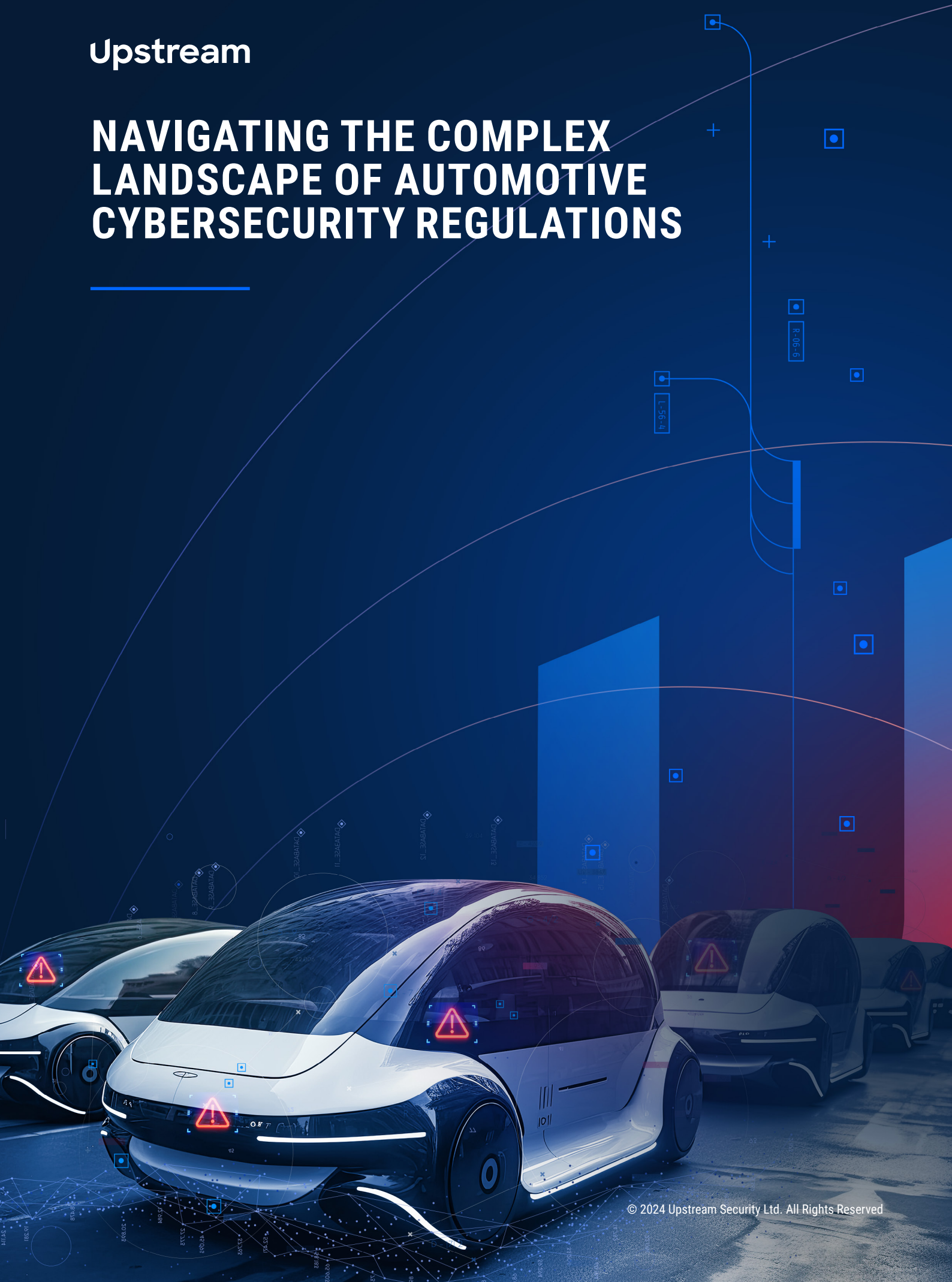
Upstream

NAVIGATING THE COMPLEX LANDSCAPE OF AUTOMOTIVE CYBERSECURITY REGULATIONS



GENERATIVE AI IS RESHAPING THE AUTOMOTIVE ECOSYSTEM, BUT REGULATIONS ARE STILL EVOLVING

Generative AI (GenAI) is reshaping the automotive industry, offering fully customizable driving experiences and personalized data-driven features. It enhances safety by adapting to individual driving patterns through continuous learning.

However, the growing influence of GenAI outlines associated risks and regulatory obstacles. Concerns such as the potential for inaccurate or harmful AI-generated outputs are significant. The use of AI capabilities raises complex questions regarding safety, responsibility, and liability.

