2025 | Automotive & Smart Mobility Global Cybersecurity Report

Upstream

MIND THE CYBER GAP

TABLE OF CONTENTS

TABLE OF CONTENTS

OPENING LETTER FROM OUR CEO

I am excited to present the 2025 Global Automotive and Smart Mobility Cybersecurity Report. This report comes at a critical time, as cyber threats are evolving faster than the industry is prepared to handle, outpacing regulation-driven measures.

While UNECE WP.29 R155 compliance, particularly with its 2024 milestone, has brought attention to regulatory adherence, it has also created a false sense of security. Cybersecurity regulations, such as R155, set the minimum required standards but are insufficient to address the dynamic and complex threats confronting our ecosystem.

Through our work with leading OEMs and mobility stakeholders, we've seen escalating cyber risks with serious implications on safety, brand reputation, operational continuity, data privacy, and financial stability. In 2024, ransomware attacks on the Automotive and Mobility ecosystem surged, causing unprecedented disruptions. The rise of software-defined and autonomous vehicles has introduced new vulnerabilities, while the integration of smart mobility devices like EV chargers and fleet systems into critical infrastructure has expanded the attack surface and magnified the stakes.

China's strategic investments and government support have propelled its Automotive industry to a position of global leadership, particularly in the electric vehicle (EV) sector. However, this rapid growth has also spotlighted critical concerns around cybersecurity, data privacy risks, and potential espionage, underscoring the need for urgent action.

Addressing these challenges requires collective action. OEMs, Tier-1, Tier-2 suppliers, and smart mobility providers must go beyond mere compliance. Stakeholders should adopt proactive, data-driven strategies and consistently invest in vSOCs, mobility-centric API security, threat intelligence, and vulnerability management to bridge cyber gaps and enhance resilience. Cybersecurity is no longer just a technical challenge—it is a strategic imperative requiring leadership commitment. By working together, we can strengthen the automotive and smart mobility ecosystem, safeguarding customer trust and ensuring industry success.

At Upstream, we have been at the forefront of securing the connected vehicle ecosystem and mobility assets since 2017, when we first introduced the Upstream Platform. The Upstream Platform has proven instrumental in helping organizations move beyond compliance to proactively monitor and protect millions of vehicles and mobility assets. With advanced AI and ML capabilities and deep industry expertise, Upstream is well-positioned to tackle the challenges ahead. As we navigate 2025 and beyond, we remain committed to leading the charge in securing the future of connected mobility.

Sincerely,

Yoav Levy

Co-Founder & CEO

METHODOLOGY

The Automotive and Smart Mobility ecosystem benefits from Upstream's continuously updated database of cybersecurity incidents, offering a critical resource for staying ahead of cyber threats.

In 2024 alone, Upstream researchers analyzed 409 new incidents, contributing to a total of 1,877 documented cases, some dating back to 2010. By monitoring hundreds of deep and dark web forums, we compiled this comprehensive and actionable report to help you navigate the evolving cybersecurity landscape with confidence. Through our global analysis of automotive cyber incidents, Upstream empowers the entire Smart Mobility ecosystem to understand, mitigate, and defend against both existing and emerging threats.

Upstream's AutoThreat® cyber threat intelligence platform leverages advanced technology, AI, and automations to continuously scan all layers of the web for new cyber incidents related to the Automotive and Smart Mobility ecosystem. The collected data is indexed and analyzed on the AutoThreat® platform, providing a centralized and actionable repository of insights. Our dedicated team of researchers and analysts meticulously categorizes and examines this data to uncover the motivations and activities of threat actors, as well as the impact of cyber threats on mobility assets.

Each incident is enriched with contextual information—such as the attack's geolocation, impact, attack vector, company type, and the required proximity of the attacker to the target. This creates an in-depth and practical repository to help organizations strengthen their security postures.

The incidents analyzed in this report were sourced from diverse channels, including media outlets, academic research, bug bounty programs, verified social media accounts of government law enforcement agencies, the Common Vulnerabilities & Exposures (CVE) database, and other publicly available online sources. Beyond these, Upstream's analysts actively monitor the deep and dark web to track threat actors operating behind the scenes of automotive cyberattacks.

In 2024, our research scope expanded significantly to address the rising risks, the growing number of targeted mobility assets, and the evolution of attack technologies. This expanded effort included tracking 1,133 of the most active threat actors, whose activities are analyzed in a dedicated chapter titled *"Cyber threats from the deep and dark web."* Notably, these incidents are excluded from the statistics and charts presented in other chapters of the report. Please note that when analyzing attack vectors and their impacts, an incident may involve multiple attack vectors and potential impact elements. As a result, the total percentages may exceed 100% across all incidents.

Despite our comprehensive approach, there may be additional incidents and attacks that remain unreported or undiscovered, and therefore not included in this report.

For further insights, a more detailed analysis is exclusively available to AutoThreat® PRO customers.

EXECUTIVE SUMMARY

The Automotive and Smart Mobility ecosystem experienced a sharp increase in cyber threats throughout 2024, with large-scale ransomware attacks causing unprecedented disruption. As cyber risks outpace regulation-driven measures, the growing gap between the risk landscape and organizational resilience has become increasingly evident.

To address this widening gap, organizations must prioritize resilience by investing beyond regulatory compliance. Upstream's 2025 Global Automotive Cybersecurity Report explores this cybersecurity gap, China's expanded EV market share, and the key trends, vulnerabilities, and incidents that shaped the ecosystem in 2024.

In 2024, automotive and smart mobility cybersecurity risk scale and impact continued to expand

The number of incidents with a high-massive impact (thousands to millions of mobility assets) continued to increase between 2023 and 2024, accounting for

OVER 60%

of all incidents

Massive scale incidents more than tripled, accounting for

19%

of all incidents

92%

of attacks were remote

65%

of attacks were executed by black hat actors

Source: Upstream Security

Black hat threat actors are increasingly motivated by the potential of large-scale impact, leveraging the deep and dark web as a fertile ground

70%

of black hat activities had a high-massive impact

OVER 76%

targeted multiple stakeholders and global reach

Source: Upstream Security

China is reshaping global Automotive markets and the cybersecurity landscape

- China's strategic investments and government support have solidified its leadership in the global EV market.
- In 2024, China advanced its automotive regulations with new cybersecurity standards for intelligent vehicles and plans to influence global industry standards.
- In response to rising cybersecurity risks, the US Department of Commerce proposed a rule in September 2024 to ban connected vehicles using certain hardware or software from China or Russia.

To **bridge cybersecurity gaps**, stakeholders must accelerate the adoption of AI-driven detection and investigation capabilities, while improving vSOC monitoring and remediation efficiencies.

01.

THE RISE OF THE AUTOMOTIVE CYBERSECURITY GAP

As the next wave of innovations amplifies risks and impact, while regulatory and cybersecurity fatigue sets in, how can OEMs strengthen their cybersecurity postures and effectively minimize cybersecurity gaps?

AS AUTOMOTIVE INNOVATION EXPANDS THE ATTACK SURFACE, AND FATIGUE SETS IN, OEM CYBERSECURITY POSTURES ARE ERODING

For the last few years, innovative software-defined and autonomous technologies, coupled with the adoption of advanced IoT technologies in the Automotive and Smart Mobility ecosystem, have resulted in growing regulatory pressures. Automotive stakeholders are challenged with preparing for new regulations, standards, guidelines, and the need to develop new best practices. According to research by BlackBerry QNX, the demand for rapid innovation weighs heavily on automotive software teams, as 75% of software developers admit deadline urgency often compromises functional safety.[1] Ultimately, software development and cybersecurity teams are pressured to innovate quickly and comply with ever expanding regulations, which introduces a continuous conflict.

In 2024, many OEMs and their suppliers continued their heightened focus on implementing UNECE WP.29 R155 for Cyber Security Management System (CSMS) and Type Approval[2] —which became mandatory for all new vehicles in production starting July 2024—as well as R156 for Software Update Management System (SUMS),[3] and ISO/SAE 21434,[4] as part of the global effort to create a unified approach to protecting connected assets against cyber threats.

Historically, periods of heightened focus on compliance activities to meet a regulatory deadline often result in some type of end-user desensitization or fatigue—which often undermines the effectiveness and intended outcome of the regulation. **In the case of cybersecurity fatigue, security postures decline once regulatory compliance is achieved, leaving organizations vulnerable to cybersecurity threats.**

This type of behavior has been observed following the adoption of other laws such as GDPR[5] and CCPA[6] in consumer privacy, HIPAA[7] in healthcare, PCI DSS[8] in payments, and NERC CIP[9] in utilities.

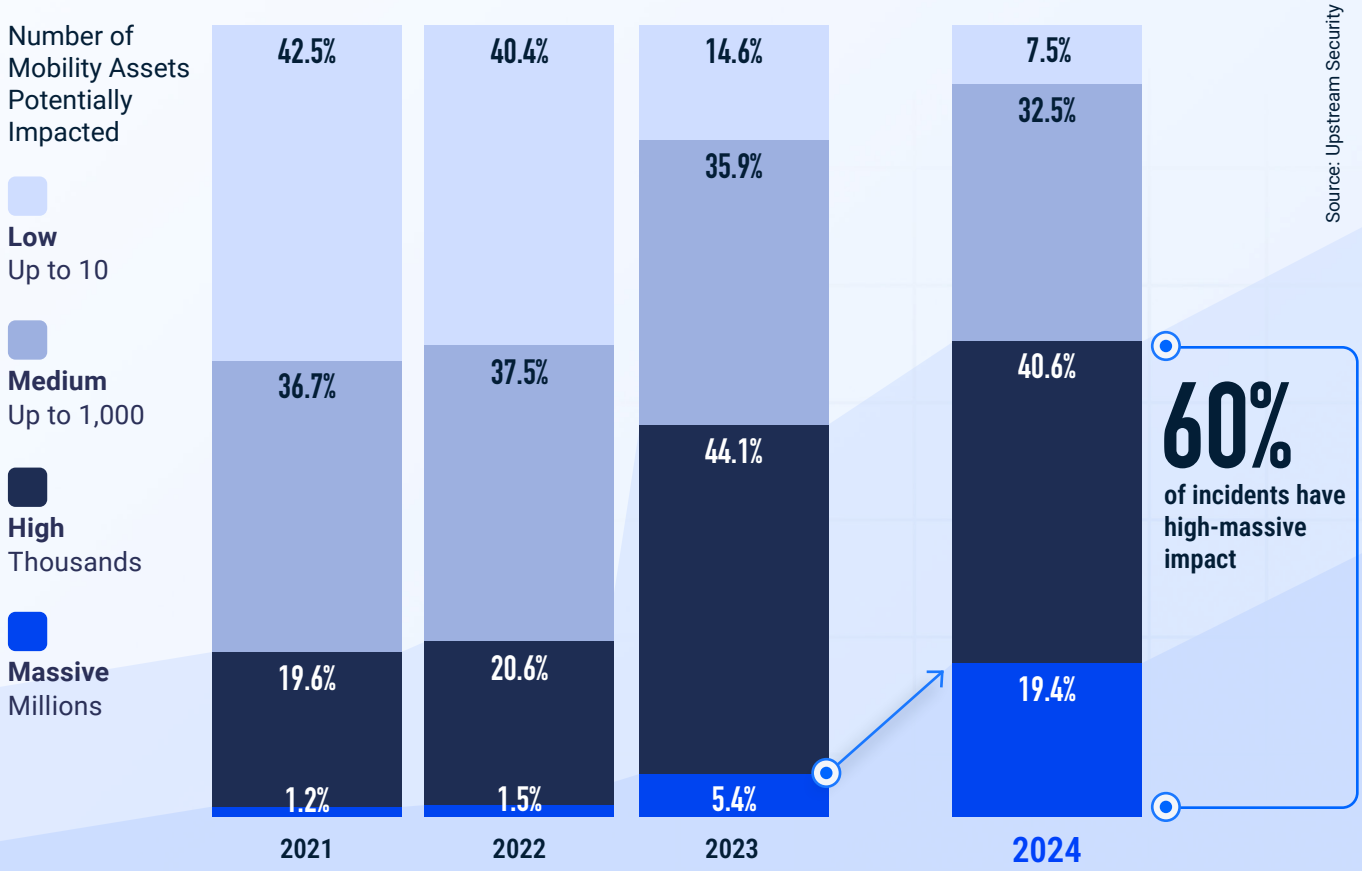
Take GDPR for example. In the six years since it came into force, it has raised awareness of personal data protection rights and made data privacy and compliance board-level issues—but it has also led to consent fatigue, weakening the effectiveness of the consent mechanism, and undermining privacy protection and trust in data processing. Additionally, the prioritization of non-compliance and fine enforcement over outcome is not indicative of effective regulation.

The same is true for the Automotive and Smart Mobility ecosystem, where today, a sense of compliance has led to the illusion that current cybersecurity postures are enough—despite cyber incidents increasing in risk and impact, with severe safety and trust, operational availability, data privacy, and financial implications.

In January 2024, Upstream's Global Automotive Cybersecurity Report declared 2023 as the automotive cybersecurity inflection point, and examined how cybersecurity risks have evolved from experimental hacking into large-scale automotive attacks.

Upstream data revealed that the proportion of incidents with a "High" (thousands of mobility assets) or "Massive" (millions of mobility assets) impact continued to increase between 2023 and 2024, accounting for nearly 60% of all incidents.[10]

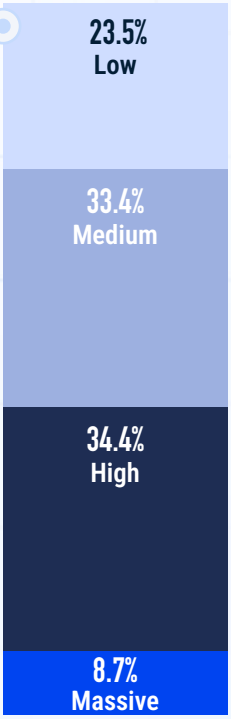
Breakdown of publicly disclosed cybersecurity incidents by potential scale, 2021-2024:



Additionally, Upstream's study of 1,133 of the most active threat actors on the dark and deep web found that threat actor motivation has shifted to scale and massive impact:[11]

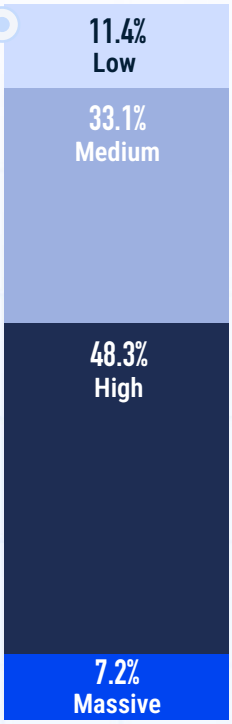
> ***In 2024, 43% of deep and dark web cyber activities had the potential to impact thousands to millions of mobility assets.***

Breakdown of deep and dark web threat actors activities by scale, 2024



Source: Upstream Security

Breakdown of black hat and fraud operators activities by scale, 2024



Source: Upstream Security

> ***When zooming in on black hats and fraud operators, 56% had the potential to impact thousands to millions of mobility assets.***

Black hat and fraud operators activity targets, 2024

55% of black hat and fraud activities on the deep and dark web during 2024 involved multiple OEMs or have global reach.

46.7%
Global

8.3%
Several OEMs/ Stakeholders

45.0%
Single OEM /Stakeholder

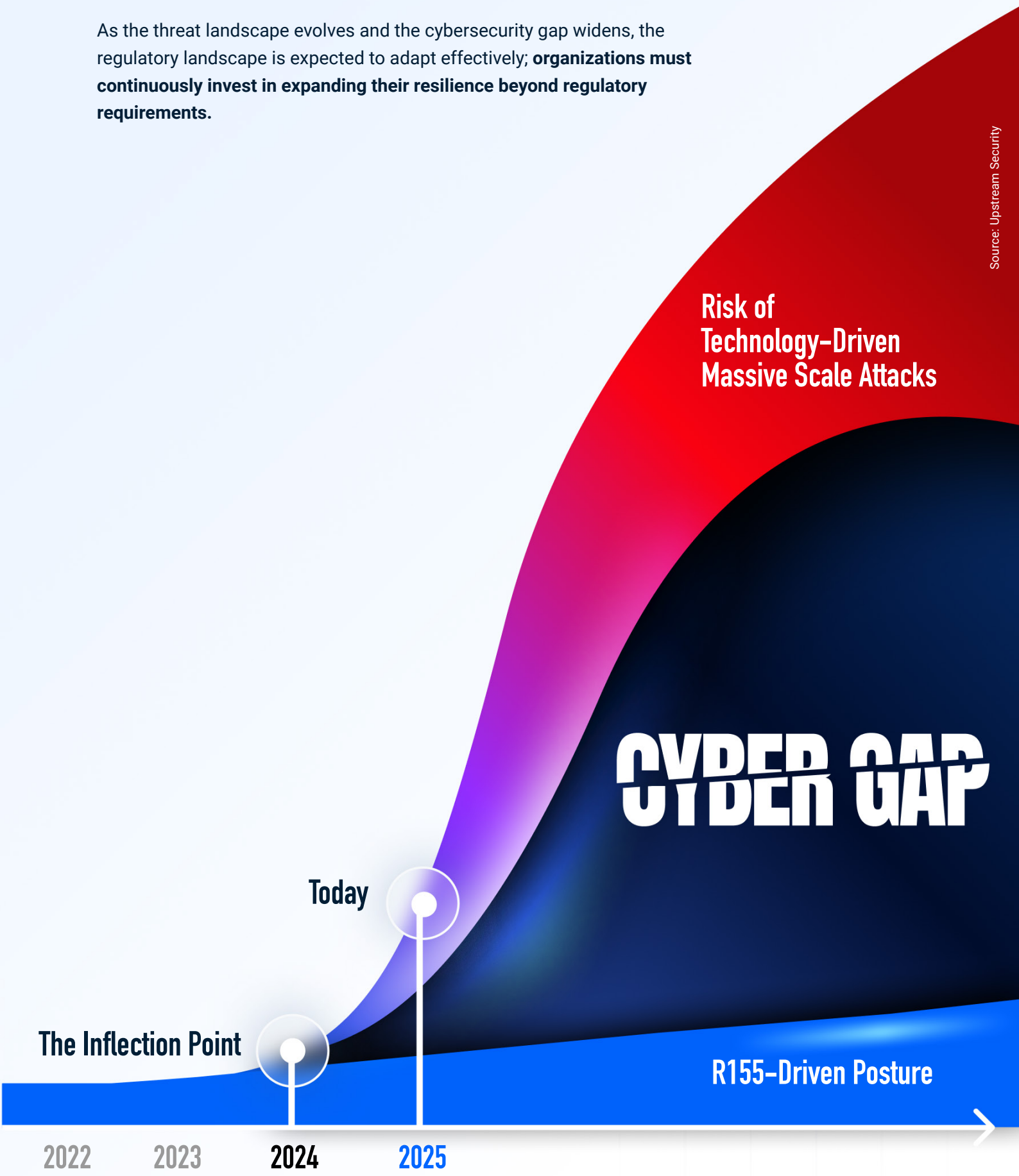
Source: Upstream Security

The rise in large-scale incidents can be attributed to several factors that point to an emerging cybersecurity gap:

- API connectivity between vehicles and multiple devices and apps (e.g., OEM companion app, charging app, dealerships, smart mobility, etc.) lowers the cyber attack threshold and represents a prime attack vector for large-scale remote attacks.
- The introduction and rapid innovation related to Software-defined Vehicle (SDV) and Autonomous Vehicle (AV) technologies that enable remote access to core vehicle functionality and result in massive-scale attacks.
- With constantly expanding attack surfaces, lower attack thresholds, and a variety of attack methods, attackers can launch a wide range of attacks.
- AI-based automation of attack processes and preliminary research offers threat actors the ability to design attacks at scale quickly and with less resources.
- Ransomware as a service (RaaS) and data exfiltration attacks are relatively easy to execute, and provide immediate financial and reputational benefits to attackers.
- Overburdened IT and product cybersecurity teams focused on regulatory compliance, coupled with increasingly complex IT, OT and product environments, provide ample opportunities for attackers to exploit.

THE AUTOMOTIVE CYBERSECURITY GAP

As the threat landscape evolves and the cybersecurity gap widens, the regulatory landscape is expected to adapt effectively; **organizations must continuously invest in expanding their resilience beyond regulatory requirements.**



THE YEAR OF RANSOMWARE: LARGE-SCALE RANSOMWARE ATTACKS WITH UNPRECEDENTED IMPACT DOMINATED 2024

As the Automotive industry rapidly integrates advanced technologies such as software-oriented architectures, autonomous driving, electric vehicles, and aftermarket IoT devices —the impact of the misalignment between current regulatory-driven cybersecurity postures and real-world threats becomes increasingly evident.

> ***One of the biggest threats to enterprise and product cybersecurity is ransomware, perhaps the most defining cybercrime of the past decade, and it continues to grow every year.***

Ransomware attacks have serious financial implications, including lost revenue from service and business disruption, ransom payments, high recovery costs, legal and regulatory compliance issues, and fines due to data and privacy breaches, as well as brand and reputation damage. **But when it comes to product cybersecurity, especially in the Automotive and Smart Mobility ecosystem, ransom attacks have direct implications on safety, uptime, and operational availability and efficiency—as well as significant risks to sensitive data.**

The adoption of Ransomware as a Service (RaaS), a ransomware distribution model similar to cloud computing models (e.g., Infrastructure as a Service and Platform as a Service) where ransomware providers maintain infrastructure and services and charge customers for access, has been a major factor in ransomware's continued growth and success.

The escalating geopolitical tensions have increasingly brought nation-state threat actors into the ransomware spotlight. In April 2024, the US Department of the Treasury sanctioned two companies and four individuals involved in malicious cyber activity on behalf of Iran, targeting more than a dozen US companies and government entities through cyber operations, including ransomware, spear phishing and malware attacks.[12] The four individuals were also indicted by the US Department of Justice for their role.[13] In July, a North Korean national was indicted for his involvement in a conspiracy to hack and extort US hospitals and other health care providers.[14]

In August, the Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Defense Cyber Crime Center (DC3) released a joint Cybersecurity Advisory (CSA) warning that a group of Iran-based threat actors continues to exploit US and foreign organizations.[15]

In 2024, attackers found new ways to hack into systems (e.g., new techniques that enable new zero-day exploits, edge device exploits, GenAI-based automations, etc.); focused their efforts on big-game hunting (e.g., large, high-value organizations or high-profile entities); increased targeting of operational technology (OT) and connected devices; and had greater concentration on data exfiltration—increasingly used in the Automotive and Smart Mobility ecosystem and driving the growth of ransomware economy in 2024, especially with the introduction of laws such as the US SEC's cybersecurity incident disclosure rules,[16] and the EU's NIS 2 cybersecurity directive.[17]

Stricter cybersecurity reporting requirements and large regulatory fines change ransomware dynamics. Attackers can inflict financial and reputational damage without encrypting data and shutting down operations, and victims can no longer ignore attacks and avoid reporting incidents.

Traditional ransomware extortion tactics, where attackers encrypt critical data, shutdown the victim's operation, and extort them with the threat of releasing sensitive data (e.g., double extortion) have proven less effective for attackers—data encryption is resource-intensive and many organizations can restore their data from backups.

In September 2023, a leading US-based trucking and fleet management solutions provider experienced a prolonged double extortion attack that resulted in customers being unable to electronically log their on-road hours—as required by federal regulations—or track their transported inventory.[18]

In response, the company hired external cybersecurity experts to investigate and applied for a waiver from the US Federal Motor Carrier Safety Administration to allow truckers to use paper logs until service was restored.[19]

In November 2024, the same company was reported to have experienced a massive data breach when a threat actor advertised on a dark web forum that he accessed and exfiltrated over 70TB of sensitive data from the company's systems. The threat actor shared evidence and samples of the stolen data to prove his claims. A copy of the data was offered for sale for $30,000, with a negotiable price of $100,000 to remove the data.[20]

By shifting focus from data encryption to data exfiltration and creating data-leak marketplaces—where stolen data is sold to the highest bidder—attackers reduce attack overhead and improve their overall efficiency and return on investment.

According to research by Check Point, global ransomware attacks increased by 30% in Q2 2024—the highest increase in two years. **In terms of industry impact, the manufacturing sector was the most affected, representing 29% of publicly known ransomware attack victims globally, with a significant 56% year-over-year increase. The transportation sector experienced a 40% increase. The communications and utilities industries, both of which rely heavily on IoT and are closely tied to the mobility ecosystem, have experienced dramatic increases in ransomware incidents, 177% and 186%, respectively.**[21]

In 2024, AutoThreat® researchers detected 108 mobility-specific ransomware attacks and 214 data breaches, which contributed heavily to the rise in cybersecurity incidents in the mobility ecosystem.

Most notably, in mid-June, a ransomware attack on a leading US-based provider of dealership management software used by 15,000 dealerships, resulted in shutting down dealer operations for nearly 3 weeks. According to a report from CNN citing multiple sources, the company likely paid the $25M ransom to expedite recovery and end the outage.[22]

> ***The Anderson Economic Group (AEG) estimated that total direct losses to franchised auto dealers reached $1.02 billion.***[23]

AEG's figure includes lost earnings from the approximately 56,000 new unit sales that AEG estimated were lost during the three-week period; lost earnings on used car sales; lost earnings on parts and service; additional staffing and IT service costs; and additional floor plan interest costs on inventory. Damages to consumers, reputational damages to dealers, litigation costs, and other categories of damages are excluded.

IN 2024, AUTOTHREAT® RESEARCHERS DETECTED

108

MOBILITY-SPECIFIC RANSOMWARE ATTACKS AND

214

DATA BREACHES

Here are a few more examples from 2024:

- In February, Japanese OEM US division allegedly hit by a ransomware attack resulting in data theft of 22GB of sensitive vehicle and customer information[24]
- In February, South Korean OEM hit by large-scale ransomware attack disrupting operations[25]
- In March, Chinese Tier-2 supplier was hit by a ransomware attack leading to a major breach of 1.2TB of data, impacting Chinese and global OEMs[26]
- In April, Italian branch of a German OEM experienced a data breach compromising customer PII[27]
- In July, Indian OEM hit by a ransomware attack resulting in company data theft[28]
- In August, South Korean automotive supplier was hit by a ransomware attack, resulting in 2.3TB of company data compromised[29]
- In September, Chinese Tier-1 specializing in automotive CAN BUS protocol solutions was hit by a cyberattack disrupting its website operations[30]

Cybersecurity risk is likely to be dramatically altered by the proliferation of SDV and AV technologies

The convergence of technologies known collectively as ACES—Autonomous Driving, Connectivity, Electrification, and Shared Mobility—has forced stakeholders to move from the traditional hardware-defined architecture to a software-oriented architecture, presenting growing cybersecurity challenges.

APIs have been playing a key role in increasing connectivity between in-vehicle components, backend systems and applications. As more functionality has been exposed through APIs, cybersecurity risks have also increased dramatically, while attack costs and thresholds have decreased.

The ability to control software components and exploit vulnerabilities poses a significant threat to the cybersecurity posture of fleet-wide control systems, opening the door for exponential growth in the scale and impact of attacks.

Frequent OTA updates mean the SBOM is no longer static—but rather constantly evolving long after a vehicle leaves the factory. Risk profiles continuously change, constantly requiring risk and vulnerability analysis—but they can be remediated in real time as well.

Furthermore, modern SDV attack surfaces go beyond in-vehicle components to include charging points and networks, as well as 3rd-party applications for smart mobility, OEM services, telematics devices, and electric vehicle (EV) charging—adding even more complexity.

Finally, the vast amount of data generated by SDVs and AVs and stored in backend systems, presents an additional risk. Backend systems (e.g., telematics servers and applications) play a crucial role in delivering advanced connected vehicle functions and services, as well as collecting and managing huge amounts of sensitive data related to vehicle state, location, usage patterns, and driver behavior.

Attackers can tap into this data, which contains the PII of millions of automotive users, without even needing to hack the actual vehicles. The threat of cyberattacks on backend servers is particularly high because of the ability of malicious threat actors to impact entire fleets, both in terms of control and data access.

The growing reliance on software-oriented architectures, APIs, and backend systems highlights the urgent need for OEMs to safeguard the software services, components and the sensitive data stored in their backend systems.

As SDVs and AVs become more prevalent, the cyber posture balance is likely to change dramatically, further widening the cybersecurity gap.

SDV and AV technologies are vulnerable to a wide range of cyber attacks

Software-defined and autonomous vehicles provide remote access to core vehicle functionality, allowing hackers to effectively attack at scale.

In 2024, security researchers discovered and exploited numerous vulnerabilities in software and hardware components used in SDVs and AVs—such as LiDAR sensors, radars, cameras, high-accuracy positioning hardware, OEM applications, and software development platforms—often directly affecting the safety and operational reliability of vehicles.

In February 2024, security researchers from Duke University could trigger hallucinations in AV sensor systems without prior knowledge of the radar system in use. In one demonstration of the attack, called MadRadar, researchers caused a hallucination in a Doppler radar system, causing it to mistakenly believe that a vehicle traveling away from the sensor turned around and was on its way to a head-on collision. According to the researchers, MadRadar detects and learns radar types "in microseconds" and adapts its attack instantly. **This type of attack can be used to fool adaptive cruise control systems that use radar, into thinking the car in front of it is speeding up, when it is not, resulting in a frontal collision.**[31]

In March 2024, security researchers from the University of California–Irvine and Japan's Keio University detected 15 vulnerabilities in 9 commercially available, first- and next-gen LiDAR systems that can allow direct spoofing of fake cars and pedestrians and the vanishing of real cars in the AV's eye. These attack capabilities on LiDAR sensors can be used to directly trigger various unsafe AV driving behaviors such as emergency brakes and front collisions.[32]

In May 2024, security researchers from Singapore proved that it was possible to interfere with AVs by exploiting their reliance on camera-based computer vision, making them ignore road signs using LEDs. The researchers were able to distort the appearance of road signs repeatedly in a stable manner, ensuring that every frame captured was distorted. The team tested their system using a real road and car with a camera used by a prominent Chinese AV developer. Two versions of this stabilized attack were developed by the team. GhostStripe1, which does not require access to the vehicle, employs a tracking system to monitor the target vehicle's real-time location and dynamically adjusts the LED flickering accordingly to ensure a sign isn't read properly. GhostStripe2 requires access to the vehicle and involves placing a transducer—an electronic device that converts energy from one form to another—on the power wire of the camera to detect framing moments and refine timing control. The researchers claim GhostStripe1 and GhostStripe2 had success rates of 94% and 97%, respectively.[33]

In May 2024, security researchers from the University of Buffalo uncovered a vulnerability in multi-sensor fusion systems—a technology that integrates data from LiDAR, cameras, and radar sensors, and is commonly used in AVs. The researchers introduced a sophisticated attack method capable of simultaneously compromising all three sensor types using a single adversarial object. This object can be easily and inexpensively fabricated, allowing the attack to be executed with a high degree of stealth and flexibility. By deploying just two small adversarial objects, the researchers demonstrated that the attack could effectively render a target vehicle invisible to the victim AV's perception systems.[34]

Multi-sensor fusion has long been considered an adequate cybersecurity counter measure as multiple sensor types provide redundancy, compensating for any compromised sensor. The researchers findings show that this is no longer the case—with attackers capable of simultaneously compromising multiple sensor types.

In June 2024 (published in September 2024), security researchers discovered vulnerabilities in a Korean OEM's dealer API, allowing them to take over vehicles using only their license plates.

The researchers went as far as building a proof-of-concept attack UI consisting of a VIN Retriever tool that converts license plate number to VIN using a third-party API; an Exploit module which can be used to takeover a victim's vehicle—or passively steal vehicle owner PII including name, email and phone number; and a Garage module, which can be used to issue commands and locate impacted vehicles.[35]

According to the researchers, "from the victim's side, there was no notification that their vehicle had been accessed nor their access permissions modified. An attacker could resolve someone's license plate, enter their VIN through the API, then track them passively and send active commands like unlock, start, or honk."[36]

The researchers informed the OEM, which fixed the vulnerabilities and validated that they were never exploited maliciously. **This incident highlights the massive impact of API vulnerabilities and demonstrates how they would affect SDVs at scale.**

In June 2024, a security researcher identified a severe vulnerability, identified as CVE-2024-35213 and assigned a CVSS score of 9.0 (critical), in the SGI Image Codec of a popular vehicle software development platform used in various automotive parts including infotainment, ADAS, telematics, and autonomous driving. Successful exploitation of CVE-2024-35213 could lead to software-driven system crashes, disruptions in image processing services, or the execution of unauthorized code.[37]

In September 2024, security researchers published research investigating the impact of Denial of Service (DoS) attacks, specifically Internet Control Message Protocol (ICMP) flood attacks, on Autonomous Driving (AD) systems, focusing on their control modules. Two experimental setups were created: the first involved an ICMP flood attack on a Raspberry Pi running an AD software stack, and the second examined the effects of single and double attacker ICMP flood attacks on a Global Navigation Satellite System Real-Time Kinematic (GNSS-RTK) device for high-accuracy positioning of an autonomous vehicle that is available on the market. DoS attacks only had a marginal impact on the AD stack, indicating a degree of resilience to these types of attacks. GNSS devices, however, showed significant vulnerabilities: under DoS attacks, sample rates dropped to about 50% and 5% of the nominal rate, respectively, for single and double attacker configurations.[38]

The results of this research have significant implications, as it shows that while the AD software stack can handle DoS attacks with minimal performance degradation, critical external components like GNSS-RTK devices are highly vulnerable. The GNSS system's vulnerability highlights a critical gap in AD system resilience, especially for real-time positioning hardware that could lead to incorrect vehicle positioning, directly affecting the safety and operational reliability of autonomous vehicles.

Recently and with the rising impact of geopolitical conflicts, Upstream's vSOC team identified GNSS spoofing at multiple OEMs across various regions worldwide.[39] False coordinates negatively impact consumer experience of being unable to properly track their vehicles, but may also disrupt customer operations, particularly related to fleet management.Furthermore, GNSS spoofing may introduce safety risks, for example preventing first responders from providing assistance in case of an accident due to false location coordinates.[40]

Ransomware may soon extend beyond enterprise IT systems to affect products, OT, and Smart Mobility devices

IoT enhances operational technology in smart mobility by enabling seamless communication between devices and systems. For instance, in vehicle assembly lines, IoT-connected nutrunners ensure precise torque applications, improving the efficiency and accuracy of the manufacturing process. Similarly, electric vehicle supply equipment (EVSE) interfaces with IoT systems to manage charging schedules and optimize energy consumption, ensuring that electric vehicles are charged efficiently and without overloading the grid.

In January 2024, security researchers discovered 25 security vulnerabilities in a widely used cordless, handheld pneumatic torque wrench (also known as a nutrunner) designed for safety-critical tightening operations in automotive production lines. Exploiting the vulnerabilities could allow unauthenticated attackers to take complete control of a nutrunner.

Lab tests showed how an attacker could launch a ransomware attack that involves making the device inoperable and displaying a ransom message on its built-in screen— such an attack can also be automated to hack all of a company's nutrunners, causing significant disruption in the production line. In another simulated attack scenario, the attacker changes tightening program configurations, specifically the final torque value applied to mechanical fastenings—which is calculated and engineered to ensure that the overall design and operational performance of the device is met—potentially resulting in mechanical failure, excessive warranty claims and reputational damage.[41]

In February 2024, a Russian hacktivist group allegedly gained unauthorized access to the data and app control panel of a state-controlled Lithuanian EV charging service. In exchange for ceasing the attacks and not leaking user data, the group demanded a ransom—the company refused, which resulted in the leak of data on over 20,000 customers, including names, email addresses, and a list of user authentication (RFID) tokens. Some users of the EV service were disconnected from the app, unable to charge their electric vehicles, and all the company's charging points in Lithuania were disconnected. All services were restored a few hours later.

In February 2024, a city in Ontario, Canada, was hit by a ransomware attack leading to a near-complete shutdown of the city's phone lines and online systems, impacting everything from transit systems, engineering services, and child care to cemeteries, libraries, city maps, public health records, and property taxes and vendor payments. City officials confirmed the attack and stated they are consulting with local authorities to investigate the incident, and cybersecurity experts to restore system functionality.[42]

SMART MOBILITY DEVICES EXPAND INTO CRITICAL INFRASTRUCTURE: THE NEXT FRONTIER IN AUTOMOTIVE & SMART MOBILITY CYBERSECURITY

The growth in Smart Mobility devices, including telematics fleet and inventory management systems, cameras, EV charging infrastructure, agriculture and heavy machinery devices, etc., ushers in a new era of cybersecurity risks on a massive scale, with a wide range of devices vulnerable to attacks such as EV charging equipment and infrastructure, autonomous systems and self-driving kits, traffic control systems, telematics systems, fleet management solutions, and smart agricultural equipment.

The attacks and vulnerabilities below highlight the significant cyber risk to Smart Mobility devices and their direct impact on the safety, data and operational availability of vehicles and Smart Mobility systems.

In February 2024, the UK's Office for Product Safety and Standards (OPSS) suspended sales of Spanish EV chargers for failing to comply with current cybersecurity regulations, raising concerns over potential risks to the national energy infrastructure.[43] Hackers might gain access to thousands of non-compliant chargers and switch them all on at once, generating peak demands that disrupt the grid. The company, which has sold 40,000 units in the UK and over half a million worldwide, was allowed to continue to sell the chargers in the UK until June 30, 2024.

The incident illustrates how EVSE vulnerabilities can be exploited to control and manipulate EV charging systems, damaging the local power grid, causing service disruption, and potentially affecting the national grid.

In March 2024, security researchers from Colorado State University showed how ELDs can be accessed over wireless connections (e.g., Bluetooth or Wi-Fi) to take control of a truck, manipulate data, and spread malware between vehicles.[44] Researchers found that ELDs are distributed with default firmware settings with considerable security risks. They also use the CAN BUS to communicate, feature an exposed API for OTA updates, predictable identifiers, and weak passwords—simplifying unauthorized connections and access to vehicle systems for attackers in wireless range. Security researchers successfully connected to a truck's Wi-Fi within 14 seconds, re-flashed the ELD, and sent malicious CAN messages, causing the truck to slow down.

There are nearly 14 million commercial medium and heavy-duty trucks in the US,[45] all of which are required to have ELDs, which poses a serious security risk for commercial fleets, their safety and operational availability.

The researchers reported the findings to manufacturers and the US Cybersecurity and Infrastructure Security Agency (CISA), highlighting the potential for widespread disruptions.

In May 2024, a German agricultural machinery manufacturer suffered a cyber attack that impacted locations worldwide, forcing the company to halt production operations, shut down all IT systems, and call in an external team of specialists. The extent of the attack is unclear, but as of May 29th, the company issued a press release stating that they have been able to resume production. However, the company was still in emergency mode and was expected to have 100% process performance available again within four weeks.[46]

In May 2024, a prominent European vehicle tracking and fleet management device provider suffered a data breach.[47] The data breach, disclosed on a dark web forum, exposed a vulnerability in the company's internal systems, compromising sensitive information including GPS IMEI numbers, real-time vehicle tracking data, billing details, and customer account information. The attacker indicated he had access to all of the company's internal systems, across more than 40 countries and over 5,000 companies.

