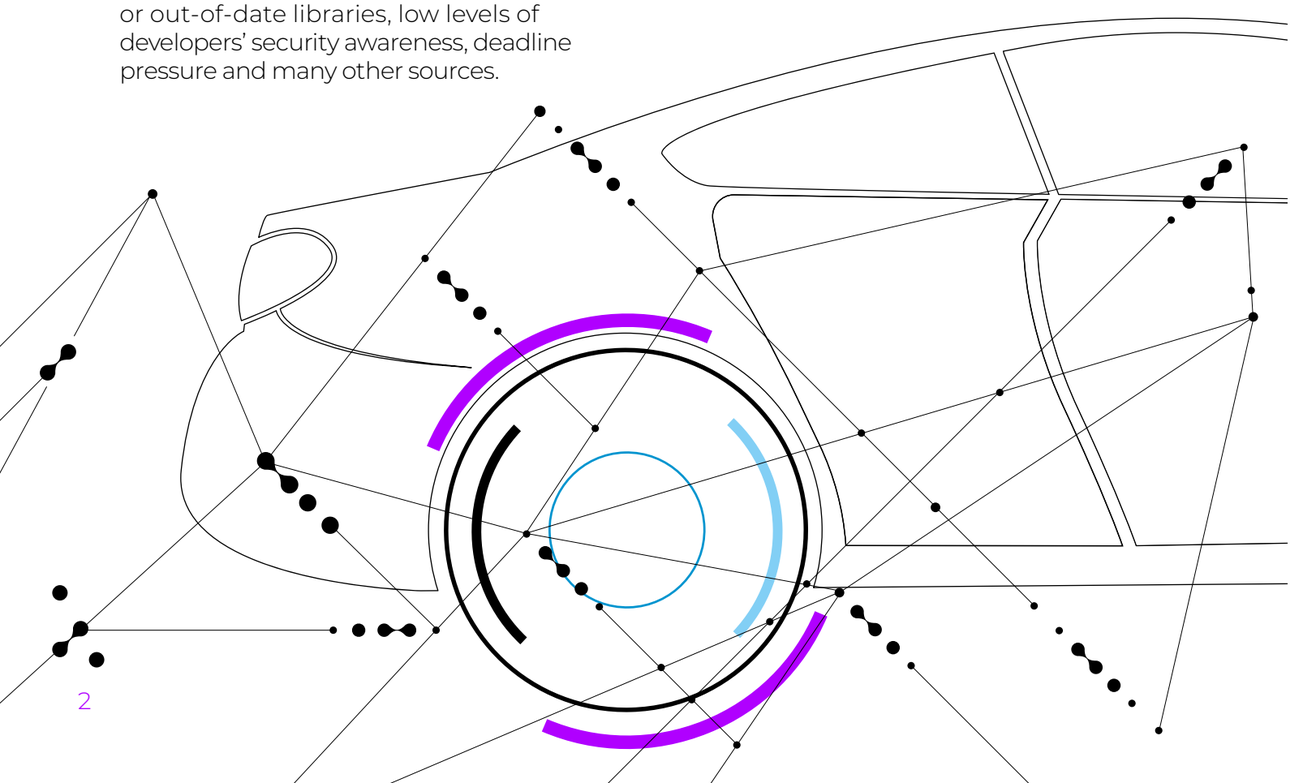
Providing continuous and reliable cybersecurity in vehicles and fleets is extremely complex given the vast digital transformation of the automotive industry.

The penetration of the software-defined vehicle (SDV) - connected, autonomous, shared, or electric (CASE) - is spiraling upwards, creating an ever-expanding potential attack surfaces.

Even prior to the software-defined vehicle, today's standard vehicle contains over 100 million lines of code where vulnerabilities are always present, enabling hackers to find ways into the vehicle's controls.

At any given moment, vehicle software development and post-production stages contain software and hardware vulnerabilities. These weak links typically result from coding errors, unpatched or out-of-date libraries, low levels of developers' security awareness, deadline pressure and many other sources.

