极牛网络安全通讯 • 社群期刊 2023 年 4 月 第 22 期

网安观察

P10 全民国家安全教育日

P7
美国政府用间谍软件监控世界各地手机用户

P30 对当前 5G 应用安全的 5 点认识
P34 美国切换国家网络防御系统大脑的背后
P38 俄乌冲突：人工智能战争的试验场

第22期
2023年4月

极牛网

极牛网 网络安全行业媒体

致力于促进中国网络安全行业创新思维的交流与碰撞，搭建中国网络安全技术社区和交流平台



技术格局

网安工程师的成长，需要锻炼开阔的技术视野和统筹全局的战略高度，能够着眼现在思考未来，做懂业务懂策略的工程师。

管理之道

网安工程师随着职业发展，必然面临着向技术总监、CTO等管理角色转型，改变管理思维，建立属于自己的管理哲学。

人才梯队

作为技术管理者，如何建立一个稳固、高效的人才队伍是核心任务，更应该从人才梯队的角度，关注人才的培养的更迭。

企业战略

技术管理者应该建立技术以外的格局，经济形势、商业模式、投融资等等，才能助力企业发展，做与创始人同频的CTO。

产品运营

敢于拥抱和应对变化，敢于创新，在创新的基础框架下，寻找创新的实践方法论，激发技术人员创新能力，推动业务发展。

布道能力

作为技术工程师，需要重点培养自己的布道能力，能将自己的技术成果和理念传播出去，才能拓宽和升级自己的认知边界。

全民国家安全教育日

2023年4月15日是第八个全民国家安全教育日。今年的主题是：贯彻总体国家安全观，增强全民国家安全意识和素养，夯实以新安全格局保障新发展格局的社会基础。

全民国家安全教育日是为了增强全民国家安全意识，维护国家安全而设立的节日。

《中华人民共和国国家安全法》中指出国家安全重点领域包括： 政治安全、国土安全、军事安全、经济安全、文化安全、社会安全、科技安全、网络安全、生态安全、资源安全、核安全、海外利益安全、太空安全、深海安全、极地安全和生物安全等重点领域安全。

在网络安全领域，我们应该全方位地武装人民的大脑，全面提升网络安全意识，真正做到网络安全靠人民。

一是强化思想引领，以习近平新时代中国特色社会主义思想武装头脑、指导实践、推动工作。深化理论武装，用好《习近平新时代中国特色社会主义思想学习纲要》等。提升传播实效，精准设置议程，开设系列专栏，推出一批原创融媒精品。

二是强化守正创新，着力塑造主流舆论新格局。提升议题引领力，强化网上重大主题宣传，营造奋进新征程、建功新时代的热烈氛围。提升内容感召力，策划推出形式多样、简洁明快、可读耐看的轻量化产品和现象级爆款。提升舆论引导力，加强形势政策网上宣传解读，加强线上线下舆论引导协同。

三是强化斗争精神，牢牢守好网络政治安全和意识形态安全“南大门”。坚持敢于斗争、善于斗争，以高度的政治敏锐性和政治鉴别力防范化解各类风险隐患，坚决打赢网络意识形态斗争。狠抓网络意识形态工作责任制落实，持续深化督查成果运用，开展“回头看”督促各地区各部门切实抓好问题整改。

四是强化综合治网，持续推动形成良好网络生态。健全完善网络综合治理体系，加大网络综合治理统筹协调力度。集中清理网络生态领域新老问题，加强网络举报和辟谣工作，大力整治网络欺凌、网络沉迷、不良亚文化等问题。深入推进依法治网，加强网络安全、数据安全和个人信息保护等领域执法。加强网络文明建设，开展网络文明宣传季系列活动，擦亮网络文化精品宣传推广品牌。

