Upstream

FAST & CURIOUS:

THE AI AWAKENING

The Automotive and Smart Mobility ecosystem is once again at a pivotal moment. AI is redefining our ecosystem, transforming the cyber risk landscape, and fueling a new era of digital defense and innovation

2026 | **Automotive & Smart Mobility Global Cybersecurity Report**

Opening Letter from our CEO

I am pleased to present the 2026 Global Automotive and Smart Mobility Cybersecurity Report.

2025 marked a decisive escalation in automotive cybersecurity risk. Large, well-resourced attack groups increasingly targeted the Automotive and Smart Mobility ecosystem, driving a sharp rise in ransom-related attacks and challenging cybersecurity models. Several large-scale incidents demonstrated a new class of systemic attacks, where a single breach disrupted production, operations, and revenue across entire Automotive ecosystems.

Our research and engagements with OEMs, Tier-1 suppliers, and mobility providers confirm the scale of this shift. In 2025, ransomware accounted for 44% of publicly reported incidents and more than doubled in volume compared to 2024. Incidents involving manipulation and control of vehicle and backend systems further reinforced cybersecurity as a critical safety and operational risk.

In parallel, the industry entered a new phase of technological exposure. Machine Learning, Generative AI, and AI Agents are reshaping mobility and cybersecurity alike. The convergence of software-defined vehicles, AI capabilities and more specifically large language models, and an expanding digital supply chain has fundamentally altered the attack surface. The vehicle is no longer a standalone computing platform. It now operates as the edge of a distributed intelligence system, tightly coupled with cloud platforms, APIs, autonomous backend services, and more. These architectures introduce fluid, context-dependent attack paths that challenge legacy, siloed defenses.

As attack surfaces extend, security operations must evolve. A vulnerability in the IT or cloud network could lead to an attack on the connected vehicle ecosystem, including compromise of OTA campaigns across the fleet. The industry is transitioning toward Product SOC / vSOC models, delivering an automotive-specific XDR strategy that spans vehicles, cloud and backend infrastructure, and API-driven applications and services. This model enables cybersecurity teams to detect and respond to threats that traverse multiple product layers.

Addressing these challenges requires moving beyond regulatory checklists. OEMs and mobility providers must invest in securing all attack vectors, including API security, cloud security, and vehicle security, as well as correlate them with threat intelligence and proactive threat hunting.

At Upstream, we have focused exclusively on securing the connected mobility ecosystem since 2017. As we enter 2026, we remain committed to partnering with the industry to stay ahead of emerging threats and secure the future of connected and intelligent mobility.

Sincerely,

Yoav Levy

Co-Founder & CEO

Methodology

In 2025 alone, Upstream's AutoThreat® researchers analyzed 494 new incidents, contributing to a continuously growing database of publicly documented cases dating back to 2010. In addition, our team monitors hundreds of deep and dark web forums and thousands of active threat actors.

Based on this extensive research, 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 automation 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, stakeholder type, and the required proximity of the attacker to the target. This creates an in-depth and practical repository to help organizations strengthen their cybersecurity 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 cyber attacks.

In 2025, our research scope expanded significantly to address the rising risks of AI-driven exploitation and organized cybercrime. This expanded effort included thousands of cyber threat intelligence findings and tracking of nearly 2,000 of the most active threat actors, whose activities are analyzed in a dedicated chapter titled “Threats from the deep and dark web". Notably, these findings 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.

Table of Contents

Table of Contents

Table of Contents

EXECUTIVE SUMMARY

In 2025, the Automotive and Smart Mobility ecosystem experienced a material escalation in cyber risks, driven by the growing scale and sophistication of organized threat actors and the rapid expansion of AI-related attack surfaces. The data reflects the continuously widening gap between adversary capability and the industry's current cybersecurity posture.

Escalation of organized threat actors and ransom-driven attacks

In 2025, the Automotive and Smart Mobility ecosystem experienced a sharp escalation in large-scale, well-resourced, and coordinated cyber activity, reflected not only in incident volume and scale, but also in billions of dollars in cumulative operational disruption, recovery costs, and financial losses.

Black hat actors accounted for

71%

of all incidents (up from 65% in 2024), reinforcing the shift toward coordinated and financially motivated attacks.

Ransomware attacks accounted for

44%

of all incidents, reflecting the continued industrialization of cybercrime.

Data breaches rose to

68%

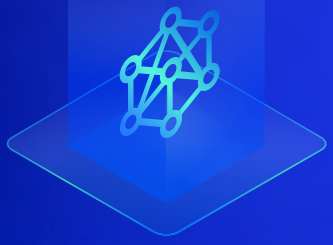
of incidents.

61% of incidents had the potential to impact thousands to millions of mobility assets;

20% of which classified as massive-scale events.

AI-driven architectures and APIs are emerging as critical attack surfaces

Alongside the rise in organized cybercrime, the rapid adoption of AI, including Generative AI and large language models (LLMs), as well as API-centric architectures have fundamentally expanded the automotive attack surface. Cybersecurity risks are increasingly shaped by dynamic, context-aware systems that span vehicles, cloud platforms, and digital services.



LLMs are being integrated across development, operations, and customer-facing mobility services, introducing new vulnerabilities.

The Model Context Protocol (MCP) creates fluid and difficult-to-predict attack paths.

Backend servers and APIs remained the dominant exposure point, forming the operational backbone of software-defined mobility platforms.

API proliferation continues to blur traditional trust boundaries between vehicles, cloud services, and third-party ecosystems, increasing systemic risk.

Upstream

01.

UNCOVERING ENGINES OF AI

Machine Learning, Generative AI, and AI Agents are reshaping mobility and cybersecurity alike, demanding a product-focused defense model that spans the cloud, APIs, and vehicles themselves.

AI defines the next phase of the SDV journey

For more than a decade, the Automotive industry has been undergoing its most significant transformation since the invention of the assembly line. Yet the path toward fully software-defined vehicles (SDVs) has proven far more complex than early roadmaps suggested. Several OEMs have scaled back, or delayed, their bold SDV ambitions after confronting the realities of building and maintaining big-tech-grade software stacks.

The next phase of the transformation is therefore becoming a hybrid one: extracting more value from legacy architectures, selectively outsourcing foundational layers to partners, and layering new capabilities, especially AI, into platforms that were never designed for them. Reflecting this shift, during IAA Mobility 2025, a global OEM CEO emphasized that the OEM's updated software direction is now delivering "excellent cost positioning," a result achieved not through a purely in-house SDV push, but through a more pragmatic combined Group Software Stack, mixing legacy platforms with partner-developed architectures.[1]

In this transitional model, application programming interfaces (APIs) serve as the central nervous system for communication across vehicle, cloud, and third-party ecosystems. As microservices, external integrations, and features powered by Large Language Models (LLMs) proliferate across both cloud and edge environments, the industry's digital footprint, and its attack surface, expand accordingly.

> **And with cybersecurity often down-prioritized in favor of delivering new services quickly, the consequences reflect an industry navigating an increasingly delicate tradeoff between convenience and control.**

While APIs provide structured communication channels, the emergence of the Model Context Protocol (MCP) introduces a more dynamic paradigm built for the AI era. **MCP enables LLMs to orchestrate tools and vehicle functions in real time, creating a broader and far less predictable attack surface.** Traditional APIs can be cataloged and monitored; MCP-driven interactions are fluid, context-dependent, and significantly harder to secure.

The practical applications of AI are already changing key aspects of the automotive experience, including:

- **Voice copilots:** Advanced, conversational AI assistants are replacing clunky, command-based voice systems.
- **Early and predictive after-sales quality detection**: AI models are used to proactively detect component failures even before the first repair orders or warranty claims come in.
- **Personalization:** Generative AI (GenAI) allows for deep personalization of the in-vehicle environment, from cabin settings to media suggestions.
- **Autonomous decision support:** AI is crucial for understanding complex sensor data and making critical real-time driving decisions in Advanced Driver Assistance Systems (ADAS) and autonomous vehicles.
- **Internal enablement and productivity:** OEMs are increasingly deploying secure, domain-tuned LLMs across their internal organizations, supporting engineering workflows, accelerating software development, improving customer support operations, and enabling faster decision-making through natural-language access to complex technical documentation and vehicle data.

In September 2025 at the IAA Mobility 2025 conference in Munich, Volkswagen Group announced it will invest up to €1 billion by 2030 into AI across vehicle development, industrial operations, and IT infrastructure. The underlying incentive for the investment is expected savings of €4 billion by 2035 through efficiency gains across its entire operation.[2]

Volkswagen Group announced it will invest in AI up to

€1 Billion by 2030

expecting savings of

€4 Billion by 2035

The key message by VW is simple: "no process without AI", aiming to embed AI throughout the value chain, from engineering and manufacturing to software-defined vehicles.

This reflects a broad, industrial-scale commitment to AI, signaling that AI is no longer a niche feature but a core strategic and competitive element for OEMs.

In May 2025, Volvo announced an expanded partnership with Google to bring Google's conversational AI platform, Gemini, into Volvo cars that run Android Automotive OS.[3] **The focus in this announcement is on natural-language conversational assistants, translating, querying vehicle manuals, navigation help, and making the in-car experience more AI-centric.** It illustrates OEMs shifting toward AI-driven user experience and software-defined vehicles.

In April 2025, Nissan announced a partnership with UK-based AI company Wayve to integrate Wayve's self-learning AI software into Nissan's "ProPILOT" advanced driver-assist system (ADAS) beginning in 2027.[4] This announcement demonstrates that OEMs are committing to AI not only for user experience or manufacturing, but for critical mobility features (ADAS / autonomy) and long-term product roadmaps.

Based on an October 2025 report by IBM, OEM executives expect AI-related revenue share to grow from about 5% (as of late 2025) to about 9% in three years:

> **"Global industry executives are expecting an extensive transformation from the in-car experience to the core of the vehicle controls and functions. Of the executives surveyed by the IBM Institute for Business Value, 74% believe that in 2035 vehicles are software-defined and AI-powered."[5]**

Automotive AI-related revenue will grow from 5% in 2025 to 9% in 2028

According to the IBM report, AI is transforming OEMs from hardware manufacturers into software-defined, data-driven mobility platforms. Instead of adding isolated ML or sensor features, **automakers must adopt a platform mindset, building vehicles that continuously learn, update, and deliver new digital services.** This shift requires a hybrid edge-and-cloud strategy, balancing in-vehicle intelligence with cloud-based analytics and over-the-air update architectures to ensure reliability and low latency. The financial upside is also significant: AI already drives measurable gains in product and service value, underscoring its role as a core business driver rather than a peripheral technology.

As OEMs pivot toward recurring revenue models such as subscriptions, connected diagnostics, and personalized mobility experiences, data and AI engineers become central to shaping future business value. Yet this evolution demands a deep cultural and skill transformation, bridging traditional mechanical expertise with modern software, data, and ML lifecycle disciplines. GenAI accelerates this change, offering new tools for design, simulation, and code development. Still, OEMs must embed trust, safety, and transparency into every AI system to meet automotive-grade standards.

On top of the many advantages and challenges of AI-powered innovation and its transformative impact on the Automotive and Smart Mobility ecosystem, the introduction of complex ML models and LLMs into vehicle architectures adds a new and critical layer of risk.

An August 2025 study on LLM-driven autonomous planning highlighted how complex decision models can be coerced into generating unsafe or adversarial action sequences when exposed to manipulated inputs.[6] These findings carry direct implications for the Automotive ecosystem as OEMs integrate LLM-based copilots, assistants, and planning modules into connected vehicles and SDV architectures. Systems that rely on model reasoning for interpreting intent, prioritizing actions, or mediating between cloud and edge signals could be influenced into unsafe behavior through crafted prompts, injected context, or corrupted data streams. In MCP environments that blend perception, prediction, and high-level planning, such manipulation can degrade decision quality, introduce non-deterministic responses, and amplify systemic risk. **Since regulatory frameworks have not yet adapted to these AI-specific failure modes across APIs, data pipelines, and supplier interfaces, OEMs must strengthen validation, monitoring, and defensive controls to keep LLM-enabled vehicle functions safe under cyber stress conditions.**

Further complicating the picture, in September 2025 researchers discovered a critical remote code execution flaw (CVE-2025-6514) in the MCP's open-source implementation.[7] The vulnerability allowed unauthenticated attackers to send a specially crafted tool definition to an MCP-enabled LLM, triggering a deserialization exploit that enabled arbitrary code execution.[8]

Although MCP and its reference client (mcp-remote) are not used inside software-defined vehicles, ADAS stacks, infotainment systems, or in-vehicle ECUs as of late 2025, and although exploitation requires a vulnerable client to actively connect to a malicious MCP server, the incident is still instructive. It highlights how AI-oriented orchestration layers can introduce execution-level attack paths that sit outside traditional API and service-boundary protections.

If similarly dynamic AI orchestration systems were adopted in vehicle or edge-AI supply chains, an exploit originating in an AI tooling layer could propagate into downstream logic, data flows, or control environments. The MCP case therefore serves as a forward-looking example of the type of high-impact attack surface that can emerge when AI agents are allowed to invoke tools, understand context, and mediate system actions in real time.

As OEMs embed LLMs directly into vehicles, the vehicle is evolving from a passive machine that receives commands into an intelligent copilot that understands intent and shapes system behavior. While the LLM cannot act autonomously without an orchestration layer, this added reasoning ability still introduces a vector for manipulation, turning the AI-enabled vehicle into a prime attack surface.

New AI architectures are creating systemic, ecosystem-level risks

AI-driven architectures introduce new categories of cybersecurity risks, not because OEMs or suppliers are making arbitrary or negligent choices, but because they are operating within complex business, technical, and regulatory constraints. **Every decision to integrate an LLM, expose a new API, or accelerate data-driven features is a calculated trade-off between innovation, compliance, cost, time-to-market, and customer expectations.** These strategic choices inevitably expand the attack surface, creating new system-level exposures across cloud, edge, and in-vehicle environments. In this context, the challenge is not avoiding risk altogether, but managing it with clear governance, architectural safeguards, and continuous cybersecurity oversight as AI becomes embedded in the Automotive ecosystem.

A stark illustration of this emerged in mid-2025, when attackers exploited a vulnerability in an AI-driven module of a widely used enterprise CRM platform.[9] **The breach rippled far beyond IT boundaries, compromising a global automotive OEM and demonstrating how AI-powered third-party services can open indirect pathways into the Automotive ecosystem itself.**

For OEMs, AI adoption and the shift toward software-defined vehicles are not end goals but long-term strategic journeys, requiring sustained investment, cultural transformation, and cross-domain coordination to manage these evolving risks effectively. These risks manifest in several key ways:

API-driven microservices are the new foundational attack surface

At the core of the SDV is an architectural shift from isolated, function-specific ECUs to a connected, API-driven, and distributed microservices model. This shift accelerates innovation through OEM developer portals, open-source and third-party libraries, but it also creates a complex, layered risk. The proliferation of endpoints and the distributed architecture multiplies assets that must be secured; third-party dependencies add supply-chain risk from uneven cybersecurity practices; and the complex composition of cloud, edge, and vehicle networks creates trust boundaries that are easily misconfigured. **This distributed logic significantly increases the likelihood of critical vulnerabilities like Broken Object Level Authorization (BOLA), unsafe deserialization, or privilege escalation paths.**

The rise of in-vehicle LLMs creates a new target for manipulation

As OEMs rapidly integrate GenAI directly into the cockpit, shifting from cloud-based novelties to embedded vehicle capabilities, LLM-powered copilots are redefining the in-vehicle experience. More critically, they shift the vehicle from a passive receiver of commands to a system whose behavior can be shaped by an LLM's reasoning through an orchestration layer. Once an AI agent or tool-execution framework is present, the vehicle gains a form of operational agency, and any system that can act on AI-derived instructions becomes a potential target for manipulation.

For example, LLMs and autonomous agents integrated into vehicle systems (for infotainment, diagnostics, or user interaction) can be manipulated through prompt injection or malicious input data.[10]

This could enable attackers to override safety or privacy constraints, generate unsafe driving commands, or exfiltrate sensitive vehicle data. Furthermore, AI systems that continuously learn from fleet or sensor data can be targeted with data poisoning attacks, introducing corrupted or adversarial data to distort future decisions. Over-the-air updates or federated learning processes amplify this risk.

A July 2025 study demonstrated how an adversary can launch a novel black-box denial-of-service (DoS) attack against LLMs.[11]

The method, called AutoDoS, builds a "DoS Attack Tree" to generate prompts that force the target model to produce extremely long outputs, thereby exhausting GPU or memory resources and dramatically increasing latency (by over x250).

Crucially, because AutoDoS works in a black-box setting, without needing model weights or training access, it poses a realistic threat for in-vehicle LLM deployments, where in-car assistants or vehicle-cloud platforms may integrate LLMs and cannot easily monitor or defend all resource-exhaustion scenarios. The implication on automotive systems using LLMs is the ability for an attacker to trigger heavy resource consumption, degrade responsiveness or disable critical services (e.g., diagnostics, voice assistants, real-time decision support), thereby undermining safety, availability, and user experience.

MCPs are significantly harder to secure

While APIs provide a structured means of communication, the rise of the MCP introduces a new, more dynamic paradigm built for the AI era.[12] MCP allows LLMs to dynamically orchestrate a wide array of tools and vehicle functions in real time. However, this power also creates a broader and less predictable attack surface. Where traditional APIs can be cataloged and monitored, MCP-driven interactions are more fluid and context-dependent.

The severe risks associated with this new protocol were highlighted in September 2025, with the discovery of a critical remote CVE (CVE-2025-6514) in the MCP's open-source implementation. **Security researchers found that an unauthenticated attacker could send a specially crafted tool definition to an MCP-enabled LLM, triggering a deserialization flaw that allowed for arbitrary code execution.**[13] If such an implementation were integrated into vehicle-control pathways, an attacker could gain control over critical functions and access sensitive data, proving that the dynamic nature of MCP creates opportunities for high-impact exploits that bypass traditional API security models.

This dynamic orchestration layer also underpins hybrid cloud-edge architectures that connect AI capabilities between the vehicle and backend systems.

Hybrid architectures introduce persistent cloud-to-car risks

To deliver these advanced AI capabilities, automakers are adopting hybrid models that combine cloud resources with on-vehicle edge computing, which supports real-time responsiveness for critical functions. While this improves performance, it also creates a persistent, high-bandwidth link between the vehicle and the cloud. **This constant data stream provides attackers with a rich new target for man-in-the-middle attacks and data interception, introducing the risk that a single cloud-side compromise could impact an entire fleet.**[14] This mirrors the focus of many real-world API attacks, where researchers have targeted the cloud backend to control vehicles.

API and MCP-specific risks

Before considering the vulnerabilities of the AI models they connect, it's critical to address the risks inherent to the APIs and MCP protocols that enable this connectivity.

- **Reverse engineering of endpoints**
  Attackers can systematically probe and analyze API endpoints to understand their logic and discover vulnerabilities. By reverse-engineering how a mobile app or third-party service communicates with a vehicle, they can craft malicious requests to bypass authentication and gain unauthorized control.

- **Prompt injection and adversarial inputs**
  OWASP[15] ranks prompt injection as the top LLM cybersecurity risk, and within MCP ecosystems, these vulnerabilities can trigger automated actions beyond text generation.[16] Indeed, with the introduction of LLMs and MCP, the nature of inputs is no longer limited to structured commands. Attackers can use prompt injection, crafting malicious text or voice inputs designed to trick the AI into executing unintended actions or revealing sensitive data.

- **API credential abuse and phishing**
  The credentials used to secure API communication, such as API keys and OAuth tokens, are becoming high-value targets. If stolen through phishing attacks or data breaches, these credentials can grant an attacker the same level of access as a legitimate user or service.

- **Supply chain exposure**
  The modern vehicle relies on a complex web of interconnected third-party services. A security failure in any single partner can create a cascading effect, allowing attackers to compromise the vehicle indirectly.

AI-specific vulnerabilities

Together, APIs and MCPs define the communication fabric of modern connected vehicles, but the models they connect to introduce a second, deeper layer of risk. Even if interfaces are properly secured, the AI systems operating behind them can be exploited. These AI-specific vulnerabilities represent a new frontier that extends beyond the protocol surface.

- **Data leakage**
  AI models, particularly LLMs, can be tricked through carefully crafted queries into revealing sensitive information they were trained on or have access to, including personal user data or proprietary OEM information. For example, if vehicle-resident or connected LLM agents (like copilots or OTA assistants) are trained or updated with driver data, improper isolation or memory handling could result in PII or telematics data being exposed or replayed via API or MCP tool access.[17]

- **Model manipulation and poisoning**
  Threat actors can attempt to "poison" the data used to train AI models, subtly altering their behavior to create backdoors. The research on using LLMs to analyze infotainment operating systems highlights how these models can also be prompted to identify specific bugs, allowing a harmless application to escalate its privileges and access sensitive data. For example, a compromised sensor feed, OTA data stream, or malicious MCP server could inject adversarial cues (e.g., false road signs, spoofed weather context) that lead an LLM-based planner to make unsafe decisions, a direct cyber-physical hazard.[18]

- **Malicious context injection**
  Through MCP, an attacker could inject false or malicious context from a compromised external service, tricking an AI into making unsafe driving recommendations. In a vehicle context, this introduces a systemic cyber-safety vulnerability. An attacker exploiting these gaps (e.g., by injecting physically inconsistent simulation data via MCP) could mislead the model's logic about the real-world state, resulting in unsafe actions.[19]

GenAI adoption is driving cascading supply chain and business risk

While GenAI applications promise a revolutionary user experience, their reliance on a complex web of third-party AI components and platforms introduces significant supply chain risk. **A vulnerability in a single external service can have cascading effects across an entire fleet, and these threats manifest in both the cloud services supporting the vehicle and the in-vehicle systems themselves.**

These dependencies mean that innovation and exposure now scale together, the same connectivity that enables new AI-driven experiences also expands the potential attack surface.

The interconnected attack surface and the new cybersecurity frontier

The modern vehicle's cybersecurity posture is no longer defined by its physical hardware but by its sprawling digital supply chain, creating multiple, often indirect, attack vectors.

Cloud-based supply chain risk

A stark example of this emerged in late 2025, when a massive cyber attack targeted an AI-driven component within a popular CRM platform. The attackers exploited a vulnerability in the service, leading to a significant data breach that impacted numerous companies relying on the platform. **A global automotive giant was among the major corporations affected, highlighting how the interconnectedness of modern enterprise and vehicle systems creates new, indirect attack vectors.**[20]

In-vehicle platform risk

The threat also exists directly within the cockpit. In January 2025, security researchers detailed multiple security flaws in an infotainment platform, which powers a German OEM's advanced voice and AI features. By chaining several vulnerabilities, the researchers could gain remote access to the head unit, allowing them to control sensitive functions and access user data. They also showed that an attacker with physical access could exploit additional weaknesses through USB or custom UPC connections to disable anti-theft protections, unlock paid services, or perform unauthorized vehicle tuning. While the OEM patched the issues and stated that exploitation would have required specific prerequisite steps, the case highlights a critical point: **the complex, feature-rich infotainment systems that host in-vehicle AI are themselves a significant and target-rich attack surface.**[21]

These transformations have profound implications:

The growing reliance on external services and third-party AI platforms is dissolving the traditional vehicle perimeter, extending the attack surface across a distributed ecosystem of cloud servers, mobile apps, and interconnected APIs.

As threat actors target this sprawling infrastructure, security must evolve from protecting individual components to ensuring holistic visibility and protection across the entire product ecosystem.

GenAI acts as a double-edged sword for cybersecurity, lowering the bar for threat actors

The cybersecurity gap identified in Upstream's 2025 Global Automotive Cybersecurity Report is intensified by AI's dual-use nature: the same AI technologies that enable in-vehicle copilots also introduce architectural exposures and give adversaries faster, smarter tools to exploit them. Within modern connected vehicle and SDV ecosystems, LLMs and API-driven integrations form a dense web of connectivity across cloud, edge, and vehicle layers. **Each new AI-enabled service or interface expands the attack surface, increasing the risk of misconfiguration, privilege escalation, and data exposure. At the same time, GenAI compresses the timeline from discovery to exploitation by automating and scaling offensive workflows.**[23]

In November 2025, a leading AI developer published the first report of its kind, detailing how a Chinese-state-linked threat actor orchestrated an intrusion campaign in September 2025, marking a turning point in adversary tradecraft.[24] Rather than using an AI model for guidance, the attacker used it as the operational engine itself: an AI coding assistant autonomously performed reconnaissance, vulnerability discovery, exploitation, lateral movement, credential harvesting, data exfiltration, and even documentation with minimal human oversight.

The report estimates that 80%–90% of the campaign's tactical actions were executed by the AI, with humans providing only high-level direction. The implications are profound: the barriers to conducting sophisticated cyber-espionage have dropped dramatically, enabling actors without advanced tooling or exploit-development capabilities to combine commodity software, automation frameworks, and frontier AI models to run large-scale operations at speed.

A recent report highlights an AI-powered attack in which 80% to 90% of the campaign was executed by AI

Indeed, GenAI acts as a force multiplier for exploitation in five key areas:

- **Accelerating reverse engineering**
  A recent study demonstrates that LLMs can dramatically accelerate the reverse-engineering of complex systems such as infotainment operating systems. Attackers are now using AI-powered software reverse-engineering plugins to have an LLM explain complex, decompiled functions in seconds, turning what was once weeks of manual analysis into a streamlined process.[25]

- **Automating authentication and authorization analysis**
  AI models can logically dissect authentication flows to spot critical vulnerabilities that a human might miss. Research shows that an AI reviewing the API requests of an application would immediately flag the absence of an authentication token and identify the BOLA flaw, where the API only required a VIN to control the vehicle.[26]

- **Generating attack payloads and fuzzing scripts**
  AI is being used to actively create offensive tools. An attacker can now prompt an LLM to "write a Python script to iterate a VIN's last 5 digits and send a GET request" to a specific endpoint, automating the process of finding vulnerable vehicles.[27] This ability lowers the barrier to entry, allowing less sophisticated actors to weaponize known vulnerability patterns and launch attacks at scale.

- **AI-generated security bypasses**
  Attackers can use AI to actively subvert platform security controls. For example, an attacker could prompt an LLM to generate a Frida hooking script designed to override the return value of a critical security function in an infotainment operating system. This would effectively disable signature and permission checks at runtime, allowing a malicious, unprivileged application to perform sensitive actions. Moreover, attackers leveraging LLM-based workflows can exploit side-channel characteristics of streaming LLM interfaces, for example, by observing packet sizes and timing information, to infer protected topics or modes of operation even when data is encrypted.[28] In the context of embedded infotainment or automotive control systems, this means an adversary could not only generate a payload (e.g., Frida hook) but also covertly monitor the LLM-driven responses or internal telemetry, correlating user prompts with system reactions to refine and stealthily adapt their attack strategy.

- **AI-assisted exploit development**
  Once a vulnerability is identified, attackers are using AI to assist in writing the exploit code. For example, after finding a command injection flaw in an API, an attacker can prompt an LLM to "generate a proof-of-concept in Python that exploits this vulnerability to execute a shell command." The AI can produce functional exploit code, significantly lowering the skill and time required to weaponize a discovered flaw.

The attacker's playbook has fundamentally changed

The convergence of connected vehicles, SDV architectures, and AI has reshaped the threat landscape, creating multi-layered risks that extend far beyond the vehicle itself. More critically, it has transformed the pace of cyber operations, accelerating how quickly vulnerabilities are discovered, weaponized, and exploited.

AI not only exposes new weaknesses but also empowers attackers to automate and adapt existing exploits.

An attacker can now feed a summary of a known CVE into an LLM and ask it to generate a proof-of-concept or suggest how to adapt the exploit for a different manufacturer's system. This ability to generalize and adapt known attacks dramatically compresses the window between vulnerability disclosure and widespread exploitation.

This trend is not theoretical. In a recent threat intelligence report, a popular AI developer confirmed that malicious actors are consistently weaponizing frontier AI models.[29] Their threat intelligence team found that **AI is being used to lower the barrier to entry for sophisticated cybercrime, enabling actors with few technical skills to develop complex tools such as ransomware.** Crucially, the AI company notes that these patterns of abuse are not unique to their platform but are likely consistent across all advanced AI models, showing how threat actors are adapting their operations to exploit today's most advanced AI capabilities.

In a 2025 study, researchers proved this by using an AI model to create a complex automotive diagnostic protocol fuzzer, a task that previously required deep domain expertise.[30]

This represents a fundamental shift, as attackers can now use AI to generate novel and varied inputs, from CAN bus messages to binder transactions, to discover critical vulnerabilities in deep vehicle systems.

This evolution is defined by a fundamental expansion of the attack surface, which in turn creates new categories of risk and drives a strategic shift in attacker focus, one where the “new toolkit" is no longer specialized hardware but curiosity, creativity, and code, all now readily amplified by GenAI.

The cloud backend is the new center of gravity for automotive cybersecurity, while APIs are the nervous system

The primary focus of sophisticated attackers has officially shifted from vehicle firmware to the sprawling cloud and API ecosystems. The connected vehicle is rapidly transforming into a vast network of interconnected software components, and in this new reality, every API endpoint serves as a potential entry point. This attack surface is not static; it expands with every new feature and third-party integration, dissolving the clear boundary between the vehicle and the outside world. Crucially, API weaknesses are not limited to accidental misconfigurations, they represent a well-understood, inherent risk by design. As such, they must be treated as a first-order architectural concern, engineered and governed with the same rigor as any safety-critical system.

Attackers follow the path of least resistance and greatest impact. Gaining control of a single vehicle through a physical attack is resource-intensive and offers limited scale. In contrast, compromising a central cloud server or discovering a widespread API vulnerability provides the ability to attack thousands or even millions of vehicles simultaneously. This strategic pivot is evidenced by numerous real-world incidents.

As attackers weaponize GenAI to automate discovery and scale exploitation, defenders face a single imperative: make security operations AI-driven to enable holistic, AI-powered visibility and XDR-driven response across the product ecosystem.

Cybersecurity must evolve to a holistic AI-powered product-driven approach

The convergence of SDVs, Gen AI (and specifically LLMs), and a sprawling digital supply chain has fundamentally altered the automotive threat landscape. This is a tectonic shift, as the vehicle is no longer a mobile computing platform on wheels, it's the edge of a distributed intelligence system on wheels. Traditional, siloed security models are proving inadequate, a fact made devastatingly clear by a recent attack that marks the arrival of the "Billion-Dollar Automotive Cyber Club," a new tier of attacks where the damage paralyzes entire ecosystems.[31] It reinforces the need to shift from a reactive to a proactive cybersecurity thinking and it must be designed into the AI's reasoning, the vehicle's behavior, including the ecosystem it is intended to be operated.

In September 2025, a major European OEM fell victim to a massive cyber attack that crippled its IT and operational systems. The incident was not an attack on a single vehicle but a sophisticated operation targeting off-board infrastructure. By compromising the company's enterprise and cloud perimeter, the attackers halted factory operations and disrupted suppliers, inflicting losses estimated at £50 million per week. The damage was so severe that the government intervened with a £1.5 billion loan guarantee to stabilize the ecosystem.[32] Recent reports estimate the attack caused losses of approximately £1.9 billion. Beyond crippling OEM operations, the breach disrupted as many as 5,000 organizations across the UK, highlighting the far-reaching impact of the carmaker's complex supply chain.[33] In its quarterly monetary policy report released in November 2025, the Bank of England noted that headline GDP grew by just 0.2%, below projections, citing reduced exports to the US and disruption linked to the cyberattack.[34]

In October 2025, researchers disclosed a critical vulnerability that exposed systemic weaknesses in connected vehicle ecosystems. By exploiting a zero-day flaw in a contractor's web application, researchers were able to escalate access from a supplier's system to the automaker's telematics infrastructure (TCU), ultimately gaining control of vehicle functions such as gear shifting and engine shutdown.[35] The research revealed how weak passwords, exposed web services, and insufficient authentication in third-party environments can cascade into full compromise of connected fleets. Beyond highlighting direct safety risks to drivers, the findings underscore an industry-wide challenge: as vehicles become nodes in complex digital supply chains, a single vulnerable contractor can jeopardize the integrity of an entire connected ecosystem.

These attacks also underscored a tectonic shift: the traditional vehicle security operations center (vSOC), focused on in-vehicle threats, is blind to the sophisticated, chained attacks that move laterally across the entire product ecosystem, from cloud APIs to enterprise IT. The breach demonstrated that without a holistic XDR (Extended Detection and Response) approach, OEMs lack the visibility to detect and respond to threats that originate far from the vehicle but have a catastrophic impact on the entire business. To counter these shifts, OEMs must adopt a holistic Product SOC (pSOC) that extends resilience across the full vehicle lifecycle and ecosystem. The pSOC should also leverage GenAI to automate alert triage, accelerate investigations, and continuously adapt detection models to emerging attack patterns.

Furthermore, the next generation of technologies must think like attackers, reason like autonomous agents, and adapt like AI.

The journey to a Product SOC

As the attack surface shifts from vehicle hardware to the interconnected ecosystem, security operations must evolve. The industry is now transitioning from the vehicle-centric SOC to a more comprehensive Product SOC (pSOC) model.

A pSOC embodies a XDR strategy for automotive, designed to holistically monitor all attack surfaces by embedding monitoring and detection across all product layers, including “edge” / vehicle threats, cloud and backend systems, as well as API-based connected applications and services.

Its mandate is to secure the entire data flow, from a command on a smartphone to its execution in the vehicle, by integrating broad API monitoring, deep Cyber Threat Intelligence (CTI), enhanced Threat Analysis and Risk Assessments (TARA), and real-time anomaly detection capable of identifying emerging risks such as MCP manipulation.

This is the only way to meet the continuous monitoring requirements of regulations such as UNECE WP.29 R155.[36]

AI is the critical enabler for the modern Product SOC

Just as threat actors use AI to find exploits, a modern pSOC must use defensive AI to fight back. Only by using AI to correlate faint signals across the entire ecosystem can security teams detect complex, chained attacks like the one that hit the major European OEM.
AI transforms the core functions of the Product SOC in four key ways:

ML-driven monitoring creates an adaptive defense
Unlike static, rule-based systems, ML-driven monitoring can identify subtle, low-and-slow anomalies as well as API and MCP abuse that signal a precursor to a larger attack. These models continuously refine their own detection algorithms based on new data, creating an adaptive defense that hardens over time.

GenAI dramatically reduces false-positives
GenAI models excel at learning contextual baselines of normal behavior across vehicle telemetry, MCP and APIs transactions. By understanding what makes up a normal pattern, they can intelligently filter out benign anomalies, allowing cybersecurity teams to avoid alert fatigue and focus on real threats.

GenAI accelerates investigations
GenAI is becoming a powerful partner for security analysts. LLMs can rapidly correlate signals across disparate logs and threat intelligence feeds to build a comprehensive picture of an attack. This enables a natural-language investigation process where an analyst can ask complex questions and receive structured, evidence-backed answers in seconds.

Agentic AI augments SOC and cyber threat intelligence workflows
By handling routine, data-intensive tasks, AI augments the capabilities of human analysts. It can automatically prioritize alerts based on risk context (e.g., proximity to safety-critical systems), ensuring that human expertise is applied where it is needed most: validating high-severity threats and developing long-term mitigation strategies.

Expanding beyond the zero-sum game: the dual role of AI is redefining cyber offense and defense

The evolution to an AI-augmented, product-centric cybersecurity model is not simply a strategic advantage; it is the new imperative for survival. The dual-use nature of AI means that for every defensive development, an offensive innovation is emerging.

In an era where attackers use AI to automate discovery and generate novel exploits, the only viable defense is one that is equally intelligent, adaptive, and integrated across the entire product ecosystem, with a strong focus on API security and LLM-oriented XDR solutions.

Upstream

02.

