极牛网络安全通讯 • 社群期刊

2025 年 5 月 第 47 期

网安观察

第47期

2025年5月

CONTEN

目录

安全态势

国际视野

P8
美国白宫发布2026财年预算提案，拟削减网络安全预算4.91亿美元

ONTENTS

专题报道

第 47 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

政策篇

国内，国务院部委单位积极出台产业数字化政策，统筹推进发展与安全。《关于加快推动银行函证数字化发展的通知》《医药工业数智化转型实施方案（2025—2030 年）》《关于加快推进教育数字化的意见》《人工智能气象应用服务办法》等文件先后发布；

国际上，美国近十年来或首次削减联邦网络安全预算。美国白宫发布 2026 财年预算提案，拟削减网络安全预算 4.91 亿美元，并重新定位 CISA 使命，聚焦联邦网络防御和关基安全韧性，缩减反虚假信息、国际协作等职责。

国内

财政部、金融监管总局发布《关于加快推动银行函证数字化发展的通知》

5 月 16 日，财政部、金融监管总局发布《关于加快推动银行函证数字化发展的通知》，要求建设安全、便捷、高效、经济的银行函证体系。该文件提出，压实各方责任，统筹保障银行函证平台运营的安全性、连续性、稳定性；掌握平台知识产权，确保平台核心底层技术的独立、自主、可控；提升平台安全性，中国注册会计师协会会商银行函证平台建设方制定、发布银行函证平台信息安全标准，相关银行函证平台建设方组织第三方机构对相关银行函证平台统一实施评估认证，并将结果提供给平台用户。

《儿童手表安全技术要求》强制性国家标准公开征求意见

5 月 13 日，工业和信息化部组织完成了《儿童手表安全技术要求》强制性国家标准（征求意见稿）的编制工作，现公开征求意见。该文件规定了儿童手表的安全技术要求，描述了相应的试验方法。在网络安全方面，该文件对信息安全、数据安全和个人信息保护、内容安全三方面做出要求，包括儿童智能手表应具备产品维保周期内操作系统安全升级的功能、具备应用程序被预置或安装时的安全管理机制、支持开机和锁屏时的密码保护、制定专门的儿童个人信息处理规则、建立儿童专属内容池、具备阻断生成式语音问答应用程序安装的功能、建立对儿童智能手表向儿童提供信息内容进行持续内容安全监测机制等。

国务院 2025 年预备制定网络安全等级保护条例

5 月 14 日，国务院办公厅印发《国务院 2025 年度立法工作计划》，其中多项内容和网络与信息安全相关，包括制定政务数据共享条例，预备制定网络安全等级保护条例、终端设备直连卫星服务管理条例，预备修订政府信息公开条例、互联网信息服务管理办法、反间谍法实施细则，推进人工智能健康发展立法工作。此前公安部于 2018 年 6 月公布《网络安全等级保护条例（征求意见稿）》对外公开征求意见，时隔 7 年后，该文件终于迎来新进展。

李强主持召开国务院常务会议，审议通过《政务数据共享条例（草案）》

5 月 9 日，国务院总理李强主持召开国务院常务会议，审议通过了《政务数据共享条例（草案）》。会议指出，要在确保数据安全基础上打通数据壁垒，推动公共服务更加普惠便捷。要构建全国一体化政务大数据体系，推动数据资源融合应用，更好赋能社会治理和繁荣产业生态，增强经济发展新动能。

中国人民银行发布《中国人民银行业务领域数据安全管理办法》

5月9日，中国人民银行发布《中国人民银行业务领域数据安全管理办法》，自2025年6月30日起施行。该文件共7章56条，包括总则、业务数据分类分级与总体要求、全流程业务数据安全管理要求、全流程业务数据安全技术要求、业务数据安全风险与事件管理、法律责任、附则。该文件要求，业务数据安全工作遵循“谁管业务，谁管业务数据，谁管数据安全”原则，数据处理者应当履行数据安全保护义务，防范业务数据被篡改、破坏、泄露或者非法获取、非法利用等风险。中国人民银行业务领域是指由中国人民银行承担监督和管理职责的货币信贷、宏观审慎、跨境人民币、银行间市场、金融业综合统计、支付清算、人民币发行流通、经理国库、征信和信用评级、反洗钱等业务领域。

自然资源部印发《地理信息数据分类分级工作指南（试行）》

5月7日，自然资源部印发《地理信息数据分类分级工作指南（试行）》。该文件主要内容包括：一是明确地理信息数据分类分级原则。在数据分类、数据分级、目录管理与更新等各环节均应遵循“科学实用、综合判定、动态更新”原则。二是确定数据分类规则。将地理信息数据分为基础地理信息数据、遥感影像数据和专题地理信息数据三大类，大类下再细分若干中类，同时可根据数据管理实际和应用服务场景再细化分类。三是提出数据分级规则。确定了识别地理信息数据分级因素、开展数据影响分析和综合评估定级的分级规则，同时给出了重要数据、核心数据识别的判定指标。四是明确分类分级管理要求。规定了地理信息重要数据目录申报、审核、认定等相关工作程序，以及动态更新情形与更新管理等若干要求。

强制性国家标准《卫星导航定位基准站网与安全管理要求》公开征求意见

5月6日，自然资源部组织起草了《卫星导航定位基准站网与安全管理要求（征求意见稿）》强制性国家标准，现公开征求意见。该文件规定了卫星导航定位基准站网安全管理的基本要求，以及设施、数据和服务的安全要求，包括卫星导航定位基准站网数据中心应配置网络安全防护专用设备和数据安全防护措施，卫星导航定位基准站网的数据处理、服务和管理系统应取得信息系统安全等级保护第三级及以上备案证明，卫星导航定位基准站原始观测数据应采用有线专网或商用密码加密保护后进行传输，卫星导航定位基准站网的其他重要数据应采取用户实名审核注册、鉴权访问控制的方式提供服务，单个基准站提供实时差分定位服务时应采用虚拟基准站技术等。

七部门联合发布《终端设备直连卫星服务管理规定》

4月30日，国家互联网信息办公室、国家发展改革委、工业和信息化部、公安部、海关总署、市场监管总局、广电总局联合发布《终端设备直连卫星服务管理规定》。该文件要求，终端设备直连卫星服务提供者应当落实网络安全等级保护、通信网络安全防护、数据分类分级保护和商用密码应用安全性评估等制度，采取必要措施保障数据和个人信息安全。终端设备直连卫星服务提供者应当建立反电信网络诈骗内部控制机制和安全责任制度，开展终端设备直连卫星服务涉诈风险安全评估。提供具有舆论属性或者社会动员能力的终端设备直连卫星服务的，应当按照国家有关规定开展安全评估。开通终端设备直连卫星服务，应当建立电信新业务安全评估制度，并具备相应的技术保障措施。

《数据安全技术 数据安全风险评估方法》等6项网络安全国家标准发布

4月30日，国家市场监督管理总局、国家标准化管理委员会发布的2025年第10号《中华人民共和国国家标准公告》，由全国网络安全标准化技术委员会归口的6项国家标准正式发布。6项标准包括《数据安全技术 数据安全风险评估方法》《数据安全技术 敏感个人信息处理安全要求》《网络安全技术 网络安全保险应用指南》《网络安全技术 生成式人工智能服务安全基本要求》《网络安全技术 生成式人工智能预训练和优化训练数据安全规范》《网络安全技术 生成式人工智能数据标注安全规范》。

《可信数据空间 技术架构》技术文件正式发布

4 月 30 日，全国数据标准化技术委员会发布《可信数据空间 技术架构》技术文件。该文件规范了可信数据空间技术架构，明确了可信数据空间在国家数据基础设施中的定位，描述了可信数据空间作为一种数据流通利用基础设施的核心技术特征、最小功能集合及关键业务流程，适用于指导地方、行业、领域、企业开展可信数据空间的规划、建设、运营和管理。该文件专设单章规定了安全要求，包括数字合约安全、数据产品安全、空间运营安全三部分。

中国气象局等发布《人工智能气象应用服务办法》

4 月 29 日，中国气象局、国家互联网信息办公室发布部门联合规章《人工智能气象应用服务办法》。该文件提出，发展人工智能气象应用服务应当坚持总体国家安全观，统筹发展和安全，将促进创新和依法治理相结合，对人工智能气象应用服务实行包容审慎和分类分级监管。该文件明确人工智能气象应用服务提供者的权利和义务，规定了算法备案和安全评估、人工智能生成合成内容标识、算法安全审核、网络安全、数据安全、信息发布审核、投诉举报等制度。

《网络安全标准实践指南——个人信息保护合规审计要求》公开征求意见

4 月 28 日，全国网络安全标准化技术委员会秘书处组织编制了《网络安全标准实践指南——个人信息保护合规审计要求（征求意见稿）》，现公开征求意见。该文件提出了个人信息保护合规审计原则，规定了个人信息保护合规审计的总体要求、内容方法和实施流程，适用于指导个人信息处理者开展个人信息保护合规审计工作，也可为专业机构开展个人信息保护合规审计提供参考。

国家数据局印发《构建数据基础制度更好发挥数据要素作用 2025 年工作要点》

4 月 28 日，国家数据局印发《构建数据基础制度更好发挥数据要素作用 2025 年工作要点》。该文件主要包括四方面内容，其中第四方面要求，建立安全可控、弹性包容的数据要素治理制度方面，推动《关于完善数据流通安全治理更好促进数据要素市场化价值化的实施方案》落地落实，逐步构建更加完善的数据流通安全治理体系，支持数据流通安全技术应用创新，依法依规培育数据流通安全服务市场。

《网络安全技术 移动终端安全技术规范》等 9 项国家标准公开征求意见

4 月 27 日，全国网络安全标准化技术委员会归口的 9 项国家标准现已形成标准征求意见稿，现公开征求意见。9 项国家标准包括《网络安全技术 移动终端安全技术规范》《网络安全技术 具有中央处理器的 IC 卡芯片安全规范》《网络安全技术 SM2 密码算法加密和签名消息格式》《网络安全技术 SM9 密码算法加密签名消息格式》《网络安全技术 密码应用标识》《网络安全技术 秘密分享技术机制》《网络安全技术 二元序列随机性检测方法》《网络安全技术 量子密钥分发的安全要求、测试和评估方法 第 1 部分：要求》《网络安全技术 量子密钥分发的安全要求、测试和评估方法 第 2 部分：测试和评估方法》。

工信部印发《智能制造典型场景参考指引（2025 年版）》

4 月 26 日，工业和信息化部组织编制了《智能制造典型场景参考指引（2025 年版）》。该文件从工厂建设、产品研发、生产管理、生产作业等 8 个重点环节，凝练出 40 个典型场景。在工厂建设环节数字基础设施建设场景，该文件建议面向数据中心、工业网络、安全基础设施建设等业务，针对工厂算力和网络能力不足、安全防护能力弱等问题，建设数字基础设施，推动 IT 和 OT 深度融合，部署安全防护设备，应用算力资源动态调配、负载均衡、异构网络融合、高带宽实时通信、5G、动态身份验证、安全态势感知、多层次纵深防御等技术，建设高性能的算力和网络基础设施，以及全方位监测防护的安全基础设施，提升工厂算力、网络和安全防护能力。

市场监管总局《商业秘密保护规定》公开征求意见

4 月 25 日，市场监管总局起草形成了《商业秘密保护规定（征求意见稿）》，现公开征求意见。该文件所称商业秘密，是指不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息。该文件要求，经营者应当落实商业秘密保护主体责任，强化自我保护意识和能力建设，根据自身行业特点、技术要求、竞争优势，积极采取有效措施加强涉密信息、涉密区域、涉密人员、涉密载体等商业秘密保护内部控制和合规管理，自觉抵制侵权行为。

七部门联合印发《医药工业数智化转型实施方案（2025—2030 年）》

4 月 24 日，工业和信息化部、商务部、国家卫生健康委、国家医保局、国家数据局、国家中医药局、国家药监局等七部门联合印发《医药工业数智化转型实施方案（2025—2030 年）》。该文件聚焦数智技术赋能行动、数智转型推广行动、数智服务体系建设行动、数智监管提升行动等四个方面系统，提出 14 项具体工作任务。该文件要求，指导医药企业开展工业操作系统和企业信息系统的网络安全防护，落实安全管理、技术防护、安全运营等防护措施，提升网络安全风险防御和处置能力；支持相关单位建立医药大模型创新平台，协同开展医药大模型技术产品研发、监管科学研究等，强化标准规范、科技伦理、应用安全和风险管理等规则建设。

工信部、国家标准委联合印发《国家智能制造标准体系建设指南（2024 版）》

4 月 23 日，工业和信息化部、国家标准化管理委员会联合印发《国家智能制造标准体系建设指南（2024 版）》。该文件提出，智能制造标准体系结构包括基础共性、关键技术、行业应用等三个部分，基础共性标准包括通用、安全、可靠性、检测、评价、人员能力等六大类。其中，安全标准主要包括功能安全、网络安全、数据安全等三个部分。功能安全标准主要包括智能制造中功能安全系统的设计、实施、测试等标准；网络安全标准指以确保智能制造中相关终端设备、控制系统、工业互联网平台、边缘计算、工业数据等可用性、机密性、完整性为目标的标准，重点包括企业网络安全分类分级管理、安全管理、安全成熟度评估和密码应用等标准；数据安全标准主要包括工业数据质量管理、加密、脱敏及风险评估等标准。

金融监管总局拟制定《银行业保险业网络安全管理办法》

4 月 18 日，金融监管总局发布《金融监管总局 2025 年规章制定工作计划》显示，年度计划修订规章 11 部，制定规章 9 部。其中，9 部拟制定规章包括《银行业保险业网络安全管理办法》。

《可信数据空间 技术架构》技术文件公开征求意见

4 月 18 日，全国数据标准化技术委员会秘书处组织编制了《可信数据空间 技术架构（征求意见稿）》技术文件，现公开征求意见。该文件规范了可信数据空间技术架构，明确了可信数据空间在国家数据基础设施中的定位，可信数据空间的核心技术特征、最小功能集合及关键业务流程，适用于地方数据基础设施试点及可信数据空间试点的规划、建设和运营、管理。该文件专设单章规定了安全要求，包括数字合约安全、数据产品安全、空间运营安全三部分。

《全国网络安全标准化技术委员会 2025 年度工作要点》印发

4 月 18 日，《全国网络安全标准化技术委员会 2025 年度工作要点》已予 2025 年 4 月 14 日全国网络安全标准化技术委员会全体委员会议审议通过。该文件要求加快推动重点领域网络安全国家标准研制，包括推动关键信息基础设施边界确定方法、安全保护能力指标体系等急需标准试点及报批，研制出台生成式人工智能服务安全基本要求、训练数据安全、数据标注安全等标准，研制电子产品信息清除技术要求强制性国家标准，研制出台数据安全保护、数据安全风险评估等标准并推动标准实施应用，加快开展网络安全产品互

联互通功能接口、行为信息格式、威胁信息格式等标准研制和试点工作等。

六部门联合印发《促进和规范金融业数据跨境流动合规指南》

4 月 17 日，中国人民银行、金融监管总局、中国证监会、国家外汇局、国家网信办、国家数据局近期联合印发《促进和规范金融业数据跨境流动合规指南》。该文件旨在促进中外资金融机构金融业数据跨境流动更加高效、规范，进一步明确数据出境的具体情形，以及可跨境流动的数据项清单，便利数据跨境流动。该文件要求金融机构采取必要的数据安全保护管理和技术措施切实保障数据安全。

九部门印发《关于加快推进教育数字化的意见》

4 月 16 日，教育部、中央网信办、国家发改委等九部门联合印发《关于加快推进教育数字化的意见》。该文件共 7 章，其中第 6 章单章要求筑牢教育数字化安全屏障。该章节提出保障重点平台高质量运行、构建网络安全防护体系、强化人工智能安全保障三部分要求，包括提升关键信息基础设施、平台体系保障能力；构建多部门协同的重点时期保障机制，定期组织开展安全评估和检测；依托国家网络身份认证公共服务，建立教育领域身份和数据可信体系，强化实名管理；全面落实教育数据全生命周期安全防护，强化核心和重要数据防篡改、防泄露、防滥用能力；建立“人工智能 + 教育”安全保障制度；落实人工智能算法与大模型备案机制，探索建立算法安全评估制度，有效规避网络攻击、信息茧房、算法霸权、依赖成瘾等问题。

《香港生成式人工智能技术及应用指引》发布

4 月 15 日，香港特区政府数字政策办公室（数字办）公布《香港生成式人工智能技术及应用指引》，为技术开发者、服务提供商和使用者提供实务操作指引，内容涵盖生成式人工智能的应用范围和局限、潜在风险与治理原则，包括数据泄露、模型偏见和错误等技术风险。该文件提出，生成式人工智能治理应遵循遵守法律、安全透明、准确可靠、公平客观、实用高效五大原则，并从个人隐私、知识产权、犯罪防治、真实可信、系统安全五大维度展开。该文件还针对技术开发者、服务提供者、服务使用者三类角色给出了实操指南。

