2026
Threat Report

汽车及智能化设备网络安全威胁报告

Automotive & Intelligent Device
Cybersecurity Threat Report

木卫四（北京）科技有限公司
www.callisto-auto.com

前言

过去十年，汽车产业的技术重心持续向软件与智能化迁移。车联网、高级驾驶辅助系统、自动驾驶系统以及车路云一体化架构，正在重塑车辆的功能形态与使用方式。与此同时，汽车也从相对封闭的机械系统，演变为高度互联、持续在线的复杂数字系统。

这一变化显著扩展了汽车的攻击面。攻击不再局限于物理接触或单一 ECU，而是逐步延伸至车云接口、远程控制服务、OTA 更新机制、移动应用、第三方平台以及软件供应链。在 2025 年，多起真实发生的安全事件表明，攻击者已能够在不接触车辆的情况下，对车辆功能、用户数据乃至业务连续性产生实质影响。

监管环境也在同步收紧。以 GB 44495-2024《汽车整车信息安全技术要求》为代表的法规进入强制执行阶段，网络安全从“推荐实践”转变为“市场准入前提”。合规不再只是文档层面的要求，而开始直接影响车型上市节奏、业务运营以及品牌风险暴露。

与此同时，安全挑战的形态正在发生变化。随着生成式人工智能、大模型和自动化运营能力被引入车联网与自动驾驶系统，安全问题不再仅限于漏洞修复与边界防护，而逐步演变为对系统行为可控性、责任可追溯性以及长期运营能力的综合考验。

在汽车之外，2025年我们对具身智能与低空飞行器的安全进行研究，并首次加入年报威胁报告中。具身智能与低空飞行器的相关安全事件开始明显增多，其风险特征与车联网高度相似，但物理后果更为直接。

正是在这样的背景下，本报告对 2025 年汽车及相关智能设备领域的网络安全态势进行了系统性梳理。报告基于真实事件、公开研究和长期安全实践，尝试回答以下问题：

> **—— 威胁正在以何种方式演进？**
>
> **—— 哪些攻击面正在成为高频风险源？**
>
> **—— 行业在合规、运营与治理层面面临哪些现实挑战？**

摘要一：2025年汽车及智能化设备安全态势概览

2025年，随着“软件定义汽车”向“AI 定义汽车”持续演进，汽车及相关智能化设备的网络安全风险呈现出攻击面持续扩大、攻击路径更加完整的发展特征。与此同时，UN R155/R156以及 GB 44495-2024和GB 44496-2024等法规与强制性标准的实施，汽车网络安全正式进入以落实合规为基础要求的阶段，您也将在报告中看到针对合规的专门内容。

木卫四威胁情报中心在2025年持续监控7大类、20个子类威胁情报，覆盖公开漏洞披露、真实安全事件、深网与暗网情报、研究披露及行业通报等近百个来源，统计结果显示，2025年共发现汽车安全事件 **206起** ，漏洞 **238个** 。与2024年相比，安全事件数量有所回升，漏洞数量也进一步上升，在合规体系逐步落地的同时，攻击者正在挖掘汽车相关的软件、云端服务与接口层面的安全漏洞。

从攻击对象分布来看，安全事件仍主要集中在智能座舱、车主应用、云平台、OTA、车载外部接口及通信接口等智能化设备及核心资产上。攻击方式以远程攻击为主，部分攻击已不再以单一ECU或功能模块为目标，而是通过云端配置错误、API 接口滥用或车辆外部接口作为入口，逐步向车内关键系统渗透。这一趋势表明，仅满足合规最低要求不足以覆盖复杂的攻击路径，车辆运行阶段的持续安全运营正变得愈发重要。

此外，我们也注意到，AI 技术正在同时影响攻防两端。一方面，攻击者利用AI辅助进行漏洞分析、脚本生成等，降低了攻击门槛；另一方面，防御侧也开始引入AI手段，以提升威胁情报的覆盖度、及时性与关联分析能力。在 UN R155 与 GB 44495-2024 所强调的“生命周期安全管理”框架下，汽车网络安全正从一次性合规建设，转向持续安全运营与动态防御。

KEY FINDINGS

206
Total Incidents
安全事件总数

238
Vulnerabilities
新增漏洞披露

摘要二：从汽车到智能化设备的攻击面扩展

随着汽车产业边界的持续外延，越来越多的车企已经成为具身机器人与低空飞行器等智能化设备的研发与商业化的主要参与者。尽管在系统架构与运行场景上并不与汽车形成直接的技术连接，但其在软件架构、通信机制、云端管理平台以及安全治理模式等方面，往往复用相似的工程体系与研发能力。

在这一背景下，具身智能体、低空飞行器及车载外设等设备所暴露的安全问题，开始对车企整体的网络安全管理能力提出更高要求。这类风险并非通过系统直连传导，而是通过研发流程、平台共用、人员能力与安全策略一致性等层面，与汽车网络安全形成间接但现实的关联。这一变化也对以整车为核心构建的现有合规边界，提出了新的延展性挑战。

> **关键场景风险扩展**
>
> - **低空飞行器场景：**安全风险主要集中于导航、通信与身份识别机制，一旦相关信息被干扰、误用或失效，将对运行安全与管理准确性产生放大影响。
> - **具身智能机器人场景：**安全挑战更多体现在数字系统与物理行为高度耦合所带来的风险放大。当 AI 模型、传感器与执行机构深度融合后，攻击影响不再局限于数据或服务层面，而可能直接作用于物理世界。

这一趋势使安全问题从信息安全，进一步扩展为运行安全与系统安全的交叉问题。在 UN R155/R156 与 GB 44495-2024和GB 44496-2024 持续推进的背景下，本报告旨在通过对真实事件、漏洞与攻击路径的系统分析，为行业提供面向运行阶段、可执行的安全决策参考。

情报来源与威胁监测体系

INTELLIGENCE SOURCES

本年度情报监测体系实现了从传统的网络层向算法层与供应链深处的延伸。我们持续构建覆盖汽车及新一代智能化设备的多源情报网络。

1. 深网与暗网

定位：深入黑产交易市场与勒索软件泄密站点，监控针对车企供应链的凭证交易、源代码泄露及勒索谈判动态。

典型情报：Jaguar Land Rover (JLR) 供应链停产勒索事件，追踪到混合威胁组织 "Scattered Lapsus$ Hunters"...

2. 网络安全大会和大赛

定位：聚合 Pwn2Own Automotive, BlackHat 等实战赛事的成果，获取针对“端-管-云”完整攻击链的高技术含量情报。

典型情报：Synacktiv - Tesla 充电桩固件降级 RCE，在 Pwn2Own 2025 上演示了通过充电接口进行固件降级...

3. 漏洞数据库和Tier1/2安全公告

定位：监测 CVE、CNNVD、CNVD漏洞数据库，Tier1/2 安全公告，建立底层硬件与组件级漏洞映射关系。

典型情报：Kaspersky - Unisoc 车载芯片基带漏洞 ("God Mode")，披露了紫光展锐底层 RCE 漏洞...

4. 社交媒体和独立研究员

定位：利用白帽黑客社区的敏捷性，快速发现未公开的云端API逻辑漏洞与身份验证缺陷。

典型情报：Sam Curry - Subaru Starlink 账户接管漏洞，仅凭 VIN 码即可接管任意用户账户...