In July 2024, a security researcher discovered a vulnerability, known as CVE-2024-38944, within the web-based UI on Traffic Controllers produced by a Norwegian-based traffic management company. The vulnerability enabled him to gain full control of a Traffic Controller, modify the configuration of a traffic intersection and traffic light sequences, or trigger the intersection to go into 4-way flash, causing a denial of service and causing traffic congestion and safety risks. The issue results from the lack of authentication before allowing access to functionality and highlights concerns with the security of Intelligent Transportation System Protocols (NTCIP) and the risks of unsecured network management protocols like Simple Network Management Protocol (SNMP).[48]

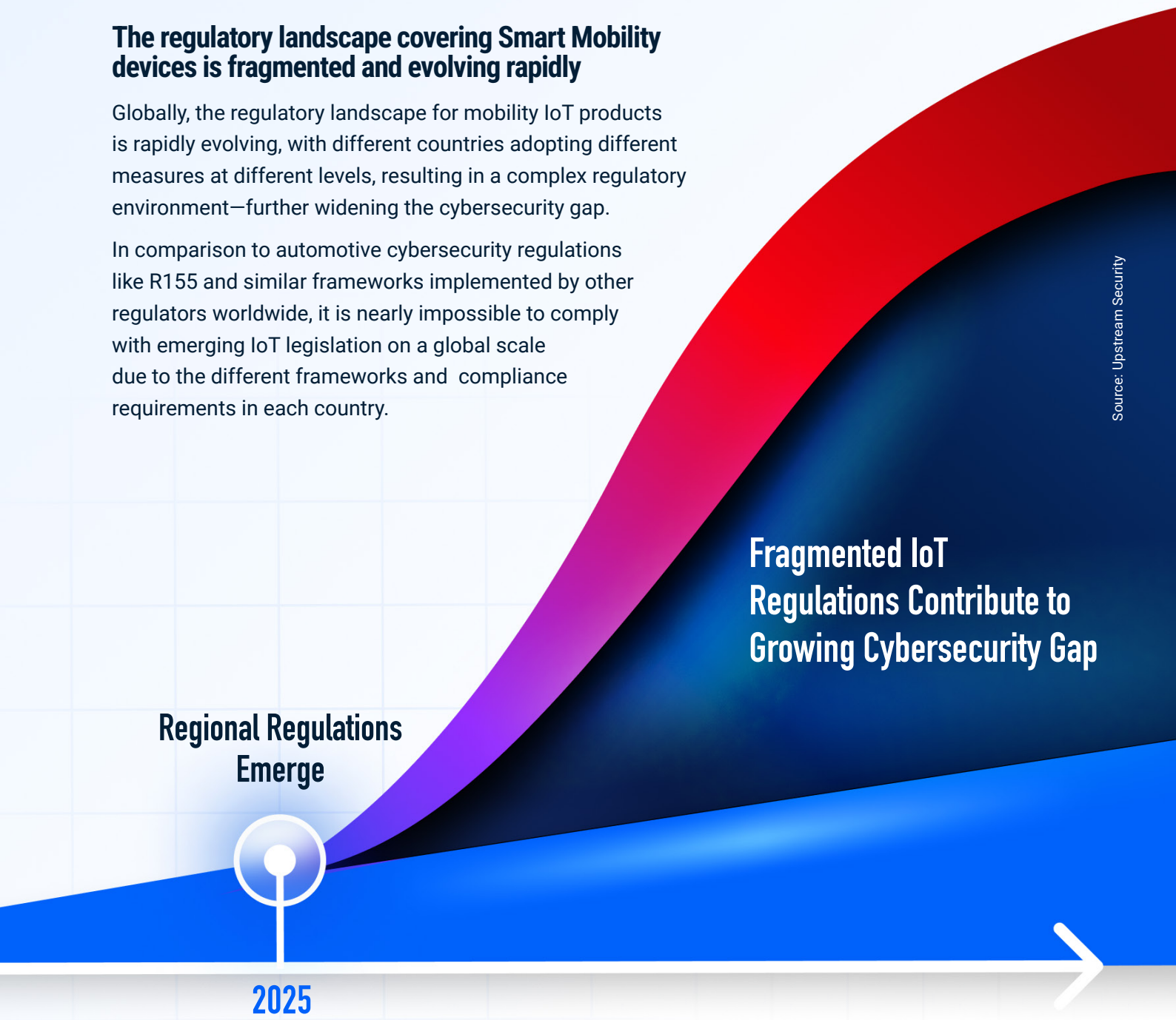
In November 2024, a UK-based telematics vendor experienced a cyber attack that disrupted many of its services, affecting fleet tracking capabilities for numerous clients.[49] Beyond operational disruptions, the attack allowed unauthorized activity within the company's network. **Several fleet operators reported significant impacts on their operations, citing issues with real-time tracking and potential delays in deliveries.** The company promptly alerted the relevant authorities, including the UK Information Commissioner's Office, and stated to be working with cybersecurity experts to investigate and mitigate.

These findings highlight the need to secure Smart Mobility devices as critical infrastructure and the implications of not doing so.

The regulatory landscape covering Smart Mobility devices is fragmented and evolving rapidly

Globally, the regulatory landscape for mobility IoT products is rapidly evolving, with different countries adopting different measures at different levels, resulting in a complex regulatory environment—further widening the cybersecurity gap.

In comparison to automotive cybersecurity regulations like R155 and similar frameworks implemented by other regulators worldwide, it is nearly impossible to comply with emerging IoT legislation on a global scale due to the different frameworks and compliance requirements in each country.



Source: Upstream Security

In the EU, the NIS2 Directive[50] —which became mandatory on October 17, 2024—focuses on establishing cybersecurity standards and resilience for the critical infrastructure and energy sectors. The NIS2 Directive is supported by the EU Cyber Solidarity Act,[51] which aims to strengthen capacities in the EU to detect, prepare for and respond to significant and large-scale cybersecurity threats and attacks. This includes forming SOC infrastructure within EU member countries to ensure coordinated handling of cyber threats, and creating a European Cybersecurity Reserve, consisting of incident response services from trusted qualified providers. NIS2 also adds reporting requirements within 24 hours, with additional reporting after 72 hours and 30 days.[52]

Companies that fail to comply with the new NIS2 Directive could face massive administrative fines, along with other punitive actions, including:[53]

- Fines up to €10 million or 2% of global annual revenues—whichever is higher—for **essential entities,** which includes public and private companies in sectors such as transport, finance, energy, water, space, health, public administration, and digital infrastructure.
- Fines of up to €7 million or 1.4% of global annual revenues—whichever is higher—for **important entities,** which includes public and private companies in sectors such as foods, digital providers, chemicals, postal services, waste management, research, and manufacturing.
- Criminal sanctions for management (e.g., personal liability) and non-monetary remedies such as suspension of service orders, compliance orders, binding instructions, security audit implementation orders, threat notification orders, and close supervision.

In March 2024, the European Parliament approved the Cyber Resilience Act (CRA),[54] a horizontal legislation, covering all products with digital components (both hardware and software).[55] The CRA covers the entire lifecycle of products, offering a framework for cybersecurity governing the planning, design, development, and maintenance of products. The CRA also requires manufacturers to report actively exploited vulnerabilities and incidents within 24 hours, and mitigate risks effectively through the support period of the product.[56]

In the UK, the Product Security & Telecommunications Infrastructure Bill represents a significant regulatory shift for the IoT ecosystem, requiring a comprehensive approach to integrating cybersecurity into product development and lifecycle management.[57] In addition to protecting consumers from cyber threats, the bill seeks to mitigate the risk of larger-scale attacks that may disrupt critical national infrastructure by exploiting interconnected devices.

In the US, the Federal Communications Commission (FCC) voted to create a voluntary cybersecurity labeling program for wireless consumer IoT products.[58] The program builds on the significant public and private sector work already underway on IoT cybersecurity and labeling. The Securities and Exchange Commission (SEC) also adopted rules on cybersecurity risk management, strategy, governance, and incident disclosure by public companies.[59]

In February 2024, the National Institute of Standards and Technology (NIST) updated the widely used Cybersecurity Framework (CSF).[60] The new 2.0 edition, which supports implementation of the National Cybersecurity Strategy, has an expanded scope that goes beyond protecting critical infrastructure to all organizations in any sector. It also has a new focus on governance and supply chain risk management, which encompasses how organizations make and carry out informed decisions on cybersecurity strategy. The CSF's governance component emphasizes that cybersecurity is a major source of enterprise risk that senior leaders should consider alongside other risks, including those that are financial, privacy, supply chain, reputational, technological, or physical in nature.

Overview of IoT regulatory landscape impacting Smart Mobility devices

Regulation	Impact on IoT	Reporting Requirements	Effective Date	Scope
GDPR	Comprehensive legal framework to protect the privacy of individuals. Fines up to €20 million or 4% of global annual revenue	Within 72 hours	May 2018	EU member states
The Cybersecurity Act	Voluntary risk-based certification requirements, emphasizing data protection and cybersecurity	Without undue delay, and no later than 72 hours when possible	June 2019	EU member states
Cyber Resilience Act	Comprehensive legal framework with strict cybersecurity requirements. Fines up to €15 million or 2.5% of global annual revenue	Within 24 hours	October 2024, with compliance requirement expected in 2027	EU member states
NIS2 Directive	Enhanced security measures and stricter enforcement measures. Fines of up to €10 million or 2% of global annual revenue	Within 24 hours, with additional reporting after 72 hours and 30 days	October 2024	EU member states
Product Security & Telecommunications Infrastructure Bill	Comprehensive approach to integrating cybersecurity into product development and lifecycle management	Disclose incidents promptly	April 2024	UK
NIST Cybersecurity Framework 2.0	Comprehensive framework to manage and reduce cybersecurity risks now includes expanded industry scope, and governance and supply chain risk management components	None	February 2024	US
Cyber Trust Mark Labeling	Voluntary cybersecurity labeling program for IoT devices	None	End of 2024	US
SEC Cybersecurity Reporting Requirements	Companies must provide detailed annual reports on their cybersecurity risk management strategies, including governance best practices, and the board's role in overseeing risks	Within 4 business days for material incidents; must provide comprehensive detail about the incident nature, scope, impact on operations and financials	December 2023	US

Source: Upstream Security

In response to increasing cyber risks, ISO/WD 24882 introduces new cybersecurity requirements for Agriculture OEMs

ISO/WD 24882 is a new standard—which is still under development and has not yet reached the final stages of approval—that aims to establish engineering requirements for the cybersecurity of electrical and electronic systems for Agriculture OEMs, including components and interfaces.[61] It covers the entire lifecycle of these systems, from concept through to decommissioning, ensuring that cybersecurity risks are managed effectively.

The new standard outlines cybersecurity requirements that highlight the importance of protecting access to devices' components, command and control functions, and sensitive data:

- **Risk Assessment:** OEMs must conduct comprehensive cybersecurity risk assessments for their connected systems and components during the concept and development phases.
- **Design & Development:** Cybersecurity must be integrated into the design and development processes of agricultural machinery, with specific requirements for hardware, software, and communication interfaces.
- **Production & Maintenance:** The standard requires the implementation of secure production and maintenance practices, ensuring that cybersecurity is maintained throughout the lifecycle of the machinery.
- **Decommissioning:** Even at the end of a device's life, OEMs need to consider secure decommissioning procedures to prevent unauthorized access to sensitive data and systems.

Whereas R155 provides a broad global regulatory framework, ISO/WD 24882 provides detailed technical guidance that is tailored to the unique challenges of the agricultural sector, and the threats associated with the rural deployment and operational environment of agricultural machinery—where connectivity may be limited and updates are less frequent, but unauthorized access or tampering could have severe consequences.

ISO/WD 24882 aligns with the EU's CRA, but expands its coverage beyond the EU, and is also expected to impact the implementation of R155, which may expand to cover vehicle categories T (e.g., agricultural machinery), R (e.g., agricultural trailers), and S (e.g., interchangeable towed agricultural equipment).[62]

As cybersecurity threats evolve, regulations and standards are likely to be continually updated as well. OEMs that adopt ISO/WD 24882 early will be better positioned to adapt to future regulatory changes, including any updates to R155 and the CRA that further tighten cybersecurity requirements.

CLOSING CYBER GAPS REQUIRES PRODUCT SECURITY TEAMS TO EXPAND RESILIENCE BEYOND REGULATORY REQUIREMENTS

A vehicle security operation center (vSOC) is an essential part of R155 & R156 compliance, enabling OEMs to monitor connected vehicles in real time and respond to threats quickly.

> ***The scope of vSOC-monitored vehicles grew substantially with the second milestone of R155 in July 2024, which expanded coverage to all new vehicles in production. OEMs had to adjust their vSOC teams, platforms, and processes accordingly.***

Many OEMs are still lagging behind in implementing their vSOC roadmaps, even though vSOCs are essential for cyber resilience.

As the threat landscape continuously evolves, and attacks with massive scale and impact dominate, cyber gaps begin to emerge and cybersecurity teams must evolve their vSOCs beyond regulatory requirements, continuously maintaining security postures.

Closing the cyber gaps requires live monitoring of fleets, Smart Mobility devices, and smart mobility systems and APIs, as well as an investment in talent and improved attack-detection and vSOC execution capabilities.

The vSOC evolution from compliance to large-scale risk mitigation can be broken down into 4 stages:

1.0 R155 & R156 Compliance

Initially, OEMs establish R155 & R156 compliance by building a dedicated vSOC with a clear framework and a well-defined strategy and scope. In addition, OEMs are required to implement Cyber Security Management and Software Update Management systems (CSMS and SUMS), and conduct a comprehensive audit of their cybersecurity framework against R155 to achieve certification. As demonstrated above, though meeting regulatory requirements is a fundamental task for product security teams, it may create a false sense of resilience and significant coverage gaps.

2.0 Remediation & Automation

Next, the vSOC develops and implements end-to-end playbooks to structure and automate response activities—continually expanding coverage and automation capabilities—and integrates the vSOC with other enterprise IT systems such as IT service management (ITSM), security information and event management (SIEM), extended detection and response (XDR), and security orchestration, automation and response (SOAR) to ensure cross-organization visibility and effective remediation.

During this stage, vSOCs focus on becoming more data-driven. vSOC teams integrate as many data feeds as possible into the detection and investigation phase and use automotive-specific cybersecurity analytics to detect threats and anomalies in near or real-time.

3.0 The GenAI-Powered vSOC

With modern vSOCs dealing with massive amounts of data from multiple sources, dynamic SBOMs, and global supply chain risks—GenAI is key to gaining greater visibility, streamlining investigations, and supporting long-term vSOC efficiency.

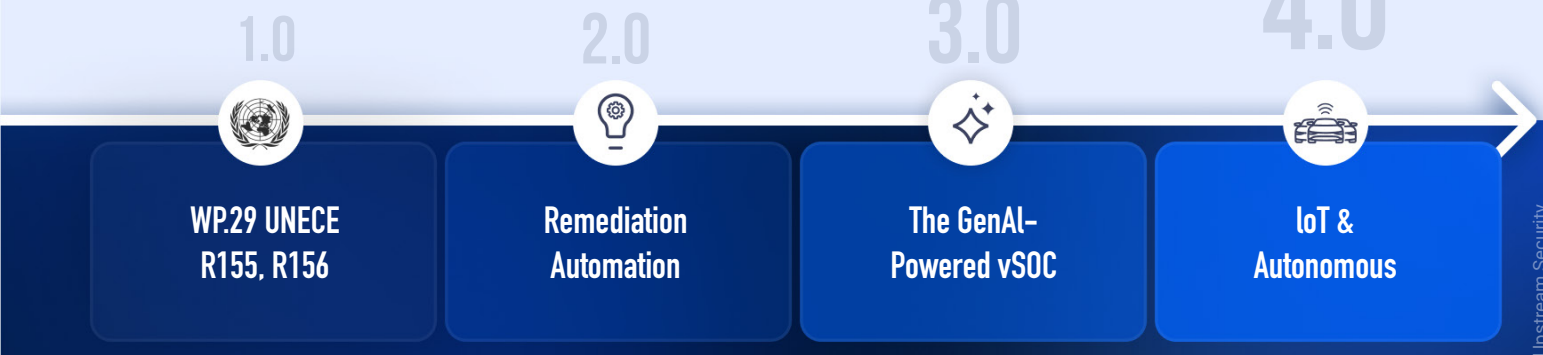
The GenAI-powered vSOC introduces unparalleled efficiencies, enabling cybersecurity teams to expand their data-driven detection and vSOC execution capabilities. They can quickly analyze massive amounts of connected vehicle and mobility data, detect patterns, filter incident alerts, automate investigations, and conduct enhanced TARA to address large-scale risks.

4.0 Smart Mobility Devices & Autonomous Technologies

Ultimately, the vSOC becomes truly cross-functional and coverage is expanded to include autonomous vehicles, mobility applications, OT, and Smart Mobility devices to protect vehicles, infrastructure, and customers during the post-production phase.

The vSOC Evolution

From compliance to large-scale risk mitigation



Source: Upstream Security

Evaluating and minimizing product cybersecurity gaps

Upstream developed a unique methodology to evaluate product cybersecurity posture and identify potential gaps. **The Automotive Cybersecurity Quadrant is a strategic framework designed to provide insights into the current cybersecurity posture, and identify areas for improvement to achieve optimal security outcomes and effectively use connected vehicle data.**

The positioning of organizations on the Automotive Cybersecurity Quadrant is determined by evaluating each organization's performance across a set of criteria for both data-driven detection and vSOC execution.

Data-driven Detection represents how effectively customers are using the data collected from their connected vehicles. Criteria include data coverage, diversity, quality, freshness, and richness. Higher data-driven detection shows that customers are using their data more efficiently to support cybersecurity strategies, enabling them to improve their security posture and unlock new business opportunities.

vSOC Execution is a measure of vSOC operations and workflows that customers have in place. Evaluation criteria include readiness, prediction, monitoring, detection, and response capabilities. A higher degree of vSOC Execution suggests a more comprehensive and mature deployment of vehicle security operations center capabilities, resulting in improved cybersecurity protection for connected vehicles.

Four types of organizations are represented in the quadrant:

The Automotive Cybersecurity Quadrant, developed by Upstream

Data-Driven Cybersecurity Leaders (Top-Right): Organizations in this quadrant excel in both data utilization and vSOC execution and have advanced in their vSOC journey to the vSOC 4.0. They effectively use connected vehicle and device data and have a robust vSOC deployment, resulting in strong cybersecurity detection and investigations. These organizations serve as industry leaders, setting high standards for connected vehicle cybersecurity.

Data-Oriented Players (Top-Left): Organizations in this quadrant have high data utilization but limited vSOC execution (vSOC 1.0-2.0) and have not yet expanded to cover Smart Mobility devices or autonomous systems data feeds. They have extensive data from their connected vehicles but may not be fully using their vSOC capabilities to maximize their cybersecurity protection. These organizations can benefit from improving their vSOC integration to better use their data for improved security.

vSOC Pioneers (Bottom-Right): Organizations in this quadrant have lower data utilization but have advanced in their vSOC execution by implementing purpose-built workflows and automations (vSOC 2.0-3.0). They might not have extensive connected vehicle data, but their effective vSOC methodologies and processes help them maintain a basic level of cybersecurity protection. These organizations can benefit from increasing their data utilization to further strengthen their cybersecurity posture.

Emerging Cybersecurity Adopters (Bottom-Left): Organizations in this quadrant are focused on compliance requirements and have lower data utilization and limited vSOC execution (vSOC 1.0). They are in the early stages of adopting product cybersecurity best practices and have the potential to improve their cybersecurity by increasing data usage and implementing a more comprehensive vSOC. These organizations can learn from industry leaders and work towards improving their data-driven cybersecurity approach.

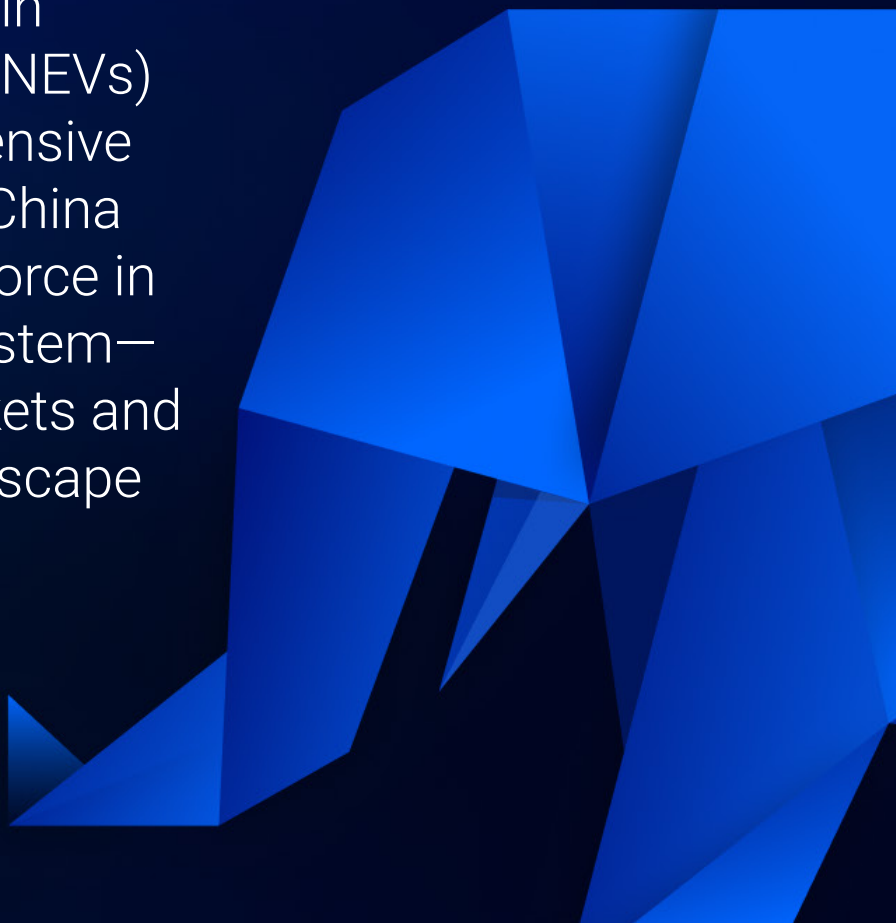
To close cybersecurity gaps, stakeholders must expand their data-driven detection and vSOC execution capabilities, including:

- Monitoring coverage — expand monitoring to all connected assets including vehicles, smart mobility applications, APIs, and Smart Mobility devices.
- Advanced ML-based modules — apply advanced AI/ML models to effectively detect unknown threats and attacks, including complex low and slow attacks.
- Vulnerability management — analyze products and components, from a single ECU or connected device and up to a complete vehicle model.
- Enhanced TARA — generate complex insights based on deep and dark web CTI data and in-depth TARA.
- GenAI-powered vSOC — transform vSOC operations and introduce unparalleled efficiencies.

02.

THE ELEPHANT IN THE BOARDROOM

By leveraging its vast manufacturing advantages, strategic investments in New Energy Vehicles (NEVs) technologies, and extensive government support, China has become a major force in the Automotive ecosystem—reshaping global markets and the cybersecurity landscape



CHINA'S STRATEGIC INVESTMENTS AND GOVERNMENT SUPPORT ARE RESHAPING THE AUTOMOTIVE INDUSTRY

Over the last decade China adopted and implemented its Made in China 2025 (MIC 2025) plan, a ten-year, comprehensive blueprint launched in 2015. MIC 2025 was designed to reduce China's dependence on foreign technology and promote Chinese high-tech manufacturers in the global marketplace.

The plan was designed to transform China into an advanced manufacturing leader and called for technological breakthroughs in ten strategic industries—electric vehicles, information technology, telecommunications, artificial intelligence, advanced robotics, agricultural technology, aerospace engineering, maritime engineering, bio-medicine, and rail infrastructure.

By early 2020, almost 1,800 government guidance funds (GGFs) tied to MIC 2025 had registered a capital target of $1.5 trillion and raised $627 billion toward it. Often, GGFs (which are state owned) take an equity stake or board position in the companies they fund and can influence corporate decision-making as a result.[63]

MIC 2025 used the power of the state to alter global dynamics in industries essential to its economic competitiveness.[64]

MIC 2025 employed a multi-step process to achieve this goal:

1. Localization and indigenization of R&D (e.g., locally developed or acquired foreign technologies, IP, and brands) and control of global supply chains segments (e.g., vertical integration);
2. Substitution of foreign technology with indigenous technologies as a strategic imperative;
3. Followed by capturing global market share across MIC 2025 industries and technologies.

China also used its legal and regulatory systems (e.g., taxes, trade restrictions, standards, forced JVs, IP transfers, procurement polices, etc.) to favor domestic Chinese companies over foreign ones in the targeted MIC 2025 sectors. The plan even went as far as setting explicit sales growth and market share targets that are to be filled by domestic companies.

With preferential access to capital, domestic companies were able to develop indigenous R&D and manufacturing capabilities, advance new manufacturing technologies, gain control and vertically integrate their supply chains, acquire foreign technology, and enhance their competitiveness.

> ***A decade later, China has become a major force in the global Automotive industry, and enjoys massive manufacturing advantages over other countries.***

OEMs have never faced a stronger, more motivated, and technologically advanced competitor:[65]

- Production scale of over ***30 million*** units in 2023
- Production capacity of over ***48 million*** units in 2023
- ***25%-30%*** cost advantage
- ***50%*** faster time to market
- ***400%-500%*** higher government subsidies
- ***76%*** of global EV batteries production
- Control of supply chains and vertical integration

Source: Upstream Security

Global OEMs operating in China are well aware of China's manufacturing advantages—like Tesla, which produces half of its global output at its Shanghai gigafactory.[66]

CHINA'S MIC 2025 HAS PROPELLED ITS NEV LEADERSHIP

China is now the world's largest market for new energy vehicles (NEVs) —which includes battery electric vehicles (BEVs), plug-in hybrids (PHEVs), and fuel cell electric vehicles (powered by hydrogen).

According to the latest official data, the number of newly registered NEVs in China jumped by nearly 40% year-on-year in the first half of 2024 to a record high.

Infrastructure for NEVs also expanded rapidly during the same period, with the number of NEV chargers jumping by 54% year-on-year to 10.2 million, including 3.1 million public charging facilities. As of June 2024, there are a total of 24.7 million NEVs registered in China, accounting for 7.2% of total vehicle ownership. The number of BEVs exceeded 18.1 million, representing 73.3% of NEVs.[67]

As of September 2024, Tesla's Model Y remained the best-selling electric car in China, according to Chinese automotive website Autohome. Chinese NEV maker BYD's Seagull trailed closely behind in second place.[68]

In October 2024, BYD's global quarterly sales overtook Tesla's for the first time, crowning a remarkable rise for the Chinese OEM.[69]

MIC 2025 TRANSFORMS THE AUTOMOTIVE REGULATORY LANDSCAPE

In January 2024, China's Ministry of Industry and Information Technology (MIIT) released a sweeping plan to accelerate the establishment of standards for automotive chips. Often referred to as the "Guidance on Formulating National Automotive Chip Standards", this plan includes more than 30 critical standards to be implemented by 2025, and more than 70 standards by 2030.[70] The standards are focused on clarifying basic requirements related to reliability as well as the environment, electromagnetic compatibility, functional safety and information security—in an attempt to further boost research and development of the critical product amid increasing international competition.[71]

Furthermore, China's automotive regulations took a significant leap forward in 2024 with the introduction of new cybersecurity standards for intelligent networked vehicles, safety requirements and testing methods for collisions—along with plans to become a key player in the global automotive industry's standards development process.

In May 2024, the Standardization Administration of China (SAC)[72] introduced new GB standards, a set guidelines and specifications, for safety requirements and test methods in the event of rear-end collision for passenger vehicles (GB 20072—202X) and the protection of the occupants in the event of a lateral collision (GB 20071—202X). The new standards replace the previous versions from 2006, and are expected to take effect in July 2026.[73]

In June 2024, MIIT announced plans to formulate new standards for the global Automotive industry, focusing on NEVs and intelligent connected vehicles. China will lead the development of nearly 20 international standards, including those for fuel cell vehicles, electromagnetic compatibility, and automotive radar. In addition, China aims to develop at least three new international standards for electric vehicle (EV) performance-testing methods and collision safety terminology, and to establish one or two international standards working groups. China will also focus on the development of global technical regulations for autonomous driving systems, and expedite the formulation of regulations on maximum EV power output measurement methods and the second phase of power battery durability.[74]

In August 2024, MIIT published the first batch of mandatory national standards for intelligent networked vehicles in China, set to take effect on January 1, 2026[75]:

GB 44495-2024	**Technical Requirements for Information Security of Automobiles** stipulates the requirements of the automobile information security management system, as well as the technical requirements and test methods for external connection security, communication security, software upgrade security, data security, etc.
GB 44496-2024	**General Technical Requirements for Automobile Software Upgrade** stipulates the management system requirements for automobile software upgrade, as well as the technical requirements and test methods for vehicle software upgrade functions such as user notification, version number reading, safety protection, prerequisites, power guarantee, failure handling, etc.
GB 44497-2024	**Intelligent Networked Vehicle Autonomous Driving Data Recording System** stipulates the technical requirements and test methods of the intelligent networked vehicle autonomous driving data recording system in terms of data recording, data storage and reading, information security, collision resistance performance, environmental evaluation, etc.

Global OEMs operating in China should prepare for the 2026 milestone, and analyze the gaps between the new Chinese national standards and current international standards.

Overall, GB 44495-2024 shares many common principles with UNECE WP.29 R155 and ISO/SAE 21434 requirements of a cybersecurity management system. However, it introduces market-specific, detailed technical requirements. [76]

In addition, GB 44495-2024 stresses the importance of risk management, like ISO/SAE 21434, which includes continuous monitoring, risk assessments, and response measures to ensure that vehicles remain secure even as new threats emerge.

Although both standards aim to enhance vehicle cybersecurity, they differ in several key aspects:

	GB 44495-2024	R155
Scope	Only applies to M (passenger), N (commercial), and O (trailers, including semi-trailers) vehicle types.	Includes L6 and L7, and is expected to expand to all category L vehicles.
Specificity	Provides detailed technical requirements and testing methods.	Offers a broader framework and risk categories (Annex 5), granting manufacturers flexibility in implementation.
Testing Requirements	Lists 27 specific cybersecurity tests that manufacturers must perform, covering various aspects of vehicle cybersecurity including: external connections, communication systems, software updates, data security, access control, Denial-of-Service (DoS) protection, and more.	Emphasizes the necessity of cybersecurity testing, but does not prescribe specific testing methods.
Certification	Requires an audit without issuing a certificate or requiring renewals.	Requires a formal certification process with periodic renewals.

Source: Upstream Security

CHINA'S FAST-GROWING NEV INDUSTRY COMES WITH INCREASED CYBERSECURITY RISKS

Cybersecurity risks are increasing in China's booming NEV industry. Threat actors are increasingly targeting Chinese NEV makers and suppliers with ransomware and data exfiltration attacks. Security researchers are also discovering critical vulnerabilities in Chinese NEVs, including their telematics systems, vehicle infotainment systems, and OEM apps. **Numerous cyber incidents involve Chinese Tier-1 and Tier-2 suppliers, heightening global supply chain concerns.**

In March 2024, a Chinese Tier-2 supplier of automotive electronic parts was attacked by a data exfiltration and extortion group. The breach involved the exfiltration of 1.2TB of data, impacting both Chinese and global OEMS. The data includes personal information, customer data, source code, SQL databases, and internal and external email correspondence with attachments.[77]

In May 2024, security researchers discovered a critical vulnerability in a Chinese EV maker's telematics system, resulting from a Radio Access Network (RAN) attack. The attack compromised GPS functionality and also disrupted the vehicle's network connectivity and associated FMS (Fleet Management System) functionalities. Consequently, tracking or locating the vehicle was impossible, and basic functionalities such as engine start or stop were also inoperable, until the vehicle was manually restarted.[78]

In June 2024, Chinese automotive Tier-1 supplier, specializing in thermostats and temperature sensors, was hit by a ransomware attack resulting in the exfiltration of over 300GB of sensitive data. The breach compromised the company's operational integrity as well as disrupted their online activities, affecting their website directly. The stolen data included confidential documentation, financial records, and personal information.[79]

In August 2024, security researchers discovered an unprotected database containing sensitive information on more than 750,000 Chinese car owners. The database, hosted on a US-based IP address, exposed names, ID numbers, phone numbers, addresses, VINs, car models, and more, leaving individuals at risk of identity theft and vehicle-related crimes. The database was locked down after 48 hours, but its ownership remains unknown. The security researchers suggest that the combination of data may have been collected by cybercriminals rather than a legitimate organization.[80]

In September 2024, a Chinese Tier-1 supplier, specializing in automotive CAN BUS protocol solutions, was targeted by a hacktivist group as part of their operation against Chinese companies.

The group claimed to have attacked and shut down the company's official website servers. There is no independent verification of these claims, and the company has not commented on the extent of the attack.[81]

In September 2024, Chinese security researchers demonstrated a Bluetooth Low Energy (BLE) relay attack to relay information between the PhoneKey system and the vehicle at the protocol level. Protocol-based relay attacks have the advantage of not requiring physical proximity between the victim (vehicle owner), who can be anywhere in the world, and the vehicle.[82]

Vehicle owners with Phone-as-a-Key (PAAK) systems can use an authorized mobile phone to unlock and control the vehicle within a certain proximity. Although PAAK uses challenge-response as an authentication mechanism, it does not enable BLE link-layer pairing or encryption, making it an ideal target for Gattacker, a Man-in-the-Middle and analysis tool for BLE devices, originally launched in 2017. Researchers successfully exploited popular models of Chinese and American EV OEMs, targeting vehicles that do not implement BLE link-layer pairing or encryption. Vehicles that had enabled PIN code requirements during the initial pairing stage were not vulnerable. The researchers reported their findings to the respective OEMs.

In September 2024, a security researcher published an article showing the exploitation of Braktooth vulnerabilities in Bluetooth chipsets used in vehicle infotainment systems. The vulnerabilities are present in various Bluetooth chipsets across many manufacturers, and allow attackers to exhaust the Bluetooth resources of the target device. The attacker can disrupt or crash other Bluetooth devices connected to the target chipset. The research was based on older analysis from 2021, while recent testing revealed that many popular vehicle models in China are susceptible to Braktooth attacks.[83]

These incidents underscore the increasing risks associated with Chinese OEMs' rapid expansion into international markets. The exposure of critical vulnerabilities in high-profile markets like the US and EU amplifies regulator scrutiny and raises barriers to market acceptance.

THE INTERNATIONAL RESPONSE TO CHINESE NEV GROWTH AND CYBERSECURITY CONCERNS—MASSIVE TARIFFS AND TECHNOLOGY BANS

The rapid rise of China's NEV sector is raising concerns about global technological growth and the cybersecurity resilience of connected vehicles, autonomous driving, electric vehicles, batteries, and EV charging infrastructure.

In February 2024, China committed to helping its EV makers cope with international trade restrictions and build overseas supply chains, as part of a major global expansion effort for the industry. The pledge comes as China's booming EV exports face increasing protectionist pushback in some regions, including Europe and the US.[84]

> ***In September 2024, the US Department of Commerce published a Notice of Proposed Rulemaking that would ban the sale or import of connected vehicles integrating specific pieces of hardware and software, or those parts sold separately, with a sufficient nexus to the People's Republic of China or Russia.[85]***

The rule focuses on hardware and software integrated into the Vehicle Connectivity System (VCS) and software integrated into the Automated Driving System (ADS) which present undue risk to US critical infrastructure, national security, and the safety of drivers. **The planned rules would effectively ban Chinese vehicles from the US market, but would also force OEMs to remove Chinese software and hardware from vehicles sold in the US.**

The proposed rule marks a significant escalation in ongoing US restrictions on Chinese vehicles, software, and components. The bans on software would take effect for Model Year 2027, and the bans on hardware would take effect for Model Year 2030, or January 1, 2029 for units without a model year.[86]

Inspired by US actions, European officials have also echoed Washington's concerns over the potential cybersecurity, espionage, and sabotage risks posed by Chinese automotive technology.[87] European officials have been drafting an Information and Communication Technology (ICT) supply-chain toolbox (non-binding)—a similar framework to the 5G Security Toolbox,[88] which led several EU countries to ban, limit, or phase-out Chinese telco vendors.

The EU's increased scrutiny of Chinese software suppliers means that OEMs, particularly those with many Chinese suppliers, will need to adapt their strategies. Furthermore, the US ban will directly impact European OEMs, forcing them to adjust the supply chain for vehicles sold in the US.

> ***In early October 2024, the EU's dramatic announcement on taxation of Chinese EVs, set to rise from 10% to up to 45% over the next five years, posed the question of what impact this might have on decisions by the Chinese government towards European automakers who are actively present in China.***[89]

By the end of October 2024, when the new EU tariff rules came into effect, Reuters reported that China had told its automakers to halt big investment in European countries that support extra tariffs on Chinese-built electric vehicles.[90]

03.

AUTOMOTIVE CYBERSECURITY TRENDS

In 2024, ransomware attacks with unprecedented impact dominated, SDV and AV technologies dramatically changed cybersecurity risks, and incidents involving manipulation and control of vehicle systems more than tripled

REVIEW OF INCIDENTS

Cybersecurity attacks grew in scale and impact in 2024, creating new challenges for the automotive and smart mobility industries.

During 2024, Upstream's AutoThreat® researchers analyzed 409 automotive and smart mobility cybersecurity incidents—an average of 34 incidents per month.

The top incidents in 2024:

○ White Hat ● Black Hat

JANUARY

- ○ A redirect vulnerability was discovered by security researchers on some German OEM subdomains.[91]
- ● Ransomware attack impacts one of the world's largest semiconductor manufacturers, shutting down its website and exfiltrating 5TB of sensitive data.[92]
- ○ A security researcher discovered a vulnerability leading to customer PII exposure in a South Korean OEM.[93]

FEBRUARY

- ○ Security researchers discovered a German OEM cloud misconfiguration that led to massive exposure of sensitive data.[94]
- ● South Korean OEM was hit by a large-scale cyberattack resulting in the exfiltration of 3TB of corporate data.[95]
- ● A cyberattack on a Lithuanian EV charging system shut down operations for hours, with attackers stealing data of 20,000 customers.[96]

MARCH

- ○ Security researchers from Colorado State University showed how ELDs can be accessed over Bluetooth or Wi-Fi connections to take control of a truck, manipulate data, and spread malware.[97]
- ● A Chinese Tier-2 supplier was hit by a ransomware attack, leading to a major breach of 1.2TB of data, impacting global OEMs.[98]
- ○ A security researcher discovered an unprotected 585GB database with more than half a million PII and business records of an American EVSE provider.[99]

APRIL

- ● The PII of over 300,000 taxi passengers in the UK and Ireland was discovered in an unprotected database belonging to an Irish smart mobility provider.[100]
- ● Chinese hackers conducted an extended cyber espionage campaign targeting a major German OEM group to steal technical knowledge.[101]
- ○ Security researchers uncovered a critical CAN BUS injection vulnerability, potentially compromising e-scooter riders' safety and privacy.[102]

MAY

- ○ Security researchers discovered a critical vulnerability in a Chinese OEM telematics system, compromising GPS functionality.[103]
- ● A prominent European vehicle tracking and fleet management device provider was hit by a cyberattack that resulted in a data breach.[104]
- ● A European non-profit shared mobility provider suffered a severe cyberattack, resulting in service disruptions across all its platforms.[105]

JUNE

- ○ Security researchers discovered a vulnerability affecting an Indian OEM's automotive management application.[106]
- ○ A security researcher identified a severe vulnerability in a popular vehicle software development platform, used in infotainment, ADAS, and autonomous driving systems.[107]
- ● A ransomware attack on a leading US-based provider of dealership management software used by 15,000 dealerships, resulted in dealer operations being halted for nearly three weeks[108] and estimated losses of $1.02 billion.[109]

JULY

- Security researchers identified vulnerabilities in EV charging stations enabling unauthorized access and operational disruptions.[110]
- A security researcher discovered a vulnerability within the web-based UI on traffic controllers in Norway, enabling them to gain full control of the traffic controller.[111]
- A German OEM's Hong Kong branch allegedly experienced a cyberattack compromising sensitive customer PII.[112]

AUGUST

- A security researcher identified critical vulnerabilities in the Android-based OS embedded in the infotainment systems of major automakers.[113]
- South Korean automotive supplier hit by a ransomware attack, compromising 2.3TB of data.[114]
- Security researchers discovered a hardware backdoor in MIFARE technology widely used in public transportation systems.[115]

SEPTEMBER

- Security researchers discovered critical vulnerabilities in autonomous driving systems' Internet Control Message Protocol (ICMP), potentially resulting in flood attacks.[116]
- A security researcher demonstrated Braktooth vulnerabilities which can lead to crashes and remote code execution affecting multiple infotainment systems of various OEMs.[117]
- Security researchers revealed major API vulnerabilities in a Korean OEM's dealership API, which allowed them to control vehicles using only license plates.[118]

OCTOBER

- A security researcher discovered a critical vulnerability in a Dutch traffic signal preemption system, resulting in replacing thousands of traffic lights.[119]
- A ransomware group claimed to have stolen internal documents, financial records, and personal information from a German OEM group.[120]
- Security researchers identified a vulnerability in the VCSEC ECU (immobilizer unit) used by a US EV OEM, potentially leading to control compromise.[121]

NOVEMBER

- A UK-based telematics provider hit by a cyberattack resulting in business disruption and potential data theft impacting multiple international clients.[122]
- Security researchers detected six critical zero-day vulnerabilities in Japanese OEM infotainment systems.[123]
- A data breach affecting multiple Charging Point Operators (CPOs) led to over 116,000 consumers' PII and OCPP data from EVSEs leaked on a deep web hacking forum.[124]

DECEMBER

- Security researchers detected multiple vulnerabilities affecting infotainment systems of a German OEM.[125]
- Security researchers discovered multiple vulnerabilities potentially leading to data theft in infotainment systems of a Chinese OEM.[126]
- Cyber attack disrupts global auto parts supplier business operations in Canada.[127]

ATTACKS BY BLACK HATS CONSISTENTLY OUTNUMBER THOSE BY WHITE HATS

As technologies and cybersecurity measures advance, threat actors have also evolved, and stakeholders must gain deep visibility into who is carrying out attacks.

Hackers are classified as black hats, white hats, or gray hats depending on their intentions, actions, and malicious intent:

Black Hat

Black hat hackers attack systems for personal gain, financial gain, or for malicious purposes. Today's black hat hackers are no longer lone malware developers. They are often part of well-organized and well-resourced operations, which employ thousands of cybercriminals worldwide, capable of coordinated simultaneous attacks against multiple organizations.