国际

美国消费者金融保护局撤回关于数据经纪人监管的拟议规则

5 月 15 日，美国消费者金融保护局（CFPB）在《联邦公报》发布公告，撤回其《保护美国人免受有害数据经纪行为侵害》拟议规则。CFPB 认为，目前进行规则制定“既无必要也不合适”，预计本届政府任期内不太可能有进一步的发展。CFPB 于 2024 年 12 月提出该规则，计划将《公平信用报告法》的适用范围扩大至涵盖数据经纪等行业，要求数据共享需获得消费者的明确同意，并限制此类数据的销售或使用目的，旨在解决国家安全、监控和消费者权益受损等担忧。

美国国防部首席信息官发布《加速安全软件》备忘录

5 月 5 日，美国国防部首席信息官 Katie Arrington 发布《加速安全软件》备忘录，拟变革国防部软件采购要求，指导制定“软件快速通道”计划。该计划将加强网络安全与供应链风险管理，实施严格的软件安全验证流程，建立安全信息共享机制，通过政府主导的风险评估加快网络安全授权，以实现软件快速采用。首席信息官办公室计划在 90 天内制定并提交“软件快速通道”计划的框架与实施方案。

美国白宫发布 2026 财年预算提案，拟削减网络安全预算 4.91 亿美元

5 月 2 日，美国白宫管理和预算办公室向国会提交了特朗普总统 2026 财年可自由支配预算请求。该文件拟将非国防可自由支配预算削减了 1630 亿美元，其中网络安全部分

削减了 4.91 亿美元。该文件提出，将美国网络安全与基础设施安全局的核心使命，重新聚焦到联邦网络防御和增强关键基础设施的安全性和韧性，取消其打击虚假信息和宣传项目，裁撤国际事务办公室，取消和联邦与州级层面重复的网络安全项目等。

乌克兰总统泽连斯基签署法律，加强国家网络和关基安全保护

4 月 17 日，乌克兰总统泽连斯基签署了第 4336-IX 号法律《乌克兰关于国家信息资源和关键信息基础设施对象的信息保护与网络安全的若干法律修正案》，以大规模改革国家网络战略。该法律引入了多项重大变化，包括建立国家网络事件响应系统、网络安全危机应急机制框架、网络事件信息交换系统、基于风险管理的关基保护体系、网络安全评估系统、网络安全人员队伍等。该法律要求关基保护放弃传统框架 CIPS，转向风险管理模式。

韩国 PIPC 发布《个人信息处理政策制定指南》

4 月 21 日，韩国个人信息保护委员会（PIPC）公布了修订版《个人信息处理政策制定指南》。依据韩国《个人信息保护法》第 30 条规定，个人信息处理者应当制定个人信息处理政策，并以适当、透明的方式公开。此次修订版旨在帮助个人信息处理者在 2025 年处理政策评估实施之前制定有效的处理政策。此次修订的方向是切实保障数据主体的权利，同时减轻个人信息处理者的负担，包括明确无需数据主体同意即可处理的个人信息处理项目和需要同意的个人信息处理项目、放宽个人信息处理场景及保存 / 使用期限的具体要求、记录直接受理数据主体个人信息投诉部门的联系方式、完善披露方式以适应移动应用环境的多样性等。

美国 NIST 隐私框架 1.1 版公开征求意见

4 月 14 日，美国国家标准与技术研究院（NIST）发布隐私框架 1.1 版草案公开征求意见。与 1.0 版相比，1.1 版草案增加了有关人工智能和隐私风险管理的章节，明确概述了人工智能与隐私的关系，以及如何使用隐私框架来管理人工智能隐私风险。1.1 版草案指出，人工智能系统可能因数据处理方式（如未经同意收集数据、隐私保护不足）或技术特性引发各类隐私风险，包括从尊严损害到具体危害（如经济损失、人身伤害）的多层次隐私问题，并可能波及群体或社会层面。当前，人工智能与隐私风险的关系高度依赖具体应用场景，隐私保护措施可能与用户控制需求冲突。因此，各组织应当进行隐私风险评估量化风险，实施包括缓解、转移、避免等方法在内的响应策略。

欧盟 EDPB《通过区块链技术处理个人数据指南》公开征求意见

4 月 14 日，欧洲数据保护委员会（EDPB）发布了《关于通过区块链技术处理个人数据的指南》公开征求意见。该文件旨在为计划使用区块链技术处理个人数据的组织提供合规框架，分析了区块链技术的分布式特性、去中心化治理及加密机制与 GDPR 要求的相互作用，阐述了其在个人数据处理中可能引发的合规风险和对数据主体权利与自由的潜在威胁。该文件指出，应用区块链技术处理个人数据具有复杂性和不确定性，数据控制者需通过数据保护影响评估识别风险，并优先采用技术措施（如数据最小化、链外存储）来降低对数据主体的威胁。该文件通过提供技术与组织措施的具体建议，帮助数据控制者在设计和实施区块链解决方案时确保符合 GDPR 的要求。

美司法部发布《数据安全计划合规指南》，以防止敏感数据外流至外国对手

4 月 11 日，美国司法部根据《关于防止受关注国家获取美国人大量敏感个人数据和美国政府相关数据的行政命令》（EO 14117），发布三份文件推进实施数据安全计划，分别为《数据安全计划：2025 年 7 月 8 日前的实施与执行政策》《数据安全计划：合规指南》《数据安全计划：常见问题》。合规指南文件是司法部公布的最佳实践，该文件建立了有效的出口管制措施，以防止外国对手及其控制、管辖、所有权和指挥下的人员访问与美国政府相关的数据，以及大量基因组、地理位置、生物特征、健康、财务和其他敏感个人数据。此前，EO 14117 自 4 月 8 日生效。

事件篇

全球各国重要行业网络威胁态势日益严峻。美国最大钢铁公司纽柯因网络攻击被迫停产；马来西亚多家券商系统遭境外攻击，大量交易账户被操纵买卖股票；韩国 SK 电讯 USIM 卡数据大规模泄露，官方要求用户换卡；巴基斯坦军方声称网络攻击已使印度 70% 电网瘫痪，但遭对方否认。

Coinbase 遭网络攻击泄露客户敏感数据，预计损失高达 28 亿元

5 月 15 日 Bleeping Computer 消息，知名加密货币交易所 Coinbase 披露称，有网络犯罪团伙收买了一批公司海外客服人员，窃取了约百万客户（占比 1%）的敏感数据，用以实施社会工程攻击，试图诱骗对方转账汇款，目前客户损失规模尚未公布。据悉，此次泄漏数据包括客户姓名、地址、电话、电子邮箱、打码社会安全号码、打码银行账户、身份证 / 护照 / 驾照照片、账户金额及交易记录、公司客服内部资料等。官方称客户密码、私钥等信息未泄露。Coinbase 表示将对被骗汇款的客户进行赔偿，并设立 2000 万美元基金用于悬赏攻击者线索，预计该事件的补救措施和客户赔偿总支出最高需 4 亿美元（约合人民币 28.8 亿元）。

迪奥中国客户信息遭泄露，官方群发短信通知客户

5 月 13 日中国新闻社消息，迪奥官方客服表示，有未经授权的外部方获取含客户信息的部分数据，但涉事数据库中未存储任何金融信息。迪奥品牌 5 月 12 日向用户发布短信，表示该品牌发生数据泄露事件，已采取措施以避免此次恶意访问事件的事态扩大。根据目前调查进展，在中国收集的受影响的客户个人信息的最大范围可能包括姓名、性别、手机号码、电子邮箱地址、邮寄地址、消费水平、偏好，以及客户可能已向迪奥提供的其他信息。被访问的数据库中不包含诸如银行账户详情、国际银行账户号码（IBAN）或信用卡信息等财务信息。迪奥建议客户对任何可疑通信（短信、电话、电子邮件）都要保持警惕，不要打开或点击来自不明来源的通信或链接，也不要透露验证码、密码等敏感信息。若收到任何以迪奥名义发送的可疑信息或联系方式，请客户咨询迪奥官方客服中心。

美国最大钢铁公司纽柯因网络攻击被迫停产

5 月 14 日 Bleeping Computer 消息，美国最大的钢铁生产商纽柯（Nucor）发布 SEC 公告披露，近日遭遇网络安全事件，第三方未经授权访问了公司的部分信息技术系统。发现该事件后，公司立即启动了应对措施，包括启动事件响应计划，主动将可能受影响的系统下线，并实施其他遏制、修复及恢复措施。此次事件导致纽柯公司多个生产基地部分运营暂停，目前正在逐步恢复中，尚不清楚该事件对公司整体业务造成了多大影响。

日本逾十家券商大量用户账户遭盗取：被操纵买卖股票 涉及金额约 20 亿美元

5 月 10 日 The Record 消息，日本金融厅发布警告称，有攻击者通过伪造券商官方网站实施网络钓鱼攻击，窃取了十余家券商大量用户证券账户，并大肆操作买卖股票，涉及金额约 20 亿美元。据悉，其中多数欺诈交易在 4 月份发生，有 9 家券商报告了 2746 笔欺诈交易，涉及近 5000 个证券账户。日本金融厅称，攻击者通常将被盗取账户的资金，大举购买国内外的小盘股及其他证券资产，试图推高股价，待股价上涨后再将其出售，从中获取高价差利润。

巴基斯坦军方声称网络攻击已使印度 70% 电网瘫痪，印度否认

5 月 10 日综合消息，印度与巴基斯坦冲突现已蔓延至数字领域，两国关键目标面临日益严峻的网络威胁，同时社交媒体上关于冲突情况的虚假消息也日益增多。巴基斯坦媒体报道称，巴基斯坦对印度发动该地区历史上规模最大、最复杂的网络攻击，摧毁了印度数字基础设施的关键目标，涉及能源、电力、铁路、天然气等多个行业的众多目标。巴基斯坦安全部门消息人士当日称，巴基斯坦通过网络攻击导致印度 70% 的电网瘫痪。印度新闻信息局则驳斥称此消息纯属谣言，并敦促公众保持警惕，避免被此类散布恐慌的帖子所蒙蔽。巴基斯坦黑客组织近日以“萨拉尔行动”为名，对印度开展网络攻击，入侵了 4 个印度网站，下载数据并篡改网站主页。同时，巴基斯坦多个官方网站和社交媒体账户也疑似遭受网络攻击。

多家企业遭伪造 VS Code 扩展攻击数据泄露，工信部漏洞平台发布预警

5 月 8 日网络安全威胁和漏洞信息共享平台消息，工业和信息化部网络安全威胁和漏洞信息共享平台（CSTIS）近日监测发现，攻击者频繁利用伪造的 VS Code 扩展程序对 JavaScript 和 Python 开发者实施攻击，已造成多起企业数据泄露及系统被控事件。攻击者在 VS Code 官方扩展市场及第三方平台部署含基础功能的诱饵程序，随后通过伪造 BitBucket 协作平台的更新链接，向开发者设备投递加密恶意模块，再利用 JavaScript 的 eval() 函数动态解密并执行恶意代码。值得注意的是，该恶意扩展在激活前会智能检测调试环境与安全工具来规避分析。植入成功后，该恶意扩展会窃取源代码、API 密钥等敏感信息，并在软件中创建后门，威胁企业信息安全。

美国医疗设备上市公司遭网络攻击，生产制造受影响 交付被迫延后

5 月 7 日 Bleeping Computer 消息，美国医疗设备上市公司迈心诺（Masimo）发布 SEC 公告称，受一起网络攻击事件影响，公司制造设施运行水平低于正常状态，暂时难以履行客户订单，目前正在努力恢复受影响网络系统。迈心诺表示，事件发生在 2025 年 4 月 27 日，公司未透露攻击的具体类型，但指出威胁行为者入侵了其本地部署的网络，迫使公司对受影响系统进行隔离。此次披露的网络安全事件，对公司的制造与业务运营造成了显著影响。迈心诺指出，事件的具体性质、范围及实际影响仍在调查中，目前尚无法确定是否涉及客户数据，或是否将对本季度财务表现产生影响。

秘鲁政府网站疑因网络攻击瘫痪，3300 万公民个人数据或泄露

5 月 4 日 SecurityLab 消息，秘鲁政府门户网站 Gob.pe 疑因网络攻击瘫痪多天，黑客组织 Rhysida 宣布对此负责，并声称窃取了 3300 万公民的个人敏感数据，包括护照、税务、医疗及警务记录等。Rhysida 在暗网门户以 5 比特币（约 48.8 万美元）出售数据，并设 5 月 9 日为支付赎金截止日。秘鲁政府否认网站遭受攻击，声称只是“技术维护”。

IPv6 网络功能遭 APT 组织滥用，大量知名软件更新被劫持

4 月 30 日 Bleeping Computer 消息，欧洲网络安全公司 ESET 披露，APT 组织“TheWizards”滥用了 IPv6 的某项网络功能发动中间人攻击，劫持大量知名国产软件更新通道，以植入 Windows 恶意软件。据悉，“TheWizards”制作的黑客工具滥用了 IPv6 的无状态地址自动配置（SLAAC）功能，发送特定流量伪造成网关，从而监听腾讯、小米、百度等多个公司的域名，劫持软件更新通道投递后门版更新。该组织至少自 2022 年起就已活跃，攻击目标涵盖菲律宾、柬埔寨、阿联酋、中国大陆及香港的多个实体，受害者包括个人用户、博彩公司及其他组织。

美情报机构利用网络攻击中国大型商用密码产品提供商事件调查报告

4 月 28 日中国网络空间安全协会公众号消息，中国网络空间安全协会发布调查报告，揭露美国情报机构在 2024 年对中国大型商用密码产品提供商发起网络攻击，企图破坏

我国关键基础设施安全，国家互联网应急中心（CNCERT）发现并处置了这一恶意行径。调查报告显示，攻击者利用该提供商的客户关系管理系统零日漏洞进行攻击入侵，并在该系统和产品及项目代码管理系统植入特种木马程序，窃取客户及合同信息、项目信息等大量商业秘密信息。

英国地方住房协会发生数据泄露事件，保险赔偿超 5800 万元

4 月 25 日 Inside Housing 消息，英国沃特福德社区住房协会（WCH）因一起内部过失数据泄露事件遭用户起诉，目前已由保险公司赔偿了 600 万英镑（约合人民币 5843 万元）。2020 年 3 月，WCH 一名员工误将一封包含 3544 名租户及员工个人数据（包括性取向和种族等敏感信息）的电子邮件发送给 3167 名收件人。按照其三份保险的组合式保障体系，WCH 的保险赔付额度高达 1100 万英镑（约合人民币 1.07 亿元），但是理赔过程中有一份 500 万英镑的保险因失误未能及时理赔，该协会成功起诉失误方，由对方负责支付该额度的理赔。

国家安全部：莫让“运维”成运“危”

4月25日国家安全部消息，国家安全机关在工作中发现，个别涉密单位网络运维不规范，或使用资质能力不匹配的运维机构，或运维人员违规操作，导致运维环节成为境外间谍情报机关对我开展网络渗透窃密的突破口，威胁我网络安全和数据安全。某企业用于监测生产流程数据的服务器遭境外间谍情报机关攻击控制。国家安全机关核查发现，负责运维该系统的企业员工，为贪图便利，私自打开服务器的远程登录端口，变驻场运维为远程运维，且未采取任何技术防护措施。境外间谍情报机关通过网络探扫、攻击控制该服务器后，以其为跳板大肆实施内网渗透活动，致使该企业大量内网数据被窃取，构成现实威胁。某企业新部署的智能云平台上线不久，便出现大量境外 IP 非法越权访问的情况，疑似遭受境外网络攻击。国家安全机关核查发现，该云平台为第三方公司开发，平台交付后，为便于远程维护，第三方公司私自向外映射了云平台的数据库端口，且直接暴露于互联网。而该企业在云平台上线前，也未开展安全测试、排查技术漏洞。境外间谍情报机关通过漏洞攻击，非法控制、窃取云平台中的数据资料，包括企业生产信息、工程项目资料及客户服务信息等，不仅对企业自身网络系统的安全稳定运行造成危害，还对众多客户单位构成安全威胁。

远程控制、窃密、挖矿！我国境内捕获“银狐”木马病毒变种

4 月 25 日央视新闻消息，国家计算机病毒应急处理中心在我国境内连续捕获一系列针对我国网络用户，特别是财务和税务工作人员用户的木马病毒。这些病毒的文件名称与 2025 年“税务稽查”“所得税汇算清缴”“放假安排”等诱饵主题相关，实际为恶意可执行程序，全部针对 Windows 平台用户，主要通过社交媒体中转发的钓鱼网页链接进行传播。经过分析后发现这些病毒均为“银狐”（又名：“游蛇”“谷堕大盗”等）家族木马病毒变种，如果用户运行相关恶意程序文件，将被攻击者实施远程控制、窃密、挖矿等恶意操作，并可能被利用，充当进一步实施电信网络诈骗活动的“跳板”。

马来西亚多家券商系统遭境外攻击，大量交易账户被操纵买卖股票

4月24日TheEdge消息，马来西亚证券交易所（Bursa Malaysia）披露，已与马拉西亚证券委员会接到多家券商上报，部分用户交易账户出现未授权访问与交易活动。据业内人士透露，被入侵的账户大多未启用预授权的互联网交易功能，境外 IP 的攻击者入侵了券商系统，操纵用户交易账户买卖股票以操纵股价，相关股票和衍生品包括高峰控股及其 B 类认股权证、马来西亚邮政、若干香港结构性认股权证等。大约六周前曾发生过一次规模较小的类似事件，该人士推测攻击者当时可能是在进行试探性攻击，为本次更大规模的行动做准备。马来西亚主要股票经纪直接市场接入平台服务商 N2N Connect Bhd 表示，已封禁高风险 IP 与境外 IP。

