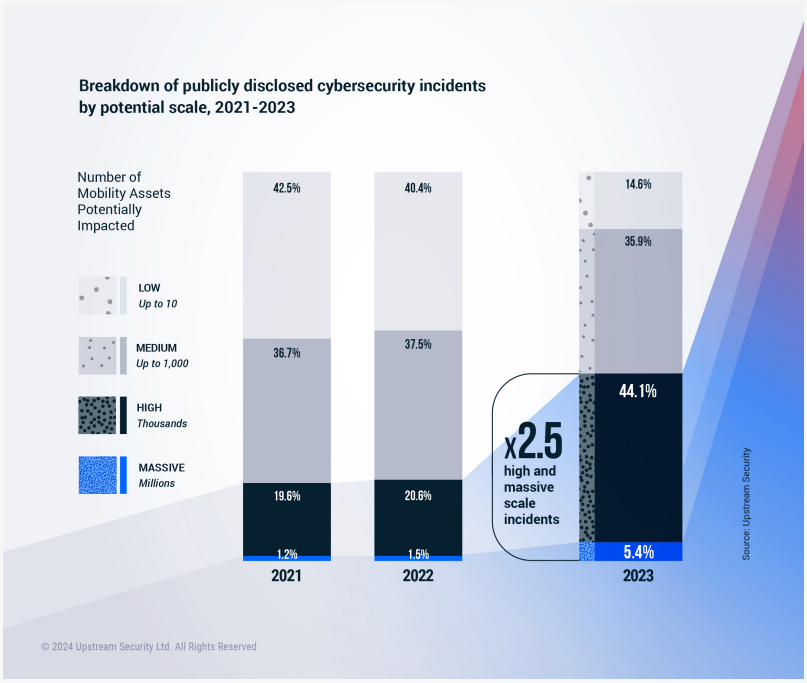
# Upstream’s New 2024 Automotive Cybersecurity Report is officially released

*Latest insights show that high-scale cyber incidents doubled in 2023, with attacks growing in sophistication and magnitude*



Cybersecurity incidents by their potential scale

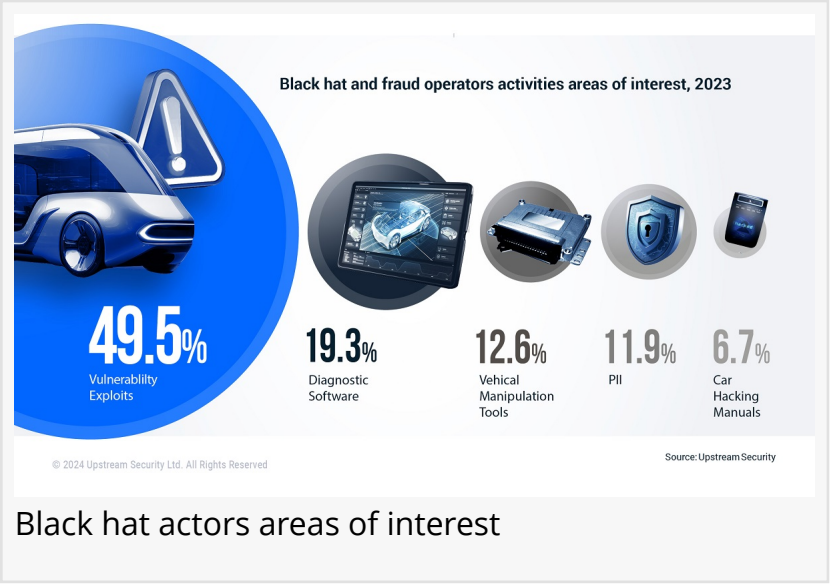
ANN ARBOR, MICHIGAN, UNITED STATES, February 7, 2024 /EINPresswire.com/ -- Upstream Security, the leading provider of the cybersecurity detection and response platform for the automotive industry, today released the 2024 Upstream Global Automotive Cybersecurity Report. This sixth edition of the report puts a spotlight on how automotive and mobility cyber threats have evolved and grown in magnitude and impact - from experimental hacks to massive-scale attacks.

