



Automotive Threat Intelligence

On the road to cyber safety

August 2023

kaspersky

Introduction

Security threats occur every day, arriving in all shapes and sizes and speaking a variety of different languages. As has previously been explored, intelligence into the nature of these threats at the highest level of business has never been more important. But in an increasingly interconnected world where almost all processes are now digitalised and back-office systems opened for previously unimagined purposes, the question for any digitally transforming organisation is: how can we gather enough actionable intelligence to protect ourselves when one device is only as secure as the device to which it is connected?

Nowhere is this truer than the complex and disparate world of automotive where the lack of industry-common requirements and varying nomenclature has meant that suppliers in collaborative relationships often struggle to scrutinise security measures elsewhere along the chain. With the average vehicle containing over 100 control units, each with its own dedicated operating system, the number of potential points for cyberattack is already high and will continue to increase exponentially as further functionality is added.

As a global company with threat intelligence experts active in every region and covering all industry sectors, Kaspersky works extensively in the automotive space supporting organisations across the supply chain. The company has used this experience to undertake research into how the evolving nature of cybersecurity threats are being interpreted by a C-Suite challenged with defending its businesses against them.

An increasing awareness about the urgent need to effectively manage the growing risk on both individual vehicles and the wider mobility ecosystem has led to the creation of new international cybersecurity regulations as set out by the United Nations' Economic Commission for WP.29 (UNECE WP.29), which will become mandatory for all new vehicles produced from July 2024. The impact of the regulation will be felt across the whole automotive supply chain, requiring every component part that goes into the creation of any vehicle containing even the most obscure piece of software to come with evidence that it has been designed with security in mind.

The regulations create an unavoidable need for component suppliers to collaborate with one another on a previously unprecedented scale, but with the deadline to achieve the right level of compliance dropping in less than 12 months, are these businesses sufficiently aware of what it is required, and do they understand why this

represents such a critical step for the industry? More broadly, with so many competing concerns, does the C-Suite really understand the impact and liability that cyber risks are having on them and their organisations? And are they able to focus on the right threats and invest in the right tools to eliminate them?

Our research exclusively reveals an automotive C-Suite that is acutely aware of the cyber threat posed to their supply chain but also one that is being swamped by a tide of competing priorities, unclear processes, and isolated threat intelligence. The findings suggest that while they are aware of the need to address cyber risks, an inability to holistically understand the whole picture is leaving many businesses inadequately prepared for a connected era of automotive where there can be no weak links.

Contents

Key findings	4
Automotive cybersecurity: a snapshot	5
The automotive supply chain is vulnerable	6
Automotive businesses know there is a problem	8
155/156 UNECE WP.29 compliance	9
Kaspersky UNECE WP.29 Checklist	10



Methodology

A total of 200 interviews with C-Level decision makers in large enterprises of 1,000+ employees in the automotive sector were conducted in July 2023. Respondents were asked about cybersecurity within their organisation, the

measures they take to protect themselves, the barriers they face as a management team, and the challenges they face across the automotive supply chain.

Key findings

The automotive C-Suite has major concerns about the potential for criminals to exploit software vulnerabilities in the production of connected cars, with the integration of connected software considered the biggest risk.

- A total of **64% of C-Suite executives** believe the automotive supply chain is currently vulnerable to cyber-attack.
- With this in mind, the **integration of infotainment systems and connectivity technology** supplied by software providers is considered the biggest supply chain risk with 34% of C-Suite respondents listing this as their top concern.

Although cybersecurity is a clear worry, the automotive C-Suite is not currently perceiving enough return on its cyber intelligence investments and struggling to prioritise action due to the confusing terminology used to describe threats.

- The biggest challenge faced by the C-Suite is connecting the implications of their threat intelligence to specific business operations, with **almost a third (29.5%) of respondents**

failing to see value from its current intelligence investments.

- A further **35% of respondents** stated that jargon or confusing terms represent the biggest barrier they face as a management team trying to develop a holistic understanding of the cyber risk.