280 万人健康数据被盗，两家美国大型医疗集团赔偿超 4700 万元

4 月 23 日 HIPAA Journal 消息，美国健康管理公司

Navvis 与 SSM 健康医疗集团已同意支付 650 万美元（约合人民币 4742 万元），以解决 2023 年发生的一起数据泄露事件相关的索赔事项。2023 年 7 月，Navvis 遭勒索软件团伙攻击，致使敏感数据失窃、部分文件被加密，SSM 健康等多家医疗机构约 280 万人身份信息、健康信息、医保信息等泄露。根据和解条款，将设立一个总额为 650 万美元的和解基金，用于支付集体成员的索赔、律师费用、集体代表的服务奖励金及相关法律费用。

俄军士兵作战规划 App 被植入后门，专门窃取通信、位置等信息

4 月 23 日 Bleeping Computer 消息，俄罗斯网络安全公司 Doctor Web 研究员发现，有攻击者在 Alpine Quest App 中植入木马，并以付费版破解包等噱头在 Telegram 频道和俄罗斯境内应用商店内分发。Alpine Quest 是一款正规的 GPS 与地形图绘制安卓 App，俄罗斯士兵经常使用该应用进行战区作战规划。安装该 App 后，用户的通信聊天、实时位置等敏感信息均会遭到窃取，可能会泄露俄军行动的关键细节。

英国零售巨头马莎百货疑遭网络攻击，门店支付和订单自取服务中断

4 月 22 日 TheRecord 消息，英国零售商巨头马莎百货（M&S）披露，最近几天一直在应对一起网络事件，对部分门店的运营进行了轻微且临时的调整。此前，许多客户在社交媒体上抱怨称，门店支付系统无法使用，包括刷卡支付、礼品卡使用，以及该公司提供的“网购自取”服务等。马莎百货表示，已聘请外部网络安全专家进行调查和处理，并已向相关监管机构及国家网络安全中心进行了报告。公司正采取更多措施来加强网络安全，确保能够持续为客户提供服务。

韩国 SK 电讯用户 USIM 卡数据大规模泄露，官方宣布提供免费换卡服务

4 月 22 日 Bleeping Computer 消息，韩国最大电信运营商 SK 电讯遭受网络攻击，黑客通过植入恶意软件，成功访问了部分用户的 USIM 卡（通用用户身份模块）相关敏感信息。事件发生后，SK 电讯已加强了对 SIM 卡更换与异常认证行为的防护机制，并宣布将对出现可疑活动的账户立即暂停服务。SK 电讯后续召开新闻发布会表示，将为 2300 万用户提供免费 SIM 卡更换服务，以缓解此次安全问题。截至目前，尚无任何网络犯罪组织对该攻击事件宣称负责。值得注意的是，USIM 数据的潜在价值不仅限于金融与诈骗用途，其在情报获取、国家安全监控等方面的利用空间，引发外界对国家级黑客背景的猜测。

个人信息 3 毛 / 条！物流公司负责人倒卖 12.9 万条客户数据被判刑

4 月 17 日交汇点消息，宿迁经开区人民法院近日审结的一起侵犯公民个人信息案，揭开了物流行业非法交易客户信息的隐秘链条。某物流公司负责人段某为拓展业务，与网点商家张某达成特殊协议：每提供一条客户收件信息可获 0.3 至 0.6 元报酬，同时以每条 0.3 元价格向快递公司陈某购买数据。经查，段某联络快递公司负责人陈某后，形成由陈某统筹指挥，郑某、陈某某、潘某某、蒋某某分工配合的 6 人团伙，专门从事信息归纳、汇总、定价工作。据法院审理查明，2024 年 4 月 1 日至 5 月 14 日期间，该团伙通过物流系统非法导出公民个人信息 12.9 万余条，其中售出部分非法获利 4.4 万元。这些精准的收件人姓名、电话、住址等信息，最终成为商家“精准营销”的工具，去年 4 月 30 日，因市民察觉信息泄露报警，该案东窗事发。法院结合各被告人犯罪情节，最终对段某、陈某等 6 人判处有期徒刑 3 年、缓刑 4 年，并处罚金等刑罚。

泄露近 50 万患者健康信息，美国知名眼科医疗集团赔偿超 2600 万元

4 月 16 日 HIPAA Journal 消息，美国知名眼科护理机构 Retina Group of Washington 已同意支付 360 万美元（约合人民币 2626 万元）达成和解，以解决一起涉及 2023 年 3 月数据泄露的集体诉讼案件。此次数据泄露事件导致 455935 人的受保护健康信息遭到未经授权的访问。此前在 2023 年，该机构遭遇勒索软件攻击，导致约 45 万患

者的个人隐私、健康信息、支付和保险信息等遭到窃取。根据和解协议，将设立一个 360 万美元的基金，用于支付索赔、律师费用及其他与法律相关的成本和开支。

英国软件厂商关键数据库公网暴露，泄露近 800 万条医护职工敏感信息

4 月 15 日 Hackread 消息，安全研究员 Jeremiah Fowler 披露，英国人力资源软件厂商 Logezy 的员工管理数据库配置错误，导致该国 800 万条医护人员的敏感信息被泄露，涉及身份证明、财务数据等。据了解，该数据库无密码保护且未加密，存储数据总量达 1.1TB，包括 7975438 个文件，里边包括工作许可文件、国家保险号码、电子签名、证书、身份证明文件、工时记录等大量敏感信息。Fowler 通知 Logezy 公司后该数据库随即被限制公开访问，但不确定此前公网暴露的时长、数据有无被访问等。

美国血液透析上市公司达维塔遭勒索攻击，部分运营中断

4 月 14 日路透社消息，美国上市公司、血液透析服务商达维塔（DaVita）披露，日前遭遇勒索软件攻击，导致部分网络系统被加密，有业务运营受影响中断服务，不过公司明确表示仍在继续提供病患护理服务。达维塔表示，4 月 12 日发现此次网络攻击，目前正在与第三方网络安全专业专家共同评估事件，并已向执法部门报告事件。该公司正在采取部分功能恢复措施，并继续提供病患护理，但目前“无法估计此次中断的持续时间或影响程度”。达维塔年报显示，公司去年在美国为约 20 万名病患提供了透析服务，并在约 760 家医院开展业务。

知名论坛 4chan 遭黑客攻击下线，管理员信息及源代码疑泄露

4 月 15 日 Bleeping Computer 消息，老牌匿名论坛 4chan 遭遇了一次严重的网络安全事件。该网站在 4 月 14 日早些时候突然无法访问，随后长时间处于下线状态。一个名为 Soyjak.party 的网络社群的成员宣称发动了此次攻击，其宣称已渗透 4chan 系统长达一年，并公布了多张据称是 4chan 管理后台界面的截图。截图内容显示，攻击者可能获得了访问管理员工具的权限，这些工具或可用于查看用户 IP 地址、地理位置信息、管理论坛版块、查看日志、访问数据库（通过 phpMyAdmin 面板）等。此外，攻击者还泄露了一份据称包含 4chan 管理员、版主及协助维护人员（Janitors）电子邮件地址的列表。同日晚些时候，又有用户在另一个匿名论坛 Kiwi Farms 上发布了据称是 4chan 网站的 PHP 源代码。4chan 官方尚未就此次攻击事件发布声明。

超 1.4 万台 Fortinet 设备长期被黑客入侵，约 1100 台位于中国

4 月 14 日 Cybernews 消息，美国网络安全公司 Fortinet 发布警告称，攻击者利用已知漏洞（CVE-2024-21762、CVE-2023-27997 和 CVE-2022-42475）并采取新型后渗透攻击，获取了 Fortinet 部分型号设备的只读权限，即使受害者更新系统修复漏洞，该权限依然保留，使得攻击者可以长期访问目标设备窃取敏感配置信息等。Shadowserver 基金会扫描发现，约 14300 台受感染的 Fortinet 设备暴露在互联网上，其中美国、中国、日本数量位列前三。

勒索攻击扰乱电商运营，欧洲家居零售公司 Fourlis 损失超 1.6 亿元

4 月 11 日 Bleeping Computer 消息，欧洲老牌家居零售公司宜家的多国代理商 Fourlis 集团发布财报披露，2024 年 11 月 27 日“黑色星期五”促销活动前夕遭遇勒索软件攻击，预计损失达 2000 万欧元（约合人民币 1.66 亿元）。该事件于 2024 年 12 月 3 日公开，Fourlis 集团当时承认宜家线上商店出现的技术问题源于“恶意的外部行为”。财报显示，该事件导致门店补货短暂受影响，电商运营受影响近 3 个月，对销售运营造成了巨额损失。Fourlis 集团并未向勒索软件攻击者支付赎金，而是在外部网络安全专家的协助下，完成了受影响系统的恢复工作。后续调查未发现此次事件中有数据被盗或泄露的证据。

漏洞篇

近期，多个安全相关产品软件曝出高风险漏洞，可被利用获得控制权限造成严重后果，包括Fortinet FortiOS身份认证绕过漏洞(CVE-2025-22252)、Elastic Kibana原型污染致任意代码执行漏洞(CVE-2025-25014)、Ivanti Endpoint Manager Mobile身份认证绕过漏洞(CVE-2025-4427)及Ivanti Endpoint Manager Mobile代码执行漏洞(CVE-2025-4428)。

Ivanti Endpoint Manager Mobile 多个漏洞安全风险通告

5月14日，奇安信CERT监测到官方修复Ivanti Endpoint Manager Mobile身份认证绕过漏洞(CVE-2025-4427)及Ivanti Endpoint Manager Mobile代码执行漏洞(CVE-2025-4428)，这两个漏洞都是由于Ivanti Endpoint Manager Mobile的API组件未能正确验证输入的数据而造成的漏洞。攻击者可以利用这两个漏洞绕过身份认证，并通过受影响的API执行任何代码，对系统安全造成严重损害。目前该漏洞PoC和技术细节已在互联网上公开，奇安信威胁情报中心安全研究员已成功复现。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Elastic Kibana 原型污染致任意代码执行漏洞安全风险通告

5月7日，奇安信CERT监测到官方修复Elastic Kibana原型污染致任意代码执行漏洞(CVE-2025-25014)，该漏洞源于Kibana中机器学习和报告端点的原型污染问题，攻击者可以通过精心构造的文件上传和特定的HTTP请求绕过验证机制，攻击者利用该漏洞后，可以在受影响的系统上执行任意代码，可能导致数据泄露、系统被完全控制等严重后果。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69,619个，关联IP总数为13,216个。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Fortinet FortiOS 身份认证绕过漏洞安全风险通告

5月15日，奇安信CERT监测到官方修复Fortinet FortiOS身份认证绕过漏洞(CVE-2025-22252)，FortiOS、FortiProxy和FortiSwitchManager TACACS+中存在一个身份认证绕过漏洞，当其配置为使用ASCII认证的远程TACACS + 服务器进行认证时（非默认配置），未经身份验证的远程攻击者可以绕过设备的正常认证机制，成功利用此漏洞可使攻击者获得设备的管理员权限。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Apple iOS 与 iPadOS 多个在野高危漏洞安全风险通告

4月17日，奇安信CERT监测到官方修复Apple iOS/iPadOS内存破坏漏洞(CVE-2025-31200)及Apple iOS/iPadOS指针认证绕过漏洞(CVE-2025-31201)，Apple iOS/iPadOS内存破坏漏洞(CVE-2025-31200)产生的原因是操作系统处理音频流时存在内存边界检查不足，导致内存破坏；Apple iOS/iPadOS指针认证绕过漏洞(CVE-2025-31201)产生的原因是系统中存在易受攻击的代码，导致指针认证机制可以被绕过。目前已经发现上述两个漏洞存在在野利用，鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

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。

RSAC 2025：新挑战、新技术与新趋势

AI 连续三年成为 RSAC 会议关键词。不同之处在于，Agentic AI 成为 AI 明星中的明星。AI 创新之下的网络安全正经历一场彻底变革。

RSAC 2025 见闻：新风险、新趋势与新热点

4 月 28 日至 5 月 1 日，RSAC 2025 年度会议于美国加利福尼亚州旧金山莫斯科尼中心（Moscone Center）召开。

RSAC 2025 的规模基本恢复到 2019 的盛况。本届会议策划了 29 个专题、37 场主题报告和 450 余场会议，超过 700 位演讲者和 650 家参展商在会议中介绍并展示了其最前沿的网络安全技术和相关理念，累计吸引全球参会者超 4.3 万名。

自 1995 年起，RSAC 每年都会围绕一个安全相关主题展开。今年大会以“多元声音，同一社区”(Many Voices，One Community) 为主题，旨在强调“人工智能时代的网络安全并非一家企业或一个行业能够独自解决的挑战，需要共同承担责任、多元视角和有针对性的合作”。

RSAC 高级副总裁 Linda Gray Martin 表示：“社区是我们一切工作的核心。不同的观点和专长不仅让我们更加多元，也让我们的声音更具力量。RSAC 2025 正是这样一个平台，让全球安全专家聚首，共同迎接日益严峻的网络安全挑战。”

一、议题趋势：聚焦 AI 与新兴安全挑战

RSAC 大会的议题设置，历来是行业技术风向的晴雨表。“AI 时代的安全”成为贯穿全场的主旋律。

从 2025 年大会的主题演讲和分论坛议程来看，人工智能安全成为最炙手可热的主题，超过 1/4 公司的介绍中有 AI 字样，议题中包含 AI 的比例更高。大会开设了专门的 AI 安全论坛，一些

重量级嘉宾（包括 Bruce Schneier 等安全专家和大型科技公司的代表）在主题演讲中深入探讨了 AI 的机遇与风险。可以说，“AI 时代的安全”成为贯穿全场的主旋律。

软件供应链安全

除了 AI 安全，软件供应链安全依旧是大会讨论的重点。近来年的多起供应链攻击事件（如开源库后门、依赖篡改等）促使业界高度重视这一领域。本届 RSAC 大会上，多场技术分享聚焦于如何保障代码供应链和第三方组件的安全，包括 SBOM（软件物料清单）的应用、CI/CD 流水线安全、防止供应链中断等议题。有厂商在大会期间发布了代码供应链风险可视化工具，帮助追踪 AI 生成代码可能引入的隐患。这些都表明供应链安全从理念走向实践，成为企业安全策略中的固定环节。

零信任

零信任（Zero Trust）架构方面，本届大会的讨论热度相对于前两年有所平稳。零信任作为一种原则，早在 2021 年前后因政府政策和远程办公趋势而大热，经过几年的实践，如今大会上更多地是分享落地经验和优化策略，而非纯粹概念炒作。许多演讲嘉宾提到，将零信任理念融入网络架构和访问控制已成为新常态，今年则更关注如何细化实施、解决用户体验和运营复杂度等问题。从参展方案看，不少厂商产品已内建零信任框架，以支持细粒度访问权限和持续验证。有分析指出，初创公司中有相当一部分强调了零信任相关能力。有观点指出，在代理型人工智能快速发展的背景下，零信任原则应超越人类和机器身份，延伸至人工智能决策系统。强调对人工智能行为也要进行实时监控和验证，防止潜在风险。

身份安全

随着生成式人工智能在企业中的应用日益广泛，身份安全的需求也日渐紧迫。本届会议设有 300 余场与身份安全相关的会议，内容涵盖“身份攻击为何屡禁不止”“如何在攻击者利用前修复身份漏洞”和“以身份为中心的防御策略如何应对人工智能驱动型攻击”等。与会专家认为，在网络边界日益模糊的今天，身份已取代传统边界，成为安全防御的第一道也是最后一道防线。

会议中，DTEX 分享了朝鲜特工伪造身份远程应聘、获取管理员权限的案例。这种“信任欺骗”在远程办公环境中更难察觉与防范。技术方面，Proofpoint 展示了一体化身份监测平台，覆盖电子邮件、终端、网页与云环境；CrowdStrike 发布 Falcon Privileged Access 解决方案，构建从入侵识别到横向移动防控的完整身份防护路径。

量子安全

量子安全也是不可忽视的议题。本届 RSAC 会议中有多家企业推介后量子、加密敏捷性或量子密钥分发等安全解决方案，旨在应对量子计算对现有加密技术所带来的挑战。

量子计算对现有加密体系的冲击仍属前瞻话题，但 RSAC 传统的“加密技术专家小组”（Cryptographers’ Panel）及相关演讲继续关注这一领域，如讨论抗量子密码算法的标准化进展、量子随机数的应用等。在 2023 年大会的“Hugh Thompson Show”环节甚至以“量子时代”命名，凸显了量子技术对网络安全的潜在影响。在 2025 年的大会上，这一趋势延续，有专门论坛探讨后量子加密和未来的密码学方向，业界专家们就如何提前布局抗量子安全，进行了热烈讨论。

