Deloitte.

亚马逊云科技

木卫四科技 CALLISTOTECHNOLOGY

如何重塑智能网联汽车安全

汽车网络安全运营中心 (VSOC) 白皮书

2023年8月

目录

本白皮书由德勤企业咨询（上海）有限公司（“**德勤企业咨询**”）、Amazon Web Services, Inc. 或其关联方（“**亚马逊云科技**”）以及木卫四（北京）科技有限公司（“**木卫四**”）分别撰写，三方就各自撰写的内容分别、独立享有相关知识产权。其中德勤企业咨询负责第一章、第二章、第四章、第五章a部分（即“VSOC技术趋势”）和第六章，单独享有该部分的知识产权；木卫四负责第三章和第五章b部分（即“木卫四VSOC整体解决方案”），单独享有该部分的知识产权；亚马逊云科技负责第五章c部分（即“亚马逊云科技基础设施是构建VSOC的重要基础设施”），单独享有该部分的知识产权。

关于德勤企业咨询部分的声明：本白皮书中所含内容乃一般性信息，任何德勤有限公司、其全球成员所网络或它们的关联机构并不因此构成提供任何专业建议或服务。在作出任何可能影响您的财务或业务的决策或采取任何相关行动前，您应咨询合资格的专业顾问。 我们并未对本白皮书所含信息的准确性或完整性作出任何（明示或暗示）陈述、保证或承诺。任何德勤有限公司、其成员所、关联机构、员工或代理方均不对任何方因使用本通讯而直接或间接导致的任何损失或损害承担责任。德勤有限公司及其每一家成员所和它们的关联机构均为具有独立法律地位的法律实体，相互之间不因第三方而承担任何责任或约束对方。德勤有限公司及其每一家成员所和它们的关联机构仅对自身行为及遗漏承担责任，而对相互的行为及遗漏不承担任何法律责任。德勤有限公司并不向客户提供服务。请参阅www.deloitte.com/cn/about了解更多信息。

关于亚马逊云科技部分的声明：本部分内容陈述了亚马逊云科技在封面页所示日期的有关服务产品及实践，该等信息可能变化且我们不会另行通知。客户对于本部分的信息以及亚马逊云科技的产品或服务应自己做出独立的判断，该等内容都是“依现状”提供，不包含任何明示或者暗示的保证。本部分内容并没有创设来自亚马逊云科技、北京光环新网科技股份有限公司（“光环新网”）、宁夏西云数据科技有限公司（“西云数据”）、或其各自的关联方、提供方或许可方的任何保证、陈述、合同性承诺、条件或者担保。亚马逊云科技、光环新网、西云数据对其各自的客户的义务和责任均由适用的客户协议管辖。本部分内容不是亚马逊云科技、光环新网、西云数据和其各自的客户之间任何协议的组成部分，也不构成对任何协议的修改。

关于木卫四部分声明：本白皮书中所含木卫四提供之内容，在做出任何可能影响用户采购决策和或相关行动前，您应参考企业需求和现状，咨询符合企业要求的合作伙伴。我们并未对本白皮书所含信息的准确性或完整性做出任何（明示或暗示）陈述、保证或承诺。木卫四（北京）科技有限公司、关联企业、员工或代理方均不对任何方因使用本信息而直接或间接导致的任何损失或损害承担责任。请参阅www.callisto-auto.com了解更多信息。

引言

智能网联汽车作为一项重要的创新技术，正在引领着汽车行业的变革。德勤汽车安全团队分析发现，随着全球联网车辆的数量的高速增长，预计将从现在的2.5亿辆增长到2040年的10亿辆以上，网络安全问题和其他数据驱动的挑战正在成为行业关注的中心议题。

汽车制造商和监管机构已经确定了汽车安全运营中心VSOC(**VSOC是一个专门的控制系统，用于检测、监控和缓解网络和其他威胁**）是解决问题的关键能力，**是确保全球数百万互联车辆安全和保障的最有效方法**。而作为智能网联汽车的核心技术之一，汽车安全运营中心（VSOC）在确保车辆网络安全的同时，也提供了更加智能化、高效化的运维管理手段。

随着技术不断发展成熟，全球各大汽车制造商和科技公司都在积极布局智能网联汽车领域，智能网联汽车市场持续扩大，预计在未来几年内将呈现高速增长趋势，这也推动了VSOC技术的快速发展。同时，不断涌现的车辆网络安全威胁也使得VSOC的需求日益迫切。

在这样的大背景下，德勤中国成立了“智能网联汽车网络安全实验室”，并积极与亚马逊云科技以及木卫四科技（简称“木卫四”）等合作伙伴开展智能网联汽车的多层次合作，持续面向智能网联汽车VSOC开展详细的趋势洞察和技术探索。

1 智能网联汽车面临的网络安全挑战

新形势下的汽车网络安全

当今世界，数字技术、呈指数增长的数据、持续发展的商业需求，这些因素都扩大了网络安全威胁的攻击面，同时网络安全的攻击事件日益繁复、层出不穷，数量和复杂度不断增加。领导者们不得不以全新的角度来看待网络安全问题，主动探寻随着新的业务或场景而伴生的安全需求及其内在价值，这不仅是为了保障企业当前的业务，更是强有力确保公司战略不被影响的关键一环。

全球各企业通过加强对于网络安全的思考、并在业务中采取相关行动，开始关注加强网络安全所带来的积极影响。网络安全领域的内外协作、主动风险管理等动作，在减缓网络威胁、保护商业价值以及巩固客户信任等方面发挥至关重要的作用。

近年来我国各监管部门快速推进汽车网络安全标准法规的制定，旨在尽快建立健全汽车行业网络安全体系和汽车企业安全管理制度，进一步提高道路车辆网络安全性能，相关标准法规均多次强调安全运营工作的重要性。企业的核心工作是需要提高预防、检测和进行快速响应的能力，消减安全事件的威胁，这将可以缓解对车辆、组织和品牌声誉的损害。

回顾2022年，德勤汽车安全团队分析发现，随着全球联网车辆的数量的高速增长，预计将从现在的2.5亿辆增长到2040年的10亿辆以上，网络安全问题和其他数据驱动的挑战正在成为中心议题。汽车制造商和监管机构已经确定了车辆安全运营中心VSOC是解决问题的关键能力，VSOC是一个专门的控制系统，用于检测、监控和缓解网络和其他威胁，是确保全球数百万互联车辆安全和保障的最有效方法。

VSOC在智能网联汽车的未来发展中将发挥越来越重要的作用。通过安全监测与防御、故障诊断与维护以及数据分析与优化等功能，VSOC能够提高智能网联汽车生态系统的安全性，进一步亦可提升交通安全与效率。VSOC的发展也面临着安全风险、技术标准和法规制定以及数据管理等挑战。通过合作共享和开放标准，以及加强安全防御和数据管理能力，VSOC有望实现更加智能化、可靠的运营管理，助力智能网联汽车行业的可持续发展。

安全合规已成为核心驱动

近几年国家陆续出台三大上位法，涵盖网络安全与数据安全，即《网络安全法》、《数据安全法》、《个人信息保护法》，汽车行业监管发布有国家网信办的《汽车数据安全管理若干规定（试行）》和工业与信息化部发布的《工信部车联网网络安全和数据安全通知》。汽车行业除了需要关注网络安全威胁，各企业在深度转型过程中，均面临越来越严峻的网络安全合规风险。

此外，汽车行业针对车辆产品的网络安全合规监管特殊要求。国际上欧洲，日本已于2022年正式实施联合国世界车辆法规协调论坛UNECE WP.29 的R155汽车网络安全管理体系和R156软件升级管理体系法规，要求汽车制造企业与各级供应商识别车辆及零部件和软件接口的网络安全风险，确保车辆产品在设计、生产、测试、运营、售后阶段具有网络安全防护能力，只有车辆获取网络安全合规准入审批后才能进入市场。 目前国内也发布了《关于加强智能网联汽车生产企业及产品准入管理的意见》和强制性标准《汽车整车信息安全技术要求（征求意见稿）》，这些强制性标准预计在2023年会定稿并正式发布，监管部门也有计划把上述强制性标准转为车辆准入强制性法规并组织实施，届时国内市场所有车辆新车型上市之前均必须符合这些要求。此外工信部基于《国家车联网产业标准体系建设指南（智能网联汽车）（2022版）》，正在起草和修订很多智能网联汽车相关网络安全合规标准。

2023年国家将进一步强化数据安全建设，围绕数据安全治理、数据分类分级、安全应急响应、数据跨境传输监管等重点工作内容，汽车行业监管在行业年度汽车数据安全年报申报基础上，积极推动各级企业开展数据安全风险评估和合规检查工作，汽车行业已进入网络安全合规的“强监管”时代。概述来看包括：

