2024

Upstream

GLOBAL AUTOMOTIVE CYBERSECURITY REPORT

The automotive cybersecurity inflection point:

From experimental hacking to large-scale automotive attacks—the focus shifts to impact.

TABLE OF CONTENTS

TABLE OF CONTENTS

OPENING LETTER FROM OUR CEO

It is my pleasure to present you with the 2024 Global Automotive Cybersecurity Report.

Connectivity and software-defined architectures have been at the forefront of monumental changes in the Automotive and Smart Mobility ecosystem over the past several years, but as more functionality is being exposed, cybersecurity risks are growing dramatically.

This report, which marks Upstream's sixth annual report, analyzes how Automotive and Mobility cybersecurity risks have evolved from experimental hacks to large-scale attacks, shifting the industry's focus to impact.

As predicted last year, automotive cybersecurity is reaching an inflection point. Cyber incidents have grown significantly in risk and impact, threatening safety and carrying operational implications. With threat actor motivation shifting towards large-scale impact on mobility assets, stakeholders across the ecosystem must also evaluate the potential financial implications of cybersecurity incidents.

Over the last year, the Automotive and Smart Mobility ecosystem adopted new standards and collaborated with regulators around the world on how to adapt future regulations to keep connected and software-defined assets secure. We've also been busy preparing for the upcoming second milestone of UNECE WP.29 R155, scheduled to take effect in July 2024, increasing its scope to all new vehicles.

2023 was the year of the GenAI revolution. GenAI is increasingly used by threat actors to introduce scale and new attack methods. But, in the coming months and years GenAI will also transform automotive cybersecurity tools and workflows and introduce unprecedented efficiencies to vSOC teams.

This inflection point illustrates the progress that adversaries continue to make, and reaffirms our commitment as an industry to continually innovate and deliver secure automotive and smart mobility experiences.

Upstream has led the effort to secure connected vehicles and mobility assets since 2017, when we first introduced the Upstream Platform, which proved to be a fundamental, innovative pillar in the automotive cybersecurity technology stack.

We've been helping some of the world's leading Automotive and Smart Mobility organizations—OEMs, suppliers, mobility IoT vendors, fleets and mobility service providers—comply with cybersecurity regulations and protect millions of vehicles and mobility assets.

With advanced cybersecurity tools and knowledge at our disposal, we are well-equipped to overcome the challenges in 2024 and ahead.

Best regards,

Yoav Levy
Co-Founder & CEO

METHODOLOGY

The Automotive industry relies on Upstream's continuously updated database of cybersecurity incidents.

To compile this comprehensive report, Upstream researchers investigated over 1468 incidents, some as early as 2010, and monitored hundreds of deep and dark web forums to compile this comprehensive, actionable report that will help you safely navigate the year ahead.

Upstream monitors and analyzes worldwide automotive cyber incidents to learn, understand, and help protect the entire Smart Mobility ecosystem from existing and emerging threats.

Upstream's AutoThreat®[1] cyber threat intelligence platform uses advanced technology and automation tools to constantly search all layers of the web for new cyber incidents in the automotive ecosystem and index them to the AutoThreat® platform.

Our researchers and analysts carefully categorize and analyze the data we collect to gain a deeper understanding of cyber threats, adversaries' motivation and activities, and their impact on mobility assets.

Each incident and relevant contextual data—such as the attack's geolocation, impact, attack vector, company type, and required proximity of the attacker to its target—are added to the platform to create an accurate and actionable repository.

Incidents examined in this report were sourced from the media, academic research, bug bounty programs, verified social media accounts of government law enforcement agencies worldwide, the Common Vulnerabilities & Exposures database, as well as other publicly-available online sources.

In addition to publicly reported cyber incidents, Upstream's analysts monitor the deep and dark web for threat actors that operate behind the scenes of automotive-focused cyber attacks. These incidents are discussed in a separate chapter of this report titled "Threats from the Deep and Dark Web", and are excluded from statistics and charts in other chapters, unless indicated otherwise.

While every effort has been made to identify and analyze every reported automotive and smart mobility cyber incident, there may be additional attacks that have not been publicly reported, and therefore, have not been included in this report.

Select details of the publicly reported incidents are available in the AutoThreat® Intelligence Cyber Incident Repository. Additionally, a comprehensive analysis is available to AutoThreat® PRO[2] customers.

EXECUTIVE SUMMARY

Connectivity is continuing to transform the Automotive and Smart Mobility ecosystem, increasing cybersecurity risks as more functionality is exposed. 2023 marked the beginning of a new era in automotive cybersecurity. Each attack carries greater significance today, and may have global financial and operational repercussions for various stakeholders. Upstream's 2024 Global Annual Cybersecurity Report examines how cybersecurity risks have evolved from experimental hacks into large-scale risks, focusing on safety and trust, operational availability, data privacy, and financial implications.

In 2023, Automotive and Mobility cybersecurity witnessed a dramatic shift toward large-scale incidents

The proportion of incidents with a "High" or "Massive" impact dramatically doubled from 2022 to 2023, accounting for nearly

50% of all incidents

95% of attacks were remote

64% of attacks were executed by black hat actors

Threat actors motivation has also shifted towards scale and massive impact

65% of deep and dark web cyber activities had the potential to impact thousands to millions of mobility assets.

37% of deep and dark web cyber activities had the potential to impact multiple stakeholders, on a global scale.

OEMs take a multifaceted approach to protecting connected and software-defined vehicles, as well as IoT/OT assets

- With frequent OTA updates, the SBOM is no longer static—but rather constantly evolving, long after a vehicle leaves the factory—and risk profiles continuously change.
- The growing reliance on backend systems highlights the urgent need for OEMs to safeguard both the software components and sensitive data.
- GenAI has the potential to transform automotive cybersecurity solutions and operations, enabling agile investigations, automating vSOC workflows, and even generating complex insights based on deep and dark web data and in-depth TARA.

PREDICTIONS FOR 2024

01

The competitive advantage in the Automotive industry will continue to be driven by digital transformation, requiring stakeholders to secure APIs and expand vSOC coverage to monitor API-related threats.

02

Generative AI will have a profound impact on automotive cybersecurity stakeholders, introducing new large-scale attack methods but also equipping stakeholders with advanced detection, investigation and mitigation capabilities.

03

Initial signs of regulatory fatigue, amid the maturity of UNECE WP.29 R155 and the abundance of new regulations emerging worldwide, mainly in China.

04

OEMs and Charging Point Operators (CPOs) continue to deepen cybersecurity risk assessments, and deploy cybersecurity solutions to protect strategic EV charging infrastructure.

01.

THE AUTOMOTIVE CYBERSECURITY INFLECTION POINT

From experimental hacking to large-scale automotive attacks, the focus shifts to impact

2023 MARKS THE BEGINNING OF A NEW ERA IN AUTOMOTIVE CYBERSECURITY

Connectivity has been at the forefront of monumental changes in the Automotive and Smart Mobility ecosystem over the past several years—enabling over-the-air (OTA) updates, software-oriented architectures, advanced digital experience, and a wide array of value-added applications and services.

In modern software-defined vehicles (SDVs), connectivity is used to improve and upgrade vehicles throughout their life cycle, generate revenue from a wide range of feature-on-demand services, and offer innovative data-driven customer experience, ultimately creating deeper and longer relationships with customers.

In connected vehicles, OEMs use OTA updates to fix quality and usability issues, tune core functional capabilities, and patch cybersecurity vulnerabilities quickly and cost-effectively, reducing warranty costs and recalls.

But connectivity has also posed growing cybersecurity challenges for OEMs and their supply chains—with cyber attacks becoming more sophisticated, frequent, and severe. As the attack landscape changed over the last few years, and new attack methods emerged, the industry became acutely aware that any point of connectivity can be attacked.

The first decade of automotive cybersecurity was marked by a rise in cyber incidents and attacks against OEMs and the ecosystem, continuously introducing new attack vectors and methods, even as OEMs invested in improving cybersecurity protections. **According to Upstream's research, between 2019-2023, incidents disclosed in the clear web (media) have increased by over 50%, reaching 295 reported incidents in 2023.** In 2023 alone, 95% of attacks were remote, and 64% of attacks were executed by black hat actors.[3]

Application programming interfaces (APIs) have been playing a key role in exposing vehicle functionality to drivers and enterprise applications, as well as delivering a data-driven experience. As more functionality has been exposed through APIs, cybersecurity risks have also increased dramatically, while at the same time, the cost of attacking and attack thresholds have decreased—opening the door for exponential growth in the scale and impact of attacks.

> ***In this year's report, we chose to zoom in on the impact of automotive and mobility cybersecurity risks.***

We'll focus on both external impact, which is visible to the ecosystem, and internal impact which refers to organizational efficiencies and processes.

Both internal and external impacts are assessed by different stakeholders in different ways—in this report we'll offer a framework which can be customized for each stakeholder's strategic goals, target market, relevant mobility assets, etc.

> ***External impact can be objectively measured in two dimensions:***
> ***scale and cost.***

We'll showcase how advanced connectivity and software-defined architectures continuously introduce new cybersecurity risks, attracting executives' attention across the entire ecosystem due to the potential impact on the safety of drivers, passengers and the integrity of data at massive scale, leading to astounding financial losses.

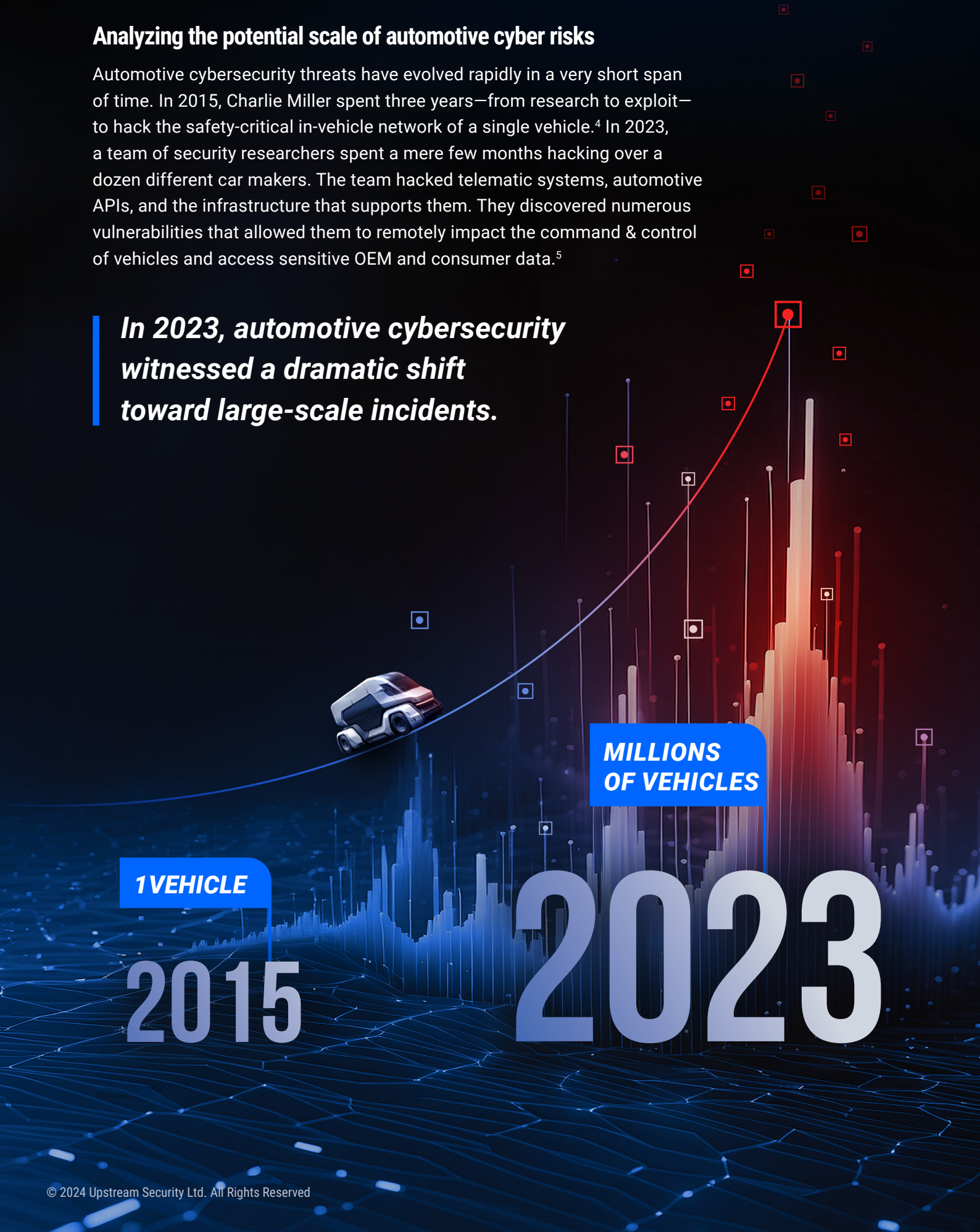
With social media becoming a major platform for consumers and professionals, threat actors are using social media to exchange knowledge with the potential to reach millions of people around the world in a matter of minutes. Based on its viral potential, social media has become one of the top distribution channels for malicious activities, both criminal and fraudulent, and should be considered when analyzing external impact and scale.

As vehicles continue to evolve well after they leave the manufacturing floor based on continuous over-the-air updates (OTAs), we'll also discuss the internal impact of cybersecurity risks on internal processes and risk evaluations that drive automotive stakeholders to adopt new frameworks and remediation processes.

Analyzing the potential scale of automotive cyber risks

Automotive cybersecurity threats have evolved rapidly in a very short span of time. In 2015, Charlie Miller spent three years—from research to exploit—to hack the safety-critical in-vehicle network of a single vehicle.[4] In 2023, a team of security researchers spent a mere few months hacking over a dozen different car makers. The team hacked telematic systems, automotive APIs, and the infrastructure that supports them. They discovered numerous vulnerabilities that allowed them to remotely impact the command & control of vehicles and access sensitive OEM and consumer data.[5]

> ***In 2023, automotive cybersecurity witnessed a dramatic shift toward large-scale incidents.***

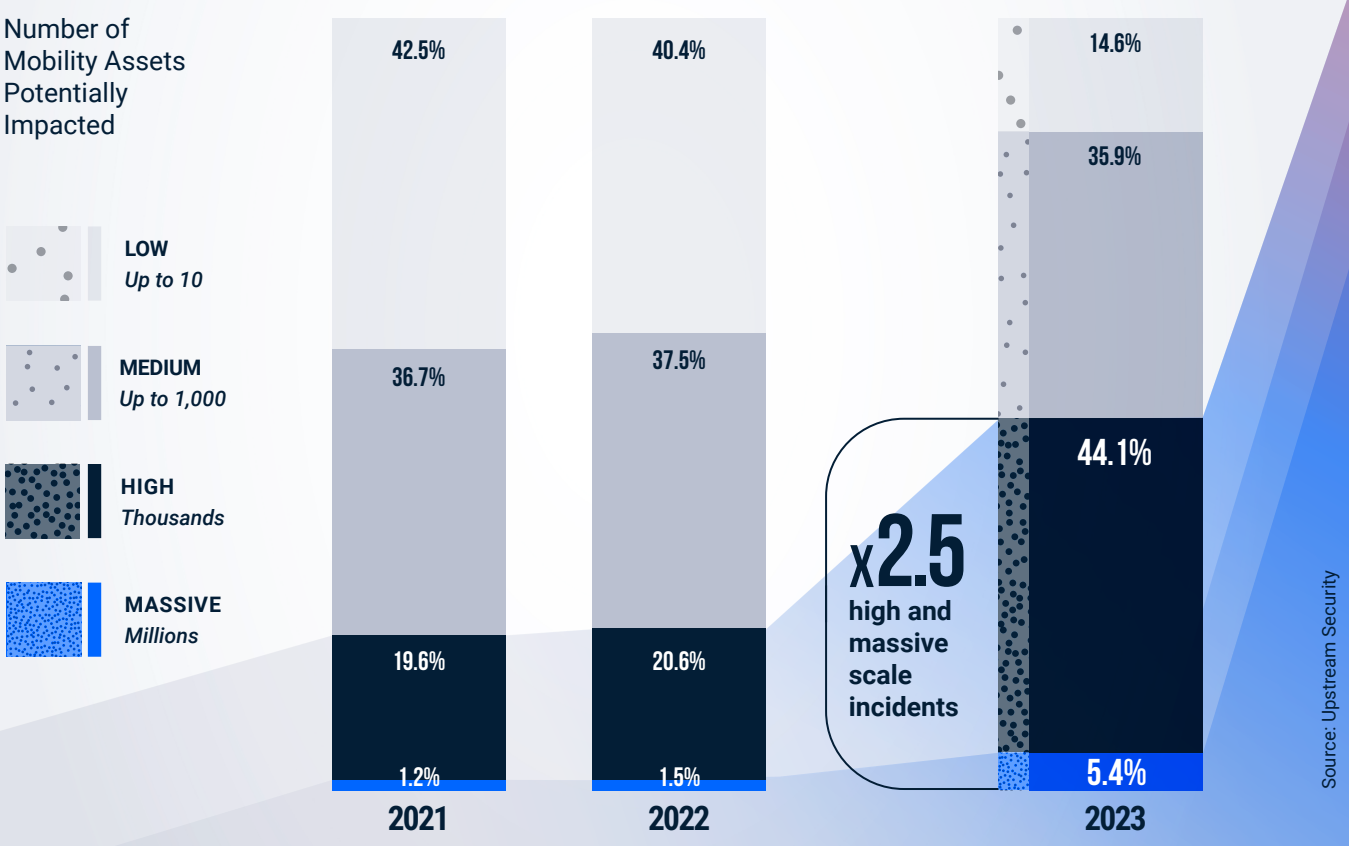


It's important to note that when analyzing scale, the focus is on potential impact. It is impossible to assess the exact impact of each incident based on publicly reported information.

Upstream analyzed publicly disclosed automotive cybersecurity incidents between 2021 and 2023 according to the potential scale of impacted mobility assets, including vehicles, users, mobility devices and more. Upstream's analysis categorized incidents according to four levels of impact—starting from "Low", which includes incidents that have the potential to impact under 10 assets, up to "Massive", which includes incidents that have the potential to impact millions of mobility assets.

IN 2023 THE PROPORTION OF INCIDENTS WITH A "HIGH" OR "MASSIVE" IMPACT DRAMATICALLY DOUBLED TO NEARLY 50%

Breakdown of publicly disclosed cybersecurity incidents by potential scale, 2021-2023



During both 2021 and 2022, “High” or “Massive” (potential to impact thousands-million of mobility assets) incidents accounted for approximately 20% of total incidents. But, in 2023, the proportion of incidents with a “High” or “Massive” impact dramatically doubled to nearly 50%.

Overall, the number of "Medium" scale attacks, which have the potential to impact up to 1,000 vehicles and mobility assets, has remained constant over the last three years. **But the number of low-scale attacks has gone down dramatically in 2023 due to the emergence of new attack vectors that enable hackers to gain control over many more vehicles and assets with lower thresholds of knowledge and resources.**

To illustrate the operational disruption impact of cyber attacks on mobility service providers consider an attack which occurred in September 2023. A leading US-based trucking and fleet management solutions provider experienced a ransomware attack that resulted in customers being unable to electronically log their on-road hours—as required by federal regulations—or track their transported inventory.[6]

In response, the company hired external cybersecurity experts to investigate the attack and applied for a waiver from the US Federal Motor Carrier Safety Administration to allow truckers to use paper logs until service was restored.[7]

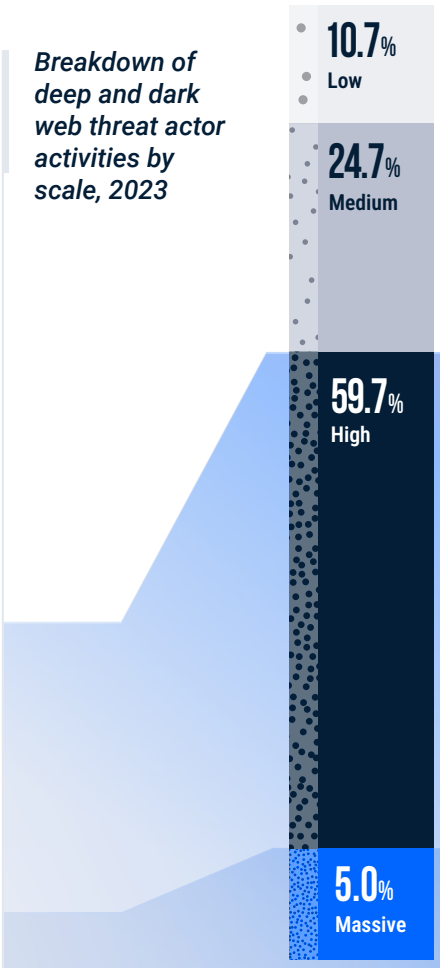
> ***Almost three weeks passed before the company was able to resolve the issue, causing serious operational disruption for thousands of truck drivers, fleet operators, and inventory management teams.***

THREAT ACTORS MOTIVATION HAS ALSO SHIFTED TOWARDS SCALE AND MASSIVE IMPACT

In addition to incidents disclosed in the media (clear web), it's critical to assess the impact of deep and dark cyber activities and the incentives driving threat actors. Based on Upstream's analysis of deep and dark web automotive cybersecurity activities, analyzing the 300 most active threat actors, nearly half of the activities (48%) were targeting more than one OEM or automotive supplier, and 37% had the potential to impact mobility assets across many stakeholders on a global scale.

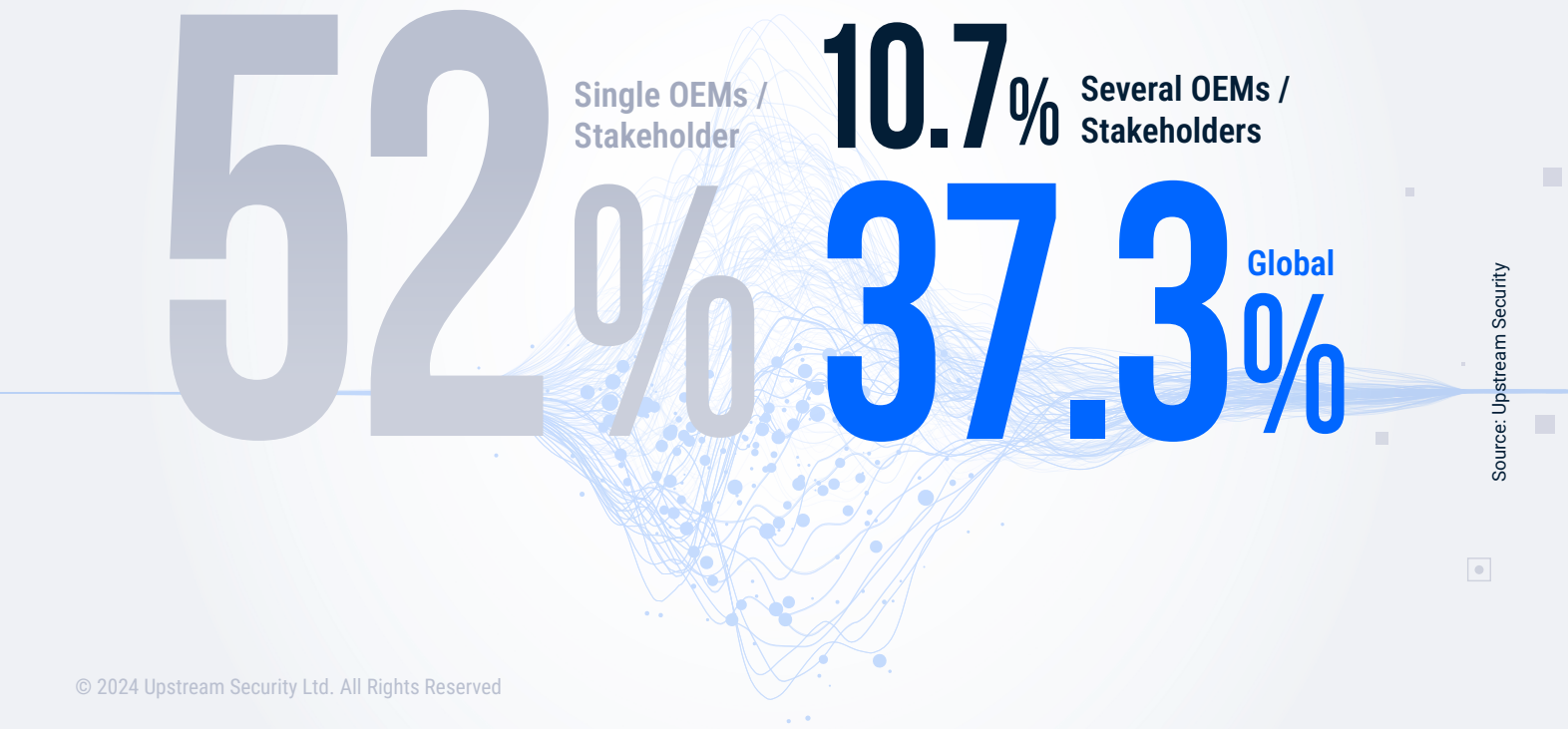
In 2023, nearly 65% of deep and dark web cyber activities had the potential to impact thousands to millions of mobility assets.

Breakdown of deep and dark web threat actor activities by scale, 2023



Source: Upstream Security

Breakdown of deep and dark web threat actor targets, 2023



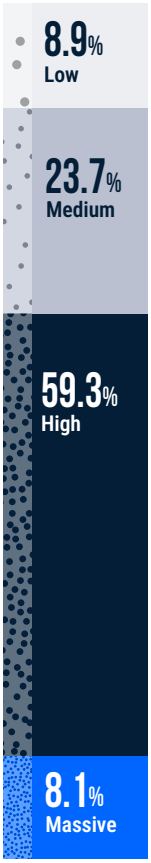
Source: Upstream Security

When zooming in on **black hat and fraud** activities in the deep and dark web, the potential scale and areas of interest also indicate a rapidly growing risk. Currently, 67% of malicious activities (threat actors categorized as black hats and fraud operators) have a "High" or "Massive" impact (compared to 45% across all actors) and 58% of activities involve multiple OEMs or have a global reach (compared to 48% across all threat actors).

> ***When analyzing the areas of interest, the impact of black hats and fraud operators continues to deepen.***

13% of activities are focused on vehicle manipulation tools, 12% of activities are focused on gaining access to sensitive data and PII, and nearly 50% are related to vulnerability exploits.[8]

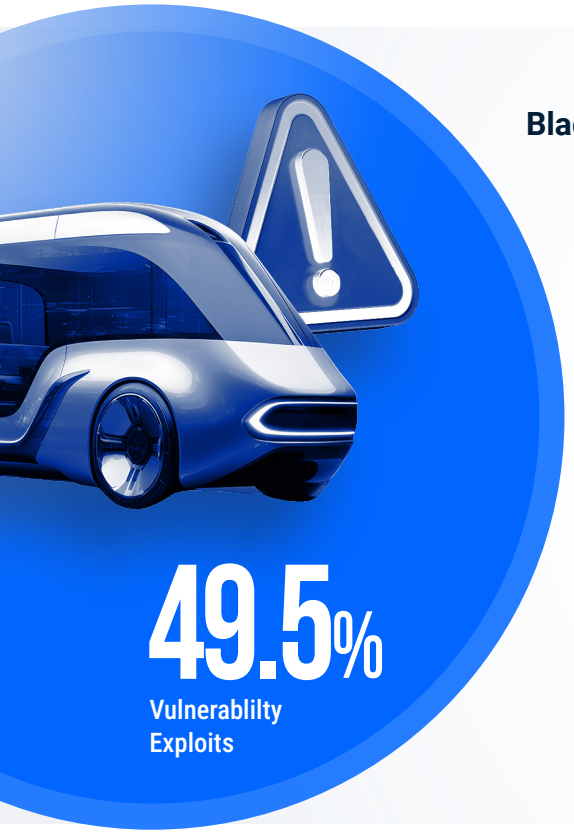
Black hat and fraud operators activities by potential scale, 2023



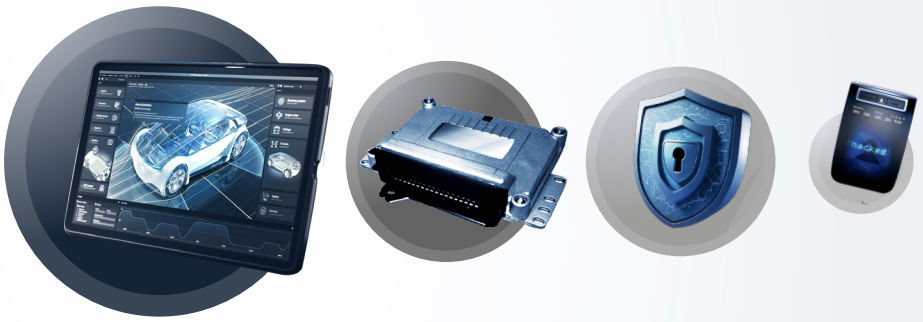
Black hat and fraud operators activities targets, 2023

Source: Upstream Security

Black hat and fraud operators activities areas of interest, 2023



49.5% Vulnerablilty Exploits



19.3% Diagnostic Software

12.6% Vehical Manipulation Tools

11.9% PII

6.7% Car Hacking Manuals

Source: Upstream Security

THE RISING COST OF CYBER ATTACKS ON THE AUTOMOTIVE AND SMART MOBILITY ECOSYSTEM

Automotive and Smart Mobility cyber attacks have severe financial repercussions leading to recalls or OTAs, production shutdowns, ransomware payments, and vehicle thefts. Additional repercussions include data and privacy breaches, which can damage a brand's reputation and customer trust and can eventually lead to large regulatory fines and diminishing revenue.