与会专家强调，量子计算具备破解当前广泛使用的传统公钥加密算法（如 RSA 和 ECC）的能力，这可能导致现有的数据保护措施失效，给企业和机构带来严重的安全风险。会议中多场活动围绕抗量子密码算法的标准化进展、量子随机数的应用等进行了讨论。其中，美国国家标准与技术研究院（NIST）在会上提出了其最终确定的抗量子加密标准，相关企业亦对该加密算法在传输协议中的首次商业部署进行了展示。专家呼吁，企业应该开始清点加密资产并制定向抗量子算法过渡的安全策略。

SaaS 安全

SaaS 安全作为新兴话题也进入了视野。随着企业 IT 全面云化，越来越多的业务依赖第三方 SaaS 服务，引发的数据保护和访问控制问题成为今年论坛上的讨论热点之一。一些议题涉及如何管理日益庞杂的 SaaS 应用权限、监控敏感数据在 SaaS 平台的流转，以及防范 SaaS 供应商自身的安全漏洞。有厂商在大会期间推出了针对 SaaS 环境的安全控制平台，实现

多工具信息整合，以提升对 SaaS 风险的可见性。可以预见，SaaS 安全将随着云端应用的普及而持续升温。

总体而言，RSAC 2025 的议程设置反映出行业技术方向正从过去的网络架构防护，扩展到应对智能化和供应链复杂化带来的新挑战。从 AI 安全、供应链风险，到量子时代的密码学、更精细的身份与访问管理，无不体现网络安全领域正在与时俱进，全面演进。这些趋势在大会上得到充分讨论，为从业者提供了宝贵的风向指引。

二、参展厂商：新兴网络安全力量崭露头角

今年共有约 600 家网络安全厂商参展，这一数字较 2023 年的 550 家有明显增长，与 2024 年持平略增。

总体来看，本届 Expo 展厅的参展厂商数量与质量齐升。“老兵”厂商展台依然人气旺盛，持续展示成熟产品的演进和集成方案；同时，新兴企业的亮相成为一大看点，不少初创公司展台前聚集了观众观看演示、交流技术。这些创业公司的崛起也反映出行业的发展方向。例如，初创展区中有相当比例的公司专注于应用安全（约占 20%，涵盖软件供应链安全、API 安全等）及身份访问管理、生成式 AI 安全和安全运营等领域。多家初创团队现场分享了各自独特的解决方案，不少产品着眼于自动化、防御主动化和 AI 赋能，体现出现代安全的新思路。

和往年相比，参展厂商的技术焦点也出现了变化。一些过去几年的热门领域（如零信任架构）仍然有厂商强调，但相比高峰时期热度有所回落，更多成为产品标配特性而非独立卖点。相反，新近兴起的领域如供应链安全（软件供应链及开源组件风险）、SaaS 安全（SaaS 应用及第三方整合风险管理）等得到更多厂商关注，相关解决方案纷纷涌现。在大会现场可以感受到，网络安全创业生态在不断扩张，与 2024 年相比，参展厂商的热情有明显好转，各展商派送礼物的数量也比 2024 年多了不少。

创新沙盒大赛

RSAC 大会的亮点之一是每年的“Innovation Sandbox”创新沙盒初创企业大赛。2025 年 Innovation Sandbox 的冠军由初创公司 ProjectDiscovery 摘得，其被大会评选为“2025 年度最具创新初创企业”（Most Innovative Startup 2025）。

ProjectDiscovery 凭借其开源漏洞扫描与攻击面管理平台脱颖而出：该平台基于开源工具“Nuclei”，能够自动化地监测企业的攻击面，并快速发现和修复漏洞，为安全团队提供高效风险检测手段。评委会认为，ProjectDiscovery 将开源社区力量与企业安全需求相结合，加速漏洞发现与响应，这一技术亮点使其在众多创新者中胜出。

今年 ProjectDiscovery 的胜出有点出乎意外，基础防御（漏洞管理、攻击面监测）虽是刚需，但在创新沙盒大赛中胜出的确没有想到，或许“开源 + 自动化”正成为安全创新的重要趋势。

另一家入围创新沙盒决赛的企业 MetalWare 公司拥有一支由来自 SpaceX 等公司的工程师和技术人员组成的优秀团队，致力于帮助运行关键任务硬件。这些技术人员，成立固件安全企业，利用自身的专业知识和对风险的深刻理解，提升关键行业的安全态势。这在安全市场中是一个值得关注的缺口，因为固件、硬件和安全方面都存在知识缺口。

Zenity 致力于解决将安全原则和治理引入低代码 / 无代码开发的问题。生成式人工智能彻底改变了这一领域，使其能够推出专注于保护人工智能智能体免受提示词注入和漏洞攻击的平台。

另一家脱颖而出的入围公司是 Twine Security。该公司开发 AI 数字助理，以扩展内部安全团队的能力。Twine 另辟蹊径，将其推出的 AI“Alex”成为 IAM 领域的专家。身份领域风险巨大，正在成为几乎所有网络安全项目中的主导因素。

初创企业展区

今年大会专门设立的Early Stage Expo 初创企业展区，汇聚了 76 家新创公司。这些新秀公司覆盖了从应用安全到云安全、从身份管理到威胁情报等各个细分领域。

在全部 76 家初创参展企业中，有 15 家聚焦于应用安全（AppSec）、11 家企业聚焦于身份与访问管理（IAM）、10 家企业聚焦于生成式人工智能安全（GenAI Security）、8 家企业聚焦于安全运营（SecOps）。初创公司的动态，显示出安全企业正向自动化、智能化与多域融合的安全运营模式迈进。

RSAC 创业舞台

RSAC 创业舞台（RSAC Launch Pad）同样是 RSAC 为早期网络安全创业项目所设立的活动平台，致力于发掘具备变革潜力的安全技术初创创意。相较于“创新沙盒”活动，创业舞台活动聚焦在商业层面更加早期、尚处萌芽阶段的网络安全项目。该项目选出三家最具潜力的初创团队，以“创投真人秀”的形式在 RSAC 大会

现场进行公开路演。

本届大会入围的三家初创团队为：Blue41、RunSybil 及 The Hacking Games。其中，Blue41 聚焦于为代理型人工智能提供安全防护；RunSybil 致力于通过人工智能赋能渗透测试强化漏洞探查；The Hacking Games 则期望通过人工智能辅助招聘“非常规”网络安全人才，促进网络安全产业发展。

三、 风头正劲的以色列企业与低调中国企业

近几年，网络安全创新和创业领域出现了一个引人注目的现象：以色列公司在全球范围内扮演了举足轻重的主导角色。2025 年 RSAC 大会的 39 场主旨演讲中，有 4 场由以色列专家主讲，论坛发言嘉宾中近 40 位来自以色列。根据安全行业研究者 Richard Stiennon 的调查，按国家统计的信息安全企业数量，以色列位居全球第二，拥有的安全公司数量竟然超过英、加、印、德、法五国的总和。考虑到以色列人口仅约 900 万，而那五国总人口高达 15 亿，这组数据更加令人惊叹。可以说，在网络安全产业版图中，以色列被誉为创新的堡垒和“创业国度”。

以色列企业为何能在网络安全创新中占据主导？利好因素来自多方面：首先，以色列独特的军民融合培养了大批安全人才。许多知名安全创业公司的创始人都出身于以色列国防军情报部门（尤以 8200 部队著称），在服役期间累积了丰富的网络作战经验。这使得以色列形成了高校—军队—高科技企业的紧密衔接，为安全创业输送了源源不断的顶尖人才。其次，以色列政府和风投界对网络安全高度重视，资本投入积极，催生了一批又一批初创公司。以色列的小体量市场迫使这些创业公司生来即面向全球，这也使其产品更具国际竞争力。

以色列企业的主导还引发了全球格局和安全主权方面的讨论。随着关键安全技术和产品由以色列（往往背后有美国资本）主导，有些国家开始担忧自身网络安全命脉受制于人。这促使各国更加重视本土网络安全产业的发展，以避免在核心安全能力上过于依赖单一国家或供应商。这种良性的竞合态势或将推动全球网络安全产业更加繁荣：一方面，以色列将继续扮演创新火车头，引领新的技术方向；另一方面，其他国家和地区也在加紧培育各自的安全新秀，与以色列企业共同构建更加多元化的技术生态。

中国企业参展 RSAC 2025 创出了自 2013 年以来的新低，仅有奇安信、飞天诚信、山石网科、绿盟科技四家企业参展，回想起 RSAC 2019 期间百度安全主办的近百人参加的“RSAC 小龙虾游艇”活动，让人不胜唏嘘。不过，华人做为在网络安全领域最活跃的族裔志毅，不少展商的展台的工作人员中能看到比往年多的华人的面孔，在 Cyera、Stellar Cyber、Netbrain 等厂商的展台，都是华人给大家做产品介绍。更有 Ridge Security 等创办的安全公司参展。在与华裔同行交流过程中，大家普遍感觉到来自以色列的压力，但大家觉得华人踏实务实的做事风格，踏踏实实做好网络安全技术和产品，未来仍有机会。

> 按国家统计的信息安全企业数量，
> 以色列位居全球第二，
> 拥有的安全公司数量竟然超过英、加、印、德、
> 法五国的总和。

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...

极牛技术社群

网络安全技术社群

Cyber Security Technology Community

PLATFORM

网络安全技术社群

极牛网旗下面向网络安全工程师的社群平台，汇聚行业中网安工程师的知识和社交平台，围绕『技术』『管理』和『圈子』三个核心能力，将前沿的技术内容、技术管理成长感悟、技术圈子社群平台等向优质的网安工程师开放，每月定期组织社群会员线下活动，强调内容分享的体系化和活动内容的多样性，为中国网络安全工程师打造专属的全方位综合赋能的社群平台。

技术

聚焦前沿技术、热点技术、难点技术，提升网安在企业架构中的决策能力和迭代能力。

管理

专注在帮助网安工程师在职业发展中，建立体系化的管理知识和技术管理转型路径。

圈子

建立精准的技术方向圈子，针对不同的职业发展阶段，组成技术成长小组一起结伴同行。

极牛技术站

以沙龙、峰会、圆桌论坛等深度学习的形式进行，满足知识获取与社交需求。

管理加油站

面向管理者的闭门活动，前瞻性的思维和观点，成熟的管理模式与领导模型。

极牛知识变现

通过帮助工程师打造个人品牌，从出书、录课、企培等形式帮助知识变现。

极牛训练营

面向社群成员的线下课程，技术架构、团队管理、商业模式、塑造个人品牌等。

极牛众星计划

社群中优秀的工程师将会被受邀签约极牛众星计划，平台辅助进行品牌孵化。

更多内容敬请期待

RSAC 2025 观察：AI 变革与网安新方向

4 月 28 日至 5 月 1 日，全球网络安全领域的年度盛会 RSAC 2025 在美国旧金山召开。本届大会以“多元声音，同一社区”(Many Voices，One Community) 为主题，旨在强调“人工智能时代的网络安全并非一家企业或一个行业能够独自解决的挑战，需要共同承担责任、多元视角和有针对性的合作”。

毫无疑问，AI 占据本届 RSAC 大会的最热门议题。根据 RSAC 主办方的统计，2025 年提交的演讲主题中，AI 相关的内容占比高达 40%。在入围今年创新沙盒十强的厂商中，有 7 家的产品与 AI 相关。有趣的是，第一天上午创新沙盒十强决赛上，非 AI 主题的演讲者为防止裁判和听众审美疲劳，开场时都先特意声明其介绍的产品不是 AI。RSAC 执行主席休·汤普森 (Hugh Thompson) 在主题演讲中表示：“人工智能正在渗透到网络安全的方方面面。”

从大会首日 Cisco 公司执行副总裁 Jeetu Patal 和微软安全 Vasu Jakkal 的演讲，以及随后几天的主题演讲和众多厂商展示的产品，反映出 AI 在网络安全方面的两大主要方向：1）AI 用于网络安全，特别是 Agentic AI 在安全方面的应用；2）安全的 AI（AI Safety）与 AI 的安全（AI Security），包括针对大语言模型的敌对攻击、AI 智能体和自动化系统的安全问题。

根据笔者现场观察，本届 RSAC 大会主要集中在以下三个主要热点。

一、AI 变革：从增强走到自主

RSAC 2025 的一个主要议题是人工智能与网络安全的融合。今年的不同之处在于，讨论的重点从生成式人工智能转向了完全自主的“自主化人工智能”系统。在 RSAC 2025 大会上，从主题演讲到厂商展览，再到小组辩论，自主化 AI（Agentic AI）无处不在。

研究机构 Forrester 甚至戏称，今年 RSAC 的非官方主题应该是“AI 智能体和自主化 AI 是（安全）未来”。

随着自主化 AI(Agentic) 新型系统

> 创新沙盒 10 强中有 4 家与 AI 安全相关，解决方案包括通过 AI 大模型运行和推理时的安全和合规保证，AI 应用的自动发现、实时监控和风险评估，员工使用 AI 应用时的数据安全问题等。

的崛起，人工智能正在从辅助性工具向核心决策与执行角色转变。与依赖人类提示的传统人工智能工具不同，Agentic AI 是指能够在设定目标内自主规划、决策和行动的系统。这些能够代表用户自主采取行动的系统被誉为下一个飞跃。

“Agentic SOC”是 Agentic AI 应用的主要方向。Agentic SOC 通过多个专门的 AI Agent 协作执行半自主和完全自主的安全运营工作流程， 这一愿景预示着未来的前景——具有特定专业知识的各种 AI 智能体，可以相互沟通并协调行动，比单个工具或孤立的人类分析师更快、更有效地解决复杂的安全事件。

2025 创新沙盒 10 强中，有 2 家将 Agentic AI 应用在安全运营中——Command Zero 和 Twin Security。RSAC 展区北区的数家大厂展台占据最醒目的位置，包括 Cisco、Microsoft、Google、CrowdStrike 等所有涉足安全运营产品的厂商都展示 AI 在其产品中的应用。

Microsoft Security Copilot 在大会期间发布多个安全 Agent 预览版，包括钓鱼邮件分类、漏洞修复、DLP 告警分诊、条件访问优化、威胁情报分析智能体等。 CrowdStrike 在会议期间发布了两个 Charlotte AI 安全智能体：Agentic Response 和 Agentic Workflows。Agentic Response 能够自动回答安全分析师通常会提出的问题，分析根本原因，并指导调查的后续步骤。Agentic Workflows 利用大型语言模型将 AI 推理集成到自动化剧本中。

业界向 Agentic SOC 的转变表明，组织在处理网络安全方面已经发生范式转变，从反应性、人力密集型模式转向更主动和自动化的系统，这有望带来威胁检测和响应的速度和准确性的显著提高。当然，成功实现这一愿景还取决于将这些 AI 智能体无缝集成到现有安全基础设施和工作流程中，以及确保其自主行动的信任和透明度。

应用安全是另一个 AI Agent 应用热门领域。Checkmarx 宣布推出 Agentic AI 赋能的应用程序安全态势管理 (ASPM) 产品，该产品可以扫描代码库中的所有包，以便在开发人员的 IDE 中，直接向开发人员显示优先漏洞和未知代码引用。Semgrep 在 RSAC 2025 上全面展示了其面向开发者与安全团队的产品组合，其中 Semgrep Assistant 作为 AI 安全智能体，可在平台内半自主执行常规安全任务，显著减少误报负担并为开发人员和安全工程师节省大量时间。

二、AI 安全已是增长最快新兴领域

AI 安全同样是今年 RSAC 的热门话题。英国人工智能安全研究所首席技术官梁晖 (Jade LEUN) 在会上强调，AI 能力的发展速度远远快于安全和防护。针对 AI 安全的挑战，RSAC 上反

复提出的应对策略是利用 AI 工具来监视 AI 工具。

大量厂商展示了自己的 AI 安全产品。专注于 AI 安全的初创公司有 10 来家，大部分参展的网络安全厂商都推出了 AI 安全的产品。连续两年未在 RSAC 参展的 Palo Alto Network，也在会议第一天发布了全新的 AI 安全平台 Prisma AIRS。

创新沙盒 10 强中更是有 4 家与 AI 安全相关。通过这 4 家公司的产品和解决方案就可以看出 AI 安全要解决的主要问题，包括通过 AI 大模型运行和推理时的安全和合规保证，企业环境中 AI 应用的自动发现、实时监控和风险评估，以及内部员工使用 AI 应用时的数据安全问题等。

Aurascape 是一家“AI 原生”网络安全初创公司，致力于为企业在生成式 AI 和智能体日益增长的背景下，提供全面的安全与可观测解决方案。其 AI 安全平台（Aurascape Platform），专为“AI 工具生态”设计，支持对数千种 AI 应用的自动发现、实时监控与风险评估。其平台采用端点客户端 + 云端“inline proxy”架构，可将所有 AI 相关流量实时拦截并在通信“流中”进行深度检测与执行策略，彻底摆脱传统事后日志和 API 轮询的模式。其次，Aurascape 处理并保护多模态数据，内置数千种 AI 协议解析器，能够对文本、图像、音视频、代码等多种数据形式进行精准解码与风险评分，误报率极低 。