The competitive pressure to adopt GenAI requires organizations to proactively develop strategies to manage risks as integration becomes more widespread. A comprehensive approach is required to navigate the multifaceted challenges associated with the rapid evolution of GenAI technologies, including the introduction of new cybersecurity risks[1].

The landscape of GenAI regulations and guidelines is evolving across many industries, with the financial industry charging ahead. In December 2023, the European Parliament announced reaching a provisional agreement on the Artificial Intelligence Act[2]. This regulation will focus on ensuring fundamental rights are protected, establishing obligations for the use of AI based on risks and impact. This regulatory effort is also designed to enable the rapid proliferation of AI-based technologies across the European market.

Anticipating a similar trend, the Automotive industry is expected to witness the development of specific GenAI guidelines and risk management frameworks, focusing on ensuring safety and privacy among other concerns.

[1] https://hbr.org/2023/11/navigating-the-new-risks-and-regulatory-challenges-of-genai

[2] https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai

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

In 2023, many automotive OEMs and their suppliers continued implementing R155 for Cyber Security Management System (CSMS) and Type Approval,[3] and WP.29 R156 for Software Update Management System (SUMS).[4] Based on the second milestone of R155, its scope will become mandatory for all new vehicles in production starting in July 2024. In the past several months, some OEMs discontinued specific models based on expected R155 compliance challenges and the upcoming second milestone.[5] Together with ISO/SAE 21434,[6] these regulations are a part of the global effort to create a unified approach to protecting against cyber threats.

Due to regulatory changes, developments in industry standards, and research learnings, several organizations updated their guidelines and best practices, including the US National Highway Traffic Safety Administration (NHTSA),[7] the European Union Agency for Cybersecurity (ENISA),[8] and member trade association Auto-ISAC.[9]

It is important to note that both R155 and ISO/SAE 21434 avoid outlining specific solutions and exact processes, instead stressing the importance of implementing a high standard of cybersecurity analysis. The guidelines outline the process and specify risk analysis and response targets, emphasizing the need to consider life-long cybersecurity threats and vulnerabilities during development, production, and post-production phases.

[3] https://unece.org/sites/default/files/2023-02/R155e%20%282%29.pdf
[4] https://unece.org/sites/default/files/2024-03/R156e%20%282%29.pdf
[5] https://www.autoexpress.co.uk/news/361808/porsche-macan-canned-european-sales-stop-2024
[6] https://www.iso.org/standard/70918.html
[7] https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf
[8] https://www.enisa.europa.eu/publications/smart-cars
[9] https://automotiveisac.com/best-practices

THE REGULATORY LANDSCAPE CONTINUES TO MATURE

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

The scope of R155 is expected to expand to include motorcycles and agricultural equipment

Modern two- and three-wheeled vehicles are becoming much more connected and designed to include multiple software-components, sensors, electronic components, and advanced infotainment systems, all of which significantly increase cyber risks. The requirements to secure motorcycles are a part of the global effort to deepen safety and trust in the Automotive ecosystem.

Indeed, in July 2023, the UNECE submitted a proposal to expand the scope of R155 to include all Category L vehicles, expanding beyond the current scope that includes L6 and L7.[10] If accepted, this proposal, initiated by CLEPA, will become effective as of July 2029 and will require motorcycle OEMs to implement CSMS.

The UNECE is also discussing the option of adding Category T vehicles, agricultural machinery, as well as the related categories R (agricultural trailers) and S (interchangeable towed agricultural or forestry equipment) to the scope of R155. Amid a lack of consensus on this expansion, a decision is expected during 2024.

The EU Cyber Resilience Act promotes extended cybersecurity resilience

Updated in December 2023, the European Cyber Resilience Act (CRA) is a horizontal legislation, covering all products with digital components (both hardware and software).[11] The focal point for the CRA is consumers, safeguarding their usage of modern connected devices, from smart watches to vehicles.

The CRA covers the entire lifecycle of products, offering a framework for cybersecurity governing the planning, design, development, and maintenance of products. The CRA also requires manufacturers to report actively exploited vulnerabilities and incidents, and mitigate risks effectively through the support period of the product.[12]

[10] https://unece.org/sites/default/files/2024-03/ECE-TRANS-WP.29-GRVA-16e.pdf

[11] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[12] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet

The CRA is expected to enter into force in May 2024, with manufacturers obligated to comply within 36 months.[13] Determining the scope of the CRA is critical for OEMs and other mobility stakeholders. The CRA specifically excludes products covered by the General Safety Regulation (EU) 2019/2144,162 which also includes R155. Therefore, vehicles under categories M, N, and some in category O, will be governed by R155. Other vehicles will be subject to the CRA. As R155 expands its scope, it will also have a direct impact on the requirements to comply with the CRA.

