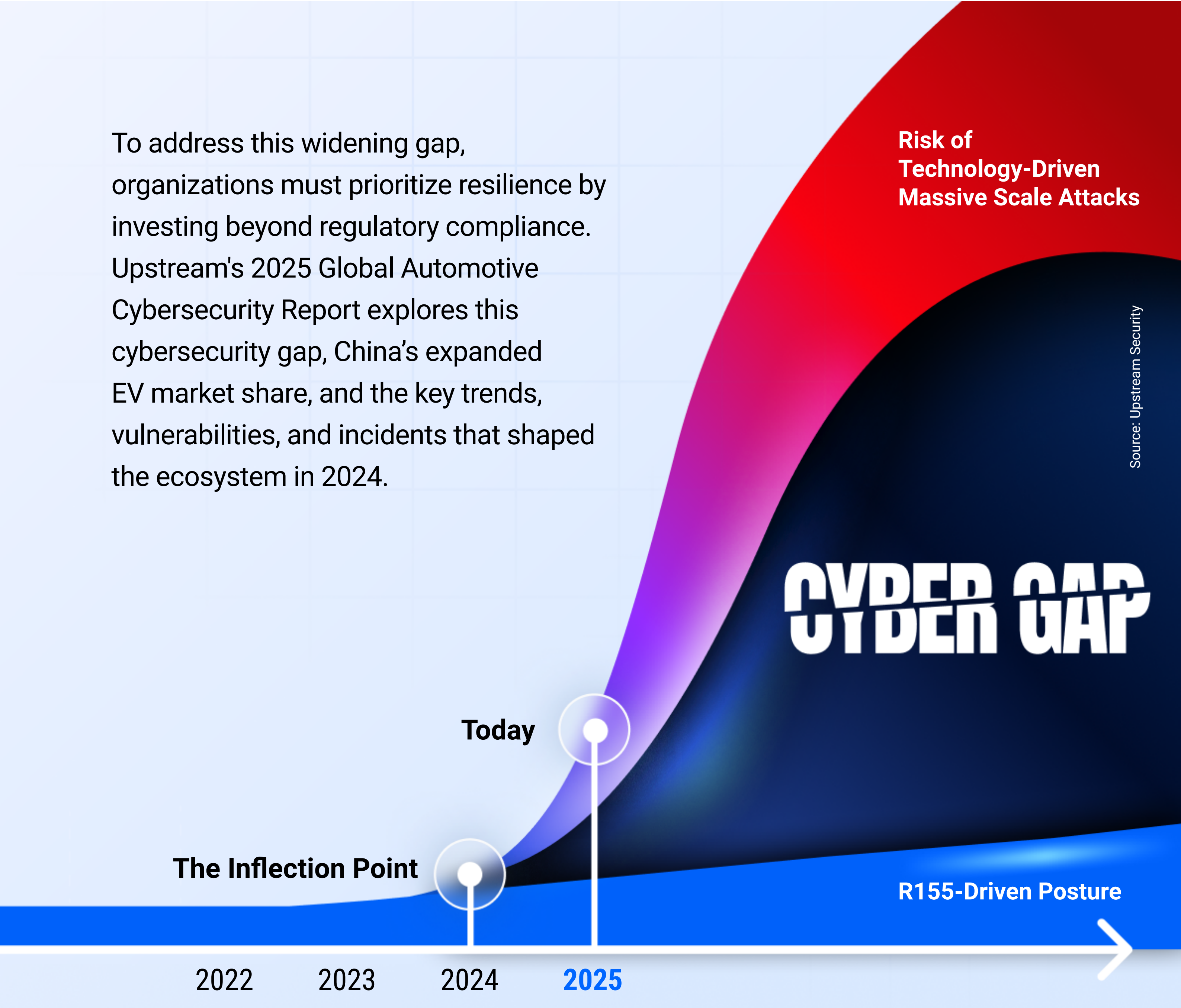
2025 | Automotive & Smart Mobility Global Cybersecurity Report

MIND THE CYBER GAP

Bridging the Cybersecurity Gap in Automotive & Smart Mobility

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

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



Source: Upstream Security

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

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

OVER 60%

of all incidents

Massive scale incidents more than tripled, accounting for

19%

of all incidents

92% of attacks were remote

65% of attacks were executed by black hat actors

Source: Upstream Security

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

70%

of black hat activities had a high-massive impact

OVER 76%

targeted multiple stakeholders and global reach

Source: Upstream Security

China is reshaping global Automotive markets and the cybersecurity landscape

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

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