CYBELLUM

How to Automate your CSMS for WP.29 Compliance

Automotive manufacturers have to move quickly to stay competitive. While sufficient for meeting old regulatory guidelines, manual processes for handling cyber vulnerability detection, prioritization, mitigation and monitoring are time-consuming, cumbersome, and leave room for human error.

With an already strained labor market carrying a shortage of 3.12 million skilled security professionals, organizations need to increase efficiency and maximize the performance of their existing staff. In order to meet new regulatory requirements, improve security, and optimize production speed, manufacturers need to automate their Cyber Security Management System (CSMS). To streamline processes, automation requires a combination of the right technology and an updated approach across the entire organization.

THE NEED FOR AUTOMATION

The automotive industry is becoming increasingly complex with new capabilities such as autonomous driving and V2X communications, all of which are driven by a lot more software. According to the ASRG's and Cybellum industry survey in 2021, there was a 200% increase in lines of code over the last two years. This growth adds complexity to systems, with a larger codebase and more vulnerabilities to analyze. According to the survey, 65% of respondents considered timely assessment of new vulnerabilities significantly important, but with this growth of the codebase, manual inspection is no longer practical and unlikely to yield accurate results.

54% & 72%

Added UNECE WP 29 R155 & ISO/SAE 21434 adjustments to their roadmaps

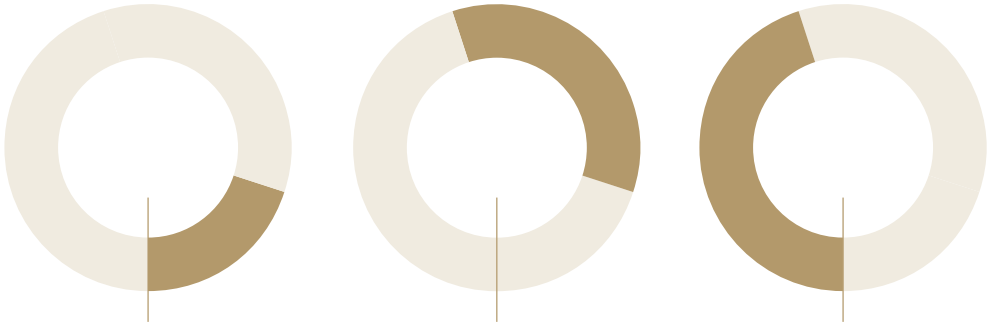
200%

Expected increase in lines of code over 2 years

65%

Consider timely assessment of new vulnerabilities to be a growing challenge

How are vulnerability management processes done in your company?



20%
Fully automated

35%
Semi-automated

45%
Manually managed

This is especially important with the need to prepare for UNECE WP29 R155/R156 and ISO/SAE 21434. Many have already added this to their roadmap, but few are fully prepared to meet the requirements.

Only a meager 6% of organizations have everything in place, and while that number is likely to have increased, it is still a known challenge putting organizations at risk of being unprepared for the July 2022 enforcement deadline. Getting up to speed requires the adoption of strict cybersecurity standards that companies can only meet fully through automation of the assessment process.

CYBER SECURITY MANAGEMENT SYSTEM (CSMS) REQUIREMENTS

UNECE WP.29 R155 requires the implementation of a certified CSMS by vehicle manufacturers for any connected vehicle. Without it, the manufacturer will not be able to get the vehicle type approval. The new CSMS requirement sets new standards for managing cybersecurity risks in vehicles, across their entire lifecycle.

The CSMS requirements include implementing security by design, mitigating vulnerabilities and supply chain risks, and managing security incidents post-production and across fleets.

