Automotive Cyber Maturity Report 2024

Dr. Teresina Herb, Michael Klinger, Dr. Robert Lambert, Dr. Moritz Minzlaff

Empowering Tomorrow's Automotive Software
www.etas.com

ETAS

Contents

Preface

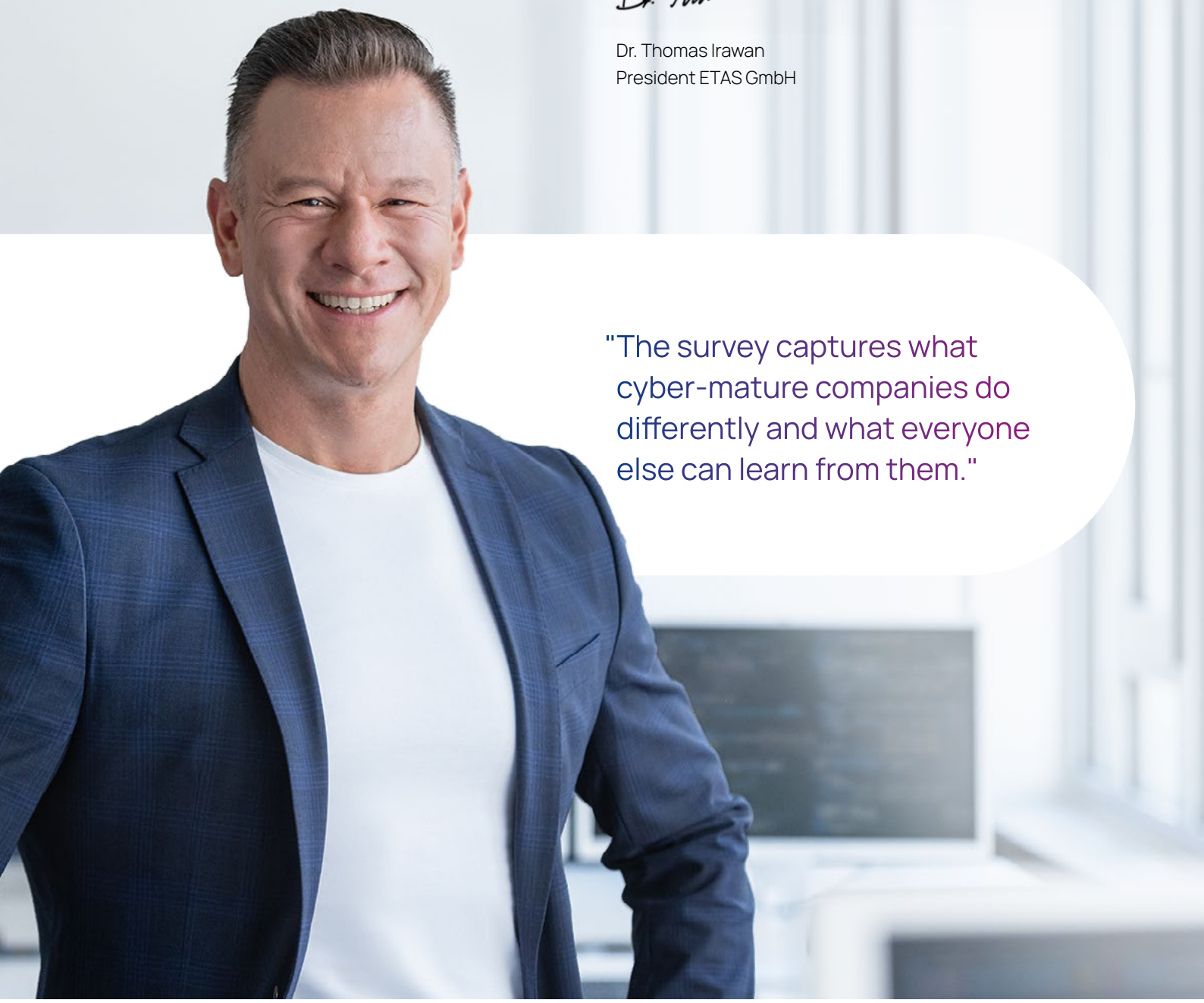
At the heart of the automotive industry's technological revolution lies a critical element: cybersecurity. As vehicles become more connected, they also become more exposed to cyber threats. I firmly believe automotive companies cannot successfully navigate the transformation on their own. They need to collaborate and share knowledge to ensure proper protection of road users and business models.

This is why I am very excited about our fourth annual Automotive Cyber Maturity Survey. It fosters an understanding among industry players of the main security challenges. With more participants from most major markets than ever before, the responses provide valuable insights. The survey captures what cyber-mature companies do differently and what everyone else can learn from them.

As the concept of software-defined vehicles has gained momentum, automotive companies need to adapt to the rapid iteration and development cycles typical of software development. This year's survey results show that advanced cybersecurity and high DevOps performance share a common core: collaboration, automation, and treating security as an indispensable software engineering concern. Indeed, the implementation of next-generation advanced driver-assistance systems and autonomous driving technologies demand agile development practices, continuous integration and delivery, and a culture of continuous improvement.

As you turn the pages of this report, you will gain insights into how a robust security framework can reach the next level of productivity.

Dr. Thomas Irawan
President ETAS GmbH



"The survey captures what cyber-mature companies do differently and what everyone else can learn from them."

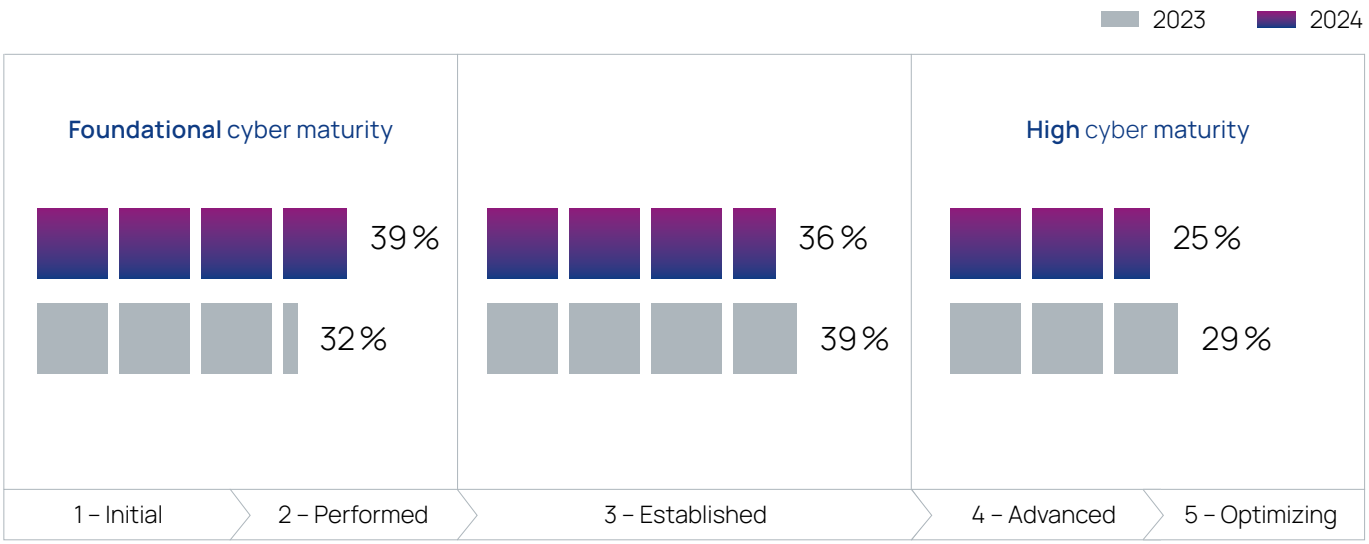
Executive summary

Insight #1: Cybersecurity drives competitiveness:
Survey data shows a strong correlation between a company's cyber maturity and its competitiveness in the automotive market. High cyber maturity is associated with a strong competitive edge, with over 90% of respondents from high-maturity organizations rating their competitiveness as "somewhat or very strong." Companies with high cyber maturity prioritize cybersecurity in their business operations, making major decisions based on cybersecurity considerations. They also believe that effective cybersecurity is essential for maintaining customer trust and loyalty, with collaboration across their teams involved in development, security, and Dev(Sec)Ops providing a competitive advantage. High-maturity organizations focus on future-proof security and risk reduction rather than low-cost solutions.

Insight #2: Cybersecurity has moved beyond peak hype:
The automotive sector has now reached a global level of cyber maturity, and the focus has shifted from reaching certification to living a cybersecurity culture, managing cybersecurity in the field, and anticipating future threats and trends. While self-reported cyber maturity has slightly dropped, this may in fact indicate progress as cybersecurity moves past peak hype. The share of automotive companies with a UN R 155 or ISO/SAE 21434 certification or incident response plans has increased to a majority, but testing this response and having backup and recovery plans has not. This year marks the first time since this survey started in 2021 that "concept & development" is not the biggest challenge. The gap between foundational and high-maturity companies is largest for threat detection and response and for employee awareness metrics. Security is now a people and mindset challenge, with competence and capacity remaining in focus.

Insight #3: Focus on security operations and ecosystem:
Automotive organizations are focusing on security monitoring and the software supply chain, with companies of higher cyber maturity ranking these as the biggest challenges, and more often implementing SIEMs and SOCs. Vulnerability management has taken center stage, with companies leveraging various sources for cybersecurity monitoring and adopting active measures to secure the ecosystem. There is a transition from document-based to integrated and automated measures in the software development workflow, aligning with the observations in Insight #1 that cybersecurity and strong Dev(Sec)Ops practices go hand in hand.

Insight #4: GenAI must receive appropriate attention:
The rise of generative AI (GenAI) in the automotive industry has led to both concern and great expectations. The survey shows a gap between the cybersecurity views of subject-matter experts (more pessimistic) and upper management (more optimistic, rising with job level). While the industry agrees that GenAI is crucial for innovations in automotive cybersecurity and competitiveness, there is also a concern that GenAI could introduce more vulnerabilities than solutions. Participants from China have the highest expectations but are highly aware of potential pitfalls. High maturity correlates with higher GenAI query response rates: these companies have gained more experience – good and bad – with generative AI, informing a keener understanding of cyber risks.



Context and design of this year's survey

The ETAS Automotive Cyber Maturity Survey has become a fixture that reflects the automotive industry's view on security topics. By asking for the opinions of automotive professionals whose daily work deals with aspects of security, the survey provides an insightful compendium of facts and figures revealing how organizations in the automotive domain master security and its challenges, and how they perceive their individual performance in this field.