5. 学术和前沿研究

定位：追踪顶级安全会议（如 NDSS, USENIX Security），重点关注AI感知层的物理对抗性风险。

典型情报：NDSS 2025 - PhantomLiDAR 攻击，揭示了通过电磁干扰向激光雷达注入虚假点云的跨模态攻击路径...

6. 新闻网站及专业论坛

定位：关注公开的安全事件，分析网络安全对车联网服务的可用性的影响及潜在的远程控制风险。

典型情报：俄罗斯保时捷大规模远程“变砖”事件，因VTS后端服务切断导致无法启动...

7. 全球监管与执法机构

定位：追踪全球主要汽车市场的强制性法规落地进程，覆盖 UN、EU、CN 及 US 四大司法管辖区。

典型情报：欧盟 UN R155 Supplement 3 生效，扩展至 L 类车辆；中国 GB 44495-2024 生效...

2025 年度网络安全威胁全景

ANNUAL THREAT LANDSCAPE

2025 安全事件

206 起

2025 漏洞数量

238 个

维度 1：ECU种类分布

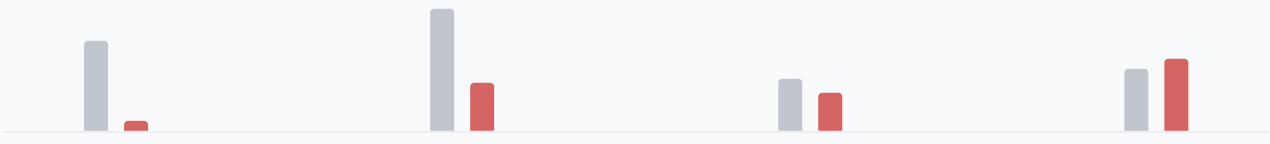
IVI	41
BCM	24
APP	15
ADAS	9
BMS	7
OTA	3
CAN	1
TBOX	1
其他	105

维度 2：攻击场景分布

信息窃取	44
远程控车	25
软件篡改	18
通信干扰	8
传感器欺骗	6
钥匙模拟	6
充电设施攻击	5
云平台攻击	4
诊断接口攻击	1
其他	89

维度 3：22-25 数据对比

YEAR	2022	2023	2024	2025
安全事件	300	405	172	206
漏洞数量	30	160	125	238



年度网络安全回顾

ANNUAL CYBERSECURITY REVIEW (TIMELINE)

云端/远程 OTA/更新 本地/IVI App/OBD 供应链 基础设施

Jan

斯巴鲁（Subaru）Starlink 远程控制漏洞 Web API / 云端

安全研究员 Sam Curry 发现斯巴鲁 STARLINK 平台存在严重漏洞，攻击者通过管理面板可完全接管任意用户账户，进而远程控制车辆（启动 / 定位）并获取隐私数据。

Feb

奥迪 Q8 FlexRay 总线中间人攻击 本地 / 物理总线

研究员 Willem Melching 成功对奥迪 Q8 的 FlexRay 总线实施中间人攻击（MitM），在严格的时序（TDMA）限制下篡改了通信消息。

Mar

Pioneer IVI 系统漏洞利用链 本地 / 近场（IVI）

详述了在 Pwn2Own Automotive 2024 上，针对 Pioneer（先锋）车载娱乐系统的三个漏洞利用链分析。

Apr

“Drive-Thru” 驾驶途经式 Wi-Fi 攻击 无线通信（Wi-Fi）

攻击者利用车辆在驶过特定区域时自动连接开放 Wi-Fi 的行为，通过近距离无线攻击入侵车载系统。

May

日产 Leaf 远程控制漏洞 远程通信 / 车云接口

研究人员披露日产 Leaf 车型存在远程接口缺陷，攻击者可在未经授权的情况下对车辆进行远程控制操作。

Jun

特斯拉充电桩远程代码执行漏洞 充电基础设施

研究发现特斯拉充电桩系统存在远程代码执行风险，攻击者可利用漏洞影响充电服务的正常运行。

Jul

XTOOL Anyscan 诊断 App 远程代码执行 移动 App / OBD-II

NowSecure 发现 XTOOL Anyscan 汽车诊断 App 存在 RCE 漏洞，攻击者可控制手机并通过 OBD 适配器向车辆发送指令。

Aug

捷豹路虎（JLR）供应链攻击致停产 供应链

捷豹路虎遭遇网络攻击，导致其生产和零售运营被迫中断，造成重大业务影响。

Sep

Stellantis 因第三方平台致数据泄露 供应链 / 第三方服务

因使用的第三方 Salesforce 平台存在漏洞，Stellantis 旗下多个品牌（克莱斯勒、Jeep 等）的客户联系信息遭到泄露。

Oct

Alpine IVI OTA 更新机制漏洞链 OTA / 远程更新

研究员发现 Alpine 车载系统 OTA 更新过程中存在 SSL 验证缺失、版本校验绕过和路径遍历漏洞，可组合实现远程代码执行并获取 root 权限。

Nov

保时捷因卫星服务故障大规模瘫痪 基础设施 / 服务中断

由于第三方卫星安全系统出现故障，导致俄罗斯数百辆保时捷汽车无法启动，车辆变为“砖块”状态。

Dec

Unisoc 车机芯片调制解调器漏洞 IVI / Head Unit

涉及中国及全球大量后装车机的 Unisoc 芯片被披露存在漏洞，攻击者可能利用该缺陷实现远程代码执行。

合规专题：中国汽车网络安全监管

从“体系合规”走向“实测准入” (GB 44495-2024)

> **2025年12月16日：准入新基调**
>
> 《GB 44495—2024〈汽车整车信息安全技术要求〉》第1号修改单正式报批。中国汽车网络安全准入从“体系合规”转向“实测准入”。监管逻辑已从审查企业的管理流程（CSMS），彻底转向验证车辆本身的防御能力。仅靠ISO 21434证书将无法满足公告准入要求。

核心差异与合规影响 (Gap Analysis)

从“管理”到“保障”的升级

全文将“信息安全管理体系”修改为“信息安全保障要求”。监管方不再只需为企业内部流程背书，转而关注车辆在最终交付状态下的结果。企业必须证明最终下线产品在物理接触、近场通信等攻击面下具备实质性防护能力。

“检验”背后的技术硬指标

修改单要求对“车云通信身份真实性”、“远程指令防伪”等高危场景进行实质性验证（检测机构将进行渗透测试性质的检验）。任何“功能设计”与“代码实现”的不一致都将导致准入失败。

木卫四建议

证据链重构

OEM需立即调整内部合规交付物标准。转向准备技术证据包（如：密钥管理日志、加密算法验证报告、防篡改机制实测截图）。

预算与周期预警

单车型的认证周期将拉长，建议在项目SOP前预留至少2个月的第三方检测机构排期与整改缓冲。

利用6个月窗口期

针对研发中车型，立即按照“检验”标准进行预测试（Pre-test），特别是针对OTA安全和车内通信加密等硬指标。

合规专题：全球监管动态

UN R155 合规边界向 L 类车辆延伸

联合国自动驾驶与网联车辆工作组（GRVA）及WP.29已完成对UN R155的第三次修订（Amendment 3），正式将网络安全合规要求从M、N、O类扩展至L类车辆。这一举措标志着两轮及轻型车辆正式纳入全球网络安全强监管体系。

