内部资料 免费交流

出版物准印证号：京内资准字 2122- L0058 号

SECURITY INSIDER

网安26号院

奇安信网络安全通讯

大模型安全该怎么办？ P13

第35期
2023 年 11 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。

人工智能需要踩踩刹车吗?

11 月份，科技领域最受关注的新闻，可能要算 OpenAI 公司的管理层戏剧性震荡了。

11 月 17 日，OpenAI 公司 CEO 山姆 · 奥特曼突然被董事会解职，此举震惊了 OpenAI 员工和科技行业的其他人士，包括已向 OpenAI 投资 130 亿美元的微软公司。这次事件的严重程度不亚于 1985 年乔布斯被迫离开苹果公司。

ChatGPT 的火爆让 OpenAI 成为科技行业最有价值初创企业之一。山姆 · 奥特曼，这位从来没有在 OpenAI 拿薪水、持有股份的 CEO，凭借 ChatGPT 成为成为人工智能时代的代言人。

OpenAI 董事会没有说明解雇奥特曼的具体原因，只是在声明中表示，山姆 · 奥特曼与董事会的沟通中始终不坦诚，阻碍了董事会履行职责的能力。但据知情人士透露，OpenAI 联合创始人、公司首席科学家 Ilya Sutskever 越来越担心 OpenAI 的人工智能技术可能存在的危险，而山姆 · 奥特曼没有对这种风险给予足够的重视。尽管 Ilya Sutskever 在 X 平台发帖称后悔参与董事会的行动，但声称有必要保护 OpenAI 让人工智能造福人类的使命。

就在不久前，山姆 · 奥特曼还雄心勃勃地宣布，OpenAI 正在稳步推进 GPT-5 的开发，标志着人工智能进步的巨大飞跃。这与 OpenAI 董事会希望在开发人工智能技术时谨慎行事形成鲜明对比。

这一戏剧性的事件，引发了人们聚焦人工智能的快速增长与安全之间的争议——人工智能究竟是一代人中最大的商机，还是会带来难以控制的危险？随着人工智能技术变得更加强大、监管机构开始针对人工智能加强监管，这种加速论者”和“末日论者”之间的争论必将愈演愈烈。

大多数科技人员认为，AI 技术快速进步带来的好处多于坏处。但对人工智能快速发展的担心日益增长，越来越多的政府机构与科技人士对 AI 的武器化，以至于人类无法控制的恐惧，推动防范人工智能风险成为全球优先事项。

人工智能被恶意应用造成的各种社会风险，可能需要未来去验证，但近期国内某大模型生成出不符合主流价值观的内容；ChatGPT 遭拒绝服务攻击发生大面积瘫痪等事实说明，研究人员所描述的大模型安全风险不是空穴来风，必将逐一得到展现。

在不久前举办的中美两国元首会晤，确定推动和加强中美在人工智能等重要领域加强合作，建立人工智能政府间对话。这意味着，以人工智能为代表的技术治理正在成为全球治理的重要方向。

现在是需要对人工智能的发展踩踩刹车吗？ 或许即使不去踩刹车，确保安全可信也应该是我们发展和采用人工智能所必须遵循的基本原则。

总编辑

李建平

2023 年 11 月 1 日

CONTENTS 目录

安全态势

月度专题

大模型安全该怎么办？P13

人工智能成为中美元首会晤的内容；受分布式拒绝服务攻击，OpenAI 的 ChatGPT 和 API（第三方应用接口）突发严重停机，大模型安全风险首次真实显现。大模型到底有哪些风险，该怎么应对？本期专题将详解大模型安全风险、国际治理趋势与应对方案。

《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
攻防一线主编：魏开元
安全之道主编：张少波
安全叨客主编：魏开元
奇安资讯主编：陈　冲
报告速递主编：闫　延
专　栏主编：李建平

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：2023 年 11 月 26 日

政策篇

国内，多个部门发布新的网络安全政策文件公开征求意见，包括《会计师事务所数据安全管理暂行办法》《工业互联网安全分类分级管理办法》《电子政务电子认证服务管理办法》等；

国际上，美国政府签署发布《关于安全、可靠和可信地开发和使用人工智能的行政令》，要求对 AI 开展新的安全评估和指导，英国也举办了首届 AI 安全峰会并通过《布莱奇利宣言》，全球 AI 治理正进入白热化阶段。

国内

四部门联合发布《智能网联汽车准入和上路通行试点实施指南（试行）》

11 月 17 日工信部官网消息，工业和信息化部、公安部、住房和城乡建设部、交通运输部等四部门联合发布《智能网联汽车准入和上路通行试点实施指南（试行）》（以下简称《指南》）。《指南》包括智能网联汽车准入、使用主体、上路通行、试点暂停与退出四个部分。《指南》对智能网联汽车生产企业、智能网联汽车产品提出了一系列网络安全和数据安全要求。智能网联汽车生产企业需在设计验证能力、安全保障能力、安全监测能力、用户告知机制等方面具备相关机制和措施，智能网联汽车产品需在产品技术要求、过程保障要求、测试验证要求等方面具备相关机制和措施。《指南》还要求，试点使用主体需具备网络安全和数据安全保障能力，并参照汽车生产企业要求执行。

《会计师事务所数据安全管理暂行办法》公开征求意见

11 月 13 日财政部官网消息，财政部、国家网信办联合起草了《会计师事务所数据安全管理暂行办法（征求意见稿）》，以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 6 章 36 条，包括总则、数据管理、网络管理、监督检查、附则。该文件提出，会计师事务所的首席合伙人（主任会计师）是本所数据安全负责人。该文件要求，会计师事务所应按照相关要求确定核心数据、重要数据和一般数据。针对核心数据，应当通过专用服务器或者会计师事务所私有云平台设置内部专门空间存储，使用加密虚拟专用网络等技术手段传输；针对重要数据，应将其存放于和互联网逻辑隔离的信息系统中，并严格控制接触人员范围；针对一般数据，应采取基于用户角色的授权访问控制，并且按照最小权限原则授权。

证监会发布《证券期货业信息安全运营管理指南》行业标准

10 月 27 日“证监会发布”公众号消息，证监会发布《证券期货业信息安全运营管理指南》金融行业标准，自公布之日起实施。该文件给出了信息安全运营管理过程中基础安全、信息资产、漏洞、开发安全、数据安全等方面的管理思路和方法，并给出了各管理域的度量指标及行业最佳实践。标准的制定实施可有效指导行业机构建立完善的安全运营体系和流程，规范信息安全运营管理过程，推动相关安全措施的有效实施和持续改进。

工信部《工业互联网安全分类分级管理办法》公开征求意见

10 月 24 日工信部官网消息，工业和信息化部起草了

《工业互联网安全分类分级管理办法（公开征求意见稿）》，现公开征求意见。该文件提出，工业互联网安全分类分级管理工作遵循统筹指导、分类施策、分级防护、突出重点的原则，指导企业提升安全防护能力。工业互联网企业安全级别由高到低分为三级、二级、一级，三级工业互联网企业每年至少开展一次评测，二级工业互联网企业每两年至少开展一次评测，一级工业互联网企业可参照二级工业互联网企业相关要求开展评测。该文件还对工业互联网企业的安全管理制度、监测预警和信息通报、应急处置和演练、检查评估等提出了细化要求。

国家密码管理局《电子政务电子认证服务管理办法》公开征求意见

10 月 17 日国家密码管理局官网消息，国家密码管理局研究起草了《电子政务电子认证服务管理办法（征求意见稿）》（以下简称“征求意见稿”），现公开征求意见。征求意见稿共 6 章 44 条，包括总则、资质认定、行为规范、监督管理、法律责任和附则。征求意见稿对电子政务电子认证服务的服务范围、业务规则、服务内容、证书内容与格式、证书申请与审核、密码使用安全与互信互认、保密义务、信息保存、合规性评估、投诉处理、岗位培训和业务终止与承接等提出了一系列规范要求。

国际

欧洲议会通过《数据法案》，明确数据访问与使用规则

11 月 9 日欧洲议会官网消息，欧洲议会投票通过《数据法案》（Data Act）。该法案旨在明确数据访问、共享和使用的规则，规定获取数据的主体和条件，使更多私营和公共实体能够共享数据。法案对商业秘密、商业秘密持有者进行定义，以防止非法数据传输和数据泄露到数据保护法规较弱的国家。法案推动提升了不同云服务商之间进行转移的能力，并提出防范云服务商非法跨境数据传输的防范措施。该法案需要欧洲理事会正式批准才能成为法律。

美国白宫发布《关于安全、可靠和可信地开发和使用人工智能的行政令》

10 月 30 日美国白宫官网消息，美国总统拜登签署了《关于安全、可靠和可信地开发和使用人工智能的行政令》，推出白宫有关生成式人工智能的首套监管规定，要求对人工智能进行新的安全评估、公平和民权指引，以及对劳动力市场影响的研究。该行政令要求，大公司在人工智能系统正式发布之前与美国政府分享安全测试结果。它还要求优先考虑使用 NIST 制定的人工智能“红队”标准，即对系统内的防御和潜在问题进行压力测试。美国商务部将制定为人工智能生成的内容加水印的标准。

欧盟《网络弹性法案》提案拟为开源软件安全监管设定规则

10 月 30 日 Euractiv 消息，欧盟政策制定者已就《网络弹性法案》提案的开源软件安全监管初步达成一致意见。该法案最新版本提出一套分层监管方法，针对三类开源软件项目制定了对应的义务。一是商业实体独立开发并控制的开源软件，需履行《网络弹性法案》包括基本要求、技术文档、合规标志等在内的所有义务，未履行义务将会被处罚；二是在支持组织（开源软件基金会或管理员）保护下协作开发的，需履行明确但少量的义务，如制定并推动漏洞处理流程，这类开发者将不会被处罚；三是没有单一实体控制完全协作开发的，将不受《网络弹性法案》管理。

美国 FTC 修改保障规则，要求非银行金融机构上报数据泄露事件

10 月 27 日 FTC 官网消息，美国联邦贸易委员会（FTC）已批准保障规则的修正版，要求非银行金融机构在 30 天内报告数据泄露和安全事件。该规定适用于抵押贷款经纪公司、汽车经销商（汽车金融）和发薪贷款机构等非银行金融机构，将于明年 4 月生效。该规定要求，如果发现涉及 500 名以上消费者信息的安全漏洞，机构必须在 30 天内向联邦贸易委员会报告事件；如果未加密的消费者信息遭到未授权访问，则需要向消费者通知事件。

事件篇

全球发生多起涉及中国企业的网络安全事件。一家汽车零部件厂商的北美公司被黑，导致下游的汽车巨头生产受到扰乱；一家国有银行的美国子公司遭到勒索攻击，导致部分系统中断服务；一家跨境电商公司的数据库在公网暴露，导致大量公民隐私可被任意访问。

因中国供应商被黑，汽车巨头斯特兰蒂斯工厂生产受扰乱

11 月 13 日底特律新闻消息，全球知名车企斯特兰蒂斯集团（Stellantis）表示，由于一家供应商遭受网络攻击，集团运营受到干扰，旗下克莱斯勒、道奇、吉普和公羊等品牌的车型的生产受到影响。这次网络攻击主要影响的是中国供应商 Yanfeng International Automotive Technology Co. Ltd.。当天晚间，该公司官网无法访问。Yanfeng 公司的北美总部位于密歇根州诺维，公司生产多种汽车零部件，包括座椅、内饰、电子设备和其他组件。斯特兰蒂斯发言人 Anne Marie Fortunate 发表声明称，“由于一家外部供应商出现问题，斯特兰蒂斯集团位于北美的部分装配厂生产受到干扰。我们正在监控情况并与供应商合作，减轻事件对我们运营的进一步影响。”

网络攻击迫使澳大利亚港务巨头环球港务运营停摆

11 月 12 日央视财经公众号消息，由于发生网络安全事件，澳大利亚第二大港口运营商“澳大利亚环球港务集团”运营已经停摆。从 10 日开始，集团在墨尔本、悉尼、布里斯班等主要城市的港口货物运输受到严重影响。12 日，集团表示，正在测试货运系统运行，港口何时恢复正常作业尚不清楚。据悉，目前货船仍可以卸货，但运输集装箱的卡车无法正常进出港。12 日，澳大利亚多个政府部门和机构举行会谈，继续商讨应对措施。澳大利亚警方正在对这起网络安全事件展开调查，在调查期间各主要港口的业务受到限制。据澳大利亚媒体报道，码头运营方尚未收到赎金要求，暂时还没有组织宣称对本次网络攻击负责。

ChatGPT 遭黑客组织 DDoS 攻击，导致服务大面积瘫痪

11 月 9 日 BleepingComputer 消息，OpenAI 官方确认，旗下服务由于遭遇 DDoS 攻击，发生大规模服务中断，导致其 API 和 ChatGPT 服务在过去 24 小时内遭受了“周期性中断”。虽然 OpenAI 并未透露 DDoS 攻击的来源，但是一个名为“苏丹匿名者”的黑客组织在 8 日声称对这些攻击负责，攻击原因是 OpenAI“对以色列的袒护以及反对巴勒斯坦”。“苏丹匿名者”还确认在这些攻击中使用了 SkyNet 机器人网络，该网络自 10 月以来一直在提供“压力测试服务”，并于日前增加了对应用层的 DDoS 攻击能力。

美国抵押贷巨头遭网络攻击：数百万用户无法还款 或影响信用评级

11 月 7 日纽约时报消息，美国最大的非银行抵押贷款服务商之一库珀集团（Mr. Cooper）在 10 月 31 日遭受网络攻击，导致数百万用户的贷款支付和其他交易中断。库珀集团 11 月 6 日下午表示，已经恢复了在线支付系统，并向用户提供电话、邮件、西联汇款等多种支付业务。针对社交媒体上用户投诉的支付问题，该公司发表声明称，在网络攻击期间如用户未能按期付款，不会产生费用或负面信用记录。信用评级公司穆迪表示正在监控这一事件，评估其影响。

中国跨境电商暴露数百万用户隐私数据，部分含身份证照片

11 月 6 日 TechCrunch 消息，云安全公司 CloudDefense.ai 的安全研究员 Viktor Markopoulos 发现，由于一家电商店铺数据库暴露在互联网上，数百万中国公民的身份证号码遭泄露。他表示，该数据库属于 Zhefengle，这家中国电商店铺专门从国外进口商品（经查询，zhefengle.com 网站隶属一家杭州公司）。数据库包含了从 2015 年至 2020 年的超过 330 万订单，包括用户的收货地址、电话号码、身份证号码，许多订单还存有用户的身份证复印件，没有受到密码保护，可以任意访问。尚不清楚这个数据库暴露了多长时间，外媒联络后不久该电商修复了漏洞。

德国爆发大规模勒索软件攻击，超 70 个城市市政服务瘫痪

11 月 1 日 The Record 消息，德国西部日前发生大规模勒索软件攻击，多个城市和地区的地方政府服务陷入瘫痪。10 月 30 日早上，德国地方市政服务商 Südwestfalen IT 公司的服务器被未知的黑客团伙加密，为阻止恶意软件传播，该公司限制了 70 多个城市对基础设施的访问权限。受限城市主要位于德国西部的北莱茵－威斯特法伦州，该地区几乎所有市政府都受到这次黑客攻击的影响。该公司在临时网站上发表声明称，这次攻击令地方政府服务“严重受限”。攻击当天，德国城市锡根大部分 IT 系统停止运行，市政府被迫取消与市民对话活动。德国警方和网络安全机构正在调查此次黑客攻击，努力帮助市政管理部门恢复服务。

国家安全部：数百个非法涉外气象探测站点向境外传输数据

10 月 31 日国家安全部消息，国家安全部公众号发布文章《国家安全机关会同有关部门开展涉外气象探测专项治理》称，发现数百个非法涉外气象探测站点实时向境外传输气象数据，广泛分布在全国 20 多个省份，对我国家安全造成风险隐患。这些非法涉外气象探测站点，有的探测项目受境外政府直接资助，部分观测点设立在军事单位、军工企业等敏感场所周边，进行海拔核准和 GPS 定位；有的布设在我主要粮食产区，关联分析我农作物生长和粮食产量；有的甚至长时间、高频次、多点位实时传输至外国官方气象机构，服务于外国国土安全和气象监测。国家安全机关联合气象、保密部门，依法对相关非法活动进行查处，及时阻断气象数据出境的违法行为。

Okta 业务系统被黑导致客户遭入侵，公司股价暴跌 11%

10 月 20 日 Bleeping Computer 消息，国际身份软件巨头 Okta 发布公告称，攻击者使用窃取的凭证入侵其支持管理系统，访问了包含客户上传的 Cookie 和会话令牌的文件。攻击者利用泄露数据进一步侵入了客户网络，目前已知 ByondTrust、Cloudflare 两家使用 Okta 服务的公司受到影响。事件曝光后，Okta 股票在上周五收盘时下跌了 11%。Okta 已通知所有受事件影响的客户。这一事件不影响生产 Okta 服务和 Auth0/CIC 案例管理系统。

超过 4 万台思科设备被植入后门账号：0day 漏洞攻击，暴露即被黑

10 月 19 日 Bleeping Computer 消息，美国思科公司 10 月 16 日发布警告称，黑客正在利用 0day 漏洞（CVE-2023-20198）攻击该公司的 IOS XE 软件设备。根据思科提供的感染指标（IoCs），网络测绘平台 Censys 在 10 月 18 日发现，公网上受感染设备数量已经增长到 41,983 台。网络测绘平台 Shodan 数据显示，在公网暴露的此类系统数量略大于 145,000 台，其中大多数位于美国。运行思科 IOS XE 的网络设备包括企业交换机、工业路由器、接入点、无线控制器、聚合设备和分支路由器。

漏洞篇

近期，思科 IOS XE 软件曝出 0day 漏洞 CVE-2023-20198。该漏洞此前遭到在野利用，官方披露后由于利用简单和暂无补丁，更是遭到疯狂滥用。互联网似乎进入了“黑暗森林”模式，至少 4 万台暴露的思科设备被劫持控制。

Google Chrome 信息泄露漏洞安全风险通告

11 月 17 日，奇安信 CERT 监测到 Google Chrome 浏览器信息泄露漏洞 (CVE-2023-4357)。该漏洞的存在是由于Google Chrome中用户提供的XML输入验证不足，远程攻击者可以创建特制网页，诱骗受害者访问该网页并获取用户系统上的敏感信息。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

金蝶云星空私有云任意文件上传漏洞安全风险通告

11 月 16 日，奇安信 CERT 监测到金蝶云星空私有云任意文件上传漏洞 (QVD-2023-44581)PoC 及 EXP 在互联网上流传，该漏洞允许未授权的远程攻击者上传任意文件，最终可能导致远程执行恶意命令，控制服务器等。目前，奇安信 CERT 已复现此漏洞，经研判该漏洞攻击利用难度低，且 EXP 已公开，被恶意利用的可能性增大。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Microsoft WordPad 信息泄露漏洞安全风险通告

11 月 1 日，奇安信 CERT 监测到 Microsoft WordPad 信息泄露漏洞 (CVE-2023-36563)，WordPad 在解析 rtf 文件包含的 ole 对象时会尝试访问 Linked object 的 Topic 指向的文件，如果 Topic 是一个 UNC 路径，则会尝试通过网络访问，并尝试使用 NTLM 认证，导致泄露 NTLM hash。鉴于该漏洞影响范围较大，并且已经监测到在野利用，建议客户尽快做好自查及防护。

Atlassian Confluence Data Center&Server 授权不当漏洞安全风险通告

10 月 31 日，奇安信 CERT 监测到 Atlassian 官方发布 Atlassian Confluence Data Center&Server 授权不当漏洞 (CVE-2023-22518) 公告，未经身份认证的远程攻击者可利用此漏洞破坏服务端的可用性及完整性，可能造成拒绝服务等影响。鉴于此产品用量较大，建议客户尽快做好自查及防护。

F5 BIG-IP 远程代码执行漏洞安全风险通告

10 月 27 日，奇安信 CERT 监测到 F5 BIG-IP 远程代码执行漏洞 (CVE-2023-46747)，未经授权的远程攻击者通过管理端口或自身 IP 地址访问 BIG-IP 系统，利用此漏洞可能绕过身份认证，导致在暴露流量管理用户界面（TMUI）的 F5 BIG-IP 实例上执行任意代码。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Squid 拒绝服务漏洞安全风险通告

10 月 26 日，奇安信 CERT 监测到官方发布 Squid 拒绝服务漏洞 (QVD-2023-30699) 公告。当 Squid 配置为接受 HTTP 摘要认证时，可能允许远程客户端执行缓冲区

溢出攻击，将高达 2MB 的任意数据写入堆内存，从而导致对 Squid 代理的所有用户的拒绝服务攻击。奇安信 CERT 已复现此漏洞，鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Apache ActiveMQ 远程代码执行漏洞安全风险通告

10 月 25 日，奇安信 CERT 监测到 Apache ActiveMQ 远程代码执行漏洞 (QVD-2023-30790) 技术细节在互联网上公开。Apache ActiveMQ 中存在远程代码执行漏洞，具有 Apache ActiveMQ 服务器 TCP 端口（默认为 61616）访问权限的远程攻击者可以通过发送恶意数据到服务器从而执行任意代码。鉴于此漏洞利用简单，产品用量较大，并已存在在野利用，建议客户尽快做好自查及防护。

VMware vCenter Server 越界写入漏洞安全风险通告

10 月 25 日，奇安信 CERT 监测到 VMware vCenter Server 越界写入漏洞 (CVE-2023-34048)。VMware vCenter Server 存在越界写入漏洞，具有 vCenter Server 网络访问权限的远程攻击者可以利用该漏洞在目标系统上执行任意代码。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Cisco IOS XE Web UI 命令执行漏洞安全风险通告

