内部资料 免费交流

出版物准印证号：京内资准字 2123- L0058 号

SECURITY INSIDER

网安26号院

奇安信网络安全通讯

协作、AI与整合

——来自RSAC 2024的一线报道

P13

第41期

2024 年 5 月

奇安信
新一代网络安全领军者

打造新一代中国特色的安全托管服务

时刻守护您的网络安全

奇安信安全托管服务以威胁发现为基础、以分析处置为核心、以发现隐患为关键、以解决客户问题为目标，7*24小时全天候全方位守护客户网络安全。

两种模式
模式随心选择

- 直营服务模式：奇安信产品+MSS
- 合作服务模式：技术、产品、服务整体托管

多种形态
全面助力建成

- 城市运营中心
- 行业安全运营中心
- 企业安全运营中心

两化融合
帮您真正实现

- 集中服务化：统一监测、预警与通报
- 服务集中化：标准统一、质量可控、资源共享

首创“云地结合”模式

打破传统的托管仅限“云端监测”的认知开辟“云地结合”模式，云端+地端实现真正的闭环服务。

7*24h实时持续监测

“地球不爆炸，我们不放假”——7*24h持续监测，充分保障常态化运营。

安全事件响应快一步

对APT攻击、网络攻击等长效监测，提前预警，响应快一步。

安全事件处置规范化

事前检测、事中分析、事后总结，真正实现闭环，并在实战中不断加固。

专家“一对一”指导

专家通过视频一对一的方式与您“面对面”沟通指导，不仅让您了解现状，还能防患于未然。

RSAC 还是 RSAI？

毫无疑问，人工智能是网络安全盛会 RSAC 2024 最热门主题，成为最受欢迎的话题。思科、微软，甚至美国国土安全部等公司都以人工智能为主题发表主题演讲，以至于有参会者认为 RSAC 应该改称为 RSAI。

对于参加 2023 年 RSAC 峰会的人而言，围绕 AI 的讨论都不应该感到意外。当时生成式 AI 才刚刚出现几个月，每个人都想谈论它，但没有人确切知道它会对网络安全产生什么影响。

一年过去了，网络安全行业已将人工智能纳入到工具和解决方案中。RSAC 2024 上有超过 100 场与人工智能有关的会议。许多与会者最感兴趣的是生成式人工智能这把双刃剑。人工智能继续重新定义网络安全，它既是增强防御机制的工具，也是复杂威胁的载体。“影子人工智能”一词被多次提及，首席信息安全官们担心影子 IT 和影子云面临的风险开始在使用未经授权的人工智能中重演。人工智能在虚假信息和深度伪造中的作用让人担心其对政治、欺诈和社工攻击的深远影响。

网络安全专家指出，现在可能需要将生成式人工智能与其他类型的人工智能区分开来。人工智能技术在整个会议中占据了压倒性的地位，给人一种新奇的感觉，好像是去年才推出的东西。许多小组讨论都涉及机器学习和大型语言模型，以及如何利用这些技术为网络安全工具带来优势。要知道，人工智能并不新鲜，它已经以某种形式存在了几十年。

从 RSAC 2024 可以看出，人工智能的发展还只是冰山一角，而且围绕人工智能的炒作短期内不会消退。RSAC 2024 为我们明确了应对网络安全错综复杂现实的战略路线图。随着数字威胁的演变，我们利用和防范 AI 的措施必须迅速跟上。

明年的 RSAC 上，AI 会继续成为热门主题吗？哪些安全问题、新兴技术或新流行语将成为与会者最关注的焦点呢？

总编辑

李建平

2024 年 5 月 1 日

CONTENTS 目录

安全态势

月度专题

协作、AI 与整合
——来自 RSAC 2024 的一线报道 P13

2024 RSAC 的主题是“可能的艺术”，反映出网络安全届对技术创新、AI 风险和社区协作的关注。“通过拥抱激发动力和想象力的社区力量，通过协作体验推动网络安全的卓越发展，让不可能变得更加可能。”

面对 GenAI 给网络安全产业带来的变革性作用，网络安全企业都努力贴上了 AI 的标签。安全专家预测，人工智能将会长期改变安全行业。“从现在起五年后，所有的攻击都将是人工智能对人工智能的攻击，因为人类无法以同样的速度进行防御。

RSAC 2024 另一个主要话题是，整合和简化安全工具。集成的趋势在整个行业中正逐步得到落实。没有任何一家供应商能够提供有效防御不断变化威胁的所有功能。转向集成解决方案、提供最佳的客户价值成为很多安全企业的选择。

安全之道

专　栏

报告速递

奇安资讯

《网安 26 号院》编辑部
主办　奇安信集团

总　编　辑：李建平
安全态势主编：王　彪
月度专题主编：李建平
安全之道主编：张少波
奇安资讯主编：陈　冲
报告速递主编：刘川琦
专　栏主编：任润波

奇安信集团　虎符智库　安全内参

索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

索阅邮箱：26hao@qianxin.com
地　　址：北京市西城区西直门外南路 26 院 1 号
邮　　编：100044
联系电话：（010）13701388557
出版物准印证号：京内资准字 2123- L0058 号
编印单位：奇安信科技集团股份有限公司
发送对象：奇安信集团内部人员
印刷数量：4500 本
印刷单位：北京博海升彩色印刷有限公司
印刷日期：2024 年 5 月 26 日

政策篇

国内，持续深入构建数据安全治理体系。财政部等印发《会计师事务所数据安全管理暂行办法》，天津自贸区发布国内首个自贸区数据出境管理负面清单，九部门联合印发方案要求增加数据安全人才有效供给；

国际上，美国总统拜登签署《关于关键基础设施安全和弹性的国家安全备忘录》，取代 2013 年奥巴马时期发布的关键基础设施保护总统政策文件 PPD-21，这是美国关基保护历程上的重要里程碑。

国内

财政部、国家网信办联合印发《会计师事务所数据安全管理暂行办法》

5 月 10 日，财政部、国家网信办联合印发《会计师事务所数据安全管理暂行办法》，要求加强会计师事务所数据安全管理，规范会计师事务所数据处理活动。该文件共五章 36 条，包括总则、数据管理、网络管理、监督检查、附则。该文件要求，会计师事务所为上市公司、国有金融企业、中央企业、关键信息基础设施运营者、超过 100 万用户的网络平台运营者、境外上市的境内企业等提供审计服务的，需遵循本办法。会计师事务所应当采用网络隔离、用户认证、访问控制、数据加密、病毒防范、非法入侵检测等技术手段，及时识别、阻断和溯源相关网络攻击和非法访问，保障数据安全。

《零信任参考体系架构》等 16 项网络安全国家标准获批发布

5 月 9 日，根据国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2024 年第 6 号），全国网络安全标准化技术委员会归口的 16 项国家标准正式发布。具体清单包括《网络安全技术 零信任参考体系架构》《网络安全技术 网络安全众测服务要求》《网络安全技术 软件供应链安全要求》《网络安全技术 软件产品开源代码安全评价方法》《网络安全技术 证书应用综合服务接口规范》等。

天津自贸试验区数据出境管理负面清单发布

5 月 9 日，中国（天津）自由贸易试验区管理委员会、天津市商务局联合印发《中国（天津）自由贸易试验区数据出境管理清单（负面清单）（2024 版）》。该文件在天津自贸试验区企业数据分类分级的基础上，将出境数据分为 13 大类 46 子类，每个子类均对数据基本特征作了出详细描述，并给出了具体示例。该文件列明了天津自贸试验区企业向境外提供数据需要申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的情形。天津自贸试验区企业向境外提供《负面清单》外的数据免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

商务部印发《数字商务三年行动计划（2024—2026 年）》

4 月 26 日，商务部印发《数字商务三年行动计划（2024—2026 年）》，提出推动商务各领域数字化发展的具体举措。该文件提出，建立商务领域数据分类分级保护制度，形成重要数据目录，提升数据处理者安全意识和防护能力，支持北京、上海、天津等自由贸易试验区探索建立合法安全便利的数据跨境流动机制。该文件还要求，守住安全底线，保障商务领域数据安全和网络安全，坚决维护国

家主权、安全、发展利益，严格落实“三管三必须”责任，防范数字商务领域安全生产风险。

九部门印发加快数字人才培育支撑数字经济发展三年行动方案

4 月 17 日，人力资源社会保障部、中共中央组织部、中央网信办、国家发展改革委、教育部、科技部、工业和信息化部、财政部、国家数据局等九部门印发《 加快数字人才培育支撑数字经济发展行动方案（ 2024—2026 年 ）》。该文件提出用 3 年左右的时间，开展多项行动增加数字人才有效供给，形成数字人才集聚效应。在数字安全人才方面，该文件提出实施数据安全等新职业工程师培育项目，举办数据安全等数字职业竞赛活动，支持各地根据需要增设数字安全等数字领域职称专业。

国际

美国政府发布第二版《国家网络安全战略实施计划》

5 月 7 日，美国政府发布第二版《 国家网络安全战略实施计划 》，提出了 100 项举措，旨在提高美国的整体数字安全和系统弹性。这些举措是根据《 2024 年美国网络安全态势报告 》研判美国在网络空间面临的挑战和机遇而制定的，包括关键基础设施风险、勒索软件、供应链利用、商业间谍软件和人工智能等。《 国家网络安全战略实施计划 》是 2023 年 3 月发布的《 国家网络安全战略 》的实施文件，第一版于 2023 年 7 月发布，其中提出的 36 项短期举措当前已完成 33 项。

美国政府发布新的国际网络空间和数字政策战略

5 月 6 日，美国国务院正式发布《 美国国际网络空间和数字政策战略：迈向创新、安全和尊重权利的数字未来 》，旨在指导国际社会参与技术外交并推动《 美国国家安全战略 》和《 美国国家网络安全战略 》。该战略重点提出名为“数字团结”的概念，即“愿意为共同目标而共同努力、站在一起、帮助合作伙伴建设能力并提供相互支持”，而该战略提出的行动和努力旨在展示并与全球合作伙伴建立“数字团结”。该战略的重点是通过未来三到五年优先考虑的三项指导原则和四个行动领域，来建立广泛的“数字团结”。

美国总统拜登签署《关于关键基础设施安全和弹性的国家安全备忘录》

4 月 30 日，美国总统拜登签署《 关于关键基础设施安全和弹性的国家安全备忘录 》（ NSM-22 ），取代奥巴马时期 2013 年发布的关键基础设施保护总统政策文件 PPD-21，保护美国基础设施免受当前和未来的所有威胁和损害。该文件提出四方面要求，一是授权国土安全部领导美国关键基础设施安全的政府方面工作，其中网络安全与基础设施安全局担任国家安全与弹性协调员；二是美国情报界应与联邦、州和地方合作伙伴及关键基础设施所有者和运营者共享情报信息；三是重申指定的 16 个关键基础设施行业和行业风险管理机构；四是提高关键基础设施行业内和行业间的最低安全与弹性要求，与国家网络战略保持一致。

五眼联盟联合发布《安全部署人工智能系统指南》

4 月 15 日，美国国家安全局人工智能安全中心、网络安全与基础设施安全局、联邦调查局与澳大利亚、加拿大、新西兰、英国政府网络安全机构联合发布《 安全部署人工智能系统指南 》。该指南旨在为部署和运行由其他实体设计和开发的人工智能系统的组织提供最佳实践，提高人工智能系统的机密性、完整性和可用性，并确保已知的人工智能系统的网络安全漏洞得到适当的缓解。该指南还提供了一些方法和控制措施，以保护、检测和应对针对人工智能系统及其相关数据和服务的恶意活动。人工智能安全近期备受关注，此前 2023 年 11 月，由英国国家网络安全中心牵头，18 国 23 家政府安全机构联合发布了《 安全人工智能系统开发指南 》。

事件篇

勒索软件疯狂肆虐，创造出史上最大的财务损失金额。美国医疗 IT 巨头联合健康集团在季度财报中披露，因子公司 Change Healthcare 2 月的勒索攻击事件，一季度初步损失超 60 亿元，全年财务总成本预计超百亿元。

因供应商被黑，欧洲银行巨头桑坦德银行所有员工和多国客户数据遭泄露

5 月 15 日 Bleeping Computer 消息，欧洲超大型银行桑坦德银行（Banco Santander SA）宣布，遭遇一起数据泄露事件，客户受到影响。事件起因是一名未经授权的人员访问了该银行某个第三方服务提供商托管的数据库。该公司发布声明称：“我们最近发现了一起未经授权访问桑坦德银行数据库的事件，该数据库由一家第三方提供商托管……经过调查，我们确认某些涉及桑坦德银行智利、西班牙和乌拉圭客户，以及公司内部的现任和部分前任员工的信息已被访问。”桑坦德银行没有透露具体受影响的数据类型，但指出交易信息及网络银行账户凭据未受影响，相关系统和运营也未受影响。桑坦德银行将直接通知受数据泄露影响的客户和员工及执法部门。

国家安全部：境外一非政府组织非法搜集窃取我国自然保护区核心敏感数据

5 月 13 日国家安全部公众号消息，国家安全部发布文章称，一所外国高校在境外非政府组织支持下，与我西南地区某国家级自然保护区科研管理单位开展所谓自然生态领域科研“项目合作”，并采取利益拉拢、色情引诱等方式将我方人员拉拢“下水”，指使、胁迫其配合非法窃取我自然保护区各类敏感数据。国家安全机关工作发现，该非政府组织背景复杂，此次实为某西方大国以开展项目合作为掩护，在未经我任何部门批准的情况下，非法搜集、窃取我自然保护区核心敏感数据资源，并通过违规在我自然保护区核心区域安装气象站、布设红外相机设备、开展 GPS 测绘、窃取我涉密计算机资料等方式，获取我重要自然保护区大量地理、气象、生物等敏感数据及图片资料并向境外传输，对我生态安全造成严重危害。

澳大利亚贷款巨头 Firstmac 遭勒索攻击，超 500G 数据泄露

5 月 12 日 Bleeping Computer 消息，澳大利亚最主要的非银行贷款机构之一 Firstmac 遭遇 Embargo 勒索软件攻击，超 500GB 内部数据被窃取。网络安全博主 Troy Hunt 在推特上公开了 Firstmac 发送给客户的通知。通知显示，Firstmac 发生了严重数据泄露事件，在外部网络安全专家的协助下，确定了泄露的信息包括客户姓名、住址、电子邮箱、电话号码、出生日期、外部银行账户信息和驾照信息等。Firstmac 向客户保证，他们的账户和资金是安全的，该公司的系统现已得到适当的支持。

戴尔泄露 4900 万用户购物数据：疑涉及大量中国用户

5 月 9 日 Bleeping Computer 消息，一位威胁行为者声称，已窃取了约 4900 万名戴尔客户的信息。随后，戴尔向客户发布了数据泄露警告，称黑客入侵了戴尔门户网站，其中包含过往购买产品的客户信息。戴尔表示，泄露数据包括姓名、收件地址、订单信息等，不涉及联络方式或支付信息。但这些仍可用作针对用户的钓鱼攻击。数据售卖者称，该数据库中用户归属最多的国家依次为美国、中国、印度等，目前尚未发现戴尔针对国内用户的响应动作。

美国主要医疗健康系统遭网络攻击，导致临床服务中断

5 月 9 日 The Record 消息，美国主要医疗卫生系统 Ascension 警告称，由于遭受网络攻击关闭部分系统，各地医院等设施可能出现临床服务中断的情况。Ascension 发布声明称，在发现网络系统异常活动后，立即聘请了 Mandiant 公司展开调查，并在不久之后通知了执法部门。该组织表示：“随着攻击事态发展，部分系统访问已中断。我们的护理团队接受过此类中断的培训，并已启动程序以确保患者护理服务安全，尽可能降低事件影响。”Ascension 敦促业务伙伴暂时中断与其技术环境的连接，等待后续通知。声明还称，该组织正在努力确认是否有数据被攻击者窃取。

伦敦证交所客户核查数据库遭泄露，内含超 520 万条敏感个人信息

4 月 26 日 Cybernews 消息，伦敦证券交易所集团旗下的客户核查数据库 World-Check 遭到泄露，自称 GhostR 的用户在知名数据泄露论坛上发帖称，在 3 月获取了该数据库，内含超 520 万条记录。World-Check 数据库可供金融机构执行“了解您的客户”（KYC）核查，其中包括有关政治公众人物、情报人员、犯罪分子、高风险组织和其他机构的记录，具体涵盖个人姓名、职务、背景信息、实体名称、列入名单原因等。伦敦证交所表示，内部系统没有漏洞，数据系攻击者从客户端非法获取。

因遭受勒索攻击，医疗诊断巨头 Synlab 在意大利全国暂停运营

4 月 22 日 Bleeping Computer 消息，国际医疗诊断和试验巨头 Synlab 的意大利分公司因遭受勒索软件攻击，被迫关闭其 IT 系统，目前所有医学诊断和试验服务均已暂停，该分公司年营收超 4 亿美元。Synlab 在声明中透露，4 月 18 日凌晨遭到安全入侵，为限制破坏活动，所有计算机不得不关闭。声明还称：“在发现入侵事件后，IT 部门立即执行了公司的安全程序，从网络中隔离了公司的所有基础设施，并关闭了所有机器。”尽管公司尚未确认，但一些敏感的医疗数据可能已经被攻击者获取。

美国知名电信运营商遭网络攻击，部分系统关停致使运营中断

4 月 18 日 Bleeping Computer 消息，美国知名电信运营商边疆通信（Frontier Communications）在 SEC 报告中披露，部分 IT 系统被不明网络犯罪团伙入侵，目前正在努力恢复系统。边疆通信表示攻击者可能访问了一些个人可识别信息（PII）。在发现攻击事件后，边疆通信被迫部分关闭一些系统，以防威胁行为者通过网络横向移动。该公司表示，系统关闭导致“相当严重的”运营中断。不过公司认为，该事件不会对公司财务状况或经营业绩产生重大影响。

史无前例！美国医疗 IT 巨头因勒索攻击初步损失超 60 亿元

4 月 16 日 The Register 消息，美国联合健康集团（UnitedHealth）在季度财报中称，为应对子公司 Change Healthcare 2 月发生的勒索软件攻击事件，2024 年第一季度付出的总成本已经达到 8.72 亿美元（约合人民币 63.13 亿元）。勒索软件攻击的影响包括 5.93 亿美元的直接网络攻击响应成本和 2.79 亿美元的业务中断成本。初步财务分析揭示了勒索攻击事件造成的巨额损失，这一数字尚未包括联合健康集团为受攻击影响的医疗服务提供商提供的预付资金和无息贷款，据称这部分金额超过 60 亿美元。该集团警告称，从财务角度看，预计 2024 年全年网络攻击造成的总成本将在 13.5 亿美元至 16 亿美元之间。

日本光学仪器巨头遭勒索攻击，被索要超 7000 万元巨额赎金

4 月 11 日 Bleeping Computer 消息，日本光学仪器巨头豪雅株式会社（Hoya Corporation）遭到 Hunters International 团伙的勒索软件攻击，该团伙要求豪雅支付 1000 万美元赎金（约合人民币 7240 万元），否则将公开在攻击期间窃取的约 1700 万份内部文件，总数据量约为 2TB。一周前，该公司公开了一起影响其生产和订单处理的网络攻击事件，表示多个业务部门的 IT 系统遭到了中断。公司当时表示正在调查黑客是否已经访问或窃取了其系统中的敏感信息，并指出确定文件是否被盗可能需要一些时间。

漏洞篇

奇安信 CERT 监测到多个国产软件的新漏洞细节在互联网公开，涉及禅道项目管理系统、kkFileView 文档在线预览组件、IP-guard 终端安全管理软件等。这些漏洞没有 CVE 编号，影响范围较大，建议客户尽快做好自查及防护。

Google Chrome Visuals 释放后重用漏洞安全风险通告

5 月 10 日，奇安信 CERT 监测到 Google 发布公告称，Google Chrome Visuals 释放后重用漏洞 (CVE-2024-4671) 存在在野利用，攻击者可通过诱导用户打开恶意链接来利用此漏洞，从而获取敏感信息或使应用程序崩溃。目前，此漏洞已检测到在野利用。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

禅道项目管理系统身份认证绕过漏洞安全风险通告

4 月 26 日，奇安信 CERT 监测到禅道项目管理系统身份认证绕过漏洞 (QVD-2024-15263) 在互联网上公开。禅道项目管理系统存在身份认证绕过漏洞，远程攻击者利用该漏洞可以绕过身份认证，调用任意 API 接口并修改管理员用户的密码，以管理员用户登录该系统，配合其他漏洞进一步利用后，可以实现完全接管服务器。奇安信 CERT 分析并复现此漏洞，鉴于该漏洞利用难度较低、影响范围较大，建议客户尽快做好自查及防护。

CrushFTP 服务器端模板注入漏洞安全风险通告

4 月 25 日，奇安信 CERT 监测到 CrushFTP 服务器端模板注入漏洞 (CVE-2024-4040) 在互联网上公开，由于 CrushFTP 存在服务器端模板注入漏洞，未经身份验证的远程攻击者可以逃避虚拟文件系统 (VFS) 沙箱，绕过身份验证获得管理访问权限，泄露敏感信息或执行代码。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。

kkFileView 远程代码执行漏洞安全风险通告

4 月 19 日，奇安信 CERT 监测到 kkFileView 发布新版本修复了 kkFileView 远程代码执行漏洞 (QVD-2024-14703)。kkFileView 的文件上传功能存在 ZIP 路径穿越问题，导致攻击者可以通过上传恶意构造的 ZIP 包覆盖任意文件，并通过调用 Libreoffice 执行任意 Python 代码。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。

IP-guard WebServer 权限绕过漏洞安全风险通告

4 月 18 日，奇安信 CERT 监测到 IP-guard WebServer 权限绕过漏洞 (QVD-2024-14103) 在互联网上公开，由于 IP-guard WebServer 的权限验证机制中存在设计缺陷，远程攻击者能够规避安全验证，通过后端接口执行文件的任意读取和删除操作。IP-guard 是由广州市溢信科技股份有限公司开发的一款终端安全管理软件。奇安信 CERT 已复现此漏洞，鉴于该漏洞影响范围较大，利用简单，建议客户尽快做好自查及防护。

注：使用公司邮箱发送企业名称和需开通订阅的邮箱地址至 cert@qianxin.com，即可申请订阅最新漏洞通告。

对抗篇

国内攻防演习 4 月态势：哪些薄弱点最易被利用？

作者 | 奇安信安服团队

一、本月演习整体情况

2024年4月，奇安信Z-TEAM团队共承接攻防演习服务 39 场，行业级攻防演习 1 场，省级行业攻防演习 1 场，客户自主攻防演习 37 场。

本月承接攻防演习数量与上月对比呈明显上升趋势（见图 1）。

本月承接的攻防演习涉及政府部委、企业、金融行业较多，此情况较上月承接攻防演习涉及行业范围数据较大，政府部委、企业、金融行业攻防演习数量明显增多（见图 2）。

本月攻防演习成果如表 1 所示。

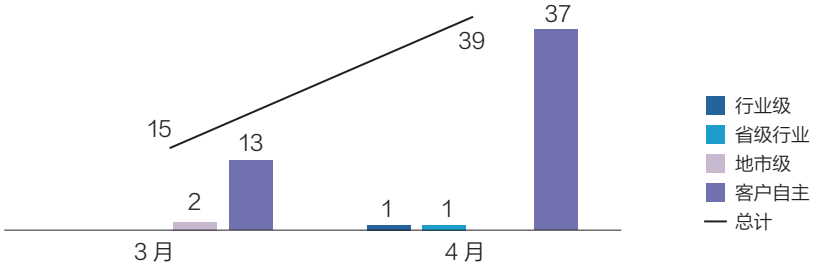


图 1 3-4 月 Z-TEAM 承接攻防演习数量统计

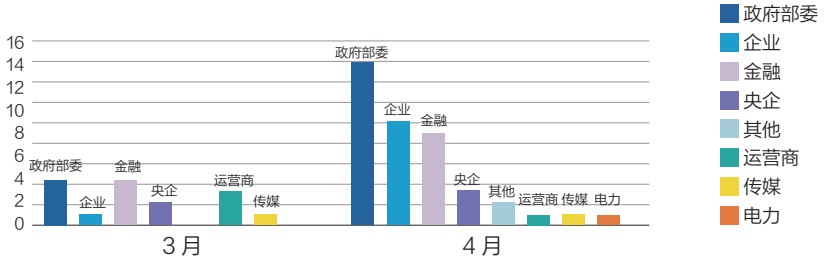


图 2 2024 年攻防演习涉及行业统计

目标系统	靶标	强隔离内网	核心业务网	网站	堡垒机	安全设备	业务系统	服务器
数量	35	39	43	63	48	61	498	10067

表 1

二、本月任务目标特点

本月攻防演习和评估任务覆盖行业比较广泛，涉及目标包括政府部委、企业、金融、央企、运营商、传媒、电力、其他等行业。随着经济全球化的发展，企业发展迅速，在国民经济中发挥着越来越重要的作用。近年来，我国企业迅猛发展，数量不断增加，业务规模不断扩大。同时由于互联网和信息技术的迅速发展，企业行业网络安全问题日益凸显。企业行业作为网络安全问题较为突出的行业之一，其网络攻击面较广、攻击手段多样、隐蔽性强，给网络安全带来了极大的挑战。因此，企业行业需要采取强有力的网络安全措施。在本月攻防演习中企业行业占比为 23%（见图 3）。

