Industry Survey by Cybellum and ASRG

Regulations Are Coming: **How Do Your Vulnerability Management Processes Stack Up?**

July 2021

Executive Summary

The introduction of Connected, Autonomous, Shared, Electrified (CASE) technologies is driving a huge evolutionary shift in the automotive industry. This trend of adding smart capabilities in every type of industrial, commercial and private vehicle is just getting started, and we're only now beginning to see the industry prepare itself for the disruptive changes underway.

According to McKinsey[1], this new generation of smart vehicles promises to deliver significant public benefits that could exceed $800 billion a year by 2030 in the US alone. These savings would derive from more productive commuting time, the redevelopment of unnecessary parking spaces and the elimination of millions of fatal and nonfatal car accidents each year.

These new, intelligent capabilities driving the CASE revolution are powered by Electronic Control Units (ECUs) embedded within the vehicle.

According to the United Nations Economic Commission for Europe (UNECE)[2], today's connected cars possess up to 100-150 of these ECUs and include around 100 million lines of software code.

These numbers are only growing year by year as advanced technology is added to more and more systems within the vehicle.

However, all these changes also bring about new cyber risks and security challenges. To achieve the benefits of CASE technologies, cybersecurity will be the enabling attribute.

To ensure that the public remains safe in our new connected reality, governments and authorities around the world are drafting new regulations. These are aimed at introducing automotive cybersecurity standards for the design, development and post-production lifecycle stages of the vehicle.

An essential part of the regulation (UNECE WP.29 chapter 7.2 and ISO/SAE 21434 chapters 5 and 6) is the establishment of vulnerability management operations including pre-defined processes, policies and dedicated resources and tools for the ongoing vulnerability identification, analysis and monitoring.

Reports show that automotive hacking incidents doubled between 2018-2019.

[1] www.mckinsey.com/industries/automotive-and-assembly/our-insights/the-trends-transforming-mobilitys-future | [2] www.mckinsey.com/industries/automotive-and-assembly/our-insights/the-trends-transforming-mobilitys-future

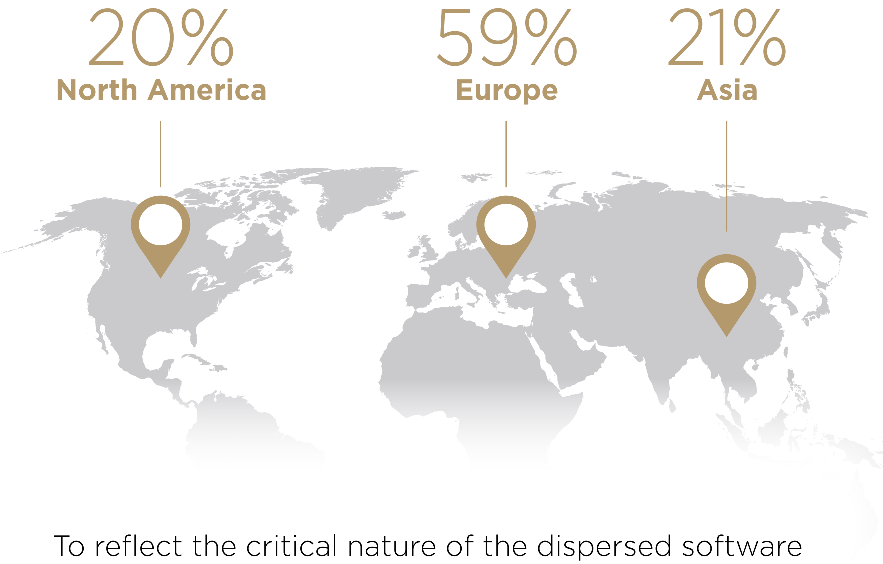
Executive Summary

Cybellum and ASRG partner to empower industry-wide transparency and openness regarding the ecosystem's vulnerability management status and provide the ecosystem with a channel through which their voice can be heard.

This survey was created with precisely that goal in mind.

It provides insights resulting from a survey conducted with leading Tier-1 suppliers and OEMs, in cooperation with ASRG. Its goal is to assess the current state of the automotive industry's vulnerability management processes in light of the recent approval of the UNECE WP.29 R155.

A truly global survey, respondents' hail from all corners of the world.