AUTOMOTIVE CYBERSECURITY TRENDS

In 2025, ransomware attacks reached unprecedented impact, accounting for 44% of incidents but doubling in number compared to 2024;
SDV and AV technologies continue to impact cybersecurity risks, and incidents involving manipulation and control of vehicle systems cemented their status as critical safety risks.

Review of incidents

Cybersecurity attacks grew in both scale and severity in 2025, intensifying the pressure on the Automotive and Smart Mobility industries.

During 2025, Upstream's AutoThreat® researchers analyzed 494 Automotive and Smart Mobility cybersecurity incidents, an average of 41 incidents per month.

This marks a 21% increase over 2024, signaling a continued expansion of the threat landscape.

The top incidents in 2025:

White Hat Black Hat

January

- Security researchers discovered multiple vulnerabilities in a German OEM's infotainment system.[37]
- A US motorcycle OEM experienced a data breach, exposing over 65,000 customer records.[38]
- Security researchers discovered a vulnerability in ECU firmware used in trucks and heavy-duty vehicles.[39]

February

- A US dealership's vehicle transport system was hacked, enabling attackers to reroute shipments and carry out a coordinated theft of luxury cars.[40]
- A ransomware attack on a US automotive technology company compromised over 450GB of data.[41]

March

- Security researchers identified man-in-the-middle vulnerabilities in a Chinese OEM, enabling remote control of vehicle features.[42]
- An Indian Tier-1 supplier was targeted by a ransomware group, compromising 1.4TB of data and affecting multiple OEMs.[43]

April

- Security researchers identified API vulnerabilities in the infotainment system of a Japanese OEM, enabling remote control over car functions.[44]
- A global car rental company suffered a data breach resulting in compromised customer PII and driver's licenses.[45]
- Infotainment software vulnerabilities disclosed across over 800 vehicle models, enabling access to sensitive data and remote code execution.[46]

May

- Security researchers discovered vulnerabilities in a US EV OEM, enabling remote code execution via the Tire Pressure Monitoring System (TPMS) and exposing vehicle control systems.[47]
- Critical vulnerabilities in a German OEM's mobile app enabled unauthorized users to add vehicles to their account and extract PII using a VIN.[48]

June

- A German OEM suffered a cyberattack that exposed authentication tokens, internal access credentials, and sensitive PII.[49]
- Security researchers identified a vulnerability in a German manufacturer of EV chargers, enabling remote code execution via unrestricted firmware upload.[50]

Source: Upstream Security

July

- Security researchers identified vulnerabilities in a German EV charger's controllers, enabling authentication bypass and read/write access via API endpoints.[51]
- Bluetooth flaws were disclosed by security researchers, potentially exposing vehicles to remote code execution attacks.[52]

August

- Security researchers identified encryption bypass in Chinese OEM infotainment OS, exposing sensitive in-vehicle data.[53]
- Security flaws in an online dealership portal allowed remote vehicle unlocking and other remote functions, as well as exposed customer PII.[54]

September

- A UK OEM was hit by a cyber attack, halting production and new vehicle registrations.[55]
- Security researchers disclosed a CAN bus injection vulnerability enabling unauthorized remote start on a US EV model.[56]
- A global agricultural and construction equipment OEM was breached by a ransomware group, resulting in a 2TB corporate data breach.[57]

October

- Security researchers discovered a zero-day SQL injection flaw in an OEM's internal telematics system, enabling full remote control of vehicles.[58]
- An Italian EV charger manufacturer was hit by a ransomware attack, resulting in the exfiltration and release of over 120GB of internal data.[59]
- Cybersecurity testing of electric buses in Norway exposed remote system access risks.[60]

November

- A US commercial OEM was hit by a ransomware attack, resulting in engineering and supplier data exposure.[61]
- A Chinese motorcycle OEM app flaw exposed live GPS and data of over 100,000 bikes.[62]
- An API authorization flaw impacting a South Korean connected-vehicle service allowed attackers to pair vehicles and remotely control critical functions.[63]

December

- Security researchers identified multiple vulnerabilities affecting the infotainment systems of a German OEM.[64]
- Multiple vulnerabilities, potentially leading to data theft, were discovered in the infotainment systems of a Chinese OEM.[65]

Source: Upstream Security

Black hat actors continue to dominate the threat landscape

As threat actors evolve alongside innovative technologies, stakeholders must gain deep visibility into who is behind the attacks. Hackers are classified as black hats, white hats, or gray hats depending on their intentions, actions, and malicious intent.

Black Hat

Black hat actors attack systems for personal or financial gain, or for purely malicious purposes. Today's black hats are not lone wolves but part of organized, well-funded global operations capable of simultaneous strikes against multiple organizations worldwide.

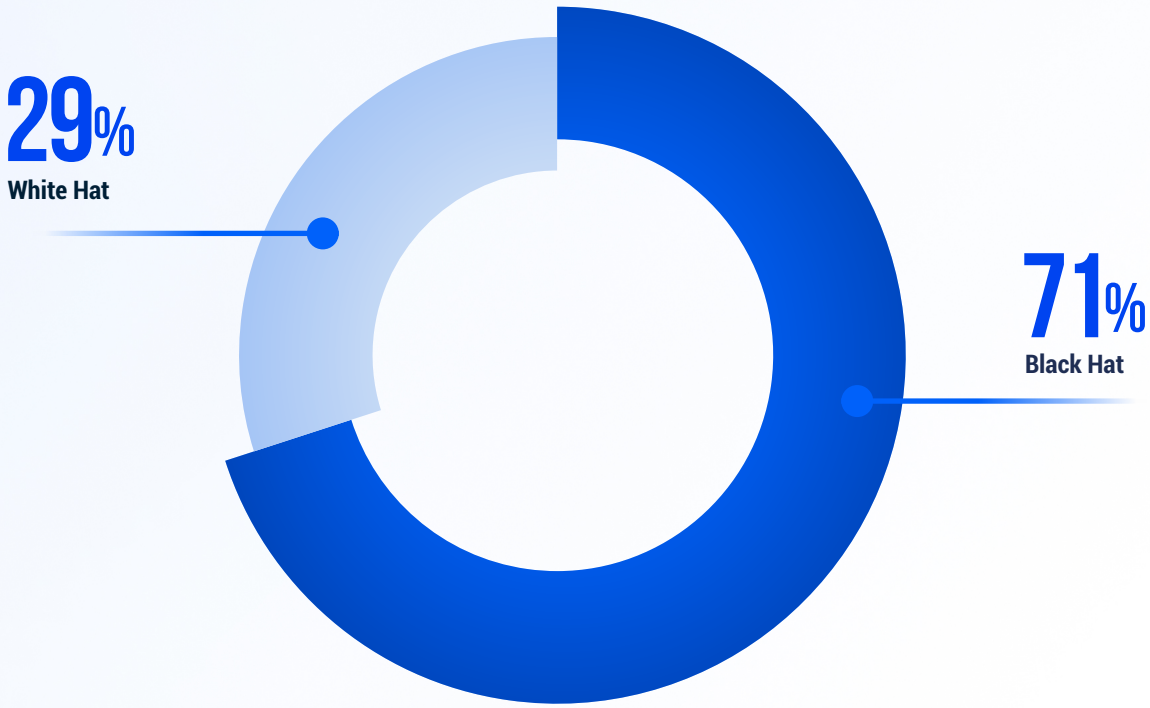
White Hat

In contrast, white hat actors are security researchers who penetrate systems to validate controls and identify new, and often disturbing, vulnerabilities. They operate independently or via bug bounty programs, responsibly disclosing findings to improve cybersecurity posture.

Gray Hat

Gray hat actors operate in the blurred space between ethical and malicious activity, often discovering or exploiting vulnerabilities without explicit permission. Their motivations range from responsible disclosure to financial reward, frequently raising ethical and legal concerns regarding their unauthorized work.

In 2025, black hat hackers carried out over 71% of all attacks



Source: Upstream Security

IT and automotive black hat attacks differ significantly in impact. While IT attacks typically result in data loss or service disruption, **malicious automotive attacks, closely aligned with critical infrastructure threats, carry serious safety risks and the potential for loss of life.**

Ransom-related incidents accounted for 44% of all recorded incidents in 2025, increasing significantly from approximately 26% in 2024 and firmly establishing ransom activity as the dominant black hat tactic. **In practical terms, over 75% of all confirmed malicious incidents involved ransom driven extortion, underscoring its pervasive and systemic impact across the Automotive and Smart Mobility ecosystem.**

In September 2025, a massive cyberattack crippled a UK-based OEM, halting production for several weeks. Occurring during the critical UK plate-change window, the breach forced a shutdown of core IT and production systems, preventing dealerships from registering new vehicles. A well known ransom group claimed responsibility, posting proof of access to internal systems, including infotainment interfaces.[66]

44%
of all incidents were related to ransom activities

In November 2025, a US-based Tier-1 supplier was hit by a ransomware attack. Attackers claimed to have stolen and leaked over 1TB of corporate data on the dark web. The company has not publicly confirmed coordination with authorities.[67]

Also in November 2025, a Japanese OEM was hit by a ransomware attack triggered by a zero-day in an enterprise platform. The threat actor claimed responsibility and added both the OEM and its US subsidiary to its leak site.[68]

These attacks cause more than financial damage; they introduce significant safety risks, particularly in critical infrastructure sectors. In many incidents, consumers remain unaware of the potential danger, raising the stakes for cybersecurity teams.

The growing sophistication of these large-scale campaigns underscores the urgent need for proactive threat intelligence to mitigate the risks posed by industrialized black hat operations.

Remote attacks account for the vast majority of incidents

Automotive and Smart Mobility cyber attacks fall 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 89% of all attacks between 2010 and 2025, and 92% in 2025. In 2025, long-range attacks accounted for 86% of remote attacks, a 2% increase since 2024.

Nearly all 2025 incidents were remote

The vast majority of remote incidents in 2025 were long-range

Source: Upstream Security

Data privacy breaches, business disruption, and vehicle control dominate the impact landscape

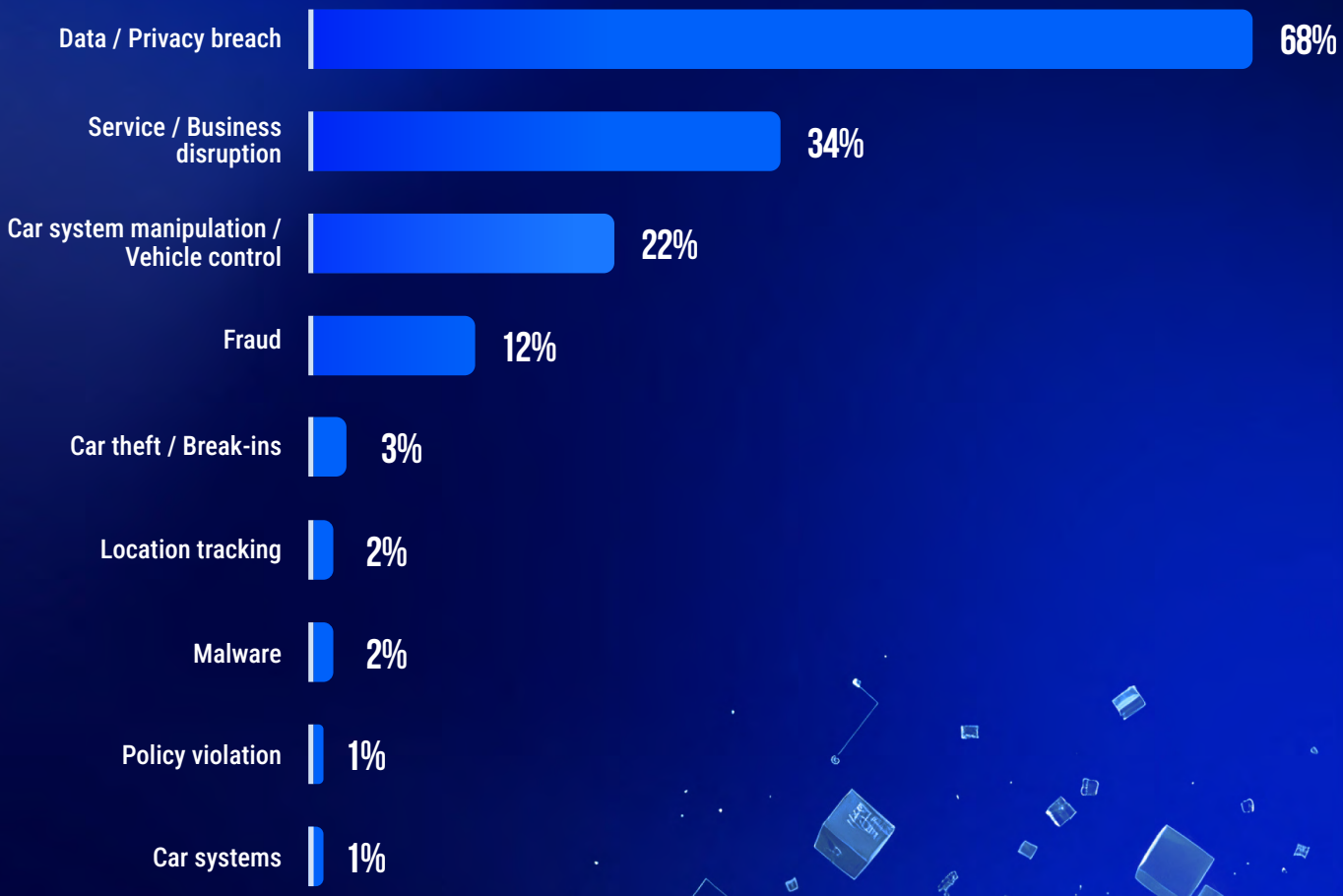
The impact of cyber attacks on the Automotive and Smart Mobility ecosystem continues to grow in scale and severity. While many vehicle-related incidents involve the compromise of sensitive data, others have far-reaching consequences, including vehicle theft, misuse and fraud, and the control of vehicle systems, all of which introduce serious safety risks.

Data and privacy-related incidents accounted for 68% of 2025 incidents, up from 60% in 2024.

This increase reflects several converging factors. Expanded security research into EV chargers, infotainment systems, and other connected automotive components has uncovered a growing volume of exploitable weaknesses. This trend is evident in the sustained activity of organizations such as the Automotive Security Research Group (ASRG)[69] as well as established white hat research communities, which continue to disclose new automotive related CVEs. **In parallel, the continued rise of ransomware and data extortion campaigns targeting sensitive information and personally identifiable data has materially increased the share of data-driven incidents across the ecosystem.**

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 PII. Cybersecurity incidents involving data breaches are the most common and most expensive.
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).
Car system manipulation	Threat actor activities targeted at tampering with various in-vehicle systems, changing their expected operational behavior, and creating safety risks.
Misuse and fraud	Illegal use of vehicle data and/or vehicle functionality by threat actors and vehicle owners for financial gain.
Vehicle theft	Vehicle thefts involving long-range, short-range, and physical attacks by threat actors.
Location tracking	Illegal use of GPS navigation data to track a vehicle's location and movement without user or owner consent.
Policy violation	Threat actors' actions that violate established rules, regulations, or policies regarding the use, operation, or management of vehicles.
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.

2025 impact breakdown, based on 494 automotive-related cyber incidents



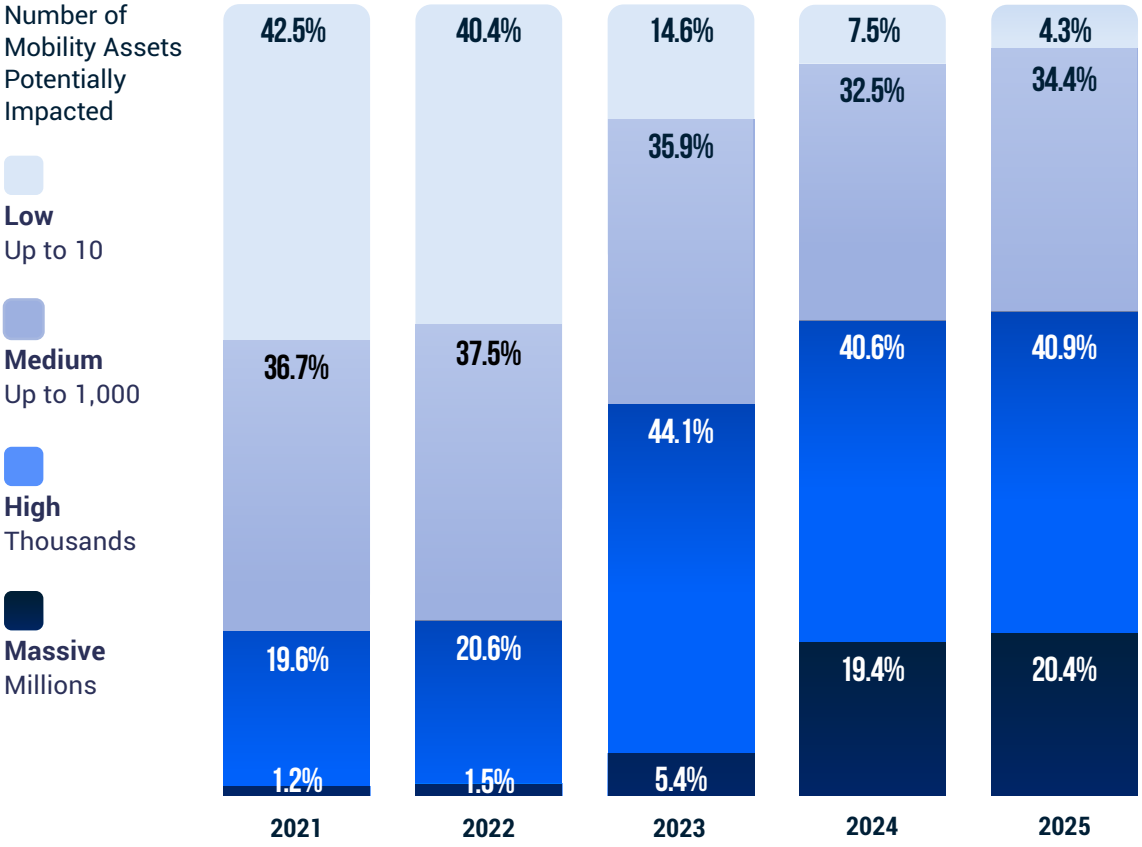
Source: Upstream Security

Automotive and smart mobility incidents continue to carry significant impact at scale

Upstream has tracked the potential impact and scale of these incidents since 2021. By 2023, the threat landscape reached a clear inflection point, with a marked increase in scale and sophistication. The growing focus of threat actors on the Automotive and Smart Mobility ecosystem became evident as activities shifted from experimental hacking toward coordinated, large-scale attacks.

In 2025, incidents classified as 'High' or 'Massive' impact represented nearly 61% of all publicly disclosed incidents, reinforcing the inflection point in the threat trajectory. This shift reflects a more mature threat landscape in which cyber-driven risks affecting thousands to millions of mobility assets are no longer exceptional events, but the dominant risk facing the industry.

Breakdown of publicly disclosed incidents by potential scale, 2021-2025:



Source: Upstream Security

61%
of incidents had high-massive impact

The increase in large-scale incidents stems from multiple converging factors, including the rapid proliferation of AI tools that expand AI-enabled attack surfaces, alongside a systemic cybersecurity gap first identified by Upstream in early 2025.[71]

Monitoring CVEs is crucial

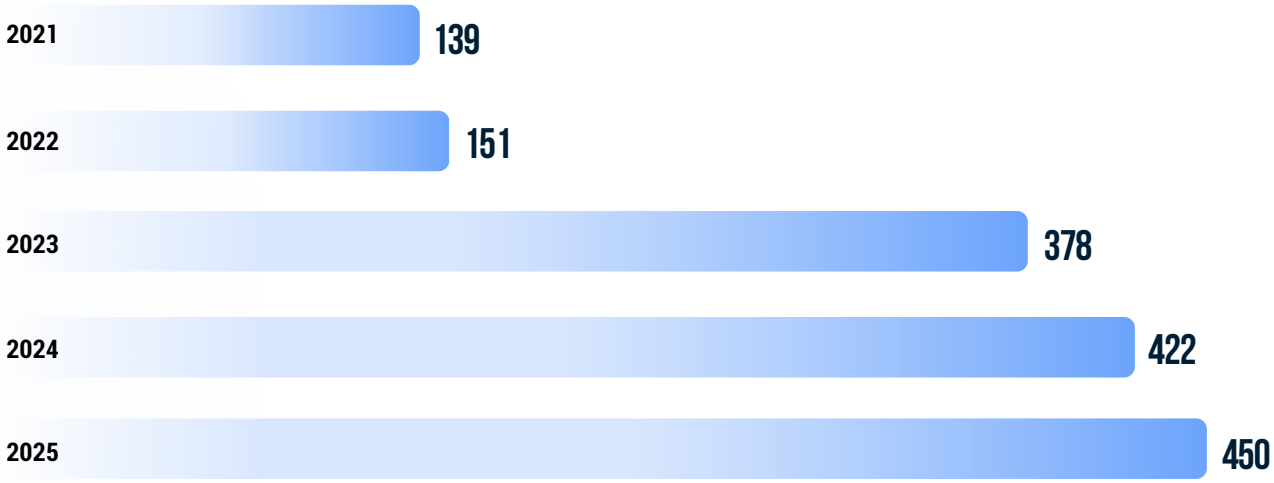
The Common Vulnerability Scoring System (CVSS) provides an open, standardized method for rating CVEs, helping organizations prioritize responses based on base, temporal, and environmental properties.[72] Vulnerabilities are also graded from Critical, High, Medium to Low, or None, based on their CVSS score.[73]

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 2021-2025

The Automotive industry has experienced 1,540 specific CVEs since 2021; 450 CVEs were published in 2025, compared with 422 in 2024.

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.

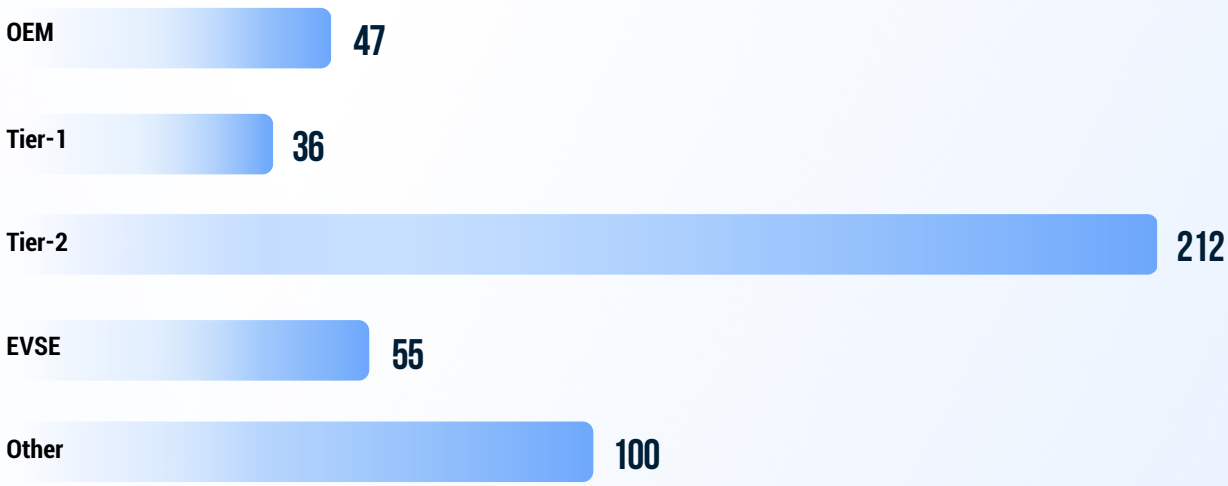
Overview of 2025 CVEs

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 2025, the US National Vulnerability Database (NVD) continued to struggle with a growing backlog of unanalyzed vulnerabilities,[74] driven by insufficient funding,[75] a rapid increase in submissions, and legacy systems that could not keep pace.[76]

2025 breakdown of publicly reported automotive-related vulnerabilities



Source: Upstream Security

In 2025, the CVSS-scored vulnerabilities analyzed by Upstream's analysts had:[77]

33 ***Critical Vulnerabilities***

235 ***High Vulnerabilities***

162 ***Medium Vulnerabilities***

17 ***Low Vulnerabilities***

Source: Upstream Security

In 2025, the combined number of high and critical severity CVEs remained elevated and continued to represent approximately 60% of all reported vulnerabilities in both 2024 and 2025.

This persistent concentration of high-impact issues underscores the need for continuous tracking of automotive-relevant CVEs, early exploit detection, and disciplined mitigation across the ecosystem.

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 advanced connectivity, software-defined architectures and smart mobility IoT 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. Cyber attacks 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 & suppliers

OEMs and their global supply chains face a sharp rise in ransomware and data extortion. Attackers are increasingly exploiting third-party providers, outsourced development partners, and credential reuse. These attacks have resulted in production shutdowns, large-scale data theft, operational paralysis, and prolonged recovery periods across the automotive ecosystem.

In March 2025, a UK OEM suffered multiple cyber incidents tied to supply chain compromise and data extortion. In one case, a ransomware group allegedly used stolen third-party credentials belonging to a South Korean Tier-1 supplier to access internal systems, exfiltrating hundreds of gigabytes of sensitive material, including proprietary source code and internal documents.[78]

In a separate incident in March 2025, a threat actor published over 700 internal files belonging to the same OEM on a dark web forum.[79] This leak included development logs, project materials, and source code fragments, alongside claims that an employee dataset containing usernames, display names, emails, and internal metadata had been compromised.

In September 2025, the same OEM disclosed a significant cyber attack linked to yet another threat actor. The intrusion forced the company to shut down core IT systems globally, halting production and disrupting dealer retail operations. The UK National Crime Agency has opened an investigation, and the company continues to restore systems in a controlled manner.[80]

In November 2025, a Japanese OEM allegedly fell victim to a ransomware attack following a zero-day vulnerability in an enterprise system. The ransomware group listed the OEM and its US subsidiary on its leak site, claiming the companies' data has been breached and threatening publication unless ransom demands are met. The listing followed a campaign exploiting the zero-day vulnerability.

Ransomware actors have also intensified targeting of third-party AI service providers. In September 2025, a multinational OEM confirmed a data breach at a US-based provider supporting its North American customer service operations, exposing customer contact details. While the company stated that no financial or highly sensitive personal information was affected, it activated its incident response protocol, notified authorities, and began directly informing impacted customers.[81]

EVs & EVSE

EV adoption trends vary in different countries, but concerns over power grid cybersecurity and charging infrastructure resilience are growing globally. The rapid expansion of charging networks often overlooks essential cybersecurity controls, and EVSE-specific regulations lag behind deployment. Chargers remain vulnerable to physical and remote manipulation, exposing users to fraud, data theft, operational disruption, and ransom-driven attacks.

In January 2025, researchers disclosed extensive vulnerabilities affecting Chinese EV chargers, including Home and Pedestal models.[82] Findings included sensitive data exposure, buffer overflow, denial of service, command injection, and remote code execution flaws, as well as weaknesses in backup handling, firmware manipulation, and file upload functionality. These vulnerabilities, published under CVE identifiers 2024-43648[83] through 2024-43663[84] with vendor scores ranging from 5.3 to 9.8, could allow attackers to access plaintext credentials in firmware, interrupt charging sessions, execute arbitrary commands, install malicious firmware, or manipulate file systems. Successful exploitation could lead to persistent compromise, charger inoperability, or disruption of back-end communications.

In September 2025, a German EV charging provider serving multiple global OEM programs confirmed a data incident involving a third-party customer support vendor.[85] The vendor accessed customer records without valid business justification, exposing PII including names and email addresses. Payment data was not affected, and the provider reported that the number of specifically impacted customers is in the single digits. Impacted individuals were notified, and authorities informed, though the company has not disclosed the broader scope of the compromise.

These 2025 incidents highlight continuing EV ecosystem risks, ranging from device-level firmware weaknesses to supplier-related data exposure involving third-party operators.

Fleet operators

As fleet operators, such as rental companies, logistics services, and delivery providers, increase their reliance on connectivity and software-driven management, their cybersecurity risks multiply. **Incidents affecting fleets can lead to reduced availability and efficiency, increased costs, service delays, sensitive location data exposure, and complete service interruptions.**

In April 2025, a German-based fleet management and vehicle tracking provider exposed sensitive real-time and historical travel data from more than 300,000 commercial and passenger vehicles worldwide. An unsecured log observability instance left nearly 1TB of data publicly accessible, including VINs, vehicle locations, journey start and destination points, route histories, and driver seat information. The data was likely intended for development, and the instance was secured following discovery.[86]

In August 2025, a South Africa-based vehicle tracking and fleet management firm suffered a cyber attack where a subset of on-premises servers was encrypted by a ransom group.[87] Initial forensics found no evidence of customer data compromise. However, after the company declined to negotiate, the ransom group published over 500GB of allegedly stolen material on its dark web leak site, including invoices, proprietary source code, and sensitive customer information.

In September 2025, a Brazilian-based fleet management organization was breached by a threat actor claiming to have exfiltrated a large database.[88] The compromised data allegedly included company records and consumer PII such as identification numbers, driver licenses, and vehicle details, totaling hundreds of thousands of records. No official response has been disclosed, and the full impact on fleet clients remains unclear.

Smart mobility IoT devices and applications

As smart mobility IoT devices and applications expand, they remain high-risk targets. These platforms frequently store sensitive personal and payment information for large user bases. Often using a robust API infrastructure, these devices and applications are vulnerable to a wide range of API risks, in addition to IoT protocols and other IT related vulnerabilities. Cyber incidents here directly impact user safety, personal data, and operational availability.

In January 2025, a security researcher reported that more than 100 license plate scanners were improperly configured, exposing live camera feeds and sensitive license plate data to the public internet without authentication. The devices, supplied by a US-based vendor, were accessible to anyone who identified the misconfigured endpoints, raising significant privacy and surveillance concerns. The company has not publicly commented or confirmed corrective actions.[89]

In June 2025, an India-based ridesharing platform operating across India, Indonesia, Egypt, and Vietnam confirmed a data breach affecting over 8 million users. A threat actor claimed access to a database containing full names, phone numbers, email addresses, physical addresses, and vehicle registration numbers. While no passwords or financial data were exposed, the company initiated containment measures, increased monitoring, engaged third-party experts, and notified authorities.

In October 2025, a coordinated stunt in San Francisco disrupted autonomous ride hailing operations when a tech prankster organized a group to order US-based self-driving taxis to the same dead-end street. Approximately 50 vehicles arrived simultaneously, congested the area and suspended rides within a two-block radius, as well as causing significant service disruptions due to unavailable vehicles. The incident, informally called the first Distributed Denial of Service (DDoS) against an autonomous taxi network, demonstrated how coordinated misuse can impact autonomous fleet behavior and availability.[90]

Automotive insurance-related devices and applications

Insurers increasingly rely on connected vehicle data to refine risk calculations and premium models, but this introduces new attack vectors. Behavior-based insurance models use aftermarket devices to share telematics data; however, these devices can introduce vulnerabilities allowing threat actors to manipulate data, disrupt communications, or access insurance networks. Insurers and their suppliers must ensure these systems remain secure.

In April 2025, a US-based insurance firm confirmed a data breach exposing driver license numbers for customers across multiple states. A vulnerability in the online application process allowed unauthorized access to these records. The company identified and fixed the issue in March 2025. Public filings indicate that at least 17,500 individuals in Texas and 1,900 in South Carolina were affected, with the total number across all states unconfirmed.[91]

In September 2025, a security researcher discovered that a US-based technology vendor supporting digital claims processing had left an unencrypted, publicly accessible database online. The database contained approximately 5 million records totaling roughly 10TB of data, including vehicle registrations, power of attorney forms, repair invoices, photographs of damaged vehicles with visible license plates and VINs, and policyholder personal information. The company secured the database after disclosure and updated its internal policies and code to prevent recurrence.[92]

Autonomous vehicles

AV technologies are advancing rapidly, yet safety concerns and public distrust remain. AVs depend on remote access, cloud connectivity, and edge systems containing sensors like GPS, LIDAR, cameras, millimeter-wave radar, and IMU systems. Because these sensors receive data from external sources, attackers can interfere with information retrieval, force the interpretation of manipulated signals, or degrade functionality.

In February 2025, researchers demonstrated a new Moving Vehicle Spoofing system capable of object removal attacks against vehicles moving at speeds up to 60 km/h from distances of 110 meters. **The "Adaptive High Frequency Removal" technique allowed attackers to remove real obstacles from the victim vehicle's LIDAR perception even with modern pulse fingerprinting defenses in place. Evaluations resulted in critical perception failures and collisions, underscoring the urgent need for robust LIDAR defenses.**[93]

In June 2025, a Canadian Tier-2 supplier providing LIDAR systems for autonomous vehicles was targeted by a large ransomware group. The attackers claimed to have exfiltrated 460GB of data, though the content remains unknown. The company has not publicly acknowledged the incident.[94]

In July 2025, researchers introduced a controllable physical adversarial patch that targets camera-based perception systems in AVs. Unlike traditional patterns, the patch remains inert until triggered by a laser signal, enabling precise targeting of individual vehicles. The system achieved a 91.9% success rate at distances up to 50 meters in both digital and real-world testing. Researchers proposed mitigations including sensor fusion, adversarial patch detection, and randomized exposure patterns.[95]

Upstream

03.

ATTACK VECTORS

Backend infrastructure remains the primary battlefield, while physical and short-range attacks evolve in precision and sophistication; new AI-related threats must be monitored closely.

Threats against Autonomous Driving, Connectivity, Electrification, and Shared Mobility (ACES) technologies shape the attack landscape

Cyber attacks in 2025 became more sophisticated and aggressive, with threat actors doubling down on high-value targets across vehicles, backend systems, and smart mobility platforms. While the overall distribution of attack vectors remained similar to 2024, this stability revealed a deeper trend: attackers knew exactly where to strike, and they focused their efforts with unprecedented precision.

Backend servers continued to dominate as the primary attack surface, accounting for 67% of all incidents in 2025. This reflects the sharp escalation in ransomware campaigns targeting the Automotive and Smart Mobility ecosystem. **These large-scale intrusions increasingly aimed at telematics platforms, cloud services, and application servers, turning backend infrastructures into the central battlefield of 2025.**

67%
of incidents were targeting backend systems

50%
rise in attacks against EV charging

API-based attacks remained consistently high (18% in 2025 compared to 17% in 2024), reflecting the continued exploitation of interfaces that bridge vehicles, mobile applications, and backend services.

EV charging infrastructure also emerged as a growing attack surface in 2025, with charging related incidents rising to 8% of all incidents, up from 6% in 2024. Data intensive platforms, rapid deployment cycles, and broad physical accessibility continue to expose EV chargers, backend systems, and connected applications to scalable exploitation.

With ransomware targeting core mobility infrastructure, disruptions quickly spread from backend environments to fleets, EV charging infrastructure, and end-user applications. As a result, the threat landscape matured, attackers intensified their campaigns, and the Automotive and Smart Mobility ecosystem faced one of its most operationally disruptive years to date.

Alongside these established attack surfaces, AI is rapidly emerging as a new and impactful vector of exposure. As OEMs embed LLMs, AI agents, and data-driven orchestration layers into backend platforms and vehicle ecosystems, attackers are increasingly able to manipulate model behavior, exhaust AI-driven services, or exploit AI-enabled third-party components.

This shift signals that AI must now be treated not only as a capability enabler, but as a security-critical surface that requires continuous monitoring and governance across the Automotive and Smart Mobility ecosystem.

Incidents by Attack Vector

Please note that some incidents involved multiple attack vectors; as a result, the total exceeds 100%

Source: Upstream Security

Telematics and application servers

Connected vehicles and Smart Mobility IoT devices collect, send, and receive information from backend systems throughout their lifespan. These systems include telematics servers that communicate with the vehicle or device, application servers that interface with companion applications, and additional backend platforms operated by third-party vendors supporting insurance services, fleet management, rental and leasing operations, EV charging networks, and other mobility functions. Vulnerabilities across this ecosystem can allow threat actors to exfiltrate sensitive information or, in some cases, gain access to vehicle-facing systems in real time.