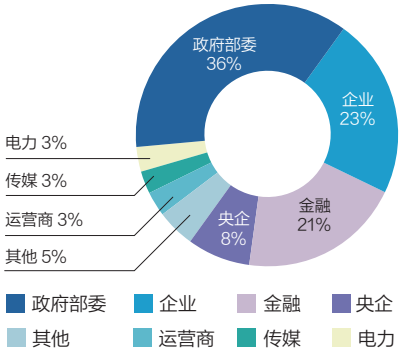


图 3 4 月攻防演习分布

三、主要攻击手段分析

基于本月奇安信 Z-TEAM 团队实战成果分析，本月任务中对多个行业的网络目标进行了攻击分析，对不同的行业目标使用不同攻击手段，如企业、传媒、其他行业外网突破的主要手段包括漏洞扫描利用和隐秘隧道外联、水坑钓鱼等；政府部委、央企、电力行业主要是漏洞扫描利用和口令爆破等；金融和运营商行业外网突破的主要手段包括漏洞利用、钓鱼攻击和 VPN 仿冒接入等。因此，我们建议各个行业加强外网安全管理，定期检测和修复漏洞，加强口令策略，增强员工安全意识，以防止攻击者利用外网攻击内网。各个行业使用的主要技术手段分布如图 4 所示。

本月攻防演习服务中，攻击队使用攻击手段主要有：漏洞扫描利用、钓鱼攻击、口令爆破、VPN 仿冒接入、隐秘隧道外联，供应链攻击技术等。

整体攻击手段与上月对比，漏洞扫描利用和口令爆破手段利用率基本趋同，VPN 仿冒接入和供应链攻击有明显下降趋势，钓鱼攻击和隐秘隧道外联有明显上升趋势（见图 5）。

本月任务中企业行业攻防演习任务占比达五分之一，通过对该行业的演习数据分析发现，外网纵向突破重点是寻找薄弱点，围绕薄弱点利用历史漏洞攻击手段实现突破；以突破点为基础进行内网横向移动，利用水坑钓鱼攻击、隐秘隧道外联等手段在内网以点带面实现横向拓展遍地开花。攻防演练中，各种攻击手段的运用往往不是孤立的，而是相互交叉配合的，一个渗透拓展步骤的成功，往往需要两种或多种手段共同配合才能成功。

四、典型攻击手段实现案例

随着计算机科学与网络技术的日新月异，企业的核心业务流程越来越离不开互联网和内部网络的支持。然而，随着技术的进步，网络安全问题也愈发突出。黑客攻击、恶意软件等威胁持续升级，给企业的信息网络系统带来了越来越大的安全风险。因此，确保企业信息网络系统的安全性已成

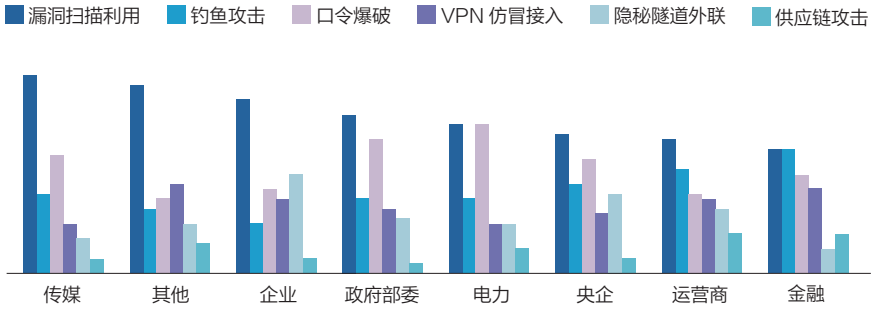


图 4 行业攻击手段分布

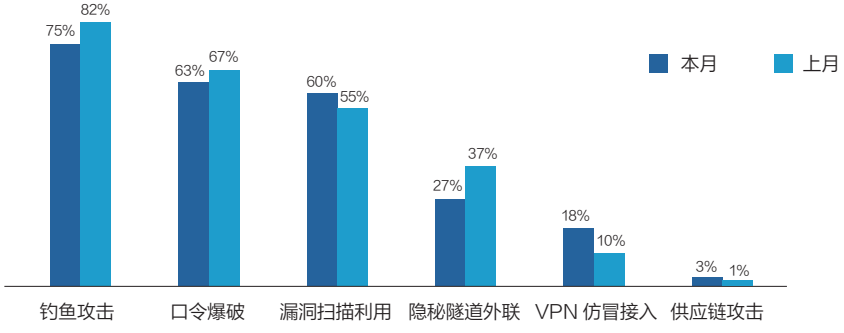


图 5 攻击手段对比

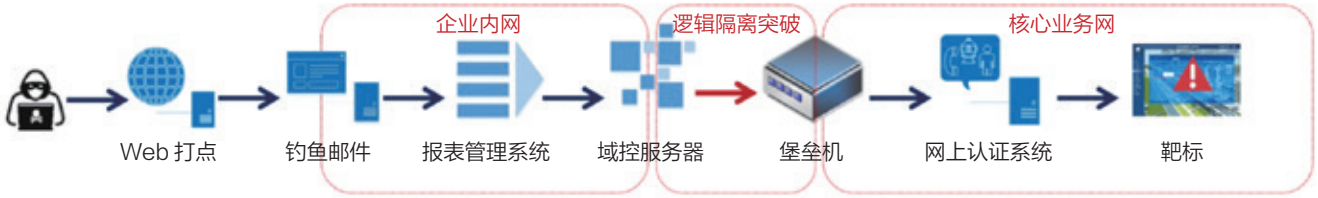


图 6 案例攻击路线图

为推动企业信息化健康、稳定发展的不可或缺的一环。

案例：曲折的靶标进军之路

在进行某企业攻防演练中，奇安信攻击队经过前期的信息收集，成功获取了目标单位大量员工的邮件信息。基于这一情况，攻击队决定采用社工手段，尝试对目标网络进行渗透。

针对目标企业员工，攻击团队通过模拟与招投标相关的电子邮件，实施了精准的钓鱼攻击，并成功获得了两名员工的终端访问权限。以这两名员工的终端作为跳板，攻击队探测到企业内部网络中存在一个报表管理系统。随后，攻击队利用该系统存在的反序列化漏洞，成功获取了服务器的管理权限和数据库的访问权限。

攻击队在内网环境持续开展信息收集工作。他们通过渗透报表管理系统的数据库，成功获取了部分敏感信息及密码。利用内网域探测技术，攻击队确定了域控制服务器的地址，并利用已知的域管理员密码，获得域控权限。通过域控，攻击队能够定位到用户哈希值，进而解密得到用户密码，从而获取统一登录平台的访问权限。通过这一平台，攻击者能够轻松跳转至其他所有业务系统，并结合域控的哈希值，全面窃取全集团用户的系统权限。

通过统一登录平台，攻击队发现重要目标——堡垒机系统。经过攻击队确认，该堡垒机存在攻击队掌握的 0day 漏洞，攻击队利用 0day 漏洞和内存马技术，成功植入 WebShell 内存马。利用该堡垒机的访问权限及后台 Admin 账号权限，实现了大量服务器的访问权限控制。经过对众多服务器的细致排查，我们并未发现靶标系统的存在。攻击队利用堡垒机作为中介，尝试寻找靶标系统。经过不懈努力，他们发现借助堡垒机可以访问即使上网认证系统通过认证也无法触及的隔离网段，其中发现 21 台关键网络设备，包括防火墙和交换机等重要网络设备。

在隔离网段，通过堡垒机可以直接访问私有云核心业务系统，并获得管理权限。在私有云环境中，攻击队发现了本次演习的靶标系统。然而，他们发现无法通过堡垒机直接访问该目标系统。为确保不引发生产故障，攻击队及时向客户提交了申请。经过靶标容器的重新挂载，攻击队最终成功地获得了该靶机目标系统的权限。

利用堡垒机系统，攻击队可以直接访问该集团的档案管理系统。在档案管理系统中，他们成功获取了超过 62 万份敏感档案文件，其中包括企业战略合作文件等关键信息。

攻击队通过邮件系统实施信息收集，收集到密码表，从密码表获取数据备份服务器的密码，该备份服务器存有大量生产业务系统的备份数据。

五、安全加固建议

1. 案例剖析

近年来，我国企业迅猛发展，数量不断增加，业务规模不断扩大。同时，由于互联网和信息技术的迅速发展，企业行业网络安全问题日益凸显。企业行业作为网络安全问题较为突出的行业之一，其网络攻击面较广、攻击手段多样、隐蔽性强，给网络安全带来了极大的挑战。

本次攻防演习采用了多种攻击手段和技术，包括钓鱼攻击、反序列化漏洞利用、内网渗透、域控制权限获取、0day 漏洞利用、WebShell 植入、网络设备访问和敏感信息的窃取等。以下是攻防演习关键点。

（1）信息收集阶段

邮件信息获取：攻击者通过前期的信息收集，获取了目标单位员工的邮件信息，这通常涉及社会工程学技巧，如钓鱼邮件、社交网络分析等。

（2）初始渗透阶段

钓鱼攻击：利用获取的邮件信息，攻击者模拟招投标相关的电子邮件，实施精准钓鱼攻击，这是利用人性弱点和社会工程学的一种手段。

权限获取：成功获得两名员工的终端访问权限，为后续的内网渗透打下基础。

（3）内网探测与权限提升

报表管理系统漏洞利用：攻击者

发现并利用报表管理系统的反序列化漏洞，获取服务器的管理权限。

数据库访问：通过渗透数据库，攻击者获取了敏感信息及密码。

(4) 域控制权限获取

域控制服务器定位：利用内网域探测技术确定域控制服务器的地址。

域管理员密码获取：使用已知的域管理员密码，攻击者获得域控权限。

(5) 用户权限扩展

用户哈希值解密：攻击者定位到用户哈希值，并解密得到用户密码。

统一登录平台访问：利用解密的密码，攻击者获得统一登录平台的访问权限。

(6) 业务系统控制

业务系统跳转：通过统一登录平台，攻击者能够访问所有业务系统。

(7) 0day 漏洞利用与 WebShell 植入

堡垒机系统发现：攻击者发现并确认堡垒机系统存在 0day 漏洞。

WebShell 植入：利用 0day 漏洞和内存马技术，攻击者植入 WebShell，获得服务器的控制权。

(8) 网络设备访问与隔离网段探测

关键网络设备访问：通过堡垒机访问隔离网段中的关键网络设备。

私有云核心业务系统管理：在私有云环境中，攻击者获得管理权限。

(9) 靶标系统发现与权限获取

靶标系统定位：攻击者在私有云中发现靶标系统。

权限申请与获取：为避免生产故障，攻击者向客户提交申请，成功获得靶标系统的权限。

(10)敏感信息窃取

档案管理系统访问：攻击者利用堡垒机系统访问档案管理系统。

敏感档案文件获取：成功窃取超过 62 万份敏感档案文件。

(11) 数据备份服务器密码获取

密码表收集：通过邮件系统收集到密码表。

备份服务器密码获取：从密码表中获取数据备份服务器的密码，访问备份数据。

2、防护策略

针对上述攻击，以下是针对性的防护策略和建议。

(1) 钓鱼攻击防护

安全意识教育：定期对员工进行安全意识培训，提升钓鱼邮件识别能力。

邮件过滤：使用邮件安全系统，如垃圾邮件过滤器和钓鱼邮件识别工具。

双因素认证：为所有账户启用双因素认证，增加账户安全性。

(2) 系统漏洞防护

定期更新：确保所有系统和应用程序都及时打上安全补丁。

漏洞扫描：定期进行系统漏洞扫描，及时发现并修复潜在的安全漏洞。

(3) 权限和访问控制

最小权限原则：仅授予员工完成工作所必需的权限。

访问控制列表：使用访问控制列表（ACLs）来限制对敏感系统的访问。

(4) 网络隔离和分段

网络分段：将网络分割成多个区域，以减少潜在的攻击面。

隔离关键系统：将关键系统和数据与普通网络隔离，以减少潜在的损害。

(5) 密码和身份管理

强密码策略：强制使用强密码，并定期更换。

密码管理器：鼓励员工使用密码管理器，以生成和存储复杂的密码。

(6) 域安全

域控制器加固：确保域控制服务器安全，因为它们是核心集权类设备。

域密码策略：实施强大的域密码策略，包括密码复杂性、长度和更换周期。

(7) 监控和日志记录

日志管理：确保所有关键系统和网络设备都有日志记录，并定期审查。

入侵检测系统：部署天眼、天堤等设备，进行日志和流量监控。

(8) 安全审计和渗透测试

定期审计：定期进行安全审计，检查安全措施的有效性。

渗透测试：定期进行渗透测试，模拟攻击者的行为，以发现和修复潜在的安全问题。

(9) 应急响应计划

应急响应团队：建立一个应急响应团队，以快速响应安全事件。

事件响应计划：制定和演练事件响应计划，确保在发生安全事件时能够迅速采取行动。

(10)数据备份和恢复

定期备份：定期备份关键数据，并确保备份数据的安全性。

恢复计划：制定数据恢复计划，以便在数据丢失或损坏时能够迅速恢复。

通过实施这些措施，企业可以显著提高其网络安全防护能力，减少潜在的安全风险。安

协作、AI 与整合

——来自 RSAC 2024 的一线报道

RSAC 2024 的主题是“可能的艺术”， 反映出网络安全届对技术创新、AI 风险和社区协作的关注。“通过拥抱激发动力和想象力的社区力量，通过协作体验推动网络安全的卓越发展，让不可能变得更加可能”。

面对 GenAI 给网络安全产业带来的变革性作用，网络安全企业都努力贴上了 AI 的标签。安全专家预测，人工智能将会长期改变安全行业。“从现在起五年后，所有的攻击都将是人工智能对人工智能的攻击，因为人类无法以同样的速度进行防御。

RSAC 2024 另一个主要话题是，整合和简化安全工具。集成的趋势在整个行业中正逐步得到落实。没有任何一家供应商能够提供有效防御不断变化威胁的所有功能。转向集成解决方案、提供最佳的客户价值成为很多安全企业的选择。

RSAC 2024 解读：AI、协作与平台化集成

本文撰稿 尹智清、邬怡、周奕、李建平

5 月 10 日，RSAC 2024 会议在旧金山落下帷幕。这一吸引全球 4 万多专业人士的行业会议，透露出安全行业的下一代趋势与变化。人工智能无容置疑是今年大会的最热门话题，包括 AI 重塑网络安全，以及 AI 相关的隐私与数据安全挑战。此外，社区协作、平台化集成也是本届大会的重要议题。美国国务卿首次现身 RSAC 2024，凸显出在全球各地陷入地缘政治冲突之际，网络安全在国家安全中的日益重要作用。

可能的艺术

RSAC 2024 的主题是“可能的艺术”，反映出网络安全届对技术创新、AI 风险和社区协作的关注。RSAC 2024 执行主席 Hugh Thompson 在演讲中表示，网络安全界的合作——这种“通过社区解决问题”的方法对于应对不断变化的威胁至关重要。他强调，当网络安全届作为一个行业共同努力时，可以做的比想象的更多。“通过拥抱激发动力和想象力的社区力量，通过协作体验推动网络安全的卓越发展，让不可能变得更加可能。”

“可能的艺术”这一主题显然一方面是为了激发业界的希望，同时也是一个警告，“我们永远不应该低估对手的潜力”。

美国国务卿布林肯首次在 RSAC 2024 发表演讲，并公布了美国的《国际网络空间和数字政策战略》。他强调这一新战略的核心是“数字团结”——与志同道合的国家合作，向恶意网络活动和其他数字威胁的受害者提供互助，并遏制意识形态上对立国家的影响。

这一新战略强调与国际合作伙伴在技术治理方面保持一致，与民间和

私营部门建立强有力的伙伴关系，并通过值得信赖的技术供应商提供的多样化产品和服务来提高网络安全弹性。

从社区协作，到政府部门与民间、私营机构建立伙伴关系，这种集体防御已经在加强关键行业的网络防御方面发挥着关键作用。作为一种网络安全协作方法，集体防御将多个组织聚集在一起，汇集各自的资源和专业知识，以改善集体的安全态势。

集体防御不仅在政府机构中具有重要意义，而且在寻求增强网络安全的私营组织中也具有重要意义。许多私营机构认识到协作和信息共享在有效应对网络威胁方面的力量。例如，网络威胁联盟 (CTA) 将网络安全公司聚集在一起，共享情报、协作进行威胁分析并针对新兴网络威胁制定主动防御措施。另一个例子是金融服务信息共享和分析中心（FS-ISAC），促进金融机构之间的信息共享和协作，以防范针对金融部门的网络威胁。

谷歌云 Mandiant 首席执行官凯文·曼迪亚（Kevin Mandia）

AI 重新定义网络安全

在会议召开前，RSAC 2024 执行主席休·汤普森 (Hugh Thompson) 撰文披露了大会的三个热点：人工智能、信息操纵和 CISO 职业倦怠。这三个热点要么与人工智能相关，要么需要人工智能解决。

展会中的网络安全企业都努力贴上了 AI 的标签，要么宣称产品与方案是 AI 赋能（Powered），要么是 AI 使能（Enabled），总之背后都是 AI 驱动。参会的首席信息安全官则渴望了解如何利用人工智能来快速准确发现和处置威胁，消除因人员不足、能力不足和工具不利导致的职业倦怠。

在 RSAC 2024 期间，云安全联盟（CSA）举办了持续一天的 AI 峰会，全面讨论如何利用 AI 保护云安全，以及应对 AI 相关的风险问题。谷歌云 Mandiant 首席执行官凯文·曼迪亚（Kevin Mandia）在围炉对话中强调，人工智能将会长期改变安全行业。他在有关“塑造人工智能和网络安全政策”的讨论中预测，“从现在起五年后，所有的攻击都将是人工智能对人工智能的攻击，因为人类无法以同样的速度进行防御。”网络安全公司 Exabeam 的首席产品官史蒂夫·威尔逊 (Steve Wilson) 则表示：“没有采用这些机器学习技术的竞争对手已经落后了。”

这或许才是网络安全从业者急于踏上人工智能快车的原因：在日趋激烈的攻防对抗中，生成式人工智能正在彻底改变网络安全。不积极采用人工智能的企业，无疑会在跟攻击者的对抗中全面落后。

思科执行副总裁兼安全与协作部总经理 Jeetu Patel 在《时机已到：

思科执行副总裁兼安全与协作部总经理 Jeetu Patel

重新定义人工智能时代的安全》主题演讲中表示，攻击的速度和复杂性正在上升，而人工智能正在释放两年前不可能实现的安全能力。现在是时候利用人工智能而不仅仅是炒作，并重新思考网络安全。

根据 Gartner 的预测，到 2028 年，生成式人工智能 (GenAI) 的采用将极大地影响网络安全，通过消除 50% 的入门级网络安全职位，从而缩小专业技能的差距。

从理解复杂的指令，到生成代码，再到解决复杂的问题，大型语言模型（LLM）展现出非凡的能力，正在迅速改变包括网络安全在内的许多领域。谷歌 & DeepMind AI 安全技术和研究主管埃利 · 布尔斯坦博士（Elie Bursztein ）分享了大型语言模型如何重塑网络安全格局的观点。他强调，现在的大模型在检测多模态恶意软件、保护代码安全、提高安全响应速度等方面展示出强大的能力。

正是由于看到 AI 改变网络安全巨大潜力，RSAC 2024 上展示的半数以上的产品都加持了 AI 技术，从代码检测、数据分级分类、威胁检测、行为分析等检测技术到威胁告警分析研判和自动化处置都体现了AI+的融入。以 SIEM 产品为例，Elastic 演示了可以集成任何第三方的威胁分析大模型，一次最多可以分析 100 个告警。CrowdStrike 则提出了新一代 SOC 是 AI 内生的 SOC，包括通过 AI 第三方介入、AI 正则化、AI 数据丰富、AI 流程自动化，以及建立自己的大大语言模型(LLM)用于提升安全运行效率。

在RSAC 2024创新沙盒比赛中，生成 AI 驱动安全运营自动化的初创企业 Dropzone AI 成功跻身 10 强。根据公开信息，通过将自主 AI 分析师无缝集成到安全工作流程中，Dropzone AI 将会改变安全运营的方式，能在不增加人员的情况下，以 10 倍以上效率开展运营。Dropzone AI 虽与冠军擦肩而过，但其通过部署预先训练的自主 AI 分析师来提升安全运营效率的思路，受到业界认可。该公司在 A 轮融资中筹集了 1685 万美元。

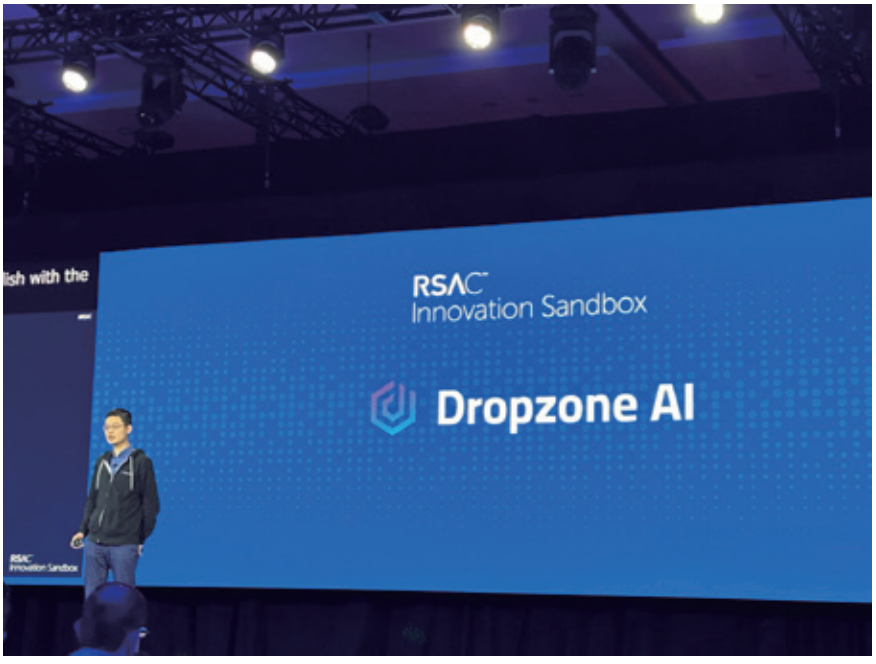
Dropzone AI 的模式与国内网络安全领军企业奇安信利用安全机器人大幅提升运营效率的思路不谋而合。根据公开的数据，QAX-GPT 安全机器人的告警研判效率达到人工研判的 60 多倍，研判误报率是人的接近一半。安全事件平均调查响应时间则从原来小时级缩短至分钟级，单一威胁事件

处理时间减少 98%。

由 McAfee 企业安全及 FireEye 合并而成的 Trellix 公司，则在 RSAC 2024 期间宣布推出人工智能和 GenAI 支持的新套件 Trellix Wise，可以跨 Trellix XDR 平台进行扩展，更有效地发现和消除威胁，同时降低安全运营成本。其关键功能包括工作流程自动化、分析师效率的提升及威胁的预防、检测、应对和调查。

网安龙头企业 Palo Alto Networks 没有参加 RSAC 2024，但在总部举行了小型会议，重点介绍其新人工智能产品 Precision AI。首席执行官 Nikesh Arora 表示，“对抗人工智能的唯一方法就是使用人工智能。”利用 Precision AI 这一技术，将机器学习 (ML) 和深度学习 (DL) 的优点，与生成人工智能 (GenAI) 实时结合，可以为用户提供人工智能驱动的安全防护，从而超越对手、主动地保护网络和基础设施。

面对 AI 的巨大潜力，人们很容易会设想 AI 取代人类安全分析师，实现安全运营自动化的场景，但事实可能并非如此。AI 将大幅提升安全运营的效率，但却不会完全取代安全专家；人工智能不会成为所有安全问题的解决方案，而是让安全解决方案更加高效、让安全投资价值最大化的重要工具。



Dropzone AI 创始人兼 CEOEdward Wu 在创新沙盒上

从 AI 武器化，到信息操纵和模型安全

安全从业者致力于实现 AI 赋能安全的未来，但用户同样关注 AI 武器化的风险：攻击者利用 AI 创建新恶意软件或网络钓鱼，从而绕开现有安全堆栈和工具。此外，AI 大规模部署带来的隐私和数据安全挑战，以及生成式 AI 引发的信息操纵风险，也是参与者关注和讨论的热点问题。国土安全部部长亚历杭德罗·马约卡斯 (Alejandro Mayorkas) 强调，应对人工智能的影响已成为当务之急。为了确保在监管和创新之间取得适当的平衡，网络安全社区显然需要合作塑造人工智能的未来。美国国土安全部人工智能安全咨询委员会将在 RSAC 2024 会议同一周召开首次会议，该委员会成员包括 OpenAI、微软、Alphabet 和英伟达的首席执行官。