10 月 21 日，奇安信 CERT 监测到 Cisco IOS XE Web UI 权限提升漏洞 (CVE-2023-20273) 存在在野利用。当 Cisco IOS XE 软件的 Web UI 暴露于互联网或不受信任的网络时，具有管理员权限的攻击者可以利用该漏洞在目标系统上执行任意命令。鉴于该产品用量较多且存在在野利用，建议客户尽快做好自查及防护。

NetScaler ADC 和 NetScaler Gateway 敏感信息泄露漏洞安全风险通告

10 月 19 日，奇安信 CERT 监测到 Citrix 官方更新安全公告说明 NetScaler ADC 和 NetScaler Gateway 敏感信息泄露漏洞 (CVE-2023-4966) 存在在野利用。远程未授权攻击者可通过越界读写利用此漏洞最终可能造成敏感信息泄露，利用此漏洞无需额外条件。鉴于此漏洞影响范围较大，且已监测到在野利用，建议客户尽快做好自查及防护。

致远 OA XML 外部实体注入漏洞安全风险通告

10 月 17 日，奇安信 CERT 监测到致远 OA XML 外部实体注入漏洞 (QVD-2023-30027) 技术细节。致远 OA 的金格控件存在 XML 外部实体注入漏洞，攻击者利用该漏洞可导致任意文件读取，配合后端 S1 服务中 H2 RCE 可达到远程未授权攻击者在目标服务器上执行任意代码。目前已监测到在野利用，同时奇安信 CERT 已分析并复现此漏洞，鉴于漏洞利用难度较低，建议客户尽快做好自查及防护。

Cisco IOS XE Web UI 权限提升漏洞安全风险通告

10 月 17 日，奇安信 CERT 监测到 Cisco IOS XE 软件 Web UI 权限提升漏洞 (CVE-2023-20198) 存在在野利用。当 Cisco IOS XE 软件的 Web UI 暴露于互联网或不受信任的网络时，未经身份验证的远程攻击者可以利用该漏洞在受影响的系统上创建具有 15 级访问权限的账户。攻击者可以利用该账户来控制受影响的系统。鉴于该产品用量较多且存在在野利用，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 10 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

2023年10月，奇安信Z-TEAM团队共承接攻防演习服务 14 场，其中省级攻防演习 2 场，省级行业攻防演习 1 场，客户自主攻防演习 11 场。

本月承接攻防演习数量与上月对比呈明显下降趋势（见图 1）。

本月承接的攻防演习涉及企业、政府部委、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变化不大，政府部委和企业行业攻防演习数量明显趋少（见图 2）。

本月攻防演习成果如表 1 所示：

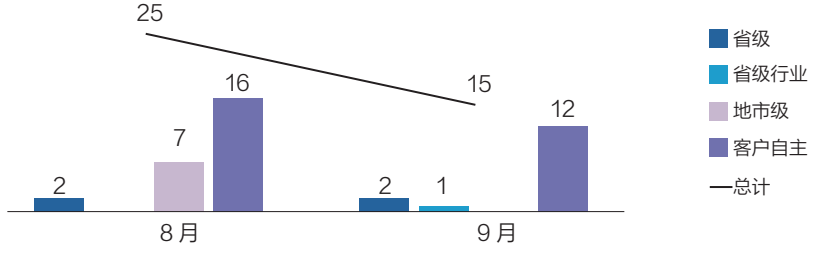


图 1 9-10 月 Z-TEAM 承接攻防演习数量统计

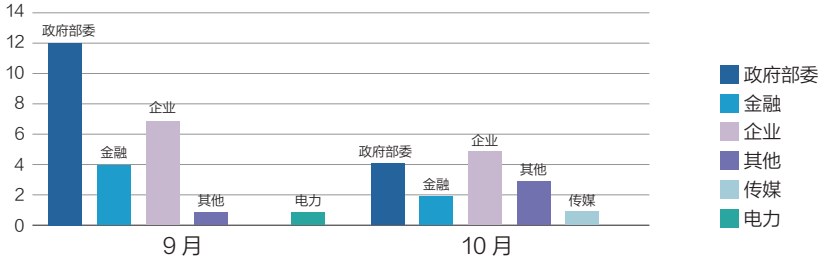


图 2 2023 年攻防演习涉及行业统计

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	41	63	77	102	112	166	582	9672

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集中，涉及的目标业务以企业、政府部委、金融、传媒为主。伴随着信息通信业的迅猛发展，计算机病毒、系统安全漏洞和网络违法犯罪等网络与信息安全问题日渐突出，网络安全对政府部委来说是一个重要且不可忽视的方面。政府部委的网络安全事关国家安全、社会稳定、公共利益，是维护国家主权、安全、发展利益的重要基础。因此，提高政府部委网络安全能力，建设坚不可摧的网络安全防线是重中之重。在本月攻防演习中政府部委行业占比为 27%（见图 3）。

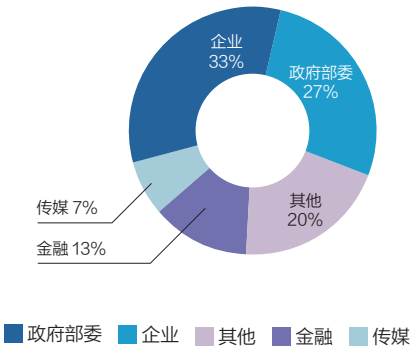


图 3 10 月攻防演习分布

三、主要攻击手段分析

基于本月奇安信 Z-TEAM 团队实战成果，对本月任务中多个行业的网络目标进行了的攻击分析，对不同的行业目标使用不同攻击手段，如政府部委行业的外网安全防护相对较强，但仍需防范漏洞扫描利用和 VPN 仿冒接入、隐秘隧道外联等手段的威胁；金融、企业行业的外网安全防护最强，但也不能忽视漏洞利用、钓鱼攻击和隐秘隧道外联等手段带来的风险；传媒和其他行业的外网安全防护相对较弱，容易被漏洞扫描利用和钓鱼攻击、口令爆破等手段成功突破。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下（见图 4）。

本月攻防演习服务中，攻击队使用的攻击手段主要有：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，钓鱼攻击手段有明显下降趋势，VPN 仿冒接入和隐秘隧道外联有明显上升趋势（见图 5）。

本月任务中政府部委行业攻防演习任务占比达三分之一，通过对该行业的演习数据分析发现，外网纵向突

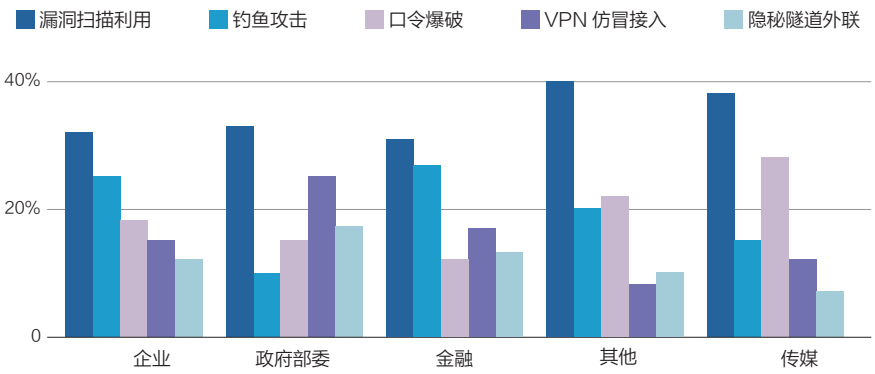


图 4 行业攻击手段分布

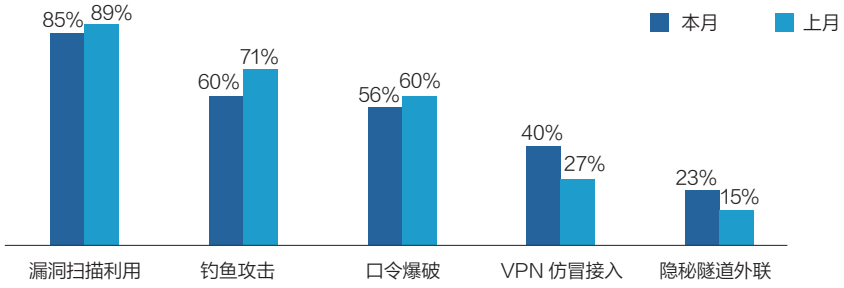


图 5 攻击手段对比

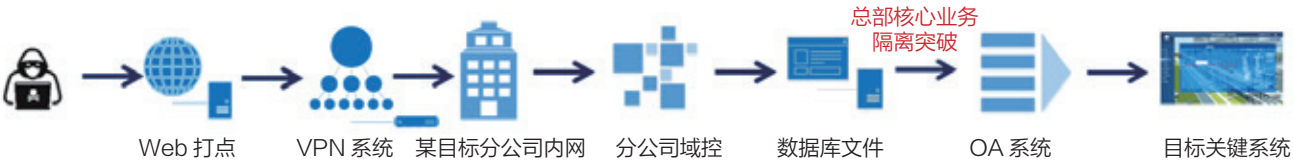


图 6 案例攻击路线图

破重点是寻找薄弱点，围绕薄弱点，利用历史漏洞攻击手段和 VPN 仿冒接入实现突破；以突破点为基础进行内网横向移动，利用隐秘隧道外联、口令爆破攻击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以上的手段共同配合才能成功。

四、典型攻击手段实现案例

随着政府网络中 VPN 的日益普及，VPN 在政府机构的远程办公中发挥着举足轻重的作用。通过 VPN，分支机构以及外地出差人员可以随时随地安全地接入内部资料、办公 OA、内网邮件系统、ERP 系统、CRM 系统、项目管理系统等。因此 VPN 仿冒接入也成为了攻击队利用的攻击手段之一。

案例：通过 VPN 仿冒控制某政府内网核心业务

奇安信攻击队在参与某政府部委的攻防演练过程中，将 VPN 作为进攻切入点，通过 VPN 仿冒穿透行为突破目标网络边界，从而直接访问该单位内部的资源。

在攻击队接收到攻击目标后，基于对目标的前期侦察和探测，未在总部网络上发现任何可利用的薄弱点。于是，攻击队根据目标业务地域分散的特点，对其分支机构进行了侦察。在全面的信息收集过程中，攻击队很快发现其集团及子公司的 VPN 仍然开放并未关闭。经过指纹识别，已确定该集团所使用的 VPN 系统来自国内某知名厂商。进一步分析发现该 VPN 系统存在任意文件读取漏洞。利用该漏洞，攻击队成功获取了入口 VPN 的用户名和密码，并仿冒登录 VPN，直接获取了服务器权限，从而接入目标内网。

在采取了 VPN 仿冒接入分公司内网的措施后，攻击队决定利用这一时机进行内网的横向拓展。他们巧妙地通过内网的横向移动，成功获取了分公司工作域控 HASH，控制该工作域网络，攻击队随即控制了大量的域内服务器和关键系统。

攻击队已圆满实现第一阶段的目标，且成果斐然。接下来的任务是，通过分公司网络系统，力争找到通向总部核心业务网络的关键入口。

首先，攻击队成功拖取了 VPN 的数据库文件，并在进一步横向扩展之前，对其进行了深入的解析。尽管目标客户已经对 OA 系统进行了迁移并修复了漏洞，但是攻击队惊喜的发现他们竟然没有删除所有的 Webshell 后门脚本。部分后门脚本仍然存在于 OA 程序中，并被重新部署在新服务器上。攻击队依然能够连接先前植入的 Webshell，逐渐提升权限，最终完全掌控服务器。

基于这些信息，攻击队伍开始利用在 VPN 服务器上创建的代理，进行内网精确打击。一方面，他们成功地控制了多个可以连接到外部网络的主机，创建了不同类型的代理隧道，以提高连接的稳定性。另一方面，他们针对该关键系统进行攻击，并最终将其攻破。

五、安全加固建议

该安全事件暴露出政府单位存在 VPN 资产管控、Webshell 后门防范等安全问题，建议开展如下安全加固整改工作：

- 梳理互联网 VPN 资产，开启 VPN 访问白名单。组织开展 VPN 用户上报其互联网出口地址，在 VPN 前的防火墙增加互联网访问白名单，确保只有白名单内用户才能接入 VPN。
- 控制 VPN 接入权限。梳理 VPN 接入后的内网访问权限，强化访问控制，设置必要的分组，不同分组不同权限，细化管控策略。
- 加强 VPN 自身安全管控。关注 VPN 自身漏洞，加强威胁情报，监控 VPN 漏洞，与厂家密切联系并及时对 VPN 进行升级加固。
- 强化对后门脚本的防范。对目录进行权限设置，不同网站使用不同的用户权限。对 FTP 进行权限设置，取消匿名访问。对系统盘的敏感目录及文件进行权限设置，提高系统安全性；定期更新杀毒软件并查杀。
- 加强对 VPN 的安全监控。确保天眼（威胁感知系统）监控范围覆盖 VPN 及其设置的地址池 IP，并进行重点监控、分析，同时加强 VPN 设备的日志监控力度，一旦发生异常事件及时处置。安

大模型安全该怎么办？

人工智能成为中美元首会晤的内容；受分布式拒绝服务攻击，OpenAI 的 ChatGPT 和 API（第三方应用接口）突发严重停机，大模型安全风险首次真实显现。大模型到底有哪些风险，该怎么应对？本期专题将详解大模型安全风险、国际治理趋势与应对方案。

未来 10 年，大模型将出现人类难以控制的风险

据新华社报道，11 月 15 日，国家主席习近平同美国总统拜登举行中美元首会晤。两国元首同意推动和加强中美在人工智能等重要领域加强合作，建立人工智能政府间对话。人工智能成为中美元首会晤的内容，这也显示出人工智能问题已成为全球治理的重点领域。

就在 11 月 1 日至 2 日，首届全球人工智能 (AI) 安全峰会在英国召开。28 个国家和欧盟共同发表的《布莱切利宣言》，警告了最先进的“前沿”人工智能系统所带来的危险。强调各国需共同协作，共同建立 AI 监管方法，同时宣言各方承诺共同在发布前对先进的人工智能模型进行一系列安全测试。

2022 年 11 月 OpenAI 公司发布 ChatGPT-3，这款聊天机器人向用户展示了生成式人工智能系统的强大通用功能。新的人工智能工具在为人类带来巨大的全球机遇的同时，也给网络安全、生物技术等关键领域带来了重大风险；而下一代系统的功能可能会强大 10 倍或 100 倍，由此可能带来更高的风险。

新一代人工智能技术所带来风险引发担忧，其安全治理攸关全人类命运，成为世界各国面临的共同课题。

> 除非迅速建立适当的保障措施和政策响应，否则前沿的 AI 系统可能会给社会带来新的风险。

一、AI 将带来难控制的风险

1. 全球的人工智能竞赛开始

ChatGPT-3 的发布，将其从软件工程师的工具，重新定位为以消费者为中心、普通人不需要任何技术专业知识就可以自己使用的工具。

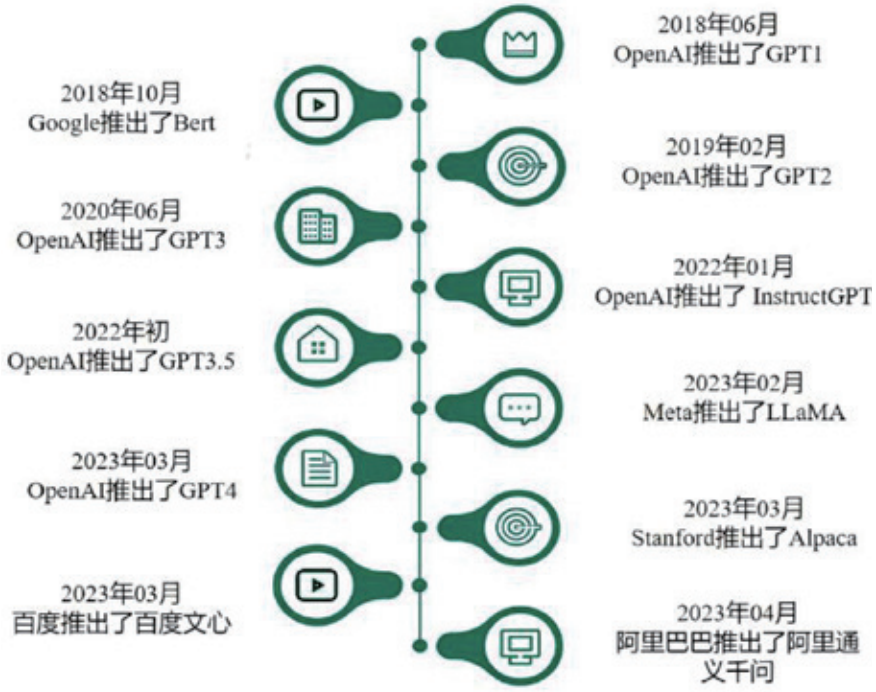
使用 ChatGPT，用户可以与人工智能机器人进行对话，要求其设计软件，而不必自己编写代码。

仅四个月后，ChatGPT 的开发者 OpenAI 就推出了 GPT-4，这是为 ChatGPT 提供支持的基础大语言模型 (LLM) 的最新版本，OpenAI 声称该模型在各种任务上“表现出了人类水平的表现”。ChatGPT 成为历史上增长最快的网站，两个月内就拥有超过 1 亿用户。

突然之间，一场人工智能竞赛开始了。微软在向 OpenAI 投资 130 亿美元后，将 ChatGPT 纳入其产品中，包括经过改进的、由人工智能驱动的 Bing。2016 年，谷歌因其 DeepMind 人工智能模型在中国围棋比赛中击败人类冠军成为头条新闻，该公司立即推出了自己的人工智能聊天机器人 Bard。Meta 首席执行官马克·扎克伯表示：“我们最大的一项投资是推进人工智能并将其构建到我

们的每一款产品中。” 多家规模较小的公司在开源代码的帮助下也加入了人工智能的追逐。

自 ChatGPT 发布以来，基于 LLM 的生成式人工智能技术呈爆炸式增长。集成 LLM 的开源项目数量也迅猛增长。例如，OpenAI 推出 ChatGPT 不到 1 年，目前 GitHub 上已有超过 3 万个使用 GPT-3.5 系列 LLM 的开源项目。开源社区每月贡献大约十几个 LLM。这些 LLM 体积更小，可训练的计算资源要少得多，并且可以使用任何特定的用例数据进行高度定制，以保护隐私和机密性。



2. 知名大模型 50 分钟被攻破

面对快速发展的 AI 技术，业界日益担忧带来的风险。《布莱切利宣言》认为，人工智能模型最重要的功能，可能会有意或无意地造成严重甚至灾难性的伤害。”即使是当前的人工智能系统（其围栏功能经常会受到阻碍）似乎也能够帮助犯罪组织更有效地制造虚假信息和设计威胁代码。

针对快速演进发展的人工智能技术，首届全球人工智能 (AI) 安全峰会期间，一位了解人工智能发展前沿情况的企业代表表示，2025 年至 2030 年间，新兴 AI 系统可能会带来人类难以控制的风险。

人工智能 (AI) 安全峰会与会代表一致认为，最先进的人工智能系统正在以惊人的速度改进。过去十年，用于训练人工智能系统的计算能力增加了 5500 万倍。下一代所谓的前沿模型可能使用 OpenAI 的 GPT-4 十倍的计算量进行训练。因此，除非迅速建立适当的保障措施和政策响应，否则前沿的 AI 系统可能会给社会带来新的风险。（这些模型最早可能在明年推出。）

在 DEF CON 2023 上，由 AI Village、SeedAI 和 Humane Intelligence 组织的大模型红队挑战赛，比以往任何时候都更清晰地展示了生成人工智能如何可能被滥用。

大约 2,244 名黑客参加了这场有史以来最大规模的大模型红队演习，研究人员有 50 分钟的时间来尝试破解随机选择的大型语言模型。接受测试的大型语言模型由 Anthropic、Cohere、谷歌、Hugging Face、Meta、英伟达、OpenAI 和 Stability 构建。

结果显示，这些大模型技术具有可被利用的较高漏洞。在 50 分钟内，研究人员发现了包括 Google 和 Open AI 等 8 种大模型的漏洞或错误，利用这些漏洞不仅可以传播不准确信息、错误信息，甚至为实施犯罪提供指南。

DEF CON 2023 期间的研究显示，这些大语言模型可能泄露数据、传播错误信息、支持仇恨言论，甚至为犯罪提供指导。DEF CON 2023 人工智能红队演习表明，大模型在阻止产生错误信息、偏见和不正确信息及信息泄露等方面，还有很长的路要走。

对于大模型提供商来说，可能永远无法阻止 AI 武器化或对 AI 的恶意利用，但在将恶意使用消灭在萌芽状态方面，需要做得更好。

二、大模型存在五大问题、十大漏洞

针对大模型的风险与安全问题，国内外的安全机构进行了相关研究，提出了大模型存在的问题、面临的安全漏洞，政企机构在广泛部署和使用

大模型之前，需要构建保证大模型安全性、信任、隐私和合规性的围栏。

1. 大模型存在五大问题

2023 年 6 月，我国之江实验室基础理论研究院人工智能与安全团队，首次全面总结了 ChatGPT 为代表的《生成式大模型的安全与隐私问题白皮书》（以下简称“白皮书”）。

白皮书认为，大批模型的出现使得在人机交互、资源管理、科学研究、内容创作等应用领域出现了新的、强有力的工具。但同时也出现了包括数据安全、使用规范、可信伦理、知识产权及模型安全方面的问题。

