Automotive Cyber Maturity Report 2023

Dr. Moritz Minzlaff, July 2023

Empowering Tomorrow's Automotive Software
www.etas.com

Contents

Preface

Mobility is experiencing a fundamental change. Software is now taking center stage and rapidly accelerating development. Software-defined vehicles are gaining importance due to the demands of increasingly personalized, automated, connected, and electrified mobility. In addition, flexibility, sustainability, and safety are emerging as significant influences on mobility software. Automotive software, however, is closely linked with automotive security. As the industry races toward realizing the enormous technological and economical potential of the software-defined vehicle, it needs a strong understanding of cybersecurity.

It is with this in mind that ETAS is proud to facilitate the annual Automotive Cyber Maturity Survey. Now in its third year, I am excited to see record participation in each of the major automotive markets. Subject matter experts, first-line managers, as well as CEOs all took part. This demonstrates a clear need and benefit for the industry to take stock of its cybersecurity practices.

I am happy to share the results with you here. Cybersecurity for the software-defined vehicle challenges the boundaries of conventional vehicles and prevalent mindsets: the survey responses show that the most cyber mature automotive manufacturers and suppliers integrate security into a highly automated, software-centric development; that they consider protection along the whole ecosystem, including open-source software projects; and that they implement security on all levels, from deeply embedded to vehicle clouds. Crucially, the organizations leading the way understand that security is a technological as well as a cultural challenge.

This same agile, secure development philosophy underpins ETAS's approach: we enable fast and secure, data-driven development, along with efficient and secure deployment and operation of automotive software. This is how we actively empower tomorrow's automotive software together with our customers and partners. Now is the time to shape a new era of mobility that will continue to protect road users and business models.

Dr. Thomas Irawan
President ETAS GmbH

Executive summary

The automotive industry is continuing its rapid transformation toward being a software business. Keeping up with the speed of the software has become a key differentiator for success: the faster that automotive companies can detect and fix software vulnerabilities, the better they can protect their customers and business models against cyber threats.

The Automotive Cyber Maturity Report provides facts and figures on how the most advanced organizations master automotive (software) security – and what challenges must still be overcome for the industry to mature further. It is based on the leading annual industry survey of cybersecurity practices at companies in the automotive value chain, from semiconductors and suppliers to manufacturers.

This year's survey is the most representative yet: with record participation from the three largest automotive markets and participation from a record number of countries, the findings depict an up-to-date view of how far the industry has come. This report also captures cybersecurity from all angles: participants come from small enterprises as well as large corporations, and they range from subject matter experts all the way to CEOs (see page 6).

There has been a major jump in self-assessed cyber maturity since the previous year (see figure below). While in 2022 most participants placed their organizations at initial maturity, this year just as many consider their organization to be highly cyber mature as not. The industry average is now at level three, meaning that processes and cybersecurity activities have become established. We can confirm an increase in cyber maturity based on our experience working with and supporting automotive companies worldwide as a security vendor, but we also stress the need to improve further: the changes brought by the software-defined vehicle demand additional increases in cyber maturity. The industry must ensure that there is no gap between perceived cyber maturity (due to improvements already made) and actually achieved security levels.

In addition, our analysis of the responses led to the following main insights:

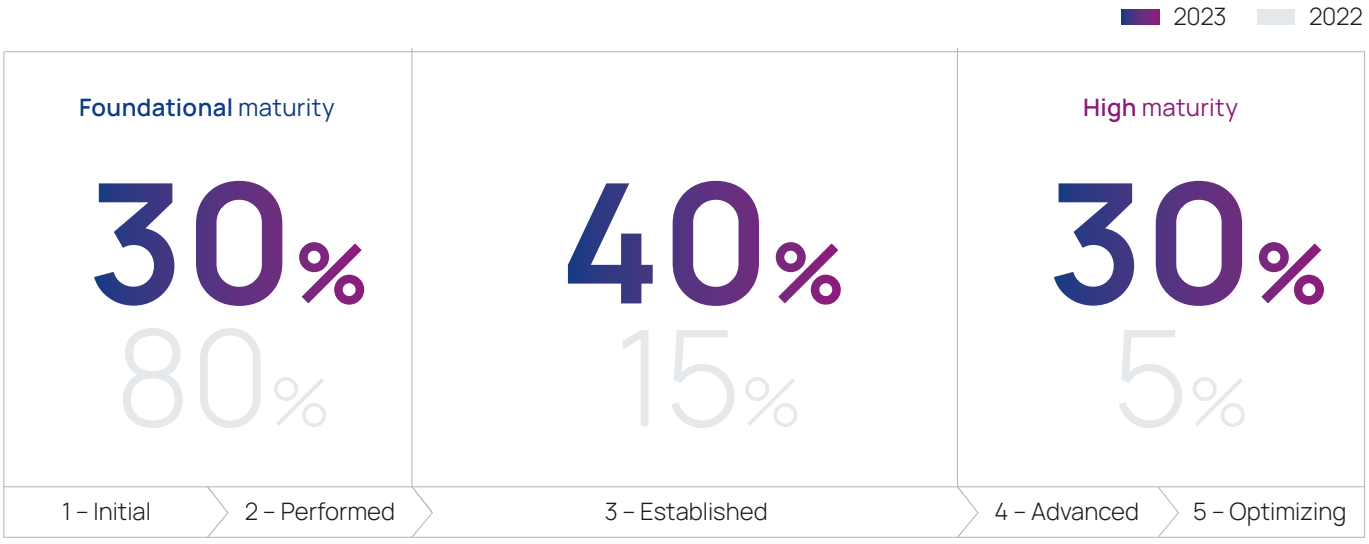
Takeaway #1: High maturity means end-to-end security
Securing automotive products along the lifetime, ecosystem, and supply chain dimensions is the main differentiating mark for high-security organizations. It starts with "why" these companies care about security. They understand that in addition to compliance, security must protect customers, road users, and business models.

Takeaway #2: Supply chain security needs more attention
The industry is at a crossroads when it comes to cyber maturity in the supply chain. The current state is much more positive than in previous years, with over one-quarter of participants being satisfied. At the same time, only one concrete measure to secure the supply chain is used by the majority of automotive companies, meaning that organizations must still adopt more comprehensive programs.

Takeaway #3: Security is a people and mindset challenge
Insufficient capacity and expertise (competence) still rank as the biggest challenge for participants. As security is not only a technical task, the solutions need people who understand and know about cybersecurity, organizations that establish an integrative, multi-disciplinary approach, and industry-wide efforts to improve cybersecurity along the automotive value chain.

Takeaway #4: On the way to securing software-defined vehicles
The survey results show positive developments in the industry across many different areas: why companies do security, how satisfied they are with progress, and where they see open challenges. Going forward, it will be mandatory to build on these accomplishments, but do not forget the road ahead: the industry as a whole must follow the direction provided by the highly mature organization and keep up with the speed of software and corresponding security challenges.

.



Context and design of this year's survey

This year's survey took place in the middle of arguably one of the greatest transformations in automotive history: the industry is moving toward the software-defined vehicle with its promises of more comfort, new business models, and even stronger safety. In this transformation, cybersecurity has become a major business factor for manufacturers and suppliers: software vulnerabilities have led to safety recalls, automotive-specific regulations mandate security in the largest markets, and most manufacturing and automotive companies recently ranked cyber incidents as a top 5 business risk. In our whitepaper on "Cybersecurity for the software-defined vehicle" we describe how security must now be ensured end-to-end along the three dimensions of product lifecycle, software supply chain, and the product ecosystem.

In this third edition of our annual automotive cyber maturity survey, we therefore ask again how far along the industry has come with this end-to-end security. The survey aims to do three things:

- Foster an understanding between different players in the industry, both within and between companies
- Capture what highly mature organizations do differently, and learn from them
- Identify challenges in maturing the industry further

The survey groups the questions into four overarching topics:

- Governance
- Progress & challenges
- Securing the lifecycle
- Ecosystem & software supply chain

The target audience of this survey are automotive professionals whose work deals on some level with security. This includes security engineers and experts, but also production engineers and the C-level management. The survey is anonymous and based on multi-choice questions. The objective was to reduce hurdles for participation and get an honest and unfiltered look at the industry's status quo of cyber maturity.

And it worked! This year's survey is the most representative yet. We are very happy to report record participation from the three largest automotive markets: China, the US, and Europe. We can segment the data according to the respondents' place in the automotive value chain (e.g., manufacturer or supplier), region, job level, and their organization's maturity, among others. This gives manifold insights into the various perspectives in the industry on cyber maturity and helps foster the understanding that is the basis for maturing the industry further.

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.