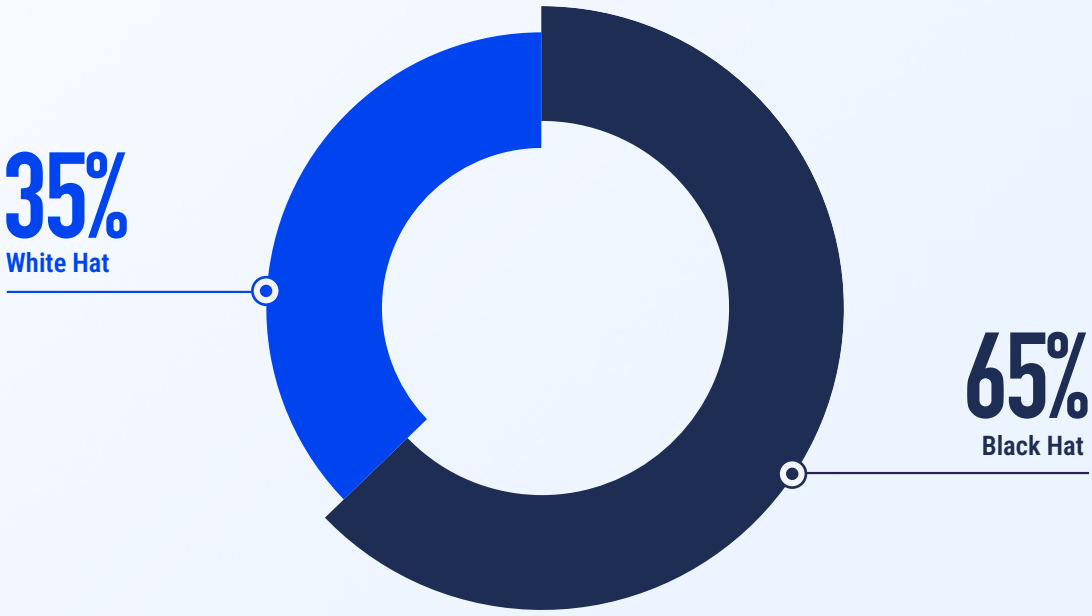
White Hat

In contrast, white hat hackers, often researchers without malicious intent, who try to penetrate and manipulate systems to validate security or assess vulnerabilities. White hat hackers continually find new and disturbing vulnerabilities. They operate independently, through companies using their services, or as part of a bug bounty program, where they are rewarded for responsibly disclosing vulnerabilities.

Gray Hat

Gray hat hackers are a subset of the general white hat attackers group, and present a dynamic landscape in which the lines blur between ethical and malicious activities. These hackers contribute both to discovering vulnerabilities and, in some cases, exploiting them. Gray hat hackers are driven by a variety of motivations, running from responsible disclosure to less altruistic incentives, such as financial reward or recognition. Also, their activities often raise ethical and legal questions regarding their work without explicit permission.

In 2024, black hat hackers carried out over 65% of all attacks



Source: Upstream Security

IT black hat attacks and automotive black hat attacks differ greatly in their consequences and impact. Malicious automotive black hat attacks—which are closely aligned with cyber attacks on IoT and critical infrastructure, such as health, energy, and governmental facilities—result in not only disruption of services and financial losses, but also potential for safety risks and loss of lives.

In February 2024, a South Korean OEM's European division was hit by a ransomware attack that disrupted its operations. The attackers claimed to have exfiltrated 3TB of data and shared images of stolen folders. The OEM confirmed the attack and collaborated with the authorities to recover and investigate the incident.[128]

In June 2024, a ransomware attack on a leading US-based provider of dealership management software used by 15,000 dealerships, resulted in shutting down dealer operations across the US for nearly 3 weeks. According to a CNN report citing multiple sources, the company likely paid a $25 million ransom to speed up recovery and end the outage.[129] The Anderson Economic Group (AEG) estimated that total direct losses to franchised auto dealers reached $1.02 billion.[130]

In November 2024, a UK-based telematics company experienced a cyberattack that impacted critical operational services and multiple international fleets.[131] The attack prevented fleet operators from accessing fleet management data, causing operational disruption and delivery delays to major retailers in various sectors. In response to the incident, the company notified authorities and began working to restore services.[132]

Also in November 2024, a prominent threat actor exposed approximately 116,000 records of sensitive data from multiple global CPOs.[133] Initially claimed to be from an American EV OEM charging network, the breach was later found to encompass data from diverse charging stations across the globe, with victims spanning the UAE, Australia, Mexico, Puerto Rico, Guyana, Saudi Arabia, Oman, and India.

These attacks result in not only disruption of services and financial losses but also potential safety risks and loss of lives, particularly in critical infrastructure sectors. In many of these incidents by black hats, consumers remained unaware of potential risks, raising the bar for cybersecurity teams. The increasing sophistication and frequency of these attacks underscore the urgent need for robust cybersecurity measures and proactive threat intelligence to mitigate the risks posed by black hat hackers.

NEARLY ALL ATTACKS ARE REMOTE

Most automotive cyber attacks can be divided into two main categories: remote attacks—which can be short-range (e.g., man-in-the middle attack) or long-range (e.g., API-based attack)—and physical attacks, which require a physical connection to the vehicle (e.g., OBD port).

Remote attacks rely on network connectivity (e.g., Wi-Fi, Bluetooth, 3/4/5G networks), and have the potential to impact numerous vehicles simultaneously.

Remote attacks have consistently outnumbered physical attacks since 2010—accounting for 88% of all attacks between 2010 and 2024, and 92% in 2024. In 2024, long-range attacks accounted for 84% of remote attacks—this remains consistent with last year, following a 30% spike in 2022 caused by the increased adoption of connectivity and software-defined architecture.

Nearly all 2024 incidents were remote

The vast majority of remote incidents in 2024 were long-range

Source: Upstream Security

INCIDENTS INVOLVING MANIPULATION AND CONTROL OF VEHICLE SYSTEMS MORE THAN TRIPLED

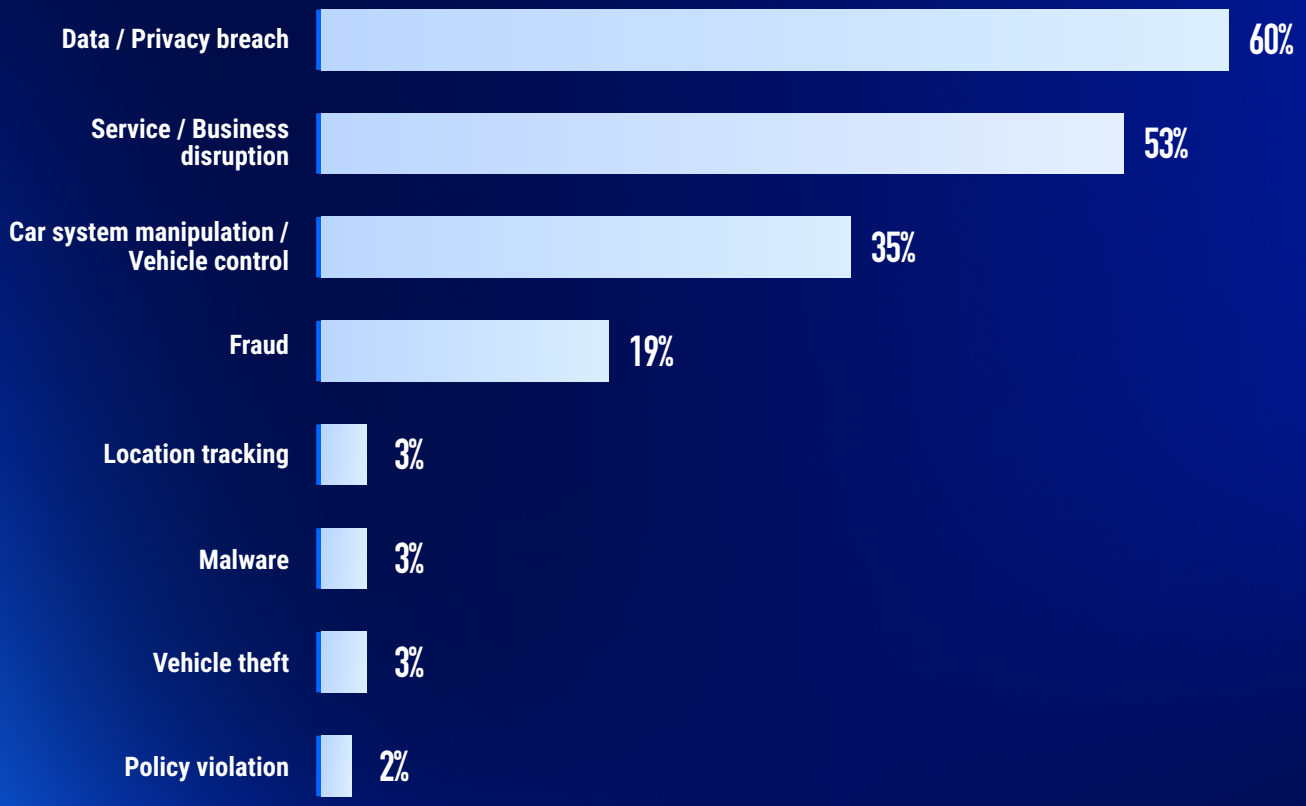
The impact of cyber attacks on the Automotive and Smart Mobility ecosystem is growing in scale. Vehicle attacks often compromise sensitive data, but they can also have far-reaching consequences, including vehicle theft, fraud, and the manipulation and control of vehicle systems, which may result in safety risks.

Data and privacy-related incidents accounted for 60% of 2024 incidents. The percentage of incidents involving car system manipulation and control of vehicle systems increased dramatically in 2024, accounting for over 35% of incidents.

The increase can be attributed to several factors. Firstly, increased research on EV chargers and infotainment systems has contributed significantly to this surge. This is evidenced by projects such as the Automotive Security Research Group (ASRG) and several other prominent white hat groups who actively discovered CVEs. Furthermore, Upstream's enhanced research into open-source software in fields like autonomous vehicles and IoT mobility, including smart mobility (e.g., telematics systems), smart city system (e.g., traffic lights systems) and EVSE, has also contributed to the upward trend.

Service / Business disruption	Disruptions to normal business operations caused by cyber attacks (e.g., shutdowns caused by ransomware, or attacks on backend systems that disrupt fleet operations).
Data / Privacy breach	A data breach occurs when a threat actor gains unauthorized access to sensitive data such as intellectual property (IP), trade secrets, financial information, or personally identifiable information (PII). Cybersecurity incidents involving data breaches are the most common and most expensive.
Fraud	Illegal use of vehicle data and/or vehicle functionality by threat actors for financial gain.
Vehicle theft	Vehicle thefts involving long-range, short-range, and physical attacks by threat actors.
Car system manipulation	Threat actor activities targeted at tampering with various in-vehicle systems, changing their expected operational behavior, and creating safety risks.
Policy violation	Threat actors' actions that violate established rules, regulations, or policies regarding the use, operation, or management of vehicles.
Location tracking	Illegal use of GPS navigation data to track a vehicle's location and movement without user or owner consent.
Control of vehicle systems	Threat actors can take full or partial control of a vehicle from long distances by overriding its systems through connected components.

2024 impact breakdown, based on 409 automotive-related cyber incidents



Source: Upstream Security

MONITORING CVES IS CRUCIAL

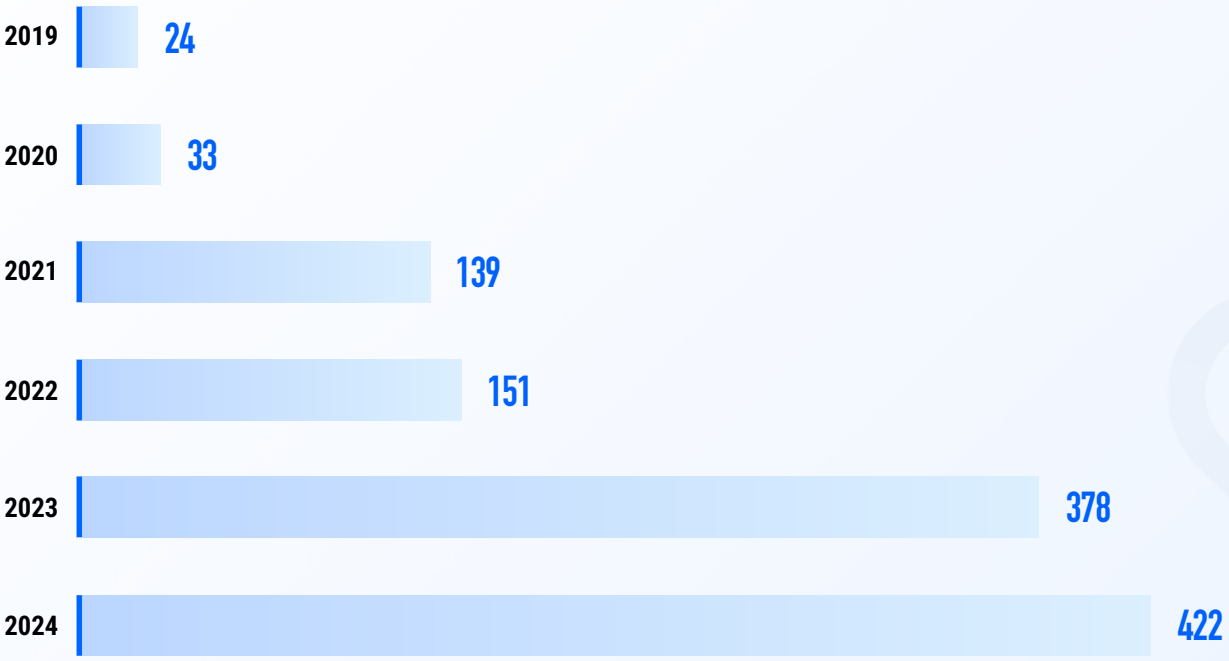
The Common Vulnerability Scoring System (CVSS) was designed to provide an open and standardized method for rating CVEs. CVSS helps organizations prioritize and coordinate joint responses based on the vulnerability's base, temporal, and environmental properties.[134] Vulnerabilities are also graded from Critical, High, Medium to Low, or None, based on their CVSS score.[135]

In our analysis of CVEs, we focus only on CVEs that directly affect the Automotive and Smart Mobility ecosystem (OEMs, Tiers-1s, shared mobility, mobility IoT devices, fleets, etc.). We exclude from this analysis CVEs that relate to generic IT hardware or open-source software components that may be used across the supply chain.

Number of automotive-related CVEs found in 2019-2024

The Automotive industry has experienced 1,147 specific CVEs since 2019; 422 CVEs were published in 2024, compared with 378 in 2023.

Several factors have contributed to the increase in CVEs, including increased adoption of connected components, greater stakeholder awareness of vulnerabilities, and more research initiatives into EV chargers and infotainment systems.



Source: Upstream Security

Security teams, developers, and researchers use CVSS together with several other methods to assess risks. CVSS scores have practical applications across the product's supply chain, such as determining whether vulnerabilities have already been exploited and prioritizing patching efforts, and allocating time and resources more efficiently. CVSS is also used by ISO/SAE 21434 as part of the standard's risk assessment process to determine attack feasibility.

CVEs should also be closely monitored by fleet managers and operators. CVEs not only factor into risk assessments across the fleet, but can also be considered when strategically designing fleet composition.

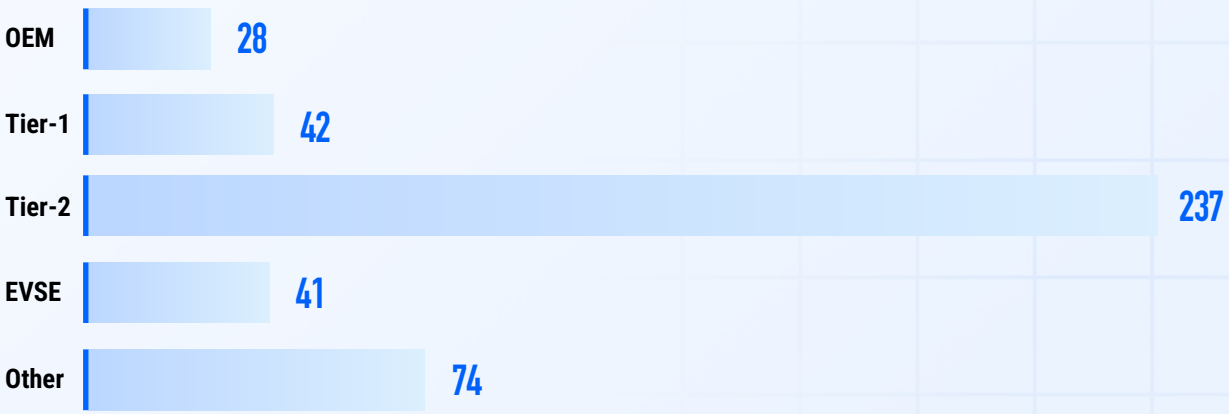
OVERVIEW OF 2024 CVES

CVEs are acknowledged and cataloged cybersecurity risks that can be quickly referenced across the Automotive and Smart Mobility ecosystem. It is common to find these threats on OEM products, but they can also appear in the products of OEM supply chain companies.

OEMs assemble vehicles from hundreds of software and hardware modules produced by Tier-1 and Tier-2 suppliers. Each component's quality and safety rests with the company that produces it. Consequently, each company involved in the supply chain has the responsibility to oversee and ensure the quality and safety of each automotive-related product. Because vulnerabilities are not always addressed on time, or even at all, a single flaw in a commonly used software module or component can impact millions of vehicles. Vulnerabilities disclosed by CVEs can also be exploited by attackers.

In 2024, the number of published CVEs was significantly impacted by funding shortages and cutbacks at the US National Vulnerability Database (NVD). Beginning early in the year, the NVD experienced a marked slowdown in vulnerability publications and analysis, leaving enterprise cybersecurity teams without timely and critical intelligence. In April, the National Institute of Standards and Technology (NIST) announced plans to collaborate with other agencies and industry partners to address a growing backlog of software vulnerabilities awaiting analysis.[136] Although the pace of publications improved later in the year, the NVD still struggled with delays in CVE analysis. Reports from May 2024 revealed that over 90% of CVE submissions remained unanalyzed or lacked enrichment.[137] By November, NIST reported having a full team of analysts in place to process incoming CVEs in real-time. However, the agency acknowledged that clearing the backlog would take longer than initially projected, despite its optimistic forecasts.[138]

2024 breakdown of publicly reported automotive-related vulnerabilities



Source: Upstream Security

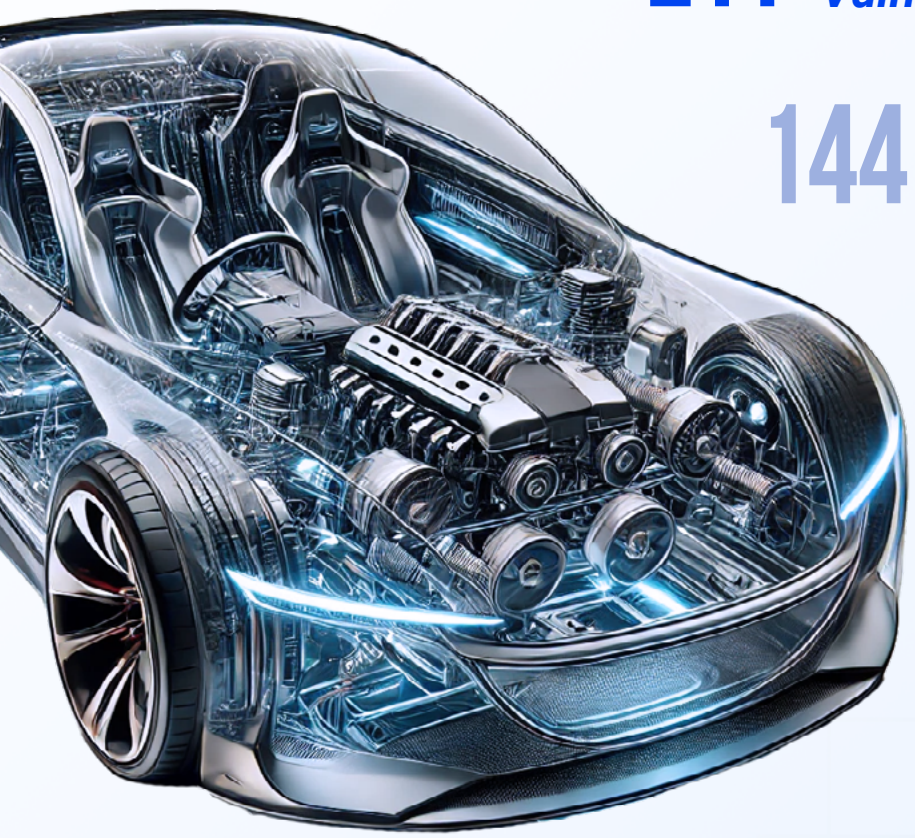
In 2024, the CVSS-scored vulnerabilities analyzed by Upstream's analysts had:

48 *Critical Vulnerabilities*

211 *High Vulnerabilities*

144 *Medium Vulnerabilities*

19 *Low Vulnerabilities*



Source: Upstream Security

Together with the increase in automotive-related CVEs in 2024, we also witnessed a nearly 41% increase in critical vulnerabilities—which accounted for over 11% of total CVEs, up from 9% in 2023. This trend amplifies the importance of closely monitoring automotive-specific CVEs by all stakeholders and proactively detecting exploits, as well as prioritizing mitigation.

THE IMPACT IS FELT ACROSS THE ENTIRE SMART MOBILITY ECOSYSTEM

Cyber attacks threaten every segment of the Automotive, Smart Mobility, and Mobility-as-a-Service (MaaS) ecosystem.

The proliferation of Smart Mobility devices ushers in a new era of cybersecurity risks on a massive scale, with a wide range of devices vulnerable to attacks such as EV charging equipment and infrastructure, autonomous systems and self-driving kits, traffic control systems, telematics systems, fleet management solutions, and smart agricultural equipment.

IoT devices in the Automotive and Smart Mobility ecosystem are now critical infrastructure. Cyberattacks on these devices pose higher risks and impacts than other IoT devices, necessitating stakeholders to ensure safety, operational availability, and data integrity.

Defining Automotive and Smart Mobility as critical infrastructure emphasizes the substantial cybersecurity risks these devices pose and reinforces the need to prioritize their resilience.

- OEMs
- Tier-1s
- Tier-2s
- Electric Vehicles
- EV Charging Infrastructure / Local Grids
- Autonomous Vehicles
- Agriculture Equipment
- Mobility IoT
- TSP / Fleet Management
- Car Dealerships
- Car, Commercial, and Delivery Fleets
- Public Transportation
- Government Fleets / Emergency Services
- Car and Bike Sharing
- Car Rental
- Ride Sharing and Hailing
- Smart Cities
- Insurance

OEMs & suppliers

OEMs and their component suppliers are increasingly being targeted by ransomware attacks that result in production shutdowns, loss of data, costly recalls, and brand damage.

In February 2024, a German-based publicly-traded Tier-1 global battery supplier was hit by a cyber attack that paralyzed production for weeks and caused damage of approximately €40 million.[139] The company's operations were substantially disrupted—including administrative, sales, financial, and customer service functions—and it took over a month to restore production at all five global production sites.[140] In mid-March 2024, the executive board decided to postpone the scheduled publication of the company's annual financial reports, stating that although they had regained partial access to IT systems and had restarted large parts of its production, the company still did not have access to financial information and business documents necessary to complete the financial reports.[141]

In March 2024, a Japanese OEM confirmed that a cyberattack, reported a few months earlier, severely impacted operations and resulted in the exfiltration of data impacting over 100,000 customers—includng PII, financial statements, employment or salary information, medicare cards, drivers licenses, passports, and tax file numbers.[142] A ransomware group took responsibility for the attack and claimed it had stolen 100GB of data, including documents containing personal employee information, NDAs, project data, and information on partners and clients. In response to the attack, the company investigated with the aid of government authorities and external cybersecurity experts, activated its response protocol, offered free identity theft and credit monitoring services, and provided reimbursement for customers needing to replace government IDs due to the breach.[143]

EVs & EVSE

EVs are increasing in number, and so are concerns over power grid cybersecurity and charging infrastructure resilience. While the fast adoption of EVs has led to the rapid development of charging infrastructure—often overlooking cybersecurity best practices and vulnerabilities—EVSE-specific regulations are still lagging behind.

Chargers are vulnerable to physical and remote manipulation that can control their functionality, and expose EV users to fraud, data breaches, and even ransom attacks.

In January 2024, security researchers found multiple vulnerabilities in a US-based EVSE's home charging station that could allow attackers to remotely access and control chargers. The cybersecurity vulnerabilities involved flaws in the implementation of a reverse SSH tunnel, an outdated HTTP server, a deprecated NTP client with known vulnerabilities, a deprecated kernel, and device certificates with unlimited expiration time. An attacker could authenticate to EVSE's central server, potentially creating their own tunnel, extending unauthorized access to each connected charger. Following the discovery, the security researchers actively collaborated with the company to address the vulnerability, which has been updated in a software release.[144]

In February 2024, the UK's Office for Product Safety and Standards (OPSS) suspended sales of Spanish EV chargers for failing to comply with current cybersecurity regulations, raising concerns over potential risks to the national energy infrastructure.[145] Hackers might gain access to thousands of non-compliant chargers and switch them all on at once, generating peak demands that disrupt the grid. The company, which has sold 40,000 units in the UK and over half a million worldwide, was allowed to continue to sell the chargers in the UK until June 30, 2024.

In April 2024, security researchers published a technical analysis PoC on the insecurity of Open Charge Point Protocol (OCPP) backend communication with the EV charging station (EVCS), identifying six zero-day vulnerabilities (impacting OCPP 1.6J) in 16 representative live EV charging management systems. The researchers managed to obtain EVCS IDs and the OCPP backend links from various online resources, which led to various attack scenarios including man-in-the-middle, denial of service, firmware theft, and data poisoning. They also developed a testbed to demonstrate the feasibility of launching switching attacks against the power grid using compromised EVCSs, and recommended countermeasures to mitigate/prevent future cyber-attacks.[146]

In July 2024, researchers found a security vulnerability in EV charging equipment. This vulnerability lets attackers exploit power line communication (PLC) protocols to gain unauthorized access and disrupt EV charging. The researchers gained access to the network keys, and digital addresses of the charger and the EV.[147]

In November 2024, an Italian EV charging company released a remote update to fix security vulnerabilities in its chargers' firmware. The flaws allowed unauthorized access to system logs, administrator privileges, and the execution of arbitrary commands through the charger's web management interface. Although no personal data was at risk, attackers could bypass charging restrictions, access system configurations, and launch denial-of-service attacks. Users with offline devices were advised to update patches via the mobile app.[148]

Also in November 2024, a prominent threat actor exposed approximately 116,000 records of sensitive data from multiple global CPOs.[149] Initially claimed to be from an American EV OEM charging network, the breach was later found to encompass data from diverse charging stations across the globe, with victims spanning the UAE, Australia, Mexico, Puerto Rico, Guyana, Saudi Arabia, Oman, and India.

Commercial fleets

As commercial fleet operators—such as car rental, logistics, and delivery companies—increasingly rely on connectivity and software for vehicle management, their cybersecurity risks multiply.

The consequences of cyber incidents are significant for commercial fleets, often resulting in decreased operational efficiency, increased operational costs, service delays, and, in extreme cases, complete service interruptions.

In March 2024, security researchers from Colorado State University showed how ELDs—mandatory in nearly 14 million commercial medium and heavy-duty trucks in the US—can be accessed over Bluetooth or Wi-Fi connections to take control of a truck, manipulate data, and spread malware between vehicles. Researchers found that ELDs are distributed with default firmware settings with considerable security risks. They also use the CAN BUS to communicate, feature an exposed API for OTA updates, predictable identifiers, and weak passwords—simplifying unauthorized connections and access to vehicle systems for attackers in wireless range. **Security researchers successfully connected to a truck's Wi-Fi within 14 seconds, re-flashed the ELD, and sent malicious messages, causing the truck to slow down.** The researchers reported the findings—which pose a serious security risk for commercial fleets, their safety and operational availability—to manufacturers and the US Cybersecurity and Infrastructure Security Agency (CISA), highlighting the potential for widespread disruptions.[150]

In May 2024, a European vehicle tracking and fleet management device provider experienced a data breach. The attacker revealed this on a dark web forum, exposing a vulnerability in the company's systems. Sensitive information, including GPS IMEI numbers, real-time vehicle tracking data, billing details, and customer account information, was compromised. The attacker claimed access to all internal systems across more than 40 countries and over 5,000 companies.[151]

In October 2024, a UK-based provider of vehicle tracking, fuel management, route optimization, and safety monitoring solutions for fleet operators fell victim to a cyber attack that affected a large portion of its services, requiring them to disable tracking systems and panic alarms in prison vans and courier vehicles. There was no compromise of customer data, but some employee data was affected.[152]

Smart mobility devices & services

As smart mobility IoT devices and services continue to grow in popularity and use, they represent high-risk targets within the Smart Mobility ecosystem. These services and devices hold sensitive PII and payment data from thousands of unique users.

Attacks on smart mobility devices and services have a direct impact on the safety, data, and operational availability of vehicles and Smart Mobility systems.

In April 2024, a ransomware attack on a US provider of real-time weather and traffic updates to drivers forced its staff to take immediate protective action by shutting down all systems. The shut-down affected the service's dynamic information boards, the official website, as well as the real-time camera system.[153]

In September 2024, a Philippines-based tollway operator experienced a data breach potentially exposing customer sensitive PII. The operator engaged cybersecurity experts and relevant authorities to thoroughly investigate the scope, strengthen compliance with local regulatory requirements, and mitigate the effects of the breach.[154]

In October 2024, the Dutch government announced that it will replace thousands of traffic lights after a security researcher discovered a critical security vulnerability in the traffic signal preemption system used to halt conflicting traffic and allow the emergency vehicles through. The exploit taps into an emergency radio signal used by ambulances and fire trucks to force traffic lights to go green so they can easily pass through intersections in the case of emergencies. According to the researcher, an attack could be executed from kilometers away and impact multiple intersections at once.

Tens of thousands of traffic lights will be replaced by 2030 with a new, secure platform, which uses mobile internet connections instead of radio signals.[155]

Insurance

Insurance companies are realizing that the cyber-threat landscape directly impacts premiums on connected vehicles. Insurers can use connected vehicle data to determine which locations, vehicle types, and components are usually more prone to cyber attacks, and calculate insurance premiums accordingly.

New behavior-based insurance models leverage aftermarket devices to share telematics with insurers to reduce premiums and insurance costs. However, threat actors can exploit vulnerabilities in these devices and manipulate data or communications to hack insurance companies' IT networks. Insurers and their telematics suppliers must work together to ensure that their telematics infrastructure is secure.

In January 2024, a security researcher found a vulnerability in a Japanese OEM's insurance broker website that exposed corporate cloud credentials. This gave him access to an email account with 657,000 emails, approximately 25GB, containing customer information, insurance policy PDFs, password reset links, OTPs, and more.[156]

Autonomous vehicles

Autonomous vehicle (AV) innovations are being introduced at a rapid pace by many stakeholders, including OEMs, smart mobility and ride-sharing services providers, and large technology enterprises. Other manufacturers are not far behind. Autonomous fleets are gaining momentum, delivering unprecedented efficiencies and customer experiences—but not without safety concerns and public distrust.

Autonomous vehicles provide remote access to core vehicle functionality, allowing threat actors to effectively attack at scale. They are equipped with and rely upon multiple sensors (e.g., GPS, LIDAR, cameras, millimeter wave radar, IMU) that receive data and directions from multiple sources, including the internet and satellites. It is therefore possible for attackers to prevent the sensor from retrieving useful data, cause it to retrieve incorrect data, or manipulate the sensor's function through crafted data.[157]

In February 2024, security researchers from Duke University demonstrated an attack that masked real objects from a vehicle's AV sensor systems without prior knowledge of the radar system in use.

In one demonstration of the attack, called MadRadar, researchers caused "phantom" objects to appear in a Doppler radar system, causing it to mistakenly believe that a vehicle traveling away from the sensor has changed direction, and is on its way to a head-on collision. According to the researchers, MadRadar detects and learns radar types "in microseconds" and adapts its attack instantly. This type of attack can be used to fool adaptive cruise control systems that use radar, into thinking the car in front of it is speeding up, when it is not, resulting in a frontal collision.[158]

In March 2024, security researchers from the University of California–Irvine and Japan's Keio University detected 15 vulnerabilities in 9 commercially available, first- and next-gen LiDAR systems that can allow direct spoofing of fake cars and pedestrians and the vanishing of real cars in the AV's eye. These attack capabilities on LiDAR sensors can be used to directly trigger various unsafe AV driving behaviors such as emergency brakes and front collisions.[159]

In May 2024, security researchers from Singapore proved that it was possible to interfere with AVs by exploiting their reliance on camera-based computer vision, making them ignore road signs using LEDs. The researchers were able to distort the appearance of road signs repeatedly in a stable manner, ensuring that every frame captured was distorted. The team tested their system using a real road and car with a camera used by a prominent Chinese AV developer. Two versions of this stabilized attack were developed by the team. GhostStripe1, which does not require access to the vehicle, employs a tracking system to monitor the target vehicle's real-time location and dynamically adjusts the LED flickering accordingly to ensure a sign isn't read properly. GhostStripe2 requires access to the vehicle and involves placing a transducer on the power wire of the camera to detect framing moments and refine timing control. The researchers claim GhostStripe1 and GhostStripe2 had success rates of 94% and 97%, respectively.[160]

In May 2024, security researchers from the University of Buffalo uncovered a vulnerability in multi-sensor fusion systems—a technology that integrates data from LiDAR, cameras, and radar sensors, and is commonly used in AVs. The researchers introduced a sophisticated attack method capable of simultaneously compromising all three sensor types using a single adversarial object. This object can be easily and inexpensively fabricated, allowing the attack to be executed with a high degree of stealth and flexibility. By deploying just two small adversarial objects, the researchers demonstrated that the attack could effectively render a target vehicle invisible to the victim AV's perception systems.[161]

04.

2024’S ATTACK VECTORS

Automotive and smart mobility stakeholders need to monitor and analyze evolving threats and their impact on cybersecurity posture

THREATS AGAINST ACES TECHNOLOGIES SHAPE THE ATTACK LANDSCAPE

Cyberattacks in 2024 became more sophisticated and frequent, targeting vehicles and backend systems, as well as smart mobility platforms, devices, and applications. The attack landscape was shaped by threats to Autonomous Driving, Connectivity, Electrification, and Shared Mobility (ACES) technologies.

Attackers found new zero-day exploits—a cyberattack vector that takes advantage of an unknown or unaddressed vulnerability—developed novel techniques, and exploited numerous vulnerabilities in software and hardware components used in SDVs, AVs, EVs, and EV charging equipment.

The Automotive and Smart Mobility ecosystem experienced a significant surge in telematics and application server attacks in 2024—from 43% in 2023 to 66% in 2024. **This dramatic increase is largely attributed to a sharp escalation in ransomware attacks targeting the mobility sector.**

APIs have been instrumental in enhancing connectivity between in-vehicle components, telematics and backend systems, as well as applications. However, they have also become a prime target for cyber threats. During 2022, API-based attacks surged by an alarming 380%, accounting for 12% of all incidents. Since then, API-related attacks have continued to rise steadily as threat actors exploit vulnerabilities to execute large-scale attacks. This trend has shown consistent double-digit growth, with a 13% increase in 2023 and a further 10% spike in 2024, **bringing API-related incidents to 17% of total attacks.**

API-related attacks outnumbered infotainment system attacks for the first time—which decreased from 15% in 2023 to 14% in 2024.

The trend is driven by threat actors' growing awareness and visibility of connected components. It shows the maturity of the automotive cybersecurity threat landscape, and the increasing efforts of threat actors to access sensitive data and control a wide range of mobility assets.

SIGNIFICANT SURGE IN TELEMATICS AND APPLICATION SERVER ATTACKS

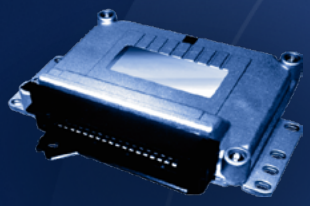
43%

IN 2023

66%

IN 2024

Incidents by Attack Vector



Source: Upstream Security

TELEMATICS AND APPLICATION SERVERS

Connected vehicles collect, transmit, and receive information from OEM backend servers and vehicle owners throughout their lifespan. This is achieved by using two types of servers: telematics servers, which communicate with the vehicle, and application servers, which interact with the vehicle's companion applications. Additionally, some vehicles have backend servers that communicate with third parties, such as insurance companies, fleet management, car rental and leasing companies, EV charging networks, and more.

A threat actor could exploit vulnerabilities in these servers to exfiltrate sensitive data and potentially launch attacks against vehicles while they are on the road.

- In January 2024, a security researcher found a vulnerability in a Japanese OEM's insurance broker website that exposed corporate cloud credentials. This gave him access to an email account with 657,000 emails, approximately 25GB, containing customer information, insurance policy PDFs, password reset links, OTPs, and more.[162]
- In March 2024, a US EV charging infrastructure installation firm experienced a data breach involving approximately 585GB of data. The breach exposed various business documents, including work invoices, price proposals, electric permits, and surveys. In addition, it exposed consumer information like PII, home photographs, and charger specifics.[163]
- In May 2024, a prominent European vehicle tracking and fleet management device provider suffered a data breach. The data breach was disclosed on a dark web forum by the attacker who exposed a vulnerability in the company's internal systems. This compromised sensitive information including GPS IMEI numbers, real-time vehicle tracking data, billing details, and customer account information. The attacker revealed he had access to all company internal systems, across more than 40 countries and over 5,000 companies.[164]
- In September 2024, a security researcher identified an Insecure Direct Object Reference (IDOR) vulnerability in the accident reporting application used by a leading car rental company, exposing customer PII in accident reports. The vulnerability allowed unauthorized access to any accident report by modifying the report numbers in the URL. The company was notified and quickly shut down the third-party application to restrict access to the compromised information.[165]

APIS

Connected vehicles as well as smart mobility devices and services use a wide range of external and internal APIs, resulting in billions of transactions per month. OTA and telematics servers, OEM mobile apps, infotainment systems, mobility IoT devices, EV charging management, and billing apps all rely heavily on APIs.

> ***APIs also present significant and fleet-wide large-scale attack vectors, resulting in a wide range of cyber attacks, such as sensitive PII theft, backend system manipulation, or malicious remote vehicle control.***

In contrast to hacking other types of systems, API hacking is relatively cost-effective and offers the ability to execute large-scale attacks. It requires relatively little technical expertise, uses standard techniques, and can be carried out remotely without special hardware.

In the last three years, the automotive industry and supply chains, as well as mobility devices and services, have experienced a significant increase in data and privacy breaches due to API-based attacks.

- In May 2024, a team of security researchers discovered multiple vulnerabilities in an EV charging station produced by a US EVSE vendor. The researchers found improper access control, improper certificate validation, and unverified password change vulnerabilities. These flaws could allow a malicious actor authenticated in the API to enable changing the system's password and access an adjacent network. The vendor published a security advisory addressing these vulnerabilities.[166]
- In June 2024, security researchers discovered vulnerabilities in a Korean OEM's dealer API that allowed them to register as a dealer, enabling them to take over any impacted OEM vehicles using only their license plate. **At the push of a button, the researchers demonstrated how they could take over a victim's vehicle—or gain access to vehicle owner PII, including name, email, and phone number—issue commands, and track exploited vehicles.** The researchers published the findings in September 2024 after the OEM patched the vulnerabilities.[167]
- In November 2024, a multinational company specializing in energy management and EV charging infrastructure, suffered a data breach. The hacker infiltrated the company's project management system and exploited a REST API vulnerability to extract 1.5TB of data, including 400,000 records and 75,000 unique emails of employees and customers.

The hacker posted a ransom demand on a dark web forum, threatening to publish the data if the company did not disclose the breach within 48 hours. The company confirmed an ongoing investigation and reported to actively contain the incident.[168]

INFOTAINMENT SYSTEMS

The in-vehicle infotainment system (IVI) is one of the most common attack vectors. It connects to the internet, and is exposed to installed applications and short-range communications with mobile phones and Bluetooth devices. As a result, it has access to PII. Additionally, IVI systems often connect to vehicle internal networks, posing a serious risk to the vehicle. IVI systems can be the path of least resistance for malicious software to penetrate internal systems.