Trace3 的创新负责人贾斯汀·哈钦斯 (Justin Hutchens) 证实，对人工智能崛起的很多担忧（尽管不是全部）是有道理的。在研究中，他发现 ChatGPT 4.0 能够自主实施渗透测试，其成功达到了“可怕”的程度。随着国家间人工智能军备竞赛的快速发展，人工智能超越控制只是时间问题，而不是是否突破的问题。哈钦斯警告说，网络安全行业需要立即采取行动并进行创新，以便为未来做好充分的防御。

谷歌云 Mandiant 首席执行官凯

文 · 曼迪亚（Kevin Mandia）主持的“塑造人工智能和网络安全政策”的讨论中，参与讨论人员一致认为，目前影响世界各地选举的信息操纵、误导和错误信息问题令人严重关切。随着深度伪造技术的日益成熟，攻击者可以生成名人、政治家和有影响人士的高度写实视频和音频形象，从而可以制造欺骗和混乱。

由深度伪造技术引发的信息战已经成为国际冲突的一部分。俄乌冲突与以哈冲突期间均出现利用深度伪造技术，生成冲突双方政治领导人的虚假视频，意图制造社会混乱，凸显出对 AI 生成内容及时、有效地检测的重要性。

从社会角度来看，网络安全专家担心即将到来的美国总统大选将催生一波深度造假浪潮，以左右美国的舆论。或者正是由于美国社会对虚假信息的忧虑，安全初创企业 Reality Defender 赢得创新沙盒冠军，该公司的 Deepfake 检测平台可以实时识别检测欺诈性音频、视频、图像和文本。Capitol Meridian Partners 运营合伙人、创新沙盒竞赛评委之一 Niloofar Razi Howe 表示，利用人工智能实施的深度伪造（Deepfake）可能是“我们面临的最重要的问题之一。

人工智能工具具有巨大的优势，但安全和隐私是组织犹豫部署人工智能工具的主要原因。令人担忧的是可能通过大型语言模型暴露敏感数据，尤其是在缺乏强大的数据治理和访问控制措施的情况下。考虑实施人工智能的公司需要优先考虑这些方面的风险，以确保其数据安全。2024 创新沙盒中，多家致力于大模型数据安全防护的创新企业跻身 10 强，凸显出业界对大模型训练、使用时的数据安全风险忧虑。

AI 系统安全也是本届 RSAC 的重点议题，安全专家从安全框架、产品方案和红队实践三个角度探讨 AI 系统安全防护。

AI 系统的安全框架方面，各主要框架研究组织都公布了自己的进展。OWASP 发布了改版的 AI 安全网站。未来，OWASP 将从 AI 风险优先级排序、与其他框架的互联互通、增强数据验证和质量控制、框架的可落地性等方面推动 AI 安全框架发展。

在产品方案层面，建制派平台安全厂商、模型开发厂商、AI 安全初创公司等三类厂商根据其在 AI 安全生态中的定位和愿景，构建了自己的策略和产品能力：（1）建制派平台安全厂商，以微软为例，整合现有的安全运营、身份安全和数据安全产品，覆盖

> 随着国家间人工智能军备竞赛的快速发展，
> 人工智能超越控制只是时间问题。
> 网络安全行业需要立即采取行动并进行创新，
> 以便为未来做好充分的防御。

AI 系统全生命周期的关键步骤，提供全面的威胁监控、防护及事件响应。（2）模型开发厂商：微软在 Azure AI Studio 增加了安全验证功能，提供安全测试数据集以验证模型的鲁棒性，并打通开发和运行过程，使客户能够将使用外部大模型时的高风险行为反馈给研发团队，帮助优化模型开发。（3）AI 安全初创公司，以 Protect.AI 为例，推出了完整的 AI 系统安全解决方案，包括模型访问控制（Guardian）、AI 供应链脆弱性数据库（SightLine）及端到端大模型威胁与可见性监控（Layer）。

在 AI 系统的红队实践方面，有关关注范围的争议较大。部分专家认为，应集中在传统安全场景及 LLM 应用安全场景，如提示注入、越狱攻击等。而另一部分专家则认为，未来应更多关注模型应用质量问题，因此 AI 红队测试将更多采用白盒测试，深入 DataOps、ModelOps 和 DevOps 全流程，对关键步骤进行审计和评估。

更高的平台化集成

RSAC 2024另一个主要话题是，整合和简化安全工具，其重点是改善告警并确定实际风险的优先级。工具复杂性是网络安全中持续存在的问题。更多的工具增加了复杂性、增加了成本，给客户带来管理的挑战。RSAC 2024 期间，笔者采访洛杉矶市 CISO Timothy Lee 时，Timothy 重点提到了快速、准确、自动化的检测和处置网络安全威胁，以及让安全产品和工具发挥更大作用等两大挑战。这都与安全工具的蔓延不无关系。

现在网络安全供应商更加重视与其他供应商产品的有效集成，以满足客户的需求，这也反映出整个行业发生了显着的变化——网络安全厂商更加关注响应客户对统一平台的需求，希望安全产品能很好地协同工作。工具疲劳和客户对安全产品合理化的需求“确实进一步推动了集成的趋势”，这一趋势在整个行业中正逐步得到落实。

有安全专家认为，这代表我们进入网络安全的第三个时代：人们越来越认识到，没有任何一家供应商能够提供有效防御不断变化威胁的所有功能。因此，开始转向集成解决方案——将多个供应商的产品和服务结合到同一安全架构中，目的是为了提供最佳的客户价值（相对于孤立安全工具与单一安全平台的时代）。

云安全初创公司 Netskope 的首席执行官桑杰·贝里 (Sanjay Beri) 表示，越来越多的供应商发现，通过与业内其他公司紧密集成，满足用户将工具整合到统一平台的需求。即使是业内提供几乎所有类别安全能力的供应商——微软，现在也比过去“更愿意集成”。

市场上五花八门的网络安全产品，是否能够很容易的组合在一起发挥 1+1>2 的作用？RSAC 2024 上，大多数厂商都展示了其平台型产品，所谓平台型产品就是能够把不同的单点的产品通过数据 / 控制的打通发挥产品组合的作用，这包括软件供应链安全平台、开发安全平台、资产暴露面管理平台、数据安全态势管理平台等，当然也包括 XDR、SIEM、KMS 等。

抛开这些平台功能不谈，还有一个更重要是这些平台之间及与单点产品之间有比较好的协作性，每个平台型的产品都预制了大量的适配器以快速集成第三方产品，这些适配器同时也在持续增加和更新。另外，这些平台的引擎及规则也会根据攻击手法的不断演进而持续更新迭代。

以 JupiterOne 的 CAASM 平台为例，它内置了超过 200 个资产采集的适配器，以帮助用户能够更加快速全面的采集资产相关数据。在本次 RSAC 2024 大会上，Splunk 介绍了自己的检测工程蓝图，其威胁分析团队从 TTP 分析、建立模拟数据集、建立 / 优化检测模型、测试验证、发布检测模型，从而使得用户能够快速检测到最新的攻击手法。

CrowdStrike 的 Falcon Next-Gen SIEM 全面推出后，与 Netskope、Zscaler、Proofpoint、ExtraHop、Trellix 和 Palo Alto Networks 等数十家供应商进行了集成。在本次大会上，CrowdStrike 宣布与 Google Cloud 扩大战略合作伙伴关系，利用 CrowdStrike Falcon 平台和 Google Cloud 安全运营平台为 Mandiant 的事件响应 (IR) 和托管检测和响应 (MDR) 服务提供支持。

专家认为，安全专业人员未来可以期待看到更多的集成，以及 AI 带来更高自动化。这一迟来的发展是对网络安全领域融合大趋势的的回应：客户和合作伙伴在安全工具蔓延和复杂性方面苦苦挣扎，自身却缺乏管理工具所需的人才，以及各方提升安全的迫切需求。

RSAC 2024 观察：SIEM/SOC 架构迎来变革

作者 叶蓬

2023 年 RSAC 大会的情景依然历历在目。彼时，由于在会前 3 个月时 ChatGPT 横空出世，各大安全厂商纷纷撤回修改自己的发言稿，并把主题与 ChatGPT、LLM 挂上钩。结果，在 2023 年的 RSAC 上，以 ChatGPT 为代表的 AI 成为了大会的最大亮点。但除了 ChatGPT 背后的微软在会上大放异彩，其他厂商的 AI 主题大都停留在 PPT 层面。毕竟那时候大家都没啥积累，更多都是对 GenAI 变革网络安全领域的憧憬，以及对 GenAI 自身安全的担忧。

在意识到 GenAI 给网络安全产业带来的变革性作用后，安全厂商纷纷大举投入。到了 2024 年的 RSAC，厂商们显然有备而来，让 GenAI 在网络安全产业的应用更加掷地有声。毫无疑问，AI（尤其是 GenAI）依然占据了本届 RSAC 的 C 位。在笔者收集的 282 个大会胶片中，仅标题带有 AI 的就有 33 个。

RSAC 大会执行主席 Hugh Thompson 在主旨演讲中表示，综合 2024 年 RSAC 所有议题，所展示出的三大趋势关键词分别是：职业倦怠（Burnout）、人工智能（AI）和风险管理（Risk Management）。细细想来，都在情理之中。简单理解，正是网络安全领域的职业倦怠促成了人们对 AI 的期待，而风险管理则是安全永恒的旋律。在笔者看来，这里的职业倦怠既包括甲方追赶不断演进的威胁形势时的力不从心和对现有技术能力的不满，也包括乙方（厂商、服务商）遭遇现有技术难以突破常态化安全防御的困境并最终归为客户堆人头的无奈。AI，在当下成为了大家克服职业倦怠的救命稻草，但它真的是灵丹妙药吗？我们已经举起过太多的圣杯。

AI 重新定义安全

来自 Cisco 安全的两位副总裁

（Jeetu Patel 和 Tom Gillis）继去年带领大家畅想了 AI 加持下的 SOC 后，今年又为大家进一步打开脑洞，畅想了一番 AI 将如何重新定义安全。

Jeetu Patel 表示，当前颠覆安全的三个关键技术分别是 AI、内核级可见性及硬件加速。AI 原生技术，基于 eBPF 获得内核的可见性技术，以及支撑算力和应用加速的硬件（DPU、GPU）技术将从根本上改变现有的安全系统架构和运行方式。他说，“这不是某个产品的新版本，这是一个全新产品的第一个版本，是前所未有的架构。”

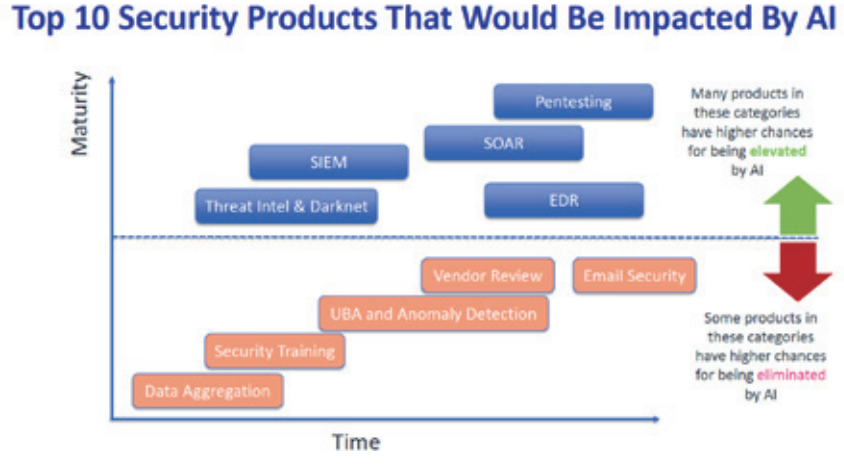
他通过 AI 驱动下的自动网络访问控制、自动网络漏洞补偿控制和自动应用升级三个典型场景为我们呈现了一幅笔者称之为 AI 自适应（Adaptive）安全的美好图景。

所谓 AI 自适应安全，是指 AI 加持下的自动闭环的自适应安全，在 AI 的驱动下和人类的参与下，预测、防护、检测和响应（或者称为 OODA）自动闭环的过程，与 CrowdStrike 提出的自适应安全姿态同义，对应微软提出的 GenAI 在安全领域应用进程预测的第三阶段（自适应推理与保护）。

而这个 AI 自适应安全也跟 Splunk 提出的完全主动自动化具有类似的含义。

让我们把视线从宏大叙事拉回到现实。在大会上有个议题评估了可能最受 GenAI 影响的 10 个安全产品，并将其分为了两类。

可以看到，安全运行基本都获益于 GenAI。



SIEM/SOC 架构迎来变革

以 EDR 起家的 CrowdStrike 公司首席执行官 George Kurtz 在大会上为大家带来了所谓下一代 SIEM 的理念。在题为《Next-Gen SIEM: Converging Data, Security, IT, Workflow Automation & AI》的演讲中，George Kurtz 开宗明义地指出，“安全是一个数据问题，现有的 SIEM 无法满足 SOC 的需求。”他表示，现有的 SIEM 面临数据悖论，一方面需要更多的安全数据，另一方面又无法及时有效地处理这些海量安全数据，导致在安全防御中无法跟上对手的节奏，无法阻止失陷。

对此，George Kurtz 提出了 CrowdStrike 的下一代 SIEM 理念，其中包括五个核心观点。

其一，下一代 SIEM 可以原生地集成到你的安全平台中，意即 SIEM 不要创建新的安全孤岛和烟囱，要跟其他安全防御设施有机融合。

其二，数据摄取与 AI 自动化是下一代 SIEM 的架构基础。George Kurtz 表示，根据他们的调研，EDR 日志是 SIEM 的核心日志源，甚至有的 SIEM 用户 EDR 日志占比高达 85%。因此，端点日志是其下一代 SIEM 新架构的构建起点。基于这个判断，CrowdStrike 为大家呈现了其下一代 SIEM 的数据摄取与分析的层次模型，如下图所示。

这个模型以自身产品家族的端点和云数据为核心，辅以第三方数据摄取，借助 AI 驱动的数据范式化和数据富化，为 SIEM 提供一个坚实的数据基础，然后在 AI 驱动的工作流自动化作用下实现自动地的威胁监测与响应。最后，上述所有功能中用到的大模型（LLM）既可以是 CrowdStrike 原装的，也可以是用户自己的，可以自由切换。

其三，下一代 SIEM 能够实现自动化的日志管理，包括日志产生、日志摄取、日志存储、日志检索、日志数据管理等。

其四，下一代 SIEM 将不再需要对数据成本妥协。就像现在再没有人会对手机通话时长或者流量焦虑一样，未来的 SIEM 数据扩张成本将在基础设施建设到一定规模后趋向于零。

其五，下一代 SIEM 将实现 AI 驱动的合规报告自动生成。CrowdStrike 认为这是很关键的一点。因为，现在人们耗费了大量时间将实证的安全数据映射到各种合规性安全框架中（如 CSF、FISMA、PCI DSS，抑或是我们熟悉的等保）。在 AI 的加持下，这些报告将可以自动生成。

George Kurtz 进一步提出，如果上述下一代 SIEM 实现，将成为 AI 原生 SOC 的操作系统，为所谓的 AI 原生 SOC【笔者注：XX 原生已经成为当下最时髦的修饰词之一】提供一个基础的编排层。

那么，Crowd Strike 眼中的 AI 原生 SOC 应该具备什么能力？George Kurtz 为我们描绘了五大能力。

第一，自动化威胁检测与响应。的确，都 AI 驱动了，再不实现自动化实在说不过去。

第二，安全预测。Predictive Security 又是当下的一个热词。毕竟，都高级 AI（尤指 GenAI）驱动了，仅做事中检测事后响应也太屈才了，总应该可以事前性预测攻击路径、预测漏洞啥的吧。

第三，工作流程自动化。理解 SOAR 的读者对此自然不会陌生。

第四，富含上下文的安全智能。没错，上下文（Context），或者情境信息十分关键，要实现安全智能，丰富的上下文必不可少。记得有一篇文章，题目为《网络安全的未来是上下文》。

第五，自适应安全姿态（Adaptive Security Posture）。在 LLM 加持下，AI 应能够在用户实际环境中自学习，自我强化，自我提升，不断适应新的威胁变化和业务变化。

最后，George Kurtz 给出了一幅下一代 SIEM 的要素关系图，如下所示，包括：人、工作流自动化、数据和人工智能。

纵览整个演讲，应该说，笔者完全认同 SIEM 到了重构的时候，也

认同 AI 加持及更基础的数据架构是整个重构的关键所在。但有趣的是，CrowdStrike 终归是 SIEM 领域的新军，其日志管理技术最早源于 2021 年对 Humio 的收购。Humio 的日志管理技术在整合到 Crowd Strike 后叫作 Falcon LogScale。而下一代 SIEM 则是 Falcon LogScale 的最新版本和最新称呼。在 Gartner 最新发布的 2024 年 SIEM 魔力象限中，CrowdStrike 未能上榜，理由是 Gartner 认为 Falcon LogScale 还是不够开放，更适合作为 CrowdStrike 家族产品和技术的扩展。当然，Gartner 这份报告调研截至时间是 2023 年 3 月，迄今一年多时间里，不排除 CrowdStrike 的下一代 SIEM 有新的变化。

作为 SIEM/SOC 领域的领导者之一，Splunk 也毫不留情的对自己的现金牛产品进行革新。在题为《Revolutionizing the SOC for the Future Threat Landscape》的主旨演讲中，Splunk 的执行副总裁、总经理 Gary Steele 为我们呈现了在跟 Cisco 兵合一处后对未来 SOC 建设的新思考。

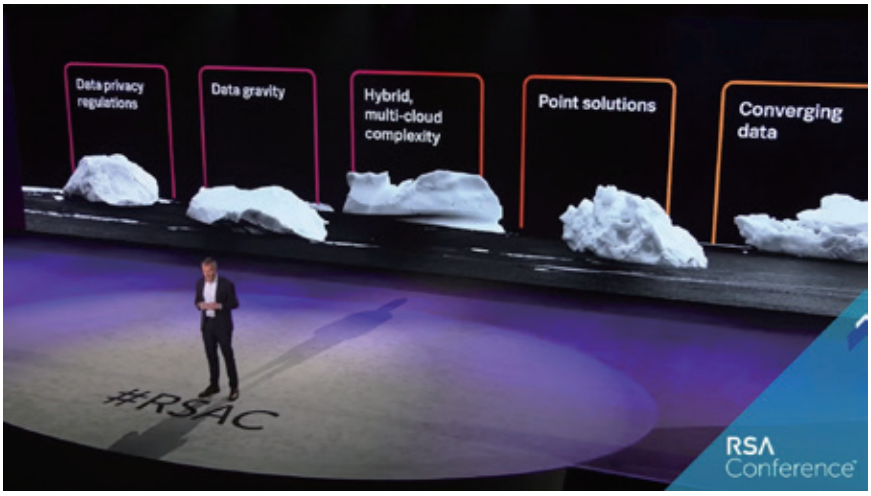
Gary Steele 表示，SOC 成功的首要能力是“看见”，而要“看见”就需要大量的数据，因此，“安全是一个数据问题”【笔者注：跟 CrowdStrike 可谓不约而同】。

接着，Gary Steele 对这个数据

问题发出了灵魂拷问：你有正确的数据吗？你能检测到威胁吗？你的数据管理有效吗？

放到以前，这些问题似乎都已经解决，但在当下的复杂威胁形势和防御体系下，面对大规模资产的、海量数据条件下的安全运行却面临重大挑战。也就是所谓 SecOps at Scale 的问题。进一步，当前威胁形势和防御体系的复杂性首先体现在碎片化上：各种各样的数据隐私法律法规要求导致数据存储和使用的地缘政治化和碎片化，数据引力问题导致数据移动困难，混合云和多云导致跨云和本地的安全运行一致性难以实现，大量的单点解决方案造成数据孤岛和应用筒仓，融合的数据在不同的团队之间（如安全团队、IT 运行团队、业务团队等）交互和共享存在困难。

如何打破这些 SOC 的藩篱？



地和对与 Cisco 整合的回应。难道未来的 SOC 就是 Splunk 的 SIEM 加 Cisco 的 XDR 吗?

不可否认，SIEM 和 XDR 在不断互相渗透和融合，但简单地将二者叠加到一起显然并不能代表未来 SOC。当然，我们还需要 AI 和自动化，但这还不够。

Splunk 对待 AI 的态度还是比较审慎的，一如业界大佬的做派。Gary Steele 表示，在 AI 的加持下，分析师的重要性将加码。AI 将用于增强而不

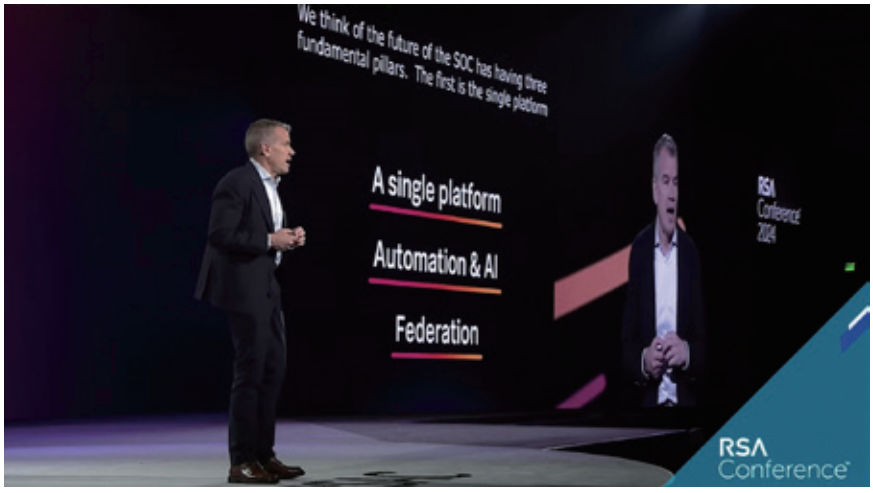
Gary Steele 认为需要重新思考数据架构。他说，“过去那种日志集中优先的 SOC 技术架构已经一去不复返了！我们要把分析向数据侧靠拢，而不是将数据向分析侧靠拢。这是一种根本性的改变”。基于此，Gary Steele 给出了未来 SOC 的三大支柱。

第一支柱：单一平台，指安全运行人员在统一的工作面上进行威胁检测、调查与响应，能够获得统一（一致）的上下文（情境）、洞察和行动。

第二支柱：自动化和 AI，指安全运行人员可以在没有噪声影响的情况下聚焦真正要做的事情，而自动化和 AI 就负责去噪。

第三支柱：数据联邦化，指安全运行人员可以根据自己的业务需求和权限检索数据，而无需关心数据位于何处。

接下来，让我感觉有些违和的是，Gary Steele 抛出了一个论断——未来 SIEM 将与 XDR 融合，成为新 SOC 的核心——作为对单一平台的落



是取代人类分析师，让分析师成为真正的防御者。Gary Steele 认为不存在自主 SOC（Autonomous SOC）【打脸 PAN】，人还是坐在副驾位置，上不了驾驶位，并提出了一个新词：Fully Proactive Automation（完全主动的自动化）。AI 可以提升防御者，帮助分析师进行告警分诊、案例管理、事件响应、漏洞管理、工作流处理、……，但整个安全运行过程依然是人在回路的，AI 更适合于解决特定问题，同时 AI 的开放性和扩展性十分重要。

最后，Gary Steele 不忘发挥一下 Splunk 跨 ITOps 和 SecOps 的数据分析优势，将安全运行推到了更广泛的业务连续性运行范畴，以实现所谓的数字弹性。

纵观整个演讲，笔者认为，除去 AI 和自动化这类显而易见的 SIEM/SOC 变革因素不谈，相较于 CrowdStrike 提出要变革数据架构但却没有具体路径，Splunk 进一步阐释了数据架构变革的关键方向之一——分析向数据侧靠拢，也即数据联邦化。但进一步来说，Splunk 对于未来 SIEM/SOC 架构的阐释也就是点到即止。

