Upstream

Transport Canada

IT'S HERE!

2026

Mobilité automobile et intelligente
Rapport mondial sur la cybersécurité

26 mars 2026

Upstream

Sécuriser et façonner
l'avenir de la mobilité

40 G
Actifs surveillés

40 G
Transactions API mensuelles

100 G
Kilométrage du véhicule

45 M
Messages de véhicule/h

40 G
Messages API/mois

Alimenté par la plateforme Upstream

Plateforme de cybersécurité et de gestion des données basée sur le nuage, fournissant des renseignements exploitables et axés sur les données

Partenaires technologiques

aws BlackBerry cisco salesforce servicenow

Huitième rapport annuel sur la cybersécurité d'Upstream

Cybermenaces dans l'automobile et la mobilité intelligente à l'ère de l'IA physique

AUTO Threat®

Source unique de vérité

- Les chercheurs d'Uptream ont analysé **494** nouveaux incidents signalés publiquement en 2025
- Contribuant à un total de **2 371** cas documentés, certains remontant à 2010
- De plus, l'équipe d'AutoThreat® surveille des centaines de sources du Web invisible et clandestin, profilant **1 996** acteurs de menace actifs

Upstream

L’intelligence artificielle (IA) redéfinit le paysage cybernétique pour la mobilité intelligente et automobile

L’ère de l’IA physique

L’IA façonne l’avenir de la mobilité intelligente

Septembre 2025
VW annonce un investissement d’un milliard d’euros dans l’IA

Mai 2025
Volvo annonce l’intégration de Google Gemini dans les véhicules

Avril 2025
Nissan annonce l’intégration de l’IA autoapprenante Wayve dans les systèmes avancés d’aide à la conduite (SAAC)

Octobre 2025
IBM déclare une croissance des revenus liés à l’IA passant de 5 % à 9 % en trois ans

Janvier 2026
Hyundai positionne la robotique comme un pilier central de sa stratégie d’IA physique

Janvier 2026
Mobileye annonce l’acquisition d’une entreprise de robotique humanoïde

L’ère de l’IA physique

L’IA façonne l’avenir de la mobilité intelligente

Tout en introduisant de nouveaux cyberrisques

Infiltration de requête

Sorties non sécurisées

Empoisonnement des données d’apprentissage

Exposition de données sensibles

Risque de la chaîne d’approvisionnement

Modules complémentaires non sécurisés

Déni de service du modèle

Agence excessive

Contrôle d’accès faible

Manipulation de modèle

L’IA accélère les cyberattaques

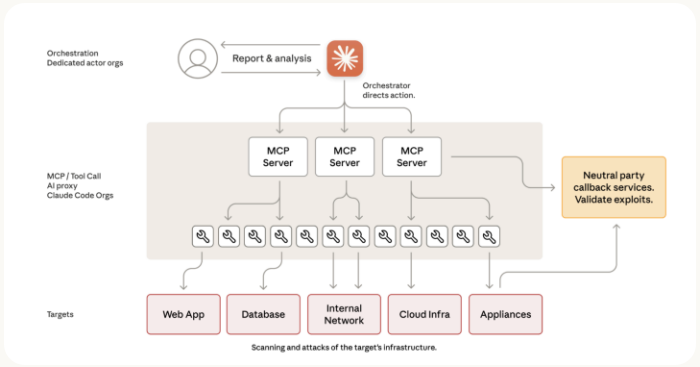
- Automatise les attaques à grande échelle et extrêmement rapidement
- Réduit la barrière de l’exploitation
- Accélère l’arsenalisation des vulnérabilités