The 2024 survey included 18 questions that were structured in the following groups:

1. Governance
2. Progress & challenges
3. Securing lifecycle and ecosystem

Participants' responses were collected anonymously within a timeframe of one month. All questions in the survey were either multiple choice (with the option to select one or multiple answers) or quantitative assessment of statements (agree, disagree, neutral; minor, moderate, major)

With the survey now already in its fourth year, there are core questions that repeat every year to identify industry trends, but also questions on new fields of interest. New topics this year include GenAI, DevOps, and linking security and business operations.

Whitepaper "Cybersecurity for the software-defined vehicle"

Automotive software is closely linked with automotive security. As the industry moves toward the so-called software-defined vehicle (SdV), it needs a strong understanding of cybersecurity. This whitepaper provides the industry with a compass and a map to successfully navigate the risks.

Building on our experience in helping automotive companies implement this new end-to-end security, we look to the software and tech industry for lessons learned, in particular the DevOps paradigm, and discuss automotive industry specifics. This allows us to define the new SdV-level cyber maturity that matches the increased cyber risk of the SdV. We conclude the whitepaper with an outlook on how automotive companies can achieve this SdV-level cyber maturity.

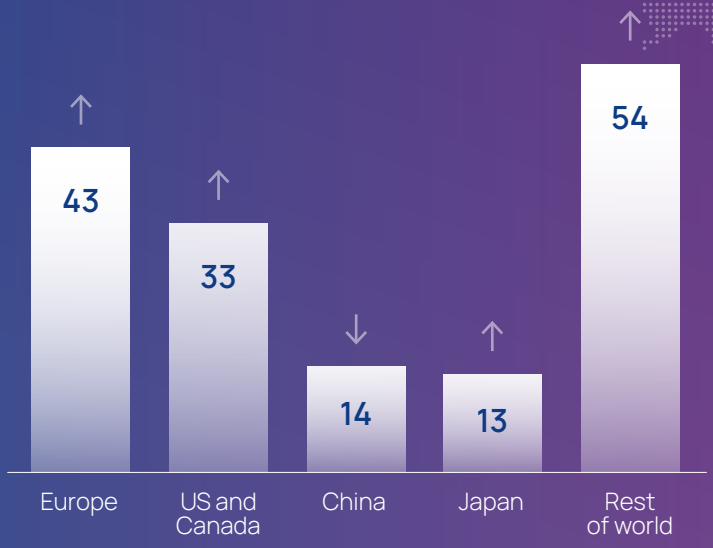
Download the Whitepaper

Survey statistics

Record participation from Europe, Japan, and the US

Regional participation

↑ increase or
↓ decrease compared to previous year

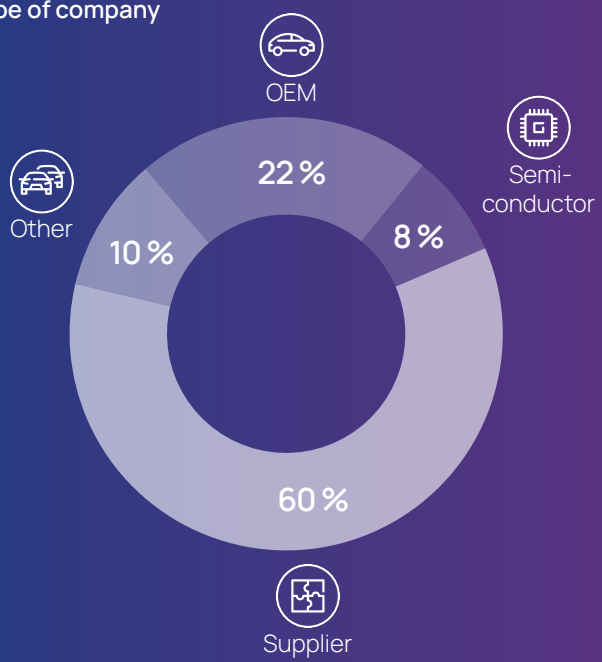


Participants from a record nineteen countries

Total number of participants: 157

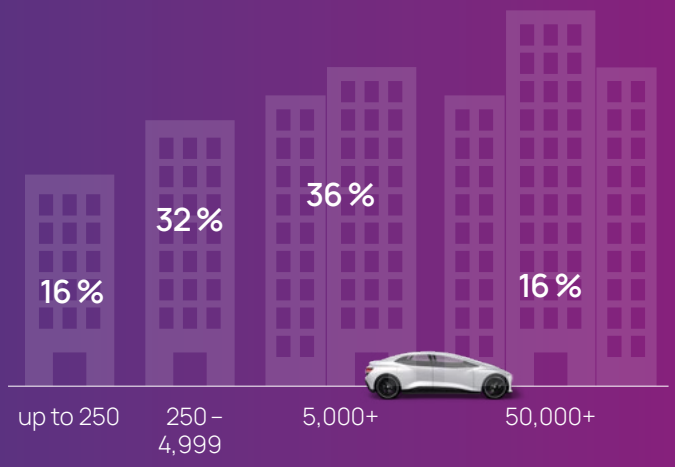
Job level

Type of company



Size of company

measured in number of employees

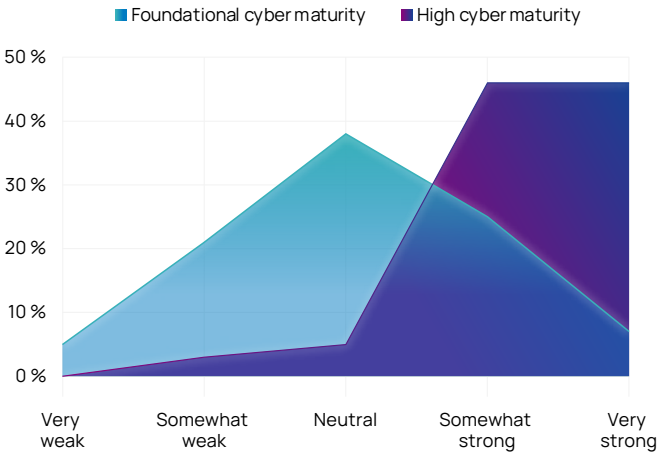


Key insights

Insight #1: Cybersecurity drives competitiveness

Security is often viewed as a cost factor and treated as a "fear" sell by vendors. Our survey data shows that this thinking is incomplete at best, but it is more likely to mean losing a competitive edge. In fact, high cyber maturity is a hallmark of automotive market leaders.

How would you rate your company's position in the market in comparison with its competitors?

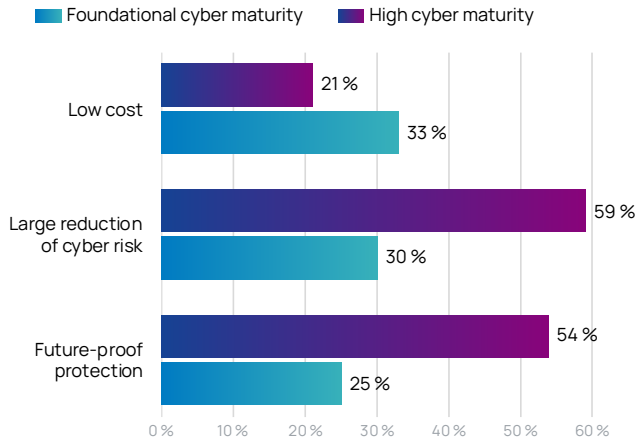


When asked about their companies' competitiveness, the participants' responses showed high correlation with their companies' cyber maturity. Over 90% of respondents from high-maturity organizations rated their competitiveness as "somewhat or very strong." The number of "very strong" responses is over 600% greater than for foundational maturity companies. Not a single participant from a highly cyber-mature organization considered their competitiveness "very weak" (see Question 3).

We can understand why when looking at the role of cybersecurity in business operations: at levels 4 and 5 of cyber maturity, major business decisions are significantly influenced by cybersecurity considerations, whereas less mature organizations do not emphasize this aspect. With high cyber maturity comes agreement that effective cybersecurity is essential for maintaining customer trust and loyalty, a key ingredient of competitiveness. This is further supported by the conviction that strong cybersecurity practices provide companies with a competitive advantage and that investments in cybersecurity are critical to sustain the business (see Question 5).

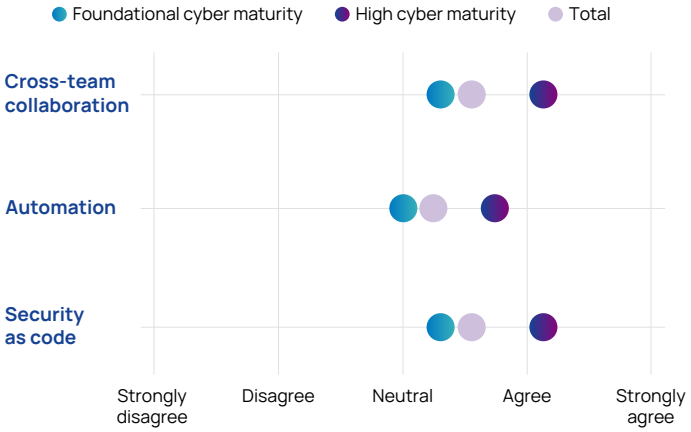
This results in drastic differences in the emphasis that participants put on technological security solutions. Participants from cyber-mature companies look to maintain their competitiveness with future-proof solutions (29 percentage points more than lower maturity organizations) and through a significant reduction of risk (also +29 percentage points) as opposed to the low cost of the solution (-12 percentage points) (see Question 12).

What are you most looking for in technical security solutions? The two answers have the largest increase from foundational to high maturity.



The survey shows that cyber-mature companies can also be expected to demonstrate high Dev(Sec)Ops performance. Indeed, high-maturity companies build and maintain their competitive edge by collaborating across their teams involved in development, security, and operations of products. They are much more likely to incorporate automation throughout their development processes, building their competitive advantage by ensuring that security measures are applied consistently and effectively. Finally, cyber-mature organizations treat security as a software engineering concern, and incorporate security controls and checks into their software development processes. This allows them to produce software with improved and consistent levels of security, improving their competitiveness (see Question 13).

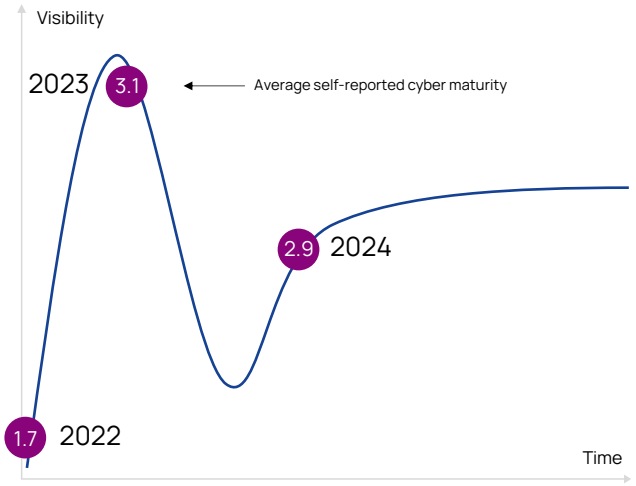
How would you describe your company's status with respect to adoption of DevSecOps practices? Rate your level of agreement with the following statements […]



Other segmentations of the data such as company size do not produce correlations with competitiveness that are as clear as those with cyber maturity. At first glance, the responses from participants in Japan seem to show a negative correlation with competitiveness; however, this can be explained by the lower rating of cyber maturity in this segment.