将 GenAI 应用于 SOC

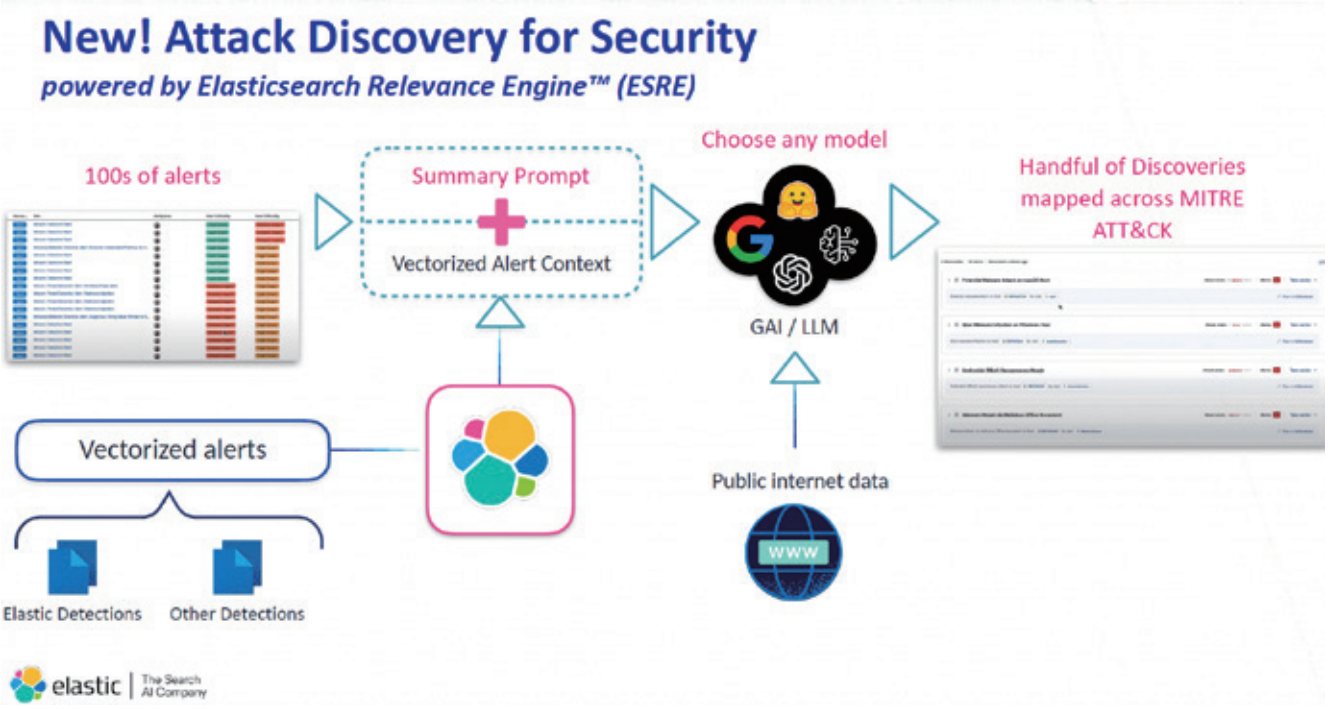
在本届 RSAC 大会的创新沙盒决赛中，出现了一家以 GenAI 赋能 SOC 的创业厂商——DropZone AI，而该公司创始人恰恰还是一位华人，并且在他去年初创业伊始就开始与笔者沟通 GenAI 用于安全运行的技术。成为极少有的站上 RSAC 创新沙盒决赛赛场的华人，笔者为他感到骄傲。对于公司名称，他解释到，DropZone AI 这个词所表达的是要做一款“增援安全运行人员的智能助力的传送门”产品。

DropZone AI 的产品引入了 AI Agent（智能体，或称为“AI 行为体”）技术，从而将 GenAI 增强 SOC 的应用水平提升到一个新的高度。

DropZone AI 的核心是告警研判和事件响应。与一般使用 GenAI 提示工程甚至是 RAG 来进行告警研判不同，DropZone AI 的核心技术在于上图所展示的“魔方”。通过这个魔方，DropZone AI 具备了推理和规划的能力，能够自主进行任务分解和动作调用与执行，代表了当前 GenAI 应用于 SecOps 领域的最高水平。

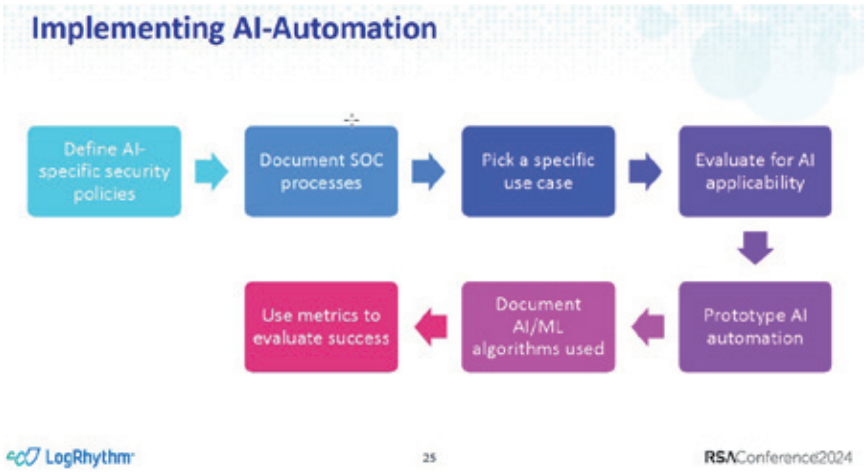
值得一提的是，DropZone AI 并不是要取代现有的 SOC，而是跟现有的 SOC 平台集成，赋能现有的 SOC 团队，减轻他们的告警疲劳。

Elastic 在大会上做了一个题为



《Fight Smarter: Accelerate your SOC with AI discovered attacks》的发言。其中介绍了他们基于RAG（检索增强生成）的攻击检测技术。

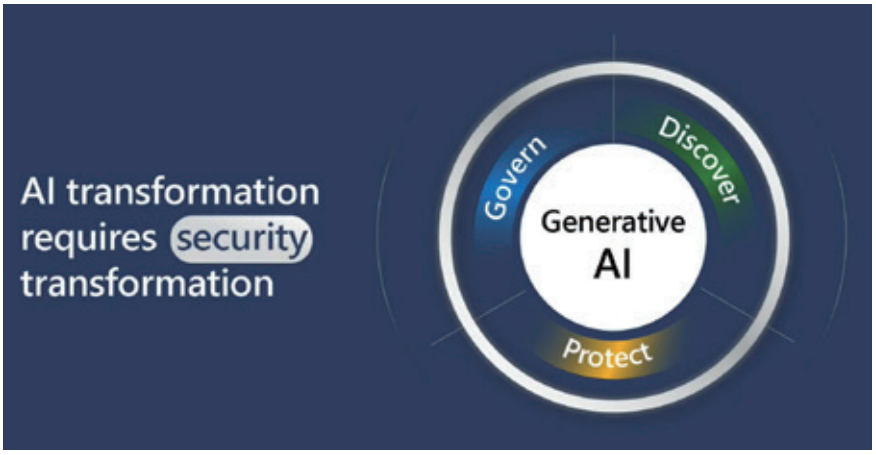
LogRhythm 的演讲则从如何缓解 AI 带来的风险角度来帮助人们更好地利用 AI 赋能 SOC。GenAI 自身的不可靠（如过时的数据、不准确的回答、隐私限制、缺乏可见性、偏见）会影响其在 SOC 中的应用。因此，在既有的限制条件下选择恰当的用例十分关键，并且还需要对用例进行验证和评估。



展开来说，GenAI 的安全可靠性不仅对 SOC 领域，对于任何要应用 GenAI 的领域都同样至关重要。在本次大会主题发言环节，微软安全业务副总裁 Vasu Jakkal 提出了一个保障 GenAI 安全可靠的三支柱框架，包括（1）发现——识别风险并映射到风险框架；（2）保护——应用和模型保护及数据保护；（3）治理。

其他厂商动态

在厂商展区，OpenText 和 Cybereason 还分别举办了产品简报活动。OpenText 的议题是《Elevating



Security with Integrated AI & Analytics》，探讨 OpenText Cybersecurity 的 AI 能力如何检测异常、识别新出现的威胁并增强防御策略。笔者没有会议的相关材料，但 OpenText 的 AI 能力加持到安全领域后，发布了所谓的 Cybersecurity Aviator。Cybereason 的议题是《How can you transform your SOC with AI》。笔者同样没有相关材料，但 Cybereason 作为 EDR、XDR 厂商，和 CrowdStrike 一样，开始进入 SIEM 市场，最近刚发布了所谓 AI 驱动的 SDR（SIEM 检测与响应）解决方案，旨在乘 SIEM 架构变革之机进入这个市场分一杯羹。所以，大家会看到，当你还在为选择 SIEM 还是 XDR 而犹豫不决的时候，XDR 厂商已经纷纷发布 SIEM 产品了！

来到展会现场，几乎每个 SIEM 厂商都打出了 AI 牌，大家的 slogan 充斥着 AI。比如，微软：AI-first end-to-end security for all（AI 优先的所有领域端到端安全）；IBM：Empower the modern SOC with enterprise-grade AI（用工业级 AI 赋能现代 SOC）；Securonix：A New Era of AI-Reinforced CyberOps（AI 增强网络运营的新时代）；Exabeam：AI-driven Security Operations（AI 驱动的安全运行）。

还有一个奇葩事件，就是网络安全榜一大哥 PAN（派拓网络）没有正式参加此次 RSA 大会！对此，有的人说是 PAN 认为 RSAC 的品推投入产出比不高，还不如自己搞活动，也有的人说 PAN 这次的品推政策踩坑了，

不应错过这次机会。就在 RSA 大会召开之际，PAN 发布了 Precision AI 及其解决方案。据报道，Precision AI 是一种专有的人工智能系统，结合了机器学习、深度学习和 GenAI，以确保实时安全。

> 现有的 SIEM 面临数据悖论，
> 一方面需要更多的安全数据，
> 另一方面又无法及时有效地处理这些海量安全数据。
> SIEM/SOC 架构迎来变革，
> 将成为 AI 原生 SOC 的操作系统。

总结

GenAI 正在席卷整个人类社会，GenAI 将深刻改变网络安全产业，笔者不敢称之为颠覆，但变革是必然的。聚焦到安全运行和 SOC 领域，GenAI 对其带来的变革可以从大小两方面来评估。

从大的方面来说，SOC 类产品要真正释放出 GenAI 的潜能，还是要首先革新自身的技术架构。这就好比生产汽车，底盘最重要，决定了基于此底盘的一系列车型的扩展上限。底盘不好，再好的发动机也难发挥最大效力，SOC 的技术架构就相当于汽车底盘。而 SOC 类产品架构革新的关键，就在数据架构的革新。正如笔者之前反复强调的，现代数据栈技术发展已经突飞猛进，传统的安全数据架构重构已成定局。而在新的架构之上，建立 AI 原生的 SOC 技术平台是远景目标。

在考虑大的方面的时候，笔者认为要对 GenAI 的边界有清醒的认识，即人依然是安全运行的主体，GenAI 提供的都是人类助理，协助人类进行多种任务处理，而不能取代人类。

从小的方面来说，在现有 SOC 技术架构之下，GenAI 依然有用武之地，可以通过外挂的方式赋能安全运行，提供一系列相关功能。目前为止，绝大部分 GenAI 应用都是外挂式的。在这种情形下，重点要关注 GenAI 如何具体赋能安全运行，降低安全运行人员的职业倦怠，并找到具体场景。技术层面，则可以考虑使用提示工程、RAG（检索增强生成）甚至是 AI Agent（智能体）等技术，要充分将新兴技术与现有成熟技术结合，不要言必称颠覆。

凡事皆有两面性。在利用 GenAI 赋能安全运行的同时，一定要关注 GenAI 自身的安全可靠性问题，尤其要避免出现数据安全问题。

最后，尽管本文聚焦于 GenAI 赋能安全运行和 SOC，但从更广泛意义上来说，我们更应该关注 AI 如何赋能安全运行，而不应仅限于 GenAI。事实上，在 AI 的诸多领域，都有很多新技术和新应用。

拐点已至，未来已来。安

RSAC 2024 观察：软件供应链安全进入 AI+ 时代

作者　董国伟

网络安全行业备受关注的 RSAC 2024 刚刚落下帷幕，虽然今年大会的创新沙盒比赛打破了之前五年均有软件供应链安全初创公司进入 10 强的惯例，但这并未影响软件供应链安全议题成为大会必选项，并引发广大从业者极大兴趣的状况。本文就来盘点一下今年 RSAC 2024 会议上软件供应链安全议题的特点、趋势及启示。

一、RSAC 2024 软件供应链安全议题内容分析

1、软件物料清单（SBOM）成为热门话题

这一现象与 SBOM 近年来的研究热度有关。在前几年完成了 SBOM 最小要素、数据格式等基础内容的规范后，美国目前正在 CISA 等机构的协调下，聚焦于 SBOM 的应用落地和易用性优化等的研究和工作。SBOM 话题在 RSAC 2024 的多个环节中都有讨论。

> 在完成 SBOM 最小要素、数据格式等基础内容的规范后，美国目前正在聚焦于 SBOM 的应用落地和易用性优化等的研究和工作。

在 Track Session 环节，Finite State 的产品安全总监分享了如何将 SBOM 纳入测试工具箱，以及具体的实例和实施流程的建议；Aloft 的安全与风险经理从供应链透明度工件 1.0、2.0、3.0 的范围定义入手，介绍了 SBOM 在合规、安全方面的作用及相关工具，并针对组织应用 SBOM 的流程给出了建议。

本次大会设立的 9 个研讨会（Seminar）中，就有一个是以“SBOM：好的、坏的和丑陋的”为主题的，该研讨会在 5 月 8 日上午举行，围绕 SBOM 的概述和实施、CycloneDX 认证、新领域的 SBOM（如 SaasBOM、AI/ML-BOM、CBOM 等）、从 SBOM 中获得商业价值等 4 个方向，探讨 SBOM 的优点、局限性和陷阱。

在赞助商简报（Sponsor Briefing）环节，Synopsys 和 Sonatype 等公司分享了 SBOM 在现代网络风险管理、漏洞识别和修复、潜在攻击防范等方面的重要作用、相关的配套技术和工具（如软件成分分析 SCA、威胁模型、

持续威胁监控等），以及相应的实践经验。

2、更多供应链安全框架纳入了对 AI 因素的考量

随着 AI/ML（开源）框架应用于业务系统、AI 技术应用于编码等开发环节的情况越来越普遍，组织在实施软件供应链安全措施时，也会更多的考虑这些 AI 因素。

GitHub 副总裁在《AI、软件供应链和其他令人费解的部分》的议题中提到，92% 的美国开发者使用 AI 编码工具。他列出了三类加强软件供应链安全的方法和系统，即软件安全和隐私（代码安全、敏感信息扫描）、平台 / 开发者安全（第三方集成安全、双因子认证 /Passkeys）、构建系统和依赖关系（依赖分析和 SBOM、构建出处分析），并探讨了 AI 与这些方法和系统一起来增强供应链保护能力的途经。

Thales 软件安全总监在《确保软件供应链安全：问题、解决方案和 AI/ML 挑战》议题中，列举了针对供应链的 8 类攻击面，介绍了业务系统因引入AI/ML框架而可能带来的安全风险，并从数据安全、模型安全、平台安全、安全合规、人员安全 5 个方面给出了保障 AI/ML 供应链的目标和技术。在最佳实践建议部分，他也提到了应定义并实现安全的 AI/ML 框架、验证 ML 模型或数据集的完整性。

3、开源软件安全议题较少，但均与 OpenSSF 相关

可能是由于近年来，美国在开源软件安全方面组织的各层次会议较多，如白宫开源软件安全峰会、北美开源峰会 SOSS，以及各种 OpenSSF 日活动等，导致了在 RSAC 2024 上专门探讨开源软件安全的议题并不多，但它们都涉及到 OpenSSF 的一些工作或项目。

> 随着 AI/ML（开源）框架应用于业务系统、AI 技术应用于编码等开发环节的情况越来越普遍，组织在实施软件供应链安全措施时，也会更多的考虑这些 AI 因素。

DARPA 主任助理和 OpenSSF 总经理联合奉献了《破解代码：揭示开源安全与 AI 的协同作用》的议题。OpenSSF 去年 8 月就与 DARPA 开展合作，支持其牵头的人工智能网络挑战赛（AIxCC）。本议题列出了能够帮助解决 AI 安全问题的多个评估框架和工具，其中包括 OpenSSF 的 Scorecard 和 Sigstore；介绍了围绕使用大模型和生成式 AI 发现开源软件漏洞的目标，在 AIxCC 中设计合理的评分公式和原则，以挑选出优秀团队和成果的方法。

Veracode 首席研究官等专家基于对实际生产应用的 1140 多万次软件成分（SCA）扫描及对其中使用的 3 万多个开源项目分析所得的数据，分享了《量化开源缺陷的概率》的议题。他们将这些扫描分析结果与 OpenSSF 已计算出的开源库 Scorecard 分值进行交叉关联，并在已知漏洞、许可证、代码审计、二进制工件、依赖更新工具、分支保护等近 20 个维度上进行量化分析，从而发现了与安全存储库相关的属性。

4、供应链安全细分领域正在得到更多关注

RSAC 2024 上还有一些关于软件供应链安全细分技术领域的议题，最典型的是对于开发工具和基础设施、知识产权、生命周期终止（EOL）软件等所涉及的安全风险应对方法的讨论。

Mitiga 首席技术官介绍了近年来针对开发工具和 SaaS、Git、CI/CD 平台、开源存储库等开发基础设施进行攻击的实例、类型和趋势，并给出了通过预防、检测、响应的三步骤方法和具体实施措施加强其安全性的方案；Akamai 高级副总裁兼首席安全

官在《确保现代应用程序的安全：从代码到基础设施》的议题中也关注了基础设施的安全性。

思科高级信息安全架构师分享了他们的供应链安全计划，包括资产识别、安全风险识别和评分、知识产权（IP）保护和防伪技术、第三方安全评估、其他安全措施 5 方面内容，其中着重介绍了 IP 保护和防伪技术的实践，涉及开发 DLP 策略、敏感数据识别和分类、使用加密等 7 方面最佳实践，以及利用思科的第三方生态系统，在整个解决方案生命周期内提供不受损害的完整性的防伪技术等。

针对 EOL 软件的安全管理，CISA 高级顾问给出了最新研究进展。在去年 7 月美国白宫发布的《国家网络安全战略实施计划》中就提到，CISA 将探讨为生命周期 / 支持终止的软件建立一个全球可访问数据库的需求。此外，OWASP 发布的 10 大开源软件风险的第 4、5 项风险，就涉及无维护和过期的开源软件。由此可见，此类问题已得到普遍的关注。演讲者介绍了相关概念和政策框架，并提出了使用数据支持政策的解决方法，即通过 CISA 的“软件识别生态系统选择分析”项目和一些自动化工具来获取相关数据，以便对 EOL 软件实施管理。

此外，在开发流程安全管理方面，Scribe Security 在赞助商简报环节介绍了基于证据的 SDLC 护栏的概念，并将其作为代码在 CI/CD 中实现。这是一项供应链安全即代码的实践，可简化安全控制，平衡大规模软件开发的敏捷性和安全性。

二、对软件供应链安全研究工作的启示

基于对 RSAC 2024 软件供应链安全议题的盘点，对软件供应链安全工作带来了两个方面的启示：

- 应充分考虑“软件供应链安全 +AI”的研究工作模式

一方面，AI 技术自身存在多方面的安全风险，特别是开发中第三方 AI/ML 框架的引入，会带来新的供应链安全问题。因此，针对这些风险，需要在框架或模型引入或系统上线之前，进行检测和处置，避免将安全问题带入运行环节引发供应链安全事件；另一方面，AI 技术本身作为能够极大提升效率的基础方法，可以应用于软件供应链安全分析、检测和管理的各个环节，如代码安全分析、开源软件漏洞分析等，从而提升相应分析的能级。因此，在软件供应链安全的研究工作中，应考虑“AI for Supply Chain Security”和“Supply Chain Security for AI”两方面的实践。

- 应加快软件物料清单（SBOM）相关的研究和应用

我国的国家标准《软件物料清单数据格式》即将公开征求意见，4 月份刚发布的《GB/T 43698-2024 软件供应链安全要求》和《GB/T 43848-2024 软件产品开源代码安全评价方法》也有关于 SBOM 基础字段的定义和对 SBOM 完备性、可追溯性的要求。应基于这些标准的要求，推进基于 SBOM 的安全风险治理的落地，具体包括：软件供应方采用开源安全治理工具监测开源物料并消减其风险，监测所使用物料的安全漏洞等风险并及时为用户提供技术支持，生成 SBOM 并随产品提供；软件最终用户验证 SBOM 以确认软件成分和安全风险，在软件日常运行中，基于 SBOM 持续跟踪软件物料相关的威胁情报，及时采取措施等。

关于作者

董国伟

虎符智库专家，奇安信集团代码安全实验室高级专家，博士，从事网络安全、软件安全、代码审计和漏洞分析相关工作近 20 年。

RSAC 2024 观察：云安全左移还是右移?

作者　鲍坤夫

RSAC 2024 上，基于 AI 安全的相关产品和服务成为网络安全创新的新趋势。纵观近几年 RSAC 大会创新沙盒十强，除了 AI 安全，云安全也一直是创新热点，RSAC 2023 创新沙盒十强中，有五家产品和云安全相关，RSAC 2024 创新沙盒十强中，也有四家产品和云安全相关。

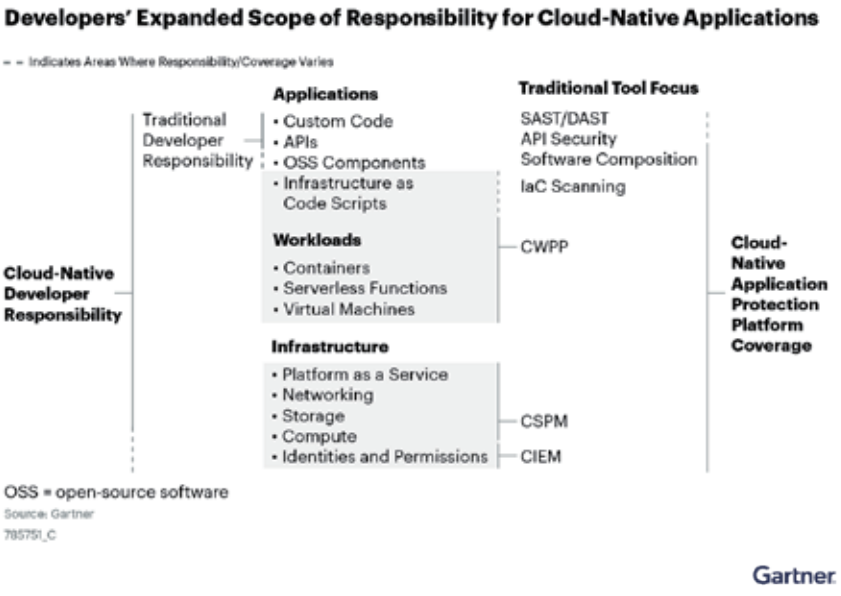
RSAC 2024 云安全仍然处于最前沿，特别是强调云原生应用保护平台（CNAPP）。如果说 RSAC 2023 云安全的创新方向主要聚焦在开发安全，包括供应链安全方面；2024 年 RSAC 云安全创新方向则主要聚焦在运行时安全方向，尤其是云原生环境下的运行时安全。随着企业越来越多地采用云原生技术，以云为中心的安全防御变得前所未有的重要。

一、云安全相关创新方向受关注的原因

为什么云安全相关创新方向如此受关注和热捧呢？一方面是因为随着数字经济的加速发展，云已经成为关键基础设施，针对云的攻击手段和数量也越来越多；同时云原生相关技术的出现，也给安全管理和安全运营带来极大挑战。

（1）容器不可变基础设施特性导致业务必须从代码源头修复，漏洞修复代价高。传统环境或者非容器环境下，运行时环境如果被扫描出漏洞，可以通过打临时补丁或者热补丁进行线上即时修复，而容器环境下因为容器的不可变基础设施特性，即容器总是根据自己的镜像重建，导致临时补丁失效，需要业务先修复代码再重新构建新的容器镜像进行更新，也就是需要全部走一遍完整的开发部署流程，导致漏洞修复代价高、周期长，业务风险变高。

（2）IaC 等技术的出现导致业务负责的范围变大，相应的安全责任也



变大，业务的整体工作量剧增。传统环境或者非云环境下，业务代码只包含自定义代码、API 和开源组件等，用到的安全工具也只有 SAST/DAST、SCA 和 API 安全工具等，而 IaC 技术和容器技术的出现，业务代码会增加基础设施代码，同时制品增加容器镜像，需要用到的安全工具相应增加 IaC 扫描工具、镜像扫描工及 CSPM 等配置扫描工具。业务在代码开发工作量增加的同时，新安全工具带来的工作量也剧增，同时业务的安全责任也变得更大。

（3）云原生分层架构导致攻击面增大，相应安全工具增多，安全工具运维和运营工作量大。云原生架构和微服务架构的出现，虽然解决了数字经济时代大型软件或复杂软件的弹性和可扩展性问题，但也带来了新的暴露面。其中，云原生基础设施带来了新的云安全配置风险，容器化部署带来了容器逃逸的运行时新风险，而应用微服务的细粒度切分导致 API 风险剧增。这些新的风险都需要新的安全工具来解决，让本身繁重的安全运维和运营工作雪上加霜。

（4）云原生业务敏捷开发效率和现有安全运营效率严重不匹配，漏洞修复不完，告警处置不完。随着 DevOps 开发流程和基于云的应用开发模式完美契合，应用开发效率得到了极大的提升。但因为容器技术和 IaC 等云原生技术的出现，不管是开发阶段，还是运行时阶段，均增加了大量新的安全工具，而这些不同的安全工具在使用的过程中会扫描出大量的安全漏洞或者告警。如果这些漏洞和告警都需要修复和处理，将极大的拖慢业务的开发速度，导致业务部门和安全部门的摩擦进一步增加，业务价值的快速变现和业务安全无法平衡。