Given the shift toward large-scale cybersecurity incidents—with nearly 50% of incidents in 2023 impacting thousands-millions of mobility assets[9]—it's crucial for vehicle security operations center (vSOC) teams to analyze the financial impact of these incidents.

In June 2023, a leading Taiwan-based semiconductor manufacturer disclosed a cybersecurity incident involving a ransomware group and one of its IT hardware suppliers, which led to the leakage of information pertinent to initial setup and configuration of the system.[10] The attackers claimed to gain access to internal documents with confidential information, demanding a $70 million ransom to decrypt the data and prevent its release online—making it the largest known ransom demand in history. While the breach could affect multiple automotive stakeholders, the company reported that neither its business operations nor customer information were affected by the cyber incident at its supplier. The company also immediately terminated its data exchange with this supplier following the incident.

In November 2023, a large Australian automotive group with 12 dealerships and hundreds of employees was attacked by the same ransomware group, who stole more than 50 GB of sensitive customer and internal data. Over 91,000 files were stolen, including payroll information, lease agreements, payout information, service quotes, invoices, crash assistance forms, CRM data, registration paperwork, and employee driver and motor vehicle sales licenses. The stolen files were published at the end of November, after the ransom deadline had expired.[11]

IN JUNE 2023, A TIER-2 WAS HIT BY A $70 MILLION RANSOM DEMAND, THE LARGEST IN HISTORY.

Analyzing the financial impact of a cybersecurity incident

Trying to quantify the safety, privacy, and financial risks of automotive cybersecurity incidents is no small feat. The potential impact of automotive cyber threats is significant and can pose risks to the safety of drivers and passengers, disrupt business operations, compromise data privacy, and result in financial losses for OEMs as well as the entire supply chain.

In the next two illustrations we will analyze two incidents that occurred in 2023 and suggest a financial impact model, based on publicly available information.

> ***The goal of this framework is to highlight the massive financial impact of cybersecurity risks.***

This analysis doesn't intend to be definitive, but rather a framework for estimating a range of potential financial risks.

Key Financial Implications of Automotive Cyber Threats

Impact	Description	Methods
Vehicle Safety, Operations, & Recall	Remote or local manipulations that can modify the normal behavior of a vehicle, endangering driver safety and leading to a recall. Cybersecurity vulnerabilities in a vehicle's software components may require manufacturers to issue recalls to update and resolve the issues, ensuring the safety and proper operation of the affected vehicles.	API exploitation; Remotely invoking commands; Malicious software update; Cybersecurity vulnerability
Data & Privacy Breaches	Disclosure of information such as customer PII, vehicle performance data, or any Intellectual property (IP) data, compromising individuals or organizations.	Data breach; Data leakage; Ransomware; Injection attacks
Vehicle Theft & Break-Ins	Unauthorized entry or theft of a vehicle, often through the exploitation of vulnerabilities in the vehicle's security systems or remote services.	Keyless entry/ start engine attack; Relay attack; Signal jamming attack; API attacks
Service & Business Disruption	Impact on an organization's operations and ability to provide goods or services as a result of a cyber incident. This impact can range from partial system outages to complete shutdowns, leading to a loss of productivity, revenue, and customer trust.	Production line shutdown due to ransomware on production systems
Legal & Regulatory Compliance Issues	Cyber threats that result in violations of laws, regulations, or industry standards.	Lawsuits; Penalties
Fraud	Deceptive actions by an individual or entity, carried out with malicious intent for personal or financial gain, such as identity theft, odometer tampering, and account hacking.	Odometer tampering; Mobile companion app (user) identity theft
Brand & Reputation Damage	A negative impact on financial valuation (market cap), trust, and perception from publicly reported cyber incidents, resulting in a damaged reputation.	Widespread negative press coverage erodes consumer and investor trust

ILLUSTRATION #1

Financial impact of an EV fleet-wide vulnerability

In March 2023, a team of French security researchers participating in a hacking contest demonstrated an exploit that involved executing what is known as a time-of-check-to-time-of-use (TOCTTOU) attack on an EV OEM's gateway energy management system that allowed them to remotely perform actions (e.g., open the front trunk or door) while the car was in motion.[12]

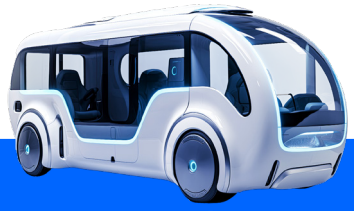
Despite the OEM's claims that this was not possible, the researchers claimed they could have remotely gained access to vehicle controls. The researchers were rewarded by the OEM with an EV and $100,000 in cash, and reported that the OEM is working on making software patches for the vulnerability and the updates should be pushed to cars soon.

INCIDENT SEVERITY
High

INCIDENT IMPACT
Potential fleet-wide implications

THREAT ACTOR TYPE
White hat

FLEET SIZE
3+ million electric vehicles



Impact	*Description*	*Baseline*	*Financial Impact*
Vehicle Safety, Operations & Recall	Aurora Labs' cost per OTA update per vehicle by type.[13] Estimations used to calculate the OTA cost: 5 large ECUs @ 500MB; 10 small ECUs @ 0.42MB.	$0.39 for Line-of-Code Update	$1,250,000 - $2,000,000
Vehicle Safety, Operations & Recall	The cost of battery replacement for vehicles with permanent battery damage.[14]	0.01% - 0.05% of fleet impacted; $15,000 per vehicle	$5,250,000 - $26,250,000
Legal & Regulatory Compliance Issues	Class-action lawsuit litigation and settlement costs for vehicles with temporary battery damage.[15]	0.5%-1% of fleet impact; $600 per plaintiff; $500,000 in legal fees	$11,000,000 - $21,500,000
		Total Potential Financial Impact	$17,500,000 - $49,750,000

ILLUSTRATION #2

Financial impact of an EV charging network data breach

In June 2023, a security researcher discovered an online database containing millions of logs (nearly a terabyte) of a global network of hundreds of thousands of electric vehicle charging stations.[14]

The internal database, hosted on one of the most popular public cloud platforms, required no password to access it and contained sensitive data of customers who used the EV charging network. Data contained names, email addresses, phone numbers of fleet customers, names of fleet operators with vehicles that recharge using the network, and vehicle identification numbers (VINs), and locations of EV public and private (e.g., residential) charging points.

INCIDENT SEVERITY
High

THREAT ACTOR TYPE
Black hat

BREACH TYPE
Unintended disclosure

BREACH SIZE
1TB of data with millions of records

CHARGING NETWOR SCALE ESTIMATION
Hundreds of thousands of charging stations in 30+ countries

Impact	Description	Baseline	Financial Impact
Data & Privacy Breach	IBM offers a detailed framework for cyber-based data breach cost estimations and a benchmark for the average cost of a mega-breach (more than 1 million compromised records) by number of records lost.[17] The costs analysis includes direct and indirect costs associated with data breach detection, escalation, notification, post-breach response, and lost business.	Average loss of $36,000,000 for data breaches that involve 1 million - 10 million records	**$30,000,000 - $40,000,000**
Legal & Regulatory Compliance Issues	GDPR Enforcement Tracker Report average fines for transportation & energy sectors, and insufficient technical and organizational measures to ensure information security.[18]	Expected range based on average fines in the transportation sector (€864,776) and insufficient measures (€1,346,050)	**$1,000,000 - $2,000,000**
		Total Potential Financial Impact	**$31,000,000 - $42,000,000**

OEMS TAKE A MULTIFACETED APPROACH TO PROTECTING CONNECTED AND SOFTWARE-DEFINED VEHICLES, AS WELL AS IOT/OT ASSETS

In this era of high-impact cyber risks, OEMs have had to adopt new internal frameworks, shifting to a multifaceted approach to protecting connected and software-defined vehicles. Connected vehicle digital experience and data-driven features are made possible by connected components, remote control, and the APIs that support them. Continuous OTA updates enable OEMs to roll out new features and functionality, and patch bugs. **The result is the emergence of the dynamic Software Bill of Materials (SBOM). As the SBOM continuously changes, it constantly requires risk and vulnerability analysis, directly impacting OEM and the supply chain cybersecurity frameworks and processes.**

The internal impact: the dynamic SBOM

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

The Automotive and Smart Mobility ecosystem acknowledges that connected and software-defined vehicles are the key to competitiveness, customer experience, operational efficiencies and future data-driven revenue streams. New research released by the World Economic Forum in collaboration with Boston Consulting Group (BCG) estimates that the emergence of SDVs will create over $650 billion in value for the auto industry by 2030, making up 15% to 20% of automotive value. OEM revenues from automotive software and electronics will grow nearly three-fold between now and 2030, from $87 billion to $248 billion, according to a BCG analysis of SDV growth.[19]

OEM REVENUES FROM AUTOMOTIVE SOFTWARE AND ELECTRONICS WILL GROW NEARLY THREE-FOLD BETWEEN NOW AND 2030, FROM $87 BILLION TO $248 BILLION, ACCORDING TO A BCG ANALYSIS OF SDV GROWTH.

While connectivity and SDVs present significant benefits, they also presents growing cybersecurity challenges for OEMs and the entire supply chain.

The distinction between hardware and software product development has become blurred, as more in-vehicle components are enabled and managed by software-oriented architectures. The decoupling of the vehicle development process from a vehicle's hardware and software integration creates a very complex and decentralized supply chain with the OEM at the center of system integration.

The Hardware Bill of Materials (HBOM) is a product development technical document that details the hardware components used to build a vehicle—such as ECUs, TCUs, infotainment systems, gauge clusters, CAN bus, and IoT controllers—each from different suppliers and supply chains with their own software and software supply chains.

The SBOM is a dynamic software development technical document that details the software components, libraries, and dependencies that are installed on a hardware component and the vehicle. Together, the HBOM and SBOM provide a comprehensive view of the supply chains, facilitating transparency and traceability to address hardware and software vulnerabilities.

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

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

Recent regulatory efforts, including UNECE WP.29 R155[20] and R156[21], ISO/SAE 21434[22], the US National Highway Traffic Administration (NHTSA) guidelines[23], and recent regulations in China[24], have mandated SBOM adoption in the Automotive industry. These regulations broaden the scope of SBOM to encompass not only OEM-developed software, but also Tier-1 and Tier-2 components and libraries—giving OEMs the ability to identify and manage software-related vulnerabilities and risks.

The ability to manipulate software components and exploit vulnerabilities poses a significant threat to the cybersecurity posture of fleet-wide control systems. By exploiting SBOM-related vulnerabilities, attackers can gain unauthorized access to critical functions and control mechanisms across entire fleets of vehicles.

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

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

> ***The growing reliance on these backend systems highlights the urgent need for OEMs to safeguard both the software components and the sensitive data stored in their backend systems.***

An ever-changing SBOM makes it extremely challenging to manage Threat Analysis and Risk Assessment (TARA) for modern vehicles. As a part of the organization's broad Risk Management efforts, TARA is a specific framework which has been developed as an in-depth yet static process**. But, TARA is rapidly evolving into a dynamic framework.** The impact of this mindset shift is dramatic, as stakeholders must adopt new tooling and platforms, and ensure teams are properly trained.

The internal impact expands with the need to add deep and dark web analysis into TARA frameworks. By integrating deep and dark web monitoring and real-time threat intelligence into the SBOM framework, OEMs can:

- Proactively identify and address vulnerabilities in software and hardware components.
- Continuously assess and manage supply chain risks to ensure integrity and security of components used in vehicles.
- Rapidly detect cybersecurity risks and attacks, and provide effective response and mitigation.

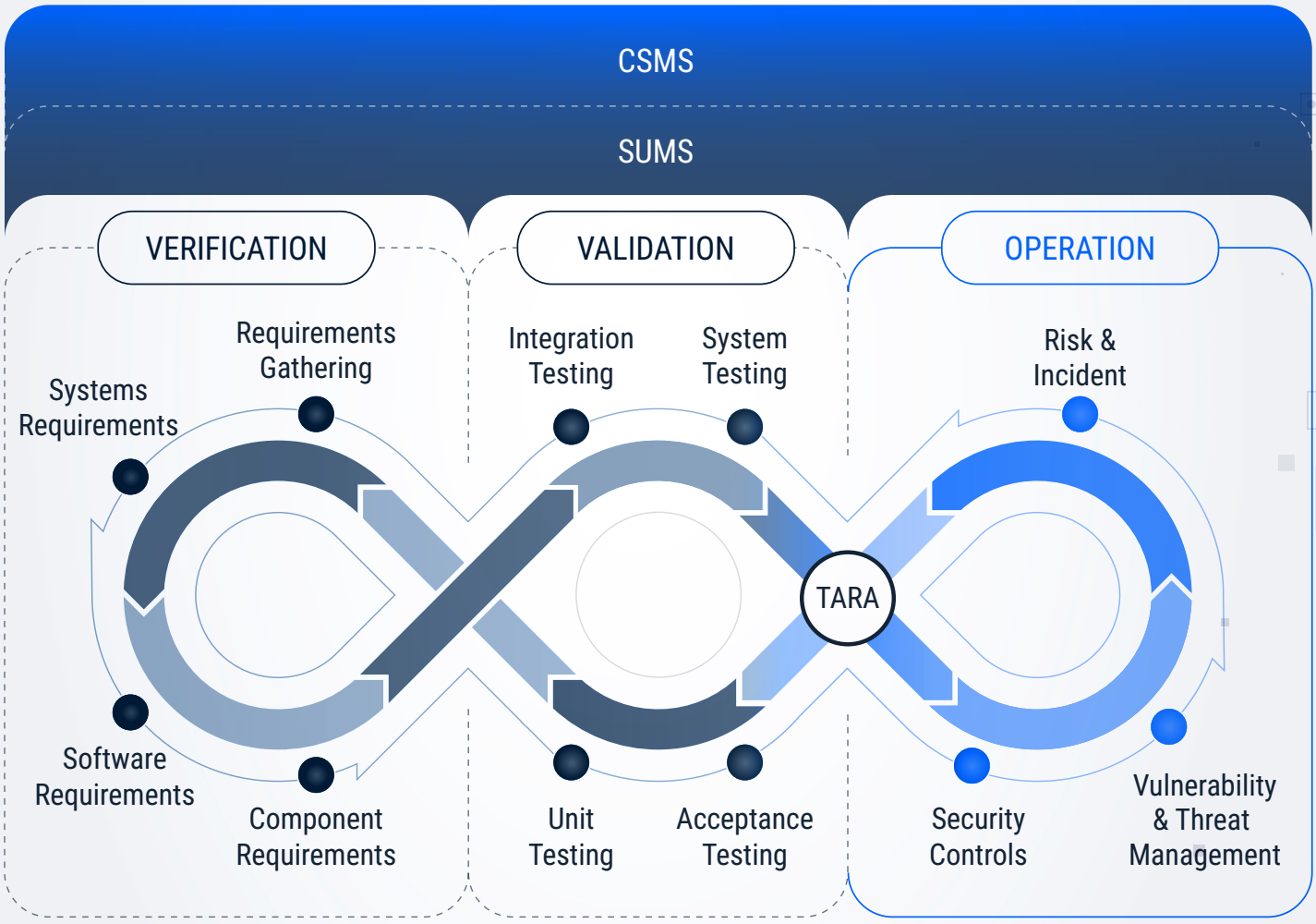
Automotive threat intelligence is now a key element in product-driven TARA, enabling proactive risk identification, prioritization, and mitigation.

A dynamic TARA framework with real-time threat intelligence based on an expanded SBOM framework is essential for OEM software development teams to enable long-term risk mitigation.

Furthermore, the vSOC adds another important layer for effective TARA, integrating real-life detected risks into the continuous TARA feedback loop. This requires adopting an interactive framework for both TARA, threat intelligence and vSOC analysts that will cooperate to ensure TARA is not only performed dynamically but also effectively.

OEMs should also link SBOM vulnerabilities, based on the dynamic TARA analysis, to enterprise security, orchestration, automation, and response (SOAR) platforms to ensure cross-organizational visibility, timely remediation, and long-term risk mitigation via focused R&D efforts.

Continuous cybersecurity orchestration:
software-defined vehicles require end-to-end software, processes, and tools



Source: Upstream Security

External APIs pose a prime attack vector for massive-scale attacks

APIs are the engine that supports automotive digital transformation, and play a crucial role in securing connected vehicles.

> ***Cybersecurity risks increase as more apps are added to support connected vehicle experiences and enable data-driven features.***

Connected vehicles and smart mobility services rely on diverse APIs, resulting in billions of transactions every month. Everything from OEM mobile companion apps, third party apps, infotainment systems, internal OEM and Tier-1 management systems, dealership systems, after-market mobility IoT devices, to EV charging management and billing apps rely heavily on APIs to achieve core functionalities.

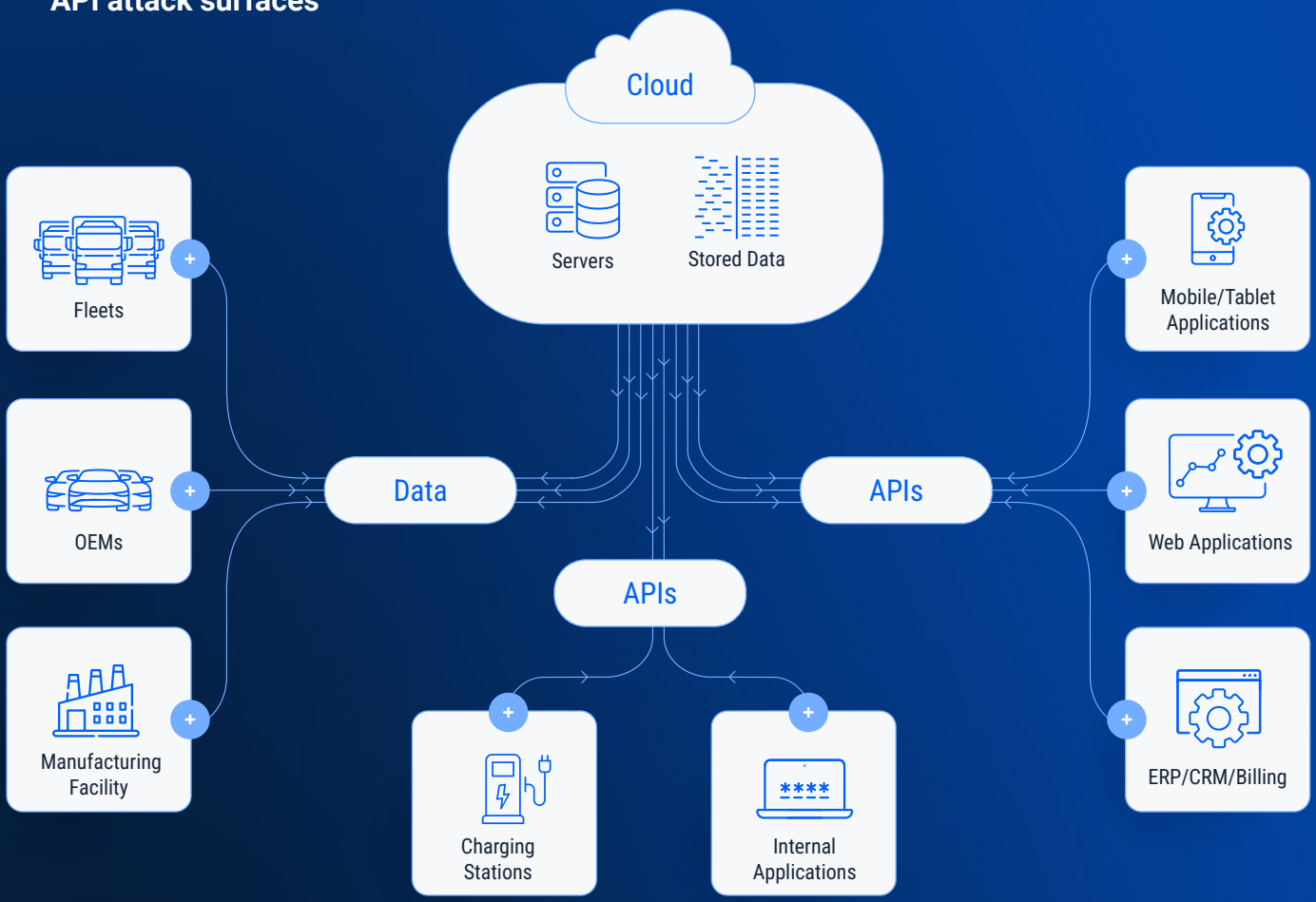
APIs also present significant and fleet-wide attack vectors and are susceptible to a wide range of cyber attacks, such as the theft of sensitive or personal identifiable information (PII), or malicious remote vehicle control.

In March 2023, a security researcher disclosed gaining access to a Japanese OEM's CRM database. The attacker modified the dev app to use the production API, which was unintentionally exposed through the loading spinner settings. This incident was a direct result of misconfigured APIs and a lack of proper authentication and verification. As a result, the researcher could access names, addresses, phone numbers, email addresses, tax IDs, and vehicle / service / ownership history of the OEM's customers.[25]

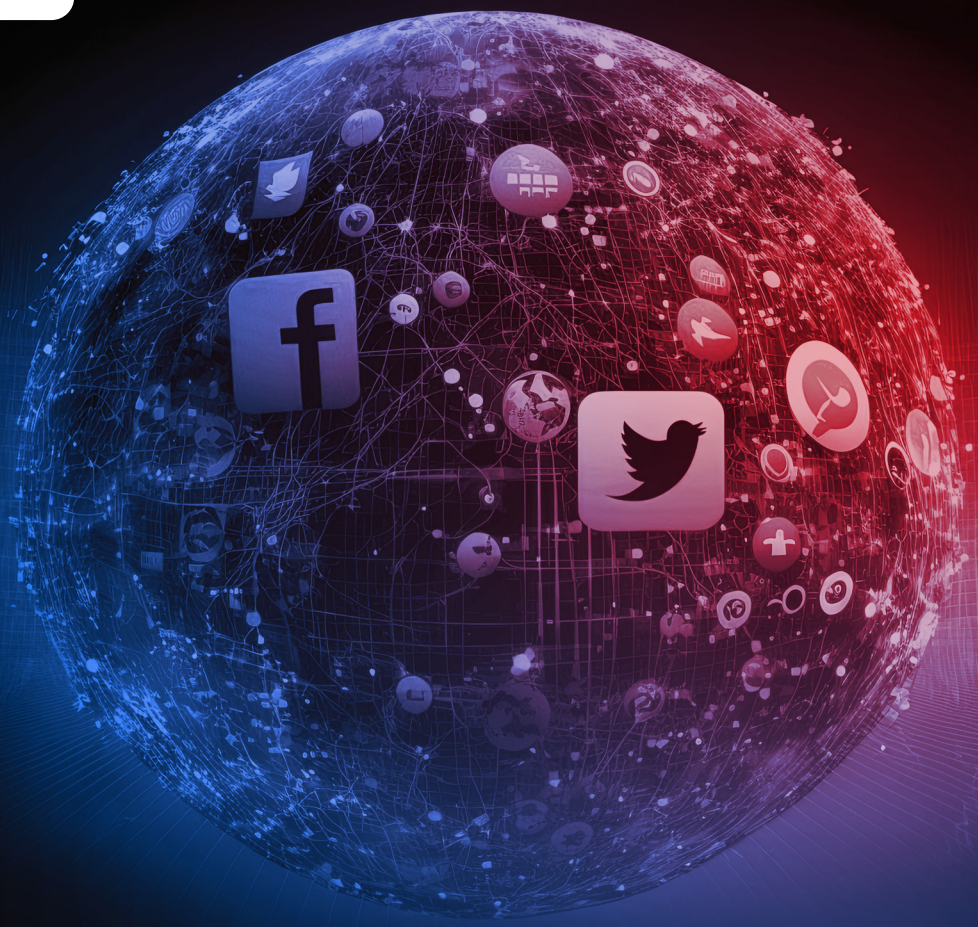
Smart mobility vendors, fleet operators, and mobility IoT devices are also threatened by API-based cyber risks that can result in large-scale operational disruption and sensitive data leakage.

In June 2023, a popular ride-hailing service in Pakistan with over 10 million users was attacked when a third-party communication API was compromised. This led to customers receiving abusive messages and notifications.[26]

API attack surfaces



Source: Upstream Security



Social Media Has Become A Breeding Ground For Automotive Cyber Activities

The impact of social media on cybersecurity cannot be overstated. With its massive reach and influence, social media has become a breeding ground for cyber activities, often blurring the lines between pop culture and malicious intent. What was once hidden in the depths of the deep and dark web is now easily exposed and accessible to a wide audience.

Thanks to social media, auto enthusiasts and hackers can now easily share their automotive hacking discoveries with a global audience.

In recent years, Facebook, TikTok, YouTube, and Instagram have become popular platforms for sharing automotive hacking tools and manuals, jailbreaks, and hacking demos - moving discussions on how to hack vehicles from the depths of the deep and dark web to the open internet.

Some automotive hacking discoveries are created and shared by cybersecurity experts and white hat hackers with the intent to raise awareness and encourage addressing risks. Other automotive hacking ploys are created and shared over social media with malicious intent.

Regardless of initial intent, information shared on social media may encourage additional threat actors, offering easy access to tools and jailbreaks.
The viral nature of social media amplifies the speed and reach of exploits, leading to reputational damage, financial losses, and operational disruption —making it crucial for OEMs to stay vigilant and adopt robust cybersecurity strategies to mitigate the risks posed by this new frontier of cyber threats.

A prime example of this is the so-called “TikTok Challenge” which went viral in October 2022, leading to the nationwide theft of tens of thousands of vehicles manufactured by one Korean OEM.

A year earlier, Milwaukee, Wisconsin, saw a significant increase in car thefts, mainly from one Korean OEM, with many of the suspected thieves being too young to drive. On social media, videos emerged showing young people joyriding in these cars—speeding and swerving, sometimes hanging out of windows. The aim of these thieves wasn’t to strip and sell parts from cars, but rather to gain social media clout and views.[27] As videos showing how to steal the vehicles spread, thefts of the Korean OEM spiked across the country the following year.[28]

In January 2023, it was reported that two of America’s largest auto insurers refused to write policies in certain cities for the affected vehicles as they were found to be easy to steal.[29]

In a February 2023 press release, NHTSA called out TikTok by name, stating that “a TikTok social media challenge has spread nationwide and has resulted in at least 14 reported crashes and eight fatalities,”[30] and advised consumers that the Korean OEM offered a free dealer-installed anti-theft software update that attempted to reduce the risk in over 8.3 million US vehicles.[31]

In May 2023, the Korean OEM also agreed to pay up to $200 million to settle one class-action lawsuit, but it still faces lawsuits from insurers and cities, with more to follow, as thefts of the affected vehicles continue to rise.

Jailbreaking infotainment systems is also trending on social media. In September 2023, unauthorized firmware updates and custom software impacting various infotainment systems of EVs from multiple OEMs were offered for sale on Facebook by a high-profile automotive threat actor.