To reflect the critical nature of the dispersed software supply chain within the manufacturing process, the survey targeted both OEMs and suppliers:

49%
OEMs

34%
Tier-1 and 2 suppliers

26%
Related service providers, TIC companies and consulting firms

There currently is no standard approach to automotive vulnerability management

Results show that the majority of respondents employ manual vulnerability management processes, and that a wide variety of tactics and processes are used to secure vehicles

6 CVE sources and counting

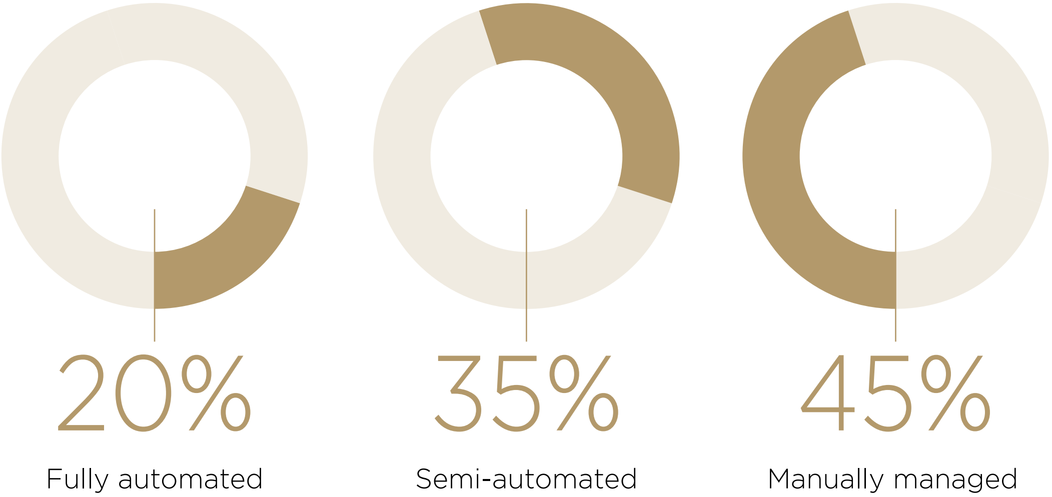
63% Haven't automated any aspect of their vulnerability management process

10 Different vulnerability management use cases

A snapshot of the state of automotive cybersecurity shows a fractured landscape.

Each industry player leverages a unique approach to handling the issue. OEMs and suppliers use multiple, disparate data sources, different vulnerability identification and analysis techniques and report different levels of vulnerability management automation.

How are vulnerability management processes done in your company?



There currently is no standard approach to automotive vulnerability management

However, best practices push for the automation of vulnerability management, as manual processes can't meet the rigorous requirements mandated by the coming regulations. Specifically, given the increase in lines of code and connected devices that go into each vehicle, all need to be analysed for risk assessment pre-SOP and throughout their entire lifespan. Furthermore, the potentially life threatening impact of automotive vulnerabilities mandates a timely, speedy approach to remediation.

After all, if your vulnerability assessment is done manually, you might not even identify some vulnerabilities which would result in continuous risk and potential damage to your company and customers.

Vulnerability management dictates that every software component within a vehicle be validated for exposure to vulnerabilities. Many respondents report that they use between 3-6 different data sources for vulnerability exposure validation. When done manually, this process is particularly time-consuming, especially considering that it must be executed every time a new version, patch or update of the component is released or vulnerability is published.

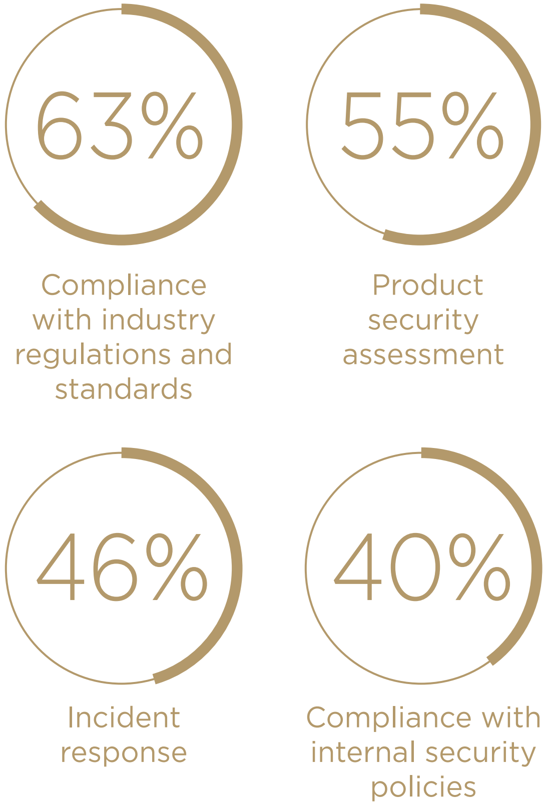
Many industry players have begun considering automated vulnerability management solutions, for a variety of different reasons.