总顾问

叶绍琛

2023年5月4日

CONTEN

目录



安全态势

P4 | 五部门印发《关于调整网络安全专用产品安全管理有关事项的公告》
P4 | 《商用密码管理条例（修订草案）》审议通过
P5 | 《电信领域数据安全指南》等 12 项网络安全国家标准获批发布
P5 | 美国发布《促进数据共享与分析中的隐私保护国家战略》
P6 | 国际支付巨头 NCR 遭勒索攻击：POS 机服务被迫中断多天
P6 | 德国药物研发巨头 Evotec 遭网络攻击，致使生产延误
P7 | 美国政府用间谍软件监控世界各地手机用户，德法多任首脑被监听
P7 | 存储巨头西部数据遭入侵：多个内部系统被访问，My Cloud 网盘服务中断
P8 | vm2 沙箱逃逸漏洞（CVE-2023-30547）安全风险通告
P8 | Google Chrome V8 类型混淆漏洞安全风险通告
P9 | vm2 沙箱远程代码执行漏洞安全风险通告
P9 | 瑞友天翼应用虚拟化系统远程代码执行漏洞安全风险通告
P9 | Spring Framework 身份认证绕过漏洞安全风险通告



国际事件

P7 美国政府用间谍软件监控世界各地手机用户，德法多任首脑被监听

CONTENTS



专题报道

P30
对当前 5G 应用安全的 5 点认识

P34
美国切换国家网络防御系统大脑的背后

P38
俄乌冲突：人工智能战争的试验场



第 22 期
《网安观察》编辑部
主办　极牛网

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

公众号　小程序　网站

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

E m a i l：hi@geeknb.com
地　　址：深圳市龙岗区天安云谷2栋2层
邮　　编：518000
电　　话：0755-33228862
印刷数量：1000 本
印刷单位：深圳彩虹印刷有限公司

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

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



政策篇

国内，国家网信办发布《生成式人工智能服务管理办法（征求意见稿）》，及时回应当前生成式人工智能带来的风险与冲击。

国际上，美国白宫科技政策办公室发布《促进数据共享与分析中的隐私保护国家战略》，确立了政府支持发展保护隐私数据共享和分析技术的指导原则和战略优先事项。

国内

五部门印发《关于调整网络安全专用产品安全管理有关事项的公告》

4 月 17 日网信办官网消息，国家互联网信息办公室、工业和信息化部、公安部、财政部、国家认证认可监督管理委员会联合印发《关于调整网络安全专用产品安全管理有关事项的公告》。该文件指出，自 2023 年 7 月 1 日起，停止颁发《计算机信息系统安全专用产品销售许可证》，产品生产者无需申领。列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应当按照《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。

《商用密码管理条例（修订草案）》审议通过

4 月 14 日中国政府网消息，国务院总理李强主持召开国务院常务会议，会议审议通过《商用密码管理条例（修订草案）》。会议指出，近年来，商用密码应用愈发广泛，在保障网络和信息安全、维护公民和法人权益方面的重要性日益凸显。要全面贯彻总体国家安全观，进一步规范商用密码应用和管理，督促平台企业依法履行用户密码保护责任，确保个人隐私、商业秘密和政府敏感数据的安全。要更好顺应数字经济快速发展趋势，建立健全商用密码科技创新促进机制，推动商用密码科技成果转化和产业化应用，促进商用密码市场持续健康发展。

网信办《生成式人工智能服务管理办法》公开征求意见

4 月 11 日网信办官网消息，国家互联网信息办公室公布《生成式人工智能服务管理办法（征求意见稿）》（以下简称《征求意见稿》），向社会公开征求意见。《征求意见稿》规定，利用生成式人工智能生成的内容应当体现社会主义核心价值观，不得含有不良信息，利用生成式人工智能生成的内容应当真实准确，采取措施防止生成虚假信息等。《征求意见稿》要求，利用生成式人工智能产品向公众提供服务前，应当向国家网信部门申报安全评估，并履行算法备案和变更、注销备案手续，提供服务时应当要求用户提供真实身份信息。