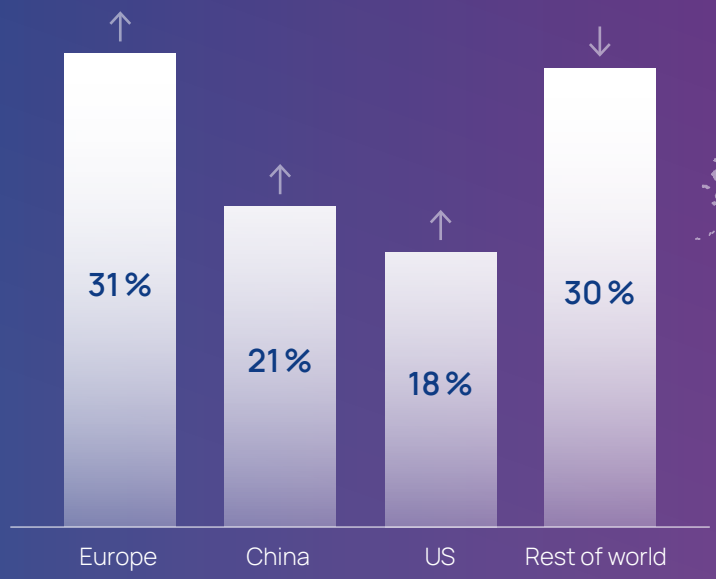
Download the Whitepaper

2022 survey design and statistics

Record participation from Europe, China, and the US

Regional share

↑ increase or
↓ decrease compared to previous year

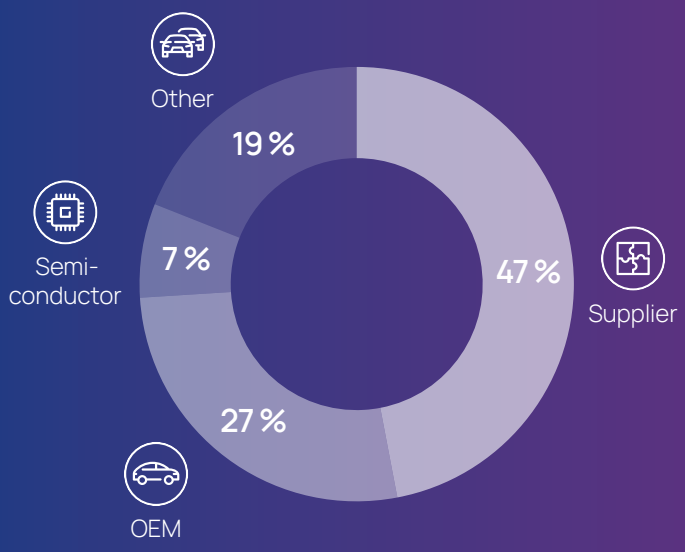


Participants come from a record fifteen countries including all top 5 automotive markets:
Brazil, China, France, Germany, Hungary, India, Italy, Japan, Korea, Netherlands, Spain, Sweden, United Kingdom, United States, Vietnam

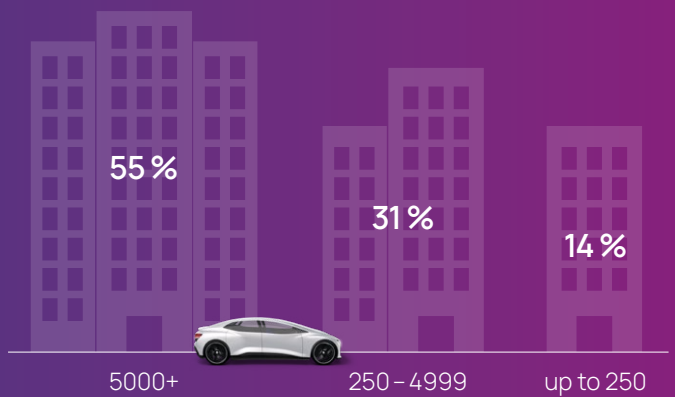
Total number of participants: 140

Job level

Type of company



Size of company
measured in number of employees



Key takeaways

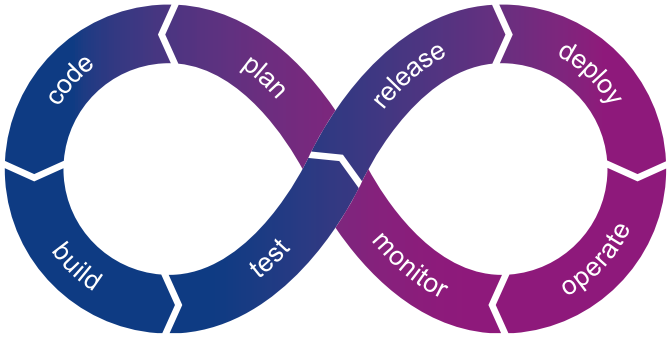
Takeaway #1: High maturity means end-to-end security

Higher cyber maturity means ensuring automotive security along three crucial dimensions: the lifetime of the product, the ecosystem of the product, and the software supply chain of the product. We call this the new end-to-end security (see also our whitepaper "Cybersecurity for the software-defined vehicle). Last year's survey already indicated that this end-to-end security is the main differentiating mark between the companies of high and low cyber maturity.

This year's data provides additional details. It starts with "why" organizations care about cybersecurity. High-maturity enterprises are much more likely to be driven by a need to protect their customers, road users, and business models. They understand that security is an integral part of resilience and business continuity. This is also reflected in how they measure security: spending on cybersecurity alone as a measure becomes less relevant, but rather a mindset of continuously keeping up the security level. Metrics that are used more often at high maturity include the number of critical cybersecurity events and the mean time to detect/repair security defects.

Main drivers for cybersecurity activities

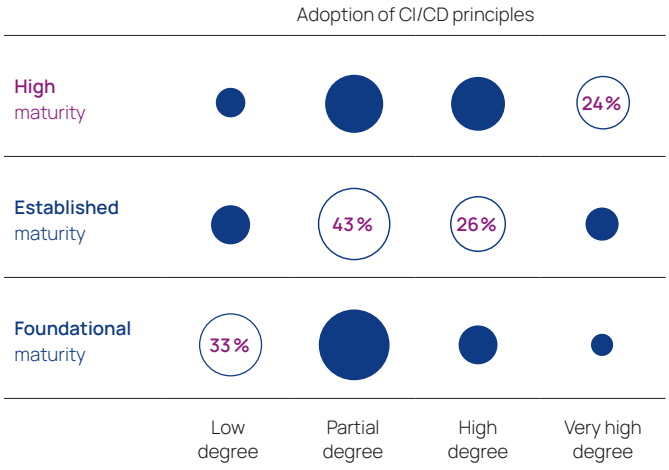
Protection of (new) business model	Protection of road users	Resilience and business continuity
+156%	**+132%**	**+59%**



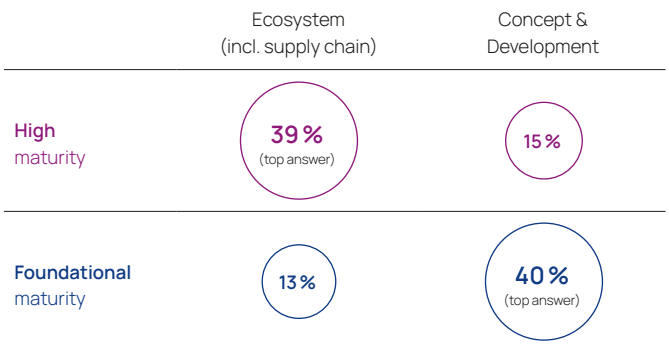
Metrics used to measure cybersecurity

Number of critical cybersecurity events	Mean-time-to-detect/repair	Budget for cybersecurity
+71%	**+65%**	**-5%**

Compliance is still relevant for high-maturity organizations, but they tackle it with more automation and a wider deployment of tools. The shift in the automotive industry toward being a software business means principles from continuous integration/continuous deployment (CI/CD) are key competitive advantages, and the highly cyber mature organizations understand this. This allows them to keep up with the speed of software and roll out fixes much faster.

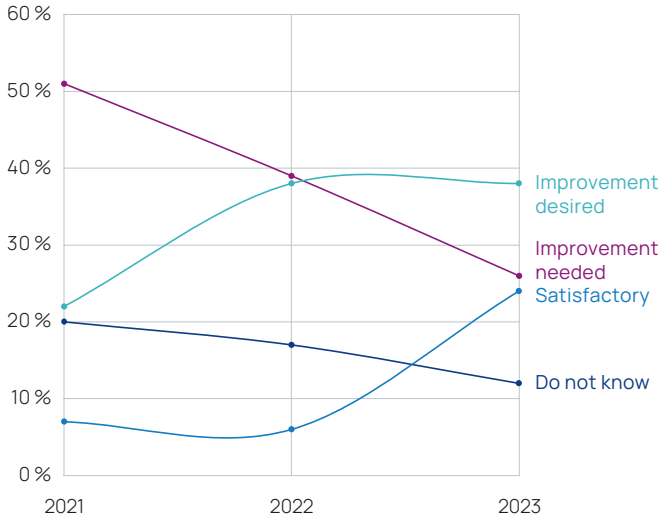


Differences in cyber maturity also come with different views of the open challenges. Where foundational maturity organizations still see concept & development including security by design as the domain with the biggest challenges, high-maturity organizations have well-established practices and dedicated security roles in this area. They are much more likely to have certified security management systems. With higher maturity, the focus shifts from development to ensuring security along the ecosystem dimension. That means looking not just at the product itself, but at how and where it is developed, how and where it is produced, and how and where it is operated, including what (offboard) devices and systems it is in contact with.