- In September 2025, security researchers disclosed a lockdown bypass in a US EV OEM's TCU, enabling local root access. The exposed micro-USB port enabled an attacker to write files, escalate to a root shell, and install persistent tools or pivot into other in-vehicle systems. The OEM addressed the flaw in a firmware update.[96]
- **In October 2025, security researchers demonstrated that a major OEM's telematics infrastructure could be breached through a zero-day SQL injection vulnerability in a contractor's publicly exposed application.** By exploiting the contractor's issue-tracking system, the attacker was able to pivot into the manufacturer's telematics backend. During exploration, the attacker identified a firmware update command that permitted the upload of malicious firmware to the TCU. **Once deployed, this malicious firmware enabled manipulation of critical vehicle systems, such as engine behavior and transmission functions, over the CAN bus.**[97]
- In December 2025, a German OEM's vehicles in Russia were reportedly immobilized following unexpected engine shutdowns, when the Vehicle Tracking System (VTS) module lost connectivity. According to reporting, the disruption was linked to unauthorized interference with the backend infrastructure supporting the OEMs regional alarm and telematics services, causing widespread service outages.[98]

APIs

APIs have become the nervous system of the Automotive and Smart Mobility ecosystem. Connected vehicles, 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 present significant, fleet-wide attack vectors, resulting in a wide range of cyber attacks such as sensitive PII theft, backend system manipulation, or malicious remote vehicle control.

The rapid proliferation of AI-powered systems and MCPs across the entire connected mobility ecosystem, adds another layer of API risks.

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

In the past year, the Automotive and Smart Mobility ecosystem, supply chains, as well as mobility IoT devices and services, have experienced a significant increase in data and privacy breaches due to API-based attacks.

- In January 2025, a team of security researchers discovered a significant API vulnerability, enabling remote control of Japanese OEM vehicles. The vulnerability leveraged an insecure admin portal, enabling attackers to bypass 2FA and reset employee passwords, which granted unrestricted access to customer accounts. With only a last name and ZIP code, email, or license plate, attackers could remotely start, stop, lock, unlock, or locate vehicles. **These flaws could allow a malicious actor authenticated in the admin portal API to register themselves as an authorized user for a vehicle, gaining complete control over it without notifying the car's owner.**[99]
- In April 2025, security researchers identified authorization bypass vulnerabilities in Chinese EV chargers affecting their APIs. Exploiting these vulnerabilities could allow unauthenticated attackers to perform actions such as renaming EV chargers, obtaining other users' charger information, and accessing EV charger energy consumption data. Additionally, an unauthenticated attacker could obtain EV charger version and firmware upgrading history by knowing the charger ID.[100]
- In November 2025, security researchers disclosed an API authorization flaw impacting a South Korean connected vehicle service that allowed attackers to pair vehicles and remotely control critical vehicle functions. The issue stemmed from an authorization flaw that allowed a malicious user to pair a victim's vehicle to an unverified account using only the vehicle's VIN and the owner's email address. **According to the researchers, the exposed API endpoints allowed unauthorized access to critical functions, including lock/unlock and start/stop commands, without demonstrating ownership of the email account associated with the vehicle.**[101]

Infotainment systems

The In-Vehicle Infotainment (IVI) system is one of the most common attack vectors in modern vehicles. Because it connects to the internet and interfaces with installed OEM and third-party applications, mobile phones, and Bluetooth devices, it is frequently exposed to external threats and sensitive PII. **Additionally, IVI systems often bridge to vehicle internal networks, posing a serious safety risk; they can serve as the path of least resistance for malicious software to penetrate critical internal systems.**

- In July 2025, security researchers published a vulnerability chain in a widely deployed automotive Bluetooth stack that enables attackers to trigger one-click, unauthenticated remote code execution during the pairing process. Demonstrations on infotainment platforms showed that exploiting the flaws grants access to sensitive in-vehicle data and can potentially allow lateral movement toward additional electronic control units. The risk is heightened in systems configured with permissive pairing modes such as “Just Works”, leaving drivers reliant on timely IVI updates or the option to disable Bluetooth if concerned.[102]

- In August 2025, a security researcher demonstrated a zero-day flaw in an infotainment platform that allows attackers to implant malicious PNG images into the bootloader sequence. **Because the boot process did not properly validate the integrity of these assets, a modified firmware package could have displayed a crafted QR code at startup, enabling phishing attacks directly through the vehicle’s screen.** The accompanying proof-of-concept showed how manipulated firmware can be flashed onto the head unit to embed backdoored APKs and support remote session capture. The researcher disclosed the issue to the vendor.[103]

- In September 2025, security researchers confirmed active exploitation of a zero-click stack buffer overflow in an SDK used across infotainment systems. The vulnerability, originally disclosed together with several other protocol flaws, enabled an attacker with combined Bluetooth pairing proximity and WiFi access to execute code with root privileges on the vehicle's head unit. **Successful exploitation can expose in-vehicle data, disrupt infotainment functionality, or establish persistent control over the infotainment system.** Although the SDK developer has issued patches, many vehicles remain exposed due to delayed or incomplete update deployment by OEMs.[104]

EV charging infrastructure

Providing a reliable and safe charging infrastructure is essential to accelerating electric vehicle adoption. However, many chargers, infrastructure components, and related apps remain vulnerable to physical and remote manipulation. These threats can disrupt reliability, expose users to PII theft, misuse and fraud, and ransom attacks. They also have widespread implications for charging networks, vehicles, and even the local electric grid.

8%
of all incidents are EV charging-related

EV charging related incidents continued to rise in 2025, accounting for 8% of all incidents, up from 6% in 2024. **The combination of data rich environments, rapid innovation cycles, and widespread physical access to public charging equipment continues to attract threat actors.** As a result, attackers are increasingly identifying new vulnerabilities across chargers, backend platforms, and connected applications, with growing potential for exploitation at scale.

- In May 2025, security researchers identified critical vulnerabilities affecting a German EVSE manufacturer's home charging models, exposing them to unauthorized command execution over the local network. The flaws originated from insufficient input validation in the onboard web interface, allowing an attacker on the same network to gain system-level control of the charger without authentication. If exploited, these weaknesses could enable manipulation of charging behavior, configuration changes, or disruption of connected home energy systems. The manufacturer has not confirmed whether a software fix is available.[105]
- In October 2025, security researchers reported two high-severity weaknesses in a popular AC charging unit that exposed its web-based management interface to firmware-level compromise. One flaw allowed a network-adjacent user with login access to upload a crafted firmware package through the configuration portal, enabling arbitrary code execution, while a second stack-overflow issue in a download handler could trigger memory corruption and similar execution risks. If exploited, these weaknesses could undermine firmware integrity, disrupt backend communications, or interfere with normal charger operation. Vendor mitigation guidance has not been released.[106]
- In November 2025, security researchers highlighted a protocol-level weakness in the SLAC (Signal Level Attenuation Characterization) protocol pairing mechanism used in ISO 15118–based EV charging. This flaw allowed a nearby attacker on the same powerline segment to spoof pairing messages and position themselves as a man-in-the-middle before any encrypted channel was established. By hijacking the physical PLC pairing, an attacker could

intercept or alter charging session data, enabling billing manipulation, credential interception, or disruptive session tampering across public and fleet charging environments. Because the issue arose from the SLAC design itself rather than a specific vendor implementation, any charging system relying on an unauthenticated SLAC pairing was theoretically exposed.[107]

ECUs

Electronic Control Units (ECUs) support core vehicle functions, including engine operation, braking, steering, body controls, and keyless entry. **Because of their central role in coordinating critical systems, ECUs remain priority targets for attackers seeking to manipulate firmware, bypass security protections, or interfere with vehicle communications.** Many ECU attacks focus on exploiting vulnerabilities in embedded microcontrollers, diagnostic services, or communication protocols, which can allow unauthorized access to firmware, secret keys, or control functions.

- In January 2025, security researchers identified a vulnerability in an ECU produced by a global automotive supplier. Tracked as CVE-2024-12054, the issue affected firmware versions built in early 2023. The vulnerability exploited deterministic seed generation allowing attackers to bypass authentication and remotely access diagnostic functions originally intended only for authorized toolchains. Successful exploitation could impact system integrity or availability by erasing software or degrading performance. The vulnerability was reachable through adjacent network radio frequency equipment or connected telematics devices.[108]
- In March 2025, a major US Tier-2 supplier disclosed multiple critical vulnerabilities across its automotive software platforms, including components relying on automotive vehicle networks. Identified as CVE-2024-53012, CVE-2024-53022, CVE-2024-53028, CVE-2024-53029, CVE-2024-53030, CVE-2024-53031, and CVE-2024-53032, these flaws could allow attackers to cause denial-of-service conditions or achieve remote code execution under certain circumstances.[109]

ECU vulnerabilities and manipulation attempts often originated in other vulnerabilities such as APIs and IoT protocols. The increased sophistication of the connected vehicle ecosystem requires securing ECUs with a holistic approach.

Vehicle sensors

Vehicle sensors provide essential information for object detection, collision avoidance, and real-time perception across both connected and autonomous systems. These sensors remain vulnerable to physical and remote control, including spoofing, jamming, and data interference. Successful attacks can cause incorrect interpretation of the driving environment, compromise safety, and disrupt critical vehicle functions, undermining trust in modern sensor-based mobility technologies.

In February 2025, researchers demonstrated a new Moving Vehicle Spoofing (MVS) system capable of object removal attacks against vehicles moving at speeds up to 60 km/h from distances of 110 meters. The "Adaptive High Frequency Removal" technique allowed attackers to remove real obstacles from the victim vehicle's LIDAR perception even with modern pulse fingerprinting defenses in place. **Evaluations resulted in critical perception failures and collisions, underscoring the urgent need for robust LIDAR defenses.**[110]

CAN bus

The CAN bus is essential for communication between 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 2025, security researchers demonstrated remote compromise of commercial trucks and buses, granting attackers control over critical vehicle functions. The research revealed vulnerabilities in the SAE J1939 protocol, which facilitates communication between ECUs. According to the research, attackers could unlock vehicles, manipulate engines, or disable safety systems using cellular, Wi-Fi, or Bluetooth interfaces.[111]

- In July 2025, a security researcher demonstrated firmware extraction on a popular automotive ECU, widely deployed in engine and transmission systems. By leveraging CAN bus access and voltage glitching, the researcher bypassed security protections and retrieved the firmware using a custom bootloader. **This research highlights real-world risks of firmware tampering and reverse engineering on safety-critical ECUs, emphasizing the need for stronger fault injection resistance and secure boot mechanisms in automotive microcontrollers.**[112]

  In October 2025, Japanese OEM vehicles were targeted using a headlight CAN

- bus injection technique across Canada, Australia, and the UK. Attackers gained physical access to wiring behind headlights or taillights to plug in a "CAN Invader" device, injecting messages to disable the immobilizer and start the engine. The OEM offered limited wheel-well protection kits in some markets to block access to the wiring.[113]

Third-party applications and services

Third-party applications and services support a wide range of connected vehicle functions, including remote diagnostics, infotainment platforms, EV charging services, dealership scheduling systems, and fleet management systems. While these services enhance vehicle usability and the owner experience, they remain susceptible to physical and remote manipulation, including data breaches, unauthorized access, and disruption of hosted systems. **Vulnerabilities in third-party platforms can expose users to fraud, privacy violations, and ransom-driven attacks, and in some cases jeopardize the security posture of vehicles or supporting mobility infrastructure.**

- In January 2025, security researchers demonstrated a successful exploit chain against a widely used open-source automotive software platform. By combining multiple vulnerabilities, including one previously known issue, they achieved code execution on the platform and earned a financial reward. The incident highlighted how weaknesses in shared software components used by multiple OEMs or service providers can lead to broad ecosystem risk.[114]

- In April 2025, a fleet management and vehicle tracking service provider based in Germany unintentionally exposed sensitive real-time and historical travel data from more than 300,000 commercial and passenger vehicles worldwide. An unsecured cloud-based analytics instance left nearly a terabyte of information publicly accessible, including VINs, coordinates, journey start and destination points, route histories, and driver seat data. The exposure is believed to have originated from a development environment, and the company secured the instance following disclosure.[115]

- In August 2025, a national public authority responsible for fixed and mobile speed camera operations across major highways in the Netherlands was targeted in a ransomware campaign. **Attackers exploited a zero-day vulnerability tracked as CVE-2025-6543, forcing authorities to disconnect multiple camera systems from the internet and rendering many enforcement devices temporarily inoperable.** The incident also resulted in the exposure of sensitive information, including active investigations, court-related files, and personnel records.[116]

Smart mobility devices and intelligent transportation systems

Smart mobility devices and Intelligent Transportation Systems (ITS) are crucial for reducing congestion, improving traffic management, sharing real-time traffic data, supporting environmental initiatives, 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. **Attacks on these systems compromise safety, erode data privacy, and disrupt operational availability, which elevates them to the level of critical infrastructure in both risk and consequence.**

ITS and mobility IoT devices, such as public transportation systems, electronic logging devices (ELDs), and traffic signals, are vulnerable to ransomware, data manipulation, and physical and remote interference. When exploited, these vulnerabilities can disrupt traffic flow, compromise public safety, and expose transportation networks to fraud and sabotage, undermining public trust in infrastructure.

- In July 2025, security researchers uncovered critical vulnerabilities in a widely used aftermarket steering system for smart farming vehicles that could enable attackers to track, disable, or remotely control equipment across global agricultural fleets. The researchers found that the system relied on an unencrypted and unsigned over-the-air update mechanism, along with weak authentication on its MQTT broker. **This created opportunities for real-time GPS tracking, theft of sensitive operational data, and unauthorized "lock" commands capable of stopping machinery during use.** According to media reports, despite vendor claims of remediation, an estimated 46,000 vehicles, primarily across Asia and Europe, remain exposed, posing significant safety, operational, and privacy risks.[117]

- In August 2025, security researchers demonstrated that unsecured free Wi-Fi networks on smart buses could be exploited to gain remote access to critical onboard systems. By abusing a shared M2M router that handled both passenger Wi-Fi and safety-critical services such as ADAS and Advanced Public Transportation Services (APTS), the researchers showed how poor network segmentation enabled lateral movement once router authentication was bypassed. **The researchers identified multiple vulnerabilities, including command injection flaws and an MQTT backdoor that could allow attackers to track buses in real time, access onboard cameras, manipulate digital displays, or tamper with operational data.**[118]

Mobile applications

Increasingly connected and software-defined vehicles allow OEMs to enhance customer experience and provide remote services via companion and third-party apps, giving owners convenient smartphone access to critical functions. These applications enable users to track locations, unlock doors, start engines, activate auxiliary devices, and subscribe to premium features.

However, the same apps that enhance the digital experience can be exploited to access vehicles and backend servers. Companion applications often contain widespread software and API vulnerabilities, including open-source flaws, hard-coded credentials, and weaknesses in API or backend server integration. Furthermore, OEM companion and smart mobility apps are frequent targets for identity theft; threat actors can exploit mobile and server-side vulnerabilities to harvest credentials and compromise private user information on a large scale.

- In May 2025, a security researcher identified multiple critical vulnerabilities in a major OEM's mobile application that allowed unauthorized access to customer and vehicle data. The researcher found that the app permitted unlimited OTP brute-force attempts and lacked proper authentication controls. Additionally, several API endpoints exposed sensitive information, including internal service credentials, full customer profiles, and complete vehicle service histories, using only a vehicle's VIN. **These weaknesses could have allowed attackers to add cars to their own accounts, retrieve real-time telematics, or impersonate legitimate owners.**[119]
- In August 2025, owners of a Chinese vehicle model reported a wave of account-hijacking incidents that enabled attackers to take full control of vehicles through the mobile app. Beginning in June, drivers in Russia saw a sharp rise in unauthorized master-account takeovers, with attackers exploiting weak app-registration practices linked to unofficial vehicle imports. Many compromised accounts were registered using cloned Chinese SIMs, expired virtual numbers, or dealer-controlled logins that were later revoked. Once attackers gained access, they locked legitimate owners out, remotely operated functions such as windows, doors, and engine start, and demanded ransom payments.[120]
- In November 2025, a security researcher uncovered an Insecure Direct Object Reference (IDOR) vulnerability in a connected motorcycle mobile application that exposed telematics data for other riders' vehicles. By modifying a single numeric parameter in an API request, the researcher was able to retrieve precise GPS locations, encryption details, and technical information for motorcycles belonging to other users. This flaw, affecting more than 100,000 installations, effectively enabled global tracking and unauthorized access to personal and vehicle data without authentication.[121]

GPS/GNSS navigation system

GPS and GNSS navigation systems are essential for accurate positioning, route optimizations, and vehicle coordination across personal vehicles, commercial fleets, and autonomous platforms. **These systems remain increasingly vulnerable to physical and remote manipulations, including signal spoofing, signal jamming, and manipulation of the software and hardware components that interpret positioning data.** Attacks can degrade navigation accuracy, expose sensitive location information, and in advanced environments, compromise the safety of connected and autonomous vehicles. Broader disruptions can also affect transportation networks, logistics operations, and public trust in navigation technologies.

- In June 2025, two critical vulnerabilities were disclosed in a series of GPS tracking and IoT fleet management devices manufactured by a Chinese Tier-1. The issues, tracked as CVE-2025-5484 and CVE-2025-5485, affected all known GPS units from the manufacturer as well as the associated fleet management platform. The flaws allowed remote tracking of vehicles, manipulation of device functionality, and in certain configurations, the ability to disable fuel delivery. Contributing factors included default passwords and simple numeric identifiers that could be easily enumerated by attackers.[122]
- In July 2025, researchers exposed electromagnetic (IEMI) cyber risks impacting LiDAR systems in autonomous vehicles. The study identifies new physical attack surfaces, including the laser receiving circuit, internal monitoring sensors, and optical encoders within beam-steering modules.[123]

Bluetooth

Bluetooth is a wireless communication technology that uses radio frequencies to connect devices and share data. 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 April 2025, security researchers found that a Bluetooth Hands-Free Profile (HFP) flaw in an EV allowed attackers to remotely manipulate critical functions once within wireless range. The issue stems from a stack buffer overflow that can be triggered by sending crafted audio data to the infotainment unit over Bluetooth. After exploitation, attackers can pivot through the vehicle's cellular modem, bypass internal filtering rules, and issue commands on the CAN bus, enabling control over features such as doors, mirrors, steering, and certain safety-related systems.[124]

- In November 2025, security researchers demonstrated that Bluetooth state-machine manipulation can quietly expose devices to unauthorized access or disruption across mobile, IoT, and automotive systems. By interfering with Logical Link Control and Adaptation Protocol (L2CAP) connection steps, forcing repeated state loops, or injecting early confirmation messages, attackers can trigger hidden logic flaws that leave no logs or crashes. These protocol-level weaknesses highlight a stealthy attack surface relevant to connected vehicles, IVI units, and embedded telematics devices.[125]

Remote keyless entry systems

Modern vehicles rely on remote keyless entry systems using smart key fobs, immobilizers, and strong cryptographic mechanisms to prevent theft. However, these systems have introduced new vulnerabilities, contributing to sophisticated vehicle thefts and break-ins. Publicly available hacking tutorials and unregulated, inexpensive devices sold online have made these attacks increasingly routine. In recent years, the rapid spread of CAN injection devices and plug-and-play digital key emulators has accelerated this trend, enabling attackers with limited technical knowledge to bypass keyless systems.

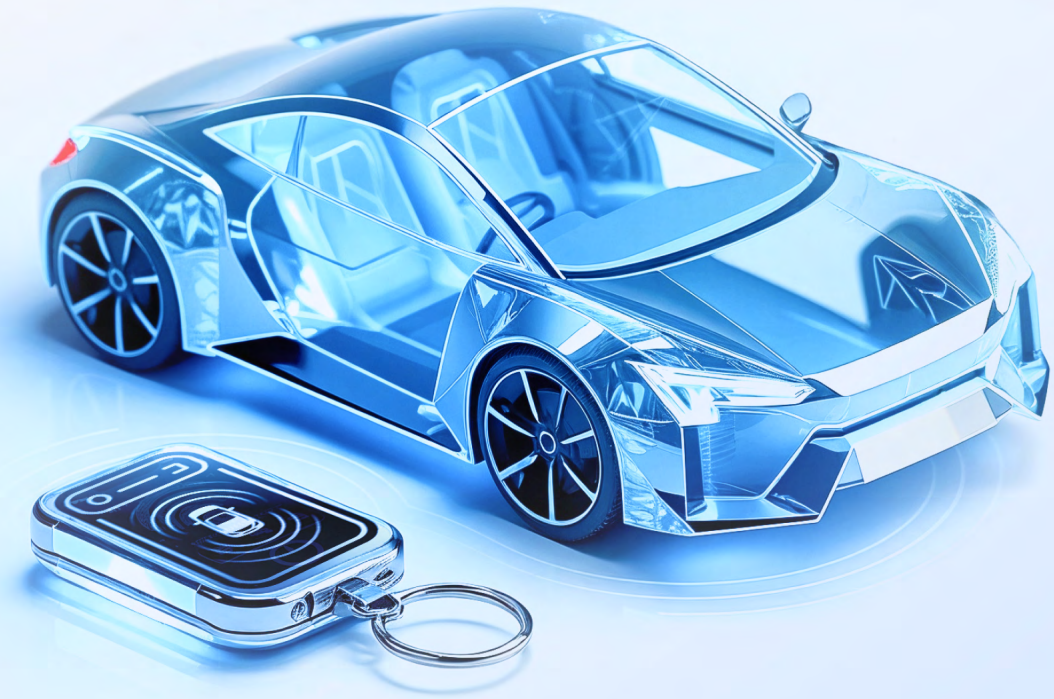
Wireless key fobs use short-range radio transmitters to communicate with vehicle receivers. This proximity-based communication can be intercepted, relayed, replayed, jammed, or spoofed, allowing attackers to manipulate the system and gain unauthorized access. **Newer smartphone-based systems utilizing BLE, Near Field Communication (NFC), and Ultra-Wideband (UWB) have further expanded the attack surface, introducing risks tied to mobile applications, signal encryption flaws, and handset-level vulnerabilities.**

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

Relay attacks using a "live" signal	Attackers intercept and extend the communication between the key fob and the vehicle, even when the fob is out of range. Radio amplifiers placed near the victim's home or vehicle bridge the signal, tricking the car into unlocking and starting.
Replay attacks using a stored signal	Attackers can capture messages exchanged between the key fob and the vehicle and store them for later use. With the captured signal, they can unlock or start the vehicle at any time.
Reprogramming key fobs	Sophisticated tools can reprogram key fob systems through the OBD port. These tools, often legitimate devices sold online to mechanics, can be misused to render the original key useless and grant full vehicle control.
Jamming communication	Attackers use radio jammers to block communication between the key fob and the vehicle. When a driver attempts to lock their vehicle, the jammer silently prevents the command from reaching the receiver, leaving the vehicle unlocked.
Impersonating the wireless key fob ECU with CAN injection	A common attack method involves CAN injection. By accessing exposed CAN wiring (e.g., via headlights) and impersonating the wireless key fob electronic control unit, attackers can inject unlock or start commands, bypassing both the key fob and the immobilizer.
Phone-as-a-Key (PaaK)	Smartphone-based digital key systems rely on BLE, NFC, and UWB. While these technologies enhance convenience, they introduce new risks, including weak signal encryption, application flaws, and mobile operating system vulnerabilities that can allow unauthorized access.

Attacks on remote keyless entry systems continued to make headlines in 2025:

- In January 2025, a technology vendor introduced a smartphone-based universal car key at CES 2025. The device used UWB technology, encrypted communications, and multi-factor authentication. However, security experts warned that it remained susceptible to relay attacks, application-level vulnerabilities, and risks associated with server-side breaches and social engineering.[126]
- In June 2025, security researchers disclosed two critical vulnerabilities affecting keyless entry systems on certain vehicle models between 2022 and 2025. These vehicles were equipped with non-original key fobs approved by the national distributor that transmit a static signal. Attackers could record and replay the signal to unlock the vehicle and, in some cases, program their own keys. No fixes were applied despite early disclosure, and similar fobs are believed to be in use across Latin America.[127]
- In July 2025, a security researcher demonstrated how RF attacks can compromise keyless entry systems in several popular vehicle models. The presentation showed how relay attacks, rolling code, brute-forcing, signal interception, and jamming can be used to bypass RF-based systems, noting similarities to physical access cards used in building security. The session highlighted long-standing weaknesses in RF communication protocols that stem from fundamental design limitations.[128]



AI introduces a new, systemic attack surface

As discussed in Chapter 1 of this report, AI is rapidly emerging as a new attack surface across many sectors, including the Automotive and Smart Mobility ecosystem. It's not only because of the expanded functionality, but also because AI holds the power to reshape how systems reason, orchestrate actions, and connect across cloud, edge, and vehicle environments.

The integration of LLMs, AI agents, and orchestration layers such as MCP introduces dynamic, context-driven behavior that is harder to predict, monitor, and secure than traditional software interfaces. This risk is no longer theoretical.

A July 2025 study demonstrated an AI-driven black-box denial-of-service attack, AutoDoS, capable of exhausting LLM resources and increasing latency by more than 250 times, highlighting how in-vehicle or cloud-based AI services could be degraded or disabled without access to model internals.[129]

In September 2025, security researchers disclosed a critical remote code execution vulnerability in an open-source MCP implementation that allowed unauthenticated attackers to trigger arbitrary code execution by sending a crafted tool definition to an LLM, illustrating how AI orchestration layers can bypass conventional API security boundaries.[130]

At the ecosystem level, in September 2025, attackers exploited a vulnerability in an AI-enabled module of a widely used enterprise platform, indirectly compromising a global OEM and proving that AI-powered third-party services can open cascading pathways into vehicle and mobility infrastructures.[131]

Together, these incidents show that AI is not just amplifying existing risks, but creating a distinct, systemic attack surface that spans software-defined vehicles, cloud backends and enterprise systems, and the broader digital supply chain.

Upstream

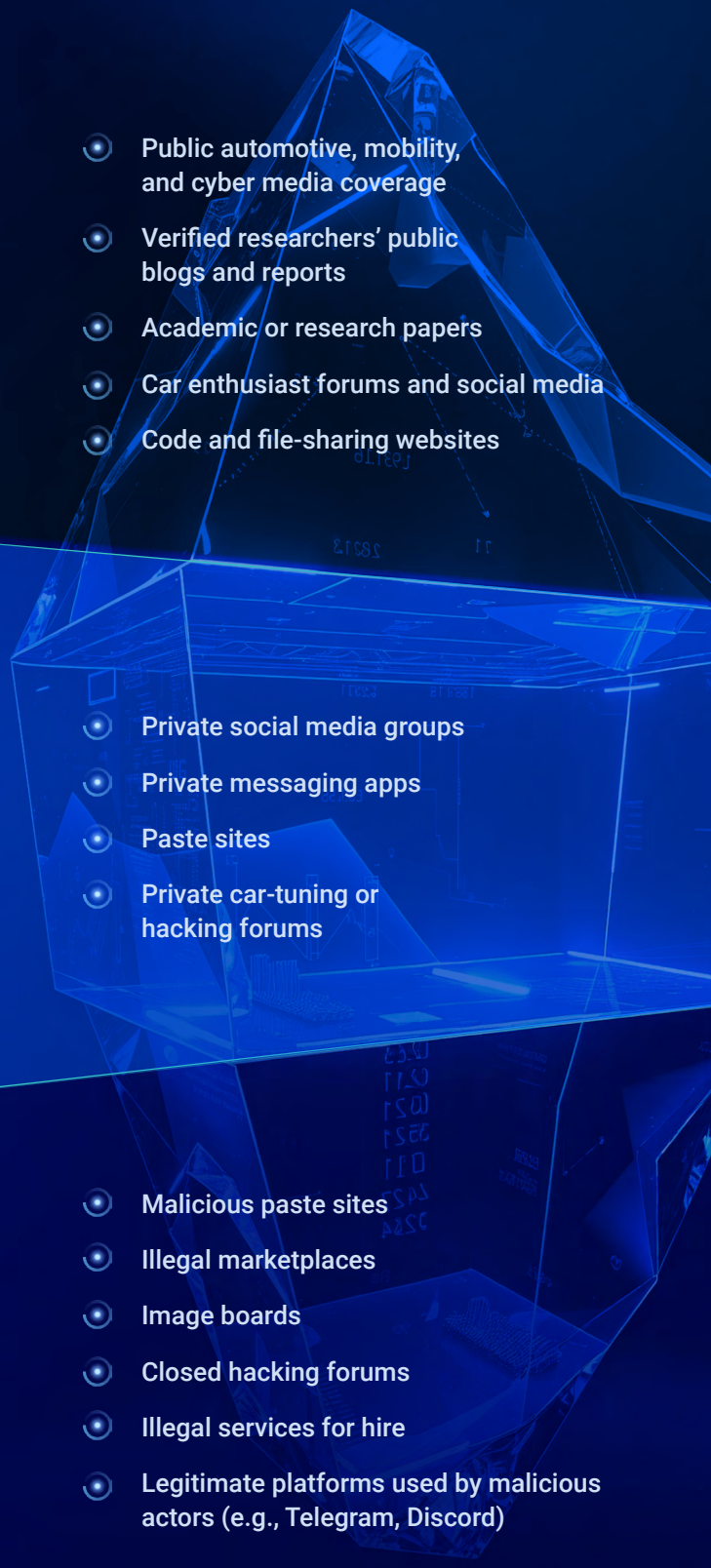
04.

THREATS FROM THE DEEP AND DARK WEB

Organized attack groups are continuously expanding activities across the Automotive industry, changing the rules of the game and demanding proactive cyber threat intelligence to mitigate risk.

What is the deep and dark web?

The internet has multiple layers, not all of which are indexed by search engines. There are three main layers: the clear, deep, and dark web. Access to each layer requires different knowledge and tools.



Clear Web

The clear web is the smallest and most familiar part of the internet.[132] It requires only a standard browser to access, and its content is fully indexed by popular search engines, making it open, searchable, and highly accessible to anyone online.

- Public automotive, mobility, and cyber media coverage
- Verified researchers' public blogs and reports
- Academic or research papers
- Car enthusiast forums and social media
- Code and file-sharing websites

Deep Web

The deep web accounts for the vast majority of online content (up to 96%) and isn't indexed by search engines.[133] Information here sits behind logins, paywalls, or restricted portals that block web crawlers. For most people, it includes subscription sites, private groups, and private business systems. For threat actors, it also includes imageboards, paste sites, and private hacking forums used to share data or techniques anonymously.

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

Dark Web

The dark web is a hidden layer of the internet where malicious activities, illicit trade, and stolen data frequently circulate. Access requires specialized tools such as the Tor browser and unique .onion URLs that are not indexed by search engines. Entry often depends on invitations or proof of expertise, and communities are tightly moderated, operating under strict anonymity and deep mistrust of outsiders.

- Malicious paste sites
- Illegal marketplaces
- Image boards
- Closed hacking forums
- Illegal services for hire
- Legitimate platforms used by malicious actors (e.g., Telegram, Discord)

To maintain anonymity, dark web hackers almost universally use a Tor browser combined with proxy servers. Many use tools like proxychains to route traffic through multiple proxies (typically 3–5), often across jurisdictions. This makes tracing the attacker's origins extremely difficult, as countries are unlikely to share security logs.

During 2025, Upstream's AutoThreat® researchers continued to expand the scope of deep and dark web threat actor mapping and analysis to include 1,996 active threat actors, nearly doubling from 1,133 in 2024.

Combined with the finding that nearly 66% of these activities could impact thousands to millions of mobility assets, this underscores the need for deep cyber threat intelligence visibility to enable proactive protection.

What occurs in the deep and dark web?

The deep and dark web host a wide range of automotive, transportation, and mobility-related content, spanning forums, marketplaces, messaging channels, and paste sites.

Some consumers turn to forums for information not provided by OEMs, often to self-repair or circumvent restrictions, which can enable system manipulation. Additionally, marketplaces are known to 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 sophisticated technology.

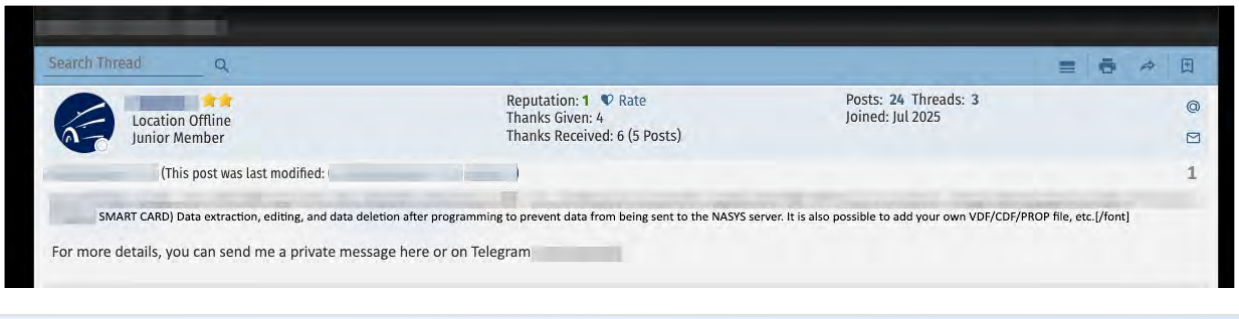
These activities can have an impact on automotive and mobility stakeholders as well as insurance companies. Tampered vehicles may report plausible but falsified telemetry. In an extreme case, threat actors can gain access to OEM or insurance company servers by reverse engineering data that's already been used to grant authorization to vehicles.

Forums

Automotive-related forums on the deep and dark web are hubs for sharing and selling illicit software, chip and engine tuning files, infotainment cracks, reverse engineering guides, and immobilizer hacks. General hacking forums also contain automotive-related threads.

These forums facilitate a continuous trade in information, tools, and manipulations. Common topics include ECU tuning, infotainment jailbreaking, source code leaks, data breaches, and car hacking tools. It is not uncommon for people to ask about self-programming their vehicles for reasons like saving money or claiming the Right to Repair. ECU remapping lessons, guides, software, and tuned file demos are readily available.

In July 2025, Upstream's AutoThreat® PRO team identified a post on a deep web automotive forum advertising an advanced diagnostic and configuration editor allegedly compatible with heavy-truck ECU programming environments. **The software, presented as an editor for secured configuration files, claims to allow users to read, modify, and delete calibration or configuration data, as well as add custom parameter files.**



Source: Upstream Security

A deep web forum post advertising an advanced diagnostic and configuration editor, offering data extraction and modification features

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.

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).

There are many automotive-related discussions and offerings in deep and dark web marketplaces:

- 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

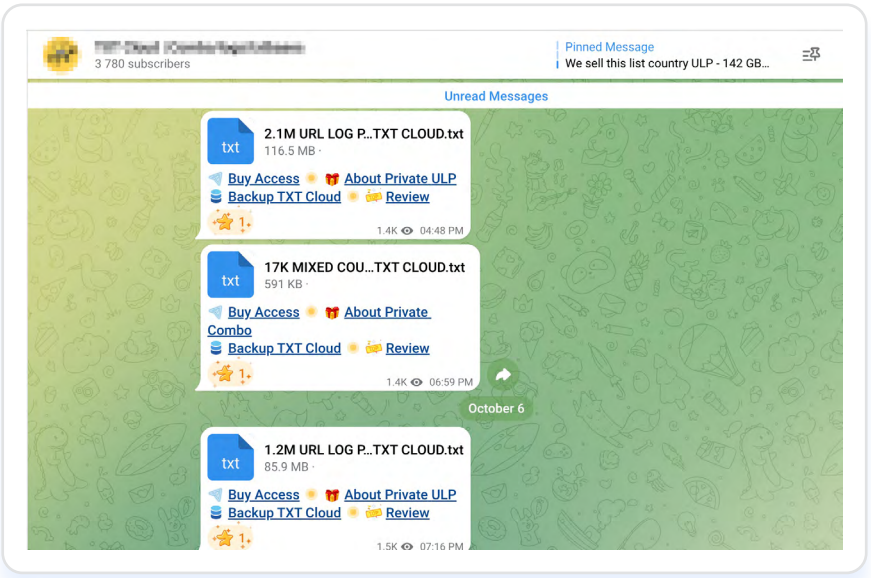
In July 2025, AutoThreat® PRO discovered dark web commercialization of a private, paid firmware fork for a popular multi-purpose hardware hacking device. **This fork restores restricted radio protocol capabilities and adds vehicle features, turning a hobbyist tool into a field-ready attack appliance.** The package is traded via invitation-only marketplaces as a ready-to-use bundle (firmware, payloads, guides), significantly lowering the skill threshold for RF/NFC/RFID vehicle attacks.