欧盟实施路线图与时间线

2024.01

UNECE GRVA 提出将 R155 范围扩大至 L 类车辆。

2024.06

WP.29 决定正式扩展适用范围至 L 类（摩托车）。

2025.03

UN R155 完成第3次修订 (Amendment 3)，覆盖 L1e-L7e 类。

2027.12.11

红线期。所有申请欧盟型式批准的新 L 类车型必须满足 UN R155 要求。

2029.06.11

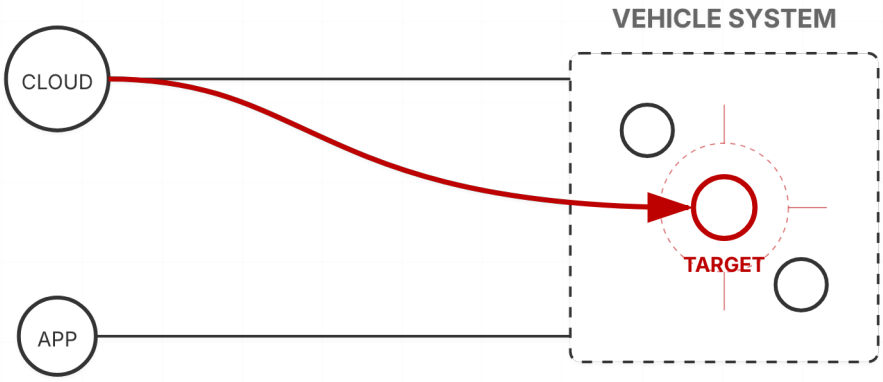
全面覆盖。所有在欧盟注册销售的新车（含旧款）必须合规。

行业影响与应对

法规的统一化有助于制造商在多市场间利用单一认证框架，降低重复合规成本。然而，相比乘用车，摩托车及轻型车辆的EE架构更紧凑、成本更敏感，如何在不显著增加成本的前提下部署IDPS、安全启动等机制，将是OEM面临的严峻挑战。

典型安全事件深度剖析

DEEP DIVE INTO SECURITY INCIDENTS



以下章节将基于真实安全事件，对攻击路径与影响进行拆解分析。
The following section deconstructs real-world security incidents, analyzing attack paths and their systemic impacts.

Case Study1：云端后门——通过管理面板接管实施的车辆非法远控

攻击目标

斯巴鲁STARLINK网联汽车服务的管理面板为员工的内部使用系统，权限高于用户端应用程序。攻击者利用该面板的身份验证逻辑缺陷与客户端安全校验缺失，可接管任意员工账户，进而实现对关联车辆的远程控制（如启动、熄火、解锁、定位）并访问车主的敏感个人信息（如位置历史、紧急联系人、支付信息等）。

攻击流程：攻击链条分为三个阶段，由外至内逐步渗透

1、攻击面发现与枚举

目标转移

在用户端App（MySubaru）验证机制健全难以绕过后，转向寻找更高权限入口。通过DNS解析与子域名枚举，发现内部管理面板 portal.prod.subarucs.com。

端点暴露

对Web资产目录进行模糊测试，发现 /assets/_js/login.js 文件，其中泄露了关键功能端点 /forgotPassword/resetPassword.json。

2、身份认证绕过与账户接管

邮箱枚举

利用管理面板的 /adminProfile/getSecurityQuestion.json?email= 接口，通过差异响应（有效邮箱返回安全问题，无效邮箱返回错误信息）批量验证员工邮箱有效性。结合从公开渠道（如LinkedIn）获取的员工姓名与推断出的邮箱格式 ([首字母][姓氏]@subaru.com)，构建攻击字典。

无验证密码重置

直接向 /forgotPassword/resetPassword.json 端点发送POST请求，仅需提供枚举得到的有效邮箱和新密码即可重置该账户密码，无需任何所有权验证（如令牌、OTP）。

登录

使用重置后的密码成功登录管理面板。

3、2FA绕过与权限提升

修改前端JS：登录后系统要求回答安全问题作为2FA。通过浏览器开发者工具修改前端JavaScript代码，注释或删除触发安全问答模态窗口的代码（如 $('#securityQuestionModal').modal('show')）。

权限获取：服务端未校验

服务端未对2FA环节的完成状态进行二次校验，攻击者可绕过客户端交互，获得完整的管理员权限，可执行车辆控制、数据查询等敏感操作。

缓解措施

1、强化身份认证与会话管理

对密码重置等敏感操作实施多因素验证，服务端应对关键安全流程（如2FA）的状态进行严格校验。

2、实施安全的API设计与输入验证

对API调用进行强身份认证机制，对错误反馈采用采一的模糊响应。对用户输入实施强校验与过滤。

3、最小化攻击面与加强监控

对内部管理系统实施严格的网络访问控制，定期进行代码审计与渗透测试。对异常登录行为与高频次敏感操作进行实时监控与告警。

4、开展安全意识培训与威胁情报应用

对内部员工进行社会工程学防范培训。建立或加入汽车威胁情报共享平台，及时获取最新安全信息。

Case Study2：OTA 更新链劫持——从移动端 RCE 到车辆物理控制

移动应用中不安全设计成为车辆的攻击入口。该事件强调了移动应用安全在连接设备生态中的关键性：任何绕过标准安全流程的实现都可能导致远程代码执行风险，并可能对依赖该应用的用户和车辆环境造成严重安全后果。

攻击目标：移动终端设备

攻击者可针对安装了 XTool AnyScan Android 应用的移动设备实施远程代码执行，进而获取应用权限范围内的设备访问和控制能力，包括访问摄像头、蓝牙、GPS 等高危权限。

攻击后果：控制连接的车辆系统

由于 AnyScan 与 XTool 车辆诊断设备通过 OBD-II 端口和移动应用进行双向通讯，攻击者在成功接管应用后可向车辆发送恶意控制指令。例如可重写钥匙、误操作紧急装置或其他安全关键系统，存在导致车辆被盗或乘员受伤的高风险。

攻击流程：攻击链从移动端漏洞扩展到物理车辆控制路径

1. **发现不安全的应用内更新机制**

   AnyScan 使用自定义插件下载和更新机制来扩展功能，并未遵循 Google Play 安全指南，这使得更新管道本身存在严重安全缺陷。

2. **绕过应用中TLS 证书验证**

   应用实现了不安全的 TrustManager，绕过了 TLS 证书验证，允许攻击者通过中间人（MITM）攻击拦截、篡改更新请求和响应内容。

3. **利用硬编码加密密钥和弱加密算法破解通信加密**

   应用在解析更新元数据时使用了 DES 56位弱加密，并将密钥与初始化向量（IV）硬编码在代码中，使得攻击者可以逆向出密钥并解密更新内容。

4. **利用不安全的更新机制应用内注入恶意插件并使用网络代理工具向服务器执行攻击**

   攻击者借助代理工具（如 mitmproxy）伪造更新元数据，指向托管恶意插件的服务器。AnyScan 不验证插件完整性，将恶意共享库（如 libscan.so）下载并加载到应用进程中，从而实现持久远程代码执行。

