AUTOThreat™
AUTOMOTIVE THREAT INTELLIGENCE

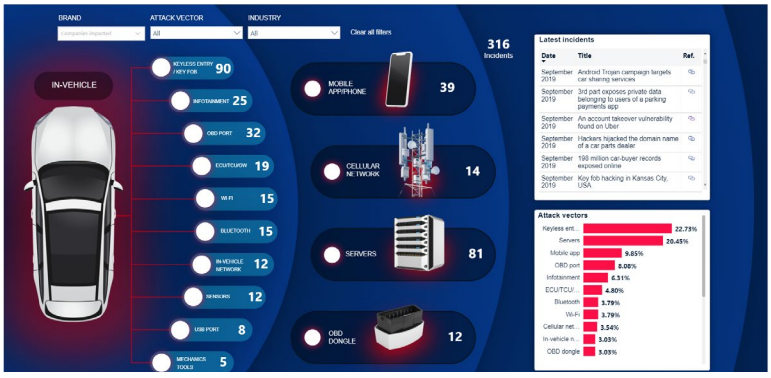
Upstream.auto
Securing Smart Mobility

THE FIRST AUTOMOTIVE THREAT INTELLIGENCE

Upstream's AutoThreat collects, analyzes, and disseminates threat intelligence specific to the automotive sector and tailored to Upstream's different customers, ranging from vehicle OEMs to connected fleets. AutoThreat helps organizations develop their own intelligence-led security operations with the unique nuances and understanding required of moving vehicle infrastructures.

PROTECTING AGAINST CONTINUOUSLY EVOLVING THREATS

Upstream's AutoThreat research team leverages intelligence from multiple internal and external sources in order to analyze vulnerabilities, automotive-oriented cyber-attacks, and threats, as well as develop countermeasures to protect Upstream's customers. Upstream uses a variety of threat analysis tools in order to capture various threat indicators from public feeds and dark web activity. Vulnerabilities in specific popular automotive components and vehicles are uncovered and combined with threat metadata gleaned from connected vehicle data feeds. Threats are then analyzed and assessed in light of a growing library of automotive components in order to distill potential impacts across a variety of vehicles.



HOW IT WORKS

Upstream's AutoThreat Intelligence works together with Upstream's C4 cloud-based cybersecurity detection and incident event management platform (SIEM), constantly collecting and analyzing data in the background, while also providing users with an accessible portal to view visual reports, trends, and more.

Accessible User-Friendly Portal

By logging into the AutoThreat portal, organizations can get a visual representation of automotive cyber threats, allowing them to take action by enhancing their security defenses and visibility in a landscape unique to their connected vehicle environments.

Fully Integrated Threat Intelligence

AutoThreat Intelligence is used in the creation of Upstream C4 correlation rules or behavioral analysis models to indicate added risk of automotive components and vehicle assets. Upstream C4 automatically leverages threat insights to drive new policies and signatures without requiring the team to install apps, write scripts, or alter workflows. New security capabilities are added with no additional cost or impact to the user. The result is that Upstream C4 deployment is constantly kept up-to-date with the threat intelligence feed integrated directly into the C4 platform. The combined solution enables users to quickly identify and mitigate new and emerging attacks.

COMPREHENSIVE AUTOMOTIVE THREAT FEED

AUTOMOTIVE THREAT REPORTS

- Black hat vs. white hat
- Remote hacks vs. local hacks
- Attack Vectors Targeting Connected Cars

AUTOMOTIVE CYBER ATTACK VECTORS

- How are hackers getting in
- Most common automotive attack vectors

VEHICLE COMPONENT AND DEVICE VULNERABILITIES

- Documented vulnerabilities at the vehicle, component and infrastructure level
- ECU and vulnerability mapping correlated to vehicle models

Contact Upstream to request access to the AutoThreat Intelligence Portal at hello@upstream.auto

www.upstream.auto