四部门：关于开展网络安全服务认证工作的实施意见

3 月 28 日市场监管总局官网消息，市场监管总局、中央网信办、工业和信息化部、公安部联合发布《关于开展网络安全服务认证工作的实施意见》，加强认证工作的组织实施和监督管理，鼓励网络运营者等广泛采信网络安全服务认证结果，促进网络安全服务产业健康有序发展。该文件提出，四部门确定网络安全服务认证目录，现阶段包括检测评估、安全运维、安全咨询和等级保护测评等服务类别。网络安全服务认证机构应当公开认证收费标准和认证证书有效、暂停、

注销或者撤销等状态，并按照有关规定报送网络安全服务认证实施情况及认证证书信息。

《电信领域数据安全指南》等 12 项网络安全国家标准获批发布

3 月 23 日全国信安标委官网消息，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（2023 年第 1 号），全国信息安全标准化技术委员会归口的 12 项网络安全国家标准正式发布。具体清单包括电信领域数据安全指南、网络安全服务成本度量指南、个人信息去标识化效果评估指南、网络安全态势感知通用技术要求、公共域名服务系统安全要求、网络安全从业人员能力基本要求等。

国际

美国发布《促进数据共享与分析中的隐私保护国家战略》

3 月 31 日 OSTP 官网消息，美国白宫科技政策办公室（OSTP）发布《促进数据共享与分析中的隐私保护国家战略》，正式确立了政府的目标，即支持保护隐私数据共享和分析（简称 PPDSA）技术。PPDSA 技术是一种平衡数据收集、分析与伦理社会技术问题的解决方案，它利用隐私增强技术进行数据分析、获取数据价值，同时确保用户隐私、秘密安全。该战略提出了包含 PPDSA 技术的未来数据生态系统的愿景，包括 PPDSA 技术有助于增进人民福祉、促进社会繁荣，与符合民主价值观的方式促进科学和创新。战略制定了四项基本指导原则和五个战略优先事项，来实现这一愿景。

美国政府更新零信任成熟度模型，将零信任转型作为长期目标

4 月 11 日 CISA 官网消息，美国网络安全与基础设施安全局（CISA）发布《零信任成熟度模型》第二版，旨在协助联邦机构制定零信任战略和实施计划，并展示 CISA 可提供的各类服务。第二版距离首版发布已经一年有余，主要针对首版反馈进行了修订。

首版将零信任成熟度阶段分为三阶段五支柱，包括传统、高级、最佳三个阶段，身份、设备、网络、应用与工作负载、数据五大支柱，并针对每个阶段的各大支柱提出了具体要求。第二版在传统阶段之上增加了初级阶段，并修订了每个阶段各大支柱的指导标准。比如，身份支柱，增加通过 FIDO2 或 PIV 实现无密码 MFA，增加身份存储的灵活性等；设备支柱，增加了设备威胁保护功能以进行集中安全管理；网络支柱，修改了网络分段功能推荐基于应用配置文件的微隔离等。

美国食品药品监督管理局发布指导文件，医疗设备上市需自证网络安全

3 月 30 日 FDA 官网消息，美国食品药品监督管理局（FDA）发布最终指导文件《医疗设备的网络安全：FD&C 法案第 524B 条下网络设备及相关系统的拒绝接收政策》。该文件指出，《2023 年综合拨款法案》第 3305 条修订了《联邦食品、药品和化妆品法案》（即 FD&C 法案），添加了第 524B 节以协助确保医疗类设备的网络安全，其中包括设备上市前的申报材料必须增加网络安全信息，证明其满足相应要求。该文件还提出，医疗保健相关方应落实软件物料清单和漏洞披露报告等规定。FD&C 法案修正案将于 2023 年 3 月 29 日颁布起的 90 天后生效。