5. **使用应用向车辆下发恶意诊断指令，进一步拓展攻击面**

   一旦恶意代码在移动端获得执行，它即可利用手机应用与设备间的通讯权限，通过 OBD-II 接口下发恶意车辆控制指令，可能影响车辆关键系统

缓解措施

弃用自定义更新机制

遵循平台安全指南，避免在应用内部实现自主更新或插件下载框架。使用官方渠道或具有完整代码审查与完整性校验的更新方式。

启用严格的 TLS 实现与证书验证

在网络通信中不能绕过 TLS 证书验证，保证从服务器获取数据的真实性与机密性。

避免使用硬编码密钥及弱算法

所有加密材料应采用安全密钥管理机制，不应硬编码在代码中，并应使用现代强加密算法替代 DES 等过时方案。

插件完整性与身份验证

所有第三方或运行时代码更新包必须经数字签名并在本地执行前验证签名，以阻止恶意代码加载。

Case Study3： 特洛伊充电桩——利用固件降级将能源设备转化为内网入侵跳板

攻击目标

攻击目标是特斯拉壁挂式充电器，但真正的意图是将其作为跳板，通过获取其Wi-Fi凭据来渗透用户所在的内部网络。攻击者通过获得对充电器的完全控制权，可以进入家庭、酒店或企业的私有网络环境，从而有机会发现并攻击连接在同一网络下的其他高价值设备，实现横向移动和更深层次的入侵。

攻击流程：多阶段、需要物理接触的复杂攻击链

01 初始访问 (Initial Access)

物理接口利用： 攻击者必须物理接触到充电器的充电端口连接器。这是整个攻击的唯一入口点。

02 协议逆向与模拟 (Protocol Reverse Engineering & Emulation)

1 发现专有协议

通过示波器分析控制导频（CP）信号，发现非标准单线CAN (SWCAN) 协议。

2 构建汽车模拟器

使用树莓派、继电器和定制USB-CAN适配器构建"特斯拉汽车模拟器"，触发SWCAN模式。

03 漏洞发现与利用 (Vulnerability Discovery & Exploitation)

1 固件降级漏洞

缺乏防降级保护，可刷入含调试功能的旧版固件(0.8.58)。

2 信息泄露漏洞

旧版UDS服务允许读取Wi-Fi SSID和密码。

3 缓冲区溢出漏洞

TCP调试Shell命令解析存在溢出，可覆盖函数指针。

04 攻击执行步骤 (Execution Chain)

- **1 固件降级**

  连接模拟器，通过SWCAN发送UDS命令，刷入旧版固件（0.8.58）。

- **2 窃取凭据**

  设备重启后，通过UDS命令提取Wi-Fi SSID和密码。

- **3 网络接入**

  使用获取的凭据，将攻击者设备连接到同一Wi-Fi网络。

- **4 获取代码执行**

  连接TCP调试Shell，利用缓冲区溢出重定向执行流，实现RCE。

缓解措施

缓解措施的核心是实施固件防降级保护，阻止攻击者将设备强制回滚到存在已知漏洞的旧版本，这一步直接切断了整个攻击链的起点。同时，通用的安全强化措施也至关重要，包括从生产固件中彻底移除所有调试代码和接口，对敏感的诊断功能采用强加密认证，以及启用内存保护机制来增加漏洞利用的难度。

Case Study4： 数据武器化——行车记录仪隐私窃取与情报自动生成

一、攻击目标

攻击以具备 Wi-Fi 通信能力的车载行车记录仪为主要目标，针对在短时间内处于静止状态并进入攻击者近场无线覆盖范围的车辆设备。攻击者通过入侵行车记录仪，非法获取车内视频、音频及位置信息，从而对车主及乘员的隐私安全构成直接威胁。在部分设备型号中，攻击目标进一步扩展至设备配置与运行状态本身，攻击者可篡改记录策略、破坏设备可用性，甚至为后续向车载系统或关联终端的横向渗透创造条件。

二、攻击流程

该案例实施了一种自动化、无关特定厂商的近场攻击模式，核心特点是在极短时间窗口（约 6 分钟）内完成设备入侵与数据处理。

1

近场无线发现与接入

- 被动扫描车辆周边 Wi-Fi SSID，识别行车记录仪特征
- 利用弱点快速建立连接：默认/固定/弱口令、不可修改的出厂密码、WPA2 握手捕获后的快速离线破解

2

配对与认证机制绕过

- 绕过“物理配对”或“设备绑定”机制，包括：
- 直接访问未受保护的 HTTP/FTP 服务
- 基于 MAC 地址的信任机制被伪造
- 通过语音提示反复触发，诱导用户确认配对

3

未鉴权服务与接口滥用

- 滥用暴露的服务接口（HTTP、FTP、Telnet、RTSP、自定义 API）
- 通过硬编码凭据、明文凭据或完全无鉴权接口访问存储内容
- 在部分型号中可上传 WebShell，实现远程命令执行与提权

4

数据外泄与设备破坏

- 批量导出视频、音频及元数据
- 远程修改配置文件，实现：禁用录像、删除历史文件、修改 Wi-Fi 密码，锁死合法用户

5

数据与情报提炼

- 利用 AI/LLM 对窃取数据进行自动化分析：
- 视频中提取路牌与地标，反推出行路线
- 音频转写车内对话并进行语义总结
- 汇总用户出行模式、生活习惯与潜在敏感信息

三、缓解措施

安全默认配置

- 每台设备使用唯一强密码，禁止通用或不可更改凭据
- 强制首次使用时修改默认口令
- 禁止不必要的服务端口与明文协议（FTP/Telnet）

强化配对与认证机制

- 禁止仅依赖 MAC 地址或客户端标识进行信任判断
- 引入基于证书或加密挑战-响应的配对机制
- 在非必要场景关闭 SSID 广播

Case Study5：从云端到 CAN 总线——以 IVI 为跳板的远程横向渗透路径

随着智能汽车人机交互系统（IVI）与外部网络及车内多域系统的深度集成，其攻击面持续扩大。本案例基于公开技术研究，分析了一起针对车载 IVI 系统的远程利用攻击路径。攻击者通过外部网络接口入侵 IVI，进一步突破系统边界，实现对车内关键网络的横向访问，验证了 IVI 在整车网络安全体系中的高风险枢纽地位。

一、攻击目标

IVI Head Unit（Linux/Android-based）	IVI 网络服务组件（远程服务 / 调试接口）	IVI 车内网络通信接口（CAN / Ethernet Gateway）

二、攻击流程

01 远程攻击入口获取

攻击者通过车辆对外暴露的蓝牙接口接触车载系统，将 IVI 作为初始攻击目标。IVI 中的蓝牙 HFP（Hands-Free Profile）服务处于常驻启用状态，且采用专有协议栈（Bluedragon Evo Bluetooth Stack）实现，使其成为可被无线访问且风险较高的攻击入口。

02 IVI 服务漏洞利用

在 HFP 服务处理 AT 命令的过程中（如 +ANDROID:probe），存在栈缓冲区溢出漏洞。攻击者可发送构造的蓝牙数据触发内存越界写入，并通过 ROP 链完成代码执行，从而在无需物理接触车辆的情况下获得 IVI 的远程执行能力。

03 IVI 系统权限控制失效

蓝牙协议栈进程以 root 权限运行，同时 IVI 操作系统整体安全加固不足，包括未启用 SELinux、内核模块缺乏签名校验以及可执行的临时目录等问题。在漏洞被利用后，攻击者可直接获得系统级控制权限，无需再进行额外的权限提升操作。

04 车内网络横向移动

取得 IVI 控制权后，攻击者可利用其合法的车内通信能力，通过 Internal Network Communication 接口向 CAN 总线发送构造报文。结合车载网关过滤策略配置不当以及 RH850 MCU 固件中的栈溢出漏洞，攻击可进一步扩展至其他 ECU，如 BCM 或 ADAS 控制单元。