With key regulation coming into play in less than 12 months' stipulating that every vehicle must be secured throughout its entire lifecycle, from development and production through to customer-use, much of the C-Suite reports being behind the curve.

- **42% of C-Suite respondents** stated that they do not currently have a plan in place ahead of R155/156 UNECE WP.29.
- **63.5% of C-Suite respondents** said they were not currently very involved in planning for upcoming regulations/standards such as R155/156 UNECE WP.29 and ISO 21434, despite 64% of agreeing that dealing with cybersecurity threats are a strategic board issue.
- **Over two-thirds (68.5%) of the C-Suite** thinks there needs to be more understanding across the automotive supply chain of the implications of standards and what it will mean for their businesses.



Automotive cybersecurity: a snapshot

INFLECTION POINT

The automotive industry has passed an inflection point: as connectivity and software-driven processes have become ubiquitous, there is a clear and present danger that privacy – and even consumer safety – is now actively being compromised. While automotive manufacturers are working hard to meet rapidly increasing demand for connected vehicles, the concern is that the cyber risk – something which touches every single component and process across one of the most sophisticated and interconnected supply chains in the world – is being inadequately addressed.

GROWING RISK

The number of automotive cyber incidents is continuing to increase rapidly year on year, with most of the growth stemming from increased hacker activities. Another clear trend is the growth of remote hacks, which includes both web-based and nearby wireless attacks. As far back as 2015, there was a glimpse at what is at stake when two security researchers hijacked a vehicle over the internet. They were able to turn the steering wheel, disable the brakes, and shut off the engine. The implications of this were clear at the time. Now, with many more cars internet-enabled, the risk, not just of hijacking, but of accessing an entire vehicle network, has exploded, and the trend will continue as consumers become more accustomed to the convenience of connectivity.

IMMINENT REGULATION

New cybersecurity regulations set out by UN Working Party UNECE WP.29, R155 and 156, will have a major impact on all aspects of automotive cybersecurity. The product of a United Nations Economic Commission for Europe working party, these regulations come into force from July 2024. A key requirement is that every new vehicle must be secured throughout its entire life cycle, from development and production through all vehicle customer-use phases. This means that all OEMs and their supply chains will be compelled to include multi-layered cybersecurity solutions to protect against current and future cyberattacks or risk ceasing the manufacturing of that vehicle.

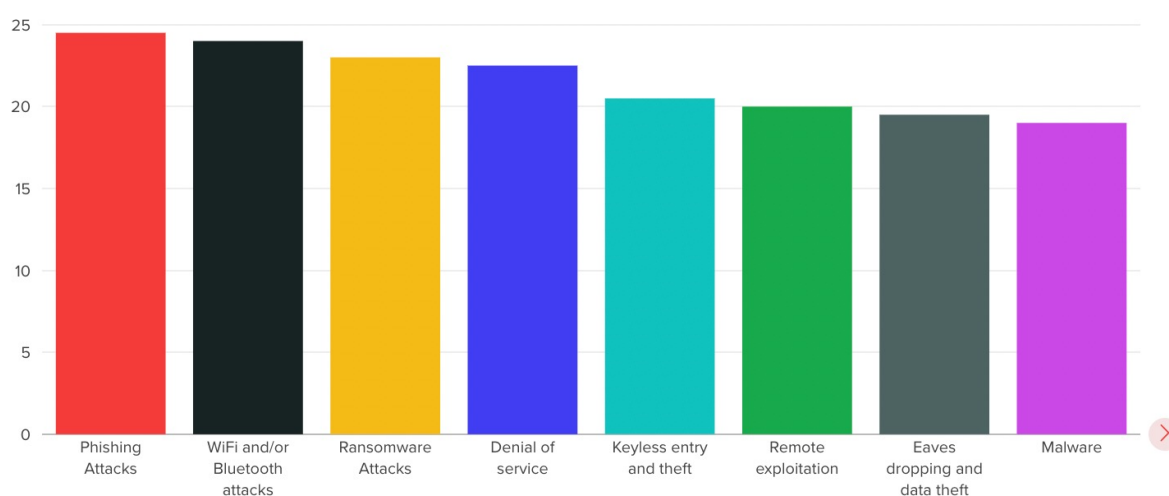
In short, everyone needs to be prepared.