一、新业务、新技术所带来的网络安全合规风险：新技术和业务可能会引入安全漏洞，车载互联使得车辆能够实现与外部世界的通信，车辆对车辆通信提高了道路安全性，同时，诸如远程诊断和升级功能使得车辆生产商可以在线更新软件和固件，但这也会让黑客入侵系统和破坏车辆变得更为容易。随着新技术和业务的不断推进，监管机构持续制定法规以确保车辆安全和隐私的保护，这可能会对企业造成合规压力。因此，汽车行业需要密切关注这些合规风险，并采取必要的策略和技术措施来保护数据和车辆的安全，保障业务的持续发展和运营。

二、供应链网络安全合规风险：汽车的研发和生产制造过程涉及大量的供应商，而这些供应商提供的产品均有可能存在网络安全漏洞，这将会成为汽车供应链安全攻击的潜在入口。于此同时，汽车制造企业作为车辆产品责任人对消费者，监管和社会承担网络安全合规的主体责任，新形势下汽车制造企业如何基于新模式下的产业供应链，确保所有供应链企业都符合统一且明确的合规标准将面临巨大的挑战。

三、海外合规风险：汽车企业出海之前，需要注意网络安全及数据安全合规风险，不同国家和地区会有不同的市场监管法规和标准，企业在开展业务前需要了解并遵守当地法规和标准。尤其是进入国外成熟市场将面临非常严苛的网络安全合规监管要求，例如车辆产品网络安全合规准入认证，个人隐私保护与数据安全等，海外业务运营过程中持续满足合规要求是车企出海制胜的关键必要条件。为此，如何建立完善的法律合规团队和流程，并及时调整相关规则将是难点。

以WP.29 R155法规为例，车企须通过信息安全管理体系认证（即“CSMS证书”）以及车辆型式审批（即“VTA证书”），才能进入欧盟上市销售。

- CSMS认证审查车企覆盖汽车全生命周期，包括车辆研发、试生产、量产、服务、运维等各阶段的车辆网络安全管理流程，以保证车辆产品设计、实施及服务响应均有车辆网络安全体系指导。
- VTA审批则进一步针对车企在车型开发中具体工作项进行产品网络安全审查，旨在保证实施于车辆的网络安全防护技术在进行审查认证时已经足够完备。换言之，CSMS认证是车型准入型式审批的前提，而最终车辆市场准入必须通过CSMS认证以及车辆型式审批。

由于汽车复杂且分散的技术架构，以及对供应链的高度依赖，新法规的发布将给OEM厂商带来巨大挑战。德勤分析发现，传统OEM厂商自主研发软件仅占百分十至百分三十。此外，不同的OEM厂商在车辆网络安全的成熟度参差不齐，OEM厂商基本是从零开始建设车辆产品网络安全能力，而新车型的开发周期通常为3-4年，对于2023年及之后的新车型开发，OEM厂商必须将网络安全融入到车辆设计过程中以满足WP.29和国内强标合规要求。随着新规生效日期逐渐临近，合规行动已刻不容缓。

开启车辆网络安全合规之旅

德勤目前联合多家头部合作伙伴正在为超过十余家的全球和中国知名的汽车制造商提供WP.29车辆产品网络安全相关服务，基于德勤的行业洞察和丰富的项目经验，我们认为OEM厂商可以实施以下步骤尽快满足WP.29网络安全合规要求：

执行WP.29产品网络安全合规速赢评估：基于WP.29网络安全框架及其合规要求快速评估组织内当前合规状态，汽车制造商可以确定实现合规所需的主要资源包括组织人员，技术能力和管理流程并制定行动计划和路线图；

设计和实施组织内WP.29 车辆网络安全“就绪"能力和程序：能力评估将为组织设计有效的安全能力提供所需信息，框架和程序实施后还需进一步细化和转化为可落地实施的具体控制措施，管理程序和报告机制从而推进整体WP.29网络安全工作；

全面审视和检查正在研发的新车型项目：企业最担心事情莫过于投入巨大的研发和生产的车辆由于合规准入问题导致无法上市销售。为避免上市准入风险实际发生，车企需要在量产之前对正在研发流程中的所有新车型进行全面的车辆网络安全合规评估和审查以确定任何潜在的WP.29安全合规风险并尽快实施整改措施。

2 VSOC 重塑智能网联汽车安全

关于汽车安全运营中心（VSOC）

网络安全工作需要持续地关注系统及外部环境变化，在安全运营过程中建立一套车辆威胁洞察的机制，并且持续对车辆网络安全风险保持监测，对当前的汽车企业来说是一项困难的工作。这些工作包含许多并行又互相关联的任务，从业务连续性和可靠性管理到网络安全策略制定执行，再到人员能力的全面培养提升，以及响应。一般的网络安全运营内容包含针对所有攻击的监测、分析、响应和恢复工作，而承载事件检测、分析和响应工作的组织或系统称作安全运营中心（Security Operations Center），自20世纪90年代以来，SOC便一直在企业IT中被广泛使用，同时随着技术的发展及应用领域的扩展，各类组织都拥有某种形式的SOC。汽车安全运营中心VSOC（Vehicle Security Operations Center）并非独立存在的概念，IT行业的实践无疑也给汽车网络安全管理带来了指导，通常，VSOC是指一个专门负责监控和管理车辆网络安全的枢纽平台。它通过连接到车辆网络并实时监测车辆的网络行为，可以快速检测并应对潜在的威胁和攻击事件。其主要功能与IT SOC之间存在众多可见的相似之处，但也存在众多差异——包括汽车领域知识、百万级数据处理要求、广泛的汽车维护策略等。

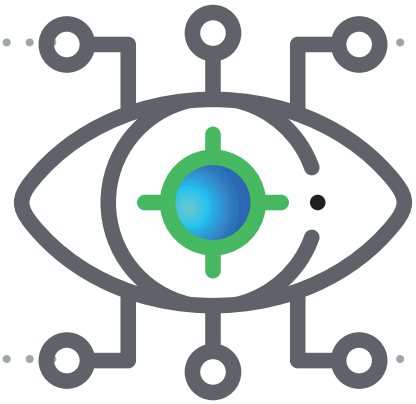
VSOC主要承担以下职责：

1. 监控和分析

VSOC通过实时监控车辆网络的活动，收集和分析车辆网络数据流量、日志等信息，以识别可能存在的安全漏洞和攻击行为。

2. 威胁检测和预警

基于实时监控和分析的结果，VSOC能够及时检测到可能的威胁和攻击，并向相关人员发送预警通知，以便及时采取应对措施。



3. 安全事件响应

一旦发现车辆网络中存在安全事件或威胁，通过VSOC可协调相关团队迅速响应，采取必要的措施修复漏洞、清除恶意代码等，以确保车辆网络的安全运行。

4. 数据分析和报告

VSOC会对收集到的车辆网络数据进行分析，提取安全相关的信息，并生成详细的报告，以帮助车企或相关团队了解车辆网络安全状态，并制定相应的安全策略和措施。

VSOC能创造什么价值

德勤在VSOC建设上有着比较长期的技术探索和技术优势，在2022亚马逊云科技中国峰会的汽车行业分论坛中，德勤中国风险咨询合伙人肖腾飞发表了题为《为车辆安全保驾护航-基于亚马逊云科技的德勤车辆安全运营中心解决方案》，其中介绍了：目前汽车行业安全态势愈发紧张，黑客正采用低成本、高便携和快速迭代的手段来攻击智能汽车，车联网安全威胁正以惊人的速度增长，道路车辆迫切需要被实时安全监控。

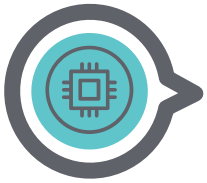
同时国家有关部门在战略目标、产业指导、安全监管、标准体系建设等方面出台了一系列指导性文件，多次强调安全监控和响应能力的重要性。在这种趋势下，德勤VSOC汽车安全运营中心解决方案将为车辆提供端到端的安全能力，包括威胁监控、威胁情报集成分析、安全事件分析（SIEM）、漏洞管理、安全事件响应等安全能力。其核心是为了提高相关企业预防、检测和进行快速响应的能力，消减安全事件的威胁，以缓解对车辆、组织和品牌声誉的损害。此外，德勤中国与亚马逊云科技在安全领域开展了一系列的合作，包括安全合规服务、安全运营中心服务（SOC/VSOC）、托管安全服务等。

合规价值：

当前情况下，一个完善的VSOC能够满足联合国世界车辆法规协调论坛（WP.29）R155法规的相应要求，如持续监控、新型攻击检测、缓解措施和合规报告等。由于我国也已出台相关的强制标准和法规，VSOC亦可以满足中国强制性法规，CSMS和VTA认证的要求。