Insight #2: Cybersecurity has moved beyond peak hype

The automotive sector has reached a global level of cyber maturity and now faces the crucial challenge of taking cybersecurity to the next level of productivity (see also Insight #1). This year's survey happened when many new vehicles platforms have passed – or soon will pass – start of production. This means the focus of organizations regarding cybersecurity must shift from reaching certification to living a cybersecurity culture, managing cybersecurity in the field, and anticipating future threats and trends.

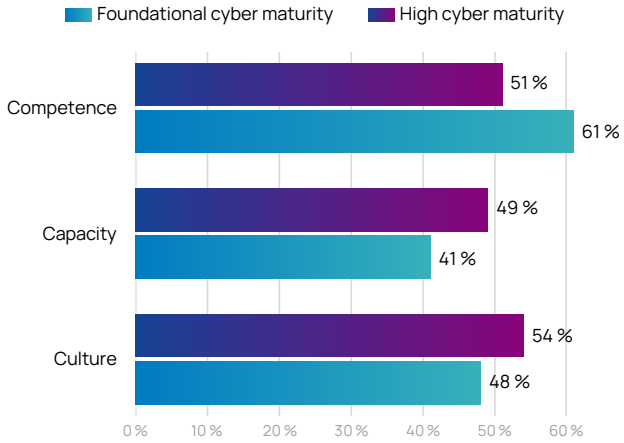


Average self-reported cyber maturity has dropped slightly from 3.0 in 2023 to 2.8 in 2024 (see Question 2). To us, this indicates progress, as cybersecurity seems to have moved past peak hype (see Figure above). Indeed, the share of automotive companies with a UN R 155 or ISO/SAE 21434 certification has increased from 44% last year to 55% this year (see Question 4). While the same amount says that they have detailed incident response plans, this drops to 47% for backup and recovery plans and to 40% for regularly testing and evaluating plans. These numbers indicate that turning a certified cybersecurity management system into an everyday part of business operations remains an open issue (see Question 17).

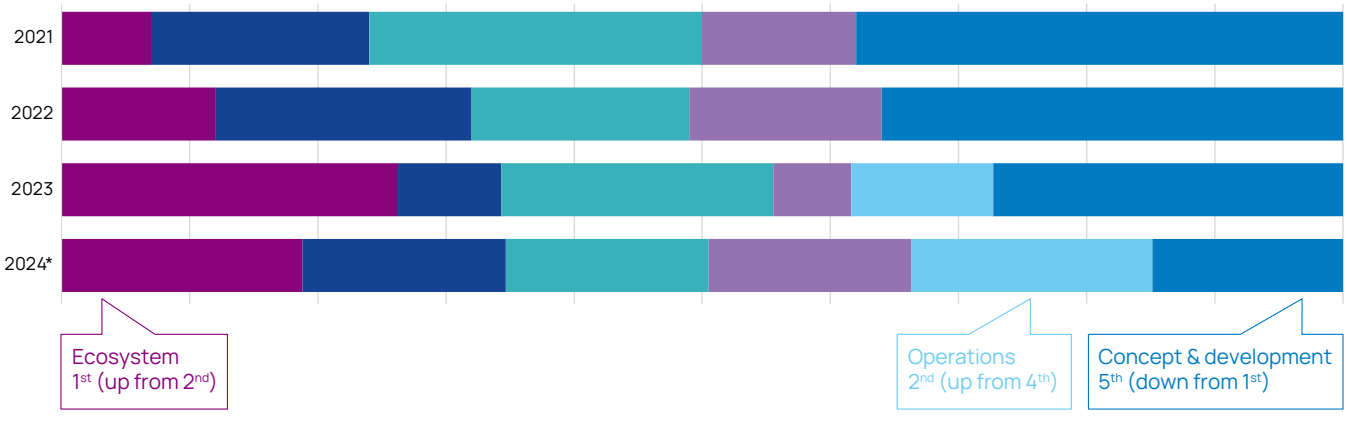
The metrics used to measure cybersecurity reflect the shift: the biggest gaps between foundational and high-maturity companies are in threat detection and response and employee awareness metrics. These are up 88% and 80%, respectively. Vulnerability management metrics saw the biggest jump overall, from roughly one-third of participants selecting this metric to about half (see Question 6).

This year marks the first time since the survey started in 2021 that concept & development is not the domain with the biggest challenges. In fact, it dropped to last place. The areas of focus are now securing the ecosystem in first place followed by security operations (see Question 9). Takeaway #3 from last year, that security is a people and mindset challenge, is gaining traction: as every year, the two biggest challenges in the respondents' areas of responsibility are competence and capacity. Cybersecurity culture is now in third place. It even tops the answers for high-maturity organizations, passenger vehicle OEMs, and semiconductors. Culture is the second most selected challenge in China, Europe, and North America. In contrast, process maturity drops to fourth place overall and sixth place among high-maturity organizations. No participant from quality departments selected process maturity as the biggest challenge. Interestingly, management awareness and commitment dropped to 0% from 23% in 2023 (see Question 10).

Specifically for your area of responsibility, what are the biggest cybersecurity challenges?



To what extent do the following domains present cybersecurity challenges for your company?



* Due to a change in methodology, the percentages from 2024 do not compare to the previous years.

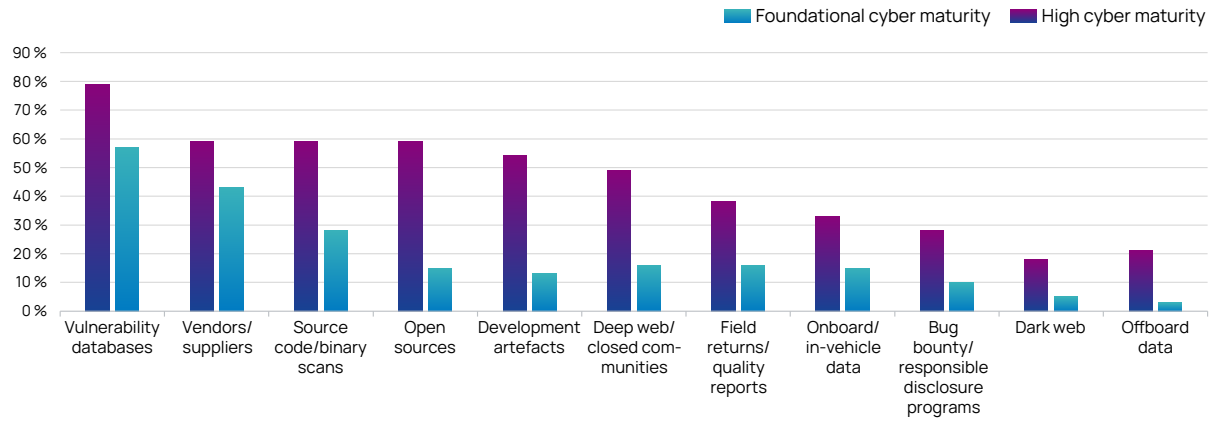
Insight #3: Focus on security operations and ecosystem

In the previous insight, we mentioned that the ecosystem and security are in focus at many automotive organizations. In fact, the largest difference between companies at the maturity levels of 1 or 2 and those at levels 4 or 5 is that they rank security monitoring and the software supply chain (both +9 percentage points) among the biggest challenges (see Question 10). Even across different maturity levels, the supply chain now comes in third (at 44%) among the most concerning attack vectors. This rises to second place (49%) for OEMs. Vehicle OS as an attack vector saw the biggest increase overall of 8.55 percentage points, but still marks a distinguishing element between foundational and high-maturity organizations. Companies with higher cyber maturity and participants from IT departments are especially concerned about this attack vector (see Question 14). This is likely to be due to the fact that many challenges in security need to be solved along the supply chain and during operations in order for the vehicle OS to solve them at all.

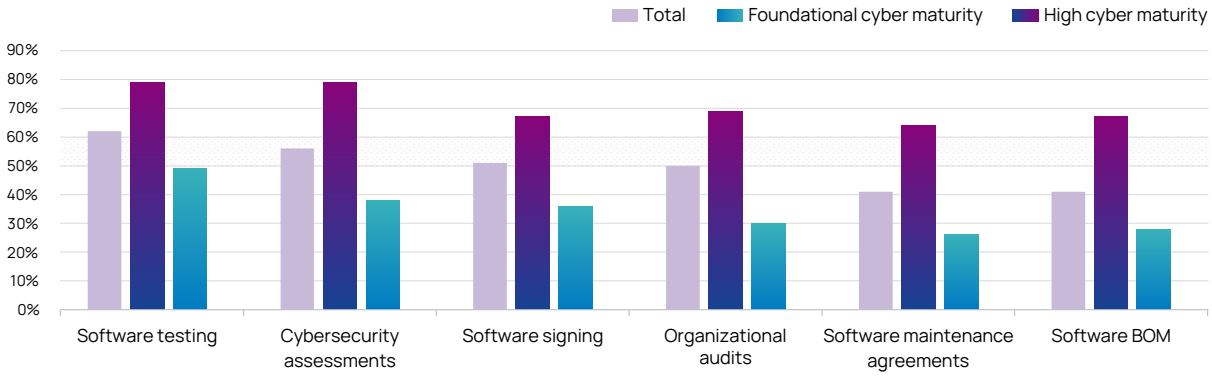
Turning from threats to monitoring and measures, vulnerability management has taken center stage: vulnerability databases and information from vendors and suppliers are the most frequently used sources for cybersecurity monitoring. This is true overall and for the segments of OEMs, suppliers, foundational, and high-maturity organizations. However, every single monitoring source is leveraged more often by companies at cyber maturity levels 4 and 5 than at levels 1 and 2. The biggest differences between those levels are found in how often they leverage open sources (+44 percentage points), development artefacts (+41 percentage points), and the deep web and closed communities, such as hacker forums (+32 percentage points). The first two options provide a clear and relatively easy path for foundational maturity organizations to close the gap (see Question 16).