- In January 2024, security researchers discovered seven vulnerabilities in European OEM vehicles and infotainment systems. Cataloged from CVE-2023-28895 through CVE-2023-28901, these vulnerabilities revealed several security weaknesses: hard-coded passwords that could allow unauthorized control over the Power Controller chip (a key component managing the vehicle's electrical functions); vulnerabilities that allowed interception and reading of vehicle diagnostic information through the CAN BUS network; risks of system crashes in the entertainment and navigation systems due to data overload; and flaws in the cloud services managing online vehicle services that could expose sensitive user data, such as trip details and vehicle statistics, by exploiting vehicle identification numbers.[169]
- Also in January 2024, security researchers discovered a vulnerability affecting all versions of head units, which are widely used by Japanese OEMs. This vulnerability, identified as CVE-2024-39339, resulted from a misconfiguration that can lead to the unintended disclosure of sensitive information (e.g., diagnostic log traces, system logs, head unit passwords, and PII).[170]
- In July 2024, a vulnerability known as CVE-2024-21462 was found in chipsets used in vehicle infotainment and telematics systems. This vulnerability, caused by a buffer-over-read weakness, could lead to a temporary Denial-of-Service if exploited.[171]
- In October 2024, a default credentials vulnerability, identified as CVE-2024-6245, was found in a Japanese OEM infotainment system. The Linux-related vulnerability allowed attackers to use common usernames and passwords to gain unauthorized access, affecting system integrity and availability.[172]

EV CHARGING INFRASTRUCTURE

Providing a reliable and safe charging infrastructure is essential to accelerating electric vehicle adoption. **But today, many chargers, charging infrastructure components, and related apps are vulnerable to physical and remote manipulation that can stop them from working reliably, expose EV users to PII theft, fraud and ransom attacks, and have widespread implications on the charging network, vehicles, or even the local electric grid.**

- In January 2024, security researchers found multiple vulnerabilities in a US-based EVSE's home charging station that could allow attackers to remotely access and control chargers. The security vulnerabilities involved flaws in the implementation of a reverse SSH tunnel, an outdated HTTP server, a deprecated NTP client with known vulnerabilities, a deprecated kernel, and device certificates with unlimited expiration time. **An attacker could authenticate to EVSE's central server, potentially creating their own tunnel, extending unauthorized access to each connected charger.** Following the discovery, security researchers actively collaborated with the company to address the vulnerability, which has been updated in a software release.[173]
- In February 2024, the UK's Office for Product Safety and Standards (OPSS) suspended sales of Spanish EV chargers for failing to comply with current cybersecurity regulations, raising concerns over potential risks to the national energy infrastructure.[174] **Hackers might gain access to thousands of non-compliant chargers and switch them all on at once, generating peak demands that disrupt the grid.**
- In April 2024, security researchers published a technical analysis PoC on the insecurity of Open Charge Point Protocol (OCPP) backend communication with the EV charging station (EVCS), identifying six zero-day vulnerabilities in 16 representative live EV charging management systems. The researchers managed to obtain EVCS IDs and OCPP backend links from various online resources. This led to various attack scenarios including man-in-the-middle, denial of service, firmware theft, and data poisoning. **They also developed a testbed to demonstrate the feasibility of launching switching attacks against the power grid** using compromised EVCSs, and recommended countermeasures to mitigate/prevent future cyber-attacks.[175]
- In May 2024, an EV charger manufacturer based in Belgium was targeted by threat actors who exploited QR codes on their charging stations to direct users to fraudulent payment pages.

Under EU regulations, ad-hoc payment solutions like QR codes are required at charging stations. The company has confirmed the discovery of several counterfeit QR codes on its equipment, which facilitated this financial theft by threat actors.[176]

- In August 2024, security researchers identified a critical vulnerability, CVE-2024-21550, in an open-source platform for managing electric vehicle (EV) charging stations via the Open Charge Point Protocol (OCPP). This flaw is a type of cross-site scripting (XSS) vulnerability that allows attackers to inject malicious HTML and JavaScript code through WebSockets into the platform's management interface. This breach allows unauthorized individuals to manipulate the interface or access sensitive information.[177]
- In November 2024, a data breach affecting multiple global Charging Point Operators (CPOs) led to leaked customer PII and OCPP from multiple countries including: UAE, Australia, Mexico, Puerto Rico, Guyana, Saudi-Arabia, Oman, and India. One common denominator among the CPOs is their apparent usage of an EV charging app developed by an Indian EV charging and energy management software provider. The data breach resulted in the exposure of roughly 116,000 records of consumer PII and sensitive data, including consumer names, charging station locations, vehicle details such as VIN numbers, raw keys, and tokens. The hacker, known for recently targeting the automotive industry, published the data on a deep-web hacking forum. While the attacker claimed the data originated from a US-based charging station, analysis revealed that it includes information from multiple global charging stations used by various OEMs.[178]

GPS/GNSS NAVIGATION SYSTEM

GPS/GNSS navigation systems are crucial for precise location tracking and efficient route guidance in vehicles. However, these systems are increasingly vulnerable to physical and remote attacks, such as signal spoofing and jamming. These attacks can disrupt navigation accuracy, expose users to privacy risks, and even compromise autonomous or connected vehicles' safety. **These vulnerabilities can also pose far-reaching consequences for transportation networks, vehicle fleets, and user trust in navigation technologies.**

- In May 2024, during a midair journey from Poland to the UK, a French-made corporate jet fell victim to a cyberattack. The pilots reported a 30-minute blockage of GPS and other navigation and communication signals. Authorities connected this incident to a large series of cyberattacks aimed at disrupting communication and signal infrastructure in the region. This attack created risks for aircraft, ships, and all forms of transportation operating in the area.[179]
- In May 2024, a security researcher found a critical vulnerability in a widely-used GPS car tracking app, affecting over 130,000 cars worldwide.The GPS brand was not revealed, but the issue allowed unauthorized access to real-time car locations due to weak security in the app's demo mode. **By changing the demo URL and cookie settings, the researcher could see car locations in different areas.** The researcher informed the company of the problem.[180]
- In August 2024, two vulnerabilities, CVE-2024-31214 and CVE-2024-24809, were found in an open-source GPS tracking system. These vulnerabilities stem from flaws in the device image file upload feature introduced in a specific version. The module is susceptible to path traversal and unrestricted upload of dangerous file types. If exploited, these vulnerabilities could lead to authentication bypass and remote code execution.[181]

THIRD-PARTY SERVICES

Third-party services enhance vehicle connectivity and user experience through features like remote diagnostics, infotainment, and fleet management. However, these services are susceptible to both physical and remote manipulation, including data breaches, unauthorized access, and service disruption. Such vulnerabilities can expose users to fraud, privacy violations, and ransom attacks. This can affect the entire vehicle ecosystem, compromising safety, and undermining trust in connected vehicle technologies

- In March 2024, an Indian OEM suffered a data breach through a third-party provider, resulting in the exposure of company data and customer PII. It remains unclear whether the OEM or the marketing provider have started an investigation or contacted law enforcement regarding the breach.[182]

- In May 2024, a security researcher discovered a vulnerability in a third-party application designed for American EV drivers that offers detailed insights into driving habits, charging behavior, and other vehicle-related metrics. The vulnerability, which involved plaintext storage of passwords and inadequate validation of credentials weaknesses, could potentially allow threat actors to gain full control of the system. The researcher reported this issue to the software developers, who acknowledged the vulnerability but indicated that they were testing it for a proper solution.[183]
- In September 2024, a US-based company specializing in AI-driven solutions for dealership scheduling and communication automation suffered a cyberattack compromising sensitive data. The threat actor leaked approximately 240,000 records of consumer PII, including VINs, and vehicle data such as mileage, repair orders, prices, and documents. It is still unknown whether the company has initiated an investigation or informed the relevant authorities regarding the breach.[184]

ECUS

Electronic Control Units (ECUs)—responsible for the engine, steering, braking, windows, keyless entry, and various critical systems—can be interfered with or manipulated. **Attackers try to manipulate ECUs and take control of their functions by running multiple sophisticated systems at the same time.**

- In April 2024, security researchers demonstrated a voltage glitching attack on microcontrollers (MCUs) used in the Automotive industry. This vulnerability allowed attackers to bypass Read Out Protection (RDP) and access protected firmware by manipulating the power supply, compromising the security of systems using these MCUs. The researchers disclosed the vulnerabilities to the manufacturer, who patched them.[185]
- In May 2024, a group of security researchers demonstrated a voltage glitching attack on MCUs embedded in various automotive Body Control Modules (BCMs), responsible for controlling power windows and mirrors, the immobilizer system, central locking, and more. By exploiting this vulnerability, they bypassed the 16-byte ID Code authentication, enabling unauthorized firmware extraction. An attacker could potentially access sensitive information, such as secret keys and vehicle control functions. The vulnerabilities were disclosed to the manufacturer and patched.[186]

- In September 2024, a US-based car dealer was charged with tampering with the odometers of over 200 vehicles, reducing their mileage by over 14 million miles. **The dealer used tools to alter odometer ECU readings, falsely documenting lower mileage on registrations. Each vehicle's mileage was reduced by an average of 65,000 miles, deceiving buyers.** The local authorities condemned the fraud, highlighting its impact on consumers and the used car market's credibility.[187]

SMART MOBILITY DEVICES AND INTELLIGENT TRANSPORTATION SYSTEMS

Smart mobility devices and intelligent transportation systems are crucial for reducing congestion, improving traffic management, sharing real-time traffic/weather data, and enhancing overall transportation efficiency. However, they are high-risk targets within the Smart Mobility ecosystem, containing real-time location data, PII, and payment information for millions of users, with attacks directly impacting safety, data, and operational availability.

Public transportation systems, electronic logging devices, and traffic signals and control systems are vulnerable to ransomware attacks, data manipulation, and physical and remote manipulation. When exploited, these vulnerabilities can disrupt traffic flow, compromise public safety, and expose transportation networks to fraud and sabotage, which undermines public trust in infrastructure and mobility systems.

- In March 2024, Security researchers from Colorado State University showed how ELDs can be accessed over Bluetooth or Wi-Fi connections to take control of a truck, manipulate data, and spread malware between vehicles.[188]
- In April 2024, a ransomware attack on a US provider of real-time weather and traffic updates to drivers along roads and highways forced its staff to take immediate protective action by shutting down all systems. The shut-down affected the service's dynamic information boards, the official website, as well as the real-time camera system.[189]
- In July 2024, research revealed a potential vulnerability in AV systems and EVs due to cosmic rays, which can disrupt critical electronic systems like microprocessors and sensors, causing malfunctions. This posed significant risks to vehicle reliability and safety. To mitigate the issue, researchers recommend modular redundancy to ensure functionality if one component fails, along with detection and correction systems to enhance resilience against cosmic ray-induced failures.[190]

- In September 2024, a Colombian company specializing in transportation ticketing and pass services, experienced a major data breach resulting in a leak of 800,000 documents, including sensitive PII and vehicle data. Security researchers discovered the breach happened due to unsecured cloud storage, which the company used to store its payment app data on.[191]
- In September 2024, a Philippines-based tollway operator experienced a data breach potentially exposing customer sensitive PII. The operator engaged cybersecurity experts and relevant authorities to thoroughly investigate the scope, strengthen compliance with local regulatory requirements, and mitigate the effects of the breach.[192]
- In October 2024, a security researcher discovered a critical security vulnerability in the traffic signal preemption system used in the Netherlands, resulting in the Dutch government replacing thousands of traffic lights with a more secure platform that uses mobile internet connections instead of short-range radio signals.[193]

MOBILE APPLICATIONS

Increasingly connected and software-defined vehicles allow OEMs to provide remote services and functionalities via vehicle companion apps and third-party apps, giving owners convenient access to critical functions via their smartphones. Mobile applications allow users to track vehicles' locations, open their doors, start their engines, turn on auxiliary devices, subscribe to premium features, and more.

The same apps that provide drivers with a digital experience can also be exploited by hackers to access the vehicle and backend servers. Companion applications may also have common software vulnerabilities, including open-source vulnerabilities, hard-coded credentials, and API/backend server weaknesses.

OEM companion and smart mobility apps can also be used to commit identity theft. Black hat actors can exploit vulnerabilities in mobile devices and application servers to obtain credentials and compromise private user information on a large scale.

- In April 2024, security researchers discovered two vulnerabilities, CVE-2024-33308 and CVE-2024-33309, in an Indian motorcycle manufacturer's companion app. The vulnerabilities allowed a remote attacker to escalate privileges via the Emergency Contact Feature and obtain sensitive information via an insecure API endpoint.[194]

- In June 2024, a cyber incident at a Japanese OEM's subsidiary led to a data breach of the OEM's companion application. The OEM stated that human error caused the unauthorized disclosure of consumers' PII, prompting a law enforcement investigation.[195]
- In June 2024, security researchers discovered another vulnerability in the same Indian motorcycle manufacturer's companion app, known as CVE-2024-35537. Researchers uncovered that the app insecurely handled the RSA key pair, allowing attackers to gain access to sensitive information via decryption.[196]

VEHICLE SENSORS

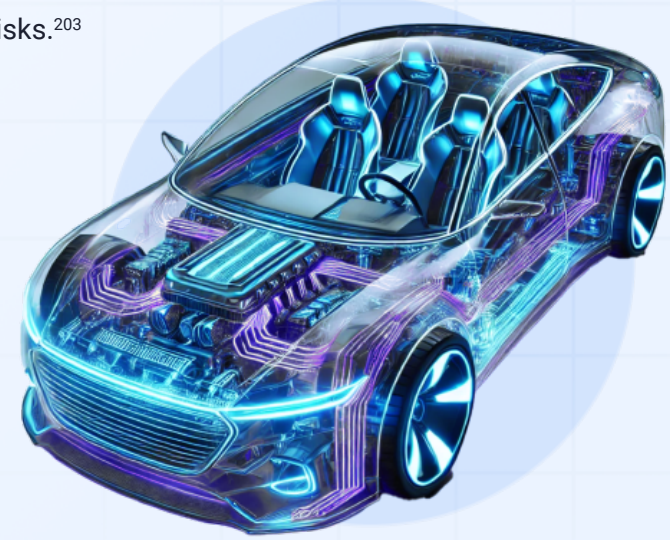
Sensors play a crucial role in modern vehicles, enabling critical functions such as object detection, collision avoidance, and real-time data collection for autonomous driving systems. However, sensors are vulnerable to both physical and remote manipulation, including spoofing, jamming, and data interference. **These vulnerabilities can lead to incorrect data interpretation, compromise vehicle safety, and disrupt essential functions, affecting connected and autonomous vehicles' overall reliability.**

- In February 2024, security researchers from Duke University were able to trigger hallucinations in AV sensor systems without prior knowledge of the radar system in use. In one demonstration of the attack, called MadRadar, researchers caused a hallucination in a Doppler radar system, causing it to mistakenly believe that a vehicle traveling away from the sensor has changed direction, and is on its way to a head-on collision.[197]
- In September 2024, security researchers from the University at Buffalo identified vulnerabilities in autonomous vehicles' AI systems, specifically in mmWave radar, LiDAR, and cameras. They discovered that 3D-printed objects and metal foils, called "brick masks," can mislead radar detection, making vehicles invisible. The research highlights the need for stronger defenses in autonomous vehicle security.[198]
- In October 2024, a vulnerability, named CVE-2024-39081, was found in a tire pressure monitoring system. This flaw allows attackers to perform a man-in-the-middle attack via Bluetooth, enabling them to manipulate TPMS data and send false alarms to users through the app. A vulnerability that can be exploited to mislead users regarding tire condition and interfere with vehicle safety monitoring systems raises significant safety concerns.[199]

CAN BUS

The CAN BUS is essential for communication between various electronic components in modern vehicles, facilitating real-time data exchange for functions like engine control, braking, and safety systems. However, the CAN BUS is vulnerable to physical and remote manipulation, including message injection, eavesdropping, and spoofing attacks. These vulnerabilities can disrupt vehicle operations, compromise safety, and lead to unauthorized control of critical systems, affecting the overall security and reliability of connected vehicles.

- In March 2024, researchers reverse-engineered the SecOC system—which provides functionality necessary to verify the authenticity and freshness of Power Distribution Unit (PDU) communication between ECUs[200]—in a popular Japanese sport utility vehicle, extracting cryptographic keys that secure vehicle communication. They retrieved firmware, identified weaknesses, and located keys in RAM by bypassing the power steering ECU's debug port. **They could control drive-by-wire features like Lane Keep Assist (LKA) and Adaptive Cruise Control (ACC). Researchers emphasized the importance of strong cryptographic protocols and secure key management in automotive systems.**[201]
- In March 2024, thousands of vehicle owners in the UK became eligible to join a lawsuit against a Japanese OEM over a rise in vehicle thefts. The suit claims that a specific component within the CAN BUS enables thieves to bypass security and steal cars without damage. Over 120,000 vehicles are allegedly at risk, and the claim seeks compensatory damages for contract breaches and consumer rights violations.[202]
- In April 2024, researchers discovered a cybersecurity vulnerability affecting several Indian e-scooter manufacturers. The security research used a remote CAN BUS injection attack, which enables attackers to halt e-scooters remotely. Security researchers informed Indian OEMs and authorities to mitigate cybersecurity risks.[203]



REMOTE KEYLESS ENTRY SYSTEMS

Modern vehicles are protected against theft by using remote keyless entry systems that include smart key fobs with very strong cryptography and immobilizers. Remote keyless entry systems may, however, create the exact opposite effect, as vehicle theft and break-ins are on the rise.

Wireless key fob manipulation is used by black hat attackers to attack freely. Publicly available hacking tutorials and devices sold online without registration have made these attacks popular.

Whenever a wireless key fob—which is equipped with a short-range radio transmitter—is within close proximity of the vehicle, it transmits a coded radio signal to the receiver unit. Using devices that intercept and relay, replay, or jam the radio signal, communication between the fob and vehicle can be manipulated.

The communication between the key fob mechanism and the vehicle can be attacked in several ways:

Relay attacks using a "live" signal

In relay attacks, hackers intercept normal communication between the key fob and the vehicle—even when the key fob signal is out of range. Hackers can amplify the radio signal using a transmitter or repeater that is placed near the car, which amplifies and relays a message to unlock and start the vehicle's engine. Thieves increasingly use this type of attack to intercept the signal from a key fob located inside a vehicle owner's house.

Replay attacks using a stored signal

In another type of relay attack, hackers intercept messages sent between the key fob and the vehicle and store them for later use. After obtaining the relevant message, the hacker can unlock the car's doors or start its engine whenever they want.

Reprogramming key fobs

A more sophisticated and expensive device can reprogram the key fob system, rendering the original key useless. The reprogramming device—which connects to the OBD port, making it relatively easy for car thieves to gain full control over vehicles—can be legally obtained online and is used by authorized mechanics and service centers.

Jamming communication between a key fob and a vehicle

It is also possible for car thieves to break into vehicles using a signal jammer that blocks communication between the key fob and the vehicle. This device prevents the owner from locking the vehicle, allowing thieves to gain access.

Impersonating the wireless key fob ECU with CAN injection

A new attack method favored by hackers is CAN Injection, widely used by criminals to steal vehicles. It is possible for attackers to bypass the entire remote keyless entry system with a CAN injector device that connects to the CAN wires and impersonates the wireless key fob ECU.

Phone-as-a-Key (PaaK)

The "Phone as a Key" (PaaK) feature transforms smartphones into digital keys through technologies like Bluetooth Low Energy (BLE), Near Field Communication (NFC), and Ultra-Wideband (UWB). While PaaK enhances convenience by eliminating the need for traditional key fobs, it also introduces new cybersecurity vulnerabilities, including weak signal encryption, flaws in the vehicle's companion app, or vulnerabilities in smartphone operating systems, potentially gaining unauthorized access to the vehicle.

Attacks on remote keyless entry systems continued to make headlines in 2024 as vehicle thefts continued to rise:

- In May 2024, a US OEM was sued over a defect in key fobs on its latest sports car models. The rise in thefts of these vehicles has been attributed to social media videos and online guides that reveal how to bypass the key fob's security. The lawsuit points out that the key fobs operate on unsecured commercial radio frequencies, which leaves them open to interception and facilitates vehicle theft.[204]
- In May 2024, a Chinese research group discovered a vulnerability in a US EV's Ultra-Wideband (UWB) technology, making it susceptible to relay attacks. The researchers found that the vehicle's UWB system signals could be intercepted, captured, and manipulated. The research demonstrated how attackers could trick the vehicle into falsely identifying the key fob was within proximity, enabling them to unlock and start vehicles remotely. The OEM acknowledged the issue and reported investigating the vulnerability, working on potential mitigations to enhance UWB security.[205]
- In July 2024, a method of exploiting known vulnerabilities in Korean OEM EV keyless systems began trending on social media. A social media account showcased a sophisticated tool, called an emulator device, that combines radio transmissions to intercept and clone the communication between a vehicle's key and the vehicle itself. The device enables hackers to mimic the key's signal, allowing them to unlock the vehicle and start it as if they were using the original key, in less than a minute.[206]
- In September 2024, Chinese security researchers demonstrated a Bluetooth Low Energy (BLE) relay attack to relay information between the PhoneKey system and the vehicle at the protocol level. **Protocol-based relay attacks have the advantage of not requiring physical proximity between the attacker, who can be anywhere in the world, and the vehicle.**[207]
- In November 2024, security researchers identified vulnerabilities in the Remote Keyless Entry (RKE) systems of several Asian OEMs. The study revealed that RKE systems across these brands remain susceptible to attacks that exploit weak rolling code implementations to gain unauthorized access. The vulnerabilities stem from insecure cryptographic schemes, outdated encryption algorithms, and inadequate countermeasures.[208]

BLUETOOTH

Bluetooth is a wireless communication technology that uses radio frequencies to connect devices and share data. Bluetooth Low Energy (BLE) is the standard protocol used for sharing data between devices that vendors have adopted for proximity communication to unlock millions of vehicles, residential smart locks, commercial building access control systems, smartphones, smartwatches, laptops, and more.

- In May 2024, Swiss electric vehicle chargers were found to have two vulnerabilities, identified as CVE-2023-0863 and CVE-2023-0864. These vulnerabilities, which can be exploited via Bluetooth Low Energy (BLE), include improper authentication and clear text transmission of sensitive information, potentially allowing control over the station to eavesdrop on communication or alter configurations.[209]
- In August 2024, a security researcher uncovered critical vulnerabilities in infotainment systems used by major OEMs. **These flaws allow the extraction of sensitive data such as GPS coordinates from vehicles running Android Automotive OS, even without internet connectivity.** The vulnerabilities also enable malware to spread through malicious USB devices and Bluesnarfing, where attackers infiltrate paired devices via Bluetooth.[210]
- In September 2024, a security researcher demonstrated BLE (Bluetooth Low Energy) relay attacks on vehicle phone-as-key systems, enabling remote unlocking without proximity. Using the Gattacker tool, the researcher exploited vulnerabilities in US and Chinese EV BLE systems, which lacked encryption and proper pairing mechanisms. Vehicles with pairing PINs were not affected. The findings were reported to manufacturers, but fixing the issue was considered complicated due to dependencies on multiple suppliers.[211]

WIFI

Wi-Fi is essential for seamless connectivity in modern vehicles, allowing for real-time data exchange, infotainment, and over-the-air updates. However, Wi-Fi networks in vehicles are vulnerable to physical and remote manipulation, including unauthorized access, data breaches, and denial-of-service attacks. These vulnerabilities can expose users to privacy risks, fraud, and potential disruptions in vehicle operations—impacting the security and reliability of connected vehicles and the broader transportation ecosystem.

- In March 2024, security researchers demonstrated a Man-in-the-Middle (MiTM) phishing attack on American OEM EVs. They created a fake 'OEM Guest' Wi-Fi network, tricking users into logging into a fake OEM page. This allowed the researchers to capture credentials and bypass two-factor authentication, enabling them to add a new Phone Key and unlock the vehicle without the owner's knowledge. The researchers suggested using a physical Card Key for added security, but the OEM claimed the process was intentional and not a security flaw.[212]
- In August 2024, a major US port, which manages key transport hubs including an international airport, suffered a cyberattack. The attack disrupted numerous systems, causing severe delays in check-in processes, and disabling Wi-Fi and display systems crucial for flight information. Port authorities have investigated the attack with federal officials and have not yet confirmed if any passenger data was compromised.[213]

V2X ATTACKS ARE EXPECTED TO RISE DRAMATICALLY

Telematics, smart mobility, in-vehicle and mobility IoT, and other services require connected vehicles to share data with servers, apps, and various vehicle components.

Connected vehicle-to-everything (V2X), is the collective term for the technology enabling vehicles, infrastructure, and other active road users to be in constant communication by leveraging existing cellular network infrastructure. There are seven primary modes of vehicle connectivity:

V2I	**Vehicle to Infrastructure**	Wireless exchange of data between the vehicle and road infrastructure to get information about accidents, construction, parking, and more.
V2V	**Vehicle to Vehicle**	Data-sharing between vehicles, typically including location, to avoid traffic jams and accidents.
V2N	**Vehicle to Network**	Communication between vehicles, traffic lights, lane markings, and other forms of the road infrastructure network.
V2C	**Vehicle to Cloud**	Communication between a vehicle and cloud-based backend systems allows the vehicle to process information and commands sent between services and applications.
V2P	**Vehicle to Pedestrian**	Communication between vehicles, infrastructure, and personal mobile devices to inform about the pedestrian environment—enabling safety, mobility, and environmental advancements.
V2D	**Vehicle to Device**	The exchange of data and information between vehicles and electric devices that directly connect with them.
V2G	**Vehicle to Grid**	Two-way power flow between vehicles and the power grid, which can create major problems across a city or nation's transportation grid if exploited.

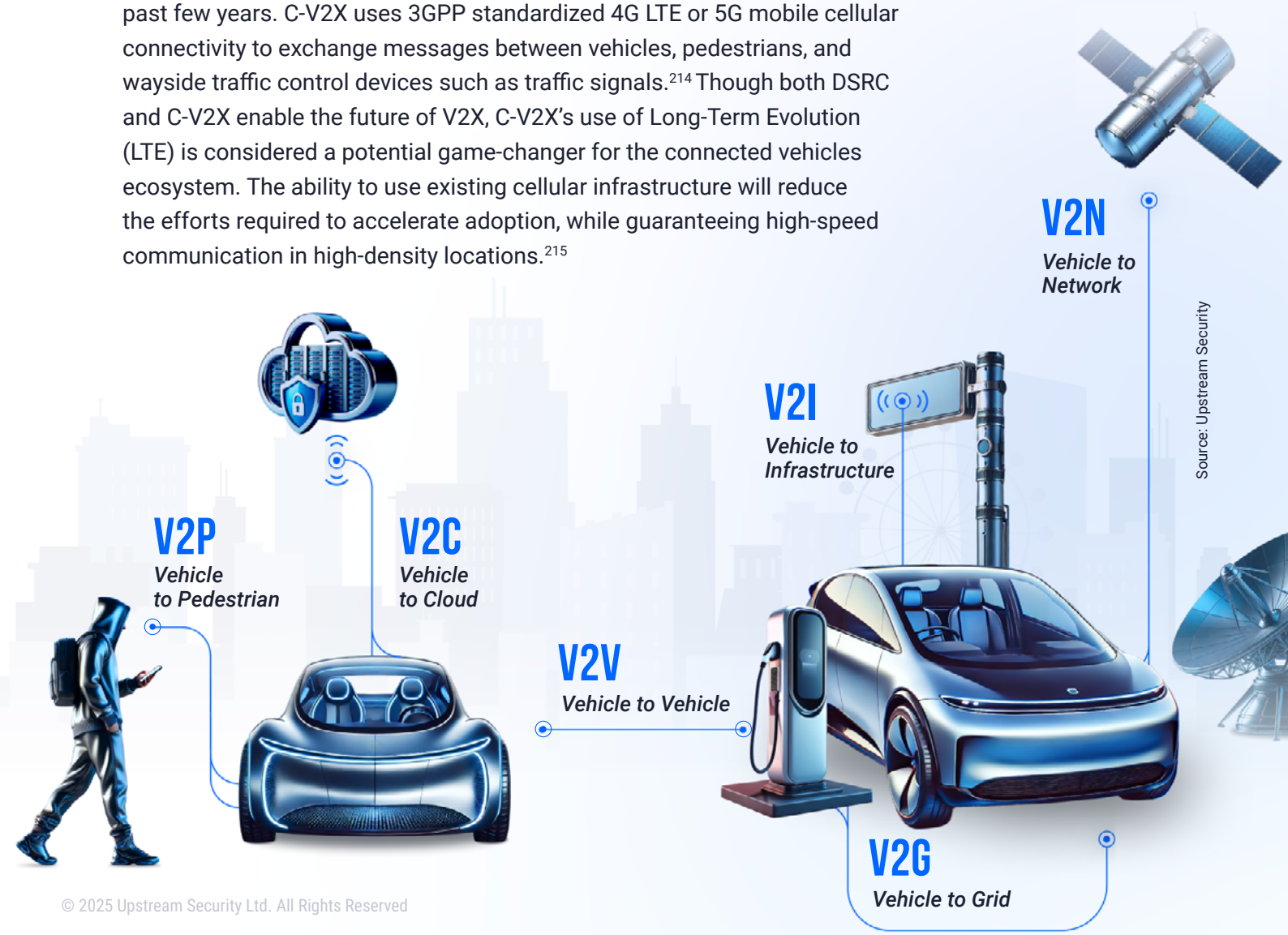
> ***Within a few years, vehicles will constantly communicate and interact with their surroundings through APIs, sensors, cameras, radars, mobility IoT modules, and more—enhancing vehicle operation by processing various inputs from the environment.***

The most profound addition will be the ability of a vehicle to communicate with other vehicles or devices on the road, and receive data from external sources such as EV chargers or road infrastructure.

It is expected that vehicles will interact with the entire environment around them, considering pedestrians and cyclists that may enter their part, traffic conditions ahead, and data from traffic lighting and control systems at intersections.

Some elements of V2X technology are already in use today. V2X is a key component of Advanced Driver Assistance Systems which use intelligent transportation systems and sensors to enhance autonomous driving and smart cities. OEMs also use V2X technology to reduce traffic congestion by providing vehicles with real-time road conditions updates. This helps drivers make safer, more informed decisions. They also enable cars to share data like speed and position in real-time, improving road safety by alerting drivers to potential accidents. Additionally, V2X EV charging technology, such as Vehicle-to-Home (V2H), allows EVs to reduce utility bills by discharging power during periods of high demand and recharging when demand and prices are lower.

The future of V2X will rely on new wireless communication technologies, such as DSRC and Cellular V2X (C-V2X), which have been in testing for the past few years. C-V2X uses 3GPP standardized 4G LTE or 5G mobile cellular connectivity to exchange messages between vehicles, pedestrians, and wayside traffic control devices such as traffic signals.[214] Though both DSRC and C-V2X enable the future of V2X, C-V2X's use of Long-Term Evolution (LTE) is considered a potential game-changer for the connected vehicles ecosystem. The ability to use existing cellular infrastructure will reduce the efforts required to accelerate adoption, while guaranteeing high-speed communication in high-density locations.[215]



In April 2023, the FCC approved C-V2X technology for connected vehicles ahead of the final national framework for intelligent transportation systems (ITS) rules. The FCC's Public Safety and Homeland Security Bureau, the Engineering and Technology Bureau, and the Wireless Telecommunications Bureau granted a joint request submitted by automotive manufacturers, equipment manufacturers, and state departments of transportation seeking a nationwide waiver of several FCC rules to permit deployment of C-V2X technology in the upper 30 MHz of spectrum in the 5.895-5.925 GHz band.[216]

The FCC granted 14 waiver requests in April 2023, 17 waiver requests in August 2023, eight waiver requests in November 2023, and 11 waiver requests in April 2024 to organizations, including State departments of transportation. As of April 2024, a total of 50 waivers have been granted.[217]

Over the last five years, the US Department of Transportation (DOT) invested $61.5 million in V2X technology research and deployment through the FHWA Turner Fairbank Highway Research Program, with $12.5 million in follow-on research projects budgeted for fiscal year 2024.[218]

In November 2023, the DOT issued a formal withdrawal notice of a previous proposal to mandate Dedicated Short Range Communications (DSRC)-V2V communications technology in all new light vehicles, because DSRC—which is not compatible with the C-V2X standard— will no longer be allowed in the 5.9 GHz band after a to-be-determined transition period.[219]

In August 2024, the DOT launched its framework to deploy vehicle-to-everything technology nationwide—officially releasing the National V2X Deployment Plan.[220]

The plan sets the DOT's vision, aspirational goals, and milestones, and issues a call to action for stakeholders, including government at all levels, public agencies, and the private sector. The aspirational goals and targets do not imply a legislative, regulatory mandate or dedicated federal funding. The plan instead offers a path that demonstrates federal leadership and allows government and industry to work together.

Along with the plan, the DOT's Federal Highway Administration (FHWA) announced that it is awarding $60 million in grants under the Saving Lives with Connectivity: Accelerating V2X Deployment program to advance connected and interoperable vehicle technologies. The grants will fund the large-scale deployments of V2X technologies in several states, including Arizona, Texas, Utah, Colorado, and Wyoming—and will serve as national models to accelerate and spur new deployments of V2X technologies.

05.

CYBER THREATS FROM THE DEEP AND DARK WEB

Cyber threat intelligence uncovers deep and dark web risks while helping automotive and smart mobility stakeholders proactively mitigate escalating cyber risks

WHAT IS THE DEEP AND DARK WEB?

The internet has multiple layers, some not indexed. There are three main internet layers: clear, deep, and dark. Access to each layer requires different know-how and tools. On dark web forums, for example, users must know the unique resource location address (i.e., no domain names exist on the dark web), use a special browser, and often demonstrate familiarity with specific topics to the site admin to gain access.

The first layer of the internet is the clear/surface web. It is the smallest yet most familiar part of the internet, requiring only a web browser to access.[221] In this part of the web, information is indexed by popular search engines, making it highly accessible and relied on by people every day.

CLEAR WEB

- *Automotive and cyber public media coverage and news*
- *Verified researchers' public blogs and reports*
- *Academic or research papers*
- *Car enthusiasts and forums*
- *Social media*
- *Code-sharing websites*
- *File-sharing websites*

The second layer of the internet is the deep web—which accounts for 96% of all web pages on the internet.[222] Data on this part of the web is not indexed by search engines, either because it is behind a sign-in (e.g., a paywall), or because its owners have blocked web crawlers from indexing it. For the average person, the deep web includes paid content, subscription websites, private groups, and private business websites. For hackers, the deep web also includes imageboards, which host anonymous, provocative, and borderline illegal content.

DEEP WEB

- *Private social media groups*
- *Private messaging apps*
- *Paste sites*
- *Private car-tuning or hacking forums*

The third, and final layer of the internet is the dark web—a fairly hidden part of the web where malicious activities, crime, and stolen data are available. To access dark web forums, users must use a special browser (e.g., Tor), know the site URL (i.e., no domain names on the dark web), and often demonstrate familiarity with specific topics to the site admin to gain access. Forums or pages are often managed by moderators, and suspicion is always high due to a lack of transparency among users and also because of the type of information in forums.

DARK WEB

- *Malicious paste sites*
- *Illegal marketplaces*
- *Image boards*
- *Closed hacking forums*
- *Illegal services for hire*
- *Legitimate platforms with malicious actors (e.g., Tor, Telegram, etc.)*

Dark web hackers often rely on proxy servers and the Tor browser to maintain anonymity. They use a tool called proxychain to chain several (usually 3-5) proxy servers. As a result, the attacker's packets pass through multiple proxy servers. Hackers intentionally use proxy servers in rival countries to prevent one country from sharing security information (e.g., proxy logs) with another, making it more difficult to identify them.

In 2024, Upstream's AutoThreat® team significantly expanded the scope of its deep and dark web threat actor mapping and analysis to include 1,133 active threat actors, up from 300 in 2023. The findings targeted OEMs, Tier-1 and Tier-2 suppliers, EV charging stakeholders, as well as smart mobile IoT devices and platforms. This data, combined with the fact that over 43% of deep and dark web cyber activities in 2024 had the potential to impact thousands to millions of mobility assets, shows that automotive and mobility stakeholders must have access to deep visibility and insights into cyber threat intelligence to proactively protect themselves.

43%

OF DEEP AND DARK WEB CYBER ACTIVITIES IN

2024

HAD THE POTENTIAL TO IMPACT THOUSANDS TO MILLIONS OF MOBILITY ASSETS

BELOW THE SURFACE: UNVEILING CYBER RISKS IN THE DEEP AND DARK WEB

Most of the internet is private, with the deep and dark web accounting for 95%-99%, according to some estimates.[223] You can find a wide variety of automotive-related content on deep and dark web forums, marketplaces, mobile messaging applications, and paste sites.

Consumers rely on web forums to find information that OEMs are unwilling to share with them—specifically information that can help them pirate-fix their vehicles or manipulate systems. Additionally, marketplaces offer auto parts, components, chips, software, and other items for sale in violation of manufacturers' terms and agreements. Many vehicle owners engage in these activities without realizing the dangers of tampering with highly complex automotive technology.

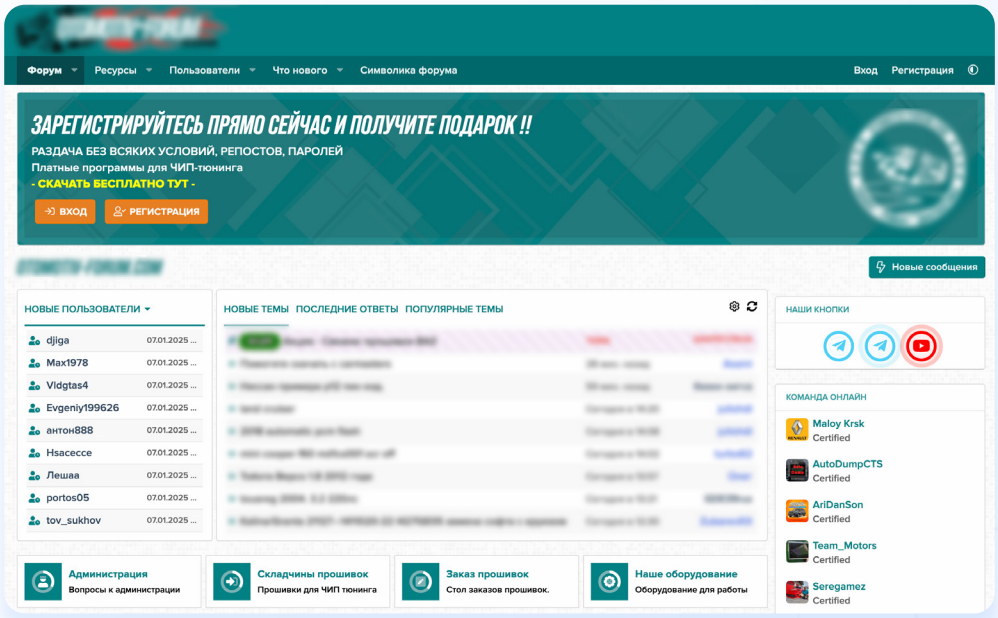
These activities can impact automotive stakeholders and insurance companies. Vehicles that have been tampered with may report false information that seems legitimate. In an extreme case, threat actors can gain access to OEM or insurance company servers by reverse engineering data used to authenticate vehicles.

Forums

On the deep and dark web, there are automotive-related forums dealing with sharing or selling automotive software, chip and engine tuning, infotainment cracking, diagnostics cracking, reverse engineering, key-fob modifications, immobilizer hacking, and more.

It is not uncommon for people to ask about self-programming their vehicles for a variety of reasons, such as gaining access to premium features or claiming the right to repair. Additionally, ECU remapping lessons, guides, software, and tuning file demos are readily available.

In August 2024, Upstream's AutoThreat® PRO team uncovered a threat actor offering cracked diagnostic software and unauthorized access to diagnostic tools on a popular deep web automotive forum. **These tools enable users to perform advanced diagnostics, firmware updates, and custom configurations that are usually limited to certified users and service centers.** This unauthorized software bypasses standard security protocols, allowing extensive access to vehicle systems and critical functions.



Example of a deep-web automotive forum

Source: Upstream Security

The rise of cracked diagnostic software and tools on deep and dark forums introduces substantial risks, undermining OEM security measures and compromising connected vehicle systems across multiple platforms.

Marketplaces

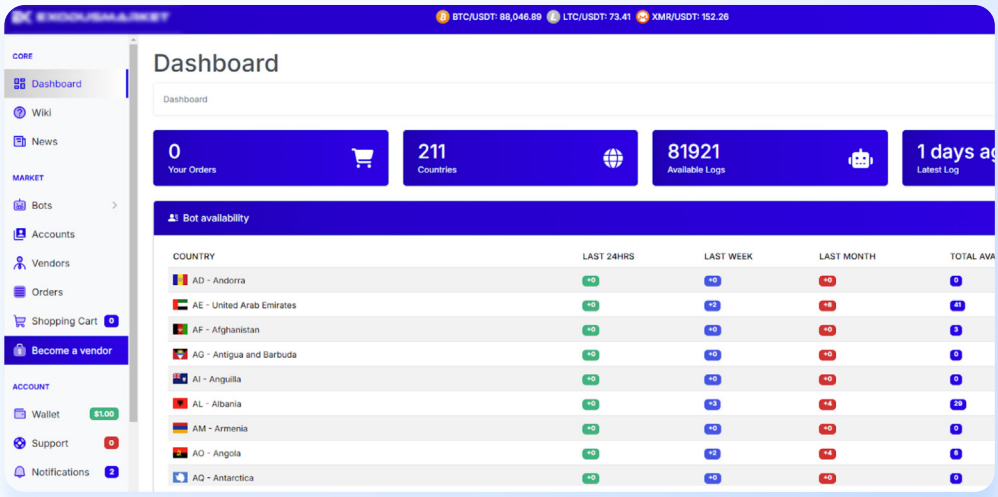
Dark web marketplaces are commercial websites that require specialized browsers, like Tor or I2P, and registration to access. They function primarily as black markets—brokering transactions involving drugs, weapons, cyber-arms, stolen data, forged documents, and other illicit goods.[224]

Some automotive-related dark web marketplace listings offer vehicle-related "products" and services like forged documents, and user credentials for automotive applications and smart mobility services (e.g., OEM connected car services, shared mobility services).