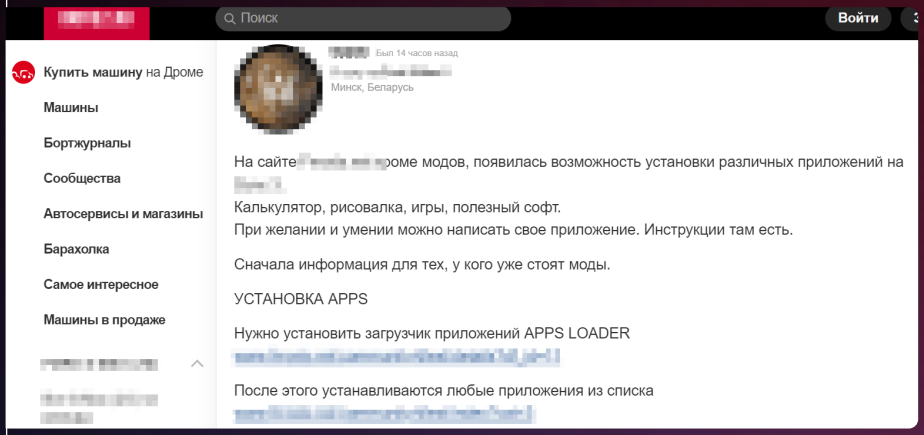
The threat actor has a large Facebook community with 44,000 followers, indicating significant exposure of the products sold, and is also highly active on other social media platforms, such as Youtube, where he publishes services and tutorials on how to conduct unofficial USB firmware updates.

In November 2023, a jailbreak that allowed unauthorized content to be installed within the head units of various OEMs was published on a popular Russian automotive social networking site, describing all the steps required for implementing the jailbreak and adding unauthorized apps to the head unit—including files for download.

Jailbreak incidents can have multiple consequences:

- As jailbreaks spread on social media platforms, the potential negative effects on vehicle cybersecurity posture, safety, consumer trust, and the Automotive industry's reputation increase.
- Jailbreaking infotainment head units can lead to stability and performance issues resulting in system failures, or compatibility problems with other features.
- Unauthorized vehicle software modification can introduce cybersecurity vulnerabilities, opening the door to hacking, which could result in theft, data breaches, or unauthorized control of the vehicle.
- Unofficial firmware updates may erode the value of official firmware updates provided by affected OEMs, making it harder to encourage customers to adopt official, tested firmware updates.
- Modifying the vehicle's firmware without authorization could void the warranty.

© 2024 Upstream Security Ltd. All Rights Reserved



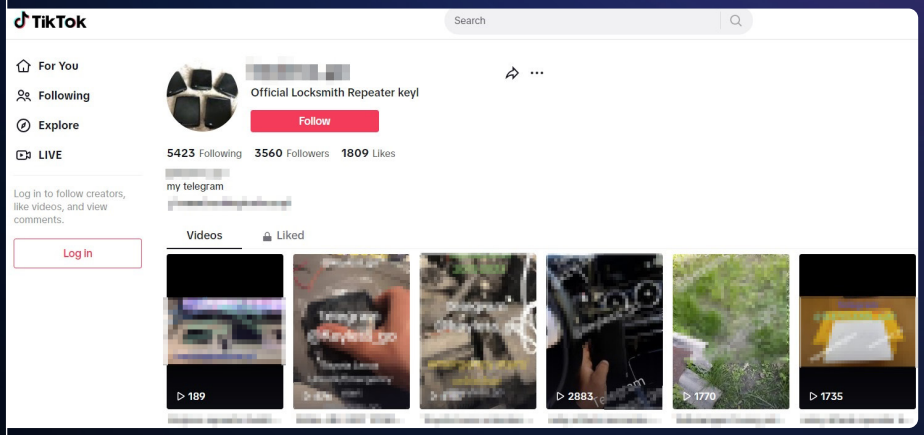
Source: Upstream Security

Post on how to implement a head unit jailbreak on a popular Russian automotive social networking site

Advanced vehicle hacking tools such as keyless repeaters, jammers, and OBD devices are also widely promoted on social media.

In May 2023, a relay attack keyless repeater promising the ability to unlock and start vehicles manufactured between 2008-2023 from multiple OEMs was offered for sale on TikTok by a threat actor promoting a Polish automotive cybersecurity and hacking ecommerce website offering a wide selection of vehicle-hacking tools.[32] Relay attack keyless repeaters make it possible for malicious actors to gain unauthorized access to a vehicle and steal it without the physical key fob.

Vehicle hacking tools are gaining widespread attention on social media platforms, resulting in immediate and severe consequences to an already massive spike in keyless vehicle theft incidents, increasing public fear and posing greater challenges for law enforcement.



Source: Upstream Security

Screenshot of the seller's TikTok page[33]

Addressing the impact of cyber activities in social media requires a coordinated effort by the Automotive industry, regulators, and social media platforms to increase public awareness and ensure that automotive technology remains safe and secure.

© 2024 Upstream Security Ltd. All Rights Reserved

THE AUTOMOTIVE AND SMART MOBILITY ECOSYSTEM IS ENTERING A NEW ERA OF GENERATIVE AI, DEMOCRATIZING ATTACKS BUT ALSO CYBER DEFENSE

The era of Generative AI (GenAI) is well underway in the Automotive industry, as OEMs rush to adopt GenAI capabilities to enhance customer experience and unleash the next wave of productivity. In 2023, a global OEM launched a ChatGPT-powered voice assistant to 900,000 beta testers using a private and secure instance of Microsoft's Azure OpenAI Service that does not share back data with OpenAI or the ChatGPT model.[34]

The GenAI revolution will have a profound impact on both automotive cybersecurity stakeholders and threat actors

GenAI is expected to become a critical tool for threat actors, enabling them to effectively perform large-scale attacks and reduce barriers to entry. By utilizing Large Language Models (LLMs), threat actors can quickly identify vulnerabilities and learn how to exploit them, standardizing their tactics, methods, and processes.

> ***APIs are specifically susceptible since attackers can use GenAI to explore API documentation, which may be publicly available, accidentally self-disclosed, or leaked on the dark web.***

GenAI can be used to map endpoints, target APIs, and identify potential vulnerabilities, as well as provide step-by-step guidance on exploiting those vulnerabilities. LLMs can also be used to generate malicious code or scripts by assimilating information from public vulnerability databases and cybersecurity research.

Threat actors can use GenAI as a tool to carry out and automate complex phishing attacks, generate convincing fake content (social engineering), and create malware that can adapt and evade detection systems.

The adaptability and efficiency allow for the execution of large-scale attacks that may bypass traditional cybersecurity measures.

LLMs trained on cybersecurity threat intelligence data can be used to escalate offensive strategies and execute sophisticated attacks with automated processes and significant scale. By analyzing vulnerabilities and attack patterns, they can generate strains of malware that self-evolve, creating variations to attack a specific target with a unique technique, payload, and polymorphic code that's undetectable by existing security measures.

For example, threat actors can use LLMs to automate the discovery of vulnerabilities, increasing efficiency and allowing them to shift resources to exploiting vulnerabilities rather than identifying them. GenAI also allows attackers to rapidly sift through vast amounts of data, identifying the most vulnerable targets. This approach not only speeds up the attack process but also increases its effectiveness, as AI models can pinpoint weaknesses that might be overlooked by human analysis.

Additionally, GenAI can simulate various attack scenarios, helping attackers refine their strategies and improve their tactics. **By using GenAI to simulate attack environments, cybersecurity faces an additional challenge, as it leads to more unpredictable and sophisticated attacks,** increasing the difficulty of detecting these attacks.

According to research by Bain & Company, mentions of GenAI on the dark web proliferated in 2023, increasing by several orders of magnitude.[35]

ACCORDING TO RESEARCH BY BAIN & COMPANY, MENTIONS OF GENAI ON THE DARK WEB PROLIFERATED IN 2023, INCREASING BY SEVERAL ORDERS OF MAGNITUDE.

Automotive cybersecurity leaders must embrace GenAI's transformative capabilities

On the defensive, GenAI has the potential to transform automotive cybersecurity solutions and operations, enabling a range of use cases—from agile investigations, to automating vSOC workflows, and even generating complex insights based on deep and dark web data and in-depth TARA.

GenAI introduces unparalleled efficiencies, enabling cybersecurity teams to quickly analyze massive amounts of connected vehicle and mobility data across multiple sources, detect patterns, filter incident alerts, and automate investigations.

> ***According to a recent report by Gartner, by 2026, more than 80% of enterprises will be using generative AI APIs and models and/or will be deploying GenAI-enabled applications in production environments, up from less than 5% in 2023.[36]***

In 2023, Upstream launched its own GenAI-enabled application (alpha release) that helps automotive stakeholders transform the vSOC through improved investigations, automation, data insights, and detailed analytics. With today's vSOC absorbing massive amounts of data from multiple sources, GenAI helps draw insights by querying the data with simple NLP questions. Upstream's GenAI-powered solution continuously monitors trends, providing context and analysis of impact.

02

AUTOMOTIVE CYBERSECURITY TRENDS

Automotive and Smart Mobility stakeholders face new challenges as cybersecurity attacks grow in scale and impact

INCIDENTS

2023 saw an increase in the scale and impact of cybersecurity attacks, creating new challenges for the automotive and smart mobility industries.

During 2023, Upstream's AutoThreat® researchers analyzed 295 automotive and smart mobility cybersecurity incidents—an average of 25 incidents per month.

The top incidents in 2023:

JANUARY

- Researchers discovered critical vulnerabilities that allowed them to remotely control vehicles of major global OEMs and access sensitive consumer PII.[37]
- A head unit installed in several South Korean OEM vehicles was compromised.[38]

FEBRUARY

- Japanese OEM affected by data breach in its Global Supplier Preparation Information System.[39]
- Global OEMs released an emergency patch for an actively exploited vulnerability that triggered a sharp rise in car theft incidents.[40]
- New destructive car theft methods using a CAN bus manipulation reported to be on the rise.[41]

MARCH

- US OEM vehicles hacked within two minutes by researchers participating in a hacking contest.[42]
- Japanese OEM's Customer Relationship Management (CRM) system was hacked by a security researcher.[43]
- German, South Korean, and Japanese OEMs were targeted as part of a supply chain attack on a VoIP software vendor.[44]

APRIL

- Researchers reported a critical CAN bus vulnerability that allowed proximate attackers to steal Japanese OEM vehicles.[45]
- Security researchers discovered critical vulnerabilities impacting a South Korean OEM's in-vehicle infotainment system.[46]

MAY

- Attack against a Japanese OEM exposed 10 years of customer data, including vehicle geolocation, in a data breach.[47]
- Swiss multinational automotive supplier hit by large-scale ransomware attack impacting business operations.[48]
- German automotive service provider hit by cyber attack, impacting accessibility to several systems.[49]

JUNE

- A security researcher discovered multiple vulnerabilities in a popular network messaging protocol that enabled fleet-wide manipulation of telemetry data.[50]
- South Korean OEM's infotainment unit hacked despite security fixes.[51]
- A US EV charging station network suffered a major data breach that exposed sensitive company data and customer PII.[52]

JULY

- US EV charging company's chargers hacked to display unauthorized content and images.[53]
- Ransomware attacks disrupted Japanese port operations, impacting the availability of major Japanese OEM auto parts.[54]
- API vulnerabilities in a German OEM's website enabled malicious data exfiltration.[55]

AUGUST

- Security researchers jailbreaked the infotainment system of a US-based EV OEM.[56]
- Security researchers discovered vulnerabilities in a popular mobility provider, enabling account hijacking and illegal financial transactions.[57]
- US EV OEM suffered data breach impacting over 75,000 employees.[58]

SEPTEMBER

- US trucking and fleet management solutions provider experienced a ransomware attack that resulted in customers being unable to electronically log their on-road hours or track their transported inventory.[59]
- Mass transit company in Germany affected by cyber attack on service provider.[60]
- One of the UK's largest logistics groups declared insolvency following ransomware attack.[61]

OCTOBER

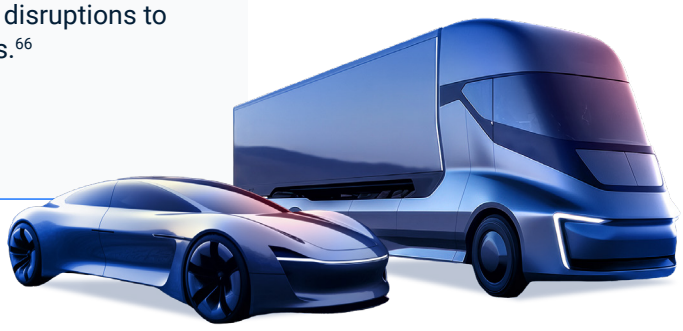
- A large US moving and storage rental company experienced a cyber attack, resulting in alleged leakage of 13GB of employee and operational data.[62]
- Brazilian dealership of a German OEM was hit with a ransomware attack.[63]

NOVEMBER

- A major US auto parts distributor suffered a data breach affecting over 180,000 employees and clients.[64]
- Major Chinese automotive supplier for global OEMs impacted by ransomware attack.[65]
- A US state transportation department impacted by a cyberattack, resulting in significant disruptions to its services.[66]

DECEMBER

- Researchers discovered a critical vulnerability in fleet management software affecting multiple vehicle fleets.[67]
- Japanese OEM impacted by a cyberattack in Australia and New Zealand, leading to a data breach posing risk to customer PII.[68]



MOST ATTACKS IN 2023 WERE CARRIED OUT BY BLACK HAT ACTORS

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

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

Black Hat

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

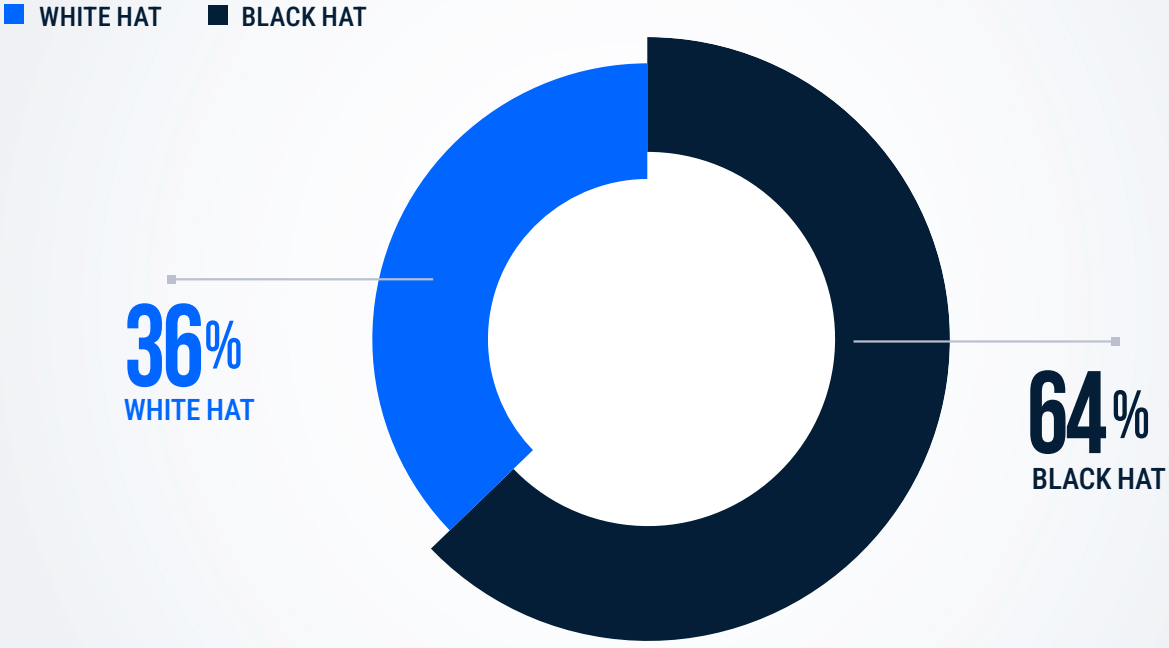
White Hat

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

Gray Hat

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

Most attacks in 2023 — 64% of incidents — were carried out by black hat actors



Source: Upstream Security

There is a major difference between automotive black hat attacks and IT black hat attacks, regarding the consequences and impact of their actions. Automotive black hat attacks—which are closely aligned with cyber attacks on critical OT infrastructure, such as health, energy, and governmental facilities—result in not only disruption of services and financial losses, but also potential for safety hazards and loss of lives.

In September 2023, a leading US-based trucking and fleet management solutions provider experienced a ransomware attack that resulted in customers being unable to electronically log their on-road hours—as required by federal regulations—or track their transported inventory.[69] In response, the company hired external cybersecurity experts to investigate and applied for a waiver from the US Federal Motor Carrier Safety Administration to allow truckers to use paper logs until service was restored.[70]

In June 2023, a Korean OEM's in-vehicle infotainment system was hacked after it issued a security update.[71] In a previous attack, the same hacker gained root access to the Linux-based system via the engineering menu and firmware image manipulation—enabling him to run custom applications. The OEM responded by releasing a new firmware image and removing the old firmware images. The OEM engineers also used a private key to sign firmware images, but didn't ensure the updater always verified the signature, which allowed the attacker to gain root access and install unsigned code—again.[72]

In December 2023, researchers reported that a fleet management software vendor ignored a dangerous telematics gateway vulnerability that had been reported in April 2023. This vulnerability poses a significant risk, since hackers may be able to target the backend infrastructure to manipulate and shut down entire fleets—impacting tens of thousands of vehicles. It is unclear to what extent these gateways were used, but the vendor is tracking over 119,000 vehicles in over 49 countries. There have been no known exploits of the vulnerability.[73]

In response to OEMs' growing use of in-vehicle subscriptions for connected services and software-enabled features, gray hat hackers are constantly looking for ways to bypass security measures to install their own applications or gain free access to paid services. Moreover, the vulnerabilities they expose, and often discuss in forums on the deep and dark web, can be exploited by black hat actors.

NEARLY ALL ATTACKS CONTINUE TO BE EXECUTED REMOTELY

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

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

Remote attacks have consistently outnumbered physical attacks since 2010, and they continue to grow—accounting for 89% of all attacks between 2010 and 2023, and 95% in 2023. The vast majority of remote attacks in 2023 were long-range attacks (85%). The percentage of long-range attacks has increased, rising from 70% in 2022, as a result of the adoption of connectivity and software-defined architectures.

Nearly all 2023 incidents were remote

The vast majority of remote incidents in 2023 were long-range

Source: Upstream Security

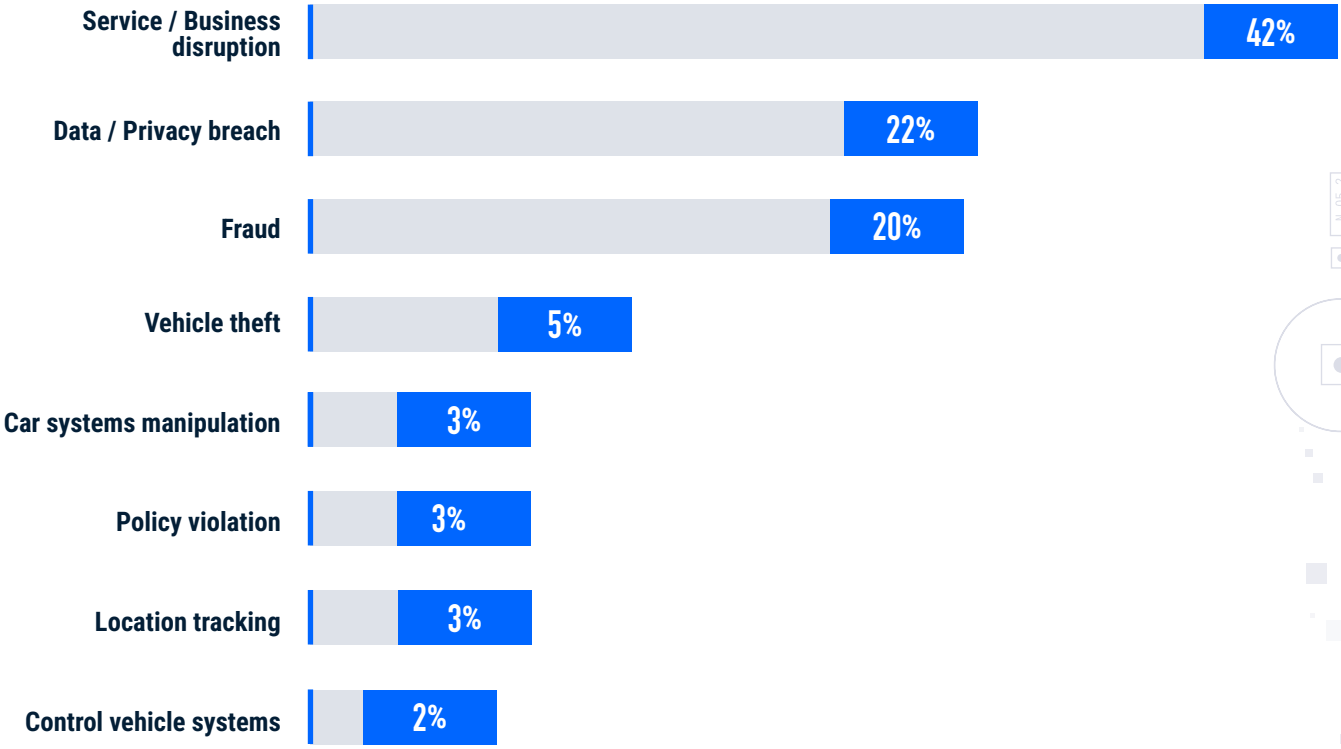
ATTACKS ARE BECOMING MORE IMPACTFUL

The Automotive and Smart Mobility ecosystem is increasingly impacted by cyber attacks. Attacks on vehicles often compromise sensitive data, but can also have far-reaching consequences, including safety hazards, business disruption, vehicle theft, system manipulation, and fraud.

Operational service and business disruption is continuously on the rise, accounting for 42% of incidents, up from 40% in 2022. We have also witnessed a dramatic increase in fraud-related incidents, accounting for 20% of 2023 incidents and up from 4% in 2022.

Service / Business disruption	Disruption to normal business operations, such as delays or halts in production, caused by a cyber attack (e.g. OEM or Tier-1 supplier ransomware attack, operational fleet disruption caused by a cyber attack on systems or devices).
Data / Privacy breach	A data breach occurs when a threat actor gains unauthorized access to proprietary, confidential data, such as intellectual property (IP), trade secrets, financial information, or personally identifiable information (PII). Cybersecurity incidents involving data breaches are the most common and most expensive.
Fraud	Illegal use of vehicle data and/or vehicle consumer data by threat actors for financial gain.
Vehicle theft	Vehicle thefts involving long-range, short-range, and physical attacks by threat actors.
Car system manipulation	Threat actor activities targeted at tampering with various in-vehicle systems, changing their expected operational behavior and potentially creating safety risks.
Policy violation	Threat actors' actions that violate established rules, regulations, or policies regarding the use, operation, or management of vehicles.
Location tracking	Illegal use of GPS navigation data to track a vehicle's location and movement without user or owner consent.
Control of vehicle systems	Threat actors can take full or partial control of a vehicle from long distances by overriding its systems through connected components.

2023 impact breakdown, based on 295 automotive-related cyber incidents



Source: Upstream Security

CVES MUST BE CLOSELY MONITORED

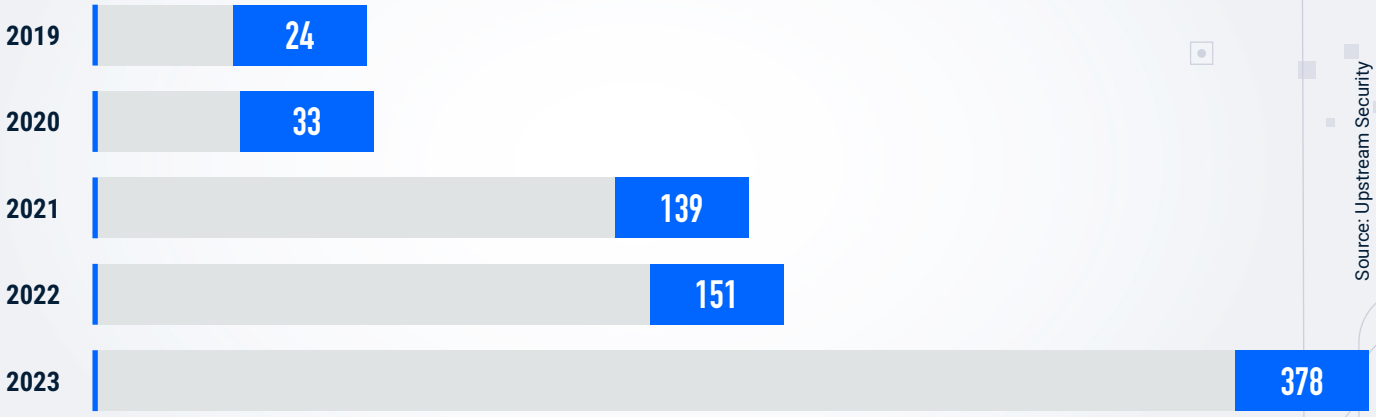
The Common Vulnerability Scoring System (CVSS) was designed to provide an open and standardized method for rating CVEs. CVSS helps organizations prioritize and coordinate joint responses based on the vulnerability's base, temporal, and environmental properties.[74] Vulnerabilities are also graded from Critical, High, Medium to Low, or None, based on their CVSS score.[75]

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.

The Automotive industry has recorded 725 specific CVEs since 2019; 378 CVEs were published in 2023, compared with 151 in 2022.

The 150% increase in CVEs in 2023 can be attributed to the continued proliferation of connected components and the growing awareness of stakeholders to proactively identify vulnerabilities.

Number of automotive-related CVEs found in 2019-2023



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. In addition to affecting risk assessments across the fleet, CVEs can also be considered when strategically designing the fleet composition.

OVERVIEW OF 2023 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.

Although CVEs disclose critical vulnerabilities, they can also be exploited by hackers.

Breakdown of publicly reported automotive-related vulnerabilities (between 2019-2023)

CVEs

Source: Upstream Security

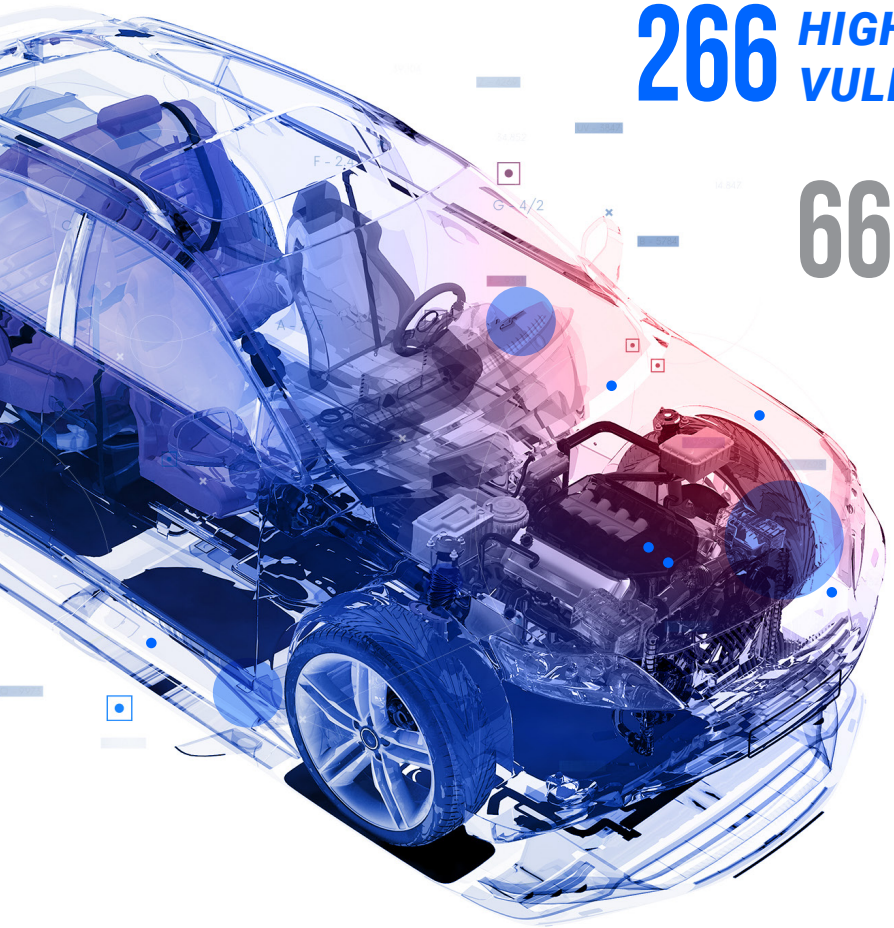
IN 2023, THE CVSS-SCORED VULNERABILITIES ANALYZED BY UPSTREAM'S ANALYSTS HAD:

34 ***CRITICAL VULNERABILITIES***

266 ***HIGH VULNERABILITIES***

66 ***MEDIUM VULNERABILITIES***

12 ***LOW VULNERABILITIES***



Source: Upstream Security

Together with the sharp increase in automotive-related CVEs in 2023, we also witnessed a rise in severity. In 2023, critical and high vulnerabilities accounted for nearly 80% of total CVES, up from 71% in 2022. This trend amplifies the importance of closely monitoring automotive-specific CVEs by all stakeholders and proactively detecting exploits, as well as prioritizing mitigation.