A distinguishing mark between foundational and high-maturity companies is that the latter adopt measures more often across the board and emphasize active measures. While (passive) monitoring is the second most frequent measure taken to secure the ecosystem, behind key management systems for both segments, the largest difference lies in implementations of SIEMs (+44 percentage points) and SOCs (+36 percentage points). All measures offered in the survey to secure the supply chain were chosen by more than 60% of organizations with cyber maturity levels 4 or 5 while all come in below 50% for levels 1 or 2. We're observing a transition away from document-based measures and toward integrating and automating them into the software development workflow. More than half of all participants selected cybersecurity assessments, software signing (+12 percentage points), and software testing (+19 percentage points) this year, whereas last year, the only measure above 50% was assessments (see Question 18). This corresponds well with the observations in Insight #1 that cybersecurity and strong DevOps practices go hand in hand.

Which sources does your company use for monitoring cybersecurity?



What measures does your company take to secure its software supply chain?



Insight #4: GenAI must receive appropriate attention

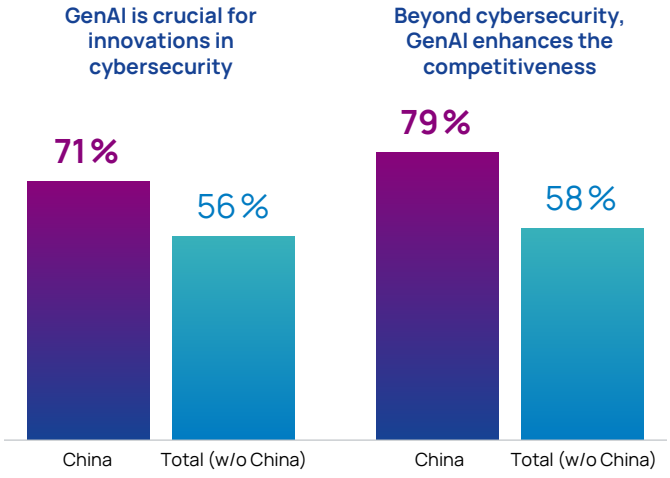
The rise of generative AI (GenAI) is leading to both concern and great expectations in the automotive industry. We see this as a sign of substantial uncertainty regarding the technology. We recommend that managers give GenAI and its introduction appropriate attention to reap the benefits while mitigating the risks. Among all participants, the ones from China seem to have the highest expectations and at the same time seem to be highly aware of potential pitfalls. The results also show a gap between the views of upper management and subject-matter experts.

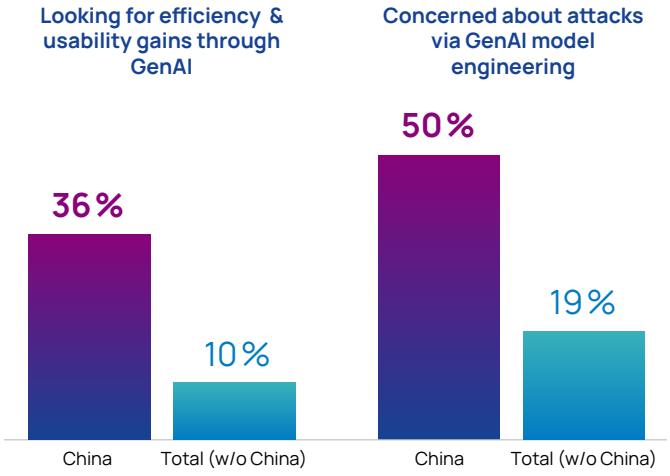
Overall, the industry tends to agree that GenAI is crucial for innovations in automotive cybersecurity and that it enhances competitiveness even beyond cybersecurity (see Question 11). This view is most pronounced in China and Japan. Consequently, participants from China also look for efficiency and usability gains through GenAI more often than those from other regions: 36% of respondents versus 15% from the next region most inclined to do so (see Question 12).

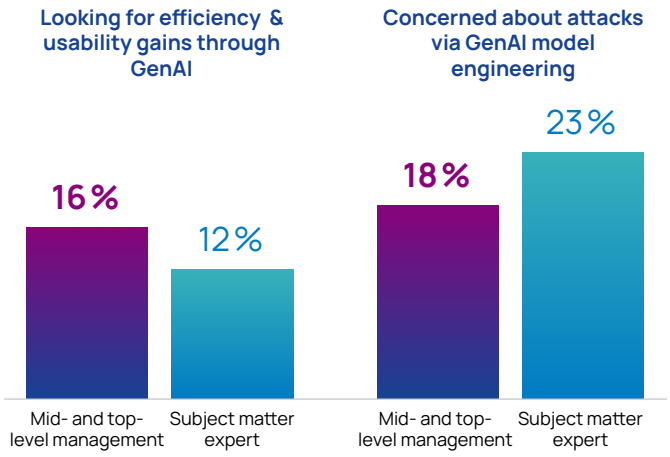
At the same time, participants on average also tend to agree that GenAI introduces more vulnerabilities than solutions (see Question 11). A total of 22% selected GenAI model engineering as one of the most concerning attack vectors. This number rises to 50% for respondents from China (see Question 14).

The higher a participant's job level, the smaller the difference in their mix of skepticism and optimism toward GenAI. Across all questions, the more positive view wins out. Mid- and top-level management are 33% more likely than subject-matter experts to look for efficiency and usability gains through GenAI, and they are 24% less likely to consider GenAI a most concerning attack vector.

Questions about GenAI as an attack vector are also the one place where the organization's maturity signals a significant change in participants' answer behavior: high maturity correlates with higher response rates. As we discussed in the previous takeaways, high cyber maturity is often correlated with an organization that is also more advanced in many other dimensions. The same factor seems to be at play here: high-maturity companies can be expected to have gained more experience – good and bad – with generative AI, and so would have a keener understanding of its cyber risks.





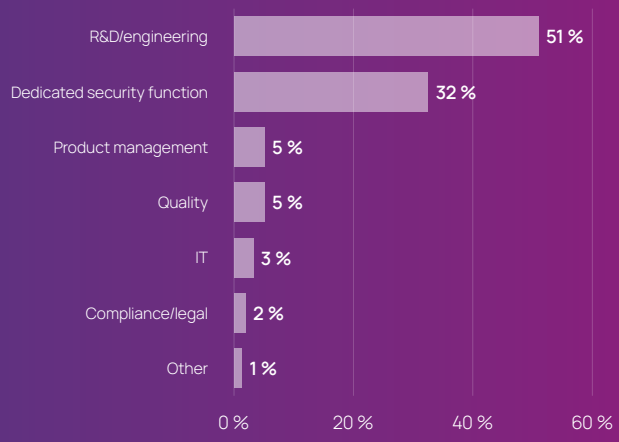


Survey results in detail

Section 1: Governance

1. Which function or department is primarily responsible for leading product-security efforts within your company? (single answer)

In foundational-maturity organizations, R&D/engineering leads security efforts twice as often as does a dedicated security team. In highly mature ones, security efforts are led by a dedicated security function.

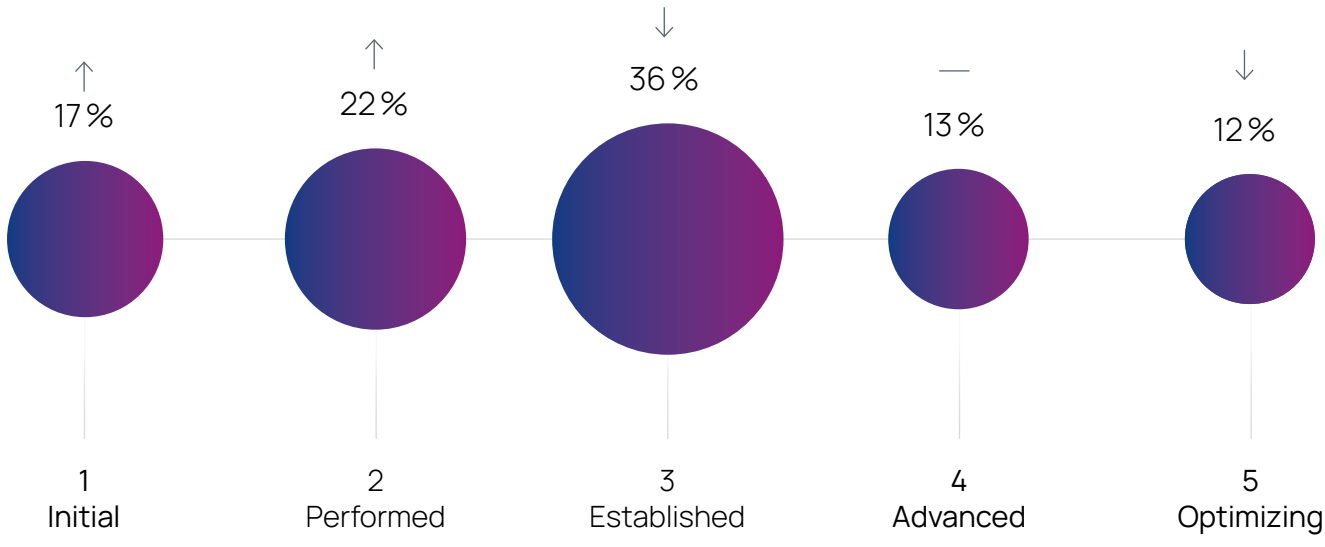


2. Overall, how would you rate the cyber maturity of your company?

(single answer)

After improvements from 2022 through 2023, cyber maturity has leveled off and has somewhat declined at the highest maturity level.

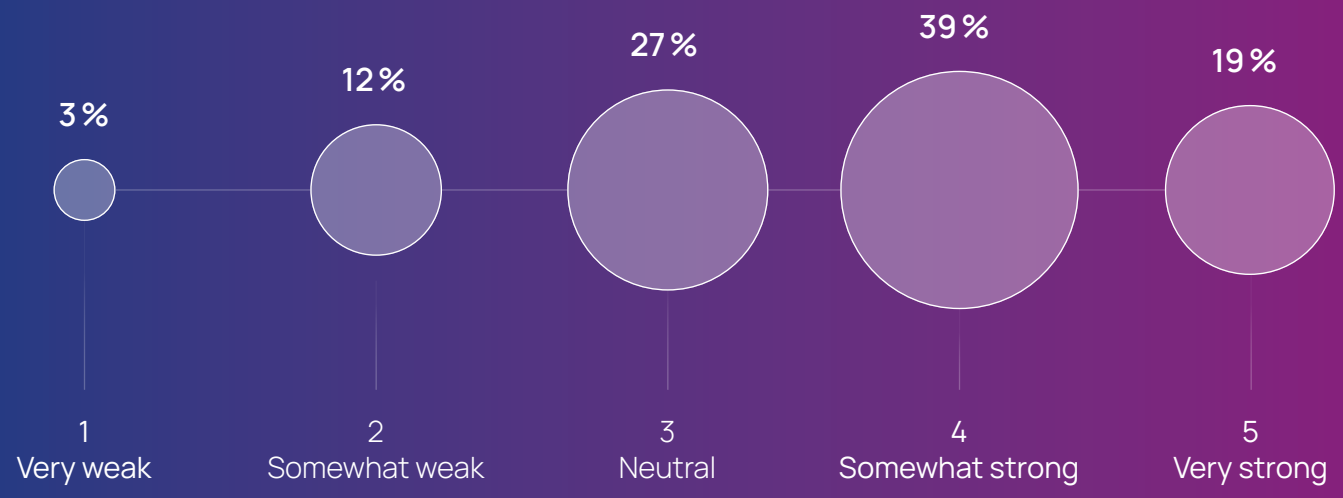
The "established" rating is now the most prevalent among subject-matter experts and management. That can be explained by a better understanding of the real work required. IT is less optimistic regarding cybersecurity than is R&D.