> Cyber incidents have grown in sophistication and reach. Findings from Upstream's report highlight why it’s more crucial than ever to proactively safeguard vehicles against automotive cyber attacks.
>
> *Yoav Levy, Upstream Security CEO and Co-Founder*

Report key insights and findings:

-In 2023, the number of high and massive-scale incidents potentially impacting thousands to millions of mobility assets increased by x2.5 compared to 2022
-95% of attacks are executed remotely, and 85% of them are long-range
-64% of cyber-attacks are performed by black hat actors
-In 2023, deep and dark web activities related to the Automotive and Smart Mobility ecosystem have increased by 165%
-Nearly 65% of deep and dark web cyber activities had the potential to impact thousands to millions of mobility assets

-Attacks on telematic and application servers account for 43% of all attacks (up from 35% in 2022)
-37% of threat actors actions had far-reaching impact - targeting multiple OEMs simultaneously (as opposed to impacting just a single OEM/auto manufacturer)
-Attacks on infotainment systems have almost doubled in 2023 - accounting for 15% of all attacks (up from 8% in 2022)
-APIs are especially susceptible to Generative AI threats  since attackers can use GenAI to explore API documentation



Black hat actors areas of interest

Yoav Levy, Upstream Security CEO and Co-Founder: “Automotive cybersecurity is reaching an inflection point. Cyber incidents have grown significantly in sophistication and reach, threatening safety, sensitive data, and carrying operational significant implications. With threat actor motivation shifting towards high and massive-scale impact on connected vehicles and mobility assets, the findings from Upstream’s new 2024 Automotive Cybersecurity Report highlight why today it’s more crucial than ever to proactively safeguard vehicles, mobility applications and IoT devices against automotive cyber threats.”

Upstream’s report is the culmination of months of research and analysis by Upstream’s  cyber research teams. Upstream experts investigated nearly 1500 reported automotive cybersecurity incidents over the last decade, 295 reported in 2023 alone, and monitored hundreds of deep and dark web forums, marketplaces and malicious ‘chatter’ to compile the comprehensive report.

This year’s report also provides eye-opening insights on the financial impact of cyber attacks, providing an actionable framework for measuring the monetary impact of cyber attacks in real-world scenarios.

Upstream’s Predictions for 2024
Looking ahead to 2024, the Upstream report also provides predictions on projected shifts in the automotive threat landscape:

-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.
-GenAI 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.

-OEMs and Charging Point Operators (CPOs) continue to deepen cybersecurity risk assessments, and deploy cybersecurity solutions to protect strategic EV charging infrastructure
-Initial signs of regulatory fatigue, amid the maturity of UNECE WP.29 R155 and the abundance of new regulations emerging worldwide, mainly in China.

Levy concluded: “There’s a growing understanding amongst cybersecurity stakeholders charged with securing connected vehicle fleets, EV charging stations and infrastructure, IoT devices and mobility services that they need to significantly bolster their cybersecurity defenses to protect against massive scale attacks. This is especially true with GenAI’s growing prevalence and its role in lowering threat actors’ barriers for entry, and enabling black hat actors to perpetrate large-scale attacks faster and more effectively than previously possible.”

Click here to download the 2024 Upstream Global Automotive Cybersecurity Report

About Upstream Security
Upstream provides a cloud-based data management platform purpose-built for connected vehicles, delivering unparalleled automotive cybersecurity detection and response (V-XDR) and data-driven applications. The Upstream Platform unlocks the value of vehicle data, empowering customers to build connected vehicle applications by transforming highly distributed vehicle data into centralized, structured, contextualized data lakes. Coupled with AutoThreat Intelligence, the first automotive cybersecurity threat intelligence solution, Upstream provides industry-leading cyber threat protection and actionable insights, seamlessly integrated into the customer’s environment and vehicle security operations centers (vSOC).
For more information go to upstream.auto.
Media Contact: media@upstream.auto

Scott Fosgard
Upstream Security
+1 734-272-7440
email us here
Visit us on social media:
Twitter
LinkedIn

---