THE IMPACT IS FELT ACROSS THE SMART MOBILITY ECOSYSTEM

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

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

Source: Upstream Security

A growing number of sectors that have expanded their digital footprints, such as EV charging, fleet management, and mobility sharing applications, face not only ransomware attacks but also attacks targeting infrastructure and public safety.

OEMS AND SUPPLIERS SHARE RESPONSIBILITY

Besides costly recalls, brand damage, and loss of data, cyber attacks against OEMs and their component suppliers have led to production shutdowns. In June 2023, a US-based Tier-1 supplier of high-performance alloys for the Automotive industry began experiencing a network outage indicative of a cybersecurity incident.[76] For the next 11 days, many aspects of the company's production were substantially disrupted—including administrative, sales, financial, and customer service functions. The company reported that the lost production time impacted net revenues by roughly $18-20 million, and diluted earnings per share by approximately $0.40-$0.45.[77]

As OEMs rely heavily on suppliers, the risk of cyber attacks is compounded. A hacker can exploit a vulnerability in a Tier-1 or 2 component supplier to gain direct access to the vehicle itself.

In August 2023, a Dutch Tier-1 supplier of electromagnets was hit by a ransomware attack in which the ransomware group gained unauthorized access to the company's business systems, disrupting its development and sales departments. The ransomware group is known for deploying models such as double-extortion, initial access broker affiliates, and advertising on hacker forums. In response, the company hired leading third-party cybersecurity experts and activated its response protocol, including its business continuity plan.[78]

The EV charging ecosystem is rapidly expanding

Concerns over grid cybersecurity and charging infrastructure increase as the number of EVs grows. The fast adoption of EVs has resulted in the relatively rapid development and deployment of charging infrastructure—often overlooking cybersecurity best practices and vulnerabilities.

Chargers are vulnerable to physical and remote manipulation that can manipulate their functionality, and expose EV users to fraud, data breaches, and even ransom attacks. There are also emerging threats associated with various charging attack vectors, including vehicle-to-charging network, grid-to-vehicle, and grid-to-fleet.

In January 2023, a security researcher exploited a popular screen sharing program to gain access to the underlying Operating System (OS) of a new 350-kW charger from a US EV charging company. The researcher could access the OS menu, open the web browser, and navigate to a competitor's website

while the charger app remained running in the background.[79] An earlier incident occurred in which another hacker gained access to the charger's critical settings and could view functions such as overheat protection.[80]

In July 2023, security researchers published a detailed report highlighting three critical vulnerabilities found in the API interfaces of a Charging Station Management System (CSMS) of a Switzerland-based provider, allowing adversaries to access files uploaded by other users, bypass the required provisioning PIN code (authentication), and hijack a charger's OCPP connection.[81] **The researchers demonstrated attack vectors that expose drivers' data and impact service availability of the vendor's provisioning process, management, and operations of charging stations.**[82]

In May 2023, security researchers reported a vulnerability, known as CVE-2023-29857,[83] in a popular 3rd-party application used by owners of US EV OEM. The vulnerability allows attackers to obtain sensitive information via directly accessing the application link.[84]

Commercial fleets

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

In September 2023, a leading US-based trucking and fleet management solutions provider experienced a ransomware attack that resulted in customers being unable to electronically log their on-road hours—as required by federal regulations—or track their transported inventory.[85] In response, the company hired external cybersecurity experts to investigate and applied for a waiver from the US Federal Motor Carrier Safety Administration to allow truckers to use paper logs until service was restored.[86]

Smart mobility IoT devices & services

As smart mobility IoT devices and services continue to grow in popularity and use, they represent high-risk targets within the Smart Mobility ecosystem.

These services and devices hold sensitive PII and payment data from thousands of unique users.

In July 2023, a cyberattack targeted the servers of a Polish city's Transport Authority, halting smart transportation systems. The attack impacted the city's public transportation ticketing system, traffic lights management, and electronic information boards at public transportation stops—causing city-wide traffic jams.[87]

Insurance

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

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

Autonomous vehicles

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

In October 2023, California ordered a US OEM's AV to remove its driverless cars from state roads, after a pedestrian in San Francisco was struck by a human-driven vehicle and then run over by a robotaxi.[88] In November 2023, the same OEM recalled its entire US fleet of 950 driverless cars, but is currently planning a slow return to service as it works to overcome safety concerns and a lack of public trust.[89]

Despite this, other AV companies are forging ahead with their own deployments and trials, acknowledging the above problems as the result of scaling too quickly before the technology was ready.[90]

This was demonstrated by the many announcements made in 2023:

- In July 2023, Waymo's co-CEOs announced that given the tremendous momentum and substantial commercial opportunity they're seeing on the ride-hailing front, they've made the decision to focus efforts and investment in ride-hailing—pushing back the timeline on technical, commercial, and operational efforts on trucking.[91]

- In August 2023, Axios reported on several autonomous trucking companies that conducting testing in the Dallas-Fort Worth area—including Aurora, Gatik, Torc Robotics, and Kodiak Robotics—which expect to deploy driverless trucks in the next couple years.[92]

- In October 2023, Waymo announced a partnership with Uber to offer a fully autonomous, all-electric Waymo ride in the 225+ square miles of Metro Phoenix where Waymo currently operates.[93]

- In November 2023, May Mobility, which is backed by Toyota and BMW, announced a new funding round of $105 million to expand its on-demand driverless transit shuttles in a handful of cities in Arizona, Michigan, Minnesota, and Texas.[94]

- In November 2023, Motional, an AV developer, and Hyundai announced plans to jointly build IONIQ 5 robotaxis in Singapore for deployment in Las Vegas and other US cities in 2024.[95]

- In December 2023, Japan decided to assign an exclusive bandwidth for Level 4 self-driving vehicles.[96]

On the technical side, new sensor types, software and hardware functionalities, services, and communication types expose potential vulnerabilities, increasing the likelihood of a future attack. Autonomous vehicles are equipped with and rely upon navigator sensors (e.g., GPS, LIDAR, cameras, millimeter wave radar, IMU) that receive data and directions from multiple sources, including the internet and satellites.

It is therefore possible for attackers to prevent the sensor from retrieving useful data, cause it to retrieve incorrect data, or manipulate the sensor's function through crafted data.[97]

The impact of Right to Repair on agriculture vehicles

Conflicts over the US Right to Repair of agricultural vehicles continued to make big headlines in 2023.

Agriculture vehicle owners, in particular, have turned to tractor hacking to bypass restrictions put in place by equipment manufacturers to prevent them from doing their own repairs, and to avoid digital lockouts on modern rigs.

Some farmers are circumventing OEM restrictions by installing pirated firmware, which may leave them exposed to malware, spyware, or ransomware. Additionally, farmers looking to self-repair their equipment without turning to authorized dealers may turn to online forums where they discuss software bugs, how to manipulate their vehicle systems, and swap code and data. Using unauthorized software and hacking equipment for self-repair can result in unintended installation of malware, spyware, ransomware and invalidate manufacturer warranties.

In response to the right to repair movement, several bills have been introduced across the US. It is their goal to require equipment manufacturers to provide software, codes, and tools to farmers and independent technicians so they can repair equipment themselves.

- In April 2023, Colorado became the first state to pass a right to repair law for farmers—which will go into effect at the start of 2024.[98]

- In June 2023, the American Farm Bureau Federation signed a memorandum of understanding (MOU) with CLAAS of America, providing even more farmers and ranchers with the right to repair their own farm equipment.[99] In 2023, AFBF entered into similar MOUs with John Deere, CNH Industrial Brands (which includes Case IH and New Holland), AGCO, and Kubota. In total, the five MOUs cover almost three-quarters of the agricultural machinery sold in the US.

- In November 2023, a US judge rejected Deere's efforts to dismiss consolidated lawsuits and said Deere must face claims from crop farms and farmers that the agricultural machinery maker has unlawfully conspired to restrict services for maintenance and repair.[100]

Regulators worldwide are shifting focus to the growing cyber risks caused by the Right to Repair Act before they reach a “tipping point”. In June 2023, NHTSA notified dozens of OEMs about safety concerns arising from the Massachusetts Right to Repair Act.[101] The NHTSA reiterated that manufacturers must comply with all federal safety requirements. These recent developments and clear indications by NHTSA serve as important guidelines for OEMs and provide a path for future resolution of this conflict.

03

2023’S DIVERSE ATTACK VECTORS

Smart Mobility and Automotive stakeholders must be aware of emerging threats and the impact they post of cyber resilience

INCREASINGLY SOPHISTICATED ATTACKS OPEN THE DOOR FOR LARGE-SCALE IMPACT ACROSS THE ENTIRE ECOSYSTEM

In 2023, cyber attacks became more sophisticated and frequent, targeting various vehicle systems and components, as well as smart mobility platforms, IoT devices and applications. New attack methods have made the industry acutely aware that any point of connectivity is vulnerable to attacks.

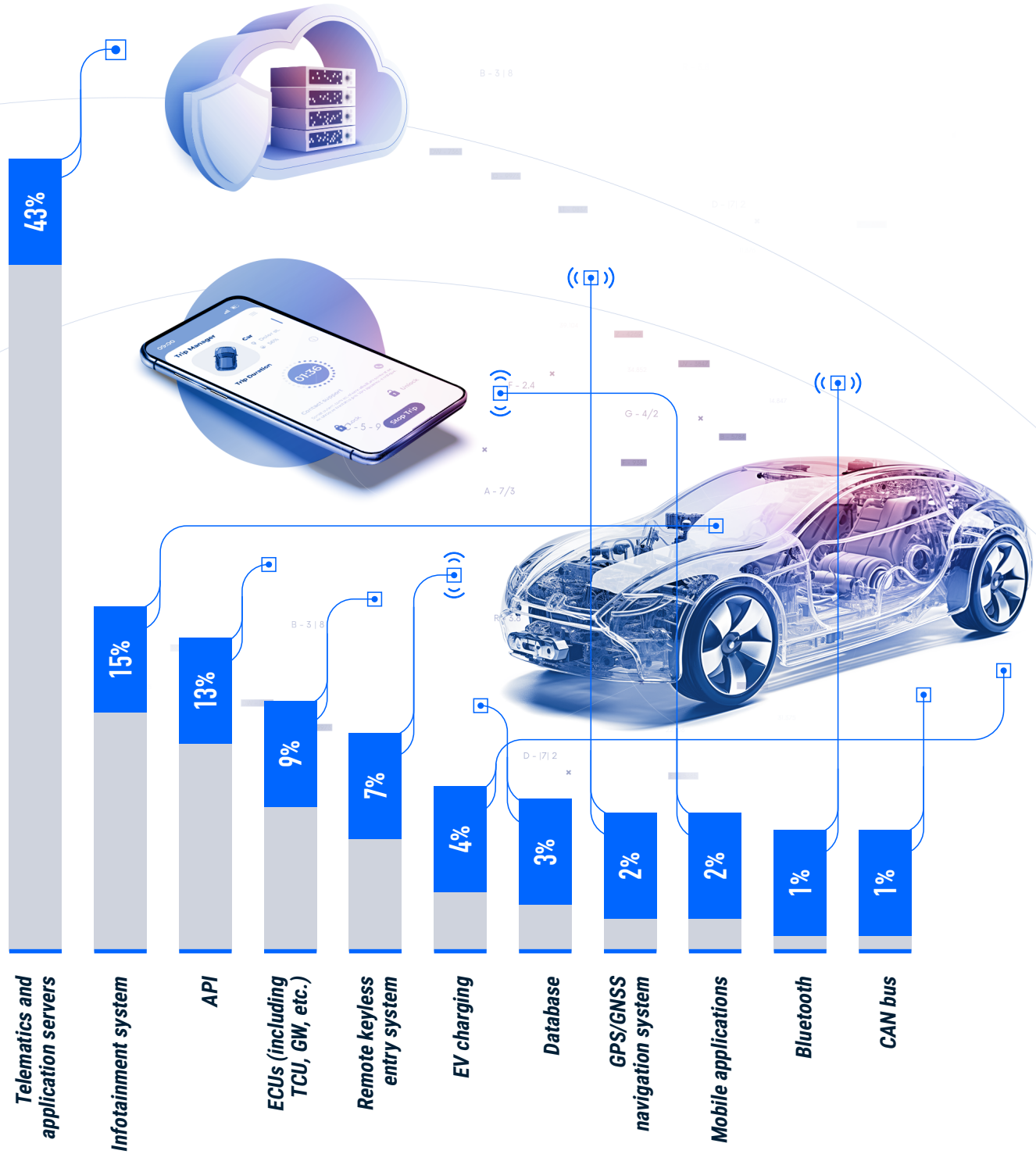
The attack landscape has driven the continued proliferation of the two new attack vectors that emerged back in 2022, which are the core of the smart mobility ecosystem: APIs for mobility applications and services, and EV charging infrastructure, which is expected to replace ICE fueling infrastructure in the next decade.

As a reminder, API-based attacks showed a dramatic increase in 2022, accounting for 12% of total incidents and demonstrating a staggering 380% growth. Moving forward we expect API-based attacks to gradually expand as various threat actors will leverage API vulnerabilities for large-scale attacks. Indeed, in 2023 APIs accounted for 13% of total incidents.

In 2023, the Automotive and Smart Mobility ecosystem experienced a sharp increase in incidents targeting backend servers (telematics, applications, etc.) as well as infotainment systems. Server-related incidents grew from 35% in 2022 to 43% in 2023; infotainment-related incidents nearly doubled, increasing from 8% in 2022 to 15% in 2023.

This trend is directly related to the growing awareness and visibility into connected components (servers, infotainment systems). It is also a result of the established maturity of the automotive cybersecurity landscape and the attempt of threat actors to gain access to sensitive data and potentially vehicle control across a large scale of mobility assets.

Incidents by attack vector



Source: Upstream Security

TELEMATICS AND APPLICATION SERVERS

Throughout a vehicle's life, connected vehicles collect, transmit, and receive information from OEM backend servers and vehicle owners. This is accomplished by using two types of servers: telematics servers, which communicate with the vehicle, and application servers, which communicate with the vehicle's companion applications.

Additionally, some vehicles have backend servers that communicate with third parties, such as insurance companies, fleets, car rental and leasing companies, EV charging networks, and more.

By exploiting vulnerabilities in backend servers, a black hat actor could attack vehicles while they are on the road.

- In June 2023, a security researcher from the Automotive Security Research Group (ASRG) discovered multiple vulnerabilities in MQTT, a widely adopted network messaging protocol used in connected vehicles, that allows an attacker to access and even manipulate the telemetry data of the entire fleet of vehicles using a popular telematics unit.[102]

A series of vulnerabilities, collectively known as CVE-2023-3028,[103] were identified:

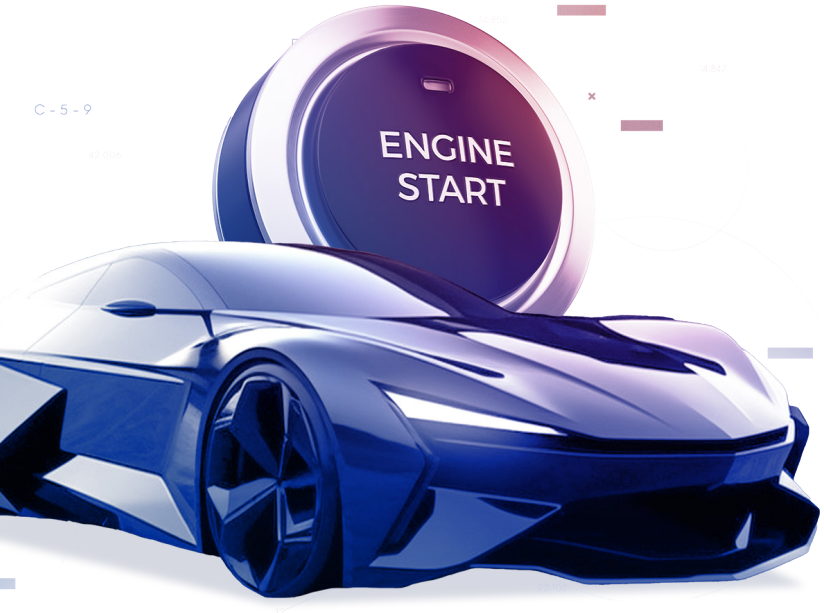
- MQTT backend does not require authentication, allowing unauthorized connections from an attacker.
- Vehicles publish their telemetry data (e.g., GPS location, speed, odometer, fuel, etc.) as messages in public topics. The backend also sends commands to the vehicles as MQTT posts in public topics. As a result, an attacker can access the confidential data of the entire fleet.
- MQTT messages sent by the vehicles or the backend are not encrypted or authenticated. An attacker can create and post messages to impersonate a vehicle or the backend. The attacker could then, for example, send incorrect information to the backend about the vehicle's location.
- Backend servers can inject data into a vehicle's CAN bus by sending a specific MQTT message on a public topic. Because these messages are not authenticated or encrypted, an attacker could impersonate the backend, create a fake message, and inject CAN data into any vehicle managed by the backend.

REMOTE KEYLESS ENTRY SYSTEMS

Modern vehicles are protected against theft by using remote keyless entry systems that include smart key fobs with very strong cryptography and immobilizers. But remote keyless entry systems may accomplish the opposite, as vehicle theft and vehicle break-ins continue to increase.

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

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



The communication between the key fob mechanism and the vehicle can be attacked in a few different ways:

Relay attacks using a “live” signal

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

Replay attacks using a stored signal

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

Reprogramming key fobs

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

Jamming communication between a key fob and a vehicle

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

Impersonating the wireless key fob ECU with CAN injection

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

- In January 2023, a security researcher discovered a vulnerability, described in CVE-2022-38766, that impacts the remote keyless system on a French OEM vehicle model. This vulnerability is based on the Rolling Code sets, a series of changing codes that is supposed to prevent replay attacks. In this case the researcher discovered that instead of generating new Rolling Code sets, the system was using the same Rolling Code sets for each door-open request. This vulnerability allows an attacker to intercept and replay the signals, using a specialized device, and manipulate the keyless system.[104]

- In February 2023, police in Glasgow, Scotland, issued a warning after 28 vehicles were stolen in the city during January 2023, citing an increase in keyless vehicle thefts.[105] On the same day, police in Suffolk, UK, warned citizens that keyless car theft has spiked after five luxury SUVs from a UK OEM were stolen in one month.[106] Between March-May 2023, similar announcements were made by the Waterloo Regional Police in Belgium,[107] the Worcestershire Police in the UK,[108] and the Franconia Police in Germany.[109] In August 2023, the UK government announced plans to ban keyless vehicle hacking devices in an attempt to combat rising vehicle thefts, which have soared by 25% year-on-year.[110]

- In April 2023, a cybersecurity researcher disclosed a new attack method, called CAN injection, which bypasses the entire smart key system by using a CAN injector device.[111] The device can be connected to the control CAN bus from the headlight connector, the taillight connector, or even by punching a hole in a panel where the twisted pair of CAN wires go right past—to impersonate the smart key ECU. The researcher discovered the method after conducting a lengthy digital forensic investigation into the July 2022 theft of his Japanese OEM vehicle, following two previous failed attempts.[112]

ECUs

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

- In February 2023, the National Highway Traffic Safety Administration (NHTSA) ordered a recall of nearly 17,000 Japanese OEM SUVs built between November 2019 and June 2021. Software in the Hybrid Vehicle Control ECU, which is used to calculate the hybrid battery output, may not limit battery output as required, causing the hybrid system to shut down completely in certain conditions[113]. It's unclear what is the reason for the issue, but it could certainly evolve into a significant cyber risk.

- In November 2023, a hacker used a device with a microcontroller to read the CAN bus of a Japanese OEM vehicle, allowing him to keep the vehicle's ACC (accessory) relay energized when the engine is turned off, maintaining power to the stereo and infotainment system.[114] This type of attack can lead to privacy violations, as well as potential exploitation of other vehicle systems.

APIs

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

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

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

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

- In January 2023, a group of security researchers published a lengthy writeup of their months-long work exploring the security of telematic systems, automotive APIs, and the infrastructure that supports them. They discovered multiple vulnerabilities across 19 major global OEMs and suppliers that allowed them to remotely control vehicles and access sensitive OEM and consumer data.[115]

- In March 2023, a security researcher disclosed that he gained access to a Japanese OEM's CRM database by modifying the dev app to use the production API—which was unintentionally exposed through the loading spinner settings. A misconfigured API and a lack of proper authentication and verification resulted in the researcher being able to access names, addresses, phone numbers, email addresses, tax IDs, and vehicle / service / ownership history of the OEM's customers.[116]

- In July 2023, security researchers reported three critical vulnerabilities found in the API interfaces of a Charging Station Management System (CSMS) platform from a Switzerland-based provider, allowing attackers to access files uploaded by other users, bypass the required provisioning PIN code (authentication), and hijack a charger's OCPP connection.[117]

- In November 2023, security researchers from ASRG disclosed a vulnerability, described in CVE-2023-6073,[118] which allows attackers to crash a specific ECU installed in German OEM vehicles and irreversibly change the volume to maximum levels via REST API calls.[119]

- The same month, a Tier-2 supplier of a popular automotive platform chip disclosed a multi-mode call processor memory corruption vulnerability, described in CVE-2023-22388,[120] that occurs while processing the bit mask API, causing unexpected behavior and crashing the system.[121]

MOBILE APPLICATIONS

Increasingly connected and software-defined vehicles allow OEMs to provide remote services via vehicle companion apps and third-party apps, allowing owners to conveniently control critical functions using their smartphones and devices. Using mobile applications, users can track the location of vehicles, open their doors, start their engines, turn on auxiliary devices, and more.

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

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

- In May 2023, security researchers reported a vulnerability, known as CVE-2023-29857,[122] in a popular third-party application used by owners of US EV OEM. The vulnerability allows attackers to obtain sensitive information by directly accessing the application link.[123]

- In June 2023, a popular ride-hailing service in Pakistan with over 10 million users was hacked, resulting in consumers receiving abusive messages and notifications. A third-party communication API had been compromised, according to the company.[124]

INFOTAINMENT SYSTEMS

The in-vehicle infotainment system (IVI) is one of the most common attack vectors. It connects to the internet, and is exposed to installed applications and short-range communications with mobile phones and bluetooth devices. As a result, it has access to PII.

Additionally, IVI systems often connect to a vehicle's internal networks, posing a serious risk to the vehicle. IVI systems can be the path of least resistance for malicious software to penetrate internal systems.

- In May 2023, a hacker and advocate for open-source implementation in the Automotive industry, successfully hacked a Japanese OEM's infotainment system using a tool sold online and posted evidence of the exploit on GitHub. The hacker managed to install multiple applications via a USB drive, including a file manager and a third-party app over the Transmission Control Protocol.[125]

- In August 2023, researchers from Germany successfully executed a jailbreak of a US EV OEM's IVI system using a voltage fault injection attack on the chip-maker's processor that gave them nearly irrevocable root access. The attack allowed the researchers to run arbitrary software on the infotainment system and unlock paid features such as faster acceleration and heated seats. Additionally, the exploit facilitated the extraction of a vehicle-unique key (cryptosystem public key) used for authentication and authorization on the OEM's internal service network. With the root permissions gained through the exploit, a malicious actor could access private user data, decrypt encrypted NVMe (Non-Volatile Memory Express) storage, and manipulate the car's identity.[126]

EV CHARGING INFRASTRUCTURE

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

- In January 2023, a hacker exploited a popular screen sharing program to gain access to the underlying Operating System (OS) of a new 350-kW charger from a US EV charging company. The hacker could access the OS menu, open the web browser, and navigate to a competitor's website while the charger app remained running in the background.[127] An earlier incident occurred in which another hacker gained access to the charger's critical settings and could view things such as overheat protection.[128] In both cases, the incidents aimed to raise awareness for electric vehicle charging security concerns.

- In June 2023, security researchers discovered an internal database—hosted on one of the most popular public cloud platforms, with no password, that contained millions of logs—nearly a terabyte of logging data belonging to a global EV charging service provider with a worldwide network of hundreds of thousands of EV charging stations. The database contained sensitive information about customers who used the EV charging network, including customer names, email addresses, phone numbers of fleet customers, names of fleet operators with vehicles that recharge the network, and vehicle identification numbers (VINs), and locations of EV public and residential charging points.[129]

BLUETOOTH

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

In March 2023, a team of French security researchers participating in a hacking contest demonstrated breaking into a US EV OEM IVI using an exploit. The exploit involved a heap overflow vulnerability and an out-of-bounds write error in a Bluetooth chipset, giving the researchers root access to other subsystems.[130] The exploit won the long-running contest's first-ever Tier-2 award reserved for exceptionally impactful vulnerabilities and exploits, along with a $250,000 prize.[131]

OTA UPDATES

Over-the-Air (OTA) programming is a method for remotely managing software that allows for wireless distribution of new software, firmware, or configuration settings from a central location to all devices through the network. With the expansion of software-defined architectures, OTA updates enable OEMs and their Tier-1 and Tier-2 suppliers to continuously update the SBOM to improve vehicle quality, safety, functionality and introduce new features.

Remote updates, however, are riskier than physical ones because wireless communications opens the door to numerous cyber attacks that can affect multiple vehicles—and even entire fleets, at once.

Additionally, updates could be crucial to the vehicle's functionality. The failure of an OTA update could cause a severe vehicle malfunction, as it did in November 2023 for a US-based EV OEM. The OEM released and then abruptly canceled an OTA update that offered bug fixes and improvements to a specific feature. As a result of the failed update, the infotainment systems, which are used to operate critical vehicle functions, of two vehicle models were bricked. The OEM stated that the issue was caused by a human error—the wrong build was sent out with the wrong security certificate—and that an OTA update would be made available to fix the issue and restore full functionality.[132]

As OTAs are used more frequently and leveraged by an increasing number of OEMs, Upstream's AutoThreat® researchers continuously monitor OTA-related activities in the deep and dark web. Our researchers have identified a growing interest by adversaries in exploiting OTA updates to execute cyber attacks.

V2X ATTACKS ARE AT THEIR INFANCY, BUT ARE EXPECTED TO BECOME MUCH MORE FREQUENT IN THE COMING YEARS

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

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

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

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

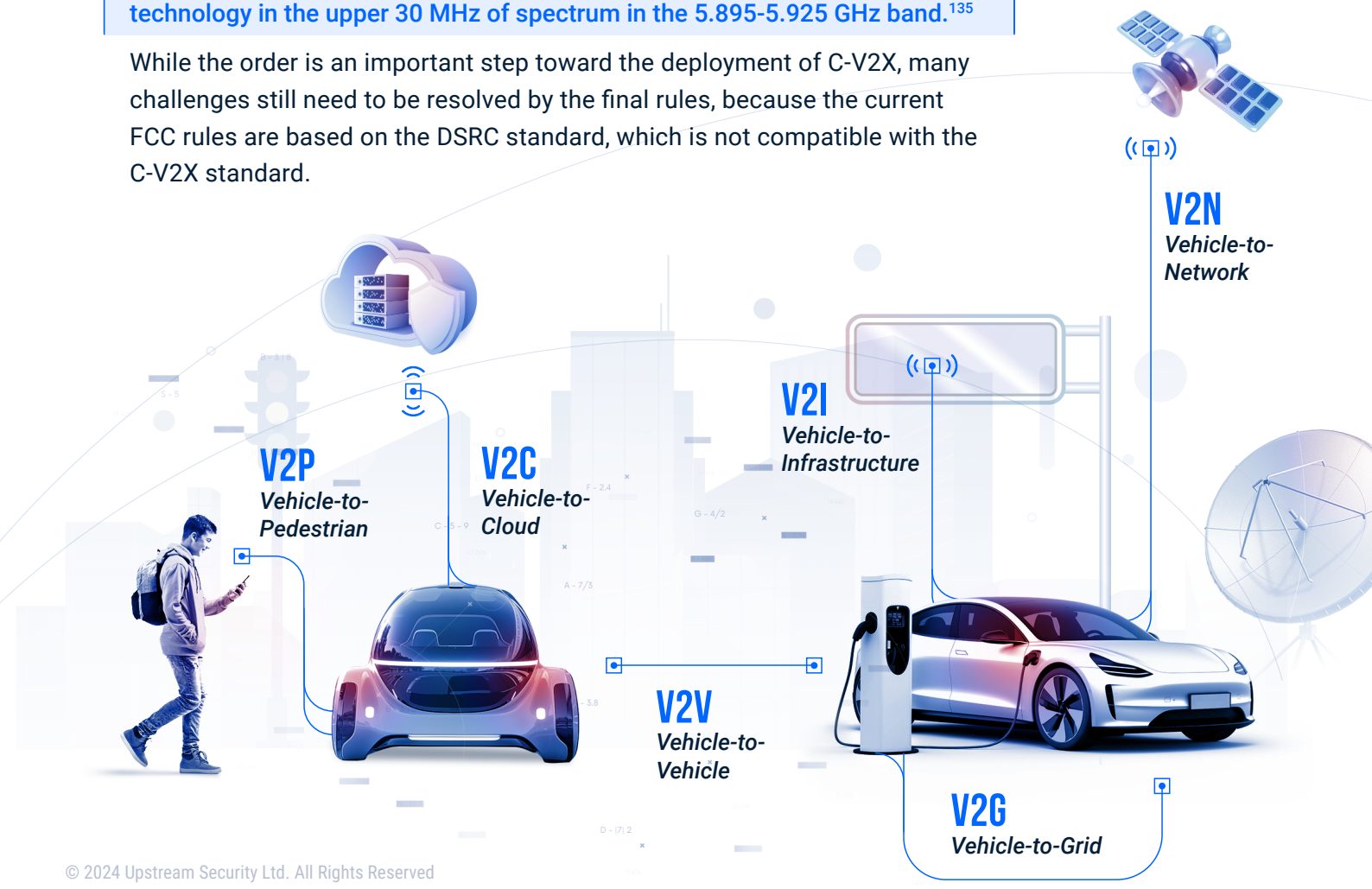
The most profound addition will be the capability of a vehicle to communicate with other vehicles or devices on the road, and receive data from external sources such as EV chargers or road infrastructure.