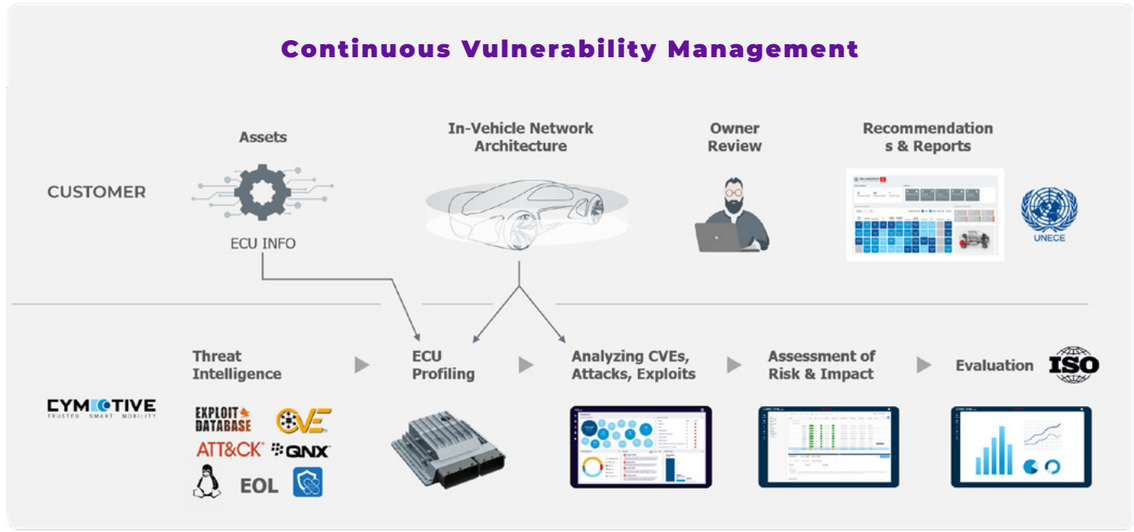
Managing vulnerabilities will soon become a requirement according to the upcoming United Nations Regulation 155 following the ISO/SAE 21434 standard.



Are the regulations sufficient for
assured cybersecurity?

The United Nations Regulation No.155 sets a low bar for the implementation of cybersecurity solutions. In contrast, CYMOTIVE's solution offers business and operational benefits that go beyond regulations.

CYMOTIVE understands that **vulnerability management should be implemented at the beginning of software development** and continue running during upload to the vehicle. As per the regulations, vulnerability management must be run in the postproduction stage.



If vulnerability management is applied late in the development stage, the results can be quite expensive to a car manufacturer (OEM) or supplier, only to increase if found in a later stage. Vulnerabilities can become potentially dangerous if discovered when the vehicle is on the road. Non-compliance of certification can bring heavy fines and damage to an OEM's brand. Once the vehicle is on the road, OEMs are required to monitor and fix the vulnerabilities by means such as over-the-air (OTA) updates or others including recalls, which result in negative publicity.

The UN R155 regulation specifies that the burden of supply-chain cybersecurity management belongs to the OEM. Although the actual method for assuring cybersecurity from its Tier 1 and Tier 2 suppliers isn't mentioned, the regulation insists that the OEM must "collect and verify the information to demonstrate that supplier-related risks are identified and are managed." CYMOTIVE's solution enables the Tier 1 and Tier 2 suppliers to present the documentation proving their cyber compliance to the OEM.

CYMOTIVE TRUSTED SMART MOBILITY

Use cases
for OEMs

Vulnerability management from development until postproduction

Assessment and risk minimization of software in the vehicle and fleets

Vehicle model type cybersecurity certification

Use cases
for Tier 1 & Tier 2 suppliers

Vulnerability management from development until postproduction

Assessment and risk minimization of software in the vehicle and fleets

For the handover of artifacts to the OEM to pass vehicle model type approval

OEM
Benefits

Facilitates cybersecurity compliance to sell within all geographic regions

Improves safety - saving lives and preventing property damage

Improves and maintains customer satisfaction

Prevents brand damage from recalls, data breach, etc.

