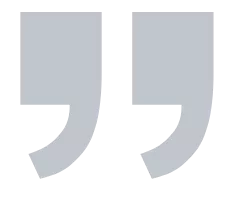
汽车信息安全运营中心-VSOC

**汽车信息安全**

智能网联汽车信息安全从业人员知识分享



随着车联网与智能汽车的快速发展，拥有愈发强大运算能力的现代汽车电子系统在带来高效的工作能力同时，也带来了越来越多可能遭受网络攻击的漏洞。而且，网络黑客的攻击手法正在以惊人的速度超过传统的信息安全保护技术。黑客采用低成本、易于使用和快速发展的工具来攻击他们的物联网目标，而这些目标通常反应缓慢，仅以预防为目标的基本安全为基础进行防御。

开发和实施可靠的网络安全是贯穿全汽车生命周期及汽车行业所面临的一个重大挑战。一个强大的汽车网络安全策略包括：

* 最先进的网络攻击检测手法
* 车辆数据监控
* 建立信息安全事件应急响应体系

# 什么是VSOC

汽车信息安全运营中心，常见的其他说法还有态势感知系统。英文亦有称为A（Automotive）SOC的习惯。以上没有统一标准。

VSOC是为了确保大量车队（Fleet，以下简称“车队”）免受网络攻击而建立的。其需要克服汽车行业特有的挑战:

### 对所有车辆攻击路径的持续可见性

* **近乎实时地检测攻击，并有能力迅速作出反应，消除对整个车队的威胁**

针对网络威胁，OEM需要有能力预防、检测和进行快速响应，以减少对车队、企业组织和制造商品牌的损害。为了实现这一目标，VSOC需要为汽车领域定制的连续监测、调查和分析工具，以及经过适当培训的安全分析人员和制定一整套工作流程。

此外，必须在遵守数据安全/隐私法规的基础上，创建可以监测、汇总和管理大量和不同类型的车队数据，包括个人数据的方法。本文中所介绍的VSOC应为OEM提供一个有效的汽车安全操作框架，旨在为

OEM提供预测、检测和快速响应网络威胁的能力，贯穿车辆（群）的整个生命周期。

本文的目的在于阐述如何建立符合OEM需求的新VSOC体系，检视从概念到落地，涵盖技术，人员及体系流程三方面的需求。

# 需求来源

### 法规

UNR155 (WP29) 要求OEM对车辆（队）的网络安全状况进行持续性的监控，并在网络安全事件发生后的合理时间内做出应对。

在我国，也有尚在制定中的《汽车信息安全应急响应管理指南》，可能会涉及相关的要求。

### 车队规模的网络安全监管

对于OEM来说，实施VSOC的主要原因之一是他们需要了解他们在世界各地所有车辆的网络安全状况。这也是只有VSOC这种模式才能实现的工作。

### 贯穿车辆生命周期的网络安全监管

另一个主要原因是通过产品（这里指车辆）的生命周期进行安全监测和管理。从网络安全的常识来看， 没有永远完美的保护，这就意味着即使是今天的最佳做法，明天可能就不那么有效了。

VSOC在产品的生命周期中提供持续的监控，这意味着新发现的攻击手法可以尽快被捕获，帮助OEM减少损失。

### 一些威胁只能通关分析来自车队的大量数据才能被检测出

尽管根据UNR155法规，车辆上会有一些车载网络安全保护措施，但受制于车辆系统的局限性，并不能检测到所有的威胁。VSOC在实施后端检测机制方面有较少的性能限制，它可以覆盖来自车载解决方案（如车载IDS）的未发现的威胁。然而一个更重要的问题是，一些威胁只能通过车队之间的联系来识别。在现实中，车载解决方案并不支持这一点，因此VSOC有必要覆盖边缘到边缘的威胁。例如，单一的DTC错误报告并不能为识别攻击提供重要依据，但从特定区域的特定船队收到的大量DTC错误报告却可能与网络攻击有关。

### 对一些攻击的溯源只能通过分析相关车队中的类似事件得到结果

不仅需要通过车队规模的分析来识别威胁，而且对攻击的溯源分析有时只能通过分析攻击之间的联系来准确识别。例如，车载IDS可能检测到对主机车辆的CAN总线的攻击，但是它可能没有足够的信息来识别被黑客利用的漏洞在哪里。通过分析不同车辆中相同/相似的攻击，VSOC可以找到攻击之间的共同点，如相同的ECU/软件/EEA等，这可以帮助我们确定这些攻击的源头。

### 一目了然的安全事件管理系统

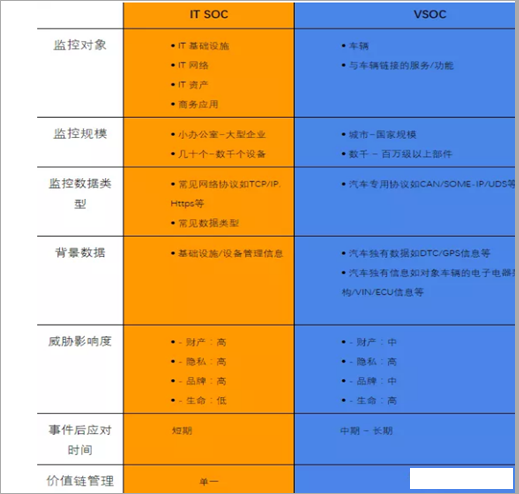
汽车产业拥有现代工业中最复杂的价值链，整个生命周期的安全事件管理并不停留在车辆层面，而是详细到ECU/软件/（程序）库等。