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

The future of V2X will rely on new wireless communication technologies, such as DSRC and Cellular V2X (C-V2X), which have been in testing for the past few years. C-V2X uses 3GPP standardized 4G LTE or 5G mobile cellular connectivity to exchange messages between vehicles, pedestrians, and wayside traffic control devices such as traffic signals.[133] Though both DSRC and C-V2X enable the future of V2X, C-V2X's use of Long-Term Evolution (LTE) is considered a potential game-changer for the connected vehicles ecosystem. The ability to use existing cellular infrastructure will reduce the efforts required to accelerate adoption, while guaranteeing high-speed communication in high-density locations.[134]

In April 2023, the FCC approved the C-V2X technology for connected vehicles ahead of the final national framework for intelligent transportation systems (ITS) rules. The FCC's Public Safety and Homeland Security Bureau, the Engineering and Technology Bureau, and the Wireless Telecommunications Bureau granted a joint request submitted by automotive manufacturers, equipment manufacturers, and state departments of transportation seeking a nationwide waiver of several FCC rules to permit deployment of C-V2X technology in the upper 30 MHz of spectrum in the 5.895-5.925 GHz band.[135]

While the order is an important step toward the deployment of C-V2X, many challenges still need to be resolved by the final rules, because the current FCC rules are based on the DSRC standard, which is not compatible with the C-V2X standard.



04

THE REGULATORY REALITY

Preparing for regulatory expansion and adopting new standards to keep connected mobility assets secure

GENERATIVE AI IS RESHAPING THE AUTOMOTIVE AND SMART MOBILITY 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. The global market for GenAI in the automotive industry was valued at $312 million in 2022, with projections reaching as high as $1.7 billion by 2030.[136]

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.[137]

The landscape of GenAI regulations and guidelines is evolving across many industries, with the financial industry charging ahead. In November 2023, Singapore's Monetary Authority (MAS) launched a GenAI risk management framework and guidelines for financial institutions. These guidelines were developed in collaboration with several banks, as well as large technology vendors.[138] In December 2023, the European Parliament also announced reaching a provisional agreement on the Artificial Intelligence Act.[139] 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.

THE GLOBAL MARKET FOR GENAI IN THE AUTOMOTIVE INDUSTRY WAS VALUED AT

$312

MILLION IN 2022, WITH PROJECTIONS REACHING AS HIGH AS

$1.7

BILLION BY 2030.

CYBERSECURITY REGULATIONS MAKE HEADWAY WORLDWIDE

Evolving regulations worldwide reflect a concerted effort by governments and regulators to adapt to technological advancements, promote safety, and address environmental concerns—showcasing a global commitment to shaping the future of the Automotive industry.

China

China has recently initiated various regulations and guidelines, demonstrating a wide effort to establish risk management frameworks related to the Automotive and Smart Mobility ecosystem.

In December 2023, China's Ministry of Transport released trial guidelines for autonomous vehicle (AV) services, including robotaxis, self-driving trucks, and robo-busses.

The nationwide guidelines, developed after a 16-month period of public opinion seeking, standardizes rules and establishes comprehensive surveillance measures to ensure the safety of self-driving vehicles. For example, AVs, regardless of their automation level, can only operate in specified areas:

- Autonomous buses are restricted to "enclosed or roads with relatively simple conditions"
- Robotaxis are allowed in "controlled and safe traffic conditions"
- Robo trucks face explicit restrictions, limited to "point-to-point highways or good traffic conditions"

Operators must obtain permits and relevant licenses for public transportation services, and AVs should be clearly labeled for road awareness. Additionally, the guidelines make a singular reference to software, emphasizing that over-the-air upgrades must adhere to safety regulations from the Ministry of Industry and Information.[140]

The Chinese Ministry of Industry and Information Technology has issued a call for public opinions on four mandatory national standards, including Technical Requirements for Automobile Information Security, and Information Security Technical Requirements for Complete Vehicles. These standards were open for feedback until July 5, 2023.

> ***While largely consistent with UNECE WP.29 R155, differences exist in areas such as the entity responsible for standard development, formulation, and effective time, vehicle security requirements, testing methods, and modification of vehicle types.***

The Chinese government aims to finalize the first version for review, with a process expected to lead to the standard's release in mid-2024. Implementation is anticipated 12 months after release, in mid-2025.[141]

In June 2023, the Chinese State Council issued a regulatory framework notice, emphasizing the necessity of advancing a high-quality charging infrastructure system in China. **The framework is a strategic response to address the challenges faced by China's rapidly growing charging infrastructure such as lack of standardization, poor construction, and unbalanced design.** The framework also addresses the broader strategic objectives set for 2030, which include building a high-quality charging infrastructure system with extensive coverage, moderate scale, a reasonable structure, and complete functions.[142]

Japan & EU

In Japan and the EU, UN regulations (UN-R157-01 series) allow for approval of Level 3 autonomous driving devices with a speed limit of 130 km/h on highways and the ability to change lanes as of January 2023. Future regulations will focus on unmanned (driverless) vehicles at Levels 4 and 5.[143]

India

In April 2023, India implemented Real Driving Emissions (RDE) regulations for passenger cars, mandating compliance with emissions limits during on-road driving. This regulation addresses the gap between testing conditions and real-world driving emissions. RDE, inspired by tighter regulations in Europe, covers diverse driving conditions, reducing reliance on conformity factors that adjust emission standards for real-world conditions. The suggestion is for Indian policymakers to set a timeline to phase out conformity factors. Notably, Europe is proposing that by 2025, all on-road emissions from light-duty vehicles measured during RDE testing should not exceed laboratory test limits under the boundary conditions of the RDE standards.[144]

Implementing RDE requires collecting and analyzing real-time data from vehicles on the road. This data may include information related to emissions, engine performance, and driving patterns. Cybersecurity measures are necessary to protect this sensitive data from unauthorized access and potential misuse of the data.

In November 2023, following global standards, India proposed a mandatory security framework for vehicle manufacturers called “CyberShield”. The plan, backed by the Minister of Road Transport, aims to fortify vehicle systems against cyber vulnerabilities, extending protection to electric vehicle charging stations. **The initiative recognizes the importance of preemptive cybersecurity measures in an increasingly interconnected automotive landscape, covering both passenger and commercial vehicles. The draft is set for expert scrutiny before parliamentary approval.**[145]

United States

In August 2023, the California Privacy Protection Agency (CPPA) launched an enforcement initiative to examine the extensive data collected by connected vehicles—through built-in apps, sensors, and cameras. The move reflects a growing focus on privacy within the Automotive industry. The CPPA aims to ensure OEM transparency and compliance with consumer data rights, such as knowing what data is collected, preventing its dissemination, and requiring its deletion. **The initiative highlights concerns about data management and may also impact industries beyond automotive, such as supply chain, logistics, and construction.**[146]

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,[147] and WP.29 R156 for Software Update Management System (SUMS).[148] **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.[149]

Together with ISO/SAE 21434,[150] 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),[151] the European Union Agency for Cybersecurity (ENISA),[152] and member trade association Auto-ISAC.[153]

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.

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*
L6	Vehicle with four wheels weighing under 350kg (~770lb.) whose engine does not exceed 50 cubic cm. and whose maximum speed is designed for 45 km/h (~28mph)	R155 if equipped with level-3 functionalities and above
L7	Vehicle with four wheels weighing under 400kg (~880lb.) and whose continuous rated power does not exceed 15kW	R155 if equipped with level-3 functionalities and above
M	A vehicle with at least four wheels and meant to carry passengers	R155 & R156
N	An automobile with at least four wheels meant to carry goods	R155 & R156
O	Trailers that have at least one ECU	R155 & R156
R	Agricultural Trailer	R156
S	Interchangeable towed agricultural or forestry equipment	R156
T	Any motorized, wheeled, or tacked agricultural equipment that has two axles and is meant to travel at speeds greater than 6km/h (~3.5mph)	R156

Source: UNECE

Vehicles are regulated under R155[154], R156[155], or both, depending on category classification.

REGULATORY IMPACT ON THE AUTOMOTIVE INDUSTRY

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

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

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

With R155, OEMs and suppliers are better able to identify and respond to security risks associated with new and emerging vehicle architectures, mobility services, and the connected vehicle ecosystem. These include threats to:

- Backend servers related to vehicles in production
- Vehicles regarding their communication channels
- Vehicles regarding their update procedures
- Vehicles regarding unintended human actions facilitating a cyber attack
- Vehicles regarding their external connectivity
- Vehicle data/code

The R155 regulation is unique both in its practical approach to automotive cybersecurity, with concrete examples of threats and specified mitigations. But it is also based on a holistic approach, covering process and governance, as well as IT, product, OT, and IoT perspectives.

In the regulation, the term 'processes' is emphasized clearly in an intent to provide guidance on cybersecurity structures without mandating low-level technical specifications. Today's automotive cyber environment is diverse and dynamic, making rigid technical measures counterproductive. The regulation was intentionally drafted in a technology-neutral way, giving some flexibility to OEMs to decide how to ensure the cybersecurity of their vehicles.

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

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

To boost collaboration among OEMs and suppliers, the European Automobile Manufacturers' Association (ACEA) and the European Association of Automotive Suppliers (CLEPA) joined forces with Auto-ISAC in October 2022, to create a central European hub for information sharing on motor vehicle cybersecurity.[156]

ESTABLISHING LONG-TERM TRUST WITH ISO/SAE 21434

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

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

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

> ***With 378 new CVEs discovered in 2023 as well as the sharp rise in deep and dark web activities, it is imperative that stakeholders continuously review and implement mitigation techniques to protect their products against both existing and future vulnerabilities and undiscovered vulnerabilities that may arise in the future.***

ISO/SAE 21434 and WP.29 work together to protect vehicles on a global scale

ISO/SAE 21434
Security by design

Engineering requirements for each step of product development

R155
Cybersecurity Management System

Cybersecurity monitoring throughout vehicle lifecycle

R155
Threat Analysis & Risk Assessment

Risk assessment and risk score for vulnerabilities

R155
Monitoring

Early detection based on vehicle logs, and rapid response to incidents

R156
Software Update Management System

Continuous safe updates throughout the vehicle lifecycle

DOES R155 ALIGN WITH IN-FIELD THREATS?

Upstream's research team analyzed publicly reported automotive cyber incidents that occurred in 2023, and correlated them to the seven threat categories presented in Annex 5 of R155.

2023 cyber incidents categorized by R155 threats & vulnerabilities

Source: Upstream Security

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.[157] 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.[158] 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).[159] 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.[160]

The CRA is expected to enter into force in May 2024, with manufacturers obligated to comply within 36 months.[161]

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.[163] **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"[164] 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).[165] 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:[166]

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.).

The SEC echoes the increasing focus on cybersecurity incidents

In July 2023, the US Securities and Exchange Commission (SEC) adopted final rules on cybersecurity disclosure for publicly listed companies.[167]

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.[168]

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—as well as 180-day extensions for Smaller Reporting Companies.[169]

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.[170] 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.

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

NHTSA updates cybersecurity best practices

In 2023, NHTSA released updated cybersecurity best practices for new vehicles.[171] 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[172] 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
- Rapid recovery when attacks do occur
- Methods for accelerating the adoption of lessons learned across the industry, including effective information sharing

> ***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.***

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

NHTSA guidelines 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. Upstream is a proponent of this; as collaborative community members, we maintain the Upstream AutoThreat® Intelligence Cyber Incident Repository[173] and share insights in our annual report. Upstream is also a proud partner and sponsor of Auto-ISAC[174] and ASRG,[175] where industry knowledge sharing occurs and cybersecurity best practices take shape.

Updated approach to ADS and ADAS

Automation is constantly evolving, and NHTSA is developing regulations for Automated Driving Systems (ADS) and Advanced Driver Assistance Systems (ADAS). In April 2023, NHTSA issued the Second Amended SGO 2021-01 – Incident Reporting for Automated Driving Systems and Level 2 Advanced Driver Assistance Systems.[176]

The updated SGO went into effect May 15, 2023 for 3 years, and includes updates to reporting requirements established in the original SGO, which was issued in 2021. **It enables NHTSA to receive standardized, timely, and transparent data of actual accidents involving ADS and Level 2 ADAS vehicles—which is essential to identifying potential safety concerns with automated technologies that are rapidly evolving and being tested on public roads.**

In July 2023, NHTSA also created the Office of Automation Safety, and the Automation Exemptions Division under NHTSA's existing Office of Rulemaking to focus internal resources on this sector.[177]

NHTSA favors safety and cybersecurity over the Right to Repair

The Right to Repair refers to the ability of vehicle owners and independent repair shops to access the information, tools, and software necessary to diagnose, service, and repair vehicles. In the context of modern vehicles, which are equipped with advanced technologies and complex systems, the Right to Repair has become a significant issue—making big headlines in 2023.

> ***In June 2023, in a dramatic move, NHTSA sent a letter to dozens of OEMs stating safety concerns related to the Massachusetts Right to Repair Act,[178] warning them to ignore the law amid cybersecurity concerns.***

NHTSA further clarified that it expects vehicle manufacturers to fully comply with federal safety obligations.

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.[179]

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.[180]

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.

EV CHARGING INFRASTRUCTURE CYBERSECURITY REGULATIONS CONTINUE TO EXPAND

EVs currently make up approximately 15% of global new car sales[181], with an expectation to reach the majority market share of new car sales by 2040.[182]

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

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

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

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

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

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

Regulations protecting EVCS can be divided into two major categories:

01

Operational standards

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

02

Regional regulations theoretical frameworks

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

Regulators worldwide have been focused on promoting different types of regulations, focused on securing EVCS against cyber risks.

Sample of recent EVCS cybersecurity regulations

Region / Country	Regulation	Focus	Implementation date	Enforcement status
US	NIST IR 8473	EVCS		Voluntary
	National Electric Vehicle Infrastructure Standards and Requirements	EVCS	April 2023	Mandatory
EU	ETSI EN 303 645	IoT	August 2025	
	NIS2 Directive	Critical infrastructure	October 2024	Mandatory
	EU Cyber Resilience Act	IoT	Expected in the beginning of 2024	Mandatory, with a 3-year transition period
UK	British Standards Institution (BSI) standards for energy smart appliances (ESAs)	Smart appliances	December 2021	Voluntary
	Complying with the Electric Vehicles (Smart Charge Points) Regulations 2021	EVCS	December 2022	Mandatory
Japan	MIC IoT 5G Comprehensive Security Measures	IoT	June 2019	Mandatory
	METI IoT Security and Safety Framework	IoT	November 2020	Mandatory

United States

In March 2023, the National Electric Vehicle Infrastructure Standards and Requirements by the US Federal Highway Administration (FHWA) came into effect.[183] This new rule establishes the requirements and minimum standards related to projects funded under the National Electric Vehicle Infrastructure (NEVI) Formula Program and projects for the construction of publicly accessible EV chargers under certain statutory authorities, including any EV charging infrastructure project funded with Federal funds that is treated as a project on a Federal-aid highway.

Essentially, FHWA adopted the principles of ISO 15118 and requires charging station conformance to ISO 15118 and Plug and Charge capability by one year after the date of publication of the Final Rule in the Federal Register. This legislation highlights the value in adopting a national standard for compliance, even though many chargers on the market are not currently using ISO 15118.[184]

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

In October 2023, the US Department of Commerce's National Institute of Standards and Technology (NIST) finalized its guidance for managing cybersecurity risks for EV extreme fast charging infrastructure with NIST IR 8473 – Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure.[185] EV charging stations and charging infrastructure are vulnerable to a wide range of cybersecurity threats since they rely on complex infrastructure, interconnectivity, and multiple data networks. **NIST IR 8473 offers a holistic framework, covering the entire EV charging landscape.** The guidelines include:

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

Furthermore, NIST IR 8473 has a well-established section for data protection, based on the ISO 21434 standard.[186]

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

EU

ETSI EN 303 645 regulation for IoT devices was issued by the European Telecommunications Standards Institute. ETSI EN 303 645 was specifically designed to ensure data protection and integrity in smart connected devices. The regulation is currently being reviewed with proposed final requirements to be presented on August 1, 2025.[187]

NIS2 Directive focuses on establishing cybersecurity standards and resilience for the critical infrastructure and energy sectors, thus including EVCS under the regulatory coverage. NIS2 Directive also covers the EU Cyber Solidarity Act which refers to cybersecurity protection for IoT devices.[188] The initiative aims at achieving detection, prevention and response to cyber risks and vulnerabilities. This includes forming SOC (security operation center) infrastructure within member countries to ensure coordinated handling of cyber threats.[189] The framework will become mandatory on October 17, 2024.

The EU Cyber Resilience Act covers digitally connected devices including IoT devices. The Act is expected to be implemented by the beginning of 2024.[190]

Also, ISO 15118 is partially and voluntarily implemented in Europe under the project name "Plug & Charge Europe". Although accepted by notable OEMs and EVCS operators throughout the region, there is no planned timeline for a full-scale implementation of the standard in the EU.[191] [192] The relevant regulations are set to be implemented during 2024-2025, and the region has already started voluntarily accepting ISO 15118.

UK

In December 2021, a proposition was made to include EVCS under the British Standard Institutes' (BSI) regulation for smart appliances (ESA) with smart energy.[193]

The UK is at the forefront of EVCS regulations, introducing the Electric Vehicles (Smart Charge Points) Regulations 2021, which came into force in June 2022 and applies to private charge points (domestic or workplace).[194]

The UK regulation specifies that chargers must meet the following requirements: smart functionality such as demand-side response services; electric supplier interoperability; enabled charging even with loss of communications network access; enhanced safety features; measuring system for increased transparency on charging statistics; default off-peak charging schedule; randomized delay to protect from surges in demand; statement of compliance for compliance assurance; and register of sales for ten years. New cybersecurity requirements are also outlined in Schedule 1 of the regulation, which came into effect in December 2022.[195] Chargers will come preconfigured with these settings, but owners can adjust them to suit their preferences.

A guidance letter for EVCS sellers and operators, published in February 2022 and most recently updated in June 2023, suggests matching EVCS cybersecurity requirements to the European ETSI EN 303 645 standard. ETSI EN 303 645 was chosen based on its suggested benchmark and measurable objectives.[196]

Japan

Cybersecurity protection of EVCS in Japan can be derived from regulations covering IoT devices such as METI (Ministry of Economy, Trade and Industry) IoT Security and Safety Framework from November 2020[197] and MIC (Ministry of Internal Affairs and Communications) IoT 5G Comprehensive Security Measures from June 2019.[198]

OPERATIONAL EV CHARGING STANDARDS WORLDWIDE

ISO 15118

ISO 15518 is the leading global cybersecurity standard to ensure encrypted, secure communication between the EVs and charging stations (EVSE/ EVCS) while charging,[199] and is considered as the high-level communication protocol, functioning as the security standard for the Combined Charging System (CCS).[200]

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

01

Confidentiality
messages are encrypted using TLS protocol.

02

Data integrity
messages are kept intact and untampered using a pair of private and public keys.

03

Authenticity
sender and received messages are ensured using Elliptic Curve Digital Signature Algorithm (ECDSA).[201]

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

- EVs
- CPOs
- Cloud operators in charge of data processing and storage
- Power grids (also referred to as Utility / Building Management Systems)

Combined Charging System (CCS)

One of the most prominent charging protocols, supported by multiple OEMs worldwide. CCS cybersecurity measures are covered under ISO 15118.[202]

DIN SPEC 70121

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

CHAdeMO

A Japanese standard (stands for "Charge de Move") that was created by OEMs including Nissan, Mitsubishi, and Toyota. CHAdeMO was first introduced in 2009 and aims to provide an alternative to the ISO 15118 standard.[203] Similar to ISO 15118, CHAdeMO covers V2G security aspects. The charging process is enabled by matching the user's VIN (Vehicle Identification Number) along with IPv6 security measures and contract key encryption.

In September 2023, CHAdeMO released the Design Guideline for External Charging ver.2.0.1, adding technical and operational requirements for safely integrating or retrofitting the Automated Connection Devices - Underbody (ACD-U) charging systems to CHAdeMO chargers/V2X equipment, EVs and plug-in hybrid EVs (PHEVs).[204]

OCPP 2.0.1

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

Notable improvements from version 1.6 to 2.0.1 include features for streamlined device management and improved transaction handling (for operators managing multi-vendor charging points), enhanced security with secure updates and authentication (using secure TLS encryption), and support for ISO 15118.[205]

While ISO 15118 secures the communication between the vehicle to the charging station, OCCP covers the security aspects between the charging stations themselves and the backend servers. This includes the CPO, telecommunications, and electricity management.[206]

VEHICLE DATA AND PRIVACY REGULATIONS ARE INEVITABLE

Connected vehicles raise unique data privacy and cybersecurity issues that must be addressed by OEMs and regulators. Much of the data generated by vehicles can be considered personal data, and most consumers feel they need legislation to protect their data.[207] Regulators around the world are taking notice and are developing consumer-centric vehicle data privacy and security standards.

In September 2023, the Mozilla Foundation assessed 25 leading OEMs on privacy and security and found poor results across the board:[208]

- Excessive collection of personal data
- Sharing or selling of personal data
- No consumer control over their personal data
- Willingness to share data with government and law enforcement agencies
- Poor cybersecurity track record

In the US, the Federal Trade Commission (FTC), the regulatory agency governing data privacy, and NHTSA currently advocate for industry self-regulation,[209] but individual states are adopting vastly different approaches, and many haven't started at all. So far, only a handful of states have enacted data privacy laws that specifically address connected vehicles, although several more are pending in legislatures across the US. Additionally, states can opt to cover connected vehicle data via comprehensive privacy bills. Proposition 24, the California Consumer Privacy Act (CPRA), is a prime example.[210] The CPRA prohibits automakers and insurance companies from using precise geolocation without the permission of the consumer.

In the EU, regulators are developing new regulatory frameworks for data and artificial intelligence, with major implications for the Automotive industry.[211]

The EU Data Act, agreed upon in June 2023, establishes principles for data access, user rights, fair contractual terms, public sector data access, and cloud service provider flexibility. These legislative developments aim to strike a balance between regulation and innovation in the evolving AI and data-driven Automotive industry.[212]

The Data Act will ensure fairness in the digital environment, stimulate a competitive data market, and open opportunities for data-driven innovation by allowing users of connected devices to access their data and share that data with third parties to provide aftermarket or other data-driven innovative services.[213]

In November 2023, the EU Council adopted the Data Act.[214] **Despite the broad scope of the legislation, sector-specific laws are being negotiated, including for the Automotive industry, where issues like vehicle data access and data modification pose challenges.**

> ***Using Artificial Intelligence (AI) in vehicles presents challenges for legislators, particularly concerning software updates and access to in-vehicle data.***

In December 2023, the European institutions—EU Commission, Council, and Parliament—reached a provisional political agreement on the world's first comprehensive law on AI—the new AI Act, intending to create a broad regulatory framework, indirectly impacting autonomous vehicles.

Work is ongoing to refine the drafting, and formal adoption by both Parliament and Council is anticipated in early 2024.[215] The UNECE also proposed guidelines for AI-related software updates, recommending approval authority engagement for impactful updates.

Autonomous and connected vehicle data and privacy laws are inevitable. In 2024-2025, we anticipate new regulations for the US and EU markets that require opt-in or minimally opt-out consent from consumers. As regulations continue to evolve, OEMs need to make strategic decisions about their own data privacy and security policies to maximize mutual trust, compliance and consumer protection.

05

THREATS FROM THE DEEP AND DARK WEB

Cyber threat intelligence offers automotive and smart mobility stakeholders actionable and proactive risk mitigation, amid the growing impact of cyber risk

WHAT IS THE DEEP AND DARK WEB?

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

The first layer of the internet is the clear/surface web—it is the smallest yet most familiar part of the internet, requiring only a web browser to access.[216] In this part of the web, information is indexed by popular search engines, making it highly accessible and relied on by people every day.

CLEAR WEB

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

The second layer of the internet is the deep web—which accounts for 96% of all web pages on the internet.[217] Data on this part of the web is not indexed by search engines, either because it is behind a sign-in (e.g., paywall), or its owners have blocked web crawlers from indexing. For the average person, the deep web includes paid content, subscription websites, private groups, and private business websites. For hackers, the deep web also includes imageboards, which host anonymous, provocative, borderline illegal content.

DEEP WEB

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

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

DARK WEB

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

Almost all dark web hackers use proxy servers along with a Tor browser to maintain their anonymity. A tool called proxychain is used to chain several (usually 3-5) proxy servers. In this case, packets from the attacker go through multiple proxy servers. Proxy servers are intentionally used in rival countries so that one country can't share security information (e.g., proxy logs) with another country—making it more difficult to identify hackers.

During 2023, Upstream's AutoThreat® researchers detected a 156% increase in deep and dark web findings compared to 2022, targeting OEMs, Tier-1 suppliers, Tier-2 suppliers for the automotive industry, mobility IoT devices, and platforms.

This data, together with the fact that in 2023—nearly 65% of deep and dark web cyber activities had the potential to impact thousands to millions of mobility assets[218] — show that **automotive and mobility stakeholders must have deep access and visibility into cyber threat intelligence to proactively protect themselves.**

DURING 2023, UPSTREAM'S AUTOTHREAT® RESEARCHERS DETECTED A

156%

INCREASE IN DEEP AND DARK WEB FINDINGS COMPARED TO 2022.

GRAY HATS BLURRING THE LINE BETWEEN BLACK HATS AND WHITE HATS

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

In October 2023, Upstream found that guidelines for jailbreaking the in-vehicle infotainment (IVI) system were published on deep web automotive forums. Using the hack, they were able to sideload unauthorized third-party applications, unlock hidden features, and remove system safety restrictions, such as watching videos while driving. Jailbreaking the IVI and installing unauthorized apps can expose consumers to cybersecurity vulnerabilities and void their warranties. Untrustworthy software may contain malware, spyware, and ransomware, as well as cause system stability issues resulting in crashes, failures, or incompatibilities.

WHAT OCCURS IN THE DEEP AND DARK WEB?

There are estimates that the deep and dark web accounts for 96% to 99% of the internet, which makes most of it private.[219] A wide range of automotive-related content can be found on deep and dark web forums, marketplaces, mobile messaging applications, and paste sites.

Often, consumers rely on web forums to find information that OEMs are reluctant to share with them—specifically information that can help them pirate-fix their vehicles or manipulate systems. 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 automotive technology.

These activities can have an impact on automotive stakeholders as well as insurance companies. Vehicles that have been tampered with may report false information that seems legitimate. In extreme cases, threat actors can gain access to OEM or insurance company servers by reverse engineering data that's already used to grant authorization to vehicles.