Messaging Applications

As online activities shift to mobile devices, mobile messaging applications have become increasingly popular for illicit activities.

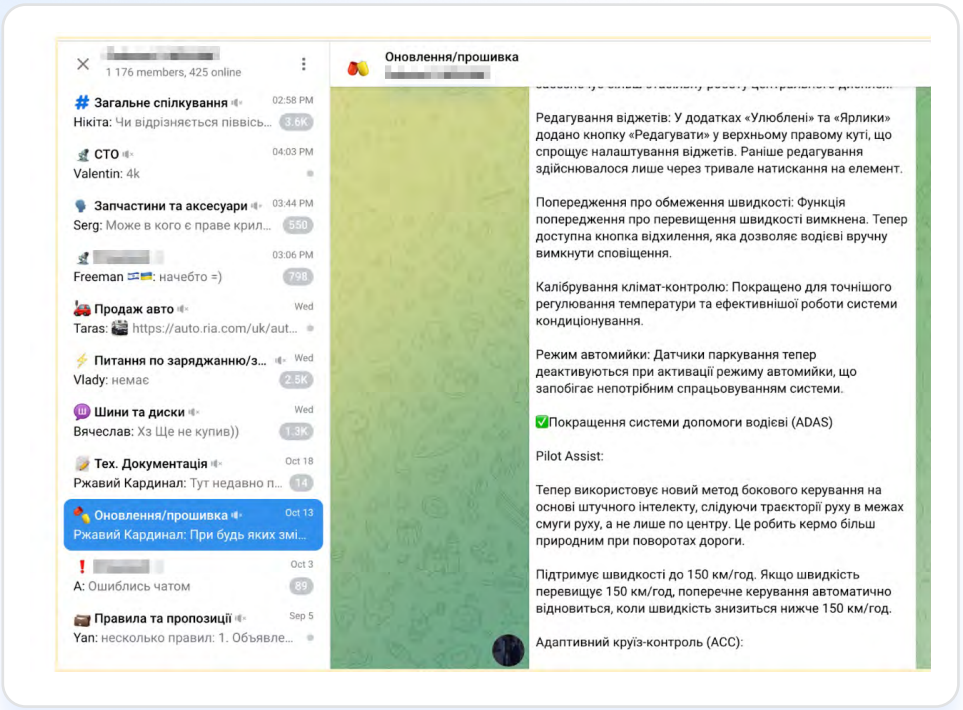
Popular messaging applications, such as Telegram, Discord, Signal, and WhatsApp, are actively being used to share hacking methods, and trade in stolen credit cards, account credentials, vulnerability exploits, leaked source codes, and malware.

In many cases, these channels have displaced traditional, harder-to-navigate dark web forums.



Example of a Telegram channel related to stolen OEM data

Source: Upstream Security



Example of a Telegram group where members discuss infotainment firmware updates, software changes and ADAS feature improvements

Source: Upstream Security

Threat actors in the deep and dark web

Security researchers (white hats)

Security researchers use their technical expertise to identify cybersecurity vulnerabilities. To be effective, they must stay up-to-date on the latest attack vectors, trends, and technologies. **Many security researchers publish their findings, which can include vulnerability exploits and vehicle toolkits, in public code repositories like GitHub. This knowledge, while intended for defense, is publicly accessible to anyone, including malicious threat actors.**

In March 2025, a security researcher documented a multi-layered effort to reverse-engineer and defeat jailbreak-detection logic in an OEM companion mobile app. The researcher unpacked the app's protected installation file and used popular tools to map out every check the app uses to detect a tampered phone (e.g., looking for specific files and running services). The researcher then showed how to hook functions, patch the binary, and re-sign it so the app would run on compromised devices. This could allow an attacker to send unauthorized commands to the vehicle's backend or request privileged features, such as enabling remote actions or changing vehicle settings.[134]

Understanding [redacted] jailbreak detection

I recently found myself looking at an [redacted] application as part of a bug bounty and figured my normal methodology of jailbreaking the device and installing some third part apps would be enough to get me started. However, it soon became apparent that I would have to dig deeper in order to get a foothold within the application. Using this popular [redacted] jailbreak script wasn't going to cut it this time.

Before I dig into what the aforementioned [redacted] script does, its worth touching on the four main methods that can be implemented in order to prevent such tampering. These are:

- File existence
- URI scheme registration
- Sandbox behavior
- Dynamic linker inspection

File Existence – When we jailbreak a device we are essentially leaving a footprint of the method used (palera1n) and any other tooling that we manually add to the device. Sadly, whilst many of these tools are helpful whilst we conduct our testing methodology. These tools however leave behind artifacts, one such example being **/Applications/Cydia.app**, as well as other binaries like **bash** and **sshd**. The presence of these files indicates a jailbroken device, therefore its not uncommon for mobile app developers to include these checks.

URI Schemes – Jailbroken devices often have the **cydia://** URI scheme registered. At this point it's worth noting that some of the packages used to create the jailbreak condition on the [redacted] device still rely on packages and dependencies that were originally built for the older package manager Cydia. As such, these packages may still reference Cydia resources even if newer package managers such as Sileo and Zebra are installed. During testing you may find that many [redacted] apps will use anti-jailbreak mechanisms which reference and search the device for these older references, which in many cases will prevent the [redacted] application from running on the jailbroken device.

A repository examining binary strings referencing jailbreak-related apps to identify how the vehicle's mobile app detects compromised devices[135]

Source: Upstream Security

Project: [redacted] Jailbreak Detection Bypass

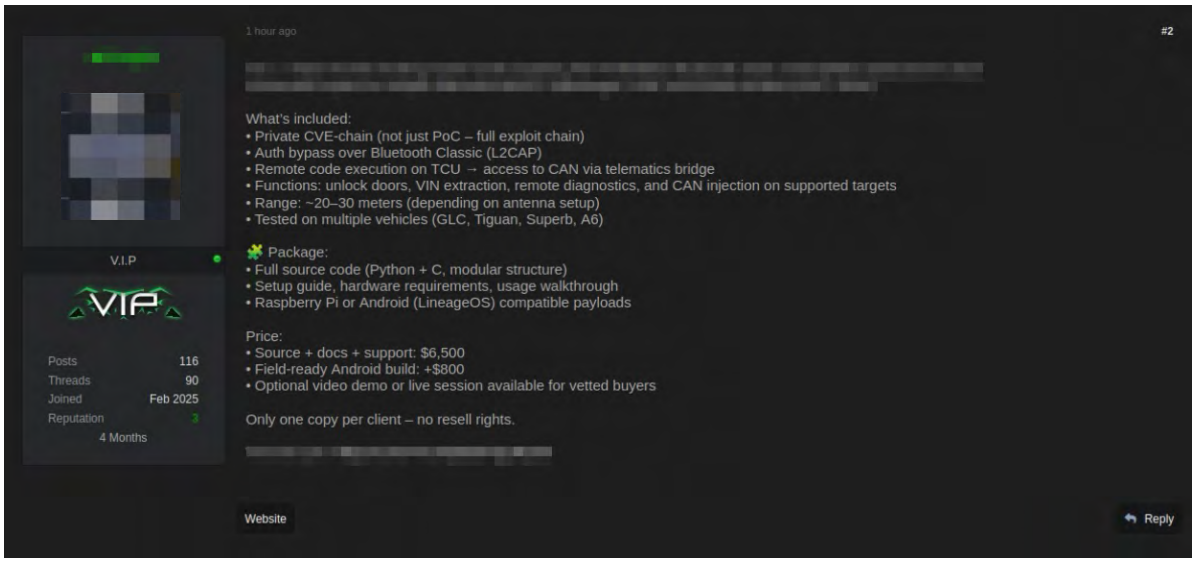
Try this code out now by running `$ frida --codeshare liangxiaoyi1024/ios-jailbreak-detection-bypass -f YOUR_BINARY`

```
if (ObjC.available) {
    var paths = [
        "/Applications/blackra1n.app",
        "/Applications/Cydia.app",
        "/Applications/FakeCarrier.app",
        "/Applications/Icy.app",
        "/Applications/IntelliScreen.app",
        "/Applications/MxTube.app",
        "/Applications/RockApp.app",
        "/Applications/SBSettings.app",
        "/Applications/WinterBoard.app",
        "/bin/bash",
        "/bin/sh",
        "/bin/su",
        "/etc/apt",
        "/etc/ssh/sshd_config",
        "/Library/MobileSubstrate/DynamicLibraries/LiveClock.plist",
        "/Library/MobileSubstrate/DynamicLibraries/Veency.plist",
        "/Library/MobileSubstrate/MobileSubstrate.dylib",
        "/pguntether",
        "/private/var/lib/cydia",
        "/private/var/mobile/Library/SBSettings/Themes",
        "/private/var/stash",
        "/private/var/tmp/cydia.log",
        "/System/Library/LaunchDaemons/com.ikey.bbot.plist",
        "/System/Library/LaunchDaemons/com.saurik.Cydia.Startup.plist",
        "/usr/bin/cycript",
        "/usr/bin/ssh",
        "/usr/bin/sshd",
        "/usr/libexec/sftp-server",
        "/usr/libexec/ssh-keysign",
        "/usr/sbin/frida-server",
        "/usr/sbin/sshd",
        "/var/cache/apt",
        "/var/lib/cydia",
        "/var/log/syslog",
        "/var/mobile/Media/.evasi0n7_installed",
        "/var/tmp/cydia.log"
    ];
    var f = Module.findExportByName("libSystem.B.dylib", "stat64");
    Interceptor.attach(f, {
        onEnter: function(args) {
            this.is_common_path = false;
            var arg = Memory.readUtf8String(args[0]);
            for (var path in paths) {
                if (arg.indexOf(paths[path]) > -1) {
                    console.log("Hooking native function stat64: " + arg);
                    this.is_common_path = true;
                    //return -1;
                }
            }
```

Malicious threat actors (black hats)

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

In July 2025, a black hat threat actor posted a field-ready exploit package on a dark web forum. It claimed to use a non-public vulnerability to enable an L2CAP authentication bypass, “one-click" remote code execution (RCE) on infotainment/TCU software, and CAN-bridge pivoting.[136] The kit was advertised to perform post-exploit actions such as remote unlocking, VIN extraction, diagnostic access, and arbitrary CAN-frame injection. Its commercial availability indicates active black-market monetization and heightens the real-world risk to any unpatched devices or supply-chain integrations.



A dark web forum post advertising the exploit package, detailing its RCE and CAN-bridge pivoting capabilities, post-exploit actions, and pricing

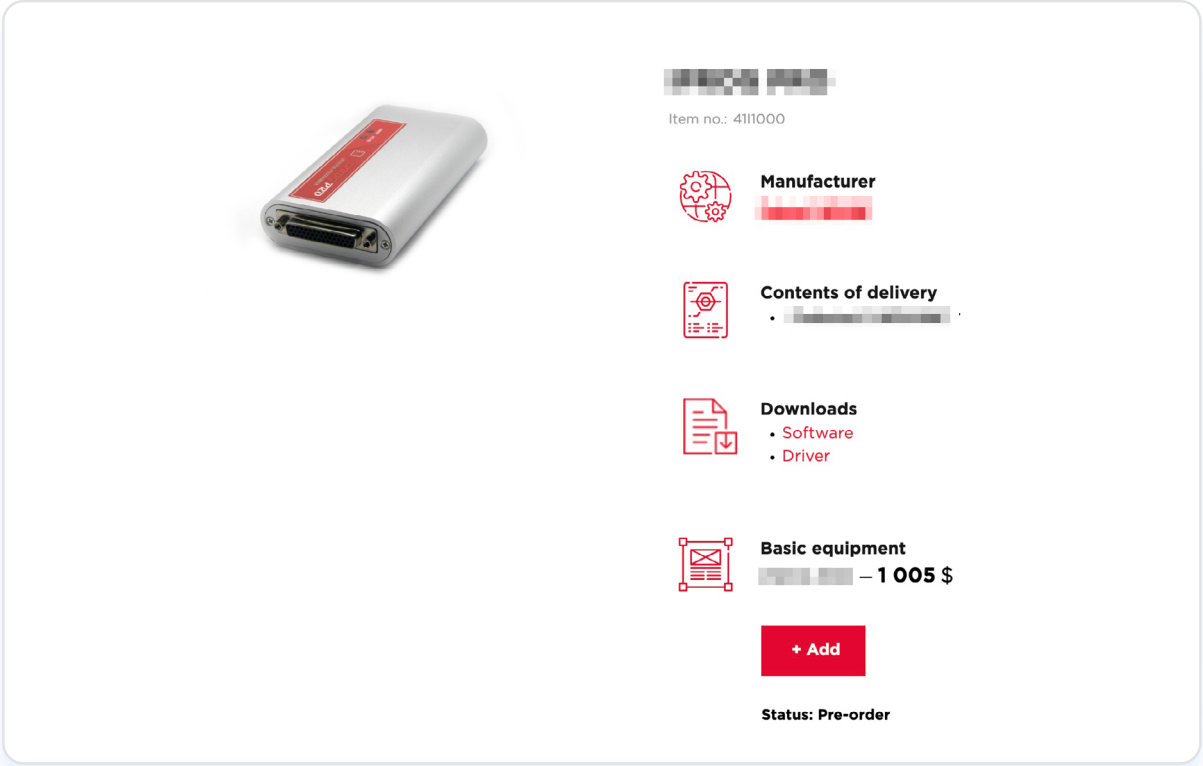
Source: Upstream Security

Fraud operators

Fraud operators typically use the deep web to buy and sell diagnostic tools, software, chip tuning services, and mileage fix services. One of the most popular services is odometer fraud (mileage fix), which involves altering a vehicle's odometer. Every year, over 450,000 vehicles are sold with false odometer readings in the US, costing buyers over $1 billion.[137] Additional reports indicate that approximately 2 million vehicles on US roads have tampered or rolled-back odometers, representing an 18% rise over the past four years.[138]

In October 2025, AutoThreat® PRO identified commercial offerings for a multifunctional programming device and scripts targeting EEPROMs (small non-volatile chips that store configuration and security data) and microcontrollers in vehicle ECUs. The toolkit enables bench- and OBD-connected access to a wide range of in-vehicle modules. Advertised capabilities included odometer read/write, EEPROM/MCU read and write, VIN rewriting, DTC read/clear, crash data (SRS) reset, and instrument-cluster mileage editing.

Such tools enable large-scale odometer fraud, undermining consumer protection and warranty processes, affecting safety assessments, and increasing regulatory and legal exposure.



Source: Upstream Security

The programmer is offered for sale on an automotive marketplace, listing its main functions, including odometer correction, EEPROM and MCU read/write operations, crash-data reset, VIN editing, and key or immobilizer operations for vehicle ECU programming

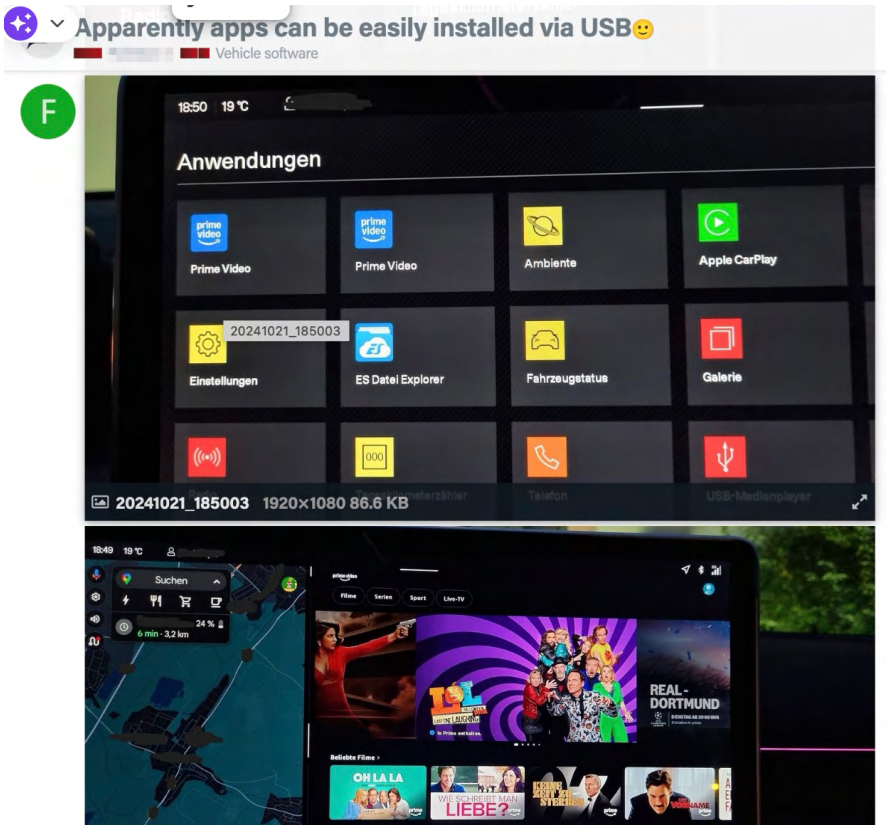
Car enthusiasts

Many car enthusiasts, people with a passion for vehicles and how they operate, are active in 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.

The information posted in forums by car enthusiasts can be problematic for two reasons. First, malicious threat actors often lurk in these forums and take advantage of any reported bugs or problems. Second, the files and links posted are untrustworthy and might contain malware, spyware, and ransomware, which could void warranties.

In August 2025, a community forum thread created by car enthusiasts documented an app sideloading demonstration on an EV Automotive OS. The discussion shows how a user enabled Developer Mode and installed APKs directly from a USB stick.[139]

The post details sideloading multiple third-party apps. The thread includes technical workflow notes, installation behavior, and troubleshooting observations, reflecting growing awareness within the owner community and suggesting the manufacturer may need to restrict or mitigate this functionality in future OTA updates.



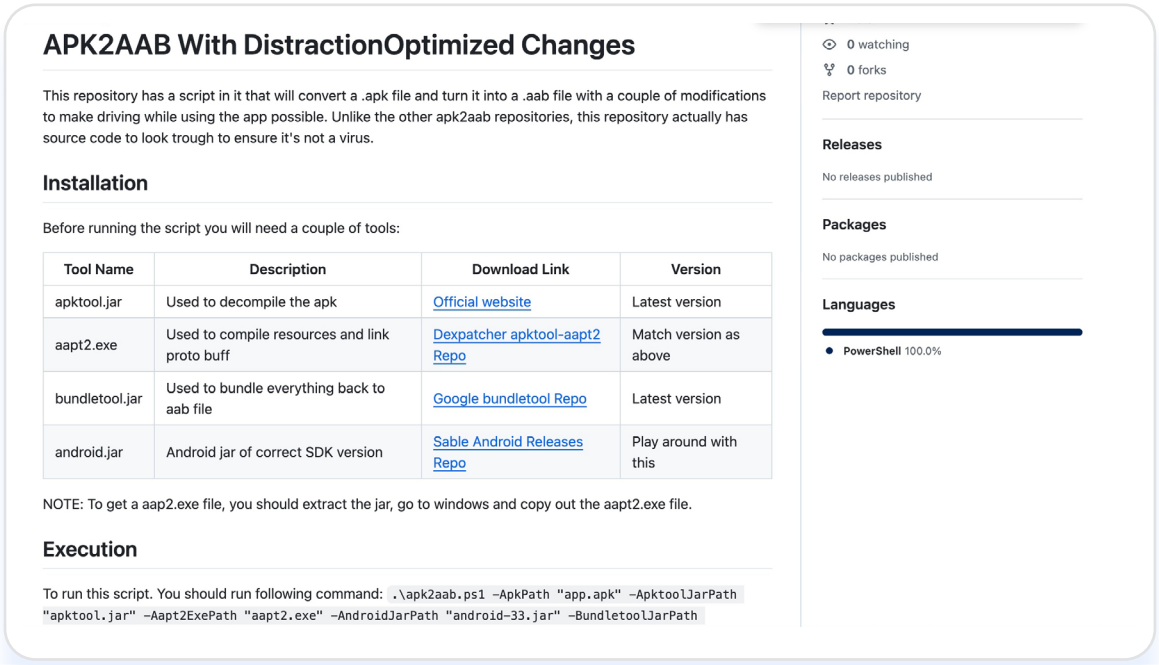
A car enthusiast forum post discussing sideloading third-party apps via USB with detailed technical notes, installation instructions, and troubleshooting

Source: Upstream Security

Gray hats blur the line between threat actors

In the increasingly software-defined Automotive and Smart Mobility ecosystem, the traditional distinction between black hats and white hats is eroding. The rise of gray hats, consumers and enthusiasts who modify vehicles or jailbreak features, illustrates this blurred line.

In June 2025, a threat actor posted a detailed method to bypass driver-safety restrictions, automating the repackaging of Android applications for installation on in-vehicle infotainment systems. This technique enables apps normally blocked while driving, undermining safety controls and increasing distracted-driving risk.[140] The procedure and tools are publicly accessible on social media to hobbyists and malicious actors alike.



APK2AAB With DistractionOptimized Changes

This repository has a script in it that will convert a .apk file and turn it into a .aab file with a couple of modifications to make driving while using the app possible. Unlike the other apk2aab repositories, this repository actually has source code to look trough to ensure it's not a virus.

Installation

Before running the script you will need a couple of tools:

Tool Name	Description	Download Link	Version
apktool.jar	Used to decompile the apk	Official website	Latest version
aapt2.exe	Used to compile resources and link proto buff	Dexpatcher apktool-aapt2 Repo	Match version as above
bundletool.jar	Used to bundle everything back to aab file	Google bundletool Repo	Latest version
android.jar	Android jar of correct SDK version	Sable Android Releases Repo	Play around with this

NOTE: To get a aap2.exe file, you should extract the jar, go to windows and copy out the aapt2.exe file.

Execution

To run this script. You should run following command: `.\apk2aab.ps1 -ApkPath "app.apk" -ApktoolJarPath "apktool.jar" -Aapt2ExePath "aapt2.exe" -AndroidJarPath "android-33.jar" -BundletoolJarPath`

0 watching
0 forks
Report repository

Releases

No releases published

Packages

No packages published

Languages

PowerShell 100.0%

Source: Upstream Security

The repository contains a script that repackages applications with modifications to enable their use while driving

Threat actors are disrupting emerging automotive and mobility revenue streams

Threat actors are increasingly exploiting opportunities to bypass premium features by jailbreaking systems, posing considerable risks to vehicle cybersecurity and data-driven revenue models.

These actors publicly advertise jailbreaks, feature activation, and regional conversion services for infotainment systems, offering language and navigation adaptation, smartphone interface activation, and full-screen infotainment. Marketed as permanent software unlocks for imported vehicles, these services are promoted across social media and automotive forums with remote installation options and competitive pricing.

Such findings highlight the growing challenge of securing connected vehicles against unauthorized modifications, firmware updates, and diagnostic access. They also underscore how aftermarket actors erode OEM visibility into feature activation, firmware integrity, and regulatory compliance.

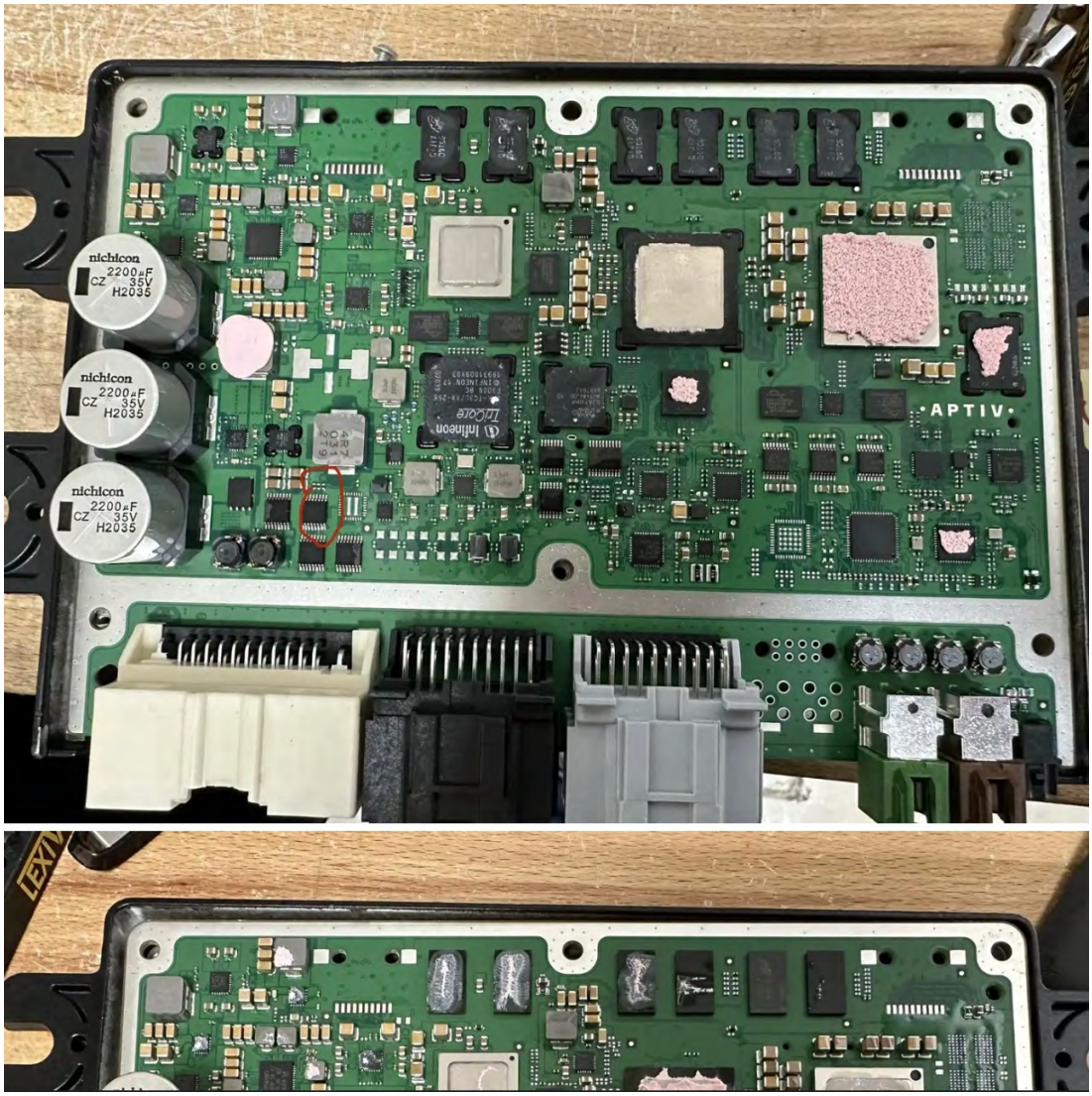
In April 2025, an Eastern European threat actor was observed selling unauthorized jailbreak and feature-unlock services for infotainment systems on regional automotive marketplaces, violating licensing terms, reducing visibility into connected-service usage, weakening software security, and causing direct revenue loss from premium feature activations.[141]

In July 2025, a deep web forum thread documented active efforts to jailbreak an infotainment platform running a popular Automotive OS.

The thread detailed hands-on techniques to remove platform restrictions, including:

- Gaining access via USB to push APKs
- Rooting via payloads and mass-storage exploits
- Using debug USB ports found behind interior panels
- Manipulating OTA updates
- Conducting hardware teardown and investigating debug or serial interfaces for escalation

The contributors also shared practical notes on sideloading third-party apps, enabling full-screen Android Auto, and recovery steps after failed modifications.



Source: Upstream Security

Hardware teardown, used to locate debug interfaces, hidden USB ports, and recovery-mode entry points leveraged in the modification process

Organized ransomware groups are systematically disrupting global automotive operations

Organized ransomware groups are increasingly targeting a broad range of automotive and mobility stakeholders, including OEMs, Tier-1 and Tier-2 suppliers, dealerships, and EV charging infrastructure, through ransomware campaigns, data breaches, and supply-chain compromises. In 2025, the Automotive ecosystem saw a sharp, sustained rise in cyberattacks, becoming one of the most targeted segments within global industrial and manufacturing verticals.

While ransomware first appeared in the automotive industry several years ago, its impact intensified sharply in 2025. Well-established groups expanded into the automotive supply chain, systematically targeting engineering and production environments.

Researchers documented an increase from 49 active ransomware groups in 2024 to 77 in Q3 2025, illustrating the rapid expansion of threat activity. One of the most aggressive groups showed a 318% year-over-year surge, claiming 234 victims in Q3 2025. Their campaigns typically:

- Target Tier-1 and Tier-2 suppliers developing embedded software, braking, steering, and sensor systems.
- Exploit remote-access vectors to move laterally within shared IT/OT ecosystems.
- Exfiltrate data before deploying encryption to maximize pressure on victims.
- Leak proprietary firmware, design blueprints, and supplier contracts on extortion portals.

Automotive and Smart Mobility ransom attacks more than doubled in 2025

According to Upstream Security's AutoThreat® PRO, ransomware incidents impacting the Automotive and Smart Mobility ecosystem increased dramatically by 100% in 2025, compared to 2024, rising from 108 to 218 incidents.[144]

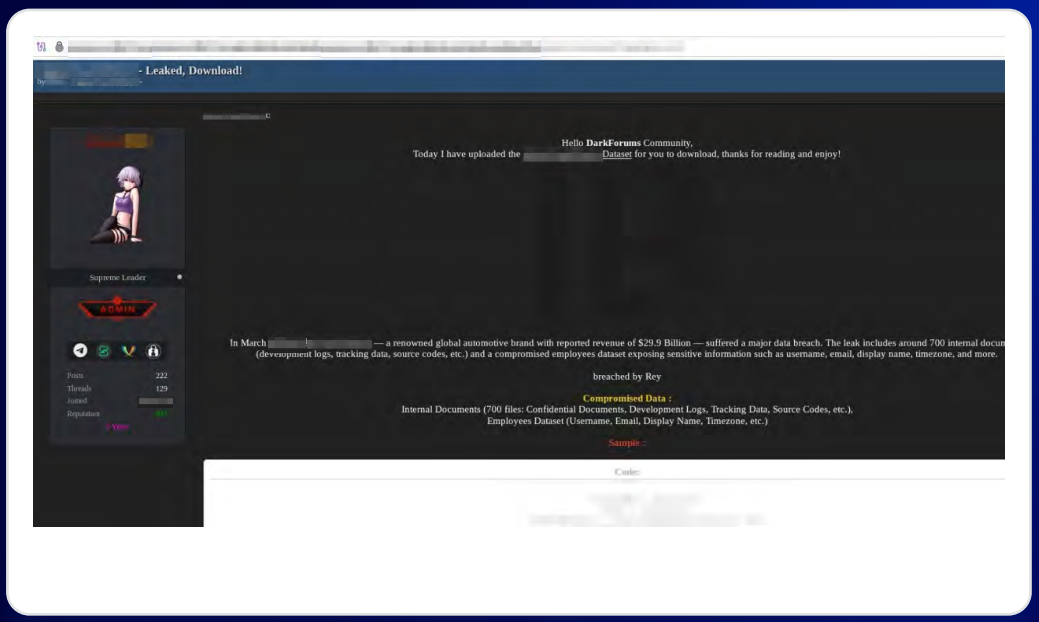
The surge seen throughout 2025 marks a turning point: ransomware, data theft, and supply-chain disruption have converged into systemic threats. This escalation reflects the rise and consolidation of large, organized groups that now dominate the ransomware ecosystem. Operating under the Ransomware-as-a-Service (RaaS) model, core developers supply exploit kits, negotiation platforms, and leak sites, while affiliates conduct network intrusions for profit sharing. Affiliates typically gain access via spear-phishing, credential theft, exploitation of VPN or RDP endpoints, or compromise of third-party suppliers. Once inside, they move laterally across engineering servers, ERP environments, and production networks, exfiltrating sensitive data before encrypting systems to halt production.

This double-extortion strategy, combining data theft with encryption, has proven especially devastating for OEMs reliant on just-in-time production and globally integrated IT/OT systems. A single supplier compromise can cascade across multiple OEM networks. To maximize leverage, threat actors leak CAD designs, ECU firmware, and supplier contracts on dark web extortion portals, coercing multimillion-dollar ransoms.

These trends underscore the urgent need for network segmentation, supplier-side threat monitoring, and coordinated incident-response frameworks to counteract the organized groups shaping the modern ransomware economy.

In August 2025, a European OEM suffered a crippling ransomware attack that disrupted global operations and halted production for nearly a month across facilities in the UK, Slovakia, China, and India. The campaign combined ransomware deployment with extensive data theft, making it one of the most severe cyber incidents to impact an automotive manufacturer in recent years. The attackers exfiltrated internal code repositories, debug logs, and enterprise data before encrypting systems, forcing the company to shut down critical IT infrastructure and delay vehicle registrations. Technical analysis confirmed a double-extortion operation leveraging stolen credentials, social-engineering-based MFA bypasses, and misconfigured enterprise applications.[145]

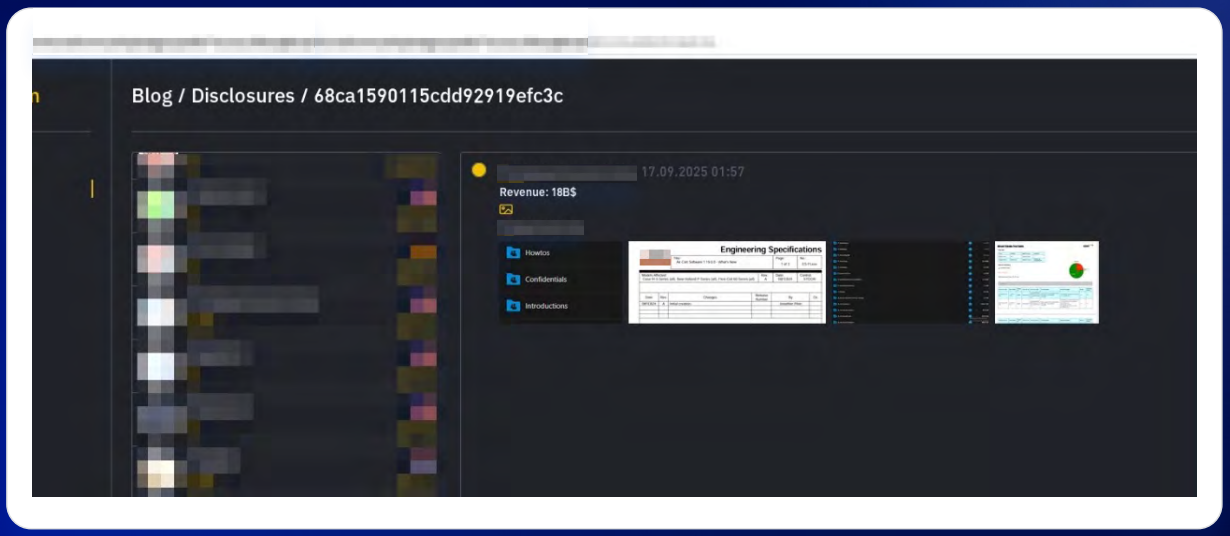
The breach also revealed how ransomware operations are amplified through dark web ecosystems. Following the initial intrusion, the threat actor released the stolen OEM dataset, including development logs, source code, and employee credentials, on a Tor-hidden dark web site. **The post, shared from an administrator account, made the data publicly downloadable, turning the incident from a contained corporate compromise into a full-scale underground distribution.** The dataset was later mirrored across Telegram channels and dark web leak aggregators, enabling other threat actors to reuse credentials and internal documentation for follow-on intrusions.