Dark web marketplaces have many automotive-related discussions and offerings:

- Instructions and guides related to infotainment hacking, CAN BUS reverse engineering, chip tuning, and software hacks or illegal upgrades
- The sale or exposure of OEM-related information and credentials stolen in data breaches
- Information and sales of tools for vehicle theft or modification, including key signal grabbers, key-fob programmers, GPS jammers, radar detectors, and more
- Hacks or fraud related to car-sharing or ride-sharing accounts
- Sales of fake driving licenses or automotive insurance

In June 2024, Upstream uncovered leaked credentials from multiple OEMs and dealers on dark web marketplaces offered by black hat threat actors.[225]



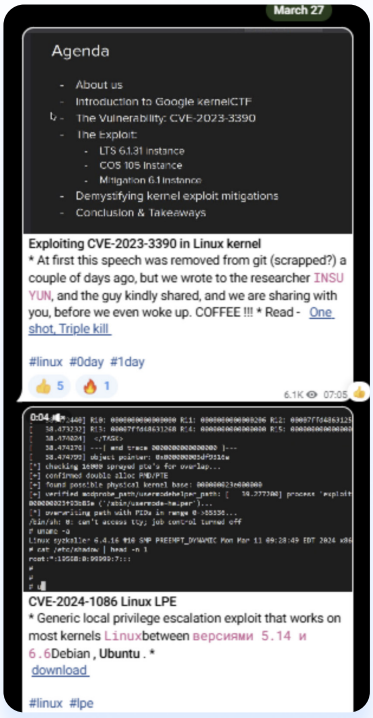
Example of a dark web marketplace with leaked dealer credentials

Source: Upstream Security

Messaging Applications

Mobile messaging applications have become increasingly popular for illicit activities. Popular messaging applications—such as Telegram, Discord, Signal, and WhatsApp—are actively used to share hacking methods, and trade in stolen credit cards, account credentials, exploitations of vulnerabilities, leaked source codes, and malware. Applications like these have replaced secretive, hard-to-navigate dark web forums.

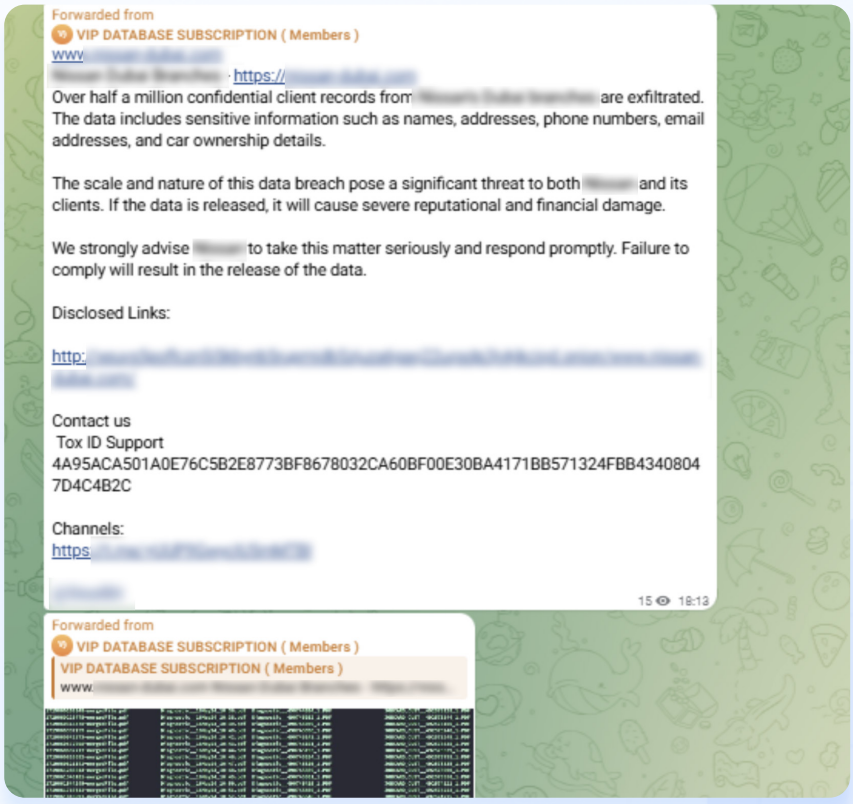
In March 2024, Upstream identified a cybercrime Telegram channel with more than 16,000 members that published information about Linux kernel exploits, affecting many large OEMs.[226]



Source: Upstream Security

Exploits found on the cybercrime Telegram channel

In October 2024, Upstream discovered a post on a ransomware Telegram channel, showcasing the results of a ransomware attack on a Japanese OEM. The stolen data included sensitive customer PII such as names, addresses, phone numbers, email addresses, and vehicle ownership information.[227]



Source: Upstream Security

Example of a Telegram message related to stolen OEM data

DEEP AND DARK WEB THREAT ACTORS

White hats (security researchers)

Cybersecurity researchers leverage their technical expertise to uncover vulnerabilities within organizations and across industries. To remain effective, they must continuously stay informed about the latest attack vectors, emerging trends, and advancements in enabling technologies. **Many researchers publicly share their findings—including vulnerability exploits and specialized vehicle toolkits—on platforms such as GitHub. While this openness fosters collaboration and innovation, it also inadvertently provides malicious actors with access to these insights, potentially amplifying cybersecurity risks.**

In December 2024, a security researcher published an exploit targeting a vulnerability in the Linux kernel, enabling privilege escalation and unauthorized control over affected systems.[228] Shortly after, the exploit was shared on a malicious Telegram channel with tens of thousands of members, many of whom are black hat actors with malicious intentions.[229] The widespread dissemination of this exploit through the channel significantly raises the risk of its deployment in attacks, particularly against Linux-based infotainment systems used by various OEMs. Such attacks could lead to unauthorized access, data breaches, or disruptions of critical vehicle functionalities.

Black hats

Black hat hackers compromise cybersecurity with malicious intent and participate in a wide range of activities on deep and dark web forums and marketplaces. **When black hat hackers publish exploits for long-range vulnerabilities in deep and dark web forums, they expose many other threat actors to exploits that could crash or control vehicles, which may result in serious safety risks on a large scale.**

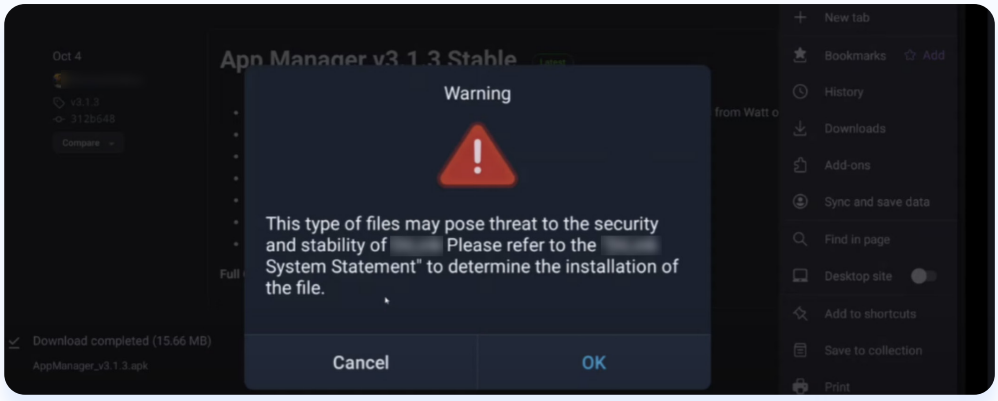
In August 2024, Upstream discovered that black hat hackers published an exploit for an OpenSSH vulnerability on a cybercrime forum, potentially impacting multiple OEMs. This vulnerability could allow code execution, denial of service, and privilege escalation, particularly affecting multiple OEM infotainment systems. Additionally, the exploit may enable attackers to execute commands on affected systems remotely.

Gray hats blur the line between black and white hats

Traditionally, the term black hats represents malicious actors seeking to exploit vulnerabilities, while the term white hats represents cybersecurity researchers working to improve defenses. **Nevertheless, the distinction is progressively fading in the Automotive industry—who's becoming more connected and software-defined—giving rise to "gray hat" involvement that now includes consumers who modify their vehicles or jailbreak components or features for customization purposes.**

In March 2024, Upstream revealed that guidelines for jailbreaking an in-vehicle infotainment (IVI) system were published on a deep web platform.[230]

The instructions outlined methods to block OTA updates, enable users to sideload unauthorized third-party apps, retain certain unsupported features like hands-free lane centering, and prevent potential software restrictions from being introduced in future updates. Two methods were described: one using an app manager installed directly from the IVI browser, and the other involving file sideloading via USB. Both approaches bypassed system restrictions to unlock hidden functionalities.



A warning prompt displayed during the instructions for blocking OTA updates on the impacted infotainment system

Source: Upstream Security

Fraud operators

Fraud operators typically use the deep web to buy and sell diagnostic tools, software, chip tuning services, and mileage-fixing services. Fraud operators are driven by a range of motivations, from financial gain to the exploitation of system vulnerabilities for competitive or malicious purposes. These actors often target high-value opportunities such as vehicle financing schemes, warranty claims fraud, and counterfeit parts distribution, leveraging weak points in connected vehicle systems or supply chain processes. **With the rise of connected and software-defined vehicles, they are increasingly exploiting digital platforms to gain access to premium features. Their actions not only result in financial losses but also erode consumer trust and compromise safety and operational reliability.**

In March 2024, a high-profile threat actor on a deep web marketplace offered unauthorized access to diagnostic software, electronic parts catalogs, and repair manuals for certain vehicles, with remote installation via TeamViewer. This fraud operator, known for active engagement in automotive forums, provided a range of unauthorized services, bypassing OEM terms and conditions, policies and safety measures.[231]

The fraud operators' website

Source: Upstream Security

Car enthusiast

Many car enthusiasts—people with a passion for vehicles and how they operate—are active on different automotive forums on the deep web. They offer advice, ask questions, discuss problems and bugs found in their vehicles, and even share automotive files or links to unofficial software updates.

Information posted on forums by car enthusiasts can be concerning for two reasons. The first concern is that malicious threat actors often monitor these forums, exploiting reported bugs or vulnerabilities for their own gain. The second is that files and links shared on these platforms are often unreliable and may contain malware, spyware, or ransomware, potentially compromising security and voiding warranties.

In June 2024, a car enthusiast published a jailbreak on a deep web platform, allowing third-party apps to be installed on a widely used automotive infotainment system. This active enthusiast, with extensive technical knowledge and experience, shares technical guides and methods for bypassing official app installation restrictions on forums. This issue underscores the growing challenges in securing automotive systems from unauthorized modifications, which can introduce potential vulnerabilities to connected vehicle platforms.

NEW AUTOMOTIVE AND SMART MOBILITY REVENUE STREAMS ARE AT RISK

Threat actors are increasingly exploiting opportunities for bypassing or jailbreaking premium features and systems, posing considerable risks to both vehicle and device cybersecurity, as well as data-driven monetization.

In May 2024, a high-profile threat actor offered unauthorized remote and non-remote services, such as firmware modifications for select electric vehicles.[232] Remote services provided by this threat actor included root access capabilities for certain vehicle models, enabling activation of hidden features and bypassing paid subscriptions. Additional services listed included region-specific configuration adjustments, disabling safety systems such as airbags, and providing unauthorized access to diagnostic software.

In September 2024, Upstream tracked a popular threat actor selling rooted infotainment modules with unlocked LAN access and SSH-based root privileges.[233] According to the threat actor, these modified units could be delivered to multiple countries, providing customers with advanced access to OEM-restricted features.

> ***These activities highlight the broader challenge facing the automotive industry in safeguarding connected vehicle systems from unauthorized modifications, firmware changes, and expanded diagnostic access. This raises critical questions about the resilience of current cybersecurity measures across various OEM platforms.***

As threat actors gain expertise in specific IVIs, ECUs, and TCUs, it becomes critical for OEMs and the supply chain to establish visibility into the deep and dark web threat landscape so they can strengthen their security protocols to safeguard against them.

RANSOMWARE ACTORS EXPLOIT AUTOMOTIVE STAKEHOLDERS, LEVERAGING THE DEEP AND DARK WEB

Malicious actors increasingly target automotive and mobility stakeholders—including OEMs, suppliers, and even EV charging infrastructure—with ransomware attacks. Any element of the supply chain can pose a risk to OEMs, service providers, or smart mobility devices and applications.

> ***Ransom attacks could severely affect operational availability and production, as well as expose sensitive customer information, system credentials and more.***

To extort money, attackers typically maintain a 'leak site' on the dark web. This is where they reveal stolen data, and share information related to their attacks and victims.

In 2024, ransomware attacks and leak sites became major news. Here are a few notable attacks:

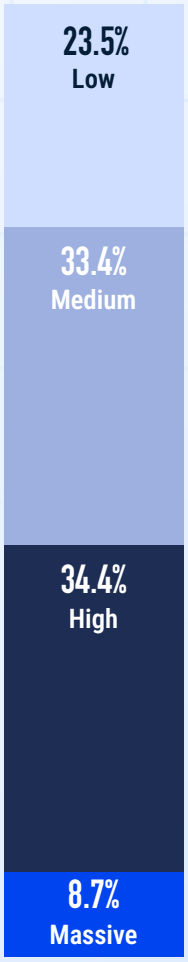
- In July 2024, a leading manufacturer of motorcycles and commercial vehicles became the target of a ransomware attack. The threat actors claimed to have exfiltrated sensitive company data, including PII and confidentiality agreements. Following the expiration of the ransom deadline, the group published the stolen data on their dark web platform.[234]
- In October 2024, a prominent dealership fell victim to a Russian-based ransomware group. The attackers utilized double-extortion tactics, exfiltrating sensitive company data such as invoices, accounting records, personal information, employment contracts, certifications, and internal documents. When the ransom payment deadline passed, the group escalated their attack by publishing the stolen data on their dark web platform.[235]

THREAT ACTORS CONTINUE TO FOCUS ON SCALE AND MASSIVE IMPACT

Analyzing threat actors' incentives and assessing the impact of deep and dark cyber activities is essential. As first introduced in 2023, Upstream initiated research focused on the 300 most active threat actors on the deep and dark web. This investigation revealed a shift toward large-scale cybersecurity incidents—with nearly 65% of incidents in 2023 impacting thousands-millions of mobility assets, and 48% targeting more than one OEM or automotive supplier.[236]

Our research scope expanded significantly in 2024—fueled by increased risks, additional mobility assets targeted, and evolving technologies—to include 1,133 active threat actors. This diverse range of actors included black hats, white hats, fraud operators, automotive fraud operators and auto enthusiasts. **This broader analysis showed over 43% of deep and dark web cyber activities could potentially impact thousands-millions of mobility assets, and 50% targeted more than one stakeholder.**

Breakdown of deep and dark web threat actors activities by scale, 2024



Source: Upstream Security

Breakdown of deep and dark web threat actor targets, 2024

Source: Upstream Security

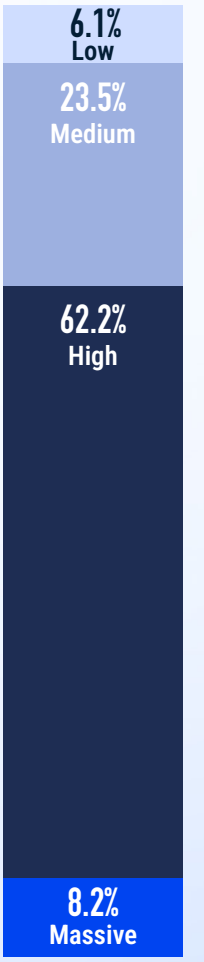
Zooming in on black hat activities in the deep and dark web

A closer look at black hat activities on the deep and dark web reveals a rapidly growing risk.

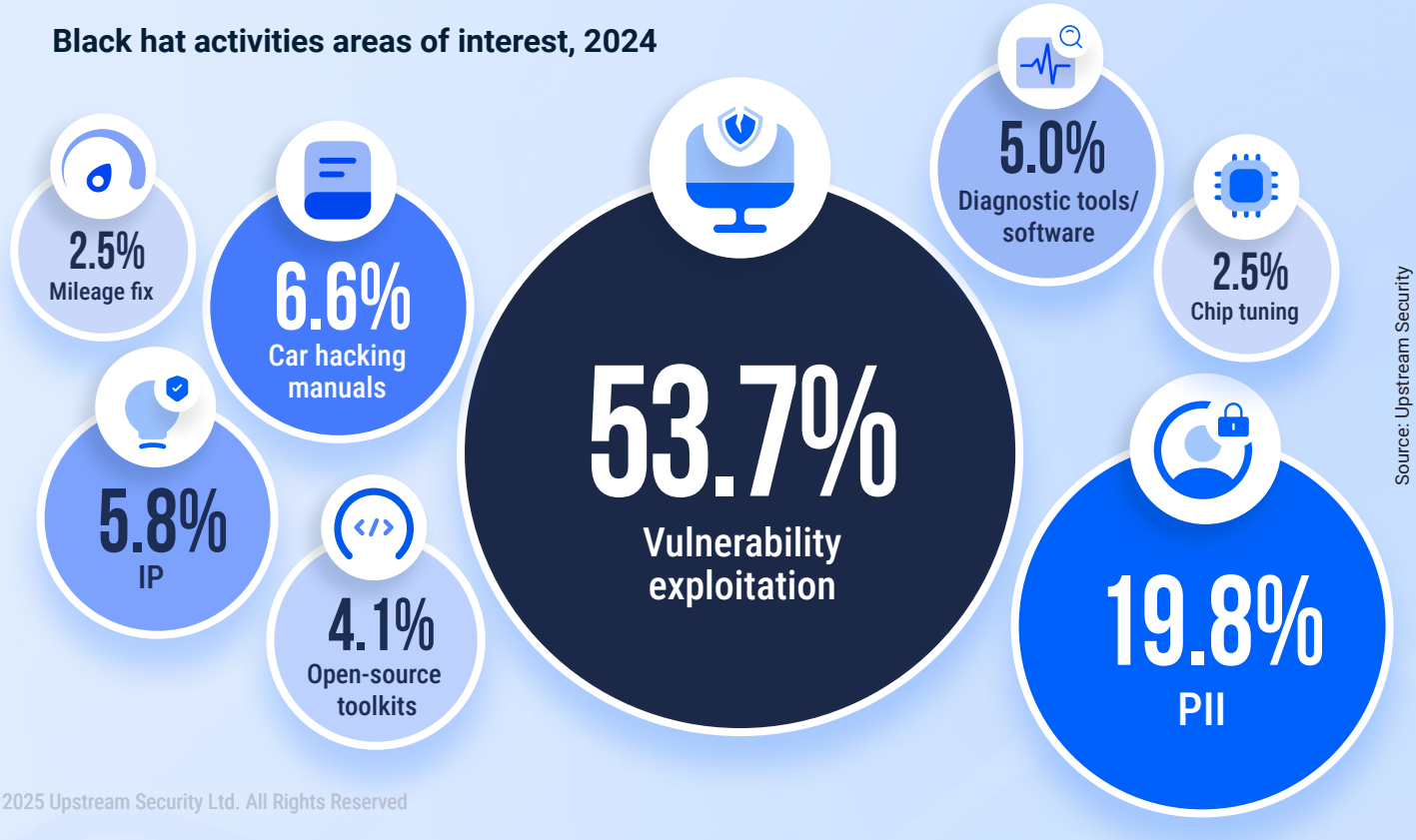
In 2024, over 70% of black hat activities had a high-massive impact, and over 76% involved multiple stakeholders with a global reach.[237]

When analyzing areas of interest, black hats continue to expand their reach and impact. Nearly 54% of activities are related to vulnerability exploits, 20% are focused on gaining access to sensitive PII, 6% are dedicated to IP theft, with the remaining 20% of activities related to vehicle manipulation (e.g., car hacking manuals, diagnostic tools/ software, open source toolkits, mileage fixing, and chip tuning).[238]

Black hat activities by potential scale, 2024

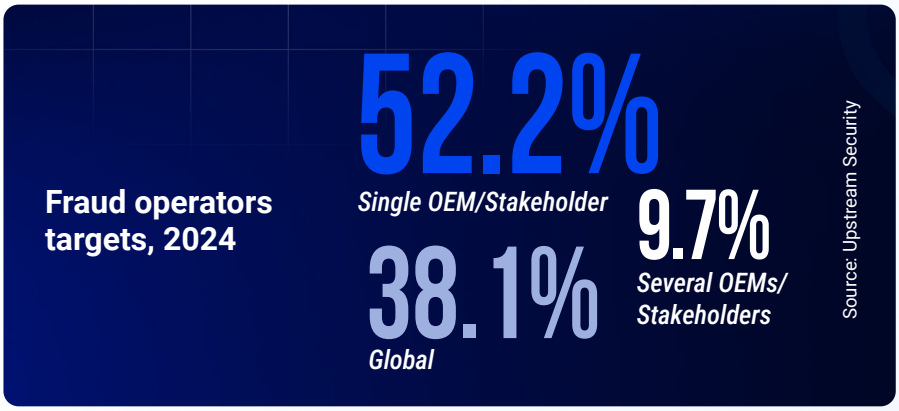


Black hat activities areas of interest, 2024



Fraud operators are also becoming more sophisticated and motivated by scale

Deep and dark web fraud operators also pose a significant and growing threat. In 2024, over 50% of fraud operator activities had a high-massive impact, and 48% involved multiple OEMs or had global reach.[239]

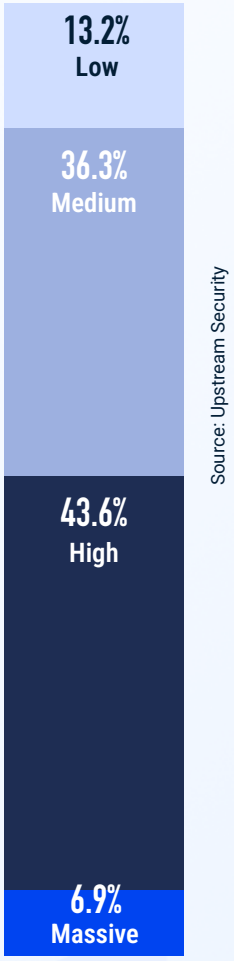


Analyzing fraud operators' areas of interest, vehicle manipulation constitutes approximately 72% of their activities. This category consists of three main areas of interest:

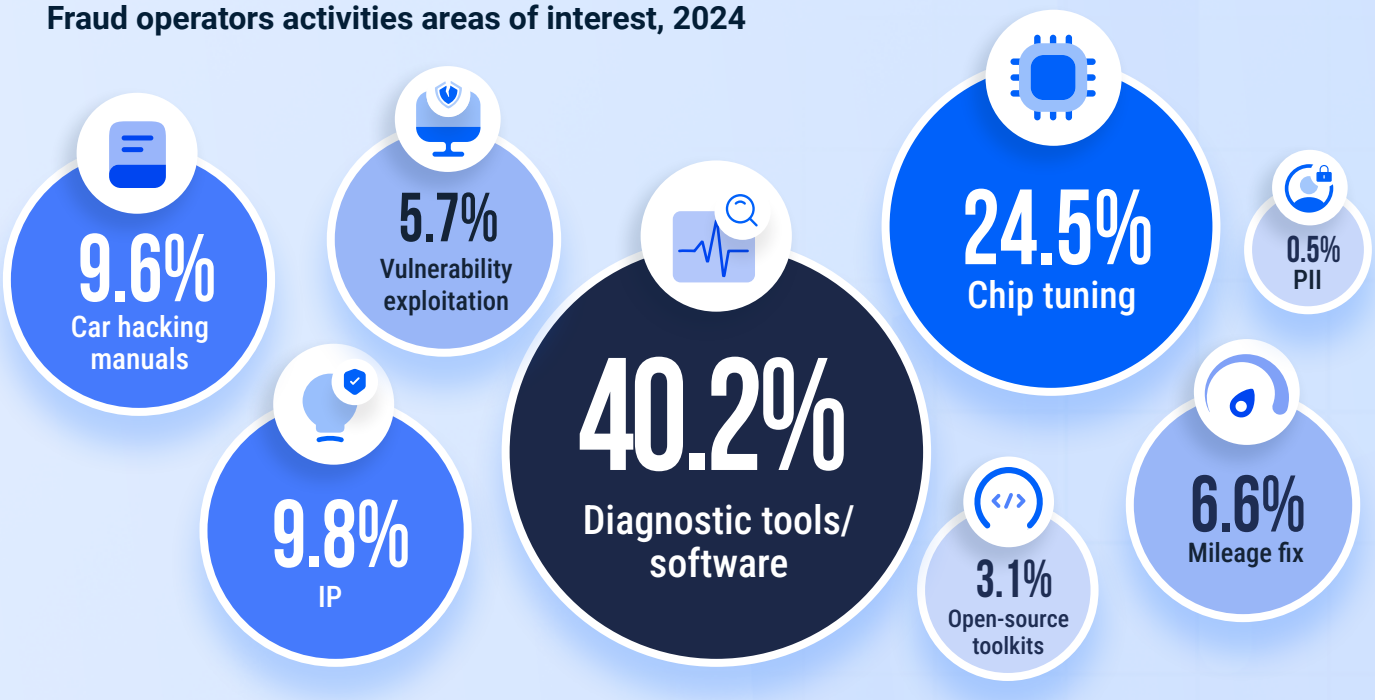
1. Diagnostic tools accounted for 40% of activities
2. Software and chip tuning accounted for 25% of activities
3. Mileage-fixing accounted for 7% of activities

Fraud operators also engaged in car hacking manuals (10%) and open-source toolkits (3%).[240] Additionally, nearly 10% of fraud operator activities involved IP, 6% vulnerability exploitation, and less than 1% focused on sensitive PII.[241]

Fraud operators activities by potential scale, 2024



Fraud operators activities areas of interest, 2024



A PROACTIVE APPROACH TO DEEP AND DARK WEB RISKS

Data sharing on deep and dark web platforms has dramatically increased in 2024, with automotive-related cybersecurity vulnerabilities, data breaches, and other cyber threats regularly published and discussed. Upstream's AutoThreat® PRO analysts have discovered a significant amount of mobility information on these sites. Stakeholders must monitor these areas to avoid serious cybersecurity gaps. **Effective cybersecurity protections require organizations to know when and in what context they are mentioned or targeted, both publicly and in gated sources.** Regulations such as UNECE WP.29 R155, ISO/SAE 21434, NHTSA guidelines, and Chinese regulations require cyber threat intelligence and vulnerability monitoring. The deep and dark web are integral elements of complying with these requirements.

> ***Continuous monitoring of the deep and dark web can improve detection and reduce the mitigation time between discovering a vulnerability or security breach and the information becoming widely known.***

Preventative measures, such as deploying software patches, changing configurations or replacing leaked credentials, are crucial. Minimizing threat actors' window of opportunity to gain access and sell breached data, and warning stakeholders, employees, key executives, and customers of potential exploitation are also essential.

Traditional IT threat intelligence offerings often lack domain expertise in connected vehicles, posing challenges for OEMs, Tier-1s, Tier-2s, and other mobility stakeholders.

Upstream's AutoThreat® PRO solution, purpose-built to overcome these challenges, collects, analyzes, and publishes cyber threat intelligence specific to the automotive and smart mobility ecosystem. It covers the entire supply chain and is tailored to various automotive segments, including OEMs, Tier-1 and 2 suppliers, smart mobility devices and applications, connected vehicle service providers, insurance companies, and other stakeholders. Upstream proactively monitors the deep and dark web to uncover emerging automotive-related cyber trends and threat actors, identifying and mitigating new threats—vulnerabilities, exploits, and fraud operations—before they become widely known. With the right cyber threat intelligence, automotive and mobility stakeholders can proactively implement the necessary cybersecurity measures to prevent the next cyber incident.

06.

THE REGULATORY REALITY

A strong emphasis on cybersecurity resilience, safety, and data protection is driving the evolution of regulatory frameworks for vehicles, EV charging infrastructure, and AI systems

Note: This chapter provides an overview of the latest updates and trends in Automotive and Smart Mobility cybersecurity regulations. For comprehensive regulatory evaluations, we recommend consulting additional sources and conducting detailed analysis.

THE EU AI ACT WILL GREATLY IMPACT THE AUTOMOTIVE INDUSTRY BY ENFORCING STRICT RULES FOR AI SYSTEMS IN VEHICLES

AI is poised to revolutionize the automotive industry. From design and R&D to personalized driver experiences and vehicle quality, its applications are vast and potentially transformative.

Significant investment and enthusiasm exists within the Automotive and Smart Mobility ecosystem. Stakeholders view AI as a game-changer, with substantial financial commitments and widespread pilot projects already underway.

According to McKinsey, 75% of companies are experimenting with at least one Generative AI application. Over 40% have invested up to €5 million, with some exceeding €20 million.[242] Indeed, in May 2024, Toyota highlighted its focus on AI and announced it would invest $13 billion in AI, EVs, and more.[243] Toyota planned to expand its AI-related investments in various areas, including autonomous driving, safety and GenAI.

Challenges to widespread adoption remain. These include addressing a shortage of skilled personnel, ethical concerns, data privacy, cybersecurity risks, and regulatory uncertainty.

> ***In August 2024, the EU Artificial Intelligence Act (AI Act) came into force, and will be phased in over a three-year period, with most provisions applying after 24 months.[244]***

This regulation—which can be directly implemented by the EU's 27 Member States without requiring any domestic legislation—focuses on ensuring basic rights are protected, establishing obligations for using AI based on risks and impact.

To achieve this goal, the EU AI Act categorizes AI systems based on their risk level into four distinct categories: unacceptable, high-risk, limited risk, and minimal risk. The EU AI Act explicitly addresses cybersecurity concerns, particularly for high-risk AI systems. Article 15 mandates that these systems be designed and developed to ensure appropriate levels of accuracy, robustness, and cybersecurity, maintaining consistent performance throughout their lifecycle.[245]

75%

OF COMPANIES ARE EXPERIMENTING WITH AT LEAST ONE GENAI APPLICATION.

OVER

40%

HAVE INVESTED UP TO €5 MILLION, WITH SOME EXCEEDING €20 MILLION.

This regulatory effort is also designed to enable the rapid growth of AI-based technologies across the European market. Penalties for infringements of the AI Act can reach up to €35 million or 7% of a company's annual global turnover, whichever is higher. Non-compliance could also lead to product recalls or market bans. The EU AI Act could drive global harmonization of AI safety standards, setting a precedent for other regions to follow.

EU AI Act's risk-based approach classifies most autonomous driving systems as high-risk, requiring strict compliance measures. Non-EU companies will also need to comply with the EU AI Act if they operate within the European Economic Area.

The AI Act recognizes existing automotive and general product safety regulations. While these laws already address some aspects of AI, they will be revised to specifically incorporate the AI Act's high-risk requirements, creating a sector-specific framework for automotive AI. The high-risk AI and low-risk AI provisions in the EU AI Act provide an early indication of the regulatory demands the industry will face.

AI is one of the key drivers and enablers of autonomous driving innovation. Though the AI Act does not apply directly to vehicles, **OEMs and more specifically autonomous technologies which are the most likely to heavily leverage AI may face new compliance obligations tied to revised Type-Approval Framework Regulation (TAFR) standards when they become available.** Given the importance of AI for AVs, this has the potential to hugely impact the automotive industry and the development of AVs.[246]

Automotive stakeholders, both within and outside the EU, will need to understand and adapt to the new requirements to ensure compliance. The interplay between existing automotive regulations and the new EU AI Act will expand the complexity of the regulatory landscape, requiring stakeholders to carefully navigate many different regulatory frameworks. They will be required to balance skills development, ethical considerations, data privacy, and regulatory compliance when designing long-term AI-driven strategies.

THE EXPANSION OF UNECE WP.29 R155 AND ISO/SAE 21434

In 2024, many automotive OEMs and their suppliers continued implementing R155 for Cyber Security Management System (CSMS) and Type Approval,[247] and R156 for Software Update Management System (SUMS).[248]

> ***The scope of vehicles grew substantially with the second milestone of R155 in July 2024, which expanded coverage to all new vehicles in production.***

These regulations, together with ISO/SAE 21434,[249] are part of a global effort to create a unified approach to Automotive and Smart Mobility cyber threats.

It is important to note that both R155 and ISO/SAE 21434 avoid outlining specific solutions and exact processes. Instead, they stress the importance of high cybersecurity standards. The guidelines outline the process and specify risk analysis and response targets. They emphasize the need to consider life-long cybersecurity threats and vulnerabilities during the development, production, and post-production phases.

R155 has been undergoing continuous expansions, since becoming effective in 2022. In June 2024, at the World Forum for Harmonization of Vehicle Regulations, the UN adopted a proposal[250] to extend R155 to category L vehicles (e.g., motorcycles and scooters).[251] By July 2029, Category L OEMs will be required to obtain Certificate of Compliance as evidence of a successfully audited CSMS.[252] Furthermore, in July 2024, the second milestone of R155 came into force, applying the cybersecurity law to all new vehicles in production.

UNECE WP.29 OVERVIEW

The primary components of regulation WP.29

R155 CSMS

Cybersecurity Management System

Cybersecurity management from ideation through post-production.

R156 SUMS

Software Update Management System

Cybersecurity measure to ensure safe software updates throughout the vehicle lifecycle.

Vehicles regulated under WP.29

Vehicle Category	Definition	Applicable Regulation
L (All)	A motor vehicle with fewer than four wheels (e.g., motorcycles and scooters)	R155
M	A vehicle with at least four wheels and meant to carry passengers	R155 & R156
N	An automobile with at least four wheels meant to carry goods	R155 & R156
O	Trailers that have at least one ECU	R155 & R156
R	Agricultural trailer	R156
S	Interchangeable towed agricultural or forestry equipment	R156
T	Any motorized, wheeled, or tracked agricultural equipment that has two axles and is meant to travel at speeds greater than 6 km/h (~3.5mph)	R156

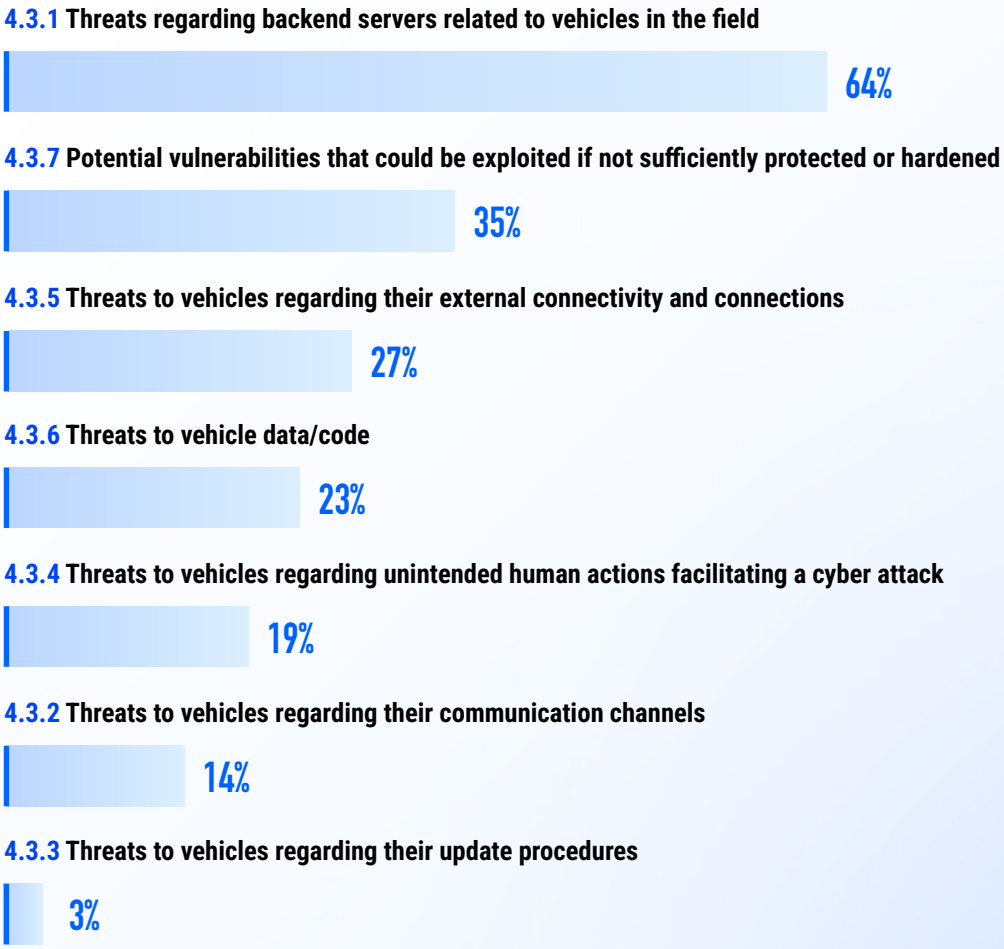
Source: Upstream Security

Vehicles are regulated under R155,[253] R156,[254] or both, depending on category classification.

Does R155 align with threats?

Upstream's research team analyzed publicly reported automotive cyber incidents that occurred in 2024, and correlated them to the seven threat categories presented in Annex 5 of R155.

2024 Cyber incidents categorized by R155 threats & vulnerabilities



Source: Upstream Security

The impact of WP.29 on the Automotive industry

Together, the new regulations, standards, and guidelines are designed to ensure a high level of cybersecurity—resulting in better safety and security for customers, while establishing uniform terminology, guidelines, targets, and scope across the industry. Manufacturers need this flexibility to implement innovative cybersecurity approaches and continuously improve.

ISO/SAE 21434, builds on ISO 26262 Road vehicles – Functional Safety standard, and requires automotive OEMs and suppliers to implement cybersecurity throughout the entire vehicle lifecycle. It focuses on adopting a 'security from the group up' mindset, and establishing engineering requirements for each step of product development and production, as well as the post-production phase.

R155 requires OEMs to implement and maintain Threat Analysis and Risk Assessment (TARA) throughout all stages of the vehicle lifecycle. **The complexity of performing effective TARA has changed dramatically as vehicles become more software-defined and software components are continuously updated throughout the vehicle's life cycle.** OEMs must also create processes to address and mitigate future attacks together with their Tier-1 and Tier-2 suppliers. Though the regulation applies to OEMs, the requirement to show that the CSMS includes the entire value chain expands the impact of R155 to suppliers. R155 applies to OEMs operating within the 54 countries that participate in the 1958 UNECE Transportation Agreements and Conventions.

The UNECE regulations and the ISO/SAE 21434 standard have reached critical mass and are changing the operations around the world. With the second milestone, which became effective in July 2024, all new vehicles will be governed under R155.

OEMs work closely with suppliers, and cybersecurity companies to support industry-wide compliance and certification efforts, and establish robust cybersecurity governance structures and testing processes.

To boost collaboration among OEMs and suppliers, the European Automobile Manufacturers' Association (ACEA) and the European Association of Automotive Suppliers (CLEPA) joined forces with Auto-ISAC in October 2022, to create a central European hub for information sharing on motor vehicle cybersecurity.[255]

Establishing long-term trust with ISO/SAE 21434

A key differentiator between ISO/SAE 21434 and R155 is that the ISO/SAE standard provides OEMs and their suppliers with a comprehensive process for calculating asset risk, and suggests methods for calculating scores and prioritizing vulnerability urgency.

The standard provides a structured cybersecurity framework, establishing cybersecurity as an integral element of engineering throughout the lifecycle of a vehicle, from the conceptual phase until decommissioning.

Additionally, to follow the ISO/SAE 21434 standard and R155 CSMS requirements, OEMs are encouraged to maintain a vSOC to enforce continuous monitoring for over a decade after vehicles roll off the assembly line.

With 422 new CVEs discovered in 2024 as well as the sharp rise in deep and dark web activities, it is imperative that stakeholders continuously review and implement mitigation techniques to protect their products against both existing and future vulnerabilities and undiscovered vulnerabilities that may arise in the future.

ISO/SAE 21434 and R155 work together to protect vehicles on a global scale

ISO/SAE 21434	R155	R155	R155	R156
Security by design	**Cybersecurity Management System**	**Threat Analysis & Risk Assessment**	**Monitoring**	**Software Update Management System**
Engineering requirements for each step of product development	Cybersecurity monitoring throughout vehicle lifecycle	Risk assessment and risk score for vulnerabilities	Early detection based on vehicle logs, and rapid response to incidents	Continuous safe updates throughout the vehicle lifecycle

Addressing RF-related cyber risks is essential to comply with automotive cybersecurity standards

While RF regulation (e.g., frequency allocation and interference prevention) is managed by local or international telecommunications authorities such as the ITU or FCC, its cybersecurity implications fall within the scope of risk management and security controls mandated by R155 and ISO/SAE 21434. Addressing RF-related threats is crucial to achieving compliance with these automotive cybersecurity standards. In fact, RF regulation is often recognized as an integral component in homologating both R155 and R156.

Relevance to CSMS (R155)

RF-based communication systems—such as V2X, Bluetooth, Wi-Fi, and keyless entry—are considered significant attack surfaces. As part of their CSMS, OEMs are required to assess RF-related threats and vulnerabilities through comprehensive threat modeling. In addition, OEMs are required to implement risk management measures to mitigate these vulnerabilities, ensuring compliance with R155 requirements.

Relevance to ISO/SAE 21434

ISO/SAE 21434 mandates detailed threat analysis and risk assessment (TARA), including RF communication threats, such as jamming, spoofing, and unauthorized access.