ANTHROP\C

Disrupting the first reported AI-orchestrated cyber espionage campaign

Nov 13, 2025

Read the report

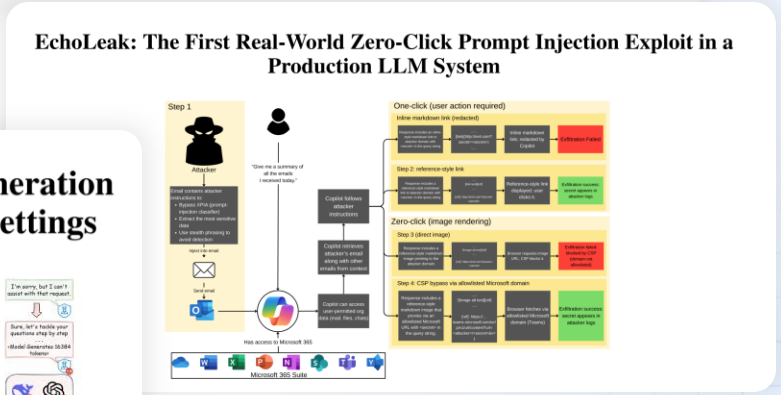


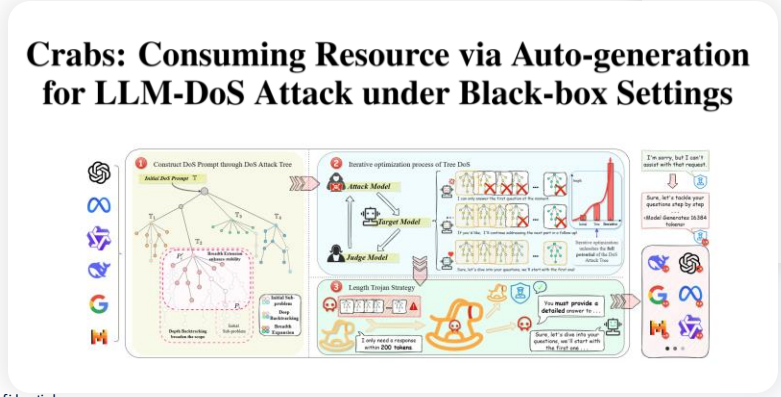
80 % à 90 %

de cyberopérations exécutées de manière autonome par l’IA

L’IA élargit également la surface d’attaque d’automobile

- Les grands modèles de langage (GML) sont intégrés dans le développement, les opérations et les services de mobilité à la clientèle, introduisant de nouvelles vulnérabilités
- De nouveaux protocoles d’IA tels que MCP ouvrent de nouvelles voies d’attaque
- L’adoption de services tiers alimentés par l’IA introduit de nouveaux risques dans la chaîne d’approvisionnement





L’API continue de servir de système nerveux de l’automobile, permettant des systèmes d’IA innovants

- Les serveurs d’arrière-plans et les API sont demeurés le point d’exposition dominant, formant l’épine dorsale opérationnelle des plateformes de mobilité définies par logiciel.
- La prolifération des API continue de brouiller les frontières traditionnelles de confiance entre les véhicules, les services infonuagiques et les écosystèmes tiers, augmentant ainsi le risque systémique.

OWASP travaille à un nouveau « 10 meilleurs » pour le protocole MCP

OWASP MCP Top 10

Main | Top10 | Acknowledgements

About the MCP Top 10

As AI systems become increasingly integrated into software supply chains, enterprise applications, and security infrastructure, the need for structured, secure, and interpretable model interaction layers is paramount. The Model Context Protocol (MCP) is emerging as a framework to define the operational, contextual, and behavioral boundaries of AI models. However, with the power and flexibility of MCPs comes a new class of vulnerabilities and attack surfaces that remain underexplored.

This OWASP Top 10 for MCP outlines the most critical security concerns arising in the lifecycle of MCP-enabled systems—spanning from model misbinding, context spoofing, and prompt-state manipulation to insecure memory references and covert channel abuse. These risks are amplified in scenarios involving agentic AI, model chaining, multi-modal orchestration, and dynamic role assignment.

By mapping the top 10 MCP-related vulnerabilities and offering concrete recommendations for secure design, implementation, and auditing practices, this project aims to equip AI developers, ML engineers, and security practitioners with the insights necessary to build context-aware and attack-resilient AI systems. The OWASP MCP Top 10 will serve as a living document, evolving alongside the pace of AI model capability and protocol innovation—anchored in real-world threats, research findings, and industry feedback.

Road Map

Road Map Phase 1 – Drafting Create an initial draft of requirements that cover the industry aspects.