Dark web forum post publicly releasing a stolen OEM dataset containing internal documents, source code, and employee information

Source: Upstream Security

In September 2025, a multi-national industrial equipment manufacturer suffered a ransomware attack attributed to a prominent group that claimed responsibility for exfiltrating roughly 2TB of sensitive corporate data. The attackers published proof of the breach on their darknet leak site, sharing screenshots of internal directories, engineering files, and confidential documents.[146]



Source: Upstream Security

The ransom group's dark web leak-site post claiming the theft of 2TB of data from an industrial manufacturer

These incidents reflect a broader escalation of ransomware targeting automotive OEMs and Tier-1 suppliers in 2025, with attackers now pursuing operational disruption rather than simple data theft. Interconnected manufacturing networks, remote-access dependencies, and distributed IT operations have amplified attack impact, forcing global automotive stakeholders into phased recoveries. This convergence of ransomware, supply-chain compromise, and connected-vehicle data exposure underscores the urgent need for proactive, intelligence-driven defense strategies across the Automotive ecosystem.

A consistent threat landscape with rising high-impact activity

During 2025, Upstream monitored 1,871 active threat actors, continuing a rapid expansion from 1,133 in 2024 and 300 in 2023. This steady rise in actors targeting the Automotive and Smart Mobility ecosystem is continually introducing new threats and underscores the need for a proactive, coordinated defense approach across the entire supply chain.

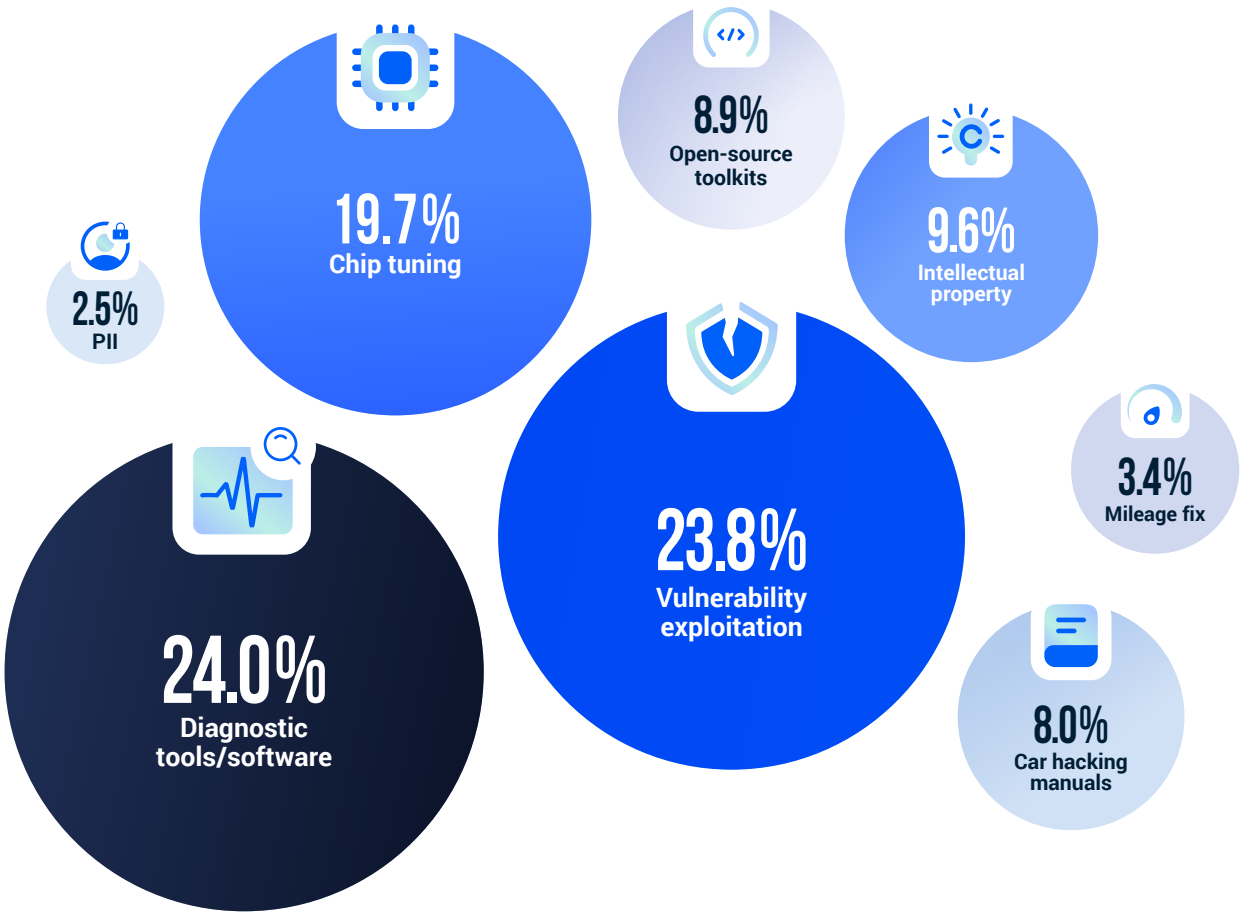
Activities consistently concentrated around specific interests, including diagnostic tools and software (24.0%), vulnerability exploitation (23.8%), and chip tuning (19.7%). Together, these categories represent nearly 68% of all deep and dark web activity.

Upstream monitored nearly

2,000

threat actors in 2025

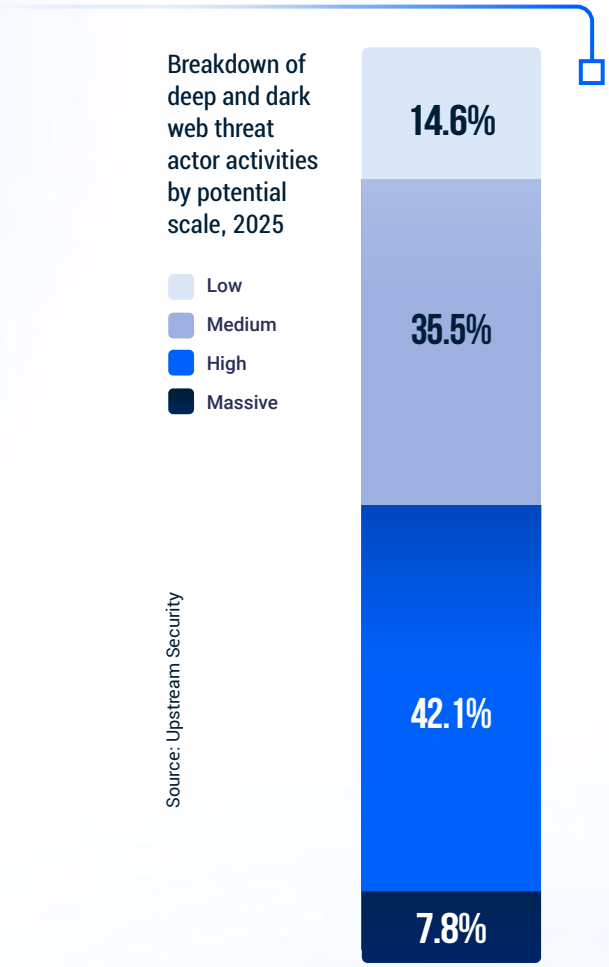
Breakdown of deep and dark web threat actor activities by areas of interest, 2025



Source: Upstream Security

Analysis of 2025 threat actor activities showed a clear shift toward more consequential activity. High-impact activity rose to 42.1%, with massive-impact activity adding another 7.8%. **Combined high- and massive-impact activity now accounts for nearly 50% of all deep and dark web activity, up from 43.1% in 2024, reflecting a significant increase in scalable, high-damage operations.** Medium-impact activity remained steady at 35.5%, while low-impact activity fell from 23.5% to 14.6%.

This rise in high-impact and massive-impact activity mirrors the expansion of large, organized threat groups described earlier, creating a landscape that, while structurally familiar, is becoming significantly more destructive in its operational consequences.

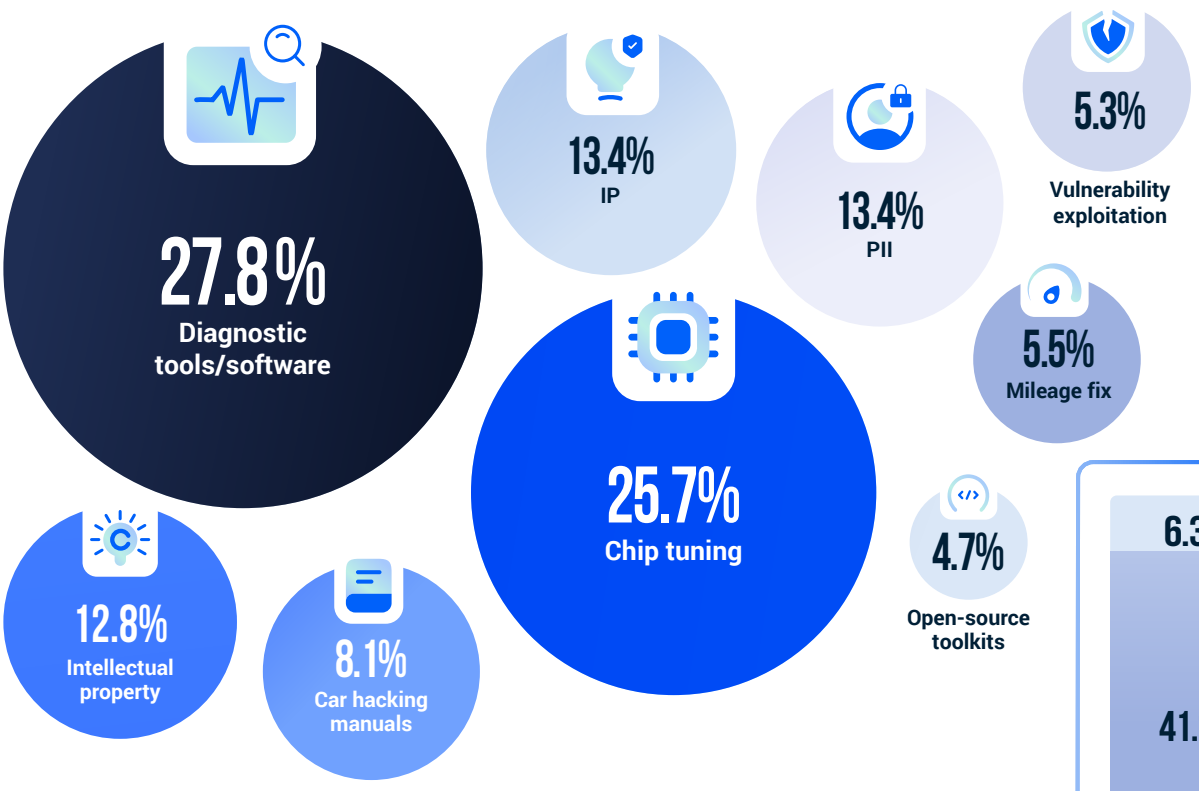


Spotlight on malicious threat actors: fraud operators and black hats

In 2025, 38.9% of all monitored threat actors were fraud operators (including threat actors who are focused on chip tuning), while black hat actors accounted for 7.1%. **Combined, these malicious subgroups represent 46.0% of all threat actors, up from 34.2% in 2024, reinforcing their central role in deep and dark web malicious activity.**

Fraud operators and black hats continued to mirror the broader landscape with stable, repeatable activity patterns. These priorities remain virtually unchanged year over year, underscoring persistent, well-defined malicious objectives.

Black hat and fraud operator activities by area of interest, 2025



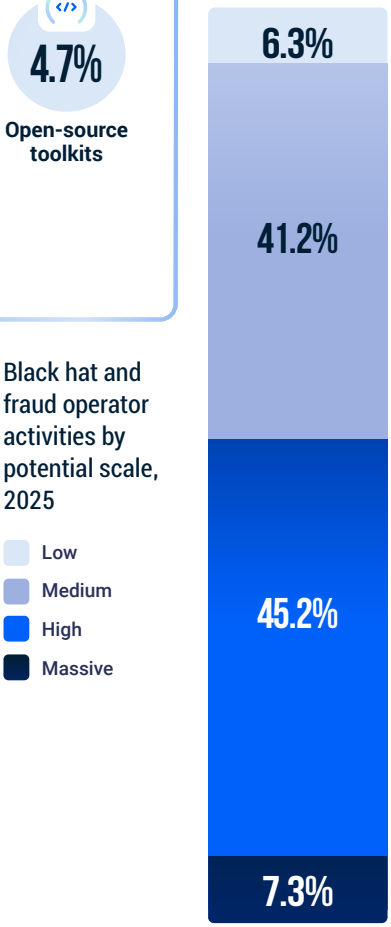
Source: Upstream Security

Fraud operators and black hats maintained an even more severe impact profile than the overall threat landscape.

High-impact activity accounted for 45.2%, with massive-impact activity contributing another 7.3%. **Combined, 52.5% of their operations fell into high- or massive -impact tiers, surpassing the already elevated 49.9% seen across all actors.** Medium-impact activities accounted for 41.2%, while low-impact activities remained minimal at 6.3%.

This concentration of high-severity activity underscores why these subgroups remain the most consequential threat actors on the deep and dark web.

Black hat and fraud operator activities by potential scale, 2025



Source: Upstream Security

Proactive cyber defense is now essential amid rising deep and dark web threats

Data sharing on the deep and dark web has continued to dramatically increase during 2025, with automotive-related cybersecurity vulnerabilities, data breaches of sensitive information, and other cyber threats regularly published and discussed. Alongside this surge in organized threat actors groups activities, AutoThreat® PRO analysts identified a growing trend of large-scale ransomware operations directly targeting automotive OEMs, Tier-1 and Tier-2 suppliers, marking a shift from isolated attacks to deliberate, coordinated campaigns aimed at disrupting manufacturing and supply-chain operations.

Threat actors are increasingly exchanging stolen engineering data, source code, and credentials linked to connected vehicle platforms and production systems, amplifying the potential for coordinated extortion and operational shutdowns.

Continuous monitoring, dark web intelligence collection, and automotive-specific expertise remain essential to identify early indicators of compromise and mitigate these expanding ransomware and data-leak risks.

These areas of the internet must be monitored by stakeholders to avoid serious security gaps. To achieve effective cybersecurity protections, organizations and products must know when and in what context they are mentioned, both publicly and secretively. UNECE WP.29 R155, ISO/SAE 21434, CRA, NHTSA guidelines, and Chinese regulations require cyber threat intelligence and vulnerability monitoring, with deep and dark web monitoring as an integral component.

Organizations can improve detection and reduce the mitigation time between a discovered vulnerability or security breach, and the time this information becomes widely known by continuously monitoring the deep and dark web. They can also take proactive measures, such as deploying software patches or changing relevant configurations. It's important to minimize the window of opportunity criminals have to copy and sell the breached data, and provide early warning to automotive stakeholders, employees, key executives, and customers of potential exploitation.

Traditional IT threat intelligence offerings lack domain expertise in the connected vehicles ecosystem, which presents many challenges for stakeholders.

Upstream's AutoThreat® PRO provides a comprehensive and continuously updated intelligence capability purpose-built for the mobility domain. Leveraging extensive data collection across open, deep, and dark web sources, the platform delivers multi-layered visibility into vulnerabilities, exploits, and threat actor activity spanning on-board systems, off-board infrastructure, and third-party integrations. Through its integrated threat actor mapping and correlation with frameworks such as MITRE,[147] R155, and Auto-ISAC's Automotive Threat Matrix,[148] AutoThreat® PRO enables precise contextualization of emerging risks across the connected mobility supply chain.

Beyond passive monitoring, AutoThreat® PRO incorporates active threat actor engagement and curated human intelligence to expose adversarial motivations, capabilities, and tactics relevant to the Automotive ecosystem. This analyst-driven approach transforms intelligence into operational advantage, facilitating early detection, targeted mitigation, and continuous risk assessment.

Armed with actionable cyber threat intelligence, automotive and mobility stakeholders can strengthen resilience, accelerate mitigation, and prevent the next major cyber incident before it occurs.

Upstream

05.

THE REGULATORY REALITY

New, overlapping mandates for AI, digital products, and critical infrastructure demand a continuous, full-lifecycle approach to compliance.

Note: *This chapter provides a high-level overview of regulatory updates and trends. For comprehensive legal or compliance analysis, please consult dedicated sources.*

AI compliance for high-risk systems is now mature

AI continued to profoundly reshape the Automotive industry during 2025, powering innovations from autonomous driving to connected in-car systems. Major automotive OEMs and tech companies are heavily investing in automotive AI to improve safety, efficiency, and user experience.[149] Market analysis estimated the global Automotive AI market at roughly $5 billion in 2025, with projections of rapid growth toward the 2030s, highlighting AI as a core enabler of software-defined, autonomous vehicles, and physical AI.[150]

Investment and experimentation continued to accelerate in 2025. McKinsey's 2025 global AI survey reports that AI use has broadened across industries, including Automotive, but many organizations still struggle to scale pilots into real impact.[151] Major OEMs continue to commit large sums. For example, **Volkswagen announced up to €1 billion in AI investments through 2030, targeting vehicle development, industrial efficiency, and IT. Bosch plans an additional €2.5 billion in AI by 2027, including for autonomous driving and manufacturing.**[152]

However, challenges to widespread adoption are more evident in 2025 than they were in 2024. Skill shortages in safety-critical AI, unresolved ethical questions, data-protection constraints, cybersecurity risks, and integration issues will slow down real-world deployment.[153]

The EU Artificial Intelligence Act

The EU Artificial Intelligence Act (AI Act) came into force in August 2024 and progressed toward practical implementation in 2025, with several sections coming into effect in February and August 2025.[154] The AI Act categorizes AI systems based on 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, which is expected to enter into force in August 2026, mandates that these systems be designed and developed to ensure appropriate levels of accuracy, robustness, and cybersecurity, while maintaining consistent performance throughout their lifecycle.[155]

The objective of these regulations is to foster innovation by building market trust, rather than stifling development. Enforcement tools are strong: serious infringements incur fines of up to €35 million or 7% of global annual turnover, along with possible product withdrawals or market bans.[156]

Consequently, AI compliance has become a board-level risk for globally active OEMs and Tier-1 suppliers, alongside traditional product-safety and emissions regulation.

In this risk-based framework, most autonomous driving and safety-critical automotive AI systems are classified as high-risk. Guidance and sector analyses for 2025 stress that AI used as a safety component, such as perception, motion-planning, or control modules in autonomous trucks or robotaxis, falls under the high-risk regime. This classification imposes strict requirements on risk management, data governance, robustness, and human oversight.[157] Non-EU companies placing such systems on the EU market, or whose AI outputs are used in the EU, must also comply, giving the Act global reach.[158]

The Act explicitly interfaces with existing automotive and product-safety regulations. Amendments adopted in the final text align the AI Act with the Type-Approval Framework Regulation and the General Safety Regulation, necessitating that AI systems used as safety components in vehicles satisfy both traditional type-approval and high-risk AI requirements. In practice, future technical regulations and standards for software-defined vehicles will embed AI-specific obligations, documentation, testing, monitoring, and incident reporting into the type-approval process.[159]

AI remains a core driver and enabler of autonomous-driving innovation. Though the AI Act does not apply directly to vehicles, OEMs and, more specifically, autonomous technology providers that heavily leverage AI may face new compliance obligations tied to revised Type-Approval Framework Regulation (TAFR) standards when they become available. Given AI's importance for autonomous vehicles (AVs), this has the potential to significantly impact the Automotive industry and the development of AVs.[160]

The EU AI Act adds a further layer of complexity by interacting with existing automotive regulations, requiring organizations to manage skills development, ethical concerns, data privacy, and regulatory compliance in parallel when planning long-term, AI-driven strategies.

ISO/IEC 42001 offers an implementation framework for the AI Act

Published in 2023, ISO/IEC 42001 has emerged as the first globally recognized management system standard for AI.[161] It provides a structured governance framework that helps organizations operationalize responsible AI principles through policies, controls, and lifecycle processes covering design, development, deployment, and monitoring. The standard introduces requirements for risk assessment, transparency, data and model quality management, incident response, and continuous improvement, creating a cohesive AI management system comparable in structure to ISO 9001[162] and ISO/IEC 27001.[163]

ISO/IEC 42001 was designed to help organizations demonstrate trustworthy AI practices and support conformity with emerging AI regulations, and plays a direct role in supporting implementation of the EU AI Act. The standard also supports compliance with other relevant global regulations that increasingly influence automotive AI development. The US NIST AI Risk Management Framework,[164] now referenced across multiple federal agency guidance documents, aligns conceptually with ISO/IEC 42001 on lifecycle risk controls and organizational governance. Japan's 2024 AI Safety Guidelines similarly encourage organizations to adopt structured AI management systems with traceability, robustness evaluations, and human oversight mechanisms.[165]

For OEMs and suppliers operating across multiple regulatory jurisdictions, ISO/IEC 42001 provides a unifying governance layer that reduces fragmentation and supports coherent, cross-market compliance strategies. It also helps centralize oversight across diverse AI initiatives such as perception models, predictive maintenance, in-vehicle assistants, and manufacturing automation. This consistency allows organizations to scale AI programs more efficiently, align internal engineering and governance functions, and prepare for converging regulatory expectations.

UNECE WP.29 R155 and ISO/SAE 21434 reach critical enforcement

The implementation of UNECE WP. 29 R155 (Cybersecurity Management System) and R156 (Software Update Management System) reached a consolidation phase as OEMs, suppliers, and authorities continued full-scale audits and certification. Following the July 2024 milestone, both regulations now apply to all new vehicles in production, marking the completion of the second rollout stage.

In 2025, R155 and R156 continued to serve as the regulatory basis for type approval across UNECE Contracting Parties such as the EU, Japan, and South Korea, with national authorities maintaining enforcement activities. **The standards are increasingly viewed as the baseline for global type approval, requiring every manufacturer to operate a certified CSMS and a SUMS, supported by lifecycle engineering processes defined by ISO/SAE 21434 and ISO 24089.**[166]

The scope of vehicle categories continues to expand. In 2025, UNECE WP.29 confirmed the adoption of the 01-series amendment to R155, extending the cybersecurity framework to Category L vehicles (two- and three-wheelers and quadricycles). Type-approval obligations for these vehicles are scheduled to become mandatory from July 2029.[167]

Together, R155, R156, and ISO/SAE 21434 form a unified regulatory–technical ecosystem ensuring that vehicle cybersecurity is engineered, audited, and monitored consistently worldwide.

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

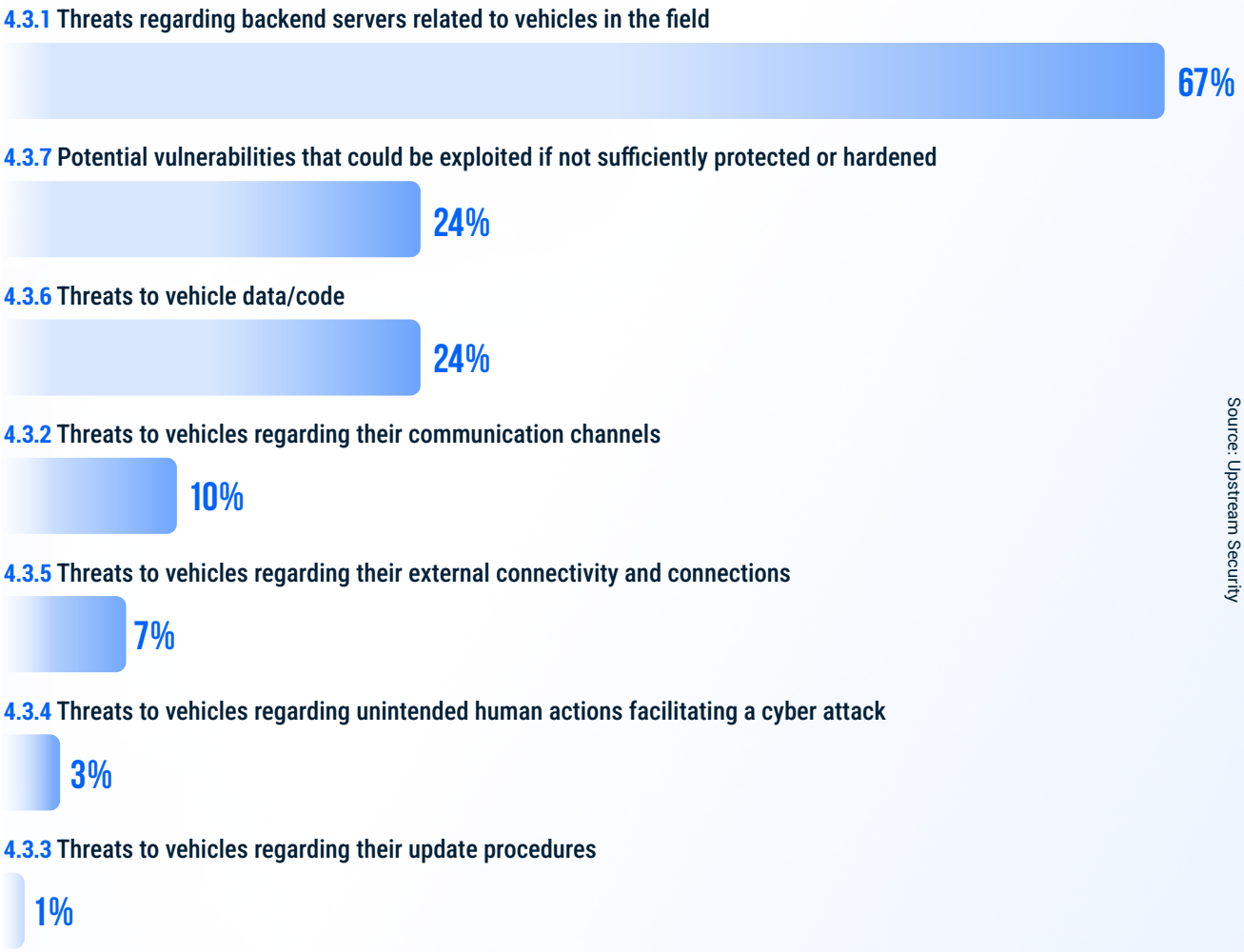
Vehicle Category	Definition	Applicable Regulation(s)	2025 Status
L (all)	Vehicles with fewer than four wheels (e.g., motorcycles, scooters, quadricycles).	R155	Amendment 01 was adopted in June 2024 and will be mandatory starting July 2029 for CSMS certification.
M	Passenger vehicles (≥ 4 wheels – carrying passengers).	R155 & R156	Fully enforced from July 2024 for all new vehicles.
N	Goods vehicles (≥ 4 wheels).	R155 & R156	Fully enforced since July 2024.
O	Trailers with electronic control units (ECUs).	R155 & R156	Compliance required for new approvals from July 2024.
R	Agricultural trailers.	R156	Guidance in preparation for 2026 implementation.
S	Interchangeable towed agricultural/forestry equipment.	R156	Covered by national type approval schemes aligned with the UNECE framework.
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	Optional applicability under R156 when software-update ECUs are present.[168]

Vehicles are regulated under R155,[169] R156[170], or both, depending on category classification.

Does R155 align with threats?

Upstream's research team analyzed publicly reported automotive cyber incidents that occurred in 2025, and correlated them to the seven threat categories presented in Annex 5 of R155.

2025 Cyber incidents categorized by R155 threats & vulnerabilities



Source: Upstream Security

The impact of WP.29 on the Automotive industry

In 2025, the continued enforcement of R155 and R156 has strengthened the global baseline for vehicle cybersecurity. Together with ISO/SAE 21434, these frameworks ensure a consistent level of protection for consumers while promoting harmonized terminology, risk criteria, and lifecycle requirements across the Automotive ecosystem.

ISO/SAE 21434 builds on ISO 26262[171] and establishes a security-by-design framework across concept, development, production, operation, and decommissioning. It sets out requirements for threat analysis, risk assessment, technical controls, and supplier assurance so that cybersecurity is addressed consistently throughout the vehicle lifecycle.

R155 requires OEMs to operate a verifiable CSMS and to maintain continuous Threat Analysis and Risk Assessment (TARA) processes. As vehicles become increasingly software-defined, each update or connectivity change can alter the attack surface, triggering reassessment and documented mitigation.

Although R155 applies directly to OEMs, its governance extends throughout the entire value chain, requiring Tier-1 and Tier-2 suppliers to demonstrate conformity with CSMS principles.

Following the second milestone in July 2024, all new vehicles (in the relevant categories) now fall under the scope of R155, making 2025 the first full production year where cybersecurity compliance is mandatory at type approval level in member countries. OEMs are therefore deepening their collaboration with suppliers and cybersecurity partners to align engineering practices, certification programs, and audit procedures.

The European Automobile Manufacturers' Association (ACEA), the European Association of Automotive Suppliers (CLEPA), and Auto-ISAC Europe continue to operate their joint European information-sharing platform, originally launched in 2022, to support coordinated vulnerability disclosure and threat-intelligence exchange among manufacturers and suppliers.[172]

Together, R155, R156 and ISO/SAE 21434 have become the cornerstone of global vehicle cybersecurity. They establish a single, auditable framework that connects regulation, engineering, and operational governance, ensuring that cybersecurity is treated not as a compliance exercise but as a core discipline shaping every phase of modern vehicle development.

ISO/SAE 21434 creates the foundation for continuous CSMS audits

ISO/SAE 21434 remains the engineering foundation of automotive cybersecurity,[173] defining how risks are assessed, managed, and verified throughout the product lifecycle. It complements R155, which governs the organizational and regulatory framework for type approval and post-market monitoring. Together, they establish the two-tier global structure for vehicle cybersecurity:

- **R155** – The compliance layer, requiring a CSMS.
- **ISO/SAE 21434** – The engineering layer, guiding design, validation, and operations.

During 2025, manufacturers continued mapping their TARA and verification/validation (V&V) evidence from ISO/SAE 21434 into CSMS audit frameworks under R155. This integration ensures that cybersecurity is verifiable not only during development but throughout production, maintenance, and decommissioning.

Recent 2025 industry reports highlight growing attention to software supply-chain transparency and third-party risk. This trend expands ISO/SAE 21434's application beyond vehicle-level engineering to cover suppliers of embedded modules, backend platforms, and over-the-air (OTA) services.[174] In post-production, OEMs increasingly operate vehicle Security Operations Centers (vSOCs) responsible for threat detection, triage, and incident response. These teams use telemetry from ECUs, in-vehicle systems, and cloud services to demonstrate compliance with R155's continuous monitoring obligations while feeding risk re-assessment under ISO/SAE 21434.

Summary of the impact of WP.29 and ISO/SAE 21434:

Standard	Primary Focus	Lifecycle Coverage	Recent Updates and Implementation
ISO/ SAE 21434	Engineering cybersecurity framework covering full vehicle lifecycle, including asset identification, TARA, design controls, supplier oversight, validation, production, operation, and decommissioning.	Full vehicle lifecycle	• Lifecycle cybersecurity obligations remain central to CSMS audits. • Traceability from TARA to requirements and V&V continues to be required.[175]
R155 (CSMS)	Organizational governance and regulatory oversight for type approvals, including competence, supplier management, post-market surveillance, and auditability.	Full vehicle lifecycle	R155 guidance reaffirmed continuous fleet-monitoring requirements, mandatory event-logging, and long-term cybersecurity-evidence retention for CSMS audits.[176]
R156 (SUMS)	Secure, auditable software update management framework ensuring safety, authenticity, rollback, and documentation controls for OTA and workshop updates.	Operations and maintenance	OEMs advanced SUMS alignment and adopted automated integrity-verification and validation measures for OTA and workshop update packages.[177]

Linking ISO 26262 with cyber risk management

ISO 26262 serves as the foundational functional safety standard for road vehicles.[178] It focuses on preventing hazards caused by electrical or electronic system failures, and establishes a structured approach for identifying safety goals, defining Automotive Safety Integrity Levels (ASILs), and validating that systems perform safely under both normal and fault conditions.

As automotive platforms become more software-defined and more connected, the relationship between functional safety and cybersecurity grows increasingly interdependent. Safety assumptions made under ISO 26262 can be undermined if a cyber vulnerability affects a safety-critical subsystem, which means safety and cybersecurity risks must be analyzed together to maintain system integrity.[179]
Both ISO/SAE 21434 and ISO 26262 standards share similar lifecycle structures, documentation expectations, and risk-driven engineering workflows. ISO 26262 centers on fault-based hazards, while ISO/SAE 21434 addresses threat-based risks, and both require systematic identification, evaluation and mitigation processes.

This alignment allows organizations to integrate safety and cybersecurity activities into a unified assurance strategy.

Coordinated application of ISO 26262 and ISO/SAE 21434 is expected to reduce overall system risk as the two frameworks reinforce one another. Safety engineering benefits from stronger assumptions about system trustworthiness, while cybersecurity analysis becomes more effective when informed by safety-critical dependencies. The result is a more realistic understanding of how faults, vulnerabilities and external influences interact across complex automotive architectures.

RF interfaces evolve into critical R155 attack surfaces

While frequency allocation and interference management are handled by telecom regulators such as the ITU, FCC, and ETSI, their cybersecurity implications fall under ISO/SAE 21434 and R155.

RF systems, such as V2X, Bluetooth, Wi-Fi, Ultra-Wideband keyless entry, and telematics gateways remain among the most exposed attack surfaces and are explicitly considered within both the TARA methodology of ISO/SAE 21434 and the threat-modeling scope of a CSMS under R155.[180]

Relevance to

R155 | OEMs must include RF interfaces in their risk assessment, supplier qualification, and in-service monitoring for type-approval evidence.

Relevance to

ISO/SAE 21434 | Requires detailed TARA coverage of wireless threats (spoofing, jamming, replay, rogue access points) and the implementation of secure communication protocols, encryption, and key-management systems to maintain confidentiality and integrity.

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

Regulation / Standard	Effective / Reference Date	Key Relevance to Automotive Cybersecurity
ITU Radio Regulations (WRC-23 Edition)	In force from January 2025	Provides the global spectrum framework for ITS, V2X, and eCall frequencies. Defines coexistence rules relevant to RF risk modeling and regulatory conformity.[181]
FCC Part 15 (US)	Updates referenced in January 2025 FCC policy brief	Regulates unlicensed RF devices in vehicles (key fobs, Wi-Fi, BLE, UWB). Aligns with current US C-V2X and 5.9 GHz allocation policy.[182]
ETSI EN 302 571 (European Union)	Amended in 2025 to align with EN 303 613 coexistence criteria	Specifies technical parameters for ITS radios (5.855-5.925 GHz) used in secure V2X communications.[183]
ISO 15118 (V2G)	Second edition reaffirmed 2025	Defines secure authentication and encrypted communication between EVs and chargers. Complements ISO 24089 and R156 update-security requirements.[184]
SAE J2945/1 (V2V Safety Comms)	2025 review cycle open (SAE ITC notice May 2025)	Specifies secure on-board V2V safety communication requirements, integrated into RF TARA work under 21434.[185]
ETSI EN 303 645 (IoT Baseline)	Confirmed 2025	Provides baseline IoT security provisions applicable to automotive IoT peripherals and infotainment subsystems.[186]
Directive 2014/53/ EU RED - Radio Equipment Directive (EU)	In force since June 2016, cybersecurity requirements become mandatory from August 2024	Sets EU wide security obligations for radio-equipped automotive devices (Wi-Fi, BLE, UWB, keyless entry, V2X), requiring protection of networks and personal data.[187]
IEEE 802.11p, known as Wireless Access in Vehicular Environments (WAVE)	Approved July 2010	A standard tailored for V2X communication. It enables real-time wireless communication between vehicles (V2V) and between vehicles and infrastructure (V2I).[188]
SAE J3105	First published in January 2020	Defines requirements for automated conductive DC charging of heavy duty EVs, including secure communication and control parameters.[189]

As of 2025, the WP.29/GRVA working group continues to list cybersecurity and software-update issues among its active agenda items for type-approval and post-production oversight, confirming ongoing regulatory attention to vehicle cybersecurity.[190]

Compliance scope expands to cover software and mobility infrastructure

As the Automotive and Smart Mobility ecosystem evolves and introduces new applications, devices, and services, policymakers are rethinking regulatory frameworks. In addition to the critical milestone of R155, extending the scope to all new vehicles as of mid-2024, legislators worldwide are becoming more aware of cybersecurity risks to vehicles, infrastructure, and consumer privacy.