Reduces development costs by early vulnerability detection

Supports fast time-to-market of new vehicle types

Supports the entrance to emerging markets such as electrification and smart cities

Enables vulnerability management along the supply chain

Tier 1 & Tier 2 Supplier
Benefits

Enables selling to OEMs in all geographic regions

Reduces development costs by early vulnerability detection

Improved vehicle and fleet safety

Prevents brand damage

Supports fast time-to-market of new software and products

Streamlines entrance to new markets

CYMOTIVE's Automated Vulnerability Management

By using CYMOTIVE's Vulnerability Management solution, car manufacturers and their suppliers can automate the identification, prioritization, and mitigation of its vulnerability management, reduce unnecessary expenses, deliver the product and comply with regulation UN R155 based on the ISO/SAE 21434. CYMOTIVE provides the documentation and evidence required for Tier 1 suppliers to pass to the OEM for successful completion of the certification process.

CYMOTIVE's goal is to improve vehicle fleet safety and security by minimizing risks resulting from vulnerabilities present in the in-vehicle software components. It fulfills this goal by continuously monitoring scored and prioritized vulnerabilities, sending alerts, and recommending the best options for mitigation.

Prioritization and scoring of vulnerabilities' risk

CYMOTIVE
TRUSTED SMART MOBILITY

Id	CVSS Vector	Severity	Base Score	Tags	Description
CVE-2014-9650	AV:N/AC:L/PR:N/UI:N/S:C/C:N/...	MEDIUM	5.8		CRLF injection vulnerability in the management plugin in RabbitMQ 2.1.0 through 3.4x before 3.4.1 allows re...
CVE-2017-4961	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I...	MEDIUM	6.1		An issue was discovered in these Povotal RabbitMQ versions: all 3.4x versions, all 3.5x versions, and 3.6x ver...
CVE-2020-5419	AV:L/AC:L/PR:H/UI:N/S:U/C:H/I...	MEDIUM	6.7	Code Execution	RabbitMQ versions 3.8x prior to 3.8.7 are prone to a Windows-specific binary planting security vulnerability...
CVE-2021-24917	AV:N/AC:L/PR:N/UI:N/S:U/C:H/...	HIGH	7.5		The WPS Hide Login WordPress plugin before 1.9.1 has a bug which allows to get the secret login page by s...
CVE-2022-0407	AV:L/AC:L/PR:N/UI:R/S:U/C:H/I...	HIGH	7.8		Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.
CVE-2021-43528	AV:N/AC:L/PR:N/UI:R/S:U/C:N/...	MEDIUM	6.5		Thunderbird unexpectedly enabled JavaScript in the compositioin area. The JavaScript execution context was...
CVE-2022-20051	AV:L/AC:L/PR:L/UI:N/S:U/C:N/I...	MEDIUM	5.5	Denial Of Service	In ims service, there is a possible unexpected application behavior due to incorrect privilege assignment. Thi...
CVE-2022-24607	AV:N/AC:L/PR:N/UI:N/S:U/C:H/...	CRITICAL	9.8		Luocms v2.0 is affected by SQL Injection in /admin/news/news_ok.php.
CVE-2022-25213	AV:P/AC:L/PR:N/UI:N/S:U/C:H/...	MEDIUM	6.8		Improper physical access control and use of hard-coded credentials in /etc/passwd permits an attacker with...
CVE-2022-20054	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I...	HIGH	7.8	Privilege Escalation	In ims service, there is a possible AT command injection due to a missing permission check. This could lead t...

CYMOTIVE improves and maintains your vehicle fleet safety & security by:

Continuously inspecting the in-vehicle software throughout the full lifecycle from vehicle development and throughout the years on the road

—

Providing ongoing visibility by indicating the vulnerabilities' risk score associated with the respective software components

—

Identifying exposures associated with vulnerabilities

Assessing and prioritizing the risks, potential damage, and impact to the vehicle

—

Proposing the optimal risk minimization course of action with prioritized mitigation recommendations