THREAT ACTORS MAY DISRUPT NEW AUTOMOTIVE AND MOBILITY IOT REVENUE STREAMS

Threat actors are increasingly exploiting opportunities for bypassing premium features by jailbreaking systems, posing considerable risks to both vehicle/device cybersecurity and data-driven commercialization.

Upstream has been tracking a popular middle-eastern threat actor, with over 38,000 followers on social media, who openly provides jailbreak services and custom software for IVI systems of various OEMs—including features such as Apple CarPlay, Android Auto, diagnostic services, and firmware upgrades. According to the threat actor, it offers unique features not available through conventional dealerships.

> ***This finding highlights the growing challenges associated with securing connected vehicles against unauthorized modifications, firmware updates, and diagnostics access. It also raises questions regarding the effectiveness of existing security measures.***

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

In September 2023, a high-profile Eastern European threat actor started selling unauthorized remote access to diagnostic software for various European OEMs on a deep web automotive forum. Providing unauthorized access to such software is in violation of the OEM's terms and conditions, and may result in limited OEM visibility of user access to premium features and loss of revenue.

In another example, in October 2023, Upstream identified a South European threat actor selling root access to IVI systems of various OEMs on a deep web forum, enabling the activation of hidden features. The threat actor indicated that the head unit could be jailbroken to accept unofficial files and modifications, enabling the user to browse folders, install apps, play videos while driving, and even tamper with the navigation system.

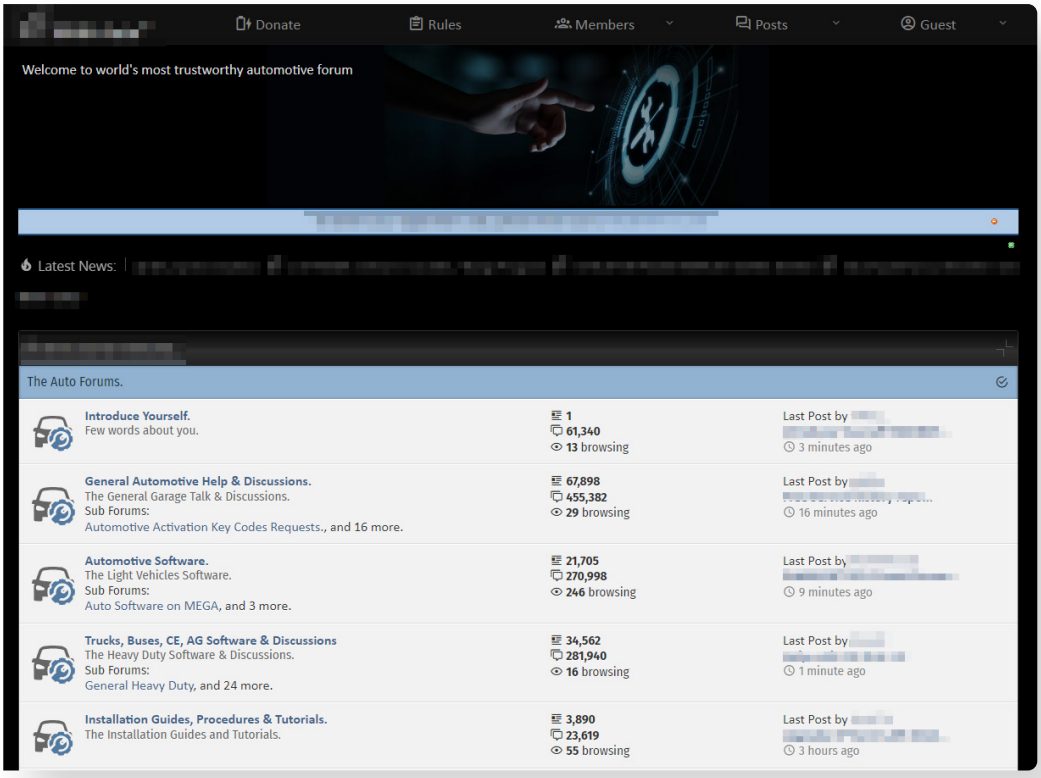
Forums

In the deep and dark web, there are automotive-related forums dealing with sharing or selling automotive software, chip and engine tuning, infotainment cracking, reverse engineering, key-fob modifications, immobilizer hacking, and automotive software—although general hacking forums also contain automotive-related hacks.

In these forums, information, insights, hacks, and software manipulations are constantly traded. Tuning ECUs is a common topic of discussion, along with jailbreaking infotainment systems, source codes, data breaches, and car hacking tools and tutorials.

It is not uncommon for people to ask about self-programming their vehicles for a variety of reasons, such as saving money or claiming the Right to Repair. Additionally, ECU remapping lessons, guides, software, and tuned file demos are readily available.

In September 2023, Upstream's AutoThreat® PRO team uncovered a threat actor operating in a popular deep web automotive forum selling remote jailbreak solutions for IVI systems of a European OEM. The jailbreak consists of a CAN patch that enables all features except subscription-based ones, including Android Auto, Android screen mirroring, Apple CarPlay, voice control, video while driving, and updates to firmware and maps.



Example of a deep web automotive forum

Marketplaces

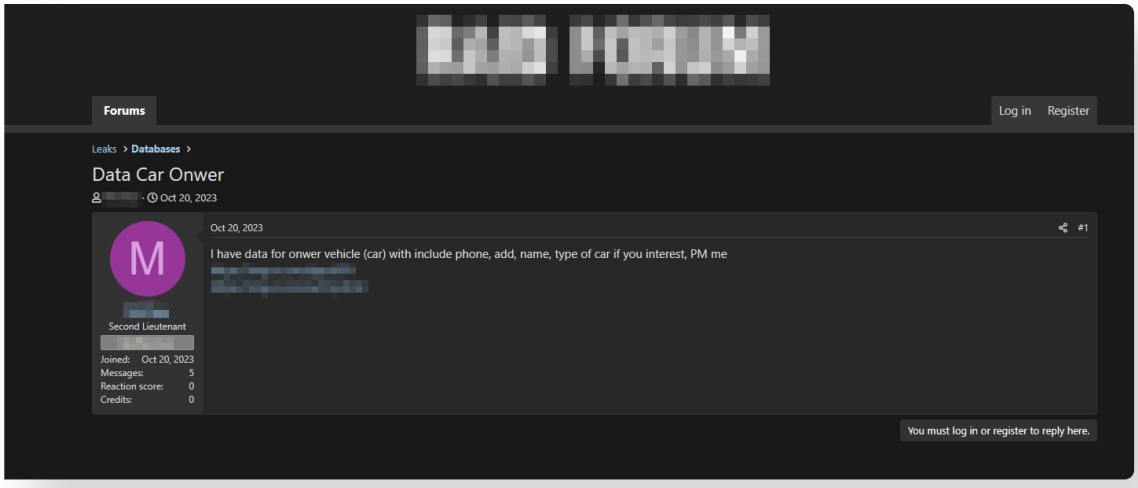
Dark web marketplaces are commercial websites that require specialized browsers, like Tor or I2P, and registration to access. They function primarily as black markets—brokering transactions involving drugs, weapons, cyber-arms, stolen data, forged documents, and other illicit goods.[220]

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 sale 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 October 2023, Upstream uncovered threat actors selling consumer databases of multiple OEMs on dark web marketplaces.



Example of a consumer database for sales on a dark web marketplace

In 2023, Upstream also discovered a threat actor selling login credentials of global OEMs' employees and dealers on a popular dark web marketplace.

Messaging applications

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

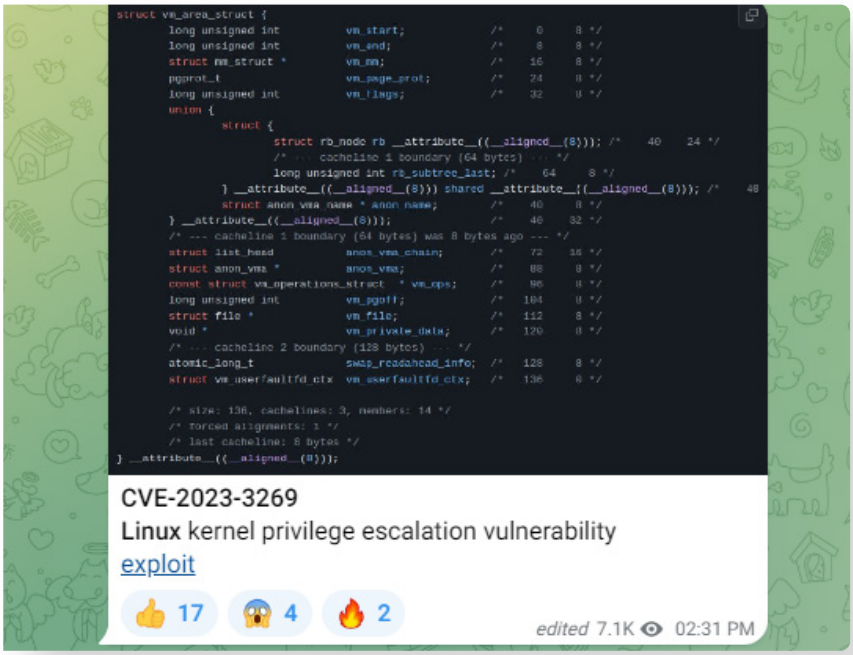
Popular messaging applications—such as Telegram, Discord, Signal, and WhatsApp—are actively being used to share hacking methods, and trade in stolen credit cards, account credentials, exploitations of vulnerabilities, leaked source codes, and malware.

Applications like these have replaced the secretive, hard-to-navigate dark web forums.

In June 2023, Upstream discovered a post on a ransomware Telegram channel leading to data stolen from a Japanese OEM, including sensitive customer PII.

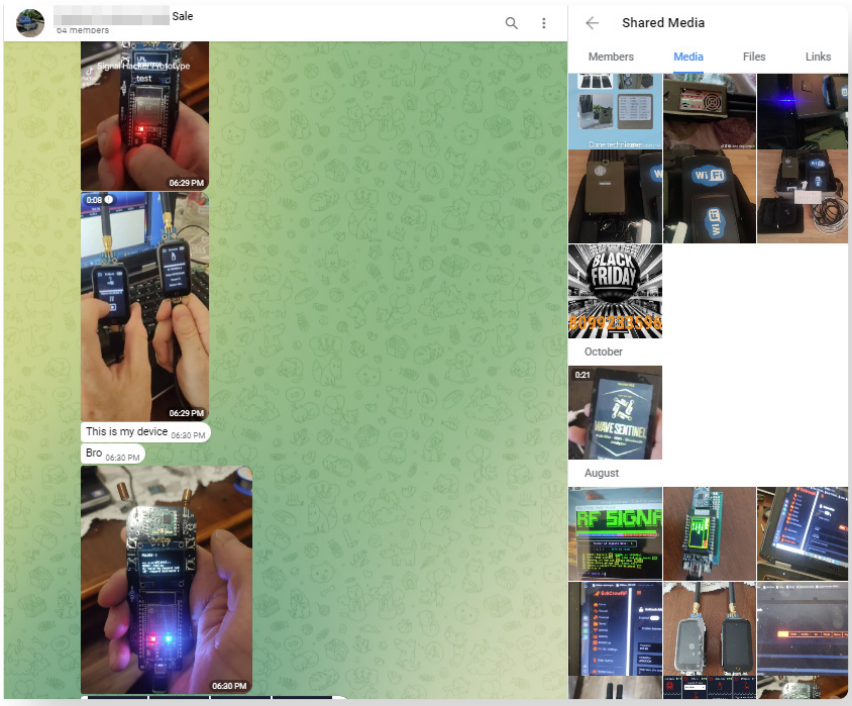
Example of a Telegram message related to stolen OEM data

In August 2023, Upstream uncovered information about a Linux kernel exploit impacting many large OEMs, known as CVE-2023-3269, posted on a 10,000-member cybercrime Telegram channel.



Exploit found on the cybercrime Telegram channel

In December 2023, Upstream tracked Eastern European threat actors operating on a popular Telegram channel, selling a relay attack keyless repeater promising the ability to unlock and start vehicles of multiple OEMs. Sellers are highly active and responsive and have a long history of unauthorized vehicle access tools.



Relay attack keyless repeater for sale on Telegram

THREAT ACTORS IN THE DEEP AND DARK WEB

Security researchers

Researchers use their technical expertise to identify cybersecurity vulnerabilities within organizations and across industries. To be effective, researchers need to stay up to date on the latest attack vectors, trends, and new enabling technologies. **Many security researchers publish their findings—which include vulnerability exploits and vehicle toolkits—in public code repositories hosting services like GitHub. The knowledge that security researchers share is usually public, making it accessible to anyone, including malicious threat actors.**

In January 2023, a security researcher hacked the head unit of a South Korean OEM vehicle model. The researcher was able to root the unit, enabling him to add and delete features, by reverse-engineering the head unit's firmware—which is also used across a wide range of other vehicle models, putting many more head units at risk.[221]

In October 2023, a security researcher exposed risks caused by misconfigured third-party self-hosted data loggers used by US EV OEM consumers.[222] Using open-source intelligence techniques (OSINT), the researcher was able to find data loggers configured without authentication, and access their dashboards—allowing them to track live location, check if driver is present in car or not, take the car offline (e.g., sleep mode), check if the trunk of the car is open or not, and more. The researcher highlighted the potential risks, including the possibility of physical harm, outlined steps owners can take to protect themselves, and shared the OEM's response to his disclosure and suggestions.

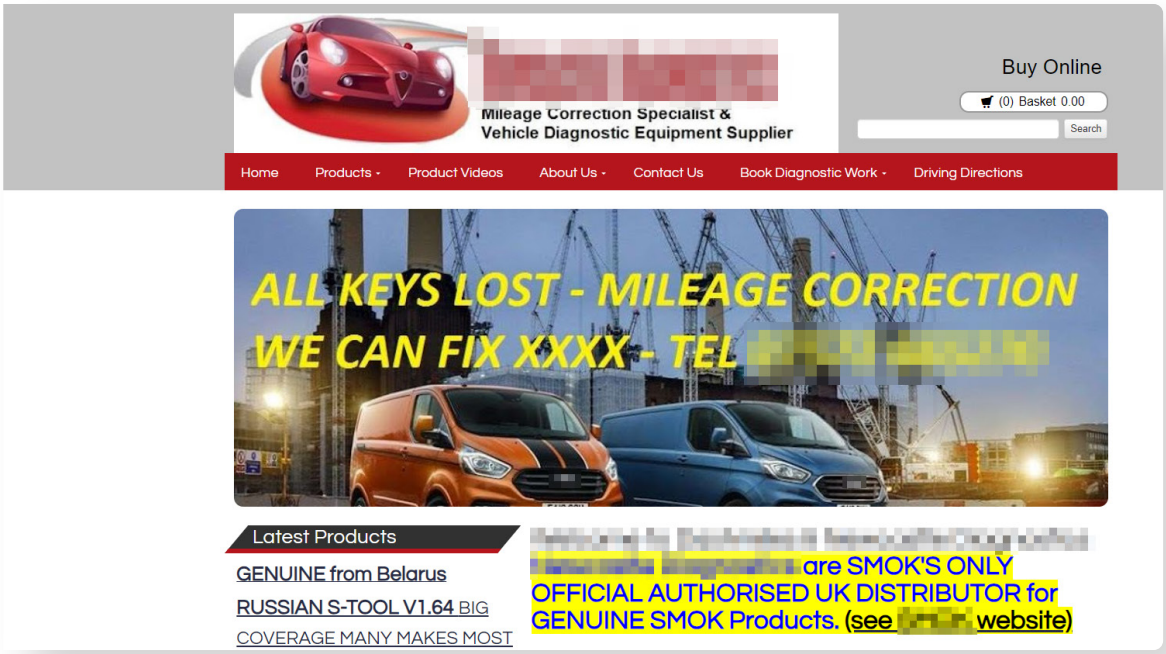
Fraud operators

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 fraud services on the deep web is mileage fix, formally known as odometer fraud, which involves disconnecting, resetting, or altering a vehicle's odometer to change the number of miles shown.

Every year, over 450,000 vehicles are sold with false odometer readings, costing American buyers over $1 billion, according to the NHTSA.[223]

In September 2023, Upstream discovered a threat actor selling mileage blockers and odometer programming tools (e.g., used for mileage correction) for specific vehicles made by Western European OEMs on a deep web automotive marketplace.



The fraud operators' website

Black hat hackers

Black hat hackers, operating in different deep and dark web forums and marketplaces, compromise cybersecurity with malicious intent and are involved in a wide range of activities. Some black hat hackers specialize in short-range hacking, such as hacking remote entry systems to steal vehicles, while others specialize in long-range hacking, mainly exploiting vulnerabilities.

When black hat hackers publish exploits for long-range vulnerabilities in deep and dark web forums, they expose many other threat actors to exploits that could crash or control vehicles, which may result in serious safety risks on a large scale.

In January 2023, Upstream discovered that black hat hackers had published an exploit for a Linux vulnerability impacting multiple OEMs on a cybercrime forum. Exploiting this vulnerability could cause a denial of service on the affected vehicles, leading their systems to crash. Moreover, exploiting the vulnerability could enable attackers to run commands on affected vehicles remotely.

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. The first issue is that malicious threat actors often lurk in these forums and take advantage of any reported bugs or problems. The second issue is that the files and links posted are untrustworthy and might contain malware, spyware, and ransomware, which could void warranties.

In June 2023, Upstream discovered that a jailbreak for major OEMs' IVI systems was available for download on a German car enthusiast blog. The blog included detailed guidelines, steps, and a video tutorial on hacking the IVI system, as well as examples for possible modifications that can be done once jailbroken.

RANSOMWARE ACTORS INCREASINGLY TARGET AUTOMOTIVE SUPPLIERS

Malicious actors are increasingly targeting a wide range of automotive and mobility stakeholders—including OEMs, suppliers and even EV charging infrastructure—with ransomware attacks. Any part of the supply chain can pose a risk to OEMs, service providers, or mobility IoT devices. Automotive suppliers are highly specialized, meaning switching costs are very high and replacement isn't straightforward.

> ***Operational availability and production could be severely affected by ransom attacks across the supply chain.***

To extort money, attackers typically maintain a 'leak site' on the dark web, where they reveal stolen data and sensitive information about organizations, and publish posts about their victims. In 2023, ransomware attacks and leak sites made the headlines often. The following are just a few notable attacks.

IN JUNE 2023, A TIER-2 WAS HIT BY $70 MILLION RANSOM DEMAND, THE LARGEST IN HISTORY

In June 2023, a leading Taiwan-based semiconductor manufacturer disclosed a cybersecurity incident involving a ransomware group and one of its IT hardware suppliers, which led to the leak of information pertinent to server initial setup and configuration.[224] The attackers claim to have access to internal documents with confidential information, demanding a $70 million ransom to decrypt the data and prevent its release online —making it the largest known ransom demand in history. While the breach could affect multiple automotive stakeholders, the company reported that neither its business operations nor customer information were affected by the cyber incident at its supplier. The company also immediately terminated its data exchange with this provider following the incident.

In August 2023, a Dutch Tier-1 supplier of electromagnets was hit by a ransomware attack in which the ransomware group gained unauthorized access to the company's systems, disrupting its development and sales departments. In response, the company hired leading third-party cybersecurity experts and activated its response protocol, including its operational continuity plan.[225]

Also in August 2023, a Thailand-based battery manufacturer partnering with a German OEM suffered a ransomware attack that resulted in data theft. Five samples of documents, showing the victim's projects and information, were leaked by the ransomware group, which threatened to publish the stolen information if it wasn't paid.[226]

Ransom attacks pose a significant risk for fleets, telematics systems, and IoT devices. **In September 2023, a leading US-based trucking and fleet management solutions provider experienced a ransomware attack that resulted in customers being unable to electronically log their on-road hours—as required by federal regulations—or track their transported inventory.**[227]

Also in September, one of the UK's largest logistics groups declared insolvency following a ransomware attack.[228]

THE AUTOMOTIVE AND MOBILITY ECOSYSTEM MUST REACT IMMEDIATELY TO THE INCREASE IN DEEP AND DARK WEB ACTIVITIES

Data sharing on the deep and dark web has continued to dramatically increase during 2023, with automotive-related security vulnerabilities, data breaches of sensitive information, and other cyber threats regularly published and discussed. **Upstream's AutoThreat® PRO analysts discovered a greater amount of automotive information on deep and dark websites. It is necessary to monitor and mitigate these risks regularly to stay ahead of threat actors on the deep and dark web—product intelligence and automotive expertise are essential for this process.**

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. **The UNECE WP.29 R155 regulations and the ISO/SAE 21434 standard, as well as NHTSA guidelines and the regulations in China, require cyber threat intelligence and vulnerability monitoring—the deep and dark web must be considered an integral part of those requirements.**

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 preventive 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 connected vehicles, which presents many challenges for OEMs, Tier-1s and 2s, as well as other mobility stakeholders.***

Upstream's AutoThreat® PRO solution—purpose-built to overcome these challenges—collects, analyzes, and publishes cyber threat intelligence specific to the automotive and smart mobility ecosystem, covering the entire supply chain, and is tailored to various automotive segments, including OEMs, Tier-1 and 2 suppliers, mobility IoT, connected vehicle service providers, insurance companies, and other mobility stakeholders.

Upstream proactively monitors the deep and dark web to uncover emerging automotive-related cyber trends and threat actors. As a result, Upstream can identify and mitigate new threats—vulnerabilities, exploits, and fraud operations—before they become widely known and spread across the deep and dark web.

Armed with the right cyber threat intelligence, automotive and mobility stakeholders can proactively implement the necessary cybersecurity measures to prevent the next cyber incident.

06

AUTOMOTIVE CYBERSECURITY SOLUTIONS

Providing the vSOC with the tools and insights it needs to effectively mitigate the increasing impact and scale of cybersecurity threats

CYBERSECURITY SOLUTIONS CONTINUE TO EVOLVE

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

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

Smart mobility stakeholders, OEMs, Tier-1s, and Tier-2s will continue to place a high priority on cybersecurity as new standards and regulations are adopted. To ensure connected cars and mobility services remain secure into the future, it's imperative they use a multilayered cybersecurity approach.

Protecting the vehicle during its entire lifecycle, across a complex supply chain and dynamic SBOM

Passenger cars typically last 12 years, commercial trucks 20 years, and agricultural vehicles 30 years. OEMs must therefore develop long-term strategies to secure products operating on decades-old technology.

UNECE WP.29 R155 and ISO/SAE 21434 establish the requirement to consider life-long cybersecurity threats and vulnerabilities during development, production, and post-production phases of the vehicle's lifecycle. OEMs and their suppliers came under regulation and standardization for the first time in 2022. In 2023, OEMs continued to focus on two key areas: preparing for the expected growth in scope of monitored vehicles with the second milestone of R155 in 2024, and securing connected vehicles across complex supply chains with dynamic SBOMs.

2023 marked the second year OEMs have required Tier-1 and Tier-2 suppliers to disclose their cybersecurity practices, easing concerns about production disruptions beyond supply chain bottlenecks.

By doing so, they have been able to reduce the risk of carrying cybersecurity vulnerabilities directly from third-party vendors onto their vehicles, and combat counterfeit components from entering legitimate facilities, threatening safety by reducing wear ratings, overriding safety limits, etc.

R155 requires OEMs to implement and maintain threat analysis and risk assessment (TARA) throughout all stages of the vehicle lifecycle. They must also create processes to address and mitigate against future attacks together with their Tier-1 and Tier-2 suppliers.

ISO/SAE 21434 can be used as guidance on how to carry out the R155 requirement together with suppliers.

01

Cyber record of capability

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

02

Define shared responsibilities

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

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

Security by design

One of the four measures explicitly specified by the R155 regulation for vehicle cybersecurity is securing vehicles "by design" to mitigate risks along the value chain.

Security by design requires evaluating the cybersecurity risks of a component or software as early as the development phase. This is done by making sure that all vehicle components are designed, developed, and tested for cybersecurity vulnerabilities, and that any risks discovered are effectively mitigated.

While OEMs are ultimately responsible for the security of their vehicle, all suppliers in the supply chain need to adopt security-by-design practices as well.

Multi-layered cybersecurity stack

Multi-layered security has already become a standard in IT and enterprise cybersecurity. Increasingly sophisticated threats and new vulnerabilities are constantly emerging, requiring businesses to improve security, and use multiple sources of data to detect threats and respond effectively. Enterprises use multiple security solutions, including end-point solutions, network security solutions, cloud security, API security, internal segmentation technology, and more.

In 2019, Gartner standardized the practice by introducing the network-centric concept of the Security Operations Center (SOC) Visibility Triad.[229] According to Gartner's research, a modern SOC must rely on three well-known core security elements for increased threat visibility, detection, response, investigation, and remediation:

01

Security Information and Event Management (SIEM)

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

02

Network-centric detection and response

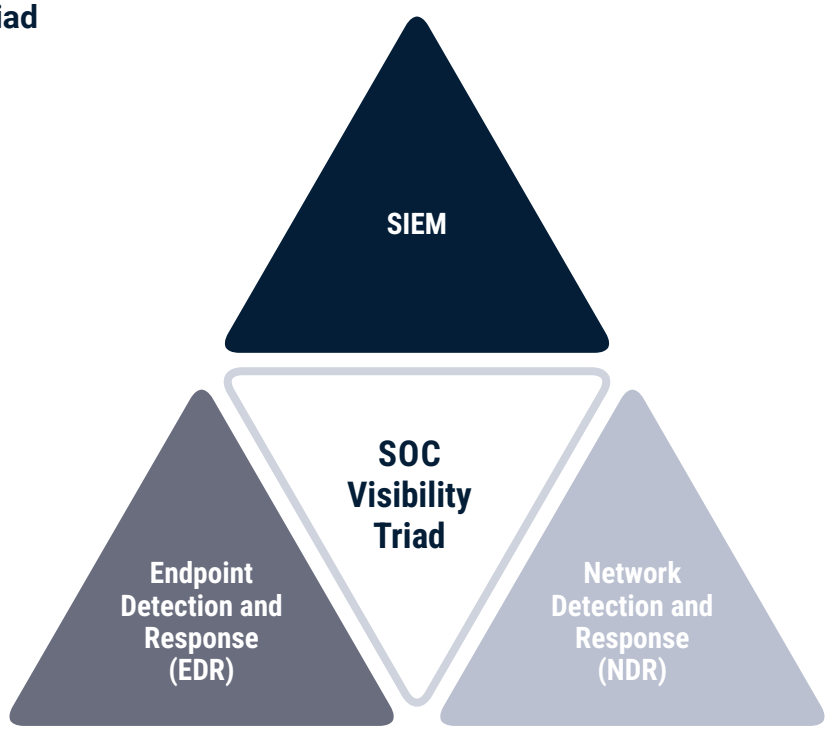
Monitors network traffic and correlates detected threats with network activity.

03

Endpoint detection and response

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

SOC visibility triad



Visual representation of a multi-layered SOC approach, based on Gartner's SOC visibility triad[229]

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

Three layers of automotive cybersecurity

API security

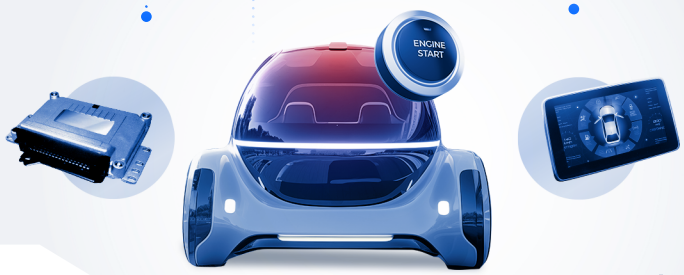
This new addition to the vSOC is a cross-functional effort between the vSOC and the IT SOC, focusing on protecting API-based applications, services, and features.

Automotive cloud security

Leverage 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, etc.; 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, DTC data streams, OS logs, CAN events, etc.



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

DEVELOPING AN EFFECTIVE VSOC

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

As the number and sophistication of cyber attacks targeting vehicles, mobility applications, OT and IoT mobility devices increase, OEMs must develop integrated vSOCs, also known as “mobility SOCs” or “automotive SOCs”, to protect their vehicles, infrastructure, and customers during the post-production phase.

An effective vSOC is essential for the security of connected vehicles and Smart Mobility ecosystems. It allows OEMs to monitor their entire infrastructure and vehicles in real-time, and respond to detected threats quickly.