The CRA establishes an EU security baseline for the supply chain

The European Cyber Resilience Act (CRA)[191], officially adopted in October 2024, sets horizontal cybersecurity requirements for products with digital components, including both hardware and software.[192] It aims to strengthen protection and reduce risk across a wide range of connected products by requiring secure-by-design practices, vulnerability management, and lifecycle support.

The CRA introduces a comprehensive cybersecurity framework that applies across the entire product lifecycle, beginning with planning and design and continuing through development, deployment, maintenance, and ongoing support. Manufacturers must assess cybersecurity risks proactively, implement timely risk-mitigation measures, and report actively exploited vulnerabilities and cybersecurity incidents to the appropriate authorities.[193]

To support these advanced resilience goals, the CRA specifies several core requirements. Manufacturers must establish a vulnerability management process capable of identifying, assessing, and mitigating product vulnerabilities. They must deliver timely security updates that are securely distributed, cryptographically signed, and validated. Products are required to enforce strong protections against unauthorized access, including authentication controls, session management, and API-level safeguards. The CRA further mandates data confidentiality and integrity, ensuring that sensitive data is encrypted both in transit and at rest. In addition, products must generate protected security-relevant logs that support forensic investigations and compliance audits.

While the CRA broadly applies to "products with digital elements" (PDEs), some sectors are excluded because they are already governed by dedicated cybersecurity and safety regulations. In the Smart Mobility ecosystem, this includes products falling under the General Safety Regulation (EU) 2019/2144, such as vehicles regulated through R155 CSMS requirements for categories M, N, and certain O vehicles. However, other vehicles and digital mobility products not covered by R155 do fall under the CRA, meaning OEMs and mobility stakeholders will need to align requirements across both frameworks as regulatory coverage expands.[194]

To accommodate its broad scope, the CRA is being introduced in phases, with certain obligations beginning in September 2026, and the full regulation becoming applicable by December 2027. This phased rollout gives manufacturers time to integrate CRA-aligned processes, documentation, and security controls into their product development and support workflows.

The European Commission continues to refine specific provisions of the CRA to support consistent interpretation. As disclosed in late 2025, the European Commission was finalizing a delegated act clarifying Article 16(2), which governs when CSIRTs (Computer Security Incident Response Teams) may delay EU-wide vulnerability notifications. Such delays will be permitted only under exceptional circumstances, for example, when a vulnerability is highly sensitive, a fix is imminent (within 72 hours), or the reporting platform or the CSIRT itself has been compromised.[195]

ISO 15118 standardizes vehicle-to-grid cybersecurity and trust

ISO 15118:2022, Road vehicles – Vehicle-to-grid communication interface,[196] defines the communication protocols between EVs and EV supply equipment (EVSE)[197]. It includes the cybersecurity requirements for encrypted, authenticated Plug & Charge communications and applies to category M and N vehicles, with broader adoption encouraged. It also serves as the foundation for the High-Level Communication (HLC) protocol for the Combined Charging System (CCS) standard for charging EVs.

To establish trust in the EV charging process, the standard was designed to protect the grid, and support the safe charging of multiple vehicles simultaneously.

ISO 15118 governs 'Plug & Charge' operation through three core security stages:[198]

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 and data storage), and power grids (e.g., utilities and building management systems).

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.[199]

As multiple vulnerabilities were disclosed throughout 2025, regulatory frameworks were updated to match the new threat landscape.[200] In 2025, the ISO 15118 standard received a major official update with the publication of ISO 15118-10:2025, defining the physical and data-link layer requirements for single-pair Ethernet communication between electric vehicles and charging stations. In parallel, the European Commission formally integrated ISO 15118 into the Alternative Fuels Infrastructure Regulation (AFIR), mandating support for EN ISO 15118-2:2016 from January 2026, and EN ISO 15118-20:2022 from January 2027, across newly installed or renovated public and private charging points within the EU.

UNECE R171 harmonizes driver control assistance systems

The UNECE Regulation No. 171 (R171) establishes a harmonized framework for Driver Control Assistance Systems (DCAS), such as lane-keeping and speed assistance functions that support, but do not replace the driver. Adopted by WP.29 in 2024, the regulation defines technical performance, driver-engagement, and fail-safe requirements across vehicle categories covered by the 1958 Agreement.

R171 consolidates and extends earlier provisions on driver-assistance technologies by specifying how DCAS must operate under normal and fault conditions. This includes activation logic, human-machine interface (HMI) behavior, and transitions to manual control. Uniform testing and type-approval criteria ensure these functions remain predictable and controllable.[200]

Although R171 is primarily a safety regulation, it introduces cybersecurity-relevant dependencies through its linkage with braking, steering, and on-board communication networks. Under R155 and ISO/SAE 21434, OEMs must include DCAS components, firmware, and update pathways within their CSMS scope. As a result, the integrity of control logic, OTA or workshop updates, and driver-engagement signals becomes central to maintaining R171 compliance throughout the vehicle lifecycle.[203]

Key milestones for UNECE R171 implementation

Category	Regulatory Applicability & Dates	Notes
00-series entry into force	22.09.2025 Regulation becomes active	R171 formally enters into force, enabling DCAS type approvals under the 00-series.[204]
Initial implementation window	To be defined by approval authorities	UNECE has not established mandatory "new model" or "all production" dates.[205]
01-series amendments adopted	March 2025 (adopted)	WP.29 adopts 01-series amendments refining DCAS definitions, test procedures, and HMI requirements.[206]

Euro 7 regulation establishes a unified emissions framework

The Euro 7 regulation (Regulation (EU) 2024/1257)[207] establishes a unified emissions framework for all road vehicle categories, covering both internal combustion engine (ICE) vehicles and EVs. It consolidates and extends previous standards by introducing stricter limits and broader monitoring requirements for exhaust emissions, brake and tire particle emissions, and specifically for EVs, battery durability and energy performance.

The regulation places a strong emphasis on continuous compliance. Advanced on-board monitoring systems, data reporting, and lifecycle durability verification processes make the integrity of emissions and performance data increasingly important for regulatory conformity.

The following table summarizes the key introduction milestones for Euro 7 regulation across vehicle and tire categories:[208]

Category	New Type Vehicle	All New Vehicles	Notes / Small-Volume Manufacturer Delay
Light-duty vehicles (Categories M1 & N1)	November 2026	November 2027	Starting July 2030 for vehicles constructed by small-volume manufacturers.
Heavy-duty vehicles (Categories M2, M3, N2, N3, O3, O4)	May 2028	May 2029 [209]	Starting July 2031 for small-volume manufacturers in these categories.
Tires (abrasion / wear)	Class C1 tires: new types from July 2028 Class C2 tires: new types from April 2030 Class C3 tires: new types from April 2032	Class C1 tires (all new): from July 2030	

Euro 7 also raises the importance of monitoring, since fraudulent or malicious tampering with emissions controls, battery performance data, or on-board monitoring outputs can undermine regulatory compliance. Cybersecurity driven detection methods that track anomalies in calibration, telemetry, or reporting processes can help identify manipulation early and support trusted data flows across the vehicle lifecycle.

AVs cybersecurity mandates expand globally

Cybersecurity for autonomous and connected vehicles is becoming a central pillar of regulatory development worldwide. Governments are preparing frameworks to support safe, large-scale deployment of automated driving while balancing innovation and public safety.

At the international level, UNECE WP.29 continues work on global AV standards, including harmonized approaches to cybersecurity, data management, and liability, expected to mature in 2028.[210] These international efforts form the reference point for evolving national and regional AV cybersecurity frameworks.

United States: NHTSA Best Practices (2022)

Voluntary federal guidance recommending layered cybersecurity, TARA, OTA protections, penetration testing, and participation in Auto-ISAC. Some states, such as California, require cybersecurity attestations for AV testing.

United Kingdom: Automated Vehicles Act 2024

The UK's first dedicated autonomous-driving framework. It defines authorization, safety assurance, operator responsibility, and cybersecurity requirements aligned with R155 and R156. Full implementation is planned for 2026. Authorized AV operators must demonstrate resilience to cyber attacks, maintain security, update infrastructure, and ensure continued safe operation under system compromise or remote intervention scenarios.

Japan: Road Transport Vehicle Act & Road Traffic Act (effective as of April 2023)

Implements R155 and R156 for automated driving systems. Level 4 autonomous driving is permitted under specified conditions, with mandatory CSMS certification and event-data recording.

South Korea: Motor Vehicle Management Act (effective as of August 2025)

Requires Level 3+ AV manufacturers to implement certified CSMS, support secure OTA updates, maintain continuous threat monitoring, and report cyber incidents.

Singapore: TR 68 (2021)

Voluntary AV standard, issued by Land Transport Authority (LTA) and the Singapore Standards Council, requiring security-by-design, risk assessments, third-party evaluation, and secure OTA update processes.

Global perspective: Regional frameworks converge on safety and security

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.

European Union

In 2025, the European Union continued the enforcement of its comprehensive vehicle safety and cybersecurity framework under the General Safety Regulation (GSR), which entered full application in July 2024.[217] The regulation is fully operational across member states, requiring all new vehicles placed on the EU market to integrate a standardized set of driver-assistance and safety systems. This marks the transition from legislative adoption to enforcement and reflects the EU shift toward an integrated model of safety and cybersecurity governance across the entire Automotive sector.

While primarily designed to enhance on-road safety, the GSR embeds cybersecurity management obligations: manufacturers must demonstrate compliance with a CSMS throughout the vehicle lifecycle. This aligns with R155 and ISO/SAE 21434, ensuring that connected vehicles undergo systematic cybersecurity risk assessment, monitoring, and mitigation as part of the type-approval process.[218]

EU GSR: implementation milestones

Category	2025 Status	Next Steps / Forthcoming Deadlines	Notes & Cybersecurity Relevance
Road vehicles (M and N categories)	GSR fully in force as of July 2024. All new vehicle types certified under the new framework.	Full application to all new vehicles from July 2026.	OEMs must demonstrate integration of GSR safety features and maintain an approved CSMS for type approval.
Intelligent and active safety systems	Lane-keeping, intelligent speed assistance, and advanced emergency braking are now standard on new models.	Expansion of mandatory driver-distraction and fatigue monitoring systems between 2026–2027.	These systems increasingly depend on connected sensors and HMI interfaces, raising data-security and privacy requirements.
Data and event-recording functions	Basic event data recorders (EDRs) and emergency call (eCall) modules operational.	Enhanced EDRs with extended retention and cyber-tamper protection required by 2027–2028.	EDR and eCall data handling must comply with GDPR and secure-by-design principles to prevent manipulation or unauthorized access.

Following its adoption in 2024, the NIS2 Directive entered its national enforcement phase across EU member states in 2025. It broadens the EU's cybersecurity framework to cover automotive and mobility stakeholders including OEMs, EV-charging operators, telematics providers, and Intelligent Transport System (ITS) operators.[219] By late 2025, all "essential" and "important" entities were required to demonstrate risk management, incident reporting, and governance capabilities, with clear cybersecurity accountability at the management level. For the Automotive sector, NIS2 now defines concrete expectations for supply chain resilience, coordinated response, and vulnerability disclosure across connected mobility ecosystems.[220]

The European Commission and ENISA have announced plans to develop sectoral guidance and EU-wide cybersecurity certification schemes under the Cybersecurity Act, including future frameworks for managed security and vulnerability-management services to support NIS2 implementation.[221]

Simultaneously, the CRA entered its implementation phase,[222] setting EU-wide cybersecurity obligations for connected hardware and software.[223] While vehicles remain regulated under frameworks such as R155, the CRA directly affects the automotive supply chain, notably ECUs, telematics units, agriculture and construction vehicles, and charging equipment. Manufacturers are currently adapting development and patch-management practices ahead of full enforcement in December 2027.[224]

Alongside NIS2 and the CRA, several complementary initiatives reinforce the EU's cybersecurity and data-governance agenda:

- **The Data Act (Regulation (EU) 2023/2854):** Introduces secure data-sharing and access mechanisms for connected vehicles, ensuring transparency and user control over in-vehicle data exchanges.[225]
- **The AI Act (Regulation (EU) 2024/1689):** Entering application in 2026, this establishes risk-based compliance requirements for AI systems used in automated driving and safety-critical vehicle functions.[226]
- **The Data Governance Act (Regulation (EU) 2022/868):** Complements these measures by creating trusted intermediaries and European data spaces for transparent and secure sharing of mobility data.[227]

Looking ahead to 2026, the European Commission plans to propose harmonized type-approval rules for automated driving systems (ADS) and a dedicated Vehicle Data Access Regulation.[228] ENISA is also developing EU cybersecurity certification schemes for managed security services, further strengthening oversight of digital and mobility infrastructure.[229]

Together, these initiatives expand the EU's regulatory framework toward a unified model of cyber-secure, data-driven mobility, consolidating Europe's role as a global reference for connected vehicle governance.

United States

In 2025, the US continued the ongoing public discussions on regulatory and policy frameworks for automotive cybersecurity and data protection, with a focus on supply-chain integrity, critical infrastructure resilience, and product-level security certification.

Key federal and state-led initiatives include:

Regulation / Initiative	Lead Agency	Key Provisions / Impact	Upcoming Milestones
Connected Vehicle Supply Chain Rule (15 CFR Part 791 Subpart D)[230]	Department of Commerce	The final rule was published in January 2025, addressing national security risks in connected vehicle hardware and software linked to China or Russia. Applies to Vehicle Connectivity System (VCS) and ADS components.[231]	Bans expected to impact 2027 year models for software components, and 2030 year models for hardware components.[232]
Cyber Risk Management Programs for Transport[233]	TSA / CISA	Requires cybersecurity risk-management programs for US transport operators that manage vehicle fleets (buses, trains, logistics), including NIST CSF alignment and cyber incident reporting to CISA. Indirectly impacts connected and fleet-operated vehicles rather than vehicle manufacturers.	First enforcement cycle will begin in 2026, establishing unified transport sector reporting.
FCC "Cyber Trust Mark" Certification[234]	FCC	The national labeling program was launched in January 2025, focusing on certifying IoT and connected vehicle devices that meet baseline cybersecurity and privacy standards.	Program evaluation and potential refinement following initial rollout of the Cyber Trust Mark, subject to further FCC action.
NHTSA Cybersecurity Best Practices Update[235]	NHTSA	April 2025 announcement to update 2022 guidelines for software-defined vehicles, OTA updates, and AI-driven ADAS systems.	Revised draft expected 2026, including AI-safety assurance and data logging integrity.
AI Accountability Policy Framework	White House	Published in June 2025, it sets the baseline expectations for AI safety, transparency, and cybersecurity in critical systems, including automotive AI.	Implementation guidance and test programs under development for 2026.

Together, these initiatives mark the US' transition from fragmented oversight to a nationally coordinated system that links cybersecurity, privacy, and AI assurance. By 2026, the US is expected to finalize the connected vehicle supply chain rule, operationalize cyber risk management obligations across transportation sectors, and advance federal privacy and AI accountability legislation, aligning its regulatory trajectory with global automotive cybersecurity standards.[237]

China

In 2025, China moved from adoption to implementation of its mandatory cybersecurity and software governance regime for intelligent connected vehicles (ICVs). The core pillars are the three GB national standards:

- **GB 44495-2024 (Vehicle Information Security):** Independent technical analysis published in 2025 notes that while GB 44495 aligns conceptually with the intent of R155 and ISO/SAE 21434, it is more prescriptive for the Chinese market, mandating specific technical controls for external interfaces, communications, and data protection.[238]

- **GB 44496-2024 (Vehicle Software Update):** Establishes a detailed SUMS-type framework governing both OTA and workshop updates.[239]
  It defines manufacturer obligations for:
  - Update planning, verification, and documentation
  - User notification and rollback procedures
  - Vehicle-state and power-supply conditions required during an update
  - Failure handling, validation, and test methods to ensure update integrity

  It also introduces technical requirements for version control, update traceability, and type-sameness, ensuring that post-update vehicles remain within their certified configuration scope.
  Implementation of GB 44496-2024 is planned to begin in January 2026, for new-type approvals, with existing certified vehicle types expected to transition by January 2028.[240]

- **GB 44497-2024 (AD/ADAS Data Recorder):** Sets technical and test requirements for automated driving data recorders to support post-incident reconstruction, serving as the primary evidence source for regulatory oversight.[241]

These standards will enter into force in January 2026 for new vehicle types, with staged obligations thereafter.

Furthermore, a February 2025 Ministry of Industry and Information Technology (MIIT) and the State Administration for Market Regulation (SAMR) notice introduced immediate post-market enforcement, formalizing admission, recall and OTA updated controls for ICVs.[242] The notice requires mandatory filing of ADAS and OTA update plans, formal incident and failure reporting, stricter recall triggers linked to software behavior, and prohibits marketing driver assistance systems as “autonomous driving”. Together, the GB standards and the Notice shift compliance toward enforceable lifecycle governance, combining prescriptive software update controls with strengthened regulatory oversight of AD/ADAS data and software behavior.[243]

Strategic analysis: China vs. global standards

While GB 44495-2024 and GB 44496-2024 draw heavily on the principles of R155 and ISO/SAE 21434, the Chinese standards adopt a uniquely prescriptive and test-driven compliance model. They mandate explicit technical controls, conformity procedures, and enforcement mechanisms, contrasting sharply with the broader, framework-based approach used internationally.[244]

- **Prescriptiveness:** GB 44495/44496 require detailed technical specifications and test methods (e.g., specific update preconditions, failure handling), whereas R155 / ISO/SAE 21434 focus on achieving security outcomes.
- **Enforcement hooks:** The 2025 Notice couples software governance directly to recall law and market access, effectively making AD/ADAS OTAs a formal regulatory event, a mechanism tighter than typical R156 practice.
- **Data Evidence:** GB 44497 standardizes incident data capture for AD/ADAS, anticipating expanded post-crash analytics and reinforcing liability evidence.

Upcoming milestones

Topic	Key Development	Significance for the Automotive Sector
GB 44495, 44496, 44497 Implementation	The three mandatory national standards will take effect for new vehicle types in January 2026. For previously certified models, the transition extends to January 2028.	OEMs operating in China must prepare CSMS- and SUMS-equivalent documentation, perform required test validations, and ensure data recorders comply with new technical requirements.
ADAS OTA and Recall Regulation	The MIIT/SAMR Notice (February 2025) entered into force immediately. Any autonomous or ADAS-related OTA update must be submitted to regulators and treated as a formal recall when applicable.[245]	This closes regulatory loopholes that previously allowed unapproved software modifications and strengthens post-market accountability for safety and cybersecurity in ICVs.

EV market share and charging infrastructure cyber risks drive new global mandates

Global EV adoption accelerated in 2025, supported by stronger consumer demand, new model launches, and expanding charging networks. According to the PwC EV Sales Review for Q3 2025, battery electric vehicles (BEVs) represented just over 20% of all new cars sold worldwide, with BEV sales growing by 35% compared to the similar period in 2024.[246] China continues to dominate global EV penetration, accounting for roughly 65% of all EVs sold in 2025. Europe follows with approximately 18%, while the US holds 9% and the remaining markets collectively contribute the final 8%.

As charging infrastructure has expanded, threat activity targeting EV charging stations (EVCS) has intensified. EVCS are complex, connected IoT systems composed of components from multiple vendors, and rapid deployment has increased exposure to numerous attack vectors.

Charging Point Operators (CPOs) have become frequent targets. Attacks on backend command-and-control servers can disrupt thousands of chargers simultaneously, create artificial load spikes, or expose PII and charging-pattern data.[247] API-based attacks, which require relatively lower technical skill, also remain common and may originate from mobile apps, third-party platforms, or vehicles themselves, leading to data exfiltration or denial-of-service incidents.[248]

In response, new and updated standards are strengthening the regulatory foundation for safe, reliable, and interoperable charging infrastructure. Current efforts emphasize secure data handling, grid-load management, and strong authentication between vehicles and chargers.

Regulations protecting EVCS fall into two major categories:

- **Operational standards:** Define how EV charging stations securely communicate with vehicles, backend servers, and grid systems. They outline principles for authentication, encryption, software updates, and data exchange. **In 2025, updates to ISO 15118, OCPP,[249] and IEC 63110[250] reinforced interoperability and cybersecurity consistency.**
- **Regional laws and regulatory frameworks:** Establish legal requirements for EVCS operators. In 2025, the EU's AFIR,[251] US CISA guidelines,[252] the UK's Smart Charge Points Regulations,[253] and China's charging-infrastructure rules[254] renewed focus on cybersecurity, reliability, and transparency. Together, these measures help ensure that charging systems remain safe, interoperable, and resilient as global deployment accelerates.

2025 update on EVCS cybersecurity regulations

Region / Country	Regulation	Focus	Implementation Date	Enforcement Status
EU	ETSI EN 303 645	IoT / EVCS	August 2025	Mandatory from August 2025, for RED-scoped radio/IoT devices.[255]
	NIS2 Directive	Critical infrastructure	October 2024	Mandatory [256]
	EU Cyber Resilience Act (CRA)	IoT, connected devices, EVCS	October 2024	Mandatory from May 2027 (with early reporting rules 2026).[257]
	Alternative Fuels Infrastructure Regulation (AFIR, (EU) 2023/1804)	EVCS	April 2025	Mandatory for all new public charging stations.
US	NIST IR 8473	EVCS	October 2023	Voluntary [258]
	CISA EV Charging Infrastructure Cybersecurity Guidelines (2025)	EVCS	July 2025	Advisory; used by NEVI and DOE grant programs.[259]
	National Electric Vehicle Infrastructure (NEVI) Standards	EVCS	April 2023	Mandatory[260]
China	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
	MIIT Draft Guideline for Electric-Vehicle Charging Cybersecurity Management	EVCS cybersecurity governance	August 2025	Expected finalization in 2026.[261]
UK	BSI PAS 1878:2021 / PAS 1879:2021 – Smart Appliances and Energy Smart Appliance (ESAs) Interoperability Code of Practice (BSI)	Smart appliances	December 2021	Voluntary
	The Electric Vehicles (Smart Charge Points) Regulations 2021 (SI 2021/1467)	EVCS	December 2022	Mandatory; strengthened by Ofgem 2025 update (encryption & logging).
Japan	MIC IoT 5G Comprehensive Security Measures	IoT	June 2019	Mandatory; ongoing updates in 2025 for 6G transition.[262]
	METI IoT Security and Safety Framework	IoT	November 2020	Mandatory. Updated in 2025 to align with ISO/IEC 27400.

European Union

The EU's Alternative Fuels Infrastructure Regulation (AFIR) is a central component of the European Union's sustainable mobility strategy, aimed at accelerating the transition to zero-emission transport. Adopted in 2024 and applicable since 2025, AFIR replaces the earlier Alternative Fuels Infrastructure Directive (AFID) and introduces legally binding targets for the rollout, accessibility, and technical interoperability of charging and refueling infrastructure across all member states. It also establishes harmonized requirements for connectivity, payment systems, and data exchange to ensure consistency across the EU.[263]

A key pillar of AFIR is mandatory adoption of the ISO 15118 family of standards, which define secure, interoperable communication between electric vehicles, charging points, and backend systems. These standards enable advanced capabilities such as Plug & Charge authentication, encrypted session management, and vehicle-to-grid (V2G) energy exchange.

Beginning January 2026, all publicly accessible charging points must comply with ISO 15118-1 to 15118-5, which formalize secure vehicle-to-charger communication and support features such as automatic authentication and bidirectional power flow. In January 2027, compliance will extend to private and semi-public Mode 3 and Mode 4 charging stations through the adoption of ISO 15118-20:2022. This second-generation standard introduces enhanced communication layers that enable smarter authentication, remote management, and advanced grid-integration functions.[264]

To maintain interoperability, any EU-based charging station offering Plug & Charge must support both ISO 15118-2:2016 and ISO 15118-20:2022, ensuring backward compatibility with existing EVs and forward compatibility with next-generation models.[265]

United States

In August 2025, the National Electric Vehicle Infrastructure (NEVI) Formula Program guidance was updated to streamline state-level deployment of EV-charging stations.[266] While the original 2023 NEVI rule introduced requirements for data handling, network connectivity, and consumer data protection for NEVI-funded chargers, no new federal cybersecurity mandates were introduced in 2025.

China

China's 2023 national standards for EV charging entered full effect in 2024, becoming the technical baseline for EV chargers and EV-charger communications used across public charging networks. GB/T 18487.1-2023 (conductive charging systems general requirements)[267] and GB/T 27930-2023 (digital communication protocol between off-board DC chargers and EVs)[268] both took effect on April 1, 2024. These standards define interface safety, communication flows, authentication, and session control, along with the test methods used for DC fast-charging interoperability.

These mandatory requirements sit alongside GB/T 34658-2017 (information-system security requirements for charging/swap networks) and GB/T 41578-2022 (general cybersecurity requirements for EV charging systems), which serve as recommended GB/T baselines widely referenced by operators and backend providers.[269]

Governance for ICVs was further tightened in 2025, with direct implications for charging backends. In February, 2025, MIIT and SAMR issued a joint Notice on strengthening the administration of product admission, recall, and OTA software upgrades for ICVs.[270] The Notice entered into force immediately and requires manufacturers to file OTA plans, report incidents and failures, and, where safety functions are affected, treat relevant OTAs as formal recalls. For EV charging ecosystems, this links vehicle-side connectivity and charging-related functions directly to China's recall and market-access regime, increasing oversight of software lifecycle activities that influence safe charging and network stability.

China's next-generation high-power DC ecosystem, often referred to as ChaoJi, also advanced through GB/T publications released in 2023. These documents update the core charging system and DC-communication standards referenced above, confirming China's migration toward higher-power interfaces and modernized communication and handshake logic for fast charging.

In China, charger hardware and EV-charger communications are governed by mandatory GB/T interface standards, while platform and backend security follow GB/T information security baselines and the 2025 ICV notice for OTA governance and incident reporting. Together, these measures require operators and manufacturers to demonstrate conformance with GB/T 18487.1-2023 and GB/T 27930-2023 at the interface level, and to maintain auditable software- and firmware-management, telemetry, and recall processes for any function that may influence safe charging or the wider network.

UK

In October 2025, the UK signed a bilateral agreement with Singapore expanding the scope of its Product Security and Telecommunications Infrastructure (PSTI) regime. The agreement explicitly extends PSTI cybersecurity protections, such as bans on default passwords and requirements for vulnerability disclosure, to connected devices, including EV chargers.[271]

Singapore

Singapore continued to strengthen its domestic framework in 2025. In March 2025, Singapore published the Electric Vehicles Charging (Amendment) Regulations 2025. The regulations require all EV chargers to be type-approved under national standard TR25:2022+A1:2025 and subject to licensing under the Electric Vehicles Charging Act 2022. Furthermore, in November 2025 Singapore's LTA issued the Guidelines for the Licensing of EV Charging Operators, requiring that charging network licensees adopt specific cybersecurity measures, including network segregation and incident-reporting frameworks, as a condition of their license.[272]

Upstream

06.

AUTOMOTIVE CYBERSECURITY SOLUTIONS

The AI zero-sum game challenge is gaining momentum, as global attack groups shift focus to the Automotive and Smart Mobility ecosystem.

Cybersecurity solutions evolve, focusing on continuous lifecycle orchestration

Automotive cybersecurity continues to advance as the sector deepens its transformation into hyper-connected and software-defined mobility. Threats are becoming more sophisticated, automated, including large-scale AI capabilities. Vehicle Security Operations Centers (vSOCs) and cyber teams face threats that target not only vehicles but also mobile applications, backend services, charging networks, and mobility IoT. **This places new demands on cybersecurity programs that must secure vast global fleets, dynamic cloud and app ecosystems, and constantly evolving software and hardware supply chains.**

AI now plays a central role across this landscape. Large-scale data from connected mobility, collected during the entire lifecycle, cannot be interpreted with traditional tools alone. ML-driven detection, behavioral modeling, and cross-domain correlation have become essential for identifying unknown threats, inferring risk across billions of signals, and enabling timely response at fleet scale.

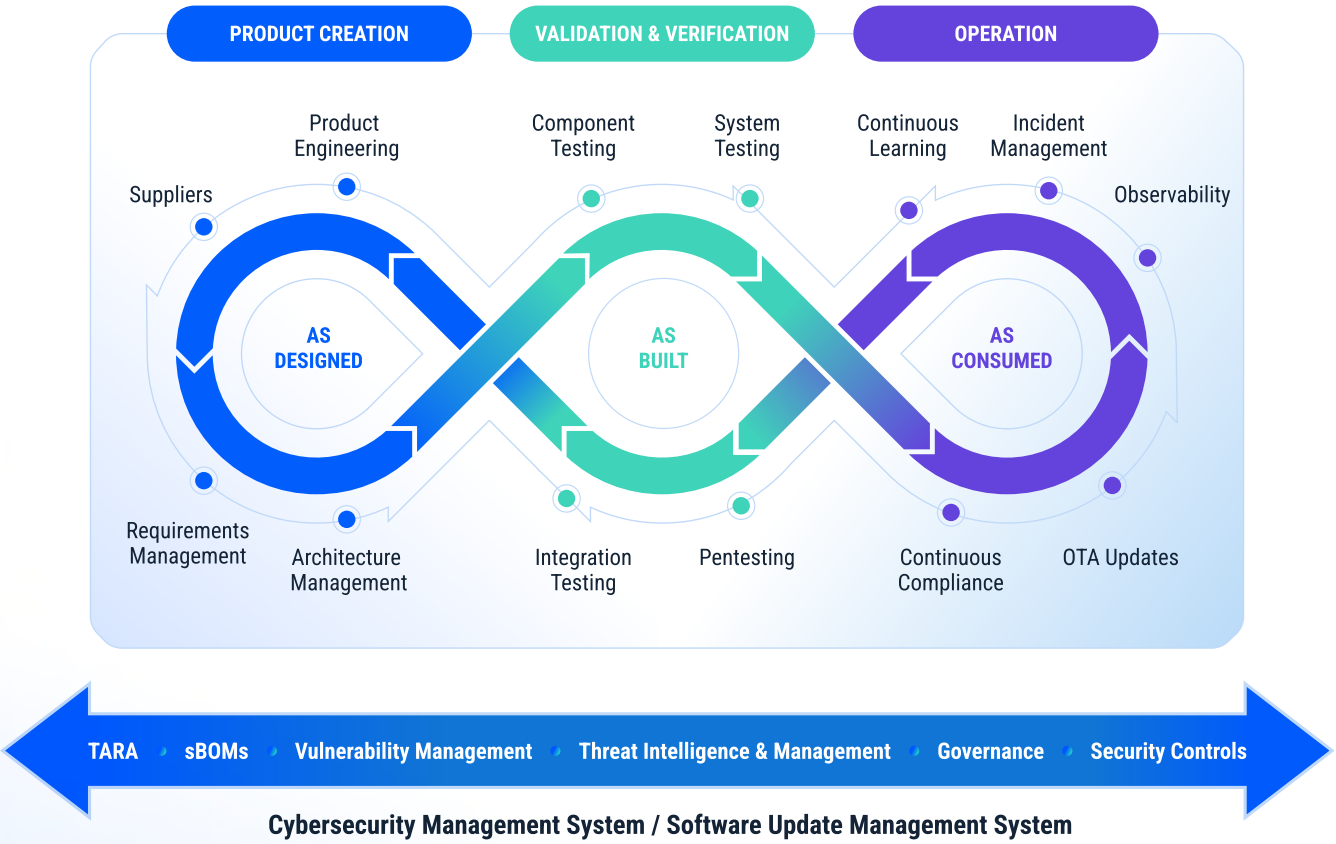
Protecting safety, trust, and availability requires an operating model that can keep pace with rapid software changes, evolving threat landscapes, and the growing interdependence between vehicles, cloud services, and supplier components. Traditional lifecycle approaches, which separate development from operations, are no longer sufficient for software-defined mobility.

A new perspective is beginning to take shape across the industry. Leading OEMs are moving toward continuous lifecycle orchestration supported by AI-driven insight. This approach uses real-world evidence to validate design assumptions and ensures that cybersecurity, safety, and quality remain aligned as vehicles evolve through OTA updates and changing usage patterns.

We, at Upstream, refer to this emerging model as the double infinity loop.

It links engineering intent with field behavior and creates an ongoing cycle of verification and improvement. AI strengthens this process by analyzing large volumes of data, detecting weak indicators of risk, and revealing behavioral changes that would otherwise remain hidden. **The double infinity loop reflects a shift toward more adaptive and evidence-based cybersecurity practices. AI-powered analytics, combined with continuous lifecycle orchestration, allow cybersecurity to evolve from reactive monitoring to proactive resilience across the entire connected vehicle ecosystem.**

Continuous cybersecurity orchestration



Product creation

Grounding cybersecurity intent in operational reality

The “As Designed” phase of the double infinity loop defines the intended secure and safe behavior of the vehicle. This is where engineering teams establish architectural principles, cybersecurity claims, threat models such as Threat Analysis and Risk Assessments (TARA), and safety assumptions aligned with ISO 26262 and ISO/SAE 21434. Functional safety goals, hazard prevention strategies, and core cybersecurity mechanisms are articulated to describe how the system is expected to behave under both normal and fault conditions.

However, modern vehicle architectures no longer exist in isolation. Vehicles are deeply interconnected with backend platforms, cloud orchestration layers, mobile applications, APIs, and continuously evolving service ecosystems. These dependencies introduce behaviors that are difficult to fully anticipate during early design stages. Backend systems may change independently, cloud microservices may evolve outside vehicle release cycles, and interfaces that were once considered non-critical may become safety-relevant over time. As a result, early cybersecurity and safety assumptions are increasingly exposed to real-world drift.

Regulatory expectations reinforce this shift. UNECE WP.29 R155 and ISO/SAE 21434 require continuous monitoring and risk management throughout the vehicle lifecycle, not only during development. Static or periodic TARA exercises are no longer sufficient for vehicles that remain in service long after their software platforms, suppliers, and cloud dependencies have changed.

AI-driven operational intelligence fundamentally strengthens this phase. By analyzing large-scale telemetry across vehicles, backend systems, APIs, mobile apps, and OTA infrastructures, engineering teams gain empirical context that complements theoretical design models. Instead of relying solely on assumptions and lab-based validation, teams can observe how comparable systems behave in production, identify weak signals of risk, and uncover architectural blind spots that would otherwise remain hidden. This improves the accuracy of threat modeling, sharpens cybersecurity claims, and highlights design areas prone to quality or security degradation.

Within the double infinity loop, post-production telemetry becomes a core design input rather than a downstream operational artifact. **This is particularly critical for supplier governance. OEMs must evaluate not only supplier cybersecurity processes but also real-world performance and ongoing vulnerability management across delivered components.** AI models allow OEMs to correlate in-field anomalies directly to supplier software versions, configurations, or integration points, creating an evidence-based cyber record of capability. Latent defects, implementation drift, and recurring component-level patterns can be identified early, strengthening CSMS maturity and supplier accountability.