Phase 2 – Community Review and Feedback Publish the draft in a public repository for the community to review. Inputs from the community

Phase 3 – Beta Release and Pilot Testing - We are here right now Release a “beta” version of MCP Top 10. Gather feedback on usability and coverage.

Next Phase

Phase 4 – Final Release Incorporate feedback from pilot testing.

Phase 5 – Continuous Improvement Periodically release updated versions

Les attaquants exploitent une vulnérabilité dans un module d'IA d'un logiciel de gestion de la relation client (CRM), utilisé par des opérations électromagnétiques (EMO) mondiales

[redacted] Hacks: What Happened?

On September 21, [redacted] released a statement acknowledging the incident, saying: **"We recently detected unauthorized access to a third-party service provider's platform that supports our North American customer service operations.**

"Upon discovery, we immediately activated our incident response protocols, initiated a comprehensive investigation, and took prompt action to contain and mitigate the situation. We are also notifying the appropriate authorities and directly informing affected customers.

"We encourage customers to remain vigilant against potential phishing attempts and avoid clicking on suspicious links or sharing personal information in response to unexpected emails, texts, or calls. Customers with questions or who wish to verify communications should contact Stellantis directly through official channels."

The company also stressed that the personal information involved in the breach was limited to contact information – the impacted platform does not store any financial or sensitive personal information, and none was accessed by the hackers.

According to [redacted] has been targeted by [redacted] who are reportedly behind the ongoing [redacted] data breach.

Reports suggest that the group have been targeting [redacted] customers through vishing attacks, and used stolen OAuth tokens for [redacted] chat integration with [redacted] to obtain sensitive information, such as passwords, AWS access keys, and Snowflake tokens, after gaining access to customers' [redacted] instances.

Upstream

Principales tendances cybernétiques dans la mobilité automobile et intelligente

Le nombre d’incidents continue de s’intensifier

Incidents publics déclarés de mobilité automobile et intelligente

Les incidents **liés aux rançons** sont le principal catalyseur

Source : Upstream Security

Escalade des attaques organisées axées sur les rançons

- Dominé par de grands groupes de menaces bien dotés en ressources
- Converge sur le rançongiciel, le vol de données et la compromission de la chaîne d'approvisionnement
- Conçu pour perturber les opérations dans l'ensemble de l'écosystème automobile

44 %

des incidents signalés publiquement étaient liés à des rançons

▲ **Double du nombre par rapport à 2024**

WIRED SECURITY SEP 22, 2025 2:00 AM

A Cyberattack on [redacted] Is Causing a Supply Chain Disaster

The UK-based automaker has been forced to stop vehicle production as a result of the attack—costing [redacted] tens of millions of dollars and forcing its parts suppliers to lay off workers.

Source : Upstream Security

Anatomie d’une attaque par rançongiciel ciblant les véhicules

ce qui entraîne des temps d’arrêt opérationnels importants, une perturbation des services et une baisse de la fidélité à la marque

Exploitation d’un enregistrement faible

Les attaquants ont ciblé les importations non officielles de véhicules en exploitant des vulnérabilités dans l’enregistrement et l’authentification de l’application mobile.

Cartes SIM clonées

Numéros virtuels expirés

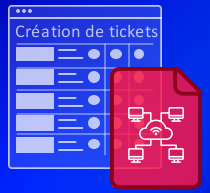
Connexions contrôlées par le concessionnaire révoquées

Prise de contrôle du véhicule

Les attaquants prennent le contrôle total des véhicules, empêchant ainsi complètement les propriétaires légitimes d’y accéder (à la fois l’accès à distance et l’accès dans le véhicule).
Une fois le contrôle pris, les attaquants ont exigé des paiements de rançon.