However, with the constant expansion and digital transformation of the Smart Mobility ecosystem, more stakeholders are expected to require a vSOC. Mobility IoT vendors, fleet systems, and other smart mobility service providers will shift to monitoring and protecting their assets via a vSOC.

When implemented properly, an effective vSOC has a clear framework—detailing capabilities, components, and operating models—and a well-defined strategy and scope—including a vision, mission, and charter.

An effective vSOC should also:

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

vSOCs can be built in three ways:

01 COMBINE

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

02 CREATE

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

03 CONTRACT

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

During 2023, many OEMs continued to focus on their vSOC implementation journey, based on the understanding that vSOCs are critical for effective mitigation and response. The scope of monitored vehicles for regulatory purposes is expected to grow significantly with the second milestone of R155 in July 2024. OEMs must ensure their vSOC teams, platforms, and processes are adjusted accordingly.

The next generation of vSOCs

OEMs are continuously working on solidifying vSOCs and positioning them internally. They are defining vSOC scope, deciding where it belongs in the organizational structure, and evaluating sourcing (e.g., in-house, hybrid or managed vSOC) and operating models (e.g., one global vSOC, multiple geographies presence, etc.).

OEMs must establish vSOCs as soon as possible to comply with R155. There are several options for vSOC implementation:

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

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

Fusion vSOC

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

IT-OT vSOC

that combines the IT SOC and the vSOC into a single entity that manages a broad security operations center, covering security elements of the entire vehicle lifecycle—from design to manufacturing (e.g., OT monitoring of vehicle production) and operations.

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

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

AUTOMOTIVE-SPECIFIC THREAT INTELLIGENCE OFFERS A PROACTIVE APPROACH TO RISK

The multi-layered approach must also include proactivity to enhance threat detection capabilities, such as monitoring cyber threat intelligence.

OEMs and mobility stakeholders should proactively identify and mitigate vulnerabilities in their products while remaining compliant. By using an industry-specific and purpose-built threat feed, stakeholders can remain continuously updated with new threats based on surface, deep, and dark web findings.

As the connected vehicle ecosystem becomes more complex and introduces large-scale cyber risks, automotive-specific threat intelligence products are becoming increasingly important. Cyber vulnerabilities and attacks impact the entire supply chain, jeopardizing trust and safety, and require all stakeholders to be proactive in analyzing risks, monitoring threats, and responding effectively to cyber attacks.

Benefits to OEMs

- Detect cyber threats against mobility assets early
- Comply with automotive standards and regulations requiring in-depth threat intelligence
- Manage reputational risk before threats, vulnerabilities, or hacks go public
- Avoid future warranty issues by discovering warranty and policy violations early
- Build trust with customers due to increased awareness of cyber threats
- Monitor and manage direct threats to the automotive supply chain
- Assess current threat posture and benchmark it against peers or competitors

Benefits to Tier-1 and Tier-2 suppliers

- Gain OEM trust through more in-depth component threat monitoring
- Reduce future warranty costs by discovering warranty and policy violations early
- Identify and remedy component vulnerabilities by monitoring popular component-hacking forums and chats
- Comply with regulatory demands by monitoring threat feeds for vulnerabilities and mitigating them

Benefits to CISOs

- Monitor for leaked organizational data, and PII to detect potential breaches that could expose an organization
- Develop steps to improve IT and OT security and implement the right cybersecurity measures within cloud services and corporate networks
- Monitor and analyze attacks on other organizations to develop defense methods against similar threats to their own assets and applications
- Develop a better understanding of the cyber threat landscape to enable an effective evaluation of cyber risks, prioritize actions, and allocate resources more efficiently
- Discover actors active on the dark web selling access to corporate networks
- Discover insider threats to an organization
- Monitor for leaked intellectual properties such as products' bill of materials

Benefits to vSOC analysts

- Monitor forum chat exchanges to detect new and emerging threats as early as possible
- Identify new fraud modus operandi (MOs), trends, and threat actors
- Recognize and monitor commonly pirated features and illegal modifications
- Detect, warn, and offer next steps regarding data breaches involving private automotive customer information
- Find new threats that could disrupt the organization's networks, resources, or business
- Stay on top of new vulnerabilities or exploits being sold in underground marketplaces
- Monitor vehicle-related software security to issue necessary OTA updates
- Prevent future connected vehicle cyber attacks by disabling compromised accounts and/or notifying their owners
- Track automotive-related zero-day vulnerabilities and exploit kits

Benefits to the insurance ecosystem

- Enable actuaries to effectively measure risk and evaluate policy costs by identifying primary causes, locations, and methods of automotive breaches and hacks
- Detect popular insurance fraud methods, such as manipulating connected vehicle dashcams
- Identify and prevent warranty and/or insurance policy violations, such as odometer manipulation
- Understand geographical risk areas in local markets and assets subsets

Benefits to smart mobility applications and services

- Identify fraud related to identity theft
- Detect the sale of fraudulent car sharing/ride hailing user and driver accounts
- Spot malicious vendors selling car sharing/ride hailing or rental user data
- Monitor hacking forums for methods of stealing or manipulating shared mobility assets

Threat actors are increasingly targeting telematics and other connected vehicle data as OEMs strive for greater connectivity in their vehicles. **Only automotive-specific threat intelligence products can understand a vehicle's context to quickly identify anomalies and remove false alarms that may desensitize cybersecurity teams.** Product cybersecurity executives and CISOs must address the growing threat of automotive hacking with a unique approach that fits their organization's needs.

OEM & SMART MOBILITY APPLICATIONS REQUIRE EXPANDED FUSION DETECTION—EXTENDING COVERAGE BEYOND OWASP TOP 10

In practice, API hacking at the entry level is relatively standardized, requires lower technical expertise, and can be done remotely without special hardware—making it more cost-effective to hack than other types of systems.

The Open Web Application Security Project (OWASP) API Security Top 10[230] serves as an IT industry standard to help developers and security teams understand API risks and is updated as threats evolve.

Updated in 2023, the top 10 list includes:

01 **Broken Object Level Authorization**

02 **Broken Authentication**

03 **Broken Object Property Level Authorization**

04 **Unrestricted Resource Consumption**

05 **Broken Function Level Authorization**

06 **Unrestricted Access to Sensitive Business Flows**

07 **Server-Side Request Forgery**

08 **Security Misconfiguration**

09 **Improper Asset Management**

10 **Unsafe Consumption of APIs**

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

But in the context of Automotive and Smart Mobility ecosystems, IT-based API security like OWASP, is not enough. IT-based security solutions focus on transactions, permissions, volumes, values, and payload correctness—often ignoring the contextual state of mobility assets, their physical behavior on the road and safety impact.

In addition to API traffic, extended detection should consider additional data sources, such as telematics data. By combining these two sources of information, organizations can gain a deeper understanding of potential threats and vulnerabilities.

API security requires a holistic view, contextualizing operational data and API traffic to reflect the state of vehicles, applications, and consumers. A variety of data sources can be leveraged alongside API traffic and documentation to identify anomalies that indicate a threat to operational systems:

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

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

UPSTREAM'S CLOUD APPROACH TO AUTOMOTIVE CYBERSECURITY

Upstream provides a cloud-based cybersecurity and data management platform purpose-built for connected vehicles, delivering unparalleled automotive cybersecurity detection and response, and data-driven applications.

Upstream's agentless solution enables the protection of mobility IoT devices and applications, as well as connected vehicles with quick time-to-security. It also offers a holistic approach that analyzes the entire fleet to detect sophisticated fleet-wide anomalies and attacks.

The Upstream Platform unlocks the value of vehicle data, empowering customers to build connected vehicle and mobility applications by transforming highly distributed vehicle data into centralized, structured, contextualized data lakes. Coupled with AutoThreat® PRO, the first mobility cybersecurity threat intelligence solution, Upstream provides industry-leading cyber threat protection and actionable insights, seamlessly integrated into the customer's environment and vSOCs.

With attack surfaces expanding and adversaries developing complex methods to gain control of connected vehicles, the strong combination of the Upstream Platform and AutoThreat® PRO has become critical in securing the automotive industry.

The data gathered and analyzed by the AutoThreat® team is continuously used to create detectors and solutions for vulnerabilities and flaws seen in the field. This puts Upstream in front of future threats that are not yet known to the industry.

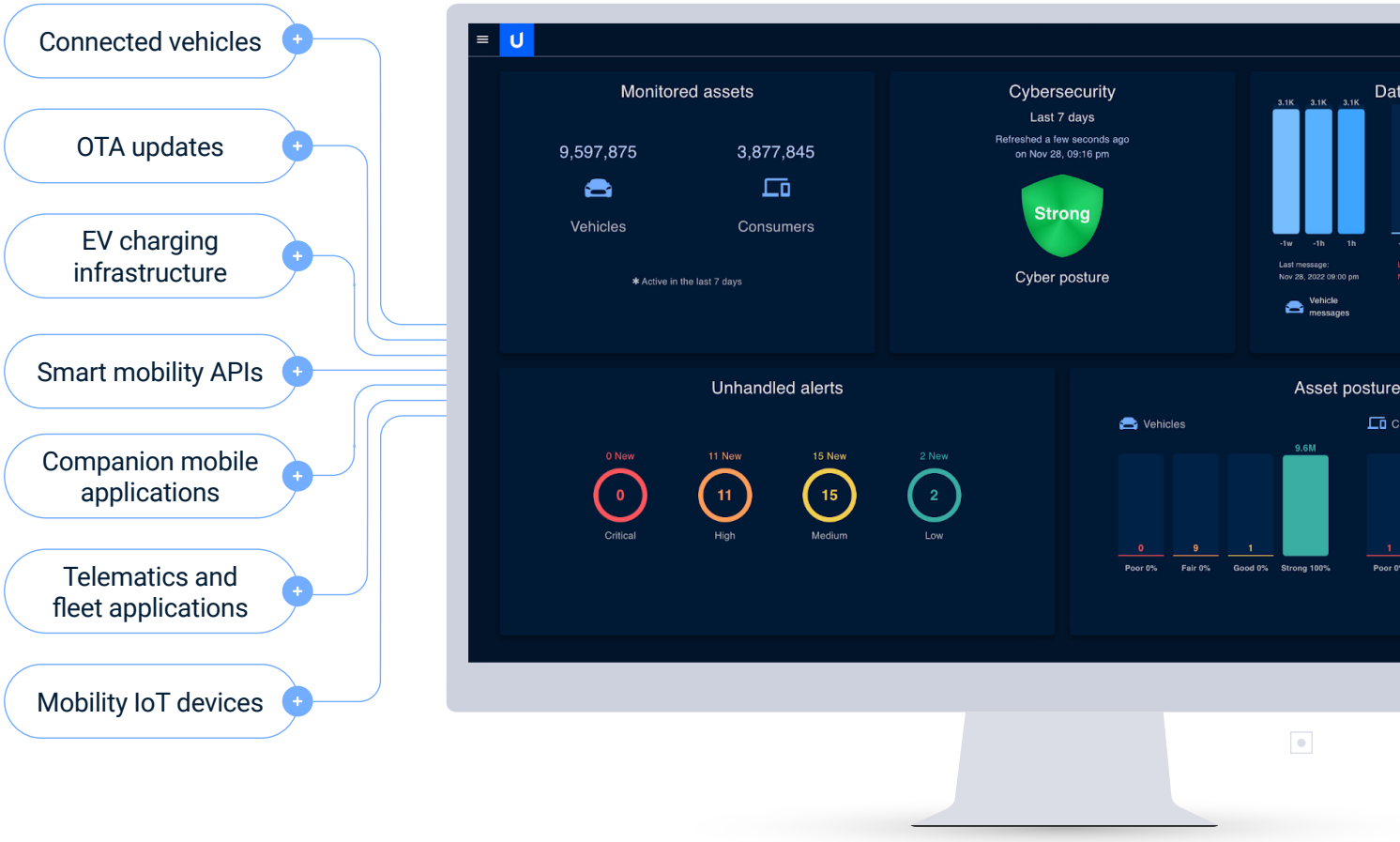
THE UPSTREAM PLATFORM

Back in 2017, Upstream introduced a fundamental innovative shift in protecting the connected vehicle ecosystem, with the first cloud-based cybersecurity and data management platform, purpose-built for connected vehicles and smart mobility.

The Upstream platform has significantly evolved into a robust cybersecurity detection and response platform (V-XDR), containing advanced machine learning models, hundreds of detectors that address both cybersecurity and mobility-related use cases for a wide range of smart mobility stakeholders, and generative AI layers for effective investigations.

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

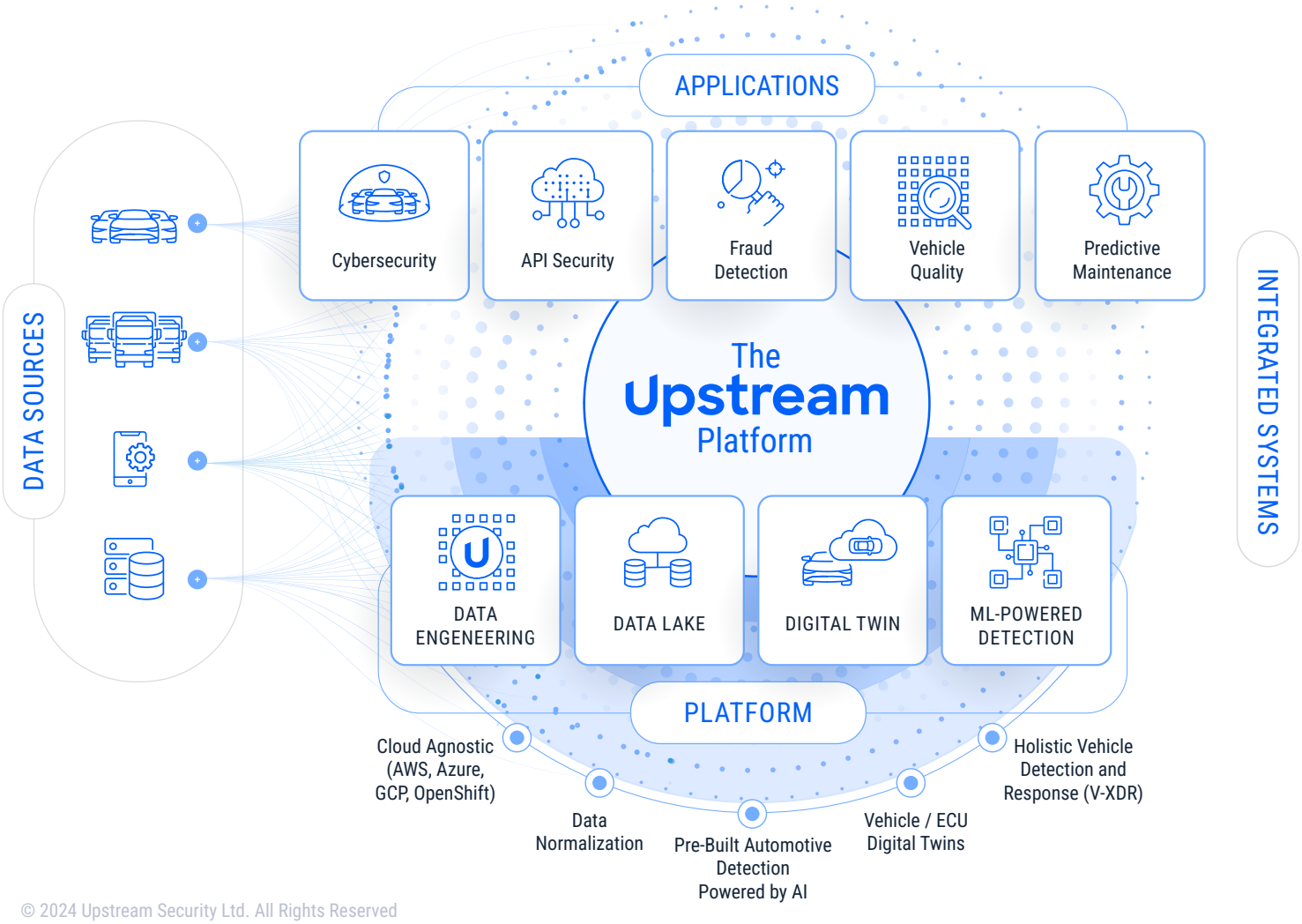
Upstream offers a ready-to-deploy solution that detects cybersecurity threats across the entire smart mobility ecosystem, covering:



Upstream's ability to handle numerous data streams and to develop advanced data analytics and ML applications has encouraged OEMs to extend their use of Upstream beyond cybersecurity, including fraud detection, predictive analytics, vehicle quality, insurance, and other data-driven use cases.

As a result, the Upstream platform was recently expanded to offer a wide range of use cases:

Cybersecurity	Monitor and detect cybersecurity-related attacks, threats, risks, and vulnerabilities.
API Security	Monitor and protect smart mobility API-based applications, devices, and services to ensure continuous operational availability and protect data.
Fraud Detection	Identify fraud-related scenarios including odometer rollback, vehicle theft, etc.
Vehicle Quality	Monitor connected vehicle quality to reduce recalls and maintenance costs.
Predictive Maintenance	Predict failure in critical modules to ensure operational availability and safety, and lower maintenance costs.



EXTENDING DETECTION AND RESPONSE TO ACCOMMODATE EVOLVING SMART MOBILITY CYBER RISKS

Smart Mobility API Security

With API-based cyber attacks and vulnerabilities proliferating, smart mobility stakeholders now face the challenge of monitoring billions of API transactions every month.

Upstream's API Security solution correlates between API transactions and the robust digital twin of the Upstream Platform, which offers a contextual and comprehensive view of all assets impacted—from the consumer application to IoT devices, and vehicles.

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

API discovery

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

API monitoring

conduct ongoing conformance analysis with continuous discovery of static and dynamic traffic sources to identify potential vulnerabilities in your API landscape introduced by updates.

Fusion detection

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

No-code detector builder

easily customize detectors and add new detection capabilities for emerging use cases and new business logic without coding or development resources.

vSOC analysts can monitor and detect API cyber threats in near-real-time, find the information they need for effective mitigation, and trigger workflows in response to alerts—ensuring uninterrupted operations.

Integrating In-Vehicle Security Data Stream

Upstream offers pre-built data ingestion and alerts for detecting in-vehicle security events triggered by Intrusion Detection and Prevention Systems (IDPS). Upstream's alerts are designed to reduce false positives that exist in many in-vehicle cybersecurity solutions. Upstream combines IDPS data flow with other connected vehicle data sources to provide vSOC analysts with additional context, allowing them to resolve issues quickly.

In-vehicle data source integrations include: Intrusion Detection System Manager (IDSM), various secured loggers, and IDPS data sources that support both Central Gateways and Telematics Control Units (TCUs).

Built-in Threat Hunting

Working closely with Upstream's AutoThreat® PRO, vSOC teams can leverage threat hunting to explore historical connected vehicle data and use cases to help analysts identify abnormal patterns and potential malicious activities.

Upstream Managed vSOC

Using the Upstream Platform, Upstream also offers a unique Managed vSOC service that provides deep and advanced detection, investigation, and mitigation capabilities—from the single ECU to the individual vehicle or device, and fleet-wide perspectives. With this holistic view, OEMs and smart mobility vendors can mitigate known and unknown cybersecurity threats against vehicles, applications, services, charging infrastructure, IoT devices, and entire fleets.

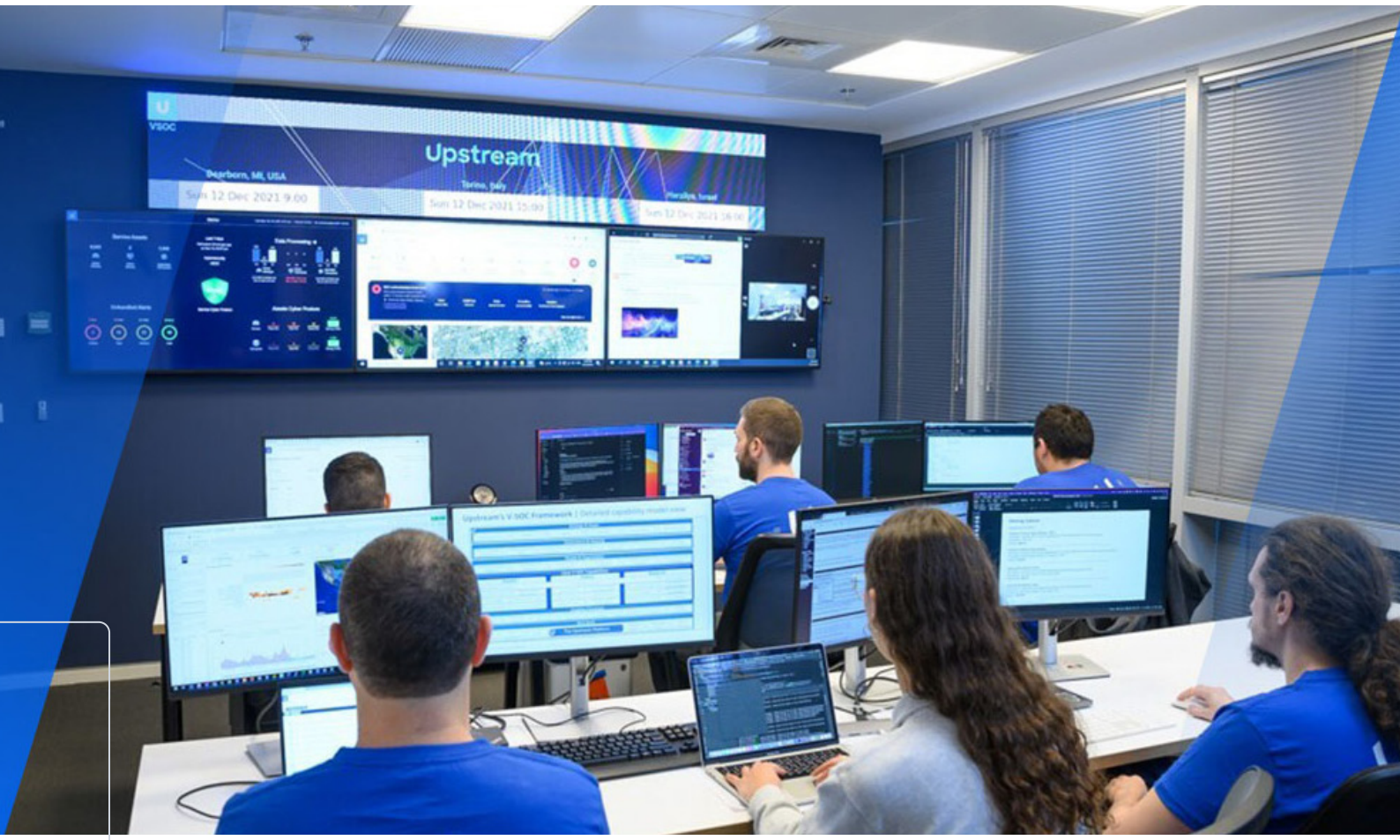
Upstream's Managed vSOC service leverages Upstream's robust technology stack as well as AutoThreat® PRO to deliver the highest possible impact. **Equipped with extensive experience monitoring millions of vehicles worldwide and proven methodologies, Upstream offers a turnkey solution with minimal ramp-up time.** Upstream's Managed vSOC integrates seamlessly with the OEM's existing processes and workflows, offering custom-built playbooks. Additionally, the service collaborates with many global MSSP partners to protect vehicles, devices and applications worldwide.

An experienced team of analysts and researchers with deep expertise in cybersecurity, mobility and IoT protocols, regulations and compliance, fraud, and operations, provides a unique perspective on the automotive ecosystem, making for a multidisciplinary vSOC.

With Upstream, OEMs and mobility stakeholders can benefit from a fully operational vSOC service that applies tried-and-true methodologies for threat detection and response, with the ability to expand coverage across geographies and scale up as needed.

OEMs can leverage a proven build-operate-transfer (BOT) model to ensure optimal flexibility and eliminate lock-in. Upstream's vSOC service trains OEM teams on implemented models, methodologies, and playbooks to ensure a smooth hand-over when needed.

The service is delivered from secure advanced facilities, in the US and Israel, and uses compartmentalized Role-Based Access Control (RBAC) data access permissions. The service is fully compliant with regulations, including the European GDPR adequacy requirements, and can be remotely audited with ease.



Upstream's vSOC

Upstream's vSOC

During 2023, Upstream has enhanced detection and investigation capabilities by extending vSOC visibility in several key areas showcased below, and integrated numerous in-vehicle data streams directly into the Upstream Platform to provide endpoint management-like functionality.

On the response side, Upstream has been focused on expanding our capabilities by building end-to-end response processes and documentation such as playbooks and cross-functional collaborations. In 2023, Upstream's vSOC expanded its cross-functional impact by deepening integration with SIEM and SOAR partners to ensure wide organizational visibility and effective shift-left remediation.

ENHANCING VSOC INVESTIGATIONS WITH GENAI

In 2023, Upstream introduced an advanced GenAI-powered query layer into the Upstream V-XDR platform. These new capabilities support vSOC teams and enable them to think “outside of the box” and effectively analyze massive amounts of data across multiple sources, detect patterns, filter incident alerts, and automate investigations.

With today’s vSOC challenged to handle large-scale risks, GenAI helps draw insights by querying the data with simple natural language Processing (NLP) questions.

GenAI transforms vSOC investigations and operations, enabling a number of use cases:

Data analysis
identify and analyze relevant historical data, such as the number of weekly cybersecurity alerts over a given period, automatically identifying patterns and anomalies.

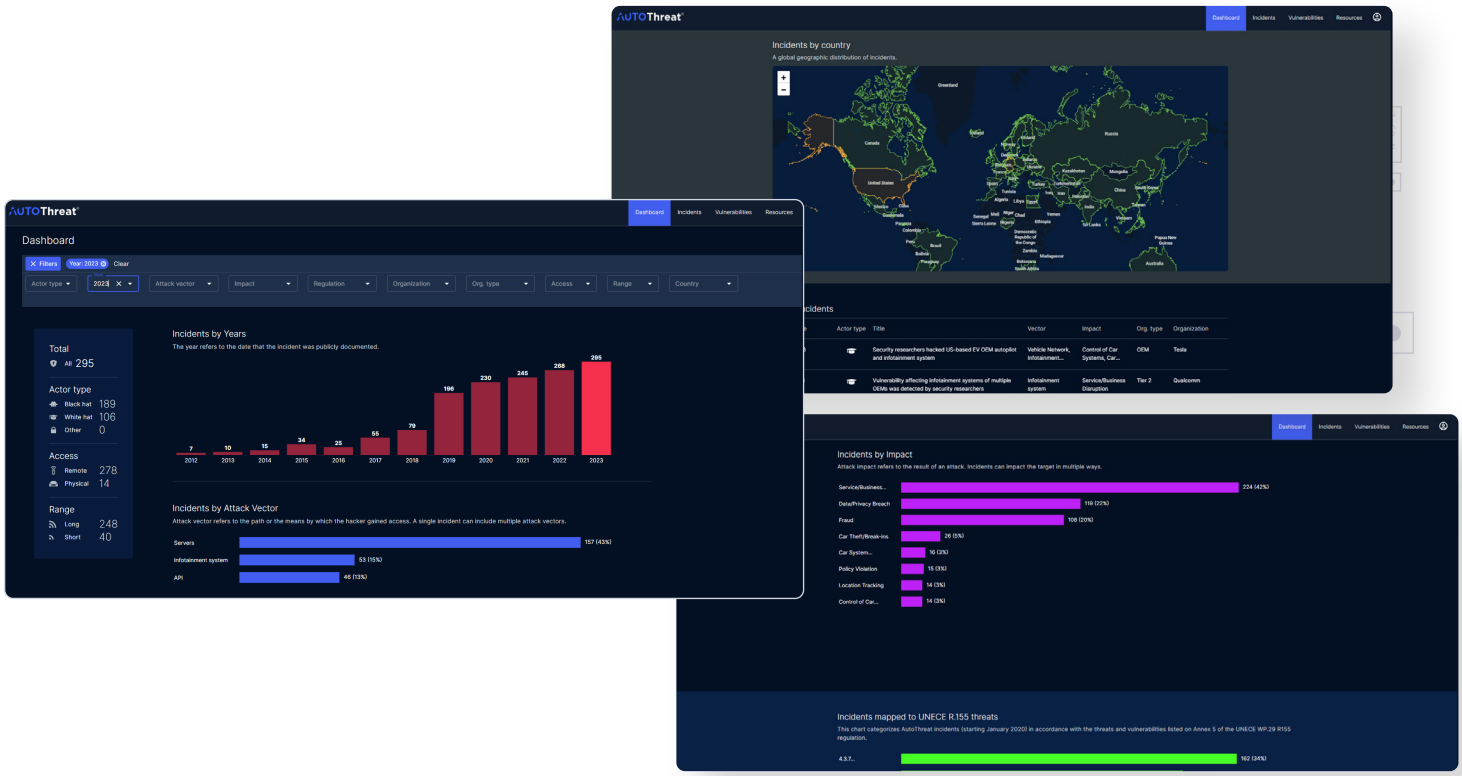
Alert filtering
track the severity of alerts, identifying trends and sudden spikes in high-severity alerts, which is crucial for prioritizing security responses.