Takeaway #2: Supply chain security needs more attention

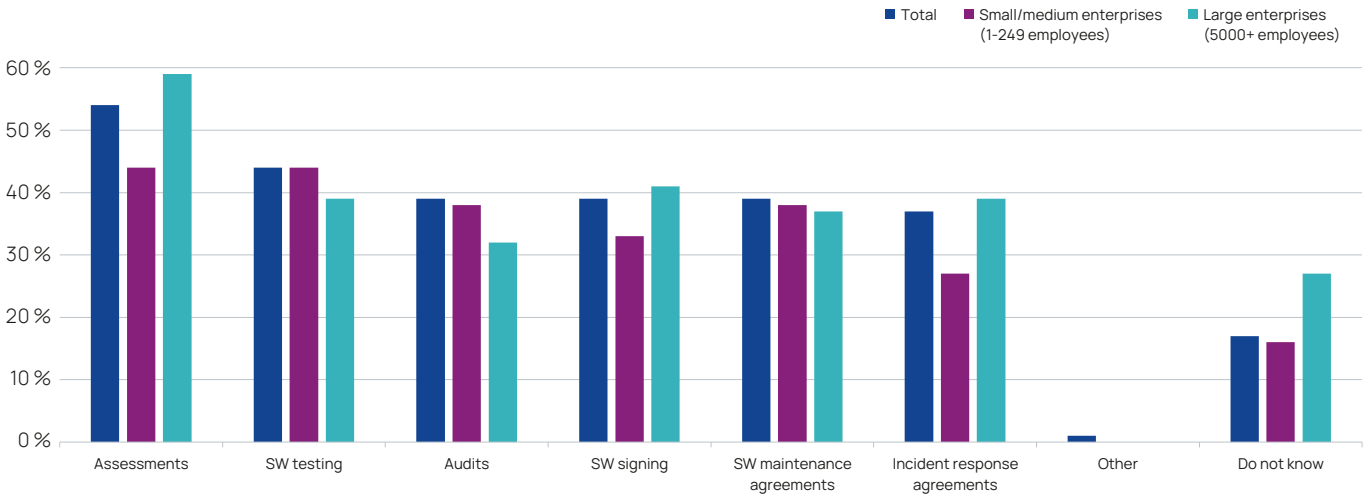
The supply chain in the automotive industry is complex, and it is one of the three dimensions of the end-to-end security for software-defined vehicles (see previous takeaway). The data paint a mixed picture: on the one hand, the survey participants report an improvement to the cyber maturity in their supply chains; on the other hand, few measures for supply chain security have been widely adopted. We therefore see a need for the industry to not let up and keep – or, better still, increase – the focus on additional activities to boost security in its supply chains.



Each year since 2021, we have asked how automotive professionals see the cyber maturity in the supply chain. Year over year the need for improvements has been dropping, while satisfaction with supply chain maturity has seen a sharp rise. Also, the share of participants who did not know the status of their supply chain has dropped for three years in a row now. This positive trend also correlates with the participants' own organizational cyber maturity: the top responses from high-maturity companies are that improvements are desired (as opposed to needed) or that supply chain cyber maturity is satisfactory. In contrast, organizations at the beginning of their cybersecurity development most often respond that improvement is needed.

This overall positive trend stands in contrast to the adoption of specific measures to secure the supply chain. Out of six measures, only cybersecurity assessments (of their suppliers' products) are used by more than half of the survey participants. Crucially, digitally signing software as a means to ensure that only authentic, tested, and released binaries are used in vehicles comes only in fourth place overall, with less than two out of five participants selecting this measure.

These results speak to a strong need for companies to adopt more comprehensive programs for supply chain security. Larger organizations seem further ahead in this regard. They have adopted on average almost twice as many measures. Also, participants from manufacturers selected more measures than those from suppliers (the biggest difference being in software signing); this was also true of those from high-maturity organizations versus foundational maturity organizations. In both segments, the overall difference is less pronounced than for company size.



Takeaway #3: Security is a people and mindset challenge

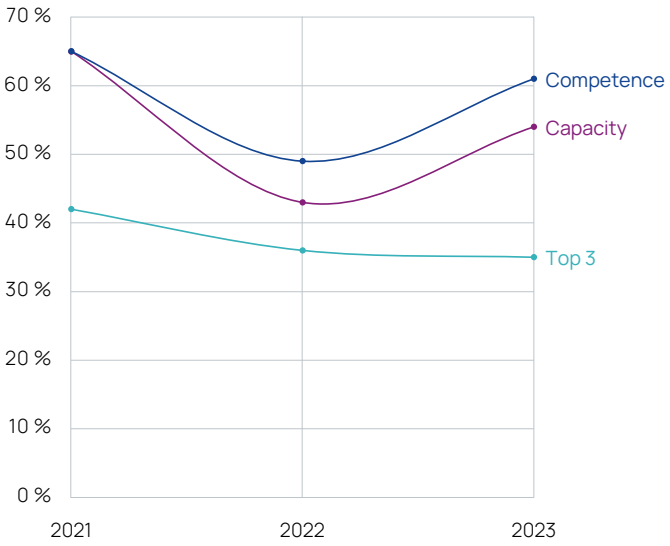
Cybersecurity is not solely a technological puzzle; it is also a topic that involves human expertise, behavior, and mindset. This approach includes people comprehending the impact of their actions, from enforcing code signing for software artifacts to identifying potential phishing attempts in emails or phone calls. Such precautions are essential components of an organization's cyber defense.

When we asked participants for the biggest challenges in their areas of responsibility, they answered (in)sufficient competence and capacity of cybersecurity skilled personnel. Both have remained the number one and number two challenges for the third year in a row, and the gap to the third-placed challenge has been growing. This also holds true across all segments of survey participants except for semiconductors and small enterprises, who do not put capacity in second place.

Beyond these two overarching topics of competence and capacity, the survey results also show that different segments have quite different perceptions of the main challenges: culture is a top three challenge for participants from larger enterprises and subject matter experts, but not for small companies or top management. Larger organizations report process maturity less often as a challenge whereas smaller organizations report higher adoption of CI/CD principles.

Subject matter experts choose "development" twice as often concerning attack vectors (see remarks on software signing and phishing above) as mid- and top-level management.

With such varied perspectives and with one-quarter of participants not knowing how often their companies' products are affected by cyber incidents, ongoing learning, adaptation, and understanding are necessary. Ultimately, the strength of cybersecurity lies in a collective, company-wide commitment to protect information and systems. This requires people who understand and know about cybersecurity, organizations that establish an integrated, multi-disciplinary approach, and industry-wide efforts to improve cybersecurity along the automotive value chain.



Culture

Culture is a top 3 challenge for large enterprises and subject matter experts, but not for small companies nor for top management

Larger organizations report process maturity less often as a challenge, but smaller organizations report higher adoption of CI/CD principles

CI/CD vs process maturity

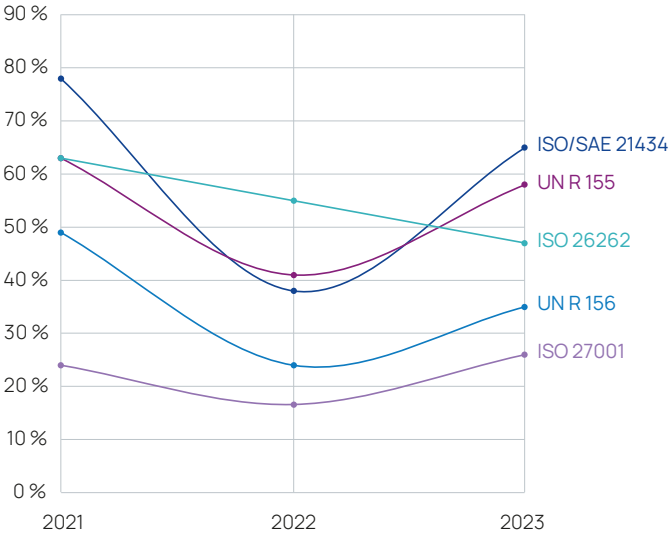
Development
as attack vector

Subject matter experts choose the development phase more than twice as often as relevant attack vector than mid- and top-level management

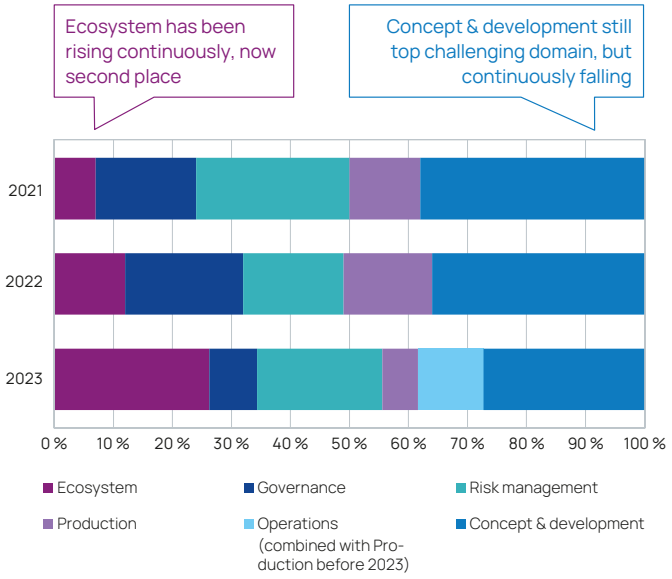
Takeaway #4: On the way to securing software-defined vehicles

In this fourth and final takeaway, we collect positive trends that together show how the industry is on the way toward implementing adequate security for software-defined vehicles – and trends that point out areas of further improvement.