三、造成的安全问题

IVI 已被成功用作从外部无线接口进入整车内部网络的攻击跳板，形成了“远程 → IVI → CAN → ECU → 功能控制”的完整攻击路径。

四、缓解措施

- 对 IVI 对外网络服务实施最小暴露原则，关闭非必要端口与接口
- 加强 IVI 系统服务的身份认证与访问控制机制
- 实施 IVI 与车内关键网络之间的强隔离与协议过滤
- 对 IVI 软件与第三方组件开展持续漏洞扫描与安全加固
- 在整车层面部署针对 IVI 异常行为的检测与响应机制

专题章节

SPECIAL TOPICS ANALYSIS

专题一：车载大模型的安全性——攻击面变化与风险放大

车载大模型安全的重要性

截至2025年，虽然市场尚未针对“车载大模型”出台单独的法规，但车载大模型通常被归入既有的汽车网络安全与软件变更治理框架：UN R155强调整车全生命周期的风险识别与缓解，UN-R156要求软件更新具备安全性、完整性与可追溯性。

从安全视角看有四类对大模型功能的更新会影响车辆功能边界，会涉及到UN-R156和GB44496-2024中OTA的安全要求，它们包括：模型权重与版本、推理策略（含工具调用策略）、能力开关/配置、外部工具与插件清单。换句话说：车载大模型不应被放在整车安全体系之外单独“豁免”，它需要被纳入既有的安全架构、验证与审计材料体系中。

> **威胁面迁移：大模型攻击手段正在“平移”到车端**
>
> 我们在2025年的车载大模型安全研究中发现三类可利用的新风险：供应链投毒、提示词劫持，以及面向智能体的“过度代理”。这些并非只存在于云端聊天机器人，当车载大模型开始接入导航、支付、充电、车控等工具链后，同样的攻击链路可以迁移到车端。

MCP协议：连接生态的同时，放大了供应链与会话层风险

MCP成为连接车载AI与外部生态（如支付、导航）的标准，但也暴露了高危漏洞：

工具投毒（Tool Poisoning）

工具投毒是2025年MCP生态中最具破坏性的攻击向量。攻击者通过污染MCP工具链来实施攻击。攻击者可以通过篡改工具的元数据描述（如未来伪装成“智能充电”插件），利用LLM对自然语言指令的盲目信任，诱导AI执行非预期操作（如重定向支付或窃取隐私）。MCP允许工具动态更新定义，使得恶意功能可在通过初始审查后被“注入”。

远程代码执行（RCE）

CVE-2025-6514 漏洞允许恶意MCP服务器在连接的客户端上执行任意操作系统命令。对于基于Linux或Android系统的IVI来说，这意味着此类风险同样存在。

提示词劫持

MCP协议依赖会话ID 来维护客户端与服务器的状态。2025年披露的CVE-2025-6515漏洞揭示了MCP在会话管理上的重大缺陷，恶意插件可声明高优先级来遮蔽合法服务。

智能体:从“会说”变成“会做”，权限治理是第一道坎

随着AI具备自主规划能力，安全风险从被动响应转向主动执行，面临如下风险：

- **过度代理（Excessive Agency）：** 智能体往往继承了车主的全部权限。一旦遭遇攻击，它可能会滥用合法权限执行恶意操作（如为优化能耗而意外关闭安全系统）。
- **间接提示词注入（Indirect Prompt Injection）：** 攻击向量物理化。路边广告牌的对抗性图案或会议邀请中的隐藏文本，被车载摄像头读取后，可被解析为高优先级指令（如“解锁车门”），直接突破物理防线。
- **级联幻觉（Cascading Hallucinations）：** 在多智能体协作中，一个Agent的错误判断（如虚构充电桩）会作为“事实”传递给下游Agent（如电源管理），引发系统性的连锁故障和瘫痪。

专题二：L3 自动驾驶商业化下的安全责任重构与不对称威胁

2026年标志着全球汽车行业正式跨越L2+向L3级有条件自动驾驶的商业化门槛。随着梅赛德斯-奔驰、本田在欧美日的规模化部署，以及中国（如极狐、深蓝）发放首批L3准入牌照，车辆安全责任主体发生根本性转移：**从驾驶员转向自动驾驶系统**。

> 这一转变将网络安全从“合规基线”升级为“业务生命线”。当前L3生态面临前所未有的网络安全威胁：攻击面已从传统的物理接触，爆炸式扩展至基于身份的云端劫持、针对AI感知的物理对抗以及供应链逻辑炸弹。为支撑“脱手/脱眼”体验，车载计算平台算力突破2000 TOPS，代码量超1亿行，这种“轮子上的高性能计算中心”正成为间谍活动与勒索软件组织（如Jackware）的高价值目标。

2026 L3 威胁趋势：从“入侵车辆”到“控制体系”

2026 年 L3 威胁重心正在从单车入侵转向整车控制体系。攻击目标由车内网络迁移至云端控制面、身份系统与软件供应链，攻击路径更多依托合法身份、合规接口与更新链路完成。

车辆不再是主要攻击终点，而是被纳入可远程调度、批量控制的系统节点。**基于身份的权限滥用、供应链投毒与配置级操控**将成为主要威胁形态。

该趋势意味着，L3 风险不再取决于单一漏洞或防护强度，而取决于**控制体系的完整性与可控性**。一旦控制面失守，车端防护难以形成有效阻断，风险将以系统级方式集中释放。

专题三：具身智能体与机器人——从数字系统到物理世界的安全挑战

具身智能商业化：从技术跃迁到安全奇点

2026 年被普遍视为具身智能商业化落地的起点。继大语言模型重塑数字系统之后，人工智能开始大规模进入真实世界运行环境。人形机器人正从实验室和封闭工厂，进入家庭、商超、柔性产线等非结构化场景，承担真实、连续且不可逆的物理任务。

这一阶段的核心变化不在于硬件形态，而在于控制范式的转移。具身智能系统的决策中枢已从确定性控制逻辑，转向以视觉-语言-动作（VLA）大模型为核心的概率性推理体系。机器人不再执行“被验证过的动作序列”，而是在持续感知与生成中决定下一步物理行为。

> 情报判断认为，这一转变构成了具身智能的安全“奇点”。传统安全模型建立在明确边界之上：输入可控、逻辑可审计、输出可预测。而 VLA 架构下，感知、理解与动作被压缩为统一的模型推断过程，逻辑边界失效，安全不再是外围属性，而是模型行为本身的一部分。
>
> 在该模式下，攻击者无需突破网络边界或系统权限，仅需影响模型的输入语义或感知判断，即可诱导机器人执行高风险动作。模型幻觉不再表现为文本错误，而是直接转化为错误的力、速度与路径选择，具备现实破坏性。

与此同时，具身智能的商业化路径正在引入新的系统性风险。技能商店、云端推理、机器人即服务（RaaS）等模式，推动机器人长期在线并接受第三方能力注入。机器人由“设备”演变为“可远程编排的物理节点”，其安全属性开始接近关键基础设施。

情报显示，勒索软件已从加密数据演进为锁定物理能力。通过篡改关节校准、力控参数或安全阈值，攻击者可以在不破坏系统完整性的前提下，使机器人失去工作能力，或在特定条件下转化为高风险执行体。