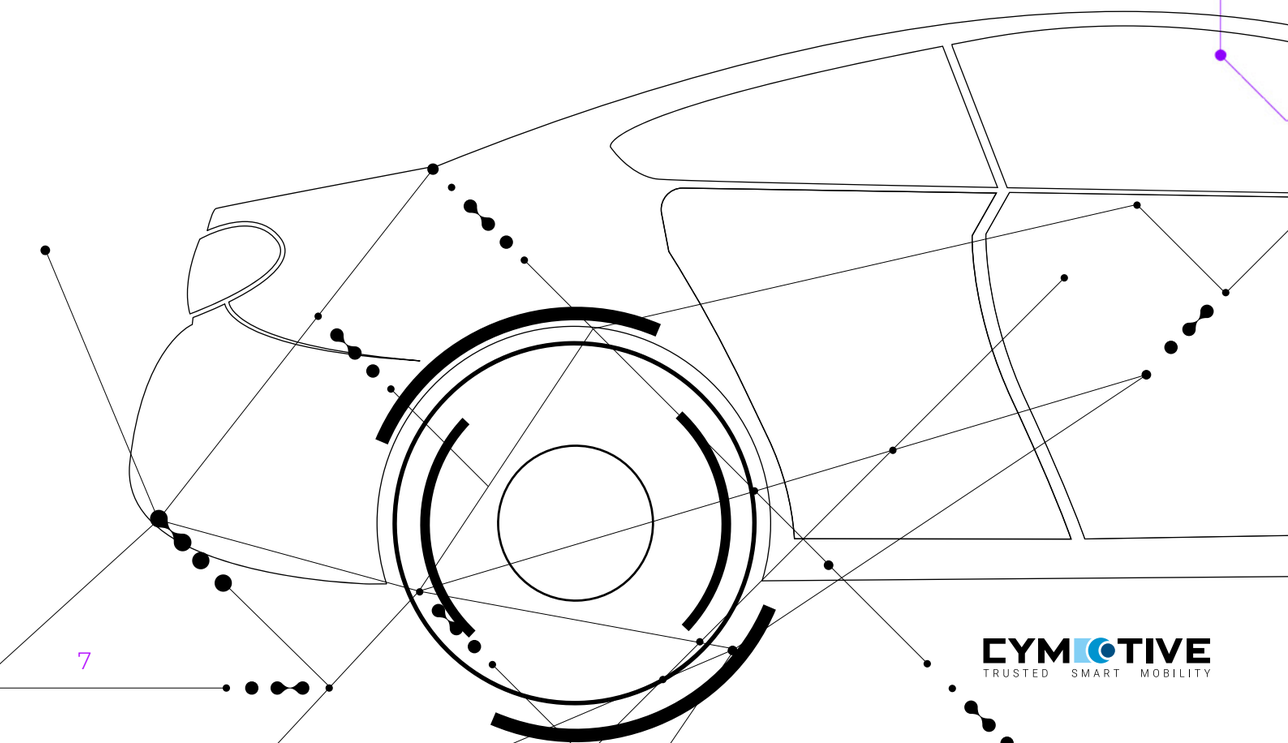
—

Providing documentation, evidence and evidence and reports required for regulatory vehicle cybersecurity compliance for certification

Proven results **on the road**

Field-proven at multi-national OEMs, CYMOTIVE manages the risk while fulfilling regulatory compliance for the entire vehicle fleet lifecycle.

With real-time visibility and insight to the critical vulnerabilities within the vehicle platform, CYMOTIVE effectively monitors the overall risk status of vulnerabilities for effective mitigation throughout the full vehicle lifecycle of development, and throughout post-production.



CYMOTIVE
TRUSTED SMART MOBILITY

CYMOTIVE
TRUSTED SMART MOBILITY

About CYMOTIVE Technologies

Founded in 2016 by top tier Israeli security experts, CYMOTIVE began as the trusted cybersecurity partner of the Volkswagen Group. Since then, the company has extended its reach to deliver pre-emptive, holistic cybersecurity solutions for vehicles, fleets and smart mobility to all car manufacturers, top suppliers and smart cities.

Our customers and partners benefit from a full lifecycle platform of trusted security solutions spanning vehicles' design, development and post-production stages. With teams working from Israel, Germany, Sweden, Italy and the U.S, CYMOTIVE offers innovation in products including vulnerability management, regulation compliance, intrusion detection & response, security testing, and related services for the smart mobility ecosystem.

cymotive.com | **sales@cymotive.com**