Top 5 most relevant frameworks



First, satisfaction with progress since the previous year is accelerating, and average satisfaction has risen year over year since 2021. The survey results contain promising data that support this satisfaction: average self-reported maturity has risen along with satisfaction, from an average of 1.6 in 2022 to an average of 3.0 this year. The number one driver for cybersecurity has shifted from compliance in 2021 to protection of customers. This speaks to a more comprehensive and less checklist-driven approach to security. Also, management awareness and commitment has improved: it is now almost one-third less likely to be selected as a challenge than in the previous year.



Overall, the industry seems to tackle secure development activities better and better, and the focus is now shifting to mastering security at the ecosystem level (see question "Which is in your view currently the domain …"). This is also reflected in the most relevant frameworks: ISO 26262, which once served as a launch pad to go from safety to security, is receding more into the background, while other standards that take a more management system level view such as ISO/IEC 27001 are rising in prominence together with regional frameworks.

Another aspect of how the shift to ecosystem security manifests itself are the most concerning attack vectors and the scope of organizations' ecosystem management. While last year's results still showed a gap between high-maturity and foundational maturity organizations regarding ecosystem-level attack vectors such as backend systems, repair shops, and the software supply chain, this year this difference has almost vanished. Overall, the industry now considers these attack vectors much more relevant – which is not surprising given recent exploits and proof of concept attacks that have been published. The industry has also expanded the number of stakeholders it considers part of its ecosystem management, with the biggest rise seen in the interaction with authorities, horizontally between automotive companies, and with customers.

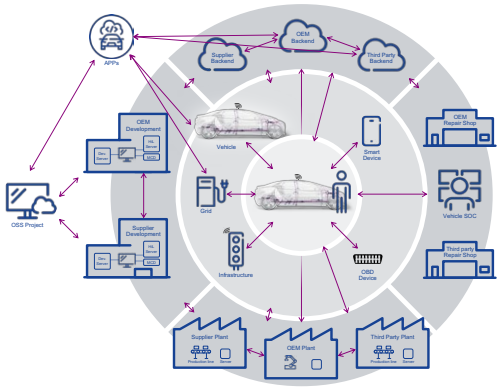
At the same time, we caution that the satisfaction with these trends must not make the industry blind to weaknesses that still exist. Takeaways #2 and #3 pointed to open challenges that each company in the automotive value chain and the industry as a whole must master, and the insights into highly mature organizations from Takeaway #1 provide a direction that others can follow.

Most concerning attack vectors

Last year showed more mature organizations put more focus on the "outer ring", too.This year, the gap is much less pronounced. Major remaining difference: Vehicle OS.

Biggest increases over previous year:

Repair shops	Backend systems	Software supply chain
+195 % (9 ↑)	**+150 % (2 ↑)**	**+100 % (4 ↑)**



Scope of ecosystem management

Biggest increases over previous year:

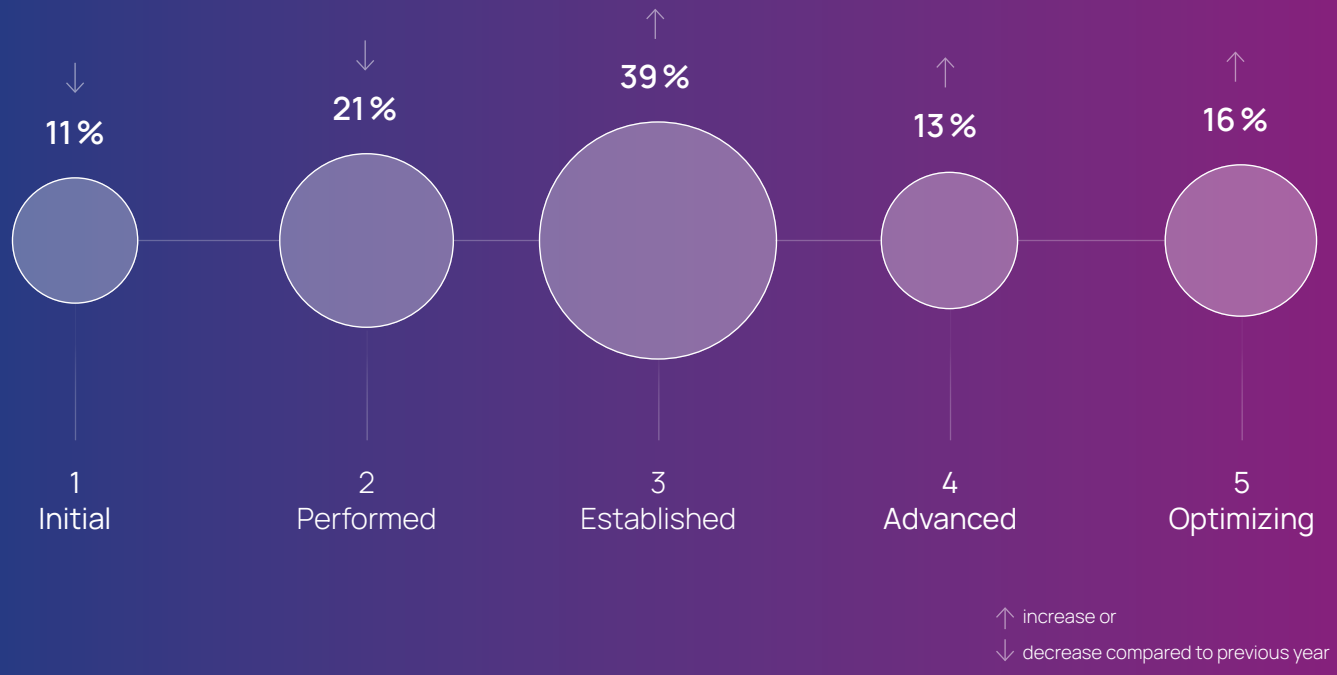
Authorities	Horizontal within industry	Customers
+340 % (4 ↑)	**+138 % (2 ↑)**	**+74 % (1 ↑)**

Survey results in detail

Governance

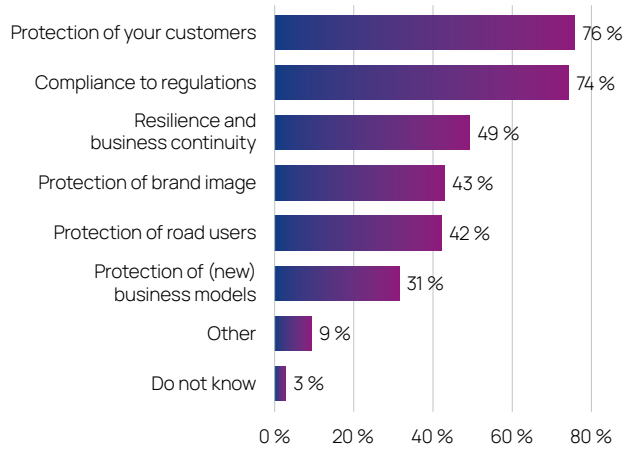
1. How do you rate the cyber maturity of your organization? (single answer)

Self-assessed cyber maturity has risen sharply over the previous year. The industry average is now at level 3 with established processes and cybersecurity activities. We also see an increase in maturity in our engagements with automotive companies worldwide, but we stress a need to improve further: the industry must ensure that there is no gap between perceived cyber maturity (due to improvements already made) and actually achieved security levels.



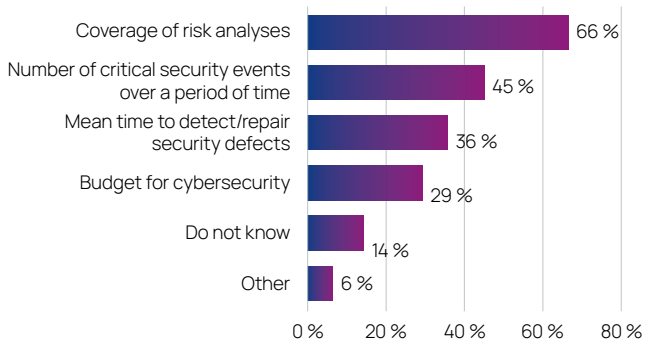
2. What are the main drivers of your organization's cybersecurity activities? (multiple answers)

Compliance is still a major driver, and jumped from half to roughly three-quarters of all responses. However, protection of customers is now the top driver. Both are the top two drivers across all job levels. Resilience and business continuity is a promising sign that enterprises are considering security more and more from an integrated and not purely technical perspective.