↑ increase or
↓ decrease compared to previous year

3. How would you rate your company's position in the market in comparison with its competitors?

In general, each company believes its position to be above average. Indeed, perhaps we can expect that those responding to this survey are likely to be above average already.

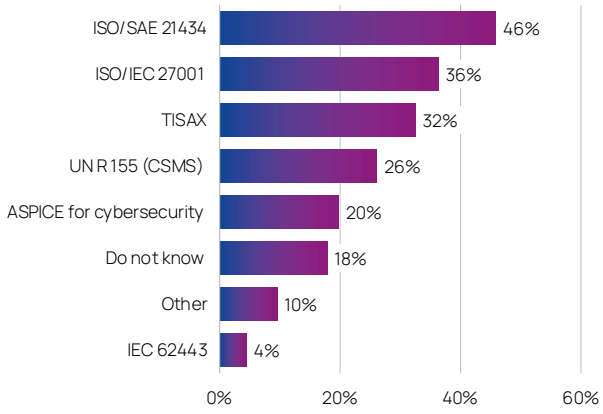


4. Which security certifications does your company have?

(multiple answers)

Not knowing which security certifications have been obtained correlates with low maturity.

- ISO/SAE 21434, ISO/IEC 27001, and TISAX are the most popular certifications.
- In comparison with the previous year, only ISO 21434 and R155 increased their share, while other certifications remained relatively static.



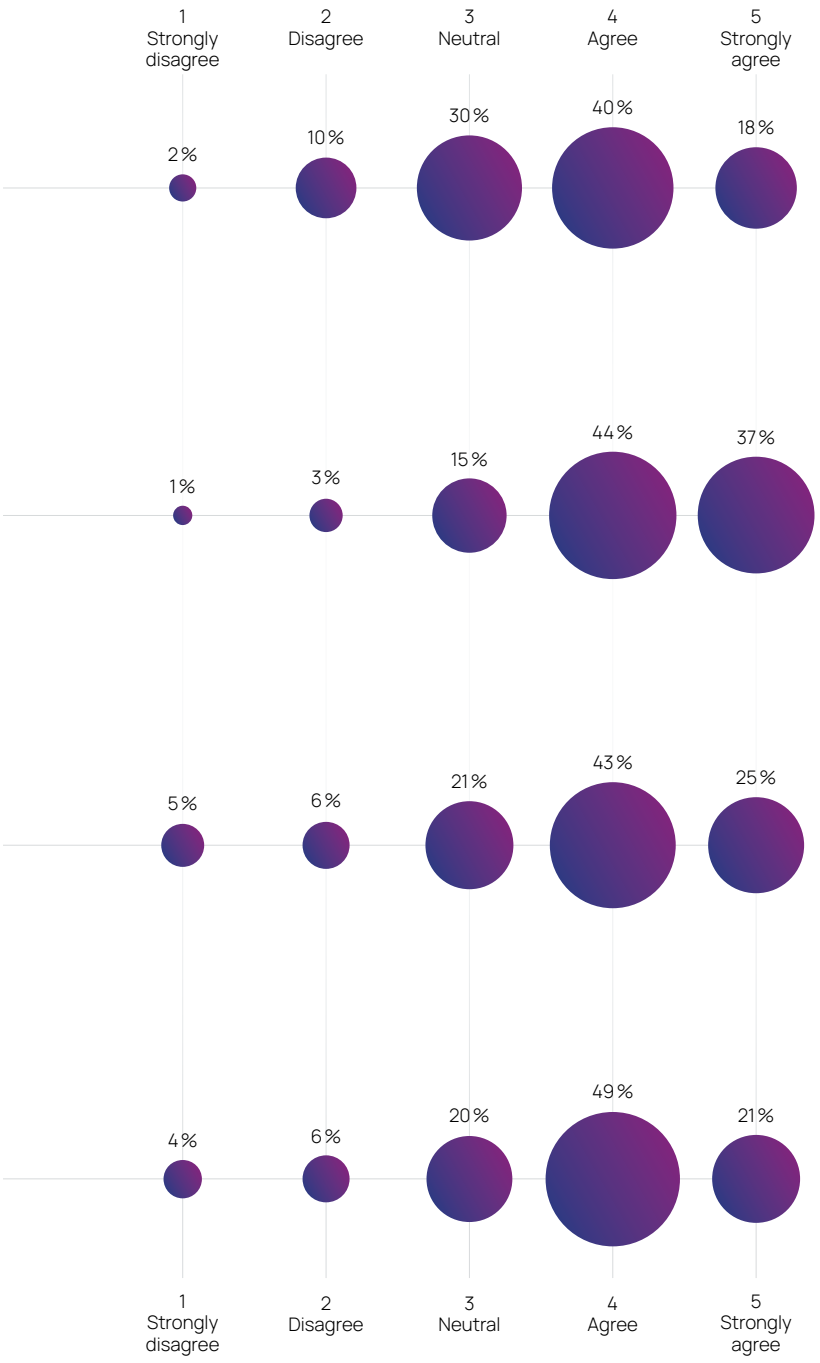
5. What is the role of cybersecurity in the context of your company's business operations? Rate your level of agreement with the following statements (single answer)

Influence on business decisions: Cybersecurity considerations significantly influence our major business decisions.
Cybersecurity's significance for business is highly correlated to maturity. Subject-matter experts agree less with this statement than do managers.
.

Impact on customer trust: Effective cybersecurity is essential for maintaining customer trust and loyalty.
Impact on customer trust is highly correlated to higher-maturity respondents. Subject-matter experts and management are in strong agreement with this statement.

Contribution to competitive advantage: Strong cybersecurity practices provide us with a competitive advantage in our industry.
Impact on competitive advantage correlated to higher-maturity respondents. First-line managers are more neutral on this statement.

Financial implications: Investments in cybersecurity are critical for the financial well-being and sustainability of the business.
Some of the least mature companies believe that cybersecurity has no financial impact on the business, while most mature companies agree or fully agree that it does. It is interesting to note that the „strongly disagree" responses come from "subject matter expert" respondents.



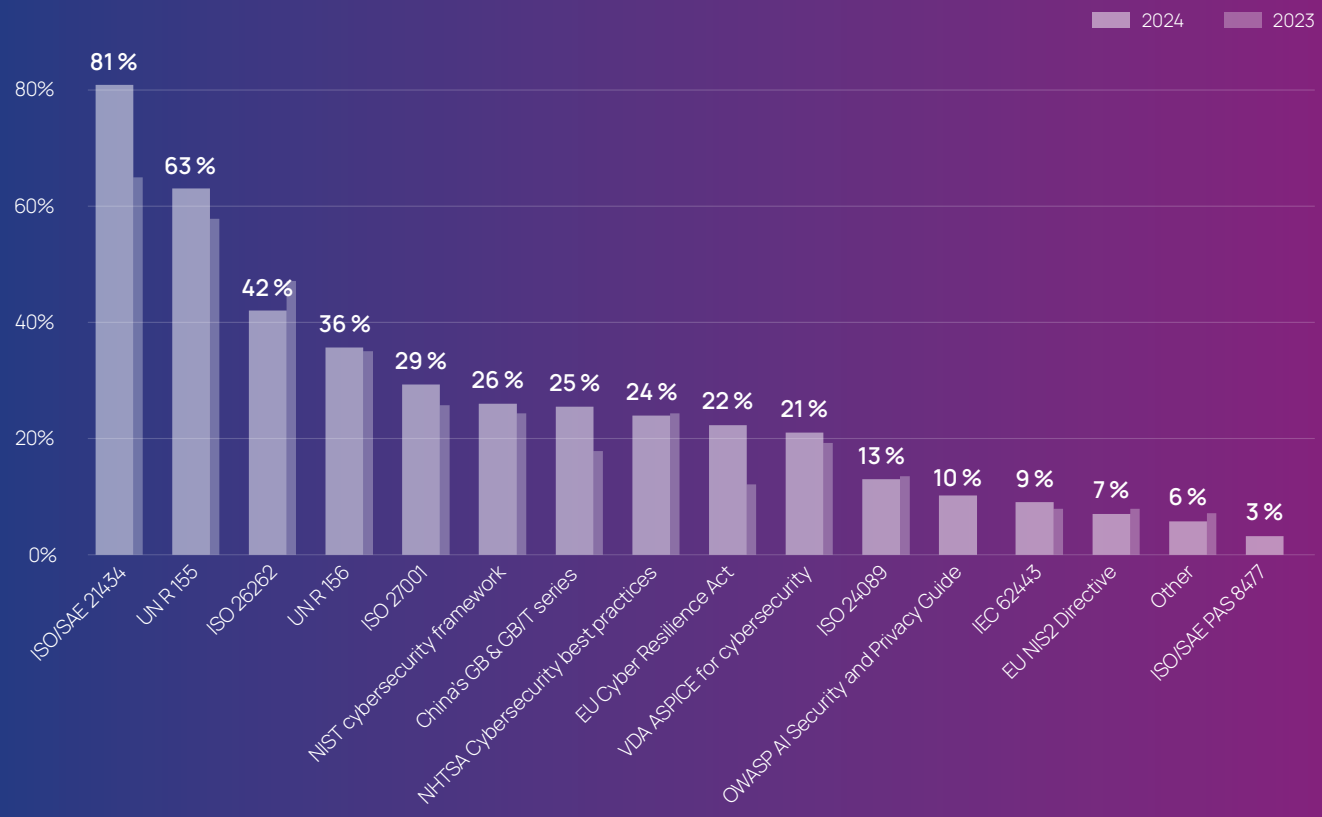
6. Which of the following metrics are used in your area of responsibility to measure cybersecurity? (multiple answers)

The highest-maturity respondents are those most likely to employ more cybersecurity metrics.

7. Which frameworks do you consider for cybersecurity in your area of responsibility? (multiple answers)

The highest maturity companies are likely to employ ISO 26262, R155, ISO/SAE 21434, ISO/IEC 27001, IEC 62443, China's GB & GB/T, EU Cyber Resilience Act, and EU NIS2 Directive. They are not likely to employ somewhat more general frameworks: UN R 156, VDA ASPICE for cybersecurity, NIST cybersecurity framework, NHTSA Cybersecurity best practices, ISO 24089, OWASP AI Security and Privacy Guide, and ISO/SAE PAS 8477.