拜登发布行政令，禁止美国政府使用商业间谍软件

3 月 27 日美国白宫官网消息，美国总统拜登发布《关于禁止美国政府使用对国家安全构成风险的商业间谍软件的行政命令》，首次禁止美国联邦机构使用可能对人权及国家安全构成威胁的商业间谍软件。该行政令适用于包括执法、国防和情报部门在内的联邦政府机构，相关机构如计划继续使用，应按照规定证明其不会对美国构成重大的反情报和安全风险。这项行政令出台之际，已有数十名美国政府人员的手机遭受间谍软件入侵。



事件篇

网络空间国家博弈与斗争手段层出不穷，美国政府遭曝光用间谍软件监控世界各地手机用户，德法多任首脑被监听；俄罗斯绝密文档遭举报者泄露，网络战核心支撑机构及武器库曝光。

国际支付巨头 NCR 遭勒索攻击：POS 机服务被迫中断多天

4 月 15 日 BleepingComputer 消息，美国支付服务商 NCR 遭受勒索软件攻击，旗下 POS 机服务发生中断。NCR 用于酒店服务的产品 Aloha POS 平台自 4 月 12 日发生故障以来，持续多天无法供客户正常使用。NCR 在 15 日对外披露称，为 Aloha POS 平台提供支持的数据中心遭受到勒索软件攻击，已经影响了部分酒店客户的一定数量的附属 Aloha 应用程序。有 Aloha POS 客户在 Reddit 论坛上表示，中断事件已经导致其业务运营出现重大问题。BlackCat/ALPHV 勒索软件团伙宣布为此负责。

德国药物研发巨头 Evotec 遭网络攻击，致使生产延误

4 月 12 日 TheRecord 消息，德国药物研发巨头 Evotec 披露，4 月 6 日遭受网络攻击，导致该公司断开了互联网连接，以“保护系统免遭数据损坏或入侵”。Evotec 公司后续公告称，尽管内部系统已经离线多天，但“全球设施的业务连续性已经得到保障”，只是可能出现延误或响应较慢的情况。Evotec 公司已对事件进行取证调查并上报德国执法部门。目前没有黑客团伙宣称对此次攻击负责。近几个月来，已经有多家制药企业受到网络攻击影响。

现代汽车发生数据泄露事件，欧洲多国车主受影响

4 月 12 日 BleepingComputer 消息，跨国汽车制造商现代汽车披露发生数据泄漏事件，意大利和法国车主及预订试驾数据遭泄露。根据推特用户反馈和安全专家 Troy Hunt 分享的通知样本，该事件暴露了电子邮箱、住址、电话号码、车辆底盘编号等敏感数据，不过用户的身份证号码和财务数据未受到影响。现代汽车表示，他们聘请了 IT 专家来处理数据泄露事件，已经将受影响的系统脱机，直到实施额外的安全措施。现代汽车还警告其客户对声称来自现代汽车的未经请求的电子邮件和短信保持谨慎，因为它们可能是网络钓鱼和社会工程攻击。

以色列地方灌溉系统遭敌对黑客攻击，农民田地无法浇水

4 月 9 日耶路撒冷邮报消息，以色列上加利利地区的灌溉系统和污水处理系统遭到网络攻击，导致负责约旦河谷农田灌溉的水位控制器，以及加利尔污水公司（Galil Sewage Corporation）的控制系统都遭到了破坏。被入侵的控制器显示着一条消息“你被黑客入侵了，打倒以色列”。据悉，至少有 10 名农民受到影响，预定的浇水被迫停止。以色列国家网络安全局上周发出警告，称在斋月期间，反以黑客将尝试发起更多网络攻击。根据预警信息，有一些农民断开了灌溉系统的远程控制功能，切换为手动操作，以防受到攻击。那些仍可远程控制的系统正是此次网络攻击的主要受害者。

知名台企微星疑遭勒索攻击，被索要 2750 万元巨额赎金

4 月 6 日 BleepingComputer 消息，中国台湾知名硬件制造商微星（MSI）已被勒索软件团伙 Money Message 列入其网站“已入侵名单”，并贴出了号称来自该硬件厂商