1）数据安全问题

白皮书提出，数据的安全和隐私是 ChatGPT 及 GPT-4 等生成式大模型使用和研发过程中一个极为重要的问题，并从「显式」和「隐式」两个方面对其进行了分析。

在显式的信息泄漏中，首先，ChatGPT 等生成式大模型的训练数据在不经意间被转换成了生成内容，其中就包括了敏感和隐私的个人信息，如银行卡账号、病例信息等。此外，ChatGPT 的数据安全和隐私隐患还体现在它对于对话框内容的存储，当用户在和 ChatGPT 互动时，他们的信息会以某些形式被记录和存储下来。

白皮书还提出了之前被大家忽略的隐式信息泄漏问题。首先，ChatGPT 体现出的数据安全和隐私的隐患是它可能通过对对话框数据的收集进行广告推荐，以及收集对话框数据进行推荐或者其他的下游机器学习任务，且 ChatGPT 有时候可能也会生成虚假的信息，以此来诱导用户泄漏一系列的数据。

2）使用规范问题

在白皮书中，作者提到 ChatGPT 和 GPT-4 等生成式大模型强大的理解和生成能力虽然为我们的生活和生产带来了很多的便利，但是，同时也存在更多的机会被恶意使用。在没有规范约束的情况下，恶意使用将带来很多的社会性问题。

其一，ChatGPT 和 GPT-4 等模型的强大能力使得某些别有用心的人想要将其作为违法活动的工具。例如用户可以利用 ChatGPT 来编写诈骗短信和钓鱼邮件，甚至开发代码，按需生成恶意软件和勒索软件等，而无需任何编码知识和犯罪经验。

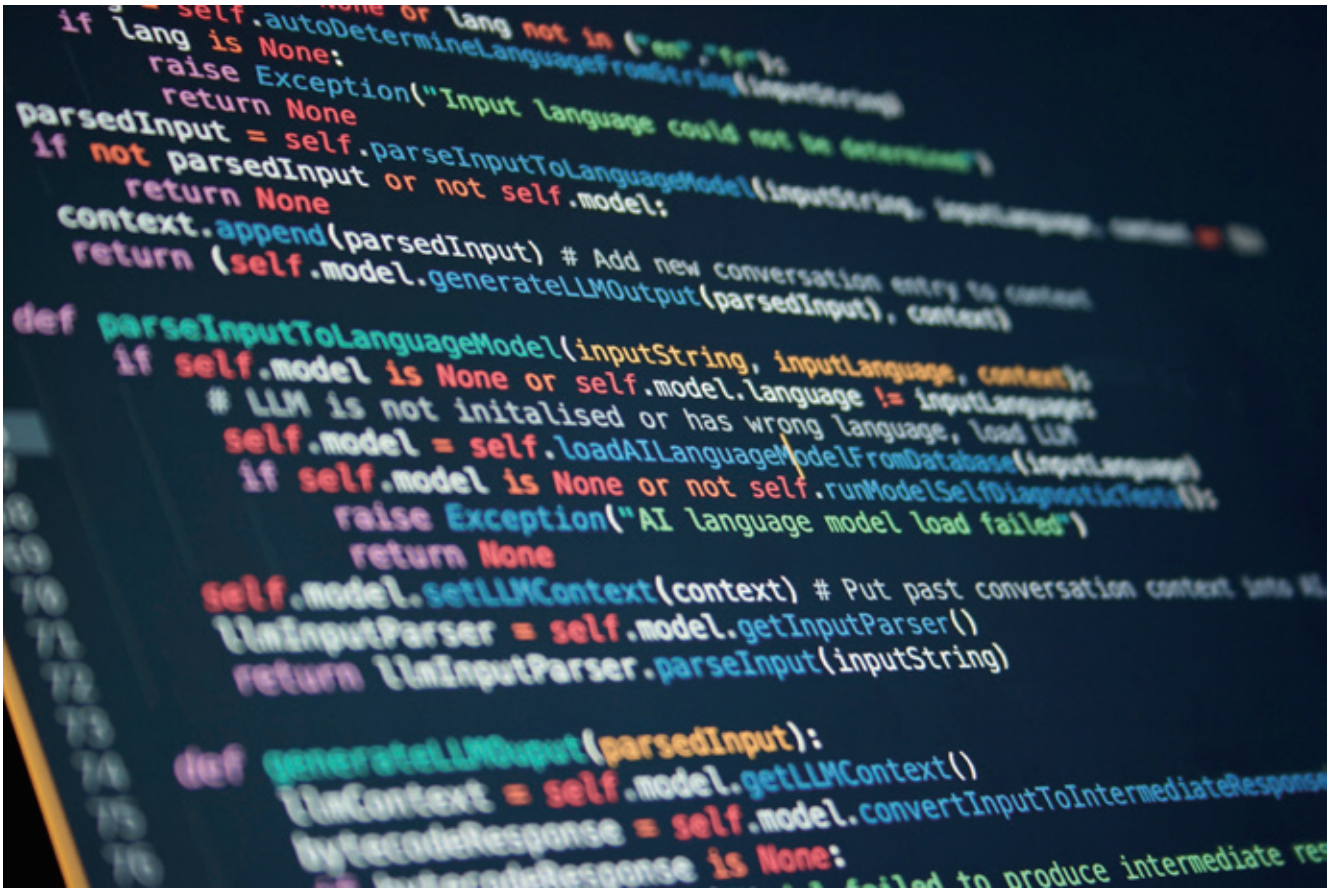
其二，ChatGPT 和 GPT-4 等生成式大模型没有把不同地区的法律规范考虑在内，在使用和输出的过程中可能会违反当地法律法规，因此需要一个强有力的当地监管系统来检测其使用是否与当地法律法规相冲突。

其三，对于一些游离于安全和危险之间的灰色地带，ChatGPT 等生成式大模型的安全能力还没有得到增强。例如，ChatGPT 可能会输出一些诱导性的语句，包括跟抑郁症患者沟通时可能会输出某些语句导致其产生轻生的心态。

3）可信伦理问题

ChatGPT 等生成式大模型以问答形态存在于社会层面，但其回复往往存在不可信或者无法判断其正确性的问题，会有似是而非的错误答案，甚至与现有社会伦理产生冲击。

> 大模型使得在人机交互、资源管理、科学研究、内容创作等应用领域出现了新的有力工具。但同时也出现了数据安全、使用规范、可信伦理、知识产权及模型安全方面的问题。



白皮书指出，首先 ChatGPT 等生成式大模型的回复可能是在一本正经地胡说八道，语句通畅貌似合理，但其实完全大相径庭，目前模型还不能提供合理的证据进行可信性的验证。例如，ChatGPT 可能会对一些历史、科学、文化等方面的问题回答错误或者与事实相悖，甚至可能会造成误导或误解，需要用户有自己的鉴别能力。

ChatGPT 等生成式大模型的伦理问题也在白皮书中被详细讨论。即使 OpenAI 等研发机构已经使用 ChatGPT 本身生成了他们的道德准则，但其中的道德准则是否符合我国国情的基本价值观原则，尚未有定论。作者提出其中存在传播有害意识形态、传播偏见和仇恨、影响政治正确、破坏教育公平、影响国际社会公平、加剧机器取代人类的进程、形成信息茧房阻碍正确价值观形成等问题。

4）知识产权问题

ChatGPT 等生成式大模型凭借强大的语言处理能力和低廉的使用成本给社会方方面面带来便利的同时，也存在侵权等问题，对现存版权法体系带来冲击。例如 ChatGPT 生成的作品可能存在著作权争议：ChatGPT 虽然有着出色的语言处理能力，但是即使生成的作品符合知识产权的全部形式要求，ChatGPT 也无法成为著作权的主体，这是因为著作权主体在享有权利的同时也要承担对应的社会责任，而 ChatGPT 只能作为用户强大的辅助生产力工具，它无法自主创作，更不要谈享有权利、履行义务的主体要求。

ChatGPT 等生成式大模型仍无法独立创作，更没有自主思维和独立思考的能力，因而，ChatGPT 根据用户的输入生成的内容不符合作品「独创性」的要求。ChatGPT 用于模型训练的数据来自互联网，不论多么高级的模型训练算法必然涉及对现有智力成果的引用、分析、处理等，必然存在对他人合法知识产权的侵犯问题。

5）模型安全问题

从攻防技术角度来看，ChatGPT 等生成式大模型也存在着模型安全的问题。ChatGPT 本质上是基于深度学习的一个大型生成模型，也面临着人工智能安全方面的诸多威胁，包括模

型窃取及各种攻击引起输出的错误（如包括对抗攻击、后门攻击、prompt 攻击、数据投毒等）。

例如，模型窃取指的是攻击者依靠有限次数的模型询问，从而得到一个和目标模型的功能和效果一致的本地模型。而 ChatGPT 已经开放了 API 的使用，这更为模型窃取提供了询问入口。又如，ChatGPT 和 GPT-4 作为一个分布式计算的系统，需要处理来自各方的输入数据，并且经过权威机构验证，这些数据将会被持续用于训练。那么 ChatGPT 和 GPT-4 也面临着更大的数据投毒风险。攻击者可以在与 ChatGPT 和 GPT-4 交互的时候，强行给 ChatGPT 和 GPT-4 灌输错误的数据，或者是通过用户反馈的形式去给 ChatGPT 和 GPT-4 进行错误的反馈，从而降低 ChatGPT 和 GPT-4 的能力，或者给其加入特殊的后门攻击。

2. 大模型存在 10 个最严重漏洞

开放全球应用程序安全项目 (OWASP) 发布了大语言模型应用常见的 10 个最严重的漏洞，强调了 LLM 面临的潜在风险、漏洞利用的难易程度和普遍性。

OWASP 给出的 LLM 漏洞包括提示注入、数据泄露和未经授权的代码执行等。

1）提示词注入

提示注入在 LLM 应用程序漏洞占据首位。攻击者通过绕过过滤器或使用精心设计的提示词来操纵 LLM，使模型忽视此前的指引，执行攻击者想要的操作。提示注入攻击的结果各不相同，范围从获取机密信息到影响关键决策。

2）输出处理不安全

对大模型输出结果未审查即接受，就会出现此漏洞，从而暴露后端系统。利用此漏洞可能产生权限升级、后端系统上的远程代码执行，使应用容易受到外部注入攻击，攻击者可获得对目标用户环境的访问特权。

3）训练数据投毒

LLM 应用的关键之一是提供给模型的庞大的、多样化的并且涵盖多语言的训练数据。大型语言模型使用神经网络根据从训练数据中学习的模式生成输出。通过训练数据投毒，可以导致改变模型的道德行为、导致应用程序向用户提供虚假信息、降低模型的性能和功能等。训练数据投毒可能导致模型无法做出正确的预测和与用户有效的交互。

4）拒绝服务攻击

攻击者与 LLM 应用程序密集交互，迫使其消耗大量资源，从而导致影响向用户提供的服务降级，并增加应用的成本。

LLM 应用的使用持续增长，以及

ChatGPT 等解决方案的普及，拒绝服务攻击的，在安全性方面的重要性将越来越高。

5）供应链漏洞

LLM 应用程序生命周期可能会受到存在漏洞的组件或服务的影响，从而导致安全攻击。使用第三方数据集、预先训练的模型和插件可能会增加漏洞。

6）敏感信息披露

大模型可能会通过向用户的回复，无意中泄露敏感和机密信息。从而导致未经授权的数据访问、隐私侵犯和安全漏洞。实施数据清理和执行严格的用户策略对缓解这种情况至关重要。

7）插件设计不安全

插件是模型与用户交互期间自动调用的扩展。许多情况下无法控制其执行。攻击者可以向插件发出恶意请求，甚至为远程执行恶意代码打开大门。LLM 插件输入不安全和访问控制不足的情况，可能会导致数据泄露、远程代码执行、权限升级。

8）过多权限

给予 LLM 过多的功能、权限或自主权也会带来风险，导致大模型执行有害操作，可能会产生影响数据机密性、完整性和可用性的后果。

9）过度依赖

系统或人员过度依赖而不受监督的 LLM，可能会因 LLM 生成的不正确或不适当的内容而面临错误信息、沟通不畅、法律问题和安全漏洞。

10）模型盗窃

即恶意行为者或 APT 组织未经授权访问和泄露 LLM 模型。

该漏洞对拥有生成式人工智能的公司造成的影响包括重大财务损失、声誉受损、失去相对于其他公司的竞争优势、滥用模型及不当访问敏感信息。

> OWASP 认为，大语言模型具有提示注入、数据泄露和未经授权的代码执行等漏洞。

OWASP 认为，组织必须采取一切必要措施保护其 LLM 模型的安全，确保其机密性、完整性和可用性。这涉及设计和实施全面的安全框架，以有效维护公司、员工和用户的利益。

三、结语

针对大模型所暴露出的问题与风险，安全人员认为，LLM 的性质和日益普及导致了一类新的漏洞利用和攻击媒介，这是传统方法无法防范的。因此，无论是专有的还是开源的 LLM 都应被视为“不受信任的”。

随着生成式 AI 和 LLM 系统的应用不断增长，由此带来的风险预计将在未来 12~18 个月内发生重大变化。

知名研究机构 Gartner 认为 ，如果组织不能管理人工智能风险，将有可能遭遇消极的人工智能结果和违规行为。模型不按预期运行，出现安全和隐私问题，将会带来财务和声誉损失，以及对个人造成伤害。错误运行的 AI 模型也会导致组织做出错误的业务决策。

安全人员建议：如果围绕 LLM 的安全标准和实践没有重大改进，针对性的攻击和发现这些系统中的漏洞的可能性将会增加。企业必须保持警惕并优先考虑安全措施，以缓解不断变化的风险并确保负责任和安全地使用 LLM。

人工智能全球治理加速推进

自去年发布 ChatGPT 以来，各国政府努力应对快速发展的技术带来的风险，在全球范围内的人工智能治理在加快推进。中国发布了《生成式人工智能服务管理暂行办法》，美国签署了一项《关于安全、可靠、值得信赖地开发和使用人工智能的行政命令》，被外界称为“有史以来政府为推进人工智能安全领域所采取的最重大行动”。

一、中国高度重视大模型安全

作为人工智能大国，中国在全球人工智能治理上从未缺位。

随着生成式人工智能的爆发，我国相关部门对其背后的大模型安全问题给予了高度重视。2023 年 2 月发布的全球安全倡议概念文件，专门强调要加强人工智能等新兴科技领域国际安全治理，预防和管控潜在安全风险。

2023 年 10 月 18 日，习近平主席在第三届“一带一路”国际合作高峰论坛开幕式主旨演讲中发布《全球人工智能治理倡议》，围绕人工智能发展、安全、治理三方面系统阐述了人工智能治理中国方案，展现了中国负责任大国担当。

《倡议》主张建立人工智能风险等级测试评估体系，不断提升人工智能技术的安全性、可靠性、可控性、公平性；支持在充分尊重各国政策和实践基础上，形成具有广泛共识的全球人工智能治理框架和标准规范，支持在联合国框架下讨论成立国际人工智能治理机构；加强面向发展中国家的国际合作与援助，弥合智能鸿沟和治理差距等。

在 2023 年 7 月 10 日，国家网信办等七部门已联合公布《生成式人工智能服务管理暂行办法》（以下简称《办法》），自 2023 年 8 月 15 日起施行。《办法》聚焦隐私安全、技术滥用、知识产权和他人权益三大问题，就生成式人工智能可能面临的安全问题提出了一系列明确的约束规范，为 AIGC 的发展建立了防护机制。

比如在第四条明确指出“提供和使用生成式人工智能服务，应当遵守法律、行政法规，尊重社会公德和伦理道德。要求不得侵害他人隐私权和个人

信息权益。AIGC 服务提供者被要求“采取有效措施提高训练数据质量，增强训练数据的真实性、准确性、客观性、多样性”。

11 月 9 日举行的世界互联网大会乌镇峰会“人工智能赋能产业发展论坛”上，中外专家共同发布了《发展负责任的生成式人工智能研究报告及共识文件》，总结提炼了发展负责任的生成式人工智能的多项共识。具体包括发展安全可靠的生成式人工智能，确保全生命周期内可控地运行；强化生成式人工智能数据治理，加强数据安全，尊重和保护个人隐私；明确生成式人工智能的归责体系，增强系统可追溯性；推动生成式人工智能，更好地理解人类意图、遵循人类指令并符合人类的伦理道德。

二、人工智能技术治理成全球重要方向

人工智能的治理正在进入一个新阶段，正在超越人与人之间的关系，上升到人与社会、国家与国家之间联系。人工智能的风险已经不局限于隐私保护、信息泄露等方面，而是更应该关注其对人类社会发展所产生的广泛影响。

但目前，在全球层面上，人工智能目前尚未形成统一标准和规范的人工智能治理体系。

2023 年 7 月，联合国秘书长古特雷斯表示，支持成立一个类似国际原子能机构的国际人工智能监管机构。他宣布将组建由人工智能专家和联合国机构首席科学家组成的科学顾问委员会，并计划在今年年底前启动高级人工智能咨询机构。古特雷斯称，利用人工智能“必须由各国展开协调设定红线”。人工智能所产生影响的外部性极容易成为全球性的问题。未来以人工智能为代表的技术治理将是全球治理的重要方向。

人工智能的风险已经不局限于隐私保护、信息泄露等方面，而是更应该关注其对人类社会发展所产生的广泛影响。

1、欧盟人工智能政策再次领先

欧盟似乎再次在制定人工智能政策方面处于领先地位。欧盟凭借其《数字市场法》和《数字服务法》，在制定数字平台政策方面处于领先地位。

从 2021 年开始，为了保障数据安全、个人隐私、道德伦理，以及从跨国市场规范、AI 平权等多项目标考虑，欧盟就开始推进《人工智能法案》。6 月 14 日，欧洲议会以压倒性多数通过了《人工智能法案》。在其通过后，欧盟委员会的监管机制将开始制定可执行的政策。

《人工智能法案》是全球第一部通过议会程序、专门针对人工智能，特别是生成式人工智能 (AIGC) 的综合性立法。它旨在确保人工智能系统受到监督。这标志着欧盟正在通过立法的形式加强对于人工智能的监管。

凭借“布鲁塞尔效应”，《人工智能法案》有可能被视为人工智能监管的全球标准之一——就像欧盟《通用数据保护条例》（GDPR）对数据保护监管的作用一样。

相较之下，欧盟国家则更多关注数据隐私问题，希望在这方面对人工智能加强监管。总体而言，欧盟《人工智能法案》对人工智能采取基于风险的监管方式，即根据人工智能技术对个人健康和安全或基本权利构成的风险程度对其进行分类。法律的风险等级或风险类别包括不可接受、高、有限或最小。10 月 24 日，欧盟就新人工智能法案中的关键部分达成一致，该法案预计于 12 月份公布。

2. 英国希望掌握更多话语权

英国政府希望在人工智能领域掌握更多的话语权。今年 3 月，英国政府公布了人工智能监管拟定办法白皮书，计划在相关部门和领域中迅速采用新的监管框架，未来数月将向金融、市场等行业领域的监管机构提供人工智能监管准则。英国采取的人工智能监管思路与欧盟提出的监管设计框架截然不同，有意对人工智能研发和使用采取宽泛的监管原则，实施更为灵活、平衡的监管办法。

11 月 1 日至 2 日，首届全球人工智能 (AI) 安全峰会在英国召开，关注被称为“前沿人工智能”的高性能通用模型的风险。28 个国家和欧盟共同发表的《布莱切利宣言》，警告了最先进

> 人工智能作为当今科技领域的热门话题，
> 单靠一个国家或一个组织的力量
> 很难全面应对其安全风险。
> 《布莱奇利宣言》指出，
> 人工智能的许多风险本质上是国际性的，
> 因此“最好通过国际合作来解决”。

的“前沿”人工智能系统所带来的危险。作为全球第一份针对人工智能新兴技术的国际性声明，《宣言》强调各国需共同协作，共同建立 AI 监管方法，同时宣言各方承诺共同在发布前对先进的人工智能模型进行一系列安全测试。

英国科学、创新和技术大臣米歇尔·多内兰在 10 月 30 日表示，世界正处于一场技术变革中，人工智能的蓬勃发展或将改变人类社会的方方面面，不仅带来巨大机遇，也会带来威胁全球稳定和破坏人类价值观的风险。抓住机遇、应对风险，全球要共同努力，“这正是英国举办首届人工智能安全峰会的原因”。

3. 美国：确保负责任使用 AI 的原则

美国政府一贯重视人工智能的应用与监管，虽然尚未在联邦层面形成统一的人工智能专门法律，但美政府依靠现有国家战略和地方法律法规，充分发挥州和地方的作用，同时采取自愿原则鼓励人工智能企业积极承担社会责任，弥补法律法规的空缺，确保人工智能可解释、可信赖。

2023 年 10 月 30 日，美国总统拜登签署了一项《关于安全、可靠、值得信赖地开发和使用人工智能的行政命令》。该行政命令为人工智能安全和保障建立了新的标准，被外界称为“有史以来政府为推进人工智能安全领域所采取的最重大行动”。

该行政命令指示采取以下行动：（一）人工智能安全和安保新标准；（二）保护美国人的隐私；（三）促进公平和美国公民权利；（四）促进创新和竞争；（五）推进美国在海外的领导地位；（六）确保政府负责和有效地使用人工智能。

该行政令将向十多个机构发布规模庞大的指令，针对它们处理人工智能系统的情况。新的指导方针通过联邦机构的购买力和执行工具赋予联邦机构在美国市场的影响力。

目前，美国国会正致力于通过立法来应对人工智能的风险和潜力。尽管一些人士希望在年底前通过有关人工智能的法律，但参议院多数党领袖查克·舒默表示，明年之前可能不会推出广泛的人工智能法案。

三、结语

生成式人工智能与传统基于自动化的人工智能系统有着根本的不同。生成式人工智能技术不断进步，其以强大功能与超强智能不断地突破技术应用，并深度影响着社会的运行和价值的追求，还在海量数据的调用、应用场域的泛化和算力资源的调用等方面提出了许多全新问题，考量社会治理的思想观念和实践方略。因此，生成式人工智能延续与发展了自有人工智能技术以来的风险挑战，又以技术范式进步的方式进一步扩展了风险。