管理价值：

通过使用VSOC，车企的风险管理者可以全局审查、评价和管理网络安全工作，联合整理工作流程、团队及工具。通过不断优化的监测和响应流程，充分保障车主用车安全，提升产品安全性能。VSOC也可以整合和提升网络安全能力，帮助团队全面管理安全，避免出现合规问题、安全工作不可见等问题，落地安全技术，提升安全运营能力。



技术价值：

通过使用VSOC，车企网络安全工程师可以减轻工作压力，并提高KPI。VSOC通过持续监测、分析和响应，形成网络安全事件管理闭环，全面掌握车辆安全状态。VSOC可以使车辆网络安全工程师主动管理攻击和威胁，支持安全工程师实现工作目标。

上述工作也可通过虚拟团队或线下流程实现，但面对日益增加的车辆资产和智能化服务，人力工作的繁琐可能对安全管理造成负面影响。我们相信，随着车辆网络安全工作的提升，VSOC团队和工具将成为车企的必备选择。

与IT 领域的SOC运营差异分析

目前来看，不少汽车企业当前也拥有IT SOC以确保IT资产的安全，然而遗憾的是，IT团队与汽车团队工作的脱节和业界传承的工作习惯导致当前的IT SOC远不能满足汽车网络安全工作的需要。VSOC与传统的IT SOC安全运营中心存在诸多不同之处：

VSOC需要更全面的汽车行业知识：不仅需要了解网络安全行业的基础概念，熟悉安全运营以外，VSOC更需要对车辆本身的了解。当车辆核心资产和智能化服务面临威胁时，车辆网络安全工程师应当结合车联网系统、车辆状态进行分析、定位并作出有效响应；

VSOC需要防范多种攻击：面对复杂的供应链、不断变化的电子电气架构、创新的智能化服务、SOA架构的引入等，智能联网汽车的接口类型越来越丰富，VSOC需要应对攻击者可能采用的多种技术手段和攻击路径；

VSOC需要管理大量的车辆资产：合格的VSOC应当具备管理数百万辆车联网资产的能力，对海量车联网资产进行持续实时分析和管理，对技术架构挑战巨大；

VSOC需要保证系统可靠性/功能安全的影响：与IT系统不同的是，车辆系统的业务连续性及可靠性要求更高，如部署的安全Agent/Sensor复杂性过高，会影响到业务连续性或车辆可靠性，甚至对企业声誉造成较大影响；

VSOC需要提高可见性和上下文：当异常事件发生时，通常情况下需要确认车辆上下文状态信息以分类事件并对攻击行为追踪和溯源，否则大量的误报会大大加重车辆网络安全工程师的工作负担；

VSOC需要调度更多的职能部门：汽车生产制造涉及到的分工部门众多，汽车行业供应链较长，一系列任务及工单可能会涉及多部门人员及角色；

VSOC需要更有针对性的威胁情报：聚焦于汽车行业的威胁情报一方面可以提供更有针对性的车辆攻击手段、不良影响及缓解措施等信息，另一方面使VSOC能够牢牢掌握与攻击相关的漏洞，并先发制人地减轻破坏性攻击；

VSOC需要灵活可扩展：为了应对技术架构的演进，新功能的快速上线，日益严格的监管要求，VSOC在技术架构上都应当具备充分的弹性，以确保在未来数年的时间内快速迁移、拓展和开发；

VSOC需要更智能：海量汽车的异常警报、不同类型的剧本流程、VSOC在部署时应充分考虑对大数据及人工智能的应用以降低车辆网络安全人员的工作压力，确保VSOC的先进性；

VSOC需要更加专业的技术人员和特定的安全工具，以满足汽车行业的特殊需求，例如对车联网协议、汽车电子系统和车载通信网络的了解。此外，VSOC还需要支持汽车行业的严格法规和标准，以确保汽车网络的安全性和可靠性。

3 打造一个易用高效的VSOC

在过去的一段时间内，我们也看到一些汽车企业积极的在尝试部署VSOC以提升汽车网络安全水平，然而根据大量调研及一线工程人员的反馈，我们也看到在VSOC建设过程中因为概念不清晰、专家知识欠缺、工程规划缺陷以及开发部署能力较弱等因素导致成本及资源的浪费，甚至可能埋下新的安全隐患并给管理带来更多问题从而导致VSOC项目的失败。

VSOC建设误区

我们总结了VSOC建设过程中几大常见误区，这些误区广泛存在于不同类型车企/供应链企业，供行业管理者及工程人员参考：

VSOC选型失策：将IDS、EDR等信息汇总工具定义为VSOC，而针对汽车核心资产及智能化服务的威胁检测能力缺失，导致VSOC形同虚设。另外缺乏拓展性及弹性架构设计的VSOC也使得车企无法应对迅速变化的车辆安全运营需要。

过于强调Dashboard而忽略了VSOC功能：调度中心的大屏幕并不能从根本上帮助安全团队真正做到安全运营。在UI及呈现方面过多的关注会分散VSOC建设的注意力，我们建议更多关注VSOC功能实现而非呈现；

分析功能不专注于汽车：威胁分析能力是决定VSOC成功的关键，对汽车的SOC来讲，车辆攻击事件的分析需要有丰富经验和持续的研究投入。仅仅分析操作系统和网络资源，会产生大量的误报和漏报，极大程度打击车辆安全运营团队的信心；

情报/数据源不够丰富：单一的数据来源无法为车辆安全事件分析提供上下文支撑，车辆安全团队无法做到全面快速响应和预警；

跨部门之间缺乏协作：缺乏组织架构保障的情况下，无法真正保障威胁分析的准确性、安全事件的及时响应能力，甚至有可能造成安全运营工作的停摆。

VSOC核心功能

VSOC 需要通过一系列的功能满足对智能网联汽车核心资产和智能化服务的监测和防御要求。尽管部分标准只关注车辆或者某个ECU 本身的安全，但是从各类攻击报告和事件的统计来看，我们倾向于将汽车智能化服务及核心资产纳入到考量范畴，因为攻击者通常不会遵循某一特定向量对汽车发起攻击。尽管当前少有企业能建设满足以下全部功能的VSOC，我们仍建议企业在实际建设过程中从自身规模、团队成熟度等因素出发，做出更为谨慎的选择：

表1：安全事件分类、分析及响应

实时告警及分类	对车辆停泊及行驶状态中产生的异常告警进行潜在安全事件分类和快速分析。
安全事件分析及调研	对汽车核心资产进行组件级安全分析，同时关联智能化服务的数据流信息。充分描述并确定安全事件的细节（背景、影响范围及程度）。
缓解措施	联动安全机制，对车辆发生的安全攻击及时遏制，可对攻击活动进行快速隔离、阻断，以减少影响、控制损失并防止扩散。
安全协作	通过集成协作工具对安全事件收集、分发和通知，指挥、协调和报告车企的不同人员、部门、供应链及主管单位。
取证分析	检查被攻击车辆的零部件、车况、数字钥匙、车辆后门、应用系统、安全日志等，归纳总结攻击行为的时间线、动作及结论。
安全事件远程响应	充分考虑在移动办公、异地协作等情况下的远程响应需要。考虑到开发部门、安全团队、供应商及用户车辆往往分布于全球各地，需要及时远程响应各种情况下的汽车安全事件。
安全事件报告接收	无缝接收和处理来自IT系统、车辆系统、安全团队、SRC以及第三方的潜在的安全事件报告。

表2：威胁的高级分析

汽车威胁情报构建	采集尽可能丰富、有针对性的汽车行业相关网络威胁情报服务/信息，处理威胁情报信息并将其整合入VSOC之中，解析并过滤相关信息以供VSOC及团队进一步使用。
威胁报告分析提交	对汽车领域攻击者画像，跟踪攻击趋势以支持非法改装、欺诈、恶意破解及非法控车等情形下的风险决策，做到知彼。导出威胁报告，描述攻击者类型、战术和活动及对供应链和车企的影响。
威胁情报信息共享	与VSOC以外的各方（监管机构、供应链、开发测试团队、合作伙伴等）共享威胁情报和事件报告。
威胁诱捕	在网联汽车的真实环境中，利用蜜罐及数字孪生技术，对新型攻击提前发现及分析，以提升和完善VSOC对新型攻击的识别。
威胁检测定制化	面对不同车型核心资产和智能化服务，依据各类攻击场景及威胁报告建模。在充分了解车辆系统的风险之后，更精确地配置、使用和自定义检测规则及引擎。
大数据和人工智能	通过先进技术处理和分析车辆异常行为，进一步分析从而发现新型威胁攻击。

表3：漏洞管理

车辆资产盘点	在TARA分析过程中盘点资产信息及关联关系，同时扩展至OTA、TSP、移动服务等平台，量化漏洞影响程度及潜在风险。
漏洞扫描及评估	持续扫描所有车辆资产的漏洞状态，包括零部件BOMs、车辆相关应用、云服务等，计算安全风险和合规状态，并评估当前防护手段的有效性。
漏洞库更新和分析	接收车企内部渗透测试团队、外部白帽子、研究机构等各方的漏洞报告，以了解漏洞并与风险管理部门、供应链等角色分享漏洞信息，以便各方采取缓解措施。
漏洞修补和缓解	及时发现并通知车辆开发部门及供应商修补漏洞，或通过多种缓解措施最大程度隐藏漏洞以减少暴露和利用的风险。

表4：态势感知及合规管理

车辆态势感知	全面感知、分析网络安全威胁及便于管理者探查现状的“汽车安全态势感知平台”
合规管理	针对不同国家和区域的汽车网络安全相关法规，配置和生成符合相对应法规要求的报告。

VSOC建设要点

除了需要时刻避免因规划不当、工程能力不足、保障不够等问题导致的VSOC项目失败之外，我们也给VSOC的管理和建设者们提供以下建议，以确保不同规模的VSOC有效运转。

充分了解车联网系统及行业：了解汽车及网络安全行业变化；合规范围及工作内容；车辆资产及供应商；用户行为及智能服务；及时关注威胁报告；深入理解关键系统和数据类型，并不断跟踪汽车行业技术变化；

充分赋予VSOC完成工作的权利：调整组织架构，充分授权给VSOC团队，确保其所需的职责、工作范围、合作关系和责任；

构建符合企业特点的VSOC：通过服务对象确认VSOC的架构，电动汽车、车队、OEM及供应链等不同类型不同规模的企业所需VSOC存在较大区别，建议优先考虑选择最高效的VSOC架构；

雇佣并培养高素质人员：考虑到汽车行业网络安全人才缺乏的现状，我们建议创造良好的职业发展机会和环境留住人才。同时考虑部门内人员流动的可能，通常情况下网络安全团队广泛的跨领域知识和风险管理经验对现代车企数字化转型具备较大价值；

优先考虑对异常的响应能力：通过所定义汽车事件类别、响应流程和转变趋势将进行编排并纳入SOP及PLAYBOOK，确定事件的优先级并分配资源以应对；

利用威胁情报提前应对：通过分析更有针对性的汽车攻击事件、漏洞情况、测试报告、研究趋势等，确认这些数据信息其与车辆资产的交叉点，以确保新型攻击在第一时间发现；

选择恰当的数据以分析：车辆异常信息的分析通常需要更多维度的数据类型，充分理解各类型的数据有利于快速锁定上下文信息并定位问题。同时也应充分考虑对已下线无Agent / Sensor / EDR 情况下的车辆威胁监测；

利用工作流程管理工具：统一和协调内部对数据和工具的使用，最大程度提升VSOC的流程能力，促进IT安全、大数据和车辆安全团队协作；

清晰沟通、保持合作、慷慨分享：利用VSOC吸引促进用户、供应商、SRC、白帽子、研究机构之间沟通协作，同时提升能力为汽车网络安全社区做出更广泛贡献；

衡量效果并不断提升：量化VSOC的运行效率，了解VSOC的运作情况以及改进目标。包括监测车辆信息、数据源处理分析、安全报告及事件响应时间等；

扩展VSOC功能提升绩效：通过实施攻防演练、渗透测试、等活动，协助提升VSOC团队的声量和VSOC的运营能力。从而提升车企安全形象。

4 联合运营VSOC成为新趋势

步入2023年后，联网汽车的数量正在急速增加，且覆盖了乘用车到商用车等多种车辆类型。同时，无论是软件定义汽车还是自动驾驶，车辆软件控制功能的数量也在激增。这两个因素结合在一起，增加了攻击面以及相关的网络安全风险的数量和严重性。这就导致了一种情况，要求：

- 基于安全设计流程的硬件基础设施
- 具有专业安全能力的分析师，以持续监测整个车队的情况；
- 易用的VSOC平台，最好是具备云端能力，来快速识别威胁；
- 能够快速反应的响应团队，以便及时发现和挫败网络攻击。

亦如前文所述，已经生效的UN R155不仅仅是一项法规，更成为车辆网络安全的一个全球基准。该法规以及预计的联网车辆数量的急剧上升和日益增长的汽车行业竞争压力，将使业内越来越关注VSOC。

虽然UN R 155没有特别要求VSOC，但在实践中，如果没有VSOC的支持，智能网联汽车要符合该法规的要求是非常困难的。UN R155附录5定义了一份直接且明确的威胁清单，而VSOC在监测和缓解网络攻击方面发挥着关键作用。

因此，需集各家所长，采取联合运营模式来有效地建立和运营VSOC，将成为各方的优先考虑，尤其是对于各车企降本增效的趋势下实现更先进的车辆网络安全性能至关重要。

常见VSOC运营模式

自建式VSOC

企业内部自建的VSOC主要关注24x7的集中的威胁检测和响应功能，有专门的团队以及处置程序和工作流程。它相对独立，拥有持续的日常安全运作所需的所有资源。一些专门的功能可能偶尔会被外包，如独立的技术测试（渗透测试/红队）、逆向工程恶意软件或使用外部威胁情报源，但是VSOC的核心功能和日常运作完全由内部团队提供。

内部VSOC通常最适合于中小型企业，这些企业需要运营年产量约数十万辆汽车的水平。VSOC团队通常由十人左右的服务工程师构成，并购买或研发了部分的安全工具和流程以及操作手册。

这些企业因为以下情况下选择建立、实施和运行自建的VSOC：

- 业务相对简单或是企业内部管理要求限制了外包的选择。
- 对特定的有针对性的潜在威胁有担忧。
- 企业内部业务方面的流程无法外包。
- 组织的自研技术栈无法得到第三方安全服务的支持。

外包型VSOC

此类型VSOC是基于企业内部团队和外部供应商资源的结合，提供综合的SOC功能以满足组织的需要。此模式更多基于企业个性化的考虑，业界并没有 "正确 "或 "错误 "的最佳实践，因为侧重于灵活性。常见到企业将一些功能外包给供应商，同时保留了组织评估和响应的内部流程等功能。

业界常见的的解决方案包括：管理安全服务（MSS）、管理检测和响应（MDR）或管理SIEM/COMSIEM。典型案例是搭建安全运营团队需要覆盖的专精需求相对成本较高，技能、专业知识和人员配置的短缺，更多的也有可能是内部预算的限制，故许多企业考虑将诸如威胁情报和威胁狩猎业务外包给第三方供应商。

针对部分外包的VSOC，企业重点需要考虑的是：

- 效益是否会超过成本?
- 它是否有助于实现整个团队更紧密的协同工作?
- 供应商能否协调企业内部运营团队，同时保持职责分离并避免利益冲突?

联合运营的托管式VSOC

此类VSOC模式是指在同一实体（常见于多实体/跨国公司）内由一家服务机构统筹协调多家供应商独立运营核心安全能力的托管式解决方案，但是核心部分仍然由企业内部（VSOC指挥中心或母公司）高层级VSOC同步提供统一的威胁检测和应急响应。

企业为了降低对单一供应商的依赖，需要依托不同供应商在各自优势领域的安全运营技术和能力，集成多家供应商能力提供全面的安全运营服务，通过供应商之间协作进行定制化解决方案配置，最终根据企业具体业务的要求提供灵活的VSOC解决方案。目前联合运营的托管式VSOC解决方案逐渐成为企业的优选，此VSOC可跨区域和实体协同工作，采用分布式管理，通常将由某一服务机构统一协助企业管理对应的各内部团队和外部供应商，并建立高层级VSOC指挥中心。

选择联合运营模式的企业重点需要考虑企业内部与各供应商之间的工具选型和流程体系的搭建。德勤建议企业需要整体考虑内外部如何协同工作在统一的云服务和共同的安全运营流程和体系上，以优化安全运营期间的各项工作和确保拥有更专业的流程，如威胁识别和应急响应。

德勤联合运营VSOC解决方案

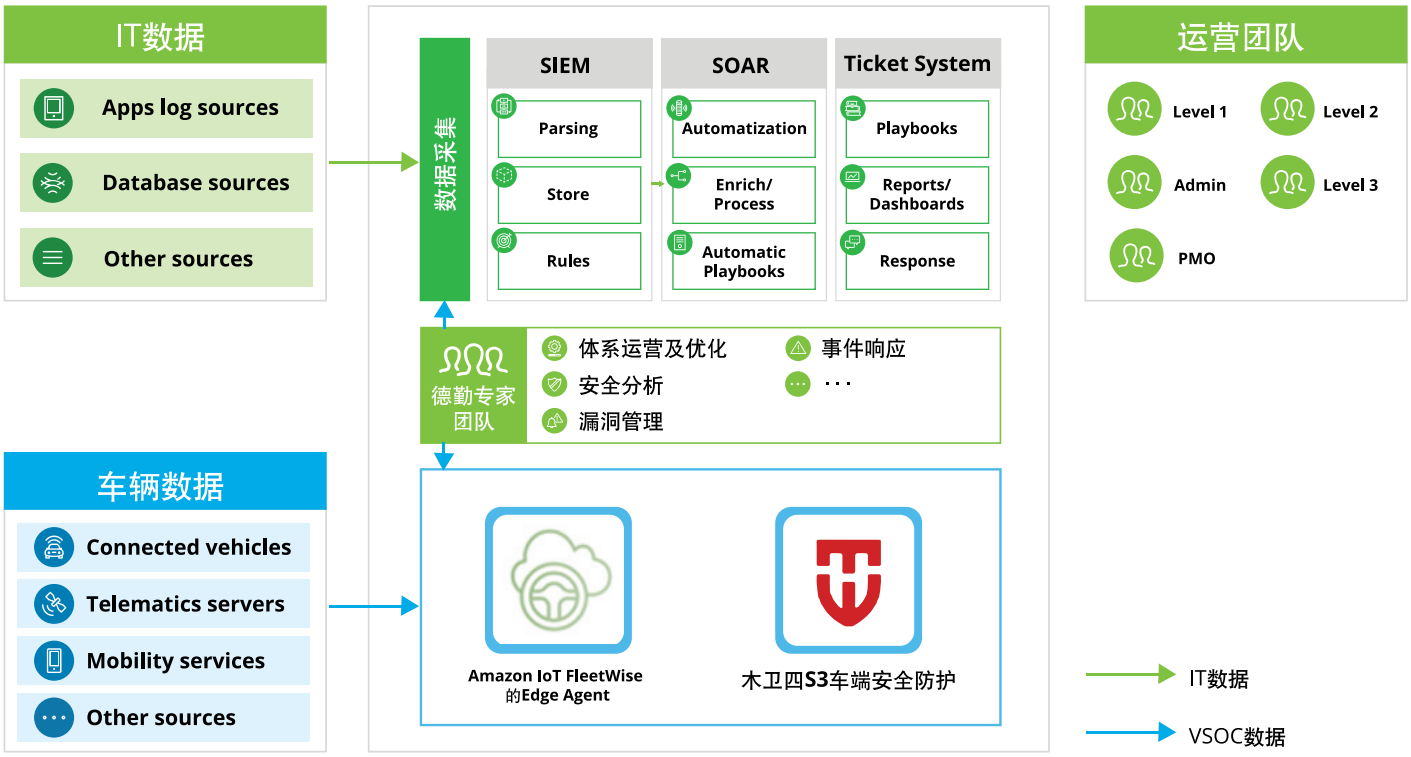
核心共性需求分析：

1. 威胁检测和应对：汽车网络安全运营中心需要实时监测车辆和网络的安全状态，以便及时识别和应对任何潜在的威胁。这包括检测和预防黑客攻击、恶意软件、网络间谍活动和数据盗窃等问题。

2. 漏洞管理和修复：网络安全运营中心还需要对车载系统、软件和硬件进行定期的漏洞检测和修复。这包括对车载系统的所有组件，如操作系统、传感器、通信模块和控制器进行漏洞扫描，以便及时发现和修复任何漏洞。

3. 数据安全和隐私保护：汽车网络安全运营中心需要确保车辆和驾驶员的个人数据得到保护，并且不会被黑客攻击者窃取或滥用。这意味着需要有高效的加密和密钥管理机制，并且需要建立完善的安全政策和操作规程，以确保数据安全和隐私保护。同时，需要建立数据备份和紧急响应计划，以应对任何数据泄露或损失的风险。

联合运营VSOC的数据流



联合解决方案的优势：

1. 全面的技术解决方案：德勤提供安全治理、合规咨询、安全运营顶层架构设计和体系咨询等专业技术，木卫四则提供深度学习和网络安全等人工智能技术，而亚马逊云科技提供基于云计算和大数据的解决方案，使汽车安全运营中心能够提供全面的、高效的技术支持和服务。

2. 强大的数据安全和隐私保护能力：德勤和亚马逊云科技在数据安全和隐私保护合规方面具有丰富的经验和能力，而木卫四在汽车安全能力领域的技术资源和经验，使汽车安全运营中心可以确保数据的安全和保密，同时还可以利用这些数据来提高车辆安全性能。

3. 高效的威胁检测和响应能力：借助德勤的专业咨询团队、木卫四的网络安全人工智能技术和亚马逊云科技的大数据分析能力，汽车安全运营中心可以实现快速准确地检测和识别网络安全威胁，并采取及时和适当的响应和预防措施。

4. 强大的技术和经验支持团队：德勤、木卫四和亚马逊云科技三家公司都拥有雄厚的技术实力和丰富的经验，并且在不同领域具有不同的专业性。这使得汽车安全运营中心可以获得全方位的支持和帮助，可确保其能够持续稳定地运营。

5 VSOC 技术实践

VSOC技术趋势

在基础功能方面，未来的VSOC主要能力包括：

1.安全监测与防御：VSOC通过实时监测车辆网络中的安全事件和威胁，及时发现并采取相应措施进行防御，确保车辆网络的安全性和稳定性。

2.故障诊断与维护：VSOC可以对车辆系统进行全面的监控和诊断，通过数据分析和算法预测，提前发现潜在故障并进行及时维护，降低故障对车辆性能和乘客安全的影响。

3.数据分析与优化：VSOC能够收集、存储和分析海量的车辆数据，通过对数据的挖掘和分析，提供运营效率的优化建议，帮助企业降低成本、提高效益。

在VSOC技术发展方面，将趋向于：

1.云端与边缘结合：未来的VSOC将更多地采用云端和边缘计算相结合的架构，利用云端强大的计算和存储能力，实现对大规模数据的处理和分析，同时将边缘计算应用于车载系统，提高实时性和安全性。

2.人工智能技术应用：人工智能技术将广泛应用于VSOC中，通过机器学习和深度学习等算法，实现对车辆网络安全事件的自动识别和响应，提高安全防御的准确性和效率。

3.合作共享与开放标准：随着智能网联汽车的普及，VSOC的发展也需要加强合作与开放。汽车制造商、技术公司、网络安全专家和政府监管机构等各方需要形成合作共享的生态系统，共同推动VSOC技术的发展。此外，制定统一的开放标准对于实现不同厂商之间的互操作性和数据共享至关重要。这样一来，不同厂商的智能网联汽车可以通过VSOC平台实现安全运营和数据交互，加强整个行业的安全性和可靠性。

VSOC的潜在挑战与应对，主要有：

1. 安全风险与隐私问题：智能网联汽车的VSOC面临着日益复杂的网络安全威胁，如黑客攻击、数据泄露等。因此，VSOC需要不断升级防御能力，并采取加密、身份验证和隐私保护等措施，确保车辆和乘客的安全。

2.技术标准和法规制定：智能网联汽车的VSOC需要建立统一的技术标准和法规框架，以确保不同厂商和地区的智能网联汽车能够实现互联互通。同时，相关政府部门需要加强监管，确保智能网联汽车的安全性和隐私保护。

3.数据管理与分析能力：随着智能网联汽车产生的数据规模不断增加，VSOC需要具备强大的数据管理和分析能力。这涉及数据采集、存储、处理和挖掘等方面，对于VSOC的算法和基础设施提出了更高的要求。

木卫四VSOC整体解决方案

木卫四科技通过云原生技术构建汽车网络安全威胁分析平台 (S3 VSOC) ，利用人工智能技术洞察智能汽车异常和威胁，整合车端数据和云端服务数据，将数据转换成有价值、可操作的预警信息，并联动木卫四汽车威胁情报，以最简化的方式操作S3 VSOC平台，持续监测和发现整个联网车辆生态系统中未知/新型威胁，主动采取有效缓解措施，从而实现云端监控联网汽车的网络安全。VSOC平台作为一种集成了多种功能模块的综合性安全运营平台，旨在帮助OEM及相关企业实现全面的威胁监测和应对能力，保护汽车核心资产和智能网联功能的安全性，符合国家和地区性法规，协助车企提升产品竞争力。以下为木卫四科技针对VSOC平台的方案设计、部署方案和运营要求的整体介绍。

表5：方案设计——VSOC 功能架构设计

<table>
<tr><td>车辆安全运营</td><td colspan="2">资产管理</td><td colspan="2">事件管理</td><td colspan="2">规则管理</td><td colspan="2">响应处置</td><td>报表管理</td><td colspan="2">工单管理</td><td colspan="2">威胁情报</td><td rowspan="2">3D态势大屏</td></tr>
<tr><td rowspan="2">安全事件响应操作台</td><td colspan="4">阻断操作（实时下发）</td><td colspan="5">安全OTA（规定期限）</td><td colspan="4">供应商安全工单(迭代修复)</td><td rowspan="2">VSOC自身安全</td></tr>
<tr><td colspan="4">IP/端口封禁　网络隔离
VSOC-IDPS/防火墙编排联动</td><td colspan="5">安全更新程序　特征库升级
VSOC升级管理启动对接</td><td colspan="4">专家工单　缓解措施库
VSOC缓解知识库威胁公告</td><td rowspan="5">主机安全
权限安全
数据脱敏
系统安全
操作审计</td></tr>
<tr><td rowspan="2">威胁分析和预测中心</td><td colspan="4">历史数据分析</td><td colspan="5">实时数据分析</td><td colspan="4">融合预测分析</td></tr>
<tr><td colspan="4">车辆资产安全管理
规则引擎</td><td colspan="5">风险事件实时告警　异常威胁关联预测
机器学习　知识图谱</td><td colspan="4">操纵行为态势感知
深度学习</td></tr>
<tr><td rowspan="2">数据标准化聚合处理</td><td colspan="4">车端消息数据</td><td colspan="5">云端服务数据</td><td colspan="4">移动应用交互数据</td></tr>
<tr><td colspan="4">威胁信息　远控消息
OTA消息　…</td><td colspan="5">指令中心消息　TSP服务状态数据
…</td><td colspan="4">埋点消息　数字钥匙消息
…</td></tr>
</table>

关于VSOC平台各个功能模块的建设建议：

数据收集：数据收集模块负责从各种来源收集数据，包括日志、事件、网络数据包、安全设备生成的安全数据等。

数据处理：数据处理模块负责处理、解码和转换收集到的数据，以便进行进一步分析和处理。此模块通常包括对数据进行清理、格式化、归一化和去重等操作。

数据丰富：数据丰富模块负责使用各种技术，例如情报共享和威胁情报分析，对收集的数据进行丰富，以获得更全面、更准确的信息。

威胁检测：威胁检测模块负责使用各种技术，例如基于规则、基于车辆行为和机器学习等技术，识别并报告潜在威胁。

事件分类：事件分类模块负责将检测到的事件进行分类，并根据其严重性和优先级进行分类。

分析和评估：分析和评估模块负责对检测到的事件进行进一步分析和评估，以确定其影响和可能性，并制定相应的响应策略。

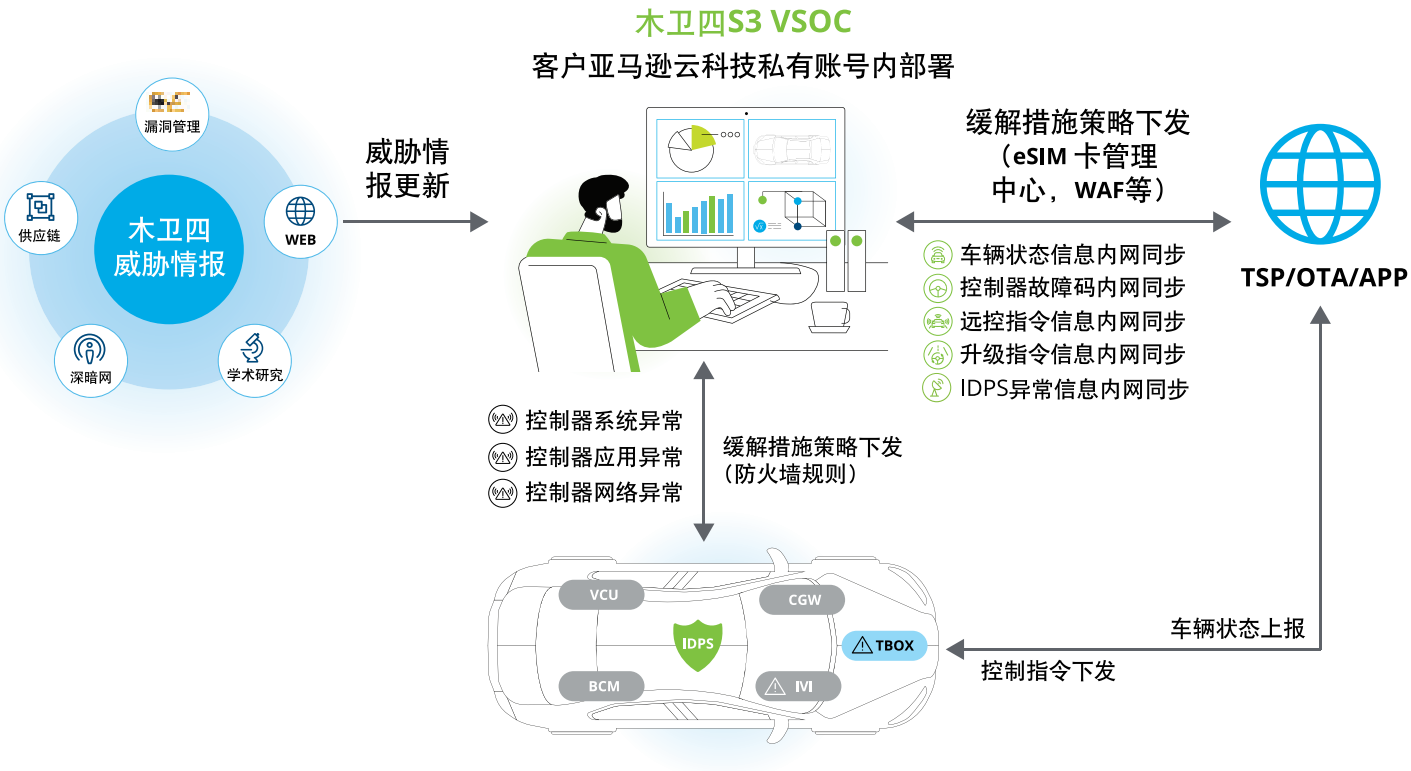
工作流集成：工作流集成模块负责将VSOC平台集成到组织的工作流程中，以确保检测到的事件得到适当的响应和处理。

报告和共享：报告和共享模块负责生成适当的报告和通知，并将其发送给相关的利益相关者。此模块还可以支持安全情报共享和其他协作机制。

部署方案：

木卫四S3 VSOC平台采用私有化部署方式，利用亚马逊云科技的Amazon IoT FleetWise服务与木卫四VSOC Data Adapter（汽车数据统一威胁建模接入系统）结合，从车端实时收集安全分析需要的数据，然后在亚马逊云科技的Amazon EMR服务的支持下进行处理。S3 VSOC TAC（汽车高级威胁分析操作台）和S3 VSOC TPM（汽车威胁和攻击行为预测模型）基于专门针对汽车网络攻击行为的算法模型，借助Amazon SageMaker进行模型的构建、训练和部署，从而训练出高质量的VSOC威胁检测和预测模型。安全运营和可视化系统，基于Amazon EKS将安全预警、分析结果进行统一展示。同时，S3 VSOC联动木卫四威胁情报，为汽车制造商和相关企业提供应对智能出行和联网化服务所产生的新型汽车网络威胁所需的缓解措施，在VSOC平台上实现汽车安全运营的闭环。

木卫四S3 VSOC核心工作流



运营要求：

VSOC是负责监测、评估和响应汽车网络安全事件的运营中心，在汽车安全生态系统中扮演着重要的角色。作为一个综合性的运营中心，VSOC负责收集来自车端ECU和后端云服务的数据，对其进行实时监测和分析，评估潜在的网络安全风险。此外，VSOC还负责快速响应和处置发生的安全事件，确保汽车关键零部件、智能化服务和供应链系统的网络安全，满足国内外汽车网络安全要求，为安全出行保驾护航。针对后期安全运营，建议从以下几方面帮助提高VSOC安全运营的效率和效果：

人员要求：

按照运营中心常任角色，一般分为三级。

初级SOC操作人员：主要从事安全事件监测、告警处理、日志分析等基础工作。

中级SOC操作人员：在初级操作员的基础上，进一步拓展了安全防御能力，能够进行复杂攻击的分析和处理。

高级SOC操作人员：拥有深入的安全知识和多年的SOC实战经验，能够负责整个SOC的运营、维护和管理，同时具备高水平的安全分析和响应能力。

专家SOC操作人员：在汽车安全攻防及安全研究方面，应该具备丰富的经验和技能，能够应对汽车行业内较大的安全攻击事件。熟悉汽车行业的安全漏洞和威胁，并能够迅速响应和应对安全事件。

数据安全合规要求：

车端IDPS数据收集需要考虑是否涉及个人隐私数据，以及敏感数据。如涉及需要满足相关安全法规的协议要求，并向当地检查机构进行报备申请。

对于车企面向跨境数据传输的需求，可通过德勤基于专业的且有实际落地经验和案例提供咨询服务，以确保数据传输的安全性和合规性。

表6：支持国内和海外的安全运营

OEM车厂		木卫四
运营阶段 海外	应遵循相关法规要求部署，例SCC\TIA; 如不数据回传，不用考虑数跨境问题； 遵循本地GDPR安全要求； 数据脱敏等；	配合当地律所机构提供相关材料； 提供属地咨询公司合作； 支持国内外7*24h运营服务； 配合OEM签署相关协议条款；
运营阶段 国内	遵循GDPR安全要求； 涉及数据跨境回传，需要向相关机构申报； 敏感数据需要脱敏； 数据分级分类；	

网络安全合规要求：
对于主机厂：

车型首先满足R155合规，拆解下来需要覆盖CSMS和VTA中涉及到的以下关键内容：

1. 详尽的风险评估（含设计资料），整车及零部件测试报告、缓解措施。

2. 在车辆类型设计中实施适当的网络安全措施。

3. 通过供应链收集和验证R155规定要求的信息，证明已识别和管理了与供应商相关的风险。

4. 检测和响应可能的网络安全攻击。

5. 持续监控，记录数据以支持检测网络攻击，并提供数据取证能力，以便分析尝试或成功的网络攻击。

R155 附录五： 七大威胁场景

对于零部件供应商：

1.建立并运行涵盖车辆及其部件整个生命周期的CSMS。

2. 差距分析，识别和评估网络风险并实施适当的网络安全措施以减轻这些风险。

3. 具备实施工具和系统来支持上述流程和方法，例如网络风险评估工具、安全组件、网络安全测试工具、软件更新交付平台等。

4. 监控和报告网络安全事件和漏洞并采取缓解措施。

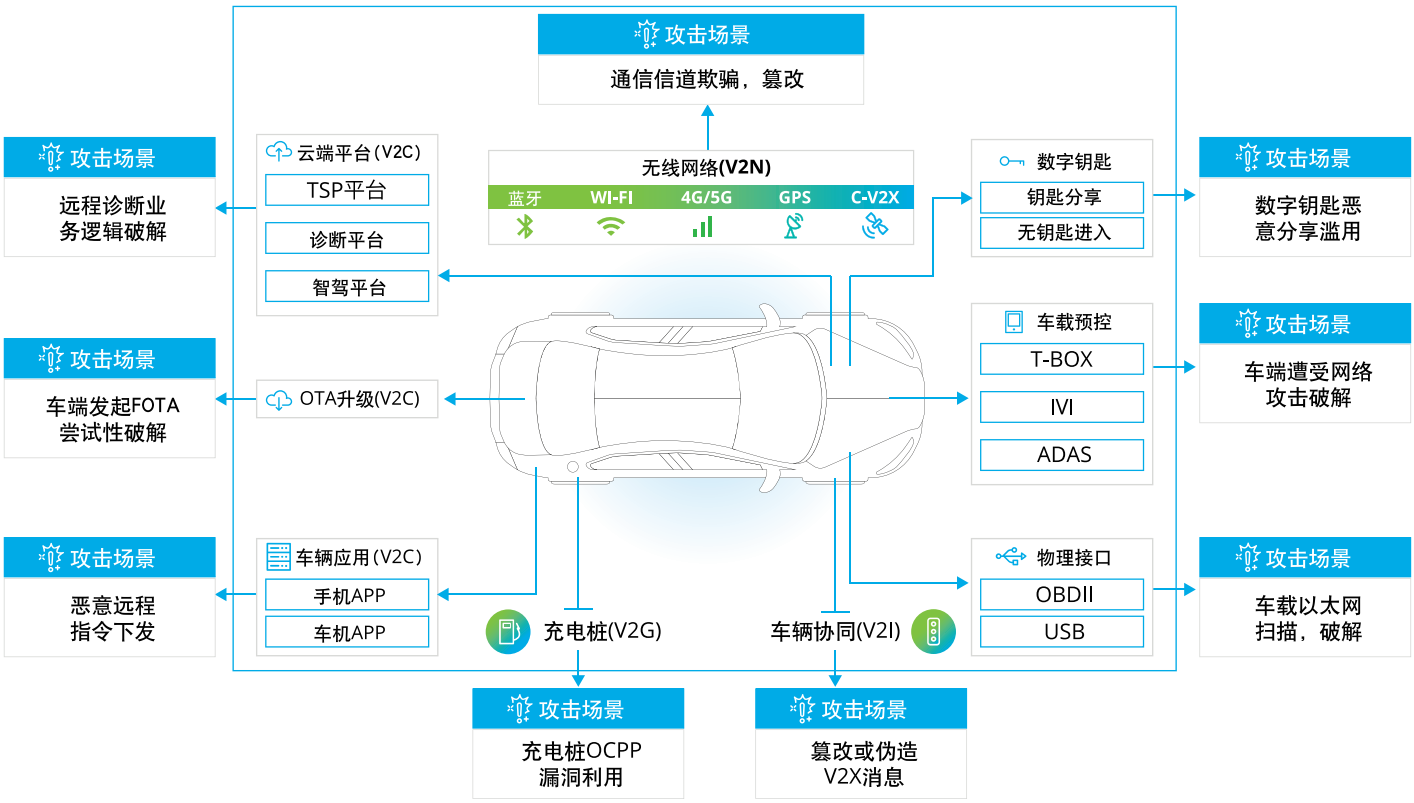
5. 与供应链中的其他利益相关者合作并共享相关的汽车网络安全信息。

6. 确保网络安全活动和决策的可追溯性和记录。

7. 对 CSMS 进行内部审计和管理审查，监控和衡量 CSMS 有效性，并将结果报告给车辆制造商和审批机构。

8. 对员工进行有关法规以及公司政策、流程和方法的培训和教育。

汽车潜在攻击场景



亚马逊云科技将是构建VSOC的重要基础设施

亚马逊云科技作为业界领先的云服务提供商，客户通过互联网平台来订阅其遍布全球的基础设施产品和服务。自2006年创立以来，亚马逊云科技不断创新，目前提供超过200项全功能的服务，涵盖计算、存储、数据库、联网、分析、机器人、机器学习与人工智能、物联网、移动、安全、混合云、虚拟现实与增强现实、媒体，以及应用开发、部署与管理等各个方面。其基础设施遍及32个地理区域（Region）的102个可用区（Availability Zone）。同时已公布计划在加拿大、马来西亚、新西兰和泰国新建4个区域、12个可用区。作为全球云计算的开创者和引领者，亚马逊云科技连续12年被Gartner评为云基础设施和平台服务魔力象限领导者。

亚马逊云科技的区域（Region）由一个地理区域内的多个物理上分隔的可用区（Availability Zone，AZ）组成。每个可用区都有独立的电力、冷却设施，通过冗余的超低延迟网络连接。区域和区域之间，通过冗余的100GbE网络相连接（中国大陆的两个区域互连，但和全球网络没有骨干网连接），因此，单个链路的故障不会影响正常访问。北京区域和宁夏区域是两个位于中国境内提供服务的亚马逊云科技区域。为保证更好的用户体验并遵守中国的法律法规，亚马逊在中国与持有相关电信牌照的本地合作伙伴开展技术合作，并由本地合作伙伴向客户提供云服务。北京光环新网科技股份有限公司，是亚马逊云科技北京区域云的服务运营方和提供方；宁夏西云数据科技有限公司，是亚马逊云科技宁夏区域云的服务运营方和提供方。亚马逊云科技、光环新网和西云数据致力于为中国的软件开发人员和企业提供安全、灵活、可靠且低成本的IT基础设施资源，帮助他们实现创新和快速扩大企业规模。亚马逊云科技中国区域目前提供了大数据、人工智能、物联网等领域涵盖计算、存储、数据库、网络以及安全管理多种云服务，并且还在不断持续扩展中。

亚马逊云科技基础设施区域满足高级别的安全性、合规性和数据保护要求。为了确保客户数据的机密性、完整性和可用性，基础设施实行全天候监控，在数据中心和区域互联的全球网络中，数据在离开安全设施之前，都经过物理层自动加密。在亚马逊云科技上，客户能够完全控制其数据，并对其随时加密、移动以及管理。基于共享责任模式，客户在自己订阅的虚拟环境中，基于亚马逊云科技构建的框架和工具，通过合理配置，能够有效地管理风险。