The automotive supply chain is vulnerable and already under attack.

A change is underway in automotive cyberattacks. Such is the ubiquity of connected software across the automotive supply chain, cybercriminals targeting vulnerable suppliers can now gain access to a manufacturer's network and compromise huge numbers

of vehicles with the potential to cost lives. Kaspersky research reveals that the range of attacks, from phishing, ransomware and Wi-Fi/Bluetooth to keyless entry, and theft, occurring every day is vast, from supplier to vendor, at almost every stage of production.

Currently, from an automotive supply chain perspective, what are your biggest cybersecurity concerns?



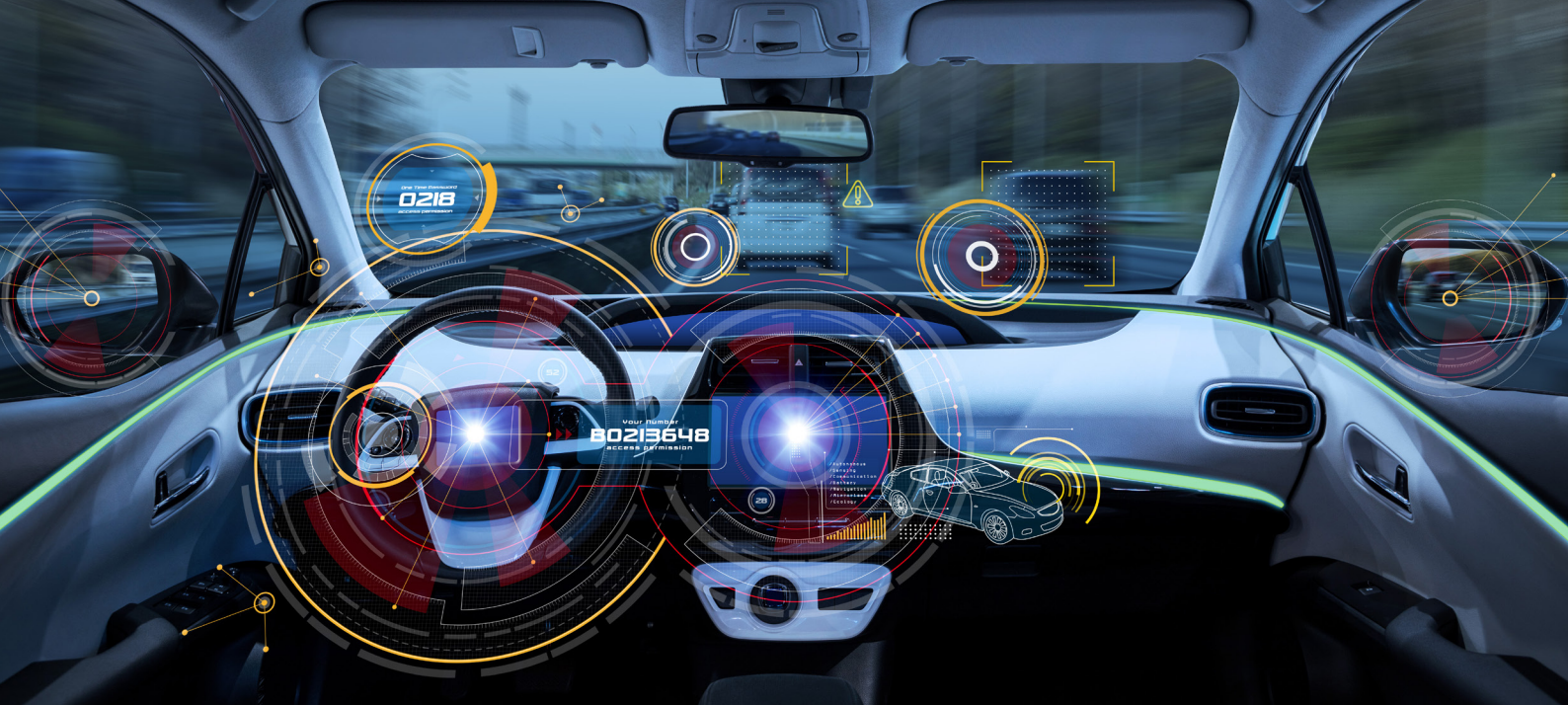
For the C-Suite, the concern is real. Almost two-thirds (64%) of all respondent's state that they believe the automotive supply chain is currently vulnerable to cyber-attack. As the connected-car ecosystem has continued to evolve, so too has the cybersecurity challenge which now extends far beyond simply being an IT issue to touch upon every aspect of vehicle