Responses clearly show that compliance is a key driver of systematic vulnerability management processes, however, it is the bare minimum needed to protect customers and businesses.

Vulnerability management automation will significantly minimize the time it takes to detect and identify a vulnerability.

What's more, as manual processes can completely overlook a significant vulnerability resulting in ongoing, continuous risk levels, the adoption of automation will substantially reduce risk over time.

Use-cases include



Manual Vulnerability Management Processes Can’t Cope with Increasing Threats and Comply with New Regulations

Industry survey results show that time-consuming manual processes leave OEMs exposed

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

The release of ISO/SAE 21434 and UNECE WP.29 R155 and R156 - which entered into force on 22 January 2021 - are catching many leading automotive Tier-1 suppliers and major OEMs off guard.

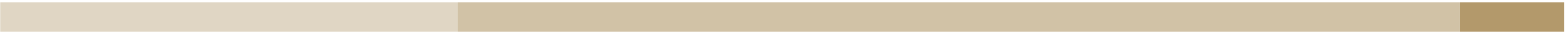
But regulations are just the tip of the iceberg. With more technology embedded within the latest model vehicles, manual vulnerability management processes will be hard-pressed to verify that every software component is secure.

Adding more teams and personnel isn’t an option. The 2020 Cybersecurity Workforce Study reports that there are currently 3 million open cybersecurity positions worldwide[3],while cybersecurity professionals with relevant automotive embedded-design experience **are in short supply**[4]. What’s more, with razor-thin profit margins and no clear path to monetize cybersecurity in sight, scaling manual processes simply doesn’t make economic sense.

29%
Haven't even began preparing

65%
In the midst of preparations

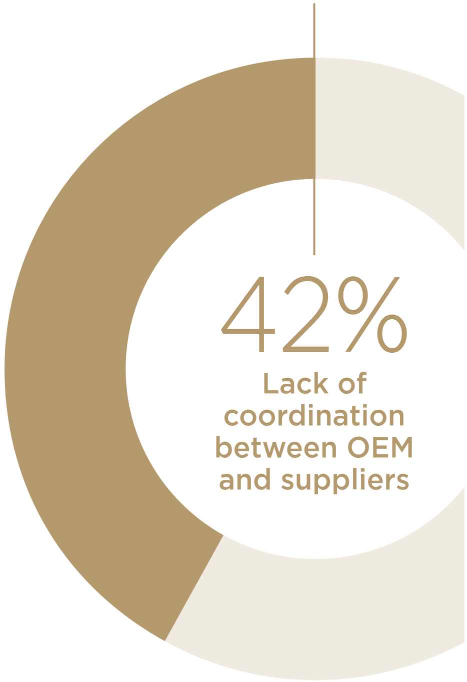
6%
Fully prepared for regulations



[3] www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B

[4] www.forbes.com/sites/stevetengler/2021/02/23/the-threat-from-within-automotive-ramps-up-cybersecurity-but-must-understand-hiring-better/?sh=555cc7f41fbc

Manual Vulnerability Management Processes Can't Cope with Increasing Threats and Comply with New Regulations

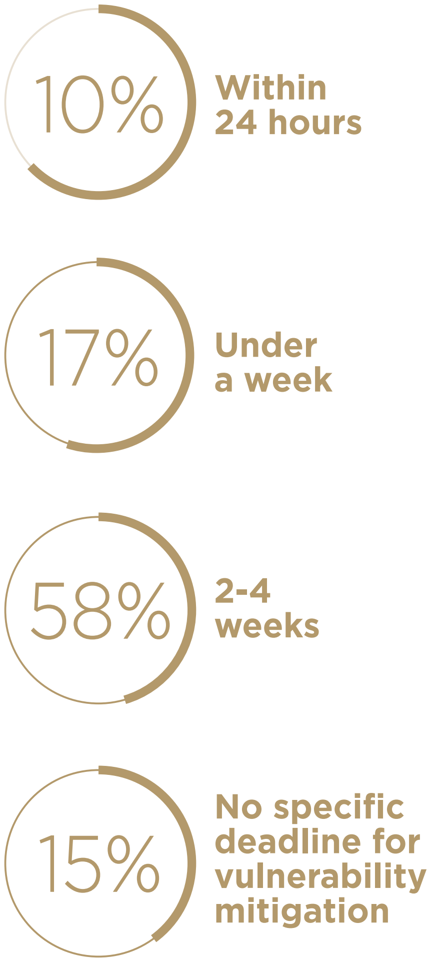


Manual vulnerability management processes are especially time-consuming, a fact which leaves many manufacturers exposed to huge risks. In a well-executed vulnerability management operation, once the binary is scanned for vulnerabilities, any identified weaknesses are analyzed, prioritized and mitigated.