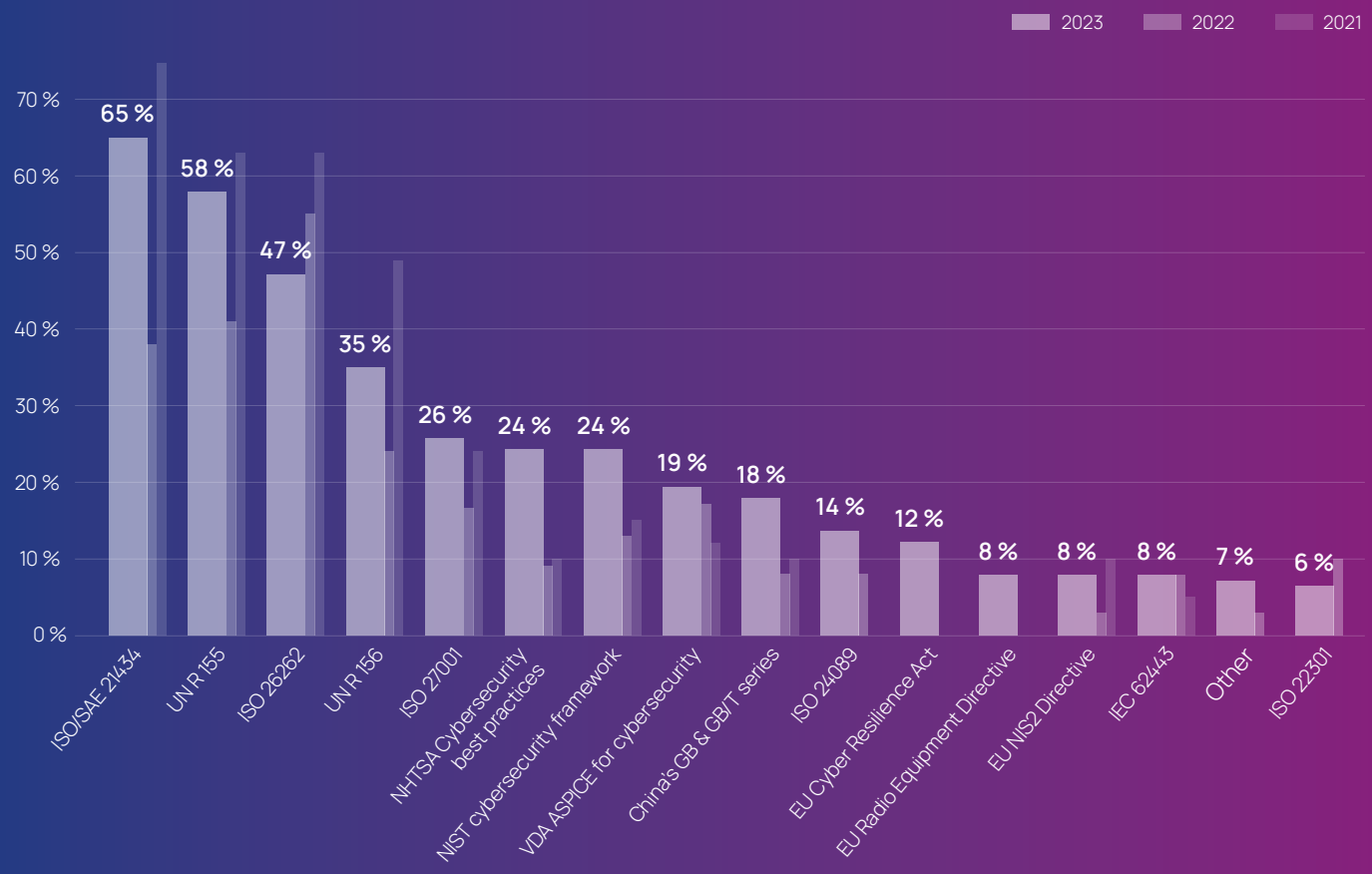
3. Which of the following metrics are used in your area of responsibility to measure cybersecurity? (multiple answers)

The fact that coverage of risk analyses was the top answer can be explained by the short-term need to become compliant (see main drivers). Number of events and especially mean time to detect and repair are key metrics in the software industry, so it will be interesting to see their ranking in the years ahead.



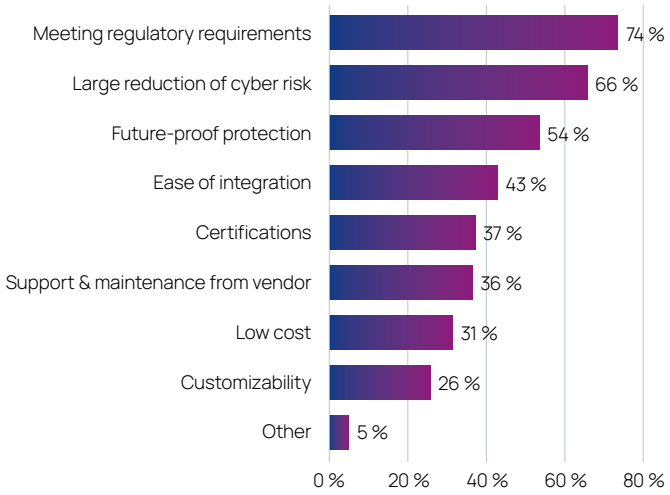
4. Which frameworks are currently most relevant for cybersecurity in your area of responsibility? (multiple answers)

The top four have stayed the same from 2021 to 2023, with ISO/SAE 21434 and UN R 155 consistently the top two independent of company type, size, maturity, or participants' job levels. The only exception are companies with less than 5,000 employees: here, ISO 26262 still ranks second place.



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

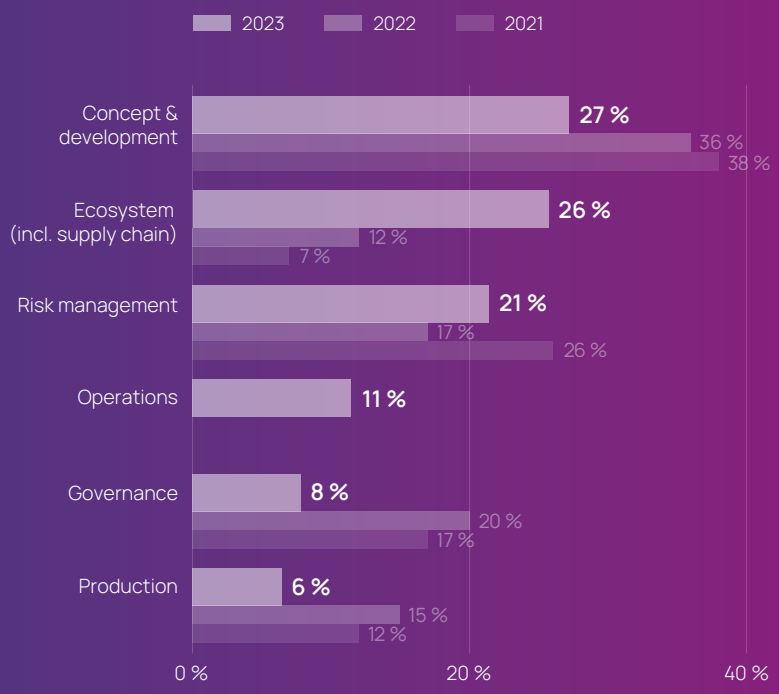
The top two choices, meeting regulatory requirements and reduction of risk, reflect the top drivers for cybersecurity (see question "What are main drivers …"). As with the main drivers, the higher a company's maturity, the higher that reduction of risk/protection of customers rank in the answers.



Progress & challenges

6. Which is in your view currently the domain with the biggest cybersecurity challenges for your organization? (single answer)

We already discussed the rise of Ecosystem as the domain with the biggest challenge in Takeaway #4, and we expect this area to drive a lot of cybersecurity activities for the foreseeable future. There are relevant regional differences and differences between OEMs and suppliers. In China and Europe, Risk Management is ranked on top, while in the US it is the Ecosystem domain. OEMs are twice as likely to choose Risk Management, Operations, and Production as suppliers are, whereas suppliers choose Concept & Development three times more often than manufacturers.



7. What are the biggest cybersecurity challenges for your area of responsibility?

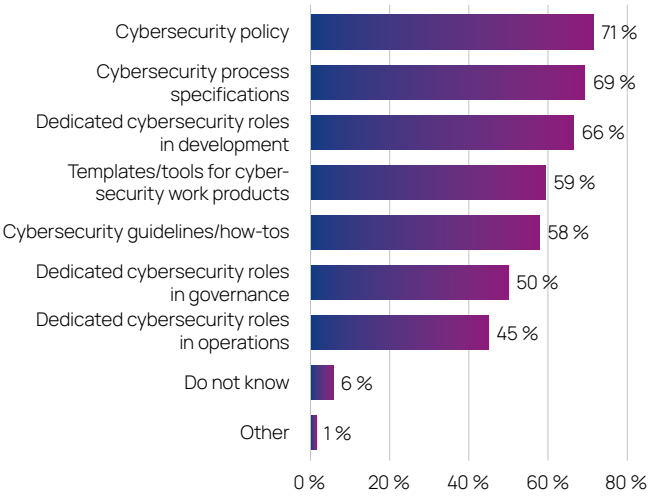
(multiple answers)

As in previous years, the main challenge for most respondents in their area of responsibility are getting sufficient competence and capacity for automotive cybersecurity. Two segments of participants deviate from this trend: semiconductors and companies of less than 250 employees do not rank capacity within the top three, but rank culture second and third place, respectively.