CTMS 与 ERP 数据库及软件源代码、私钥和 BIOS 固件文件的屏幕截图。该团伙宣称，从微星系统中窃取到 1.5 TB 数据，包括源代码和数据库，并要求受害者支付 400 万美元赎金（约合人民币 2750 万元）。微星官方确认遭受了网络攻击，但没有透露任何细节。



美国政府用间谍软件监控世界各地手机用户，德法多任首脑被监听

4 月 5 日央视财经消息，据美国《纽约时报》2 日报道，美国政府通过第三方公司，在 2021 年 11 月 8 日与以色列间谍软件公司 NSO 集团在美国的分支机构签署秘密合同。根据合同的约定，NSO 将向美国政府提供间谍软件，用于秘密跟踪身处世界各地的手机用户。美国政府可以使用 NSO 集团一款名为“地标”（Landmark）的地理定位黑客工具，政府官员通过访问一个特殊的网站，在输入目标用户的手机号码后，即可在该用户不知情或未同意的情况下精确定位手机的位置。美国实施“无差别”监视监听。从竞争对手到盟友，甚至包括德国前总理默克尔、法国多任总统等盟国领导人，无不在监听范围之内。



存储巨头西部数据遭入侵：多个内部系统被访问，My Cloud 网盘服务中断

4 月 3 日 BleepingComputer 消息，美国存储巨头西部数据当天披露，内部网络遭到入侵，未授权黑客已获得公司多个系统的访问权限。据披露，这起事件于 3 月 26 日被发现，该公司认为入侵者已经访问了部分内部数据。攻击发生之后，西部数据实施了额外的安全措施以保护其系统和运营，但这些步骤可能会影响一部分服务。该公司表示，安全事件“已经并可能继续导致公司部分业务陷入运营中断”。据多位用户报告，西部数据旗下网络存储服务 My Cloud 至少已中断超 24 小时。



绝密文档遭举报者泄露，俄罗斯网络战核心支撑机构及武器库曝光

3 月 30 日英国卫报消息，多家西方媒体报道称，一名反乌克兰战争人士向媒体提供了一批被称为“Vulkan 文件”的泄露资料，指责一家名为“NTC Vulkan”的私人公司与俄罗斯军事和情报机构合作，支持后者发动所谓“针对西方的网络战争”。

报道称，“Vulkan 文件”的时间跨度从 2016 年到 2021 年，其中显示 NTC Vulkan 公司支持俄罗斯军事和情报机构开展黑客行动、在发起针对国家基础设施的攻击前训练操作员、传播虚假信息及扫描互联网漏洞并对其进行分区控制；同时，该公司还帮助俄罗斯官方通过互联网影响社交媒体观点、公众意见走向及西方国家的最终选举结果。报道还称，NTC Vulkan 公司的网络攻击工具包括全网漏洞扫描系统“Scan-V”、信息操纵系统“Amezit”、社交媒体数据分析工具“Fraction”、攻击培训系统“Crystal-2V”等。



荷兰知名海运企业遭勒索攻击：大量内部数据失窃 已有 5GB 被公开

3 月 21 日 SecurityWeek 消息，荷兰知名海运物流服务公司 Royal Dirkzwager 遭 Play 勒索软件团伙入侵，失窃数据已被部分公布。Royal Dirkzwager 在 3 月 6 日遭遇勒索软件攻击，导致该公司系统宕机，多项服务被迫暂停。3 月 16 日，该公司宣布各项服务恢复正常，但同天 Play 勒索软件团队也在泄密网站上公布了 5GB 的部分窃取数据，据称包含私有及个人数据、合同、员工 ID、护照等信息。Play 团伙威胁称，如果该公司不满足其勒索要求，将公布全部数据。