This process is carried out multiple times, for each vulnerability, for each program / product and for each version. Given the more than 100 ECUs embedded within the modern vehicle, these slow manual processes can potentially cause delays in SOP or hinder any timely response to post-production cybersecurity incidents.

If that wasn't enough, respondents cite a lack of coordination between OEM and suppliers (42%) to be a significant impediment to timely assessments. Manufacturer requests for mitigation need to trickle down the supply chain, until the specific sub-vendor that supplied the vulnerable component is identified. Product security teams coordinate with both internal and supplier development teams to understand who should handle their change request, and how and when it will be handled; depending on the development cycle, even once the correct team is identified, prioritization often kicks in and fixing bugs, for example, may no longer be the dev team's focus. This lack of coordination often results in wasted time and resources and is often a leading factor in the decision to not mitigate a certain vulnerability, either before or after production.

Time for risk assessment



Yet the time it takes for a product security team to assess new publicly reported vulnerabilities is a pressing issue.

Less than 10% of respondents perform risk assessments within 24 hours of the exposure of a new vulnerability, while for a whopping 58% it takes more than a week and up to 4 weeks.

Why does this even matter? It gives hackers more time to learn about vulnerabilities and exploit them in a method that is referred to as N-day vulnerability exploit.

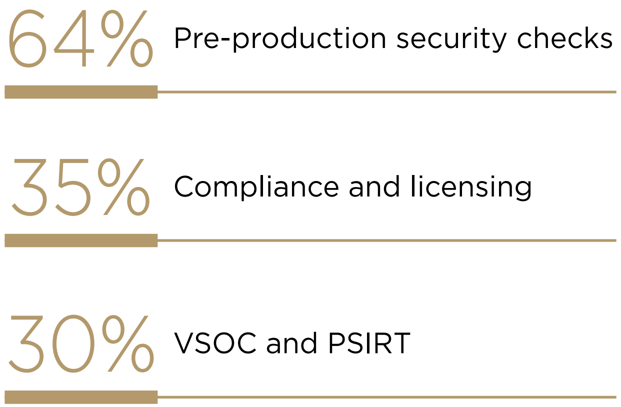
For automotive manufacturers this means a greater risk for a security event impacting their products in the field.

With the clock quickly ticking down on the launch of new standards and regulations, industry players are becoming apprehensive. Many are considering upgrading their vulnerability management solution as a way to cope with these significant challenges.

64% report that they're looking for a vulnerability management solution with pre-production security checks, as mandated by regulations. Another 35% reported that they see compliance and licensing as one of the main drivers for a vulnerability management solution.

For many of these industry players, compliance requires significant upgrades to their current development processes.

Vulnerability Management Use Cases

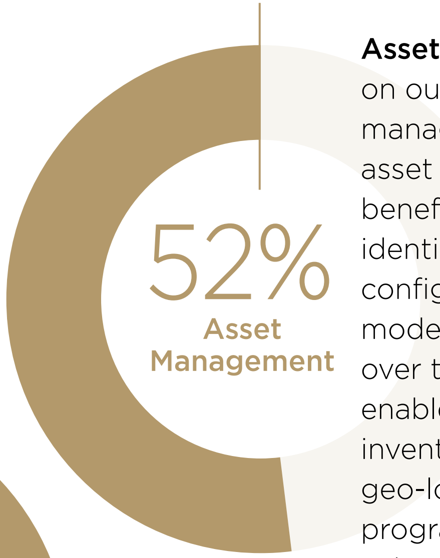


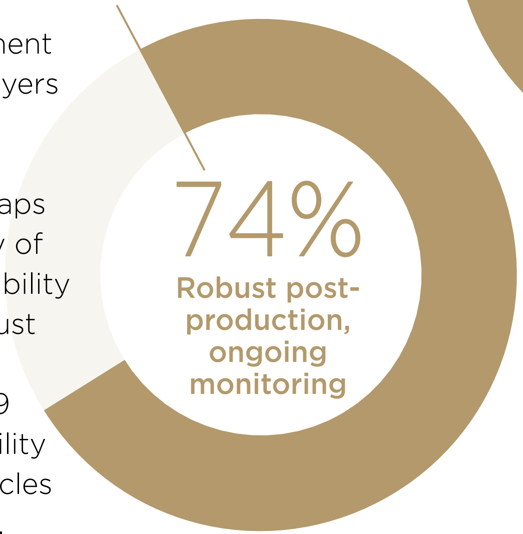
A Fully Automated Vulnerability Management Process Is The Only Way Forward

Automotive OEMs and Tier-1 suppliers are looking to focus on the aspects of automation that provide the most value

With new cybersecurity challenges increasing on every front, the automation of vulnerability management processes is the best option for industry players. The combination of the acute automotive cybersecurity skills shortage, the critical importance of timely vulnerability assessment and mitigation processes and the increasing scale of software within vehicles leaves little choice.