CalypsoAI 致力于为企业在整个 AI 生命周期中提供端到端的安全与合规保障，其核心产品包括基于云的 SaaS 平台、实时推理防护层（Inference Perimeter）及多种安全评估工具。平台实现了模型无关（model-agnostic）的架构，支持与任意大模型或生成式AI服务无缝集成，并通过自主式红队测试（agentic red-teaming）、实时防御和持续可观察性，为 AI 推理阶段提供动态安全防护。其技术与产品的关键创新包括全生命周期覆盖、模型安全排行榜（Security Leaderboard）与安全指数（CASI）、可定制化安全扫描器，以及自动化漏洞修复与合规审计功能，从而在安全性、灵活性与可扩展性上形成差异化优势。

EQTY Lab 致力于通过先进的加密技术和硬件信任增强，为 AI 数据、模型和智能体提供端到端的可验证治理和安全保障；其核心技术“AI

Integrity Fabric”涵盖软件物料清单（AI SBOM）、运行时可验证计算（Verifiable Compute）和合规即代码的 SDK（Verifiable AI SDK），并通过与 Intel、NVIDIA 等业界巨头的深度合作，将硬件与软件层面紧密结合，以实现动态审计与保真；其产品矩阵包括 AI Integrity Suite、MCP Guardian、Verifiable Compute、行业定制解决方案（如生命科学）等，形成了从开发到部署、从静态到运行时的全栈可信 AI 生态；创新之处在于其首创的“可验证计算”概念、垂直整合的实现路径、对开源标准的贡献，以及面向高度合规行业的深度定制能力。

Knostic.ai 是业内首家针对大型语言模型（LLM）提出“Need-to-Know（按需知悉）”访问控制框架的企业 AI 安全厂商，致力于防止内部员工使用 AI 应用引起的数据泄露，同时推动 AI 与安全的深度融合。其产品矩阵涵盖从 AI 部署前评估（Copilot Readiness Assessment）、实时访问控制引擎、持续监测与补救，到行业合规的安全部署框架，形成闭环式安全流程。技术上采用“知识图谱 + 联邦学习”架构提升模型训练效率 40%，基于多维情境的策略引擎实现上下文感知的响应重塑（Response Shaping），并通过自适应学习动态调整策略。

三、开源为 AI 时代的网络安全发展带来新动能

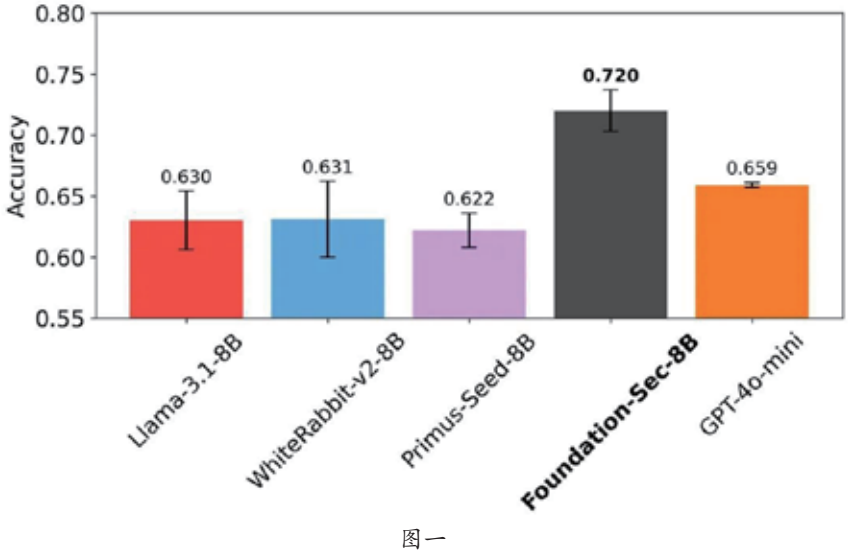
在 RSAC 2025 大会上，思科、Meta 和 ProjectDiscovery 宣布推出新的开源安全大模型，以及由社区驱动的攻击面与漏洞检测开源项目，共同定义了开源在网络安全领域的未来。

在 RSAC 2025 第一天，Cisco 公司执行副总裁兼首席产品官 Jeetu Patal 在主旨演讲最后发布开源安全大模型 Foundation-sec-8B。这一模型由思科新成立的 Foundation AI 团队开发，基于 Meta 的 Llama3.1 架构，专门针对网络安全任务进行优化。与通用模型不同，Foundation-sec-8B 在训练过程中使用了经过精心筛选的漏洞数据库、威胁情报报告和安全工具文档等精选数据集，确保其能够准确理解和应对各种网络威胁，拥有 80 亿个参数，旨在为网络安全领域提供专门的 AI 基础设施。

思科将这一专为网络安全设计的大型语言模型开源，赢得现场阵阵掌声，国内安全行业也非常关注，甚至认为 Cisco 这类大厂开源安全大模型可以实现类似于 DeepSeek 的大模型技术平权。

目前，Cisco 开源 Foundation-Sec 安全大模型已公开了一些安全知识测试集的对比数据（图一），在 CTI-Bench 测试集上的表现确实好于通用大模型。在某些安全任务上可以与 Llama 3.1-70B 和 GPT-4o-mini 相匹敌。

但在 RSAC 期间的交流中，国外同行就对 Cisco 开源的 8b 安全大模型的反应相对比较平淡。从现场展区已集成 AI 能力的厂商来看，基本都是接入



图一

OpenAI、Claude 和 Gemini 等先进通用大模型，并通过 RAG 等技术实现多智能体。这可能与国外企业上云比例较高有关。国内客户更喜欢私有部署，受限于算力，会考虑性价比更高的支持本地部署的安全大模型。

Cisco 的 Foundation-sec-8B 安全大模型计划中还包括公开现实世界实际安全运营和任务的测试集，对于行业推动大模型在安全任务上的效果评估会有些促进作用，至少会导致一批能力欠佳的安全垂域大模型裸泳者退去。

Meta 也在 RSAC 2025 大会上强化其开源 AI 战略，扩展了 AI 卫士套件（AI Defenders Suite），以增强生成式 AI 基础设施的安全性。Meta 的开源工具包现已包含多模态分类器 Llama Guard 4，可检测文本和图像中的策略违规行为，从而改进 AI 工作流程中的合规性监控。同时推出的还有集成模块化功能的开源实时安全框架 LlamaFirewall，其中包括检测提示词注入和越狱的 PromptGuard 2，监控和保护 AI 代理决策过程的 Agent Alignment Checks，以及用于检查生成代码以识别和缓解漏洞的 CodeShield。

荣获创新沙盒冠军的初创安全公司 ProjectDiscovery，凭借其开源漏洞扫描工具 Nuclei，获得“最具创新性初创公司”奖项。作为一款可定制的漏洞扫描器，Nuclei 利用全球社区，快速识别 API、网站、云环境和网络中的漏洞。ProjectDiscovery 首席运营官 Andy Cao 强调了开源在网络安全领域的重要性，认为这种社区驱动的方法能够极大地提升安全防护的效率和有效性。

思科的 Foundation-sec-8B、Meta 的扩展版 AI Defenders Suite 及 ProjectDiscovery 的 Nuclei 共同证明，当跨公司界限的开放性、协作性和专业领域专业知识相融合时，网络安全创新才能蓬勃发展。这些开源解决方案不仅提升了企业应对网络威胁的能力，也降低了安全防护的成本。未来，网络安全有望依赖开源合作与共享技术，助力企业在数字化转型中安全前行。

自主化人工智能、量子计算正带来前所未有的挑战，对于努力适应这种新形势的企业来说，RSAC 2025 传递的信息非常明确：网络安全行业正处于变革的转折点。过去的安全模式已不足以应对未来的威胁。

新兴的技术变革也将推动构建更具弹性、更智能、更自适应的安全框架，从而实现以更简单的工具、更快的速度、更少的资源，实现降低风险的目标。

RSAC 2025 观察：Agentic AI 变革安全运营中心

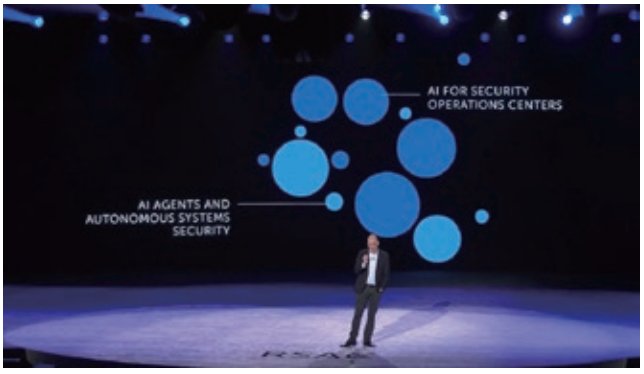
RSAC 2025 已落下帷幕。AI 依旧是大会上最闪亮之星。不同之处在于，Agentic AI 成为了 AI 明星中的明星。Agentic AI 正在成为网络空间安全的未来（不论是防御还是攻击）。

本文详细分析 RSAC 2025 大会上有关安全运营的议题，希望从中一窥安全运营技术的未来发展趋势。内容涉及 Agentic AI 赋能 SOC 的新理念、新架构、新产品、新交互、新场景和笔者从业 20 多年来的感悟，以及对未来的研判。

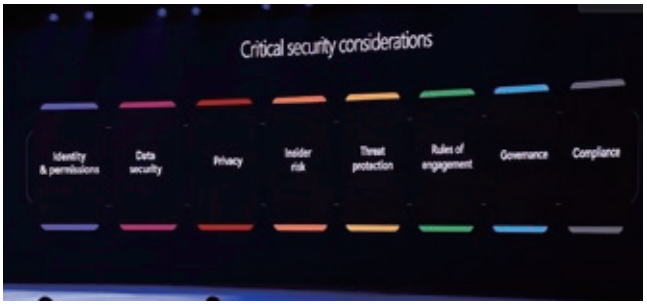
一、Agentic AI 深刻变革 SOC

大会执行主席 Hugh Thompson 表示，今年有两个 AI 主题尤其值得关注。一个是 Agentic AI，包括它如何应用于安全，以及它自身的安全性，包括身份的问题、治理的问题、可追溯性的问题等。另一个是 AI 应用于 SOC（AI in the SOC，AI for SOC），今年有很多大大小小的此类议题，包括多个顶级赞助商的主题演讲都与此相关。

在首日主题演讲环节，微软安全业务的副总裁 Vasu Jakkal 以《Agentic AI 时代的安全》为题，带领大家畅游了一番 Agentic AI 时代的网络安全。Vasu Jakkal 认定 Agentic AI 将 AI 带入了一个新时代，将改变人类生活的方方面面，成为人类的助手、同事和思想的伙伴。



在拥抱 Agentic AI 之前，其自身的安全性必须首先予以保障，因为 AI 也面临着前所未有的威胁挑战。AI 越重要，AI 安全就越迫切，Vasu Jakkal 提出了 8 个方面的关键安全考量，包括身份和权限、数据安全、隐私、内部风险、威胁防护、（智能体之间的）沟通规则、治理、合规。



在保护好 AI 安全后，就要利用 AI 赋能安全去保护我们的网络空间。当前，聚焦安全的 AI 已经集成了我们所有的经验和思想，包括数据、优秀的安全模型，以及对 AI 的观测、审计和治理。

畅想未来，Vasu Jakkal 认为 Agentic AI 未来可以快速胜任所有安全防御领域的工作。她提出了四大畅想：

- **在威胁检测方面**，智能体可以预测新型攻击并在它们发生前就阻止掉
- **在数据安全方面**，智能体可以协助识别数据风险并采取措施提升安全和生产力
- **在零信任方面**，智能体可以自动地在正确的时间向正确的人（和 Agent）提供正确的访问权限，并根据团队和工

作的变化动态调整此权限

· **在应用安全方面**，智能体可以协同工作实现默认安全和设计安全

未来，自主 AI 的演进将重新定义当今安全的每个方面，为防御者带来全新的安全范式。智能体正在向人类学习，不断适应、行动和规划，自主工作，帮助人类实现目标，当然都在人类的参与下。

最后，Vasu Jakkal 指出，Agentic AI 将重塑安全角色。对此，笔者深有感触。AI 改变的不仅是安全技术，更重要的是透过这些技术重塑了我们从事安全的方式，改变了安全组织结构和岗位职责，改变了安全工作的流程。这种改变是建立在 AI 优先和自动化优先基础上的，这种改变绝不是简单的减少工作岗位，而是工作岗位的职责变化。从目前来看，可能还需要更多的人，懂 AI 的人。

作为对 Vasu Jakkal 演讲的呼应，在大会第二天上午的分会场，来自微软 Security Copilot 部门的市场负责人 Dorothy Li 详细介绍了释放 Agentic AI 潜力的五个关键。

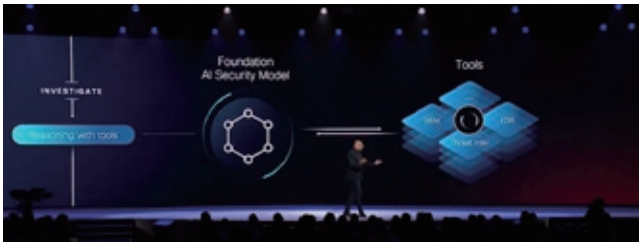
Dorothy Li 表示，AI 正在改变安全产业，我们正处于从自动化向智能体跃升的奇点，Agentic AI 将重新定义我们现在的安全，我们需要善用智能体。

第一，智能体最基本的工作方式是赋能现有的工作过程，使之更高效。第二，借助智能体消除安全中的苦力活。最典型的用例就是通过自主告警分诊找到真正重要的问题，将运营人员从告警疲劳中解救出来。第三，使用智能体的过程要完全透明，全程可控（Total clarity, full control），通过透明度建立人类对智能体的信任。第四，借助智能体变被动为主动，尤其是针对漏洞扫描、排序、修复过程的自动化。第五，从实战出发应用智能体，而不仅仅是炒作。智能体的设计要以人为本，立足于赋能人类（这才是实战），而非取代人类（这是炒作）。

思科的首席产品官 Jeetu Patel 在主会场演讲时则提到了当前安全领域面临的三大挑战——技能短缺、告警疲劳和安全的复杂性，并认为 AI 是当下最好的解药。

思科公司认为要应对以上三大挑战，不仅需要用到 GenAI，还需要一个安全垂域 LLM。在大会上思科宣布推出开源的基础 AI 安全模型（Foundation AI Security Model）。模型具备 80 亿参数规模，可以跑在 1 到 2 个 A100 GPU 上，具备推理能力（推理版目前尚未发布），因而引发了业界的强烈关注。

基于该 AI 安全大模型，Jeetu Patel 也给大家分享了安全运营的数个用例，展示了思科 AI 安全大模型的能力，都是采用智能体的形式，包括推理链、分析报告、使用外部工具、出具调查结果和推荐处置操作。



Jeetu Patel 表示，未来的安全智能将是一个由多种模型、多个智能体互相协作的全面编排的超级智能系统（Super Intelligent System）。这无疑是一个 Agentic 安全系统。

思科基础设施与安全集团的总经理 Tom Gillis 与旗下 Splunk 安全产品负责人 Mike Horn 在题为《威胁检测与响应的未来》的联合演讲中，热烈讨论了 AI 给 SOC 带来

的机遇和变革。Gillis 认为 AI 在安全领域最大和最直接的影响就是正在深刻变革安全运营。Horn 则表示，SOC 从来没有像今天一样令他兴奋。

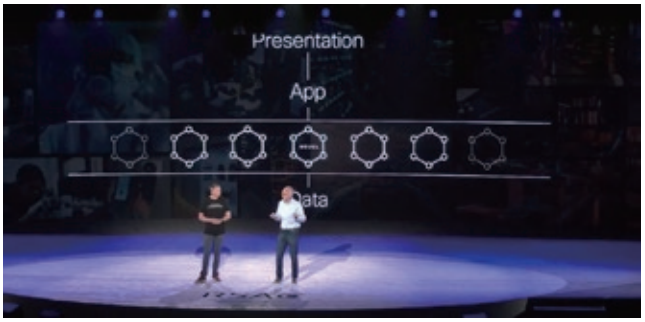
针对 AI 对 SOC 的变革， Horn 指出，首先是自动化的融合，以及更高级的自主自动化的引入，赋能安全运营人员，提升他们的工作层次。其次是将变革 SOC 的组织和人员结构。Horn 表示，AI 正在带来一场彻底的变革，而安全也需要随之进行彻底变革。

二、SOC 技术架构正在重构

当人们把 Agentic AI 为核心的各种 AI 技术应用于 SOC 的时候，SOC 的技术架构也在不可避免地进行着重构。

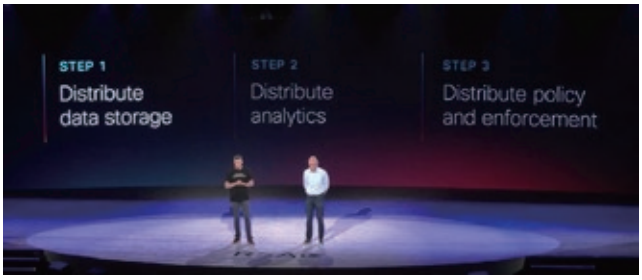
思科基础设施与安全集团的总经理 Tom Gillis 与旗下 Splunk 安全产品负责人 Mike Horn 共同在大会主会场做了一场《威胁检测与响应的未来》的演讲，从战略视角探讨了网络安全的新架构，以及现有安全运营中心 (SOC) 技术架构重构的必要性。