ISO 15118 secures vehicle-to-grid communications

ISO 15118 "Road vehicles – Vehicle to grid communication interface"[14] is the leading communications standard, covering also cybersecurity features and requirements and ensuring encrypted, secure communication between the electric vehicle (EV) and the electric vehicle supply equipment (EVSE). It applies to category M and N vehicles, but encourages other OEMs to also adopt its framework. It also serves as the foundation for the high-level communication protocol (HLC) for the Combined Charging System (CCS) standard for charging EVs.

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

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

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.
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 (CPOs); cloud service providers (CSPs, e.g., edge computing & data storage); and electricity grids (e.g., utilities, building management systems, etc.).

[13] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet

[14] https://www.iso.org/standard/69113.html

New SEC cybersecurity regulations are expected to drive a wave of filings by automotive and mobility stakeholders as they are challenged with cybersecurity attacks

In July 2023, the US Securities and Exchange Commission (SEC) adopted final rules on cybersecurity disclosure for publicly listed companies.[15] The final rules, which took effect on December 15, 2023, have two components: a requirement to disclose material cybersecurity incidents (using Form 8-K) four business days after a public company determines the incident is material; and a requirement to disclose annually information (using Form 10- K) regarding cybersecurity risk management, strategy, and governance.[16]

Under the new rule, public companies traded under the SEC regulations must disclose the occurrence of a material cybersecurity incident and describe the material aspects of the nature, scope, and timing of the incident, as well as the material impact or reasonably likely material impact of the incident on the company, including its financial condition and results of operations. This disclosure is focused on the material impacts of a material cybersecurity incident. The rules also allow the delayed reporting of cybersecurity incidents that pose a substantial risk to national security or public safety—contingent on written notification by the Attorney General.[17]

In November 2023, a ransomware group, not knowing the effective date, tried to file an SEC complaint against a publicly listed company it attacked. This attack was performed against a provider of a loan origination system and digital lending platform for financial institutions. The attacker complained that its victim, the listed company, did not disclose the breach under the new rules.[18] At the time of the alleged attack, the new SEC were not in effect yet and the targeted company reported it acted immediately upon discovery to mitigate the threat. With these rules, the SEC emphasizes the importance of transparency and accountability in cybersecurity incidents and data breaches, which now must be reported to shareholders and the SEC as material events based on the well established materiality standard.

[15] https://www.sec.gov/news/press-release/2023-139

[16] https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214

[17] https://www.sec.gov/education/smallbusiness/goingpublic/SRC

[18] https://www.databreaches.net/alphv-files-an-sec-complaint-against-meridianlink-for-not-disclosing-a-breach-to-the-sec/

NHTSA updates cybersecurity best practices

In 2023, NHTSA released updated cybersecurity best practices for new vehicles.[19] While these guidelines are non-binding, their objective is to reflect evolving attack methods and the sense of urgency in mitigating cybersecurity risks across the entire ecosystem.

The standardization of cybersecurity practices across the Automotive industry, such as R155, and the release of NHTSA's Cybersecurity Best Practices for Modern Vehicles[20] signals that governments and regulators around the world understand the importance of protecting vehicles as they become more vulnerable to hacking.

The final version of this iteration considers new industry standards and research and incorporates knowledge gained from real-world incidents and comments submitted on the 2016 and 2021 drafts. NHTSA will continue to assess cybersecurity risks and update best practices as motor vehicles and their cybersecurity evolve.

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

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

The latest recommendation from NHTSA is inspired by ISO/SAE 21434 in structure and process, but is also affected by R155 as it includes the protection from remote attacks. The updated guidelines emphasize the connection between cybersecurity and safety, making it clear that as the Automotive industry becomes more connected, safety engineers and security stakeholders should also consider the ability of adversaries to manipulate signals.

NHTSA guidelines emphasize the importance of collaboration to ensure security and safety, suggesting participation in Auto-ISAC as a means of effective information sharing across the industry.