production. Aware of this challenge, cybercriminals are routinely targeting weak links and looking to exploit system or network vulnerabilities to intrude on the vendor network or gain unauthenticated access permission. Conti, LockBit, and Hive were among the ransomware most commonly found in automotive cyberattacks over the past year.

"The growing use of technology in modern vehicles, the complex supply-chains required in their development and manufacture, and the need to comply with imminent new regulatory requirements have made it essential that decision-makers in the automotive industry understand the cyber-risk their companies face and take steps to ensure that their staff have the appropriate threat intelligence to inform their cyber-security strategy. Failure to do so threatens the security of both their own organisation, and a highly complex, interconnected network of suppliers, manufacturers and service providers that involves the procurement of everything from raw materials and components to the logistics and distribution processes of the vehicles themselves."

David Emm,
Principal Security Researcher, UK&I, Kaspersky





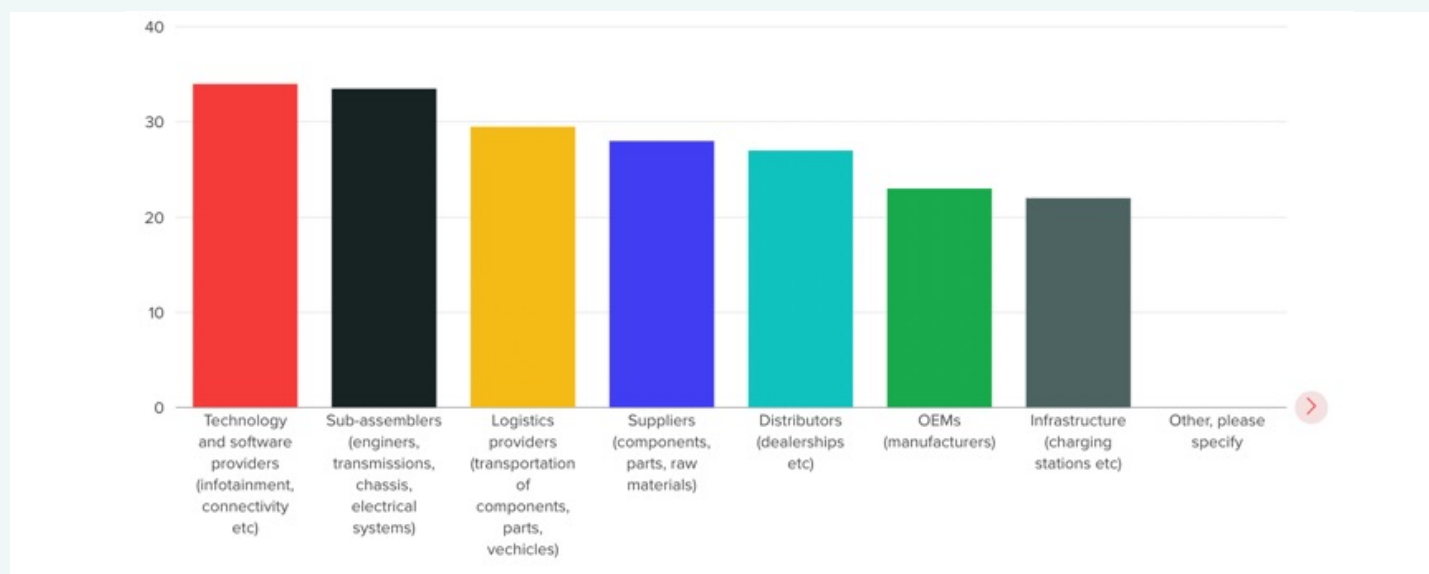
The integration of infotainment systems and connectivity technology provided by software providers is considered the biggest supply chain risk with 34% of C-Suite respondents listing this as their top concern from a cybersecurity perspective. Infotainment systems which include voice control, interactive map access, entertainment options and an increasing array of connected functionality, have become a main selling point, particularly amongst a younger generation of drivers, but they also introduce a range of new vulnerabilities.