除了上面这些难题，基于多云或混合云的应用部署模式正变得越来越普遍，安全的统一管理和防护也变得越发困难，迫切需要安全企业开发创新的方法或技术来解决这些问题。

二、云安全技术创新三大方向

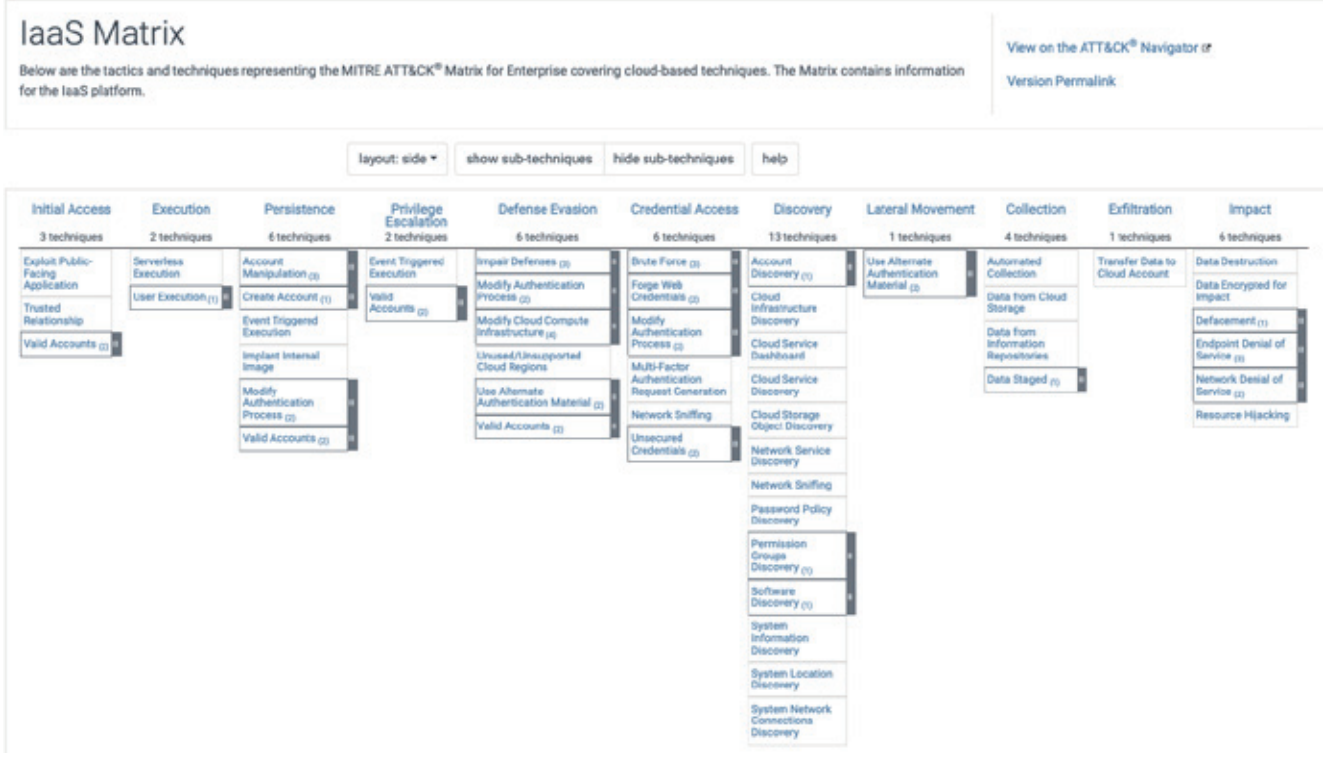
从 RSAC 2024 看，云安全创新的方法或技术主要聚焦在以下方向。

（1）聚焦安全左移：安全左移概念很早就被提出，并不是云原生时代特有的，但因为容器不可变基础设施特性导致业务必须从代码源头修复，漏洞修复代价高，因此安全左移被越发重视。安全左移的目标是为了保障业务尽可能安全的上线，因此要求上线前发现所有的安全问题并修复问题。为了实现这一目标，诞生了各种白盒、灰盒和黑盒安全工具，如各种 SAST、SCA、DAST、IAST，以及

Fuzz 测试工具。除了这些安全工具，因为 IaC 和容器等技术的出现，也出现了 IaC 扫描、镜像安全、CI/CD 管道安全等工具。这些安全工具都能够帮助检测或者发现应用在开发阶段中的安全问题，包括漏洞、配置、协议和弱口令等脆弱性风险，但因为扫描或检测技术的不同，工具的误报率或准确率有所区别。现有安全企业的创新方向是在尽可能的发现更多风险的前提下降低误报率，如使用 AI 技术或机器学习技术来提升代码安全的识别能力。除了单个工具自身的误报率和精准率的问题，多个安全工具一起使用扫描出的风险太多，导致修复工作量大的问题也非常突出。工具越多，扫描出的风险越多，评估和修复的工作量越大，越影响业务发布上线的速度，但是如果减少工具，虽然扫描出的风险变少了，但是漏报的风险也高，和安全左移的目标不符。为了解决多个安全工具扫描出的风险怎么统一评估和修复的问题，ASPM（应用程序安全态势管理）就成为大家越来越关注的创新方向和解决方案。ASPM 工具通过收集、分析整个软件生命周期中的安全问题并确定其优先级，持续管理应用程序风险。他们从多个来源获取数据，关联并分析结果，以便于解释、分类和补救。它们支持安全策略的实施并促进安全问题的修复，同时提供整个应用程序风险的全面视图。

（2）聚焦安全右移：随着云成为新的基础设施，针对云的攻击正变得越来越多，攻击手法也越来越复杂，为此 MITRE 开发了针对云的 ATT&CK 攻击矩阵，帮助企业安全人员分析黑客攻击所使用的技战术，如下图所示。为了检测和防护这些针对云的攻击，相关的安全工具被开发出来，如 CWPP 产品能覆盖云上工作负载的安全防护，包含主机、容器和 Serverless 等工作负载，CSPM/KSPM 工具用于检测云原生基础设施的配置风险，CIEM 工具用于检测云上用户权限的配置风险。

同时，伴随应用微服务架构的大量普及，云上 API 安全和数据问题越发突出，针对云上 API 安全防护和数据安全防护的产品也越来越多。另外，针对云内特有的东西向攻击风险，基于云内全流量采集和威胁检测技术的



NDR 和 XDR 产品也应运而生。和安全左移一样，安全右移也面临风险过多无法及时评估和修复的问题。例如，通过 CWPP 和网络漏扫设备都可以扫描出漏洞，但是漏洞太多，漏洞修复的优先级就变成一个亟待解决的问题，为此，VPT 相关技术和产品就成为一个热门创新方向。除了漏洞修复优先级问题，运行时告警降噪的能力也是云原生安全运营一直追求的方向，伴随 AI 技术的辅助加持，通过 AI 驱动告警研判和处置，提升安全运营效率就成为当前最热门的创新方向。

为了满足用户对云数据泄露的快速响应与检测需求，在 RSAC 2024 期间，安全厂商展示丰富的云安全态势评估和检测工具，专注于广泛的多云检测和响应。

其中，Palo Alto Networks 的安全运营平台 Cortex XSIAM 引入了云检测和响应 (CDR) 功能，提供云资产、事件、覆盖范围和漏洞的可见性，并与 Prisma Cloud 集成，以增强事件分组和导航。借助 XSIAM 提供的统一用户界面，安全分析师可以高效、有效地响应基于云的威胁，增强态势感知并增强整体安全态势。CrowdStrike 推出新的云检测和响应 (CDR) 功能，将行业领先的托管威胁狩猎与跨云、

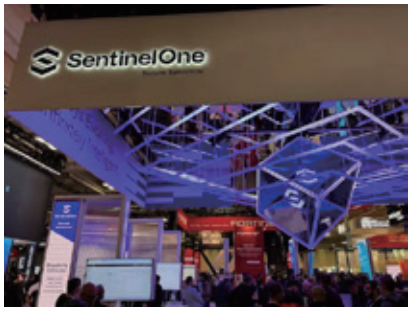
身份和端点的可视性统一起来，以加快对每个阶段云攻击检测及响应速度。

专注于云原生异常检测和响应创新解决方案的 RAD Security 跻身创新沙盒 10 强。该公司提供实时 Kubernetes 安全态势管理 (KSPM) 工具，云原生身份威胁检测和响应、基于 eBPF 技术的云原生工作负载指纹。

（3）聚焦全生命周期安全：安全左移是为了让应用尽可能安全的上线，而安全右移是为了尽可能检测和防护运行时攻击，那这两者有没有什么关联呢？首先，运行时攻击利用的主要是应用和基础设施本身的脆弱性，而这些脆弱性本身是开发阶段引入的，如果开发阶段能提前发现和修复这些风险，运行时就不存在这些攻击路径。其次，运行时发现的风险问题必须经过新的开发阶段才能彻底修复，因此两者是有很强关联关系的。那有没有办法把安全左移和安全右移结合起来提升整体安全效果和运营效率呢？答案是有的。例如在开发阶段，大量安全工具的使用导致漏洞修复的优先级评估一直是一个难题，这时可以结合安全右移阶段发现的应用风险暴露面或者攻击面拓扑来帮助评估漏洞的影响范围。而在运行时阶段，可以结合安全左移阶段积累的应用制品资产库和制品风险库，帮助安全运营人员迅速定位风险引入的位置和责任人，从而快速推动风险的彻底修复。为了实现这一目标，需要使用创新的设计方法来整合安全左移和安全右移，因此 CNAPP 平台产品应运而生。按照 Gartner 的定义，云原生应用程序

保护平台（CNAPP）是一组统一且紧密集成的安全性和合规性功能，旨在跨开发和生产保护云原生应用程序。CNAPP 产品将多种不同的安全和保护功能整合到一个平台中，最重要的是，该平台能够跨现代云原生应用程序极其复杂的逻辑边界识别、确定优先级、实现协作并帮助修复过度风险。CNAPP 平台的核心设计思想是以应用为中心，基于应用上下文的统一安全视角，覆盖应用全生命周期，包括资产管理、风险评估和告警处置，让应用安全可观测。

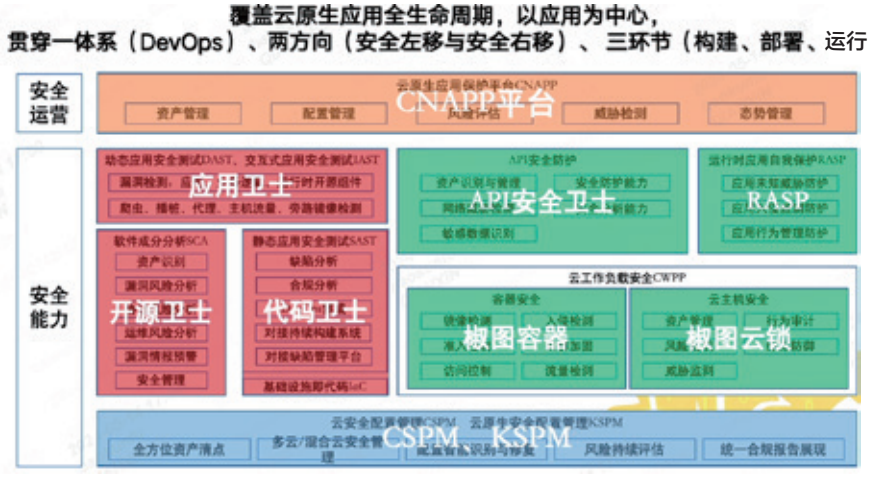
SentinelOne 在 RSAC 2024 期间宣布推出 Singularity 云原生安全（CNS）——无代理云原生应用保护平台（CNAPP），以帮助云团队、开发人员和安全专业人员减少云和容器攻击面。



奇安信云原生应用安全保护管理平台（CNAPP）则获得国际领先信息安全媒体 CDM《网络防御杂志》的先锋产品奖。平台针对云原生带来的安全挑战，以云原生应用为核心保护目标，提供覆盖整个云原生架构及云原生应用的全生命周期的完整保护。

RSAC 2024 大会虽已落幕，但围绕安全左移、安全右移和应用全生命周期安全相关的创新热点讨论仍在继续。对于大部分创业安全公司来说，围绕安全左移或者安全右移其中的一个点进行创新将成为主流，而对于大的网络安全厂商而言，聚焦应用全生命周期安全，通过集成、整合自有及生态合作产品，推出 CNAPP 平台将成为主流。

奇安信作为一家为客户提供综合安全解决方案的网络安全领先厂商，除了为客户提供覆盖从安全左移到安全右移的各种单项安全能力，更是在国内率先推出并落地了 CNAPP 平台产品。奇安信 CNAPP 平台包括三大核心能力，一是代码到云的应用资产拓扑，以云原生应用为中心，提供全生命周期的应用资产拓扑和关联关系，从而全方位掌握保护对象和暴露面。二是提供统一的风险评估，通过整合各安全扫描工具风险数据，统一进行风险评估，提供漏洞修复优先级，从而提升应用上线评估和日常运营的效率。三是代码到云的攻击路径溯源，通过绘制应用代码到云的漏洞 \ 威胁攻击路径，提供影响范围和攻击证据，打通开发态和运行态的风险关联，使安全左移可落地。



构建统一防线，消除运维安全风险

——新奥集团特权访问安全解决方案

作者 数据安全事业部 晏瀚

新奥集团，作为知名互联网科技集团企业，主要业务包括互联网信息服务、增值电信业务、信息咨询服务、区块链技术相关软件和服务等。旗下包含多家子公司分支机构，包括新奥智城、新智认知、新绎文化、新奥股份、数能科技。

挑战：资产数量激增 账号风险随之而来

随着新奥集团数字化建设进程的加速，集团的资产数量呈现几何倍数增加，截至当前已经达到2万多的规模，其资产运维账号达到了约 5 万，运维人员超过 1000 人。快速的数字化建设进程，提高了企业的生产效率，但也带来了诸多安全挑战，尤其是来自资产运维的网络攻击风险不断增加。

这促使新奥创建了一个针对资产运维账号（特权账号）和运维操作（特权会话）的全面安全管控计划。该计划的一个关键要素是改进现有的运维管理架构实现运维操作的统一化监控管理，并加强对资产运维账号使用的监督和控制。

图：新奥集团

应对：从资产运维管控切入，全面降低安全风险

新奥集团项目负责人孙建磊表示：“资产运维管控对于任何想要保护系统和数据的组织来说都是关键。我们需要确保能够严格控制用户对内部资产的运维访问请求，并以‘及时’的方式提供请求，以减少滥用的机会。该计划的重点是减轻无意和恶意攻击的风险。”

另外，加强对《网络安全法》、《信息安全技术 网络安全等级保护基本要求（GB/T22239-2019）》、ISO27001 等标准的遵守，以及新奥

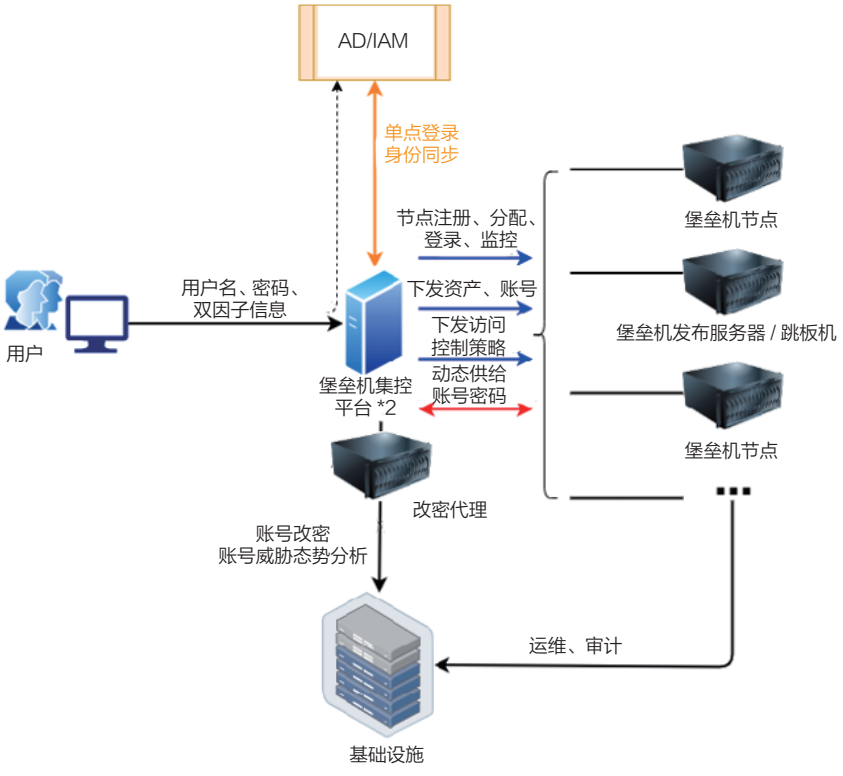
集团内控规范的遵守也是变革的重要驱动力。

为了选择最佳的资产运维管控解决方案，新奥集团总部将利益相关方（新奥智城、新智认知等）聚集在一起，以确保跨业务协作并在选择新解决方案后快速推动落地。

奇安信是少数几家受邀提交详细方案的供应商之一，方案在所有评估标准中获得了高分，并随后被选为首选解决方案。其他因素还包括奇安信提供的全国范围内的优质服务保障，并且在河北省也拥有极高的知名度。新奥集团通过与其他客户的交流及行业分析师对奇安信的认可和突出地位的验证，进一步确认了这一决定。

新奥集团有多个子分支机构，包括新奥智城、新智认知、新绎文化、新奥股份、数能科技，各子分支机构的运维安全管控目前“各自为政”，分别通过建设堡垒机来对各自分支的资产开展运维操作管理，并且对资产运维账号缺乏有效的管控措施。

基于以上问题，新奥集团推出了特权访问安全解决方案，一种混合本地和云的运维安全管控专属解决方案，通过在新奥集团总部部署堡垒机集管平台形成运维改密策略统管面，而在新奥新智基础网络及各分支机构的 VPC 环境（IoT 系统 VPC、技术中台 VPC、质采智购 VPC 等）中部署堡垒机节点 / 资产运维账号自动改密节点形成运维改密策略执行面，实现新奥集团的资产运维账号（特权账号）和运维操作（特权会话）的统一管理。



新奥新智项目架构图

效果：特权访问安全，简单高效化解资产运维风险

奇安信特权访问安全解决方案使得新奥集团能够构建一个全方位无死角查看组织内部资产运维活动，并有效防御资产运维攻击的安全解决方案。

“衡量奇安信特权访问安全解决方案效果的一个指标是，我们现在知道每个资产运维账号的使用情况，而且显著减少了他人对我们环境造成破坏的机会。”

——新奥集团项目负责人 孙建磊

“以前，我们的资产运维管控只能尽力而为，依赖于手动审查和人员的信任关系。现在，它是基于事实的。如果有人想要对权限进行变更，后续的资产运维控制过程将严格遵循一套强制的规则。” 孙建磊继续说道。

新奥集团过去的运维管控体系架构分散，不同分支不同角色的人员可能拥有同样的资产访问权限，而管理员却很难得知。奇安信特权访问安全解决方案限制了具有资产运维权限的用户数量，并在需要时强制执行访问权限供应策略。这使得流程更具可观测和可预测，很好地符合集团的规范要求。通过更好的访问权限控制和可见性可以在确保符合网络安全法等相关标准的同时，还提高了审计效率。

图：奇安信特权账号管理系统账号风险态势

另外，方案还减少了管理员追踪工单、审批流程等内容所耗费的时间。

不仅如此，奇安信特权访问安全解决方案还能显著提高业务效率。

“部署奇安信特权访问安全解决方案意味着我们的批准流程基本不会出现纰漏，因为我们现在有了一种常见的运维资产访问权限的供应方式。这是一个非常重要的进步，因为它不仅更安全，而且提高了效率，”孙建磊说道，“这减轻了负担，更加灵活，因为我们不需要联系十个不同的人来了解他们各自的流程。”

现在，新奥集团内的其他业务部门已经看到这次项目的未来蓝图，在项目建设的协同过程中也非常的配合。未来，孙建磊和他的团队将在整个集团范围内继续扩展特权访问安全的实施领域。

建议：企业部署特权访问安全是大势所趋

有数据统计，80% 的黑客攻击中涉及的数据泄漏事件与失窃的特权身份有关。失窃的特权身份是几乎每次严重攻击的共同因素，原因很简单：攻击者需要通过窃取的特权身份凭证，

图：奇安信特权账号运维安全管理系统

图：奇安信特权账号管理系统界面

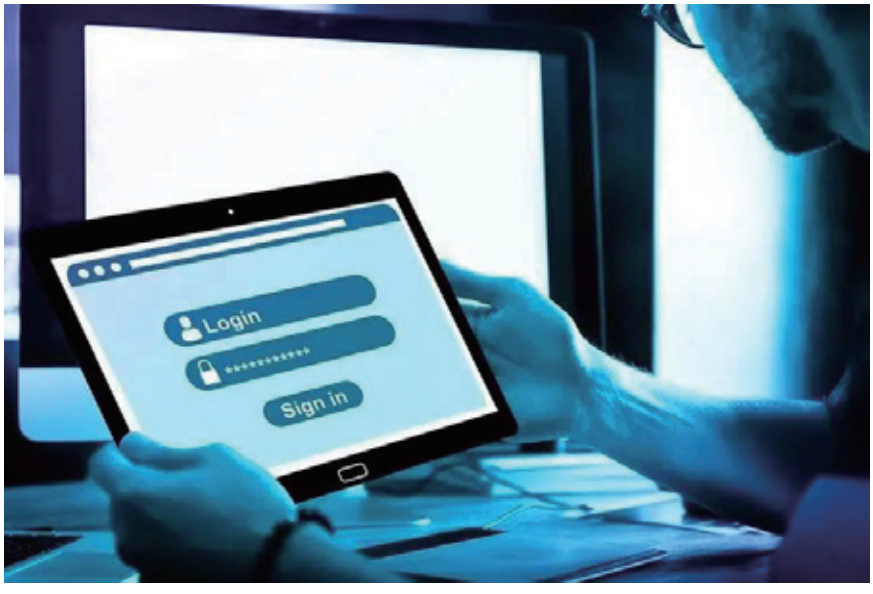
来获得访问企业最关键资产信息的权限。可见，特权身份凭证是访问网络关键基础设施及窃取数据所必需的前提条件。

奇安信已经开发了一套成熟的特权访问安全解决方案，以帮助组织建立行之有效的特权访问安全计划。奇安信在“特权访问安全”领域拥有近 10 年的技术积累，也是国内独家将 SDP 架构应用于特权访问安全领域的厂商，相比传统堡垒机只关注特权会话的单一方案，在特权安全性、特权身份管理成本、特权身份纳管范围等维度都进行了全面升级，为特权访问提供端到端的访问安全防护。

奇安信提供给组织一套简单而全面的“特权访问安全”指导性蓝图，使组织的特权访问安全计划与潜在的数据泄漏 / 勒索病毒等安全风险降低目标紧密结合，从而帮助组织能够尽快解决其当前最大安全困扰。

蓝图考虑了数字化时代的组织及其业务可扩展性的需求。它可以为使用传统的本地基础设施和软件开发方法的组织，以及正在进行数字转型（如将基础设施迁移到云端、采用 CI/CD 实践或通过机器人流程自动化流程等）的组织，提供了特权访问安全控制的最佳实践建议。

专家认为，作为直接接触组织关键 IT 资产和数据资源的入口，特权账号是通往企业数据大门的“钥匙”，要实现数据安全的精准防护，首先就是要管特权、“防内鬼”。在技术变革快、安全风险复杂、合规性要求越来高的背景下，企业迫切需要一套体系化的安全能力来应对新技术、新场景带来的新挑战，新奥集团在特权访问安全方面的探索，无疑对同行具有广泛的借鉴意义。安



图：特权账号是通往企业数据大门的“钥匙”

阴影之下：揭示 API 威胁的攻击趋势

API 是公司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，安全团队将会惊觉其系统中存在诸多以前从未意识到的漏洞。

Akamai 公司最新发布的《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。

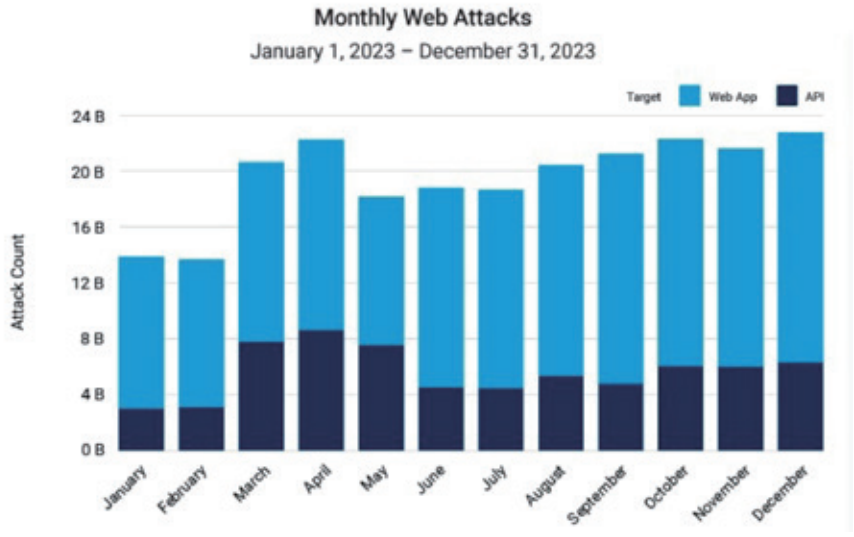


图 1：针对 API 的 Web 攻击

一、主要见解

• 2022 年 Gartner 预计，到 2024 年，API 滥用和数据泄露将翻一番。2023 年，29% 的网络攻击针对 API，这表明 API 是网络犯罪分子锁定的重点领域。