8. Which of the following does your organization have?

(multiple answers)

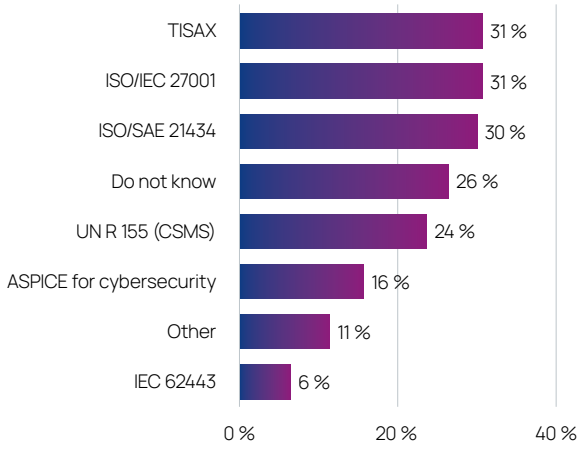
The results indicate that policies and process specification rather than dedicated cybersecurity roles are the starting point for participants' cybersecurity activities. This seems to align with the answers to the previous questions, which showed that staffing those roles adequately would be a prime challenge. Larger organizations seem stronger in formalizing cybersecurity: the larger the participant's company is, the more likely each individual option was selected.



9. Which certifications does your organization have?

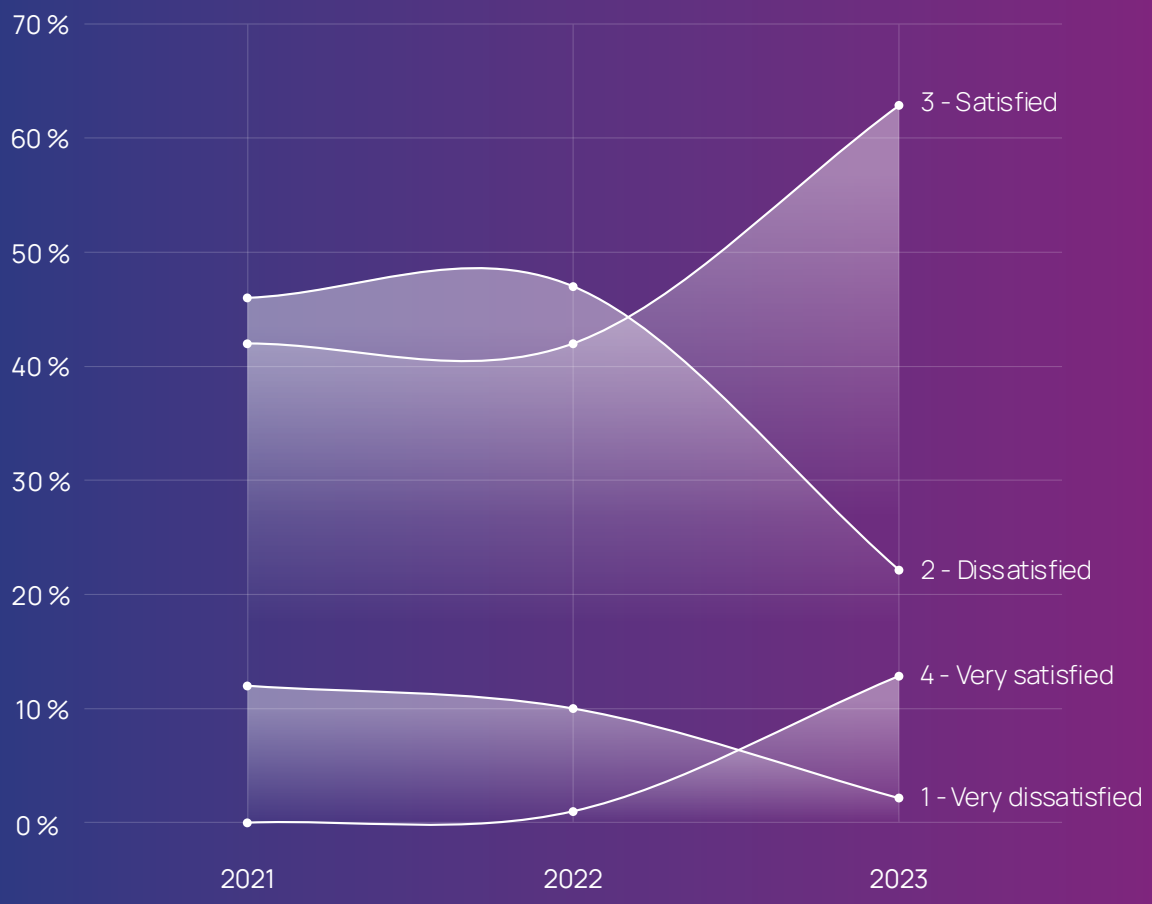
(multiple answers)

Classical information security certification such as TISAX and ISO/IEC 27001 are still the most frequent in the industry. It will be interesting to see how this develops, with UN R 155 CSMS and ISO/SAE 21434 certification becoming increasingly relevant and commonplace. We also note that according to the responses almost half of small enterprises (less than 250 employees) do not have any certification in place at all.



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

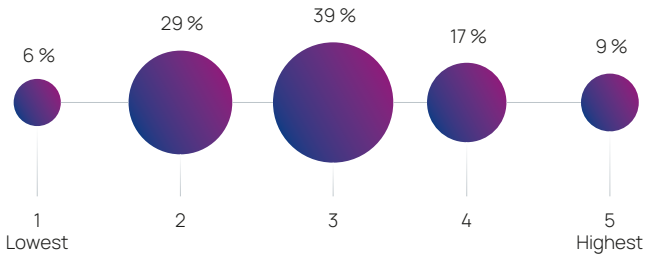
Overall, participants are satisfied with the progress of cybersecurity in their organizations. This holds true across regions, company sizes, and types. Compared to 2022, average satisfaction increased by almost one-third. We are glad to see the industry's efforts seem to be paying off, but at the same time we advise that satisfaction must not make us blind to the improvements that are still to be made (cf. also comment on the question "How do you rate the cyber maturity …").



Securing the lifecycle

11. Overall, how do you currently rate the cyber risk for your company's products? (single answer)

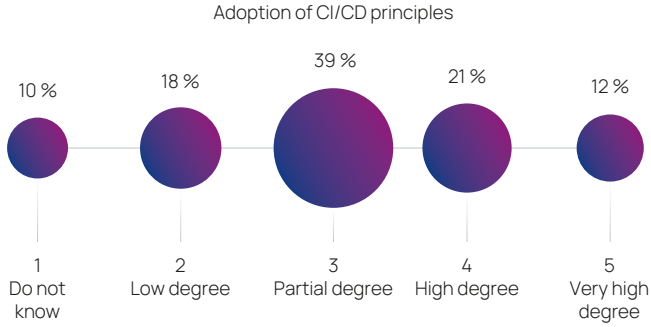
This is the first year that we have tracked how the industry rates overall cyber risk. In the future, the changes in response can be used to measure whether the industry sees itself as on the right track to keep up with the rapidly evolving threat landscape. This year, the average is 2.9; manufacturers and semiconductors perceive a higher risk, with averages of 3.3 and 3.7, respectively.



12. What best describes your organization's status with respect to continuous integration/continuous deployment (CI/CD)?

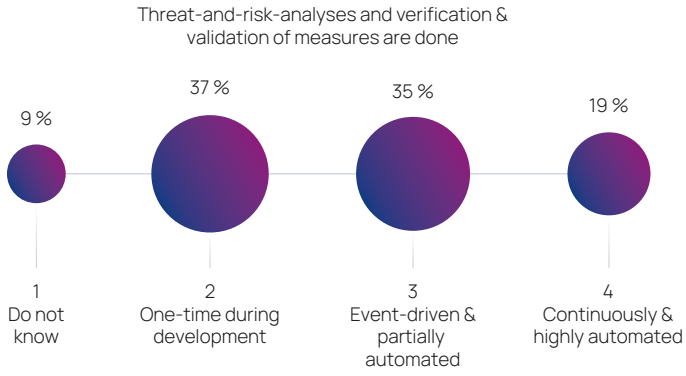
(single answer)

The numerical industry average according to the responses is 2.9, but there is a strong positive correlation with self-assessed maturity and a strong negative correlation with company size: larger enterprises seem to struggle more to get CI/CD rolled out in their organizations.