Gillis 首先分析了 AI 大模型的引入对当前应用软件架构带来的变革。



这种变革就在于 AI 大模型在传统的应用三层架构之间插入了模型层。模型以其特有的方式将数据变成洞察并给到上层的应用，同时也不可避免的看到了所有数据，包括机密和隐私数据。大模型输出的不确定性使得人们对于大模型能否保守这些秘密心存疑虑。这种融合 AI 的应用架构变革是前所未有的，将改变 IT 架构，进而改变安全防御的架构。

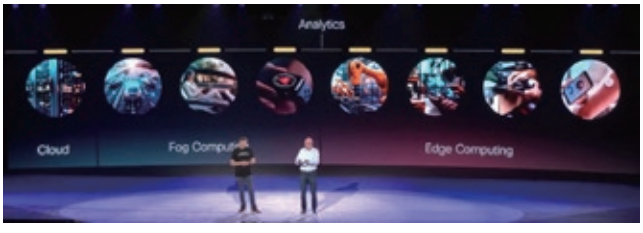
Gillis 表示，鉴于当前以 SIEM 为核心的集中式安全架构存在的弊端，在 AI 时代，（SIEM 和 SOC 平台）必须转向分布式安全架构。



Splunk 的 Horn 将这个分布式架构分为三部分：分布式的数据存储、分布式分析、分布式策略执行。

未来的安全架构必定转向分布式数据存储，这是由安全防御体系的演进规律决定的。为了避免将数据集中起来分析的低效、高成本和拖沓问题，未来用户网络中必定存在多个安全数据湖 / 库，之间的数据移动将变得十分昂贵。在摄取数据这方面我们已经取得了很大的进步，但是在访问数据这块，未来一定要支持分布式数据检索。

Horn 表示，“应用正在迁出数据中心”，分析正在向分散的数据靠拢，而 AI 正在推动这一进程。将所有数据集中到一个系统中是不现实的，最后得到的只能是一个怪兽数据湖（Monster Data Lake）。



分布式策略执行最显著的例子就是调用分散的安全设备进行响应（如遏制），策略的执行（PEP）是分布式的，但策略的管理（PDP）将维持在一个单一的策略管理平台之上。

Gillis 和 Horn 表示，未来的（SOC）安全架构一定是融合到网络编织中，分布到各处的。

SentinelOne 美洲地区 CTO Dave Gold 表示，自主 SOC 的平台架构设计需求发生了变化，更加强调可伸缩性、开放数据集成和联邦数据搜索、低成本海量数据存储、快速、云原生【笔者发现这一点在国内并不显著】、长周期数据存储。

此外，在大会分论坛上，创新公司 Auguria 在题为《为什么 AI 无法在没有正确数据的情况下拯救你的 SOC》的分享中指出，数据就绪是 AI 应用产生效果的前提和基础，强调了新型数据架构对于释放 AI 能量的意义，而这正好与笔者提出的“数据驱动是 SOC 原动力”的观点相吻合。

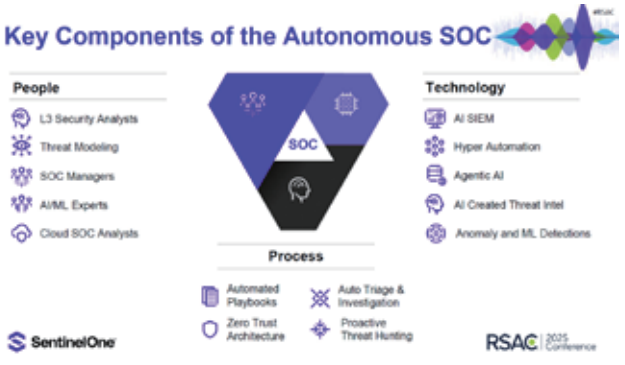
四、Agentic AI 时代的 SOC 未来趋势

1、新产品

SentinelOne 的 CEO Tomer Weingarten 在大会主会场宣发了他们的“AI 赋能的自主网络安全平台”。这个平台采用开放架构连接所有安全产品、控制器、网关、平台，汇集所有的安全数据，混合多种 AI 技术（包括编排化的 Agentic 工作流）去实现实时的观察、监测、推理和响应，功能涵盖资产攻击面、弱点、威胁等诸多方面的安全运营。

很显然，SentinelOne 紧随 CrowdStrike，实现了从 EDR/EPP 厂商向 SOC 和安全平台厂商的转型。打开 SentinelOne 的网站，可以看到除了最初的 EDR、EPP，更多看到的是 SIEM、SOAR、XDR、ITDR、TIP、VM，以及 CWPP、CNAPP、CSPM。他们公开把 CrowdStrike、微软、Wiz、Splunk、PAN 作为自己的竞争对手。SentinelOne 向我们诠释了单点产品厂商最后是如何演进为平台厂商的历程。

在次日的分会场，SentinelOne 美洲地区 CTO Dave Gold 做了一个题为《AI 驱动时代下 SOC 的未来》的报告，分享出了 SentinelOne 的自主 SOC 关键能力构成图。笔者理解，主要表现在：技术融入了 AI（包括传统 AI 和 Agentic AI），流程上以自动化为优先，人员结构上进行了调整，初级岗位（如 L1 和 L2 分析师）取消或减少，并出现更多高级岗位，譬如增加了 AI 专家。



SentinelOne 的自主 SOC 强调要用 Agentic AI 来赋能，但又不仅限于使用 Agentic AI，而要应用各种 AI 技术（即采用复合式 AI）。

Dave Gold 给用户迈出自主 SOC 转型之路的第一步提出了几点建议，包括要重构数据平台、要让 AI 无所不在、要秉持自动化优先的设计原则等。

此外，在大会的第一天，CrowdStrike 发布了基于 Agentic AI 的新组件赋能其 SOC 产品，包括名为 Charlotte AI Agentic Response 的事件调查智能体和 Charlotte AI Agentic Workflows 的 AI SOAR 组件。而 Google 也撰文介绍自己由 Gemini 赋能的 Agentic SOC，以期通过互联互通的多智能体技术，代表防御者自主或半自主地执行安全运营工作流程。

2、新交互

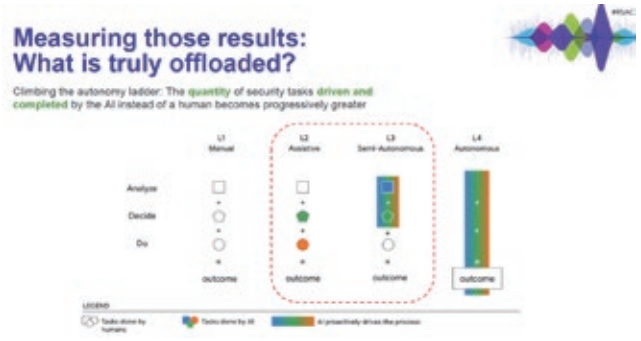
本次大会上，AI 相关的议题多如牛毛，但有一个不起眼的发言引起了笔者的关注。来自 Google 云安全的产品和用户体验高级总监 Steph Hay 做了一个题为《How Security UX Must Change, with Agentive AI》的发言，分享了他对未来 Agentic 系统的用户体验设计的想法。笔者认为，用户体验（UX）对于安全运营平台至关重要，是降低安全运营复杂性、提升平台实战化水平的关键环节。

当前，将 GenAI 作为助理的 UX 设计已经比较成形。但是对于 Agentic AI 时代的多轮交互和内容生成的结果展示还没有形成良好实践。很关键的一点就在于这个交互过程是动态的，生成的内容本身事先是不可控的，不能采用固定的 UI 设计，而要采用自适应 UI 设计。

Agentic AI 时代的系统 UX 设计还有一个很重要的原则就是要顺应 Agentic AI 的价值取向，UX 的设计要能更好地体现自主化、自动化给用户带来的成效。

3、新场景

在大会各个分论坛上，众多安全运营厂商分享了他们基于 Agentic AI 赋能安全运营的用例和场景。譬如，Opentext 介绍了如何利用基于 MITRE ATTCK 框架的 RAG 和 LLM 来增强威胁告警；Elastic 详细介绍了它们基于 RAG 的 LLM 来赋能安全运营；Exabeam 分享了应用



Agentic Workflow 实现自主安全运营的实例。此外，在简报环节，DropZone AI 发表了题为《SOC 中的 AI 蓝图：如何评估、部署和指导 AI 分析师》的报告，讲解如何将智能体集成到 SOC 分析师的工作流程中。

四、Agentic AI 深刻变革暴露管理

暴露管理作为安全运营领域一个重要组成，也受到了极大的关注。在主会场，Tenable 联合 CEO Mark Thurmond 分享了 Agentic AI 时代给暴露管理带来的机遇和变革。

Mark Thurmond 表示，网络风险就是一种业务风险。暴露管理正面临着资产暴增，工具纷乱的时代，像极了最初 SIEM 所处的时代，而暴露管理技术发展正在重蹈传统 SIEM 失败的覆辙，那就是手工的规则、机械的关联，随之而来的必定就是告警疲劳。AI 给暴露管理的未来发展带了新的机遇，有机会避开 SIEM 曾落入的陷阱。而 AI 不仅是暴露管理技术升级的机会，也是攻击者的机会，AI 时代的暴露越发充满挑战，这也更要求我们利用好 AI 去对抗 AI。安全暴露每年都在数倍的增长，但安全预算不可能每年翻番式增长，必须利用 AI 去提升运营效率，AI 将成为新一代暴露管理的核心。

Mark Thurmond 表示，暴露管理必须实现三个转变：从分散到统一、从静态到情景化和预测性、从手动到自动和 Agentic。

Agentic AI 能够帮助我们回答四个问题：需要修复什么？谁来修复？响应流程是怎样的？人类何时参与其中？AI 不仅是一个分析师，也是一个操作者；不仅仅是一个推荐者，

也是一个深思梳理的问题解决者，并且 AI 还会持续学习和进步。

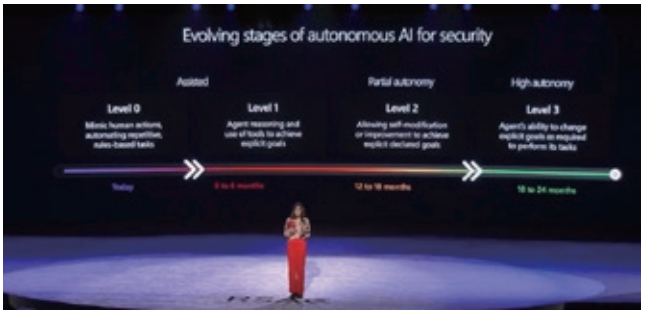
Mark Thurmond 表示，在 AI 赋能之下，暴露管理正在使我们从一个记录系统转向一个行动系统。笔者认为，SIEM 同样如此。如果说 SOAR 让安全运营实现了自动化的闭环，Agentic AI 则更进一步让安全运营实现了自主化（智能自动化）的闭环。

在分论坛上，调研咨询公司 ESG 也带来了他们对 AI 驱动的暴露管理的见解。ESG 认为，随着网络风险管理的难度不断增大，必须变被动为主动。在构建暴露管理平台的时候，必须充分利用情境数据，要将资产数据与弱点、暴露、威胁数据结合起来，做出更全面的风险分析。基于此，ESG 给出了一个 AI 驱动的威胁与暴露管理平台（TEMP）框架。

六、AI 时代是人机共智的时代

本届 RSAC 演讲者都认为，完全自主的安全（运营）不会存在——AI 不会取代人，AI 时代将是人机共智的时代。

微软安全业务的副总裁 Vasu Jakkal 在演讲时向与会者展示了自主 AI 赋能安全的演进路线图。



微软将自主 AI 赋能安全分为四个阶段，当前正在迈入第二阶段（Level1），即智能体能够推理并利用工具实现显性化的目标。而到明年，很可能会出现能够自我修改和优化模型以完成显性化声明式目标的半自主智能体。从上图可以看出，最高阶段叫高度自主化阶段，也就是说不会有完全自主化。

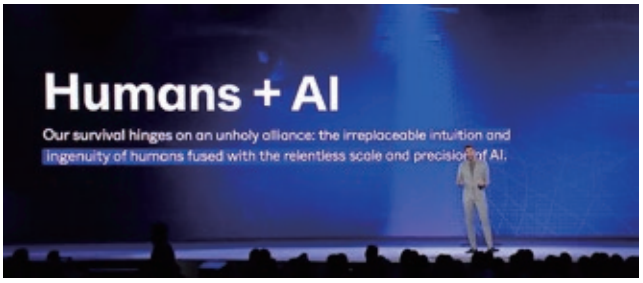
SentinelOne 美洲地区 CTO Dave Gold 在演讲中也提出了向未来的自主 SOC 演进的路线图，即从 L0 逐步向 L4 演进，目前尚处于 AI 辅助的 L2 级别。

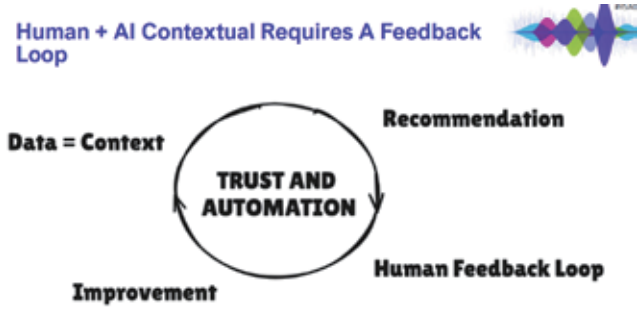
上述演进路线的阶段划分与此微软自主 AI 赋能安全的路线图大体一致，并且都不约而同地回避了“完全自主”的概念。

知名 SOC 专家 Anton Chuvakin 更是直言，现在的 AI 赋能距离真正的自主化、自动化还差得很远，并对“人工智能的进步可能会导致包括 IT 和安全在内的技术团队在

几年内大幅缩减甚至为零”的言论进行了驳斥，表示“所谓的无人自动化完全是胡扯”。

对于 AI 和人类在安全防御领域的关系，思科公司 Jeetu Patel 指出，最好的防御是二者之间紧密协作。SentinelOne 的 CEO Tomer Weingarten 在主会场的发言中也表达了相同的观点。





七、总结

从 2023 年开始正式进入安全领域，GenAI 应用模式迅速发展，从聊天式应用模式到 AI 助理应用模式，再到现在最流行的 Agentic AI 应用模式，现在 GenAI 已经成为安全运营未来发展的决定性力量。

尤其是 Agentic AI，其迭代思考和行动的工作过程，正好符合安全运营工作中绝大部分流程性任务的工作过程，完美适合应用于安全运营。Agentic SOC 时代已经来临。

当前，业内对 GenAI 和 Agentic AI 寄予厚望，大大小小的安全厂商纷纷投入这个领域，GenAI 和 Agentic AI 赋能安全运营的用例和场景不断涌现，有的已经实现了产品化，但距离真正解决安全运营面临的三大难题（人才短缺、技能不足、工作倦怠），以及应对安全工具的复杂性方面还有不小的差距。正如知名 SOC 专家 Anton Chuvakin 在 RSAC 期间接受采访时所言，（对相关难题）AI 可应对，但非 AI 可解。（AI Addressable, Not AI Solvable）。他认为，目前 AI 给安全运营带来的价值主要还是缓解而非消除（这些）难题。

本次 RSAC 大会已经清楚表明，新一代 AI 要真正赋能安全运营，仅靠 AI 自身是不够的，需要变革现有安全运营平台的技术架构，尤其是数据架构！此外，要真正让 AI 赋能的 SOC 形成持久的战斗力，还需要变革 SOC 的组织和流程，让人类和 AI、各种安全工具有效协作起来，实现人机共智。

最后，在充分利用 AI 赋能安全运营的同时，还需要充分认识到 AI 自身面临的安全问题，尤其是未来的安全运营系统也是一个 Agentic 系统，必然存在较大的安全风险，需要有效加以管控。

附：相关概念

以下为笔者梳理的相关概念。

生成式 AI（Generative AI，GenAI）：根据 NIST 的定义，生成式 AI 是指模拟输入数据的结构和特征以生成衍生的合成内容的人工智能模型，这些内容可以包括图像、视频、音频、文本和其他数字内容。Gartner 将 GenAI 定义为从数据中学习“工件(Artifacts)表示”的人工智能技术，并使用它来大规模生成全新的、完全原始的工件，以保持与原始数据的相似性。

大语言模型（Large Language Model，LLM）：根据 Gartner 的定义，大语言模型是指通过 AI 在大量文本上接受训练，使其能够解释和生成类似人类的文本输出的一种模型。通常 LLM 属于一种 GenAI，但 GenAI 不一定都是 LLM。当前网络空间安全领域应用 GenAI 主要就是指利用 LLM。

大模型（Large Model，LM）：通常指的是具有庞大

参数数量和复杂结构的机器学习或深度学习模型，具有参数规模大、架构规模大、训练数据量大和算力需求大等特点。LLM 属于一种 LM，但 LM 不等于 LLM，LM 既可以用于生成式 AI，也可以用于判别式 AI。现在很多人经常提“大模型”，同时将其与“大语言模型”等同看待，其实大语言模型（LLM）和大模型（LM）不是一个意思，需要加以辨别。