Additionally, ISO/SAE 21434 emphasizes the implementation of robust cybersecurity controls for wireless communication, including use of secure communication protocols and adoption of advanced encryption techniques to safeguard data integrity and confidentiality.

Summary of key RF-focused regulations, related to the Automotive and Smart Mobility ecosystem:

	Regulations / Standard	Impact
Global and regional regulations	ITU Radio Regulations (International Telecommunication Union)[256]	Updated in August 2024, this global regulation governs the use of radio frequencies, including automotive applications such as V2X and eCall.
	FCC Part 15 (US)[257]	Regulates unlicensed RF devices, including automotive key fobs, Bluetooth, Wi-Fi, and other short-range communication systems.
	ETSI EN 302 571 (EU)[258]	Focusing on V2X communication, the regulation outlines technical specifications and measurement methods for radio transmitters and receivers operating in the 5,855 MHz to 5,925 MHz frequency range, allocated for Intelligent Transport Systems (ITS) in the EU.
	Directive 2014/53/EU RED - Radio Equipment Directive (EU)[259]	Covers RF equipment compliance, including vehicles with radio communication functions sold in the EU.
Automotive-specific standards	ISO 15118 (Road Vehicles - Vehicle-to-Grid Communication Interface)[260]	Defines communication between EVs and charging stations, including secure RF communication protocols.
	IEEE 802.11p, known as Wireless Access in Vehicular Environments (WAVE)[261]	A standard tailored for V2X communication. It enables real-time wireless communication between vehicles (V2V) and between vehicles and infrastructure (V2I).
Cybersecurity-related standards	SAE J3105[262]	Covers secure wireless charging communication for EVs.
	SAE J2945/1[263]	Specifies the system requirements for an on-board V2V safety communications system for light vehicles, including RF management for security and efficiency.
	ETSI EN 303 645[264]	Focuses on cybersecurity for IoT devices, with specific applications to RF-based automotive IoT systems, including sensors and infotainment platforms.

Source: Upstream Security

THE REGULATORY LANDSCAPE CONTINUES TO MATURE

As the Automotive and Smart Mobility ecosystem evolves and introduces new applications, devices, and services, policymakers are rethinking laws. In addition to the critical milestone of R155, extending the scope to all new vehicles as of July 2024, legislators worldwide are becoming more aware of cybersecurity risks to vehicles, infrastructure, and consumer privacy. They are drafting new laws, including those for autonomous vehicles, to address these risks.

The EU Cyber Resilience Act promotes extended cybersecurity resilience

The European Cyber Resilience Act (CRA), officially adopted in October 2024, serves as horizontal legislation covering all products with digital components, including both hardware and software. Emphasizing consumer protection, the CRA seeks to improve cybersecurity across a wide range of modern connected devices, from wearable technology to vehicles.[265]

The CRA establishes a comprehensive cybersecurity framework that spans the entire product lifecycle, from planning and design through development and maintenance. It requires manufacturers to report actively exploited vulnerabilities and incidents and implement timely risk mitigation throughout the support period of their products.[266]

Manufacturers must comply by October 2027, although some provisions may apply earlier. OEMs and mobility stakeholders must carefully consider the CRA's scope. Products governed by the General Safety Regulation (EU) 2019/2144, including those under R155 for cybersecurity management in categories M, N, and certain O vehicles, are excluded from the CRA. However, other vehicles fall under the CRA's jurisdiction. As R155 and similar regulations expand, OEMs will need to align with both CRA and R155 requirements. This will ensure a robust cybersecurity posture across all applicable vehicles and digital products.[267]

ISO 15118 secures vehicle-to-grid communications

ISO 15118:2022, Road vehicles — Vehicle to grid communication interface,[268] is the leading communications standard, covering also cybersecurity features and requirements and ensuring encrypted, secure communication between the electric vehicle (EV) and the electric vehicle supply equipment (EVSE).[269]

It applies to category M and N vehicles, but encourages other OEMs to also adopt its framework. It also serves as the foundation for the High-Level Communication (HLC) protocol for the Combined Charging System (CCS) standard for charging EVs.

Based on the need to establish trust in the EV charging process, the standard was designed to protect the grid and support the charging of multiple vehicles at once while preventing the grid from overloading.

The ISO 15118 standard governs a "Plug and Charge" operation involving three basic stages:[270]

01

Confidentiality

Transport Layer Security (TLS v1.2) protocol is used to establish an encrypted communication session with a shared key that is valid for one charging session—using the Elliptic Curve Diffie-Hellman (ECDH) key agreement protocol.

02

Data integrity

All messages are encrypted and decrypted during a charging session using the symmetric TLS session key.

03

Authenticity

The authenticity of the sender and the integrity of the message are both verified using an Elliptic Curve Digital Signature Algorithm (ECDSA).

ISO 15118 applies to all entities involved in the charging process, including EVSE manufacturers, EV OEMs, charging point operators, cloud service providers (e.g., edge computing & data storage), and electricity grids (e.g., utilities, building management systems, etc.).

The California Energy Commission (CEC) has actively promoted ISO 15118. In May 2024, the CEC hosted a technical workshop to discuss industry updates on the implementation of the ISO 15118 standard for EV charging. This workshop featured presentations from CEC staff and industry representatives, emphasizing the importance of secure and standardized communication protocols in the EV charging infrastructure.[271]

In October 2024, the International Organization for Standardization (ISO) released a draft amendment to ISO 15118-20:2022, designated as ISO 15118-20:2022/DAmd 1. This amendment introduces enhancements such as improved security protocols to address emerging cybersecurity threats, ensuring V2G communications integrity and confidentiality.[272]

Ransomware attack reveals gaps in SEC cybersecurity disclosure requirements for publicly listed companies in the US

In July 2023, the US Securities and Exchange Commission (SEC) adopted final rules on cybersecurity disclosure for publicly listed companies.[273]

The final rules, which took effect in December 2023, have two parts: a requirement to disclose material cybersecurity incidents (using Form 8-K) four business days after a public company determines the incident is material; and a requirement to disclose annual information (using Form 10-K) regarding cybersecurity risk management, strategy, and governance.[274]

According to the new rules, public companies traded under the SEC rules must disclose the occurrence of a material cybersecurity incident and describe the material aspects of the nature, scope, and timing of the incident, as well as the material impact or reasonably likely material impact of the incident on the company, including its financial condition and results of operations. This disclosure is focused on the material impact of a cybersecurity incident.

The rules also allow the delayed reporting of cybersecurity incidents that pose a substantial risk to national security or public safety—contingent on written notification by the Attorney General—as well as 180-day extensions for smaller reporting companies.[275]

With these rules, the SEC stresses the importance of transparency and accountability in cybersecurity incidents and data breaches, which now must be reported to shareholders and the SEC as material events based on the well-established materiality standard. This new regulation by the SEC is expected to drive a wave of filings by automotive and mobility stakeholders as they are challenged with cybersecurity attacks.

In November 2023, a ransomware group, not knowing the effective date, tried to file an SEC complaint against a publicly listed company it had attacked. This attack was performed against a provider of a loan origination system and digital lending platform for financial institutions. The attacker complained that its victim, the listed company, did not disclose the breach under the new rules.[276] At the time of the alleged attack, the new SEC rules were not in effect yet and the targeted company reported it acted immediately upon discovery to mitigate the threat.

In June 2024, a ransomware attack on a leading US-based provider of dealership management software used by 15,000 dealerships halted dealer operations for nearly three weeks and tested SEC disclosure rules.[277]

Several affected dealerships filed disclosures with the SEC, citing the attack's negative impact on their business. However, the publicly traded parent company of the dealership management software, which suffered the ransom attack, stated the incident wouldn't have a "material impact" on its operations and therefore did not require disclosure.[278]

This discrepancy highlights gaps in SEC disclosure rules for cybersecurity incidents, allowing companies to choose their own response strategies and transparency levels, which can sometimes downplay incident severity.

It may take SEC enforcement actions and case law to establish clearer boundaries for companies regarding materiality standards for cyber incident reporting, according to experts. The current ambiguity in SEC disclosure rules necessitates a review and potential refinement to ensure timely and transparent reporting of cyber incidents.

NHTSA's cybersecurity best practices for the safety of modern vehicles

The National Highway Traffic Safety Administration (NHTSA) released updated cybersecurity best practices for new vehicles in September 2022.[279] While these guidelines are non-binding, their purpose is to reflect evolving attack methods and the sense of urgency in mitigating cybersecurity risks across the entire ecosystem.

The standardization of cybersecurity practices across the automotive industry, such as R155, and the release of NHTSA's Cybersecurity Best Practices for Modern Vehicles signals that governments and regulators around the world understand the importance of protecting vehicles as they become more vulnerable to hacking.[280]

The final version of this iteration considers new industry standards and research and incorporates knowledge gained from real-world incidents and comments submitted on the 2016 and 2021 drafts.

NHTSA recommended a layered cybersecurity approach, based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework's five principal functions: Identify, Protect, Detect, Respond, and Recover, including:

- Risk-based prioritization of protection for safety-critical vehicle control systems and sensitive information
- Timely detection and rapid response to potential threats and incidents
- Rapid recovery when attacks do occur
- Methods for accelerating the adoption of lessons learned across the industry, including effective information sharing

The updated guidelines emphasized the connection between cybersecurity and safety, making it clear that as the automotive industry becomes more connected, safety engineers and security stakeholders should also consider the ability of adversaries to manipulate signals.

The latest recommendation from NHTSA is inspired by ISO/SAE 21434 in structure and process, but is also affected by R155 as it includes the protection from remote attacks.

NHTSA guidelines emphasized the importance of collaboration to ensure security and safety, suggesting participation in Auto-ISAC as a means of effective information sharing across the industry. Upstream is a proponent of this; as collaborative community members, we maintain the Upstream AutoThreat® Intelligence Cyber Incident Repository[281] and share insights in our annual report. Upstream is also a proud partner and sponsor of Auto-ISAC[282] and ASRG,[283] where industry knowledge sharing occurs and cybersecurity best practices take shape.

The NHTSA has taken several measures to improve vehicle safety and address emerging ADS challenges

In April 2024, NHTSA introduced a rule requiring all new passenger vehicles to be equipped with automatic emergency braking systems within five years. This mandate aims to reduce traffic fatalities and injuries by ensuring vehicles can detect and respond to potential collisions, including those involving pedestrians, even under low-visibility conditions. The agency projects that this measure will save approximately 362 lives annually and prevent 24,000 injuries.[284]

In May 2024, the NHTSA's Office of Defects Investigation (ODI) opened a preliminary evaluation to investigate the performance of an Automated Driving System (ADS) of an American autonomous driving technology company. The fifth generation of the company's ADS received 22 reports of incidents, where the ADS-equipped vehicle was either the only vehicle involved in a collision or exhibited driving behavior that may have violated traffic safety laws. The investigation was focused on assessing the ADS's ability to detect and respond to traffic control devices and avoid collisions with stationary and semi-stationary objects and vehicles.[285]

In October 2024, the NHTSA intensified its scrutiny of autonomous and semi-autonomous vehicle technologies. The agency launched an investigation into a US EV OEM's Full Self-Driving (FSD) software following multiple crashes, including a fatality. The probe examines FSD's performance under reduced visibility conditions, covering approximately 2.4 million vehicles.[286]

Auto-ISAC introduced the Automotive Threat Matrix

In March 2024, Auto-ISAC introduced the Automotive Threat Matrix (ATM), an innovative initiative that marked a significant leap forward in bolstering the assessment of automotive threats and risks, as well as the classification and sharing of cyber threat intelligence across the automotive industry. ATM is modeled after the MITRE ATT&CK framework,[287] and offers a standardized taxonomy meticulously tailored for automotive-specific adversarial cyber tactics and techniques.[288]

ATM provides a structured resource for identifying, assessing, and mitigating cyber threats to connected and software-defined vehicles. By using a cross-industry universal language, ATM encourages collaboration across the automotive industry, helping stakeholders and security experts work together to enhance security resilience against evolving adversarial threats.

Implementing the ATM framework represents a significant step towards a comprehensive approach to risk management in the automotive industry. With over 70 techniques nested under 13 tactics, ATM establishes a structure addressing various attack vectors and impacted components. The framework strengthens several key aspects of risk management, such as vulnerability management, threat assessment and risk analysis (TARA), and cyber threat intelligence, thus setting an industry standard for handling cybersecurity-related events unique to the automotive sector.

Vehicle data and privacy regulations are emerging

Connected vehicles raise unique data privacy and cybersecurity issues that must be addressed by OEMs. Regulators around the world are taking notice and developing consumer-centric vehicle data privacy and security standards.

In June 2024, the EU officially adopted the Data Act,[289] granting users more control over data collected by connected devices, including vehicles. This legislation encourages OEMs to enable third-party access to vehicle data for aftermarket services, fostering competition while ensuring consumers' data rights. In August 2024, the EU also finalized the AI Act,[290] which impacts vehicle data by establishing requirements for AI-driven functionalities, such as autonomous driving, mandating data transparency and real-time monitoring to ensure compliance with data protection and safety standards.

In May 2024, the US Federal Trade Commission (FTC), the regulatory agency governing data privacy, highlighted its concerns regarding data collected by vehicles It emphasized the need for strong privacy and security measures, especially around location data and other sensitive information.[291]

This follows a letter from several Senators urging the FTC to investigate automakers' practices, particularly the sharing of location data with law enforcement agencies.[292] Additionally, in June 2024, the Federal Communications Commission (FCC) announced its intent to scrutinize automakers' connectivity practices due to potential abuses of consumer data.[293]

Regulatory developments at the state level also continue to expand, including:

- **New Jersey:** Enacted a law requiring auto dealers to delete consumers' personal information from vehicles they sell or trade in.[294]
- **Tennessee:** Introduced a bill to create a driver registry that allows individuals to opt out of data collection by automotive companies.[295]
- **New York:** Proposed a bill to update insurance laws, requiring automotive insurers to disclose how they use telematics data in rate calculations.[296]
- **California:** Passed legislation mandating that auto manufacturers disclose the presence of in-vehicle cameras.[297]
- **California:** Considering additional security measures in connected vehicles to protect victims and survivors of domestic violence.[298]

Much of the data generated by vehicles can be considered personal data, and most consumers feel they need legislation to protect their data.[299]

In the upcoming years and with the rise in autonomous technologies, we expect continuing growth in new regulations for the US and EU markets that require opt-in or minimally opt-out consent from consumers. As regulations continue to evolve, OEMs need to make strategic decisions about their own data privacy and security policies to maximize mutual trust, compliance, and consumer protection.

A GLOBAL PERSPECTIVE ON AUTOMOTIVE CYBERSECURITY REGULATIONS

Evolving regulations worldwide reflect a concerted effort by governments and regulators to adapt to technological developments, promote safety, and address security issues, showing a global commitment to shaping the future of the automotive industry.

EU

In July 2024, new rules on vehicle safety and automated mobility came into effect as part of the EU's General Safety Regulation. Vehicles now sold in the EU have to be equipped with a series of new safety features to assist the driver and help better protect passengers, pedestrians, and cyclists across the EU.[300]

While primarily focused on physical safety measures, the regulation also mandates certification for a cybersecurity management system to demonstrate the ability to ensure cybersecurity throughout the entire product lifecycle. Additionally, it establishes a comprehensive framework of requirements that manufacturers must meet to obtain vehicle Type Approval.

EU General Safety Regulation – new rules on vehicle safety and automated mobility

	All Road Vehicles	Cars and Vans	Buses and Trucks
New safety features required in all new vehicles, as of July 2024 **These measures apply to all new vehicle types since July 2022*	• Intelligent speed assistance • Reversing detection with a camera or sensors • Attention warning in case of driver drowsiness • Emergency stop signal • Cybersecurity measures	• Lane-keeping assistance • Advanced emergency braking—detecting cars, pedestrians, and bicycles • Event data recorders	• Detection and warnings to prevent collisions with pedestrians or cyclists • Tire pressure monitoring systems
Measures being progressively introduced between July 2024 to January 2029	• Advanced driver distraction warning • Safe and longer-lasting tire performance **These measures apply for: new vehicle types from July 2024; new vehicles from July 2026*	• Safety glass **These measures apply for: new vehicle types from July 2024; new vehicles from July 2026*	• Improved direct vision to better see cyclists and pedestrians • Event data recorders **These measures apply for: all new vehicle types from January 2026; all new vehicles from January 2029*

In October 2024, the EU implemented the NIS2 Directive to strengthen cybersecurity across critical sectors, impacting the entire smart mobility ecosystem, including connected vehicles, EV charging infrastructure, and Intelligent Transport Systems (ITS) like adaptive traffic signals and smart motorways.[301] This update expands the initial NIS Directive, requiring both "essential" and "important" entities to adopt comprehensive cybersecurity practices such as risk management, incident response, and detailed reporting of cyber incidents. EV charging operators and ITS providers must implement strong defenses against unauthorized access and data breaches, essential for securing the EU's sustainable mobility goals. Under NIS2, companies are obligated to designate senior management roles for cybersecurity, ensuring accountability and integration of cybersecurity into organizational strategies. With high penalties for non-compliance, the directive drives proactive investment in security operations and resilience, aiming to protect the integrity of interconnected mobility networks against rising cyber threats.[302]

In October 2024, the EU officially adopted the Cyber Resilience Act, a landmark law aimed at enhancing the cybersecurity of products with digital elements, including connected vehicles and potentially also EV charging infrastructure. This act introduces EU-wide cybersecurity requirements for the design, development, production, and marketing of hardware and software products, ensuring they are secure before entering the market. The law applies to all products connected directly or indirectly to another device or network, with certain exceptions for products already covered by existing EU rules, such as medical devices and automobiles. **By 2027, manufacturers must ensure their products are compliant on the EU market.**[303]

Though not directly impacting cybersecurity posture, in 2024, the European Union implemented several regulations to enhance the deployment and standardization of Electric Vehicle Supply Equipment (EVSE):

- The alternative fuels infrastructure, and repealing directive (AFIR) came into effect in 2024 and requires the installation of public fast chargers every 60 kilometers along the Trans-European Transport Network (TEN-T). This regulation aims to ensure that 1.3 kW of publicly accessible chargers are available for each registered Battery Electric Vehicle (BEV) and 0.8 kW for each Plug-in Hybrid Electric Vehicle (PHEV).[304]
- Euro 7 Emission Standards (Regulation (EU) 2024/1257) was adopted, introducing strict type-approval requirements for motor vehicles and engines, focusing on emissions and battery durability. It combines previous regulations to create a uniform system for emission type-approvals across the EU.[305]

- Net-Zero Industry Act (Regulation (EU) 2024/1735) aims to strengthen Europe's net-zero technology manufacturing ecosystem, including the production and deployment of EVSE. It sets a framework of measures to improve the Union's resilience and security of supply in the field of net-zero technologies.[306]

United States

In 2024, the United States introduced several significant measures to improve cybersecurity within the automotive sector:

In March 2024, the US Department of Commerce published an Advance Notice of Proposed Rulemaking seeking public comment on issues and questions related to supply chain risks in the Automotive industry, primarily related to China and Russia.[307]

> ***In September 2024, the US Department of Commerce published a Notice of Proposed Rulemaking that would ban the sale or import of connected vehicles integrating specific pieces of hardware and software, or those parts sold separately, with a sufficient nexus to the People's Republic of China or Russia.[308]***

The rule focuses on hardware and software integrated into the Vehicle Connectivity System (VCS) and software integrated into the Automated Driving System (ADS) which present undue risk to US critical infrastructure, national security, and the safety of drivers. **The planned rules would effectively ban Chinese vehicles from the US market, but would also force OEMs to remove Chinese software and hardware from vehicles sold in the US.**

The proposed rule marks a significant escalation in ongoing US restrictions on Chinese vehicles, software, and components. The bans on software would take effect for Model Year 2027, and the bans on hardware would take effect for Model Year 2030, or January 1, 2029 for units without a model year.[309]

Following the September 2024 proposal, industry stakeholders, including OEMs, Tier-1 suppliers, and governments, have expressed concerns about the challenges of implementing the proposed regulations. The comments emphasize that the new requirements could disrupt existing supply chains, increase operational complexity, and lead to higher production costs. Additionally, there are apprehensions about potential conflicts with international trade agreements and broader economic implications of compliance.

Stakeholders are urging a balanced approach that enhances cybersecurity while minimizing disruptions to industry operations and trade.[310]

In November 2024, the Transportation Security Administration (TSA) issued a Notice of Proposed Rulemaking requiring cyber risk management programs for surface transportation—including freight and passenger railroads, mass transit networks, highway-based logistics and potentially also EV charging infrastructure— pipeline operators, responsible for transporting energy products such as natural gas, oil, and hazardous materials to bolster national cybersecurity resilience.[311] The proposed rule requires high-risk operators across pipeline, passenger rail, freight rail, and certain over-the-road long-distance bus operators to establish comprehensive cybersecurity risk management protocols, aligned with the NIST Cybersecurity Framework.[312] These operators would also need to report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (CISA) and inform the TSA of physical security risks. The proposal underscores TSA's ongoing collaboration with industry and federal partners to respond to elevated cyber threats from nation-state actors targeting critical infrastructure.[313]

China

In 2024, China introduced a series of regulations, and policies related to the Automotive and Smart Mobility ecosystem, showing a wide effort to establish risk management frameworks and drive the intelligent transformation and upgrading of the sectors.

In June 2024, the Ministry of Industry and Information Technology (MIIT) announced plans to formulate new standards for the global Automotive industry, focusing on NEVs and intelligent connected vehicles. China will lead the development of nearly 20 international standards, including those for fuel cell vehicles, electromagnetic compatibility, and automotive radar. In addition, China aims to develop at least three new international standards for electric vehicle (EV) performance-testing methods and collision safety terminology, and to establish one or two international standards working groups. China will also focus on the development of global technical regulations for autonomous driving systems, and expedite the formulation of regulations on maximum EV power output measurement methods and the second phase of power battery durability.[314]

In August 2024, MIIT opened a 30-day public consultation on strengthening the access, recall, and online upgrade management of connected vehicles. The consultation seeks input to improve the management of intelligent connected vehicles, particularly those with combined driver assistance systems and over-the-air (OTA) upgrades. It sets out measures like mandatory reporting of system failures, strengthened recall procedures, and detailed OTA update filings for automotive companies.[315]

In August 2024, MIIT published the first batch of mandatory national standards for intelligent networked vehicles in China, set to take effect on January 1, 2026:[316]

GB 44495-2024	Technical Requirements for Information Security of Automobiles stipulates the requirements of the automobile information security management system, as well as the technical requirements and test methods for external connection security, communication security, software upgrade security, data security, etc.[317]
GB 44496-2024	General Technical Requirements for Automobile Software Upgrade stipulates the management system requirements for automobile software upgrade, as well as the technical requirements and test methods for vehicle software upgrade functions such as user notification, version number reading, safety protection, prerequisites, power guarantee, failure handling, etc.[318]
GB 44497-2024	Intelligent Networked Vehicle Autonomous Driving Data Recording System stipulates the technical requirements and test methods of the intelligent networked vehicle autonomous driving data recording system in terms of data recording, data storage and reading, information security, collision resistance performance, environmental evaluation, etc.[319]

Global OEMs operating in China should prepare for the 2026 milestone, and analyze the gaps between the new Chinese national standards and current international standards.

Overall, GB 44495-2024 shares many common principles with R155 and ISO/SAE 21434 requirements of a cybersecurity management system. However, it introduces market-specific, detailed technical requirements.[320]

In addition, GB 44495-2024 stresses the importance of risk management, like ISO/SAE 21434, which includes continuous monitoring, risk assessments, and response measures to ensure that vehicles remain secure even as new threats emerge.

Although both standards aim to enhance vehicle cybersecurity, they differ in several key aspects:

	GB 44495-2024	R155
Scope	Only applies to M (passenger), N (commercial), and O (trailers, including semi-trailers) vehicle types.	Includes L6 and L7, and is expected to expand to all category L vehicles.
Specificity	Provides detailed technical requirements and testing methods.	Offers a broader framework and risk categories (Annex 5), granting manufacturers flexibility in implementation.
Testing Requirements	Lists 27 specific cybersecurity tests that manufacturers must perform, covering various aspects of vehicle cybersecurity including: external connections, communication systems, software updates, data security, access control, Denial-of-Service (DoS) protection, and more.	Emphasizes the necessity of cybersecurity testing, but does not prescribe specific testing methods.
Certification	Requires an audit without issuing a certificate or requiring renewals.	Requires a formal certification process with periodic renewals.

Source: Upstream Security

In October 2024, three new national safety standards in the field of Smart Mobility were approved for development by the China National Standards Administration:[321]

- **Intelligent Connected Vehicle Data Security Management System Specification:** This standard focuses on data security within automotive companies, emphasizing a lifecycle approach to data protection in R&D, design, and production. It aims to guide companies in establishing robust data security management practices.
- **Automobile Security Vulnerability Classification and Grading Evaluation:** This standard provides a framework for categorizing and evaluating security vulnerabilities in vehicles based on severity and potential harm. It strengthens vulnerability management and improves automotive cybersecurity standards.
- **Technical Specifications for Automotive Digital Key Systems:** Outlines functional and security requirements for digital keys using NFC, UWB, and Bluetooth technologies. The standard ensures the safe use of digital keys, supporting their secure integration into vehicles.

Under the guidance of MIIT, the National Technical Committee for Automobile Standardization will lead drafting and validation processes to accelerate approval and adoption of these standards, supporting key technology development in the Smart Mobility ecosystem.

India

In 2024, India made significant strides in enhancing vehicle cybersecurity through the development and implementation of standards and regulations.

India is developing its own standards to improve vehicle cybersecurity and align with global regulatory frameworks such as ISO 21434 and R155/R156.

India is expected to implement its AIS 189 – Cyber Security Management System[322] and AIS 190 – Software Update and Software Updates Management System[323] by 2027, which will require the inclusion of cybersecurity features in all connected vehicles sold in the country.[324]

In June 2024, the Bureau of Indian Standards (BIS) introduced new standards to ensure EV safety and quality—IS 18590: 2024[325] and IS 18606: 2024.[326] These standards focus on EV powertrain and battery safety and performance for L, M, and N vehicle types. By setting strict requirements, they ensure the reliability and safety of these critical components. This is crucial for boosting consumer confidence and accelerating EV adoption. BIS has now set 30 Indian standards for electric vehicles and accessories, including charging systems.[327]

Singapore

In May 2024, Singapore enacted the Cybersecurity (Amendment) Act 2024, which broadens the scope of the original Cybersecurity Act 2018 to address evolving cyber threats and technological advancements.[328]

The Amendment seeks to tackle the growing cybersecurity challenges brought about by increased connectivity, the proliferation of cloud platforms, and the complexities of modern supply chains, which have significantly expanded the attack surface. It also enhances the powers of the Cyber Security Agency of Singapore (CSA), enabling it to investigate cyber incidents more effectively and mandate organizations to provide critical information. Penalties for non-compliance can now reach up to 10% of an organization's annual revenue or SGD $500,000, whichever is greater.[329]

While the Act does not specifically target the automotive or mobility sectors, it emphasizes that any entity providing essential services or handling critical information infrastructure must comply with enhanced cybersecurity standards.

The Act is focused on several sectors, including energy, water, banking and finance, healthcare, transport (which includes land, maritime, and aviation), infocomm, media, security and emergency services, and government.[330] Therefore, automotive, smart mobility service providers and EV charging stakeholders would be required to adhere to the updated cybersecurity regulations.

CHARGING INFRASTRUCTURE REGULATORY FRAMEWORKS CONTINUE TO ADVANCE, AS EV MARKET SHARE INCREASES

A recent PWC report on Q3'2024 EV sales shows that the global electric vehicle market share is increasing. In the first quarter of 2023, 28% of vehicles sold in the analyzed markets were electric. By the third quarter of 2024, this figure rose to 41%.[331]

Factors contributing to the rise in electric vehicle market share include the rapid expansion of the Chinese PHEV market and a surge in China's PHEV exports. A significant increase in electric vehicle sales was recorded in the top five European markets, where EV sales s—now accounting for 56% of all new vehicle registrations. In the US, total electric vehicle market share exceeded 20% for the first time.[332]

BY THE THIRD QUARTER OF 2024

41%

OF VEHICLES SOLD WERE ELECTRIC.

With the number of electric vehicle charging stations (EVCS) growing rapidly, the market has been challenged by attempts by threat actors to manipulate EVCS all over the world.

EVCS are connected IoT devices that contain components from multiple vendors and are installed rapidly to meet market requirements. This makes them exposed to multiple attack vectors:

- Charging Point Operators (CPOs) are a vital stage in the charging ecosystem, but can be attacked on a wide scale by hacking the backend Command and Control (C&C) servers. CPOs can be attacked remotely by targeting multiple charging stations or by creating extensive charging demand, causing a widespread denial of service. Additionally, attackers can gain unauthorized access to private consumer data, including personal information (PII) and charging patterns.

- API-based attacks often require a lower threshold of cyber and technical skills. This attack vector leads to a simpler yet sufficient attack surface with a potential fleet-wide impact. API attacks can target and impact backend servers, resulting in potential data theft or a denial of service. API attacks can emerge from any entity in the ecosystem communicating with it and vice versa, including vehicles themselves, charging stations, mobile apps, third-party applications, etc.

As the number of EVs continues to rise, new standards are emerging focused on EV chargers and charging infrastructure.

> ***EV charging standards will focus on providing safe, reliable, and accessible chargers, as well as managing increased electricity demand on the grid.***

Regulations protecting EVCS can be divided into two major categories:

- **Operational standards**

  Guidelines on how EVCS should safely communicate with backend servers, vehicles, the CSMS, how data is stored and encrypted, etc. This includes ISO 15118, OCCP (currently in transition between 1.6 to 2.0.1), CHAdeMO, and IEC 63110 which is currently under development. These operational standards are made by EVCS manufacturers themselves along with vehicle OEMs to ensure data integrity.

- **Regional laws theoretical frameworks**

  Consists of the actual actions and preconditions to be met by EVCS operators, along with the theoretical frameworks that led to its creation. Laws are enforced by the state on the national or regional level. This includes the US NIST IR 8473, the EU NIS2 Directive, Cyber Resilience and Cyber Solidarity Acts, UK Electric Vehicles (Smart Charge Points) Regulations, and more (further discussed in this report).

EVCS cybersecurity has been the focus of regulatory efforts worldwide.

Sample of recent EVCS cybersecurity regulations

Region / Country	Regulation	Focus	Implementation date	Enforcement status
	ETSI EN 303 645	IoT	August 2025	
	NIS2 Directive	Critical infrastructure	October 2024	Mandatory
	EU Cyber Resilience Act	IoT	October 2024	Mandatory compliance within 36 months,with some provisions applying earlier
	NIST IR 8473	EVCS	October 2023	Voluntary
	National Electric Vehicle Infrastructure Standards and Requirements	EVCS	April 2023	Mandatory
	GB/T Cybersecurity Standards	IoT, EVCS	May 2022	Voluntary
	GB/T 18487.1-2023	EVCS	April 2024	Mandatory
	GB/T 27930-2023	EVCS	April 2024	Mandatory
	GB/T 34658-2017	EVCS Information Systems	December 2017	Voluntary
	British Standards Institution (BSI) standards for energy smart appliances (ESAs)	Smart appliances	December 2021	Voluntary
	Complying with the Electric Vehicles (Smart Charge Points) Regulations 2021	EVCS	December 2022	Mandatory
	MIC IoT 5G Comprehensive Security Measures	IoT	June 2019	Mandatory
	METI IoT Security and Safety Framework	IoT	November 2020	Mandatory

Source: Upstream Security

EU

ETSI EN 303 645 regulation for IoT devices was issued by the European Telecommunications Standards Institute. In September 2024, ETSI released an updated comprehensive document, ETSI EN 303 645 V3.1.3 (2024-09), outlining high-level security provisions for consumer IoT devices in response to growing concerns over cybersecurity and data protection.[333]

The document includes baseline provisions, establishing fundamental security requirements applicable to all consumer IoT devices; guidance for implementation, providing organizations with clear examples and explanatory text on how to apply the provisions; compliance with GDPR, ensuring that IoT devices processing personal data align with GDPR standards; and future-proofing, anticipating that future revisions will transition current recommendations into mandatory provisions. The standard provides a flexible framework for innovation while ensuring a baseline level of security, emphasizing outcome-focused provisions and avoiding overly prescriptive measures. This allows organizations to tailor security solutions for specific products.[334]

The NIS2 Directive[335] became mandatory in October 2024 and focuses on establishing cybersecurity standards and resilience for the critical infrastructure and energy sectors. The NIS2 Directive is supported by the EU Cyber Solidarity Act,[336] which aims to strengthen capacities in the EU to detect, prepare for, and respond to significant and large-scale cybersecurity threats and attacks. This includes forming SOC (security operation center) infrastructure within EU member countries to ensure coordinated handling of cyber threats, and creating a European Cybersecurity Reserve, consisting of incident response services from trusted, qualified providers. NIS2 also adds reporting requirements within 24 hours, with additional reporting after 72 hours and 30 days.[337]

In October 2024, the European Commission set the first rules for implementing the NIS2 Directive for critical entities and networks in the EU. These rules outline cybersecurity risk management measures and establish criteria for reporting significant incidents to national authorities. Key measures include cybersecurity risk management, incident reporting, supervisory and enforcement actions, supply chain security, and streamlined reporting with enhanced sanctions.[338]

In October 2024, the European Parliament officially adopted the Cyber Resilience Act (CRA),[339] a horizontal legislation, covering all products with digital components (both hardware and software).[340] The CRA covers the entire lifecycle of products, offering a framework for cybersecurity governing the planning, design, development, and maintenance of products.

Regulatory measures include mandatory obligations for manufacturers, importers, and distributors, as well as product classification and security measures, and surveillance and enforcement. The CRA also requires manufacturers to report actively exploited vulnerabilities and incidents within 24 hours, and mitigate risks effectively through the support period of the product.[341]

ISO 15118 is partially and voluntarily implemented in Europe under the project name “Plug & Charge Europe.” Although notable OEMs and EVCS operators throughout the region have accepted it, there is no planned timeline for full-scale implementation in the EU. The relevant regulations will be implemented by 2025, and the region has already started voluntarily accepting ISO 15118.

Also, ISO 15118 is partially and voluntarily implemented in Europe under the project name Plug & Charge Europe.[342] Although accepted by notable OEMs and EVCS operators throughout the region, there is no planned timeline for a full-scale implementation of the standard in the EU.

United States

In March 2023, the National Electric Vehicle Infrastructure Standards and Requirements by the US Federal Highway Administration (FHWA) came into effect.[343] This new rule establishes the requirements and minimum standards related to projects funded under the National Electric Vehicle Infrastructure (NEVI) Formula Program and projects for the construction of publicly accessible EV chargers under certain statutory authorities, including any EV charging infrastructure project funded with federal funds that is treated as a project on a Federal-aid highway.

Essentially, FHWA adopted the principles of ISO 15118 and requires charging stations to conform to ISO 15118 and Plug & Charge standards within a year. This legislation highlights the value in adopting a national standard for compliance, even though many chargers on the market are not currently using ISO 15118.[344]

The rule mandates the implementation of appropriate physical strategies for the location of the charging station and cybersecurity strategies that protect consumer data and ensure the safety of charging infrastructure and power grids.

In October 2023, the US Department of Commerce's National Institute of Standards and Technology (NIST) finalized its guidance for managing cybersecurity risks for EV extreme fast charging infrastructure with NIST IR 8473 – Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure.[345]

EV charging stations and charging infrastructure are vulnerable to a wide range of cybersecurity threats since they rely on complex infrastructure, interconnectivity, and multiple data networks. NIST IR 8473 offers a holistic framework, covering the entire EV charging landscape. The guidelines include:

- Electric vehicles
- Extreme fast charging (XFC)
- XFC cloud or third-party operations
- Utility and building networks

Furthermore, NIST IR 8473 has a well-established section for data protection, based on the ISO 21434 standard.[346]

The framework suggested by NIST is voluntary, but it's designed to help EV charging stakeholders develop specific processes to understand, assess, and communicate their cybersecurity posture as a part of their risk management process.

In August 2024, the US government unveiled a comprehensive plan to bolster cybersecurity for clean energy systems, with a specific focus on protecting the nation's electric grid and EV charging infrastructure. Recognizing the increasing reliance on interconnected and smart technologies in clean energy, the initiative seeks to mitigate vulnerabilities that could be exploited by cyberattacks. The plan prioritizes modernizing grid defenses, implementing robust security measures for EV charging networks, and ensuring the resilience of these critical systems to support the ongoing clean energy transition.[347]

UK

The UK is at the forefront of EVCS regulations. In December 2021, a proposition was made to include EVCS under the British Standard Institutes' (BSI) regulation for smart appliances (ESA) with smart energy.[348]

In June 2022, the Electric Vehicles (Smart Charge Points) Regulations 2021 came into force and applied to private charge points (domestic or workplace).[349]

The UK regulation specifies that chargers must meet the following requirements: smart functionality such as demand-side response services; electric supplier interoperability; enabled charging even with loss of communications network access; enhanced safety features; measuring system for increased transparency on charging statistics; default off-peak charging schedule; randomized delay to protect from surges in demand; statement of compliance for compliance assurance; and register of sales for ten years. New cybersecurity requirements are also outlined in Schedule 1 of the regulation, which came into effect in December 2022.[350] Chargers will come preconfigured with these settings, but owners can adjust them to suit their preferences.

A guidance letter for EVCS sellers and operators, published in February 2022 and most recently updated in June 2023, suggests matching EVCS cybersecurity requirements to the European ETSI EN 303 645 standard. ETSI EN 303 645 was chosen based on its suggested benchmark and measurable objectives.[351]

In October 2024, the UK Department of Transport issued updated guidance to help operators of publicly accessible electric vehicle charge points understand The Public Charge Point Regulations 2023.[352] These regulations were published and came into force in November 2023, with many requirements becoming mandatory for public charge points depoled after November 2024.[353] The regulations focus on areas such as payment methods, pricing transparency, reliability, and data accessibility. Although the regulations do not detail specific cybersecurity protocols, compliance inherently requires operators to implement strong cybersecurity practices to safeguard data, payment systems, and the operational integrity of charge points.

Japan

Cybersecurity protection of EVCS in Japan can be derived from regulations covering IoT devices such as METI (Ministry of Economy, Trade and Industry) IoT Security and Safety Framework from November 2020[354] and MIC (Ministry of Internal Affairs and Communications) IoT 5G Comprehensive Security Measures from June 2019.[355]

Global operational EV charging standards

ISO 15118

ISO 15518 is the leading global cybersecurity standard to ensure encrypted, secure communication between the EVs and charging stations (EVSE/EVCS) while charging,[356] and is considered as the high-level communication protocol, functioning as the security standard for the Combined Charging System (CCS).[357]

The ISO 15118 standard governs a “Plug and Charge” operation involving three fundamental stages:

01

Confidentiality

Messages are encrypted using TLS protocol.

02

Data integrity

Messages are kept intact and untampered using a pair of private and public keys.

03

Authenticity

Sender and received messages are ensured using Elliptic Curve Digital Signature Algorithm (ECDSA).[358]

ISO 15118 covers Vehicle to Grid (V2G) cybersecurity aspects and applies to all entities involved in the charging process:

- EVs
- Charging stations and CPOs
- Cloud operators, in charge of data processing and storage
- Power grids (also called Utility / Building Management Systems)

Combined Charging System (CCS)

One of the most prominent charging protocols, supported by multiple OEMs worldwide. CCS cybersecurity measures are covered under ISO 15118.[359]

DIN SPEC 70121

DIN SPEC 70121 is the German predecessor to ISO 15118 and was built on the theoretical principles of an initial, unpublished version of ISO 15118. DIN SPEC 70121 does not include any of the updated features of ISO 15118, such as smart charging and secure TLS communication.

CHAdeMO

A Japanese standard (stands for “Charge de Move”) that was created by OEMs including Nissan, Mitsubishi, and Toyota. CHAdeMO was first introduced in 2009 and aims to provide an alternative to the ISO 15118 standard.[360] Similar to ISO 15118, CHAdeMO covers V2G security aspects. The charging process is enabled by matching the user’s VIN (Vehicle Identification Number) along with IPv6 security measures and contract key encryption.

In September 2023, CHAdeMO released the Design Guideline for External Charging ver.2.0.1, adding technical and operational requirements for safely integrating or retrofitting the Automated Connection Devices - Underbody (ACD-U) charging systems to CHAdeMO chargers/V2X equipment, EVs, and plug-in hybrid EVs (PHEVs).[361]

OCPP 2.0.1

Open Charge Point Protocol (OCPP) was created by the Open Charge Alliance and was introduced in 2013, and is currently migrating from version 1.6 to 2.0.1. OCPP is a prominent open-source secure communication standard for EVCS and CSMS. The standard operates alongside ISO 15118.

Notable improvements from version 1.6 to 2.0.1 include features for streamlined device management and improved transaction handling for operators managing multi-vendor charging points, enhanced security with secure updates and authentication using secure TLS encryption, and support for ISO 15118.[362]

In November 2024, an update was released to OCPP 2.0.1 (Edition 3), addressing various corrections and clarifications to enhance the protocol's functionality and reliability.[363]

While ISO 15118 secures the communication between the vehicle to the charging station, OCCP covers the security aspects between the charging stations themselves and the backend servers. This includes the CPO, telecommunications, and electricity management.[364]

07.