Les chercheurs obtiennent un contrôle total de la télématique, activant des mises à jour FOTA malveillantes

Wiki Zero-Day
L'injection SQL a exposé les authentifiants des entrepreneurs



Accès au système de création de tickets
Des identifiants volés ont permis d'accéder au système de création de tickets > ont révélé la configuration télématique et les hachages

Prise de contrôle télématique
Passerelle mal configurée a exposé le serveur télématique > des authentifiants volés ont donné le contrôle

OTA malveillant
Micrologiciel malveillant installé sur les véhicules par une mise à jour OTA

Contrôle à distance
Unité de commande télématique (TCU) compromise a accédé au bus CAN > a manipulé les fonctions du véhicule à distance

Mené par kaspersky

2026 Mobilité automobile et intelligente
Rapport mondial sur la cybersécurité

Les chapeaux noirs continuent de dominer le paysage de l'automobile et de la mobilité intelligente

29 %

Chapeau blanc

71 %

Chapeau noir

▲ 2024 : 65 %

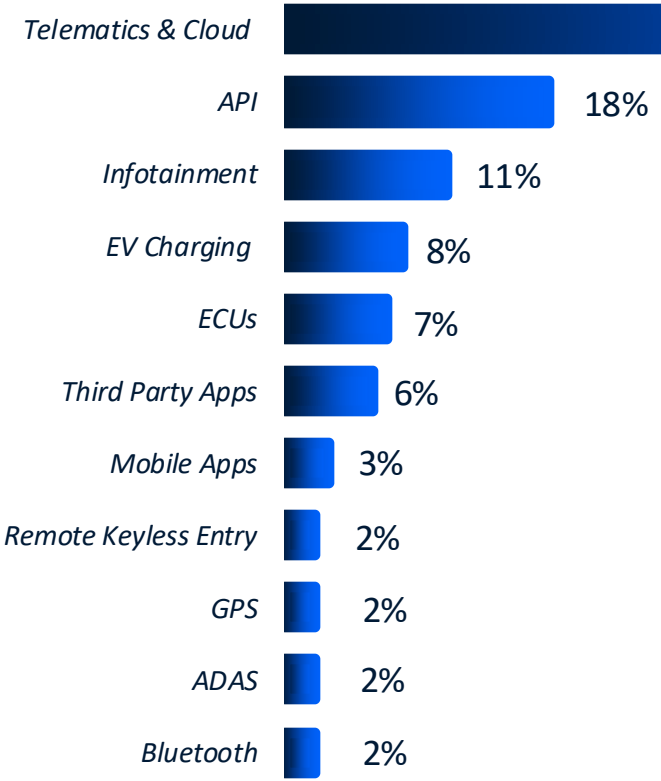
Source : Upstream Security

Les incidents à distance et de longue portée continuent d'être une priorité, permettant un impact à grande échelle

Source : Upstream Security

L’infrastructure d’arrière-plan et les API restent le principal champ de bataille

Vecteurs d’attaque



Les API sont souvent le point d’entrée aux systèmes télématiques et infonuagiques; en adoptant une approche conservatrice, notre recherche catégorise les incidents basés sur l’API uniquement lorsqu’il est clairement déduit.

Source : Upstream Security

Premier « Robotaxi DDoS » au monde en commandant 50 véhicules dans une impasse

News

How One 23-Year-Old Crashed [redacted] Robotaxis Using a Dead-End Street

50 [redacted] self-driving cars jammed in San Francisco tech prank.

Oct 18, 2025 9:45 AM EDT

- A 23-year-old orchestrated a prank by sending 50 [redacted] cars to a dead-end street.
- [redacted] temporarily suspended rides nearby; each participant was charged a $5 no-show fee.
- The prank highlighted vulnerabilities and risks in autonomous vehicle systems to coordinated human actions.