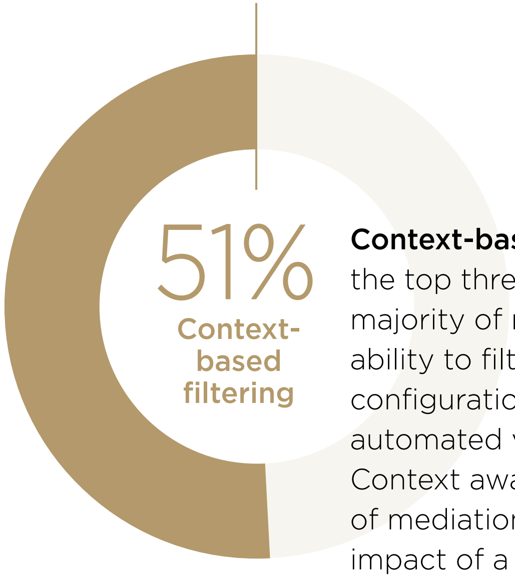
However, not every vulnerability management solution is built the same, and industry players clearly prefer features that enable them to speed up vulnerability assessment and remediation by focusing on the security gaps that matter most. Specifically, the majority of respondents (74%) are prioritizing vulnerability management solutions that empower robust **post-production, ongoing monitoring**. This is a central tenet of the UNECE WP.29 R155 regulation, formalizing the responsibility of the OEM to ensure that connected vehicles remain secure even after they hit the road.





Asset management also ranks high (52%) on our respondents' automated vulnerability management solution wish list. With effective asset management in place, industry players benefit from the ability to quickly and easily identify all of the ECUs, licenses and software configurations embedded within a given model and keep that information updated over time. Additionally, asset management enables the slicing and dicing of asset inventory by various attributes such as geo-location, business-unit or development program. Such a vulnerability management solution should also be able to automatically detect vulnerabilities across the entire asset inventory, both during and post development, so they can be remediated before any exploitation can take place.

A Fully Automated Vulnerability Management Process Is The Only Way Forward



Context-based filtering was also ranked among the top three desired capabilities, with the majority of respondents (51%) prioritizing the ability to filter vulnerabilities based on the exact configuration in place as a critical feature in an automated vulnerability management solution. Context awareness enables the prioritization of mediation efforts according to the potential impact of a vulnerability, specifically the most pressing issues. Context-based filtering eliminates irrelevant vulnerabilities based on the exact configuration within a given model. With context-based filtering a part of their vulnerability management solution, product security teams can prioritize their efforts and quickly eliminate security gaps, significantly speeding up vulnerability prioritization and mitigation.

Cyber Digital Twins™

Enabling Automotive Manufacturers to Develop and Maintain Secure Products

Cybellum's Cyber Digital Twins™ platform provides comprehensive visibility into automotive software, revealing their make-up, characteristics and the context in which they operate. All this using only binary files, no source code needed.

It exposes the underlying S-BOM, hardware architectures, operating systems, configurations, control flows, API calls, licenses, encryption algorithms and keys, hardening mechanisms and more – generating an accurate digital replica - a Cyber Digital Twin - of every vehicle component.

Armed with such a deep understanding of vehicle software, Cyber Digital Twins™ automates vulnerability management, compliance validation, continuous monitoring and incident response, minimizing risk to your customers and your organization.

Cyber Digital Twins™ provides your product security team and PSIRT with the visibility, context and agility needed to focus on the most relevant and pressing cyber threats, trace their origin across the supply chain and quickly mitigate them, during and post-development.

ABOUT ASRG

The Automotive Security Research Group (ASRG) is a non-profit organization focused on the advancement of the automotive security industry. Through knowledge, networking and collaboration, we enable the worldwide community of nearly 8000 members in 42 locations to create more secure products by building competencies in automotive security. To get more involved, make an impact on the industry, participate in a technical committee, or become part of a project, please reach out to us.