The core frameworks remained the same as the previous year but with different proportions.

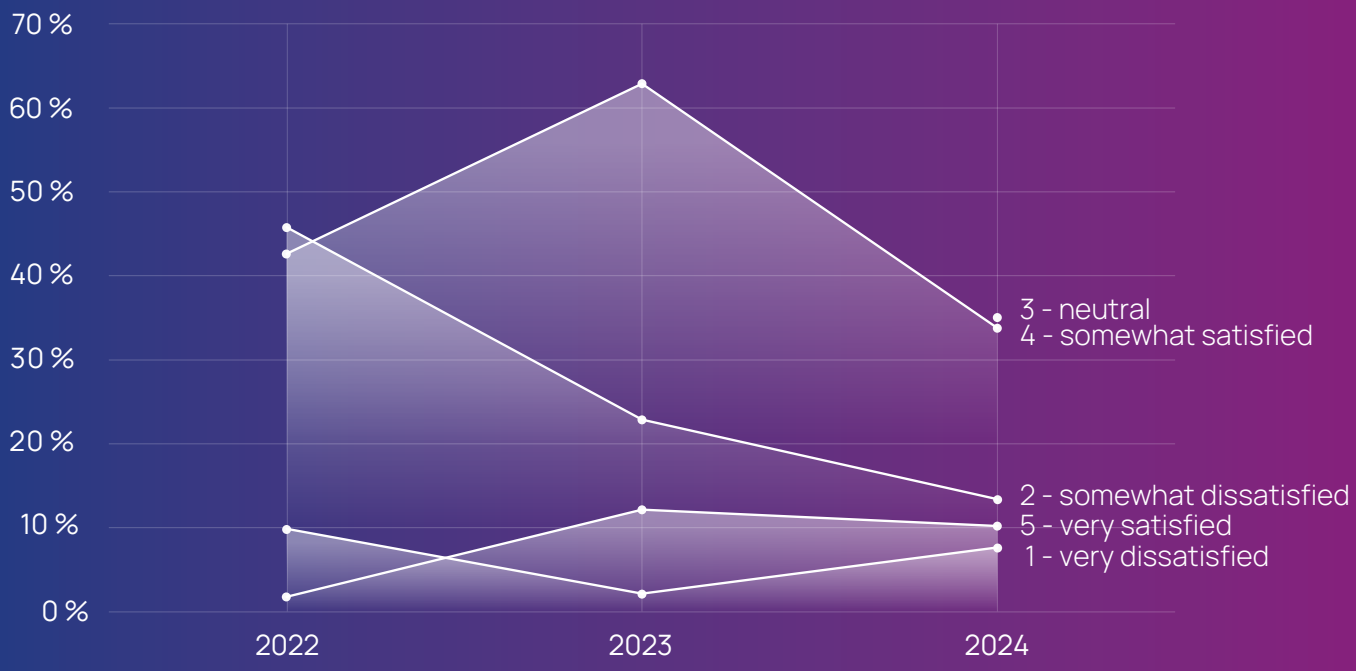


Section 2: Progress & challenges

8. How satisfied are you with the progress regarding cybersecurity in your area of responsibility since last year? (single answer)

Satisfaction correlates directly with maturity, with only the most mature respondents describing themselves as very satisfied.

After a very optimistic view in 2023, the maturity acquired through implementing cybersecurity processes has highlighted all the activities still to be done. This year, this is reflected in a more realistic view of the current progress in implementation.



9. To what extent do the following domains present cybersecurity challenges for your company? (single answer)

Concept & development
Lowest-maturity respondents tend to see fewer security challenges, while middle maturity respondents see significant and severe challenges. Only at the highest maturity does this difference even out. Concept & development challenges are moderate for subject-matter experts and management.

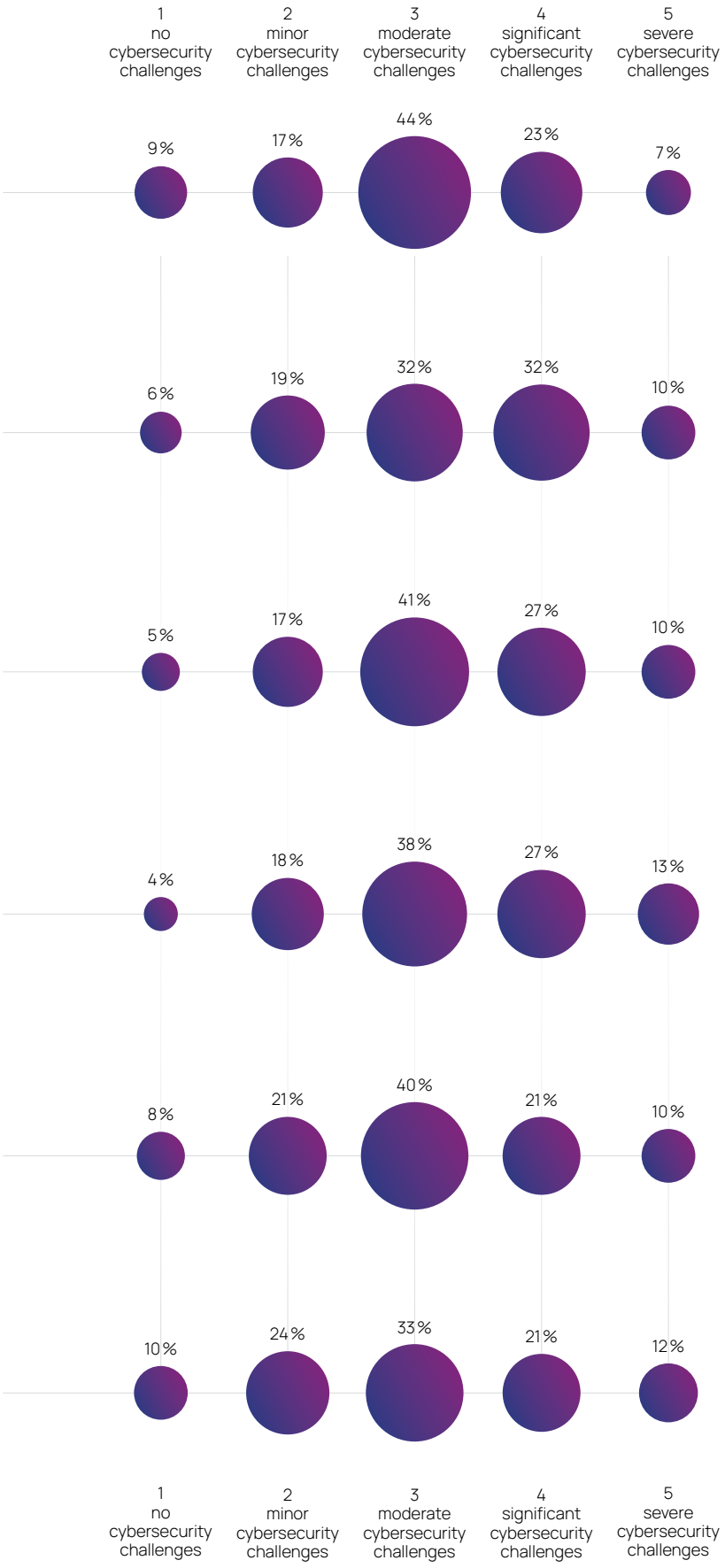
Ecosystem incl. supply chain
Ecosystem challenges are not well correlated with maturity. Ecosystem and supply chain challenges are moderate to significant for subject-matter experts and management.

Risk management
Risk management challenges are not well correlated with maturity. This issue is a concern for management and subject-matter experts.

Operations incl. maintenance and updates
Operational challenges do not become easier with increased maturity. Operations is a moderate issue for management but is significant or severe for subject-matter experts.

Governance incl. audits
Governance challenges are significant in the beginning and do not get easier with increased maturity. Governance is a moderate issue for management but a significant one for subject-matter experts.

Production
With increased maturity, production security challenges diminish. These challenges are moderate to significant for subject-matter experts and management.



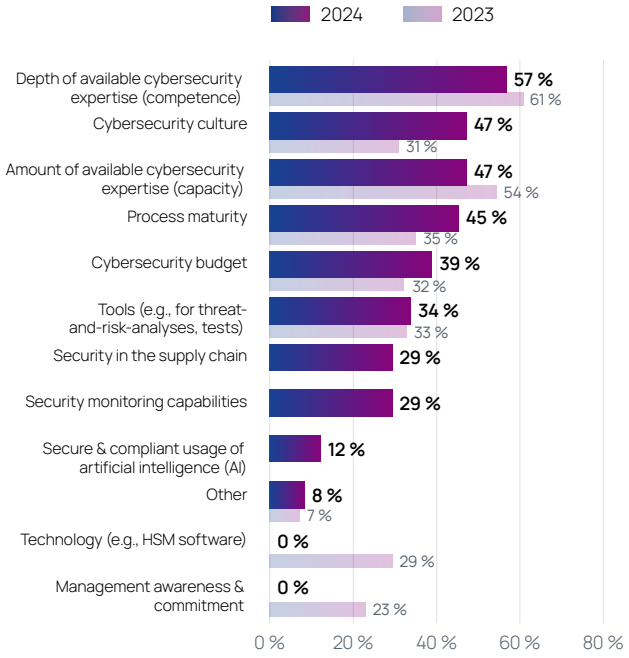
10. Specifically for your area of responsibility, what are the biggest cybersecurity challenges?

(multiple answers)

Less mature organizations are challenged by:
- Process maturity
- Cybersecurity budget
- Tools
- Security monitoring capabilities

More mature organizations struggle with:
- Cybersecurity culture
- Amount of available cybersecurity expertise (capacity)
- Security in the supply chain
- Depth of available cybersecurity expertise (competence)

Management awareness and commitment as well as technology were not cited as matters of concern.