Indeed, such is the concern about connectivity that the C-Suite lists connected vehicles, over the air software updates, and vehicle-to-vehicle (V2V) communication as

the biggest (15.5%) automotive cybersecurity challenge over the next two years. However, for a C-Suite that is acutely aware of the risks their businesses are being exposed to, the challenge is developing a holistic approach to defending against these sorts of attacks given that they also cite other pressing cyber issues such as collaboration and information sharing (13.5%), and addressing the cyber skills gap (12%) closely behind.

Simply put, Kaspersky research findings reveal a rapidly evolving, but highly complicated and fragmented automotive threat landscape. This is presenting significant obstacles to the C-Suite developing a comprehensive approach to dealing with the most important cybersecurity issues facing their businesses.

Which points in the supply chain are you most concerned about from a cybersecurity risk perspective?



Automotive businesses know there is a problem but are currently struggling to decipher what to do about it.

Companies in all industries understand the need to address cyber risks, the critical step is moving away from classifying it simply as a technology issue to one that instead covers the whole business. All organisations are now dealing with sophisticated, adept, and opportunistic cybercriminals, and the automotive sector is no different. Simply put, failure to move on from tactics that rely on reactive security and risk management principles will provide inadequate security protections, exposing organisations to unnecessary and significant cyber risk and the consequences of intrusions.

Kaspersky research finds an automotive C-Suite that is struggling to connect the very real implications of their threat intelligence to specific business operations, with almost a third (29.5%) of C-Suite respondents currently not seeing value from their cyber intelligence investments. The data suggests that, for automotive businesses to start seeing true value from their threat intelligence investments, they need to start viewing the challenge more holistically.

The challenge faced by the C-Suite is compounded by ongoing issues associated with interpreting and understanding cybersecurity jargon. 35% of all C-Suite respondents currently believe that confusing industry terms present the biggest barrier to the broader management team's ability to develop a holistic understanding of the cyber risk and, most importantly, what they should do about it.

For a problem that touches everyone, from top to bottom in any organisation, cyber literacy is a critical component if an increasingly interconnected automotive industry is to develop a culture of cybersecurity best practice, share knowledge, and, ultimately, institute actionable intelligence with clear and quantifiable return on investment.

“Protecting business operations while tackling cybersecurity threats has radically changed from basic IT configurations, installing an antivirus, and following best practices, to a whole new level of complex coding, unknown threats, and continuous cyber-attacks. Good intelligence reports and timely warnings are critically important when it comes to helping businesses to prevent and protect their products, IP and, most importantly within the context of the automotive industry, customers' safety. Access to understandable and actionable threat intelligence is now a must have tool to support all businesses on their hunt for the unknown. This is particularly relevant for car manufacturers as cybercriminals turn their focus increasingly towards the automotive industry.”



Clara Wood,
Global Business Development Executive and
Partnership Strategy, Kaspersky



With UNECE WP.29 right around the corner, many automotive businesses need urgent help to get the compliance process started.

With a multitude of cybersecurity standards and frameworks, it has been a challenge for automotive OEMs to develop common platforms. The first-ever regulation requiring vehicle type approval with regards to cybersecurity, UNECE WP.29 delivers a harmonisation of fragmented regulations. Critically for OEMs and their suppliers, any vehicles which are already under development for production from mid-2022 onwards will need to comply with these new regulations. Failure to do so could lead to vehicle production being shut down.

