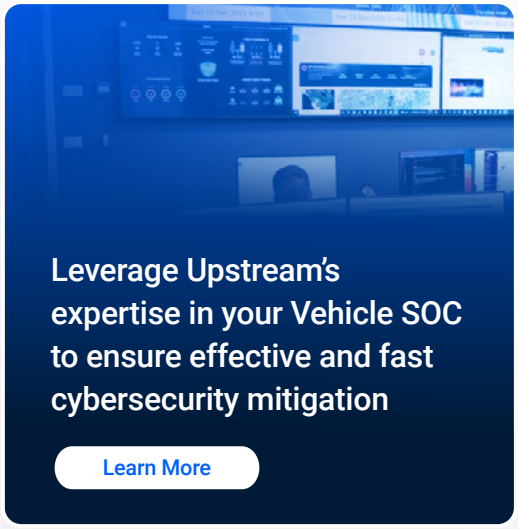
Upstream vSOC

The Leading Managed Vehicle SOC: Actively Protecting Millions of Vehicles for OEMs Worldwide

The IT Security Operations Center (SOC), which started as a means to adhere to compliance requirements, has evolved into a proactive, agile, cross-functional effort that can address the converged IT, OT, IoT, fraud, and cybersecurity risks.
Managing multiple converging data sources and risks required by an increasingly connected automotive industry moves the vSOC (Vehicle SOC) along a similar route. But, unlike traditional SOCs, where the focus was on compliance and IT assets, for vSOCs to achieve success, they need to monitor a growing number of data sources and build cross-functional response capabilities to mitigate threats.



Leverage Upstream's expertise in your Vehicle SOC to ensure effective and fast cybersecurity mitigation

Learn More

Upstream's Holistic VSOC Approach Contextualizes Connected Vehicle Data to Effectively and Rapidly Mitigate Cybersecurity Threats

Based on Upstream's cloud-based cybersecurity solution, Upstream's vSOC service leverages deep and advanced detection capabilities from the single ECU, to the individual vehicle and the entire fleet's perspective enabling the vSOC team to effectively mitigate known and unknown threats and attacks. This holistic view allows OEMs to mitigate cybersecurity risks against vehicles, services, and entire fleets.
Integrating organically with existing processes and workflows, Upstream's vSOC requires minimal ramp-up time. The team includes experienced analysts and researchers and offers a **unique perspective and understanding of the automotive ecosystem.** Coupled with deep expertise in cybersecurity, fraud, and operations, making for a multidisciplinary vSOC.

The service utilizes a robust technology stack and leverages Upstream's extensive experience of monitoring millions of vehicles of various global OEMs, established methodologies, and battle-tested tools, ensuring the highest possible impact on the organization. In addition, Upstream's vSOC service works closely with our MSSP partners to protect vehicles across the globe.

Employ a Designated Team with Purpose-Built Methodologies

Automotive Focused
Address automotive-specific malicious and fraudulent threats with advanced detection, investigation, and response methodologies built using the insights gained from the Upstream platform's contextual understanding of vehicles and fleets, along with our deep understanding of the regulations applying to the automotive industry.

Cybersecurity Expertise
Access a team of cybersecurity researchers and data analytics experts with a broad, worldwide know-how of the automotive industry's threat vectors, from close-range attacks utilizing keyfobs or OBDs and remote attempts to manipulate consumer applications or infotainment units, to name a few.

Fast Time-to-Security
Utilize a fully operational vSOC service that is ready to deploy applying tried and true methodologies for threat detection and response, with the ability to expand coverage across geographies and scale up as needed.

Custom Built Playbooks
Gain playbooks and methodologies built for your needs that draw on the Upstream vSOC team's experience from multiple OEMs and knowledge as resources to guide your cybersecurity success continuously.

BOT Model Eliminates Lock-In
All mitigation and response methodologies are built for your operation. To ensure optimal flexibility and eliminate lock-in, you can leverage a robust and proven build-operate-transfer (BOT) model. Upstream's vSOC service trains OEM teams on implemented models, methodologies and playbooks to ensure a smooth hand-over when needed.

Compliant & Secure
Run from a secure state-of-the-art facility, Upstream's vSOC 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.