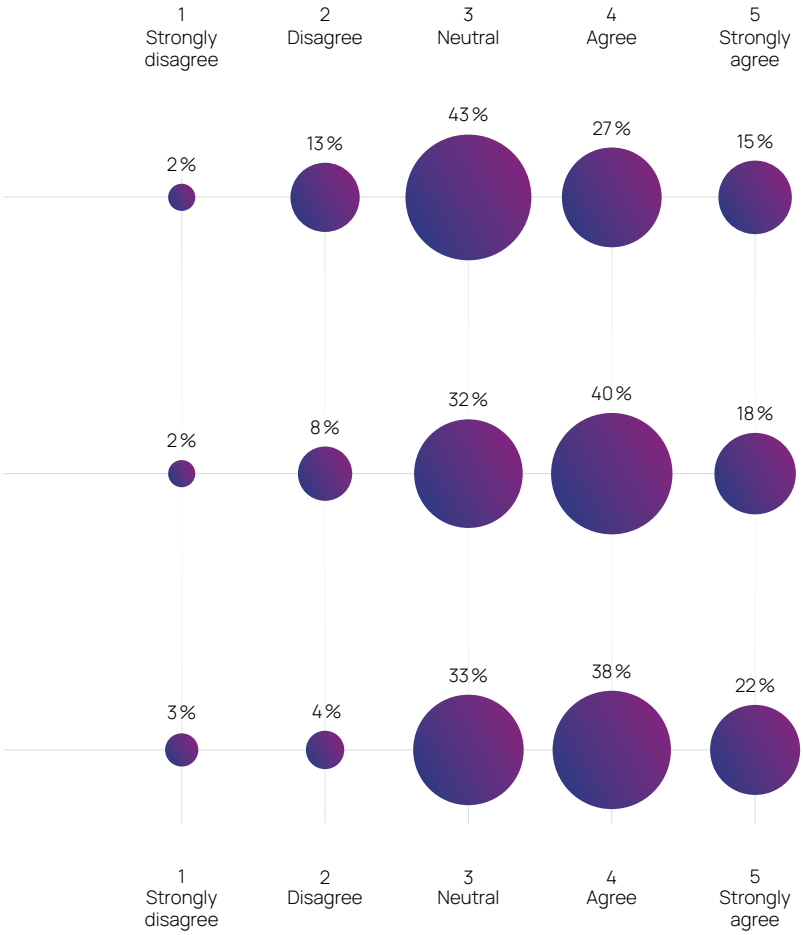


11. How would you assess the influence of Generative AI (GenAI) on automotive security? Rate your level of agreement with the following statements (single answer)

GenAI introduces more vulnerabilities than solutions in automotive cybersecurity.
Greater maturity correlates with disagreement with this statement. Subject-matter experts and first-line management agree with this statement more than higher-level managers do.

GenAI is crucial for future innovations in automotive cybersecurity.
Maturity correlates with agreement, except for some highly mature respondents who disagree.

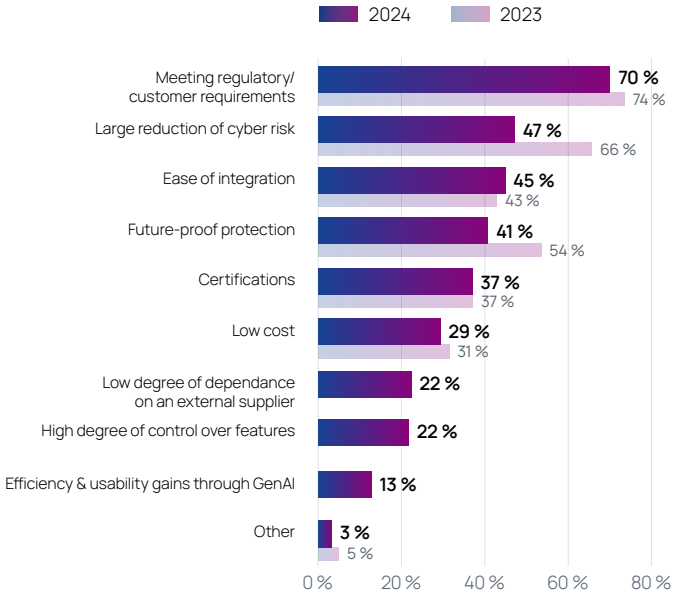
Beyond cybersecurity, GenAI enhances the competitiveness of companies in the automotive market.
Companies at the lowest maturity levels have no clear opinion how GenAI will impact automotive security, whereas other levels anticipate an improvement. All job levels agree on this statement. Japan and China think that the impact will be more profound than the other regions do.



12. What are you looking for most in technical security solutions? (multiple answers)

Less mature organizations:
- Low cost

More mature organizations (in decreasing order):
- Meeting regulatory/customer requirements
- Large reduction of cyber risks
- Future-proof protection, e.g., adaptability to future threats, crypto agility
- High degree of control over features

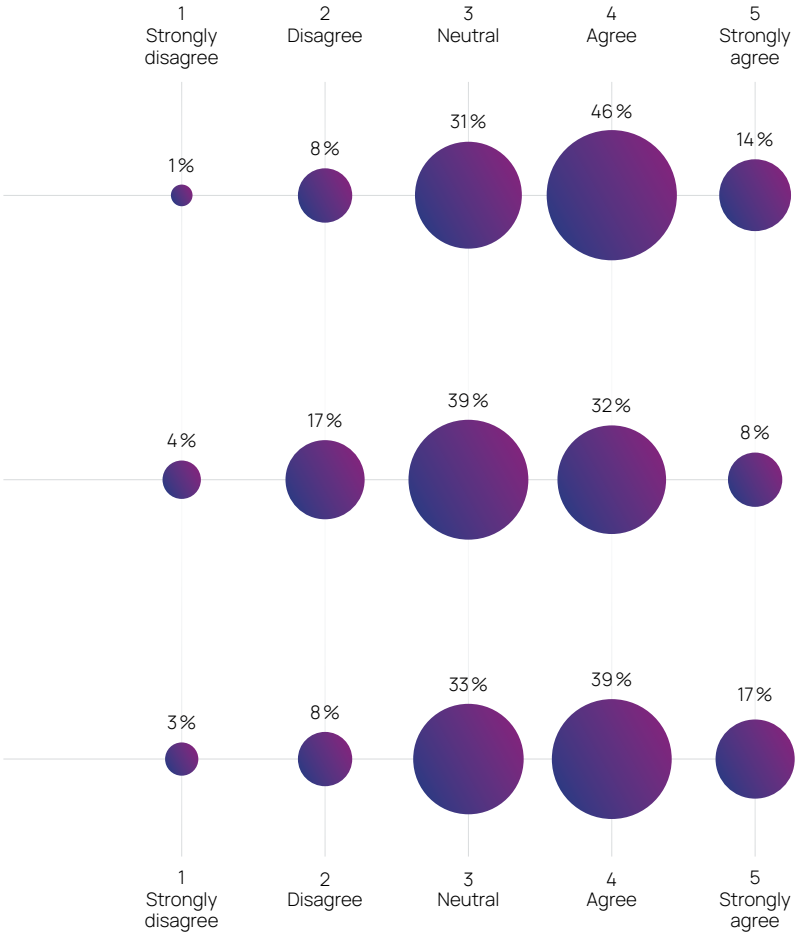


13. How would you describe your company's status with respect to adoption of DevSecOps practices? Rate your level of agreement with the following statements (single answer)

Collaboration: Our company emphasizes collaboration across all teams involved in the development, security, and operations of products.
DevSecOps collaborative deployment across teams correlates strongly with maturity.

Automation: Our company incorporates automation throughout the development process to ensure consistent security measures are applied and to increase overall efficiency.
DevSecOps being deployed throughout the development process correlates strongly with maturity. Higher-level management is more optimistic regarding this deployment than are first-line managers and subject-matter experts.

Security as code: Our company treats security as a software engineering concern and incorporates security controls and checks into our application code as part of our software development process.
DevSecOps treating security as a software engineering concern correlates strongly with maturity.

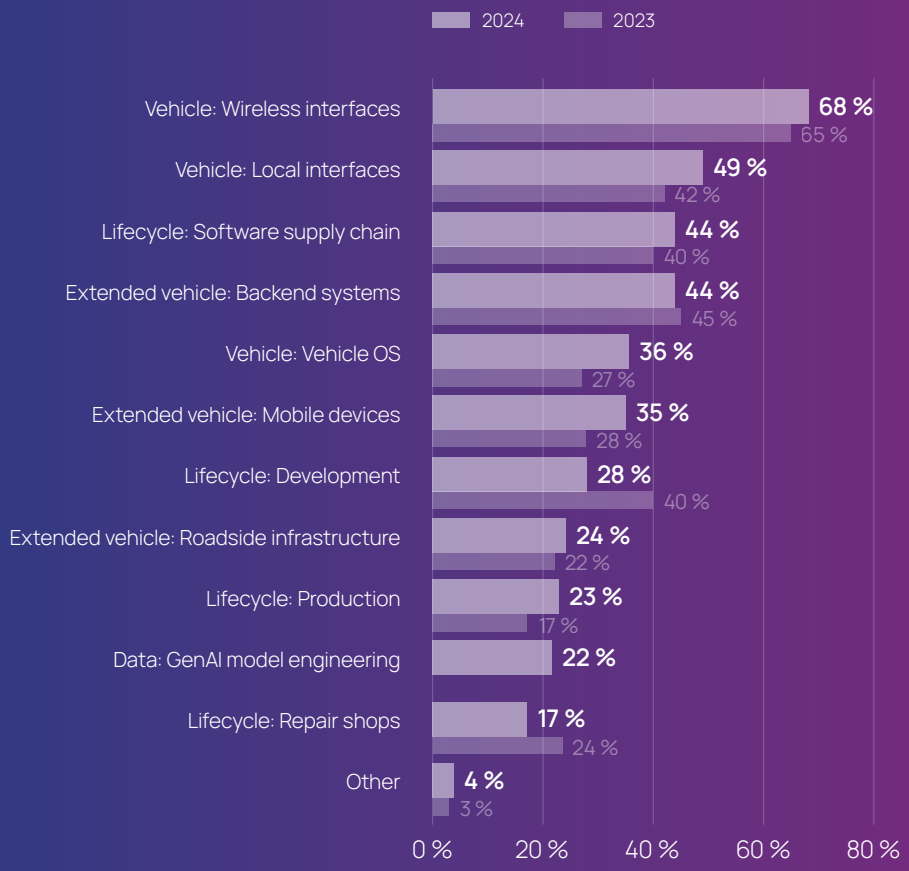


Section 3: Securing lifecycle and ecosystem

14. What attack vectors on vehicles are you most concerned about?

(multiple answers)

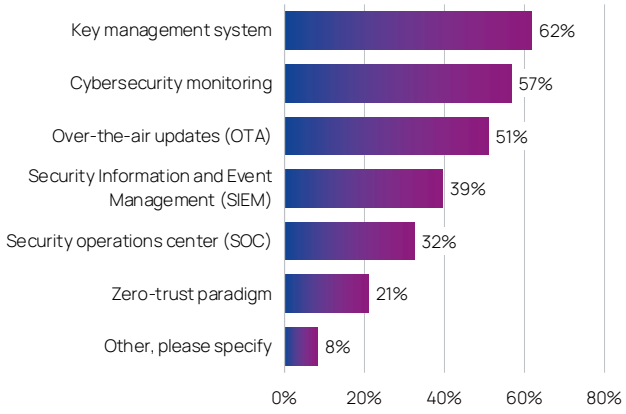
Concern about wireless, local, and mobile device interfaces has risen, as has concern about the software supply chain and production. Subject-matter experts are more concerned about the security of vehicle OS than management is.