You can find out more about ASRG at www.asrg.io or send us an email at hello@asrg.io

ABOUT CYBELLUM

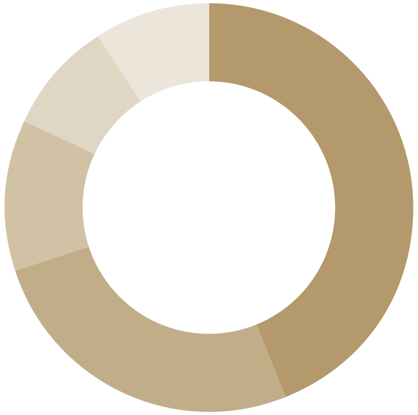
Cybellum is where teams do product security.

Top Automotive manufacturers such as Jaguar Land Rover, Nissan, Audi, and Faurecia use Cybellum's Product Security Platform and services to manage cybersecurity risk and compliance across business units and lifecycle stages. From SBOM to Vulnerability Management, CSMS Management, and WP. 29 Compliance Validation, teams ensure their connected products are fundamentally secure and compliant – and stay that way.
For more information:

Please visit www.cybellum.com
or connect with us on:

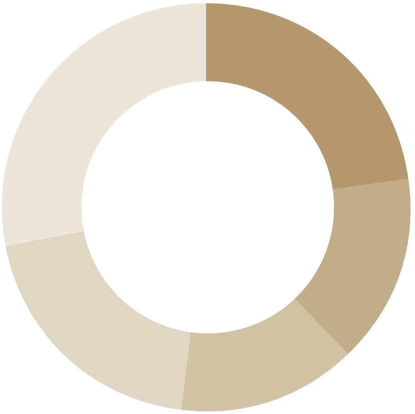
A Detailed Look at the Numbers Behind this Report

How many different ECUs did your team manage for cybersecurity over the last 12 months?



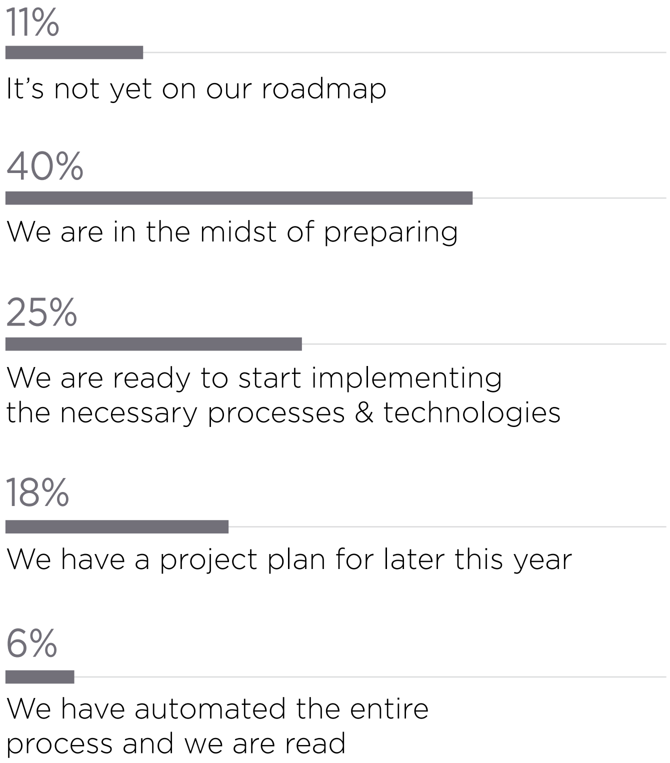
●	1-5	44%
●	6-10	26%
●	11-15	12%
●	16-20	9%
●	21 & more	9%

How many different ECUs do you expect to manage in two years?



●	1-5	23%
●	6-10	15%
●	11-15	14%
●	16-20	20%
●	21 & more	28%

How prepared are you for the new standards and regulations coming into effect?



11%

It's not yet on our roadmap

40%

We are in the midst of preparing

25%

We are ready to start implementing the necessary processes & technologies

18%

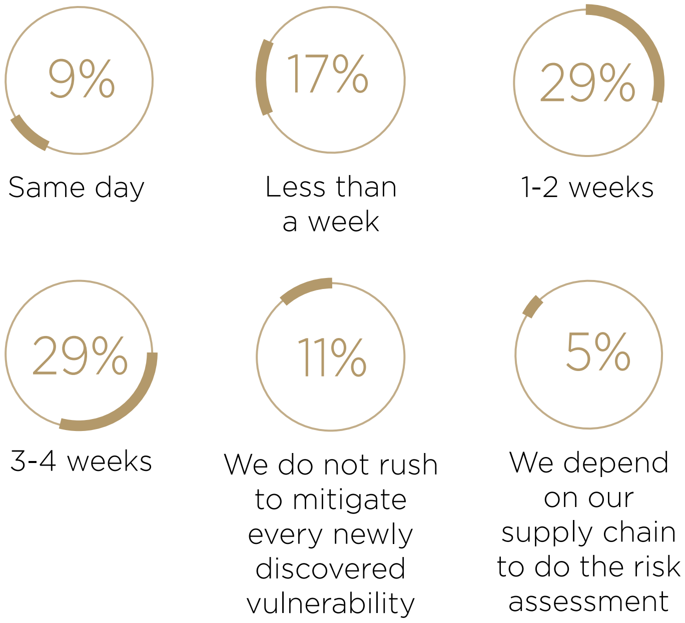
We have a project plan for later this year