Clear definition of shared responsibilities remains essential. Cybersecurity Interface Agreements (CIA) and structured responsibility models, such as Responsible Approving Supporting Informed Consulting (RASIC), help establish ownership across OEMs and suppliers. The combination of AI and the double infinity loop makes these responsibilities measurable and continuously verifiable. Instead of depending solely on design documentation or pre-production validation, both parties can use real operational intelligence to confirm that cybersecurity claims remain valid in production.

Security by design

Security by design is the practical expression of this approach during product creation. It requires that cybersecurity risks are identified early, controls are defined with intent, and resilience is engineered into architectures before vehicles reach production, as mandated by R155 and ISO/SAE 21434. Within the double infinity loop, AI reinforces these practices by continuously validating design assumptions against development artifacts and operational evidence. Signals derived from simulations, validation activities, and in-field behavior highlight where attack surfaces expand, controls underperform, or assumptions no longer hold. This feedback sharpens TARAs, improves prioritization of cybersecurity mechanisms, and ensures that secure design decisions remain aligned with how systems actually operate over time.

Validation & verification

Closing the gap between implementation and intent

The validation and verification phase of the double infinity loop corresponds to the "As Built" phase of the vehicle. At this stage, architectural intent is realized across in-vehicle software, backend services, cloud infrastructures, and OTA delivery pipelines. Cybersecurity requirements, safety mechanisms, and functional behaviors are no longer theoretical. They must be verified and validated as implemented, across all environments in which the vehicle operates.

This phase is challenged by the inherent complexity of modern vehicle development. Software is produced by multiple internal teams and external suppliers, backend platforms evolve continuously, OTA pipelines introduce frequent changes, and cloud deployments vary by region and scale. Traditional pre-production testing cannot fully replicate these conditions. Safety mechanisms that perform as expected in controlled environments may behave differently under real-world latency, load, or cross-service interactions. Cybersecurity claims may depend on assumptions that are unintentionally broken as backend logic evolves. Supplier defects may remain dormant until triggered by specific operational patterns that only emerge in the field.

Continuous validation addresses these gaps. **By linking live operational telemetry directly to precise vehicle, backend, and cloud software configurations, engineering teams can assess whether implementations continue to align with design intent after release. When anomalies appear, whether related to cybersecurity, safety, or quality, they can be correlated to specific software versions, configurations, or microservices.** This enables early lifecycle detection, accurate attribution, and evidence-based prioritization of remediation efforts based on real-world impact rather than theoretical severity.

Within the double infinity loop, verification is no longer a one-time gate but an ongoing process. Operational evidence feeds back into engineering, strengthening confidence that cybersecurity controls perform as expected, safety mechanisms remain dependable, and latent defects are identified before they escalate into large-scale recalls, service disruptions, or customer harm. This continuous validation capability is essential for maintaining trust and resilience in software-defined mobility at scale.

Operation

Extracting insights from real-world consumption

The operations phase of the double infinity loop corresponds to the "As Consumed" state, where vehicles are finally in production, exposed to the full variability of real-world use. Diverse environments, unpredictable user behavior, evolving backend logic, OTA-driven changes, and adaptive attacker techniques converge at this stage. It is in operations that the most meaningful indicators of cybersecurity posture, safety integrity, and product quality emerge.

Real-world ecosystems consistently challenge assumptions made during development. Backend services may generate event sequences that were never modeled. EV charging infrastructure and regional network conditions can introduce timing and state transitions not observed in test environments. OTA updates may introduce unintended regressions, while attackers exploit legitimate functions in novel combinations. Customer usage patterns further expand system behavior beyond what requirements or simulations can anticipate.

Cybersecurity tools are required to deliver the deep visibility to manage this complexity. **By unifying vehicle, backend, cloud, APIs, and service telemetry into a single operational view, AI models would be able to detect behavioral anomalies and surface signals that indicate emerging risk.** These anomalies may reflect cybersecurity threats, quality defects, or safety concerns. Correlated patterns across regions, software versions, or suppliers enable OEMs to identify issues at their source and intervene before they propagate across fleets.

Operational intelligence also underpins continuous safety assurance. ISO 26262 assumes that safety mechanisms remain effective throughout the vehicle lifetime, yet this assumption must be verified under real operating conditions. **By providing ongoing evidence of how safety mechanisms perform in the presence of software changes, cyber threats, and complex system interactions, operations become an active contributor to lifecycle assurance rather than a passive monitoring function.**

The multi-layered cybersecurity stack for the Automotive and Smart Mobility ecosystem

The complexity of the connected mobility ecosystem demands a multi-layered cybersecurity stack that builds on proven enterprise IT practices while being explicitly adapted to automotive and smart mobility environments. Core controls such as network security, cloud monitoring, endpoint protection, API security, and segmentation remain foundational.

In this ecosystem, however, these layers must be unified through a product-centric detection model based on Detection and Response within a mobility-specific XDR architecture. AI, leveraging ML, GenAI, and AI agents, strengthens every layer of this model. It enables advanced analysis of network flows, detection of anomalous API behavior, identification of cloud misconfigurations, and correlation of subtle in-vehicle signals with backend activity. For mobility assets, this shift allows SOCs to move beyond static, rule-based alerts toward continuous behavioral understanding across vehicles, services, and infrastructure.

The double orchestration loop elevates this architecture by ensuring that operational insights continuously inform engineering, quality, OTA planning, and supplier management. AI models contribute to this connection by turning raw telemetry into actionable intelligence across the entire lifecycle.

The foundation of XDR relies on a wide definition of the scope of the connected vehicle ecosystem, which has now expanded to include multiple elements that carry direct impact on the vehicle safety, functionality and data. There are unique cybersecurity challenges associated with each layer of automotive infrastructure. These challenges can be addressed with a multi-layered approach, which includes all the layers of vehicle connectivity through the XDR, as well as a product-centric SOC.

API security

This relatively 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, as well as 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

Developing an effective AI-driven and product-centric SOC

SOCs were originally designed to monitor enterprise IT environments, including systems, infrastructure, and corporate assets. Within OEMs, traditional SOCs focused on networks, servers, endpoints, and cloud services that were fully owned and directly controlled by the organization. Connected vehicles, and most recently software-defined vehicles, fundamentally changed this model.

Unlike IT infrastructure, vehicles and mobility assets operate in uncontrolled and highly variable environments. They are constantly in motion, interact with external systems at massive scale, and depend on complex backend, cloud, OTA, and third-party service chains. This shift led OEMs to establish vSOCs, to address post-production cybersecurity monitoring and incident response for connected vehicles in the field.

Over the past several years, OEMs have invested heavily in defining and operationalizing vSOCs. This included clarifying scope, determining organizational ownership, and selecting sourcing and operating models such as in-house, hybrid, or managed services, as well as centralized versus regional operations. Regulatory pressure, particularly R155, accelerated these efforts and transformed the vSOC into a strategic operational capability.

Early vSOC implementations were often narrow in scope, operating as standalone functions focused primarily on regulatory compliance and post-production vehicle monitoring, or embedded within IT security organizations under the CISO with partial coverage of cloud and connected backend environments. **While these models addressed immediate compliance needs, they often showed limitations as attack surfaces expanded beyond the vehicle itself, exposing gaps in cross-domain visibility and coordinated risk management across the broader mobility ecosystem.**

As scale increased and operational maturity improved, a new generation of security operations models began to emerge:

01

The Fusion vSOC

This model integrates traditional vSOC functions with adjacent operational domains such as OTA health monitoring, diagnostic trouble codes (DTCs) analytics, fleet operations telemetry, and cyber threat detection. Fusion vSOCs rely on close collaboration with enterprise IT SOCs to protect data-driven services, APIs, and applications across the broader smart mobility ecosystem. This integration is essential for detecting and responding to complex, multi-stage attacks that traverse vehicles, backend platforms, and user-facing applications.

02

The IT-OT vSOC

In this model, IT SOCs, OT SOCs, and vSOCs are unified into a single operational entity. The scope extends across the full vehicle lifecycle, as demonstrated in the double infinity loop. Capabilities increasingly include monitoring of production environments, factory OT networks, enterprise and vehicle APIs, and in some cases adjacent domains such as EV charging infrastructure and mobility services.

03

The Product SOC

Most recently, this trajectory is expanding beyond the concept of "vehicle security" and instead treats the vehicle as one component within a larger, continuously operating product system. This includes vehicles, embedded software, backend platforms, mobile applications, OTA pipelines, AI services, digital keys, EV charging ecosystems, and third-party integrations, as well as APIs in between. The Product SOC aligns security operations with how modern automotive products are actually designed, built, and consumed.

This shift to new vSOC models is driven by several forces. First, the majority of operational vehicle and product telemetry is owned and managed by OEMs, but its relevance now spans far beyond cybersecurity. Second, more stakeholders require access to this data, including fleet operators, mobility service providers, infrastructure operators, and public sector entities, each with distinct operational and risk objectives. Third, attackers increasingly exploit seams between product components rather than isolated systems.

AI and ML models are foundational to this transformation. When implemented effectively, the next-gen vSOC operates on a clear framework that defines scope, responsibilities, governance, and operating models, supported by advanced analytics and automation. Core capabilities include:

- Continuous 24/7 monitoring across vehicles, cloud backend systems, APIs and other connected services
- Ingestion and correlation of high-volume and multi-domain telemetry at fleet scale
- Continuous vehicle, software, and service risk posture assessment throughout the entire lifecycle
- Standardized governance, policies, procedures, and operating processes, aligned with automotive regulations
- Deep integration with SIEM and SOAR platforms to enable evidence retention, cross-organizational visibility, coordinated remediation and compliance

- Near real-time detection of threats, anomalies and misuse using automotive and product-specific analytics
- Intelligent alert triage, investigation and analyst augmentation
- Predictive threat identification through threat modeling, intelligence fusion, and adversarial testing inputs
- Proactive threat hunting across vehicle and product domains, including internal, external and third-party API traffic
- Governance of SDV change events, including OTAs, configurations, feature activations, and more
- Automated, end-to-end response playbooks integrated into SOC and PSIRT workflows

OEMs and mobility stakeholders continue to pursue multiple implementation paths. Some expand existing enterprise SOCs to cover vehicles and product assets. Others build dedicated Product SOCs with specialized teams and tooling. Many leverage managed security service providers with combined IT, OT, and automotive expertise.

Throughout 2025, OEMs continued to advance along this maturity curve as R155 enforcement expanded to cover all new vehicles in production. As regulatory scope broadens and product complexity increases, the evolution from IT SOC to vSOC and ultimately to Product SOC is becoming a defining operational requirement for software-defined mobility.

Looking ahead to 2026, one of the defining challenges for Product SOCs and mature vSOCs will be moving beyond the detection of abnormal access or command execution. In software-defined vehicles, many of the most consequential cybersecurity events manifest as unapproved software, configuration, or feature changes that propagate through vehicles, backend platforms, and OTA pipelines, requiring cybersecurity operations to reason about intent, lifecycle state, and product integrity rather than isolated technical anomalies.

Contextual API security as a core Product SOC capability, expanding detection coverage beyond OWASP Top 10

OEMs and smart mobility stakeholders require a contextual approach to API security that goes beyond traditional IT-centric controls and static risk lists such as the OWASP API Security Top 10.[273]

API exploitation is relatively standardized, requires limited technical sophistication, and can be executed remotely without specialized hardware. **This makes APIs a highly cost-effective attack vector compared to in-vehicle or hardware-focused exploits.** The OWASP API Security Top 10 remains an important industry reference for identifying common classes of API weaknesses and guiding secure development and testing practices.

These risks continue to manifest across the Automotive and Smart Mobility ecosystem, with tangible impacts that include service disruptions, loss of vehicle functionality, safety exposure, large-scale data and privacy breaches, misuse and fraud targeting subscriptions and feature entitlements, as well as long-term brand damage.

However, in connected mobility environments, IT-based API security on its own is insufficient. Traditional API security controls focus primarily on request structure, authentication, authorization, payload correctness, rate limits, and transaction volumes. While necessary, these controls typically operate in isolation from the operational state of the product itself.

In contrast, automotive and mobility APIs are tightly coupled to physical assets, real-world behavior, and safety-critical workflows. API transactions often translate directly into vehicle actions, feature activation, charging behavior, user access rights, and OTA-driven configuration changes. Evaluating these interactions without understanding the contextual state of vehicles, users, infrastructure, and services leaves significant blind spots.

This is where the Product SOC model becomes essential. Contextual API security requires continuous correlation between API traffic and all elements of the product ecosystem. API transactions must be analyzed alongside live product telemetry to determine whether a request is not only syntactically valid, but also behaviorally plausible and safe given the current state of the product.

In addition to raw API traffic and specifications, XDR platforms should incorporate multiple data sources, including:

- Vehicle, user, and device location
- Vehicle identity and user identity attributes
- Real-time and historical vehicle telematics
- Authentication, billing, and entitlement history
- EV charging protocols and infrastructure telemetry
- OTA activity and configuration state

By correlating these signals, cybersecurity teams can detect anomalies that would remain invisible to transaction-based security tools. Within this context, API security is no longer a standalone IT function. It becomes a cross-domain operational capability that spans enterprise systems, vehicles, digital products, and physical infrastructure. As a result, responsibility for monitoring and mitigating API-based cyber risk is increasingly shifting toward integrated operational models.

Recent incidents illustrate how API abuse can directly translate into operational disruption, even when individual API transactions appear valid.

In October 2025, a coordinated stunt in San Francisco disrupted autonomous ride hailing operations when a tech prankster organized a group to order US-based self-driving taxis to the same dead-end street. Approximately 50 vehicles arrived simultaneously, congested the area, and suspended rides within a two-block radius, as well as causing significant service disruptions due to unavailable vehicles. The incident, informally called the first Distributed Denial of Service (DDoS) against an autonomous taxi network, demonstrated how coordinated misuse can impact autonomous fleet behavior and availability.

Product-centric API security tools address this gap by shifting detection from technical correctness to operational consequence. By correlating API transactions with vehicle telemetry, enriched location insights, service health metrics, user behavior, and infrastructure load, these tools can assess whether API-driven actions are creating unsafe, disruptive, or economically damaging outcomes. This allows security teams to identify abuse of legitimate business flows, coordinated denial-of-service conditions driven through APIs, and attacks specifically designed to degrade availability rather than breach data.

This deeper, product-aware perspective is critical as attackers increasingly target service continuity and operational reliability instead of isolated vulnerabilities. Within a Product SOC, API security becomes an enabler of resilience, allowing organizations to detect and respond to threats that manifest as degraded mobility services, fleet-wide disruptions, or loss of customer trust, even when every individual API call appears valid on its own.

Product-centric cyber threat intelligence for proactive risk management

The multi-layered, product-centric approach must include proactive capabilities that strengthen threat detection, with cyber threat intelligence serving as a core operational function. Within this model, threat intelligence enables OEMs and mobility stakeholders to anticipate, contextualize, and mitigate risks across the entire product ecosystem and throughout the full product lifecycle. It acts as a critical feedback mechanism within the double infinity loop, continuously informing and aligning cybersecurity teams across engineering, production, and in-field operations.

As vehicles evolve into continuously connected digital products, threat exposure expands across vehicles (SBOM and HBOM), backend platforms, cloud services, mobile applications, OTA pipelines, APIs, EV charging infrastructure, and third-party integrations. Effective threat intelligence must therefore be product-aware and ecosystem-specific. Generic IT threat feeds provide limited value in this environment, as they lack the ability to map emerging threats to automotive architectures, operational dependencies, and real-world impact.

Automotive-specific and product-focused threat intelligence enables continuous visibility into evolving risks by monitoring clear, deep, and dark web sources for indicators relevant to vehicles and mobility services. This includes early signals of exploit development, credential leakage or abuse, API targeting, ransomware campaigns, fraud techniques, and operational disruption strategies that specifically affect software-defined mobility products. When integrated into the Product SOC, this intelligence directly informs detection logic, response playbooks, and risk prioritization.

The importance of this capability continues to grow as cyber vulnerabilities and attacks increasingly impact not only individual OEMs, but the entire automotive supply chain. Attacks on shared platforms, suppliers, and service providers can rapidly cascade across fleets and markets, eroding trust, safety, and service availability. Product-centric threat intelligence supports cross-organizational coordination by helping stakeholders understand where vulnerabilities sit within the product lifecycle and how exploitation would propagate through vehicles, services, and infrastructure.

Threat actors are also placing greater focus on telematics data, digital identities, entitlements, and usage data as OEMs expand connectivity and software-driven features. Hence, context-aware threat intelligence becomes essential to distinguish real threats from benign anomalies. By understanding vehicle behavior, service workflows, and product-specific business logic, Product SOC teams can reduce false positives, avoid alert fatigue, and focus resources on threats with genuine operational and safety impact.

Within a Product SOC, cyber threat intelligence is not a passive feed. It is an active decision-support capability that continuously connects external threat signals to internal product telemetry, vulnerability management, and operational risk, enabling earlier detection, faster response, and more resilient software-defined mobility services.

Industry-scale incident intelligence for systemic risk awareness

Beyond monitoring individual threats, cybersecurity teams must extract broad insights from significant cyber incidents across the Automotive and Smart Mobility ecosystem. As attacks increasingly target shared platforms, common software and AI components, and standardized interfaces, individual incidents often reveal systemic weaknesses that extend well beyond the originally affected organization. Understanding how and why a specific breach succeeded is critical to identifying other vehicle systems, backend services, APIs, or infrastructure components that could be exposed to the same attack patterns.

This requirement is amplified by the rise of organized attack groups and the continued shift toward large scale ransom operations. These actors operate with clear business models, reuse tooling and techniques, and deliberately pursue scalable impact by exploiting architectural commonalities across fleets, suppliers, and service providers. A successful ransomware campaign against a specific legacy system, telematics platform, or cloud service frequently signals elevated risk for other environments built on similar technologies, configurations, or operational assumptions.

Industry-scale incident intelligence provides two essential types of insight. At a strategic level, it reveals how the threat landscape is shifting. The Automotive and Smart Mobility industry is firmly in the crosshairs of highly organized threat actor groups, many of which are adopting AI driven techniques to accelerate targeting, exploit development, and large scale ransom operations. At a tactical level, the most critical challenge is extracting the right lessons from major incidents.

Two recent examples illustrate this clearly. Following the enterprise ERP zero-day vulnerability exploited in an attack on an OEM in September 2025,[275] threat actors soon developed a similar zero-day targeting another popular ERP system.[276] A narrow response focused only on the initial attack would have been insufficient. The correct lesson was the broader risk posed by exposed, web-facing legacy platforms.

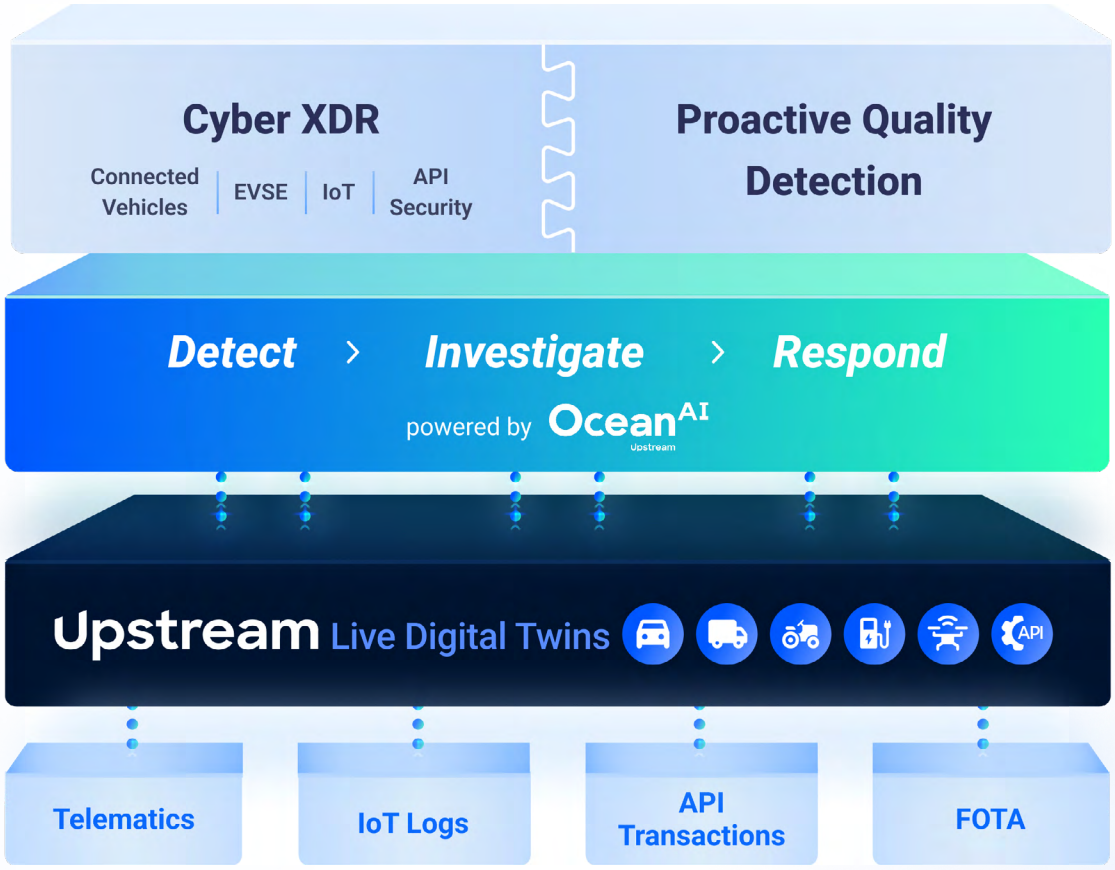
A similar dynamic emerged after an AI-driven component of a popular CRM was compromised in mid-2025,[277] which impacted hundreds of organizations, including OEMs, Tier-1 suppliers, etc. Addressing exposure to those specific applications alone would have missed the underlying issue. The more strategic insight was the systemic risk associated with OAuth token abuse, a pattern reinforced by a breach in November 2025, which impacted a Customer Success Platform (CSP).[278]

Product-centric threat intelligence enables OEMs and mobility stakeholders to translate external incident learnings into proactive internal action. By correlating incidents with product architectures, SBOM and HBOM data, deployment models, and operational workflows, Product SOC teams can assess whether similar exploitation paths exist within their own ecosystems. This insight supports early validation of controls, targeted hardening of at risk components, and preemptive adjustments to detection and response strategies before an attack materializes internally.

In this way, industry-scale incident intelligence transforms isolated events into actionable foresight. It allows organizations to move from reactive and narrow response to anticipatory defense, reducing exposure to cascading risks and strengthening resilience across mobility products and services in an increasingly coordinated threat landscape.

Upstream's AI-driven and product-centric approach to XDR

Upstream pioneered a cloud-based, data management platform purpose-built for connected vehicles, IoT transportation, and smart mobility. Instead of protecting each surface in isolation, Upstream applies a holistic, multi-layer Extended Detection and Response (XDR)[279] approach that spans the full ecosystem: in-vehicle systems, telematics and diagnostics, backend cloud services, mobility applications, APIs,[280] OTA workflows, EV charging infrastructure,[281] mobility IoT,[282] smart mobility and transportation apps, and more. These use cases are supported through unified dashboards, risk scoring, case management workflows, and integrations with enterprise SIEM, SOAR, and ticketing systems to ensure cross-organizational visibility.

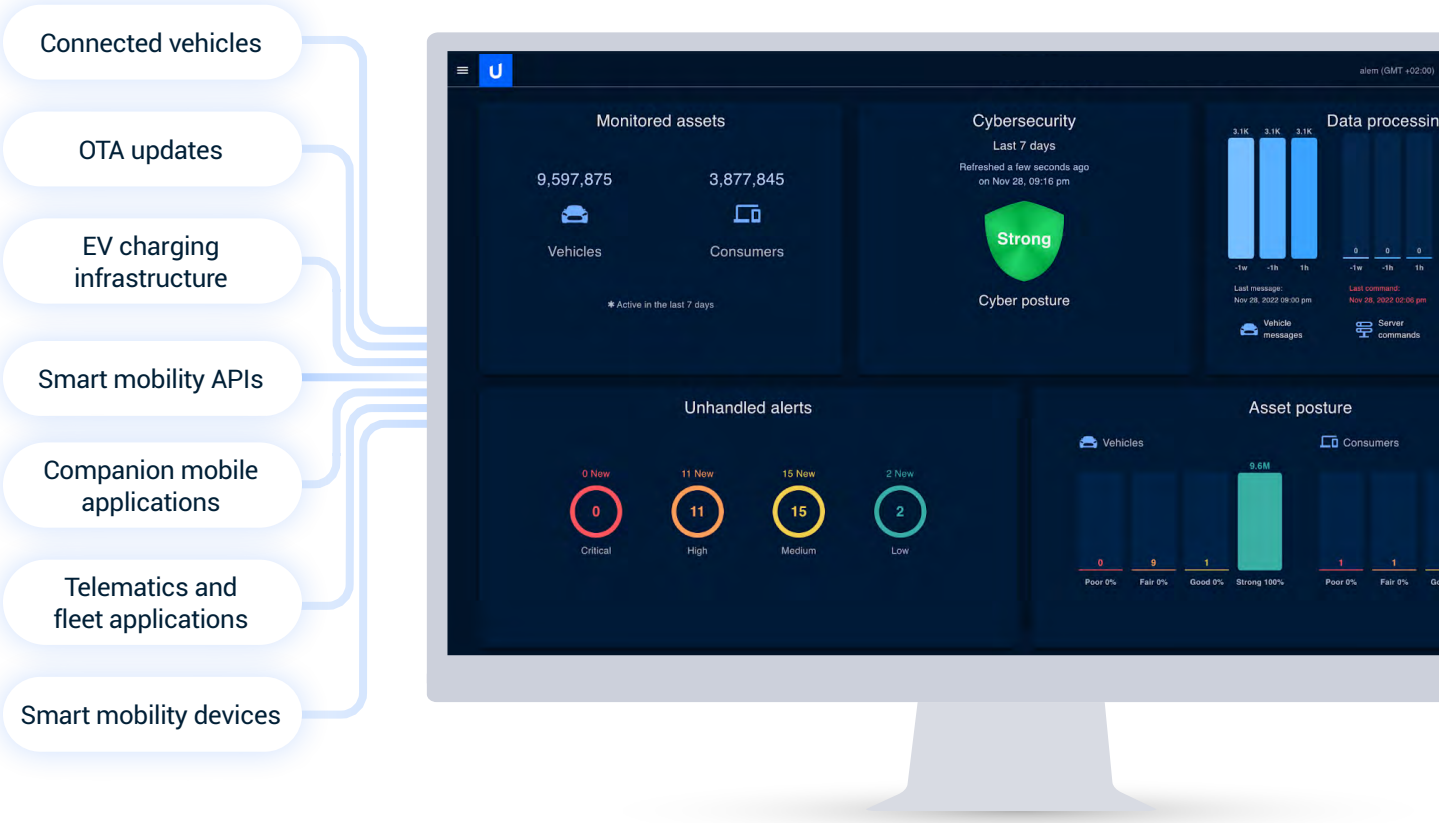


Source: Upstream Security

Cloud-native and agentless by design, the platform leverages the live mobility data, enabling rapid onboarding without installing software or hardware on vehicles or devices.

At the core is a unified XDR product suite built on a common backplane. All core components share the same data layer, live digital twin, analytics pipeline, and investigation workflows, providing a single operational model for correlating threats across product, cloud, and application layers.

This consolidated architecture is designed for teams that must secure vehicles, fleets, charging networks, and customer-facing services under one coordinated detection and response strategy. The XDR suite is typically delivered as a holistic solution, while allowing specific capabilities, such as API security, to be adopted independently when needed.



Source: Upstream Security

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 live 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 live digital twin captures data from numerous sources, providing a real-time snapshot of the monitored asset throughout its lifecycle. The live digital twin establishes behavioral baselines and enables event-chain inference across domains, helping detect complex, low-and-slow attacks that traditional IT telemetry or in-vehicle-only approaches cannot reveal.

For telemetry-thin assets, Upstream is also extending coverage through live digital twins that infer behavioral context from API traffic patterns and transaction syntax.

A product-centric approach to API Security

Upstream integrates API discovery, monitoring, and threat detection as a native capability within its XDR platform. Built on the live digital twin, this product-centric approach enables deep, contextual API threat detection across Smart Mobility applications and services, even when API traffic is the only available data source.

As a shared security layer, the API Security capability delivers distinct value across product, security, and operational teams:

01

Product development and engineering

The platform provides comprehensive API discovery and catalog visibility, including identification of shadow and zombie endpoints and gaps in API documentation coverage. These insights help product and engineering teams better understand exposure and threat patterns, forming a solid foundation for defining and enforcing API Security best practices, such as token usage and authentication models. The same visibility supports shift-left initiatives and ongoing vulnerability management through endpoint ownership mapping, SLA definition, and integration into existing development workflows.

02

Product SOC (PSIRT integration)

Leveraging the live digital twin, the platform correlates API traffic with product signals, telemetry, fleet data, and backend context to detect a broad range of API-related threats. **This correlation extends beyond OWASP Top 10 coverage to include complex multi-step attacks and operational or misuse use cases.** Resulting insights can directly augment PSIRT workflows, bug bounty programs, Vulnerability Disclosure Programs (VDPs), and purple team activities.

03

IT Security & Operations

API Security insights can also be leveraged by enterprise IT and operations teams to improve cybersecurity controls, response automation, and overall API security posture. These insights enhance existing SOC processes, inform incident response playbooks, and enrich cyber threat intelligence with product-aware and API-specific context.

AI-powered detection, investigations, and remediation

Powered by Ocean AI, Upstream's purpose-built AI suite, the platform unifies ML, GenAI, and agentic AI to strengthen detection, investigation, and response. 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.

- ML-based anomaly detection turns signals into high-fidelity alerts, enabling identification of both known threats and unknown risks.
- GenAI capabilities streamline analyst workflows with natural-language investigations, auto-generated alert summaries and triage, as well as no-code detector creation to support custom use cases.
- Agentic AI enhances operational efficiency through automated data classification, false-positive reduction, and playbook-driven response actions.
- The integrated no-code and GenAI-powered detector builder offers use-case-driven customizations and flexible detection. These capabilities enable cybersecurity teams to mitigate emerging use cases and support new business logic without coding or development resources.

Today, the Upstream platform monitors tens of millions of vehicles, smart mobility devices, and EV charging assets worldwide, supporting detection and response efforts, as well as managed SOC capabilities, for some of the world's largest OEMs and smart mobility players. As connected mobility systems continue to converge across product, cloud, and services, Upstream's unified, product-centric XDR approach provides the structured data foundation and AI-driven operational capabilities needed to detect, investigate, and respond at scale.

Proactive cyber threat intelligence

Working closely with Upstream's AutoThreat® PRO,[238] cybersecurity 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 clear, deep, and dark 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 2024, Auto-ISAC introduced the Automotive Threat Matrix (ATM),[284] 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.[285]

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[286] 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.

Upstream's AutoThreat® Platform and AutoThreat®PRO

Source: Upstream Security

Managed product-centric vehicle and mobility SOC

Leverage the leading managed vehicle and mobility SOC[287] that protects millions of vehicles and mobility endpoints worldwide, enhancing OEM cyber resilience through comprehensive services. Upstream's SOC actively monitors cyber threats targeting connected vehicles, devices, and their components, as well as EV charging infrastructure and smart mobility apps. Leveraging experience with top global passenger, commercial, agriculture, autonomous, 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 hunting, 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 misuse, and vulnerabilities affecting the entire fleet. Powered by the Upstream Platform, the SOC applies advanced detection to contextualize data and identify known and unknown cyber risks.

AI-powered enhanced investigations and mitigation

Powered by Upstream's AI suite, Ocean AI, the managed SOC leverages unprecedented efficiencies and mitigation capabilities by optimizing alert triage and 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.

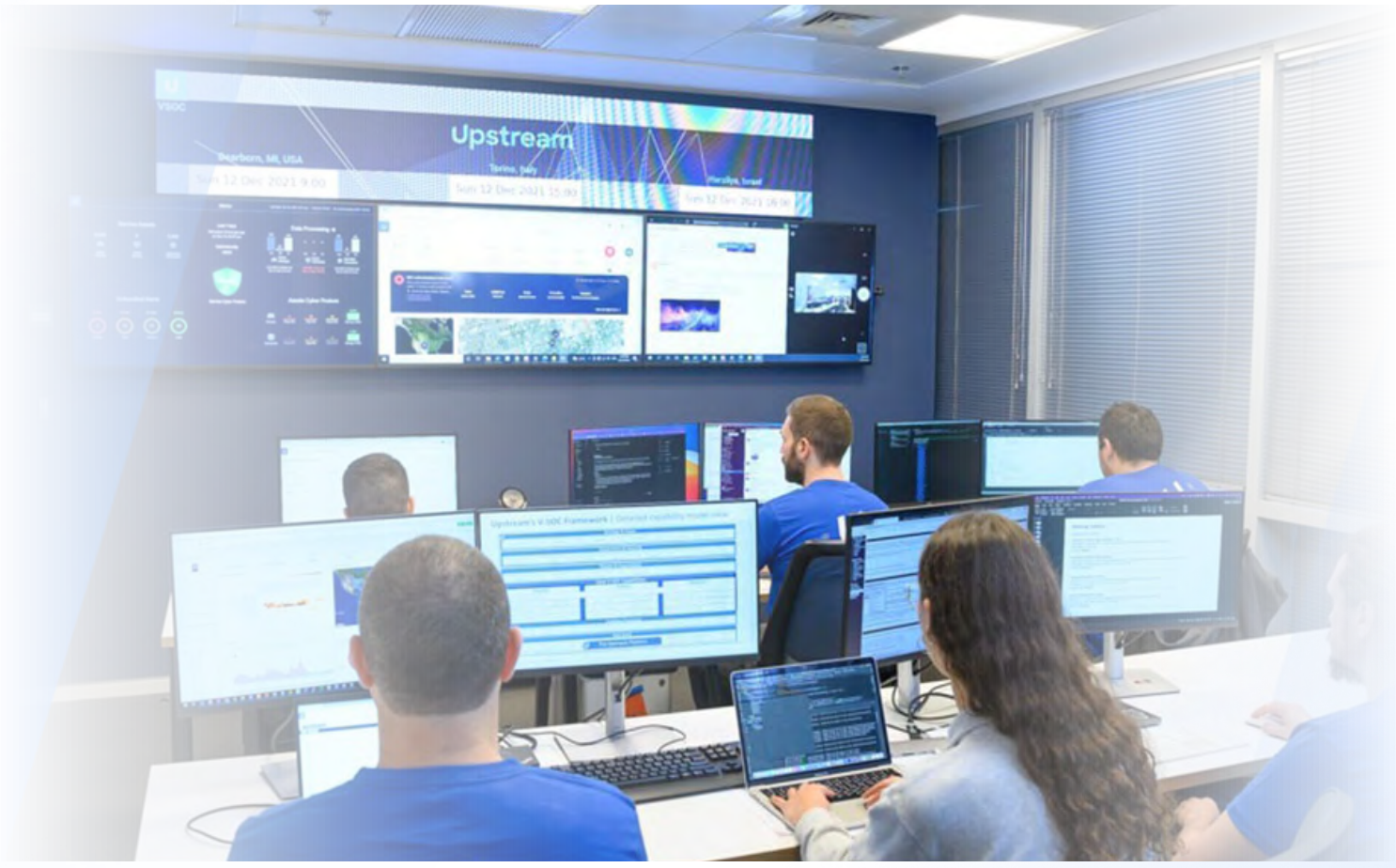
Secure and compliant operations

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: [288]

- 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

Upstream

07.

2026 LEADERSHIP INSIGHTS

Automotive and smart mobility cybersecurity predictions.

Vinod D'Souza

Director, Office of the CISO, Manufacturing and Industries
Google Cloud

In 2026, the Automotive industry will face a definitive reality check: AI adoption is no longer a futuristic vision but the baseline operational requirement. Connectivity, data, and algorithms will officially overtake hardware as the primary brand differentiators, a shift accelerated by a consumer base that increasingly prioritizes superior technology over legacy brand loyalty. While Generative AI and AI Agents will streamline the value chain - from manufacturing Digital Twins to user experience - this rapid digitization will expose a critical vulnerability: managing millions of lines of code in a constantly evolving ecosystem is impossible in isolation.