综合判断，2026 年具身智能所面临的风险不再是单点漏洞或工程缺陷，而是由控制方式的变化引发的从网络到功能级的安全。物理世界正在成为攻击面的延伸，安全失败的后果将变得更加不可控。

2026 具身智能威胁趋势：从“攻破系统”到“操纵行为”

情报显示，2026 年具身智能威胁正在发生方向性转移。攻击目标不再以“控制机器人”为终点，而是以“操纵其行为输出”为目的。入侵路径由系统层转向认知层，由权限突破转向模型诱导。

趋势一：VLA 模型本身成为主要攻击面，对抗手段已从像素扰动升级为语义级操纵，通过物理提示、语言歧义或多模态输入组合，绕过模型内置的安全对齐机制。这类攻击不依赖系统漏洞，难以通过传统补丁方式修复。

趋势二：供应链攻击向“认知层”延伸，微调模型、技能包、训练数据正在成为新的投毒入口。攻击逻辑不再表现为显性恶意代码，而是潜伏于权重与策略中，在特定条件下触发偏移行为。该类后门在测试阶段高度隐蔽，却在真实场景中具备致命影响。

趋势三：低成本具身智能设备的规模化部署放大了系统性风险，为抢占市场而牺牲安全设计的硬件与软件，在家庭和工厂中形成大规模可控节点。这些节点既可能演化为移动式情报与攻击平台。

趋势四：机器人即服务模式正在集中风险，车队管理系统、云端调度平台与计费体系成为高价值目标。一旦控制面被劫持，攻击者可通过合法接口批量下发恶意指令，形成物理层面的拒绝服务或连锁事故。

趋势五：具身智能开始进入国家级威胁视野，具备自动化能力的机器人集群正被视为关键基础设施组成部分。情报显示，具备国家背景的攻击组织已开始测试针对机器人网络与 OT 系统的渗透路径，其目标并非即时破坏，而是长期潜伏与战时失能。

总体判断是：具身智能的主要风险不再来自“被入侵”，而来自“被误导、被操纵、被滥用”。未来安全能力的核心不在于封堵接口，而在于控制模型行为的可解释性、可约束性与可降级性。如果不能在商业化早期建立这一安全防御能力，具身智能将在规模化部署后暴露出不可承受的系统性风险。

专题四：eVTOL 与低空飞行器——天空中的灰色安全地带

2025年的威胁态势监测表明，针对eVTOL和无人机的对抗模式发生了转移，攻击重心已从传统的物理拦截（如网枪、激光干扰）向设备控制和拒绝服务演变。攻击者正利用底层通信协议（如ISO 15118, MAVLink）的先天缺陷和软件供应链漏洞，成功实施针对关键基础设施的攻击。这种攻击不仅能导致服务中断，更可直接转化为设备坠毁等后果。

协议层深潜：基础设施的信任危机

地面充能网络的“中间人”渗透

随着eVTOL商业化运营对高功率快充的依赖，充电基础设施成为了新的高危攻击面。CVE-2025-12357（CVSS 8.3）的披露揭示了国际标准 ISO 15118-2 在设计上的重大疏漏。该标准在利用电力线通信进行车辆与充电桩物理配对时，其SLAC协议缺乏强制性身份认证机制。攻击者只需在充电站附近部署低成本信号注入设备，即可通过伪造更强的响应信号劫持配对过程，建立中间人连接，能导致拒绝服务阻断起飞，同时攻击者可篡改电池管理系统的关键参数，诱发电池热失控等。

飞控系统的内存安全崩溃

在航空器端侧，广泛应用于物流与工业级UAS的开源飞控 PX4 Autopilot 被曝出严重的内存安全漏洞 CVE-2025-15150。该漏洞位于 mavlink_log_handler.cpp 模块，因对输入数据缺乏严格的边界检查，允许攻击者通过构造恶意的MAVLink日志请求触发堆栈缓冲区溢出。一旦攻击者通过数传链路或被攻陷的机载电脑（Companion Computer）触达飞控，即可导致飞控进程Panic重启引发坠机，甚至在硬件层面执行任意代码以接管飞行控制权。这再次证明，在缺乏内存安全语言（如Rust）重构的情况下，传统C/C++航空代码库仍是极度脆弱的。

电子战（EW）与信号情报：隐形战场的对抗

全球GNSS欺骗（Spoofing）常态化

国际航空运输协会（IATA）数据显示，2025年GPS欺骗事件同比激增500%。

- **圆圈欺骗（Circle Spoofing）**：在波罗的海和黑海区域，电子战系统通过注入虚假坐标，诱导飞行器自动驾驶仪进入盘旋模式，ADS-B轨迹呈现完美的圆形。
- **机场位移攻击**：在中东地区，高功率欺骗信号使航空器导航系统误判位置（如将坐标瞬移至贝鲁特或开罗机场）。这对高度依赖自动化精密进近着陆的eVTOL构成了灾难性风险。

远程ID（Remote ID）的攻防博弈

随着Remote ID法规的强制执行，攻防博弈升级：

- **幽灵机群（Ghost Fleet）**：GitHub开源项目如 "Drone Swarmer"，利用ESP8266等廉价硬件广播数千个虚假位置信号，旨在通过饱和攻击瘫痪AeroScope等空域态势感知系统。
- **隐私裸奔**：安全研究人员逆向DJI DroneID协议证实，包括飞手位置在内的关键数据在传输层未加密，极易被第三方截获并用于定位操作员（反制打击）。

监管重构：国家层面的要求与合规的“双重枷锁”

美国：多重禁令

美国的《安全无人机法案》（ASDA）在2025年全面执行，禁止联邦资金采购“受关注国家”制造的无人机。除硬件禁令外，FCC加强了对通信模块的审查。任何无法证明固件底层不存在“回传后门”的设备，面临FCC ID撤销风险，直接切断了存量机队的合法性。

欧洲：数字主权与适航的“强绑定”

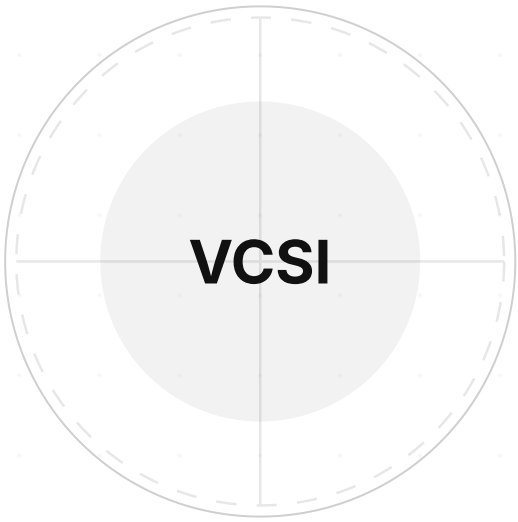
- **EASA ED-203A 标准**：EASA将网络安全纳入型号合格证（TC）的前置条件。eVTOL必须证明其具备对抗GNSS欺骗、链路劫持的安全能力，否则无法获得商业运营许可。
- **网络弹性法案 (CRA)**：要求厂商对上游组件（含开源代码）负责，迫使大量缺乏DevSecOps能力的中小厂商退出市场。