AUTOMOTIVE CYBERSECURITY SOLUTIONS

Stakeholders should consider leveraging AI-powered cybersecurity tools to effectively address growing cybersecurity risks and emerging gaps

CYBERSECURITY SOLUTIONS CONTINUE TO EVOLVE

Automotive cybersecurity solutions are evolving as the industry continues its digital transformation. With cyber threats getting more sophisticated, frequent, and large-scale, cybersecurity solutions must provide effective and rapid remediation across a massive scale of mobility assets and an ever-changing SBOM. Vehicle cybersecurity teams and Vehicle Security Operations Centers (vSOCs) must also investigate threats that go beyond direct attacks on vehicles—targeting fleets, companion applications, mobility services, mobility IoT devices, EV charging infrastructure, and more.

Increased connectivity in modern vehicles has opened the door to exponential growth in the scale and impact of cyber attacks—posing growing cybersecurity challenges for OEMs and their supply chains, and putting trust, safety, and operational availability at risk.

Smart mobility stakeholders, OEMs, Tier-1s, and Tier-2s will continue to place a high priority on cybersecurity as new standards and regulations are adopted.

> ***To ensure connected vehicles and mobility services remain secure into the future and minimize cybersecurity gaps, it's imperative they use a multilayered cybersecurity approach.***

Protecting vehicles during their entire lifecycle—across a complex supply chains and dynamic SBOMs

Passenger cars typically last 12 years, commercial trucks 20 years, and agricultural vehicles 30 years. OEMs must therefore develop long-term strategies to secure products operating on decades-old technology. UNECE WP.29 R155 and ISO/SAE 21434 establish the requirement to consider life-long cybersecurity threats and vulnerabilities during the development, production, and post-production phases of the vehicle's lifecycle.

For the first time, in 2022, OEMs and their suppliers came under formal regulation and standardization. By 2024, the UNECE regulations and the ISO/SAE 21434 standard have reached critical mass, fundamentally transforming global operations. A key milestone occurred in July 2024, when the second milestone of R155 became effective, requiring monitoring across all newly manufactured vehicles. This transparency has addressed long-standing concerns about production disruptions beyond supply chain bottlenecks. By requiring suppliers to adhere to stringent cybersecurity protocols, OEMs have reduced the risk of vulnerabilities introduced by third-party vendors.

R155 requires OEMs to implement and maintain threat analysis and risk assessment (TARA) throughout all stages of the vehicle lifecycle. They must also create processes to address and mitigate future attacks together with their Tier-1 and Tier-2 suppliers. ISO/SAE 21434 can be used as guidance on how to implement the R155 requirement together with suppliers.

01

Cyber record of capability

OEMs are responsible for checking suppliers' cyber histories and ensuring suppliers conduct ongoing risk and vulnerability management for all relevant components.

02

Define shared responsibilities

Cybersecurity responsibilities are shared and documented using cybersecurity interface agreements (CIAs) to ensure that nothing is missed due to a lack of clarity in delegation. This can be done using established project management methods such as Responsible Approving Supporting Informed Consulting (RASIC).

Regardless of the method OEMs and suppliers agree on, the OEM bears the responsibility to follow R155 & R156 and implement practices that follow the ISO/SAE 21434 requirements.

Security by design

One of the four measures explicitly specified by the R155 regulation for vehicle cybersecurity is securing vehicles "by design" to mitigate risks along the value chain. Security by design requires evaluating the cybersecurity risks of a component or software as early as the development phase. This is done by making sure that all vehicle components and subsystems are designed, developed, and tested for cybersecurity vulnerabilities, and that any applicable risks discovered are effectively mitigated. While OEMs are ultimately responsible for the security of their vehicles, all suppliers in the supply chain need to adopt security-by-design practices as well.

Multi-layered cybersecurity stack

In the post-production phase, connected vehicles, smart mobility applications, and devices demand a robust, multi-layered cybersecurity stack. This approach, long established as a standard in IT and enterprise cybersecurity, is now being adopted by automotive and smart mobility stakeholders to counter increasingly sophisticated threats and emerging vulnerabilities.

Enterprises use multiple security solutions, including end-point solutions, network security solutions, cloud security, API security, internal segmentation technology, and more.

In 2019, Gartner standardized the practice by introducing the network-centric concept of the Security Operations Center (SOC) Visibility Triad.[365]

According to Gartner's research, a modern SOC must rely on three well-known core security elements for increased threat visibility, detection, response, investigation, and remediation:

01

Security Information and Event Management (SIEM)

Collects and analyzes event logs and security alerts generated by IT infrastructure, applications, and other security tools.

02

Network-centric Detection and Response

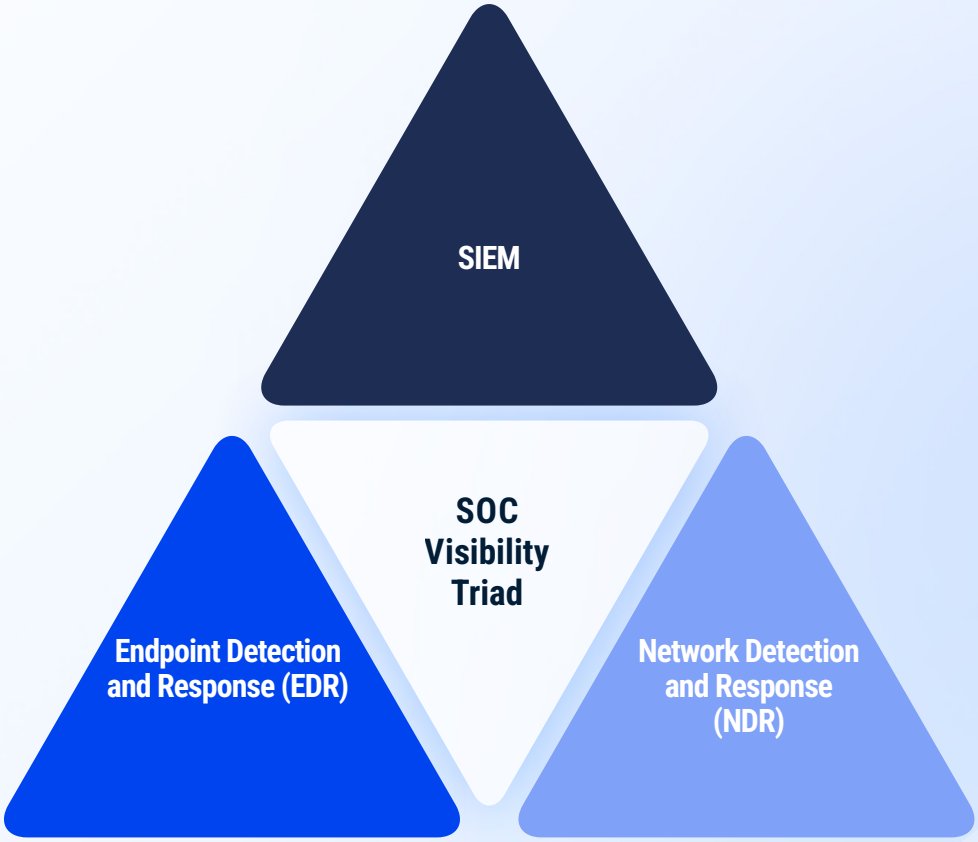
Monitors network traffic and correlates detected threats with network activity. AI and ML are critical technologies to ensure effective detection of known and unknown risks.

03

Endpoint Detection and Response

Captures endpoint (server, desktop, laptop) operations to identify signs of attacks as early as possible.

SOC visibility triad



Source: Upstream Security

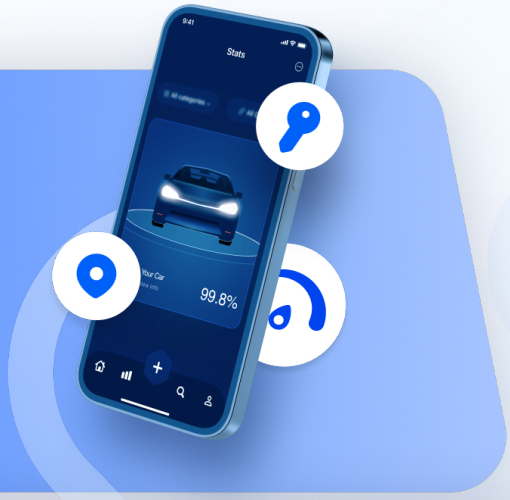
Visual representation of a multi-layered SOC approach, based on Gartner's SOC visibility triad[366]

With the expansion of the Automotive industry into the Smart Mobility ecosystem, vehicles are not the only mobility assets that challenge cyber teams. Applying a SOC approach to the vSOC creates a more secure layering between OEMs, Tier-1s, Telematics Service Providers (TSPs), and other stakeholders in the ecosystem, minimizing threats and preventing attacks. In addition to IT network security, which protects OEM servers and IT backend infrastructure from cyber attacks, the vSOC adds a new layer of protection, focusing on Vehicle Detection and Response (V-XDR):

Three layers of automotive cybersecurity

API security

This new addition to the vSOC is a cross-functional effort between the vSOC and the IT SOC, focusing on protecting API-based applications, services, and features. API security also implements protective measures for vehicles, as APIs are integral to vehicle access and a wide range of functions.

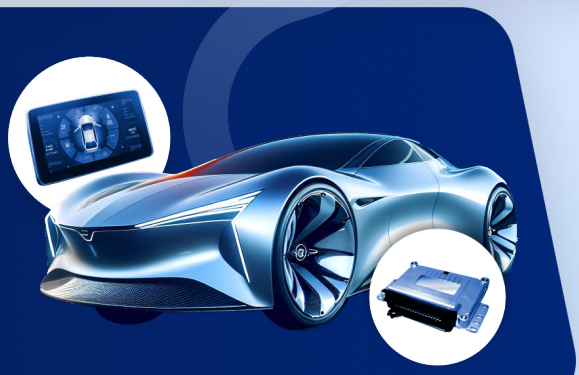


Automotive cloud security

Leverage and monitor the automotive cloud to expand detection to a wide range of mobility assets and cyber threats—including vehicle telematics, OTA updates, remote commands, and diagnostics—and identify multi-vehicle attacks with a fleet-wide view of security across vehicles, applications, and other connected services.

Vehicle security

Monitor and protect internal vehicle components, including ECUs, diagnostics data streams, host security information, CAN / Ethernet events, etc.



Source: Upstream Security

There are unique cybersecurity challenges associated with each layer of the automotive infrastructure. These challenges can be addressed with a multilayered approach, which includes a V-XDR and a purpose-built vSOC.

DEVELOPING AN EFFECTIVE AI-DRIVEN VSOC

SOCs are routinely used to monitor IT systems, infrastructure, and assets at large organizations, including OEMs. But unlike IT infrastructure, which is directly managed by OEMs, vehicles are constantly in motion, not directly under OEM control, and interact with external systems and applications thousands of times a minute.

OEMs are continuously working on solidifying vSOCs and positioning them internally. They are defining vSOC scope, deciding where it belongs in the organizational structure, and evaluating sourcing (e.g., in-house, hybrid, or managed vSOC) and operating models (e.g., one global vSOC, multiple geographies presence, etc.). OEMs must establish vSOCs as soon as possible to comply with R155. There are several options for vSOC implementation:

- Mostly “pure” / standalone vSOCs
- Focused strictly on post-production connected vehicles and driven by regulatory requirements and compliance
- Part of the IT organization; reporting to the CISO; sometimes part of after-sales or global operations
- Sometimes also focused on IT aspects of the connected vehicles infrastructure—the automotive cloud

Some OEMs, however, have already reached higher vSOC maturity. Two new types of vSOCs are emerging in response to the growth in scale and maturing vSOC processes and knowledge:

Fusion vSOC

Incorporates a cross-functional approach combining the basic vSOC functions with OTA health monitoring, DTC monitoring, cyber, etc. The fusion vSOC requires close collaboration with the IT SOC to protect data-driven services and applications across the entire smart mobility ecosystem, which is critical to detect and effectively mitigate complex attack vectors.

IT-OT vSOC

Combines the IT and OT SOCs with the vSOC into a single entity that manages a broad security operations center, covering security elements of the entire vehicle lifecycle— from design to manufacturing (e.g., OT monitoring of vehicle production) and operations. Many OEMs are already expanding the scope of their IT-OT vSOCs to monitor API security risks across their organizations, including both vehicle-related APIs and other enterprise APIs. Some are even exploring further expansion to encompass EV charging stations and related infrastructure.

The vast majority of operational connected vehicle data is owned and managed by OEMs. As we look into the future, we see a dramatic shift in the need for more stakeholders to have access to connected vehicle data, as well as AI tools and capabilities.

Smart mobility stakeholders such as fleet owners and operators, mobility service providers, state governments, local municipalities, and others may need to establish their own independent vSOCs with completely different business objectives than those run by OEMs.

As the number and sophistication of cyber attacks targeting vehicles, mobility applications, OT and IoT mobility devices increase, OEMs must develop integrated vSOCs, also known as “mobility SOCs” or “automotive SOCs”, to protect their vehicles, infrastructure, and customers during the post-production phase. **AI and ML technologies are critical components in combatting the impact of new cybersecurity risks.**

When implemented properly, an effective vSOC has a clear framework—detailing capabilities, components, and operating models—and a well-defined strategy and scope—including a vision, mission, and charter. Advanced AI models are a critical element in many of the vSOC functions:

- Operate 24/7
- Ingest data from various automotive-related feeds and correlate them
- Outline governance and steering policies, standards, procedures, and processes
- Integrate with SIEM and SOAR platforms to ensure cross-organizational visibility and effective remediation
- Detect threats and anomalies in near or real-time using automotive-specific cybersecurity analytics
- Effectively triage and investigate alerts
- Predict threats before they emerge by leveraging purple teams, threat models, and threat intelligence fusion
- Conduct proactive threat hunting
- Build and implement end-to-end playbooks to structure and automate response activities

To ensure the required functionalities are delivered, vSOCs can be built in three ways:

01

Combine

Existing enterprise SOCs can be expanded to include mobility assets, which would require adding OT expertise, specific platforms, and changing operating procedures.

02

Create

Those who are just starting their vSOC journey can create a new dedicated vSOC, building a dedicated team, processes, and playbooks.

03

Contract

The vSOC can be outsourced to a Managed Security Service Provider (MSSP) with both IT and automotive-related cybersecurity capabilities.

During 2024, many OEMs continued to focus on their vSOC implementation journey, working to align their operations with R155. The second milestone of R155, which came into effect in July 2024 and expanded coverage to include all new vehicles in production as well as Category L vehicles,[367] marked a significant step toward harmonizing cybersecurity standards across the automotive industry. As R155's scope expands further, the need for deeper regulatory efforts and stricter compliance measures becomes increasingly critical.

OEMs and Smart Mobility stakeholders need a contextual approach to API security that goes beyond the OWASP Top 10

In practice, API hacking at the entry level is relatively standardized, requires lower technical expertise, and can be done remotely without special hardware—making it more cost-effective to attack than other types of systems. The Open Web Application Security Project (OWASP) API Security Top 10[368] serves as an IT industry standard to help developers and security teams understand API risks and is updated as threats evolve.

Updated in 2023, the top 10 list includes:

01 **Broken Object Level Authorization**

02 **Broken Authentication**

03 **Broken Object Property Level Authorization**

04 **Unrestricted Resource Consumption**

05 **Broken Function Level Authorization**

06 **Unrestricted Access to Sensitive Business Flows**

07 **Server-Side Request Forgery**

08 **Security Misconfiguration**

09 **Improper Asset Management**

10 **Unsafe Consumption of APIs**

The updated OWASP API Top 10 risk list underscores the evolving threat landscape and the crucial need for vigilance and proactive cybersecurity measures. The impact of API-based attacks is felt in service disruptions, vehicle and driver safety, data breaches, and privacy, fraudulent activities aimed at bypassing subscriptions and feature limitations, as well as brand reputation.

But in the context of the Automotive and Smart Mobility ecosystem, IT-based API security like OWASP, is not enough. IT-based security solutions focus on transactions, permissions, volumes, values, and payload correctness—often ignoring the contextual state of mobility assets, their physical behavior on the road and safety impact. In addition to API traffic, extended detection should consider additional data sources, such as telematics data. By combining these two sources of information, organizations can gain a deeper understanding of potential threats and vulnerabilities. API security requires a holistic view, contextualizing operational data and API traffic to reflect the state of vehicles, applications, and consumers.

A variety of data sources can be leveraged alongside API traffic and documentation to identify anomalies that indicate a threat to operational systems:

- Vehicle, user, and device location
- User and vehicle identification numbers
- Vehicle telematics
- Billing and login history
- Charging station protocols

Mobility stakeholders are evaluating responsibilities related to monitoring and detecting API-based cybersecurity risks. Such risks can be analyzed under the enterprise SOC, the vSOC, or a new IT-OT SOC.

Proactive risk management with automotive-specific threat intelligence

The multi-layered approach must also include proactive measures to enhance threat detection capabilities, such as monitoring cyber threat intelligence. OEMs and mobility stakeholders should proactively identify and mitigate vulnerabilities in their products while remaining compliant. By using an industry-specific and purpose-built threat feed, stakeholders can remain continuously updated with new threats based on surface, deep, and dark web findings.

Automotive-specific threat intelligence has become increasingly important as the connected vehicle ecosystem evolves and introduces large-scale cyber risks. Cyber vulnerabilities and attacks impact the entire supply chain, jeopardizing trust and safety. They require all stakeholders to be proactive in analyzing risks, monitoring threats, and responding effectively to cyber attacks.

Threat actors are increasingly targeting telematics and other connected vehicle data as OEMs strive for greater connectivity in their vehicles. Only automotive-specific threat intelligence products can understand a vehicle's context to quickly identify anomalies and remove false alarms that may desensitize cybersecurity teams.

UPSTREAM'S AI-DRIVEN AND CLOUD-BASED APPROACH TO AUTOMOTIVE CYBERSECURITY

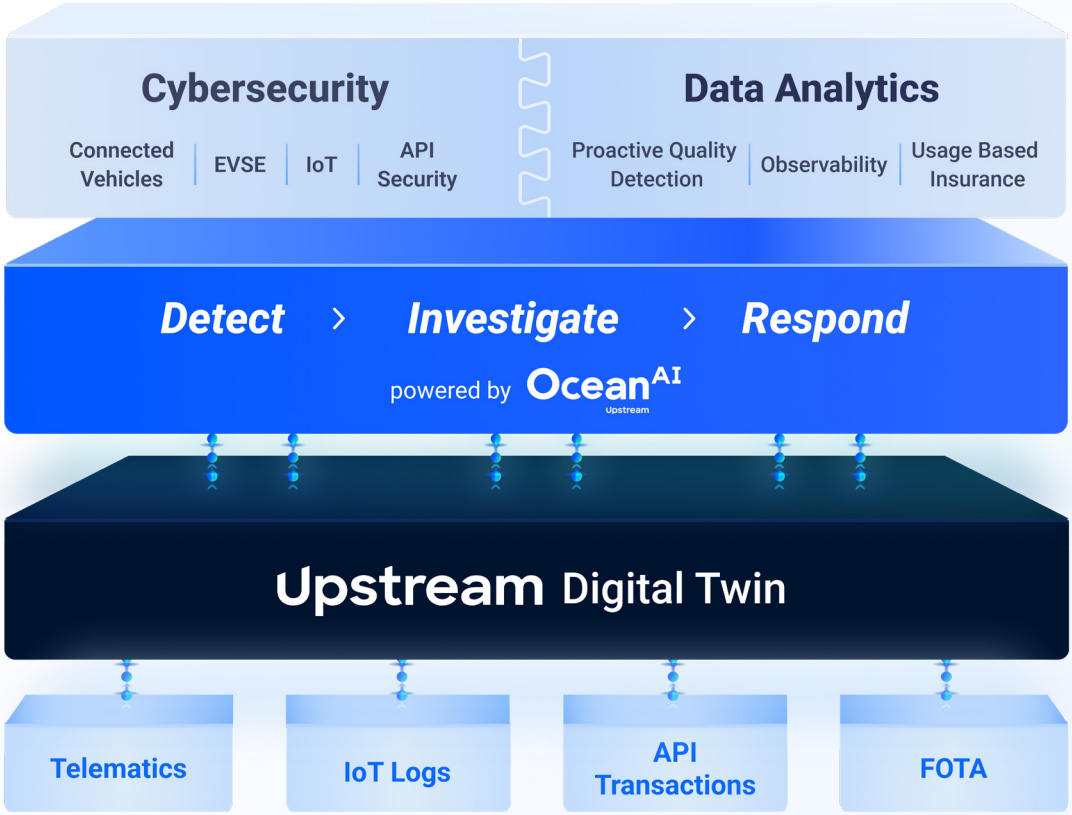
Upstream introduced a fundamental and innovative shift in Automotive and Smart Mobility cybersecurity with the first cloud-based data management platform, purpose-built for connected vehicles, IoT, and smart mobility. Unlike other cybersecurity protection approaches that cover each surface in isolation, Upstream developed a unique approach that monitors cyberattack surfaces across the entire smart mobility ecosystem, including in-vehicle components, IoT devices, telematics, diagnostics, consumer applications, OTA updates, EV chargers, and more.

The Upstream Platform[369] is agentless, with no need to install hardware or software on vehicles or devices, and delivers unparalleled cybersecurity detection and response.

> ***Powered by Ocean AI, Upstream's advanced AI capabilities, the Platform enables stakeholders to effectively detect, investigate, automate and mitigate a wide range of cybersecurity attacks.***

The Upstream Platform transforms fragmented, distributed mobility data into centralized, structured, and contextualized data lakes, unlocking its full potential. **By leveraging this data, Upstream empowers customers with advanced, AI-driven applications across various use cases, including cybersecurity detection and response (XDR), fraud prevention, proactive vehicle quality, observability, usage-based insurance, and more.**

In early 2024, Upstream unveiled Ocean AI,[370] a cutting-edge suite of AI and ML capabilities designed to revolutionize detection, investigation, and response processes. Beyond its advanced platform features and robust ML-based detection, which focus on data efficiency, detection, and actionable insights, Ocean AI incorporates Generative AI (GenAI) capabilities to maximize the ROI of connected vehicle data. These capabilities empower organizations with unparalleled flexibility in conducting cyber investigations and optimizing outcomes.

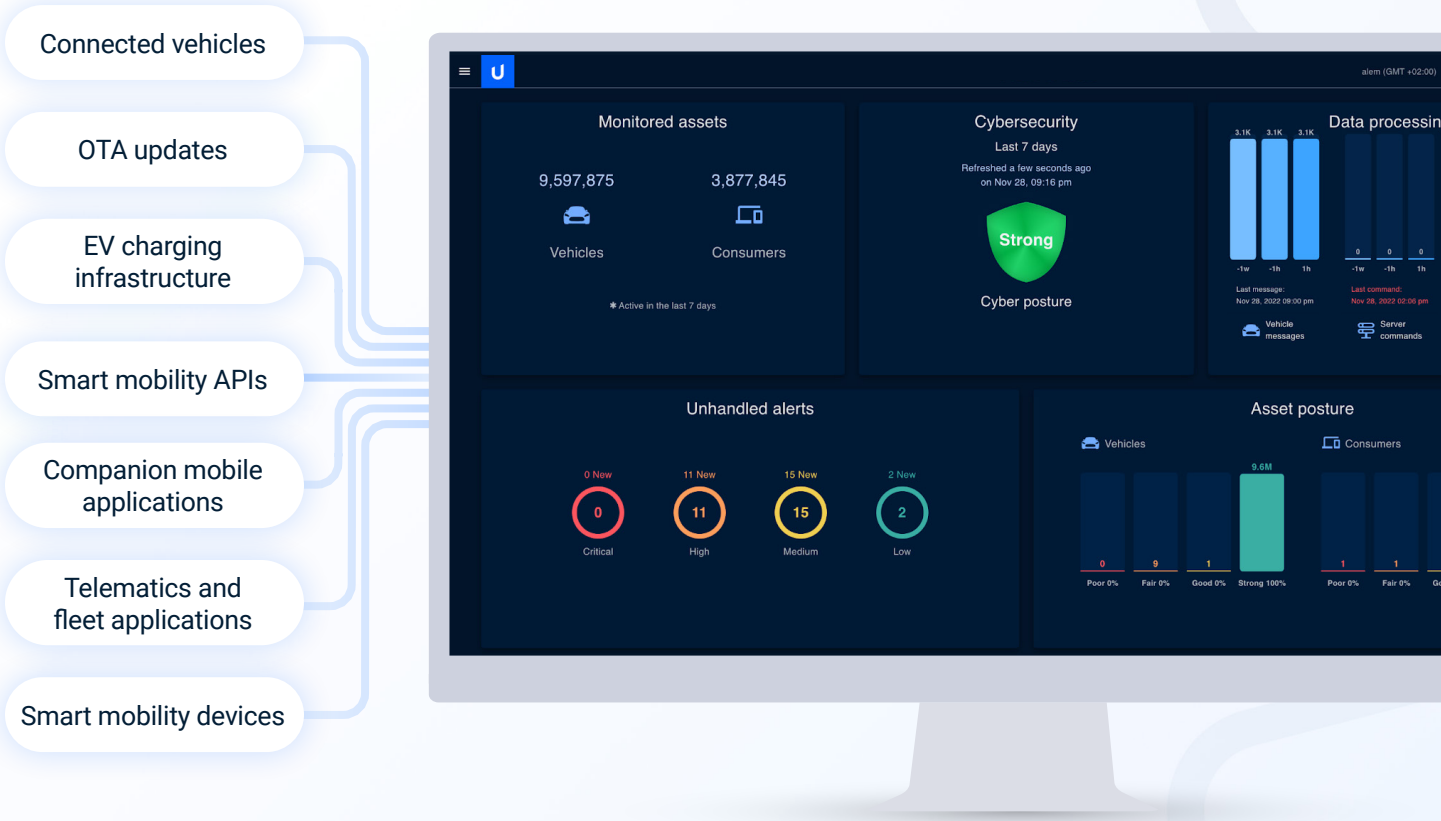


Source: Upstream Security

Purpose-built Detection & Response platform (XDR)

Designed to use IT, OT, IoT, and connected vehicle data, the Upstream Platform has significantly evolved into a robust cybersecurity detection and response platform (XDR),[371] containing advanced machine learning and AI models, and hundreds of detectors that address unknown and unknown mobility-related cybersecurity risks.

Today, the Upstream Platform monitors tens of millions of vehicles, smart mobility devices and charging stations worldwide, supporting detection and response efforts, as well as vSOCs, for some of the world's largest OEMs and smart mobility players. Additionally, the platform monitors billions of API transactions each month and has expanded its scope to include EV charging infrastructure[372] and mobility IoT,[373] all of which are at the heart of automotive and smart mobility digital transformation.



Source: Upstream Security

The Upstream Platform utilizes data normalization and cleansing, live digital twin profiling, mobility intelligence, AI and ML-powered detection, and unique GenAI capabilities to identify anomalies in mobility data and offer unparalleled data-driven actionable insights through mobility-specific applications.

Upstream's ability to handle numerous data streams and develop advanced data-driven applications has encouraged automotive and smart mobility stakeholders to extend its use beyond cybersecurity:

Cybersecurity XDR	Monitor, detect, and investigate cybersecurity-related attacks, threats, risks, and vulnerabilities.
EV charging	Monitoring EV charging stations and infrastructure to detect and mitigate cyber attacks targeting EV charging operational availability, safety and data, as well as risks affecting vehicles and power grids.
Smart mobility devices	Secure and monitor connected devices in the Mobility and Transportation ecosystem to mitigate operational disruptions and protect sensitive data.
API security	Monitor and protect smart mobility API-based applications, devices, and services to ensure continuous operational availability and protect data.
Proactive quality detection	Monitor component failures earlier, predict scale and severity, and help after-sales quality engineers with Root Cause Analysis (RCA), ultimately reducing warranty and recall costs.
Fraud detection	Identify fraud-related scenarios including odometer rollback, vehicle theft, etc.

Data engineering designed for Automotive and Smart Mobility data streams

To address the diverse data sets inherent in the automotive, mobility, and transportation industries, Upstream leverages a universal dictionary for data normalization. Consequently, the Platform efficiently centralizes and standardizes multiple data feeds, sources, and telematics services.

The live digital twin

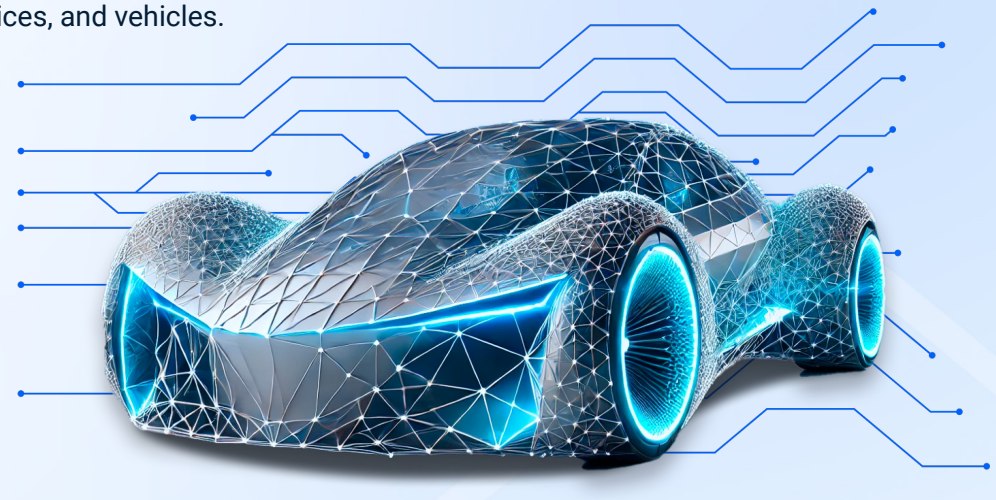
The digital twin is a core element of the Upstream Platform. Stored in the cloud and continuously enriched, it digitally represents any asset, such as vehicles, smart mobility devices, EV charging stations and infrastructure, and application consumers. The digital twin captures data from numerous sources, providing a real-time snapshot of the monitored asset throughout its lifecycle. By synthesizing events and anomalies in data, it effectively detects potential attacks and pinpoints threats.

AI and ML-powered detection and investigations

The Upstream Platform leverages domain expertise and ML-powered anomaly detection to identify both known and unknown threats. AI and ML-powered anomaly detection excels at uncovering hard-to-recognize attacks. Using proprietary models, the Platform monitors individual vehicles, consumers, and overall fleet behavior. It identifies abnormal activities isolated to a single endpoint or across the entire fleet. Upstream enables prompt and effective threat mitigation and SOC optimizations with Generative AI-powered investigations, automated remediation and response, leveraging domain expertise in automotive cybersecurity and field-proven playbooks.

Extending detection and response to mitigate API-driven risks

With API-based cyber attacks and vulnerabilities proliferating, smart mobility stakeholders now face the challenge of monitoring billions of API transactions every month. Upstream's API Security layer[374] correlates between API transactions and the robust digital twin of the Upstream Platform, offering a contextual and comprehensive view of all assets impacted—from the consumer application to IoT devices, and vehicles.



With Upstream's API stecurity solution, mobility stakeholders can benefit from:

01

API discovery

Get a complete catalog of all documented, undocumented, and deprecated-but-alive APIs with real-time traffic data, including APIs used by 3rdparties or internal services.

02

API monitoring

Conduct ongoing conformance analysis with continuous discovery of static and dynamic traffic sources to identify potential vulnerabilities in the API landscape.

03

Fusion detection

Apply advanced AI and ML models to effectively detect unknown threats and attacks, including complex low and slow attacks.

No-code detector builder

Insuring customizations and flexible detection is critical for long-term agility. The Upstream Platform offers a no-code detector builder, leveraging Upstream's digital twin, to easily customize detectors and add new detection capabilities. These capabilities support customers ability to mitigate emerging use cases and support new business logic without coding or development resources.

Proactive cyber threat intelligence

Working closely with Upstream's AutoThreat® PRO,[375] security teams can gain unparalleled visibility into the mobility threat landscape with actionable asset-specific intelligence.

AutoThreat® PRO combines vulnerability intelligence with automotive-specific exploit research. It leverages hundreds of deep, dark, and clear web sources to uncover vulnerabilities and exploits, as well as map and engage with threat actors. The scope spans across both on-board and off-board systems: on-board intelligence includes findings related to in-vehicle tampering of connected products such as IVI jailbreaks or TCU rooting; whereas offboard intelligence expands to external and third-party vulnerabilities, including unauthorized access to vehicle data and controls via diagnostic tools or mobile app tampering.

Curated intelligence (HUMINT) allows stakeholders to leverage Upstream's robust intelligence collection infrastructure to expand coverage, and safely and anonymously interact on the deep and dark web. Upstream's expert cyber threat intelligence analysts are deeply familiar with the Automotive and Smart Mobility ecosystem, which allows them to offer unique insights into threat actor motivations and effective mitigation recommendations.

Source: Upstream Security

In March 2024, Auto-ISAC introduced the Automotive Threat Matrix (ATM), a significant initiative to improve automotive cyber threats assessment and sharing. Upstream recently integrated the ATM with AutoThreat®PRO to help automotive stakeholders effectively operationalize it.[376]

AutoThreat®PRO utilizes ATM's tactics and techniques, and organizes attacks based on affected components, vectors, and potential impact, which helps cybersecurity teams pinpoint vulnerabilities more precisely, and links attacks to the MITRE ATT&CK framework for a comprehensive view.

The Upstream Platform automatically links findings from the deep and dark web with relevant ATM techniques, offering a comprehensive view of current threats. It also aligns these findings with regulatory requirements, such as R155 Annex 5, providing actionable insights and accelerating compliance.

AutoThreat®PRO provides a unique view of threat actors' activities and motivations by mapping threat actor intelligence to ATM. This helps cybersecurity teams prioritize risks and implement proactive risk management strategies.

Source: Upstream Security

Upstream's AutoThreat® Platform and AutoThreat®PRO

Managed vehicle and mobility SOC

Leverage the leading managed vehicle and mobility SOC that protects millions of vehicles and mobility endpoints worldwide, enhancing OEM cyber resilience through comprehensive services. Upstream's SOC[377] actively monitors cyber threats targeting connected vehicles, devices, and their components. Leveraging experience with top global passenger, commercial, agriculture and EV OEMs, Upstream's SOC integrates mobility data sources to build cross-functional response capabilities.

Upstream's managed SOC deploys rapidly, integrating into existing enterprise processes and platforms. The Build-Operate-Transfer (BOT) model offers flexibility without vendor lock-in, enabling security teams to take over operations at any time. Custom playbooks and automated workflows tailored to each customer's organization and work methodologies ensure that response protocols fit specific customer needs and promptly address threats. The playbooks include automated workflows such as blocking suspicious IP addresses, alerting vehicle owners to phishing attempts, controlling the OTA servers, and more.

Comprehensive threat detection and response

Upstream's managed SOC monitors connected vehicle and device data in near real-time, securing against a wide range of cyber threats, including API security risks, emerging IoT threats, EV charging manipulations, vehicle-related fraud, and vulnerabilities affecting the entire fleet. Powered by the Upstream Platform, the SOC applies AI and ML-based detection to contextualize data and identify known and unknown cyber risks.

AI-powered enhanced investigations and mitigation

Powered by Upstream's AI capabilities, Ocean AI, the managed SOC leverages unprecedented efficiencies and mitigation capabilities by optimizing alert handling, identifying unique patterns, and accelerating mitigation. Ocean AI taps into Upstream's enriched data, live digital twin, and detection capabilities to deliver deep insights and support advanced investigations. It also integrates threat intelligence feeds to enhance risk assessments.

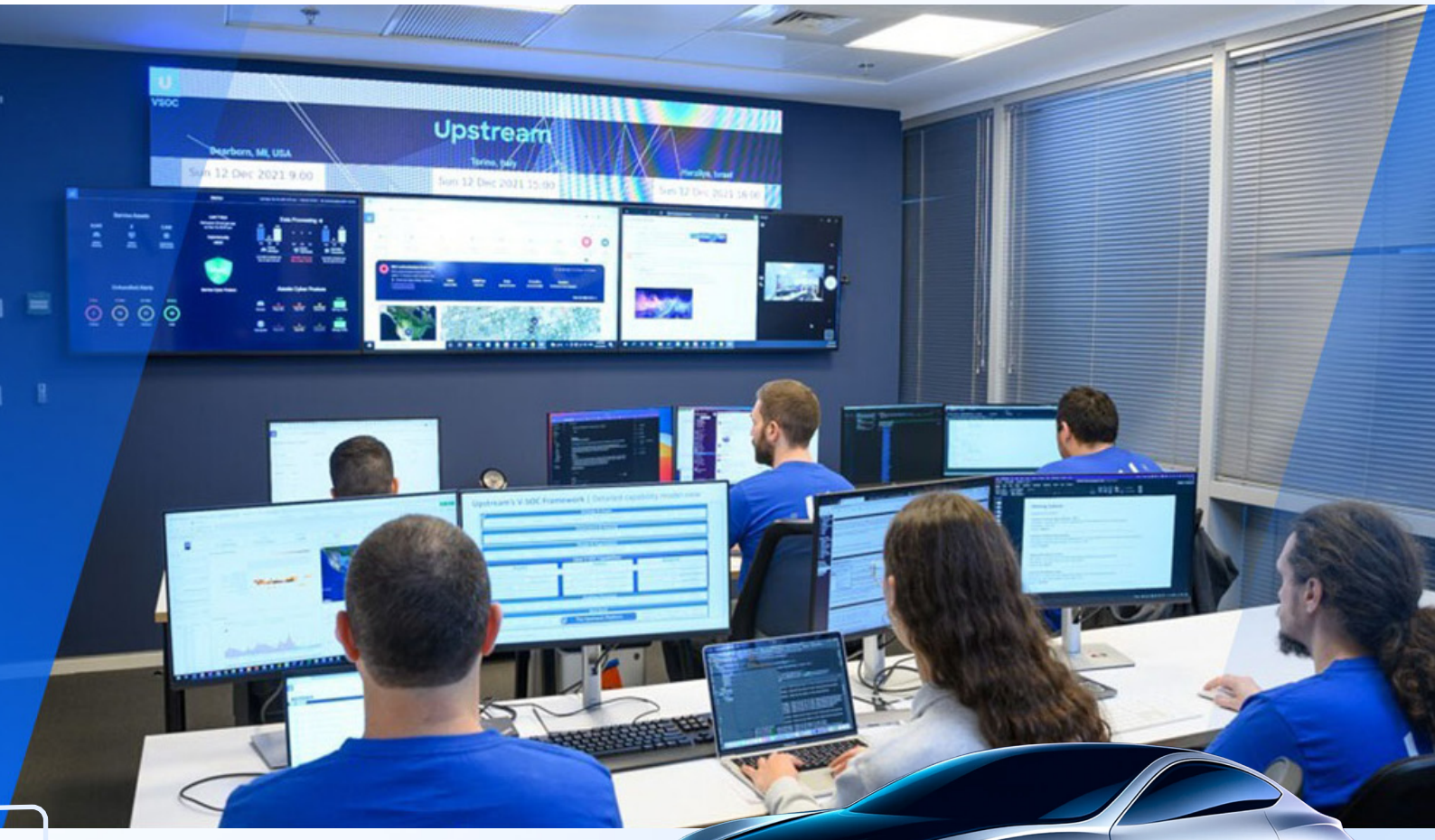
Secure and compliant operations

Upstream's managed SOC operates from state-of-the-art secure facilities using a follow-the-sun model. It complies with global data protection regulations, such as GDPR, and employs role-based access control (RBAC) to protect data privacy. The SOC also offers remote auditing capabilities to maintain high security standards across operations.

Mobility & IoT cyber readiness services

Upstream has expanded its cybersecurity services portfolio to empower Product Security Incident Response teams (PSIRT) with a comprehensive suite of tools and simulations, purpose-built for the Automotive and Smart Mobility ecosystem:[378]

- **Incident Response Training:** Hands-on practice through extensive simulations to enhance preparedness and operational readiness.
- **Maturity Assessments:** Rigorous benchmarking of cybersecurity posture against industry standards to identify strengths and areas for improvement.
- **Stakeholder Education:** Tailored training programs to align team capabilities with industry best practices and evolving threats.



Upstream's vSOC

08.

PREDICTIONS FOR 2025

Martin Arend

General Manager Automotive Security, BMW Group

As we look ahead to 2025, threats are expected to be on the rise within the Automotive ecosystem, increasingly driven by AI. These threats may target the vehicle itself, its backend systems, or the mobile applications that interact with it.

At BMW Group, maintaining a sharp focus on the effectiveness of our field measures is paramount to ensure we can respond swiftly and comprehensively. To meet these challenges, we will continue prioritizing the reliability and scalability of our detection systems, making them a cornerstone of our cybersecurity strategy.

Karin Shopen

VP of Product Management, Cisco Talos Intelligence Group, Cisco Security

Connected Autonomous Vehicles (CAVs) are a transformative innovation in transportation. However, like any new technology, they present associated cyber threats that could have financial consequences for organizations and physical safety risks for the public.