Alert analysis
get in-depth insights into specific types of alerts, such as those related to unauthorized OTA software updates, highlighting security risks.

Investigation and automation
improve investigations and automate vSOC workflows using conversational chat, saving time and resources.

Enhanced TARA
generate complex insights based on deep and dark web data and in-depth TARA.

UPSTREAM AUTOTHREAT® PRO CYBER THREAT INTELLIGENCE



Upstream's AutoThreat® PRO is the first and only cyber threat intelligence (CTI) solution, purpose-built for the Automotive and Smart Mobility ecosystem. It provides customized CTI, deep and dark web research, and analyzes client-dedicated assets (e.g., SBOM), automotive and mobility threat actors, and specific automotive cyber risks. Upstream's CTI is tailor-made to identify vulnerabilities, exploits, fraud, and counterfeits within the automotive and mobility threat ecosystem.

Upstream's unique perspective on automotive CTI is focused on uncovering the unknown pieces of the product cybersecurity puzzle. By analyzing products and components, from a single ECU and up to a complete vehicle model or connected device, mobility stakeholders can boost vulnerability management, threat awareness, and product intelligence — and ensure regulatory compliance.

Upstream's AutoThreat® team includes cybersecurity researchers and analysts with deep automotive and mobility expertise, as well as extensive product cybersecurity experience. The service includes periodic and urgent CTI deep and dark web research reports and customized queries. AutoThreat® PRO also offers an easy-to-use online platform, as well as access to a clear-web cyber incident portal, vulnerability management via Upstream's automated CVE feed, and a dedicated automotive threat actor repository.

07

PREDICTIONS FOR 2024

New technologies such as Generative AI, as well as the growing reliance on APIs and IoT devices, will present new opportunities and challenges.

Looking into 2024, here are our top predictions:

01 The automotive digital transformation will continue to introduce large-scale attack vectors

Seeking a competitive advantage will continue to drive the industry's digital transformation, based on the rapid introduction of mobility applications, in-vehicle subscriptions, data-driven services, etc. As vehicles become more software-defined, enabling remote access to critical vehicle functions, the attention must shift to securing APIs and expanding vSOCs coverage to monitor API-related threats.

02 Generative AI emerges as a double-edged sword

GenAI will have a profound impact on automotive and smart mobility stakeholders, introducing new large-scale attack methods. GenAI is expected to become a critical tool for threat actors, enabling them to quickly identify vulnerabilities, learn how to exploit them, and perform fleet-wide attacks—standardizing their tactics, methods, and workflows.

However, GenAI also offers stakeholders the ability to transform automotive cybersecurity, enabling a range of use cases from agile investigations, to automating vSOC workflows, and even generating complex insights based on deep and dark web data and in-depth TARA.

03 Automotive cybersecurity regulations are becoming overwhelmingly complex

The industry is experiencing initial signs of fatigue as compliance deadlines approach and new standards are constantly introduced. With the upcoming second milestone of UNECE WP.29 R155, the potential inclusion of new regulations for 2- and 3-wheelers and agricultural vehicles, new regulations in China and other countries–stakeholders are facing an extremely complex regulatory landscape.

04 Rapid EV adoption expands cyber risks and drives regulations

OEMs and EV charge point operators (CPOs) continue to deepen cybersecurity risks assessments, expanding processes to also cover IoT protocols, standards and regulations. It is also crucial to evaluate and adopt purpose-built solutions to protect strategic EV charging infrastructure. New regulations for electric vehicle supply equipment (EVSE) have emerged in the US and UK. China is also enacting regulations for EVSE, AVs, and Automotive Information Security.

REFERENCES

1. https://upstream.auto/research/automotive-cybersecurity/
2. https://upstream.auto/autothreat-intelligence/
3. Upstream Security
4. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
5. https://samcurry.net/web-hackers-vs-the-auto-industry/
6. https://therecord.media/orbcomm-trucking-software-ransomware, https://www.bleepingcomputer.com/news/security/orbcomm-ransomware-attack-causes-trucking-fleet-management-outage/ , https://www.marketscreener.com/quote/stock/HAYNES-INTERNATIONAL-INC-46351/news/Haynes-International-Inc-Begins-Network-Outlet-of-Cybersecurity-Incident-44109194/
7. https://www.bleepingcomputer.com/news/security/orbcomm-ransomware-attack-causes-trucking-fleet-management-outage/
8. Upstream Security
9. Upstream Security
10. https://voonze.com/tsmc-supplier-suffers-ransomware-attack-and-has-data-leaked-by-hacker-group/ , https://finance.yahoo.com/news/chipmaker-tsmc-confirms-data-leak-151811628.html
11. https://www.cyberdaily.au/security/9879-lockbit-ransomware-gang-claims-hack-on-queensland-based-q-automotive-group
12. https://techcrunch.com/2023/03/28/hackers-could-remotely-turn-off-lights-honk-mess-with-teslas-infotainment-system/, https://insideevs.com/news/659185/tesla-model-3-compromised-in-under-two-minutes-at-hacking-contest/
13. https://www.auroralabs.com/ota-ccg-lp-1/
14. https://www.reuters.com/legal/tesla-owners-sue-over-impact-software-update-ev-batteries-2023-05-12/
15. https://www.reuters.com/legal/tesla-owners-sue-over-impact-software-update-ev-batteries-2023-05-12/
16. https://techcrunch.com/2023/06/09/shell-recharge-security-lapse-exposed-drivers-data/
17. https://www.ibm.com/reports/data-breach
18. https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/numbers-and-figures
19. https://www.bcg.com/publications/2023/rewriting-rules-of-software-defined-vehicles
20. https://unece.org/sites/default/files/2021-03/R155e.pdf
21. https://unece.org/sites/default/files/2021-03/R156e.pdf
22. https://www.iso.org/standard/70918.html
23. https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf
24. https://www.asiafinancial.com/china-plans-rules-to-regulate-data-flows-from-smart-cars
25. https://eaton-works.com/2023/03/06/toyota-c360-hack/
26. https://www.latestly.com/socially/world/bykea-app-hacked-pakistans-ride-hailing-application-gets-hacked-users-receive-abusive-messages-see-pics-5197926.html
27. https://www.thedrive.com/news/43454/why-milwaukee-might-sue-hyundai-kia-over-stolen-car-epidemic
28. https://urbanmilwaukee.com/2022/08/17/kia-hyundai-thefts-now-national-problem/
29. https://edition.cnn.com/2023/01/27/business/progressive-state-farm-hyundai-kia/index.html
30. https://www.nhtsa.gov/press-releases/hyundai-kia-campaign-prevent-vehicle-theft
31. https://www.techradar.com/news/hyundai-and-kia-cars-could-be-stolen-with-just-a-usb-cable, https://www.malwarebytes.com/blog/news/2023/02/tiktok-car-theft-challenge-hyundai-kia-fix-flaw
32. https://hackingtoolscar.pl/shop/
33. https://www.tiktok.com/@keyless_go
34. https://www.mckinsey.com/features/mckinsey-center-for-future-mobility/our-insights/drivers-of-disruption/gen-ai-in-high-gear-mercedes-benz-leverages-the-power-of-chatgpt
35. https://www.bain.com/insights/generative-ai-and-cybersecurity-strengthening-both-defenses-and-threats-tech-report-2023
36. https://www.gartner.com/en/newsroom/press-releases/2023-10-11-gartner-says-more-than-80-percent-of-enterprises-will-have-used-generative-ai-apis-or-deployed-generative-ai-enabled-applications-by-2026
37. https://samcurry.net/web-hackers-vs-the-auto-industry/
38. https://xakcop.com/post/hyundai-hack-2/
39. https://www.bleepingcomputer.com/news/security/researcher-breaches-toyota-supplier-portal-with-info-on-14-000-partners/amp/
40. https://www.malwarebytes.com/blog/news/2023/02/tiktok-car-theft-challenge-hyundai-kia-fix-flaw
41. https://www.motor1.com/news/654686/car-thieves-destructive-can-bus-hack-steal/
42. https://insideevs.com/news/659185/tesla-model-3-compromised-in-under-two-minutes-at-hacking-contest/

REFERENCES

43. https://eaton-works.com/2023/03/06/toyota-c360-hack/
44. https://www.bleepingcomputer.com/news/security/hackers-compromise-3cx-desktop-app-in-a-supply-chain-attack/
45. https://nvd.nist.gov/vuln/detail/CVE-2023-29389
46. https://nvd.nist.gov/vuln/detail/CVE-2023-26244
47. https://www.cybersecurityconnect.com.au/industry/9052-toyota-data-breach-exposes-10-years-worth-of-data-for-over-2m-customers
48. https://www.bleepingcomputer.com/news/security/multinational-tech-firm-abb-hit-by-black-basta-ransomware-attack/
49. https://www.stern.de/gesellschaft/regional/bayern/internet--einschraenkungen-bei-werkstattkette-atu-nach-cyberangriff-33482946.html
50. https://garage.asrg.io/cve-2023-3028-improper-backend-communications-allow-access-and-manipulation-of-the-telemetry-data/
51. https://hackaday.com/2023/06/08/hacking-a-hyundai-ioniqs-infotainment-system-again-after-security-fixes/
52. https://www.globalvillagespace.com/tech/shell-recharge-data-breach-exposes-ev-drivers-information/
53. https://grist.org/technology/hackers-already-infiltrate-ev-chargers-it-could-only-get-worse/
54. https://therecord.media/major-japanese-port-suspends-operations-following-lockbit-attack
55. https://thehackernews.com/2023/07/a-data-exfiltration-attack-scenario.html
56. https://www.blackhat.com/us-23/briefings/schedule/index.html#jailbreaking-an-electric-vehicle-in--or-what-it-means-to-hotwire-teslas-x-based-seat-heater-33049; https://www.darkreading.com/application-security/tesla-jailbreak-unlocks-theft-in-car-paid-features
57. https://therecord.media/moovit-vulnerabilities-allow-free-subway-rides
58. https://www.foxbusiness.com/technology/tesla-data-breach-affects-75735-people-state-attorney-general-announces
59. https://therecord.media/orbcomm-trucking-software-ransomware; https://www.bleepingcomputer.com/news/security/orbcomm-ransomware-attack-causes-trucking-fleet-management-outage/
60. https://www.nw.de/lokal/bielefeld/mitte/23661084_Mobiel-nach-dem-Cyberangriff-Displays-konnten-Pendlern-keine-korrekten-Zeiten-anzeigen.html; https://www.radiobielefeld.de/nachrichten/lokalnachrichten/detailansicht/cyberangriff-bei-mobiel-partner-keine-aktuellen-fahrplan-anzeigen-in-bielefeld.html
61. https://therecord.media/knp-logistics-ransomware-insolvency-uk
62. https://restoreprivacy.com/threat-actor-claims-data-breach-on-american-moving-firm-u-haul/
63. https://thecyberexpress.com/cyberattack-on-bmw-munique-motors/
64. https://www.bleepingcomputer.com/news/security/auto-parts-giant-autozone-warns-of-moveit-data-breach/
65. https://www.bleepingcomputer.com/news/security/qilin-ransomware-claims-attack-on-automotive-giant-yanfeng/
66. https://www.seattletimes.com/seattle-news/transportation/cyberattack-shuts-down-wa-transportation-website-causing-havoc-for-ferry-passengers-others/
67. https://cyberscoop.com/fleet-management-vulnerability-digitial-communications-technologies/
68. https://www.bleepingcomputer.com/news/security/nissan-is-investigating-cyberattack-and-potential-data-breach/amp/
69. https://www.bleepingcomputer.com/news/security/orbcomm-ransomware-attack-causes-trucking-fleet-management-outage/
70. https://www.bleepingcomputer.com/news/security/orbcomm-ransomware-attack-causes-trucking-fleet-management-outage/
71. https://hackaday.com/2023/06/08/hacking-a-hyundai-ioniqs-infotainment-system-again-after-security-fixes/
72. https://hackaday.com/2023/06/08/hacking-a-hyundai-ioniqs-infotainment-system-again-after-security-fixes/
73. https://cyberscoop.com/fleet-management-vulnerability-digitial-communications-technologies/
74. https://www.cvedetails.com/cvss-score-distribution.php
75. https://nvd.nist.gov/vuln-metrics/cvss
76. https://www.wjhl.com/business/press-releases/globenewswire/8856072/haynes-international-announces-network-outage/
77. https://www.globenewswire.com/en/news-release/2023/07/19/2707585/9124/en/Haynes-International-Provides-Cybersecurity-Update-and-Estimated-Third-Quarter-Financial-Impact.html
78. https://www.kendrion.com/en/news-events/news/news-detail/kendrion-experiences-cyber-security-incident
79. https://www.autoevolution.com/news/new-electrify-america-charger-gets-hacked-displays-tesla-s-supercharging-network-209367.html
80. https://twitter.com/MichaelMuni/status/1617272328626360321
81. https://c2a-sec.com/a-case-study-on-the-importance-of-security-validation-done-right-abb-chargersync-platform/
82. https://c2a-sec.com/a-case-study-on-the-importance-of-security-validation-done-right-abb-chargersync-platform/
83. https://nvd.nist.gov/vuln/detail/CVE-2023-29857
84. https://nvd.nist.gov/vuln/detail/CVE-2023-29857
85. https://therecord.media/orbcomm-trucking-software-ransomware
86. https://www.bleepingcomputer.com/news/security/orbcomm-ransomware-attack-causes-trucking-fleet-management-outage/

REFERENCES

87. https://www.rmf24.pl/regiony/olsztyn/news-atak-hakerski-sparalizowal-olsztyn-ustalenia-rmf-fm,nId,6866990#crp_state=1; https://cyberdefence24.pl/cyberbezpieczenstwo/atak-hakerski-w-olsztynie-sparalizowal-miasto
88. https://www.reuters.com/business/autos-transportation/california-suspends-gm-cruises-driverless-autonomous-vehicle-permits-2023-10-24/
89. https://www.reuters.com/business/autos-transportation/gms-cruise-recall-950-driverless-cars-after-accident-involving-pedestrian-2023-11-08/
90. https://www.axios.com/2023/11/27/self-driving-cars-robotaxis-trust
91. https://waymo.com/blog/2023/07/doubling-down-on-waymo-one.html
92. https://www.axios.com/2023/08/07/dallas-autonomous-trucks
93. https://waymo.com/blog/2023/10/the-waymo-driver-now-available-on-uber.html
94. https://www.prnewswire.com/news-releases/may-mobility-announces-105-million-series-d-investment-round-led-by-ntt-to-scale-autonomous-transit-services-301979363.html
95. https://www.hyundai.com/worldwide/en/company/newsroom/detail/motional-ioniq-5-robotaxi-to-be-manufactured-at-new-hyundai-motor-group-innovation-center-singapore-0000000360
96. https://asia.nikkei.com/Business/Technology/Japan-to-assign-bandwidth-for-Level-4-self-driving-vehicles
97. https://drivingpress.com/the-risks-of-autonomous-vehicles/
98. https://apnews.com/article/colorado-right-to-repair-farming-equipment-1da00ea957fd1057bf522cb4725e62d4
99. https://www.fb.org/news-release/farm-bureau-continues-to-advance-farmers-right-to-repair
100. https://www.reuters.com/legal/litigation/deere-must-face-us-farmers-right-to-repair-lawsuits-judge-rules-2023-11-27/
101. https://www.vice.com/en/article/m7bbkv/biden-administration-tells-car-companies-to-ignore-right-to-repair-law-people-overwhelmingly-voted-for
102. https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-3028
103. https://nvd.nist.gov/vuln/detail/CVE-2023-3028
104. https://nvd.nist.gov/vuln/detail/CVE-2022-38766
105. https://news.stv.tv/west-central/surge-in-keyless-car-thefts-sees-28-vehicles-stolen-in-glasgow-in-january-2023
106. https://www.suffolk.police.uk/news/latest-news/vehicle-owners-urged-be-vigilant-following-number-thefts
107. https://kitchener.ctvnews.ca/police-say-relay-and-reprogramming-thefts-are-on-the-rise-in-waterloo-region-here-are-the-most-targeted-vehicles-1.6308378
108. https://www.worcesternews.co.uk/news/23493583.keyless-theft-land-rovers-rise-warn-police/
109. https://www.infranken.de/lk/forchheim/blaulicht/heroldsbach-erneuter-autodiebstahl-wegen-keyless-go-funktion-taeter-stoeren-schluessel-signal-art-5691576
110. https://www.telegraph.co.uk/news/2023/08/29/keyless-car-hacking-equipment-ban-to-cut-car-thefts/
111. https://nvd.nist.gov/vuln/detail/CVE-2023-29389, https://kentindell.github.io/2023/04/03/can-injection/
112. https://kentindell.github.io/2023/04/03/can-injection/
113. https://www.carscoops.com/2023/02/toyota-rav4-prime-ecu-software-could-shut-down-the-hybrid-system/
114. https://hackaday.com/2023/11/22/keeping-a-mazdas-radio-on-after-the-engine-shuts-off/
115. https://samcurry.net/web-hackers-vs-the-auto-industry/
116. https://eaton-works.com/2023/03/06/toyota-c360-hack/
117. https://c2a-sec.com/a-case-study-on-the-importance-of-security-validation-done-right-abb-chargersync-platform/
118. https://nvd.nist.gov/vuln/detail/CVE-2023-6073
119. https://nvd.nist.gov/vuln/detail/CVE-2023-6073
120. https://nvd.nist.gov/vuln/detail/CVE-2023-22388
121. https://nvd.nist.gov/vuln/detail/CVE-2023-22388
122. https://nvd.nist.gov/vuln/detail/CVE-2023-29857
123. https://nvd.nist.gov/vuln/detail/CVE-2023-29857
124. https://www.latestly.com/socially/world/bykea-app-hacked-pakistans-ride-hailing-application-gets-hacked-users-receive-abusive-messages-see-pics-5197926.html
125. \https://juniperspring.xyz/posts/honda-reverse-engineering/
126. https://www.blackhat.com/us-23/briefings/schedule/index.html#jailbreaking-an-electric-vehicle-in--or-what-it-means-to-hotwire-teslas-x-based-seat-heater-33049 , https://www.darkreading.com/application-security/tesla-jailbreak-unlocks-theft-in-car-paid-features
127. https://www.autoevolution.com/news/new-electrify-america-charger-gets-hacked-displays-tesla-s-supercharging-network-209367.html
128. https://twitter.com/MichaelMuni/status/1617272328626360321
129. https://www.globalvillagespace.com/tech/shell-recharge-data-breach-exposes-ev-drivers-information/

REFERENCES

130. https://insideevs.com/news/659185/tesla-model-3-compromised-in-under-two-minutes-at-hacking-contest/
131. https://insideevs.com/news/659185/tesla-model-3-compromised-in-under-two-minutes-at-hacking-contest/
132. https://techcrunch.com/2023/11/14/a-software-update-bricked-rivian-infotainment-systems/
133. https://en.wikipedia.org/wiki/Cellular_V2X
134. https://gttwireless.com/dsrc-vs-c-v2x-comparing-the-connected-vehicles-technologies/
135. https://www.dwt.com/blogs/broadband-advisor/2023/05/fcc-connected-vehicles-c-v2x
136. https://www.leewayhertz.com/generative-ai-in-automotive-industry/
137. https://hbr.org/2023/11/navigating-the-new-risks-and-regulatory-challenges-of-genai
138. https://www.thebanker.com/The-world-s-first-GenAI-guidelines-for-banks-1702900543
139. https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai
140. https://techcrunch.com/2023/12/13/china-autonomous-vehicle-driving-regulation/ , https://xxgk.mot.gov.cn/2020/jigou/ysfws/202312/t20231205_3962490.html
141. https://www.miit.gov.cn/jgsj/zbys/qcgy/art/2023/art_439d600cba254bd5b426d4dadc6d82b5.html; https://unece.org/sites/default/files/2021-03/R155e.pdf; https://en.wikipedia.org/wiki/World_Forum_for_Harmonization_of_Vehicle_Regulations
142. https://www.gov.cn/zhengce/zhengceku/202306/content_6887168.htm
143. https://www.marklines.com/en/report/rep2457_202303
144. https://theicct.org/pv-india-rde-testing-apr23/
145. https://www.cybersecurity-insiders.com/india-to-make-cybershield-mandatory-for-vehicles/; https://timesofindia.indiatimes.com/business/dontgetscammed/news/cybershield-mandate-for-vehicles-govt-takes-preemptive-action-against-cyber-threats-to-cars-trucks/articleshow/105208966.cms
146. https://www.jdsupra.com/legalnews/california-takes-the-wheel-a-closer-9580097/
147. https://unece.org/sites/default/files/2021-03/R155e.pdf
148. https://unece.org/sites/default/files/2021-03/R156e.pdf
149. https://www.linkedin.com/pulse/automotive-cybersecurity-2023-horizontal-europe-sight-tschersich-hesre/?utm_source=share&utm_medium=member_ios&utm_campaign=share_via
150. https://www.iso.org/standard/70918.html
151. https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf
152. https://www.enisa.europa.eu/publications/smart-cars, https://www.enisa.europa.eu/publications/recommendations-for-the-security-of-cam/
153. https://automotiveisac.com/best-practices
154. https://unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf
155. https://unece.org/fileadmin/DAM/trans/doc/2020/wp29/ECE-TRANS-WP29-2020-080e.pdf
156. https://clepa.eu/mediaroom/clepa-and-acea-join-with-auto-isac-on-motor-vehicle-cybersecurity/
157. https://unece.org/sites/default/files/2023-07/ECE-TRANS-WP.29-GRVA-16e.pdf
158. https://www.linkedin.com/pulse/automotive-cybersecurity-2023-horizontal-europe-sight-tschersich-hesre/?utm_source=share&utm_medium=member_ios&utm_campaign=share_via
159. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act#:~:text=Less%20apparent%20to%20many%20users,software%20with%20a%20digital%20component
160. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet
161. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet
162. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32019R2144
163. https://www.linkedin.com/pulse/automotive-cybersecurity-2023-horizontal-europe-sight-tschersich-hesre/?utm_source=share&utm_medium=member_ios&utm_campaign=share_via
164. https://www.iso.org/standard/69113.html
165. https://www.switch-ev.com/blog/what-is-iso-15118
166. https://www.switch-ev.com/blog/basics-of-plug-and-charge
167. https://www.sec.gov/news/press-release/2023-139
168. https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214
169. https://www.sec.gov/education/smallbusiness/goingpublic/SRC
170. https://www.databreaches.net/alphv-files-an-sec-complaint-against-meridianlink-for-not-disclosing-a-breach-to-the-sec/
171. https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf

REFERENCES

172. https://www.govinfo.gov/content/pkg/FR-2022-09-09/pdf/2022-19507.pdf
173. https://upstream.auto/research/automotive-cybersecurity/
174. https://automotiveisac.com/press-news/auto-isac-partners-with-upstream-security-to-enhance-automotive-threat-landscape-visibility
175. https://www.telematicswire.net/asrg-partners-with-upstream-to-enhance-automotive-cyber-threat-intelligence/
176. https://www.nhtsa.gov/laws-regulations/standing-general-order-crash-reporting
177. https://www.nhtsa.gov/speeches-presentations/automated-road-transportation-symposium-arts23-keynote-address
178. https://www.vice.com/en/article/m7bbkv/biden-administration-tells-car-companies-to-ignore-right-to-repair-law-people-overwhelmingly-voted-for
179. https://www.nhtsa.gov/press-releases/nhtsa-proposes-seat-belt-warning-system-expansion
180. https://www.nhtsa.gov/sites/nhtsa.gov/files/2023-09/NTSB-Response_September-2023_Speeding_Rear-Impact-Guards_ADB-Headlamps-v2.pdf
181. https://www.iea.org/reports/global-ev-outlook-2023/executive-summary
182. https://www.progressive.com/lifelanes/on-the-road/future-of-electric-cars
183. https://www.federalregister.gov/documents/2023/02/28/2023-03500/national-electric-vehicle-infrastructure-standards-and-requirements
184. https://www.foley.com/insights/publications/2023/04/us-dot-finalizes-ev-charging-infrastructure-rules/
185. https://www.nccoe.nist.gov/projects/cybersecurity-framework-profile-electric-vehicle-extreme-fast-charging-infrastructure
186. https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8473.ipd.pdf
187. https://www.nemko.com/blog/cybersecurity-requirements-ce-marking-postponed-till-1-august-2025
188. https://data.consilium.europa.eu/doc/document/ST-12041-2023-INIT/en/pdf
189. https://www.consilium.europa.eu/media/69093/st16996-en23.pdf
190. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
191. https://www.electrive.com/2021/04/21/partners-pledge-to-implement-plugcharge-across-europe/
192. https://www.charin.global/technology/plug-charge
193. https://www.gov.uk/government/consultations/electric-vehicle-smart-charging/public-feedback/electric-vehicle-smart-charging-consultation-summary-of-responses
194. https://www.legislation.gov.uk/uksi/2021/1467/made
195. https://www.legislation.gov.uk/uksi/2021/1467/made
196. https://assets.publishing.service.gov.uk/media/628ce214e90e071f653a494a/Guide-to-evscp-regulations-2021-V2.1.pdf
197. https://www.meti.go.jp/press/2020/11/20201105003/20201105003-1.pdf , https://www.dataguidance.com/news/japan-meti-releases-iot-security-and-safety-framework
198. https://www.dataguidance.com/news/japan-mic-announces-publication-iot-5g-security , https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00036.html
199. https://www.switch-ev.com/blog/what-is-iso-15118
200. https://en.wikipedia.org/wiki/Combined_Charging_System
201. https://www.switch-ev.com/blog/basics-of-plug-and-charge
202. https://www.charin.global/technology/iso15118/
203. https://www.cinch.co.uk/guides/electric-cars/what-is-chademo-ev-charging
204. https://www.chademo.com/design-guideline-for-external-charging-updated
205. https://www.openchargealliance.org/protocols/ocpp-201/
206. https://www.linkedin.com/pulse/how-does-ocpp-201-iso-11518-work-together-why-do-matter-beckmann/
207. https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf
208. https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/
209. https://www.nhtsa.gov/technology-innovation/vehicle-data-privacy
210. https://www.forbes.com/sites/stevetengler/2022/05/17/privacy-battle-over-connected-cars-takes-an-interesting-turn-in-california/
211. https://europe.autonews.com/guest-columnist/connected-cars-evolving-eu-regulatory-landscape
212. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3491, https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai
213. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113
214. https://www.consilium.europa.eu/en/press/press-releases/2023/11/27/data-act-council-adopts-new-law-on-fair-access-to-and-use-of-data/
215. https://www.dentons.com/en/insights/articles/2023/december/14/the-new-eu-ai-act-the-10-key-things-you-need-to-know-now
216. https://www.cyberghostvpn.com/en_US/privacyhub/dark-web-vs-deep-web/
217. https://www.cyberghostvpn.com/en_US/privacyhub/dark-web-vs-deep-web/

REFERENCES

218. For more details, see Chapter 1
219. https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html
220. https://en.wikipedia.org/wiki/Darknet_market
221. https://xakcop.com/post/hyundai-hack-2/
222. https://infosecwriteups.com/how-i-hacked-1000-tesla-cars-using-osint-4cd837b8c530; https://www.ctfiot.com/142013.html
223. https://www.nhtsa.gov/equipment/odometer-fraud
224. https://voonze.com/tsmc-supplier-suffers-ransomware-attack-and-has-data-leaked-by-hacker-group/
225. https://www.kendrion.com/en/news-events/news/news-detail/kendrion-experiences-cyber-security-incident
226. https://thecyberexpress.com/qilin-leaks-data-from-the-tesm-cyber-attack/
227. https://therecord.media/orbcomm-trucking-software-ransomware
228. https://therecord.media/knp-logistics-ransomware-insolvency-uk
229. https://www.gartner.com/en/documents/3904768
230. https://owasp.org/API-Security/editions/2023/en/0x11-t10/

ABOUT UPSTREAM

Upstream Security offers a cloud-based automotive cybersecurity and data management 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:

Upstream