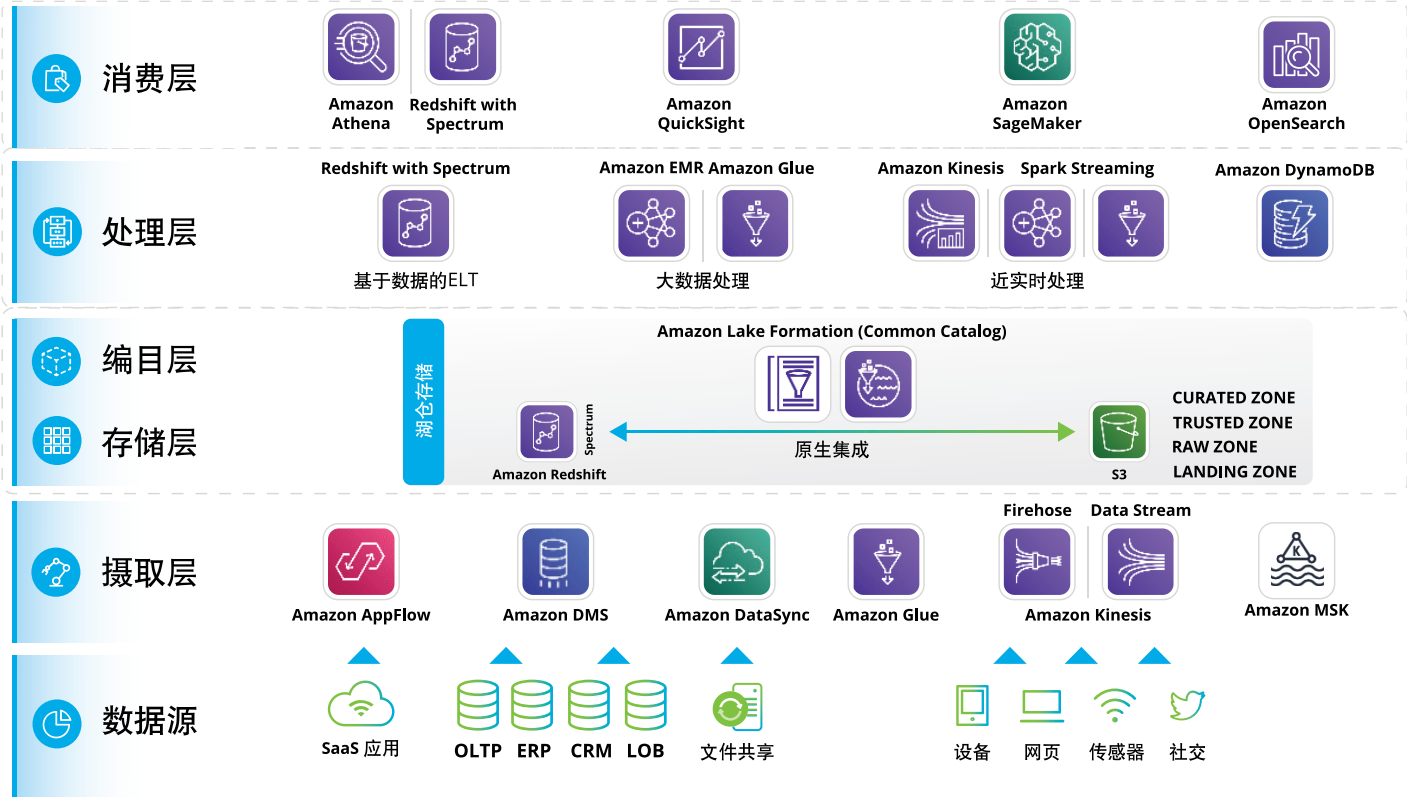
自成立以来，亚马逊云科技，根据客户的需求，不断向用户交付新产品和服务；并根据客户反馈，快速迭代和改进产品和服务。快速的创新节奏和持续的服务改进，让亚马逊云科技始终保持着云计算领导者的地位。如今，越来越多的汽车行业客户选择亚马逊云科技来托管他们的基础设施，不断提高性能、安全性、可靠性和可扩展性。并利用人工智能/机器学习和物联网等新兴技术的数据存储，计算和分析的要求，木卫四VSOC就是利用亚马逊云科技的技术来提升运营质量的典范。

基于亚马逊云科技“智能湖仓”架构对车辆安全数据进行分析

在亚马逊云科技上打造VSOC系统，可以充分利用亚马逊云科技的“智能湖仓”架构，对数据进行分析，以获取洞察。在亚马逊云科技的“智能湖仓”中，数据湖、数据仓库以及人工智能进行了深度的融合，客户能够选择更熟悉的方法，更加简便的方式进行数据分析和机器学习。从而达到真正的敏捷分析和深度智能。

德勤与木卫四联合运营的VSOC基于亚马逊云科技的智能湖仓的架构对车辆数据进行分析，提供安全态势感知，进一步提升了系统的弹性和可靠性。

基于亚马逊云科技“智能湖仓”架构



基于亚马逊云科技的车联网云端安全检测

亚马逊云科技提供很多安全服务，帮助客户实现云端的数据安全，以满足各类数据保护，隐私保护相关的合规。这些服务涵盖数据访问的数据资产识别，保护，检测，自动化及调查响应，持续合规检查及恢复等方面。

这些安全服务共同组成了亚马逊云科技的安全防护，通过将德勤及亚马逊云科技的安全服务和木卫四安全技术通过VSOC进行集成，不但可以对车辆本身的态势进行感知，还可以对基于亚马逊云科技打造的云端车联网后端进行安全感知。

云端安全检测

借助Amazon Fleetwise集成从车到云，云到车的闭环

亚马逊云科技的Amazon IoT FleetWise服务是一项托管服务，可以近乎实时地收集、转换车辆数据并将其传输到云端，用于构建VSOC，为OEM、移动出行公司提供预测、监控和快速响应网络威胁的能力，保护车辆（队）免受网络攻击，这项服务将贯穿车辆（队）的整个生命周期。

Amazon IoT FleetWise 还提供车辆建模框架，可以在云中对车辆及其传感器、执行器进行建模。借助Amazon IoT Fleetwise，甚至可以在云端定义数据收集方案，并将其部署到车端，进而在车端运行的边缘代理软件中使用数据收集方案来指定要收集的数据，以及何时将其传输到云端。客户可以通过配置Amazon IoT FleetWise，或者结合亚马逊云科技的其他相关服务，例如Amazon IAM， Amazon CloudWatch等来实现其自身的安全和合规性目标。

6 智能网联汽车网络安全的趋势与展望

展望2023年，网络安全远不止关乎其背后的技术基础。对许多企业组织来说，网络安全已更加紧密地围绕在日常业务运营和新机遇的碰撞当中，这不仅关乎技术本身，更成为了基础性的常规动作。正如网络威胁从IT问题转变为商业挑战，我们现在也看到了网络安全的定位从基础技术到业务战略的转变，着重为了服务战略业务目标增长而把关最后一公里。大量的企业高层已意识到网络安全与企业影响力之间的紧密关系，可以预见很多企业必将在未来大幅增加网络安全方面的投资。

鉴于网络安全能力建设作为车企运营的关键成功要素已成为行业共识，德勤认为2023年汽车行业需持续关注以下网络安全趋势和方向：

汽车行业正在面对越来越复杂多变的网络安全攻击

随着汽车网联化、智能化转型，行业呈现多样化复杂业态，出行服务提供方、车辆基础设施提供方、金融服务方等都在参与其中，各方提供以数据驱动的各类产品和服务时涉及大量个人信息和重要数据的收集、存储、处理与分享等场景，数据在跨组织，跨平台流动时大大增加了数据外泄，不当使用的安全合规风险，内外部攻击和数据窃取行为屡见不鲜。

汽车行业经历数字化转型和产业链协同变革，大大增加车辆产品和服务遭受外部攻击的暴露面，例如电动车充电基础设施正沦为新型网络攻击的对象；数字化营销平台和移动互联程序漏洞被利用而导致大量个人信息发生数据泄露；以服务导向方式SOA构建的新型应用系统和外部网络API接口可能遭受远程网络攻击等，这些网络攻击将对企业正常运营造成极大干扰，甚至产生影响社会稳定和和人身安全的重大事件。

车企主动采取更积极行动提升网络安全能力

过去几年各类车企已明显加大网络安全合规领域的投入，组建网络安全团队履行法规要求的责任和义务、开展各类安全合规管理和技术落地措施。德勤认为车企在2023年及之后还会进一步、更积极的加大资源投入，包括重新定位网络安全合规组织边界及其职责；网络安全合规人才建设；网络安全合规生态协同等。

联合出品

德勤中国

风险咨询网络安全合伙人：肖腾飞

风险咨询网络安全总监：肖康

风险咨询网络安全副总监：金成

风险咨询网络安全经理：李强

亚马逊云科技

亚马逊云科技大中华区行业方案部高级总监：苏卓

亚马逊云科技大中华区数据产品部高级总监：崔玮

亚马逊云科技大中华区汽车行业首席架构师：许军

亚马逊云科技大中华区合作伙伴架构师：张亮

亚马逊云科技大中华区汽车行业高级架构师：孙健

木卫四科技

木卫四科技创始人兼CEO：云朋

木卫四科技创始人兼CTO：汪明伟

木卫四科技Marketing VP：郭斌

木卫四科技解决方案经理：郭艳

特别鸣谢

德勤风险咨询中国合伙人

薛梓源，冯晔，张震

Designed by CoRe Creative Services. RITM1486629

这是环保纸印刷品