13. What best describes your organization's approach to risk management? (single answer)

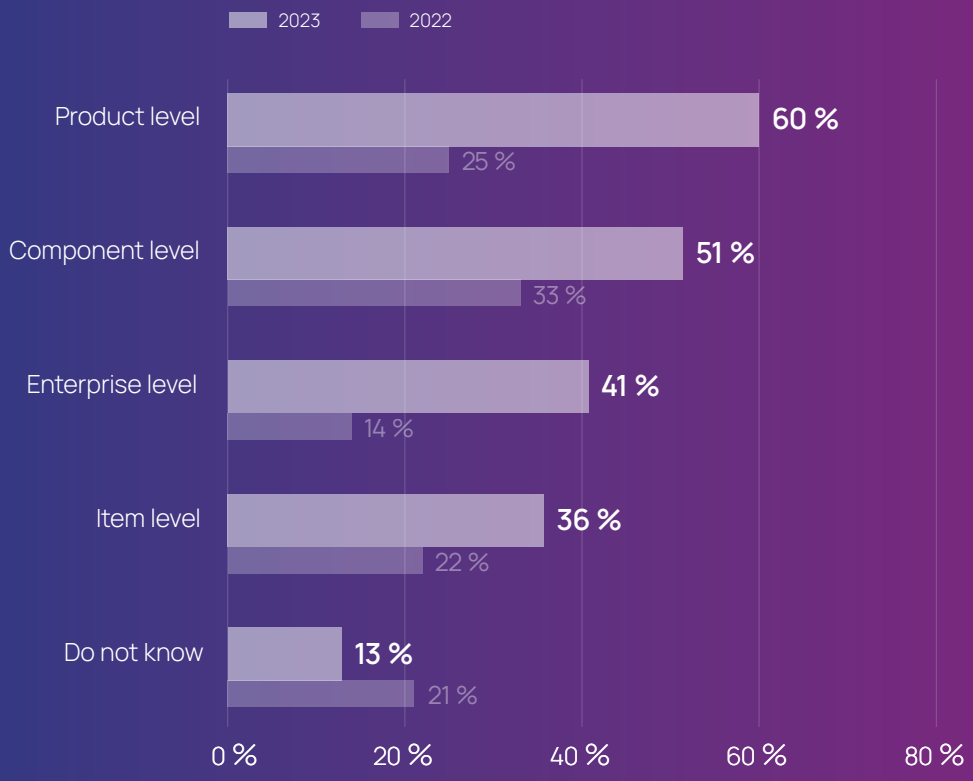
The answers to this question tell a similar story to the answer to the question regarding adoption of CI/CD principles: increasing cyber maturity and decreasing company size lead to higher scores in the organization's approach to risk management.



14. On what levels does your organization perform risk management?

(multiple answers)

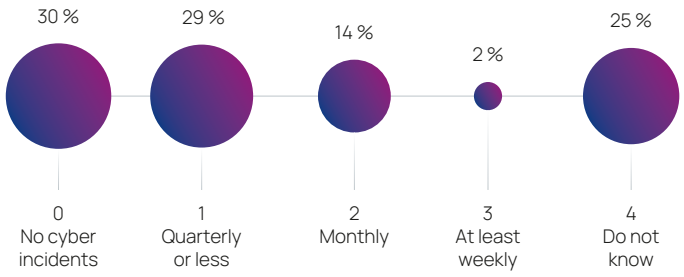
We find it encouraging to see that adoption of risk management on all levels is increasing compared to the previous year. The biggest increase is on the enterprise level, so it seems that cybersecurity management systems are now more often living up to the expectation of connecting individual cybersecurity activities into an overall whole and connecting them to the enterprise risk management.



15. Roughly how frequently have cyber incidents impacted your organization's products?

(single answer)

The average frequency is almost every month, while one-quarter of participants do not know how often their company's products are impacted. These results show a need for organizations to improve their monitoring of cybersecurity events (see also question "What kind of sources …") as well as their capability to respond to incidents, which impact products on average up to a dozen times a year.

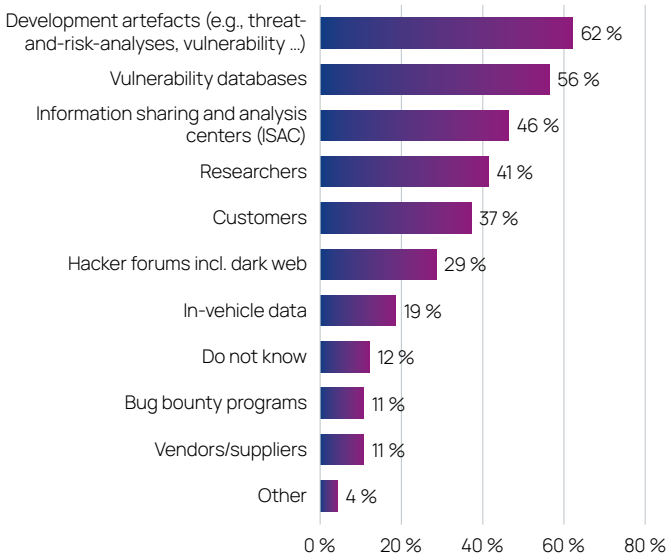


Ecosystem & software supply chain

16. What kind of sources does your organization use for cybersecurity monitoring?

(multiple answers)

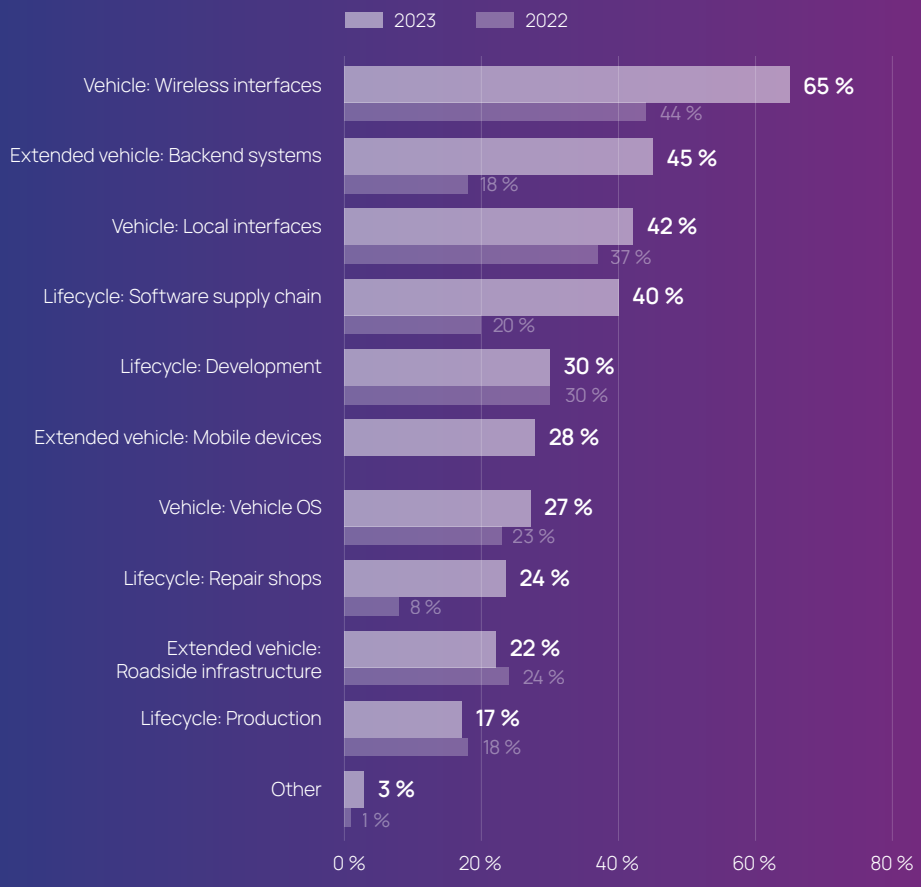
The top three overall choices are the same for manufacturers and for suppliers. The biggest differences are with customers as a source of monitoring (less than half for OEMs) and – unsurprisingly – in-vehicle data (twice as likely for OEMs). In the US and Japan, information sharing and analysis centers (e.g. Auto-ISAC, J-Auto-ISAC) are the most selected choice.