To standardize the implementation of WP.29 R155, ISO/SAE 21434 comes into play. Combined, they outline the requirements for cybersecurity engineering that manufacturers and suppliers must uphold. These standards focus primarily on the following:

- **Risk Assessments** — analysis of potential damage scenarios that might impact vehicle operations and planning for how to mitigate the associated risks.
- **Security assessments** — requires a holistic analysis of code that may include source code analysis, binary analysis, penetration testing, protocol analysis, and direct application security testing.
- **Threat identification** — goes beyond simply identifying the possible bad actors but also identifying potential vulnerabilities, and discerning associated threats and their estimated impact and likelihood.
- **Continuous vulnerability monitoring** — includes monitoring potential new vulnerabilities, which may be listed in public, commercial, or private data sources. Not every vulnerability detected requires immediate mitigation, but new actionable exploits and known high-risk threats should be remediated quickly, especially when they exist in vehicles that are already on the road.

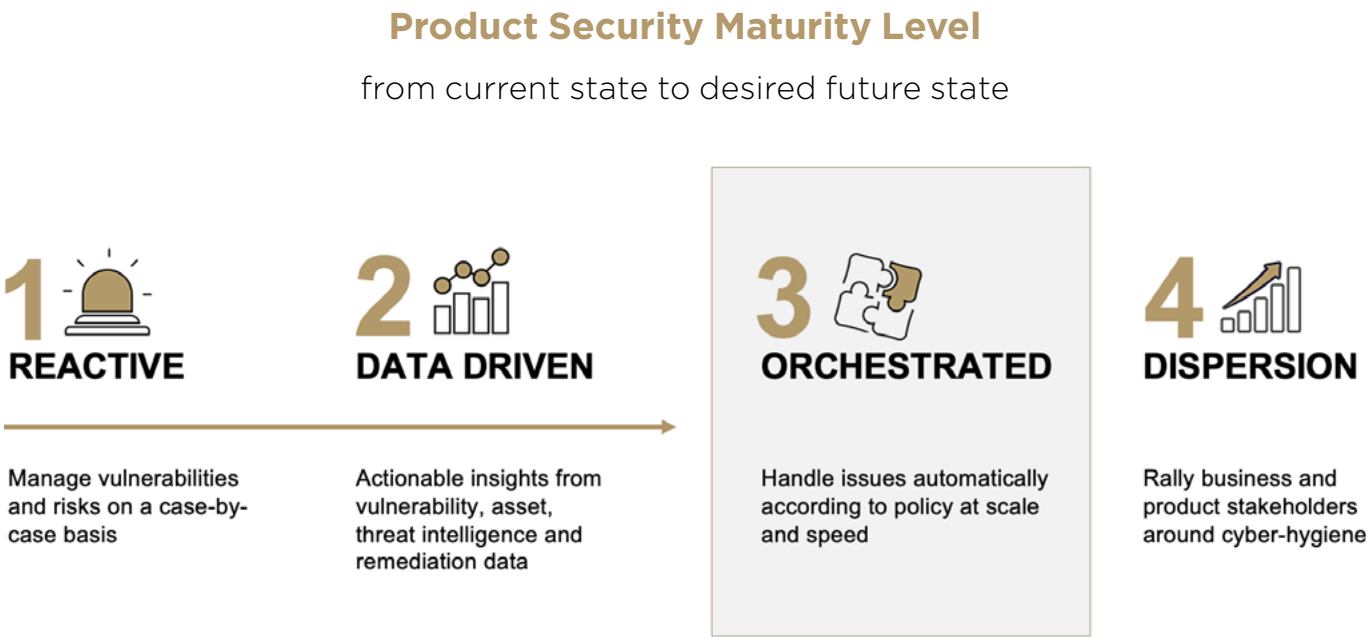
Mandating the standardization of security engineering practices upon manufacturers and their suppliers will improve the overall security of vehicles before they hit the market as well as once they're in operational use.

Product Security Maturity Model

When evaluating the maturity of product security processes at automotive manufactures, it still seems that many organizations take a reactive approach to security. They manage vulnerabilities and risks on a case-by-case basis as they are discovered. This approach is the equivalent of fire fighting and it becomes rather easy to be overwhelmed as the number of vulnerabilities rises daily.