如《布莱奇利宣言》指出的那样，人工智能的许多风险本质上是国际性的，因此“最好通过国际合作来解决”。人工智能作为当今科技领域的热门话题，其发展速度之快、应用范围之广、影响力度之大、技术之复杂，单靠一个国家或一个组织的力量很难全面应对其安全风险。

对于生成式人工智能可能的风险，必须除了关注数据安全、隐私安全等传统安全，还需要对于数据被投毒、模型被操纵造成的后果有清晰的认知，真正从社会发展角度规制技术产生的社会风险。

为了更好地应对人工智能带来的风险，各国机构需要加强合作，共同研究和分析人工智能的安全风险，并采取有效的措施来降低这些风险。此外，还需要加强对人工智能技术的监管，确保其符合道德和法律标准。同时，还要共同制定人工智能安全治理的国际标准和规范，促进人工智能技术的安全和可持续发展。

AI 风险与安全管理工具：大模型应用需全程监控、闭环管理

当前，国内“百模大战”如火如荼，通用类、垂直类井喷之势发展。IDC 预测，2026 年中国 AI 大模型市场规模将达到 211 亿美元，人工智能将进入大规模落地应用关键期。

与此同时，我国数据安全相关法律法规为大模型应用定下了监管红线，相继出台了《网络安全法》《数据安全法》《中华人民共和国个人信息保护法》，以及数据跨境相关法律监管体系，这要求企业在使用大模型时亟需守住合规底线。

8 月 25 日，奇安信依托安全和人工智能两大领域的深厚积累，奇安信正式发布了业内首款大模型卫士产品 GPT-Guard，帮助客户有效监控和防护大模型在使用过程中可能引发的数据泄露、法律合规、知识产权等一系列安全风险，消除其对于大模型“想用不敢用”的顾虑，让企业更安全的使用大模型应用，向科技要生产力，走好数智时代的发展之路。

国内大模型应用存在三大安全挑战

奇安信大模型卫士负责人刘岩认为，目前国内大模型应用的安全存在以下三个方面的挑战：首先是大模型应用的监测和风险评估难，大模型应用的数量飞速增加、应用更新变化快，缺少风险评估工具，企业使用风险难以评估；其次是上传敏感数据等异常高危行为，将会引发敏感信息泄漏或其他风险；最后是大模型工具的使用缺乏有效的记录手段，各类信息缺失，使用风险难以追溯。

奇安信集团副总裁张卓表示，“ChatGPT 等大模型，会泄露企业的商业秘密，已经引起广泛关注。据统计，在使用 ChatGPT 的员工中大多数会泄露数据，其中 11% 的数据为企业敏感数据。越来越多的办公产品如 Microsoft 365 Copilot、WPS AI、通义听悟等都集成了大模型，就意味着将有更多的员工使用大模型，这会

> 我国数据安全相关法律法规
> 为大模型应用定下了监管红线。
> 企业在使用大模型时亟需守住合规底线。

加剧企业敏感数据的泄露风险。解决大模型数据泄露难题，迫在眉捷。”

张卓认为，数据泄露带来的直接结果，就是企业核心竞争力的逐步丧失。以某行业龙头企业 A 为例，该企业拥有大量核心技术专利，形成了强大的技术壁垒。然而，由于员工大量使用大模型应用处理日常工作，且缺乏监管，最终数据投喂过程中，公司敏感技术信息不断泄露，时而久之，这些重要技术信息变成 GPT 知识库的一部分，又通过 GPT 传授给同行对手企业，导致企业的核心竞争力逐步丧失。

知名研究机构 Gartner 认为，AI 的全民化使得对 AI 信任、风险和安全管理（AI TRiSM）的需求变得更加迫切和明确。在没有护栏的情况下，AI 模型可能会迅速产生脱离控制的多重负面效应，抵消 AI 所带来的一切正面绩效和社会收益。

根据 Gartner，AI TRiSM 提供用于模型运维（ModelOps）、主动数据保护、AI 特定安全、模型监控（包括对数据漂移、模型漂移和 / 或意外结果的监控）及第三方模型和应用输入与输出风险控制的工具。除此之外，AI TRiSM 还有助于满足全球范围内激增的人工智能法规。

大模型应用需全程监控、安全闭环管理

针对汹涌而来的大模型浪潮，促进发展和防范风险需要两者并重。

刘岩表示，奇安信大模型卫士将成为大模型的“过海法器”，GPT-Guard 能够完美适配并识别海量主流大模型应用，让企业全面掌控大模型的使用情况；具备领先的大模型风险发现能力及风险检测库，可以检测大

模型应用自身安全风险、服务商风险及大模型使用过程产生的数据泄露风险、数据跨境风险、服务风险、用户及设备风险、业务安全风险等多维度安全风险，帮助企业及时感知大模型的风险情况。

具体而言，奇安信大模型卫士GPT-Guard提供了“应用发现、风险评估、合规管控、数据保护、安全检测、溯源处置”6大核心功能，实现对大模型应用的全程监控、安全闭环管理。

第一是应用发现。GPT-Guard可支持多种类型的大模型应用识别及发现，除传统的问答类大模型应用外，还可识别检测多种类型的大模型应用，包括图片处理、编程助手、文档撰写、音频编辑、视频编辑等各种类型的应用，从而全面掌握企业中大模型使用情况。与此同时，GPT-Guard大模型应用库具备实时动态更新能力，从而保证新应用第一时间可见可控。

第二是风险评估。GPT-Guard能够基于流量实时分析企业大模型应用使用情况，通过多维度评估企业大模型应用风险；另一方面，基于应用自身的风险属性变化，以及企业的风险应用使用情况，及时感知企业的大模型使用风险情况，并动态对风险进行调整。

第三是合规管控。GPT-Guard遵循最小必要权限原则，限制可访问GPT应用的组织及人员，对API进行监控，避免未上报应用的投喂训练，限制私搭代理、在GPT网站上传文件及图片等高危行为。

第四是数据保护。GPT-Guard能够检测并保护聊天、API及文件上传等途径的外发内容，能够实时发现并阻断包含敏感信息的问题及上传的文件。除此之外，大模型卫士还搭载了奇安信自研的智能分析引擎，支持毫秒级数据检索，实现“以人追数”和“以数找人”。通过分析引擎实时分析违规异常行为，并进行告警上报。

第五是安全检测。GPT-Guard能够监控并记录终端和网络侧的所有的GPT访问行为，检测各种异常使用，帮助客户满足《网络安全法》《数据安全法》《个人信息保护法》等相关法律法规要求。

第六是溯源处置。违规行为产生告警后，客户通过查看详情可进行追溯，一键追溯到原始日志，并查看完整事件链，精准定位到风险源头。

“大模型风险管理需要持续的运行监控及保护，发现、检测、策略、保护、响应、处置缺一不可。”刘岩强调。

据悉，目前，大模型卫士能够完美适配主流大模型应用，并在终端侧和网络侧，通过奇安信可信浏览器、安全代理网关（SWG）等全链条工具，对大模型应用实现精准管控，全面降低数据安全风险。安

> 大模型风险管理需要持续的运行监控及保护，发现、检测、策略、保护、响应、处置缺一不可。

烟草公司如何破解 IT、OT “两张皮”的安全难题?

作者 | 张少波

烟草制品业，是中国税收的主要贡献行业之一，对推动国家经济发展、解决社会就业等起着重要支撑作用。党的二十大报告强调，要“加快发展数字经济，促进数字经济和实体经济深度融合”，加快推进数字产业化和产业数字化，成为催生我国各行各业实体经济高质量发展新动能的关键举措，烟草行业也是如此。

我国烟草制造历经多次大规模的技术改造，其各个工艺环节的自动化技术水平已得到大幅提升。目前，工控系统已深入到烟草生产的诸多环节，同时，随着智慧烟草工作的推进，工业互联网等新一代信息技术广泛应用于烟草行业，工控生产网 (OT) 与商业办公网（IT）的互联互通成为常态。

某烟草公司作为当地的重要制造企业，近年来积极数字新技术对传统产业进行全方位、全链条的改造，并依托 IT 与 OT 深度融合及物联网的快速发展的浪潮，加速全业务、全场景的数字化转型。为了解决日益严峻的攻击威胁，保障两大系统安全稳定运行，提升网络安全防护能力，该烟草公司于 2022 年启动“烟草商业工控安全一体化建设”，通过与奇安信合作，启动了以态势感知与安全运营平台（简称 NGSOC）为主的安全建设，全力护航“数实融合”，为智慧烟草筑牢安全底座。

破解 IT 和 OT “两张皮”难题，为“两化融合”铺平道路

“目前，很多国际领先的自动化和工控网络技术已经率先在烟草制造业得到广泛应用，然而，这些先进技术在提升烟草企业生产力的同时，也埋下了安全隐患。”该烟草相关负责人表示。尤其是 2017 年“永恒之蓝”勒索攻击爆发之后，很多烟草制造、物流等环节都系统蓝屏而被迫停产，加之近年来数据泄露、勒索攻击等网络威胁正加速向工业控制系统扩散，为烟草生产稳定运

行造成了重大隐患。

从 2019 年开始，该烟草公司已初步建立了工业物流安全防护体系和商业办公网安全防护体系，构建了基础的安全防护措施，可配合上级安全部门进行合规性检查及基础的安全运维工作，但是在网络安全监测、告警、分析、控制等方面，尚存在一些不足，具体包括以下几个方面：

首先是 IT 和 OT 的“两化融合”问题。该烟草公司的商业办公和工业控制是分开的两个系统，因此就出现了 IT（商业办公网）和 OT（工控网）安全管理两层皮的情况，IT 工作无法为 OT 提供有效的支撑。 尤其是 IT 和 OT 的各种系统日志数据、告警数据、资产数据、安全设备的告警信息各自独立存放。如果敏感数据区域遭受攻击，由于攻击痕迹存放在各个分散的信息孤岛上，难以统一的分析、研判和溯源，给网络的整体稳定运行造成安全隐患。

其次是资产和风险管理的挑战。安全管理工作需要全面掌握资产信息、漏洞信息、脆弱性信息和威胁信息等安全信息。要知道资产风险在哪里，是什么样的风险，什么时候会发生风险，就需要给管理者提供网络资产管理和安全监管的技术支撑平台，实现资产数据、脆弱性分布、安全威胁状况、安全防御状态等数据信息的全面深度掌控，建立资产风险评估能力，使资产风险量化、可视化，实现资产风险的可持续跟踪和管理，为安全决策提供有力支撑。

再次是事件分散导致溯源困难。从烟草行业当前的情况来看，网络安全设备的检测结果只能从单一维度反映某个系统存在的具体问题，但告警信息较分散，无法针对海量告警数据进行统一安全监测和宏观风险预警，无法从全局视角对安全事件进行分析和处置，更无法综合各种情报等还原攻击链条，实现精准溯源。

在过去的安全体系中，大量的安全监测结果只是单一维度反映某个系统存在相关问题，无法实时、整体掌控网络安全的态势，面对安全事件时容易滞后，效率低且比较被动。

最后是缺乏统一、实时、可视化的监控，应对事件较为被动。

在过去的安全体系中，大量的安全监测结果只是单一维度的反映某个系统存在相关问题，呈现的方式也多种多样，并没有针对海量的安全数据进行统一的可视化展现，也不能将安全数据进行分类、分场景展现，无法实时、整体掌控网络安全的态势，因此面对安全事件时容易滞后，效率低且比较被动。

多个“统一”实现闭环管理，可视化呈现整体风险

2022 年，国家烟草局发布了《关于组织开展行业数字化转型“大安全”建设试点示范工作的通知》（国烟信办[2022]5 号），通知要求，为深入推进行业数字化转型“大安全”建设，持续提升网络安全保障能力，将在行业组织开展数字化转型“大安全”建设试点示范工作。基于这样的背景下，该烟草公司通过商业工控一体化平台建设，以资产为核心，安全事件告警与分析为主线，实现网络资产台账画像、网络异常行为统一监控、威胁告警统一分析、统一安全预警、威胁处置统一闭环管理的全流程管理，动态调整安全策略，为网络的连续性和体系化建设提供决策支撑。

经过一年来的项目建设，目前商业工控一体化平台建设已取得了以下成果：

首先是实现了统一的网络资产台账管理。新建成的商业工控一体化平台，实现了物流 OT/IT 融合网络资产详细台账管理，包括 IP 地址、MAC 地址、资产分类、责任人、重要成度、端口服务、活跃状态、流量、资产通讯关系、风险值、开放服务、漏洞、告警、注册时间、变更时间、使用状态、操作系统、负责人等详细信息，都能一目了然、清晰呈现。

其次是实现了网络异常行为统一监控。新的平台依托 NGSOC，实现了利用图形化连线拖拽的交互方式，对流量、日志等数据进行关联分析，构建网络资产白名单、网络通讯模型、关键工艺执行模型，并利用模型基线有效识别行为异常。

第三是实现网络威胁统一管理，并实现威胁处置闭环。新平台打通了网络威胁的告警孤岛，并通过二次分析，全面展示攻击者和受害者信息，直观了解攻击发生的基本时间范围和影响。在处置方面，平台基于一体化纵深防御机

制，通过 NGSOC+SOAR(自动化编排技术) 与相关设备联动，实现威胁从发现、验证、通报、处置、核查等环节的自动化闭环处置，显著提升安全运营处置效率。

第四是实现网络威胁整体可视化。新平台以资产为核心，通过对风险、漏洞、威胁、异常行为的分析和技术监控，利用可视化技术从安全综合态势、资产态势、漏洞态势、威胁态势、异常行为态势、网络监控态势等维动态展示整体网络风险。

“新平台采用了大量业界领先的创新技术，如通过微服务架构，将各业务模块划分为独立微服务进行管理，可以快进行版本迭代；而自动化编排技术的使用，将原有单点防护转变现为协同处置，实现威胁自动化安全运营处置；新平台还引入‘零信任’防护理念，可通过资产识别、持续监测、联动处置等技术实现技术监测和动态防护；尤其上采用流式分布式关联分析引擎实时计算能力及复杂事件处理引擎，大大提高威胁分析效率，精准识别网络中的各类风险。”该烟草公司相关负责人表示。

经济效益和社会效益双见效，示范效应明显

在该烟草公司和奇安信的共同协作之下，该项目建设非常顺利，并如期完成目标。据介绍，新平台上线之后，在几个方面均获得了超出预期的效果。

首先是经济效益立竿见影。

提升全网安全处置能效：通过部署奇安信 NGSOC 系统的自动化编排技术，降低网络安全运行和维护成本，节约人工运维成本。提升全网安全管理能效：从局部整改为主的外挂式建设模式走向深度融合的体系化建设模式，输

某烟草公司全局安全态势

出体系化、全局化、实战化的网络安全能力。

其次是社会效益非常显著。

商烟“两化融合”网络安全示范效应：商业信息化发展和业务特性及网络威胁的多样性，平台建设对烟草行业数字化转型“大安全”建设起到带动示范效应。

推动行业威胁数据情报共享：通过全网的技术监测和机器学习能力，形成行业安全大数据，提升行业对新威胁的整体安全防护预警能力。

再次是整体安全水平明显提高。

通过平台的运行，可以实现主动防御、实战化协同防御，解决了网络资产不清、全网异常行为统一分析、全网各类威胁统一监测，网络威胁处置闭环管理机制等一系列问题，最终大幅度提升工控信息安全保障水平，形成一套完整的工控安全技术保障体系。同时，通过保障体系的实施做好规划引领，积极准备，合理部署，保证有效应对，由“被动查改”变“主动升级”，带来管理上的巨大红利。

最后是易被复制，推广价值和示范效应重大。

平台的全面推广，将实现从被动防御到积极防御、静态防御向动态防御的转变、分散防御向协同防御的转变，切实落实“大安全”示范工程项目工作，切实落实行业“十四五”规划网络安全综合防控能力，保障网络信息系统安全、可靠、平稳运行。

尤其在复制方面，该平台可以适用于 IT 网、OT 网及“两网融合”网络环境下，可以在已具备防火墙、网闸、工控安全监测等基础防护条件下均可复制，具有极强的推广价值和示范效应。

结束语

当前，在数字化转型加速，网络攻击愈发频繁，以及关基保护等合规要求下，烟草行业对网络安全的需求正在持续提升。该烟草公司作为当地先进制造、绿色制造的代表企业，加速落实行业“十四五”规划网络安全综合防控能力，通过商业工控安全一体化建设，实现了常态化“监、防、控”为一体的联动能力，有效应对“两化融合”的网络环境下全局监测各类安全风险，并可快速分析、预警和处置，构成“全网监测、协同联动”机制，全面应对各类安全风险，最终形成涵盖 OT 和 IT 两大网络，统一监测、全面感知、统一分析、统一响应、统一处置、自动联动处置的闭环防御体系。安

APT 攻击的关联分析，为什么不能只靠 ATT&CK

作为网络空间的公敌，APT 攻击自首次曝光以来，已经变得无孔不入，严重威胁着现有的网络安全体系。

不过随着行业对 APT 攻击研究的不断深入，APT 攻击的神秘面纱正在被一层层揭开，人们也在长时间的对抗中，找到了一些足以发现和对抗 APT 攻击的有效手段。

在常用的手段里，ATT&CK 框架可以说受到了很多人的青睐。

2013 年，MITRE 公司为了摆脱网络安全治理中防守方所面临的困境，基于现实中发生的真实攻击事件，创建了一个丰富的对抗战术和技术知识库，即 ATT&CK。ATT&CK 框架中明确记录了攻击者发起攻击所采用的战术、技术和子技术，并且战术、技术和子技术的种类一直处在迭代增加的过程中。

诚然，作为一个记录、总结攻击者技战术方法的知识库，ATT&CK 框架能够有效帮助安全分析人员跟踪攻击者的攻击活动。但在奇安信威胁情报中心看来，如果作为 APT 攻击分析的关键基石，它还差点意思。

记录事实的能力受限

在“教科书”上，ATT&CK 经常表现得无所不能。

一个用于展示 ATT&CK 的 Demo 里，一个攻击从初始的 Payload 投递、CC 连接到最终的数据外泄整个过程在产品里一目了然，各种日志和原始数据随时可下钻展现在你面前，还给出了在 ATT&CK 矩阵里的对应的条目，所有攻击细节都清清楚楚。

但别忘了，这个只是 Demo，成年人都应该知道 Demo 和实际到手的区别。就像医生看病，没有一个患者会按照教科书那样病得如此标准，所有症状、病程都严丝合缝。如果碰巧遇上一个，那一定能引来整个科室大半人的围观。

在实际的对抗过程中，受制于各种因素，绝大部分的组织采集威胁元数据的能力非常有限。无论是来自终端侧还是网络侧的告警，准确度先不论，最大的问题是这些告警本质上是观点而不是事实，换句话来说，就是

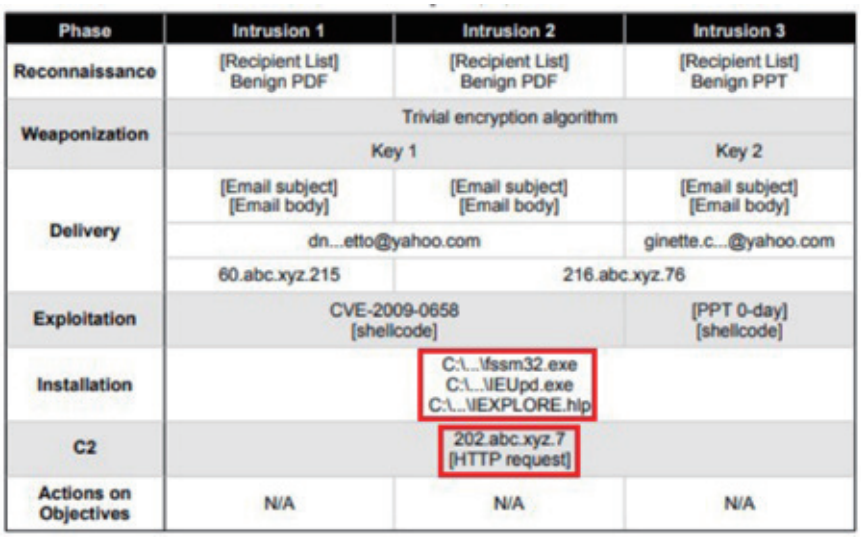
> APT 攻击关联分析的核心是看见细节的能力，而看见细节的关键在于获取信息量的能力。

机器基于已有规则对某些行为的判断。

在这种情况下，如果历史记录的原始信息收集不完整，一旦攻击者采免杀做得好，从而逃避了安全产品的检测，攻击环节一旦漏掉就会永远错过，所以大多数情况下很难看到攻击的全过程。

即便是做事后排查，断链也随处可见，关联分析更是无从谈起。

“无论是终端检测与响应 EDR，还是网络检测与响应 NDR，都在努力覆盖 ATT&CK 矩阵，它对于威胁检测和溯源分析的价值从来都不会有人去怀疑。”奇安信威胁情报中心表示。但是从 APT 分析的角度看，光看到环节本身是远远不够的，目击到一系列环节本身并不足以导向足够的区分度，甚至都不是关联归属的核心点所在。



Phase	Intrusion 1	Intrusion 2	Intrusion 3
Reconnaissance	[Recipient List] Benign PDF	[Recipient List] Benign PDF	[Recipient List] Benign PPT
Weaponization	Trivial encryption algorithm		
	Key 1		Key 2
Delivery	[Email subject] [Email body]	[Email subject] [Email body]	[Email subject] [Email body]
	dn...etto@yahoo.com		ginette.c...@yahoo.com
	60.abc.xyz.215	216.abc.xyz.76	
Exploitation	CVE-2009-0658 [shellcode]		[PPT 0-day] [shellcode]
Installation		C:\...\fssm32.exe C:\...\EUpd.exe C:\...\EXPLORE.hlp	
C2		202.abc.xyz.7 [HTTP request]	
Actions on Objectives	N/A	N/A	N/A