[19] https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf
[20] https://www.govinfo.gov/content/pkg/FR-2022-09-09/pdf/2022-19507.pdf

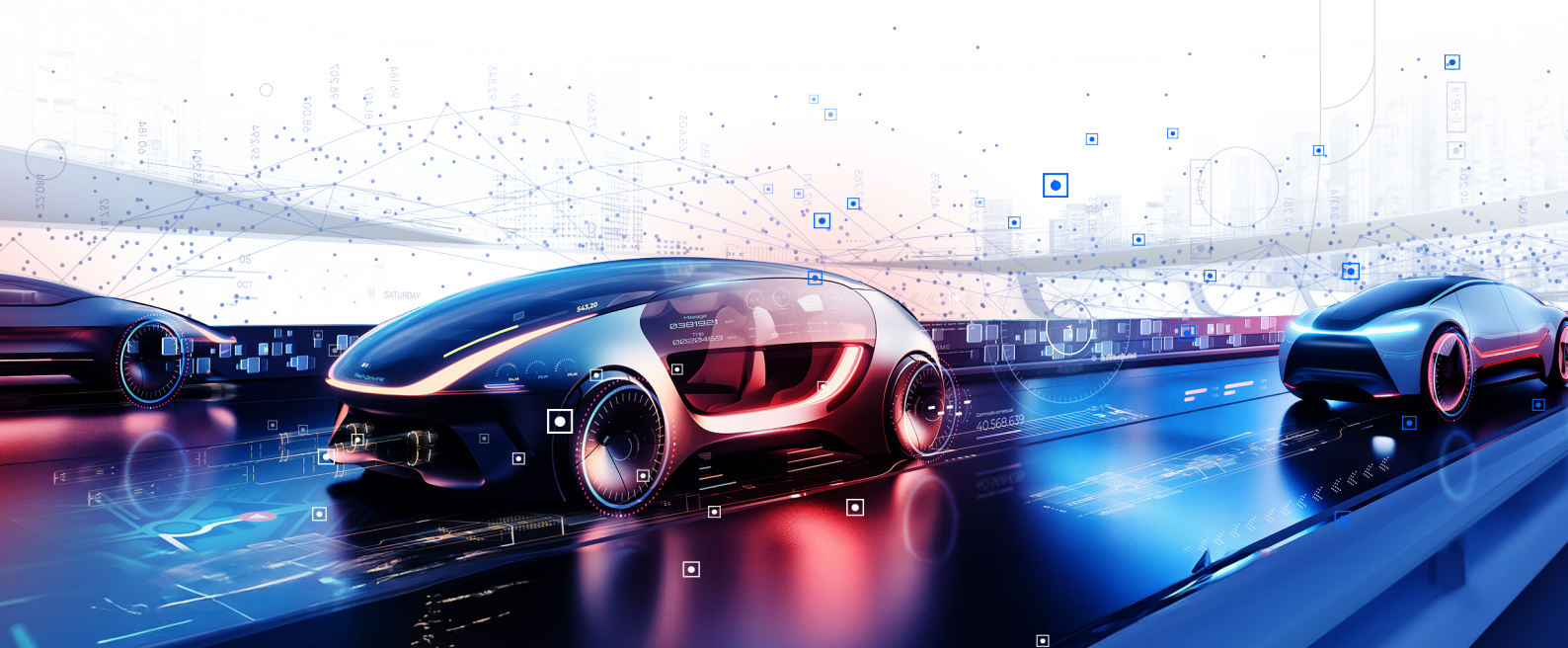
A few more NHTSA updates for 2023

In August 2023, NHTSA issued a proposed rule which requires OEMs to equip vehicles with seat belt use warning systems for the right front passenger and rear seats to increase seat belt use. The proposed regulations would apply to passenger cars, trucks, buses, and multipurpose passenger vehicles weighing less than 10,000 pounds.[21]

In September 2023, NHTSA addressed safety recommendations related to reducing speed-based traffic fatalities issued by the National Transportation Safety Board (NTSB) regarding rear impact guards and adaptive driving beam (ADB) headlamps.[22]

Both initiatives may draw the attention of fraud operators, looking for cyber-driven methods to disable safety features and manipulate vehicle systems. Once published on deep or dark web forums and marketplaces, these manipulations may be also used by other malicious actors. These potential manipulations, regardless of the motivation, not only compromise safety, but may also void warranty.

[21] https://www.nhtsa.gov/press-releases/nhtsa-proposes-seat-belt-warning-system-expansion
[22] https://www.nhtsa.gov/press-releases/nhtsa-proposes-seat-belt-warning-system-expansion



ABOUT UPSTREAM

Upstream Security offers a cloud-based automotive cybersecurity and data analytics platform purpose-built for connected vehicles and smart mobility services. Upstream's platform fuses machine learning, data normalization, and digital twin profiling technologies to detect anomalies in real-time using existing automotive data feeds. Coupled with AutoThreat® Intelligence, the first automotive cybersecurity threat intelligence feed, Upstream provides unparalleled cybersecurity and data-driven insights, seamlessly integrated into the customer's environment.

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

For more information

VISIT US AT:
www.upstream.auto

CONTACT US:
hello@upstream.auto

FOLLOW US: