极牛网络安全通讯 • 社群期刊

2024 年 9 月 第 39 期

网安观察



P13
阴影之下：揭示API威胁的攻击趋势

P26 汽车行业成API风险高地，数据安全亟待加强

P36 世界主要国家跨境数据流动的政策法规及启示

P42 AI语言模型应用中的数据安全挑战与应对策略

第39期

2024年9月

CONTEN

目录



安全态势

P4 | 国家金监总局印发《关于加强银行业保险业移动互联网应用程序管理的通知》
P4 | 国家网信办《人工智能生成合成内容标识办法》公开征求意见
P5 | 《网络安全技术 网络身份认证公共服务应用接入规范》等 4 项国家标准公开征求意见
P5 | 工信部印发《关于推进移动物联网“万物智联”发展的通知》
P6 | 工信部《电子认证服务管理办法》修订版公开征求意见
P6 | 李强主持召开国务院常务会议，审议通过《网络数据安全管理条例（草案）》
P7 | 强制性国家标准《汽车整车信息安全技术要求》正式发布
P7 | 欧洲委员会发布《人工智能与人权、民主和法治框架公约》
P8 | 九国网络安全机构联合发布《事件日志记录和威胁检测最佳实践指南》
P8 | 美国海军部发布《信息优势愿景》2.0 版
P9 | 美国 AI 医疗公司服务器配置错误，泄露 5.3TB 心理健康记录
P9 | 网络攻击影响国家金融稳定！伊朗被迫支付超 2000 万元赎金
P10 | 全球石油巨头哈里伯顿因网络攻击被迫关闭系统
P10 | 美国知名军工芯片厂商因网络攻击生产能力受损
Ivanti Endpoint Manager 反序列化远程代码执行漏
P11 | 洞安全风险通告
P11 | GitLab 身份认证绕过漏洞安全风险通告
P11 | 微软 9 月补丁日多个产品安全漏洞风险通告
P12 | Apache OFBiz 远程代码执行漏洞安全风险通告
P12 | Apache OFBiz 服务端请求伪造漏洞安全风险通告
P12 | Windows TCP/IP IPv6 远程拒绝服务 / 代码执行漏洞 PoC 已公开风险通告



国际视野

P9 网络攻击影响国家金融稳定！伊朗被迫支付超 2000 万元赎金

ONTENTS



P13
阴影之下：揭示API威胁的攻击趋势

专题报道

P19
《黑神话：悟空》发行平台遭DDoS 攻击细节

P26
汽车行业成API风险高地，智能网联车数据安全亟待加强

P42
AI 语言模型应用中的 数据安全挑战与应对策略



第 3 9 期

《网安观察》编辑部

主办　极牛网

总　　编　　辑：陈鑫杰
总　　顾　　问：叶绍琛
副　　总　　编：王文彦
威胁情报主编：陈艇鑫
移动安全主编：蔡国兆
网安人才主编：林俊濠
涉网犯罪主编：胡铭凯
网安产业主编：张九史
网安态势主编：郑泽彬

公众号　小程序　网站

电子版请访问 www.geeknb.com 阅读或下载索阅、投稿、建议和意见反馈，请联系极牛网期刊编辑部。

E m a i l：hi@geeknb.com
地　　址：深圳市龙岗区天安云谷2栋2层
邮　　编：518000
电　　话：0755-33228862

印刷数量：1000 本
印刷单位：深圳彩虹印刷有限公司

版权所有 ©2021 极牛网，保留一切权利。
非经极牛网书面同意，任何单位和个人不得擅自摘抄、复制本资料内容的部分或全部，并不得以任何形式传播。

无担保声明
本资料内容仅供参考，均“如是”提供，除非适用法要求，极牛网对本资料所有内容不提供任何明示或暗示的保证，包括但不限于适销性或者适用于某一特定目的的保证。在法律允许的范围内，极牛网在任何情况下都不对因使用本资料任何内容而产生的任何特殊的、附带的、间接的、继发性的损害进行赔偿，也不对任何利润、数据、商誉或预期节约的损失进行赔偿。



政策篇

国内，人工智能安全、数据安全、汽车信息安全等领域纷纷推进。网信办就《人工智能生成合成内容标识办法》《网络安全技术 人工智能生成合成内容标识方法》征求意见，国常会审议通过《网络数据安全管理条例（草案）》，强制性国家标准《汽车整车信息安全技术要求》正式发布；

国际上，AI 安全亦备受关注。欧洲委员会发布全球首部具有法律约束力的 AI 公约，美国加州议会通过“业界争议巨大”的人工智能法案，澳大利亚工业、科学和资源部发布自愿性人工智能安全标准等。

国内

国家金监总局印发《关于加强银行业保险业移动互联网应用程序管理的通知》

9 月 14 日，国家金融监管总局印发了《关于加强银行业保险业移动互联网应用程序管理的通知》。该文件从四方面提出 18 条工作要求。一是加强统筹管理，要求金融机构明确移动应用管理牵头部门、建立移动应用台账、完善准入退出机制、控制移动应用数量；二是加强全生命周期管理，要求金融机构规范移动应用的需求分析、设计开发、测试验证、上架发布、监控运行等环节，强化移动应用与运行环境的兼容性、适配性管理；三是落实风险管理责任，要求金融机构落实移动应用备案、网络安全、数据安全、外包管理、业务连续性及个人信息保护等监管要求；四是加强监督管理，要求金融监管总局各级派出机构加强移动应用监管工作。

国家网信办《人工智能生成合成内容标识办法》公开征求意见

9 月 14 日，国家互联网信息办公室起草了《人工智能生成合成内容标识办法（征求意见稿）》，现公开征求意见。该文件提出，人工智能生成合成内容标识包括显式标识和隐式标识。该文件要求，服务提供者提供生成合成内容下载、复制、导出等方式时，应当确保文件中含有满足要求的显式标识。如用户需要服务提供者提供没有添加显式标识的生成合成内容，可在通过用户协议明确用户的标识义务和使用责任后，提供不含显式标识的生成合成内容，并留存相关日志不少于六个月。

强制性国家标准《网络安全技术 人工智能生成合成内容标识方法》公开征求意见

9 月 14 日，中央网络安全和信息化委员会办公室已组织完成了《网络安全技术 人工智能生成合成内容标识方法》国家标准的征求意见稿，现公开征求意见。该文件描述了人工智能生成合成内容显式标识和隐式标识的方法，适用于规范生成合成服务提供者和内容传播服务提供者，对人工智能生成合成内容开展的标识活动。

九部门联合发布《关于智慧口岸建设的指导意见》

9 月 13 日，海关总署、国家发展改革委、工业和信息化部、财政部、交通运输部、国家移民局、国家铁路局、中国民航局、国铁集团联合印发《关于智慧口岸建设的指导意见》。该文件共 7 章 17 条，其中第 16 条提出强化安全运行和客户服务，包括落实国家网络和数据安全管理要求，推进可信环境下的隐私计算技术应用，完善联合运维保障机制，提升故障快速响应处置能力，确保系统安全、稳定、高效运行。

《网络安全技术 网络身份认证公共服务应用接入规范》等 4 项国家标准公开征求意见

9 月 12 日，全国网络安全标准化技术委员会归口的《网络安全技术 网络身份认证公共服务应用接入规范》等 4 项国家标准现已形成标准征求意见稿，现公开征求意见。其他 3 项标准包括《网络安全技术 公钥基础设施 时间戳规范》《网络安全技术 公钥基础设施 PKI 组件最小互操作规范》《网络安全技术 公钥基础设施证书管理协议》。

工信部印发《关于推进移动物联网“万物智联”发展的通知》

9 月 11 日，工业和信息化部印发《关于推进移动物联网“万物智联”发展的通知》。该文件共 6 节 13 条，其中第 10 条提出完善安全保护机制，包括基础电信企业要强化移动物联网安全防护能力建设，不断深化移动物联网安全风险评估。加强物联网卡安全管理，严格落实物联网卡安全管控措施，提升物联网模组、终端等设备安全性。加强数据分类分级保护，引导数据处理者加强数据安全防护和风险监测预警能力建设，定期开展数据安全风险评估，不断提升数据安全保护水平。立足国家安全，科学规划物联网网络建设和业务发展，规范落实“三同步”要求。

国家密码管理局发布《电子政务电子认证服务管理办法》

9 月 10 日，《电子政务电子认证服务管理办法》（以下简称《办法》）已于 2024 年 8 月 26 日国家密码管理局局务会议审议通过，现予公布，自 2024 年 11 月 1 日起施行。《办法》共 6 章 42 条，包括总则、资质认定、行为规范、监督管理、法律责任和附则。《办法》对电子政务电子认证服务的业务规则、服务内容、证书内容、证书申请、使用密码安全与互信互认、保密义务、信息保存、合规性评估、投诉处理、岗位培训及业务终止与承接等提出了一系列规范要求。同时，为保护政务活动敏感信息和数据安全，《办法》明确要求外商投资电子政务电子认证服务，应当依法进行外商投资安全审查。

《粤港澳大湾区（内地、澳门）个人信息跨境流动标准合同实施指引》发布

9 月 10 日，国家互联网信息办公室与澳门特别行政区政府经济及科技发展局、澳门特别行政区政府个人资料保护局共同制定《粤港澳大湾区（内地、澳门）个人信息跨境流动标准合同实施指引》，现予公布。粤港澳大湾区个人信息处理者及接收方可以按照该文件要求，通过订立标准合同的方式进行粤港澳大湾区内内地和澳门之间的个人信息跨境流动。被相关部门、地区告知或者公开发布为重要数据的个人信息除外。

全国网安标委发布《人工智能安全治理框架》1.0 版

9 月 9 日，全国网络安全标准化技术委员会发布《人工智能安全治理框架》1.0 版（以下简称《框架》）。《框架》以鼓励人工智能创新发展为第一要务，以有效防范化解人工智能安全风险为出发点和落脚点，提出了包容审慎、确保安全，风险导向、敏捷治理，技管结合、协同应对，开放合作、共治共享等人工智能安全治理的原则。《框架》按照风险管理的理念，紧密结合人工智能技术特性，分析人工智能风险来源和表现形式，针对模型算法安全、数据安全和系统安全等内生安全风险和网络域、现实域、认知域、伦理域等应用安全风险，提出相应技术应对和综合防治措施，以及人工智能安全开发应用指引。

十一部门发布《关于推动新型信息基础设施协调发展有关事项的通知》

9 月 4 日，工业和信息化部、中央网信办、教育部、财政部、自然资源部、住房城乡建设部、农业农村部、国家卫生健康委、中国人民银行、国务院国资委、中国国家铁路集团有限公司等十一部门联合印发《关于推动新型信息基础设施协调发展有关事项的通知》，以推动新型信息基础设施，跨区域、跨网络、跨行业协同建设为重点方向，提出了“1 统筹 6 协调”等 7 方面主要工作，即全国统筹布局、跨网络协调、发展与安全协调等。该文件单章要求增强全方位安全保障能力，包

括提升网络和数据安全保障能力，增强跨行业安全服务赋能，增强信息基础设施稳定安全运行能力。

工信部《电子认证服务管理办法》修订版公开征求意见

9 月 2 日，工业和信息化部修订了《电子认证服务管理办法》，现予以公示征求意见。该文件共 7 章 56 条，包括总则、资质认定、行为规范、监督管理、投诉举报、跨境互认、附则。据介绍，此次修订一方面是解决部分电子认证服务机构“持证不经营”、服务不合规等问题，另一方面是引导电子认证服务行业高质量发展。

李强主持召开国务院常务会议，审议通过《网络数据安全管理条例（草案）》

8 月 30 日，国务院总理李强 8 月 30 日主持召开国务院常务会议，审议通过《网络数据安全管理条例（草案）》。会议指出，要对网络数据实行分类分级保护，明确各类主体责任，落实网络数据安全保障措施。要厘清安全边界，保障数据依法有序自由流动，为促进数字经济高质量发展、推动科技创新和产业创新营造良好环境。

《网络安全技术 网络安全试验平台 体系架构》等 3 项国家标准公开征求意见

8 月 30 日，全国网络安全标准化技术委员会归口的《网络安全技术 网络安全试验平台 体系架构》等 3 项国家标准现已形成标准征求意见稿，公开征求意见。据悉，《网络安全技术 网络安全试验平台 体系架构》给出了网络安全试验平台的参考体系架构，包括总体架构、组件功能和安全性设计，并提供组件间工作过程参考；《网络安全技术 网络空间安全图谱要素表示要求》规定了网络空间安全图谱要素分类、代码与图形符号表达；《数据安全技术 二手电子产品信息清除技术要求》规定了二手电子产品信息清除各个环节应遵循的技术要求。

国家标准《网络安全技术 网络安全 第 7 部分：网络虚拟化安全》公开征求意见

8 月 29 日，全国网络安全标准化技术委员会归口的国家标准《网络安全技术 网络安全 第 7 部分：网络虚拟化安全》现已形成标准征求意见稿，公开征求意见。该文件旨在识别网络虚拟化安全风险，并为网络虚拟化的安全实施提供指引。总体上，本文件目标在于为组织虚拟化安全的全面定义和实施提供帮助，适用于负责实施和维护安全虚拟化环境并进行相应技术控制的用户和实施者。

工信部、国家标准委联合印发《物联网标准体系建设指南（2024 版）》

8 月 26 日，工业和信息化部、国家标准化管理委员会联合印发《物联网标准体系建设指南（2024 版）》。该文件提出，物联网标准体系框架由基础标准、技术标准、建设运维标准、应用标准四大类组成。其中，基础标准包含安全可信分类，用于规范物联网终端、网络、平台（系统）、网关等关键构成部分的安全、可信要求及保障措施，包括物联网安全架构、安全分级、终端安全、传输安全、数据安全、平台（系统）安全、安全管理等标准，以及物联网可信架构、可信分级、身份可信、数据可信、系统可信等标准。

旅游行业标准《旅游大数据安全与隐私保护要求》公开征求意见

8 月 9 日，全国旅游标准化技术委员会组织编制了《旅游大数据安全与隐私保护要求（征求意见稿）》，现公开征求意见。该文件规定了旅游大数据的通用安全目标、安全与隐私保护生命周期管理、安全与隐私保护运维管理、安全与隐私保护监控管理，以及典型旅游应用场景大数据安全等方面的内容。该文件适用于旅游管理和服务机构开展旅游大数据收集、传输、存储、提供与公开、使用与加工、退役等过程中的安全管理组织、人员安全管理、相关系统建设等，也可为有关部门对旅游大数据相关活动进行监管管理提供参考。

强制性国家标准《汽车整车信息安全技术要求》正式发布

8 月 23 日，由工业和信息化部归口的强制性国家标准《汽车整车信息安全技术要求》正式发布，于 2026 年 1 月 1 日起实施。该标准文本目前尚未公布，根据此前的征求意见稿，该标准规定了汽车信息安全管理体系要求、车辆信息安全一般要求、车辆信息安全技术要求、审核评估及测试验证方法，适用于 M 类、N 类及至少装有 1 个电子控制单元的 O 类车辆，其他类型车辆可参考执行。

国际

欧洲委员会发布《人工智能与人权、民主和法治框架公约》

9 月 5 日，欧洲委员会宣布《人工智能与人权、民主和法治框架公约》（以下简称《AI 公约》）正式向全球各国开放签署，这是该领域全球首部具有法律约束力的公约。《AI 公约》共 8 章 36 个条款，为 AI 规定了一系列原则，包括保护隐私和个人数据、平等和非歧视、不损害人的尊严和自主等，并要求签署国对 AI 产生的任何有害和歧视性结果负责，并要求 AI 侵权的受害者拥有法律追索权。《AI 公约》由欧洲委员会牵头制定，46 个欧盟成员国与美英澳等 11 个非成员国参与了讨论过程，目前欧盟、英国、美国、以色列等 10 个国家和组织已正式签署，其他国家均可加入签署。

澳大利亚工业、科学和资源部发布自愿性人工智能安全标准

9 月 5 日，澳大利亚工业、科学和资源部（DISR）发布自愿性人工智能安全标准，为该国所有组织建立了一套统一的实践，以确保安全和负责任地开发和部署人工智能。该文件共 10 条内容，包括建立、实施和发布问责流程；建立和实施风险管理流程，以识别和降低风险；保护 AI 系统并实施数据治理措施，以管理数据质量和来源；测试 AI 模型和系统，以评估模型性能并在部署后监控系统；使人工控制或干预 AI 系统以实现有意义的人工监督；告知最终用户支持 AI 的决策、与 AI 的交互及 AI 生成的内容；为受 AI 系统影响的人们建立流程，以质疑其使用或结果；对 AI 供应链中的其他组织保持数据、模型和系统的透明性，以帮助他们有效应对风险；保存和维护记录，以便第三方评估对护栏的遵守情况；让利益相关者参与进来，评估其需求和情况，重点关注安全、多样性、包容性和公平性。

美国白宫网络总监办公室发布《增强互联网路由安全路线图》

9 月 3 日，美国白宫网络总监办公室发布《增强互联网路由安全路线图》，旨在解决边界网关协议（BGP）的安全漏洞。该文件建议采用资源公钥基础设施（RPKI）方案来缓解 BGP 缺乏安全验证机制的问题，目前欧洲的 RPKI 采用率较高，而美国采用率较低，仅 39%。该文件提出了一系列建议行动，包括提供采用协议模版，设立公私合作的利益相关者工作组，制定采用框架等，以提高联邦政府及关键基础设施的 RPKI 采用度。

韩国政府发布 2024 版国家网络安全战略实施计划

9 月 1 日，韩国国家安保室发布了由韩国国家情报院、外交部、国防部、科学技术信息通信部、大检察厅和警察厅等 14 个政府部门和机构联合制定的《韩国国家网络安全基本计划》。该计划是韩国政府 2 月 1 日公布的《韩国国家网络安全战略》的后续措施，包括落实该战略五大战略任务的具体实施措施，共计包含 100 项行动任务，其中 14 个部委分别承担 93 项单独任务和 7 项联合任务。五大战略任务包括加强进攻性网络防御活动、建立全球网络合作框架、提高关键基础设施的网络弹性、确保关键和新兴技术的竞争优势、强化运营基础。

美国加州议会通过人工智能法案

8 月 28 日，美国加利福尼亚州议会通过了《前沿人工智

能模型安全创新法案》（编号 SB 1047），下一步将提交至州长审议。该法案旨在为训练成本超过 1 亿美元或者达到一定算力的开发商制定安全标准，确保大规模人工智能模型的安全开发。法案要求对先进人工智能模型进行安全测试，确保该技术不会造成“严重伤害”，并要求开发人员设置终止开关，赋予州检察长在开发商不遵守规定时提起诉讼的权力等。该法案部分条款引发了科技公司和立法者之间关于“扼杀创新”的激烈争论。

九国网络安全机构联合发布《事件日志记录和威胁检测最佳实践指南》

8 月 21 日，澳大利亚、美国等五眼联盟国家及日本、韩国、新加坡、荷兰九国网络安全机构联合发布《事件日志记录和威胁检测最佳实践指南》，针对恶意攻击者常使用的离地攻击手法（如无文件攻击），给出了事件记录的最佳实践，以捕获高质量的安全日志，帮助网络防御者正确识别安全事件。该指南适用于 IT、OT 环境，可作为关键基础设施提供商的参考指南。

美国海军部发布《信息优势愿景》2.0 版

8 月 15 日，美国海军部发布《信息优势愿景 2.0》，对 2020 年发布的首个信息优势愿景进行更新，强调向“以数据为中心”“数据优先”机构的转变，并明确数据管理的重要性，旨在指导海军的 IT 发展规划，将海军部转变为一个数据运转更加流畅的现代化组织，从而在执行作战和商业任务时能够更加快速高效地生成和使用数据。该文件要求构建一个以保密数据为中心的生态系统，以实现更广泛、更安全地机密信息共享能力，包括与海军以外的授权用户共享；基于零信任原则实施支持所有涉密数据的单一结构；加快美军和任务伙伴对不同分类数据的访问速度，以提高美军决策优势。

美国联邦航空管理局发布《人工智能安全保障路线图》

7 月 25 日，美国联邦航空管理局发布《人工智能安全保障路线图》第一版，概述了如何将人工智能技术安全整合至航空领域的方法。该文件提出，在现有航空生态系统内运行、聚焦安全保证和安全增强、避免拟人化、采取渐进式方法等 7 项指导原则，协作、监管人员准备、确保 AI 安全、利用 AI 提高安全性、航空安全研究等 5 项关键领域行动计划。该文件要求，在近期研究人工智能风险建模、异常行为监测、软件运行时保障、软件验证、系统安全审查等一系列项目。

美国 NIST 正式发布首批 3 项后量子加密标准

8 月 13 日，美国 NIST 正式发布首批 3 项后量子密码标准，以应对即将到来的量子威胁。3 项标准分别如下：ML-KEM（基于 CRYSTALS-Kyber）是基于模块格的密钥封装机制，速度很快，适用于快速加密操作，如安全访问网站；ML-DSA（基于 CRYSTALS-Dilithium）是用于数字签名的标准，能够确保文件或软件在传输过程中的完整性和真实性；SLH-DSA（基于 SPHINCS+）也是一种数字签名标准，但其安全性更强，代价是需要更大的签名或更长的签名生成时间。

美国议员提出《联邦承包商网络安全漏洞消减法案》

8 月 9 日，美国民主党参议员 Mark R. Warner 和共和党参议员 James Lankford 联合推出一项立法提案《联邦承包商网络安全漏洞消减法案》，旨在加强联邦承包商的漏洞披露规则。该立法提案要求美国联邦和国防供应商全部强制实施漏洞披露政策（VDP），执行和联邦机构一致的漏洞披露要求，以实现漏洞消减目标。对于实施漏洞披露政策的组织，研究人员如在这些组织的软件产品中发现漏洞，将有途径进行报告，以便在漏洞被利用进行攻击之前进行处理。参议员们认为，接收漏洞报告能够让开发人员和服务提供商意识到问题。目前，美国要求联邦民事行政部门实施漏洞披露政策，联邦承包商却不受约束。



事件篇

网络攻击破坏社会功能稳定性，银行、机场、工厂等均受到影响。伊朗遭遇大规模网络攻击，银行系统瘫痪、数据泄露影响金融稳定，该国被迫支付赎金；美国超级机场遭网络攻击致使 IT 系统瘫痪、航班延误；美国一军工芯片厂商因网络攻击生产能力受损。

美国 AI 医疗公司服务器配置错误，泄露 5.3TB 心理健康记录

9 月 6 日 vpnMentor 消息，美国人工智能医疗公司 Confidant Health 的服务器配置错误，泄露了 5.3TB 的敏感心理健康记录，其中包括个人信息、心理评估和医疗信息等，对患者构成严重的隐私风险。vpnMentor 网络安全研究员 Jeremiah Fowler 发现了一个未受密码保护的服务器，其中包含来自 Confidant Health 的机密记录，Jeremiah Fowler 通过博客文章披露了这一发现。Confidant Health 为美国康涅狄格州、佛罗里达州、新罕布什尔州、德克萨斯州和弗吉尼亚州的居民提供心理健康和成瘾治疗服务。

网络攻击影响国家金融稳定！伊朗被迫支付超 2000 万元赎金

9 月 4 日 Politico 消息，多位知情人士透露，8 月伊朗遭遇的大规模网络攻击，导致银行系统稳定性受到威胁，伊朗被迫支付了数百万美元赎金以平息事态。伊朗 IT 厂商 Tosan 8 月向一个匿名黑客组织支付了至少 300 万美元（约合人民币 2130 万元）赎金，以阻止该组织泄露多达 20 家国内银行的个人账户数据。加密货币情报厂商 Chainalysis 表示，涉事钱包已收到至少 2 个不同伊朗交易所的付款，这与受害者的付款可能一致。这次攻击被认为是伊朗史上最严重的网络安全事件之一。据称，曾多次攻击伊朗企业的黑客组织 IRLeaks 对此次事件负责。

网络攻击迫使美国超级机场 IT 系统瘫痪、航班延误

8 月 26 日 Bleeping Computer 消息，美国西北太平洋沿岸地区最繁忙的机场西雅图 – 塔科马国际机场确认，日前出现的 IT 系统中断可能是由网络攻击引起，这一中断扰乱了预订和登机手续系统，并导致航班延误。西雅图港 8 月 24 日警告称，港口和塔科马机场因为“可能的网络攻击”正在遭受持续中断。为了控制影响范围，他们被迫隔离某些关键系统。西雅图港在推特上表示：“西雅图港，包括西雅图 – 塔科马机场，正在经历互联网和网络系统中断，这影响了机场的某些系统。我们建议乘客与航空公司联系，以获取航班的最新信息。有机场乘客报告称，由于多家航空公司手工签发机票，旅客排起了长队。当地媒体报道，“数千”名旅客受到影响。据悉，航站楼的显示屏也遇到了技术问题，进一步加剧了混乱。

马来西亚国家基建公司遭勒索攻击 疑泄露超 300GB 数据

8 月 26 日 FMT 消息，马来西亚公共交通服务商国家基建公司（Prasarana Malaysia Berhad）确认，社交媒体上关于其内部系统部分被未经授权访问的网络安全事件的报道属实。该公司声明称，此次事件并未影响其日常运营，公司正与网络安全专家合作，调查并缓解这一情况，但并未透露是否有泄漏数据的情况。这份声明意在回应社交媒体关于其网站可能因勒索软件攻击而导致 316GB 数据泄露的报道。8 月 25 日夜间，网络安全平台 Falcon Feeds.io 在推特上发帖称， RansomHub 勒索软件组织威胁将在 6 到 7 天内

公布国家基建公司的数据。

全球石油巨头哈里伯顿因网络攻击被迫关闭系统

8 月 24 日 The Record 消息，美国油田巨头哈里伯顿（Halliburton）22 日提交 SEC 报告披露，21 日遭遇了一次网络攻击，影响了休斯敦总部的运营。该公司表示黑客“获取了部分系统的访问权限”。哈里伯顿副总裁 Charles Geer 表示：“公司采取了多项应对措施。为了保护某些系统，我们选择将其主动下线，并通知执法部门。公司正在实施的调查和应对措施包括系统恢复和事件严重性评估。”据路透社报道称，作为网络攻击后的预防措施，哈里伯顿告知一些员工不要连接公司的内部网络。

美国知名军工芯片厂商因网络攻击生产能力受损

8 月 21 日 The Register 消息，美国半导体制造公司微芯科技（Microchip Technology）通过 SEC 文件披露，“未经授权的第三方破坏了公司对某些服务器的使用，以及部分业务操作。”该公司在 8 月 17 日检测到可能涉及其信息技术系统的可疑活动。随后展开调查，19 日调查结果确认存在未经授权的访问。该公司采取了隔离相关系统、关闭其他系统等多项措施，并聘请了外部网络安全顾问来确定问题范围。“由于该事件，公司某些制造设施的运营低于正常水平，公司目前履行订单的能力受到影响。”文件没有提及事件原因、对芯片制造商造成的破坏程度、是否涉及勒索软件。微芯科技的产品被设计用于军事关键任务，常用于汽车、飞机、导弹等高速移动的设备，或在恶劣的偏远地区运行的设备。

国内某上市公司疑遭勒索攻击泄漏 2.3TB 数据

8 月 20 日 GoUpSec 消息，据 FalconFeeds、Ransomlook 等多家威胁情报平台报道，某 A 股上市建筑公司某集团疑似发生大规模数据泄漏，勒索软件组织 The Ransom House Group 在数据泄漏论坛发帖，称窃取了该公司 2.3TB 数据，并宣称如果未来 2~3 天内不支付赎金将撕票（公布数据）。此次针对某集团的攻击事件未得到官方确认，也未公布具体被窃数据的种类和数量，但报道该事件的威胁情报平台预计可能涉及公司内部敏感信息。RansomHouse 是近年来新兴的数据勒索团伙之一，自 2021 年末开始活跃，曾成功攻击过包括半导体巨头 AMD、非洲零售巨头 Shoprite 在内的多家大型公司。

伊朗遭遇大规模网络攻击，银行系统瘫痪

8 月 15 日财联社消息，伊朗央行和该国多家银行 14 日遭受了一次重大网络攻击，导致伊朗银行系统大面积中断。初步评估表明，这可能是针对伊朗国家基础设施的最大网络攻击之一。据悉，黑客还窃取了伊朗多家银行客户的信息。此次网络攻击正值中东地缘政治风险加剧之际，因此受到了高度关注。很多伊朗人认为，此次网络攻击是以色列情报部门实施的，然而这些指控并没有实质性证据。以色列媒体也报道了针对伊朗银行系统的重大网络攻击，但伊朗官方至今尚未证实这一消息，该国媒体也保持了沉默。

巴黎奥运会期间共发生超 140 起网络攻击事件

8 月 14 日法新社消息，法国当局表示，在巴黎奥运会期间，共报告了超过 140 起网络攻击，但均未对比赛造成干扰。在奥运会筹备期间和整个比赛期间，法国的网络安全机构一直保持高度警戒，防范可能破坏组委会、票务或交通的攻击。从 7 月 26 日到 8 月 11 日，法国政府网络安全机构 ANSSI 记录了 119 起影响较低的“安全事件”，以及 22 起“恶意行为者”成功攻击受害者信息系统的事件。该机构表示，这些攻击主要针对政府实体及体育、交通和电信基础设施。根据 ANSSI 的数据，三分之一的事件是宕机事件，其中一半是通过拒绝服务攻击压垮服务器造成的。其他网络事件则与既遂或未遂系统入侵和数据泄露等相关。



漏洞篇

Windows TCP/IP IPv6 组件曝出严重漏洞(CVE-2024-38063)，攻击者可通过向使用 Windows 的设备发送特制 IPv6 数据包，在无需用户交互或身份验证情况下实现远程代码执行，并进一步控制设备。该漏洞影响所有已启用 IPv6 协议的 Windows 操作系统。该漏洞被微软标记较大可能被利用，目前奇安信威胁情报中心已成功复现该漏洞，强烈建议用户马上安装补丁。

Ivanti Endpoint Manager 反序列化远程代码执行漏洞安全风险通告

9 月 13 日，奇安信 CERT 监测到 Ivanti Endpoint Manager 反序列化远程代码执行漏洞(CVE-2024-29847)在互联网上公开，在 Ivanti EPM 的代理门户中，存在一个反序列化未受信任数据的安全漏洞。该漏洞允许远程未经身份验证的攻击者执行远程代码，从而控制受影响的系统，造成敏感信息泄露甚至获取系统权限等危害。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

GitLab 身份认证绕过漏洞安全风险通告

9 月 12 日，奇安信 CERT 监测到官方修复 GitLab 身份认证绕过漏洞(CVE-2024-6678)，攻击者可以在某些情况下以其他用户的身份触发 pipeline，从而造成身份验证绕过。奇安信鹰图资产测绘平台数据显示，该漏洞关联的国内风险资产总数为 1,256,109 个，关联 IP 总数为 24,463 个。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

微软 9 月补丁日多个产品安全漏洞风险通告

9 月 11 日，微软共发布了 79 个漏洞的补丁程序，修复了 Windows Win32k、Windows Installer、Microsoft SharePoint Server 和 Microsoft Publisher 等产品中的漏洞。经研判，以下 27 个重要漏洞值得关注(包括 7 个紧急漏洞、19 个重要漏洞、1 个中等)，如下表所示。鉴于这些漏洞危害较大，建议客户尽快安装更新补丁。

编号	漏洞名称	风险等级	公开状态	利用可能
CVE-2024-43491	Microsoft Windows 更新远程代码执行漏洞	紧急	未公开	在野利用
CVE-2024-38217	Windows Web 查询标记安全功能绕过漏洞	重要	已公开	在野利用
CVE-2024-38226	Microsoft Publisher 安全功能绕过漏洞	重要	未公开	在野利用
CVE-2024-38014	Windows Installer 权限提升漏洞	重要	未公开	在野利用
CVE-2024-43464	Microsoft SharePoint Server 远程代码执行漏洞	紧急	未公开	较大
CVE-2024-38018	Microsoft SharePoint Server 远程代码执行漏洞	紧急	未公开	较大
CVE-2024-38119	Windows 网络地址转换(NAT)远程代码执行漏洞	紧急	未公开	较小
CVE-2024-38194	Azure Web 应用权限提升漏洞	紧急	未公开	较小
CVE-2024-38220	Azure Stack Hub 权限提升漏洞	紧急	未公开	较小
CVE-2024-38216	Azure Stack Hub 权限提升漏洞	紧急	未公开	较小
CVE-2024-38246	Win32k 权限提升漏洞	重要	未公开	较大
CVE-2024-38243	内核流式处理服务驱动程序权限提升漏洞	重要	未公开	较大
CVE-2024-38237	Kernel Streaming WOW Thunk 服务驱动程序权限提升漏洞	重要	未公开	较大
CVE-2024-38249	Windows 图形组件权限提升漏洞	重要	未公开	较大
CVE-2024-43461	Windows MSHTML Platform 欺骗漏洞	重要	未公开	较大

CVE-2024-43457	Windows 安装和部署权限提升漏洞	重要	未公开	较大
CVE-2024-38247 CVE-2024-38245 CVE-2024-38244	Windows 图形组件权限提升漏洞	重要	未公开	较大
CVE-2024-38238	内核流式处理服务驱动程序权限提升漏洞	重要	未公开	较大
CVE-2024-38228	Microsoft SharePoint Server 远程代码执行漏洞	重要	未公开	较大
CVE-2024-38227	Microsoft SharePoint Server 远程代码执行漏洞	重要	未公开	较大
CVE-2024-38253	Windows Win32 内核子系统权限提升漏洞	重要	未公开	较大
CVE-2024-38252	Windows Win32 内核子系统权限提升漏洞	重要	未公开	较大
CVE-2024-38242	内核流式处理服务驱动程序代码执行漏洞	重要	未公开	较大
CVE-2024-38241	内核流式处理服务驱动程序权限提升漏洞	重要	未公开	较大
CVE-2024-43487	Windows Web 查询标记安全功能绕过漏洞	中	未公开	较大

Apache OFBiz 远程代码执行漏洞安全风险通告

9 月 6 日，奇安信 CERT 监测到官方修复 Apache OFBiz 远程代码执行漏洞 (CVE-2024-45195)，Apache OFBiz 存在远程代码执行漏洞，远程攻击者可通过控制请求从而写入恶意文件获取服务器权限。目前该漏洞技术细节与 PoC 已在互联网上公开，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Apache OFBiz 服务端请求伪造漏洞安全风险通告

9 月 4 日，奇安信 CERT 监测到官方修复 Apache OFBiz 服务端请求伪造漏洞 (CVE-2024-45507)，该漏洞是由于 Apache OFBiz 在从 Groovy 加载文件时对 URL 的验证不足，导致远程攻击者可以通过服务器端请求伪造的方式向任意系统发起请求，并可能导致远程代码执行，成功利用此漏洞可允许攻击者完全控制受影响的系统，包括访问敏感数据、执行任意命令或进行进一步的网络攻击。目前该漏洞技术细节与 PoC 已在互联网上公开，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Jenkins Remoting 任意文件读取漏洞安全风险通告

9 月 3 日，奇安信 CERT 监测到 Jenkins Remoting 任意文件读取漏洞 (CVE-2024-43044)，由于 Remoting 库 ClassLoaderProxy#fetchJar 方法没有限制代理请求从控制器文件系统读取的路径，可能导致拥有 Agent/Connect 权限的攻击者从 Jenkins 控制器文件系统读取任意文件（如凭证、配置文件等敏感信息）并进一步利用，导致远程代码执行。奇安信鹰图资产测绘平台数据显示，该漏洞关联的国内风险资产总数为 138,868 个，关联 IP 总数为 57,359 个。目前该漏洞 PoC 已在互联网上公开，建议客户尽快做好自查及防护。

Windows TCP/IP IPv6 远程拒绝服务 / 代码执行漏洞 POC 已公开风险通告

8 月 27 日，奇安信 CERT 8 月 15 日监测到微软发布 8 月补丁日安全更新修复 Windows TCP/IP 远程代码执行漏洞 (CVE-2024-38063)，Windows TCP/IP 组件中发现了一个整数下溢漏洞，可能会触发缓冲区溢出。未经身份验证的远程攻击者可以通过发送特制的 IPv6 数据包到目标 Windows 系统机器导致目标蓝屏崩溃，精心构造请求理论上存在远程代码执行的可能性。该漏洞影响了所有受 IPv6 支持的 Windows 版本，包括即将发布的 Windows 11 版本 24H2。禁用 IPv6 的系统不受此漏洞的影响，但对于启用 IPv6 的系统，存在很大的利用风险。该漏洞被微软标记较大可能被利用，鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。目前，奇安信威胁情报中心安全研究员已成功复现该漏洞，强烈建议马上安装补丁。

红帽人才工程

Cyber Crime Governance Talent Training Project

工程简介

在“全国网络警察培训基地”的指导下，中国下一代网络安全联盟牵头发起「红帽人才工程」，联合华云信安、美亚柏科、高联通信等知名网络安全企业，围绕“网络犯罪治理、涉网犯罪打击”等相关网络安全课题，持续挖掘、培养、资助、赋能网络安全人才，构建红色基因的网络空间安全人才防线。

申报流程

课题征集 → 课题公示 → 立项评审

研究课题计划征集

研究课题信息公示

研究课题立项评审

申报说明

项目资讯

培养对象

政企单位在职人员、高校全日制在校生（含研究生）、互联网企业技术人员、网络安全企业技术人员以及社会网络安全人才...

核心课题

内网攻防、社工钓鱼、远控木马、免杀加壳、情报甄别、资金分析、调证溯源、取证固证、远程勘验、APP反编译、二进制逆向...

阴影之下
——揭示 API 威胁的攻击趋势

API 是企业内部许多技术创新的基础，这些创新改善了员工和客户体验。不幸的是，数字创新和 API 经济的快速扩张为网络犯罪分子提供了新的利用机会。可视性成为关乎 API 安全的关键方面。一旦影子 API 或流氓 API 等盲点被发现，安全团队将会发现其系统中存在诸多以前从未意识到的漏洞。

《阴影之下：揭示 API 威胁的攻击趋势》报告中，研究人员强调了一系列针对 API 的攻击（包括传统的 Web 攻击），并按行业和地区呈现风险概况，以便组织可以更准确地评估自身面临的风险。

主要见解

• API 是当今大多数数字化转型的核心，因此了解行业趋势和相关用例（如会员欺诈、滥用、授权和刷卡攻击）至关重要。

• 2022 年 Gartner 预计，到 2024 年，API 滥用和数据泄露将几乎翻一番。2023 年 29% 的网络攻击针对 API，这表明 API 是网络攻击者锁定的重点领域。

• 针对 API 的攻击包括 OWASP OWASP 十大 API 安全风险和十大 Web 安全风险中强调的风险，攻击者使用结构化查询语言注入（SQLi）和跨站脚本（XSS）等经过验证的方法渗透目标。

• 业务逻辑滥用是关键问题，因为在没有为 API 行为建立基线的情况下，检测异常 API 活动极具挑战性。没有解决方案来监控其 API 活动中的异常情况的组织将面临运行时攻击的风险，如数据抓取——一种新的数据泄露矢量，使用经过身份验证的 API 从内部缓慢抓取数据。

一、API 成最大的攻击向量

按照设计，API 是数据的管道。一旦攻击者通过漏洞利用或针对业务逻辑的攻击获得对 API 的未经授权访问，就无异于获得了数据的访问权。根据 Gartner 的数字，从 2022 年到 2024 年，API 滥用和数据泄露将翻一番。现在，高调的 API 事件比以往任何时候都更常见。事实上，去年，OWASP 发布一个单独的 API 特定风险列表——OWASP 十大 API 安全风险——其中识别了 API 构成的独特威胁。

研究发现，API 正成为传统攻击和 API 特定技术的目标。从 2023 年 1 月到 12 月，近 30% 的 Web 攻击都是针对 API 的（图 1）。随着对 API 使用需求的增加，这些攻击可能还会继续增长，除非组织适当地保护其 API 或考虑其环境中的所有 API。要全面了解攻击面，首先要了解全面而准确的 API 清单。

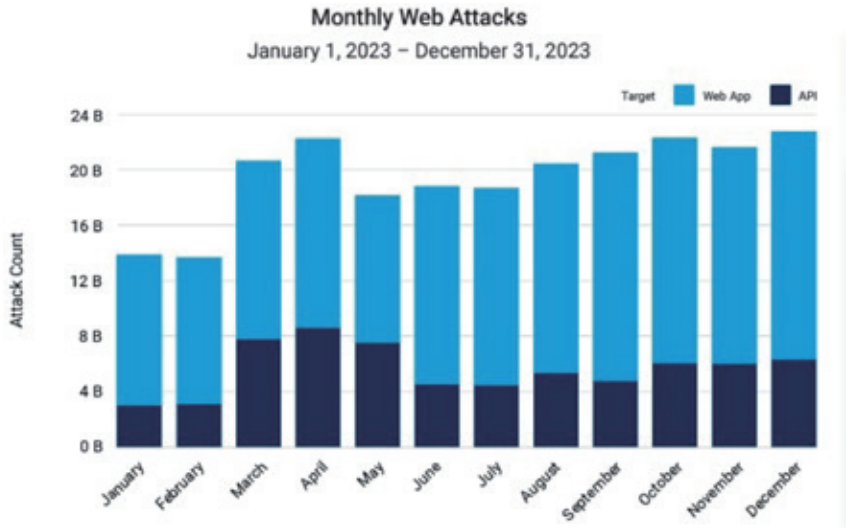


图 1：针对 API 的 Web 攻击

研究人员在全球范围内观察到一些有趣的趋势，其中欧洲、中东和非洲（EMEA）地区遭遇的针对 API 的网络攻击比例最高（47.5%），其次是北美（27.1%）和亚太及日本（APJ）地区（15%）。造成区域攻击差异的原因有很多，比如，监管环境、地缘政治冲突、基础设施类型、访问和教育差异、商业模式和社会因素等。

1、API 攻击策略

分析攻击者瞄准企业 API 的方式及其经常使用的攻击策略，可以揭示组织应该重点关注的防御领域。调查结果显示，在过去的 12 个月里，HTTP 协议（HTTP）、结构化查询语言注入（SQLi）和数据收集攻击是攻击者最为青睐的一些技术（见图 2）。在 HTTP 攻击场景中，攻击者会利用各种协议中的漏洞进行恶意攻击，如读取敏感数据和欺骗客户端或服务器等。另一种流行的技术是活跃会话（Active Session），它适用于在该会话期间标记并阻止可疑攻击流量的任何实例。至于数据收集（Data harvest），顾名思义，指的就是集成或收集信息的攻击，攻击者可以利用这些信息进行其他后续攻击。

值得一提的是，虽然本地文件包含（Local File Inclusion，LFI）并非 API 的首要载体，但它仍然是一个值得关注的领域，因为它可以用来渗透预定目标；然而，仔细观察一下针对 Web 应用程序和 API 的攻击分布，就会发现 LFI 仍然是最主要的攻击媒介之一。

研究结果还显示，机器人请求也是一个令人担忧的领域。根据数据，到 2023 年，全球近三分之一的可疑机器人请求都是针对 API 的。虽然不一定都是恶意的，但这些机器人请求可以用于进行凭据填充攻击和数据抓取，进而可能导致信息盗窃。

强调这些类型的攻击是为了表明，除了 OWASP 十大 10 API 安全风险外，还有许多直接攻击，需要机构跟踪和安排渗透测试团队和红队进行检查。

通过分析 API 活动，研究人员发现了两种截然不同的问题：态势问题和运行时问题。

• 态势问题（Posture problem）与企业 API 实现中的缺陷有关。指示态势问题的警报可以帮助安全团队在攻击者利用高优先级漏洞之前识别和修复

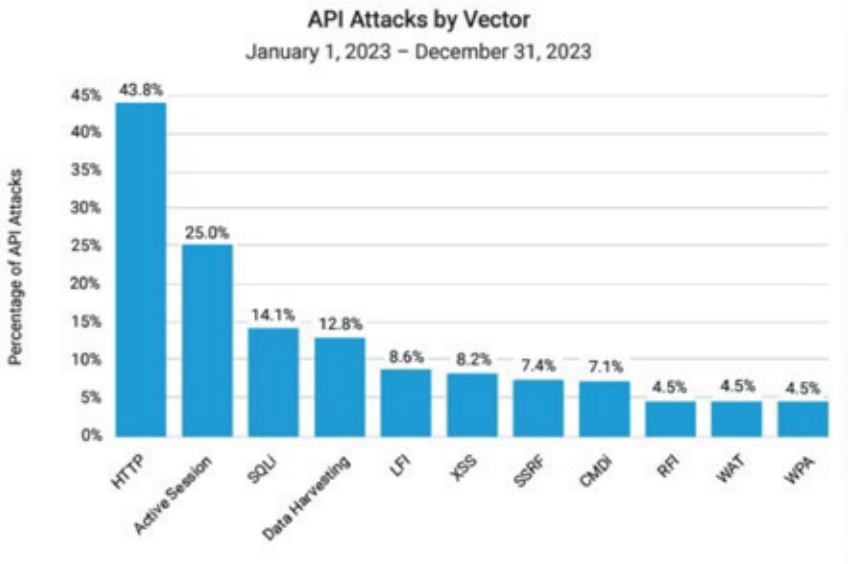


图 2：攻击者最青睐的 API 攻击向量

它们。

• 运行时问题（Runtime problem）是需要紧急响应的活跃威胁或行为。虽然本质上通常是关键的，但这些警报比其他类型的安全警报更微妙，因为它们多以API滥用的形式呈现，而非更明确的基础设施破坏尝试。

2、最常见的态势问题

以下是研究人员观察到的最常见的态势问题。如果不解决，将对企业造成各种潜在影响。

• 影子端点：影子端点是过时的或未记录的 API 先前版本。它们有时也被称为僵尸 API、流氓 API 或遗留 API，由于它们不受组织的标准安全控制和措施的约束，因此它们具有更高的被利用风险。

• 未经身份验证的资源访问：未经身份验证的资源访问是指用户或系统能够在不提供任何形式的身份验证的情况下访问 API 资源的情况，这通常是由于API实现或配置中的缺陷而造成的。尽管许多未经授权的资源是通过模糊手段处理隐藏的，但是发现它们的攻击者可能会利用它们来访问敏感数据或应用程序功能。

• URL 中的敏感数据：在某些情况下，可以在 API 请求的 URL 中观察到敏感数据，如密码、身份验证令牌、信用卡详细信息和个人身份信息（PII）。URL 中的数据通常存储在可能被攻击者访问的地方（如日志和缓存），这会造成敏感数据泄露和遵从性问题等重大风险。

• 宽松的 CORS 政策：在宽松的跨域资源共享（CORS）策略下，API 将允许请求来自比必要范围更广泛的源（如协议、域和端口）。过于宽松的策略使攻击者更容易从不受信任的来源访问敏感资源，并且更容易执行跨站点脚本（XSS）等攻击技术。

3、常见的运行问题

以下是研究人员观察到的最常见的运行时的问题及其潜在风险概况。

• 未经身份验证的资源访问尝试：这是上一节中描述的“未经身份验证的资源访问”态势警报的衍生物，它允许攻击者在没有适当身份验证的情况下访问敏感 API 资源。

• JSON 属性异常：具有异常 JSON 有效负载（如意外数据类型、异常大小或过度复杂性）的 API 活动可能表明有人试图利用脆弱的 API，以执行各种恶意操作，如注入攻击、拒绝服务、数据泄露或滥用 API 逻辑缺陷。

• 路径参数模糊化尝试：路径参数模糊是指故意发送意外或格式错误的数据作为 API 请求的一部分，其重点是 RESTful API 用来指定某些资源或操作的 URL 部分。这是攻击者用来执行

研究发现，API 正成为网络攻击的重要目标。
根据 Gartner 从 2022 年到 2024 年，
API 滥用和数据泄露将翻一番。
2023 年 1 月到 12 月，
近 30% 的 Web 攻击都是针对 API 。

侦察的另一种技术，目的是发现潜在的易受攻击的 API 以执行数据泄露或服务中断等尝试。

· 数据抓取：数据抓取是指以与 API 的预期用途和服务条款不一致的方式和数量从 API 中自动提取数据。攻击者通常缓慢地收集这些数据，以逃避检测并窃取知识产权，收集敏感客户数据，或获得某种利润。当它在 API 中未被发现时，这种低调且缓慢的数据抓取往往意味着潜在的大规模数据泄露攻击。

除了这些态势和运行时问题，API 还面临三个更普遍的挑战：

· **可见性**——您是否有流程和技术控制来确保所有 API 都受到合理保护？这是一个关键问题，因为 API 通常是转型的一部分或嵌入到新产品中，因此许多 API 没有与传统 Web 存在相同级别的指导、保护和验证。

· **漏洞**——您的 API 是否遵循了开发的最佳实践？您是否在避免 OWASP 提及的最常见的编码问题？此外，您是否跟踪并检查了漏洞？

· **业务逻辑滥**——您有设定预期流量的基线吗？您确定什么是可疑活动了吗？

总而言之，无论是对于面向客户的 API 还是内部 API，拥有对 API 的可视性和调查能力并建立流程，以快速缓解威胁都是至关重要的。

二、行业趋势凸显 API 攻击的危险

API 是组织数字化转型的核心。然而，API 的存在也增加了企业的风险暴露面，并带来了重大的安全挑战。报告显示，44.2% 影响商务机构的网络攻击以 API 为目标，其次是企业服务机构，占比 31.8%（参见图 3）。这种对商务的严重倾斜是由多种因素造成的，包括其生态系统的复杂性、对 API 的高度依赖，以及存在大量机密客户信息。

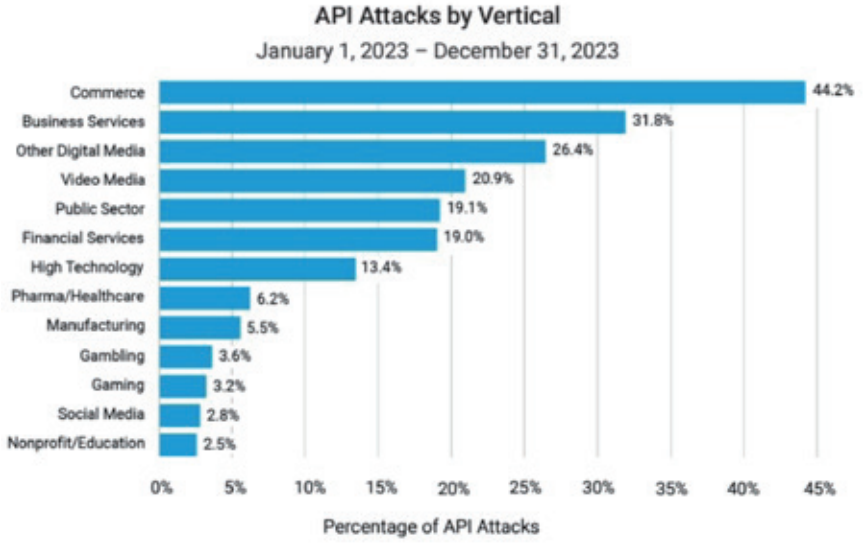


图 3：2023 年商务和企业服务领域遭受 API 攻击比例最高

值得关注的是，企业服务排名第二的一个关键因素是考虑到供应链攻击的潜在威胁。提供企业服务的第三方公司可能拥有有关其附属组织的机密信息，甚至可以访问其环境，攻击者可能将其用作通往高价值目标的途径。

仔细观察上述数据不难发现，没有哪个垂直行业能够免受 API 攻击。例如，医疗物联网（IoMT）的爆炸式增长和数据互操作性的努力推动了医疗保健行业的 API 采用率，同时也为医疗保健行业带来了重大风险。

1、案例研究

为了让您深入了解针对不同行业的攻击类型，研究人员提供了几个现实案例及其对组织和客户的实际影响。

1) 商务垂直领域中的会员欺诈

欺诈者的目标是会员计划账户，因为它们包含有价值的通货（如积分、里程或信用度）可以兑换现实世界的商品或现金。研究人员在一个 API 上检测到一个用户访问超过五个会员账户的行为。经调查发现这些账户中的这种行为属于欺诈。大多数账户仅由少数授权用户访问，因此访问多个账户的用户可能暗示有滥用行为。为了帮助减少欺诈，最好理解正常行为和滥用行为之间的区别。

2)SaaS 通知服务中的 API 滥用

研究人员在一家金融服务公司的软件即服务（SaaS）通知系统中，发现了 API 滥用。有效负载中的授权标头和签名丢失使得该公司无法检查谁在系统中发出请求并发送通知。因此，任何有权访问该 API 的人都可能滥用它向公司员工和客户发送消息。

3) 潜在的 BOLA 攻击

研究人员在一家航空公司发现了潜在的破坏对象级别授权（BOLA）攻击，其中来自近 200 个 IP 的经过身份验证的用户模糊了 {customer_id} 路径参数，然后如果提供的参数有效，则返回敏感的用户信息（见图 4）。由于此 ID 是一个简单的整数，因此模糊处理非常容易，但影响可能是破坏性的，因为它可能导致客户信息的数据泄露。据悉，目标API返回的敏感信息包括名字、中间名和姓氏，以及政府 ID、国籍、居住国家和出生日期等。

4) 隐藏在众目睽睽之下的刷卡攻击

在另一种情况下，一开始是异常的 API 流量变成了刷卡攻击（Carding attack，一种自动化或机器人驱动的网络攻击，攻击者获取被盗的信用卡号后尝试授权被盗信用卡凭据）。最初，受影响的组织认为是 DDoS 活动导致了 API 流量激增；然而，经过仔细检查，发现是攻击者正在试图验证信用卡，一旦验证成功，攻击者就可以在暗网市场上出售这些号码或进行其他欺诈性交易。

2、API 成为新的数据泄露载体

在大多数 API 环境中，存在的一个常见业务问题是在 API 安全程序的发现阶段检测到编程错误或配置错误。这些错误中的大多数从未被利用，一旦安全团队获得了对 API 资产和每个 API 上运行的流量的可见性，潜在的损害将会很明显。

通常，涉及 API 的应用和业务流程的启动和部署速度，比安全团队评估其状态的速度要快。这似乎使错误配置和漏洞不可避免。再加上大多数组织内部缺乏 API 安全专业知识，这就导致了下述这个令人不快的安全等式。

API 安全错误的条件：

使用 API 快速部署关键业务流程 + 缺乏对 API 的可见性 = 配置错误或易受攻击的 API

随着时间的推移，未知的 API 漏洞通常与编程错误密切相关。如今，涉及 API 的公开数据泄露已经司空见惯，这表明攻击者现在正在探索 API 资源并执行侦察，以识别要利用的特定 API。这种探索，加上数据抓取的自动化威胁，意味着 API 已经成为新的数据泄露载体。此类成功攻击的后果包括对品牌和声誉的损害，机密数据和客户信任的丢失，以及其他合规和立法问题。

观察数据不难发现，
没有哪个垂直行业能够免受 API 攻击。
报告显示，44.2% 的 API 攻击针对商务机构的，
其次是企业服务机构，占比 31.8%。

因此，API 安全性比以往任何时候都更加重要。

API 数据泄露的条件：

在生产环境中配置错误或易受攻击的 API + 数据抓取自动威胁（机器人）= 持续数周或数月的低调且缓慢的数据泄露

防止 API 漏洞导致的数据泄露，第一个关键方面是了解您的环境，了解哪些是异常行为，哪些数据在哪些 API 上。这包括将所有 API 置于安全控制之下，并具有自动响应以缓解攻击或提醒安全运营团队。接下来，在开发过程中实践“左移”测试，以便在攻击者利用漏洞和缺陷之前及时解决它们。最后，您还需要通过模拟演习，来验证预防措施和应急响应策略的有效性。

三、提高可见性：管理 API 资产生命周期的关键

我们已经了解缺乏 API 可见性所带来的危险，接下来我们将展示采用强大的 API 安全程序如何带来许多不同的可见性体验，具体表现如下：

- 发现：组织内的 API 库存可见性；
- 风险审计：每个发现的 API 的风险状态可见性；
- 行为检测：正常使用与异常滥用的可见性，以了解每个 API 上的活跃威胁；
- 调查和威胁捕获：由人类威胁猎人专家发现潜伏在 API 资产中的威胁的可见性。

由于 API 的快速部署，它们中的许多都不具备该有的网络安全成熟度。问题是许多 API 都有可被利用的敏感数据。为了提高可见性并改善 API 安全成熟度，组织可以遵循下述建议：

1、照亮阴影

“你不能保护自己看不到的东西”这句古老的格言同样适用于今天的 API。对于许多增加 API 活动可见性的企业来说，最大的惊喜之一是在其环境中悄悄运行的影子端点数量锐减了。发现流氓或僵尸 API 令安全团队倍感欣喜，因为这让之前的阴暗之处照进来光亮。通常，实现 API 安全成熟度的第一步是系统地发现这些影子 API，并确保每个影子 API 要么退役，要么正式记录，并纳入组织的 API 安全控制。这对降低意外 API 滥用和其他风险具有直接影响。

2、实现文档化

影子 API 得到了解决，但在合理化和组织已批准的 API 清单方面仍有工作要做。这包括根据广泛的类别（如开发、测试和生产）进行分段并建立层次结构，以确保安全警报和分析具有适当的上下文，从而允许团队了解与 API 相关的风险。为每个 API 编写文档是改进可见性的下一步。文档使安全团队能够更有效地对态势警报做出反应，因为它将警报带入上下文中，并使其与他们对应用程序、API 和业务流程的思考方式保持一致。

3、强化 API 态势

企业接收到的初始态势和运行时警报，通常会通知其 API 实现的一组高优先级更改。例如，安全团队通常会查看最常见的警报类型，并确定降低风险的策略和优先级。这包括纠正 API 代码中的缺陷、解决错误配置问题，以及根据吸取的教训实现防止未来漏洞的流程。这可以帮助确定渗透测试验证计划的优先级，并可以告知管理层必要的编码最佳实践，以避免潜在的漏洞。

4、加强威胁检测和响应

虽然前三个步骤通常会导致 API 安全警报总数的总体下降趋势，但随着时间的推移，我们通常会看到偶尔的高峰。这些可能是由内部驱动的因素引起的，例如，业务模型的广泛更改、新功能的获取，或者引入新漏洞或流氓系统的 API 足迹的添加。峰值也可能由外部因素引起，包括来自对手的攻击企图。最明智的组织会为这些峰值制定计划，并在它们发生时制定明确的响应程序，将风险和警报量降至正常水平。他们还将采取措施，不断加快响应、调查、遏制和从活跃 API 威胁中恢复所需的时间。这可能需要基于 API 环境的新技能。

5、发展更强大的进攻性方法

随着组织改进其防御性 API 安全措施，下一阶段是用进攻性方法来补充防御措施，以发现和缓解 API 威胁。这包括建立一个正式的 API 威胁搜索规则和节奏，目标是在它们升级为反应性场景之前尽早识别可能的威胁。这可能极具挑战性，因为它需要高度专业化的人才，以及将资源从中断驱动的任务中隔离出来的能力。出于这个原因，一些企业会聘请专门的第三方服务提供商来提供这一重要功能。

深度披露：《黑神话：悟空》发行平台遭 DDoS 攻击细节

8 月 24 日晚，《黑神话：悟空》发行平台 Steam 因遭到大规模 DDoS 攻击突然崩溃，奇安信 XLab 实验室第一时间公布了近 60 个僵尸网络主控、一夜发起 28 万次攻击、暴涨 2 万多倍的事件解读。

事件回顾

8 月 24 日晚，Steam 平台突然崩溃，国内外玩家纷纷反馈无法登录。许多玩家猜测崩溃是由于《黑神话：悟空》在线人数过多所导致。然而，根据完美世界竞技平台的公告，此次 Steam 崩溃实际上是因为遭受了大规模 DDoS 攻击。

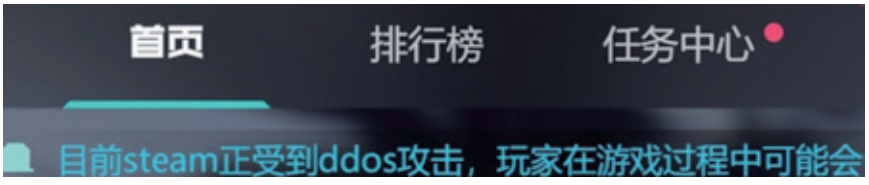
此次事件的 XLab 观察

XLab 大网威胁感知系统对最近的 DDoS 攻击事件进行了深入观察。我们注意到，此次攻击涉及了近 60 个僵尸网络主控节点，这一规模远超常规僵尸网络的控制范围。这些主控节点协同指挥了大量被感染的 bots，以波次方式发起了攻击。

攻击的目标包括 Steam 在全球 13 个地区的服务器 IP，包括中国、美国、新加坡、瑞典、德国、奥地利、西班牙、英国、日本、韩国、澳大利亚、智利和荷兰。值得注意的是，除了 Steam 自身的服务器，国内完美世界代理的 Steam 服务器也被列为攻击目标。总计，有 107 个服务器 IP 遭到了攻击。

攻击行动主要分为 4 个波次，攻击者似乎有意选择在各个时区的游戏玩家在线高峰时段发起攻击，以实现最大的破坏效果。

从攻击的时间选择、地域分布，以及同时针对国内外 Steam 服务器的策略来看，攻击者的目的显然是在重



完美世界公告

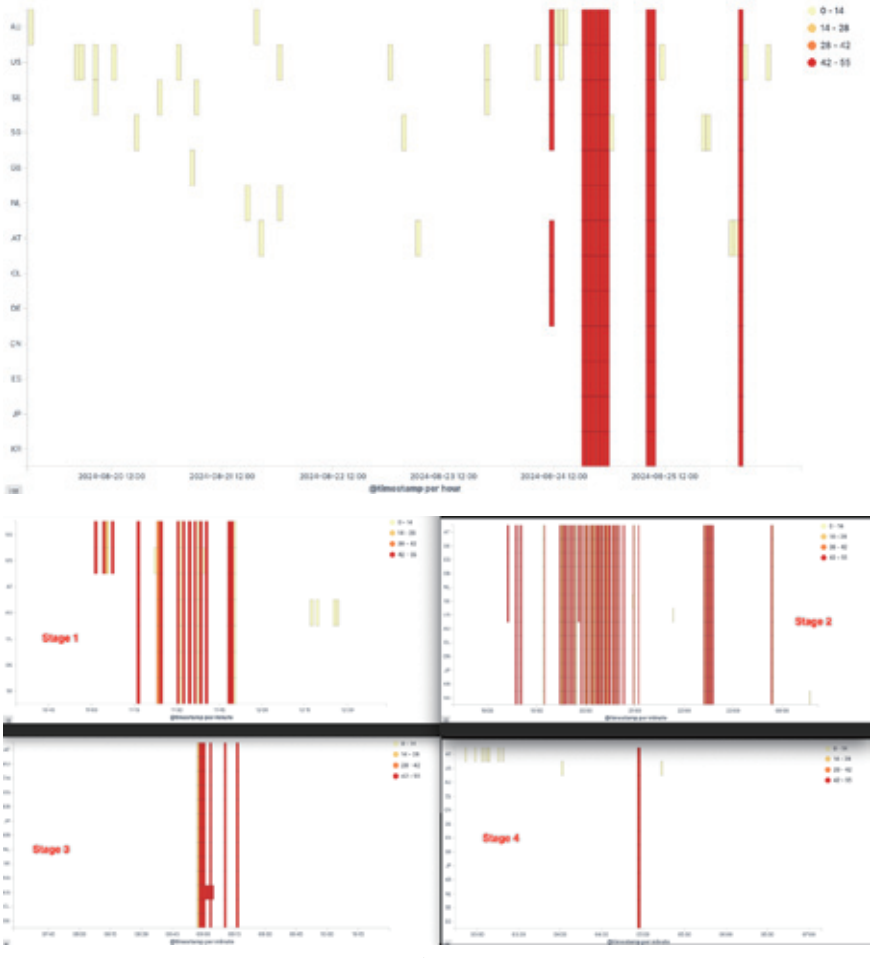


Downdetector 用户报告的 Steam 中断情况

点扰乱中国市场的同时，在全球范围内对 Steam 平台的正常运营造成全面干扰。这种有组织的攻击行为表明了攻击者在策略上的计划性和对目标的明确针对性。

攻击时段分析

此次攻击事件主要分 4 个批次、追着时区打。分别是东半球周六中午、东半球周六晚间、西半球周六晚间和欧洲地区周日晚间、都是游戏玩家在线的高峰时段。具体攻击时段和地区如下图（图表说明：横坐标为攻击时间、纵坐标为被攻击地区、色块表示该地区被攻击的服务器数量）。



4 波攻击的详细时间和地区

详细攻击时间线

- 北京 24 日 11 点前后，第一波尝试攻击，影响 7 个地区 Steam 服务器，攻击持续时间近 1 小时（东半球周六中午）
- 北京 24 日 21 点前后，第二波攻击，影响 13 个地区 Steam 服务器，断断续续攻击将近 5 小时（东半球周六晚间）
- 北京 25 日 09 点前后，第三波攻击，影响 13 个地区 Steam 服务器，攻击将近 15 分钟（西半球周六夜晚）
- 北京 26 日 04 点前后，第四波攻击，影响 13 个地区 Steam 服务器，攻击持续时间近 2 分钟（欧洲周日夜晚）

Steam 被攻击的服务

从这些 Steam 服务器的关键字猜测，被攻击的主要是内容服务器、ingest、broadcastcs，相关的服务。

27 ext2
27 ext1
18 cm2
18 cm1
11 ext3
9 ext4
5 cm5
5 cm4
5 cm3
4 cm6

3 ext5
1 ingest
1 ext6
1 cm05
1 broadcastcs

攻击动机推测

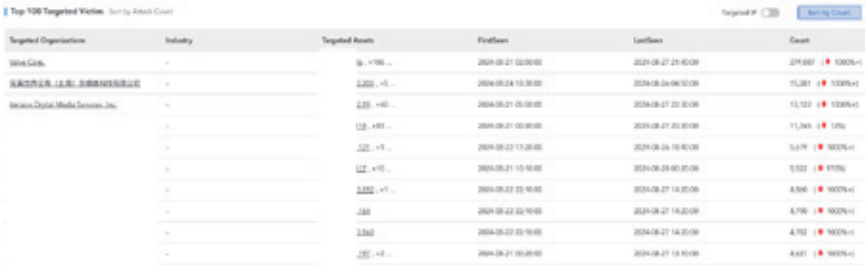
此次攻击事件我们一共观察到了28万条针对Steam平台的攻击指令，根据我们的长期观察，作为知名的游戏平台，Steam 的攻击时常发生，但往往都是零散的服务器被小规模的攻击，攻击指令数目几次到几十次不等。此次事件攻击指令直接暴涨 2 万多倍，峰值时攻击指令 25 万，这种涨幅是非常罕见的（见下图，攻击指令趋势图，巨大的尖峰）。Steam 全球各地区机房服务器被轮着打，包括国内完美世界代理的 Steam 服务器也一并被扒出来攻击，《黑神话：悟空》上线之前我们没看到完美世界 Steam 服务器遭遇过成规模的 DDoS 攻击。且攻击时长多达几个小时，专挑各地区玩家在线高峰期攻击。这是极其少见的。

下图是我们的大网威胁感知系统的截图，大家看到是被攻击企业排名，可以看到在过去一个月的数据里，Steam（Valve 公司）和完美世界排在第一、第二，远超后续的 Verizon 等知名企业。

结合最近火出圈的国产游戏《黑神话：悟空》在 Steam 平台上线，包括主要为国内游戏玩家服务的完美世界 Steam 服务器也遭到攻击，《黑神话：悟空》上线之前，我们没看到完美世界 Steam 服务器遭遇过成规模的 DDoS 攻击。又是周末夜晚，广大游戏玩家在线的高峰时期，Steam 平台遭遇如此大规模的 DDoS 攻击，很难让人不联想此次攻击事件不是针对国产 3A 游戏大作《黑神话：悟空》。



过去一年针对 steam 平台的攻击事件攻击指令趋势



主要涉事僵尸网络

Steam 做为一个世界性的游戏平台，不可能被区区一两个僵尸网络打崩，肯定是非常多的僵尸网络被组织起来协同攻击。世界上没有任何组织可能拥有全知视野，本文只是从 XLab 的视野出发，就此次攻击事件进行分析。

在我们的视野中，多个僵尸网络参与了此次攻击，其中的主力是自称 AISURU 的僵尸网络，在其 telegram 频道中声称拥有超过 30,000 个 bot



此外，该频道还提到了国外厂商 GSL 的一篇 Blog，Blog 声称是有史以来向公众报告的最大规模的攻击，我们也在该僵尸网络的攻击日志中找到了相同时间节点发出的攻击：

部分读者可能对于这些数字没有概念，让我们看一看当下最火的人工智能大模型的回答。

一个僵尸网络（botnet）拥有 30,000 个节点，并且其攻击能力在 1.3 Tbps（太比特每秒）到 2 Tbps 之间，



这代表了一个非常强大的网络攻击能力。要理解这个概念，可以从以下几个方面来分析。

1. 攻击规模：1.3 Tbps 到 2 Tbps 的攻击流量已经非常巨大，足以造成严重的分布式拒绝服务攻击（DDoS），这类攻击会使目标服务器、网络或应用程序瘫痪。一般来说，传统的企业网络带宽远低于这个水平，因此，这样的攻击会对目标产生毁灭性影响。

2. 节点数量：30,000 个节点意味着有 25,000 台受控设备参与了攻击。每个节点可能会贡献一定的带宽来发起攻击，集合起来的总攻击流量达到了 1.3 Tbps 至 2 Tbps。

3. 实际影响：这种规模的 DDoS 攻击可以轻松压垮大部分互联网服务，除非被攻击方拥有非常强大的防护措施和足够的带宽冗余。这类攻击常见于高调的黑客活动，针对大型企业、政府机构或关键基础设施。

相信读者现在已经有了一定的认识，总体来说，像 AISURU 这样的僵尸网络是一种非常强大的网络武器，能够通过数量巨大的设备同时发起攻击，使得任何几乎没有特别强大防护措施的在线服务都可能被击垮。这种攻击不仅对目标造成直接影响，还可能影响到大量依赖这些服务的普通用户，正如此次攻击，让大量玩家无法登录平台，畅玩悟空，喊出那一句“广智救我”。

AISURU 僵尸网络技术细节

正所谓罗马并非一日建成，AISURU 僵尸网络也有自身的发展历程。其实我们在 2023 年 10 月就捕获到该僵尸网络的样本，不过它在短暂运营之后便销声匿迹，直到今年 5 月初以 'NAKOTNE' 的名字再次进入我们的视野，随后进入高速发展期，先后投入十几个 Nday 漏洞组建网络，最终进化为今天的 AISURA。

AISURA 在战术、技术层面都和 2022 年我们发现并命名的僵尸网络 Fodcha 有着千丝万缕的联系。Fodcha 因参与攻击健康码、Navicat 等一系列有影响力的事件而在安全圈内臭名昭著，被我们戏称为“DDoS 狂魔”。最终，在我们一系列的曝光和打击下，其被迫关停。

在我们看来，AISURA 像是 Fodcha 的“追随者”或“信徒”，它在战术与技术层面很好的继承了 Fodcha 的遗产，但同时也发展出了独特的风格，其威胁性不弱于 Fodcha。

首先从战术层面上来说，它也和 Fodcha 一样，喜欢挑衅安全公司，希望被知名安全公司点名曝光，为自己带来流量热度，通过这种另类的广告方式，为自己在激烈的黑产竞争中赢得优势，似乎深谙“酒香也怕巷子深”之理。

AISURA 在最早的样本中是这样表达它对安全社区的“尊重”，"N3tL4b360G4y"，

"paloaltoisgaytoo"。paloalto，即 Palo Alto Networks，是美国一家非常著名的安全公司，市值超过千亿；那“N3tL4b360”呢？其实是一种在安全圈颇为流行的 Hexspeak，它指的是我们前团队的名字。当我们披露这批样本后，它马上很知趣的在新样本中将 N3tL4b360G4y 替换成 Xlab gay。毫无疑问，这又迎来了我们的曝光。此外 AISURU 非常关注我们 Blog 的动态，在最新的样本中又增加了一条消息 Today at Xlab, botnet operators learn how to dance macarena，这让我们想起了之前公开的 Rimasuta 僵尸网络：曾经在样本中留言 This week on Netlab 360 botnet operator learns chacha slide。过去学 chachaslide，现在跳 macarena，俩个都是跳舞，难道僵尸网络的作者多为舞蹈爱好者？对此，我们想对僵尸网络团体说，“好好练，将来开发出更精彩的 botnet 之舞，惊艳我们！”。

另外，样本中的 C2 域名 foxnointel.ru，实在让我们有些忍俊不禁。读者或许会问，笑点何在呢？请容许我们解释一下黑客的幽默，在 X 平台上有一个非常活跃的安全研究员，ID 是 Fox_threatintel，他几乎每天都会分享一些威胁情报（threatintel）；AISURA 使用 C2 域名 foxnointel，即 fox no intel，“嘲讽”他其实根本没有情报。

接着我们来看技术层面，AISURA 在代码结构上保留了部分 Fodcha 的风格，比如使用和 Fodcha 类似的 switch-case 进行各个阶段的处理；在基础设施投入上延续了 Fodcha 的“危机意识”，即将 C2 映射到 20 多个 IP，而且分布在美国、英国、韩国、日本、俄罗期等多个国家，同时分散在 Azure、Linode、Vdsina、Google 等多个平台，极大的增加了处置的难度。AISURA 主控地理位置分布如下：

8 United States
3 United Kingdom
3 South Korea
3 Russia
2 Singapore
2 Japan
2 India
1 The Netherlands
1 Switzerland
1 Poland
1 Brazil

当然喜欢彰显特立独行的黑产团体，肯定不甘心被人贴上模仿者的标签，AISURA 在加密，网络通信等方面，实现了自己独特的创新。

字符串解密

早期版本使用 ChaCha20 算法对样本中的字符串进行加密，在后期的版本中使用 XXTEA 加密。

NAKOTEN_XXTEA_KEY_HEX: 1234567890ABCDEFFEDCBA9876543210

在最新的版本中，样本中仍保留了之前的 KEY，但长度缩短为 4，算法也在朝着简单的方向发展，更换为 BYTES_XOR。

AISURU_BYTES_KEY_HEX: 12345678

0x1a42c snow slide

0x1a6d0 a|b|c|d|e|f|g|h|j|k:printerconsulting.ru|foxnointel.ru

0x1a438 reports.printerconsulting.ru

0x1a708 5.35.45.162|5.35.44.21|166.1.160.38|194.147.35.35

0x1a458 /login|/products|/contact|/register|/user

0x1a484 /dev/null

0x1a490 /dev/tty

0x1a49c /dev/pts/1

0x1a4a8 /dev/console

0x1a4b8 /.ai

0x1a4c0 /proc/

0x1a4c8 /proc/self/exe

0x1a4d8 /proc/net/tcp

0x1a4e8 /cmdline

0x1a4f4 /exe

0x1a4fc /proc/uptime

0x1a50c /maps

0x1a514 /fd/

0x1a51c socket

0x1a524 wget|curl|ftp|ntpdate|echo

0x1a540 telnetd|upnpc-static|udhcpc|/usr/bin/inetd|ntpcli

```
(b'a|b|c|d|e|f|g|h|j|k:printerconsulting.ru|foxnointel.ru')
(b'xlab gay')
(b'paloaltoisgaytoo')
(b'today at xlab, botnet operators learn how to dance macarena')
```

ent|boa|lighttpd|httpd|goahead|mini_http|miniupnpd|dnsmasq|sshd|dhcpd|upnpd|watchdog|syslogd|klogd|uhttpd|uchttpd|pppd|dhclient

0x1a5f4 /dev/watchdog

0x1a604 /dev/misc/watchdog

0x1a618 TSource Engine Query

0x1a630 xlab gay

0x1a63c paloaltoisgaytoo

0x1a650 shell

0x1a658 system

0x1a660 enable

0x1a668 sh

0x1a73c /bin/busybox AISURU

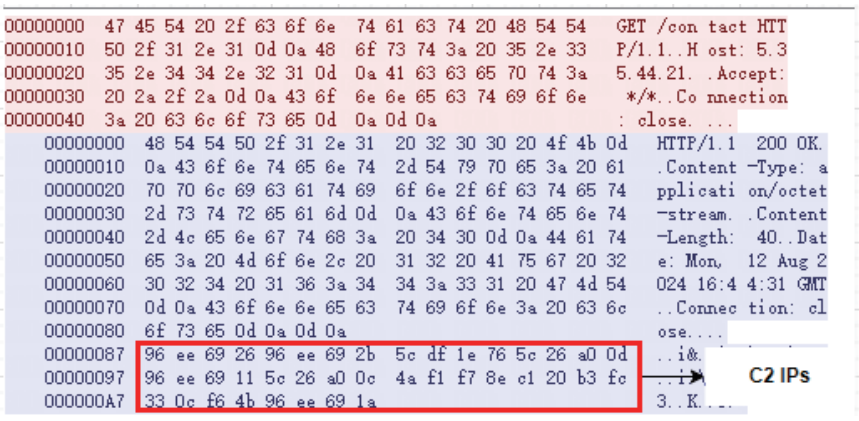
0x1a66c AISURU: applet not found

0x1a688 ncorrect

0x1a694 today at xlab, botnet operators learn how to dance macarena

网络协议

2023 年 10 月 的 版 本 以 N3tL4b360G4y 作为上线包，并将该字符串明文硬编码在样本中。被曝光之后，我们收到了新的“回应”：从 NAKOTNE 版本开始，以 xlab gay 作为上线包，并且将其加密编码到字符串表中。



C2 获取

在 8 月初，我们在新样本中收到 留 言：Today at xlab, botnet operators learn how to dance macarena，以往域名或 IP 被直接加密编码在字符串表中，而新样本中加入了新的机制获取 C2。

通过解密字符串表，我们发现了以下可疑字符串：

[1] a|b|c|d|e|f|g|h|j|k:printerconsulting.ru|foxnointel.ru

[2] 5.35.45.162|5.35.44.21|166.1.160.38|194.147.35.35

[3] /login|/products|/contact|/register|/user

经过分析后，使用以下机制获取 C2：

1. 通过 : 分割 [1] 中的子域名和二级域名，再通过 | 分割每一项

2. 随机选择一个子域名和一个二级域名，拼接后得到 C2

3. 若解析上述 C2 失败，则用 | 分割 [2]、[3]，得到 IP 和 URI

4. 根据 IP 和 URI 构造 GET 请求并发送

5. 以 4 字节为单位获取返回包中的 C2

C2 使用的端口被硬编码在样本中，从 21 个端口中随机选择一个：

2348,12381,8932,8241,38441,23845,8745,6463,7122,1114,6969



,1337,4200,3257,7214,2474,4444,2222,3333,5555,24811

通信过程

通信过程在多个版本中都没有发生变化，使用和 Fodcha 类似的 switch-case 进行各个阶段的处理：

1. 上线包发送：xlab gay

2. 协商密钥

• 使用 XXTEA 解密得到 CHACHA20_KEY、CHACHA20_Nonce

• 硬编码的 NET_XXTEA_KEY_HEX: 428723212B0106344C7A095322236921

3. 密钥验证

• 使用协商后的密钥解密数据，通过对比字符串 paloaltoisgaytoo 验证双方密钥一致性。

4. 发送 bot 分组信息

• 先发送明文的分组长度，再发送 ChaCha20 算法加密的分组信息

至此，AISURU 僵尸网络的主要技术细节介绍完毕。DDoS 这一古老的网络威胁，游戏行业的天敌之一，就是如此朴实无华但粗暴有效。

总结

XLab 团队专注大规模僵尸网络发现 & 跟踪领域已经超过 10 年，参与过全球众多知名和未公开的各种攻击事件预警、防御和协作，但对此次攻击的组织度、烈度依然感到惊奇。中国出了一款登顶全球的游戏，有人这么不开心吗?

最后引用一句伟人的诗做为本文的结束，" 金猴奋起千钧棒，玉宇澄清万里埃 "，祝福悟空，祝福中国的游戏产业。

部分 IOC

SHA1:

b6e5c9e65682ccac071b65743595dae475f7a8b8

458d541bc93937ae6d0139f3f9d42b50fe255636

f0760aeaa0d667a1c100e3d348dbc383451587b1

Domain:

nakotne.pirate

nvr.libre

a.printerconsulting.ru

关于作者

关于 XLab 实验室

奇安信 XLab 实验室专注于大规模数据环境下的网络态势感知、威胁分析溯源及安全数据平台建设，拥有业内领先的超大规模多维安全基础数据平台和恶意样本及载荷捕获分析平台，覆盖 PassiveDNS、僵尸网络跟踪、高级蜜罐系统等关键技术模块。Xlab 实验室不仅为内部安全产品及业务提供海量数据支持，还持续进行威胁分析与情报产出，特别是在大规模僵尸网络监控方面，披露了 30 多个具有全球影响力的僵尸网络，如 Mirai、Bigpanzi 等，发现了近年来几乎所有具有影响力的僵尸网络。XLab 实验室众多研究成果引发业界广泛关注，赢得了多国政府和安全机构的高度评价与感谢。

汽车行业成 API 风险高地，智能网联车数据安全亟待加强

2023 年年初，据安全组织披露，有近 20 家知名品牌车企存在 API 安全漏洞，黑客能远程解锁、启动车辆、跟踪汽车行踪，窃取车主个人信息，造成大量客户数据泄露；同月，T-Mobile 公开承认，黑客利用一个 API 漏洞窃取了 3700 万客户的数据。

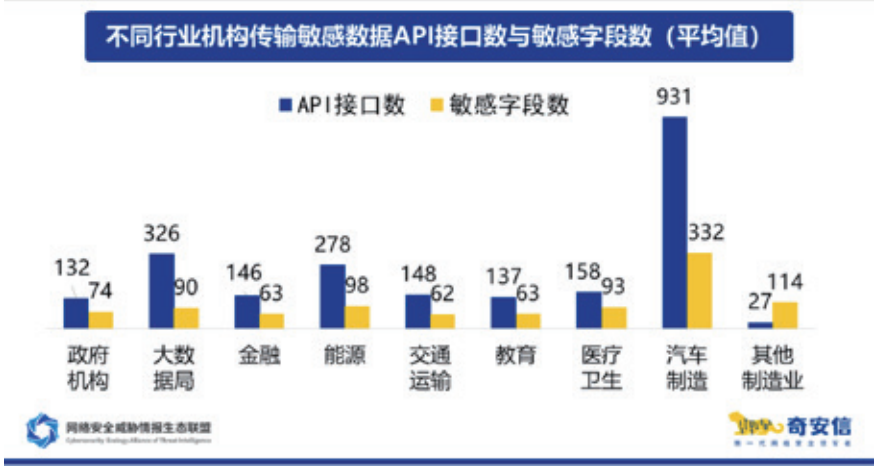
2024 年 1 月，《检查日报》报道，有黑客利用 API 接口漏洞，对全国 21 个省市、29 个行业的 51 个系统发动了网络攻击，非法获取了大量公民个人信息并进行贩卖，获利人民币 500 余万元。经查，王某等人通过网络渠道委托黑客，利用搜集到的各种政府、企业网络平台的 API 接口漏洞，进行数据抓包、参数解析，开发出 100 余款黑客软件。



汽车行业成为 API 安全风险重灾区

根据奇安信集团发布的《2023 中国政企机构数据安全风险分析报告》（以下简称《报告》）显示：API 安全是数据安全的重要一环，也是最容易被忽视的薄弱环节，已经成为黑客入侵系统和窃取数据的重要渠道。在对 128 家大型政企机构的抽样分析发现，平均每家机构约有 206 个 API 接口会用来传输敏感数据，约占 API 接口总数的 2.5%。其中，汽车制造业的“潜在”数据安全风险最大，其传输敏感数据的 API 接口数平均超过 900 个，传输敏感字段多达 332 个，这两项指标均是其他行业的 3~7 倍。

同时，汽车制造业 API 接口传输的个人信息也最多，平均每天涉及 1.5 万多个自然人，是金融、能源、医疗等行业的 30~70 倍，可谓“遥遥领先”。《报告》指出： 从某种程度上来看，一辆智能网联汽车，就是一个移动的敏感数据发生源，持续不断的通过各种 API 接口，向服务器传输敏感数据。不仅如此，这些数据还会一刻不停的在各种车联网业务系统中周转和使用。



这也使得汽车制造业及智能网联汽车，都成为数据安全的高风险地带。

近年来，面向 API 应用的网络攻击已经开始对各大汽车企业组织造成严重的破坏。因此，每家组织都需要提升对 API 应用安全的重视度。网络安全研究员 Sam Curry 和他领导的研究团队，在数十家全球顶级汽车制造商生产的车辆和车联网服务中，发现了许多 API 应用缺陷，利用这些缺陷，攻击者可以进行广泛的恶意活动，从非法窃取车主个人隐私信息，到远程解锁车辆、监控车辆等。

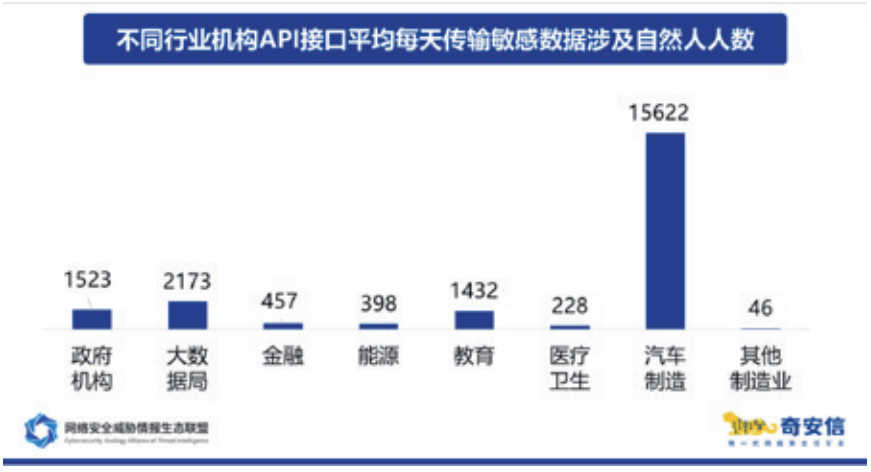
Sam Curry 表示，通过深入地研究分析和实际测试，他的团队发现，API 应用安全问题几乎影响了目前所有主流的汽车品牌，包括奔驰、宝马、劳斯莱斯、法拉利、保时捷、捷豹、路虎、本田、英菲尼迪、日产、讴歌、丰田、福特等 20 多个知名品牌。此外，该研究团队还发现，在 Reviver、SiriusXM 和 Spireon 等主流车联网服务商的应用方案中，同样存在大量严重的 API 安全缺陷。

事实上，放眼全球领域，数据安全尤其是 API 安全正成为汽车行业的一个严重问题。根据相关数据显示，汽车 API 攻击惊人地增长了 380%，同时还有 34% 的汽车行业员工表示，公司现在所面临的安全威胁比两年前要多。

分析人士认为，随着汽车行业迅速向软件定义车辆过渡，势必要求对数据和系统的保护采取得力措施。为了保障行业内客户数据及企业信息的安全，汽车厂商需将 API 安全作为整体安全的重要组成部分。

API 安全需成为汽车数据安全的核心链条

奇安信数据安全专家认为，随着数字经济的发展，API 作为对外提供数据服务的主流通道，在 API 爆发式增长的环境下，对外也产生了大量的暴露面和攻击面，对于 API 的安全防护而言，传统的安全防护设备无法解决 API 安全的问题，因为从防护的维度和防护的模型均已经发生了质的变化，另外目前大多数用户对于 API 安全的建设均处于一个盲区，如何梳理清楚 API 资产，看清 API 风险、如何进行防护成为当前用户的主要痛点。





对于 API 安全的防护体系，奇安信认为从 API 安全全生命周期来看，可以将 API 分为设计、开发、测试、运行、上线、发布、下线等几个流程，这几个流程可以拆分为事前、事中和事后三个阶段。

在事前阶段，也就是开发设计和测试阶段，可以通过管理体系制定相关的管理制度来对开发进行约束，将 API 的漏洞风险在开发侧进行闭环。

在上线运行阶段，需要建立一套完整的技术体系，从资产管理、安全检测、安全分析、安全防护形成一套闭环的监测手段。

在API的评估处置以及下线阶段，需要建立完整的运营体系针对 API 进行常态的运营，针对风险的 API 及未知的 API 进行处置，当遇到 API 安全风险事件的时候，有相关的应急响应手段。

新技术、新场景层出不穷，包括 API 安全在内的数据安全合规建设也成为一项非常复杂的系统工程。奇安信数据安全专家认为，数据安全建设应当遵循内生安全原则，从设计规划之初就把数据分类分级、数据防泄露、防勒索、API 安全、跨境数据治理等关键问题列入整体规划，确保数据安全工作与数字化建设同步规划、同步建设、同步运行，用系统性的方法解决数字系统的安全问题。

同时，仅依靠建立制度和管理层面的静态体系是远远不够的，必须借助技术手段实现覆盖数据全生命周期和业务全流程的安全与合规管控，实现动态及持续性的实质性合规。其中包括：企业要结合自身的实际情况，定期开展数据安全及合规风险评估和建设工作，借助技术手段，将数据合规和安全贯穿于数据处理活动的全过程，确保在合法合规的框架下，充分释放数据要素的价值。



CTFWAR.ORG

网络安全的本质是攻防对抗
讲百遍不如打一遍

---习近平

CTFWAR介绍

CTFWAR攻防战争平台是CTFWAR网络安全攻防对抗联赛的官方平台，是由中国网络安全攻防大咖联合发起的创新型学习平台，以游戏的形式融入多种网络攻防场景进行答题、竞赛、互动。CTFWAR攻防靶场分为初级新手区、中级进阶区、高级挑战区，同学们可根据自身技术能力及技术方向进行筛选，整个学习过程将有全面的数据化呈现。

攻防答题模式

CTFWAR攻防战争平台采取主流的CTF夺旗赛和AWD攻防赛的答题模式，提供云端的攻击终端，同学们在云端攻击平台上进行攻防实战操作，通过 Flag 判定和操作用时进行综合评分，以获得积分升级和金币奖励。

积分等级体系

CTFWAR攻防战争平台采取主流的CTF夺旗赛和AWD攻防赛的答题模式，提供云端的攻击终端，同学们在云端攻击平台上进行攻防实战操作，通过 Flag 判定和操作用时进行综合评分，以获得积分升级和金币奖励。

世界主要国家跨境数据流动的政策法规及其启示

引言

在科技与产业深度融合的数字经济全球化时代，数据作为战略资源在全球经济发展中的地位日益凸显，数据跨境流动已经成为全球资金、信息、技术、人才、货物等资源要素交换、共享的基础。数据跨境流动是一项综合议题，涉及国家法律、地缘政治、技术和经济安全、国家税收等各个方面，需要政策制定者构建安全有效的治理体系，进一步扩大数据的社会和经济效益。对此，世界各国一方面在国内强化战略布局和政策落实，另一方面引领数据跨境流动瞄准国际规则主导权，力争数据有效流动和自身利益最大化。这就导致各国跨境数据流动管理政策和管理体系的差异性，形成了基于数据主权独立性而产生的多重管辖权冲突和数据治理困境。

跨境数据流动的监管是一个复杂的问题，涉及数据保护、隐私和安全需求与信息跨境自由流动需求的平衡。无序的数据流动可能对国家安全利益、监管框架、执法等构成严重挑战。一方面，数据跨境流动催生新的国际经贸形式，促进科技创新，全球价值链“分工锁定”的国际政治与经济格局有望改变，需要全球治理的介入与保障；另一方面，数据跨境流动伴生数据滥用、数据垄断、数字鸿沟及数据霸权等问题，并对个人基本权利、整体国际安全与发展构成新的威胁，成为新的全球治理难题。

对此，不同国家对跨境数据流动采取了不同的监管模式，以应对数据跨境流动带来的风险。美国表面上强调数据跨境自由流动，实则实施损害他国数据主权的强势“长臂管辖”政策；欧盟则以倡导数据保护的名义向世界推广欧洲规则，通过技术进一步推进数据主权；俄罗斯通过数据本地化措施维护数据主权。为了充分维护数据主权，中国也应制定域外实践的相关规则。

对于中国跨境数据流动而言，具有异构性和缺乏标准化的特点，这使得跨境数据流动采集和处理面临挑战。近年来，中国通过设立数据出境安全

跨境数据流动的监管是一个复杂的问题，涉及数据保护、隐私和安全需求与信息跨境自由流动需求的平衡。无序的数据流动可能对国家安全利益、监管框架、执法等构成严重挑战。

评估、网络安全审查、关键信息基础设施等机制逐步完善跨境数据流动制度框架，实现对跨境数据流动的监管，促进数字经济的发展。已有相关研究涉及内容广泛，对于厘清主要国家跨境数据流动政策法规、全球跨境数据规则体系等相关内容具有一定的解释和借鉴作用。本文以美国、欧盟、日本、印度以及国际组织的跨境数据流动政策法规为研究对象，系统梳理和分析世界主要国家跨境数据流动监管措施及动向，对进一步完善中国跨境数据流动规制及加强国际合作具有重要的现实意义。

1 主要国家加强跨境数据流动的监管措施

当前，主要国家（地区）在“基于开放、动态的数据安全主权理念和兼顾安全与发展的风险规制进路”框架下，确保数据高效畅通，最大限度地挖掘数据资源红利。但是，由于不同国家处于数字经济发展的不同阶段，技术对以数据支撑的数字贸易诉求存在较大差异，对数据跨境传输采取不同程度的管制措施。

1.1 主要国家数据监管模式

由于数据使用和共享所带来的风险，需要制定适当的监管政策以保护个人隐私和公共利益。虽然许多国家已经认识到数据的社会和经济价值，但不同国家和地区的政治制度、经济、文化等方面存在差异，它们为实现数据价值最大化而采取的政策差别也很大。因此，不同国家和地区需要根据自身利益和实际情况，制定符合自身的模式，但因其制定的目标、范围、法规等方面的差异而有所不同。当前全球跨境数据流动管理模式可以划分为 3 类，其中美欧两种不同路径分别反映了各自本质立场，日、印等国家也积极寻求自由流动与安全保障相协调的规制路径。

第一，美国为了保障自身在数据领域的支配地位，采取市场为导向的全球化“长臂管辖”策略，形成“宽入严出”的“美国模式”。美国具有显著的数字竞争优势，具体围绕与数字经济相关的政策制度进行战略布局，以推动数字服务贸易发展。一方面，美国依靠其技术和经济领先地位掌握大量数据资源，倡导以企业为中心、市场为导向的“数据自由论”，允许境外数据自由流入但限制国内数据流出。如美国《数据科学战略计划》要求对数据进行存储和管理，并进行标准化建设和数据公开，以巩固其技术优势。美国制定严格的法律法规，对涉及国防、国家安全和个人隐私的数据采取严格限制，尤其禁止敏感个人数据和政府相关数据向“受关注国家”转移。2024 年 2 月 28 日，美国总统拜登签署并发布了《关于阻止受关注国家获取美国人的大规模敏感个人数据及合众国政府相关数据的行政命令》（以下简称《行政命令》），随后白宫与美国司法部陆续发布了一系列文件。相关数据包括基因组数据、生物识别数据、个人健康数据、地理位置数据、财务数据及其他可以识别个人身份的信息，同时包括与政府有关的“敏感信息”，主要针对中国、俄罗斯、朝鲜、古巴、委内瑞拉和伊朗这 6 个所谓“受关注国家”，以及与其存在关联的实体与个人。这是美国首次采取此类措施。《行政命令》在一定程度上表达出美国的数据政策和法律由鼓励自由流动向设立跨境传输审查机制的重大转变。

另一方面，美国在以追求商业利益为导向的模式下，采取“长臂管辖”措施打消其他国家采取数据本地化存储的目的。最具代表性的是美国于 2018 年出台了《澄清域外合法使用数据法案》（简称“CLOUD 法案”），确立了美国政府对境外数据的管辖权，进一步强化了“谁拥有数据谁就拥有数据控制权”的理念。

第二，欧盟从人权和技术的角度出发，采取人权至上为原则的域内效果管辖策略，形成“外严内松”的欧盟模式。欧盟强调数据流动的目的地与流出地需要有对等的人权保护力度和技术水平，立足保护公民基本权利，确立了“数据主权论”。采取统一立法与各成员国立法相结合的形式构建数据保护体系，颁布了《通用数据保护条例》（GDPR）、《关于非个人数据自由流通的规定》（FFD）及一揽子数据战略，制定成员国数据共享原则，即数据流通遵循属地原则，从而实现数据的统一认证和管辖，以此加强成员国间的数据共享，为打造数据空间奠定基础。

第三，日本、印度等国家寻求自身跨境数据流动路径，采取主动制定治理标准、分类治理和技术法律机制等策略，形成适度的本土化模式。2019 年，日本推出“基于信任的数据自由流动”（DFFT）倡议，力图打通国内和国际的双向数据流通。对内原则上禁止数据本地化存储，并不断完善关于个人信息保护的法律框架；对外在亚太地区主导构建全面且先进的跨太平洋伙伴关系协定（CPTPP），推动跨境隐私规则体系（CBPRs）的建设，试图为数字经济发展谋求更为宽松的外部国际环境和内部催生动力。

印度聚焦数据分类治理和本土技术法律机制，为个人数据、非个人数据、政府数据分别制定不同的治理框架。针对个人数据，提出“数据授权和保护架构框架”（简称“DEPA”），从技术上解决数据处理者对数据的权利以消除数据可移植性阻碍。针对非个人数据，既致力于产业数据共享，也大力推动政府数据流通利用规则制定。

1.2 国际组织助力跨境数据流动规则整合

为了促进跨境数据流动，各国在国际组织下推动合作，积极主导或参与双边、多边跨境数据流动规则制定。目前，以经济合作与发展组织（OECD）和亚太经济合作组织（APEC）为代表的许多国际组织和贸易协定已经制定了具有代表性的规则体系，这些规则体系涉及数据流动的诸多方面，如数据保护、数据安全、跨境数据流动的监管和合规等。这些国际组织和贸易协定为推动数据区域有序流动、最大限度地发挥数据红利，提供了有利的支持和指导。

第一，美欧在双多边机制中主导多项国际规则，双方既有合作也有博弈。2000 年和 2016 年，美国与欧盟经过谈判分别达成了《安全港协议》和《隐私盾协议》，核心是在充分保障个人数据主体权利前提下加强数据跨境传输的透明度，但这种方法很难成为常态机制。2020 年 7 月《隐私盾协议》失效后，标准合同条款（SCC）成为欧盟与美国数据流动的主要替代法律机制。直到 2023 年 7 月，欧盟委员会通过《欧美数据隐私框架协议》的充分性决议，美欧之间数据自由传输才得到恢复，双方试图建立稳定的跨大西洋数据制度安排。包括全面与进步跨太平洋伙伴关系协定（CPTPP）和区域全面经济伙伴关系协定（RCEP）在内的多国协议中，都对跨境数据流动规则作出了详细介绍。美国以《美墨加协定》《美日数字贸易协定》扩展在印太地区的数字经济影响力，首次成功地取消了数据本地化例外条款，提升了贸易活动中数据存储和流动的自由度。欧盟与日本达成了《欧日经济伙伴关系协定》，打造欧日双边数据自由流动圈。在美欧主导跨境数据流动之外，新加坡、新西兰和智利在 2020 年签订了《数字经济伙伴关系协定》（简称“DEPA”），成为全球首份数字经济区域协定。2022 年 8 月，正式成立中国加入 DEPA 工作组，全面推进相关进程。

第二，世界贸易组织（WTO）、经济合作与发展组织（OECD）、亚太经济合作组织（APEC）等国际组织，在多边机制中力推数据政策的公开透明和可信数据流动。充分发挥国际组织的作用，将有助于塑造全球数字经济发展新模式。WTO 强调跨境数据流动对贸易的重要作用，促进包括跨境数据流动在内的数字贸易活动。2021 年 1 月，东盟批准《数据管理框

当前全球跨境数据流动管理模式可以划分为 3 类，其中美欧两种不同路径分别反映了各自本质立场，日、印等国家也积极寻求自由流动与安全保障相协调的规制路径。

架》（DMF）和《跨境数据流动合同范本》（MCC），旨在减少谈判和合规成本，同时确保东盟国家个人数据的保护。同年 10 月，七国集团（G7）贸易部长会议发布了可信数据流动的多项原则，包括数据应当在可信的个人和商业机构间进行跨境流动等内容。

2 全球跨境数据流动的关键问题

目前，国际上尚未形成统一的跨境数据流动规制规则，在“数据保护自主权”“跨境数据自由流动”“数据安全”的三难选择下，存在国家层面、双多边规则体系呈现重复性和碎片化特点，中国数字经济发展的国际空间面临多重外部挑战。尤其是，全球初步形成数字经济发展的先后梯队，美国、欧盟、日本等国家制定并实施的系列跨境数据流动政策法规已渐成国际规则并主导未来体系建设，对中国跨境数据流动政策和实践产生重要影响。

2.1 对数据主权的争夺激化跨境数据管辖冲突

美国、欧盟、日本等国家试图通过构建符合本国利益的跨境数据流动治理规则，强化数据所有权与管辖权，形成“进攻型”数据主权战略，谋求更广阔的国际市场。俄罗斯、印度、中国等国家由于数据技术与产业实力存在差异，被迫采取“防守型”战略。发达国家主导的“进攻型”治理规则体系对全球跨境数据流动产生了深刻的影响。一是加剧了发展中国家“数字鸿沟”问题。加速数字经济发展的不平衡性，为发展中国家在公平发展权基础上追求跨境数据的国际合作权带来重大冲击。二是使中国面临被“数字同盟圈”边缘化的风险。美国、欧盟、日本三大经济体因利益趋同，将吸引更多发达国家加入其形成的“利益共同圈”，把中国排斥在外，导致中国很难通过对接发达国家主导的多边跨境数据流动规则体系实现利益最大化，并制约中国数字经济发展空间。三是主要国家获得跨境数据流动规则制定的“先行者优势”。主要国家在国际规则中占据主导地位并对后续规则的制定产生显著影响，尤其体现在相关的贸易协定和合规审查中。这对中国参与或主动制定与国际接轨的跨境数据流动规则提出了前所未有的挑战。

2.2 加强数据分类治理和管理机构建设

在分级分类治理方面，主要国家不断调整针对个人数据、产业数据、政府（行政机构）数据跨境流动的政策法规，逐渐形成相对完善的数据分级分类管理模式。在组织管理机构方面，很多国家已建立了统一高效的数据管理机构。如欧盟成立了欧洲数据保护委员会，日本成立了日本数字厅，印度了成立数据管理办公室（IDMO），韩国也在考虑建立一个数据管理部门，平衡保护数据和提供更多数据访问的关系。这就迫切要求中国学习主要国家的已有经验和做法，加强数据管理。目前，中国在数据管理方面存在的问题如下：一是在数据分类分级治理方面还缺乏详细的制度方案和评估方法，凸显核心制度供给不足、监管手段单一等问题。由于缺乏跨境数据分类分级落地细则，在个人数据保护、产业数据合规、政府数据开放共享等的实操和执法方面存疑；二是中国虽已建立国家数据局，但需要在跨境数据流动管理组织体系方面进一步提出整合方案。各部门多头管理的现实问题依然存在，社会协同治理体系尚未建立，特别是一些企业在开拓国际市场方面几乎都是单打独斗。因此，被美国信息技术与创新基金会视为全球数据限制最多的国家和“数据民族主义”的代表。

2.3 技术变革创新监管手段但也容易诱发制度失效风险

技术变革促进各国创新技术监管手段，帮助打破国家间数据流动壁垒，解决发展不平衡、技术正负效应等矛盾。一是“数据空间”作为一种新技术理念，通过提高可操作性和信任度，加强实体和个人之间的数据共享。二是印度“数据赋权保护架构”（DEPA）用于数据受托人之间统一的数据共享。这个框架将把法律原则嵌入为 DEPA 开发的技术基础设施中，为数据监管提供新的解决方案。与此同时，技术变革也对传统监管模式带来新的问题。一是技术变革带来“制度失效”风险。隐私计算技术、云计算技术的发展可能使数据本地化的监管要求流于形式，更为灵活和高效的云计算技术将凸显数据本地化的隐形成本。二是技术变革模糊了数据流入、流出的“边界”概念，欧美等地区和国家正在对中国数据企业发起“围剿”。如欧盟通用数据保护条例（GDPR）规定，无论数据控制者或处理者在欧盟境内是否设有实体机构，只要对欧盟境内数据主体的个人数据进行处理，即适用 GDPR 的规定，这意味着 GDPR 已突破地区“边界”，成为事实上“世界性适用”的法律。

3 中国跨境数据流动治理的进展与不足

随着数字经济的发展及国外政策

法规的变化，中国一直在不断完善跨境数据流动管理机制。当前，中国已初步形成“分散立法 + 专门规定”的制度框架，呈现出“鼓励流动为基础、重要数据加强审批”的基本特点。2017 年实施的《中华人民共和国网络安全法》首次从国家法律层面明确和规制跨境数据流动问题，并分别于 2021 年 6 月、2021 年 8 月颁布实施了《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》。为落实上述法律的相关规定，国家网信办分别于 2022 年 7 月 7 日、2023 年 2 月 22 日公布了《数据出境安全评估办法》和《个人信息出境标准合同办法》。中共中央、国务院于 2022 年 12 月发布了《关于构建数据基础制度更好发挥数据要素作用的意见》（简称“数据二十条”），主要内容涉及构建数据产权、流通交易、收益分配、安全治理等制度，初步形成了中国数据基础制度体系。国家网信办于 2024 年 3 月 22 日公布了《促进和规范数据跨境流动规定》，对数据出境安全评估、个人信息出境标准合同、个人信息保护认证等数据出境制度作出优化调整，并设立自由贸易试验区负面清单制度，旨在促进数据依法有序自由流动，降低企业合规成本，充分释放数据要素价值。从当前国内外数字经济发展需要来看，中国在跨境数据流动问题上，还存在一些不足和挑战。

国际上尚未形成统一的跨境数据流动规制规则，在“数据保护自主权”“跨境数据自由流动”“数据安全”的三难选择下，存在国家层面、双多边规则体系呈现重复性和碎片化特点。

3.1 立法有待加强，数据分类分级政策不够细化

当前，“数据二十条”已明确数据三权分置的战略方向，但尚未有具体有效的落地举措。中国针对数据跨境流动的法规多以原则性、概况性为主，具体条例细则还有待细化，特别是在数据的分类分级管理方面，政府需要更加注重实际操作，推动数据的分类分级管理规定一步落地。数据的分类分级需根据不同的安全等级制定不同的管理措施，以保证数据的安全和合法使用。中国现有规定更多侧重于“个人信息”保护，对产业数据仍需提出具有法律效力且有指导意义的细则文件，需要政府对行业和领域进行分级管理的指导，特别是针对发达国家管辖给中国数字企业带来的巨大挑战，如何赋予这些企业充分的数据合规动力，并指导其完成数据合规工作、更好地走向海外，变得尤其紧迫和必要。

3.2 顶层设计不足，管理机构比较分散

中国目前颁布的一系列关于数据治理的法律法规缺乏明确的战略目标，没有一套具有顶层设计意义的跨境数据规制和国际战略，尚未构建各个利益相关方协同推进的跨境数据流动机制。跨境数据流动的管理机构比较分散，部门间缺乏统筹协调。如网络安

全由公安部门分管，网络内容由网信部门分管，网络和云计算由工业和信息化部门分管，大数据产业由发展改革部门及工业和信息化部门分管，电子商务由商务部、国家发展改革委和工业和信息化部分管。2023 年 3 月组建国家数据局，表明国家高度重视数据要素的统筹管理。对此，应加强顶层设计，充分发挥国家数据局统筹规划作用，加强协调不同部门和机构之间合作，避免重复建设和资源浪费，推进全国性数据治理标准制定与执行。

3.3 国际发展态势制约，国际话语权不足

长期以来，中国的网信战略主体任务聚焦于国内信息化事业发展和安全保障，偏向于内敛型格局。因此，西方国家认为中国的数据政策阻碍了全球数据的自由流通和共享，进而不利于全球创新。具体表现是很多国际互联网公司或者科技企业无法在中国运营。一方面，引起其他国家的反对与不满，影响中国与其他国家的贸易关系；另一方面，影响中国企业在海外业务的发展。结果就是中国在国际数据治理中有限的参与度，对现有跨境数据流动规制主要依靠单边规制和国内立法，双多边合作对话缺乏造成国际话语权不足，这为中国主动对接主要国家制定的已有规则体系造成困难，难以在国际上发挥更大的影响力，阻碍中国在全球贸易中的发展。

4 完善中国跨境数据流动规制的建议

习近平总书记强调，要加强国际数据治理政策储备和治理规则研究，提出中国方案。中国应在学习借鉴主要国家规制经验的基础上，以《全球数据安全倡议》为基础，以维护中国数据主权为基本价值立场，坚持“立足安全、重视自由”的基本原则，统筹谋划数据主权和跨境数据规制的内在逻辑和外在规范，加快完善法律法规和监管方案，积极参与国际合作，形成互信、互动的多边治理模式，构建安全有序、合作共赢的跨境数据流动规制框架。

4.1 健全相关法律法规体系和基础制度，完善数据流动顶层设计

综合来看，中国应结合美国鼓励自由流动型和欧盟规制型数据政策的长处，兼顾数字经济发展的基本规律和多种数据保护的要求，完善中国跨境数据流动战略。一是尽快出台专门的顶层设计文件，以平衡安全和自由的关系为主要目标，建立统筹协调的法规体系。在制定具体跨境数据流动政策时，要综合“没有网信安全就没有国家安全”和“没有信息化就没有现代化”两方面去全面、合理、准确理解国家网信战略。二是在修订完善《刑法》《刑事诉讼法》《民事诉讼法》《合同法》等法律法规中有关个人数据和隐私保护的相关条款基础上，完善推进中国数字经济“走出去”、服务贸易发展等诸多任务要求的法律条款。

4.2 构建政府与社会联动的跨境数据流动管理体系，加强数据协调与管控能力

一方面，充分发挥国家数据局统筹管理职能，实现国内外大数据产业发展的一体化管理，将跨境数据流动作为一个独立的议题进行研究部署，统筹协调跨境数据流动政策体系，落实跨境数据流动监管措施，对企业数据跨境合规性实施监督和问责。另一方面，加强行业自律体系建设，形成内部自律与外部监督相结合的机制。建立跨境数据流动行业自律机制，促进国内个人数据和隐私保护、行业数据流动，形成数据跨境流动的多元治理模式。

4.3 建立跨境数据分类分级管理机制，完善数据出境安全评估机制

依照上位法确定“元概念”建立统一权威的分类分级体系、构建合理高效的数据跨境流动评估监管体系，以及设置国内规则与国际规则的制度对接路径。在政府公共数据、产业数据和个人数据三个大类基础上，按照数据功能对每类数据进行颗粒度更加细致的分类，对不同类型和不同级别的数据赋予不同的权限。在已出台法律法规的基础上，不断完善和落实数据出境规则，指导和帮助数据处理者规范有序申报数据出境安全评估，提升合规水平和安全防护能力。将政府数据安全评估监管与企业数据出境风险自评估有机结合，建立一个“规划先行，上下互动协调，动态可控、持续合规”的数据出境安全体系，在保证数据安全的前提下以监管促进产业发展。

4.4 参与国际规则制定，推出跨境数据流动治理的“中国方案”

一是要积极参与 WTO 框架下跨境数据流动全球治理基本原则的讨论，掌握全球发展态势。二是要积极参与 APEC、CBPR 等国际数据规则体系，增进国际互信。三是要积极探索多样灵活的跨境数据流动规制方案，充分利用“一带一路”国际合作倡议等契机，推动形成共同认可的数据保护认证、标准合同条款等机制。在 RCEP、中日韩 FTA 等双多边贸易谈判中，增加

跨境数据流动的谈判内容，尽力实现跨境数据流动规则的统一，尝试提出符合中国利益的国际规则。

4.5 探索多种数据共享模式，从技术层面实现与国际数据的互通共享

新技术可以帮助克服数据跨境流动中隐私保护、控制权等障碍，但这些技术需要较高的协调性和大量的成本。因此，政府需要探索多元化的数据共享方法，加大投入资助数据共享技术研发。一方面，要加快联邦数据分析等隐私增强技术的研发，探索数据共享伙伴关系、数据联盟、数据信托等多种模式，实现供应链的数据统筹，促进数据的纵向和横向流动，纵向通过产业联通国家和企业，横向起到跨产业交流作用；另一方面，要加强国际规则和数据标准制定，积极与国际数据空间接轨，建立安全规范的数据跨境流动方式。

4.6 开展先行先试，推进自主可控的跨境数据流通机制

在建立粤港澳大湾区数据跨境流动安全规则基础上，在海南等地也尝试建立跨境数据流动试点并形成可推广的经验，为建立与国际接轨的跨境数据流动体系奠定基础。可从数据局部流动开始，积极支持有关地方探索数据跨境流动的新模式和新路径，在数据治理规则、数据要素定价、安全评估与安全监管等方面率先进行探索，充分发挥前沿技术对规则探索的支撑作用，为数据跨境规则提供更多的基础设施与平台支持。以此为基础，推动国内外企业开展数据跨境流通业务合作，鼓励企业和研究机构进行创新和技术研发，建立跨境数据流通交换平台，不断提高跨境数据流通的效率和安全性。

5 结语

数据对经济增长、国家竞争力、科学发现和社会进步的作用日益增强，为了使数据的价值最大化，各个国家加紧制定符合本国利益的跨境数据流动政策法规和规则体系。本文重点探究考察了美国、欧盟、日本、印度等国家和地区在跨境数据流动领域的立法、政策及技术标准，以及国际合作中的单边与多边规则体系，以期对继续加强推动跨境数据流动规则中的中国方案提供参考。中国应在数据政策法规顶层设计、数据协调与管控能力、数据出境安全评估、国际规则制定、地方先行先试等方面持续发力，积极构建数据安全合规有序的跨境流通机制。

本文来源：《中国科技资源导刊》

关于作者

杨晶

中国科学技术发展战略研究院副研究员，主要研究方向为科技创新理论、国家创新体系、数字化转型。

霍佳鑫

中国科学技术发展战略研究院副研究员，主要研究方向为科技创新理论、国家创新体系、数字化转型。

一体化 vs. 模块化，谁才是 SOC 的未来?

目前，主要网络安全企业都在努力进入安全运营（SOC）领域。众所周知，最近业界发生了多起并购整合、发布了多个 SIEM 平台：Palo Alto Networks 收购 IBM 的 QRadar、CrowdStrike 宣布推出其完整的 SIEM 平台，LogRythmn 和 Exabeam 合并成为一个平台；Zscaler 收购 Avalor，Fortinet 也推出了 SIEM 产品。

但目前，还没有一个平台能够满足 SOC 的所有技术要求。实际上，未来 SOC 领域不太可能出现一个主要平台——至少在短期内不会。CrowdStrike 导致的全球 IT 基础设施瘫痪事件，意味着企业安全领导者会毫不犹豫地从单一厂商购买整个技术堆栈，以避免将来再发生这种情况。

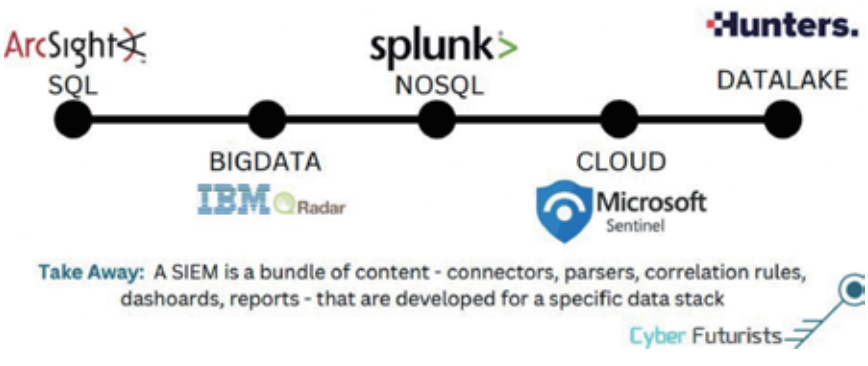
但目前，还没有一家机构能完整构建这种 SOC 技术平台。该平台涵盖大型平台主导的所有领域，提供从数据管道、数据采集、分析到自主应对威胁的统一系统。大型厂商有动力推广一体化战略。不过，相信未来业界可以实现“SOC 内的模块化整合”，即拥有符合安全需求的模块化 SOC，从而可以为 XDR/SIEM、自动化或数据管道选择最佳解决方案。

这一前提的大部分原因，在于目前仍没有一家成功的一体化 SOC 公司。Splunk 目前在 SIEM 市场占据主导地位，但 Splunk 不受欢迎，且在被思科收购后，未来几年可能会走下坡路。成功的网络安全企业在各自领域赢得了声誉，如 CrowdStrike 在终端领域、Wiz 在云安全领域、Okta 在身份领域。但在 SOC 市场上，可能很长一段时间都不会拥有公认的顶级品牌。

一、SOC 的发展历程

多年来，SIEM/SOC 市场经历了许多转型，从 ArcSight 到 Splunk，再到市场上新兴的原生解决方案。对于需要存储数据的企业来说，可用的解决方案一直不缺。

深入研究基础安全知识，会了解



到，安全运营中心 (SOC) 的主要目的是持续监控、检测、分析和应对组织内的网络安全事件和威胁。安全运营中心 (SOC) 是网络安全的中央枢纽，利用各种技术来检测和应对安全威胁。其所使用的一些核心技术包括 SIEM、SOAR、EDR、NDR、CASB、VM、IAM、TIP 和 UEBA。大多数 SOC 都将终端安全作为技术的核心，其中许多解决方案会持续监控终端和整个网络的可疑活动。

SOC 的核心是 SIEM。SIEM 背后的核心前提是收集数据、分析数据并根据检测规则发送警报。SIEM 系统会汇总、分析和关联来自组织内各种来源的安全事件数据，以实时检测、监控和应对安全威胁。它们通过识别异常或可疑活动来提供集中可见性并促进事件响应。

SIEM 的最终输出始终由安全自动化解决方案处理。当 SIEM 检测到任何工具中的安全事件时，就会触发 SOAR/ 自动化解决方案，根据预定义的剧本自动执行某些响应操作。例如，如果检测到未经授权的访问，SOAR/ 超自动化平台可以自动启动协议，以更改密码或关闭账户。

二、当前 SOC 的范式

近年来，网络安全工具已经发生了巨大变化。过去几年市场快速发展，SIEM 领域出现了越来越多的供应商，但在 Gartner 2024 年 SIEM 魔力象限中，排名靠前的多家供应商在最近数月经历了重大组织和业务变化。很多供应商在开展并购活动，以合并成为更强大的参与者。

与此同时，SOC 的工具堆栈也得到了大幅扩展。现在，企业在努力收集和存储大量数据的同时，还试图平衡相关成本。大多数企业系统在实现可扩展的数据收集时，都会不可避免地增加成本，这使得组织不得不在管理成本和财务约束之间做出选择。因此当前存在一条成本 – 生产率曲线，客户必须根据可用数据的获取成本来管理其规模。这种价格的复杂性和广泛的数据点促成了 Cribl 和 Anvilogic 等公司的崛起和成功，这些公司在安全数据到达 SOC 之前发挥着关键作用。

三、对大型 SOC 平台的评价

1.CrowdStrike

CrowdStrike 在业界提出打造完全一体化的平台，并在 RSAC 会议上宣布了其完整的 AI 原生 SOC 平台。该平台建立在其最初的 SIEM/ 日志管理平台之上 (收购 Humio 之后启动)。在最近的公告中，CrowdStrike 又增加了一种解决方案，将更多的 AI 工作流自动化融入到已获得的从终端 / 云数据生成的现有告警中。

CrowdStrike 还宣布了平台的多项增强功能，包括改进了快速数据摄取功能，为 AWS、Azure 和 GCP 提供更好的连接器，以及使用高级 AI 实现数据自动规范化，以实现准确的检测和响应。CrowdStrike 的 SOC 平台还集成了 Charlotte AI，这是一款生成式 AI 安全分析师，能以通俗易懂的语言提供解决方案，并自动开展调查，使搜索速度提高 150 倍，成本降低 80%。新的提示词和 Falcon Fusion SOAR UI 还增强了工作流程自动化，简化了检测、调查和响应，从而实现更好的数据处理和缩短安全事件的响应时间。

Crowdstrike 在 SIEM 竞争中的优势

Crowdstrike 的 Falcon Next-Gen SIEM 的一个重要特性是其单代理、单平台架构，可统一本机数据和第三方数据。SOC 团队都知道，端点 / EDR 数据是使用 SIEM 时必须处理的最大数据集之一。

CrowdStrike 认为，自己可以让客户将部分端点数据指向其打造的 SIEM。终端数据处理起来也很复杂，需要复杂的工程来处理极端情况、减少重复等。CrowdStrike 宣布了一个利用人工智能自动解析和规范化的系统，该系统丰富了数据，以更好地识别和确定威胁的优先级，并支持高级威胁检测和自动响应机制。

CrowdStrike 计划整合 Fusion SOAR 自动化解决方案，来完成 SIEM 的响应和补救。作为最大的 EDR 供应商之一，通过添加合适的增强功能，CrowdStrike 可以轻松将使用相同终端的客户迁移进入其 SIEM 解决方案。

2.Palo Alto Networks

五年前，Palo Alto Networks 收购了 Demisto，该公司的产品是最接近完全一体化的产品，涵盖了从终端代理到安全数据湖和 SOAR 的一系列产品。

为了进一步加强其 SIEM 解决方案的战略转型，Palo Alto Networks (PANW) 收购了 IBM 的 QRadar。此次收购标志着 PANW 改变了其近期专注于收购前沿技术，以填补其平台空白的策略。

相反，PANW 正在迅速采取行动以确保市场份额。此次收购使 PANW 成为 SIEM/ 安全分析市场前三大供应商之一，预计到 2026 年该市场规模将超过 200 亿美元。

QRadar 历来占据 12% 的市场份额，此次收购大大提升了 PANW 的地位，旨在将 QRadar 本地 /SaaS

客户过渡到 PANW 的 Cortex 平台(XSIAM)，该平台已被公认为 XDR 领域的领导者。

PANW 估计，此次迁移将带来超过20亿美元的总合同价值(TCV)机会。IBM 的 QRadar 资产（包括 QRadar SOAR 和 Randori Recon）现在将归 PANW 所有。此次整合预计将加速 PANW 的市场渗透。

PANW 于 2022 年年初推出的 Cortex XSIAM 将从这一扩大的客户群中受益匪浅。最大的好处之一是，此次合作将使 IBM 成为 PANW 经销商和集成合作伙伴，拥有 1,000 名接受过 PANW 产品培训的 IBM 顾问，以处理非战略性任务。此次收购和合作凸显了 PANW 巩固其在 SIEM 市场地位的战略举措。PANW 旨在利用 IBM 现有的客户群和技术资产来增强其 Cortex 平台。

3.SOC 一体化的评价

CrowdStrike 和 Palo Alto Networks 持续推动 SOC 领域的供应商整合。实际上，2024 年网络安全行业一直强调供应商整合的紧迫性。主流安全厂商自然有理由积极推动。

在这种情况下，供应商选择将其大多数平台与一家供应商进行整合。在大多数情况下，安全厂商会将其所有数据发送到 SIEM，并围绕平台供应商构建其 SOAR、XDR、威胁情报、云日志和其他产品。这是领先的大型安全厂商推动的策略。

一体化 SOC 的优点

简化安全基础设施：将安全工具集成到单一平台可简化安全基础设施，减少安全团队需要管理的工具和供应商数量。这种“单一管理平台”方法可简化操作，并最大限度地降低合同、关系和集成工作的复杂性。

增强告警上下文：统一平台通常附带大量威胁情报数据，为安全分析师提供 SIEM 生成的警报的更丰富上下文（这可能会减少警报）。例如，像 Palo Alto Networks 这样拥有现有云和网络安全产品组合的公司，可以关联并提供跨安全领域的更广泛可见性，从而增强其威胁检测和响应能力。

集中管理：部署 SIEM 通常涉及在多个系统上安装代理。让单个供应商集中管理这些传感器，可以简化部署和管理，提高效率并降低开销。

一体化 SOC 的缺点

供应商锁定：依赖单一供应商提供多种安全解决方案存在供应商锁定风险。如果组织对供应商不满意，或者供应商遇到问题（例如，中断——最好的例子是 CrowdStrike 目前的问题），由于系统和数据依赖关系的深度集成，更换供应商可能会很困难，而且成本高昂。

定制化和灵活性降低：大型供应商通常设计其平台以吸引广泛的市场，这可能会限制定制化和模块化选项。集成解决方案可能会变得复杂且臃肿，充斥着不必要的功能，对于有特定需求的组织来说，这会使其变得繁琐且难以管理。

成本逐年增加：虽然初始集成可能会带来成本效益，但供应商可能会随着时间的推移提高价格，尤其是在管理计算和存储方面的数据摄取成本方面。随着使用量的增加，Splunk 等平台的集中化功能可能会导致成本增加。

行业特定要求：不同行业具有独特的安全要求。例如，金融和保险等监管严格的行业可能更喜欢采用集中式方法的传统 SIEM 解决方案，而以消费者为中心的企业可能需要更加模块化和灵活的 SOC 设置。集成平台可能无法同样好地满足这些不同的需求。

实际情况是，组织可以做出明智的

决策，将安全工具集成到统一平台中，平衡简化管理和增强环境的好处与供应商锁定和降低灵活性的风险。

四、最佳 SOC 评价（及未来可能）

如果未来的 SOC 没有完成一体化整合，就可能会更加模块化，尤其是在进入生成式人工智能的新型攻击所主导网络安全世界时，我们需要专门的解决方案来应对可能出现的各种威胁。

这种安全检测和响应架构强调标准化、灵活性、数据所有权、成本效益和采用先进技术的原则，尤其是大语言模型带来新架构变革。

这一概念已发展成为无头 SIEM，即安全数据架构产品（安全数据湖、SIEM、数据仓库、XDR 等）仅仅专注于安全数据处理、分析和管理。其功能性可通过 API 或某些命令行界面进行访问和管理。

一体化 SOC 平台可以减少 SOC 团队所需的工具数量，但推动 SOC 整合的最大驱动力在根本上是管理成本，并能应对最重要的威胁。

1. 模块化 SOC 核心组件

笔者不主张在 SOC 中整合大量（30 个以上）解决方案，而主张采用由同类最佳方案组成的 SOC 架构，该架构有三个主要组件作为 SOC 的核心组件（这是一个简单的模型，因为许多组织都有不同的堆栈，但从研究来看，这大体上是一个很好的框架）：

- 预数据处理器和 ETL 解决方案
- 安全数据分析与存储引擎
- 自动化解决方案

模块化安全架构围绕数据编织概念（Data Fabric）构建，Gartner 将其定义为一种架构和一组数据服务，可在混合和多云环境中提供跨终端的一致功能。它旨在使数据在各种系统中更易于访问和使用，从而实现数据管理和集成的简化。

（1）预数据处理器和 ETL 解决方案

这是一个新兴类别，自 IT 和安全数据引擎 Cribl 诞生，就经历了迅速增长，ARR 已达 1 亿美元。这些供应商是安全工具和 SIEM 的中间人，一旦模块化 SOC 采用了这些供应商的产品，就会显著降低成本和警报，理想情况下是在 SIEM 内部，这是 SOC 面临的最大挑战。

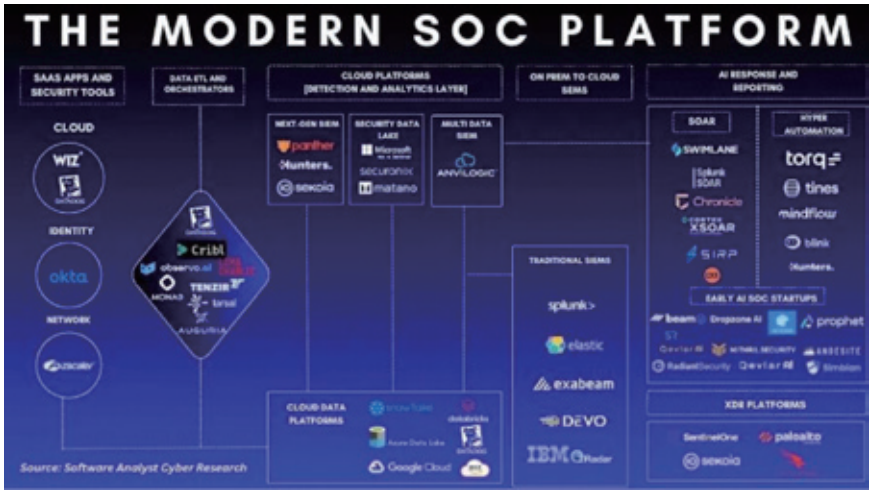
这里有两种类型的厂商：

数据管道和 ETL 供应商：这些供应商专门从各种来源收集数据，包括来自不同安全应用和 IT 系统的日志、事件、指标和跟踪数据，然后整理、转换这些原始数据集，并将其规范化为更易于分析的结构化格式，其中包括规范化数据和过滤掉不相关的信息。这一类别有许多供应商，如 Tarsal、Monad 等。

数据路由供应商：这些供应商专门在数据进入 SIEM 之前对其进行优化和丰富。可以使用上下文信息（如威胁情报源、用户身份信息和地理位置数据）丰富数据，从而为安全告警和事件提供更多背景信息。处理完数据后，这些编排器会将其路由到适当的目的地，无论是 SIEM、数据湖、分析平台还是其他存储解决方案。这一类别有许多供应商，其中包括 Cribl 等知名公司，以及 Observo.ai 等新兴公司。

（2）安全数据分析和存储解决方案

传统的一体化 SIEM 供应商通常占据主导地位。目前企业可以使用四种类型的架构——一是公认的 SIEM，此外还有新兴的多数据 SIEM（如 Anvilogic）、基于 EDR 构建的 XDR



解决方案，以及数据仓库解决方案（如 Snowflake）。

大型组织有使用 Databricks 和 Snowflake 等数据湖技术进行标准化的案例，亚马逊安全湖等产品也可以发挥作用。这在今天很有意义，未来，我们将看到具有令人信服安全用例的新数据管理平台。在这些部署方法中，企业可以采用开放网络安全架构框架（OCSF）等标准，以确保数据格式一致，以及更轻松与未来支持 Gen AI 的产品集成。

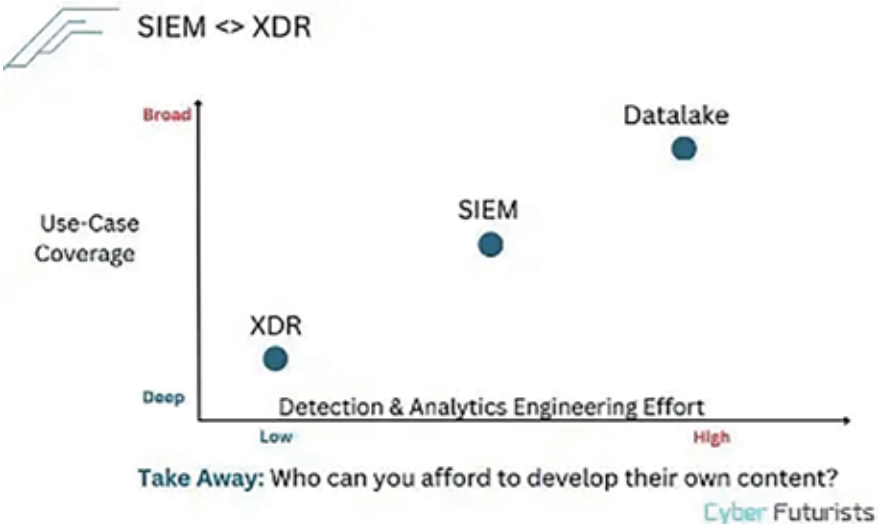
Securonix 应用研究总监奥利弗·罗奇福德（Oliver Rochford）所说，如果一家企业拥有更多具备检测工程技能的建设者原型 / 安全人才，可能会更倾向于数据湖选项，反之亦然。

A. 联合数据模型该模型还催生了一种日益流行的趋势：联合数据模型，这是一种分散的数据管理方法，其中数据仍保留在其原始位置，但可以在不同的系统和环境中访问和查询。由于当今架构中的不断变化和数据量，该模型不是将所有数据移动到一个存储库，而是允许不同团队和部门实时访问和分析共享数据，从而促进彼此之间的协作。它还通过将数据保留在其原始环境中来增强数据主权和安全性，从而降低与数据传输和存储在集中位置的相关风险。

B. 更符合涉及 AI/LLM 的未来架构此外，检索增强生成 (RAG) 可以让企业利用大型语言模型 (LLM) 来访问和分析自己的数据——检索增强生成 (RAG) 允许安全数据成为查询 LLM 模型提示词的一部分，从而为安全数据提供巨大的检测洞察力，并实现强大的威胁狩猎功能。

(3) 自动化解决方案

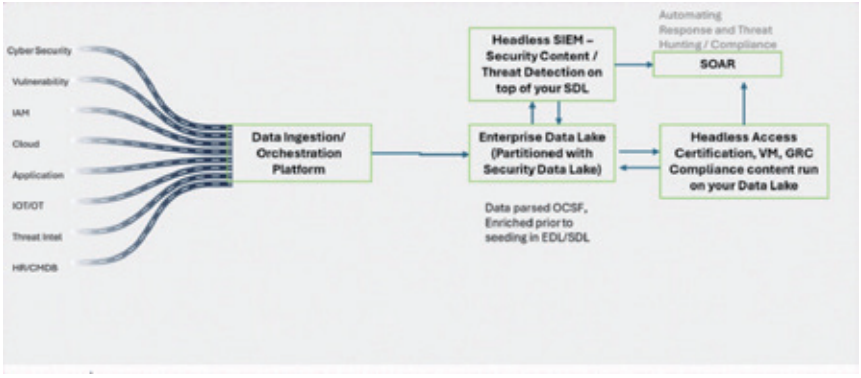
公司可以采用更加模块化的一流自动化技术来执行重复且耗时的任务。传统 SOAR 供应商面临的最大挑战是构建工作流程的成本和巨大的实施工作



量。对于许多想要专注于重要告警的 SOC 团队来说，为新类型的威胁和规则开发和维护自动化剧本可能很复杂。可以借助 Torq 等更现代的超自动化解决方案或 Intezer 等 Tire 1 解决方案，这些解决方案可以根据预定义规则和机器学习算法对告警进行过滤和优先排序。这减少了 SOC 团队需要分析的误报数量，并突出显示需要立即关注的最关键告警。这些解决方案有助于加快检测和响应时间，同时最大限度地减少人为错误，并提高威胁检测和事件响应的准确性。

2. 选择模块化 SOC 架构的原因

它之所以能成为许多组织的通用框架，原因如下：



基于合规要求的垂直解决方案：不同行业具有独特的 SOC 要求或需要遵循的合规性协议。例如，由于严格的法规，金融服务需要集中式 SOC，而 AI/云原生公司则受益于分布式架构。这种多样性使得很难对 SOC 应用采用通用的方式。组织可以根据特定安全功能需求选择最佳解决方案。这种灵活性确保可以部署专门的工具（如入侵检测或恶意软件分析工具）来有效满足特定需求。

成本效率：尽管人们认为将采用一家企业的一体化解决方案，可以有效管理成本，但根据研究，没有有效的证据表明，企业长期使用大型平台可以节省成本。前期成本较低，但会随时间推移而增长。相反，使用最佳方案组合则可以降低成本，因为企业可能会采用最佳存储引擎，从而实现成本优化。如果需要处理更多实时、热数据的用例（如媒体公司等），则可以使用 XDR 或安全数据湖。企业还可以部署专门的工具，来优化安全技术的支出。这种部署方式通过将高优先级安全数据从常规日志中分离到替代的低成本解决方案，有助于实现数据湖优化和成本效益。

可扩展性问题：随着新威胁的出现或组织网络的扩展，最佳方案组合的 SOC 可以更轻松进行扩展。这种模块化方式可以在不造成重大系中断的情况下进行增量升级和变更，从而促进增长和采用。例如，随着 Airbnb 的员工从 600 多名发展到 6000 多名，所面临的安全数据挑战也在不断演变，这促进了创业公司 Panther Labs 的成立。

冗余和弹性：使用来自不同供应商的多种解决方案，可提高安全运营的冗余和弹性。CrowdStrike 引发的全球 IT 故障很好地证明了这一观点。如果一种技术解决方案出现故障，其他解决方案可以维持安全运营，最大限度地减少宕机时间，并增强整体安全性。

五、未来的 SOC 会怎样?

总之，一体化综合 SOC 简化了操作、降低了复杂性并通过集成平台增强了警报上下文，但它的“一刀切”原则，同时带来了一些风险，包括供应商锁定、有限定制化及成本随着时间不断上升。

相反，模块化 SOC 具有针对特定安全功能量身定制的最佳解决方案的优势，具有更大的灵活性和可扩展性，并通过与多家供应商的合作鼓励创新。尽管存在管理复杂性、集成性和潜在告警疲劳（取决于组织的具体环境）的潜在挑战，模块化 SOC 却能够提供专业化、高弹性且适应性强的安全解决方案，这使其成为旨在保持强大和动态的网络安全态势的组织的最佳选择。

需要注意的是，各种组件都需要整合，但在 SOC 内，通过架构模块化，企业可以在攻击形势发生变化时随时替换任何组件，同时保持对安全基础设施的完全控制。模块化架构允许轻松更换或升级单个组件，确保对安全基础设施的适应性和控制力。



关于作者

弗朗西斯 · 奥杜姆

加拿大网络安全研究员和独立分析师，曾在 Investi Analyst 担任网络安全和 AI/ML 投资人。

AI 语言模型应用中的数据安全挑战与应对策略

近年来，随着人工智能领域的迅猛发展，各种 AI 语言模型如雨后春笋般涌现。这些模型通过学习海量数据，便能够生成高质量的内容。用户只需输入具体需求或提供参考性文档资料，即可一键生成所需的文章，这在一定程度上极大地提升了工作效率。然而，用户在处理组织敏感数据时，如果不正确使用或忽视数据安全的重要性，就有可能给组织的敏感数据带来严重的安全隐患。

从合规角度来看，AI 语言模型应该严格遵守行业规范，按规定履行算法备案手续和合规义务，遵循合法性、公平性、透明度、目的限制、数据最小化、准确性、存储限制、完整性和保密性等原则，从而确保为用户提供高效服务的同时保障用户数据安全，避免违规收集或使用用户上传的数据。

尽管如此，当前 AI 语言模型种类繁多，其中难免会有某些模型存在违规收集用户输入数据的问题，这无疑给组织的数据安全带来了潜在风险。因此，在应用 AI 技术的同时，必须高度重视数据安全问题。

一、数据安全风险

（一）个人原因造成数据泄露

因个人原因造成的数据泄露包括无意识的数据泄露和有意识的数据泄露，这两种情况都有可能给组织的敏感数据带来安全隐患。

无意识的数据泄露：用户在使用 AI 语言模型时，可能在不知道自己的操作存在风险的情况下，不经意间上传了敏感信息，如组织的敏感文档。

有意识的数据泄露：少数用户在使用 AI 语言模型时，明知组织不允许将敏感文档上传到互联网平台，但出于尽快完成交付的工作压力，有意的将组织的敏感数据上传到 AI 语言模型中。

（二）平台原因造成数据泄露

目前 AI 语言模型种类繁多，虽然人工智能相关的监管政策明确要求禁止违规收集和使用用户的输入数据，但目前 AI 语言模型良莠不齐，这其中不乏存在一些模型正在违规收集和使用用户上传的组织敏感数据，而用户对此状况并不知晓。这些模型在收集用户上传的组织敏感数据之后，可能因自身存在安全问题、不合规处理或系统漏洞，而导致这些数据的二次泄露。

模型自身安全：部分 AI 语言模型自身存在安全问题，可能将训练数据中的内容作为输出展示给使用模型的用户，即大模型的数据泄露问题。如果用户的输入被违规收集和使用，极有可能因上述原因造成所收集的数据的二次泄露。

不合规处理：部分 AI 语言模型可能存在不合规的处理，比如，未经许可收集用户数据，并将其用于非法目的，从而损害用户的隐私和安全。

系统漏洞：部分 AI 语言模型违规收集用户输入的数据后，因存储数据的操作系统存在漏洞而遭受黑客攻击，也可能导致数据二次泄露。

二、应对策略

为了有效应对与人工智能相关的数据安全挑战，建议组织在使用 AI 语言模型时采取以下措施。

（一）技术措施

1. 分类分级

为了妥善管理存储在工作机中的大量组织敏感数据，我们需要建立健全业务数据安全分类分级管理机制。首先，在梳理本机构业务数据资产目录的基础上，依据国家、行业相关的数据安全标准和最佳实践，制定覆盖全部业务数据的标准和数据安全分类分级清单，详细列出每种数据类型的重要性和敏感性水平，并明确区分敏感数据和非敏感数据。根据不同类别和级别，设定相应的访问权限和控制措施，明确规定哪些数据不应上传至AI语言模型或其他外部系统，以防止敏感信息被不当收集或使用。实

施数据安全分类分级后，定期进行审查和更新，以防止数据泄露和越权使用。

为了进一步提高数据分类分级的效率和准确性，可采用基于国家、行业数据分类分级标准的敏感数据深度识别模型，利用先进的数据识别工具和技术，比如，深度学习算法和自然语言处理技术，来识别和标记敏感信息，高效且准确地识别和管理敏感数据，形成一个完整的敏感数据资产目录清单，确保数据分类分级工作的准确性和全面性，并对文件内容、组织敏感信息等进行多维度快速检索。通过以上方法，更好地了解数据的分布情况，从而更加有效地管理和保护组织的数据资产。

2. 风险监测

基于数据流动全程及数据全生命周期持续感知评估风险，对终端敏感数据运行过程进行无改造映射，自动标注敏感数据，并跟踪数据状态变化过程，持续监控数据传输的敏感度、分类分级、频率、数据的数量和目的地等，跟踪敏感数据在 AI 语言模型和终端之间的运行流转轨迹，完整追溯敏感数据流转过程，并快速识别敏感数据流出业务范围或越权上传等风险，通过实时监控和异常分析，及时发现是否存在向 AI 语言模型上传组织敏感数据的行为，并采取措施有效预防数据泄露。这意味着不仅要定期检查数据传输的日志，还要利用先进的深度数据内容识别技术、基于人工智能的数据安全风险分析技术来识别异常模式，如敏感数据流向有风险的目的地的情况。一旦检测到可疑行为，应立即启动风险处置流程，包括但不限于告警、切断数据传输、隔离受影响的系统、调查事件原因等，从而有效减少数据泄露的风险，并确保组织的敏感信息得到妥善保护。

3. 安全防护

构建数据安全管控体系，加强数据全生命周期的安全防护能力。对敏感数据进行自适应细粒度的精准防护，针对不同的业务部门、用户角色、数据分类及不同的数据安全风险等级，执行细粒度的访问控制策略，如禁止未经许可的数据上传至 AI 语言模型，并设置警报机制，以便在未经授权的情况下立即触发警告。对高敏感级别的数据进行加密处理，确保即使数据被不合规的上传，也不会泄露文件内容。同时，应定期审查和更新安全策略，以适应不断变化的安全威胁，确保安全措施的有效性和时效性，包括但不限于定期评估现有安全措施的效果，引入新的技术和方法来加强数据保护，并根据最新的安全趋势和法规要求调整策略。

（二）组织管理措施

建立健全数据安全治理体系，制定常态化的数据安全风险评估机制，并定期进行全面的系统评估。定期组织员工进行数据安全和隐私保护的专业培训，提高员工对于 AI 语言模型使用过程中潜在风险的认识，强调遵守相关法律法规的重要性。

（三）个人安全意识培养

在使用任何 AI 语言模型之前，个人应仔细阅读其隐私政策，了解数据如何被收集、存储和使用，在使用中谨慎分享组织敏感数据，并注意选择合规且具备安全措施保障的 AI 语言模型提供商。

（四）AIPC 方法

AIPC（AI Personal Computing Device），作为一款集成人工智能算力的个人设备，能够在本地设备上处理数据和运行 AI 语言模型，这意味着数据不必上传到云端，通过本地化处理技术手段来减小了数据的泄露风险面，解决 AI 语言模型使用计算中的数据泄露问题。与此同时，AIPC 要获得较好的表现，需要硬件的高配支持，这会导致价格偏高，产品性能和用户体验尚需时间优化，可能限制其在市场侧的普及。

三、小结

当前，人工智能技术正迅猛发展并日益深入地融入我们的日常生活和工作，虽然 AI 语言模型为我们带来了诸多便利和正向影响，但也伴随着数据泄露等风险和问题。因此，我们在使用 AI 语言模型时应该时刻保持警惕，并采取适当的安全措施来保护组织的敏感数据，如本文提到的数据分类分级、风险监测、安全防护等技术手段，加强组织的数据安全管理，提高个人的安全意识，通过一系列措施，确保我们在应用 AI 语言模型的同时，有效保障组织敏感数据的安全。

关于作者

郭灵

CCIA 数据安全工作委员会，北京数安行科技有限公司。

华云信安

以人才梯队为依托，以自主创新为核心，深耕网络空间安全产业

华云信安(深圳)科技有限公司（简称 华云信安™ ）成立于2016年，是一家深耕于网络空间安全领域，拥有自主研发能力及核心知识产权，提供网络安全解决方案与技术服务的高新技术企业。华云信安™总部位于深圳，在广州、上海、武汉设有分支机构，公司核心团队来自奇安信、网易、华为、绿盟、思科等国际知名科技企业，具有深厚的网络安全技术实力和管理经验。

华云信安™目前拥有数十项计算机软件著作权和十余款自主研发产品，具备“风险评估类”和“安全工程类”两项信息安全服务资质，通过ISO9001质量管理体系认证，现为深圳市信息安全行业协会理事单位和深圳市信息网络安全管理协会会员单位。

华云信安™凭借创新的网络安全产品体系、深厚的网络安全服务能力以及丰富的服务经验，为互联网、金融、能源、制造、交通、医疗、政务等领域的广大客户，提供专业优质的网络安全产品、网络安全解决方案和网络安全技术服务。

网络犯罪研究中心

华云信安·网络犯罪研究中心，是专注于打击网络犯罪的安全服务部门，致力于打击涉网新型犯罪领域的安全技术研究与产品研发，包括涉网犯罪案件技术支撑、网络诈骗案件技术支撑、涉众型经济犯罪案件技术支撑等，以攻防实验室和极牛技术社群组成创新型的安全研究团队，为国家及各省市公安机关提供高效专业的打击涉网犯罪情报分析服务和实战解决方案。

极牛攻防实验室

华云信安·极牛攻防实验室，由内部成员及外部知名技术专家团队组成，致力于最前沿网络安全技术的研究和调研，以指导技术研发路径和产品发展方向。其职责除开展传统的网络安全技术研究外，还跟踪国内外网络安全技术趋势并进行相关技术研究。现已协助国家互联网应急中心(CNcert)发现并修复数百个安全漏洞，获得数十张高危原创漏洞证明证书。

涉网犯罪对抗　护网重保服务　安全咨询服务　安全保障服务　安全培训服务

丰富的解决方案

我们提供卓越、丰富的信息安全产品及各行业解决方案、信息安全技术服务和基础架构咨询服务。

专业的团队服务

我们拥有资深、专业的服务团队，按需为用户提供多元化、多级别的咨询规划服务和技术实施服务。

众多的行业案例

我们拥有众多行业应用案例，包括制造、快消、航空、金融、物流、建筑、服务、互联网等行业。

深入的厂商合作

我们与多家国内外知名厂商建立战略合作关系，共同致力于优质解决方案及相关服务的推广落地。

全国范围的服务

我们公司总部在深圳，同时在上海、广州、武汉等设有分支机构，具有全国范围内的业务服务能力。

公众号 小程序 官网

网安观察

没有网络安全就没有国家安全



7436084028