

Full Throttle Cybersecurity

How McLaren Uses Cybellum to Drive
Product Security Excellence



Background: The Need for (Cyber) Speed

McLaren Automotive is a brand that needs no introduction. Renowned for its high-performance super cars, the company is producing some of the most innovative, iconic, and exciting cars ever made, both on and off the racing tracks. For that reason, the company places a significant emphasis on automotive cybersecurity.

Bruce McLaren, the company's legendary founder, once famously said, "Life is measured in achievement, not in years alone." Following his vision, the automotive cybersecurity team at McLaren set a goal to achieve the highest possible cybersecurity standard for their cars and their CSMS (Cybersecurity Management System), in line with regulatory requirements. With the increasing complexity of connected vehicles and stringent regulations, McLaren sought a solution to ensure comprehensive security and compliance for their automotive software and electronic control units (ECUs).

On the Fast Track to CSMS:

McLaren's Cybersecurity Goals

McLaren's Automotive Cybersecurity team had three primary goals for their cybersecurity operation, which demanded a comprehensive solution:



Risk Assessment and Analysis

Understanding and managing the risks associated with their connected vehicles, including vulnerabilities, to mitigate them quickly.



Regulatory Compliance

Ensuring McLaren's vehicles meet legislative standards for cybersecurity, such as ISO 21434, WP. 29 R155, and more.



Engineering Team Training

Upskilling the team to design secure embedded systems.

The McLaren team needed a solution that offered detailed vulnerability information and supported their internal software development processes, requiring comprehensive asset management and vulnerability management capabilities, as well as robust integration with McLaren's existing toolchain and workflow.

A Winning Team:

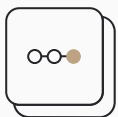
Choosing Cybellum's Product Security Platform

McLaren evaluated multiple solutions before choosing Cybellum's Product Security Platform. A few key factors influenced their decision:



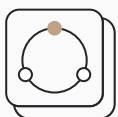
Customized for the Automotive Industry

The team at McLaren was looking for a solution that was tailored specifically for automotive cybersecurity, differentiating it from other enterprise-focused solutions.



Advanced Vulnerability Management Capabilities

The ability to detect vulnerabilities, prioritize them quickly and efficiently, and provide actionable insights was crucial.



Integration with McLaren's Ecosystem

The solution needed to fit seamlessly into McLaren's existing infrastructure, allowing them to maintain control over their software and data.

”

Collaborating with McLaren Automotive's cybersecurity team is a true masterclass. McLaren is setting new benchmarks in automotive cybersecurity, and with Cybellum's Product Security Platform, I'm confident they'll not only achieve their ambitious goals but also become renowned for both their incredible cars and unmatched cybersecurity.

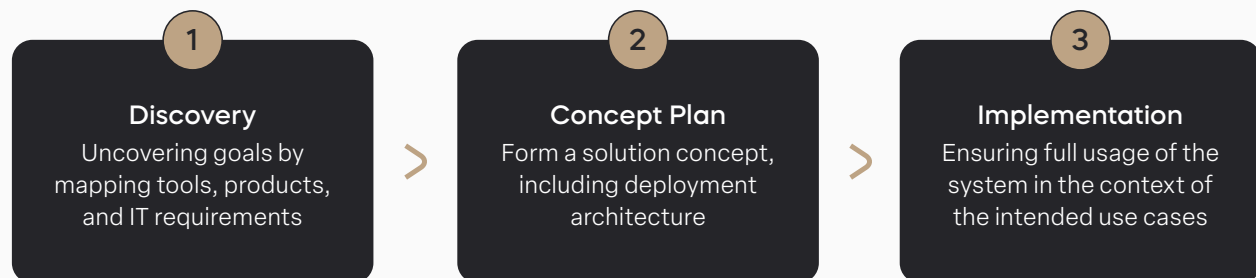
Eddie Lazebnik, VP Channel Sales, Cybellum

Jump Starting:

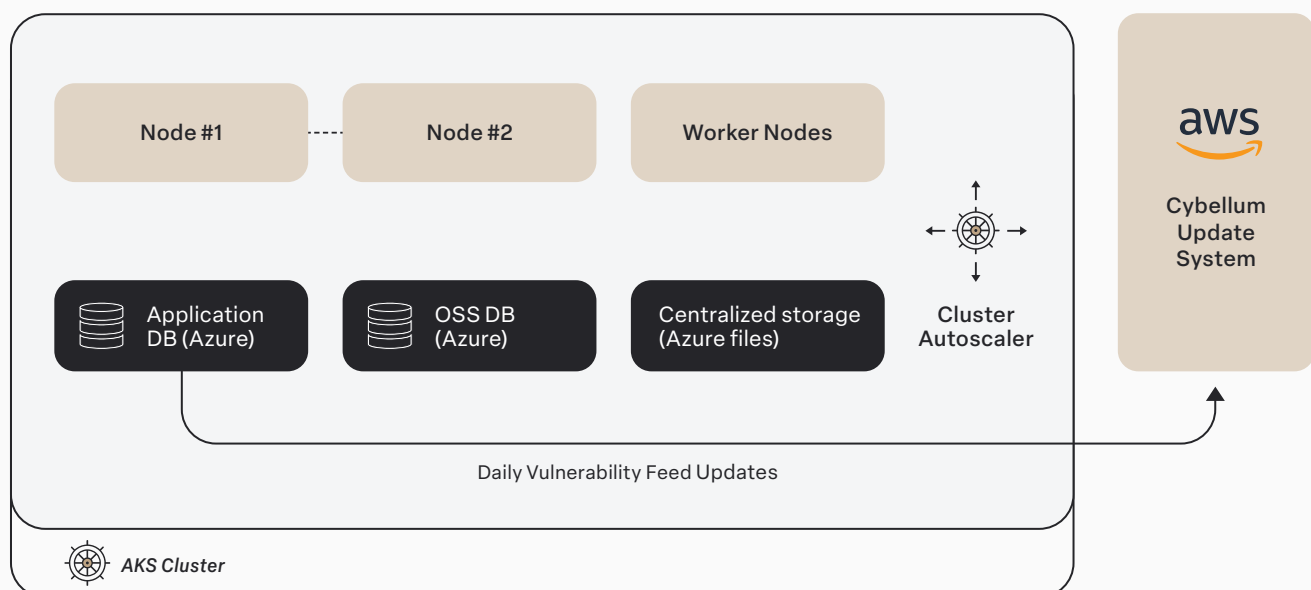
Deployment & Customization

As part of the engagement, Cybellum provided a dedicated team of experts to integrate and customize the Product Security Platform for McLaren's unique IT infrastructure.

The goal is to develop additional integrations and capabilities tailored to McLaren's needs and ensure extensive utilization of the platform's features by McLaren's team. The deployment and customization process includes the following steps:



One of the main goals of this process was to ensure full support for Kubernetes AKS in McLaren's instance of the Product Security Platform. After a joint discovery session between Cybellum and McLaren Engineers, the following high-level deployment architecture was built to allow for accurate and automatic data exchange with AKS:



Enjoying the Ride:

How McLaren Will Use Cybellum's Solution

McLaren's goal is to streamline the management of multiple CSMS activities using Cybellum's platform:



Comprehensive Software Audits & Asset Management: Conducting a thorough software audit to produce a detailed SBOM, enabling visibility into the full range of software used within McLaren's products.



Vulnerability Detection and Management: Detecting known and potential vulnerabilities, covering both Common Vulnerabilities and Exposures (CVEs) and Common Weakness Enumeration (CWEs).



Vulnerability Prioritization: Using Cybellum's smart triaging assistant, the VM CoPilot, the McLaren team will narrow down and mark irrelevant vulnerabilities automatically based on customer input and filtering criteria.



Regulatory Compliance & Evidence Creation: Defining and implementing controls and processes aligned with automotive UN Regulation No. 155, and producing compliance-ready reports.