关联分析的核心在于细节

如前文所述，ATT&CK 本质上是一个描述攻击者技战术的知识库，目前正在经历由粗到细的进化，正向总结 APT 团伙的 TTP 对了解对手来说当然是有用的，但是从观察到的一些活动反向确认来源归属则是另外一回事。

因为 ATT&CK 所枚举的技术手段应该理解为 Key，除非手法本身已经有高度的独特性，不然绝大多数用于关联的特征存在于 Key 对应的 Value 或“参数”中，而不是手法本身。

下面是洛克希德 · 马丁公司提出的网络杀伤链 Kill Chain 文档中的一个基于鱼叉邮件渗透的关联分析，大多数 APT 活动都有鱼叉邮件的 Payload 投递，使其能被关联到一起的并不是大致的攻击过程环节，而是恶意代码执行阶段的特定文件名和 C2 阶段的同一个域名这些攻击“参数”。

这些分析所需细节的获取，是 ATT&CK 框架力所不能及的范围，这也是为什么说 ATT&CK 所提供的泛泛的 TTP 枚举对 APT 分析帮助不大的原因。

结合奇安信威胁情报中心跟踪 APT 活动近十年的实践，现阶段及在未来相当长的一段时间内，APT 关联分析还是基于强特征的。

什么是强特征，就是体现足够独特性的细节。

从信息论的角度看，特征的价值高低取决于其消除不确定性的能力，所以不是所有的特征都是平等的，比如知道已知某个攻击团伙的 C2 域名用到了某个域名注册商远不如知道其用到了某个特定 IP，因为域名注册商并不只服务于攻击者，而 IP 在特定阶段只被特定攻击者使用，排他性消除了很大部分不确定性。

比如以下几种。

· 非常特定的目标

特定的行业和人群，如沙特的某些异见人士经常成为 NSO 工具的对象，攻击来源可以非常容易地猜测到。

· 只被某特定团伙使用的数字武器

如海莲花团伙以前所使用的 Denis 家族木马（现在基本都用商业产品 CobaltStrike 了）；恶意代码在机器上执行过程中输出的特征数据，

如互斥体、执行路径、命令参数、创建的文件和注册表项等。

· 已有明确归属的网络资源

攻击者使用的特定IP、域名、邮箱、社交账号、服务器及相应的“业务系统”，目前的 IOC 主力就是这类数据。

Paragraph	Nodel	Relation	Node2	Time
2	Jin Hyok Park	alias of	PARK JINHYOK	
2	Pak Jin Hek	alias of	PARK JINHYOK	
2	PARK	alias of	Pak Jin Hek	
6	PARK JINHYOK	Related	Chosun Expo Joint Venture	
6	Korea Expo Joint Venture	alias of	Chosun Expo Joint Venture	
6	Chosun Expo	alias of	Chosun Expo Joint Venture	
6	PARK	employed by	Chosun Expo Joint Venture	
6	Chosun Expo Joint Venture	related to	DPRK	
	SPE	alias of	Sony Pictures Entertainment	
13	Lazarus Group	attacked	SPE	201411
13	Lazarus Group	attacked	Bangladesh Bank	201602
13	Symantec	Reported	Lazarus Group	
13	Novetta	Reported	Lazarus Group	
13	BAE	Reported	Lazarus Group	
16	ttykim1018 @gmail.com	tied to	PARK	
16	tty198410@ gmail.com	used with	Kim Hyon Woo	
16	Chosun Expo Accounts	Contains	ttykim1018 @ gmail.com	
37	North Korean IP Address #5	linked to	DDNS Domains	
37	Contopee	used	DDNS Domains	
37	Polish Banking Sector Campaigt used	used	Contopee	
37	Group IB	Reported	Polish Banking Sector Campaign	
37	North Korean IP Address #3	Accessed	Chosun Expo Accounts	
37	North Korean IP Address #7	Accessed	Chosun Expo Accounts	
37	North Korean IP Address #4	used by same subject	North Korean IP Address #7	
37	North Korean IP Address #8	referred by	North Korean IP Address #7	
39	Brambul	referred by	W32.Brambul.A	
39	Brambul	accessed	Trojan/Brambul-A	
39	Brambul	attacks	SMTP protocol	
40	Brambul	Uses	SMTP protocol	
41	Brambul	uses collector email account	mrwangchung01@ gmail.com	
41	Brambul	uses collector email account	mrwangchung01@ gmail.com	
41	Brambul	uses collector email account	laohu1985 @ gmail.com	
41	Brambul	uses collector email account	diver.jacker @ gmail.com	
41	Brambul	uses collector email account	whiat1001 @ gmail.com	
41	North Korean IP Address #6	accessed	mrwangchung01@ gmail.com	2017
41	North Korean IP Address #7	accessed	diver.jacker@ gmail.com	20161114
41	North Korean IP Address #7	accessed	diver.jacker@ gmail.com	20161216
41	xiake7220 gmail.com	created from same North Korean IP Addres laohu19850 gmail.com	laohu1985@gmail.com	2009
41	Brambul	attacked	SPE	
52	North Korean IP Address #6	aocessed website	Lockheed artin	
52	North Korean IP Address #6	online searched persons	Lockheed artin	
52	North Korean IP Address #6	sent message to emplovees	Lockheed artin	
57	yardgen @ gmail.com	sent test spear-phishing email to	tty198410@ gmail.com	
57	yardgen @ gmail.com	used	http://www.fancug.com link/facebook en.htr	
57	Kim Hyon Woo	used with	tty198410@ gmail.com	
58	http://www.DOMAIN REDA linked	linked	Google's Drive Service	
63	Frank David	sent spear-phishing email to	SPE	20141121
63	Frank David	used	Proxy IP Address	
64	GOP	alias of	Guardians of Peace	
64	SPE	compromised by	GOP	20141124
66	SPE	compromised Twitter by	GOP	20141124
67	GOP	sent email to emplowees	SPE	20141126

· 源操控能力的手法

0day 的使用，BGP 的劫持，甚至海底光缆的窃听，从能力上体现出来的鹤立鸡群。

上面这些特征的列举暗合了钻石模型的分析需求，钻石模型定义了对手、能力、基础设施和受害者这四个核心对象，给出了它们之间的 Pivot 交互方式。分析人员按照其约束的 Pivot 方向循环挖掘相关的特征信息，确认其中的 Overlap，这才是关联归属分析比较有成效的工作方法。

元数据为王

综上所述，APT 攻击关联分析的核心是看见细节的能力，而看见细节的关键在于获取信息量的能力。有了足够的细节，分析方法上其实并不需要多复杂。

随着摩尔定律主导下的计算存储成本的指数级降低，以及支持大数据处理技术的完善，我们因此拥有了足够的大数据搜集、存储和计算分析的能力，从而进入了元数据为王的时代。

左侧表格展示了当年美国司法部用于起诉 Lazarus 团伙成员而搜集的部分数据。从中可以看出，美国司法部展现了相当强大的元数据搜集能力

· 特定 IP 的访问记录
· 特定 IP 与社交账号的关系
· 人员所使用的 IP
· 人员使用的社交账号
· 人员的邮件记录
· 人员的社交信息收发
· 人员的搜索记录

有了这些数据之后，安全分析人员可以非常清楚地看到 APT 攻击所使用的基础设施、攻击手法等，就像拼乐高积木一样，这远比强行使用粗糙的 ATT&CK 的 TTP 枚举有意义。安

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

报告：数据合规驱动隐私科技行业迅猛发展

作者｜安永 & 赛博研究院

近年来，数据要素的重要程度提升，数据流通与安全合规之间的不对称呈现加剧的趋势，让全球范围内的隐私科技和数据合规产业也迎来了迅猛发展。《全球数据合规与隐私科技发展报告》梳理了国内外数据安全与算法应用的合规体系，对隐私科技的概念、内涵和外延进行更新，并为国内外企业数据合规实践提供参考案例与创新思路。

摘要

＊全球近 100 个国家和地区已制定数据保护相关法律，数据安全、算法应用有关立法进程加快，合规本地化的全球性趋势将进一步加强。

＊企业更加重视数据合规与隐私保护，22% 的企业直接向高级管理层汇报工作，82% 的企业认为在过去 12 个月的投入满足需求。

＊隐私计算在更多风险控制和数据流通等业务场景中发挥着重要作用，并在元宇宙、工业互联网与区块链等新兴科技中崭露头角。

＊从隐私科技产业发展来看，数据分类分级、数据流通监控、数据风险与隐私影响评估、数据与隐私综合治理是当前的热门细分赛道。

隐私科技概念图示（2022 版）

一、企业数据合规与隐私保护面临四大挑战

第一，需适应不断发展变化的法律法规：首先是适应全球不断发展变化的法律法规，其次是适应“当地”法律法规。跨国企业在不损害国家安全、公民个人信息安全的前提下，要以“安全合规本土化”为原则，提升企业境外市场的综合竞争力。

第二，高昂合规成本带来的经济压力：企业为了适应日益严格的监管与处罚，面临更大的经济压力。一是表现在不合规成本支出上，即支付因违规带来的高额罚款。二是表现在企业在数据合规与隐私保护工作上投入更多预算，对于初创企业或中小企业来说更明显。

第三，复杂的第三方风险管理挑战：企业不仅面临自身的内外部安全威胁，还需要承担第三方数据处理者因供应链攻击或数据安全合规能力不足而产生的风险，尤其在网络安全、数据合规、隐私保护方面，影响更加明显。

第四，数据频繁流动引发的安全威胁：在数据流通利用过程中，部分企业由于安全管控措施不足、数据可信流通能力建设滞后，导致企业的风

险暴露面增加，造成数据泄露、隐私泄露等风险。

二、全球 75% 人口将受“数据安全保护专项立法”保护

统计显示，目前全球已有近 100 个国家和地区制定了数据安全保护相关法律，数据安全保护专项立法成为国际惯例。到 2024 年，全球 75% 的人口将在个人数据方面受到隐私法规的保护。

随着数据作为生产要素的价值愈发凸显，数据立法不仅针对个人信息保护，而是已经广泛地涵盖公共数据开发利用、企业数据共享流通、个人数据保护（包括个人信息及个人隐私数据）等多个场景。

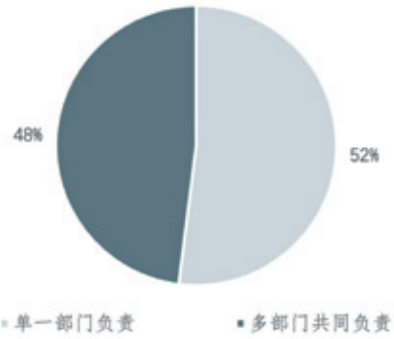
2023 年以来，全球数据安全相关立法进程再次提速，一方面通过推动数据流通、共享、开发利用充分释放数据红利，另一方面通过分行业分场景、分企业推动重点监管。

另外，隐私科技的市场需求虽然越来越大，但其市场应用仍然面临着推广困难的问题。应从法律规则层面进行先行引导和规划，具体措施包括提高数据的匿名化程度、增强算法规则可解释性和遵循应用伦理先行原则等。

三、企业隐私保护现状：汇报层级大幅提升、投入日趋满足需求

数字化时代，数据合规与隐私保护成为企业关注的一大重点，为了更好地遵守发展变化的法律法规要求，同时增强客户体验，不少企业将数据合规和隐私保护视作企业的生命线。

1、数据合规与隐私保护职能所属部门呈多元化。信息安全部门、法务部门和合规部门仍是数据合规与隐私保护的主责部门，但考虑到数据合规与隐私保护工作的复杂性和学科交互性，在 48% 的被调查企业当中，数据合规与隐私保护工作由多部门共同负责。



企业数据合规与隐私保护职能模式

2、数据合规与隐私保护工作直接汇报层级越来越高。22% 的被调查企业数据合规与隐私保护职能直接向企业高级管理层（董事会或企业法人）汇报，而去年仅有 9% 的企业直接汇报到高级管理层，该比例增长了2倍多。

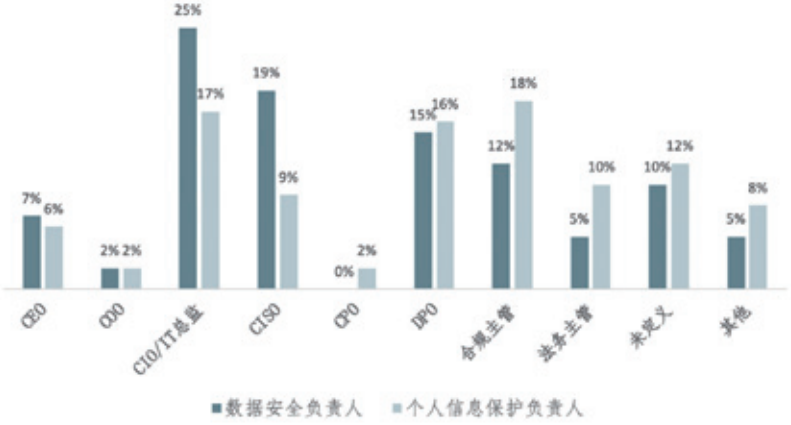
3、大部分企业已委任数据安全负责人和个人信息保护负责人。研究发

企业数据合规与隐私保护职能直接汇报工作的角色比例

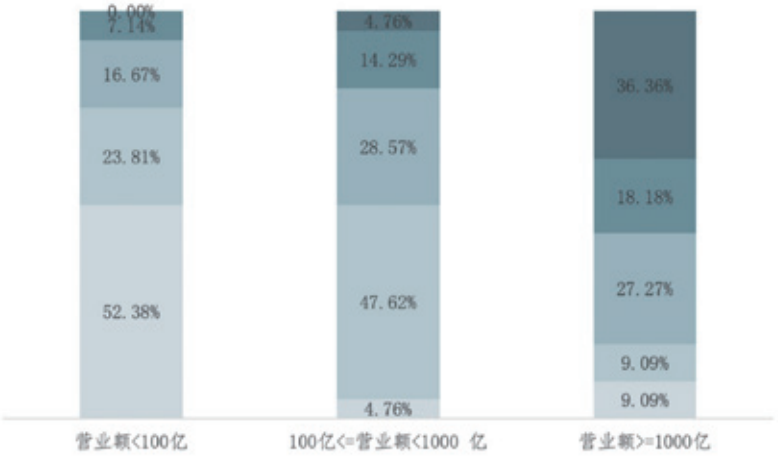
现，大部分被调查企业已委任数据安全负责人（90%）和个人信息保护负责人（88%）。

4、企业负责数据合规与隐私保护工作的人员数量逐年提升，随着企业营业额的增加而增多，但仍存在人才缺口。而人员问题，也成为了部分企业无法满足实际的数据合规和隐私保护工作需求原因之一。

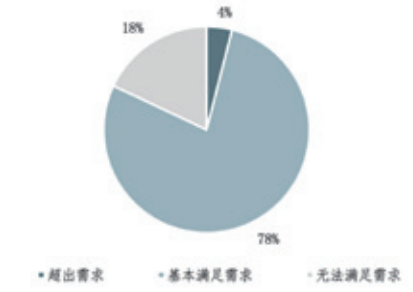
5、数据合规与隐私保护的投入日趋满足实际需求。82% 的被调查企业认为公司在过去 12 个月内数据合规与隐私保护方面的投入基本满足需求或超出需求，而去年这个比例仅为 52%。



数据安全负责人和个人信息保护负责人的设立



企业数据合规与隐私保护工作的人员数量分布图（单位：人民币）



过去 12 个月企业数据合规与隐私保护的投入满足需求程度

6、数据合规与隐私保护成熟度逐步提升。在制度建设方面，有 92% 的被调查企业定义了相关方针政策及管理制度与操作规程。在制度执行情况和效果方面，大部分（81%）被调查企业对制度要求进行了落实执行，相比去年（74%）有所提升。

7、企业积极开展数据出境安全评估工作。随着 2022 年 9 月 1 日《数据安全评估管理办法》的正式实施，适用该办法大部分（75%）被调查企业都进行了积极响应。其中 42% 的被调查企业处于数据出境安全评估工作前期，17% 的被调查企业已完成了评估，16% 的被调查企业已经开始进行安全评估申报。

四、未来展望：隐私科技产业正驶入快车道

预计未来 5~10 年，隐私计算技术会被大规模商业化应用。到 2025 年，60% 以上的大型组织将在数据分析、商业智能或云计算中，使用一种或多种隐私计算技术。

市场层面：数据合规即服务衍生新的商业机会，继网络即服务、网络安全即服务等商业市场蓬勃发展，数据合规即服务将成为未来重要商业模型之一。

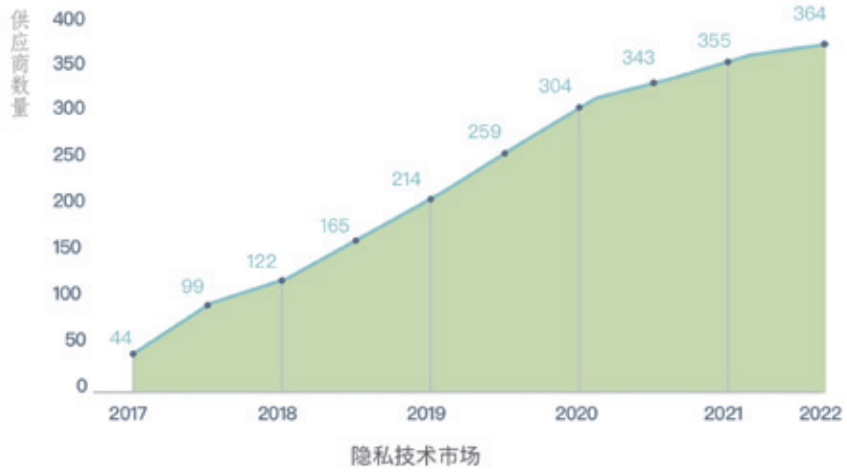
应用层面：随着科技的发展，企业隐私保护理念逐步拓展，将安全前置，将数据合规贯穿于数据安全生命周期，成为数据合规与治理的重要思路。

人才层面：人才市场的供需明显不对称，将激发培训服务的增长，积极开展外部人才引进和内部人员定期隐私保护的相关培训，成为企业完善数据安全能力、推动合规实践的必然举措。

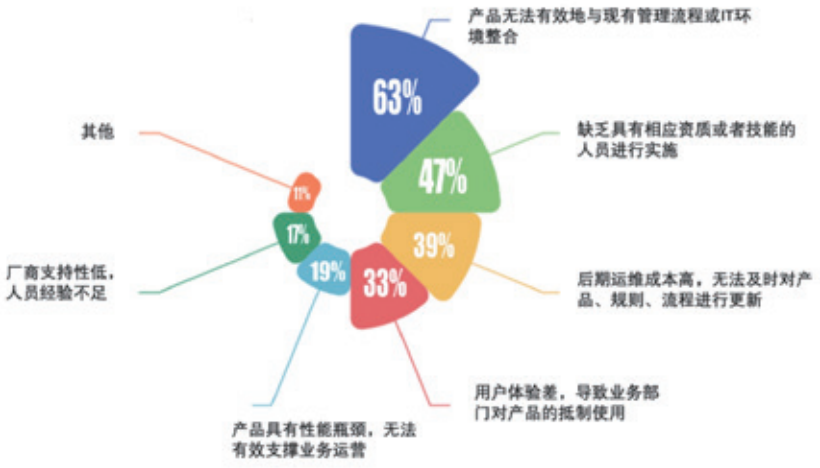
标准层面：未来超大规模云提供商，将进一步提供可信的执行环境，帮助越来越多上云企业，在云环境获得安全性和隐私性的保障。

技术层面：开源生态在隐私科技的“商业化蓝图”中发挥着重要作用，隐私计算的发展路径将与技术开源休戚与共。

产业层面：当隐私科技的行业应用达到一定规模之后，将构建一个庞大的数据智能网络生态，降低个人信息合规成本，创造更多的业务发展可能性。安



2017–2022 年隐私技术供应商增长情况（IAPP）



企业实施隐私科技面临的挑战

大事记

奇安信亮相 2023 中国 5G+ 工业互联网大会

以“数实融合 大力推进新型工业化”为主题的 2023 中国 5G+ 工业互联网大会于 11 月 19 日至 21 日在湖北武汉举行。奇安信集团作为网络安全领军企业，受邀出席本次大会。

在 5G+ 工业互联网赋能未来产业创新发展专题会议上，奇安信集团总裁吴云坤表示，5G+ 工业互联网已经成为工业转型升级的核心驱动力，在新技术与工业场景和业务融合的过程中，迫切需要网络安全、网络通信、信息化、工业控制等不同领域在一起，从业务出发进行融合技术和方法创新，共同保护 5G+ 工业互联网安全。

由奇安信集团承办的数据安全平行会议在大会期间同步举行。

齐向东：“一个体系、一套系统、一支队伍、三级联动”实现数据安全“内管外防”

在 11 月 16 日举行的 2023 数字经济峰会上，齐向东表示，面对数据安全的“内忧外患”，要用“一个体系、一套系统、一支队伍、三级联动”实现“内管外防”，护航数字经济行稳致远。

一个体系指的是纵深防御的内生安全体系；一套系统指的是全链条的数据安全保护系统；一支队伍指的是“人 + 智能”的高水平运营队伍；三级联动指的是三级联动的网络安全运营指挥体系。