Due to increased vehicle connectivity, complex supply chains, and manufacturers' data monetization efforts, CAVs' attack surfaces are expansive—hence the importance and urgency of developing and executing a full-cycle security practice for CAVs and their ecosystem.

Wulf Schlachter

CEO, Management Advisory, DXBe

The risk of hacking EV charging infrastructure is a pressing concern, particularly as it intersects with critical IT systems and infrastructure. With charging networks becoming increasingly interconnected, they present new vulnerabilities for cybercriminals to exploit. A compromised charging station could act as a gateway for broader attacks, potentially jeopardizing other critical infrastructure such as the power grid or backend networks.

In the context of recent discussions around hybrid warfare, the growing digitization and interconnectedness of charging infrastructure heightens its appeal as a target for cyber threats. To mitigate these risks, EV charging operators and manufacturers must adopt robust cybersecurity standards and prioritize regular updates to safeguard against evolving threats.

Ozgur Tohumcu

General Manager, Automotive & Manufacturing, AWS

In 2025, the adoption of advanced SDV modules and ECU virtualization will deepen, driving the shift to end-to-end E/E architectures. Virtualized ECUs and tools will streamline vehicle software development, while Generative AI will accelerate workflows, enhance cybersecurity testing, and enable automated reasoning for assisted code remediation. OEMs will leverage Generative AI to strengthen security operations, detection, vulnerability management, and incident response capabilities.

The proliferation of AI will also push OEMs to adopt responsible AI practices and address the security challenges of automotive generative AI edge applications. Key considerations will include content moderation at the edge, securing OTA model updates, and safeguarding cyber-physical systems against foundation model theft via physical attacks. Despite significant investments in AI-driven cybersecurity, OEMs must continue prioritizing foundational security practices such as identity and access management, data protection, and threat modeling to ensure a robust defense against evolving threats.

Martin Hofmann

Chief Business Officer, Terra Quantum AG

The growing influence of global regulations such as UNECE WP.29 and the Cyber Resilience Act is pushing automakers to implement robust cybersecurity measures across their entire lifecycle and supply chain.

However, as the industry embraces electrification, AI, and autonomous technologies, cybersecurity has evolved from being merely a compliance necessity to a strategic competitive advantage.

These transformative technologies require a proactive and scalable approach to identifying and addressing cyber risks with far-reaching implications.

Vinod D'Souza

Office of the CISO, Head of Manufacturing and Industry, Google Cloud

In 2025, geopolitical tensions and state-sponsored cyberattacks will escalate risks for automotive manufacturers, targeting critical infrastructure and intellectual property. The convergence of IT and OT systems and reliance on interconnected technologies will expand the attack surface, exposing new vulnerabilities. Ransomware is also expected to grow more disruptive, focusing on production lines and supply chains, while AI-powered attacks will become more sophisticated, leveraging automation and ML to challenge defenses.

Continued adoption of AI by defenders will help them stay ahead of attackers in 2025, but a collaborative approach to cybersecurity is needed for effectively mitigating risks across the entire lifecycle and supply chain. Adopting secure cloud platforms and fostering greater information sharing will be key strategies for enhancing supply chain security and improving resilience in an interconnected ecosystem.

Tim Geiger

Senior Director, Vehicle and Connected Cyber Security, Ford Motor Company

Automakers face a growing cybersecurity challenge as connected vehicles become increasingly prevalent. APIs play a crucial role in enabling communication between vehicle systems, external devices, and cloud services. At the same time, attackers are becoming increasingly sophisticated in exploiting API vulnerabilities.

Safeguarding automotive APIs is essential to ensure the safety, privacy, and trust of connected vehicles as proactive measures today can prevent significant incidents tomorrow.

Mike Lexa

CISO & Vice President IT Infrastructure, CNH Industrial

In 2025, CISOs in the automotive industry will encounter heightened cybersecurity challenges driven by the proliferation of connected, autonomous, and electric vehicles. These innovations significantly expand the attack surface, introducing vulnerabilities in areas such as over-the-air updates, infotainment systems, and vehicle-to-everything (V2X) communications. Compounding these risks are stricter regulations, supply chain complexities, and the dual use of AI for both cyberattacks and defense.

To navigate this evolving landscape, CISOs must adopt robust cybersecurity frameworks, conduct rigorous vendor assessments, and implement proactive threat detection strategies. Prioritizing regulatory compliance, leveraging AI-driven cybersecurity solutions, and investing in workforce training will be essential to safeguarding against evolving threats.

Yoav Levy

CEO and Co-Founder, Upstream Security

As we look toward 2025, the cybersecurity landscape in the automotive industry is poised to become more complex than ever. Threat actors have already shifted toward large-scale, sophisticated attack methods, targeting not only vehicles but also interconnected systems such as EV charging infrastructure, API-driven companion apps, and dealership networks. This growing attack surface will demand a transformative and proactive approach to cybersecurity.

AI will take center stage in addressing these risks. While many OEMs have already made early investments, 2025 will see an acceleration in AI adoption, integrating it across detection, investigation, and mitigation processes. Real-time data processing will enable faster anomaly detection, more precise threat identification, and swift, automated responses—setting a new benchmark for protection in the mobility ecosystem. To navigate this evolving landscape, a forward-looking strategy combining advanced XDR and robust API security will be essential.

REFERENCES

1. https://www.blackberry.com/us/en/company/newsroom/press-releases/2024/blackberry-qnx-research-reveals-rising-pressure-on-software-engineers-leads-to-critical-trade-offs-in-safety-and-security
2. https://unece.org/sites/default/files/2021-03/R155e.pdf
3. https://unece.org/sites/default/files/2021-03/R156e.pdf
4. https://www.iso.org/standard/70918.html
5. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504
6. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
7. https://www.govinfo.gov/app/details/CRPT-104hrpt736/CRPT-104hrpt736
8. https://www.pcisecuritystandards.org
9. https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx
10. Upstream's 2024 Global Automotive Cybersecurity Report
11. Upstream's 2024 Global Automotive Cybersecurity Report
12. https://home.treasury.gov/news/press-releases/jy2292
13. https://www.justice.gov/opa/pr/justice-department-charges-four-iranian-nationals-multi-year-cyber-campaign-targeting-us
14. https://www.justice.gov/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals
15. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a
16. https://www.sec.gov/newsroom/press-releases/2023-139
17. https://eur-lex.europa.eu/eli/dir/2022/2555
18. https://therecord.media/orbcomm-trucking-software-ransomware
19. https://www.bleepingcomputer.com/news/security/orbcomm-ransomware-attack-causes-trucking-fleet-management-outage/
20. https://cyberpress.org/orbcomm-data-breach-exposes-70-tb-of-data/
21. https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/
22. https://edition.cnn.com/2024/07/11/business/cdk-hack-ransom-tweny-five-million-dollars/index.html
23. https://www.andersoneconomicgroup.com/dealer-losses-due-to-cdk-cyberattack-reach-1-02-billion/
24. https://www.cyberdaily.au/security/10245-who-is-mogilevich-the-newest-ransomware-gang-on-the-darknet
25. https://www.bleepingcomputer.com/news/security/hyundai-motor-europe-hit-by-black-basta-ransomware-attack/
26. https://hackmanac.com/news/hacks-of-today-14-03-2024
27. https://www.quattroruote.it/news/industria-finanza/2024/04/15/mercedes_benz_rilevato_attacco_hacker_possibili_violazioni_ai_dati_dei_clienti.html
28. https://x.com/H4ckManac/status/1808912853526794442
29. https://x.com/FalconFeedsio/status/1822544253882614181
30. https://dailydarkweb.net/cybervolk-group-claims-cyber-attacks-against-chinese-companies/
31. https://www.hackster.io/news/madradar-triggers-hallucinations-in-autonomous-vehicle-sensor-systems-researchers-say-b56b87763cbd
32. https://www.techexplorist.com/study-finds-security-flaws-first-next-gen-lidar-systems/81641/
33. https://www.theregister.com/2024/05/10/baidu_apollo_hack
34. https://dl.acm.org/doi/10.1145/3636534.3649372
35. https://samcurry.net/hacking-kia
36. https://samcurry.net/hacking-kia
37. https://securityonline.info/cve-2024-35213-critical-vulnerability-discovered-in-blackberry-qnx-sdp/
38. https://arxiv.org/html/2409.01324v1
39. Source: Upstream Security
40. https://www.iata.org/contentassets/c8e90fe690ce4047a8edfa97f4824890/iata_safety_risk_assessment_gnss_interference.pdf
41. https://www.securityweek.com/bosch-nutrunner-vulnerabilities-could-aid-hacker-attacks-against-automotive-production-lines/
42. https://www.cbc.ca/news/canada/hamilton/ransomware-attack-1.7133457
43. https://www.telegraph.co.uk/news/2024/02/21/car-charger-withdrawn-hackers-could-attack-national-grid/
44. https://www.ndss-symposium.org/wp-content/uploads/vehiclesec2024-47-paper.pdf
45. https://www.trucking.org/economics-and-industry-data
46. https://lemken.com/de-de/lemken-aktuelles/landtechnik-news/detail/lemken-von-cyberattacke-betroffen
47. https://thecyberexpress.com/alleged-frotcom-data-breach/
48. https://www.redthreatsec.com/blog/greenlightspart1
49. https://www.fleetnews.co.uk/news/telematics-giant-microlise-suffers-cyber-attack
50. https://eur-lex.europa.eu/eli/dir/2022/2555

REFERENCES

51. https://data.consilium.europa.eu/doc/document/ST-12041-2023-INIT/en/pdf
52. https://www.consilium.europa.eu/media/69093/st16996-en23.pdf
53. https://www.cnbc.com/2024/09/20/eu-nis-2-what-tough-new-cyber-regulations-mean-for-big-business.html
54. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
55. https://www.europarl.europa.eu/news/en/press-room/20240308IPR18991/cyber-resilience-act-meps-adopt-plans-to-boost-security-of-digital-products
56. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet
57. https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime
58. https://docs.fcc.gov/public/attachments/DOC-401201A1.pdf
59. https://www.sec.gov/news/press-release/2023-139
60. https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework
61. https://www.iso.org/standard/88353.html
62. https://upstream.auto/blog/agricultural-oems-new-safety-and-availability-standards/
63. https://sgp.fas.org/crs/row/IF10964.pdf
64. https://www.uschamber.com/assets/archived/images/final_made_in_china_2025_report_full.pdf
65. https://newsletter.dunneinsights.com/p/surrender-to-china-or-punch-back
66. https://insideevs.com/news/715427/tesla-ev-production-shanghai-vs-global/
67. https://www.globaltimes.cn/page/202408/1317819.shtml
68. https://www.autohome.com.cn/rank/1
69. https://www.cnbc.com/2024/10/31/chinese-ev-maker-byds-quarterly-sales-overtook-teslas-for-the-first-time.html
70. https://www.globaltimes.cn/page/202401/1305028.shtml
71. https://english.www.gov.cn/news/202401/09/content_WS659ced27c6d0868f4e8e2e3b.html
72. https://www.sac.gov.cn/
73. https://igarr.com/2024/05/06/china-new-collision-safety-standards-for-passenger-vehicles/
74. https://english.www.gov.cn/news/202406/22/content_WS6676229dc6d0868f4e8e8708.html
75. https://wap.miit.gov.cn/jgsj/zbys/qcgy/art/2024/art_e1bb0d211dbf40a2949b28deb8a96d19.html
76. https://dissec.to/general/chinas-new-vehicle-cybersecurity-standard-gb-44495-2024/
77. https://ransomwareattacks.halcyon.ai/attacks/bianlian-attacks-keboda-technology
78. https://www.linkedin.com/posts/arun-mane-272456166_cybersecurity-iso21434-r155regulation-activity-7191932471561617409-MUPA/
79. https://ransomwareattacks.halcyon.ai/attacks/lockbit-ransomware-strikes-qufu-temb-auto-parts-in-china
80. https://www.techradar.com/pro/security/mystery-database-containing-sensitive-info-on-762-000-car-owners-discovered-by-researchers
81. https://dailydarkweb.net/cybervolk-group-claims-cyber-attacks-against-chinese-companies/
82. https://kevin2600-cmd.github.io/2024/09/13/Grand-Theft-Auto-A-peek-of-BLE-relay-attack.html
83. https://kevin2600-cmd.github.io/2024/09/13/Braktooth-Hunting-in-the-Car-Hacker%27s-Wonderland.html
84. https://edition.cnn.com/2024/02/07/cars/china-ev-global-push-intl-hnk/index.html
85. https://www.bis.gov/press-release/commerce-announces-proposed-rule-secure-connected-vehicle-supply-chains-foreign
86. https://www.reuters.com/business/autos-transportation/us-propose-barring-chinese-software-hardware-connected-vehicles-sources-say-2024-09-21/
87. https://www.politico.eu/article/europe-looks-to-follow-on-tackling-risk-of-chinese-car-software/
88. https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security
89. https://www.bbc.com/news/articles/cly20n4d0g9o
90. https://www.reuters.com/business/autos-transportation/china-tells-carmakers-pause-investment-eu-countries-backing-ev-tariffs-sources-2024-10-30/
91. https://securityaffairs.com/156843/reports/bmw-affected-by-redirect-vulnerability.html
92. https://therecord.media/foxsemicon-ransomware-attack-taiwan
93. https://techcrunch.com/2024/01/11/hyundai-motor-india-data-exposed/
94. https://techcrunch.com/2024/02/14/bmw-security-lapse-exposed-sensitive-company-information-researcher-finds
95. https://www.bleepingcomputer.com/news/security/hyundai-motor-europe-hit-by-black-basta-ransomware-attack/
96. https://www.delfi.lt/en/business/data-of-20-000-ignitis-on-clients-leaked-in-cyber-incident-95857777
97. https://www-theregister-com.cdn.ampproject.org/c/s/www.theregister.com/AMP/2024/03/22/boffins_tucktotruck_worm/
98. https://ransomwareattacks.halcyon.ai/attacks/bianlian-attacks-keboda-technology
99. https://hackread.com/ev-charging-firm-spills-trove-of-customer-info
100. https://www.techradar.com/pro/security/taxi-software-firm-breach-exposes-details-of-over-300000-passengers

REFERENCES

101. https://www.manager-magazin.de/unternehmen/autoindustrie/volkswagen-chinesische-hacker-sollen-vw-ueber-lange-zeit-ausspioniert-haben-a-2936f896-4d41-4ee3-8ccd-8abafc6b016d
102. https://www.youtube.com/watch?v=qWmiyprxziw
103. https://www.youtube.com/watch?v=B0yzk0Oi6mE
104. https://thecyberexpress.com/alleged-frotcom-data-breach/
105. https://www.standaard.be/cnt/dmf20240523_94739718
106. https://nvd.nist.gov/vuln/detail/CVE-2024-35537
107. https://securityonline.info/cve-2024-35213-critical-vulnerability-discovered-in-blackberry-qnx-sdp/
108. https://en.as.com/latest_news/cdk-global-and-their-car-dealership-software-what-we-know-about-the-ransomware-attack-n/
109. https://www.andersoneconomicgroup.com/dealer-losses-due-to-cdk-cyberattack-reach-1-02-billion/
110. https://blog.ret2.io/2024/07/17/pwn2own-auto-2024-charx-bugs/
111. https://cybersecuritynews.com/traffic-light-controller-authentication-bypass-vulnerability/
112. https://www.redhotcyber.com/post/il-threat-actors-888-rivendicata-una-compromissione-ai-danni-dei-clienti-bmw/
113. https://cybernews.com/security/android-head-units-drivers-data-safety/
114. https://www.businesskorea.co.kr/news/articleView.html?idxno=223166
115. https://innovationorigins.com/en/chip-hacking-poses-threat-to-public-transport-security/
116. https://arxiv.org/html/2409.01324v1
117. https://kevin2600-cmd.github.io/2024/09/13/Braktooth-Hunting-in-the-Car-Hacker's-Wonderland.html
118. https://samcurry.net/hacking-kia
119. https://cybernews.com/news/dutch-government-will-replace-hackable-traffic-lights/
120. https://cyberinsider.com/volkswagen-says-its-monitoring-the-situation-following-8base-ransomware-claims/
121. https://www.synacktiv.com/sites/default/files/2024-10/hexacon_0_click_rce_on_tesla_model_3_through_tpms_sensors_light.pdf
122. https://www.fleetnews.co.uk/news/telematics-giant-microlise-suffers-cyber-attack
123. https://cyberinsider.com/zero-day-flaws-in-mazdas-infotainment-expose-cars-to-takeover-attacks/
124. https://www.cyberdaily.au/security/11395-tesla-data-breach-falsely-claimed-by-intelbroker-third-party-ev-charging-firm-actually-breached
125. https://techcrunch.com/2024/12/12/researchers-find-security-flaws-in-skoda-cars-that-may-let-hackers-remotely-track-them/
126. https://github.com/zgsnj123/BYD_headunit_vuls/tree/main
127. https://www.bleepingcomputer.com/news/security/auto-parts-giant-lkq-says-cyberattack-disrupted-canadian-business-unit
128. https://www.bleepingcomputer.com/news/security/hyundai-motor-europe-hit-by-black-basta-ransomware-attack/
129. https://edition.cnn.com/2024/07/11/business/cdk-hack-ransom-tweny-five-million-dollars/index.html
130. https://www.andersoneconomicgroup.com/dealer-losses-due-to-cdk-cyberattack-reach-1-02-billion/
131. https://www.fleetnews.co.uk/news/telematics-giant-microlise-suffers-cyber-attack
132. https://theloadstar.com/cyber-attack-on-tech-provider-blacks-out-live-tracking-for-uk-retail-deliveries/
133. https://www.redhotcyber.com/en/post/intelbroker-claims-tesla-charging-database-breach/
134. https://www.cvedetails.com/cvss-score-distribution.php
135. https://nvd.nist.gov/vuln-metrics/cvss
136. https://www.thestack.technology/nvd-crisis-vulnerabilities-data-update/
137. https://therecord.media/nist-database-backlog-growing-vulncheck
138. https://www.nist.gov/itl/nvd
139. https://medium.com/@ravi8383soni/varta-shares-in-focus-looming-insolvency-and-cyber-attack-e1ae429e7bb3
140. https://www.varta-ag.com/en/about-varta/news-press/details/varta-makes-good-progress-in-solving-the-cyberattack
141. https://www.varta-ag.com/fileadmin/varta_ag/publications/ad-hoc_announcements/240315_VARTA_AG_Ad_hoc_Postponement_of_financial_reports_EN_final.pdf
142. https://www.nissan.com.au/website-update.html
143. https://www.bleepingcomputer.com/news/security/nissan-confirms-ransomware-attack-exposed-data-of-100-000-people/
144. https://www.eenewseurope.com/en/vulnerability-found-in-chargepoint-home-ev-chargers/
145. https://www.telegraph.co.uk/news/2024/02/21/car-charger-withdrawn-hackers-could-attack-national-grid/
146. https://www.researchgate.net/publication/377183224_Uncovering_Covert_Attacks_on_EV_Charging_Infrastructure_How_OCPP_Backend_Vulnerabilities_Could_Compromise_Your_System
147. https://www.greencarcongress.com/2024/07/20240717-swri.html
148. https://support-emobility.enelx.com/content/dam/enelxmobility/italia/documenti/manuali-schede-tecniche/Waybox-3-Security-Bulletin-06-2024-V1.pdf

REFERENCES

149. https://www.redhotcyber.com/en/post/intelbroker-claims-tesla-charging-database-breach/
150. https://www.ndss-symposium.org/wp-content/uploads/vehiclesec2024-47-paper.pdf
151. https://thecyberexpress.com/alleged-frotcom-data-breach/
152. https://www.securityweek.com/cyberattack-on-microlise-disables-tracking-in-prison-vans-courier-vehicles/
153. https://statescoop.com/kansas-city-traffic-system-still-down-after-cyberattack/
154. https://www.zigwheels.ph/car-news/mptc-encounters-data-breach
155. https://cybernews.com/news/dutch-government-will-replace-hackable-traffic-lights/
156. https://eaton-works.com/2024/01/17/ttibi-email-hack/
157. https://drivingpress.com/the-risks-of-autonomous-vehicles/
158. https://www.hackster.io/news/madradar-triggers-hallucinations-in-autonomous-vehicle-sensor-systems-researchers-say-b56b87763cbd
159. https://www.techexplorist.com/study-finds-security-flaws-first-next-gen-lidar-systems/81641/
160. https://www.theregister.com/2024/05/10/baidu_apollo_hack
161. https://dl.acm.org/doi/10.1145/3636534.3649372
162. https://eaton-works.com/2024/01/17/ttibi-email-hack/
163. https://hackread.com/ev-charging-firm-spills-trove-of-customer-info/
164. https://thecyberexpress.com/alleged-frotcom-data-breach/
165. https://cybernews.com/security/hertz-vulnerability-reveals-customers-data/
166. https://community.ui.com/releases/Security-Advisory-bulletin-039-039/44e24007-2c2c-4ac0-bebf-3f19b9b24f09
167. https://samcurry.net/hacking-kia
168. https://www.it-daily.net/en/shortnews-en/hacker-demands-125000-dollars-in-baguettes-from-schneider-electric
169. https://nvd.nist.gov/vuln/detail/CVE-2023-28895, https://nvd.nist.gov/vuln/detail/CVE-2023-28896, https://nvd.nist.gov/vuln/detail/CVE-2023-28897, https://nvd.nist.gov/vuln/detail/CVE-2023-28898, https://nvd.nist.gov/vuln/detail/CVE-2023-28899, https://nvd.nist.gov/vuln/detail/CVE-2023-28900, https://nvd.nist.gov/vuln/detail/CVE-2023-28901
170. https://nvd.nist.gov/vuln/detail/CVE-2024-39339
171. https://nvd.nist.gov/vuln/detail/CVE-2024-21462
172. https://nvd.nist.gov/vuln/detail/CVE-2024-6245
173. https://www.eenewseurope.com/en/vulnerability-found-in-chargepoint-home-ev-chargers/
174. https://www.telegraph.co.uk/news/2024/02/21/car-charger-withdrawn-hackers-could-attack-national-grid/
175. https://www.researchgate.net/publication/377183224_Uncovering_Covert_Attacks_on_EV_Charging_Infrastructure_How_OCPP_Backend_Vulnerabilities_Could_Compromise_Your_System
176. https://www.bright.nl/nieuws/1198728/phishing-met-valse-qr-codes-op-laadpalen-ontdekt-in-brussel.html
177. https://nvd.nist.gov/vuln/detail/CVE-2024-21550
178. https://www.redhotcyber.com/en/post/intelbroker-claims-tesla-charging-database-breach/
179. https://securityaffairs.com/160499/cyber-warfare-2/electronic-warfare-hit-defence-secretary-jet.html
180. https://ahmadmansourr.medium.com/hacking-more-than-130-000-car-worldwide-in-5-minutes-766e76003c67
181. https://cybersecuritynews.com/traccar-gps-system-vulnerability/
182. https://cybernews.com/security/gamooga-data-leak/
183. https://infosecwriteups.com/hacking-into-30-tesla-cars-around-the-world-using-a-third-party-software-00957ac68c92?gi=ce897b36be4a
184. https://darkwebinformer.com/888-allegedly-has-leaked-the-data-of-blink-ai-automotive/
185. https://jerinsunny.github.io/stm32_vglitch/
186. https://jerinsunny.github.io/blogs/2024/02/14/rh850-voltage-glitching.html
187. https://www.carscoops.com/2024/09/indiana-car-dealer-sued-for-rolling-back-odometers-14-million-miles/
188. https://www-theregister-com.cdn.ampproject.org/c/s/www.theregister.com/AMP/2024/03/22/boffins_tucktotruck_worm/
189. https://statescoop.com/kansas-city-traffic-system-still-down-after-cyberattack/
190. https://www.automotiveworld.com/articles/research-tackles-cosmic-ray-threat-to-avs-and-evs/
191. https://cybernews.com/security/gopass-colombia-data-leak/
192. https://www.zigwheels.ph/car-news/mptc-encounters-data-breach
193. https://cybernews.com/news/dutch-government-will-replace-hackable-traffic-lights/
194. https://nvd.nist.gov/vuln/detail/CVE-2024-33308, https://nvd.nist.gov/vuln/detail/CVE-2024-33309
195. https://www.autoindustriya.com/auto-industry-news/toyota-ph-reports-mytoyota-app-data-breach-some-customer-data-compromised.html
196. https://nvd.nist.gov/vuln/detail/CVE-2024-35537
197. https://www.hackster.io/news/madradar-triggers-hallucinations-in-autonomous-vehicle-sensor-systems-researchers-say-b56b87763cbd

REFERENCES

198. https://www.buffalo.edu/provost/messages.host.html/content/shared/university/news/news-center-releases/2024/08/self-driving-cars-attackers.detail.html
199. https://nvd.nist.gov/vuln/detail/CVE-2024-39081
200. https://www.autosar.org/fileadmin/standards/R20-11/FO/AUTOSAR_PRS_SecOcProtocol.pdf
201. https://icanhack.nl/blog/secoc-key-extraction/
202. https://www.gbnews.com/lifestyle/cars/toyota-lexus-drivers-compensation-keyless-car-theft
203. https://www.youtube.com/watch?v=qWmiyprxziw&ab_channel=AmynasecLabs
204. https://www.carscoops.com/2024/05/general-motors-faces-class-action-lawsuit-over-camaro-key-fob-security/
205. https://thecyberexpress.com/tesla-ultra-wideband-vulnerable-relay-attacks/
206. https://www.thestreet.com/electric-vehicles/forget-the-kia-boyz-a-new-exploit-leaves-kias-and-hyundais-vulnerable
207. https://kevin2600-cmd.github.io/2024/09/13/Grand-Theft-Auto-A-peek-of-BLE-relay-attack.html
208. https://eprint.iacr.org/2024/1816
209. https://nvd.nist.gov/vuln/detail/CVE-2023-0863, https://nvd.nist.gov/vuln/detail/CVE-2023-0864
210. https://cybernews.com/security/android-head-units-drivers-data-safety/#comments-reply
211. https://kevin2600-cmd.github.io/2024/09/13/Grand-Theft-Auto-A-peek-of-BLE-relay-attack.html
212. https://www.bleepingcomputer.com/news/security/mitm-phishing-attack-can-let-attackers-unlock-and-steal-a-tesla/amp/
213. https://www.infosecurity-magazine.com/news/cyber-attack-travel-chaos-seattle/
214. https://en.wikipedia.org/wiki/Cellular_V2X
215. https://gttwireless.com/dsrc-vs-c-v2x-comparing-the-connected-vehicles-technologies/
216. https://www.dwt.com/blogs/broadband-advisor/2023/05/fcc-connected-vehicles-c-v2x
217. https://www.its.dot.gov/research_areas/emerging_tech/pdf/Accelerate_V2X_Deployment_final.pdf
218. https://www.its.dot.gov/research_areas/emerging_tech/pdf/Accelerate_V2X_Deployment_final.pdf
219. https://www.its.dot.gov/research_areas/emerging_tech/pdf/Accelerate_V2X_Deployment_final.pdf
220. https://www.its.dot.gov/research_areas/emerging_tech/pdf/Accelerate_V2X_Deployment_final.pdf
221. https://www.cyberghostvpn.com/en_US/privacyhub/dark-web-vs-deep-web/
222. https://www.cyberghostvpn.com/en_US/privacyhub/dark-web-vs-deep-web/
223. https://forestvpn.com/blog/cybersecurity/how-much-of-the-internet-is-the-dark-web/
224. https://en.wikipedia.org/wiki/Darknet_market
225. Upstream Security
226. Upstream Security
227. Upstream Security
228. https://github.com/google/security-research/security/advisories/GHSA-c45w-xwww-rfgg
229. Upstream Security
230. Upstream Security
231. Upstream Security
232. Upstream Security
233. Upstream Security
234. Upstream Security
235. Upstream Security
236. Upstream Security
237. Upstream Security
238. Upstream Security
239. Upstream Security
240. Upstream Security
241. Upstream Security
242. https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/automotive-r-and-d-transformation-optimizing-gen-ais-potential-value
243. https://asia.nikkei.com/Business/Automobiles/Toyota-to-invest-13bn-in-EVs-AI-and-supply-chain
244. https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en
245. https://artificialintelligenceact.eu/article/15
246. https://www.twobirds.com/en/insights/2023/global/impact-of-the-eus-ai-act-proposal-on-automated-and-autonomous-vehicles
247. https://unece.org/sites/default/files/2021-03/R155e.pdf
248. https://unece.org/sites/default/files/2021-03/R156e.pdf

REFERENCES

249. https://www.iso.org/standard/70918.html
250. https://unece.org/sites/default/files/2024-05/ECE_TRANS_WP.29_2024_40e.pdf
251. https://unece.org/sites/default/files/2024-11/ECE-TRANS-WP.29-1179e.pdf
252. https://www.cyres-consulting.com/un-regulation-no-155-now-also-applies-to-motorcycles/
253. https://unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf
254. https://unece.org/fileadmin/DAM/trans/doc/2020/wp29/ECE-TRANS-WP29-2020-080e.pdf
255. https://clepa.eu/mediaroom/clepa-and-acea-join-with-auto-isac-on-motor-vehicle-cybersecurity/
256. https://www.itu.int/en/mediacentre/Pages/PR-2024-07-04-ITU-Radio-Regulations.aspx
257. https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-15
258. https://www.etsi.org/deliver/etsi_en/302500_302599/302571/02.01.01_60/en_302571v020101p.pdf
259. https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en
260. https://www.iso.org/standard/77845.html
261. https://standards.ieee.org/ieee/802.11p/3953/
262. https://www.sae.org/standards/content/j3105_202305/
263. https://www.sae.org/standards/content/j2945/1_202004/
264. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf
265. https://www.consilium.europa.eu/en/press/press-releases/2024/10/10/cyber-resilience-act-council-adopts-new-law-on-security-requirements-for-digital-products/
266. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
267. https://unece.org/sites/default/files/2023-05/GRVA-16-26e.pdf
268. https://www.iso.org/standard/69113.html
269. https://www.switch-ev.com/blog/what-is-iso-15118
270. https://www.switch-ev.com/blog/basics-of-plug-and-charge
271. https://www.energy.ca.gov/event/workshop/2024-05/iso-15118-implementation-updates-workshop
272. https://genorma.com/en/standards/iso-15118-20-2022-awi-amd-1
273. https://www.sec.gov/news/press-release/2023-139
274. https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214
275. https://www.sec.gov/education/smallbusiness/goingpublic/SRC
276. https://www.databreaches.net/alphv-files-an-sec-complaint-against-meridianlink-for-not-disclosing-a-breach-to-the-sec/
277. https://edition.cnn.com/2024/07/11/business/cdk-hack-ransom-tweny-five-million-dollars/index.html
278. https://cyberscoop.com/cdk-ransomware-attack-sec-disclosure-material-impact/
279. https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf
280. https://www.govinfo.gov/content/pkg/FR-2022-09-09/pdf/2022-19507.pdf
281. https://upstream.auto/research/automotive-cybersecurity/
282. https://automotiveisac.com/press-news/auto-isac-partners-with-upstream-security-to-enhance-automotive-threat-landscape-visibility
283. https://www.telematicswire.net/asrg-partners-with-upstream-to-enhance-automotive-cyber-threat-intelligence/
284. https://apnews.com/article/automatic-emergency-braking-requirement-stop-standards-366abf6958eaf4e48e7ca4737075071b
285. https://static.nhtsa.gov/odi/inv/2024/INOA-PE24016-12382.pdf
286. https://nypost.com/2024/10/18/business/nhtsa-to-investigate-elon-musks-tesla-after-several-full-self-driving-crashes/
287. https://attack.mitre.org
288. https://automotiveisac.com/press-news/the-auto-isac-launches-automotive-threat-matrix-atm-tool-to-enhance-vehicle-cybersecurity-governance
289. https://eur-lex.europa.eu/EN/legal-content/summary/the-european-data-act.html
290. https://artificialintelligenceact.eu/
291. https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/05/cars-consumer-data-unlawful-collection-use
292. https://www.wyden.senate.gov/news/press-releases/wyden-investigation-reveals-new-details-about-automakers-sharing-of-driver-information-with-data-brokers-wyden-and-markey-urge-ftc-to-crack-down-on-disclosures-of-americans-data-without-drivers-consent
293. https://www.lexology.com/library/detail.aspx?g=c6ed5413-e6d1-4883-b164-d343fa199a83
294. https://complyauto.com/2024/03/05/wiping-in-vehicle-data-nj-dealers-now-required-to-offer-to-delete-certain-information/
295. https://news.bloomberglaw.com/privacy-and-data-security/internet-connected-car-privacy-questions-prompt-states-to-act
296. https://www.lexisnexis.com/community/insights/legal/capitol-journal/b/state-net/posts/states-beginning-to-regulate-popular-usage-based-car-insurance

REFERENCES

297. https://trustcassie.com/resources/blog/californias-new-car-privacy-law-sb-286/
298. https://www.reuters.com/business/autos-transportation/california-enacts-car-data-privacy-law-curb-domestic-violence-2024-09-30/
299. https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf
300. https://single-market-economy.ec.europa.eu/document/download/cd243af9-c877-401e-9f69-d7d4ab6a90c6_en
301. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
302. https://upstream.auto/blog/nis2-directives-impact-on-the-smart-mobility-ecosystem/
303. https://www.consilium.europa.eu/en/press/press-releases/2024/10/10/cyber-resilience-act-council-adopts-new-law-on-security-requirements-for-digital-products/
304. https://alternative-fuels-observatory.ec.europa.eu/general-information/news/questions-and-answers-regulation-deployment-alternative-fuels
305. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401257
306. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1735
307. https://www.federalregister.gov/documents/2024/03/01/2024-04382/securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles
308. https://www.bis.gov/press-release/commerce-announces-proposed-rule-secure-connected-vehicle-supply-chains-foreign
309. https://www.reuters.com/business/autos-transportation/us-propose-barring-chinese-software-hardware-connected-vehicles-sources-say-2024-09-21/
310. https://www.regulations.gov/document/BIS-2024-0005-0059/comment
311. https://www.federalregister.gov/documents/2024/11/07/2024-24704/enhancing-surface-cyber-risk-management
312. https://www.nist.gov/cyberframework
313. https://www.cybersecuritydive.com/news/tsa-cyber-risk-management/732257/
314. https://english.www.gov.cn/news/202406/22/content_WS6676229dc6d0868f4e8e8708.html
315. https://digitalpolicyalert.org/event/21880-closed-consultation-on-miit-notice-on-further-strengthening-the-access-recall-and-online-upgrade-management-of-intelligent-connected-vehicles
316. https://wap.miit.gov.cn/jgsj/zbys/qcgy/art/2024/art_e1bb0d211dbf40a2949b28deb8a96d19.html
317. https://dissec.to/general/chinas-new-vehicle-cybersecurity-standard-gb-44495-2024/
318. https://www.codeofchina.com/standard/GB44496-2024.html
319. https://www.chinesestandard.net/Related.aspx/GB44497-2024
320. https://dissec.to/general/chinas-new-vehicle-cybersecurity-standard-gb-44495-2024/
321. https://www.eet-china.com/mp/a358838.html
322. https://morth.nic.in/sites/default/files/ASI/12_Draft_AIS_189_CSMS_DF.pdf
323. https://morth.nic.in/sites/default/files/ASI/13_Draft_AIS_190_SUMS_DF.pdf
324. https://bwsecurityworld.com/technology/cybersecurity-standards-for-connected-vehicles-to-be-mandatory-by-2027-in-india-report/
325. https://www.services.bis.gov.in/php/BIS_2.0/bisconnect/standard_review/Standard_review/Isdetails?ID=MzA2MDY%3D
326. https://www.services.bis.gov.in/php/BIS_2.0/bisconnect/standard_review/Standard_review/Isdetails?ID=MzA2MDU%3D
327. https://www.theweek.in/news/biz-tech/2024/06/23/what-are-is-18590-2024-is-18606-2024-bis-introduces-two-standards-ev-safety-quality.html
328. https://sso.agc.gov.sg/Acts-Supp/19-2024/Published/20240704?DocDate=20240704
329. https://www.herbertsmithfreehills.com/notes/cybersecurity/2024-06/singapore-expands-the-scope-of-the-cybersecurity-act-?
330. https://www.herbertsmithfreehills.com/notes/cybersecurity/2024-06/singapore-expands-the-scope-of-the-cybersecurity-act-?
331. https://www.strategyand.pwc.com/de/en/industries/automotive/electric-vehicle-sales-review-2024-q3.html
332. https://www.strategyand.pwc.com/de/en/industries/automotive/electric-vehicle-sales-review-2024-q3.html
333. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf
334. https://www.etsi.org/newsroom/press-releases/2457-etsi-releases-new-guidelines-to-enhance-cyber-security-for-consumer-iot-devices
335. https://eur-lex.europa.eu/eli/dir/2022/2555
336. https://data.consilium.europa.eu/doc/document/ST-12041-2023-INIT/en/pdf
337. https://www.consilium.europa.eu/media/69093/st16996-en23.pdf
338. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5342, https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks
339. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
340. https://www.europarl.europa.eu/news/en/press-room/20240308IPR18991/cyber-resilience-act-meps-adopt-plans-to-boost-security-of-digital-products
341. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet
342. https://www.charin.global/technology/plug-charge

REFERENCES

343. https://www.federalregister.gov/documents/2023/02/28/2023-03500/national-electric-vehicle-infrastructure-standards-and-requirements
344. https://www.foley.com/insights/publications/2023/04/us-dot-finalizes-ev-charging-infrastructure-rules/
345. https://www.nccoe.nist.gov/projects/cybersecurity-framework-profile-electric-vehicle-extreme-fast-charging-infrastructure
346. https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8473.ipd.pdf
347. https://www.theverge.com/2024/8/9/24216329/cybersecurity-clean-energy-biden-administration-priorities
348. https://www.gov.uk/government/consultations/electric-vehicle-smart-charging/public-feedback/electric-vehicle-smart-charging-consultation-summary-of-responses
349. https://www.legislation.gov.uk/uksi/2021/1467/made
350. https://www.legislation.gov.uk/uksi/2021/1467/made
351. https://assets.publishing.service.gov.uk/media/628ce214e90e071f653a494a/Guide-to-evscp-regulations-2021-V2.1.pdf
352. https://www.gov.uk/government/publications/the-public-charge-point-regulations-2023-guidance/public-charge-point-regulations-2023-guidance#background
353. https://www.legislation.gov.uk/uksi/2023/1168/contents/made
354. https://www.meti.go.jp/press/2020/11/20201105003/20201105003-1.pdf, https://www.dataguidance.com/news/japan-meti-releases-iot-security-and-safety-framework
355. https://www.dataguidance.com/news/japan-mic-announces-publication-iot-5g-security, https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00036.html
356. https://www.switch-ev.com/blog/what-is-iso-15118
357. https://en.wikipedia.org/wiki/Combined_Charging_System
358. https://www.switch-ev.com/blog/basics-of-plug-and-charge
359. https://www.charin.global/technology/iso15118/
360. https://www.cinch.co.uk/guides/electric-cars/what-is-chademo-ev-charging
361. https://www.chademo.com/design-guideline-for-external-charging-updated
362. https://www.openchargealliance.org/protocols/ocpp-201/
363. https://openchargealliance.org/my-oca/ocpp/
364. https://www.linkedin.com/pulse/how-does-ocpp-201-iso-11518-work-together-why-do-matter-beckmann/
365. https://www.gartner.com/en/documents/3904768
366. https://www.gartner.com/en/documents/3904768
367. https://unece.org/media/press/387828
368. https://owasp.org/API-Security/editions/2023/en/0x11-t10/
369. https://upstream.auto/platform/
370. https://upstream.auto/press-releases/upstream-unveils-ocean-ai/
371. https://upstream.auto/platform/cybersecurity/
372. https://upstream.auto/solutions/sector/electric-vehicle-charging/
373. https://upstream.auto/solutions/sector/sim-enabled-mobility-iot/
374. https://upstream.auto/platform/api-security/
375. https://upstream.auto/autothreat-intelligence/
376. https://upstream.auto/blog/deep-dark-web-intelligence-proactive-automotive-cybersecurity/
377. https://upstream.auto/solutions/vehicle-security-operations-center/
378. https://upstream.auto/solutions/cyber-readiness-services/

ABOUT UPSTREAM

Upstream delivers a cloud-based, AI-powered data management and cybersecurity platform purpose-built for connected vehicles, smart mobility, and IoT ecosystem. The Upstream Platform transforms fragmented, distributed mobility data into centralized, structured, and contextualized data lakes, unlocking its full potential. By leveraging this data, Upstream empowers customers with advanced, AI-driven applications across various use cases, including cybersecurity detection and response (XDR), fraud prevention, observability, proactive vehicle quality management, usage-based insurance, and more.

Upstream is privately funded by Alliance Ventures (Renault, Nissan, Mitsubishi), Volvo Group, BMW, Hyundai, MSI Insurance, Nationwide Insurance, Salesforce Ventures, Cisco Investments, CRV, Glilot Capital Partners, and Maniv Mobility.

For more information

Visit us at:
www.upstream.auto

Contact us:
hello@upstream.auto

Follow us