Kaspersky research finds that, although many companies have already begun to map out a timeline implementing changes to their existing supply chains to ensure that new vehicle models will be compliant with UNECE WP.29, the comprehensive nature of the compliance regulations is proving to be a huge roadblock for a lot of businesses. Given the need for OEMs to not just be thinking about their own approach to cybersecurity, but also actively surrounding themselves with proven and trusted suppliers who have security as a core principle for their offerings, it is perhaps surprising that 42% of automotive C-Suite respondents admit to not currently having a plan in place.

Moving forwards, OEMs will require all suppliers to show compliance with the regulations. This means that every component part that goes into a vehicle containing software will need to come with evidence that it has been designed with security in mind – failure to provide this proof will make it impossible for an OEM to accept or integrate the code into their UNECE WP.29 compliant vehicles or risk liability. However, there is a feeling across the industry that the C-Suite needs to know more, with Kaspersky research revealing that 68.5% of executives believe they need to develop a more comprehensive understanding of the regulation and the impact it will have on their businesses.

In short, the automotive C-Suite is currently grappling to put their plans in place before they can execute. The challenge to do so, however, is illuminated by a further 63.5% of C-Suite respondents saying that they are not currently involved in initiatives to implement a UNECE WP.29 strategy. This suggests that responsibility lines, roles, and ownership might be unclear within their organisations and hindering progress towards achieving compliance.


“The security of any supply chain is defined by its weakest part, and the automotive industry is no exception. Delivering secure vehicles in the connected era will require a more tightly integrated set of working relationships across the supply chain, but our research highlights the challenges faced by these businesses. Firstly, in interpreting and actioning appropriate measures to defend against an increasingly varied threat landscape, and secondly, balancing these actions with the necessary steps that will be required to become compliant with industry regulations. The next few months will be critical for suppliers whose solutions are covered by UNECE WP.29 – act now with the right processes in place and there is the potential to forge new long-term relationships to ensure OEMs have complete solutions with the right level of security compliance. Or fail to do so and risk being left behind by an industry which is being compelled to act on the imminent cyber threats they are facing daily.”




David Emm,
Principal Security Researcher, UK&I, Kaspersky




Kaspersky R155/156 UNECE WP.29 Checklist:

- **Get your house in order. Carry out a supply chain risk assessment**


The most important – and often overlooked step – for any organisation. Make an inventory of whom you buy products and services from and where your organisation sits in the supply chain, so you can start drawing a map of potential risks.

You should carry out a thorough audit evaluating your suppliers' cybersecurity credentials, risk management plans and whether or not they scrutinise their own suppliers in the same way. This should give you a good indicator of risk and what processes, products and/or services should be carefully managed.
- **Map and prioritise your cybersecurity governance processes**


It is important to be aware of processes and procedures that will require strict compliance, from the definition of a software update system to product testing and certification. These governance frameworks include all the policies for handling cyber-risk, for the entire lifecycle of the vehicle and the services that are associated with it, going beyond OEMs and vehicle design, to operations, production, maintenance... as well as the decommissioning stage.

An update to a single chipset might not sound as important, but it can introduce new vulnerabilities; as such, any change in the development and design process has to be continuously recorded in a structured and well-defined process across the supply chain, where only affected customers' vehicles can be updated accordingly and users informed on updates required.
- **Establish your security in-vehicle lifecycle**

Prevention is key. It is vital to have a framework whereby training and auditing take place regularly, as well as partnering with a cybersecurity provider that can understand and decode cyberthreats regardless of language or provenance in order for VSOCs to be able to take prompt action.