会上，河南投资集团与奇安信集团签署了战略合作协议。双方将发挥各自能力与优势，围绕企业数字化转型、网络安

全人才培养、网络安全运营等方面开展深入合作，协力助推河南网络安全上下游产业集群式发展。

由奇安信集团主办的网络和数据安全论坛同步举行。

凯捷集团 (Capgemini) 全球副总裁一行到访奇安信安全中心

总部位于法国的凯捷 (Capgemini) 是欧洲第一的管理

咨询、技术和服务供应商。11 月 14 日，凯捷全球副总裁陈友合（Huu-Hoi Tran）一行到访奇安信安全中心。

陈友合表示，凯捷作为全球众多头部汽车企业的咨询、技术和工程解决方案提供者，引领着产品研发、创新商业模式、用户服务体系等广泛领域的数字化转型步伐，并将转型带来的收益带给各大汽车行业的客户。期待与奇安信展开长期友好合作，全方位的为各汽车行业客户在安全策略、产品安全合规及安全风险验证等领域一起保驾护航。

中标全国海关浏览器采购 企业浏览器成为网络安全新赛道

近期，奇安信中标全国海关企业浏览器采购项目。该项目覆盖了海关总署及 40 多个直属单位，部署包含终端总数超过 18 万点。本项目奇安信独家中标，充分体现了奇安信可信浏览器作为办公基础软件，可以深入业务场景，持续为客户提供包括业务系统承载平台、统一安全管控等丰富的产品价值。

奇安信圆满完成 2023 中国国际进口博览会网络安全保障任务

11 月 10 日，2023 中国国际进口博览会顺利闭幕。本次进博会期间，有超过 3400 家企业参展和近 41 万名专业观众注册报名，参展的世界 500 强、行业龙头企业及创新型中小企业，数量均为历届之最。作为网络安全“国家队”，奇安信统一思想、提高认识、强化管理、狠抓落实，圆满完成了此次进博会的网络安全保障任务。

截至目前，奇安信已完成了 2022 北京冬奥会和冬残奥会、建党 100 周年、国庆 70 周年、全国两会、春晚、中非合作论坛、上合组织成员国峰会等国家级网络安全保障任务，用自己的能力和行动捍卫着国家和企业的网络安全。接下来，奇安信必将继续肩负国家使命，践行企业社会责任，为国家重大活动提供专业的网络安全保障服务。

奇安信亮相 2023 年世界互联网大会乌镇峰会

11 月 7 日 ~10 日，2023 年世界互联网大会乌镇峰会，在浙江省乌镇举行。奇安信携新产品、新形象、新方案、新思考，深度参与开幕式、论坛演讲、产品发布、“互联网之光”博览会等环节。

在网络空间技术发展与国际合作论坛上，奇安信集团总裁吴云坤表示，应对网络空间对抗升级，需要建设和发展五大能力，多方相互协同支撑，建立起国家级网络安全能力体系，保护网络空间安全。

在下一代前沿数字技术创新与安全论坛上，吴云坤表示，工业级大模型应用可以解决安全生产力短缺的问题，但需要以大模型应用安全作为生产力输出的前提和基础。只有将既有网络安全知识和能力、网络安全实战场景和实践充分结合、深度融合，才能真正让大模型应用落地，解决网络安全生产力短缺难题。

在下一代互联网创新发展论坛上，奇安信集团总裁吴云坤表示，安全是下一代互联网发展的基础和保障，下一代互联网面临“看不见”“理不清”“防不住”三大安全威胁，需要通过持续的技术创新来解决问题，保护互联网安全。

在“互联网之光”博览会上，奇安信举办了 NGSOC 产品战略升级发布会，首次发布中英文双语版 NGSOC，提供一致的安全运营能力支撑。

奇安信受邀出席 2023 数字科技生态大会 达成云网融合深度科技创新合作

11 月 10 日，奇安信受邀出席由中国电信、广东省人民政府主办的 2023 数字科技生态大会，与中国电信在“云网融合大科创装置”达成科研创新合作，并共同发布《软件供应链安全产品白皮书》。

齐向东：防护体系化是应对网络安全挑战的“金钥匙”

11 月 1 日，全国信息安全标准化技术委员会 2023 年第二次“标准周”全体会议在湖北武汉召开。齐向东表示，数智时代，安全挑战前所未有，防护体系化作为迎接网络安全挑战的“金钥匙”，需要通过标准让防护体系真正发挥防护能力，具体要从纵深防御体系化、行为管控体系化、数据保护体系化、安全运营体系化四个方面落实。

Z 世代接棒再破纪录 “天府杯”网络安全大赛落下战幕

经过两天的激烈赛程之后，2023“天府杯”国际网络安全大赛于 11 月 1 日在成都天府国际会议中心落下帷幕。大赛创下了历届大赛的多个“首次”：首次覆盖国内主流安全防护产品和办公类供应链软件、系统，国内主流安全厂商首次为比赛提供产品支持，知名高校战队首次参与产品破解赛，首次设立监督委员会。更值得称赞的是本届大赛战队呈现年轻化趋势，以 95、00 后等 Z 世代为参赛选手的主力军，也将大赛推向新的高度。

在开幕式上，奇安信集团董事长齐向东表示，漏洞是难以避免的，数智时代的大背景下，传统安全防护存在着短板，要坚持走网络安全的体系化之路，构建起数智时代的网络安全防线。

奇安信集团旗下陕西洞鉴云侦科技有限公司荣获 CMA 资质认定

10 月 27 日，经陕西省市场监督管理局正式批准，奇安信集团旗下的陕西洞鉴云侦科技有限公司顺利通过 CMA 计量认证，正式获得检验检测机构资质认定证书。

至此，陕西洞鉴云侦已具备电子数据领域各项鉴定项目的检测资质。

奇安信 10 大领域入选 Gartner®2023 中国安全技术成熟度曲线报告

近 日，Gartner 发 布《Hype Cycle™ for Security in China, 2023》，对国内 20 项热门网络安全技术发展阶段进行了深度分析。其中，奇安信共计在 10 项细分赛道（去年数量为 8），被 Gartner 认可为代表厂商 (Sample Vendors)，包括云安全资源池、中国 CPS 安全、攻击面管理 ASM、软件成分分析 SCA、IoT 身份认证、安全服务边缘 SSE、SASE、态势感知、CWPP 云工作负载保护平台和攻防团队。

第七届“蓝帽杯”全国大学生网络安全技能大赛圆满落幕

10 月 29 日，第七届“蓝帽杯”全国大学生网络安全技能大赛决赛及颁奖仪式在中国人民公安大学圆满落幕。来自全国 33 所公安院校与地方知名高校的 92 支队伍同场竞技，

选拔出一、二、三等奖及杰出指导教师和优秀指导教师奖，并为获奖师生颁发了荣誉证书及奖杯。

为提升参赛学生对真实涉网犯罪场景问题的发现和解决能力，本次决赛采用了综合渗透赛赛制，同时根据真实案例改编，模拟复刻公安机关“亮剑”打击整治专项行动的真实网络环境，更加强调实战和实际业务场景结合；赛题方面，首次推出网络反诈相关场景创新赛题，包括“仿真博彩系统”“仿真棋牌场景”“交易平台”“借贷支付平台”等，考察参赛学生在创新场景中的应变能力和综合技术水平。

中国职业技术教育学会网络安全专业委员会成立 奇安信任执行主任单位

10 月 24~25 日，中国职业技术教育学会网络安全专业委员会成立大会在重庆举行，奇安信集团被选举为网络安全

专业委员会执行主任单位。

全国网络空间安全行业产教融合共同体第一次理事会同期举行。会议全体审议表决通过了《网络空间安全行业产教融合共同体章程》，审议表决了网络空间安全行业产教融合共同体理事长、副理事长单位，讨论了共同体《2023—2025年工作目标及规划》《2023—2024年重点工作任务》。中国职业技术教育学会会长、教育部原副部长鲁昕为奇安信集团、北京理工大学、重庆电子工程职业学院3家理事长单位授牌。

千万级项目 奇安信16类产品中标河北联通网络安全集采

近日，河北联通公布了2023—2024年河北联通网络安全设备集中采购项目结果，奇安信集团旗下网神公司以综合排名第一的成绩，成为该项目第一中标候选人，项目规模为千万级。

中标产品涵盖了防火墙、天擎、态势感知、VPN、上网行为管理、WEB安全、堡垒机等16类主流产品，这也是奇安信在运营商行业的又一重大突破，为该行业网络安全综合建设树立了新的标杆示范。

荣誉墙

奇安信牵头项目荣获北京市科学技术奖

近日，北京市政府公布关于2022年度北京市科学技术奖励的决定，由奇安信科技集团股份有限公司牵头申报的“基于应用程序接口精准检测和高效动态防护的云安全关键技术与应用”项目获得北京市科学技术进步一等奖，是本年度一等奖项目中唯一的网络安全项目。同时，这也是首个由奇安信牵头、获得省部级科学技术一等奖的项目。

序号	获奖编号	项目名称	提名者	完成单位	主要完成人
5	2022-J02-1-00	基于应用程序接口精准检测和高效动态防护的云安全关键技术与应用	北京市西城区人民政府	奇安信科技集团股份有限公司 中国科学院信息工程研究所 北京数字认证股份有限公司 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） 奇安信网神信息技术（北京）股份有限公司 北京数字认证股份有限公司	刘 勇 刘 浩 贾晓启 朱 江 张永振 魏坤元 闫 雷 刘文强 吴 震 孙宇彤 刘洪奎 杨 波 周 灿 高 山 张 凯

奇安信隐私合规解决方案荣获CCIA优秀创新成果大奖

奇安信集团旗下奇安盘古（上海）信息技术有限公司，凭借移动应用隐私合规解决方案，在中国网络安全产业联盟（CCIA）组织的“2023年网络安全优秀创新成果大赛”总决赛中，作为典型的个人信息保护合规解决方案荣获优胜奖。

从创新成果大赛总决赛名单中看，奇安信集团的“移动应用隐私合规解决方案”是得奖项目里唯一面向于移动互联网应用程序（App）个人信息处理活动合规检测的解决方案，为监管调查、企业审查、开发者自查提供一站式全面保障。

《漏洞》第二版入选 2023 年中央企业科普作品

近日，为加强中央企业科普能力建设、提升中央企业科普形象，国务院国资委举办了 2023 年中央企业科普作品选拔活动。由奇安信集团董事长齐向东所著的《漏洞》第二版作为网络安全方向唯一的科普书籍，入选“央企科普图书”板块。

赛迪报告：奇安信多赛道持续领跑

近日，赛迪顾问发布了《2022—2023 年中国网络信息安全市场研究年度报告》（以下简称《报告》）。《报告》显示，2022 年，中国网络信息安全市场依然保持增长，整体市场规模达到 920.0 亿元，同比增长 7.2%。

其中，奇安信集团以 62.2 亿元的营业收入位居市场第一位，销售额占市场总收入 6.8%，并且在终端安全、安全管理平台和安全服务等多个热门细分赛道，都占据了领头羊位置，在 UTM、Web 安全等传统安全硬件市场也位居前二。

连获五项荣誉 奇安信亮相 2023 工业信息安全大会

11 月 2 日，由国家工业信息安全发展研究中心、工业信息安全产业发展联盟主办的 2023 年工业信息安全大会在北京举行，并对优秀成员单位和行业优秀案例进行表彰。

凭借在工业信息安全领域长期积累的技术和能力优势，奇安信获得“2023 年优秀联盟成员单位”和“2023 年度优秀技术支撑单位”荣誉称号，并入选了国家工业信息安全漏洞库（CICSVD）2024 年度技术组成员单位。

同时，由奇安信为某原油储运公司打造的工控安全体系化建设项目获评“2023 年工业信息安全优秀应用案例”，为某民航行业单位打造的数据安全态势感知体系建设方案获评“2023 年数据安全典型应用案例”。

2023 年数据安全服务前五家企业名单发布 奇安信蝉联第一

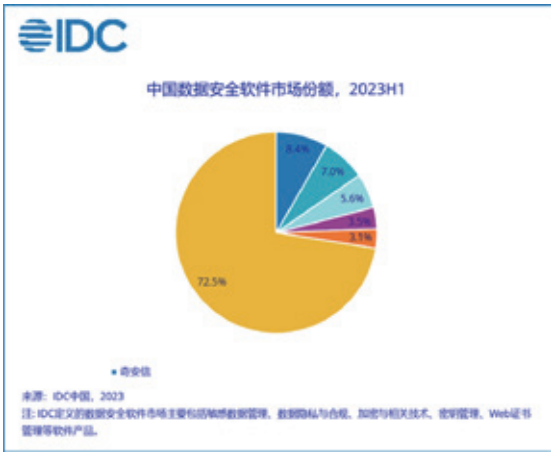
10 月 26 日，由中国互联网协会主办的中国互联网企业综合实力指数（2023）发布会暨百家企业论坛在厦门举行。会上发布了《2023 年中国互联网企业综合实力指数报告》，作为报告的重要研究成果，中国互联网综合实力企业、中国互联网成长型企业与数据安全服务企业名单同步发布。奇安信连续两年位居数据安全服务企业名单第一。

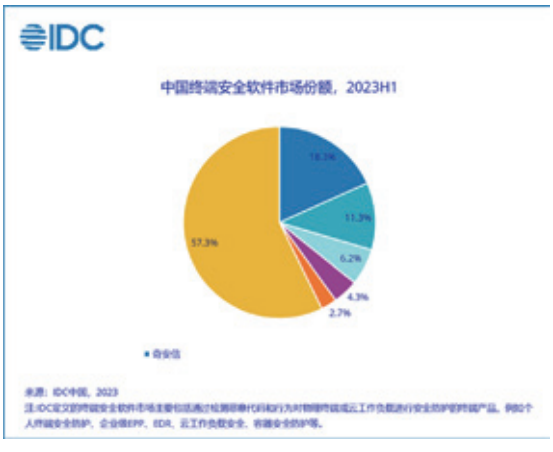
为加强推进互联网产业发展，中国互联网协会已连续 11 年开展中国互联网企业综合实力研究工作。其中，数据安全服务企业名单自 2022 年开始发布，围绕业务规模、成长能力、

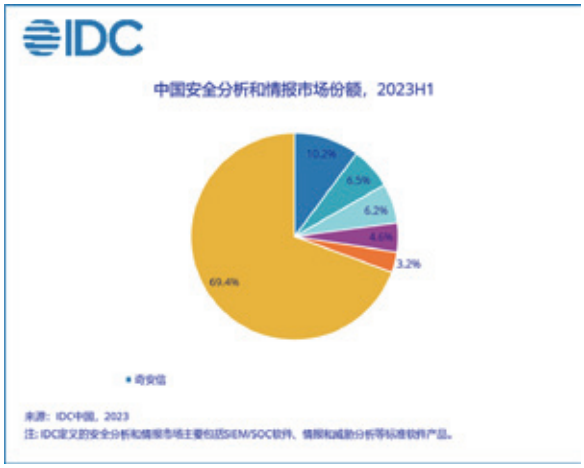
创新能力、社会责任等方面进行综合评价。连续两年入选并位居第一，是行业对奇安信数据安全产品、服务及综合能力的极大认可。

三项第一！奇安信 IT 安全软件市场份额持续扩大

近日，IDC 发布了《2023 年上半年中国 IT 安全软件市场跟踪报告》（以下简称《报告》）。《报告》显示，2023 年上半年中国 IT 安全软件市场规模为 107.8 亿元（约合 15.6 亿美元），同比上升 7.8%。其中，奇安信在数据安全、终端安全、安全分析和情报三大子市场位居第一，市场份额分别为 8.4%、18.3% 和 10.2%，是唯一一家占据三项头名的入围企业。







奇安盘古获评中国反网络病毒联盟“杰出工作单位”

近日，中国反网络病毒联盟对外发布了 2022 年中国反网络病毒联盟优秀成员单位名单。奇安信集团旗下奇安盘古作为中国反网络病毒联盟成员单位，凭借其在 2022 年度移动应用程序安全检测工作中的突出贡献，被授予“2022 年度中国反网络病毒联盟杰出工作单位”荣誉称号。

奇安信入选全球终端安全代表供应商

近日，某权威咨询机构在其发布的一份终端安全报告

中，推荐了来自全球范围内的数十家具有代表性的终端安全供应商及旗下终端安全产品，微软、思科、Crowdstrike、PaloAlto 等全球知名企业均位列其中。

其中，奇安信凭借旗下天擎终端安全管理系统脱颖而出，成功被推荐为全球终端安全代表供应商。据 IDC 数据显示，天擎已连续五年独占国内终端安全市场鳌头。此次入围，意味着天擎已步入全球头部终端安全产品之列。

社会责任

心安助农 · 内蒙古巴林左旗乡村振兴项目赴经棚镇、乌兰达坝深入调研

为助力巴林左旗高质量、可持续发展，10 月下旬，北京奇安信公益基金会秘书长梅冬与中国社会科学院社会学所研究员、农禾之家农村发展基金会理事长杨团及其专家团队一行 8 人，与赤峰市巴林左旗统战部副部长昭日格图、乌兰达坝苏木党委书记斯钦巴特尔、苏木党政班子成员及嘎查书记共 20 余名巴林左旗党政班子成员，一起赴内蒙古赤峰市克什克腾旗经棚镇调研。

在完成克什克腾旗经棚镇考察学习后，奇安信基金会委托农禾之家专家团队，与巴林左旗主管干部和乌兰达坝苏木党政班子成员，带着最新学习的经验和思路，深入乌兰达坝苏木进行第二次实地调研，切实了解当地农牧户的发展困难与需求，为制定科学有效的“乌兰达坝苏木乡村振兴三年规划”提供进一步依据。

未来，奇安信基金会“心安助农 · 内蒙古巴林左旗乡村振兴”项目将利用三年时间，委托专业团队，帮助乌兰达坝苏木做规划、育团队、促产业、稳生态，陪伴乌兰达坝苏木巩固脱贫攻坚成果，把乡村振兴的道路走实、走宽。乌兰达坝苏木拥有独特的自然资源优势，发展农牧产业大有可为，相信通过后续的项目合作，坚持一张蓝图干到底，以实际行动推动苏木产业发展，协助乌兰达坝苏木成为内蒙古自治区乡村振兴的新典范。

奇安信基金会积极开展路口文明引导志愿服务活动

11 月 1 日，北京市西城区启动 2023 年“文明交通 安全出行”宣传周系列活动，进一步加强电动自行车骑乘人员安全意识和安全防护水平，预防和减少道路交通事故，营造文明交通环境，助力建设更高水平的全国文明城区。11 日 3 日周五下午，北京奇安信公益基金会组织志愿者，在展览馆路和车公庄大街交叉口开展了路口文明引导志愿服务。

美国爱因斯坦计划跟踪与解读（2023 版）

作者 | 叶蓬

引言

本文在 2022 年版本的基础上进行了较大修订，全面更新了爱因斯坦计划的相关数据，反映了 2022 年以来的最新进展，尤其是替代 NCPS 的 CADS 计划。

一、项目概述

爱因斯坦计划，其正式名称为“国家网络空间安全保护系统”（NCPS），是美国“全面国家网络空间安全行动计划”（ CNCI）的关键组成部分。

NCPS 以 DFI、DPI 和 DCI 技术为抓手，以大数据技术为依托，以威胁情报为核心，实现对美国联邦政府民事机构互联网出口网络威胁的持续监测、预警、响应与信息共享，以提升联邦政府网络的态势感知能力和可生存性。

NCPS 由美国国土安全部（DHS）下属的网络安全与基础设施安全局（CISA）负责设计、运行和协调。借助 NCPS，美国联邦政府为其互联网侧态势感知构建起了四大能力：入侵检测、入侵防御、安全分析和信息共享。

1. 入侵检测

NCPS 的入侵检测能力包括爱因斯坦 1（简称 E1）探针中基于 Flow 的检测能力、爱因斯坦 2（简称 E2）和爱因斯坦 3A（简称 E3A）探针中基于特征的检测能力，以及 2015 年启动的在 E1、E2 和 E3A 中基于机器学习的行为检测能力（代号 LRA）。

2. 入侵防御

NCPS 的入侵防御能力是从爱因斯坦 3A（简称 E3A）阶段开始的。

NCPS 的入侵防御不是一般意义上的入侵防御系统（IPS），主要包括 4 种能力：恶意流量阻断、DNS 阻断、电子邮件过滤、Web 内容过滤（WCF）。

3. 安全分析

NCPS 的安全分析能力主要包括：安全信息与事件管理（SIEM）、数字

> 随着攻击面日益扩大， 攻击手法日趋复杂，
> 现有的 NCPS 系统功能已经落后，
> 架构也再难以扩展以满足新的需求。

媒体分析环境、高级恶意代码分析中心（AMAC）、各种分析工具可视化工具等。

4. 信息共享

信息共享就是情报共享，这是NCPS的核心能力。NCPS的信息共享能力主要包括：自动指标共享（AIS）、指标管理平台（IMP）、统一工作流、跨域解决方案（CDS）等。

二、从NCPS到CADS

随着攻击面日益扩大，攻击手法日趋复杂，现有的NCPS系统功能已经落后，架构也难以再扩展以满足新的需求。NCPS存在两个关键的缺陷：（一）前端难以检测未知威胁；（二）后端难以处理为实现全面可见性而引入的天量多源数据。尤其是Solarwinds攻击事件对美国联邦政府造成了较大的影响，而NCPS并未在开始阶段及时发现攻击。为此，NCPS近些年来一直受到质疑。因此，CISA在2024财年的预算申请中首次正式提出了NCPS的替代计划——网络分析与数据系统（CADS）。而根据美国政府问责局（GAO）对国土安全部（DHS）的年度评估报告，早在2021年7月CADS计划便已形成，但直到2023年初提交FY2024预算时才公开。