• 针对 API 的攻击包括 OWASP TOP 10 API 安全性和 OWASP TOP 10 Web 应用程序安全性中强调的风险，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。

• 业务逻辑滥用是一个关键问题，因为在没有为 API 行为建立基线的情况下，检测异常 API 活动是极具挑战性的。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，例如，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。

• 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。

二、API：最大的攻击向量

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（见图 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。

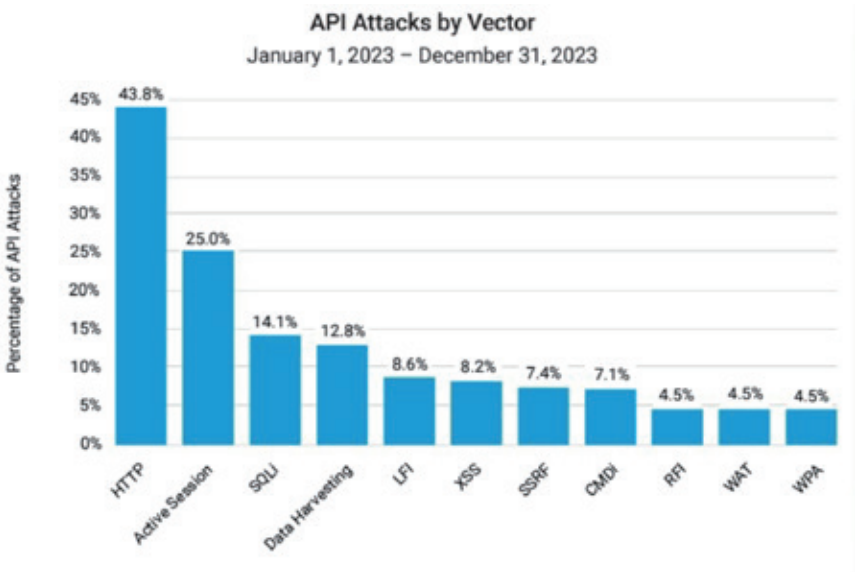


图 2：攻击者最青睐的一些 API 攻击向量

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。

2、困扰 API 安全的现实问题

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。

3、最常见的态势问题

研究人员观察到最常见的态势问题：影子端点、未经身份验证的资源访问、URL 中的敏感数据及宽松的 CORS 政策，如果不解决，将对企业造成各种潜在影响。

4、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问题及其潜在风险概况：未经身份验证的资源访问尝试、JSON 属性异常、路径参数模糊化尝试、数据抓取。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？

- 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？

- 业务逻辑滥用——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。

三、行业趋势凸显供应链攻击危险

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%（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。

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。

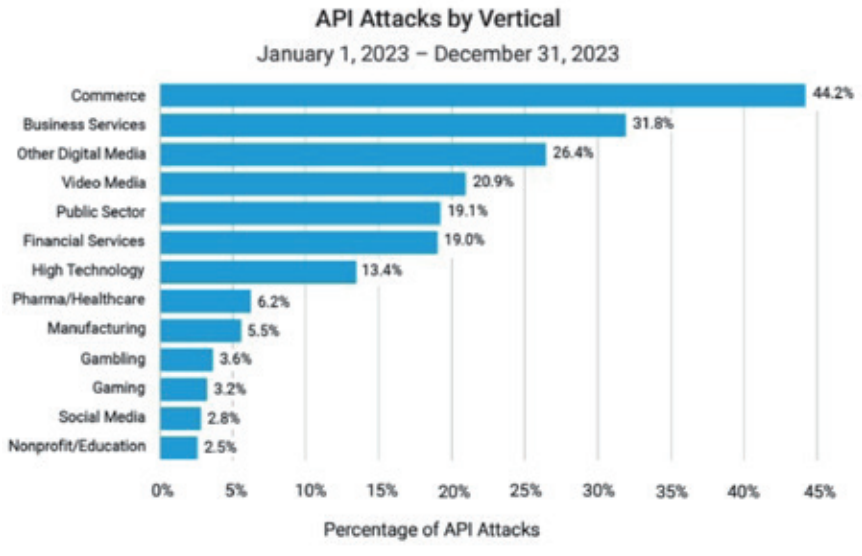


图 3：2023 年，商务和企业服务领域遭受 API 攻击比例最高

四、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。

奇安信网络安全实战攻防演习报告（2023）摘录

注：本文为报告摘要，联系奇安信集团销售人员，可申请免费获取完整报告。完整报告含更多数据、演习案例及详细的安全建议。

综述篇

2023 年，奇安信共参与实战攻防演习 670 次，参演单位总计 974 家，参演总计 3419 人次，参与攻防演习时长累计 8071 天，总计投入 61,615 人天。总计攻破系统 18,020 个，抵御攻击 1.33 亿次。

1. 攻击队主要成果

2023 年，奇安信攻击队共参与实战攻防演习 263 次，累计参演时长 2191 天，参演人员 1154 人次，演习累计投入 9975 人天。成功攻破目标单位 582 家，总计攻破系统 18,020 个，其中内网一般业务系统占比 39.2%；互联网业务系统占比 18.4%。成功对 50 家企业实施钓鱼攻击。

2. 防守队主要成果

2023 年，奇安信防守队共为 392 家政企机构提供实战攻防演习防守服务，其中主防单位 105 家（含二级单位），协防单位 287 家（含二级单位），累计参演时长 5880 天，参演人员 2265 人次，演习累计投入 51,640 人天。抵御各类网络攻击共计 1.33 亿次，其中，漏洞利用攻击 11,400 万次、蜜罐攻击 649 万次、主机攻击 527 万次、暴力破解 253 万次。

演习期间，研判专家累计分析确认攻击事件 91,423 起，其中：漏洞利用事件 55,572 起、恶意软件事件 9630 起、网络钓鱼事件 7975 起。一线防守团队第一时间采取处置措施：封禁 IP 3271 万个、清除恶意样本 2947 个、上机排查 581 次。红雨滴沙箱确定攻击队 IOC 标签 3440 个，共享情报超过 28.1 万条，输出溯源分析报告 857 份。

攻击篇

以下为奇安信攻击队 2023 年参与的 263 次实战攻防演习成果分析。从目标单位行业分布来看，26.2% 的机构来自政府机构事业单位，12.7% 来自金融行业；制造业排名第三占 9.2%，具体分布见图 1。

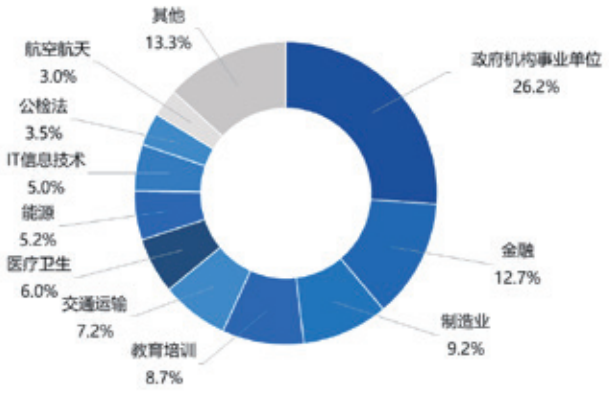


图 1. 网络安全实战攻防演习目标单位行业分布

组织单位分布：其中，国家部委占比 15.7%、省级单位占比 20.0%，央企占比 17.0%。详见图 2。

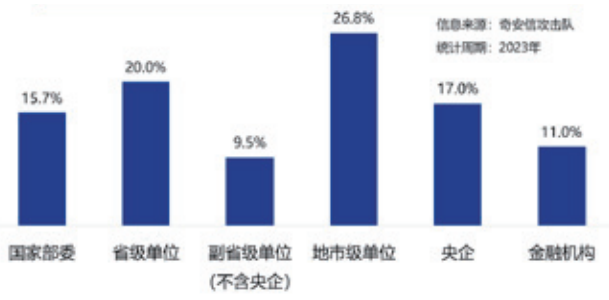


图 2. 网络安全实战攻防演习组织单位分布

2023 年，奇安信攻防演习攻击队总计拿下 18,020 个系统，其中，互联网基础设施系统占比 22.3%、办公系统占比 12.0%、生产系统占比 11.0%、业务系统占比 39.2%、安全设备 / 系统占比 2.4%、身份认证系统占比 1.6%。具体分布见图 3。

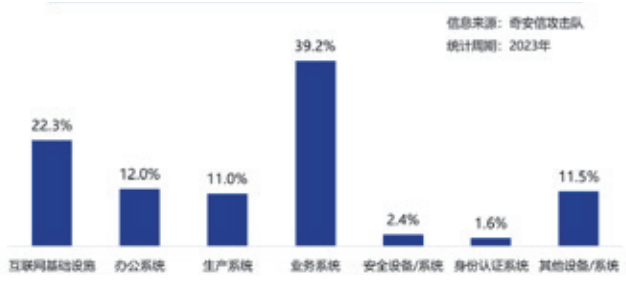


图 3. 网络安全实战攻防演习中攻击队拿下系统类型分布

行业分布：奇安信攻防演习攻击队 2023 年累计获得 56.7 万台服务器权限，平均每家单位获取 975 台服务器权限。从行业分布来看，金融业被控制服务器数量最多，占总量的 14.3%；其次为 IT 信息技术行业，被控制服务器数量均约占服务器总量的 14.2%。网络安全实战攻防演习中攻击队控制服务器数量行业分布 TOP10 见图 4。

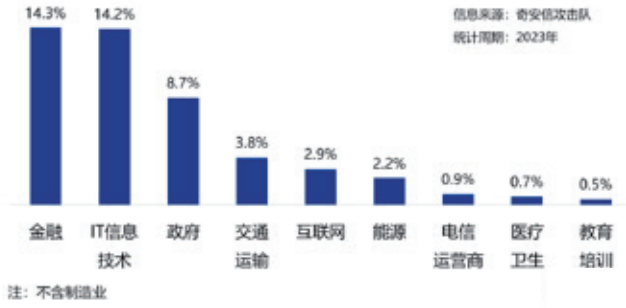


图 4. 网络安全实战攻防演习攻击队控制服务器行业分布 TOP10

数据泄露量分布：数据泄露，是政企机构面临的重大网络安全风险。2023 年，奇安信攻击队累计发现演习目标单位可泄露数据 350 亿条，约合 4680TB，平均到每家演习单位，可泄露数据 0.6 亿条，约合 8.0TB。从行业分布来看，政府机构可泄露数据最多占比约为 79.6%；医疗卫生行业紧随其后，可泄露数据占比约为 9.2%。各行业存在数据泄露风险的数据量 TOP10 见图 5。

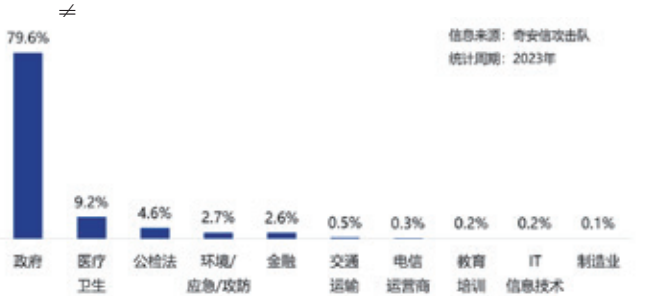


图 5. 网络安全实战攻防演习不同行业存在数据泄露风险数据量分布

攻击手法：如图 6 所示，2023 年奇安信攻击队在 74.1% 的攻击中使用了已公开漏洞，在 67.8% 的攻击中使用了弱口令。此外，还有 48.1% 的攻击使用了口令复用。这些攻击手法的有效性，恰恰反映出相关机构网络安全防护的薄弱。

图 6. 网络安全实战攻防演习中常用的攻击手法

特别值得注意的是，奇安信攻击队会在 61.8% 的攻击行动中，使用 0day 漏洞。这些 0day 漏洞绝大多数都是这些机构的业务系统、生产系统或网络安全系统中存在的尚未未公开的安全漏洞。这表明，0day 漏洞利用在实战攻防演习中，已经是非常普遍的技术行动。

从社工钓鱼的具体途径来看，微信钓鱼使用率最高，其次是邮件钓鱼、QQ 钓鱼，具体分布详见图 7。

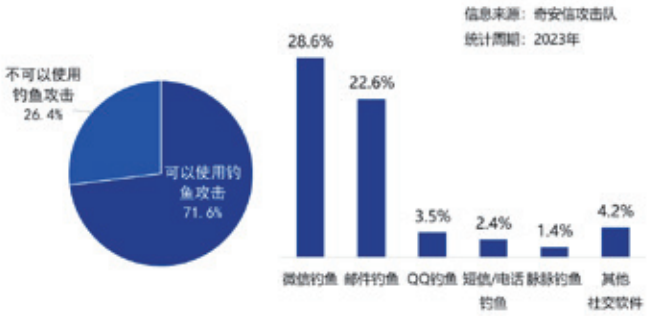


图 7. 网络安全实战攻防演习中社工钓鱼手法使用情况

防守篇

2023 年，奇安信集团在网络安全实战攻防演习活动中，共为 392 家政企单位提供防守任务，其中，奇安信担任主防单位 105 家，担任协防单位 287 家。总计投入 2265 人次，参与攻防演习时长累计 5880 天。总计投入约 51,640 人天。从具体分工来看，其中一线防守人员 1844 人，占总量的 81.4%；二线支持人员 421 人，占总量的 18.6%。

行业分布：奇安信集团参与防守的单位中，金融行业机构最多，其次是政府机构、电信运营商。此外，电力、交通、能源、医疗、公检法、教育等行业也是奇安信集团服务的重点。具体分布见图 8。

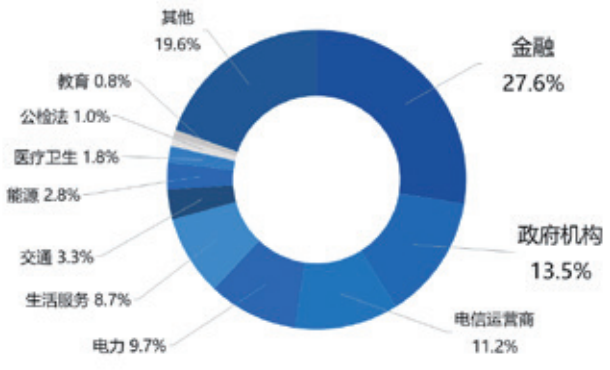


图 8. 网络安全实战攻防演习防守方行业分布

产品部署：据不完全统计，2023 年实战攻防演习期间，奇安信共为 392 个客户提供 49 类网络安全产品 14,948 套。其中，威胁监测与分析系统（天眼）占比 36.3%，是攻防演习的首选装备； 新一代防火墙（NGFW）占比 22.1%，位列第二；终端安全管理系统，占比 9.3%，排名第三。此外，态势感知与安全运营平台（NGSOC）占比 5.8%、网络安全准入系统占比 4.9%、上网行为管理占比 4.5%。详情见图 9。

图 9. 网络安全实战攻防演习产品部署情况分布

拦截告警：2023 年，在全国各级、各类网络安全实战攻防演习活动中，奇安信防守队结合现场部署的各类防御及检测系统，共截获各类网络攻击 1.33 亿次。从具体的告警信息来看，攻击利用类告警最多，攻击 11,400 万次，占所有告警信息的 85.7%；其次是蜜罐告警 649 万次、主机威胁类告警 527 万次、暴力破解类告警 253 万次。具体分布见图 10。

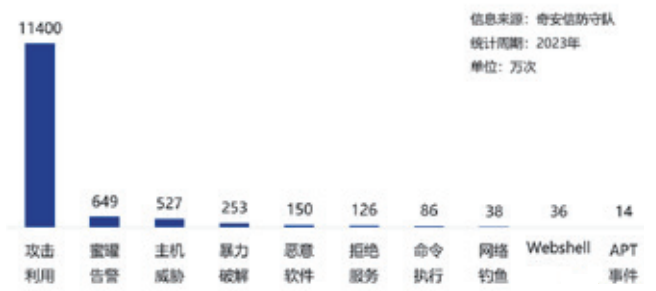


图 10. 防御和检测系统截获各类威胁告警信息类型分布

分析研判：在 2023 年网络安全实战攻防演习过程中，奇安信防守队研判专家共筛选分析确认安全事件91,423起。其中，攻击利用事件 55,572 起，占比 60.8%；恶意软件事件9630起，占比10.5%；网络钓鱼事件7975起，占比8.7%。具体分布见图 11。

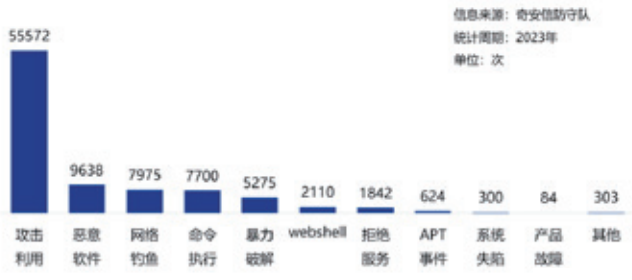


图 11. 网络安全实战攻防演习安全事件研判分析结果与类型分布

事件处置：2023 年，奇安信防守队在网络安全实战攻防演习过程中，共协助政企机构处置各类安全事件 3852 次。其中，清除恶意样本 2947 次，占比 76.5%；上机排查 581 次，占比15.1%；下线问题设备115台、下线僵尸业务系统（长期无人运维和使用的业务系统）107 个。具体分布见图 12。

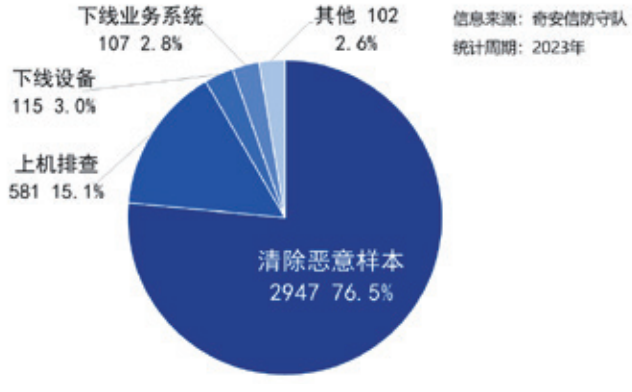


图 12. 网络安全实战攻防演习事件处置类别分布

应急响应：此外，在 2023 年的全国网络安全实战攻防演习过程中，奇安信 95015 平台，还协助 66 家事先未邀请奇安信参与防守任务的演习单位，完成网络安全应急事件 97 起，覆盖 18 个行业。其中，协助 59 个演习单位成功溯源。应急过程中，排查被攻击设备近 1200 台，发现 0day 线索 5 个，为 73 家参演单位提供了针对性的系统失陷分析报告。

溯源分析： 2023 年，奇安信威胁情报中心及白泽系统，共协助参演防守单位溯源分析应用程序 205,252 个，鉴定 API 接口 335,372 个；捕获演习攻击队 96 个，向参演防守单位提供高价值攻击队基础设施情报信息 151 条，确定攻击队 IOC 标签 3440 个；发现被攻击队利用的安全漏洞 294 个，其中，已公开漏洞 123 个，0day 漏洞 171 个。

恶意样本：此外，在演习期间，奇安信红雨滴团队共捕获恶意样本2817（按哈希值统计），判定黑IP地址90.9万条。

总结篇

结合 2023 年实战攻防演习攻击侧和防守侧的经验，我们对参与攻防演习的政企机构，提出了九项具体的安全建议（详细建议与分析，请见报告完整版），分别是：验证防护安全有效能力、建设终端安全管理能力、构建服务器安全防护能力、增强威胁监测能力、增强全局态势感知与运营能力、搭建自动化响应系统、部署攻击诱捕平台、强化邮件安全检测与员工反钓鱼意识、增加供应链安全防护能力。

奇安信 | BEIJING 2022

北京2022年冬奥会官方网络安全服务

奇安信威胁情报中心

中国威胁情报行业领军者

奇安信威胁情报中心是奇安信集团旗下专注于威胁情报收集、分析、生产的专业部门，以业界领先的安全大数据资源为基础，基于奇安信长期积累的威胁检测和大数据技术，依托亚太地区顶级的安全分析师团队，通过创新性的运营分析流程，开发威胁情报相关的产品和服务，输出威胁安全管理与防护所需的情报数据，协助客户发现、分析、处置高级威胁活动事件。

威胁情报中心

威胁研判分析平台ALPHA： 一站式云端SaaS服务的威胁分析工具平台。是安全分析师为同行打造的利器，针对IOC查询、线索关联、事件溯源、样本行为检测和同源分析等威胁分析场景提供全面的解决方案。

高对抗云沙箱分析平台： 提供多种动静态检测、分析技术，展现文件各方面特征，帮助分析师快速判别、并掌握恶意软件的详情。

威胁分析武器库： 服务于安服、安运、安全分析师及各类企业用户。支持IOC自动化数据流检测、失陷情报、恶意IP批量查询；支持邮件批量自动化检测；支持WEB应急日志、主机应急日志分析。

威胁情报系统QAX TIP： 威胁情报平台是情报收集、维护、使用的综合性平台。可帮助企业在安全运营中，利用威胁情报快速检测、响应、分析和预防各类网络攻击威胁，并分析产生行业威胁情报。

威胁雷达： 利用大数据和威胁情报监测技术，整合了奇安信的高、中位威胁情报能力，提供指定区域内网络威胁高位监控、案件拓线分析、样本深度分析等多种能力。

样本同源分析系统： 奇安信威胁情报中心红雨滴团队基于样本基因深度解析，使用机器学习算法用于APT数字武器追踪的可视化分析系统。

高级威胁分析服务： 为网络安全主管单位，政府机构、行业客户及高校科研机构提供情报线索拓线和威胁分析服务，输出深度分析报告供其决策参考。

奇安信威胁情报中心：
ALPHA网址：https://ti.qianxin.com
雷达网址：https://r.ti.qianxin.com
扫描关注我们的微信公众号
邮箱：ti_support@qianxin.com

大事记

第二届 BCS 企业数字化转型及数据安全专题研讨会在成都举行

5 月 18 日，BCS2024 全国系列活动——第二届 BCS 企业数字化转型及数据安全专题研讨会在成都举行。本次活动由电子科技大学、鹏城实验室、2024 北京网络安全大会主办，奇安信集团、小鱼易连科技有限公司、四川亿览态势科技有限公司承办，大湾区中央企业数字化协同创新联盟协办，邀请了专家院士、高校学者、政企机构信息化部门负责人、网络安全专家等，聚焦“‘人工智能 + 安全’护航高质量发展”主题，展开精彩分享和深入交流，为 6 月 5 日即将启幕的 2024 北京网络安全大会打响了头阵。

奇安信集团与智能汽车创新发展平台公司签署战略合作协议

5 月 16 日，智能汽车创新发展平台（上海）有限公司（以下简称“平台公司”）总经理邱国华一行访问了奇安信安全中心，并与奇安信集团签署了战略合作协议。双方将发挥各自优势，在“车路云”一体化安全体系建设、云控平台信息安全与数据安全、数据交易等方面开展紧密协作，旨在全面提升我国智能网联汽车，特别是智能网联新能源汽车的安全体系自主创新能力和核心竞争力。

齐向东：发展新质生产力要找准方向、做好研发、踏实落地

5 月 15 日至 17 日，由全国工商联、共青团中央主办 的第六届全国青年企业家大会在武汉举行。大会以“勇立潮头 智启未来——为推进中国式现代化贡献青春力量”为主题，旨在搭建全国青年企业家共享交流平台，团结和引导全国优秀青年企业家听党话、跟党走，推进民营经济高质量发展。

全国工商联副主席、奇安信集团董事长齐向东受邀做主题演讲。他表示，青年企业家是企业家队伍里最有活力和创造力的群体，也是发展新质生产力的生力军，并分享了奇安信发展新质生产力的“三宝”：方向要准、研发要狠、落地要实。

奇安信牵头！我国首个零信任国家标准正式发布

近日，国家市场监督管理总局、国家标准化管理委员会

发布了中华人民共和国国家标准公告（2024 年第 6 号），由奇安信牵头的《 网络安全技术 零信任参考体系架构 》（ GB/T 43696-2024 ）正式发布。该标准是我国网络安全领域首个规范零信任理念的国家标准。

《 网络安全技术 零信任参考体系架构 》的制定历经四年，由奇安信集团董事长齐向东担任项目负责人。在全国网络安全标准化技术委员会的管理指导下，奇安信联合零信任领域国内一流的产学研用机构，在给出零信任基本概念、零信任参考体系架构等内容上开展了大量研究工作，并最终推动标准顺利发布。