Evolving from this is the data-driven approach that organizations move to as they start to adopt the tools to help them to proactively identify and remediate threats and vulnerabilities. These tools create actionable insights that assist in triaging and remediating vulnerabilities. Unfortunately, these tools are not sufficient to handle the scale and speed that organizations require in order to operate effectively vis-a-vis cyber threats and cyber compliance needs.

This is where an orchestrated approach that leverages automation comes into play. Successfully implementing automation is not simply about throwing technology at the problem. It is about organizing people, processes, and technology around agreed upon policies, to create a scalable identification, management, and resolution system. It does not eliminate the need for a decision-making process, but instead streamlines operations, guiding the processes to flow seamlessly towards resolution by the right teams.



CSMS AUTOMATION OPPORTUNITIES

Automated practices are necessary to drive security assessment, threat identification, and vulnerability monitoring at scale to help make products secure throughout their entire life cycle, and meet new cyber compliance requirements such as WP.29 and ISO/SAE 21434.

Below is a list of automation opportunities in support of a certified CSMS.

Generating SBOMs

A fundamental step in assessing device security is understanding the make-up and composition of your vehicle software. This is where SBOMs are a must have.

SBOMs can be received from your suppliers, or generated from source code –if available. However, in many cases, product security organizations only have the binaries available – e.g. ECU firmware. In these cases automated scripts and SBOM generation tools can be used to expose the software composition of your vehicle components, directly from the binary files.

However, this is not a one-off process, it has to be repeated continuously with every new build and software release to validate the security of your products.

Things to watch out for include:

- Extraction of file formats
- Nested software libraries
- Impact of architecture on detection performance
- Inconsistent naming (vs. NVD taxonomy etc.), though standards like SPDX are helping out.
- False positives and false negatives
- Accurate detection of package version
- Commercial and proprietary software typically are not covered well

Vulnerability Analysis

Vulnerability analysis requires going beyond simply knowing what assets are present. It requires cross-referencing known vulnerabilities vs. the assets identified with the wide selection of vulnerability repositories, a rather significant quantity of data exceeding what can be parsed manually.

Here as well, automation is essential to the process. The threat landscape is constantly evolving with new vulnerabilities being disclosed daily, including zero-day vulnerabilities that have no patch or remediation. Consistent vigilance is required to stay abreast of the latest discoveries and take action to mitigate the vulnerabilities before the attackers can make use of them.

It is also important to note that the context of a vulnerability is crucial for determining whether it requires mitigation. Not every vulnerability in a software library used in your product is high risk and affects the final product. Using automated contextual analysis of vulnerability data, teams can automatically triage threats and prioritize their work on the most relevant vulnerabilities.

OS Hardening

In the past, hardening the OS was a manual process, ensuring that lists of security requirements were followed on every new system created. This process was time-consuming and had no guarantee of consistent implementation. Inconsistencies led to vulnerabilities being present on some systems while not on others. In addition, requirements differ between vendors and product types, making it much harder to keep track of the state of compliance.

The latest solutions leverage automation to create consistent implementation across suppliers and products. An organizational-level security policy can be compiled and centrally managed. By managing requirements in a single policy, scripts and tools can be configured to validate these requirements in every new build, across all products.

OS hardening issues to watch out for:

- Unsafe software (troubleshooting/debugging utilities etc.)
- Linux kernel configuration (flags, sysctl)
- Insecure file permissions
- Authentication issues (passwd/shadow, PAM etc.)
- Insecure access issues

Automated Threat Identification

UNECE WP.29 R155 Annex 5 includes guidelines for threat identification

- Part A covers the creation of a baseline for threats, vulnerabilities, and attack methods
- Part B specifies mitigation of threats that are intended for vehicle types

Meeting these requirements manually is challenging. Automating threat detection efforts is the practical way to efficiently and effectively guarantee compliance. You can create an automated process like the following one:

Step 1 — Map threats to CWEs: each Annex 5A threat can be mapped to actual vulnerabilities that can be identified in a firmware

		Vulnerability	How to detect using firmware analysis
4.3.2 Threats to vehicles regarding their	Spoofing of messages or data received by the vehicle	4.1 **Spoofing of messages** by impersonation (e.g. 802.11p V2X during platooning, GNSS messages, etc.)	Search for vulnerabilities tagged with the these weakness types: • CWE-290 - Authentication Bypass by Spoofing • CWE-345 - Insufficient Verification of Data Authenticity • CWE-924 - Improper Enforcement of Message Integrity During Transmission in a Communication Channel • CWE-353 - Missing Support for Integrity Check • CWE-354 - Improper Validation of Integrity Check Value • CWE-346 - Origin Validation Error

Step 2 — Identify Threats from Asset: CWE mapping to identified vulnerabilities

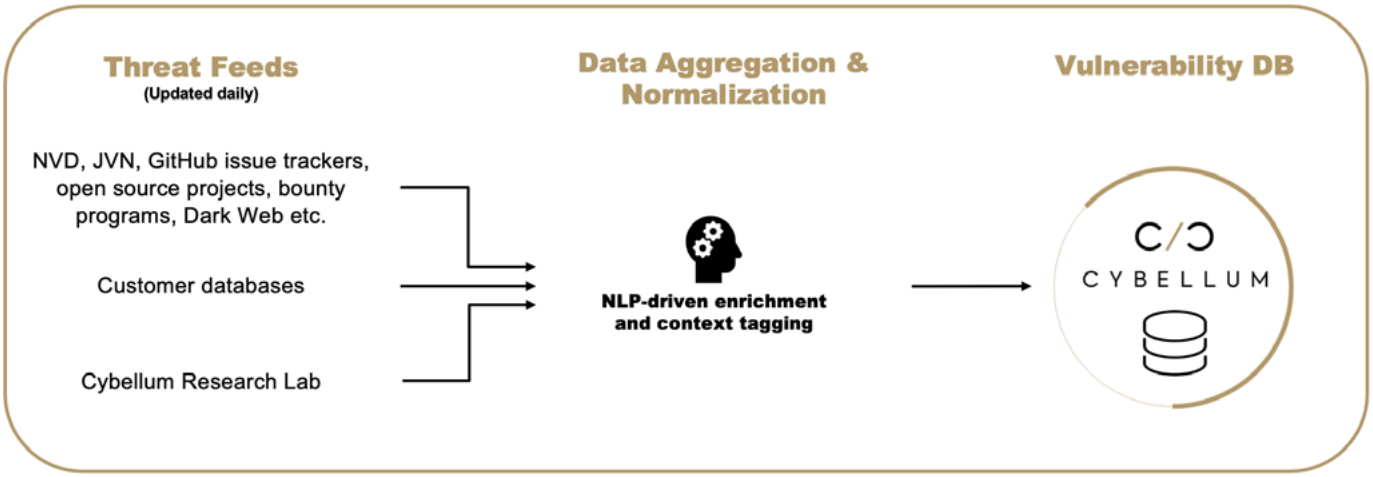
Weakness	Vulnerability	Example vulnerability
CWE-290	Authentication Bypass by Spoofing	CVE-2021-23984 / Firefox A malicious extension could have opened a popup window lacking an address bar. The title of the popup lacking an address bar should not be fully controllable, but in this situation was. This could have been used to spoof a website and attempt to trick the user into providing credentials. This vulnerability affects Firefox ESR < 78.9, Thunderbird < 78.9, and Firefox < 87.

Threat Intelligence Monitoring

As part of threat identification, organizations need to create scripts or use tools that monitor vulnerability feeds and match them against SBOMs. Some organizations subscribe to a single feed such as NIST NVD and consider that enough to stay on top of new vulnerabilities.