15. What measures does your company take to secure its product's ecosystem?

(multiple answers)

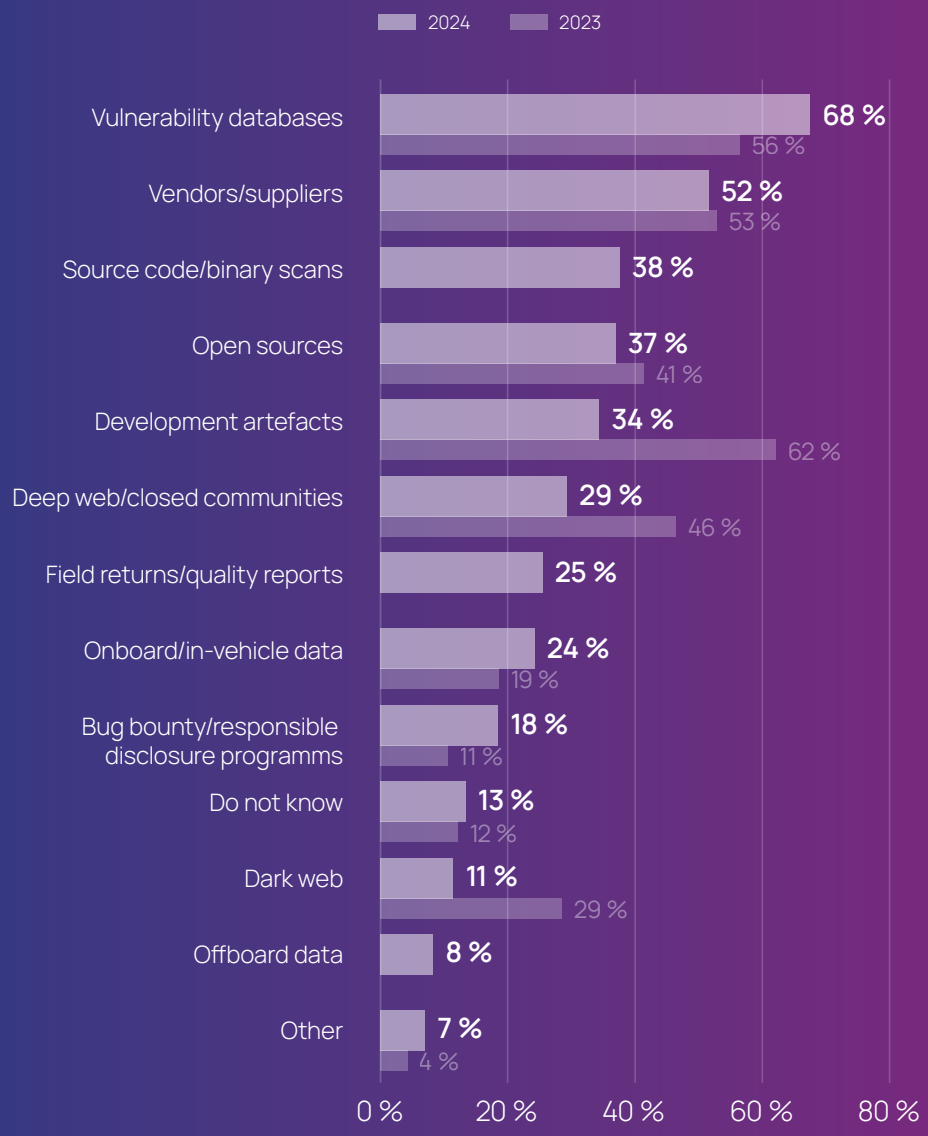
Subject-matter experts are more aware of OTA updates and security monitoring than management is.



16. Which sources does your company use for monitoring cybersecurity?

(multiple answers)

Use of vulnerability databases, responsible disclosure/bug bounty programs, code analysis, and return analysis has increased, while use of information sharing (e.g. ISAC), open research, and hacker forums have decreased. This indicates a more active response. The more mature an organization is, the more monitoring sources it uses.

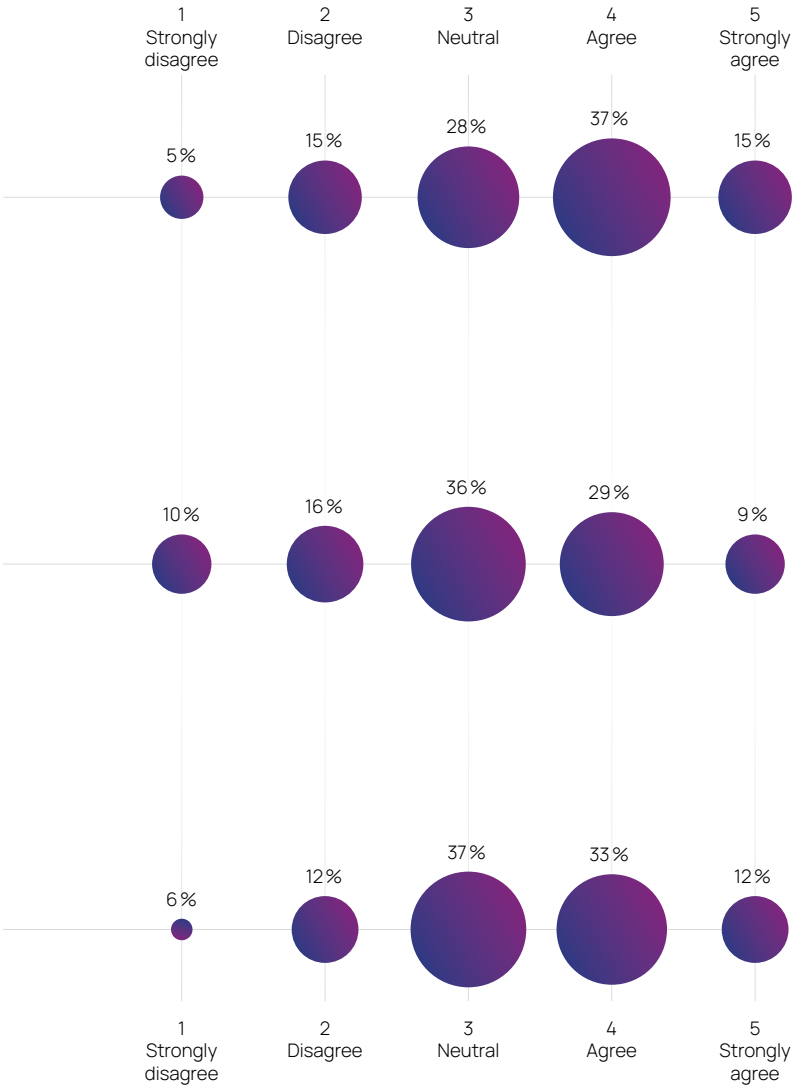


17. How well is your area of responsibility prepared for a cyber incident or attack? Rate your level of agreement with the following statements (single answer)

In my area, we have a detailed incident response plan that specifies roles and responsibilities, escalation procedures, and communication protocols.
Only the most mature organizations feel prepared at all. Subject-matter experts are less assured than management.

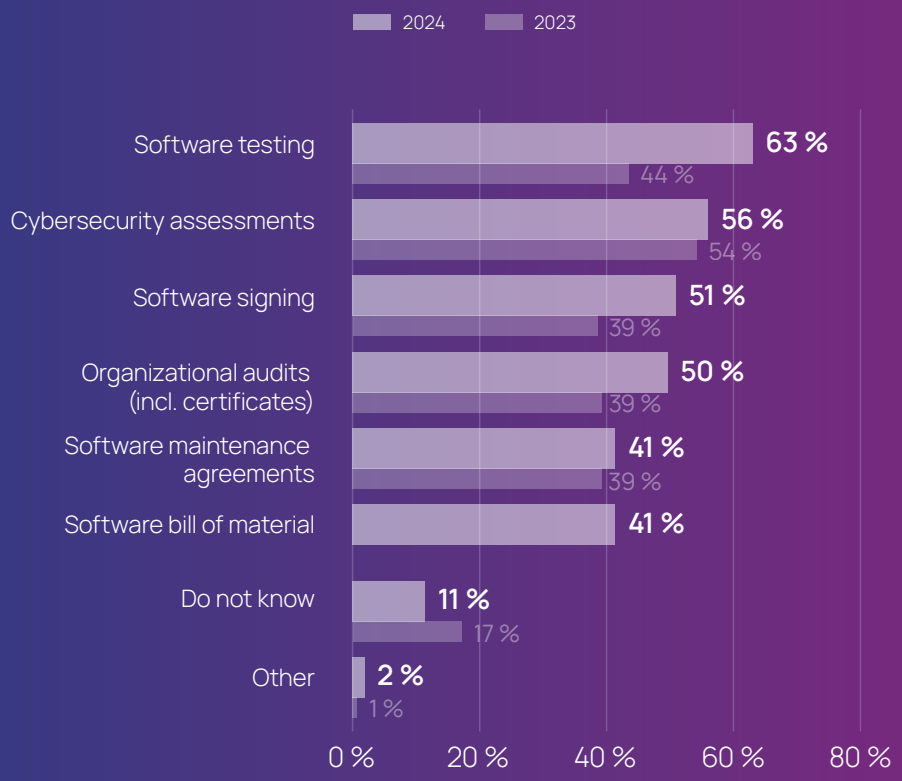
In my area, we regularly test and evaluate our incident response plan to validate its effectiveness and identify areas for improvement.
Agreement with this statement correlates directly with maturity.

In my area, we have a backup and recovery plan in case of a cyber incident, including data backups, restoration procedures, and testing to ensure data integrity.
Agreement here correlates directly with maturity. Subject-matter experts are less assured than management.



18. What measures does your company take to secure its software supply chain? (multiple answers)

Software signing, testing, and maintenance agreements have increased, and respondents are better informed on supply chain security.



Contacts & acknowledgements

Dr. Teresina Herb
Product Field Architect
Offboard Security
teresina.herb@etas.com

Michael Klinger
Head of Security
Western Europe
michael.klinger2@etas.com

Dr. Robert Lambert
Cryptography Lead
Technical Officer
Robert.Lambert@etas.com

Dr. Moritz Minzlaff
Head of Professional
Security Services
moritz.minzlaff@etas.com

The Automotive Cyber Maturity Survey 2024 is joint work with: Beate Boy, Bastian Groba, Janina Hofer, Jan Holle, Youngeun Kim, Michael Lüke, Christopher Lupini, Huang Mendi, Michael Schneider, Sven Schran, Anna-Lena Sentker, Fatima Smati, Furue Takahiro and many more.

Big thanks also to ASRG, Auto-ISAC, Autosar, escar US, GlobalPlatform, and isits for sharing and promoting the survey.

Last updated: 07/2024