数据安全危机席卷全球医卫行业，奇安信发布百家医院免费体检计划

5 月 14 日，奇安信集团在京召开“百家医院数据安全免费体检计划”发布会。在发布会上，奇安信对外披露了全球医疗卫生行业面临的网络安全现状，以及对国内 25 家医疗机构的数据安全体检状况，并宣布向全国医疗卫生机构推出“百家医院数据安全免费体检计划”，为构筑医疗卫生行业数字时代的新质生产力保驾护航。

体检计划将持续进行至 2024 年年底，为全国至少 100 家大型医疗机构进行为期 7 天的数据接口暴露面检查、数据接口安全风险检查、敏感数据违规传输检查，为其展开数据安全规划建设工作提供科学的参考依据。体检完成后，奇安信将向医院提交一份详细的体检报告及初步整改建议，帮助他们看清自身数据安全风险，助力数据安全工作开展。

首实安保科技董事长浦义富一行到访奇安信安全中心

5 月 9 日，首都实业投资有限公司董事、副总经理、首实安保科技有限责任公司董事长浦义富，首实安保科技有限责任公司总经理刘杰一行到访奇安信安全中心，并与奇安信集团总裁吴云坤、副总裁张龙及安全专家，就数据安全、信创安全、AI 安全等领域的战略合作进行了深入交流。

奇安信携 AI 加持重磅产品亮相 RSAC2024

美国时间 5 月 6 日 ~9 日，全球网络安全行业的盛会——RSAC 在美国旧金山隆重举行。奇安信集团携全新升级的

QAX C-SOC 解决方案与最新的 SkyEye XDR 产品亮相，展示国内网络安全领军企业的最新技术创新。

本届 RSAC 大会上首次展出的 SkyEye XDR 是一款支持 SaaS 化和私有化（On-Premise）部署的下一代可扩展检测与响应平台，集成了奇安信业界领先多项方案——EDR（端点检测与响应）、NDR（网络检测与响应）、VPT（高风险漏洞管理）、Auto Pentesting（自动化渗透测试）、BAS（安全有效性评估）等，配合实时更新的云端威胁情报、沙箱、欺骗诱捕等领先工具，以及 QAX-GPT 安全机器人，可以帮助用户快速消除高危风险，及时检测和响应新兴的安全威胁。

AI 加持的 QAX C-SOC 解决方案再次亮相 RSAC，新增了智能问答、智能研判、智能运营等重要能力。自 2023 年 RSAC 上首次亮相以来，QAX C-SOC 已经发展成为针对全球市场的成熟解决方案，其主要组件均得到 Gartner、Forrester、IDC 等国际权威咨询机构的认可。其中，QAX SIEM 已进入 Gartner MQ 魔力象限，成为全球领先的 SIEM 品牌。

金融行业零信任标杆！奇安信中标某大型国有银行项目

近日，奇安信集团中标某大型国有银行全行零信任安全访问项目。根据合作内容，奇安信将为客户提供整体的零信任产品体系，以构建动态的、实时的业务安全访问体系。

该项目标志着奇安信零信任产品体系已经在多家大型国有银行、超半数全国性股份制商业银行，以及多家城市商业银行和农村商业银行中广泛落地，在金融行业已经取得显著的领先优势。

齐向东出席德胜门大讲堂：“人工智能 + 安全”护航数字经济

4 月 27 日，由全国工商联主办，全国工商联网络与数据安全委员会、商会发展服务中心、组织建设部承办的第 64 届德胜门大讲堂在京举行。活动以“‘人工智能 + 安全’护航数字经济”为主题，邀请主管部门、研究机构、算法、算力、数据等人工智能与安全产业链代表，共同探讨“人工智能 + 安全”前沿技术、创新思路和实践经验。

全国政协委员、全国工商联副主席、奇安信集团董事长齐向东在《高质量发展：数字经济时代的“人工智能 + 安全”》主题演讲中表示，“人工智能 +”在为我国迈向数字经济强国提供宝贵机遇的同时，也带来难以回避的安全风险。网络安全行业作为人工智能技术最快落地应用且最快见到实效的行业之一，应积极探索“人工智能 + 安全”创新应用，夯实数字经济高质量发展的安全底板。

齐向东：人工智能是推动京津冀协同发展再上新台阶的关键引擎

4 月 27 日，2024 中关村论坛期间，由北京市人民政府、

天津市人民政府、河北省人民政府联合主办的“京津冀协同创新与高质量发展论坛”在京举行。全国政协委员、全国工商联副主席、京津冀企业家联盟主席、奇安信集团董事长齐向东受邀出席并做主题演讲。他表示，人工智能是推动京津冀协同发展再上新台阶的关键引擎，在“人工智能 + 安全”的创新发展领域，需要聚焦技术护航、产业协同、人才培养三个方向，护航京津冀协同创新和高质量发展。

京能集团董事长姜帆一行到访奇安信安全中心

4 月 26 日，京能集团党委书记、董事长姜帆，总经理阚兴一行到访奇安信安全中心，参观了奇安信网络安全保障中心、工业系统安全场景展示等，双方就数字化转型、网络安全形势进行了深入的交流。一同到访的还有京能集团旗下北京热力、清洁能源、京能电力、京煤集团、昊华能源、京能国际、能源研究院、京能信息等企业的主要领导。

齐向东：强化“人工智能 + 安全”创新引擎 为京港协同发展注入“安全力”

4 月 26 日，中关村论坛“京港科技创新论坛”在北京举行。全国政协委员、全国工商联副主席、奇安信集团董事长齐向东在“强化创新引擎 为京港协同发展注入‘安全力’”主题演讲中提出，京港两地应通力合作，发挥政策、科教、安全运营三大优势，为两地科技创新协同发展注入源源不断的“安全力”。

湖北工会大讲堂首期开讲 在推动新质生产力发展中争当先锋

4 月 23 日上午，2024 年湖北工会大讲堂在湖北省图书馆拉开帷幕。第一期工会大讲堂由省总工会主办、省文旅厅联办、省图书馆承办，邀请全国政协委员、奇安信科技集团党委书记、董事长齐向东做精彩授课。

“发展新质生产力是实现中国式现代化的必然选择。”“人工智能技术是当下发展新质生产力的‘牛鼻子’。”

齐向东以《创新发展“人工智能＋安全”护航中国式现代化》为题，从人工智能促进生产力跃升形成新质生产力、人工智能在提效的同时带来多层次安全风险、发展“人工智能＋安全”护航中国式现代化等方面进行深入浅出地阐述。

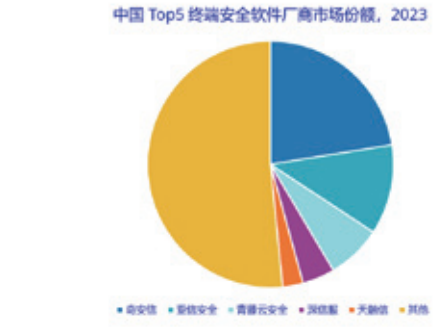
奇安信中标深圳市国家气候观象台信息安全支撑项目

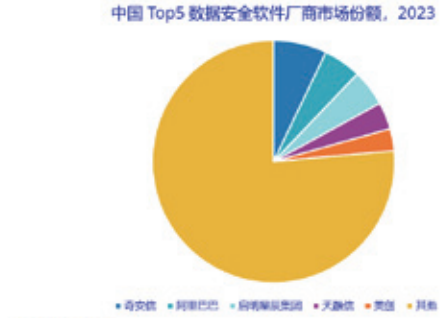
近日，奇安信中标深圳市国家气候观象台信息安全技术支撑服务项目，项目内容涵盖网站扫描、应急处置、网络安全培训、安全值守、渗透测试、攻防演练等服务。该项目中标，彰显了奇安信在安全服务领域的领先地位，为政府行业提供全方位的安全服务树立了新的标杆。

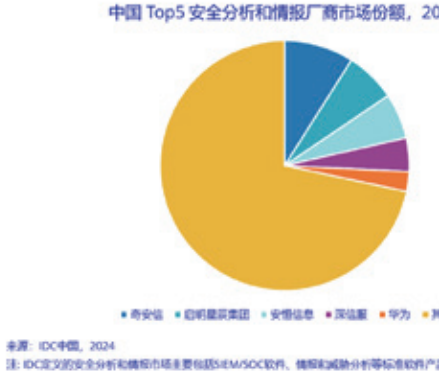
荣誉墙

三大市场持续领先！奇安信终端安全、数据安全、分析和情报市场再获第一

5 月 13 日，全球领先的 IT 市场研究和咨询公司 IDC 发布了《中国 IT 安全软件市场跟踪报告，2023H2》（以下简称《报告》）。《报告》统计显示，奇安信凭借卓越的技术实力和优秀的市场表现，再次领跑终端安全、数据安全、安全分析与情报市场。特别是终端安全领域，在奇安信连续 6 年稳居市场第一的基础上，再次扩大了市场占有率，彰显了强劲的产品竞争力和市场地位。

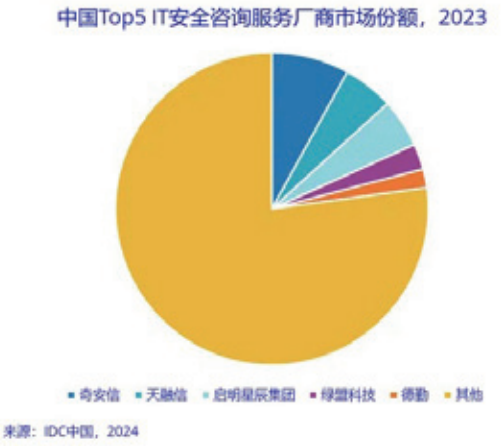






蝉联第一！奇安信安全咨询服务多年稳居市场领先地位

全球领先的 IT 市场研究和咨询公司 IDC 近日发布《中国IT安全服务市场跟踪报告，2023H2》(以下简称《报告》)。在安全服务市场中，奇安信安全咨询服务凭借 8.0% 的占有率排名第一，自 2020 年起，连续 4 年蝉联该细分市场份额第一。



RSAC2024 期间奇安信荣膺两项大奖

美国时间 5 月 6 日 ~9 日，全球网络安全行业的盛会——RSAC 在美国旧金山隆重举行。会议期间，国际领先的信息安全媒体 CDM (《网络防御杂志》) 颁发先锋产品系列奖项，奇安信的云原生应用安全保护平台（CNAPP）、网络资产攻击面管理系统 (CAASM) 荣膺先锋产品奖。

成绩 A 奇安信 QAX-GPT 安全机器人通过工信领域联合检测

近日，由中国软件评测中心（工业和信息化部软件与集成电路促进中心）联合数据安全关键技术与产业应用评价工业和信息化部重点实验室、中国计算机行业协会数据安全专业委员会发起的大模型安全性测评——“磐石·X”榜单计划，正式公布首批名单，奇安信 QAX-GPT 安全机器人以“A”


CSTC 中国软件评测中心
（工业和信息化部软件与集成电路促进中心）
证书编号：ZS-AIAQ-2024041801　　报告编号：AIAQ24041801
大模型产品安全性检测证书
奇安信科技集团股份有限公司
单位地址：北京市西城区西直门外南路26号院
产品名称：QAX-GPT安全机器人系统
产品型号：QAX-GPT
产品版本：V1.0
检测依据：大模型安全性检测基准
经中国软件评测中心和中国计算机行业协会数据安全专业委员会联合检测，贵单位的 QAX-GPT安全机器人系统（产品型号：QAX-GPT，产品版本：V1.0）符合指令安全、内容安全、模型安全、网络安全和数据安全的 A级 安全性要求，特发此证。
批准人：
二零二四年四月十八日
中国软件评测中心
（工业和信息化部软件与集成电路促进中心）
中国计算机行业协会数据安全专业委员会
数据安全产业公共服务平台
www.china-ds.org.cn

的最好成绩通过了联合检测，并拿到大模型产品安全性检测证书。

“磐石 · X”榜单计划通过指令安全、内容安全、模型安全、网络安全和数据安全五大维度测评大模型安全性，对来自来自基础电信运营商、互联网企业、人工智能厂商和安全厂商等各个领域大模型展开了联合检测。结果显示，奇安信 QAX-GPT 在内容安全方面表现优秀，贯彻落实了国家相关政策文件要求，大模型输出内容符合大模型安全性测评基准要求，切实保障行业用户的安全权益。

安全创新能力再获肯定 奇安盘古荣获“闵行区企业技术中心”认定

近日，奇安信集团旗下奇安盘古获得了上海市闵行区经济委员会颁发的区企业技术中心认证奖牌及证书。这一荣誉不仅代表了闵行区对奇安盘古技术研发能力的认可，也为奇安盘古打开了更多与重大项目合作、参与高端研发活动的大门。

企业技术中心是指企业根据市场竞争需要和发展战略规划设立的技术研发与创新机构，负责制定企业技术创新规划、开展产业技术研发、创造运用知识产权、建立技术标准体系、凝聚培养创新人才、构建协同创新网络、统筹推进技术创新全过程实施等，是体现区域科创能力和活力的标志性指标及重要引擎。


荣誉证书

HONORARY CREDENTIAL

奇安盘古（上海）信息技术有限公司：

你单位技术中心被认定为上海市闵行区企业技术中心，特发此证。

闵行区经济委员会

二〇二三年十二月

社会责任

深化“万企兴万村”行动 “心安助农 · 巴林左旗乡村振兴项目”正式签约启动

5 月 10 日，“心安助农 · 巴林左旗乡村振兴项目”签约启动仪式在巴林左旗正式举行。全国工商联党组成员、副主席杨佑兴，全国工商联副主席、奇安信集团董事长齐向东，内蒙古自治区党委统战部副部长、工商联党组书记梁淑琴，市委常委、统战部部长孟和巴特尔，巴林左旗旗委书记任玺出席活动。

杨佑兴指出，自 2023 年以来，在全国工商联党组的重视领导下，263 家执委企业、直属商会对 160 个重点县实现走访全覆盖，5784 家企业与重点县建立对接关系，在产业帮扶、公益帮扶、消费帮扶、人才帮扶、就业帮扶等方面做出了很多有益尝试和探索，取得了很好的经济和社会效益。奇安信集团积极响应号召，多次蹲点调研，研究有效帮扶模式，把追求企业成功和社会责任有机统一起来，为推动巴林左旗发展积极探索实践，具有很好的示范表率作用。希望奇安信集团探索出一条既能促进农牧民增收和企业发展双赢，又具备生态友好特点的乡村振兴之路；其他参与帮扶的民营企业积极探索新模式、展现企业新担当。

启动仪式后，项目组成员于 11 日 ~13 日，深入乌兰达坝苏木开展调研考察，聚焦当地的肉牛产业发展、生态环境治理、服务体系建设、群众生产生活等方面开展实地走访、座谈研讨。

奇安信
新一代网络安全领军者

聚焦安全运营，构建智能平台

奇安信网神态势感知与安全运营平台（简称NGSOC）以大数据平台为基础，通过收集多元、异构的海量日志，利用关联分析、机器学习、威胁情报等技术，帮助政企客户持续监测网络安全态势，为安全管理者提供风险评估和应急响应的决策支撑，为安全运营人员提供威胁发现、调查分析及响应处置的安全运营工具。

国内领先的威胁情报能力

奇安信威胁情报中心在情报数量及数据覆盖度方面国内第一。

首款分布式关联分析引擎 - Sabre

国内首款具备分布式关联分析能力的安全运营平台，提供多元异构数据关联分析、灵活威胁建模、丰富的告警上下文信息展示及分布式横向扩展能力，已获得数十个相关专利。

将平战结合进行落地

演练态势监测攻防演练中防守方管理信息、系统建设、威胁运营等信息的总体状况，平战结合，全面提升安全防御能力。

重大安全事件的威胁预警

当出现重大网络安全事件时，帮助用户第一时间掌握是否遭受到攻击？首个被攻击的资产？影响部门？影响面趋势？事件处置情况？

专业的安全运营服务

奇安信集团具有专职产品运营服务团队，可提供原厂一线驻场、二线分析、运营方案咨询及培训服务，帮助客户解决无人运营困难。

市场占有率NO.1

连续2年中国安全管理平台市场占有率第一——赛迪顾问认证
态势感知解决方案市场领导者——IDC认证
态势感知技术创新力和市场执行力双第一——数世咨询认证

欧洲学者分析军事人工智能系统面临的网络安全风险

欧洲学者分析对军事人工智能系统的三种网络攻击方式

作者 赵慧杰

编者按：欧洲领导网络（ELN）研究协调员爱丽丝·萨尔蒂尼撰文，分析军事人工智能系统面临的网络攻击风险、军事人工智能系统遭网络攻击的全球影响及可能导致的冲突升级路径，并向西方国家提出对策建议。

文章称，人工智能技术的快速进步有可能彻底改变包括军队在内的社会各个领域，全球各国希望将人工智能技术与军事行动融合以增强决策流程和作战效率；尽管具有潜力，当前的人工智能系统仍存在严重缺陷，其稳健性和可靠性的不足，无法保证在高风险军事行动领域的可靠性能；与传统军事平台不同，人工智能系统极易受到网络攻击，这为黑客访问和操纵敏感军事数据或破坏军事行动提供了新的切入点，针对此类网络威胁的防御措施滞后会导致对手可以利用军事系统的漏洞。

文章称，当前人工智能系统中存在的漏洞，为黑客破坏完整性、损害机密性和破坏可用性提供了机会，从而会导致错误结果、数据泄露和系统故障。其中，完整性攻击旨在欺骗人工智能系统做出错误的决策，方式包括操纵训练数据的数据毒害及利用模型缺陷的逃逸攻击；机密性攻击旨在推断出有关系统运行或其训练数据的受保护信息，并通过了解底层模型来发现更多漏洞；可用性攻击旨在削弱关键系统的可用性，方式包括拒绝服务和勒索软件等。

文章称，网络攻击因其易于执行、依赖广泛的人工智能漏洞及防御此类攻击的挑战而成为令人担忧的趋势；对人工智能系统开展网络攻击较设计和训练上述系统需要更少的专业知识和资源，故障恢复导致的性能妥协加剧这一不平衡情况；上述权衡可能会解决特定的漏洞，但同时可能会无意中放大其他漏洞，为攻击者提供利用新漏洞的机会。

文章称，随着世界各国加大在常规军事系统中部署人工智能技术的力度，对手毫无疑问会寻求识别和利用这些系统中的漏洞；网络攻击威胁可能源自网络战强国、资源较少但想要破坏西方防御系统的国家及非国家行为体，导致网络威胁形势进一步恶化；对于国家和非国家行为体来说，网络攻击可能是一种有吸引力且具有成本效益的替代方案，可以实现非对称优势并挑战技术更先进的对手；西方国家的对手可能已经在努力实现通过利

> 当前人工智能系统中存在的漏洞，
> 为黑客破坏数据完整性、
> 损害机密性和破坏可用性打开了大门，
> 从而导致错误结果、数据泄露和系统故障。

用网络漏洞破坏军事人工智能平台的目标。

文章称，人工智能漏洞表明，在安全至关重要的核领域依赖该技术是不稳定的，如核指挥、控制和通信（NC3）系统；常规军事平台中广泛采用人工智能也可能对核风险产生意想不到的下游影响；人工智能集成到常规军事系统或情报平台中的总体效应可能会导致对核领域产生不可预测的影响；通过网络攻击开展的对抗性干扰可能会导致大规模欺骗，进而导致广泛的误判和误解，从而可能在地缘政治不稳定的环境中增加无意或意外升级的风险；间接影响 NC3 的欺骗性因素可能会给利用网络攻击能力的对手带来优势，诱使一方将先发制人式的打击视为对抗或减轻感知威胁的可行策略；高度联网化的军事系统被利用可能会导致灾难性的级联故障，削弱常规威慑能力，在极端情况下可能迫使国家考虑通过核反应来恢复威慑。

文章提出，西方国防机构必须适应网络威胁不仅无处不在且随着人工智能技术的融合而不断演变的安全环境，为对手通过威胁人工智能核心数据集并开发新颖的漏洞来利用人工智能模型漏洞的风险做好准备；在网络威胁变得更加复杂和普遍的情况下，必须对军事人工智能整合采取极其谨慎的态度；西方国家必须通过制定基于网络风险的指标来为人工智能的军事应用制定明确的指导方针，相关指标应评估网络漏洞如何影响军事系统中的人工智能集成领域，强调人类监督的必要性，以及在出现异常情况时恢复手动控制的能力；西方国家应共同努力，通过有针对性的研究来加强网络防御，以抵御此类攻击；鉴于目前人工智能技术的不可靠性，以及核威慑系统遭渗透的固有风险和潜在灾难性后果，需要采取保守方法，不应将人工智能集成到关键的 NC3 功能中。

奇安网情局编译有关情况，供读者参考。

解决人工智能军事系统中的网络漏洞

人工智能（AI）的快速进步展现出惊人的能力，有可能彻底改变包括军队在内的社会各个部门。随着人工智能技术的发展，其与军事行动的融合越来越被渴望增强决策流程和作战效率的国家视为战略优先事项。然而，尽管具有潜力，当前的人工智能系统仍存在严重缺陷：其稳健性和可靠性尚未足够先进，无法保证在高风险军事行动领域的可靠性能。

除其他风险外，与传统军事平台不同，人工智能系统极易受到网络攻击，这为黑客访问和操纵敏感军事数据或破坏军事行动提供了新的切入点。针对此类网络威胁的防御措施滞后，导致对手可以利用军事系统的漏洞。

随着各国继续将人工智能纳入常规军事系统，相关国家应该做好准备，应对对手将（而且很可能已经）通过威胁人工智能核心数据集并开发新颖的漏洞来利用人工智能模型弱点的风险。任何人工智能平台的集成都必须认识到它们很容易出现故障，包括为对手提供操纵的新切入点。此外，在各种常规军事系统的狭窄范围内整合人工智能——尤其是那些与核决策相关的系统，甚至是间接的系统——可能会在核领域产生不可预见的影响。因此，各国应采取基于风险的战略，制定指标来评估漏洞将如何影响人工智能集成领域。

当前人工智能系统产生的网络漏洞

当前人工智能系统中存在的漏洞，为黑客破坏数据完整性、损害机密性和破坏可用性打开了大门，从而导致错误结果、数据泄露和系统故障。

完整性攻击是最普遍的网络攻击

形式，旨在欺骗人工智能系统做出错误的决策。在数据中毒的情况下，攻击者操纵训练数据，导致人工智能学习错误的模式。在军事平台中，这些操纵可能会导致一系列情况，从未能识别正确目标到灾难性失败，如将友军误认为敌方。逃逸技术是另一种完整性攻击，涉及利用模型中的缺陷，导致检测系统中的错误识别，即使是单个被篡改的数据点。一个例子是修改无人机图像数据，以伪装对手的移动导弹发射器。

通过机密性攻击，黑客推断出有关系统运行或其训练数据的受保护信息。由于某些军事模型训练所用的机密或敏感数据被泄露，这些攻击可能会导致严重的安全漏洞。随着对底层模型的更多了解，会发现更多的漏洞，其中可能包括欺骗检测功能的方法。

最后，可用性攻击，包括拒绝服务（DoS）和勒索软件，旨在削弱关键系统的可用性。在军事背景下，这可能意味着扰乱管理物流和供应链的人工智能系统，导致关键时刻供应短缺。这些攻击方法并不是人工智能系统独有的，尽管它们仍然构成威胁。

网络攻击因其易于执行、依赖广泛的人工智能漏洞，以及防御此类攻击的挑战而成为一个令人担忧的趋势。执行网络攻击通常需要比设计和训练这些系统所需的专业知识和资源更少的专业知识和资源。由于人工智能对故障的恢复能力经常需要在性能上做出妥协，这一事实加剧了这种不平衡。因此，这种权衡可能会解决特定的漏洞，但同时可能会无意中放大其他漏洞，为攻击者提供利用新漏洞的机会。

对全球稳定的影响

随着各国加大在常规军事系统中部署人工智能技术的力度，毫无疑问，对手可能会寻求识别和利用这些系统中的漏洞，特别是在冲突前的情况下。鉴于俄罗斯等对手积极从事网络行动，这对西方防御系统的影响是巨大的。这些国家向网络战投入了大量资源。

例如，俄罗斯利用网络行动来控制本国民众并影响敌对国家的政治格局，其对 2016 年美国总统选举的干预就证明了这一点。这些行动表明俄罗斯有能力利用网络策略破坏其他国家的稳定。

由于网络攻击可能来自非国家行为者，以及可能想要破坏西方防御系统的资源明显较少的国家，威胁形势进一步恶化。鉴于执行人工智能系统渗透的障碍相对较低，而且不一定需要大量资源或专业知识，因此存在非国家行为者可能损害军事行动的切实风险。

朝鲜等资源有限的国家也在这一领域表现活跃。朝鲜的网络攻击主要集中在间谍活动和金融犯罪上，以支持其军事能力并规避制裁。这表现为一种旨在获取经济收益和投射力量的战略网络行动运用。朝鲜正在寻求具有潜在军事应用的人工智能计划，并且已经使用人工智能来协助网络攻击行动，尽管制裁和资源限制对短期内发展强大的军事人工智能项目构成了重大障碍。