Google Play 下架拼多多，称存在恶意软件

3 月 21 日 TechCrunch 消息，Google 将中国电商平台拼多多的多个 App 标记为恶意程序。Google 发言人 Ed Fernandez 表示，Google 已经基于 Android 手机的安全机制 Google Play Protect 阻止用户安装这些恶意应用程序，并警告那些已经安装的用户，提示他们卸载这些应用程序。“Google 出于安全考虑，已经下架拼多多在 Play 商店的官方应用程序，我们将继续调查”，Ed Fernandez 说道。此前，有匿名安全研究人员披露拼多多应用包含有恶意功能，能利用漏洞提权阻止卸载并能监视用户。拼多多称，强烈反对一些匿名研究人员的猜测和指责，以及 Google 关于拼多多 App 是恶意的非结论性回应。



漏洞篇

JavaScript 流行沙箱库 vm2 接连曝光 3 个任意命令执行漏洞，均已成功复现，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

vm2 沙箱逃逸漏洞 (CVE-2023-30547) 安全风险通告

4 月 18 日，奇安信 CERT 监测到 vm2 沙箱逃逸漏洞 (CVE-2023-30547)。vm2 是一个 npm 包，实现了沙箱环境，可以用 vm2 创建沙箱环境并运行 nodejs 代码。在 vm2 的源代码转换器异常清理逻辑中存在沙箱逃逸漏洞，攻击者可绕过 handleException() 并泄漏未清理的主机异常，进而逃逸沙箱实现任意代码执行。目前奇安信 CERT 已成功复现该漏洞，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Google Chrome V8 类型混淆漏洞安全风险通告

4 月 17 日，奇安信 CERT 监测到 Google Chrome V8 类型混淆漏洞 (CVE-2023-2033) 被在野利用，攻击者可通过诱导用户打开恶意链接来利用此漏洞，从而在应用程序上下文中执行任意代码。目前，此漏洞已检测到在野利用。鉴于此漏洞影响范围较大，建议客户尽快升级到安全版本。

Apache Solr 代码执行漏洞安全风险通告

4 月 15 日，奇安信 CERT 监测到 Apache Solr 代码执行漏洞，Apache Solr 默认配置下存在服务端请求伪造漏洞，当 Solr 以 cloud 模式启动且可出网时，远程攻击者可利用此漏洞在目标系统上执行任意代码。目前奇安信 CERT 已成功复现该漏洞，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Artifex Ghostscript 代码执行漏洞安全风险通告

4 月 14 日，奇安信 CERT 监测到 Artifex Ghostscript 代码执行漏洞 (CVE-2023-28879)，Ghostscript 存在越界写入漏洞，s_xBCPE_process 函数在转义时，如果最后一个字符需要转义，则会写入 2 字节，导致越界写入了 1 字节。成功利用该漏洞能够在目标系统上执行任意代码。目前该漏洞细节已公开，奇安信 CERT 已成功复现该漏洞。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

vm2 沙箱逃逸漏洞 (CVE-2023-29199) 安全风险通告

4 月 14 日，奇安信 CERT 监测到 vm2 沙箱逃逸漏洞 (CVE-2023-29199)。在 vm2 的源代码转换器异常清理逻辑中存在沙箱逃逸漏洞，攻击者可绕过 handleException() 并泄漏未清理的主机异常，进而逃逸沙箱实现任意代码执行。目前该漏洞细节及 PoC 已公开，奇安信 CERT 已成功复现该漏洞。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Windows 通用日志文件系统驱动程序权限提升漏洞安全风险通告