CADS可以看作是对前述NCPS缺陷二的直接回应，并能够间接提升缺陷一的未知威胁检测能力。CADS是一个系统之系统（system of system，是一个系统工程领域的术语），它提供了一个强大且可伸缩的分析环境，能够集成数据集并提供工具和功能。CADS工具和能力将促进数据的摄取和集成，并通过对数据分析（过程）的编排和自动化，以支持快速识别、检测、缓解和阻断恶意网络活动。

总的来说，CADS基于数据驱动安全的思想，采用云计算架构，应用DevSecOps的运营模式，通过统一数据平台实现对包括NCPS入侵检测和防御信息、CDM EDR信息、情报、情境数据在内的CISA内外部多源天量数据的摄取、集成、建模和治理，掌握更全面的态势信息；通过对各种工具集的智能编排与自动化，实现便捷灵活的安全分析、情报融合与共享；通过编排和自动化实现对攻击和恶意行为的阻断与缓解；通过基于DevSecOps的CI/CD管道，以及策略即代码的方式，使得开发团队能够快速集成并上线新的功能和安全内容。

CADS将过去的数据烟囱集成到新的核心基础设施、分析工具和工程知识库上，为CISA的网络安全运行人员、分析师和决策者，以及地方政府机构、关键基础设施运营者，甚至私营公司和公众，提供统一的数据管理和分析工具。

同时，CADS被CISA看作是其实现日光浴委员会（CSC1.0）提出的

> 网络分析与数据系统（CADS）
> 可以看作是对NCPS缺陷的直接回应，
> 并能够间接提升缺陷一的未知威胁检测能力。

旨在构建新一代联邦网络空间势感知能力的联合协作环境（JCE）的关键项目。JCE 将通过集成内部和外部信息源（包括 CADS、威胁情报平台源和各种来源输入）来支持实时数据和信息共享及运营协作。

三、2024 财年项目预算分析

1. 整体预算分析

根据 CISA 在 2024 财年预算中提供的针对 NCPS 投资的表格，2024 财年的 NCPS 预算约合 0.67 亿美元。因为 2024 财年开始从 NCPS 迁移到 CADS，因此 2024 财年的 NCPS 预算大幅减少，主要就是 3000 万美元的遗留 NCPS 中的入侵检测能力（E1 和 E2）升级，以及 3700 万美元的遗留 NCPS 运行维护费用。

如右图所示，截至 2021 财年，美国爱因斯坦计划已经累计投入 42.8 亿美元，加上 2022 财年的 4.09 亿美元和 2023 财年的 4.11 亿美元，到 2023 财年已共计投入 51 亿美元。目前，NCPS 已经进入末期，主要是现有系统的运营，以及必要的入侵检测能力升级。

右图是 CISA 在 2024 财年预算中提供的针对 CADS 投资的表格，2024 财年的 CADS 的预算约合 4.25 亿美元。

如果将遗留 NCPS 预算和 CADS 预算加起来，则 2024 财年用于联邦政府互联网侧的态势感知预算依然高达 4.92 亿美元，创下单年申请预算新高。

2. 运行支撑预算分析

CISA 在 2024 财年的预算申请书中将遗留 NCPS 与 CADS 合在 JCE 中统一列支运行支撑预算。

首先，运行支撑人员的薪酬包继续上涨，2024 财年的人员薪酬预算高达 4407.2 万美元，人均 25.3 万美元，高于去年的 24.3 万美元。

其次，在 2.95 亿运行支撑（Operations and Support）预算中，有 2.51 亿是非支付性成本（Non Pay Budget，绝大部分计入“咨询与协助服务”科目）。

上表列举了非支付性成本的支出项。

以上支出分为遗留 NCPS 和新的 CADS 两部分，具体说明如下：

Overall Investment Funding

(Dollars in Thousands)	Prior Years	FY 2022	FY 2023	FY 2024
Operations and Support	$2,410,784	$317,379	$320,009	$37,272
Procurement, Construction, and Improvements	$1,866,868	$91,193	$91,193	$30,000
Research and Development	-	-	-	-
Legacy Appropriations	$4,277,652			
Total Project Funding	**$4,277,652**	**$408,563**	**$411,202**	**$67,272**
Obligations	$85,554			
Expenditures	$4,192,098			

Overall Investment Funding

(Dollars in Thousands)	Prior Years	FY 2022	FY 2023	FY 2024
Operations and Support	-	-	-	$257,913
Procurement, Construction, and Improvements	-	-	-	$166,993
Research and Development		-	-	-
Legacy Appropriations	-			
Total Project Funding	-	-	-	**$424,906**
Obligations	-			
Expenditures	-			

	FY 2022 Enacted	FY 2023 Enacted	FY 2024 President's Budget	FY 2023 to FY 2024 Total Changes
CADS: Cyber Mission IT Infrastructure	-	-	$103,210	$103,210
CADS: Cyber Operations Tools	-	-	$64,782	$64,782
Intrusion Prevention	$81,089	$37,000	$26,000	($11,000)
CADS: Program Management Office	-	-	$24,121	$24,121
CADS: Cyber Mission Engineering	-	-	$22,000	$22,000
Intrusion Detection	$14,208	$9,472	$11,000	$1,528
Development & Engineering	$43,784	$52,200	-	($52,200)
Core Infrastructure	$63,768	$78,206	-	($78,206)
Analytics	$58,236	$58,236	-	($58,236)
Information Sharing	$20,509	$43,163	-	($43,163)
Total - Non-Pay Cost Drivers	**$281,594**	**$278,277**	**$251,113**	**($27,164)**

项目	项目含义	2024 财年支出说明
NCPS 部分		
入侵检测	支持获取对联邦民事行政部门机构（FCEB）云安全遥测数据的访问权限，以提高保护云中 FCEB 数据所需的可见性	现有的 NCPS E1 和 E2 能力将继续为 CISA 网络运营提供有用的能力，并将继续运行和维护，同时 CISA 探索发展联邦网络发送能力的选项，以适应可信互联网连接 3.0（TIC 3.0）架构的采用，并扩大使用云技术
入侵防御	NCPS 入侵防御功能包括 E3A，它通过提供主动网络防御能力及防止和限制恶意活动侵入联邦网络和系统的能力，进一步推进对 FCEB 部门和机构的保护。该系统由向联邦政府提供互联网访问的互联网服务提供商部署为托管服务，利用涉密和非涉密指标来主动阻止已知的恶意流量	在 2023 财年，资金将支持运营和维持成本，以维持联邦网络保护性服务（FNPS）提供商提供的 DNS Sinkholing 和电子邮件过滤功能。 E3A 将过渡到商业、非机密服务，如 CISA 的保护性 DNS (pDNS) 服务。在整个 2024 财年，遗留的 NCPS 计划将继续运行并维护现有的入侵防御功能
核心基础设施	包括后端数据存储和处理环境，称为使命运行环境（MOE），包括网络设备、存储设备、数据库服务、应用程序托管服务、网络电路（线路）和安全控制	从 2024 财年开始，NCPS 的核心基础设施能力将切换到 CADS 中继续运行和维护
分析	使用本地和云基础设施及相关工具套件提供可扩展的环境，使 CISA 分析师能够关联和可视化数据集并快速得出结论，以应对高级威胁和漏洞	从 2024 财年开始，NCPS 的后端分析能力将切换到 CADS 中继续运行和维护
信息共享	NCPS 信息共享工作是一组灵活的功能，允许在 CISA 网络安全分析师及其网络安全合作伙伴之间快速交换网络威胁和网络事件信息	从 2024 财年开始，NCPS 的后端信息共享能力将切换到 CADS 中继续运行和维护
开发和工程	为 NCPS 计划提供对需求收集、工程解决方案、功能测试、安全测试、安全认证和配置管理提供必不可少的工程支持，并支撑技术更新工作和其他必要的环境变化，以维持基础设施和部署工具的可靠性、可访问性和可维护性指标	相关工作和预算全部转入 CADS 的计划办公室
CADS 部分		
网络使命 IT 基础设施	CADS 将作为网络数据摄取、管理、分析和信息共享平台的使命系统。它将在适当的情况下利用通用的 DHS 和 CISA IT 基础设施核心服务，并开发和提供使命系统基础设施服务，包括基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS），以满足 CSD 网络任务需求	资金包括硬件和软件维护成本及设备的标准技术更新；包括分析师用来访问数据、分析和信息共享的桌面设备。资金还包含与网络通信基础设施相关的年度电路（线路）成本和云业务交换（CBX）的扩展成。资金还用于支持扩大网络使命基础设施的容量，以支持额外的数据集，改善分析师对数据和工具的访问，并交付持续实施 / 持续交付（CI/CD）管道，使开发团队能够快速集成新功能以支持不断变化的需求
网络行动工具	CADS 将为 CISA 网络运营人员提供分析和信息共享工具，以便他们能够跟上数据量的步伐，以识别趋势、关键漏洞等。这些工具还将提供数据和分析编排，以改进自动分析和信息传播、数据可视化以及恶意软件取证和分析能力	将继续运营和维护的工具包括：安全和事件管理（SIEM）、数据包捕获、恶意软件下一代环境、云分析环境、部署在国土安全信息网络（HSIN）上的 CISA 网络门户，以及维护用于支持 AIS、指标管理、跨域解决方案和统一工作流程的基础设施和工具。这笔资金还将使战术支持小队（TST）和数据科学家能够为 CISA 威胁搜寻分析师提供现场支持
网络使命工程	包括提供架构和工程框架的工程资源，使得 CISA 的网络探针、遥测数据、基础设施、分析和信息共享工具能够集成到一起，进一步促成 CSD 达成网络使命	包括各种标准、最佳实践和知识库
计划管理办公室		项目管理办公室支持与管理 CADS 计划相关的管理成本，包括需求收集、客户拓展和沟通、工程流程支持、功能测试、安全测试、安全认证和 CADS 计划的配置管理支持

3. 采购实施与提升预算分析

进一步分析 2024 财年采购建设和提 升（Procurement, Construction and Improvements）的预算（1.97 亿美元）的构成，比上一财年增加一倍多，包括遗留 NCPS 和新的 CADS 两大部分。

下表是遗留 NCPS 的采购建设与提升预算明细：

这里，入侵检测就是爱因斯坦的前端，相当于探针、传感器；分析就是爱因斯坦的后端，相当于一个态势感知平台、安全运营平台；而信息共享（代号 Albert）就是爱因斯坦的威胁情报平台（TIP）；开发与工程包括需求收集、工程方案、能力测试、绩效评估等。2024 财年，除了入侵检测能力继续升级，其他能力的采购实施与提供资金都转入 CADS 中了。

此外，借助《美国救援计划法案》，CISA 在 2023 财年对爱因斯坦计划进行扩展，让 NCPS 能够采集和分析新的数据集（如 EDR、保护性 DNS），并将其命名为使命系统工程环境（MSEE）。如今，这项工作成果正好为 CADS 所用。

2024 财年投资在入侵检测上的 3000 万美元主要支持探索和初步推出功能，以取代当前的爱因斯坦技术堆栈。这将涉及市场调查，重新调整计划和资源，探索特定技术，探索传感器在本地网络中潜在的放置位置，将现有机构级数据与通过现有传感器功能获取的数据相结合，以及购买、安装和集成初始技术、数据路径和分析的工程。

下表列出了 CADS 的采购建设与提升预算明细，包括三个领域：网络使命 IT 基础设施、网络行动工具和网络使命工程。它们在 2024 财年各自的预期目标如下表所示。

4. 主要合同分析

下图展示了 2024 财年预算报告中列举的 NCPS 及 CADS 相关的合同信息：

可以发现，目前 NCPS 及 CADS 最大的供应商（集成商）还是雷神公司，

(Dollars in Thousands)	FY 2022 Enacted	FY 2023 Enacted	FY 2024 President's Budget
Intrusion Detection	$7,355	-	$30,000
Analytics*	$29,931	$29,679	-
Information Sharing*	$14,059	$10,689	-
Development and Engineering*	$39,848	$29,461	-
American Rescue Plan – Mission System Engineering Environment (MSEE)	-	$21,364	-
Total, NCPS PC&I	**$91,193**	**$91,193**	**$30,000**

*These capabilities will be transitioned to CADS as a result of the program restructure.
Amounts shown for FY 22 and FY 23 represent the funding CISA executed or plans to execute by category at the time of the Congressional Justification submission.

(Dollars in Thousands)	FY 2022 Enacted	FY 2023 Enacted	FY 2024 President's Budget
Cyber Mission IT Infrastructure	-	-	$31,388
Cyber Operations Tools	-	-	$95,887
Cyber Mission Engineering	-	-	$39,718
Total, CADS PC&I	-	-	**$166,993**

领域	里程碑事件
网络使命 IT 基础设施	· 该计划将与 CISA CIO 密切合作，将电子邮件和办公生产力应用程序实施并迁移到 CISA 的 M365 实例。 · 继续扩展 DevSecOps 管道，以支持 CADS 功能的快速开发、测试和实施。 · 增加云和通信基础设施的容量，以增加整个计划工具和功能套件的容量
网络行动工具	· 数据摄取与处理：继续将其他数据集与云分析环境集成，包括事件数据、主机级别可见性数据以及 PDNS 数据。 · 数据管理与治理：对数据管理功能进行增强，以应对数据量的增长，并解决与数据虚拟化和治理相关的多重挑战。 · 分析工具和应用：实施额外的分析工具，进一步实现网络威胁分析、搜寻和响应活动的自动化。 · 分析工具和应用：在云分析环境中开发新的分析工具，以支持对聚合多个 CSD 服务 的额外数据集进行分析。 · 工作流程管理：在统一工作流功能中继续实施和落地工作流程。统一工作流功能提供了一个单一平台，用于跨独立的 CSD 业务和使命支撑应用程序自动执行管理和运营工作流，以提高 CSD 运营的效率和有效性
网络使命工程	· 工程和架构致力于支持未来 CSD 服务的集成，包括保护性电子邮件服务、额外的端点检测数据集和联邦网络可见性数据

Contract Number	Contractor	Type	Award Date (mo/yr)	Start Date (mo/yr)	End Date (mo/yr)	EVM in Contract	Total Value *(Dollars in Thousands)*
70QS0122F00000011	Raytheon (TO11)	Task Order	05/2022	06/2022	06/2024	No	$226,800
70QS0119F00001415	BAE	Task Order	02/2019	03/2019	03/2024	No	$208,503
70QS0122F00000009	Raytheon (TO9)	Task Order	05/2022	06/2022	06/2024	No	$147,498
70QS0122F00000010	Raytheon (TO10)	Task Order	05/2022	06/2022	06/2024	No	$125,871
70QS0120E00000002	Sandia	Interagency Agreement	07/2020	08/2020	08/2025	No	$120,296

其三个合同的总值达到了 2 年 5 亿美元。

四、总结和启示

通过以上分析，结合其他材料，笔者谈一谈个人的几点体会作为本文总结。

1） NCPS 项目从一开始就是站在国家战略高度来推进的，采用法规先行（法案、总统行政令、NIST 标准等）、制度开道、统一建设、持续投入的方式，从一个 US-CERT 下面的初级态势感知项目，在 CNCI 计划的推动下，逐步成为了一个规模庞大的国家战略级项目。

2） 从项目定位上，NCPS 区别于各个联邦民事机构自己的安全防护。二者不是替代关系，而是叠加关系。并且 NCPS 更加注重针对高级威胁的监测与响应，更加重视跨部门 / 厂商的协调联动、信息共享、集体防御。

3） NCPS项目的投入时间很长，尤其是 2009 年 CNCI 计划出台之后，资金和人员投入逐年稳步提升，并维持在较高的水平线上。可见，国家级态势感知系统的建设需要长期持续的投入。

4） 从资金分布上看，DHS 越来越重视 NCPS 的运行维护，技术和产品采购的比重越来越低。要想实现 NCPS 常态化的运营，就必须有持续的、大量的运营投入，并且需要大量的安全分析师。

5） 从运营方式上看，NCPS 被尽可能地封装为一系列托管服务和安全服务的形式，以服务的方法提供给各个联邦机构，并且正在切换为单一的、统一的服务提供商。

6） CISA 自己说过，“有效的网络安全需要强大的度量机制”。正如“没有度量就没有管理”，必须对 NCPS 的效果进行持续度量，才能持续改进。但如何度量始终是一个问题，至今 CISA 也没有给出一套稳定的度量指标。

7） 经过十几年的持续建设，NCPS 取得了不少成绩，但仍然存在不少问题，已经难以适应威胁和技术的最新发展。CISA 提出了 NCPS 的升级替代版本——CADS，通过采用当前最先进的数据驱动安全的思想，大数据架构、云计算架构，应用数据管理与治理、编排自动化、人工智能等技术，构建新一代联邦互联网侧态势感知体系，强调更全面多源的数据采集与分析，更多源的安全情报整合，以及跨 CISA、政府部门、私营企业的安全协同联动。

8） 在技术层面，NCPS 正在积极上云，充分利用云来降低整体投入的成本，提升服务能力，改进服务方式。在数据中心的基础设施建设方面，云在可伸缩性、可用性和可靠性方面表现更佳。

9） 我们常把爱因斯坦计划指代美国政府的网络安全态势感知项目，其实这是不完整的。美国联邦政府的网络安全态势感知是由一系列国家级大项目共同支撑起来的，至少包括用于收敛互联网暴露面的 TIC（可信互联网接入）、互联网侧态势感知系统 NCPS 及升级版 CADS、联邦各机构内部态势感知系统 CDM（持续诊断与缓解），以及共享态势感知。安

关于作者

叶蓬

虎符智库专家、北京盛华安信息技术有限公司联合创始人、副总裁。具有 20 余年 SIEM、安全管理（SoC）平台和态势感知领域从业经验，并对 SOAR 有较深入研究。

以哈冲突表明：网络战现已成为新常态

作者 | 赵慧杰

网络安全研究员杰里迈亚 · 福勒发文，分析围绕以色列与哈马斯冲突的网络战的主要方法和策略，并指出此场冲突表明网络战争伴随实体冲突已成为新常态。

文章称，在以色列与哈马斯冲突中主要存在四种网络战方法：一是拒绝服务攻击，方式是通过海量恶意流量来消耗网络资源，从而对网络、服务或网站造成恶意破坏，使得合法用户无法使用相关网站或网络；二是宣传和发布错误信息，方式是利用机器人网络在社交媒体开展宣传或发布错误信息，从而影响观点或为特定事业或意识形态获得支持，以及使受众被虚假信息迷惑；三是网络间谍活动，方式是通过监控通信、渗透网络来获取情报信息，甚至利用遭黑系统和数据进一步开展网络间谍活动；四是黑客攻击和网站污损，方式是对重要目标开展网络攻击并泄露目标敏感数据，以及通过 SQL 注入来污损和篡改网站、社交媒体账户和数字平台。

文章称，围绕俄乌冲突的非政府黑客活动是世界上首次成功的无法追溯到任何特定国家或政府的“众包网络战争”。

以色列与哈马斯冲突中的网络攻击展现出信息战和网络活动已经与传统战争相互交织，网络战争伴随实体冲突似乎已成为新常态；网络战将在当前和未来的任何冲突中发挥重要作用，网络空间现在充当了没有明确交战规则的“第二战线”。

在俄乌战争初期，黑客组织“匿名者”宣布对俄罗斯发动网络战。当时，对一群半无组织的非政府黑客活动分子如何在俄罗斯造成重大破坏的方法、策略和结果进行了广泛的研究发现，他们的策略包罗万象，从对新闻媒体、家用打印机和联网设备开展黑客攻击，到下载属于公司和政府机构的大量俄罗斯数据，然后在网上公开发布这些数据。这是世界上首次成功的无法追溯到任何特定国家或政府的“众包网络战争”。

在当前以色列和哈马斯之间的冲突中，黑客组织尝试了许多与俄罗斯成功使用的技术相同的技术。然而，现在它们的效果似乎不太明显。使这些网络战争策略不同的一个主要因素是冲突之间的时间。自黑客活动分子向俄罗斯发动网络战以来的19个月里，世界各地的网络安全专家和情报部门有时间进行分析、准备，并通过从俄

在当前以色列和哈马斯之间的冲突中，黑客组织尝试了许多与俄罗斯成功使用的技术相同的技术。

罗斯网络防御的失败中吸取教训来尝试使自身免受不良影响。毕竟，网络战将在当前和未来的任何冲突中发挥重要作用，这是事实。网络空间现在充当第二战线，没有明确的交战规则。黑客活动分子和政府附属团体可以选择一方，并根据其特定技能发动大量攻击，看似只需点击几下鼠标就可以扭转冲突的局面。

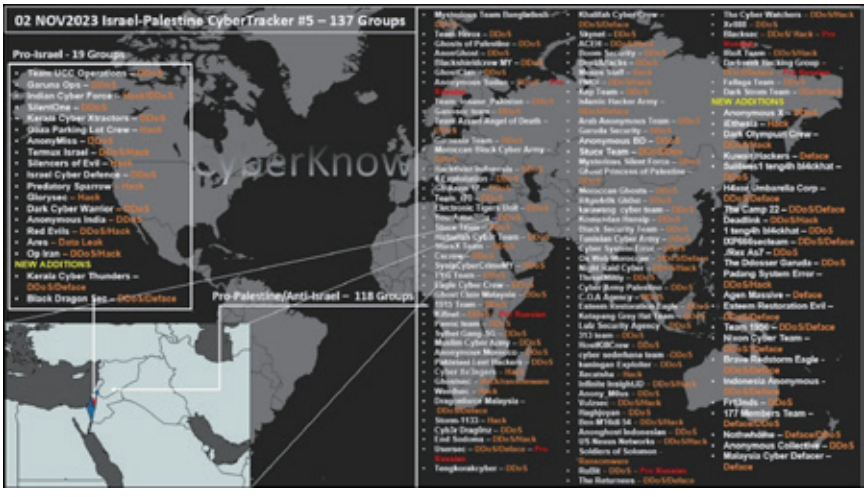
以色列－巴勒斯坦在线冲突中最常见的策略是拒绝服务（DoS）攻击。在最近的对抗的最初几天，攻击似乎集中在以色列政府网站、民事服务、新闻网站、金融机构及电信和能源公司。通过瞄准这些网站，攻击者可以操纵信息并限制平民获取实时新闻、政府指令和其他重要情报。

一、谁在对谁开展黑客攻击?