Unfortunately, one single feed as a source does not provide a comprehensive view of all known vulnerabilities and threats, especially those from hard to scour sources like the dark web, making it insufficient to provide the necessary intelligence for monitoring.

It is only through the aggregation of multiple feeds that an organization can feel confident that they are able to detect all of the new vulnerabilities or newly affecting vulnerabilities for their product. This is an impossible task to manage manually and without automated aggregation and normalization of the results, it is easy to drown in the flood of data, and not be able to discern what is relevant and what is superfluous.



SUMMARY

Automation implemented throughout the entire software lifecycle is key to ensuring security. It is essential for parsing through large volumes of data to ensure that accurate information is delivered for smart decision making. Without effective automation, manual tasks bog down discovery and analysis, creating the potential for vulnerabilities to be missed.

Implementing a certified CSMS and meeting all of the requirements set out by UNECE WP.29 cannot be effectively accomplished through manual efforts. Automation streamlines the processes and guarantees that the required procedures are followed every time.

SUCCESS WITH CYBELLUM

Cybellum enables automotive OEMs and suppliers to keep the products they build secure and compliant, every single moment of their life.

Industry leaders use Cybellum's product security platform to fuse security into every phase of the product lifecycle. Powered by Cyber Digital Twins™ technology -- a live digital replica of every software component inside your devices – Cybellum allows product security teams to manage cyber risk continuously, whatever new threat arises.

From living SBOMs, to automated vulnerability management and continuous monitoring, teams can ensure their product portfolio is secure from design to post-production and beyond.

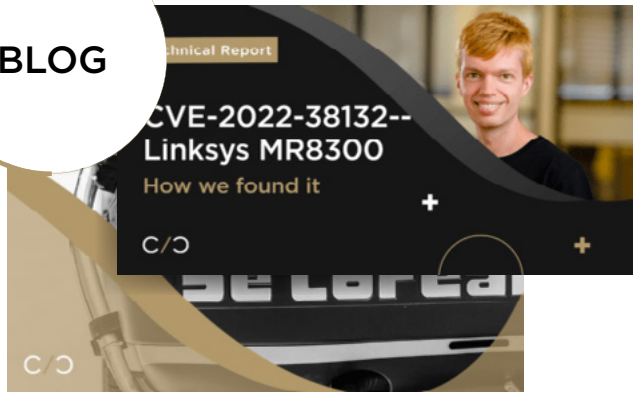
Schedule a demo today to discover how Cybellum can help your organization meet your security automation needs.

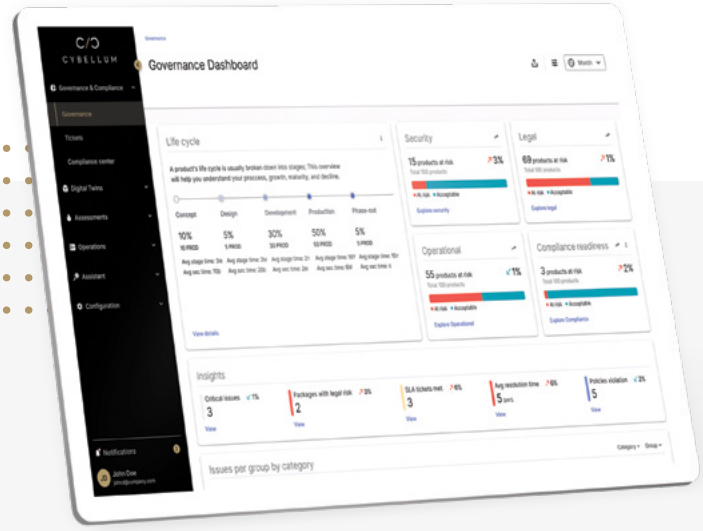
RESOURCE CENTER

PODCAST

LEARN MORE ABOUT PRODUCT SECURITY

BLOG





MORE ABOUT
The Product Security Platform

FOLLOW US FOR NEWS AND UPDATES

CYBELLUM.COM