4 月 12 日，奇安信 CERT 监测到 Windows 通用日志文件系统驱动程序权限提升漏洞 (CVE-2023-28252)，由

于 Windows 进行基本日志文件操作时存在越界写入，本地攻击者可利用此漏洞获得对内核的读写权限，从而将自身权限提升至 SYSTEM。目前已发现此漏洞的在野利用，同时奇安信红雨滴团队已成功复现此漏洞。鉴于此漏洞影响较大，建议客户尽快做好自查及防护。



vm2 沙箱远程代码执行漏洞安全风险通告

4 月 11 日，奇安信 CERT 监测到 vm2 远程代码执行漏洞 (CVE-2023-29017)，由于 vm2 处理异步错误时未正确处理 Error.prepareStackTrace 的宿主对象，导致攻击者可以绕过沙箱保护，在运行沙箱的主机上远程执行任意代码。值得注意的是，经测试，在 Node.js <= 16.14.0、Node.js <= 17.4.0 及 Node.js 16.xx 以下的所有版本不受此漏洞影响。目前奇安信 CERT 已成功复现该漏洞，鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。



瑞友天翼应用虚拟化系统远程代码执行漏洞安全风险通告

4 月 10 日，奇安信 CERT 监测到瑞友天翼应用虚拟化系统远程代码执行漏洞。瑞友天翼应用虚拟化系统是西安瑞友信息技术资讯有限公司研发的基于服务器计算架构的应用虚拟化平台。未经身份认证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。目前奇安信 CERT 已成功复现该漏洞，鉴于该漏洞影响范围较大，建议客户尽快升级到安全版本。



Apple 多个产品高危漏洞安全风险通告

4 月 10 日，奇安信 CERT 监测到 Apple 发布安全通告，Apple IOSurfaceAccelerator 权限提升漏洞 (CVE-2023-28206) 和 Apple WebKit 代码执行漏洞 (CVE-2023-28205) 存在在野利用，未经身份认证的远程攻击者可以组合利用这两个漏洞，通过诱导受害者打开特制网站，最终导致在受害者系统上以内核权限执行任意代码。鉴于这些漏洞影响范围较大且存在在野利用，建议客户尽快做好自查及防护。



SonicOS 拒绝服务漏洞安全风险通告

4 月 4 日，奇安信 CERT 监测到 SonicOS 拒绝服务漏洞，SonicOS 中存在栈溢出漏洞允许未经身份验证的远程攻击者通过发送特制 HTTP 请求造成栈溢出，覆盖 canary，导致防火墙崩溃重启。目前已监测到该漏洞细节及 PoC 在互联网公开，经研判该 PoC 稳定有效。鉴于该漏洞影响范围极大，建议客户尽快做好自查及防护。



3CXDesktop App 代码执行漏洞安全风险通告

3 月 31 日，奇安信 CERT 监测到 3CXDesktop App 代码执行漏洞 (CVE-2023-29059)，3CXDesktop App 部分版本在构建安装程序时，内嵌了攻击者特制的恶意代码，在程序安装时会执行恶意代码，并进一步下载恶意负载到目标环境中执行。鉴于该产品用量较多，建议客户尽快做好自查及防护。

3CXDesktop App 是一款跨平台桌面电话应用程序，适用于 Linux、MacOS 和 Windows。3CX 在全球 190 多个国家和地区提供服务，拥有超过 1200 万日活用户和 60 万以上的客户群体。



Spring Framework 身份认证绕过漏洞安全风险通告

3 月 22 日，奇安信 CERT 监测到官方发布了 Spring Framework 身份认证绕过漏洞 (CVE-2023-20860)，当 Spring Security 使用 mvcRequestMatcher 配置并将 "**" 作为匹配模式时，在 Spring Security 和 Spring MVC 之间会发生模式不匹配，最终可能导致身份认证绕过。鉴于此产品用量较大，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。

全民国家安全教育日

2023 年 4 月 15 日是第 8 个全民国家安全教育日。这一节日的设立是为了增强全民国家安全意识，维护国家安全。作为国家安全的重要内容，政企机构不断增加在安全软硬件方面的投入，但却忽视了对员工进行适当的安全实践培训。研究表明，降低网络风险的最佳方法之一是建立有影响力的网络安全文化，让人成为抵御网络攻击的第一道防线。