许多国家和其他全球行为者花费数年时间测试彼此的网络防御，并在进攻和防御安全方面拥有丰富的经验，这是一个公开的秘密。国家支持的网络攻击在战争与和平时期都是严重威胁，但网络战争伴随实体冲突似乎已成为新常态。网络战争格局似乎瞬息万变，但许多知名组织已经宣布参与以色列与哈马斯的冲突，其中包括各个 Anonymous 派系、KillNet、AnonGhost 等。

据网络战跟踪者 CyberKnow 反映，在冲突的最初几天，估计有 58 个不同的组织参与了网络攻击。初步报告声称有 10 个团体支持以色列，大约有 48 个团体支持巴勒斯坦。一般来说，由于黑客行动主义、网络犯罪和间谍组织的匿名性和隐蔽性，很难确定他们的意图是什么，及他们到底有多大影响。匿名是他们生存和效率的核心部分，他们试图通过隐藏自己的位置、身份和任何国家关系来确保这一点。也有可能其中一些组织实际上是由同一个人组成的，只是使用不同的操作名称，以使攻击看起来比实际规模更大。网络战的主要挑战之一是将网络攻击归咎于特定的国家支持的行为者或独立的黑客组织。由于并不确切知道谁在瞄准什么，因此很难定责和问责。

尽管如此，各种网络攻击已被公开与某个政府或另一个政府联系起来。例如，KillNet 和“匿名者苏丹”等多个与俄罗斯保持一致的组织已公开声称参与了针对以色列的网络攻击。KillNet 推出了一个名为 KILLNET PALESTINE 的新 Telegram 频道，在该频道中重申了其与“匿名者苏丹”的关系，并宣布打算协调针对以色列资产的攻击。此外，根据微软新发布的《2023 年微软数字防御报告》，2022 年 7 月至 2023 年 6 月期间，伊朗针对以色列政府和私营部门基础设施的攻击次数比任何其他国家都多。反过来，伊朗也指责以色列多年来发



动了多次网络攻击。

二、目前使用的网络攻击方法

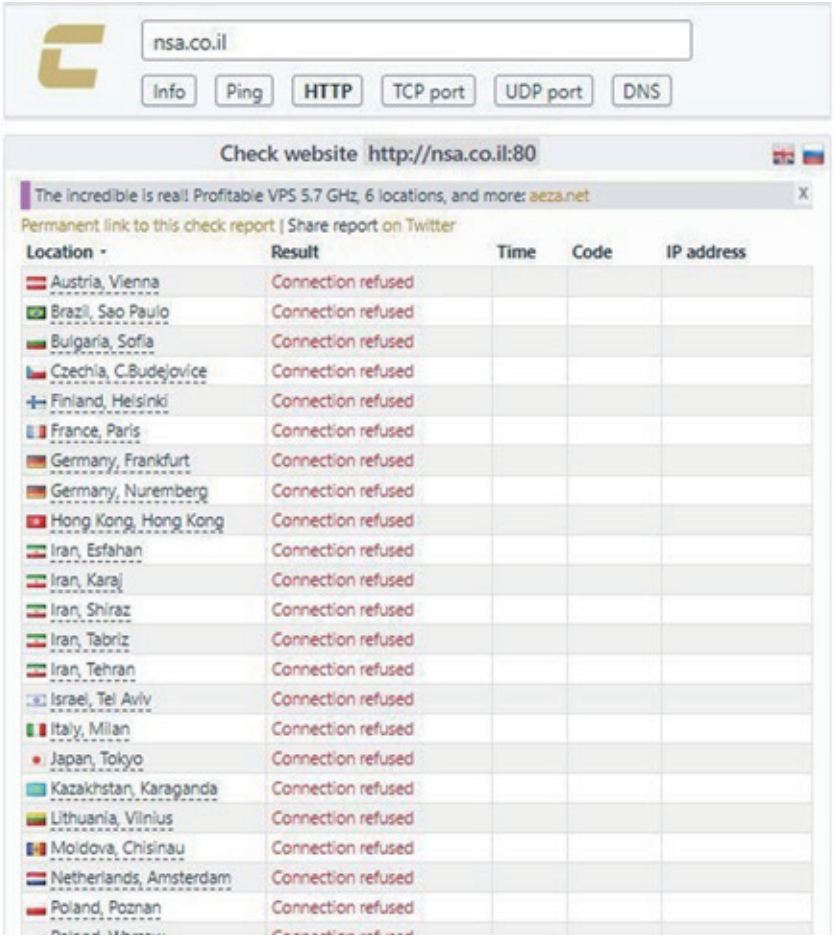
毫无疑问，网络战争正在与当前的实体战争一起在网上发生。截至目前，这些网络攻击的影响似乎很小，只造成了轻微的破坏。随着越来越多的团体和参与者加入战斗，网络安全威胁只会增加。

被黑客入侵的数据可能在未来几年内带来重大风险，并可能成为收集情报或发起未来攻击的拼图。网络战没有规则，这意味着所有类型的数据都可以被视为公平的游戏和有价值的目标。了解网络战的方法和策略有助于保护人员、企业和政府实体。

1. 拒绝服务（DoS）

有大量关于针对以色列和巴勒斯坦私营企业和政府实体的 DoS 攻击的报道。这些来自世界各地的攻击只会用大量的流量请求淹没网站。这种“不良流量”会消耗网络资源（如带宽、处理能力、内存或网络连接），并且几乎没有能力满足合法用户请求，因此称为“拒绝服务”。换句话说，DoS 攻击是一种技术相对较低但有效的方法，通过大量流量请求淹没网络、服务或网站，从而对网络、服务或网站发起恶意破坏。DoS 攻击的主要目标是使合法用户无法使用网站或网络数小时，甚至在极少数情况下长达数天。

自冲突爆发以来，已经发起了各种 DoS 攻击。例如，哈马斯官方网站被短暂关闭，据称是由亲以色列的黑客组织“印度网络部队”（India Cyber Force）关闭的。最大的英语新闻提供商《耶路撒冷邮报》成为“匿名者苏丹”组织的攻击目标，尽管该组织名称所示，许多专家认为该组织的运作地点是俄罗斯。另一个与俄罗斯有联系的组织 KillNet 声称已经摧毁了以色列政府的主要网站。亲以色列组织 ThreatSec 疑似攻击了加沙的互联网服务提供商。通过中断互联网访问，来阻碍人们获取信息的能力，以及无法连接到网络的人的网络能力。



2. 宣传和错误信息

对于普通人来说，这可能是所有网络战策略中最简单的，因为它几乎不需要技术知识，只需要互联网连接。然而，复杂的机器人网络在社交媒体上比以往任何时候都更加普遍，使得使用这种策略变得更加容易。赢得支持者的心灵和思想一直是所有全球冲突的首要目标，而宣传是影响观点或为特定事业或意识形态获得支持的有效工具。

社交媒体正在努力跟上大量的错误信息和机器人活动。2022 年，估计仅 X（前身为 Twitter）上就有 1650 万个机器人。一份关于俄乌冲突期间俄罗斯在 X 上的宣传的报告发现，机器人在宣传亲俄内容方面发挥了重要作用，估计有 20% 的消息是由机器人发布的，覆盖了近 1440 万用户。社交媒体上很可能仍然存在同样水平的机器人活动，最大的风险是普通用户可能无法区分机器人和人类间的差异，

并可能被虚假信息所迷惑。欧盟就有关哈马斯袭击、虚假新闻和断章取义的视觉内容的虚假信息向埃隆·马斯克和马克·扎克伯格发出了通知。欧盟要求采取缓解措施，以应对虚假信息给公共安全和公民言论带来的风险。

3. 网络间谍活动

以色列、巴勒斯坦和其他实体正在积极寻求监控通信、渗透网络并获取可用于其优势的宝贵信息。总部位于加沙的黑客组织 Storm-1133 曾针对以色列的电信、能源和国防公司发起攻击，但取得的成功有限。Storm-1133 采取了与其他组织略为不同的方法，使用从 LinkedIn 到 Google Drive 的一切工具来发起社交工程活动。他们的目标是部署绕过传统安全方法的后门，然后通过社会工程收集信息，而不是仅仅依靠暴力破解尝试。被黑客入侵的系统和数据的使用也在网络间谍活动中发挥着作用。一旦数据或入侵被渗透，它就可以成为进一步攻击或有针对性的活动以获得额外间谍能力的“垫脚石”。

4. 黑客攻击和污损

黑客行为：在当前的冲突中，似乎只有少数经过证实的黑客行为对双方都产生了重大影响。AnonGhost 是一个总部位于非洲、中东和欧洲的黑客组织，声称他们破坏了以色列的紧急警报应用程序。一个自称为“Team Insane PK”的组织声称他们入侵了以色列的一座水力发电厂。支持哈马斯的组织 Cyber Av3ngers 声称其试图攻击以色列电网机构。如果属实，这将增加关键基础设施（包括电网和供水设施）遭受网络攻击的可能性。

遭黑数据是冲突期间的另一个主要问题。例如，某俄语论坛似乎正在出售以色列国防军的个人数据。这些记录可能会泄露敏感的个人信息，这些信息可能远远超出个人安全和保障范围，因为这些数据可能包括家庭住址、联系方式，甚至家庭成员的姓名，这些信息可能被黑客活动分子利用进行骚扰或额外的网络攻击。访问士兵的数据会帮助攻击者了解士兵的数字生活，使士兵面临针对性的网络钓鱼和恶意软件攻击风险。当任何国家的国防部队卷入数据泄露事件时，意识到网络安全最佳实践并了解维护个人信息安全的重要性是当务之急。

污损：与以色列和巴勒斯坦实体相关的网站、社交媒体账户和数字平台已成为污损目标。冲突第一周，双方估计有 100 个网站遭到污损。这些攻击的目标是侵入网站并传达政治信息和意识形态。这些攻击通常通过 SQL 注入来完成，黑客利用网站输入字段中的漏洞来操纵网站的数据库。通过注入精心设计的 SQL 查询，攻击者可以绕过安全措施并获得未经授权的访问。这种形式的攻击允许黑客检索机密用户凭据，或控制网站并对其进行破坏。尽管这些看起来是重大事件，但它们不太可能向黑客提供任何敏感数据或信息，因为敏感记录通常不存储在面向公众的网站上。通常，这些凭据专门用于网站管理面板的一个区域，只要不重复使用或共享凭据来访问网络的其他部分，严重数据泄露的风险就会降低。

三、从冲突中学到的经验教训

以色列 – 巴勒斯坦冲突中的网络攻击展现出信息战和网络活动如何与传统战争形式交织在一起。网络战的使用凸显并定义了数字时代冲突的新现实，并彰显了解决这些网络安全挑战的重要性。针对任何国家的网络攻击都会带来重大危险，并产生深远的后果。破坏电网和通信系统等关键基础设施也会直接影响平民。这些攻击向世界各国发出警告——各国应对未来可能发生的攻击做好充分准备，并采取积极主动的网络安全措施。不幸的是，当谈到网络攻击时，问题不再在于是否发生，而在于何时发生。展望未来，同样的潜在威胁也适用于公司、私营企业和个人。黑客活动分子当前使用的工具和方法未来可能会被用于针对个人、公司或政府。了解黑客攻击是如何发生的是保护自己在线和数字生活的第一步。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。

博彩酒店业史上最严重攻击有哪些看点?

作者 | 虎符智库

近期，针对米高梅和凯撒娱乐公司的勒索软件攻击成为新闻焦点。美国博彩酒店行业正在遭遇史上最严重的网络攻击。9 月 10 日开始的网络攻击给米高梅造成严重的破坏，影响了其旗下拉斯维加斯及其他州的酒店预订系统和赌场，导致其关闭了全国范围内的酒店系统。米高梅国际酒店的顾客需要等待数小时才能入住；老虎机、自动提款机和停车系统均无法使用。另据《华尔街日报》报道，为避免米高梅的遭遇，凯撒酒店选择向攻击组织支付了 1500 万美元的赎金，为索要 3000 万美元勒索赎金要求的一半。

恶意软件研究组织 VX-Underground 在社交媒体声称，Alphv（又名 BlackCat）勒索软件组织是事件背后的黑手。联邦调查局已经着手调查攻击事件。系列勒索攻击给拉斯维加斯赌场造成巨大的破坏，但最让安全行业人士感到沮丧的是，事件背后攻击组织的社工攻击和攻击策略数月前已都被业界掌握。针对米高梅和凯撒娱乐公司的成功社会工程攻击，引发了业界对攻击者及其利用漏洞相关攻击活动的关注，为何众多的机构败于看似简单的社工攻击。

一、价值 339 亿美元的公司被 10 分钟通话攻破

尽管米高梅尚未证实此次攻击事件是如何发生的，VX-Underground 在社交媒体表示，攻击者只是在领英网站上找到了一名米高梅的员工，然后致电 IT 服务台，利用 10 分钟的电话通话中，攻击者成功侵入了米高梅的系统。一家价值 339 亿美元的公司被一通 10 分钟的电话击败。

Phosphorus 首席战略官索努·尚卡尔（Sonu Shankar）也证实：从公开信息看，攻击似乎是通过传统的社会工程攻击实施的——攻击者冒充员工，并说服 IT 帮助台为高特权账户重置登录凭证和 MFA。攻击首先从 IT 系统开始，但影响很快蔓延到米高梅的 xIoT 网络，包括老虎机、客房电子钥匙、ATM 机、销售点终端，甚至是停车系统。

另一方面，在向美国证券交易委

员会提交的文件中，凯撒公司宣称，该公司的安全事件是由针对外包 IT 支持供应商的社工攻击引起的，但没有提供进一步细节。勒索软件组织 UNC3944 也声称对凯撒的攻击负责，据报道，攻击可能早在 8 月 27 日就开始了。凯撒宣称，已经采取了措施，确保外包 IT 支持供应商实施补救措施，以防止未来可能的威胁与攻击。为了避免米高梅的类似损失和遭遇，凯撒选择了向勒索者支付赎金。

米高梅和 BlackCat/ALPHV 之间的谈判一直在进行中。攻击者宣称窃取了数 TB 的数据，并保持对米高梅部分基础设施的访问权限，同时威胁要实施新的攻击，除非米高梅最终同意支付赎金。

针对两家博彩公司的攻击都是利用身份管理供应商 Okta 发起的，黑客使用 Okta 技术作为访问媒介。在得知 BlackCat/ALPHV 潜伏在其 Okta 代理服务器上后，米高梅已经关闭了其 Okta 服务。但黑客在声明中表示，他们仍然存在于米高梅网络中。

Okta 公司表示，其美国客户报告了一种一致的攻击模式：黑客冒充受害企业员工，然后说服 IT 服务台为其提供重复访问权限。

据派拓网络 (PANW) Unit 42 工程副总裁兼首席技术官迈克尔 · 斯科尔斯基（Michael Sikorski）也证实，攻击组织 UNC3944 擅长给受害者打电话，说服其访问恶意网站或者欺骗 IT 服务台重制密码。“他们在追求目标时有条不紊，攻击策略高度灵活，会毫不犹豫地快速转换策略。”

在今年 6 月的一份报告中，Unit 42 研究人员表示：UNC3944 的武器库丰富，从娴熟的社会工程和网络钓鱼攻击，到利基渗透测试和取证工具，使得该攻击组织比强大的现代网络防御计划更具优势。

针对社工攻击的影响，南内华达反恐中心高级情报分析师内特 · 富达拉（Nate Fudala）表示，对任何网络来说，最大的威胁是用户，是你和我！不是系统本身，而是使用它的人。

社交媒体上发布的关闭老虎机照片

二、每一分钟都在赔钱

网络攻击导致的混乱持续了一周，令米高梅和凯撒公司遭受巨大的财务损失。由于酒店预订和博彩系统持续多日瘫痪，“这是一个非常昂贵的攻击，米高梅每分钟都在赔钱。”

勒索软件组织声称，已经加密了米高梅 100 多个 ESXi 虚拟机管理程序，并从米高梅（MGM）和凯撒娱乐（CZR.O）的系统中窃取了 6TB 的数据。凯撒公司的文件透露，攻击者利用针对 IT 外包供应商的社会工程攻击，获取了凯撒的重要数据，包括大量会员的驾驶执照号码和 / 或社会保障号码。黑客组织在网站上警告，如果与米高梅不能达成协议，将会发起更多的攻击。

酒店和赌场业掌握大量客户的个人和财务数据，正在越来越多地成为利润丰厚的黑客攻击目标。2023 年针对博彩行业的网络攻击激增。黑客不仅破坏酒店与赌场的计算机系统，还窃取敏感信息并威胁要披露这些信息，除非支付赎金。

2022 年对洲际酒店集团的网络攻击破坏了其特许经营商的预订和其他系统。万豪国际集团 2018 年披露网络攻击，泄露了旗下喜达屋超过 3 亿客户的数据，包括护照号码和支付卡等敏感细节。

三、年轻而又危险的攻击者

当米高梅努力恢复系统之时，ALPHV/BlackCat 正忙着发布另

一名攻击受害者——半导体制造商 Seiko——2.5TB 被盗数据。针对该公司的攻击于 8 月被公开。

ALPHV /BlackCat 勒索软件团伙自 2021 年以来一直存在，以勒索软件即服务 (RaaS) 模式运作，以使用 Rust 编程语言而闻名。根据 Microsoft 的资料，ALPHV/BlackCat 还与 Conti、LockBit 和 REvil 等其他勒索软件组织密切合作，并与 Darkside 和 Blackmatter 网络犯罪集团有联系。网络安全分析师 ANOZR WAY 称，2022 年该组织约占所有勒索攻击的 12%。

派拓网络 (PANW) Unit 42 工程副总裁兼首席技术官迈克尔 · 斯科尔斯基（Michael Sikorski）介绍，提供勒索软件即服务 (RaaS) 的 BlackCat/ALPHV ，已将此次实施攻击的 UNC3944 列为其附属组织，向其提供了“工具包”的访问权限，包括勒索软件、技术支持，以及对其泄漏网站的访问权限。

作为一个经济利益驱动的攻击组织，UNC3944 有多个名字，包括 Scattered Spider、Muddled Libra、Scatter Swine 和 Oktapus。UNC3944 的成员由美国和英国黑客组成，一些成员年龄只有 19 岁，至少从 2022 年 5 月开始就一直保持活跃。

谷歌曼迪安特首席技术官 Charles Carmakal 表示，与许多成熟勒索软件组织和国家攻击组织相比，UNC3944 成员的经验略显不足且年轻，但因许多成员的母语是英语，且是非常高效的社会工程攻击人员，对美国大型组织带来严重的安全威胁。

Critical Start 网络威胁研究高级经理卡利 · 巩特尔（Callie Guenther）介绍，UNC3944 专门尝试绕过 Microsoft Defender for Endpoint、Palo Alto Networks Cortex XDR 和 SentinelOne 等安全产品。这一组织利用英特尔以太网诊断驱动程序的旧漏洞（CVE-2015-2291 ），在被攻击设备上植入了较旧且仍易受攻击的版本，使其能够利用此漏洞，而不管系统是否更新。由于设备驱动程序可以直接访问内核，利用其中的缺陷，网络攻击者就可在 Windows 中以最高权限执行代码。

UNC3944 不断变化的作案手法，特别是其使用社会工程攻击和“自带易受攻击的驱动程序”(BYOVD) 策略，赋予他们提升 Windows 权限的策略，突显网络威胁环境的多面性。

研究人员发现，UNC3944 组织对攻击目标的挑选非常谨慎，重点关注估值在 150 亿美元至 450 亿美元之间的企业，并且不会攻击医院、炼油厂和发电厂。快速致富并争取逃脱惩罚是该团伙的主要目的。

安全人士认为，尽管攻击者通过针对 IT 帮助台的社工攻击，在网络中提供了立足点，但在网络内的后续行动才是最令人担忧的。攻击者发现并利用未知漏洞，就会放大漏洞的严重性，这表明攻击的复杂程度，以及在网络中移动而不被发现的能力。

四、未来有哪些教训需要吸取?

针对米高梅和凯撒公司以社工攻击作为入手的勒索攻击，安全专家建议从多个方面加强安全防护。

首先是构建弹性的基础设施，有力维护数据安全。 攻击的影响远超博彩行业，这意味着各个行业都须为此类威胁和攻击的可能影响做好准备，提升威胁的可见性，最大程度降低威胁造成的损失。

其次是构建纵深防御的体系，确保关键任务应用受到多层防御和冗余的保护，而不会因一次社工攻击而导致百亿美元企业的业务瘫痪。这一个成本高昂的投入，但从长远来看会带来更安全的环境和更稳定的业务。

第三，企业需要为 xIoT 系统的安全防范做好准备。米高梅的遭遇说明，任何网络攻击都可以快速传播到您的 xIoT 系统，对企业的业务运营和安全产生真正的影响。

最后，建议立即采取多种措施来防御社工攻击，比如，更新身份验证方式，采用经验证的通信渠道发送的一次性密码等。随着组织 IT 基础设施日益复杂社工攻击的风险不仅针对该公司的员工，还针对外部业务合作伙伴。 安

关于作者

虎符智库

“虎符智库”是由国内领先网络安全企业奇安信集团汇聚院士、国内外顶级安全专家，以及行业专家组建的网安行业顶级智库，旨在深度解读网络安全领域政策、剖析重大安全事件，洞察前沿产业趋势，为产业发展和安全建设建言献策。虎符智库”诚邀业界专家参与，定期开展深入交流。

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