VSOC可以帮助OEM在大规模的情境下下将车辆和ECU/软件之间的关联性联系起来。

# 从IT SOC到VSOC

在通常语境上，SOC常指代IT SOC，负责监控企业的IT基础设施和设备的网络安全状况。毫无疑问， VSOC是SOC在汽车产业的变体，这意味着IT SOC是VSOC的起源。

相比之下IT SOC的历史要长得多，但处理的任务与VSOC完全不同。下表显示了我们发现的IT SOC和VSOC之间的主要区别。



从上表中我们可以看出，IT SOC不能简单地完成VSOC的任务，因为在几个领域中存在着巨大的差距， 特别是:

**完全不同的监控目标**，这也意味着它们中的任何一个都不能轻易取代对方。

**数据类型完全不同**，IT SOC工具不对车辆指定数据进行建模，也不需要处理地理信息。**规模上的巨大差距**，最小的VSOC的规模被认为是一个城市，比企业大得多。

**威胁生命安全**，对企业IT基础设施的网络攻击大多不会威胁到人员生命，而是勒索攻击，例如DDoS。但是，对车辆的攻击会严重危害乘员甚至是周围人员的生命安全，这给厂商带来压力，必须尽快进行缓解。

**极其复杂的价值链管理**，正如上文所说，从一般意义上讲，汽车产业拥有现代工业中最复杂的价值链。不仅如此，对汽车ECU漏洞的管理是与硬件相结合的，而硬件通常不是IT SOC管理的关键部分。

# VSOC架构及核心元素

汽车信息安全运营中心（VSOC）是一个组织内的集中职能部门，涉及操作人员、操作流程和监管技术。VSOC持续监测和改善车队的安全状况，同时预防、检测、分析和应对网络安全事件。

安全运营团队负责监测和保护许多资产，如知识产权、个人数据、业务系统和品牌完整性。作为一个组织的整体网络安全框架的执行部分，安全运营团队在监测、评估和防御网络攻击的协调努力中充当了核心合作点。

# VSOC 监管技术

|  |  |
| --- | --- |
| **核心功能** | **描述** |
| 数据收集 | 从数据源收集数据。 |
| 威胁检测 | 从收集到得数据中检测到威胁（攻击）。 |
| 事件调查 | 对安全事件进行调查，对攻击进行溯源并重建攻击路径。 |
| 事件管理 | 对已确定得安全事件进行管理，并分配缓和工作。 |

**数据收集:** 收集数据是VSOC工作流程的第一步，OEM/供应商可以根据他们的监控目标选择车内数据/车联服务数据/线下数据。但请注意，VSOC只负责针对车辆的攻击有关的数据源，而对IT基础设施的攻击则应由IT SOC处理。

**威胁检测：**VSOC负责从收集的数据中识别安全事件，目标可能是已知的攻击、零日攻击甚至是未知的攻击。

**威胁调查：**VSOC应该为操作人员提供调查攻击的根本原因和重建攻击路径的能力。不是所有的工作都需要通过该工具完成，更多的工作可能需要安全专家在线下进行。

**事件管理：**一旦安全事件被确认，OEM不能对其置之不理，必须贯穿整个价值链进行管理。同事需要针对损害安排缓和计划，但不一定需要通过VSOC系统进行。

# VSOC 操作人员

VSOC由先进的技术和面向汽车的专业流程组成，旨在为OEM提供准确的网络安全事件识别、分析和调查，贯穿整个车队。

SOC通常采用了3个级别的工作组对事件进行检测和响应，以迅速启动事件升级。除了这3个级别外，更高级别的工作（包括对汽车系统、汽车安全和后端IT服务的深入了解，以及对众所周知的漏洞和响应机制的广泛熟悉）可由事件响应研究小组提供，该小组可在事件响应期间根据需要被动员起来提供额外资源。这个事件响应团队应该被定义为SOC的一个可选的4级工作组。

# VSOC 流程

VSOC是集合监测、评估和验证跨车队数据（即从车内组件、车外支持服务和产品后端产生的数据）的工作中心。因此，事件响应程序的效率需要非常高，这一点至关重要。

企业的IT团队拥有并管理其IT资产，而各种安全工具负责验证这些资产是否被正确使用。当一个资产被攻击者破坏时，SOC团队就可以发布一个缓解活动来解决这个威胁。这个过程通常发生在SOC团队内部 的 "短周期 "或与IT部门的共享过程中。

然而，出于两个主要原因，在汽车、IOT和OT SOC团队中通常不是这样的，这两个原因便是**流程**和**第三方供应商**。

许多安全组织缺乏**处理当今网络安全威胁环境所需的流程和先进能力。**而这一过程在汽车领域变得更加复杂，因为OEM通常不是车辆的所有者，因此他们不能强迫消费者安装部件或在发现威胁时将汽车送到修理厂。

使问题更加复杂的是，汽车制造商在很大程度上依赖第三方供应商为其车辆提供系统、软件和硬件组

件。然而，除非汽车制造商对其一级和二级供应商提出严格的网络安全要求，否则他们有可能通过这些组件引入安全漏洞。伪造的组件也可以进入供应链，通过降低磨损等级、超越安全限制等方式威胁到安全。

### 处理信息安全事件的基本流程包括以下步骤：

|  |  |  |  |
| --- | --- | --- | --- |
| **步骤** | **任务** | **描述** | 负责的相关功能 |
| 1 | 原始数据处理 | 源自多个数据源的数据被VSOC工具进行规范化并存储在日志库中。 | 数据收集 |
| 2 | 发送警报 | 当车辆中发生某些网络安全事件时，VSOC会产生警报。 | 威胁检测 |
| 3 | 优先级处理 | 对警报进行分类并根据OEM的规定进行优先级分级（自动或手动）。 | 事件管理 |
| 4 | 遏制过程 | 应该进行适当的事件遏制（如果可能的话）以补救安全事件。这一过程可以是自动的，也可以是手动的。 | 事件管理 |
| 5 | 调查 | 对于每个安全警报，都要进行调查，并将结论交付给任何关联的团队。 | 威胁调查 |
| 6 | 事件后缓和处理 | 在调查之后，应对发现的漏洞进行修复，并（如果可能的话）对车内安全保护进行升级。 | 事件管理 |

下面的结构图说明了一个基本的VSOC的建议设置，请牢记以下原则：

* + 监管技术能够对基于汽车的事件进行检测和适当的反应。
  + SOC操作人员分为三个级别，第四个级别包括外部专家/汽车事件响应者（见SOC操作人员部分）。
  + VSOC应与OEM的IT-SOC对接，以评估和缓解可能影响车辆和企业网络的违规行为。

# 部署VSOC所面对的挑战

毫无疑问，在汽车工业中部署新的解决方案有很多挑战，我们在此提出了一些关键点：

**缺少汽车网络安全知识：**许多IT SOC供应商在尝试提供VSOC服务，但威胁检测、分析和管理的关键部分需要全面的汽车网络安全知识和汽车电子电器系统的相关背景知识，这对IT SOC供应商来说是非常新的领域。

**缺少熟练的操作人员和完善的流程：**虽然VSOC供应商可以提供技术解决方案，但是OEM厂商仍然需要足够和熟练的人力资源来运作VSOC，目前如果不违反OEM的安全政策，委托第三方运作VSOC是一个可行的解决方案。除此之外则需要OEM花费时间来培训他们自己的IT SOC操作员，使其有足够的技能来运作VSOC。

另一方面，VSOC流程需要在部署VSOC之前建立，OEM可以在内部进行，或者委托熟悉法规的咨询公司来帮助建立。

**价值链事件和漏洞管理：**正如我们上面两次提到的，汽车行业拥有最复杂的价值链，IT SOC在规模上相比有很大的差距。尽管如此，在具体操作阶段，OEM必须与他们的供应商的事件管理团队频繁合作。另一方面，管理这些大量复杂的数据也带来了其他的安全/隐私问题，OEM必须考虑到这些问题。

**旧款车辆：**UNR155法规针对有联网功能和自动驾驶功能的车辆，这些车辆能够提供与后台服务器的连接，但它们可能还没有收集车载日志的能力。然而，在法规之外，如果OEM需要监测更早期的旧款车辆， 他们可能需要增加远程数据传输和日志记录功能，更不用说增加日志记录功能可能影响整个车载系统。

**时间紧迫：**最后一点，需要面对欧洲/日本市场的OEM没有太多的时间做准备，因为UNR155将在2022 年7月实施。当然这两地之外也会有相似的法规出台，但简单地说，无论是否有法规要求，由于汽车世界的网络安全风险的现实，OEM事实上没有时间犹豫。

# 当今市场中常见的VSOC部署方案

市场已有多种常见的部署方案，他们各有利弊，需要OEM针对自己的需求进行选择，以下举出三种我们所了解的最常见方案：

**后端安全日志分析工具：**这种最简单的实现方式只提供对已经被车载安全保护（如IDS）检测到的可疑活动的调查和管理。然而，作为车载解决方案，可检测的范围很狭小，换句话说，如果OEM希望有更广泛的可检测范围，那么在可持续的计划中，它可能会消耗OEM更多的成本，因为实施更广泛的车载解决方案从成本上讲非常昂贵的。

**后端 IDS：**具有检测能力的VSOC可以被看作是一个在后端（云端）服务器上的IDS，可支持扩大检测范围，特别是对未知和零日漏洞。然而，它需要收集大量的数据，同样有管理和成本的困难。另外请注意，根据UNR155，拥有后端IDS并不意味着车载保护是不必要的。

混合型后端解决方案。前两种方案的混合体将提供最全面的保护。不管是OEM还是供应商都应该根据具体需求灵活地选择，以提供适应性强、成本效益高的解决方案。