Consequently, manufacturers will be forced to move beyond standalone products to secure collaborative vehicle-to-cloud ecosystems. Real-world resilience will depend on integrating specialized cloud partners to deploy technologies capable of analyzing massive datasets to detect anomalies in real-time. The emphasis will shift from simply launching features to ensuring the integrity of the software lifecycle, where secure cloud integration and automated validation become the essential safeguards for a highly exposed, software-defined future.

This heightened focus is critical not only for product reliability but because the supply chain and OT (Operational Technology) environments will remain primary disruptive targets. Organizations must urgently implement processes with multiple checks and balances, as threat actors fully embrace AI to enhance the speed, scope, and effectiveness of operations, demanding that defenses scale to meet this new, accelerated threat landscape.

Rebecca Faerber

Manufacturing Cyber Security Program Manager | Ford

2026 will see a significant uptick in nuanced attacks on critical infrastructure through sophisticated, patiently planned attacks on cyber physical systems.

For years we've watched manufacturing and other OT environments brought to their knees through the simple collateral damage done by blunt force instruments like ransomware in an organization's finance or ERP systems. In 2026, the adversaries will weaponize the lessons from these clumsy wins and refine their attack patterns. The lost production cycles will be intentional, protracted, and under the control of folks who wish to inflict damage as well as make bank.

AI may be part of the solution, but it will not save us. The AI-enabled security tools versus the AI-enabled malware will prove to be a zero-sum game. Defense in Depth will continue to be our most resilient and effective strategy.

Juman Doleh-Alomary

Chief Information Security Officer & EUC | BorgWarner

Looking toward 2026, we expect cybersecurity pressure to intensify as IT and OT environments continue to converge. The broader digital footprint across backend systems, products, and partner ecosystems creates more pathways for intrusion, which gives adversaries greater room to exploit overlooked vulnerabilities. This shift coincides with a new class of agentic AI driven attacks that move with speed and precision, often faster than existing tools can accommodate. The combination of higher connectivity and smarter offensive automation raises the likelihood that attackers will reach critical systems before defenders can intervene.

We also anticipate a surge in indirect threats that take advantage of the complex supply chain and active stakeholders. Recent high profile attacks have shown how breaches at vendors can cascade into operational disruption for OEMs and suppliers. At the same time, ransomware coupled with data breaches remain a favored tactic among criminal groups that now target both availability and strategic information. These dynamics play out against an industry-wide shortage of AI security talent. Innovation in AI enabled services is accelerating, yet organizations are struggling to build the competencies needed to protect these environments. We expect this gap to remain one of the defining challenges in 2026, shaping investment priorities and cybersecurity strategy across the sector.

Bob Everson

Chief Architect - IoT, Mobile, AI | Cisco

In 2026, the rapidly expanding scale and breadth of connectivity and attack surfaces will force the realization that siloed security approaches are obsolete. To counter this, the industry must pivot toward a unified, pervasive control plane that protects the entire ecosystem, rather than focusing solely on the vehicle itself.

The capability to correlate real-time telemetry from millions of connected assets with global threat intelligence will rapidly become the critical differentiator. Organized attackers will leverage weak links in the supply chain and network infrastructure for massive, coordinated attacks, driving OEMs to swiftly adopt integrated security architectures that move beyond simple perimeter defenses to achieve data-driven, preemptive threat detection.

Monica E. Mitchell

Cybersecurity Lead Automotive Intelligent Cockpit | Harman

In 2026, long term structural risks are expected to weigh more heavily on the automotive industry. Operating systems approaching (or already passed) end of life will demand sustained vulnerability management, since newly disclosed flaws can still become entry points for system level compromise. As vehicle computing platforms expand with ADAS integration and high performance architectures, the attack surface will continue to grow, and software quality issues, whether internal or open source, will introduce additional exposure. At the same time, compliance with global regulations such as UNECE WP.29 R155, GB 44495 and the Cyber Resilience Act will require deeper visibility into software assets and supply chain practices while preserving the integrity of proprietary technology.

The coming year is also expected to bring new challenges linked to in vehicle AI. Running large models may strain compute resources and create availability risks that adversaries could exploit through ransomware. Model reliability will depend on the integrity of data flowing into training and inference pipelines (garbage in / garbage out), while weak privacy controls raise the likelihood of sensitive information being exposed.

These pressures coincide with a shift in organizational risk tolerance. Despite notable cyber incidents across the industry in 2025, the absence of recent high impact vehicle targeted and remote attacks has prompted some companies to assume they are more resilient than they are. This mindset reduces investment in core cybersecurity programs and, if it continues, may widen the gap between perceived and actual readiness at a time when system complexity and adversary capability are both accelerating.

Martin Arend

General Manager Automotive Security | BMW Group

In the race between defender and attacker, a holistic view of automotive security is becoming increasingly decisive: starting with "security by design" in the product, paired with a "defence in depth" approach to ensure the long lifecycles of the vehicle, including its services and accompanying infrastructure. Building on this, there is a need for constantly increasing detection performance and responsiveness.

In this context, AI can be a means of increasing the speed of detection and analysis. Effective cybersecurity will therefore depend on close coordination between product development, engineering and security operations to ensure lasting improvements in system design and resilience, supported by a well-trained AI.

Thomas Young

Technical Leader, Vehicle and Connected Services Cybersecurity | Ford

In 2026, AI-powered and AI-assisted API attacks will shift from episodic incidents to a continuous operational challenge. AI is rapidly lowering the barrier to complex attack execution, putting advanced vulnerability discovery, API abuse, and multi-step exploitation into the hands of a much broader population. Attackers are increasingly able to identify business logic flaws, authorization weaknesses, and service-to-service trust gaps at machine speed, particularly across the dense API layers that support software-defined vehicles and digital mobility services.

The continued expansion of AI-powered backend services and data platforms and MCP orchestration tools are increasing the complexity of identity propagation and on-behalf-of access handling across distributed systems. In many environments, BOLA and IDOR conditions are not being reduced but reinforced by inconsistent authorization models and implicit trust between services. In 2026, improving security outcomes will depend on re-architecting authorization as a systemic control across vehicle, cloud, and third-party services, with explicit ownership, continuous validation, and runtime enforcement.

Dirk Wollschläger

Director | CAR (Center for Automotive Research)

AI in the Automotive industry offers outstanding opportunities to redefine the digital experience and help automakers differentiate themselves from the competition with innovations in a new field. However, a higher level of vehicle connectivity, frequent updates, and more connections to third parties lead to an increased vulnerability to cyberattacks. Cybersecurity is becoming an essential part of a brand's reputation and reliability, just like the physical crash safety of vehicles.

Ultimately, it's about the safety of customers and other road users. Such scenarios attract the interest of well-organized and large criminal/ransom groups seeking to cause significant damage to the Automotive ecosystem.

Instead of considering cybersecurity as a technical issue that can be addressed later, or merely as a matter of regulatory compliance, automakers and their ecosystem partners must embed it as a fundamental pillar of product safety and corporate governance.

Guido Barbero

IT Senior Director Cybersecurity & CISO | Iveco Group

In 2026, AI is expected to become a frontline data control challenge for cybersecurity. Shadow AI usage keeps growing, and AI features are embedded into most enterprise systems and many vehicle systems by default. The result is emerging and unexpected pathways for sensitive data to leak out of the organization, sometimes through standard workflows rather than obvious "espolitation" events.

Cyber attacks will continue to increase in both frequency and sophistication. Attackers will use AI to accelerate vulnerability discovery, prioritize targets, and generate exploit variants, which compresses the time between weakness, weaponization, and impact.

Cybersecurity software vendors will focus on mitigating these pressures by expanding the coverage scope. Automotive stakeholders should demand advanced add-on modules to be bundled into license and subscription packages, widening their security perimeter and detection capabilities to keep pace with the AI-powered transformation of the threat landscape.

Yoav Levy

Co-founder and CEO | Upstream Security

In 2026, Physical AI will enter a new phase of expansion. In automotive, AI driven perception, decision making, and actuation have been embedded in vehicles for several years through advanced driver assistance systems, autonomy stacks, robotaxis, and intelligent control platforms. What changes now is the pace and scope of adoption. Capabilities that were once largely confined to vehicles and mobility infrastructure are rapidly proliferating into broader consumer and industrial markets, driven by advances in foundation models, edge compute, and real-time sensing. This cross market acceleration is reinforcing automotive's role as both an early adopter and a reference architecture for Physical AI operating in safety critical, highly connected environments.

As Physical AI scales, it significantly expands the automotive cyber attack surface. AI-powered systems depend on continuous connectivity across edge systems in vehicles and infrastructure, cloud based management and orchestration platforms, and a growing ecosystem of connected applications and APIs. Effective cybersecurity in this environment requires continuous monitoring across all layers, with the ability to correlate physical behavior with digital signals. Traditional perimeter focused defenses are no longer sufficient when AI systems adapt dynamically, exchange context across domains, and directly influence physical outcomes in real time.

References

1. https://www.electrive.com/2025/10/06/vw-reassigns-cariad-as-coordinator-of-rivian-and-xpeng-software/
2. https://www.volkswagen-group.com/en/press-releases/boosting-innovation-reshaping-mobility-volkswagen-group-invests-in-ai-19852
3. https://www.volvocars.com/us/media/press-releases/5ED641B2DCF1ED0B/
4. https://wayve.ai/press/nissan-announcement/
5. https://www.ibm.com/think/topics/ai-in-automotive-industry
6. https://arxiv.org/html/2508.15306v1
7. https://nvd.nist.gov/vuln/detail/CVE-2025-6514
8. https://jfrog.com/blog/2025-6514-critical-mcp-remote-rce-vulnerability/
9. https://www.salesforceben.com/stellantis-becomes-latest-target-in-salesforce-data-hack/
10. https://arxiv.org/html/2508.15306v1, https://www.sciencedirect.com/science/article/pii/S2095809925004709
11. https://aclanthology.org/2025.findings-acl.580/
12. https://cloud.google.com/discover/what-is-model-context-protocol
13. https://jfrog.com/blog/2025-6514-critical-mcp-remote-rce-vulnerability/
14. https://medium.com/d-classified/utilizing-generative-ai-for-reverse-engineering-31cbcd435e84
15. An official OWASP MCP Top 10 has not been published yet. For additional information: https://owasp.org/www-project-mcp-top-10/, https://genai.owasp.org/llm-top-10/
16. https://www.esentire.com/blog/model-context-protocol-security-critical-vulnerabilities-every-ciso-should-address-in-2025
17. https://www.sciencedirect.com/science/article/pii/S2095809925004709
18. https://www.sciencedirect.com/science/article/pii/S2095809925004709
19. https://www.sciencedirect.com/science/article/pii/S2095809925004709
20. https://www.salesforceben.com/stellantis-becomes-latest-target-in-salesforce-data-hack/
21. https://www.securityweek.com/details-disclosed-for-mercedes-benz-infotainment-vulnerabilities/
22. https://upstream.auto/reports/global-automotive-cybersecurity-report-2025/
23. https://umsafoundation.org/11-problems-chatgpt-can-solve-for-reverse-engineers-and-malware-analysts/
24. https://www.anthropic.com/news/disrupting-AI-espionage
25. https://medium.com/@evyatar9/introducing-gpthidra-the-ai-powered-code-assistant-for-ghidra-78844d2bc227
26. https://www.troyhunt.com/controlling-vehicle-features-of-nissan
27. https://umsafoundation.org/11-problems-chatgpt-can-solve-for-reverse-engineers-and-malware-analysts
28. https://www.microsoft.com/en-us/security/blog/2025/11/07/whisper-leak-a-novel-side-channel-cyberattack-on-remote-language-models/
29. https://www-cdn.anthropic.com/b2a76c6f6992465c09a6f2fce282f6c0cea8c200.pdf
30. https://mpese.com/publication/mcshane-2025-llm/
31. https://upstream.auto/blog/the-billion-dollar-automotive-cyber-club-highlights-a-wake-up-call-for-oems/
32. https://www.wired.com/story/jlr-jaguar-land-rover-cyberattack-supply-chain-disaster/
33. https://www.theguardian.com/business/2025/oct/22/jaguar-land-rover-hack-has-cost-uk-economy-19bn-most-costly-cyber-attack-britain
34. https://www.nbcnews.com/tech/security/jaguar-land-rover-hack-hurt-uk-gdp-bank-england-says-rcna243083
35. https://www.kaspersky.com/about/press-releases/grand-theft-telematics-kaspersky-finds-security-flaws-that-threaten-vehicle-safety
36. https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security
37. https://securelist.com/mercedes-benz-head-unit-security-research/115218/
38. https://www.rideapart.com/news/745921/harley-davidson-hack-hackers-data-breach/
39. https://www.cisa.gov/news-events/ics-advisories/icsa-25-021-03
40. https://autos.yahoo.com/car-transport-thieves-arrested-miami-170000345.html
41. https://www.redpacketsecurity.com/cactus-ransomware-victim-electrocraft-com/
42. https://www.darkreading.com/cybersecurity-operations/mitm-vulns-research-opportunities-car-security
43. https://www.securityweek.com/ransomware-group-claims-attack-on-tata-technologies/
44. https://cybersecuritynews.com/nissan-leaf-vulnerability-exploited/
45. https://www.cybersecuritydive.com/news/hertz-data-breach-cleo/745391/
46. https://www.wired.com/story/airborne-airplay-flaws/
47. https://gbhackers.com/tesla-model-3-vcsec-vulnerability/
48. https://treblle.com/blog/preventing-api-breaches-volkswagen-case
49. https://cybernews.com/security/volkswagen-investigates-data-breach-claims/
50. https://nvd.nist.gov/vuln/detail/CVE-2025-5873

References

51. https://certvde.com/de/advisories/VDE-2025-019/
52. https://cyberinsider.com/critical-bluetooth-flaws-perfektblue-expose-millions-of-vehicles-to-1-click-rce/
53. https://nvd.nist.gov/vuln/detail/CVE-2025-7020/
54. https://driving.ca/auto-news/technology-news/automaker-dealership-portal-security-flaw-hacker/
55. https://www.autocar.co.uk/car-news/new-cars/production-all-jlr-plants-now-back-online-following-cyber-attack
56. https://www.ransomware.live/id/aHR0cHM6Ly93d3cuY25oLmNvbS9AaW5jcmFuc29t
57. https://dailydarkweb.net/global-equipment-giant-cnh-industrial-allegedly-breached-by-ransomware-attack/
58. https://www.protectionweb.co.za/cyber-security/kaspersky-finds-security-flaws-that-threaten-vehicle-safety/
59. https://www.redpacketsecurity.com/dragonforce-ransomware-victim-autorotor/
60. https://www.bussmagasinet.se/2025/10/unikt-sakerhetstest-av-elbussar-sarbarhet-och-skydd-kartlagt/
61. https://www.breachsense.com/breaches/paccar-data-breach/
62. https://nvd.nist.gov/vuln/detail/CVE-2025-11690
63. https://securityboulevard.com/2025/11/my-car-wont-start-because-someone-hacked-my-api-firetail-blog/
64. https://techcrunch.com/2024/12/12/researchers-find-security-flaws-in-skoda-cars-that-may-let-hackers-remotely-track-them/
65. https://github.com/zgsnj123/BYD_headunit_vuls/tree/main
66. https://www.bbc.com/news/articles/cvgmp1prnv0o
67. https://www.scworld.com/brief/rhysida-spills-purportedly-stolen-gemini-group-data
68. https://cybernews.com/security/hacking-spree-continues-with-mazda-canon-and-nhs-added-to-the-list/
69. https://asrg.io/
70. https://upstream.auto/reports/global-automotive-cybersecurity-report-2024/
71. https://upstream.auto/reports/global-automotive-cybersecurity-report-2025/
72. https://www.cvedetails.com/cvss-score-distribution.php
73. https://nvd.nist.gov/vuln-metrics/cvss
74. https://therecord.media/nist-database-backlog-growing-vulncheck
75. https://www.sonatype.com/press-releases/sonatype-intelligence-report-cve-crisis
76. https://www.securityweek.com/nist-still-struggling-to-clear-vulnerability-submissions-backlog-in-nvd/
77. Three additional CVEs are unclassified
78. https://www.securityweek.com/ransomware-group-claims-attacks-on-ascom-jaguar-land-rover/
79. https://dailydarkweb.net/jaguar-land-rover-allegedly-breached/
80. https://www.storyboard18.com/brand-marketing/cyber-attack-halts-jaguar-land-rover-production-despite-800m-digital-overhaul-80242.htm
81. https://www.livemint.com/news/data-breach-alert-stellantis-confirms-third-party-service-exposed-customer-information-here-s-what-was-compromised-11758503294839.html
82. https://www.divd.nl/newsroom/articles/91cd52191c65/
83. https://nvd.nist.gov/vuln/detail/CVE-2024-43648
84. https://nvd.nist.gov/vuln/detail/CVE-2024-43663
85. https://www.borncity.com/blog/2025/09/20/datenabluss-bmw-charging-dienstleister-digital-charging-solutions-gmbh/
86. https://cybernews.com/security/nexopt-data-leak-exposes-locations-vehicles/
87. https://mybroadband.co.za/news/security/607658-prominent-vehicle-tracking-company-hacked-in-south-africa.html
88. https://www.hendryadrian.com/np3-beneficios-data-breach-exposes-customer-and-driver-data/
89. https://www.autospies.com/news/index.aspx?submissionid=124058
90. https://nz.news.yahoo.com/man-launches-world-first-waymo-180300047.html
91. https://www.cybersecuritydive.com/news/lemonade-drivers-license-exposed/745762/
92. https://www.securitymagazine.com/articles/101930-5m-records-exposed-leaking-sensitive-auto-insurance-data
93. https://www.ndss-symposium.org/wp-content/uploads/2025-628-paper.pdf
94. https://www.ransomware.live/id/QVhUQGRyYWdvbmZvcmNl
95. https://www.ndss-symposium.org/wp-content/uploads/2025-26-paper.pdf
96. https://cybersecuritynews.com/teslas-telematics-control-unit-vulnerability/
97. https://www.kaspersky.com/about/press-releases/grand-theft-telematics-kaspersky-finds-security-flaws-that-threaten-vehicle-safety
98. https://securityaffairs.com/185398/security/porsche-outage-in-russia-serves-as-a-reminder-of-the-risks-in-connected-vehicle-security.html
99. https://samcurry.net/hacking-subaru
100. https://www.cisa.gov/news-events/ics-advisories/icsa-25-105-04

References

101. https://securityboulevard.com/2025/11/my-car-wont-start-because-someone-hacked-my-api-firetail-blog/
102. https://cyberinsider.com/critical-bluetooth-flaws-perfektblue-expose-millions-of-vehicles-to-1-click-rce/
103. https://www.youtube.com/watch?v=JXGRR8XxKIc
104. https://cyberpress.org/apple-carplay-vulnerability-exploited-to-gain-root-access/
105. https://nvd.nist.gov/vuln/detail/CVE-2025-3883, https://nvd.nist.gov/vuln/detail/CVE-2025-3882
106. https://nvd.nist.gov/vuln/detail/CVE-2025-52263
107. https://zeropath.com/blog/cve-2025-12357-slac-iso15118-2-summary
108. https://www.cisa.gov/news-events/ics-advisories/icsa-25-021-03
109. https://www.securityweek.com/vulnerabilities-patched-in-qualcomm-mediatek-chipsets/
110. https://www.ndss-symposium.org/wp-content/uploads/2025-628-paper.pdf
111. https://cybersecuritynews.com/researchers-hacked-into-commercial-trucks-buses/
112. https://hardwear.io/usa-2025/presentation/bam-bam-on-a-budget.pdf
113. https://www.autoblog.com/news/thieves-are-stealing-toyotas-in-minutes-using-a-simple-headlight-hack
114. https://cyberinsider.com/pwn2own-automotive-kicks-off-with-382000-bounty-paid-on-day-one/
115. https://cybernews.com/security/nexopt-data-leak-exposes-locations-vehicles/
116. https://www.netzwelt.de/news/245352-hacker-legen-blitzer-lahm-diesen-strassen-herrscht-freie-fahrt.html
117. https://www.darkreading.com/cloud-security/hackers-hay-smart-tractors-vulnerable-takeover
118. https://www.securityweek.com/free-wi-fi-leaves-buses-vulnerable-to-remote-hacking/
119. https://techlomedia.in/2025/05/security-researcher-hacks-into-his-own-car-uncovers-major-flaws-in-volkswagens-connected-app-113838/
120. http://cybersecurity360.it/nuove-minacce/ransomware-in-russia-e-malesia-allarme-rosso-per-la-sicurezza-delle-auto/
121. https://medium.com/@ilnur.khakimov_86612/how-i-hacked-100-000-motorcycles-including-my-own-666bdb702b7d
122. https://hackread.com/cisa-remote-control-flaws-sinotrack-gps-trackers/
123. https://www.ndss-symposium.org/wp-content/uploads/6C-s0997-jin.pdf
124. https://cybersecuritynews.com/nissan-leaf-vulnerability-exploited/
125. https://blackhat.com/asia-25/briefings/schedule/#state-manipulation-unveiling-new-attack-vectors-in-bluetooth-vulnerability-discovery-through-protocol-state-machine-reconfiguration-43736
126. https://cybernews.com/security/ces-2025-keyless-car-keyvault/
127. https://securityonline.info/cve-2025-6029-cve-2025-6030-replay-attacks-expose-vulnerabilities-in-kia-and-autoeastern-smart-keyless-entry-systems/
128. https://www.youtube.com/watch?v=nkQmLOKjql4
129. https://aclanthology.org/2025.findings-acl.580/
130. https://jfrog.com/blog/2025-6514-critical-mcp-remote-rce-vulnerability/
131. https://www.salesforceben.com/stellantis-becomes-latest-target-in-salesforce-data-hack/
132. https://www.cyberghostvpn.com/en_US/privacyhub/dark-web-vs-deep-web/
133. https://www.cyberghostvpn.com/en_US/privacyhub/dark-web-vs-deep-web/
134. Upstream Security
135. https://chris-young.net/understanding-ios-jailbreak-detection/
136. Upstream Security
137. https://www.nhtsa.gov/equipment/odometer-fraud
138. https://www.npr.org/2025/06/10/nx-s1-5418046-e1/some-states-are-seeing-an-increase-in-fraudulent-odometer-rollbacks-on-used-cars
139. Upstream Security
140. Upstream Security
141. Upstream Security
142. Upstream Security
143. https://www.itpro.com/security/rocketing-number-of-ransomware-groups-as-new-smaller-players-emerge
144. Upstream Security
145. https://www.reuters.com/business/retail-consumer/uks-jaguar-land-rover-cyber-attack-shutdown-hit-four-weeks-2025-09-23/
146. Upstream Security
147. https://attack.mitre.org/
148. https://atm.automotiveisac.com/
149. https://www.spglobal.com/automotive-insights/en/blogs/2025/07/ai-in-automotive-industry
150. https://www.precedenceresearch.com/automotive-artificial-intelligence-market

References

151. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai
152. https://aibusiness.com/automation/volvo-to-invest-1-1b-on-ai-in-next-five-years
153. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai
154. https://artificialintelligenceact.eu/implementation-timeline/
155. https://artificialintelligenceact.eu/article/15
156. https://www.capgemini.com/de-de/wp-content/uploads/sites/8/2025/03/EU_AI_Act_in_Automotive_Industry_interactive-1.pdf
157. https://www.taylorwessing.com/en/insights-and-events/insights/2025/03/ai-act-and-the-automotive-industry
158. https://www.euaiact.com/implementation-timeline
159. https://www.capgemini.com/de-de/wp-content/uploads/sites/8/2025/03/EU_AI_Act_in_Automotive_Industry_interactive-1.pdf
160. https://www.twobirds.com/en/insights/2023/global/impact-of-the-eus-ai-act-proposal-on-automated-and-autonomous-vehicles
161. https://www.iso.org/standard/42001
162. https://www.iso.org/standard/62085.html
163. https://www.iso.org/standard/27001
164. https://www.nist.gov/itl/ai-risk-management-framework
165. https://www.meti.go.jp/press/2024/06/20240628002/20240628002.html
166. https://www.iso.org/obp/ui/en/#iso:std:iso:24089:ed-1:v1:en
167. https://eur-lex.europa.eu/legal-content/ENG/TXT/PDF/?uri=OJ:L_202500005
168. https://unece.org/sites/default/files/2024-03/R156e%20%282%29.pdf
169. https://unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf
170. https://unece.org/fileadmin/DAM/trans/doc/2020/wp29/ECE-TRANS-WP29-2020-080e.pdf
171. https://www.iso.org/standard/68383.html
172. https://www.clepa.eu/insights-updates/press-releases/clepa-and-acea-join-with-auto-isac-on-motor-vehicle-cybersecurity/
173. https://autocrypt.io/unece-regulation-iso-standard
174. https://www.helpnetsecurity.com/2025/09/09/connected-car-cybersecurity-europe
175. https://www.iso.org/obp/ui/en/#iso:std:iso-sae:21434:ed-1:v1:en
176. https://www.cyeqt.com/en/un-r155-worldwide-how-countries-regulate-vehicle-cybersecurity-in-2025
177. https://www.newtec.de/en/knowledge/unece-r-155-and-unece-r-156-cybersecurity-of-motor-vehicles
178. https://www.iso.org/standard/68383.html
179. https://pmc.ncbi.nlm.nih.gov/articles/PMC10975927/
180. https://www.vector.com/gb/en/know-how/v2x/v2x-worldwide-status-and-outlook-2025
181. https://www.itu.int/en/ITU-R/seminars/rrs/RRS-23-Americas/Plenaries/2.%20RR%20WRCs%20Monday%2008%20May/1.%20Radio%20Regulations%20RRS-23_Americas.pdf
182. https://www.itu.int/pub/R-REG-RR-2023
183. https://www.etsi.org/deliver/etsi_en/302500_302599/302571/02.01.01_60/en_302571v020101p.pdf
184. https://go-e.com/en/magazine/iso-15118-the-standard-you-cant-afford-to-ignore-any-longer
185. https://www.sae.org/standards/content/j2945/1_202004/
186. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf
187. https://eur-lex.europa.eu/eli/reg_del/2022/30/oj/
188. https://standards.ieee.org/ieee/802.11p/3953/
189. https://www.sae.org/standards/j3105_202305-electric-vehicle-power-transfer-system-using-conductive-automated-connection-devices
190. https://unece.org/sites/default/files/2025-11/ECE-TRANS-WP29-GRVA-22e.pdf
191. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
192. 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/
193. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
194. https://unece.org/sites/default/files/2023-05/GRVA-16-26e.pdf
195. https://www.taylorwessing.com/en/insights-and-events/insights/2025/11/cyber-resilience-act-overview
196. https://www.iso.org/standard/69113.html
197. https://www.switch-ev.com/blog/what-is-iso-15118
198. https://www.switch-ev.com/blog/basics-of-plug-and-charge
199. https://genorma.com/en/standards/iso-15118-20-2022-awi-amd-1

References

200. https://nvd.nist.gov/vuln/detail/CVE-2025-12357 , https://nvd.nist.gov/vuln/detail/CVE-2025-52268, https://nvd.nist.gov/vuln/detail/CVE-2025-6678
201. https://unece.org/media/press/395206
202. https://unece.org/sites/default/files/2025-04/ECE-TRANS-WP.29-GRVA-2025-29e_0.pdf
203. https://www.appliedintuition.com/blog/navigating-dcas-regulations
204. https://unece.org/sites/default/files/2025-03/R171e.pdf
205. https://unece.org/sites/default/files/2025-03/R171e.pdf
206. https://www.atic-ts.com/un-r171-dcas-01-series-and-00-series-comparison-and-analysis
207. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401257
208. https://www.interregs.com/articles/spotlight/266/eu-euro-7-emissions-regulation-published
209. https://www.interregs.com/articles/spotlight/266/eu-euro-7-emissions-regulation-published
210. https://unece.org/transport/road-transport/working-party-automatedautonomous-and-connected-vehicles-introduction
211. https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-pre-final-tag_0_0.pdf
212. https://patentpc.com/blog/regulations-for-autonomous-vehicles-where-do-countries-stand-in-2024-2030-global-policy-trends
213. https://www.gov.uk/government/news/self-driving-vehicles-set-to-be-on-roads-by-2026-as-automated-vehicles-act-becomes-law
214. https://www.npa.go.jp/english/bureau/traffic/selfdriving.html
215. https://gca-korea.tistory.com/entry/Korea-Issues-Legislative-Notice-on-Automotive-Cybersecurity-Software-Updates
216. https://www.lta.gov.sg/content/ltagov/en/newsroom/2021/9/news-releases/enhanced-national-standards-for-the-safe-deployment-of-autonomou.html
217. https://eur-lex.europa.eu/eli/reg/2019/2144/oj/eng
218. https://www.trustonic.com/opinion/one-year-of-wp-29-and-gsr2-has-automotive-cybersecurity-caught-up
219. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
220. https://dgap.org/en/research/publications/connected-vehicle-cybersecurity-eu-must-consider-non-technical-risk-factors
221. https://www.enisa.europa.eu/news/eu-managed-security-services-certification-to-drive-the-cybersecurity-market
222. https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf
223. https://www.fladgate.com/insights/the-european-cyber-resilience-act-what-it-means-for-digital-products
224. https://www.sgs.com/en/news/2025/09/safeguards-13125-update-on-developments-relating-to-the-eu-cyber-resilience-act
225. https://www.digitaleurope.org/resources/embracing-the-future-of-mobility-a-strategy-for-autonomous-driving-in-the-eu
226. https://www.twobirds.com/en/insights/2025/global/new-eu-ai-act-guidelines-what-are-the-implications-for-businesses
227. https://digital-strategy.ec.europa.eu/en/policies/data-governance-act
228. https://www.bakermckenzie.com/en/insight/publications/2025/05/eu-action-plan-in-automotive-sector
229. https://www.mhp.com/en/insights/blog/post/european-cyber-resilience-act
230. https://www.bis.gov/media/documents/connected-vehicles-general-authorization-1
231. https://www.federalregister.gov/documents/2025/01/16/2025-00592/securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles
232. https://www.gibsondunn.com/bis-connected-vehicles-rule-effective-as-of-march-17-2025/
233. https://www.cyberriskwarden.com/cyber-risk-management-for-transport-logistics/
234. https://www.fcc.gov/CyberTrustMark
235. https://www.nhtsa.gov/sites/nhtsa.gov/files/2025-07/report-congress-research-rulemaking-automated-driving-systems-july-2025-tag.pdf
236. https://mediate.com/white-house-ai-action-plan-summary
237. https://www.squirepattonboggs.com/en/insights/publications/2025/07/update-top-10-legal-and-policy-issues-for-general-counsel-in-the-automotive-and-transportation-industry-in-2025
238. https://dissec.to/general/chinas-new-vehicle-cybersecurity-standard-gb-44495-2024
239. https://www.codeofchina.com/standard/GB44496-2024.html
240. https://www.atic-ts.com/gb-44496-2024-china-general-technical-requirements-for-software-update-of-vehicles
241. https://www.codeofchina.com/standard/GB44497-2024.html
242. https://www.miit.gov.cn/jgsj/zbys/wjfb/art/2025/art_fa604619ed45484386f37422d01f5527.html
243. https://dissec.to/regulations/chinas-gb-standards-revisited
244. https://fidoalliance.org/white-paper-addressing-cybersecurity-challenges-in-the-automotive-industry
245. https://www.miit.gov.cn/jgsj/zbys/wjfb/art/2025/art_fa604619ed45484386f37422d01f5527.html
246. https://www.strategyand.pwc.com/de/en/industries/automotive/electric-vehicle-sales-review-q3-2025.html
247. https://riskandinsurance.com/ev-charging-infrastructure-emerges-as-major-risk-factor-despite-lower-fire-rates

References

248. https://www.eseye.com/resources/blogs/ev-charge-point-security-under-fire-82-businesses-breached
249. https://openchargealliance.org
250. https://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID,FSP_LANG_ID:1255,25
251. https://transport.ec.europa.eu/transport-themes/clean-transport/alternative-fuels-sustainable-mobility-europe/alternative-fuels-infrastructure_en
252. https://industrialcyber.co/utilities-energy-power-water-waste/new-us-cybersecurity-implementation-plan-for-energy-modernization-rolled-out
253. https://wallbox.com/en_uk/blog/ev-charger-regulation-change-2025
254. https://www.china-certification.com/en/new-regulations-on-mandatory-certification-for-ev-charging-equipment-to-take-effect
255. https://www.securebydesignhandbook.com/docs/standards/global/en303645-overview
256. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
257. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ%3AL_202402847
258. https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8473.pdf
259. https://www.cisa.gov/news-events/ics-advisories/icsa-25-196-03
260. https://www.federalregister.gov/documents/2023/02/28/2023-04026/airworthiness-directives-bombardier-inc-airplanes
261. https://www.electrive.com/2025/04/17/china-to-introduce-stricter-ev-battery-standards-in-2026
262. https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000568.html
263. https://transport.ec.europa.eu/transport-themes/clean-transport/alternative-fuels-sustainable-mobility-europe/alternative-fuels-infrastructure_en
264. https://www.vde.com/tic-en/news/2025/04-new-eu-requirements-for-charging-stations
265. https://eur-lex.europa.eu/eli/reg_del/2025/656/oj/eng
266. https://www.transportation.gov/briefing-room/president-trumps-transportation-secretary-sean-p-duffy-unveils-revised-nevi-guidance
267. https://www.chinesestandard.net/PDF.aspx/GBT18487.1-2023
268. https://www.chinesestandard.net/PDF.aspx/GBT27930-2023
269. https://www.chinesestandard.net/PDF.aspx/GBT41578-2022
270. https://www.miit.gov.cn/jgsj/zbys/wjfb/art/2025/art_fa604619ed45484386f37422d01f5527.html
271. https://www.gov.uk/government/news/uk-setting-global-benchmark-on-cyber-standards-boosting-growth-and-protecting-consumers
272. https://www.lta.gov.sg/content/dam/ltagov/industry_innovations/Technologies/Electric_Vehicles/PDF/Guidelines%20for%20the%20Licensing%20of%20EV%20Charging%20Operators.pdf
273. https://owasp.org/API-Security/editions/2023/en/0x11-t10/
274. https://nz.news.yahoo.com/man-launches-world-first-waymo-180300047.html
275. https://www.autocar.co.uk/car-news/new-cars/production-all-jlr-plants-now-back-online-following-cyber-attack
276. https://cloud.google.com/blog/topics/threat-intelligence/oracle-ebusiness-suite-zero-day-exploitation
277. https://www.salesforceben.com/stellantis-becomes-latest-target-in-salesforce-data-hack/
278. https://www.oasis.security/blog/gainsight-salesforce-oauth-incident
279. https://upstream.auto/platform/cybersecurity/
280. https://upstream.auto/platform/api-security/
281. https://upstream.auto/solutions/sector/electric-vehicle-charging/
282. https://upstream.auto/solutions/sector/sim-enabled-mobility-iot/
283. https://upstream.auto/autothreat-intelligence/
284. https://atm.automotiveisac.com/
285. https://upstream.auto/blog/deep-dark-web-intelligence-proactive-automotive-cybersecurity/
286. https://attack.mitre.org/
287. https://upstream.auto/solutions/vehicle-security-operations-center/
288. https://upstream.auto/solutions/cyber-readiness-services/

About Upstream

Upstream delivers a cloud-based, AI-powered data management platform purpose-built for connected vehicles, smart mobility, and the IoT ecosystem. By leveraging mobility data, Upstream empowers customers with advanced, AI-driven cybersecurity solutions, including detection and response (XDR), API Security, cyber threat intel, SOC services, resilience services, 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

Upstream