中国：低空经济的安全强管

- **UOM平台强制接入**：所有民用无人机必须接入统一监管平台（UOM），实现“一机一码”实时身份识别。

安全指数与建议

SECURITY INDEX & RECOMMENDATIONS



2025年车联网网络安全指数（VCSI）

从合规驱动到“AI原生”的战略进化：

合规成熟度提升

2024年是法规落地的奠基之年。2025年，随着GB 44495-2024等标准的强制执行，安全基线和体系化建设将成为行业标配，推动安全水位普遍提升。

运营能力成为新战场

基础建设完成后，竞争焦点将转向大规模车辆安全运营(VSOC)的效率和成熟度。弥合2024年暴露的运营能力短板是企业的核心挑战。

AI安全治理的兴起

生成式AI既是防御的利器，也带来了新的攻击面。2025年，对AI应用的安全治理能力将成为衡量企业安全领导力的全新维度。

从奠基到加速，安全成熟度全面跃升：

2024年打下的基础将在2025年转化为全面的发展势头。随着法规进入强制执行期、初始投资开始见效、以及对运营短板的集中攻克，我们预测车联网安全指数将在所有维度上实现加速增长。行业正从“有没有”安全建设，迈向“好不好”的运营效果比拼。

整体指数迎来飞跃，最大增幅出现在“安全基线”和“运营能力”两大维度，反映出行业在补齐合规短板和提升实战能力方面的双重发力。

1 关键驱动力一

GB 44495-2024《汽车整车信息安全技术要求》进入强制执行阶段，未达标车辆无法上市销售，倒逼企业将安全基线建设作为最高优先级。

2 关键驱动力二

2024年暴露的远程控车、充电桩等实战攻击，使企业认识到仅有合规是不够的。VSOC从“合规展示品”向“实战指挥部”转变，其在降低风险、保护品牌声誉方面的价值凸显。增加对VSOC人员和技术的投资；引入AI和机器学习技术提升海量告警的分析效率和威胁溯源能力

安全建议

EXECUTIVE & ENGINEERING VIEW

01 构建L3级“责任溯源”与“感知抗扰”融合防御体系

2025年L3级车辆在京渝等地获得正式号牌，法律要求车辆在特定条件下可“脱手脱眼”。这要求安全体系必须能处理复杂的责任界定与极端场景接管。

建立不可抵赖的数字记录系统

依据最新的L3准入导则，部署抗篡改的自动驾驶数据记录系统。引入区块链或可信执行环境（TEE）对关键日志进行实时签名，确保在发生交通事故时，能从法律上厘清是“人为误操作”还是“系统被攻击/故障”

强化预期功能安全与网络安全的融合

设计独立的最小风险机动（MRM）模块，一旦检测到网络入侵或感知异常，系统应立即引导车辆靠边停车，而非直接交还控制权给可能已惊慌失措的驾驶员。

02 VSOC运营转型——基于“资产上下文”的动态漏洞治理

面对海量且低效的日志警报，VSOC（车辆安全运营中心）需将“流量监控”与“资产全生命周期管理”深度融合，实现综合研判。其核心在于构建以动态 SBOM（软件物料清单）为基座的监测体系，结合 VEX（漏洞利用交换）机制对流量警报进行上下文验证，在分钟级内自动剔除那些“虽有漏洞但因配置限制无法被利用”的无效告警，将误报率降低 90% 以上。

同时，深化 VSOC 与 OTA 平台的协同联动，打造“监测-评估-备案-响应”的全链路闭环能力：高危漏洞（如 Log4j）爆发时，系统可基于资产图谱在分钟级内精准锁定受影响车辆（VIN）并输出业务影响评估；在完成人工备案与变更审批后，自动编排并触发安全隔离或补丁推送策略，确保处置全过程日志留存以供 UN R155 / GB 44495 合规审计。

03 实施“零信任”供应链隔离与敏捷合规策略

2025年Nissan的重大泄露事件源于第三方供应商（如Red Hat开发环境、IT外包商）的失守。供应链已成为攻击者进入主机厂内网的“高速公路”。

- **推行“供应商开发环境隔离”政策：**不再默认信任 Tier 1 或软件供应商交付的代码。强制要求供应商在交付前提供完整的代码扫描报告及 SBOM。对于敏感项目，要求供应商在交付前提供完整的代码扫描报告及 SBOM。对于敏感项目，要求供应商在物理隔离的“洁净室”环境中进行开发，严禁将生产凭证硬编码在 Git 仓库中。
- **建立软件成分的“动态准入”机制：**在 CI/CD 流水线中部署自动化卡点。任何含有已知高危漏洞或来自受制裁实体（响应 BIS 禁令）的开源组件，都应直接阻断构建，防止其流入量产车辆。

04 强化EV充电基础设施的“桩-车-网”三端身份互信

随着新能源车渗透率突破新高，充电桩成为连接电网与车辆的高风险接口。攻击者可能通过充电桩窃取支付信息，甚至发起“某区域千桩同停”的电网冲击攻击。

- **实施“桩-车-网”三端双向认证：**推广 ISO 15118 标准的“即插即充（PnC）”技术，利用 PKI 证书体系确保车辆与充电桩之间的身份合法性。严禁使用明文协议传输支付数据或 BMS（电池管理系统）数据。
- **物理防篡改与电网隔离：**对公共充电桩的维护接口（USB/调试口）实施物理封锁。在充电站后台部署针对 DDoS 攻击的流量清洗设备，防止攻击者控制大量充电桩同步开启/关闭大功率充电，造成局部电网波动。

05 确立AI模型的完整性校验与红蓝对抗机制

随着端到端大模型上车，针对 AI 算法本身的“投毒”和“欺骗”成为新型威胁。攻击者可能通过污染训练数据或生成对抗样本，诱导车辆做出危险决策。

- **安全基线：**严格 Schema 校验与参数清洗
- **安全架构：**构建“确定性”物理防线
- **安全存储：**向量库隔离与全链路审计
- **安全测试：**Fuzz 验证与红蓝对抗

06 治理“影子API”

车云互联及手机 App 控车功能的普及，导致 API 调用量激增。黑客通过 API 遍历漏洞批量窃取用户数据的事件频发。

- **全域 API 资产测绘与治理：**关闭“影子 API”“僵尸 API”，统一身份认证与访问控制。
- **业务逻辑风控前置：**在 API 网关层部署风控能力，重点防御对车主隐私数据的自动化爬取。

产品与解决方案（一）

PRODUCTS & SOLUTIONS

S3-VSOC | 汽车网络安全运营平台

S3-VSOC 是面向汽车主机厂与车联网业务的统一网络安全运营平台，以国内外法规与合规监管要求（UN R155 / GB 44495）为指导，以通车端、云端与企业侧安全数据为基础，以实现车企安全运营合规化、体系化、常态化、实战化为目标，构建面向全生命周期的汽车网络安全运营管理体系的整体解决方案，帮助车企与运营方实现车辆网络安全态势的可视、可管、可控。它不是单一工具，而是承载 CSMS 落地与车型全生命周期安全运营的核心中枢。

● 数据治理

车企业务数据孤岛、合规取证难？S3-VSOC以UN R155 / GB 44495为指导，将法规条款拆解为数据证据，汇聚车端、车云与企业侧数据，将碎片化数据转化为可持续更新的高质量数据资产，支撑合规审计与业务决策。合规审计材料准备时间缩短60%，证据链完整性提升100%，确保新车型上市合规。并通过VSOC数据打通运营、保险、研发、质控等部门业务壁垒，激活数据资产价值。