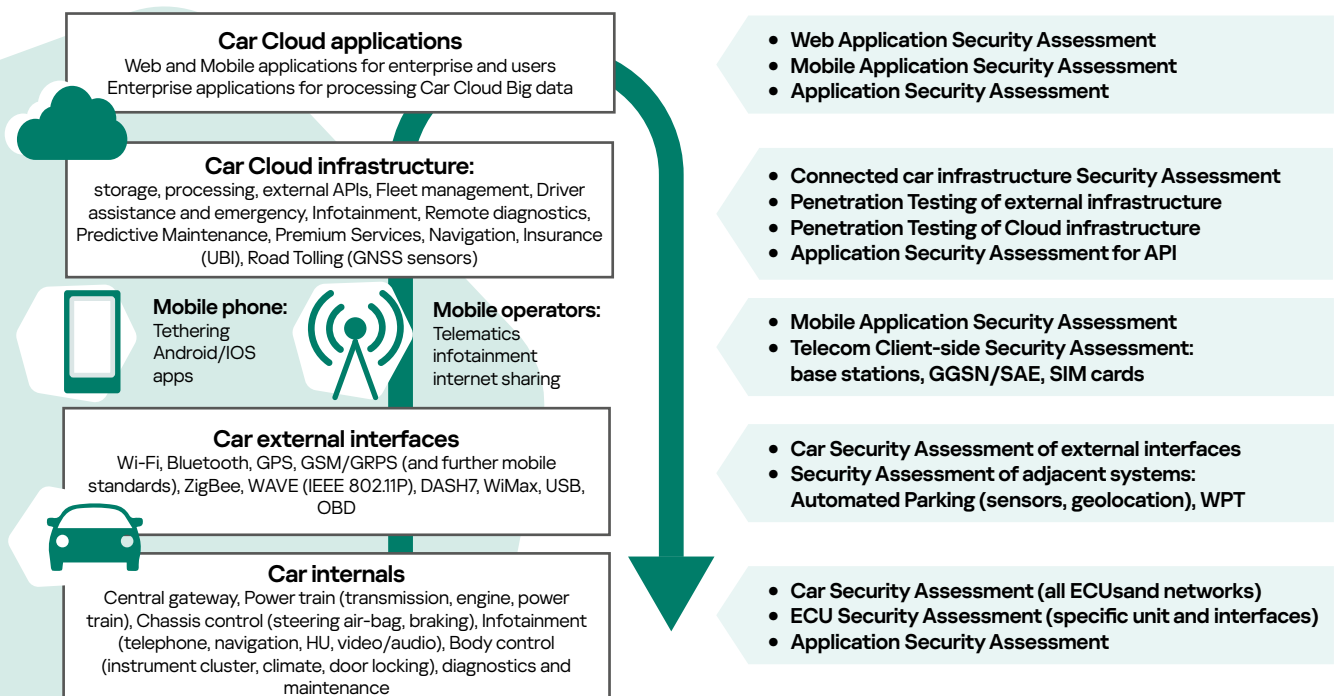
It is advisable to implement cybersecurity solutions that are able to detect any threats that may permeate through the supply chain in real-time, as well as rolling out measures to detect and mitigate cyberattacks while providing evidence that an intrusion has successfully been mitigated for compliance purposes.
- **Vehicle threat monitoring (real-time and offline)**

It is important to be aware of the latest cyber threats that are specific to a certain vehicle type, through regular monitoring and log collection. Monitoring reports can then be sent to the relevant authority that is responsible for approving vehicles for sale (such as the homologation authority) to demonstrate the right steps have been followed.

Threat intelligence plays a key role here, as it enables the business to detect anomalies in the network and getting a preview of any threats targeting specific chipsets, for example components, tools or even suppliers, before a disaster can occur.
- **Take action**

Businesses should develop a robust incident response plan, with a well-prepared – and dedicated – team and clear objectives. This should also include a critical risk mitigation steps in case an attack was to strike.

A cybersecurity partner can ensure the early detection of cyberattacks through firewalling, intrusion detection mechanisms (IDS) as well as network isolation and management, whilst providing forensic data analysis capabilities to break down an attempted attack.





kaspersky

<https://www.kaspersky.com/enterprise-security/threat-intelligence>
<https://www.kaspersky.com/enterprise-security/transportation-security>
<https://www.kaspersky.com/enterprise-security/professional-services>

© 2023 AO Kaspersky Lab.
All rights reserved. Registered trademarks and service marks are the property of their respective owners