小模型（Small Model）：顾名思义，就是相对大模型而言，具有参数规模小、架构规模小、算力需求较小的特点，特别适用于算力资源有限的环境中。这里的小是跟大相较而言的，没有绝对的数值区间，跟 1000 万参数模型比，80 亿参数算大，但跟 1000 亿参数模型比，80 亿就算小了。大模型和小模型有各自适合的应用场景，实际应用中要按需而定，并可以互相配合。

传统 AI：没有明确定义，只是一种表达方式，泛指除 GenAI 外的 AI，譬如传统的符号主义的 AI，非神经网络的机器学习，使用神经网络的判别式 AI，统计分析技术（数据科学），知识图谱等技术。通常这些 AI 技术在 GenAI 大行其道之前已经有了较为成熟的应用，包括当前已经大量使用在网络空间安全领域的各种非生成式 AI，譬如基于规则推理的关联分析、基于各种机器学习的异常检测等。

复合式 AI（Composite AI）：这是 Gartner 提出来的面向工程化应用的 AI，指组合利用不同 AI 技术（包括 GenAI、数据科学、机器学习、知识图谱等技术）来提高学习效率，以生成层次更丰富的知识表示的 AI。可以将复合式 AI 理解为 GenAI 和传统 AI 的结合。当前，国际上主流的安全厂商都是用复合式 AI 赋能安全，而非仅仅依靠生成式 AI，譬如 Palo Alto Networks 的精准 AI（Precision AI），CrowdStrike 的夏洛特 AI（Charlotte AI），以及 Splunk AI 等。

智能体（AI Agent）：根据人工智能促进协会（AAAI）的定义，智能体是指能感知环境、处理信息并自主决策行动的智能实体。根据 Gartner 的定义，智能体是利用人工智能技术进行感知、决策、采取行动，并在数字或物理环境中自主或半自主地追求既定目标的软件实体。行为体（Agent）这个概念已经有几十年的历史了，当 AI 应用到行为体中之后，就出现了智能行为体（简称智能体）。可以认为，AI Agent 是 Agent 的一个发展方向和发展阶段，但 AI Agent 中的 AI 并不限于当前热门的 LLM / GenAI，而是泛指各种 AI。

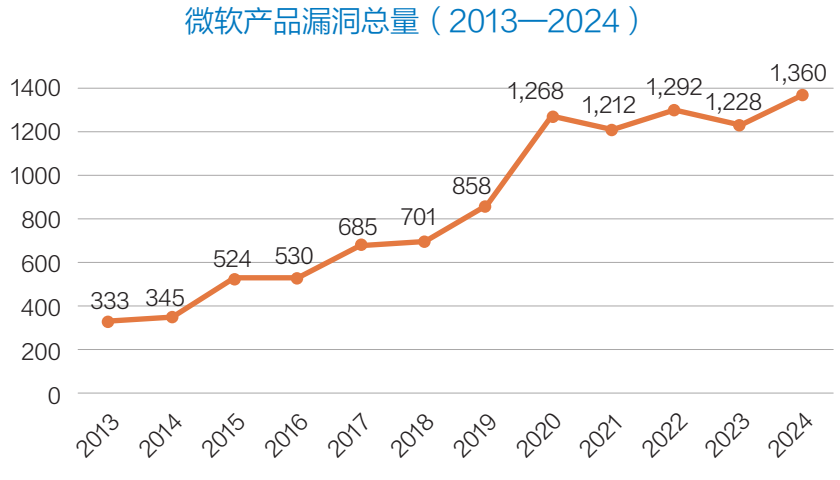
自主式 AI（Agentic AI，暂译为“自主式 AI”）：这个概念最早见于 OpenAI 在 2023 年 12 月发布的一份白皮书，但其真正成形要归功于吴恩达。他在 2024 年年初红杉资本举办的 AI 峰会上提及，随后又在 Snowflake 峰会上进行了完善，并给出了 Agentic 推理的四种设计模式：反思、工具使用、规划和多行为体协作，从而奠定了 Agentic AI 的框架基础。2024 年 10 月，Gartner 发布 2025 年十大战略技术趋势，Agentic AI 居首。Gartner 将 Agentic AI 定义为目标驱动的软件实体，这些实体被授予代表组织自主决策和采取行动的权限，使用人工智能技术——结合记忆、规划、感知、工具和护栏等组件——来完成任务并实现目标。

Agentic AI 和 AI Agent 区别：两者的区别在于看问题的视角不同：AI Agent 是一种对 Agent 的类型划分，关键点还是落在 Agent 上，AI Agent 代表了所有利用 AI 赋能的 Agent，但具体如何赋能、赋能到什么程度，尤其是 Agent 的“自主程度”（Agency / Agenticness，暂译为“自主程度”）无法表达。正如吴恩达所述，“Agent 这个名词是一个二元性的术语，无法进一步区分不同自主程度的 Agent”。而 Agentic AI 代表了一种 AI 技术的类型划分，并可以认为是生成式 AI 的一个演进方向，关键点落在了 AI 上，如吴恩达所言，“Agentic 作为形容词可以（从 AI 这个视角来）观察和思考不同自主程度的 Agent”。Agentic AI 代表了一种新型的 AI，这种 AI 超越了当前的 GenAI，其本质是 AI 从被动执行任务向主动实现目标的进化，代表了 AI 从单一功能工具开始向通用智能体跃迁。因此有一种观点进一步认为 Agentic AI 代表了比 AI Agent 更高的自主程度，Agentic AI 具有调度编排多个不同 AI Agent、通过 AI Agent 间的协作达成既定目标的能力。

自主式系统（Agentic System）：是指应用了 Agentic AI 技术的各种应用系统。

2025 年微软漏洞报告：数量再创纪录，应对更复杂

过去 12 年来，BeyondTrust 发布的年度《微软漏洞报告》（以下简称《报告》）一直是评估软件生态系统安全性的重要晴雨表。《报告》将微软 CVE（通用漏洞与披露）数据转化为可操作情报，帮助安全领导者理解漏洞的演变、产品相关风险的变化、微软防御能力的增强，以及仍然存在严重漏洞，以及未来漏洞风险的走向。



2024 年微软总漏洞数量达到 1360 个，创历史新高

《报告》既是历史教训，也是前瞻性预测。近年来，《报告》显示“身份”已成为攻击链的核心部分，现代的入侵行动常常要结合传统漏洞和基于凭证的攻击路径。

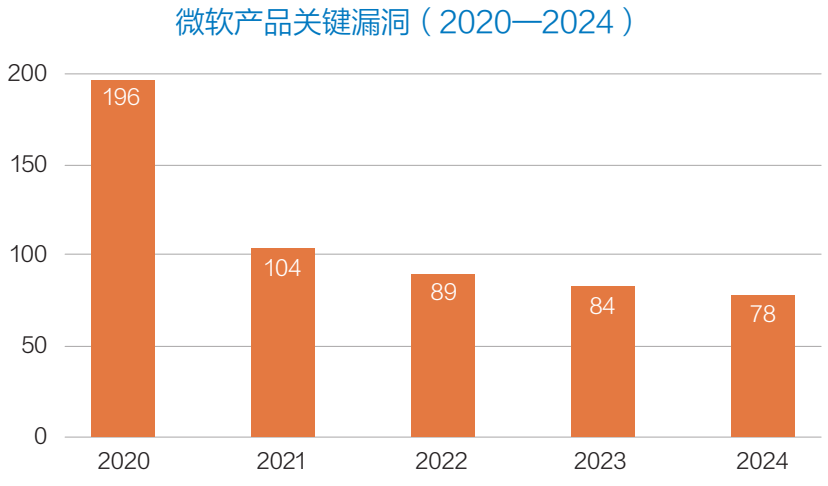
2025 年《报告》调查结果和分析强调，需要深思熟虑并确保及时部署安全补丁，但前提是经过内部测试。

一、2024 年微软披露漏洞创新纪录，增长 11%

2025 年《报告》指出，2024 年共披露了创纪录的1,360个微软漏洞，比 2022 年的前高点（1,292 个）增长了 11%。

这提醒我们：无论制定了多少最佳实践、开发人员受过多专业培训，或者通过质量保证和渗透测试进行过多么全面的测试代码，人类和 AI 依然会写出可被利用的软件漏洞。无论使用什么样的代码审查其实都不重要——即便是 AI 生成的代码。本质上我们仍然是人，仍然会犯错。

在众多漏洞中也有一丝曙光：微软发布的“严重”漏洞（即令首席信息安全官彻夜难眠的那些）下降到十多年来的最低水平。2024 年，仅 78



严重漏洞在整个微软生态系统中的比例持续下降

个漏洞被评为严重漏洞， 2020 年为 196 个。2013 年发布的严重漏洞占微软公开披露漏洞的 44%，而 2024 年的这一比例降至不到 6%。

在解决严重漏洞和减少高风险代码方面，微软确实取得了进展。微软改进了工具，并培训了开发人员。当然，如今出现的严重漏洞往往具有新颖性，且更难利用。

虽然“总数上升”与“严重程度下降”似乎是矛盾的说法，但事实更为复杂。微软及其生态系统在一些关键领域确实取得了进步。这是一个胜利，但不是全面的胜利。攻击面仍在扩大，漏洞数量仍在增长，而攻击者也在快速适应，采用新的方式（包括基于身份的攻击路径）来利用这些漏洞。

二、EoP 和 RCE 仍是主要威胁

任何攻击者想要利用系统，目标无非两点：

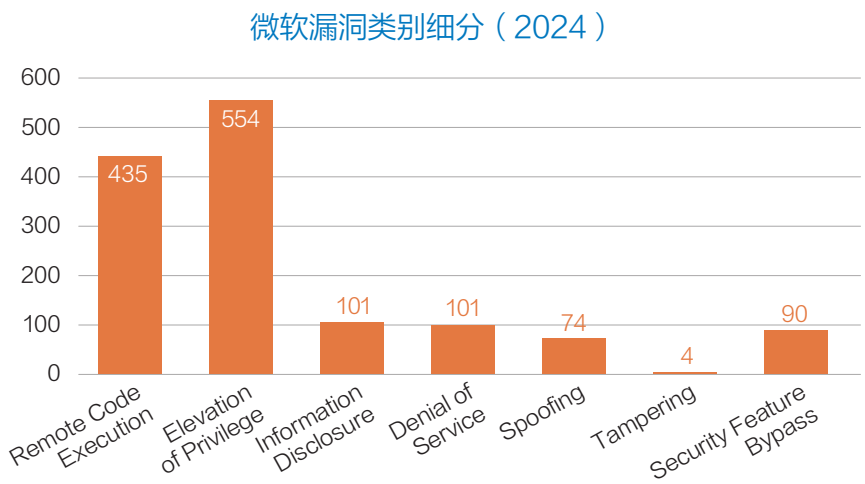
1. 执行代码，无论通过恶意软件还是“利用系统自带功能”的攻击（LOTL）；

2. 拥有足够高的权限，以执行这些代码，从而实现攻击目的。

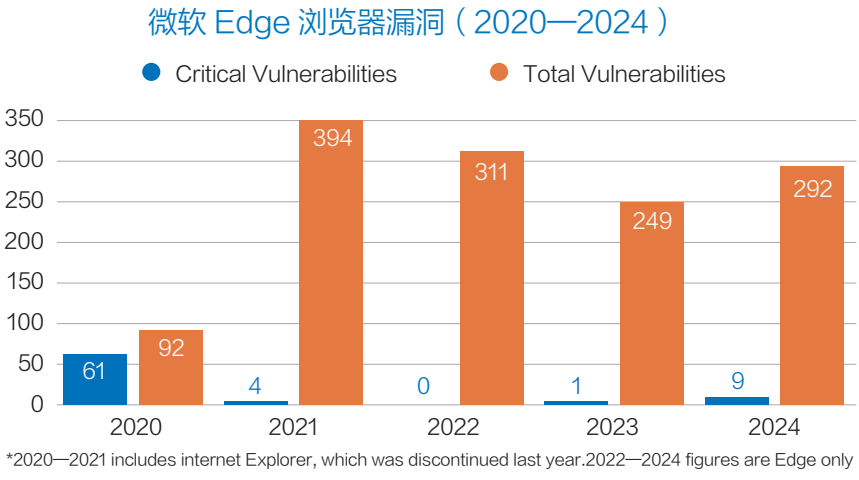
远程代码执行（RCE）和权限提升（EoP）漏洞正好提供了完美的组合，实现这两个目标，攻击者对此非常清楚。

2024 年，EoP 漏洞连续第五年领跑所有漏洞类别，占微软所有漏洞披露的 40%。这说明攻击者往往更容易“登录”系统而不是“入侵”系统，特别是当攻击者能够利用合法账户进行权限升级时。一旦入侵成功，权限就是力量。拥有权限就如同拿到钥匙，可以随意行动。

RCE 漏洞允许攻击者在未认证的情况下远程执行恶意代码，常见攻击媒介包括未打补丁的软件、Web 服



EoP 漏洞占 2024 年微软漏洞的 40%



2024 年 Edge 浏览器发现 292 个漏洞，严重漏洞 9 个，2022 年为零

务或恶意文档。2024 年，RCE 占微软漏洞总数的 32%，虽较 2013 年的 58% 显著下降，但考虑到微软产品的覆盖面，这仍是巨大的攻击面。

单独来看，每类漏洞都很危险。当 RCE 和 EoP 结合时，威胁就更加严重：RCE 传递有效载荷，EoP 授予权限，则可能导致严重的安全事件。即使整体上严重漏洞数量有所减少，RCE 和 EoP 仍然占据主导地位，这足以引起高度重视，提醒我们及时修复所有漏洞。

三、“意想不到的风险”：过时协议卷土重来

另一个令人不安的趋势是安全功能绕过漏洞的激增（允许攻击者规避或绕过系统原有安全机制的漏洞类型）：自 2020 年以来已增长三倍，从 2020 年的 30 个增至 2024 年的 90 个。

这些并非理论上的担忧，攻击者正积极利用易被突破的老旧安全机制。例如，俄罗斯网络犯罪组织 RomCom，利用 CVE-2023-36884 绕过微软的“Web 标记”防护。2024 年又有类似漏洞被用于攻击老旧防御手段。

这只不过是软件上的软件叠加而已。安全工具仍然是软件，可以像其他任何东西一样被利用。这就是为什么现在 60% 的绕过漏洞都针对这些保护层本身。

微软在这方面需要迎头赶上。诸如用户账户控制和 Web 标记（Windows XP 时代的遗留功能）等老旧功能，在如今的网络钓鱼工具包和社会工程攻击面前已不堪一击。微软在安全现代化方面取得了长足进步，但对过时协议和老旧控件的持续利用表明，微软迫切需要淘汰过时的系统，淘汰构建这些系统所基于的陈旧安全假设。不幸的是，这进一步表明，这些老旧系统并非设计就安全，而是事后才进行的补救。

四、漏洞对微软产品的影响

IE 浏览器已于 2022 年正式退役，它的幽灵仍徘徊在企业环境中。2024 年，攻击者仍在利用 IE 组件 MSHTML 伪装恶意文件，凸显了过

时技术在生产环境中依然存在的危险。微软当前的Edge浏览器也未能幸免，2024 年报告了 9 个严重漏洞，打破其此前“零严重漏洞”的纪录。这些漏洞允许攻击者突破浏览器沙盒限制，并以本地权限执行代码，引发多次 CISA 的多项安全警告。如果与糟糕的权限管理（如允许用户以本地管理员身份运行）相结合，这些漏洞会显著增加组织的风险敞口。

Windows 仍是微软的主力产品，也是其软肋。2024 年 Windows 报告了 587 个漏洞，其中 33 个被评为严重漏洞。虽然有些漏洞源于仍在使用的过时技术（如 IE），但也有一些漏洞是全新的，如 CLFS 驱动程序中的零日漏洞 CVE-2024-49138，可获得系统级访问权限。讽刺的是：尽管 Windows 11 被誉为微软迄今为止最安全的操作系统，但根植于 20 年前遗留代码的漏洞仍在不断涌现，破坏了其现代安全的承诺。

不幸的是，云环境的形势也不容乐观。自 2020 年以来，Azure 漏洞数量几乎翻倍。人工智能成为新的风险前沿：2024 年，CVE-2024-38206 与 CVE-2024-38109 暴露了微软 Copilot Studio 和 Azure Health Bot 中存在的漏洞，涉及信息泄露和权限提升。

人工智能正在成为每个人都应该关注的攻击媒介。我们在将人工智能工具嵌入到系统中，但通常并不清楚哪些数据被捕获、这些数据将流向何处、存储多长时间，以及是否受到强加密保护。对人工智能在企业环境中的风险的认识才刚刚起步。