6%

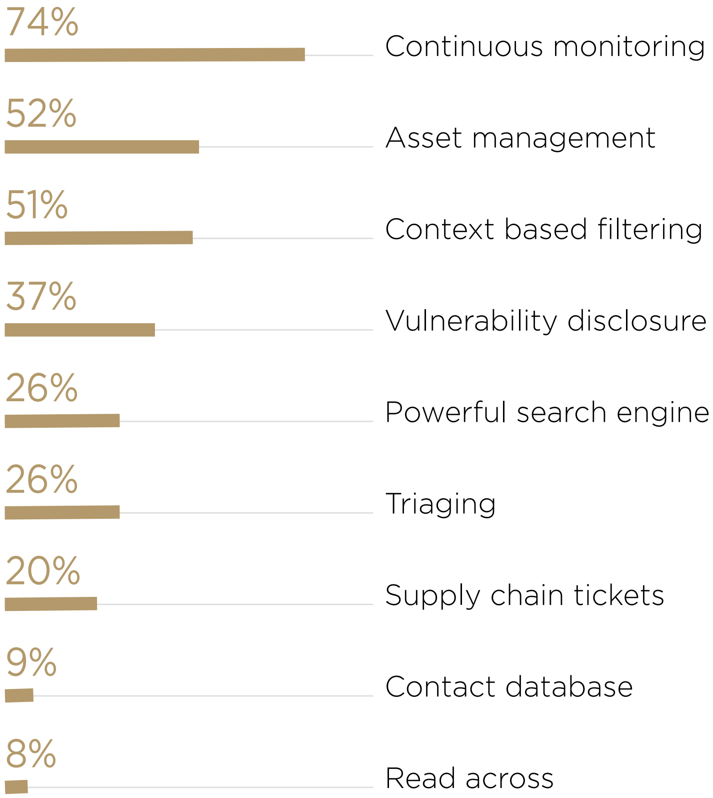
We have automated the entire process and we are read

A Detailed Look at the Numbers Behind this Report

On average, how long does it take your organization to do a risk assessment when a new vulnerability is published?



What are the top 3 most important features your vulnerability management solution should support?



A Detailed Look at the Numbers Behind this Report

What are the two biggest impediments to a timely risk assessment process?

43%
Manual investigations require time

42%
Lack of coordination between stakeholders and with suppliers

38%
Lack of trained security researchers

32%
Lack of data about vehicle/components programs

23%
There are too many components to cover

22%
Delays in notifications of new vulnerabilities

What are your threat intelligence sources of information?

45%
Internal

40%
MITRE NVD

35%
Auto to ISAC

29%
ASRG

17%
IBM X - to Force

8%
Chinese Vulnerability DB (CNNVD)

8%
Japanese Vulnerability notes (JVN)

2%
Flexera

2%
Research

2%
ThreatQ

A Detailed Look at the Numbers Behind this Report

What are your top 3 use cases for vulnerability management today?