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

(multiple answers)

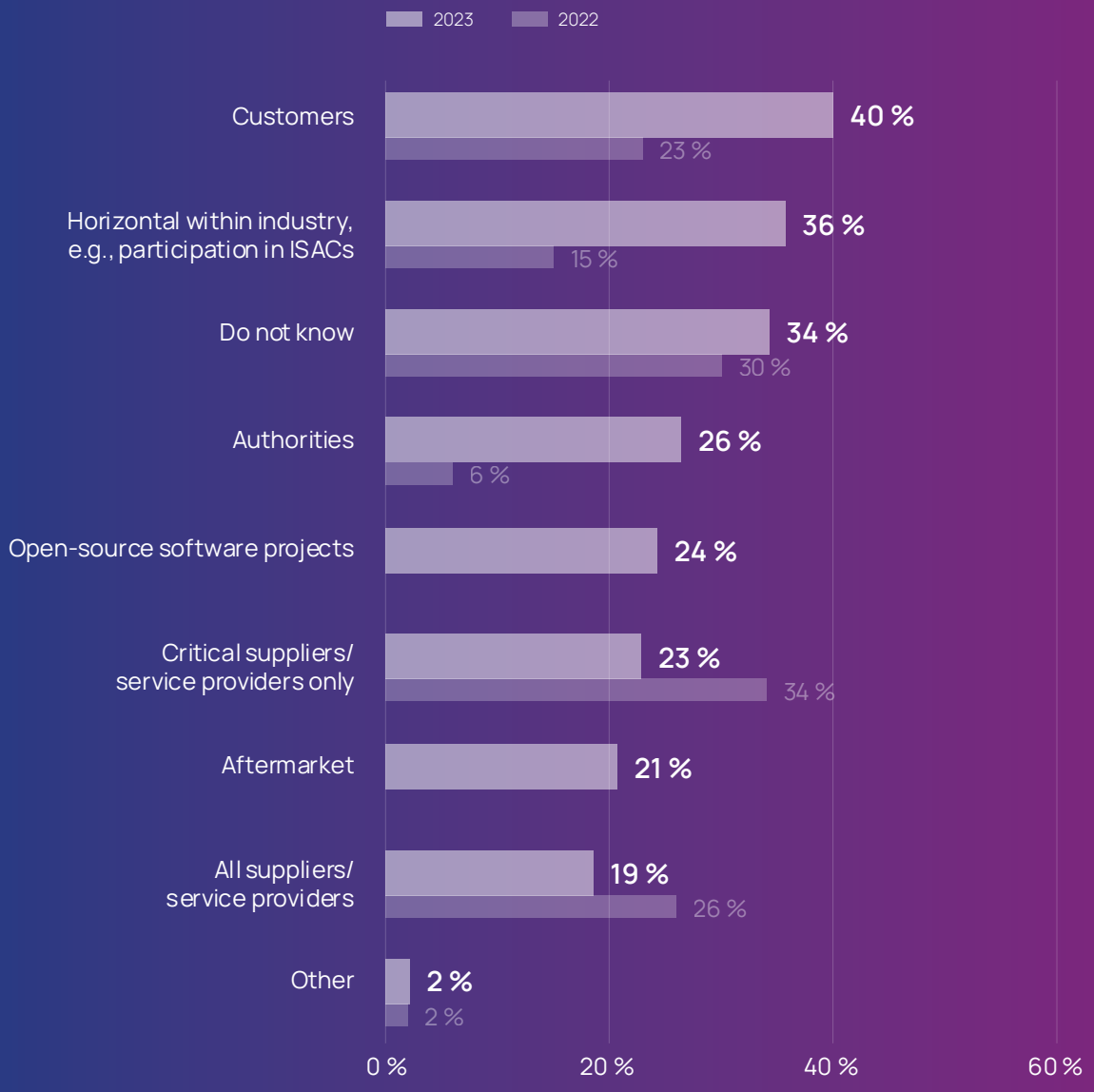
All but the two bottom-ranked attack vectors were selected more often than in the previous year by participants. Repair shops, backend systems, and the supply chain saw the biggest increases, speaking to a growing need for offboard security solutions. Supply chain as an attack vector is in fourth place overall, but among participants from China and the US it is in first and second place, respectively.



18. What is in scope of your organization's CSMS ecosystem management?

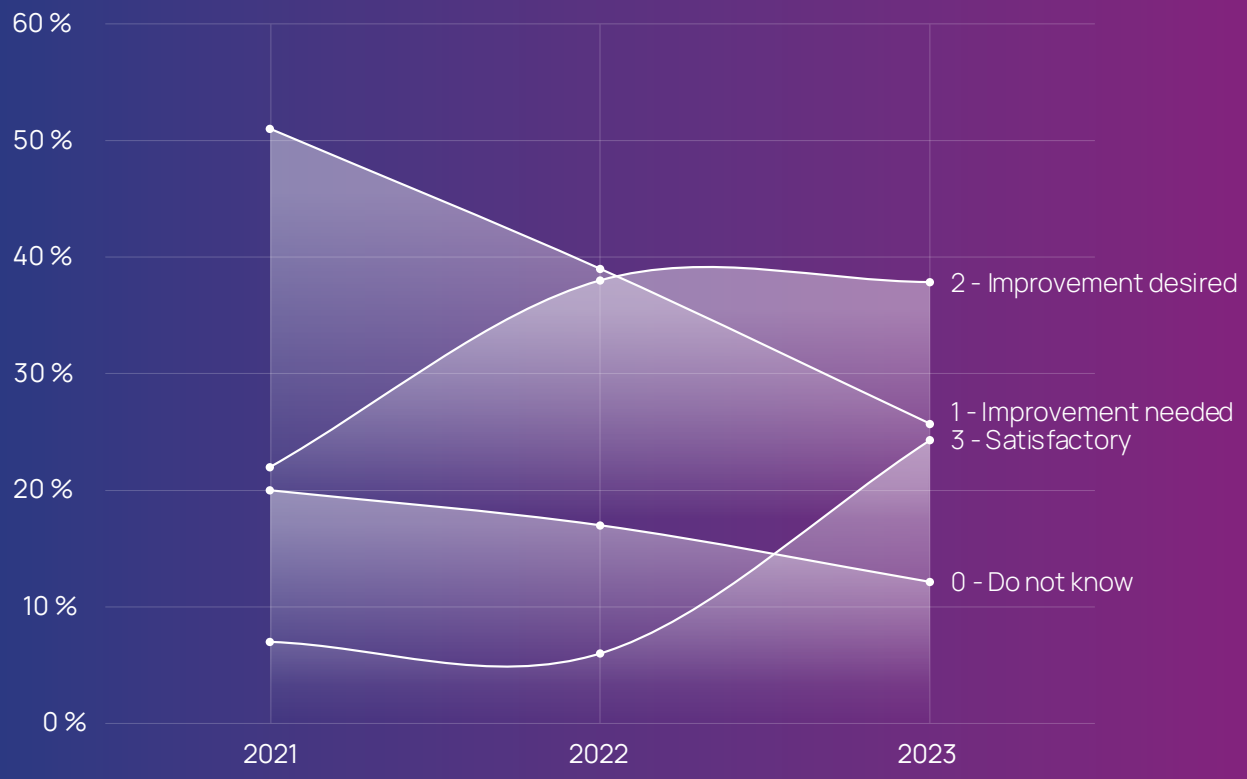
(multiple answers)

The top choice this year is customers. Differentiating between manufacturers and their tiers, we see authorities and horizontal within the industry as the two top choices for OEMs, while suppliers selected their customers (i.e. the manufacturers) and horizontal within the industry most often. Interestingly, "critical suppliers" and "all suppliers" as answer options rank in the bottom half for both OEMs and tiers, in contrast to the rising relevancy of supply chain as an attack vector (see question "What attack vectors …").



19. How do you rate the cyber maturity of your organization's software supply chain? (single answer)

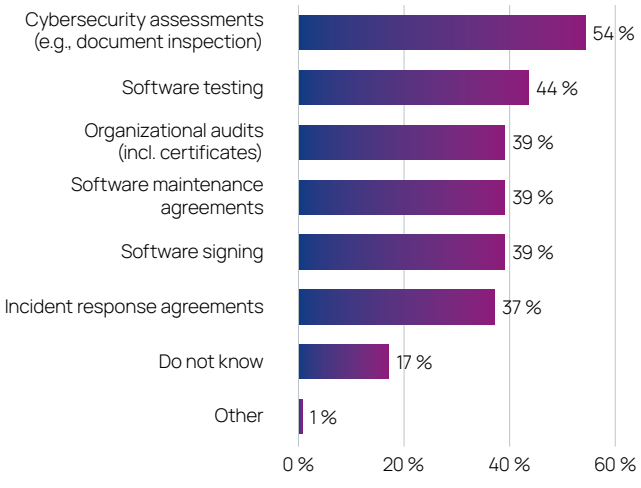
These results might answer why the supply chain is considered as one of the top attack vectors, while suppliers are often not in the scope of ecosystem management (see previous questions): Satisfaction with supply chain maturity is increasing, while the perceived need to improve is decreasing. As with overall cyber maturity in the industry, we note that organizations must ensure that satisfaction does not lead to blind spots that are not yet sufficiently mature (see also next question).



20. What measures does your organization take to secure its software supply chain?

(multiple answers)

All measures but the top one are used by less than half of the participants' organizations. Crucially, software signing as a means to ensure that only tested, released, and authentic software is used in products is selected only by just over one-third of participants. This indicates a heightened risk of vulnerable software in products. Interestingly, responses from employees at OEMs chose the measure of software signing over 50% more often than employees of suppliers.



Contacts & acknowledgements

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

Michael Lüke
Senior Manager
michael.lueke@etas.com

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

The Automotive Cyber Maturity Survey and Report are the work of many people including Beate Boy, Timo Bunghardt, Renee Guo Chen, Julia Faustel, Josephine Förster, Claudia Hartwell, Jan Holle, Huang Mengdi, Marc-Oliver Schandera, Christian Schleiffer, Anna-Lena Sentker, Jeong Seoyeon, Furue Takahiro, Larissa Ulshoefer.
We thank you all!

escar Embedded Security in Cars

The Automotive Cyber Maturity Survey 2023 was supported by escar – the world's leading automotive cybersecurity conference.

Last updated: 10/2023