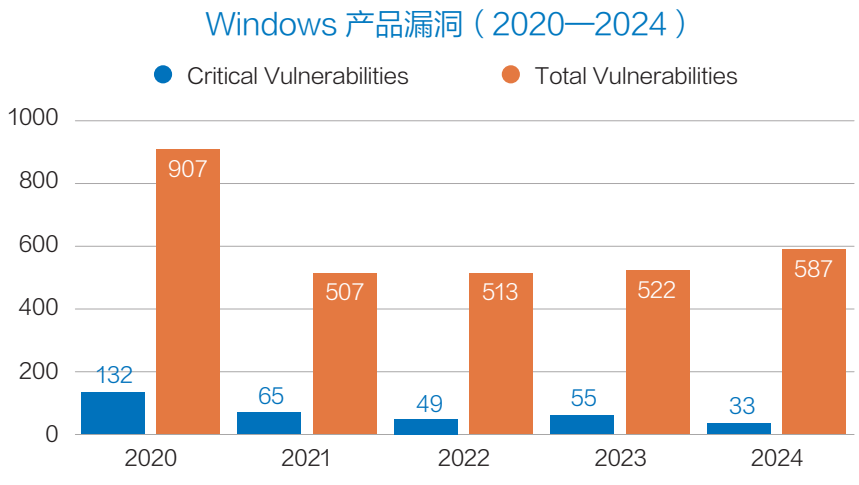
随着各大机构争相采用人工智能平台，AI 正成为一个新的攻击面。这些攻击面难以量化、难以测试，并且可能被滥用。

五、漏洞补丁的困境

如果说“人”是网络安全的最大弱点，“未打补丁的漏洞”则紧随其后。及时修补，对领先于攻击者至关重要。漏洞一旦被披露并发布补丁，攻击者往往会竞相对修复应用进行逆向工程，力图在组织应用更新之前利用系统漏洞。

然而，出于对稳定性和潜在中断的担忧，企业往往不愿立即部署补丁。没有什么比常规安全补丁导致资源离线甚至更糟的情况更能毁掉一个周末了。对微软补丁不稳定性问题的担忧并非毫无根据。2024 年，微软发布了多个补丁，但问题比修复的还多；此外，微软的更新还引发了系统回滚、关键功能失效，甚至禁用自动更新机制。

业界将补丁服务级别协议（SLA）压缩至 24 ~ 48 小时，但这也减少了



2024 年 Windows 系统报告 587 个漏洞，其中 33 个为严重漏。

充分验证的时间。结果一些补丁导致生产环境崩溃，从而导致对补丁的信任被削弱，组织陷入“要安全还是要稳定”的两难境地。

预览版本功能（包括自动更新系统本身）的崩溃，给企业带来了不同程度的问题和镜像构建问题。正如近期事件及 2024 年臭名昭著的 CrowdStrike 更新事件所表明的那样，在没有经过适当测试和验证的情况下，加速发布更新可能会带来灾难性的后果。

微软的补丁声誉此前曾出现过动摇。2025 年，微软应更加注重补丁的质量和稳定性，以重建信任，并鼓励更快地采用整个漏洞和补丁管理生命周期。因为在网络安全领域，快速发布补丁并不等同于正确发布补丁。

六、降低微软漏洞风险的实用建议

在当今混合且快速演变的威胁形势下，要缓解 Microsoft 漏洞，需要建立战略性的多层防御机制。

以下是企业现在可以采取的最有效的措施，能够降低风险并增强网络弹性：

1. 实施最小权限与零信任架构

移除本地管理员权限并持续执行最小权限原则，可减轻多达 75% 的严重漏洞影响。

2. 制定针对性漏洞管理策略

摒弃一刀切的补丁思维。应根据企业环境背景、威胁模型及业务影响，对漏洞实行优先级排序。

3. 保护远程访问路径

使用增强身份验证和会话控制，对所有远程访问进行分段、监控和保护，尤其要防范特权用户，以及来自承包商或第三方等不可信来源的访问。

4 集成身份威胁检测与响应（ITDR）

可视性是关键。ITDR 工具可识别身份相关风险，快速响应特权滥用与横向移动。ITDR 工具能够快速响应身份滥用、特权滥用和横向移动。这些都是现实世界中 Microsoft 漏洞利用链中常见的策略。

2025 年微软漏洞报告数据也带来一些积极信号：严重漏洞数量下降、披露实践更加完善，且在曾经构成持续风险的领域取得了进展。但有一点未变：安全责任归根结底在于企业自身。

微软可以开发更安全的软件，但如何部署、维护和保护则取决于各组织自身。以“最小权限 + 零信任 + 身份安全”为核心的策略，在补丁发布之前也能显著降低风险。此外，通过漏洞优先级排序、远程访问加固和强特权访问控制，将不仅是被动响应，更能实现主动防御。

针对 2025 年安全漏洞的首要建议： 增强对环境的可视性。记住，Windows 10 将在 2025 年 10 月终止支持，除非你付费购买延长支持。这将是下一个风险高峰，而且来得很快。

关于作者

Morey J. Haber

BeyondTrust 首席安全顾问

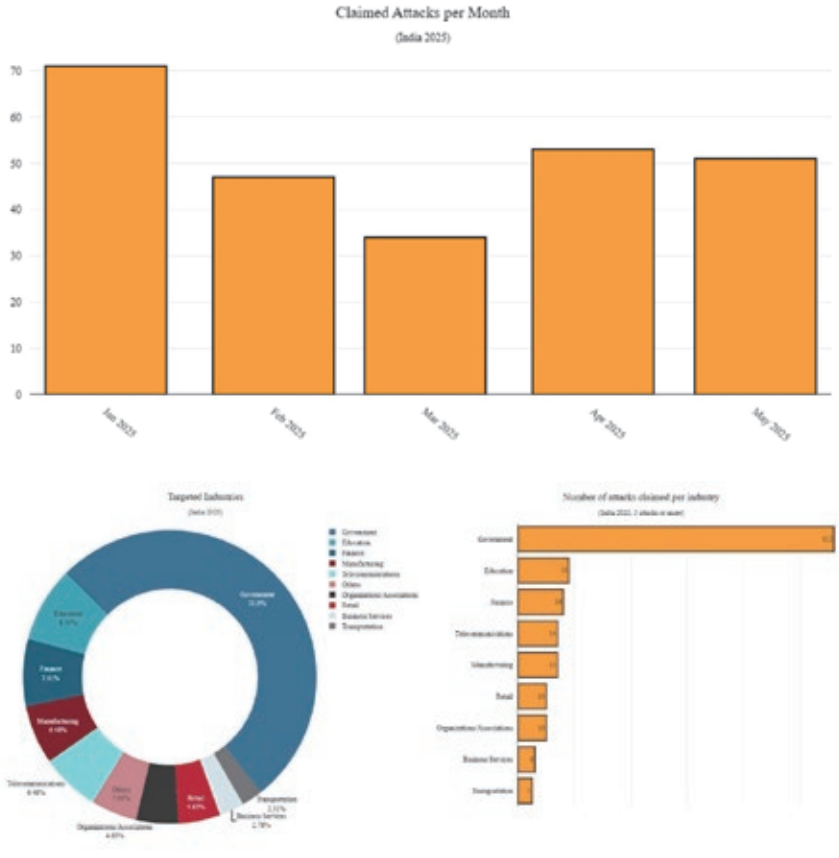
印巴最新冲突导致两国处于阵营性黑客网络战边缘

近日，谷歌公司宣布斥资 320 亿美元收购热门云安全公司 Wiz。这是该公司在斥资 56 亿美元收购曼迪安特后不到两年，在企业网络安全业务方面又迈出的重大一步。

这不仅是谷歌公司有史以来规模最大的一笔收购，也是自印巴最新冲突爆发以来，印度政府、国防、教育等目标遭受亲巴基斯坦黑客组织的大量网络攻击，虽然相关攻击未造成重大损失，但印度仍面临国家级黑客的重大网络威胁，同时印巴两国也处于阵营性黑客网络冲突边缘。

根据印度网络安全公司 CloudSEK 的监测情况，5 月初以来，针对印度政府和教育服务器的网络攻击总计超过 100 起，但大多数攻击的影响甚微；虽然该公司检测到了重大的网络威胁，但相关攻击并未成功影响关键基础设施或其他服务；网络攻击主要针对印度政府和教育部门，但自 5 月 7 日以来，攻击次数正在大幅下降。以色列互联网安全公司 Radware 发布的研究报告称，针对印度的网络攻击事件在 5 月 7 日激增，但随后有所缓和；针对印度 DDoS 攻击事件超过 75% 针对印度政府机构，其次分别是金融行业（8.5%）和电信行业（6.4%）；参与攻击的黑客组织包括 AnonSec、Keymous+、Mr Hamza、Anonymous VNLBN、Arabian Hosts、Islamic Hacker Army、Sylhet Gang、Red Wolf Cyber 和 Vulture 等。

CloudSEK 公司表示，该公司已追踪到 200 多起网络事件，其中 95% 并未造成实际影响，大多数攻击是短暂的 DDoS 攻击或网站页面破坏；黑客所声张的数据泄露情况，通常缺乏证据且难以核实，经常是夸大其词或完全捏造；有的黑客组织甚至重新打包旧数据，伪造成影响深远的新入侵行为，目的是引起恐慌和开展宣传。Radware 公司表示，黑客行动主义者的复杂程度和技能参差不齐，有些激



自印巴紧张局势升级以来，印度网络安全公司 CloudSEK 追踪到 200 多起网络事件，但内部人员表示约 95% 的攻击并未造成实际影响，主要是短暂的 DDoS 攻击或对网站页面的短暂破坏。

进组织无所作为却又大肆声张，更多的是在制造混乱和散布虚假信息，但也有一些黑客组织会自己开发工具；基本的 DDoS 防御措施，足以防御最常见的拒绝服务攻击类型，同时最大限度地减少任何破坏的影响。

网络安全公司认为，尽管与巴基斯坦有关的黑客组织的言论大多是虚张声势，但国家级 APT 组织的网络攻击威胁对印度构成重大风险；与巴基斯坦有关的黑客组织 APT36，至少自 2013 年以来便攻击印度军事、政府和国防相关部门，经常利用 Crimson、Eliza 和 Capra 等恶意软件开展鱼叉式网络钓鱼攻击。

国际刑警组织网络取证专家认为，近期的攻击是巴基斯坦黑客针对印度数字资产发动的更广泛网络信息战的一部分，攻击活动可分为 5 个阶段：

- 第一阶段（4 月 23 日至 4 月 26 日），由宗教黑客组织进行小规模破坏；
- 第二阶段（4 月 27 日至 5 月 2 日），针对电子政务平台发起拒绝服务攻击；
- 第三阶段（5 月 6 日），高技能攻击者开始在制造业和石油天然气行业发动勒索软件攻击和数据盗窃；
- 第四阶段（5 月 7 日至 5 月 12 日），APT36 等 APT 组织将目标锁定在银行和支付系统，其中包括印度国家支付公司（NPCI）；
- 第五阶段（5 月 13 日至今），相关攻击得到土耳其、伊朗和朝鲜等国家的国家行为者支持。

随着地缘政治紧张局势加剧，印度和巴基斯坦正处于不断演变的网络战边缘，印巴冲突也成为网络威胁行为者聚焦的最新地区冲突。印度马哈拉施特拉邦网络部门透露，印度已确认多个 APT 组织在 4 月帕哈尔加姆恐怖袭击后对印度关键基础设施网站发动了超过 150 万次网络攻击，尽管只有 150 次袭击成功；印巴停火后，印度政府网站仍面临来自巴基斯坦、孟加拉国、印度尼西亚、摩洛哥和中东地区国家的大量网络攻击。

Radware 公司 5 月 8 日发布的题为《印度和巴基斯坦紧张局势加剧黑客攻击》的最新报告称，出于政治、社会和宗教动机的黑客行动组织正在加强协调，加大针对共同对手的攻击力度。黑客行动分子正在使用混合策略，利用应用层和容量耗尽型 DDoS 攻击，使防御变得更加复杂；双方的黑客活动分子都利用 DDoS 攻击、僵尸网络、数据泄露和破坏等手段攻击关键基础设施，目的是破坏服务并削弱公众信任；自印巴冲突以来，东南亚黑客组织间正在形成新的联盟，其中一些联盟甚至延伸到传统上反对以色列的组织，如伊朗黑客组织 Vulture；双方阵营的网络互攻击可能会形成一个“危险的报复循环”，增加进一步网络攻击的风险，并可能使双方的关键基础设施都成为攻击目标。

关于作者

赵慧杰

虎符智库专家、网络空间安全军民融合创新中心高级研究员。长期从事网络安全、互联网发展等领域研究工作，对外军网络战、国际网络安全态势、全球网络空间竞合及新技术新应用发展等具有深厚研究造诣，先后获得军内成果奖七项。

每年 HW 演习中，弱密码贡献了多少扣分？

就在每年 HW 结束之后，没错是之后不是之前，网络安全行业里的众多朋友，有甲方，也有乙方，都会纷纷找到我、告诉我，自己某个系统被攻击队打穿了，手段朴素至极，利用的就是开放到公网的某个系统的用户弱密码。

如果你以为朋友们是想亡羊补牢，采取合理且积极的手段去彻底治理这个风险，那你就大错特错了。大家只是需要一个向上汇报的材料，去跟老板讲“我们接下来可以怎么做”“我们应该怎么做来解决这个风险”。然后，事情就闭环且完结了，一切都没有任何改变，来年继续在同一个地方栽跟头，当然可能只是在攻防对抗中被扣掉 1 分 2 分，无伤大雅。

时间就在历史的不断重复中，缓缓向前推进。

01 强密码，本身就是违背人性的

作为安全从业者，我们十分擅长为用户制定安全的密码规则，从密码的构成到强制更新的周期设定，再到复杂的多因子认证，我们如数家珍。

抛去安全从业者自嗨，我们也得承认，这些真的是没啥人性的规则，凡是逆人性之事，必遭受人性的敷衍和对抗。

因此我们会看到，虽然强制要求 90 天更换密码，但员工采取“规律性递增”（如 Password01 → Password02）的方式应付，反而降低了账户安全性。根据 Verizon 数据报告，此类“伪强密码”在泄露事件中的占比，从 2019 年的 17% 升至 2023 年的 29%；我们也会看到，28% 的高管存在多个系统共用同一密码的情况。这种普遍存在的“安全惰性”，使得企业制定的 16 位混合字符密码策略形同虚设。

上有政策，下有对策，人性的懒惰，就是弱密码的永久温床。

02 越容易被验证的地方，越不安全

企业密码管理存在明显的“二八悖论”，80% 的防御预算投入在应对高级威胁，却放任 20% 的基础安全漏洞持续存在。企业投入大量资源构建防火墙、部署入侵检测系统、升级威胁情报能力，却常常在一个看似简单的问题上“翻车”——弱密码。这个被反复提及却始终未被根治的漏洞，成为攻击者撬开企业安全防线的万能钥匙。

为什么会出现这样的现象，作者

看来主要是有以下几个缘由。

1、利益平衡：假设安全防线失守，弱密码此等问题引发不了灾难级别的事故，风险结果可承受。同样的道理，如果企业卖数据可以赚 1000 万，政府罚款 200 万，那么这事就无法禁止；如果银行安全建设要全部合规，成本也是 1000 万，但银保监罚款才 200 万，那么就有银行选择对风险视而不见；如果金融放贷公司，将利息层层包装为高额服务费，只会招来政府批评和要求整改，那他们就会不停想办法把利息包装成保险、理财产品等等。

2、瓜田不纳履，李下不正冠：经过瓜田，不可弯腰提鞋；经过李树下不要举起手来整理帽子，避开易被质疑的情境。怎么理解，企业老板很难懂得网络渗透的技术，无法演说防火墙的话术，更难以猜测黑客的手腕，但他真懂什么是应用账号啊。企业 IT 或者安全团队，将重兵和预算用在防火墙、蜜罐、APT 这些事物上面，老板难以评价，更无法验证有效性，安全团队的工作反而变得简单。但如果花在应用账号治理上，难免被老板指点江山（他以为他懂），且效果好不好过于容易被验证，这与职场人来讲，极度缺少了辩解的空间，不利也。

3、需要过多安全之外的协同：应用系统非安全团队开发，如何改；并非上个产品功能，或者买个安全软件就能搞定的事，太难；老板只听方案，不批预算，神仙来了也得叹息。

03 破局密码困局的一个路径，消灭密码

人们倾向于选择阻力最小的道路来完成任务，当安全措施增加了工作的难度时，他们会寻找绕过这些障碍的方法，从而导致潜在的安全风险。

传统基于账号和密码的身份验证方式存在固有的弱点。即使用户选择了强密码，并定期更换，也无法完全避免被钓鱼网站或恶意软件捕获的风险。当涉及到复杂的密码管理和多平台的账户时，用户体验也会变得非常糟糕，导致很多用户选择更容易记住但也更不安全的简单密码，或是重复使用相同的密码。

因此，一个激进但可能最有效的解决方案是，彻底消除账号密码机制，或者不让员工掌握应用的账号密码，这样即使遇到了钓鱼网站，也能达到防止被钓鱼的事情发生，这或许能从根本上解决弱密码攻击的问题。

关于作者

胡珍凯

LOCKet 联合创始人，国内最早的 CASB 网络安全服务公司。前阿里巴巴数据安全负责人，全面负责阿里巴巴数据安全产品线。现数影星球创始人，致力于为企业提供高效、安全、智能的数字办公空间。

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