63%
Compliance with industry standards and regulations

55%
Product security assessment

46%
Incident response

40%
Compliance with internal security policies

34%
keeping up to date with vulnerability landscape

34%
Threat intelligence

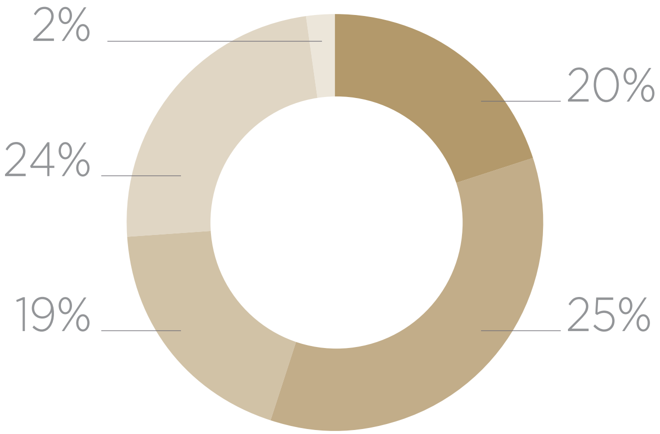
23%
VSoC

20%
Read across all components

17%
Governance to privacy

17%
licenses and cryptographic concerns

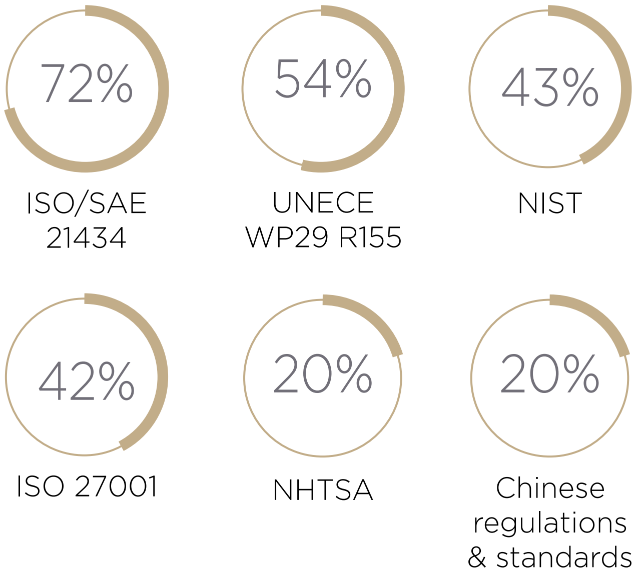
What does your vulnerability management program look like?



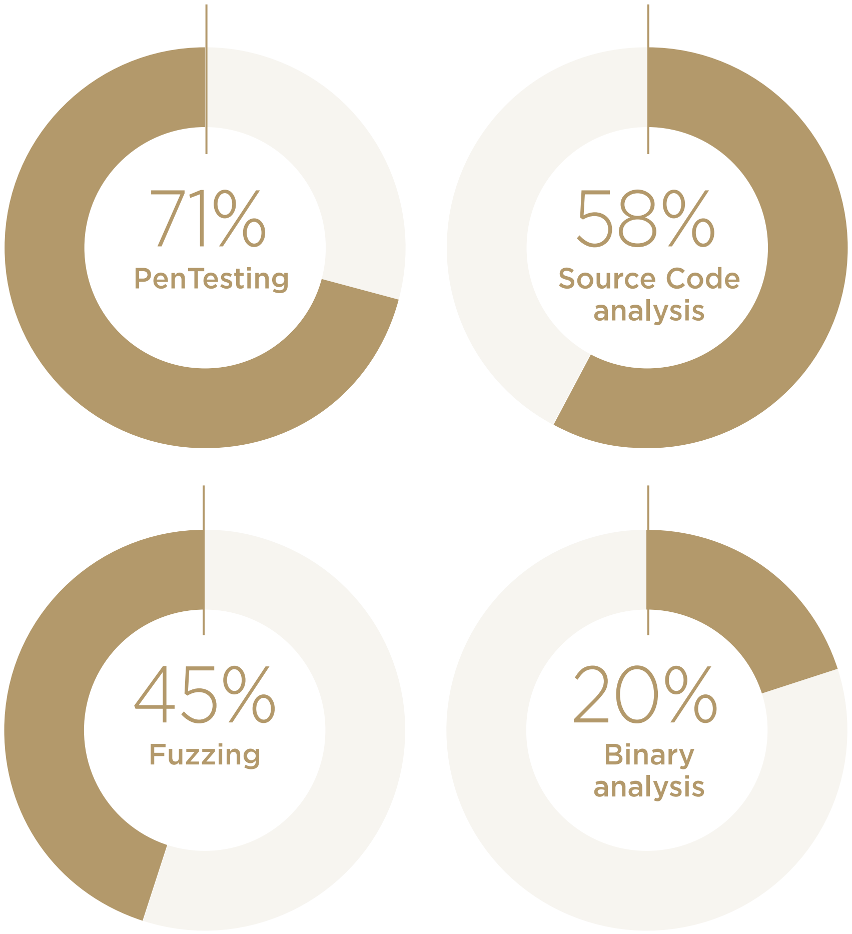
- ● **20%** A fully automated vulnerability management solution
- ● **25%** An internally developed operatio
- ● **19%** We plan to automate the manual processes in 2021
- ● **24%** A manually managed operation with which we are satisfied
- ● **2%** We still need to establish a vulnerability management progra

A Detailed Look at the Numbers Behind this Report

What industry standards and regulations are on your roadmap?



Which vulnerability scanning and management techniques do you use?



ASRG

www.asrg.io

CYBELLUM

www.cybellum.com