● 风险降噪

车型不断增加、告警爆炸、误报多？通过“规则引擎+算法小模型+AI Agent”的多层级智能检测机制，对海量安全数据进行持续降噪与优先级重构，精准狙击可行动的高置信度安全事件，显著提升关键风险可见性，低危告警误报率下降90%，高危告警漏报率几乎为零。

● 辅助运营

运营团队能力参差不齐、新人培养周期长？AI以“运营Copilot”形式融入日常运营，通过自然语言交互与可解释推理，协助完成告警分析、调查研判与决策支持。通过VSOC AI Copilot 降低对顶尖专家的依赖，提升团队整体效能与决策质量，新员工可快速完成100%重复性任务及约70%的专家级研判工作。

● 无人值守

人工值守成本高、非工作时间存在防护盲区？通过智能值守机制，VSOC实现7×24×365全天候自动化安全运营，从威胁发现、研判到处置形成闭环。基于分级信任框架（Staged AI Trust Frameworks），从AI增强人工能力（AI Copilot）到内嵌AI能力减少人工操作（AI-Native），再到高信任场景下全自动替代人工操作（Autonomous），安全运营能力由“依赖人工经验”升级为“AI+workflow+专家思维链+知识库”驱动的体系化能力，夜间与节假日运营值守人力成本可降低约60%，关键威胁响应时间平均缩短50%。

S3-VTI | 汽车威胁情报服务

S3-VTI 是专为汽车行业打造的威胁情报订阅服务，通过持续监测全球汽车网络攻击方法、漏洞利用趋势和恶意活动，围绕“车、云、软件、供应链”构建具备资产上下文的汽车威胁情报体系，将分散、模糊的外部情报转化为可判断、可关联、可行动的行业安全洞察，助力提前发现风险、定制防御策略，提升整体安全响应效率。

● 高质量

通用 IT 威胁情报在汽车领域“水土不服”？建立专注于汽车产业的威胁情报库，持续监控整车、车云、软件及供应链威胁，过滤掉所有非汽车（通用 IT）领域的无关噪音，聚焦汽车行业关键威胁。

● 高可信

情报来源分散、可信度参差不齐？通过整合公开情报、行业通报、漏洞数据库、攻击事件及舆情等信息，并通过平台过滤+AI分析+人工校准进行可信度评分，确保情报100%真实可靠、可溯源。

● 高可用

情报与车企资产脱节、响应滞后？基于资产上下文将威胁情报与车型、ECU、软件组件关联，支持按维度个性化订阅，可快速集成到VSOC，实现闭环“情报-监测-响应”，关键威胁响应时间缩短40%。

产品与解决方案（二）

PRODUCTS & SOLUTIONS (CONT.)

S3-TARA｜大模型智能体 TARA 管理平台

S3-TARA是基于大模型技术的智能威胁分析与风险评估平台，以ISO 21434等法规为牵引，通过AI驱动自动化完成资产识别、威胁建模、风险量化与处置建议，大幅提升车企在概念设计阶段的合规效率与风险评估精度。

● 知识复用

TARA 分析专家稀缺、新人上手慢？通过私有化汽车攻击与法规知识库，将专家经验沉淀为可复用的平台能力，AI辅助非资深人员也能完成高质量TARA分析，团队TARA分析效率提升3倍。

● 风险量化

TARA 风险评估主观性强、缺乏统一评价标尺？沉淀专家经验，融合CVSS、攻击可行性、影响范围等多维因子，自动量化风险等级，实现数据驱动的安全决策，并将风险结论无损转化为可执行的安全工程需求，团队TARA分析一致性提升70%。

● 一键过检

TARA 报告输出耗时耗力、文档变更频繁？将ISO21434最佳实践固化于平台流程，形成可复制的标准化能力，自动化执行TARA分析流程，自动化生成TARA报告，动态管理文档版本，文档交付效率提升80%。

S3-IDPS｜车载入侵检测与防护系统

S3-IDPS 是面向车载网络与车端系统的入侵检测与防护能力，通过持续监测车内通信行为与异常模式，提供实时、可验证的车端安全防护与合规取证能力。

● 合规证据链

新车型合规审计成本高？检测项对齐UN R155/GB 44495要求，沉淀事件记录与合规取证方法论，新车型上市合规速度提升60%。

● 低成本部署

车端硬件有限、部署难？提供可快速集成的IDPS SDK，无需额外硬件资源，100%可直接嵌入ECU车载环境，实现低性能消耗下的持续安全监控，跨车型、跨零部件适配。

● 端云联动

车端检测孤立、整体闭环链路长？基于端云协同架构，将检测结果实时回传至云端VSOC，构建“检测-分析-响应”的端云闭环安全运营体系，情报驱动的事件平均响应时间缩短40%。

木卫四（北京）科技有限公司是由全球首批专注于汽车网络安全的技术专家创立、由全球知名机构投资、具备多项自主知识产权的国家高新技术企业和专精特新企业。

木卫四正为全球智能汽车领域、自动驾驶和高级驾驶辅助系统的领军企业提供强有力的网络安全支持。客户包括但不限于宝马中国、福特中国、赛力斯、奇瑞、上汽、广汽、蔚来、吉利、北汽、一汽等汽车行业佼佼者。

生态合作伙伴 ECOSYSTEM PARTNERS

木卫四的发展得益于众多生态伙伴的大力支持，包括华为云、亚马逊云、百度、腾讯云、微软云、地平线、天准科技、艾拉比、鱼快创领、德勤、普华永道、安永等知名企业。

参考（References）

SOURCES & CITATIONS

[1] https://mp.weixin.qq.com/s/YSNqYdsKlxG218k-2rHCwg

[2] https://i.blackhat.com/Asia-25/Asia-25-Chen-Drive-Thru-Car-Hacking-wp.pdf

[3] https://www.securityweek.com/nissan-leaf-hacked-for-remote-spying-physical-takeover/

[4] https://www.synacktiv.com/en/publications/exploiting-the-tesla-wall-connector-from-its-charge-port-connector#

[5] https://www.nowsecure.com/blog/2025/07/16/remote-code-execution-discovered-in-xtool-anyscan-app-risks-to-phones-and-vehicles/

[6] https://cj.sina.com.cn/articles/view/1872005590/6f9489d601901afle?froms=ggmp&

[7] https://www.ithome.com.tw/news/171342

[8] https://www.bilibili.com/video/BV14eWxzbEL6

[9] https://cyberpress.org/satellite-security-glitch-leaves-hundreds-of-porsche-cars-immobilized/

[10] https://cybersecuritynews.com/hackers-could-take-control-of-car-dashboard/

[11] https://atm.automotiveisac.com/technique

[12] https://cybermagazine.com/news/jlr-cyber-breach-financial-disaster

[13] https://www.ndss-symposium.org/ndss-paper/phantomlidar-cross-modality-signal-injection-attacks-against-lidar/

[14] https://openreview.net/forum?id=H6UMc5VS70

[15] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202500005

[16] https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=2DB552CAA58F589705C3DC7AD47AC2AB

[17] https://samcurry.net/hacking-subaru#unlocking-a-friends-car

[18] https://www.startus-insights.com/innovators-guide/future-of-autonomous-vehicles/

[19] https://mp.weixin.qq.com/s/SwkOn_RQU6IIZI7S1sp7RQ

[20] https://vicone.com/zh/blog/breaking-down-the-pioneer-ivi-system-3-bug-exploit-chain-from-pwn2own-automotive-2024