对于国家和非国家行为体来说，网络攻击可能是一种有吸引力且具有成本效益的替代方案，可以实现非对称优势并挑战技术更先进的对手。西方国家的对手可能已经在努力实现通过利用网络漏洞破坏军事人工智能平台的目标。

AI 和升级途径

在核领域，人工智能漏洞表明，在安全至关重要的领域依赖该技术是不稳定的，如核指挥、控制和通信（NC3）系统。但即使拥有核武器国家对于将人工智能纳入 NC3 的关键功能犹豫不决，常规军事平台中广泛采用人工智能，仍可能对核风险产生意想不到的下游影响。

人工智能集成到常规军事系统或情报平台中的总体效应可能会导致核领域产生不可预测的影响。此外，通过网络攻击进行的对抗性干扰可能会导致大规模欺骗，进而导致广泛的误判和误解。例如，如果输入 NC3 的人工智能情报和监视系统遭渗透，正在处理和转发的信息的完整性就会受到威胁。这可能会导致对迫在眉睫的威胁的错误认知或对对手行为的误解，从而可能引发意外或升级的反应。在地缘政治不稳定的环境中，这种误判可能会增加无意或意外升级的风险。

此外，间接影响 NC3 的欺骗性因素可能会给利用网络攻击能力的对手带来优势，诱使一方将先发制人的打击视为对抗或减轻感知威胁的可行策略。

此外，高度联网化的军事系统如果被对手利用，可能会导致灾难性的级联故障。这些失败削弱了常规威慑能力，在极端情况下，可能迫使一个国家考虑将有限的核反应作为恢复威慑的最后手段。

结论

鉴于这些考虑，西方国防机构必须适应网络威胁不仅无处不在，而且随着人工智能技术的融合而不断演变的安全环境。这些技术的整合必须极其谨慎，特别是当网络威胁变得更加复杂和普遍时。

为解决此问题，这些国家必须通过制定基于网络风险的指标来为人工智能的军事应用制定明确的指导方针。这些指标应评估网络漏洞如何影响军事系统中的人工智能集成领域，强调人类监督的必要性，以及在出现异常情况时恢复手动控制的能力。与此同时，应该共同努力，通过有针对性的研究来加强网络防御，以抵御此类攻击。

不言而喻，由于涉及高风险，不应追求将人工智能集成到关键的 NC3 功能中。由于目前人工智能技术的不可靠性，核威慑系统受损的固有风险和潜在的灾难性后果，因此需要采取保守的方法。安

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。

欧盟关键基础设施网络安全防护体系政策法规研究

作者 国家工业信息安全发展研究中心 王丽颖

当前，网络空间已成为继海、陆、空、天之后的第五大主权领域空间，不仅事关经济安全和社会稳定，更是国际竞争与政治博弈的关键领域。同其他领土主权一样，保障网络空间安全就是保障国家安全。关键基础设施（以下简称“关基”）作为网络空间的“神经中枢”，其功能稳定与服务持续是维护国家安全和社会稳定的核心要素。以欧盟、美国和日本等为代表的国家纷纷出台相关战略规划、法律法规及实施方案，进一步加大对关基的网络安全保护力度。其中，欧盟较早认识到关基网络安全保护的重要性，陆续颁布《保护关键基础设施的欧洲计划》《欧盟网络安全战略》等一系列政策指令。尤其在协调成员国强化关基网络安全防护力度方面，欧盟更是加大工作力度。2022 年以来，欧盟又通过了《关于在整个欧盟全境实现高度统一网络安全措施的指令》《关于关键设施弹性的指令》《网络弹性法案》、关基保护蓝图、《数字运营弹性法案》及《人工智能法案》等多项政策，这些政策的实施将进一步提升关基网络安全防护能力和水平。

网络空间已成为继海、陆、空、天之后的第五大主权领域空间。
欧盟全面强调关基网络安全保护的重要性，陆续出台多项政策，
实行以风险管理为基础的网络安全治理策略。

一、搭建了一套较为完善的关基网络安全防护法律体系

欧盟全面强调关基网络安全保护的重要性，陆续出台多项政策，实行以风险管理为基础的网络安全治理策略。

一是 NIS 2 指令是欧盟关基网络安全防护的“基准线”。2022 年 12 月，欧洲议会和理事会共同通过了《关于在整个欧盟全境实现高度统一网络安全措施的指令》（NIS 2 指令），确定了整个欧盟关基的网络安全法律框架。NIS 2 指令作为欧盟关基网络安全防护的核心法规，构建了一套基于分级分类原则的网络安全防护体系。根据关基实体的重要性和规模上限要求，NIS 2 指令明确十类基本实体和六类重要实体，清晰界定受管辖范围和具体对象。针对不同类别的实体规定不同的网络安全风险管理和事件报

告要求，提高了关基网络安全防护的针对性，并规定了违规行为的具体惩罚措施，通过制定极高的罚款金额，倒逼关基实体提高对内生网络安全的重视。

二是 CER 指令是欧盟关基网络安全防护的“配套法则”。2022 年 12 月，欧盟通过了《关于关键设施弹性的指令》（CER），该指令明确了欧盟地区的关基领域主要涉及 11 个领域，并明确识别关基实体的考虑因素和安全义务。CER 指令是 NIS2 指令的“配套法则”，根据 CER 指令被确定为关基实体的重点行业企业和机构也将受到 NIS 2 指令的网络安全义务约束。同时，CER 和 NIS 2 指令下的国家主管部门必须定期合作和交换相关信息，如网络和非网络风险、威胁和事件等。

三是 CRA 法案是欧盟关基网络安全防护的“产品检验法”。2022 年 9 月，欧盟委员会发布《网络弹性法案》（CRA），该法案规定，特定关基实体必须使用经安全认证的信息和通信技术产品，进一步加强关基中数字产品的网络安全。CRA 法案是欧盟关基实体中软、硬件等数字产品的“检验法”，根据网络安全风险级别的不同，数字产品被划分为 I 类和 II 类，为产品制造商、进口商和分销商等主体设定了不同的网络安全评估要求，确保不同主体在数字产品供应链的网络安全中承担起各自的责任。

四是关基保护蓝图是欧盟关基网络安全防护的“国际协作指南”。2023 年 9 月，欧盟委员会提出“协调联盟层面行动以应对关键基础设施中断造成重大跨境影响的规划蓝图”（以下简称“关基保护蓝图”）。该蓝图旨在通过落实国内协调联动措施，提升国际联合应对能力，实施关基网络安全事件分类分级管理，以改善关基网络安全等危机造成的破坏性跨境影响，加大智能化响应能力，强化关基复原力，确保关基恢复的时效性和有效性。

五是 DORA 法案及 AI 法案是欧盟关基网络安全防护的“细分法则”。为配合 NIS 2 指令的落地与实施，欧盟在金融等特定关基领域中，制定了更为细致的法则。在金融领域，2022 年 11 月，欧盟理事会通过了《数字运营弹性法案》（DORA），主要针对金融领域中的关基实体，该法案由 DORA 主管部门与 NIS 2 指令下设的单一联络点（SPOCs）和计算机安全事件应急响应小组（CSIRT）协商并共享安全信息，以预防和减轻针对金融领域的网络威胁，确保金融实体的弹性运作。同时，就关基领域中的 AI 技术使用问题，2022 年 6 月，欧洲议会通过了《关于“欧洲议会和理事会条例：制定人工智能的统一规则（人工智能法案）并修订某些联盟立法”的提案》（以下简称“AI 法案”）。该法案将关基领域中的 AI 应用风险列为高风险，作为重点监管对象，并提出了具体的监管措施。

> NIS 2 指令、CER 指令、CRA 法案、关基保护蓝图、DORA 法案及 AI 法案分别是欧盟关基网络安全防护的“基准线”“配套法则”“产品检验法”“国际协作指南”“细分法则”。

二、明确关基实体范畴 确立分类分级的关基实体清单

一是清晰界定关基实体涉及的 11 个领域和范畴。欧盟 CER 指令中界定的关键实体指提供基本服务，维护关键社会职能、经济、确保公众健康和安全、环境的机构，具体包括能源、交通、银行、金融市场基础设施、医疗、供水、废水、数字基础设施、公共管理、太空、食品等 11 个领域。在这些领域内，CER 指令要求欧盟成员国详细梳理出本国的关基实体清单，并对其开展全面的安全风险评估。评估内容涉及两个主要方面：一是关基实体面临的各种风险，包括自然灾害人为事故、突发公共卫生事件、潜在的敌对威胁和恐怖主义活动等；二是关基实体提供的基础服务特性，以及这些服务对其他领域的依赖程度。一旦实体发生安全事件，它可能对所提供的基本服务或该领域其他基本服务产生重大破坏性影响。在梳理安全风险的过程中，还需考虑关基实体提供的基本服务的用户数量、其他部门对该服务的依赖程度、安全事件可能对经济、社会运转、

环境和公共安全造成的影响程度和持续时间等因素。此外，实体在基本服务领域所占的市场份额、可能受事件影响的地理区域、实体在维持基本服务水平方面的重要性，以及其他替代方案的可行性。

二是通过自主登记制度确定关基实体清单。为了进一步落实关基实体清单，NIS 2 指令敦促欧盟成员国在 2025 年 3 月前通过基本实体和重要实体的自我注册机制，形成关基管辖范围内的所有实体清单。该清单详细列出每个实体的名称、内部下属部门和分部门、地址、电子邮件和电话号码等联系信息，以及实体活跃的成员国名单。因此，NIS 2 指令按照“规模上限原则”，将未达到一定规模门槛的实体排除在管理范围之外。例如，员工数量少于 10 人、年收入 200 万欧元或以下的小型和微型企业被排除在外。然后根据这些实体的规模大小、所在领域和重要程度，分为基本实体和重要实体两类，其中基本实体包括能源、健康、交通、饮用水、废水、空间、公共政府、信息通信技术服务管理（B2B 商家对商家）、金融市场基础设施、银行业、数字基础设施（包括互联网服务提供商 ISP 和云）等。这类实体的员工数量通常为 250 人，年营业额为 50 万欧元或资产负债表为 43 万欧元。重要实体则包括数字供应商、研究、邮政和快递服务、食品生产与分销、制造业、化学品制造生产和分销、废弃物管理等，这类实体的员工数量通常为 50 人，年营业额为 10 万欧元或资产负债表为 10 万欧元。

三是根据网络安全风险级别划定关基中数字产品的不同类别。关基中使用的数字产品涵盖了各种软件和硬件产品，以及远程数据处理解决方案。CRA 根据产品存在网络安全风险的相关级别，分为三类“具有数字元素的关键产品”，即 I 类、II 类和默认类别。其中，关基中的数字产品涉及 I 类和 II 类，这两类产品须满足不同的网络安全要求。I 类产品包括 NIS 2 指令中描述的基本实体使用的集成电路和门阵列、移动设备和应用程序管理软件、远程访问软件、身份和访问管理软件、浏览器等。这些产品必须坚持应用标准或完成第三方评估以证明网络安全的符合性。II 类产品包括供 NIS 2 中描述的基本实体使用的工业物联网设备、供 NIS 2 中描述的基本实体使用的工业自动化和控制系统、智能电表、工业开关、安全元件、硬件安全模块、工业用防火墙等，须完成第三方符合性评估。

三、建立关基实体网络安全责任制 并明晰具体职责和义务

欧盟 CER 指令中界定的关键实体，具体包括能源、交通、银行、金融市场基础设施、医疗、供水、废水、数字基础设施、公共管理、太空、食品等 11 个领域。

一是确定关基实体的风险评估职责和义务。CER 指令规定，关基实体应开展安全风险评估，及时采取技术和组织等措施增强安全弹性，并向当局报告安全事件。欧盟成员国当局应向关基实体提供支持，对跨国和跨部门风险、最佳实践、方法、跨国培训

和演习活动等方面给予补充支持，并确保国家当局拥有权力和手段对关基实体进行现场检查，能够对不遵守指令的行为进行处罚。

二是规定关基实体承担网络安全管理责任、风险管理、事故通知等义务。NIS 2 指令提出了关基实体应承担的具体网络安全义务。在管理责任方面，基本实体和重要实体必须批准并监督网络安全措施的实施，对违规行为问责，并定期组织网络安全培训。在风险管理方面，基本实体和重要实体必须加强风险分析与信息系统安全，优化网络安全事故处理流程，采取备份、灾难恢复、危机管理等确保供应链安全和业务连续性，实施加密策略确保网络卫生。在事故通知方面，简化重大网络安全事件的报告义务，基本实体和重要实体须在 24 小时内向国家主管部门或 CSIRT 报告重大事件，72 小时内对事件严重性、影响等进行初步评估，1 个月内对事件详细信息、根本原因等进行总结上报。

三是规定关基中数字产品制造商、进货商和经销商等主体的不同义务。CRA 提出，关基中数字产品的规制主体包括制造商、进口商、分销商及其他必须履行法案规定义务的自然人或法人，并针对不同类型的主体施加了不同义务。其中，制造商对设计、开发和生产的数字产品需符合 CRA 规定的网络安全要求。经质量评估和网络安全评估后，制造商必须为产品张贴 CE 标志，并提供清晰、易懂、可理解和易读的产品随附信息和说明，以确保用户安全地安装、操作和使用。进口商需确认数字产品符合质量和网络安全要求，并在产品包装或随附文件中标明商家名称、注册商标、电子邮件等，并对产品的网络安全漏洞或事件承担报告义务。经销商则需要确保销售的数字产品带有 CE 标志，产品中包含制造商的随附信息和说明及进口商的联系信息等。

四是规定关基中高风险 AI 系统的网络安全义务。AI 法案针对关基中的高风险 AI 系统，从入市前到入市后，制定了全流程风险管理措施。在高风险 AI 系统投入市场前，AI 提供者应建立和维持风险管理系统，识别潜在的风险，确保人工可对 AI 系统进行监督，并干预存在“自动化偏见”的输出结果。投放入市时，AI 提供者需向主管机关提供 AI 系统开发过程、检测、运作和控制等系统相关必要信息，确保 AI 系统的性能符合预期目的及各项管理要求，并贴上 CE 标志。投入使用后，AI提供者应当建立入市后的检测系统，收集、记录和分析 AI 系统在整个生命周期的可靠性、性能和安全性等数据，评估 AI 系统对法规的持续遵守情况。当 AI 系统发生严重故障或侵犯人类基本权利的事件时，提供者需在 72 小时内向国家监督机构报告。

四、完善关基事件协调应对制度 以及时提升关基复原力

一是明确关基事件协调应对机制启用的触发条件。关基保护蓝图明确了触发联盟应对机制的两类重大关基事件：第一，对六个及以上成员国提供基本服务的关基造成破坏性影响；第二，对两个及以上成员国提供基本服务的关基造成破坏性影响，且理事会轮值主席国与其他成员国一致认为由于具有广泛且重大的技术或政治影响，需要联盟层面协调和响应的情况。通过设定联盟协同应对机制的触发条件，可以迅速精准地识别和理解关基面临的威胁程度，确定关基事件的优先级和紧急程度，合理分配不同等级资源，采取适宜的安全措施和防护策略。

二是构建分工明确的协调管理机制。关基保护蓝图建立了按照职责分工相互配合、层次分明的联盟协作应对体系。但当关基事件达到联盟应对机制的触发条件时，欧盟成员国、欧盟理事会、欧盟委员会、欧盟对外行动署（EEAS）等联盟机构及欧洲刑警组织等执法机构，应在关基保护蓝图框架内相互合作，通过固定的联络点交流事件信息并协调应对行动，这样可以最大程度地缓解关基事件带来的破坏性跨境影响，并及时恢复关基的正常运行。为了确保应对举措的有序性和应急性，上述参与者应联合关基运营商等私营企业定期演练联盟协调应对机制，不断优化国家、区域和联盟层面的协调响应能力。同时通过理顺职能部门和执法部门的职责关系，逐步构建并优化协同高效的多部门间应急履职体系。此外，完善突发事件应急流程，提高关基安全事件处置效率，并针对应急演练中发现的突出问题和漏洞隐患，及时整改加固，完善保护措施。

三是规定信息交换和公开沟通流程。关基保护蓝图提出针对重大关基事件启动联盟协调应对机制的第一步是确保所有相关者的信息交流及公共沟通的顺畅。发生重大关基事件后，由国家主管部门率先通过单独联络点与轮值主席国联络，交换关基运营主体及已采取的网络和物理措施等详情。欧盟应急协调反应中心（ERCC）作为危机应对业务部门，实时监控、协调和支持联盟层面的紧急情况，增强跨部门协调。与此同时，欧盟委员会立即组织召开关基恢复小组专家会，所在国家主管部门汇报重大关基事件

违反法律要求未履行及时报告义务、未实施网络安全风险管理措施的关基实体，基本实体将面临高达年营业额 2% 或 400 万欧元的罚款，重要实体将面临高达年营业额 1% 或 200 万欧元的罚款。

的性质、原因、影响、应对举措、对受影响成员国提供的技术支持等。欧盟委员会根据交换信息编写综合态势感知和分析报告（ISAA），包括从网络安全角度评估欧盟层面的风险情况及委员会等各机构采取的缓解举措，旨在提高联盟层面的透明度，以信息共享为基础，加强态势感知，积极构建欧盟成员国及委员会等相关方广泛参与的信息共享、协同联动的防护机制。

四是确定联盟协调应对和处理规则。关基保护蓝图提出针对重大关基事件启动联盟协调应对机制的第二步是基于关基事件的规模和影响而采取协调应对行动。欧盟理事会民事保护工作组关基恢复小组基于 ISAA 组织召开专家会议，搭建沟通平台，请求其他成员国或联盟机构的技术支持。其他成员国及欧洲刑警组织等机构评估可提供的技术支持以减轻重大关基事件的影响。在必要情况下，可配合启动快速警戒系统机制（ARGUS）、综合政策威胁响应机制（IPCR）、共同体民事保护机制（UCPM）等其他应急响应机制，请求更多成员国帮助并探讨协调应对举措。若涉及国际安全影响，EEAS 可召开欧盟——北约恢复结构性对话会议，交流欧盟和北约分别采取的有关措施，加强国家主管部门的响应及与其他成员国、联盟机构等的合作，做到统一指挥、快速调度，迅速解决关基中断问题并重建基本服务。另外，由欧盟理事会和委员会准备公共沟通话术，消除公众信息差，最大程度地减少重大关基事件后向公众传达的信息差异，避免虚假信息传播。

五、设立针对关基实体的惩罚制度 以倒逼网络安全水平提升

一是明确关基中基本实体和重要实体违规的惩罚举措。NIS 2 指令对违反法律要求未履行及时报告义务、未实施网络安全风险管理措施的关基实体提出了严格的惩罚举措，基本实体将面临高达年营业额 2% 或 400 万欧元的罚款，重要实体将面临高达年营业额 1% 或 200 万欧元的罚款，二者均以较高者为准，这一举措旨在提高关基实体对内生网络安全的重视。

二是明确关基中使用违规数字产品的惩罚举措。关基中使用的数字产品，如果违反 CRA 规定的网络安全要求和制造商义务，将面临最高 1500 万欧元或上一财政年度全球年营业额的 2.5% 的罚款，以较高者为准。若违反其他义务，将面临最高 1000 万欧元或上一财政年度全球年营业额 2% 的罚款，以较高者为准。若向指定机构和市场监督机构提供不准确、不完整或误导性的信息，将受到最高 500 万欧元或上一财政年度全球年营业额的 1% 的罚款，同样以较高者为准。安

（《中国信息安全》杂志 2024 年第 1 期）

包以德循环：加快网络安全响应的军事模型

作者　埃泰 · 马奥尔

防御者和事件响应者可以将包以德循环（OODA Loop）用于各种用例，如威胁评估、威胁监控和威胁搜寻。

时间是宝贵的商品，尤其是在网络安全领域。网络犯罪分子可以在初次侵入系统后 24 小时内进出受害者环境。专业网络犯罪分子和高级持续性威胁 (APT) 利用 0 day 漏洞，很容易使软件开发人员毫无头绪。

当网络攻击发生时，防御者只有几分钟的时间来检测和响应。检测速度越快，就能越早阻止病毒传播。反应时间越快，就能越早战胜敌人。为了赢得这场与时间的竞赛，防御者需要两件事：1）强大的决策模型，有助于快速而准确地做出决策；2）对整个基础设施进行实时状态检查，使安全团队有机会做出明智的决策。

OODA Loop 军事模型及其安全应用

包以德循环是空军战略家约翰 · 博伊德上校在 20 世纪中叶开发的一种军事心理模型，旨在提高战斗机飞行员在空战中的决策技能。

包以德循环由四个迭代阶段组成：观察、定向、决策和行动。“观察”是指全面了解情况。“定向”意味着联系现实，避免认知偏差，深入了解形势及其背景。“决定”意味着根据观察做出决定，但不急于下结论。“行动”是指执行或按照所做的决定采取行动。

包以德循环是一种通用模型，显然可以应用于网络安全。防御者（和事件响应者）可以将其用于各种用例，如威胁评估、威胁监控和威胁搜寻。包以德循环的成功很大程度上取决于用于决策的安全信号和数据的质量。换句话说，质量差的数据等于糟糕的决策，反之亦然。

使用 SASE 来利用包以德循环

安全复杂性是有效及时检测威胁的最大障碍之一。部署许多不同的安全工具（平均 45 ~ 75 个）来解决大量威胁向量和安全用例是常见的做法。因此，安全工具无法“连接各个点”，无法生成及时、准确和上下文相关的安全数据来进行有效的决策。由于数据和应用程序与远程工作的用户一起转移到云端，因此安全团队无法洞察或控制数据的盲点。

SASE 是一种单通道、云原生架构，通过将多个安全控制（如数据泄漏防护、安全 Web 网关、零信任网络访问、云访问安全代理和其他控制）融合到单个服务中来解决复杂性问题。整合的安全工具和本机集成可实现跨端点、多云、应用程序、身份、设备和物联网的网络流量的实时可见性。然后，通过位置和身份等上下文详细信息丰富实时数据，从而使安全团队能够进行更精细的安全控制和更明智的决策。SASE 主干网还可以通过虚拟补丁对零日攻击进行即时威胁响应。换句话说，SASE 显著增强了 OODA 循环过程，因为它可以查看所有网络流（“观察”），将其接收到的所有数据置于上下文中（“定向”），调用需要应用的策略（“决定”），并且在整个基础设施中端到端地执行策略（“法案”）。

最后的想法

包以德循环专为在高压力情况下快速做出决策而设计，这是任何安全团队都熟悉的领域。由于威胁日益复杂，因此需要更快的响应时间；控制和可见性变得更加紧迫。关键是对所有数据及其上下文具有这种可见性。通过丰富上下文数据，安全团队可以做出明智的策略决策。一致地执行这些策略需要融合安全功能。通过单通道处理，安全团队可以做出明智的数据驱动决策，立即执行正确的策略，加速实现所需的安全结果，并快速实现网络弹性。安

关于作者

埃泰 · 马奥尔（ Etay Maor ）

Cato Networks 安全战略高级总监。此前，曾担任 IntSights 首席安全官，并在 IBM 和 RSA Security 的网络威胁研究实验室担任高级安全职位。

奇安信

敏感信息泄露情报服务

- 攻击队视角的全网敏感信息情报
- 急需补上的防守盲点
- 供应链安全的管控抓手
- 预防性进攻反制利器

纵深防御的马奇诺防线，为什么会被攻破？

- 完整的防御体系，既要考虑正面防御，侧翼的情报收集和对抗也必不可少！
- 忽视全网视角的情报，是防守的重大盲点！

服务定位 SERVICE POSITIONING

- **攻击队视角**：使用渗透专家交付，不是简单的信息收集。
- **全网视角**：核心功能是从外部探测全互联网第三方应用中的敏感泄露数据；而非只关心自己的网络和应用。
- **情报级**：专家梳理的情报级信息，而不是简单数据抓取：给出利用思路和可能的攻击链，更有详细的整改建议。

奇安信安服团队

奇安信
新一代网络安全领军者

「零事故」安服团队重磅力作

900余次实战攻防演练的经验总结
从红队、蓝队、紫队视角全面解读攻防演练

扫码购买

奇安信连续三年位居
“中国网安产业竞争力50强”
第一名

6月20日，中国网络安全产业联盟（CCIA）
公布“2023年中国网安产业竞争力50强”榜单，
凭借扎实的技术实力和领先的市场表现，
奇安信连续三年高居榜单第一名。

“2022年中国网安产业竞争力50强”榜单

TOP15	公司名称
1	**奇安信科技集团股份有限公司**
2	深信服科技股份有限公司
3	启明星辰信息技术集团股份有限公司
4	华为技术有限公司
5	天融信科技集团股份有限公司
6	绿盟科技集团股份有限公司
7	腾讯云计算（北京）有限责任公司
8	新华三技术有限公司
9	阿里云计算有限公司
10	杭州安恒信息技术股份有限公司
11	三六零数字安全科技集团有限公司
12	亚信安全科技股份有限公司
13	中电科网络安全科技股份有限公司
14	杭州迪普科技股份有限公司
15	山石网科通信技术股份有限公司