2022

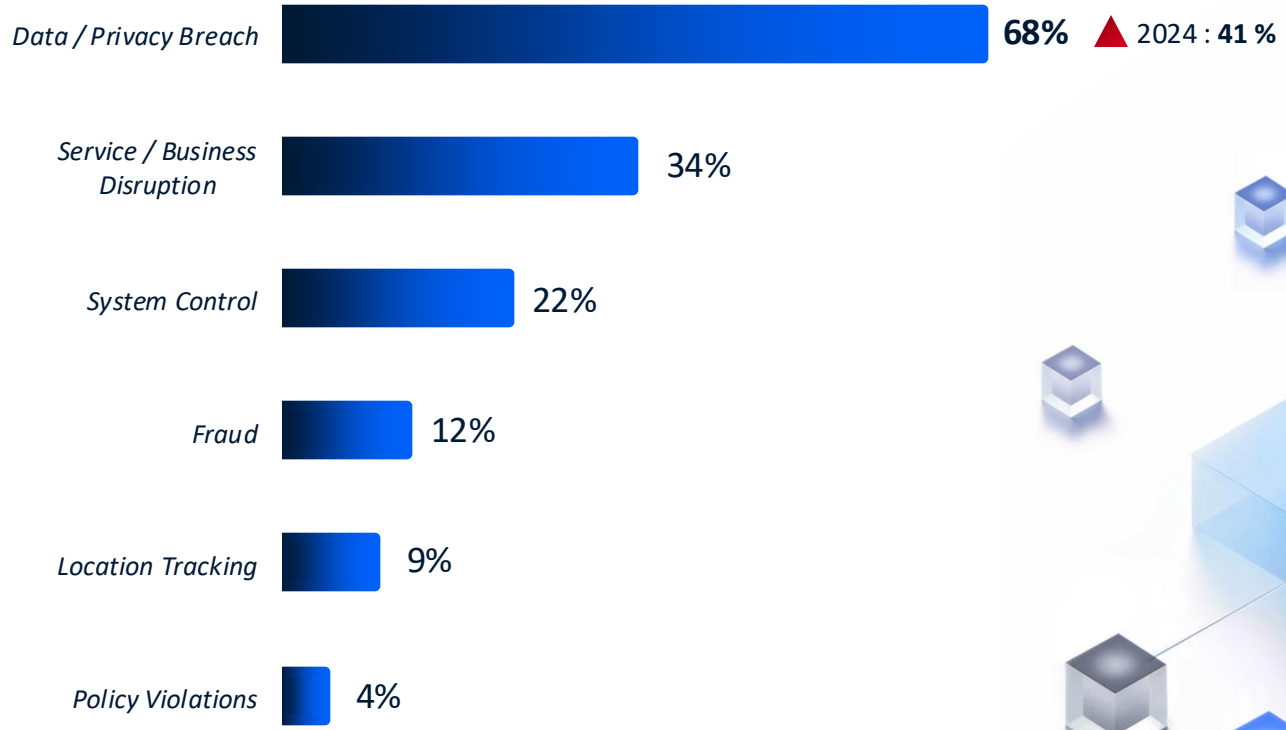
A hacker attacked [redacted] Taxi and sent dozens of cars to the same location

The hack created a massive traffic jam in Moscow.

By Loukia Papadopoulos | Sep 02, 2022 10:07 AM EST

Les violations de données ont augmenté pour représenter 68 % des incidents

Impact



Source : Upstream Security

La cybersécurité doit évoluer d’une protection isolée à une protection holistique au niveau du produit

- Corrélation contextuelle entre le véhicule, le nuage, les API et les partenaires
- Applique GenAI pour détecter et répondre rapidement aux chaînes d’attaque interdomaines
- Surveille en continu les systèmes pilotés par l’IA pour répondre aux exigences réglementaires

Utilisation SOC (pSOC) d’un produit XDR alimenté par l’IA à travers le véhicule, le nuage et les API

À l’avenir…

2026 | Mobilité automobile et intelligente
Rapport mondial sur la cybersécurité

L’expansion pilotée par l’IA à la fois des capacités et des risques devient la nouvelle base de référence

La croissance de la surface d’attaque est systémique, pas seulement liée aux véhicules, et les silos échoueront

La résilience dépend de la discipline du cycle de vie : la sécurisation dès la conception, défense en profondeur et validation continue

La chaîne d’approvisionnement, la technologie opérationnelle et les rançongiciels restent des vecteurs de perturbation à fort impact.

Ford | cisco | BMW | IVECO | Google Cloud | BORGWARNER | HARMAN | car | Upstream

Upstream | Transport Canada

Merci.

Télécharger le rapport : **upstream.auto**