国际电信联盟
电信标准化部门

建议书

# ITU-T X.1382 (03/2023)

X系列：数据网、开放系统通信和安全性

安全应用和服务（2）– 智能交通系统（ITS）安全

# 联网汽车安全威胁信息共享导则

ITU-T X系列建议书

**数据网、开放系统通信和安全性**

| | |
|---|---|
| 公用数据网 | X.1–X.199 |
| 开放系统互连 | X.200–X.299 |
| 网间互通 | X.300–X.399 |
| 消息处理系统 | X.400–X.499 |
| 号码簿 | X.500–X.599 |
| OSI组网和系统概貌 | X.600–X.699 |
| OSI管理 | X.700–X.799 |
| 安全 | X.800–X.849 |
| OSI应用 | X.850–X.899 |
| 开放分布式处理 | X.900–X.999 |
| 信息和网络安全 | |
| 一般安全问题 | X.1000–X.1029 |
| 网络安全 | X.1030–X.1049 |
| 安全管理 | X.1050–X.1069 |
| 生物测定 | X.1080–X.1099 |
| 安全应用和服务（1） | |
| 组播安全 | X.1100–X.1109 |
| 家庭网络安全 | X.1110–X.1119 |
| 移动安全 | X.1120–X.1139 |
| 网页安全（1） | X.1140–X.1149 |
| 安全协议（1） | X.1150–X.1159 |
| 对等网络安全 | X.1160–X.1169 |
| 网络身份安全 | X.1170–X.1179 |
| IPTV安全 | X.1180–X.1199 |
| 网络空间安全 | |
| 网络安全 | X.1200–X.1229 |
| 反垃圾信息 | X.1230–X.1249 |
| 身份管理 | X.1250–X.1279 |
| 安全应用和服务（2） | |
| 应急通信 | X.1300–X.1309 |
| 泛在传感器网络安全 | X.1310–X.1319 |
| 智能电网安全 | X.1330–X.1339 |
| 验证邮件 | X.1340–X.1349 |
| 物联网（IoT）安全 | X.1360–X.1369 |
| **智能交通系统（ITS）安全** | **X.1370–X.1389** |
| 分布式账簿技术（DLT）安全 | X.1400–X.1429 |
| 应用安全（2） | X.1450–X.1459 |
| 网络安全（2） | X.1470–X.1489 |
| 网络安全信息交换 | |
| 网络安全概述 | X.1500–X.1519 |
| 漏洞/状态信息交换 | X.1520–X.1539 |
| 事件/事故/启发式信息交换 | X.1540–X.1549 |
| 政策的交换 | X.1550–X.1559 |
| 启发式和信息请求 | X.1560–X.1569 |
| 标识和发现 | X.1570–X.1579 |
| 确保交换 | X.1580–X.1589 |
| 网络防御 | X.1590–X.1599 |
| 云计算安全 | |
| 云计算安全概述 | X.1600–X.1601 |
| 云计算安全设计 | X.1602–X.1639 |
| 云计算安全最佳做法和指导原则 | X.1640–X.1659 |
| 云计算安全实施方案 | X.1660–X.1679 |
| 其他云计算安全 | X.1680–X.1699 |
| 量子通信 | |
| 术语 | X.1700–X.1701 |
| 量子随机数发生器 | X.1702–X.1709 |
| QKDN安全框架 | X.1710–X.1711 |
| QKDN安全设计 | X.1712–X.1719 |
| QKDN安全技术 | X.1720–X.1729 |
| 数据安全 | |
| 大数据安全 | X.1750–X.1759 |
| 数据保护 | X.1770–X.1789 |
| IMT-2020的安全性 | X.1800–X.1819 |

欲了解更详细信息，请查阅ITU-T建议书目录。

**ITU-T X.1382建议书**

# 联网汽车安全威胁信息共享导则


## 摘要

随着车联网的快速发展，车联网面临的网络安全问题日益突出。联网汽车的安全威胁信息在保护联网汽车方面发挥着不可或缺的作用，可以帮助相关组织识别、评估、监控和响应联网汽车的任何信息。共享联网汽车威胁信息的组织可以改善自身和其他组织的安全状况。

ITU-T X.1382建议书为联网汽车共享安全信息的原则、规则、方法和程序提供了指导。此外，本建议书还简要描述了参与安全威胁信息共享生命周期的各个组织的不同职责范围、角色和有效性。

本建议书旨在帮助相关组织与联网汽车共享社区保持联系，并为支持联网汽车安全保护做法提供威胁信息。总体而言，本建议书旨在加强安全威胁信息共享，减轻网络安全攻击对联网汽车的潜在影响。



## 历史沿革

| 版本 | 建议书 | 批准 | 研究组 | 唯一识别码* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1382 | 2023-03-03 | 17 | 11.1002/1000/15104 |

## 关键词

联网汽车、威胁信息共享


* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

## 前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

## 注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

## 知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联未收到实施本建议书可能需要的受专利/软件版权保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列ITU-T网站查询适当的ITU-T数据库：http://www.itu.int/ITU-T/ipr/。

# 目录

# ITU-T X.1382建议书

# 联网汽车安全威胁信息共享导则

## 1 范围

本建议书的目的是为共享联网汽车生态系统的威胁信息提供指南，所涉内容包括相关组织的角色和合作伙伴关系、共享范围、程序以及共享联网汽车威胁信息的要求。

## 2 参考文件

以下ITU-T建议书和其他本文档中提到的参考文献包含的条款构成了本建议书的条款。所有的建议书和其他参考文献均会得到修订，本建议书的使用者应查证是否有可能使用下列建议书或其他参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

[ITU-T X.1371] ITU-T X.1371建议书（2020年），联网汽车面临的安全威胁。

[NIST SP 800-150] 网络威胁信息共享指南。

## 3 定义

### 3.1 他处定义的术语

本建议书使用了下列他处定义的术语：

**3.1.1 告警（alert）**[NIST SP 800-150]：一个简短且通常是人类可阅读的，关于当前漏洞、弱点和其他安全问题的技术通知。亦称为建议、公报或漏洞说明。

**3.1.2 安全威胁信息（security threat information）**[NIST SP 800-150]：与威胁相关的信息，可能有助于相关组织保护自己免受威胁或检测某一参与方的活动。

**3.1.3 威胁（threat）**[b-ISO/IEC 27000]：能对某个系统或组织造成伤害的有害事件的潜在起因。

### 3.2 本建议书中定义的术语

本建议书定义了下列术语：

**3.2.1 参与方策略（actor tactics）**：对参与方执行某项操作的技术目标的描述。

**3.2.2 参与方的技术（actor techniques）**：描述参与方如何通过执行某一操作实现技术目标。

**3.2.3 参与方的程序（actor procedures）**：对参与方执行特定技术的描述。

## 4 缩写词和首字母缩略语

本建议书使用了下列缩写词和首字母缩略语：

ACL 访问控制列表

APP 应用程序

CERT 计算机应急响应小组

CSIRT 计算机安全事故响应小组

ECU 电子控制单元

GSMA GSM协会

ISAC 信息共享和分析中心

MEC 多址边缘计算

T-BOX 远程信息处理技术盒

TSP 远程信息处理技术服务提供商

TTP 策略、技术和程序

V2X 车联网

## 5 惯例

本建议书使用以下惯例：

关键词“建议”（is recommended）指的是一项建议性的、并非绝对需遵守的要求，因此，宣称遵循本建议书时无需提及该项要求。

## 6 概述

联网汽车威胁信息共享的主要元素包括威胁信息的类型、共享原则、角色、规则、社区和程序。通常，与联网汽车连接的不同组织会生成不同类型的安全威胁信息。不同类型的代理在联网汽车的威胁信息共享活动中扮演不同角色。不同组织间有关联网汽车的威胁信息共享活动需遵循一定的原则、规则和程序，而威胁信息会产生不同效果。不同的组织可以按照一定的共享模式和共享平台组成共享社区。

### 6.1 联网汽车威胁信息的类型

参考[NIST SP 800-150]，联网汽车的威胁信息可分为指标、策略、技术和程序（TTP）、安全告警和威胁情报的报告：

a) 指标是表明攻击即将发生或正在进行的可观测到的迹象。指标可用于检测和应对潜在威胁。联网汽车的一些指标涵盖了可疑的车联网（V2X）攻击者所在的组织。

b) TTP描述参与方的行为。TTP可以描述参与者使用特定恶意软件变体、操作顺序、攻击工具、传送机制或利用系统的偏好。联网汽车面临各种威胁，包括针对后端服务器和服务器的威胁，以及针对车辆通信信道的威胁。TTP可能涵盖操纵车辆功能连接或绕过监控系统的行为，这此威胁与传统的网络威胁不同。

c) 安全告警是关于漏洞、攻击、恶意软件和其他安全问题的技术通知。安全告警通常来自声誉良好的来源，如计算机应急响应小组（CERT）或计算机安全事件响应小组（CSIRT）。当受影响的联网汽车所面临的威胁多种多样或威胁可能造成巨大伤害时，会发出安全告警。

d) 威胁情报报告提供对威胁的深入分析，内容包括事件参与者、目标系统、攻击类型和其他信息，此外还提供减轻威胁的行动建议。威胁情报报告还可以显示威胁的未来发展趋势。威胁情报报告在防止联网汽车遭受新攻击方面发挥着重要作用。

## 6.2 联网汽车共享威胁信息的优势与挑战

凭借联网汽车共享的威胁信息，与联网汽车行业相关的组织可以通过主动利用其合作伙伴的知识、经验和能力来增强其安全态势。联网汽车共享威胁信息的好处包括：

a) 增强相关组织在联网汽车上的防御能力。联网汽车会带来新的威胁，而信息共享可以帮助相关组织提高威胁防御能力。新的漏洞经常被当作主要的攻击工具。威胁信息共享可以及时应对新的漏洞攻击，以提高防御攻击的能力。虽然联网汽车面临许多新攻击，但威胁信息共享有助于应对联网汽车面临的新威胁并提高防御能力。

b) 保持联网汽车生态系统的健康。威胁信息共享有助于提高联网汽车经济环境的安全性，并确保所有联网汽车的生态安全。联网汽车制造链的安全涉及服务提供商、远程信息处理技术服务提供商（TSP）、汽车制造企业、电信运营商、车载及手持终端设备提供商、移动智能终端设备提供商等的安全。

虽然共享威胁信息有益处，但仍存在一些挑战。信息共享的挑战包括：

a) 建立联网汽车共享标准系统的威胁信息。为了保持车联网生态系统的健康，有必要制定一个合理的车联网威胁信息共享标准体系。目前，联网汽车威胁信息共享还没有统一的国际标准体系。如果不建立标准体系，就会阻碍信息共享，最终影响其发展。

注 – 一些导则，如[ITU-T X.1371]和GSMA物联网安全导则[b-GSMA CLP.11]可以提供安全问题的注意事项，作为信息共享的可能最佳做法。

b) 定义威胁信息的范围。车联网产业链由不同的环节组成，每个环节面临不同类型的威胁。需要明确各环节的威胁信息共享，以及环节之间的信息共享方式。

c) 保护敏感和机密信息。共享联网汽车的威胁信息存在敏感信息泄露的风险。加密技术可能会受到破坏或应用得不充分。加密技术使用不充分也可能导致密钥和/或证书的泄露。

此外，使用已损坏和过时的加密技术会增加信息泄露的风险。受保护的敏感信息包括车辆的版权或专有软件；所有者的私人信息，例如个人身份、支付账户信息、地址簿信息、位置信息和车辆电子标识符、密钥等等。此外，未经授权的组织不得访问机密信息。对于某组织而言，获取和维护持续访问机密信息源所需的许可既昂贵又耗时。

# 7 联网汽车共享威胁信息的原则

为了确保威胁信息共享和传输过程的有效性、准确性和安全性，相关组织和企业有必要遵循一些原则。

## 7.1 互惠

安全威胁信息共享的本质是通过协同努力，增强网络安全对联网汽车的防护能力。建议联网汽车安全威胁信息共享的参与方了解威胁信息共享活动中各方的相互权利、义务和责任。除了接收与自身组织相关的威胁信息，还建议相关组织积极贡献自己的力量，实现互利共赢。

## 7.2 分类和归类

不同的组织在安全威胁信息共享过程中扮演不同的角色。某些威胁信息对不同组织的意义和重要性似乎不同。建议相关组织对联网汽车的威胁信息进行分类和归类，并定义有效范

围。此外，建议根据类别、分类和范围标签建立不同级别的管理系统。建议使用适当的加密技术保持敏感信息的机密性、完整性和/或真实性。

### 7.3 数据安全

威胁信息数据的非法使用、窃取和篡改以及未授权用户访问等问题严重影响了数据共享方共享情报的主动性，降低了情报共享活动的安全性和有效性。为此，共享风险的控制也是共享威胁信息的重点所在。包括加密、共享数据脱敏、识别与销毁等在内的对策，可为与联网汽车安全威胁信息相关的数据提供有效保护。

## 8 组织、作用和伙伴关系

### 8.1 组织及其作用

#### 8.1.1 汽车制造商

汽车制造商在联网汽车的威胁信息共享活动中发挥着最重要的作用，因为汽车制造商直接与用户互动，对其车辆的安全负责。

通过从自己的生产系统、车载组件和联网汽车基础设施中收集数据，汽车制造商收集、整合、生成并分析与联网汽车相关的安全威胁信息，同时采取措施以减轻威胁。

#### 8.1.2 供应商

供应商为联网汽车提供车载硬件或软件，包括车辆芯片、远程信息处理技术盒（T-BOX）设备和内部/外部网关。供应商收集和接收与其产品相关的安全威胁信息，并协助协调小组、汽车制造商和其他相关方减轻威胁和/或防止和减少与其产品相关的安全事故。

#### 8.1.3 第三方产品和服务提供商

第三方产品和服务提供商主要是指除汽车制造商及其零部件供应商之外，提供与联网汽车相关的独立产品和服务的机构，如TSP、云计算服务提供商、硬件厂商、移动终端制造商、车辆保险服务提供商、其他第三方服务平台运营商等。

第三方产品和服务提供商收集/制作/共享其产品或服务平台上的安全威胁信息，如联网汽车的故障、未经授权的用户行为或远程攻击的威胁信息，并协助相关方（如联网汽车协调组和汽车制造商）减轻威胁和/或处理联网汽车的安全事件。云计算服务提供商还负责共享信息，包括错误配置或错误、滥用控制端口、不当凭证管理、云数据泄漏等。

#### 8.1.4 协调组

联网汽车协调组通常作为独立实体工作，专注于安全威胁信息和事件响应的协调，如CERT/CSIRT和Auto-ISAC。

联网汽车协调组协助相关方跨组织协调安全威胁的信息共享，并为相关方提供通知和预警服务。

#### 8.1.5 电信运营商

电信运营商为联网汽车提供基础电信服务。

电信运营商确保核心网络、基站、MEC平台等电信网络基础设施的安全。

注 – 作为联网车辆背景下电信运营商的一个示例，可以考虑网络运营商GSMA导则[b-GSMA CLP.14]。

### 8.1.6 网络安全服务供应商

网络安全服务供应商是提供网络安全产品或服务的车辆企业和组织中涉及网络的公司或组织。

网络安全服务供应商通过安全设备、终端软件和互联网等来源，协助相关组织收集、整合和分析联网汽车的安全威胁信息，并提供安全支持和服务，以预防和减少安全事件。

## 8.2 在组织间共享的范围

建议相关组织定义信息共享活动的范围，包括确定可以共享的威胁信息的类型、允许开展威胁信息共享活动的情况，以及联网汽车威胁信息共享的优先级。

信息共享活动的广度会因组织的资源和能力而异。针对不同类型组织，联网汽车共享威胁信息的范围各不相同。例如，网络安全供应商、汽车制造商、V2X设备提供商、通信设备提供商和电信运营商等的范围就各不相同。建议资源有限的联网汽车相关威胁信息的生成方专注于规模较小的威胁生成/收集活动，这些活动为相关组织及其共享合作伙伴提供更高价值的威胁信息。某组织或可扩大共享威胁信息的范围，作为额外的能力和资源。拥有更多资源和高级功能的组织可能会选择更大的初始范围，从而通过更广泛的威胁信息共享活动支持实现其目标和目的。

表1介绍了哪些组织会受[ITU-T X.1371]定义的各种威胁的影响。

**表1 – 受联网汽车各种威胁类型影响的不同组织的对照图**

| 威胁的类型 | 共享威胁信息的组织 | | | | | |
|---|---|---|---|---|---|---|
| | 汽车<br>制造商 | 供应商 | 第三方产品和<br>服务提供商 | 协调组 | 电信运营商 | 网络安全<br>服务供应商 |
| 车辆在后端服务器面临的威胁 | ✓ | | ✓ | ✓ | | ✓ |
| 车辆在通信信道面临的威胁 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 车辆在更新程序面临的威胁 | ✓ | | ✓ | ✓ | | ✓ |
| 车辆在不经意人类行为方面面临的威胁 | ✓ | ✓ | ✓ | | | |
| 车辆在外部连通与连接方面面临的威胁 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 攻击的潜在目标或动机 | ✓ | ✓ | ✓ | ✓ | | ✓ |
| 潜在漏洞 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

## 8.3 组织间的信息共享规则

基于联网汽车威胁信息的特征和分类，组织间威胁信息共享的规则可描述如下：

a) 建议相关组织共享联网汽车的威胁信息。

b) 联网汽车威胁信息共享的对象通常为联网汽车管理平台、共享出行服务的提供商、车辆制造企业、V2X设备提供商、通信设备提供商和电信运营商。

c) 许多组织，如汽车制造商和网络安全供应商，同时扮演着威胁信息提供者和消费者的角色。

d) 建议威胁信息提供者要有专业性。

e) 建议采用威胁信息筛选和订阅验证等管理要求。

### 8.4 建立共享社区

建议建立一个社区，以共享和分析联网汽车的威胁信息。威胁信息共享模型包括对等型、源与用户型以及轴辐型[b-OASIS TAXII]。通过共享社区，相关组织可以接收联网汽车的实时网络威胁和漏洞数据。下面以2015年汽车企业成立的Auto-ISAC为例。重点是与越来越多的智能车辆建立信息共享社区。Auto-ISAC的门户网站允许其成员匿名提交和接收信息，并帮助成员更有效地应对网络威胁。Auto-ISAC一直在积极推动供应商、商用车公司和汽车制造商在汽车网络安全领域的合作和信息共享。附录一介绍了Auto-ISAC的威胁信息共享活动。

一个共享社区可以设置多个共享子社区，相关组织可以选择加入一个或多个与联网汽车相关的子社区。建议共享社区为开放社区，允许不同组织通过自愿合作的方式自由加入和退出。在选择加入子社区时，建议相关组织选择联网汽车威胁信息资源互补的社区。各组织自愿向共享社区发布联网汽车威胁信息，并负责确保提供给社区的威胁信息适合共享。

## 9 共享联网汽车威胁信息的程序和指南

### 9.1 引言

[ITU-T X.1371]定义并描述了联网汽车的威胁。相关组织可利用内部资源检测、分析和处理安全威胁，亦可通过建立跨组织共享框架共享威胁信息。在跨组织共享过程中，相关组织可以：

a) 获取和使用外部威胁信息，以防止并减轻联网汽车面临的威胁。

b) 与其他组织一起生成并提供联网汽车威胁信息，以增强车辆生态系统的安全性。

根据威胁信息传输链的态势，相关组织可分为两种类型：消费者和威胁信息提供者。许多组织（如汽车制造商和网络安全供应商）通常同时扮演威胁信息提供者和威胁信息消费者的角色。

### 9.2 威胁信息共享活动的程序

消费者是联网汽车威胁的潜在受害者。通过获取和使用威胁信息，消费者可以快速找到受影响的资产，并采取必要对策以减轻威胁。在所有相关组织中，汽车制造商是主要的威胁信息消费者。针对消费者的程序包括五个阶段：

a) 准备：制定适当的机制，为参与威胁信息共享活动做好准备；

b) 接收：接收外部威胁信息；

c) 分析：对接收到的威胁信息进行分析；

d) 缓解：根据分析结果采取措施缓解威胁；

e) 预防：采取行动防止未来发生威胁事件。

威胁信息提供者是车辆生态系统中具有技术能力、分析能力和共享意图的实体。通常，威胁信息提供者还需要使用安全威胁信息，因为生成/收集威胁信息需要多个来源，其中包括接收到的威胁信息。威胁信息提供者的工作程序包括三个阶段：

a) 准备：制定适当的机制，为参与威胁信息共享活动做好准备；

b) 分析：进行分析以生成高质量的威胁信息；

c) 共享：将生成的威胁信息共享给相关方。

## 9.3 程序各阶段的指导

### 9.3.1 为作为消费者的组织提供指导

#### 9.3.1.1 准备阶段的指导

建议相关组织制定联网汽车的安全威胁信息政策，包括设定目标、定义范围和建立决策流程。指导内容如下：

a) 设定目标：相关组织需要注意他们面临的安全威胁。基于对组织安全威胁的分析，建议相关组织设立安全目标，以增强其安全防护能力。

b) 定义范围：结合组织的安全目标、技术能力、财务预算以及各种威胁对组织的潜在影响，建议组织定义其所需威胁信息的范围并确定优先级。

c) 建立决策流程：建议根据组织所需威胁信息的类型和优先级确定决策所需时间，避免决策流程过长对威胁信息的及时处置产生影响。

#### 9.3.1.2 接收阶段的指导

指导内容如下：

a) 建议相关组织正确存储共享的安全威胁信息。

b) 建议相关组织采取措施确保威胁信息存储的安全性。

c) 建议相关组织清除过时和无用的威胁信息。

#### 9.3.1.3 分析阶段的指导

指导内容如下：

a) 建议相关组织评估威胁信息的价值。附录二显示了评估威胁信息价值的参考方法。建议开展自动评估。

b) 建议相关组织验证并进行分析，以评估对其产品和服务的潜在损害。

c) 建议相关组织分析背景，以识别攻击者、TTP和目标等信息。

d) 建议相关组织确定受影响的资产，如服务器、域、电子控制单元（ECU）、系统等。

e) 建议相关组织在安全的环境中进行筛选、验证和分析，以避免对组织的关键系统造成影响。

#### 9.3.1.4 缓解阶段的指导

指导内容如下：

a) 建议相关组织根据威胁信息和分析结果制定处理方案并实施处理流程。解决方案包括隔离受影响的硬件、安装补丁、更新软件、修改配置等。

b) 如果组织缺乏处理能力，建议相关组织联系相关车辆协调组并寻求帮助。

c) 对于指标，建议相关组织将收到的指标应用到网络安全设备上。

d) 对于合法用户通过修改配置和传播恶意程序带来的安全威胁，建议相关组织立即开展分析并加强管理。组织可以通过使用获取的威胁信息（包括处置措施）修复和管理网络中可被利用的漏洞、缺陷或不正确的配置。

#### 9.3.1.5 预防阶段的指导

建议相关组织继续监控其产品和服务。

### 9.3.2 为作为威胁信息提供者的组织提供指导

#### 9.3.2.1 准备阶段的指导

建议相关组织制定政策，包括设定目标、定义范围和建立决策过程。指导内容如下：

a) 建议相关组织建立响应管理流程，以防止重要数据泄露。

b) 建议各组织部署必要的资源和工具，以生成指标和其他威胁数据。

c) 建议相关组织对多源异构网络威胁数据进行识别、评估和分类，以确保所有与威胁相关的信息得到充分描述并随时更新。

d) 建议相关组织建立或加入一个共享社区，通过购买/接收非公开情报和收集公开情报获取数据，根据一些应用场景和业务需求分析这些数据，然后生成相应的威胁情报。在共享的框架下，共享社区根据实际需要整合所有成员共享的威胁信息，产生更有针对性、更完整、更准确的威胁情报，并根据情报的类型和价值，以开源或付费销售的形式共享。

e) 建议相关组织定义信息共享活动的范围，包括定义要共享的威胁信息，决定交换的形式。

#### 9.3.2.2 分析阶段的指导

指导内容如下：

a) 建议相关组织自动或手动筛选告警日志，以删除无价值的告警甚至错误告警。

b) 建议相关组织评估共享信息的价值，并确定共享组织的范围。

c) 建议相关组织定义不同网络威胁场景的可观测性及其相关元数据，然后对这些威胁特征指标的比较结果进行分析和处理。

#### 9.3.2.3 共享阶段的指导

指导内容如下：

a) 建议相关组织按照定义的范围进行威胁信息共享。

b) 建议相关组织以标准化格式提供安全威胁信息。

c) 建议相关组织提供更多背景信息。

d) 建议相关组织制定共享模式和机制，解决情报交换共享的有效性和交易的公平性问题。

e) 随着行业发展需要，建议建立联网汽车威胁信息共享交换平台，进行信息共享。

f) 建议相关组织建立威胁信息数据共享的控制机制，包括共享数据的脱敏、认证和销毁。

g) 建议相关组织凭借生成联网汽车威胁信息的能力，与声誉良好的组织共享威胁信息。

# 附录一

## Auto-ISAC威胁信息共享活动的最佳做法

（此附录不构成本建议书不可分割的组成部分）

汽车信息共享和分析中心[b-AUTO-ISAC]于2019年发布了最佳做法指南“与适当的第三方合作和接触”1.3版。在本最佳做法指南中，Auto-ISAC提供了信息共享的最佳做法，其中包括相关第三方、开放程度、有助于共享的内容以及信息共享流程等。

为增强车辆网络安全，这些组织可能会在联网汽车生态系统中与多种类型的第三方合作和接触。相关第三方包括行业合作伙伴、行业组织、政府、学术界、研究人员和媒体。

相关组织可以根据各自的车辆网络安全目标和自身特有的风险状况确定适当的开放级别。开放程度可分为有限、适度和广泛。

不同利益攸关方之间共享信息的关键流程包括：

a) 识别有助于分享的内容。

b) 让合适的内部利益攸关方参与进来。

c) 创建接收和处理共享信息的流程。

d) 创建向外部第三方推送信息的流程。

e) 获得适当的工具和技术。

# 附录二

## 评估威胁信息价值的方法

（此附录不构成本建议书不可分割的组成部分）

在评估每种威胁信息的价值时，相关组织可以通过下面列出的五项因素进行评估：

a) 威胁源的信誉：威胁源的信誉是不同的。可信度高的来源可以提供更有价值的威胁信息。

b) 及时性：威胁信息有时效性。及早提供的信息可以帮助组织保护和防止对其资产的攻击。

c) 描述的完整性：通常描述更详细和有背景资料的威胁信息更有价值。

d) 与组织的相关性和影响：一些威胁信息针对特定行业、特定产品甚至特定公司。需要特别注意与组织有关的威胁信息。

e) 威胁信息的有效性：多种资源导致威胁信息存在重复和冲突，合并相似的威胁并确定其真实性可以提高组织使用威胁信息的效率。

# 参考文献


[b-AUTO-ISAC] *Collaboration and Engagement with Appropriate Third Parties Best Practice Guide, Version 1.3, 2019.*

[b-ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology -- Security techniques -- Information security management systems – Overview and vocabulary.*

[b-GSMA CLP.11] GSMA CLP.11 (2020), *IoT Security Guidelines Overview Document, Version 2.2.*

[b-GSMA CLP.14] GSMA CLP.14 (2020), *IoT Security Guidelines for Network Operators, Version 2.2.*

[b-OASIS TAXII] *OASIS Committee Specification, TAXII™ Version 2.1*.

## ITU-T 建议书系列

| | |
|---|---|
| 系列 A | ITU-T 工作的组织 |
| 系列 D | 资费及结算原则和国际电信/ICT 的经济和政策问题 |
| 系列 E | 综合网络运行、电话业务、业务运行和人为因素 |
| 系列 F | 非话电信业务 |
| 系列 G | 传输系统和媒介、数字系统和网络 |
| 系列 H | 视听及多媒体系统 |
| 系列 I | 综合业务数字网 |
| 系列 J | 有线网络和电视、声音节目及其他多媒体信号的传输 |
| 系列 K | 干扰的防护 |
| 系列 L | 环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护 |
| 系列 M | 电信管理，包括 TMN 和网络维护 |
| 系列 N | 维护：国际声音节目和电视传输电路 |
| 系列 O | 测量设备的技术规范 |
| 系列 P | 电话传输质量、电话设施及本地线路网络 |
| 系列 Q | 交换和信令，以及相关联的测量和测试 |
| 系列 R | 电报传输 |
| 系列 S | 电报业务终端设备 |
| 系列 T | 远程信息处理业务的终端设备 |
| 系列 U | 电报交换 |
| 系列 V | 电话网上的数据通信 |
| **系列 X** | **数据网、开放系统通信和安全性** |
| 系列 Y | 全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市 |
| 系列 Z | 用于电信系统的语言和一般软件问题 |

瑞士印刷
2023年，日内瓦