CSMS Risk Management: Using the platform's CSMS Cockpit, the McLaren team will track cybersecurity KPIs such as risk scores, vulnerability mitigation status, and more.



Software Security Strategy: Developing a comprehensive strategy aligned with ISO 30111, utilizing data and workflows provided by the platform.



Continuous Monitoring: Maturing the product software security process through regular reviews and adaptive responses to new threats and vulnerabilities.

By using Cybellum's Product Security Platform, McLaren plans to achieve ongoing identification of vulnerabilities relevant to its products and components, based on SBOMs, binary files, and other sources of asset data. The platform's context-aware detection and prioritization capabilities provide McLaren's security team with a contextual evaluation of threats and vulnerabilities, enabling them to address the most relevant high-severity threats.



The Road Ahead:

McLaren's Future Cybersecurity Vision

McLaren aims to automate their cybersecurity processes further and integrate Cybellum's solution with other tools in their engineering ecosystem, such as Jira. This will enhance their ability to manage vulnerabilities across the numerous electronic control units (ECUs) in their vehicles.

McLaren's engagement with Cybellum exemplifies a strategic approach to automotive cybersecurity. By partnering with Cybellum, McLaren aims to ensure their vehicles are not only technologically advanced but also secure, providing their customers with peace of mind. This collaboration highlights McLaren's commitment to continuous innovation and excellence in the automotive industry and beyond.



About us

CYBELLUM IS WHERE TEAMS DO PRODUCT SECURITY.

Device manufacturers such as Jaguar Land Rover, Supermicro, Danaher, and Faurecia use Cybellum's Product Security Platform and services to manage cybersecurity risk and compliance across business units and lifecycle stages. From Asset & SBOM Management to Assurance & Vulnerability Management, Compliance Validation, and Incident Response, teams ensure their connected products are fundamentally secure and compliant – and stay that way.

Follow us for news and updates

cybellum.com

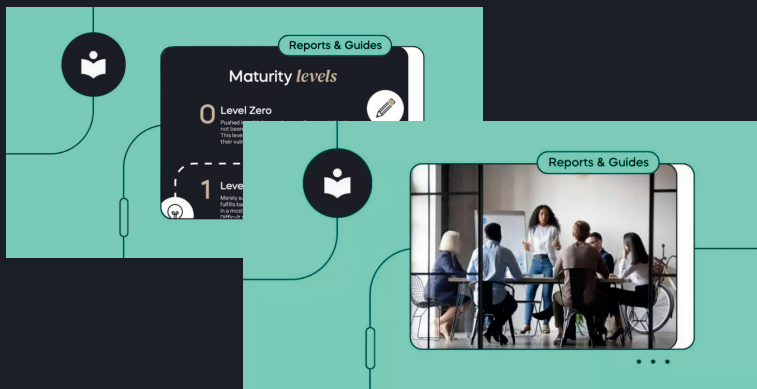


Stay in the know about everything product security

Listen to “Left to Our Own Devices” - the product security podcast



Subscribe to the Product Security Knowledge Center



See the Product Security Platform in Action

Learn how device manufacturers keep their connected products cyber secure and cyber compliant across teams, business units and lifecycle stages.

C/C

Risk Management Cockpit

On track

At risk

Off track

Not started

Product	Supplier	Risk	Submission Readiness	Next Milestone	Threat Modeling	Risk Monitoring
JX700	Nuwheel	8.4	78%	MS1 9/4/2024	<div>Mary</div>	<div>John</div>
VX800	VMG	7.4	89%	SOP 1/26/2024	<div>Ronald</div>	<div>Jenny</div>
VX900	VMG	7.4	23%	FC 5/17/2024	<div>Cameron</div>	<div>Darrell</div>
TM500	Nuwheel	6.9	57%	QP 2/26/2024	<div>Ralph</div>	<div>Robert</div>
LMIC	MF	5.3	90%	MS3 12/25/2023	<div>John</div>	<div>John</div>
MIB3	VMG	3.9	11%	QP 5/7/2024	<div>Cody</div>	<div>Darrell</div>





C Y B E L L U M