应对网络威胁始于安全文化建设

2023 年全民国家安全教育日的活动主题为“贯彻总体国家安全观，增强全民国家安全意识和素养，夯实以新安全格局保障新发展格局的社会基础”。总体安全观要求我们更加全面地认识和对待安全问题。

一、人为因素仍是头号安全问题

网络安全领域的一个普遍误解是，认为在技术上投入更多资金就可以降低网络攻击。但研究和实际状况却戳穿了这一神话：波士顿咨询集团的研究表明，只有 23% 的安全事件源于网络安全技术不足，而 77% 是人为错误造成的。威瑞森公司《 2022 年数据泄露调查报告 》则显示，82% 的数据泄露涉及人为因素。《 世界经济论坛 》2022 年的全球风险报告也指出，95% 的网络安全问题可追溯到人为错误。

人的确会造成很多漏洞和错误，给攻击者造成机会，比如，对外发送包含敏感数据的邮件、被人尾随进入限制区域，或者点击恶意邮件与链接，登录凭据失窃等。这些都可能被黑客用于恶意目的。

事实上，现在大量网络犯罪事件都是由针对员工的网络攻击造成的。全球网络安全研究发现，社会工程攻击仍然是全球组织面临的巨大威胁。97% 的网络攻击都涉及某种类型的社会工程攻击。

攻击者已经意识到，对人下手远比攻击技术基础设施要简单得多了。很多网络攻击都利用人员漏洞。攻击技术可以是高度针对性的，也可以是大范围施展的。这通常是通过网络钓鱼攻击实施——攻击者诱使用户点击恶意链接、交出敏感信息或安装恶意软件。安全公司趋势科技曾发布研究称，91% 成功的网络攻击都始自于网络钓鱼邮件。

研究人员发现，网络犯罪分子越来越多采用网络钓鱼，2022 年钓鱼攻击出现飙升。卡巴斯基的反钓鱼系统在 2022 年成功阻止 5 亿次访问欺诈内容的尝试，是 2021 年阻止次数的两倍。国际联盟和防欺诈组织反钓鱼工作组（APWG）在 2022 年前三个季度记录的钓鱼攻击，打破了 APWG 有

网络安全领域的一个普遍误解是，
认为在技术上投入更多资金就可以降低网络攻击。

史以来最糟糕的季度纪录。

Cyber Security Hub 在 2022 年针对网络安全专业人士的调查中，75% 认为社工与网络钓鱼攻击对组织构成最危险威胁。在 2022 年，Dropbox、Revolut、Twilio、Uber、LastPass 和万豪国际等机构先后遭受社工与网络钓鱼的攻击，凸显出这一攻击的危险性。

在人为原因中，除了社工与钓鱼攻击，人为错误也是造成安全事件的重要原因之一。威瑞森《 2022 年数据泄露调查报告》中，82% 的数据泄露中，其中 13% 直接归因于人为错误。2022 年国内某地发生数亿规模的居民数据泄露，直接原因是开发人员在论坛中泄露了数据库的访问凭据。这说明，除了密码保护系统，政企机构还需要采用更多措施来应对人的错误，以确保数据的安全。

Osterman Research 的调查结果显示，目前组织的安全团队担心一系列网络威胁——数据泄露、凭据泄露、恶意邮件附件、账户接管、勒索软件、鱼叉式网络钓鱼、恶意 URL、邮件欺诈 (BEC)、文件共享和非邮件渠道的社工攻击。这些威胁的大多数都依赖于人为错误才能成功。

万豪酒店	黑客组织使用社会工程手段侵入员工计算机，泄露 20 GB 数据	22 年 6 月
密码管理器提供商 LastPass	通过开发者帐户获得对未授权访问	22 年 8 月
Twilio	因 SMS 网络钓鱼攻击，发生数据泄露	22 年 8 月
金融科技公司 Revolut	因社工攻击发生用户数据泄露	22 年 9 月
优步	通过承包商账户，访问公司内部服务器	22 年 9 月
游戏开发商 R 星	因网络钓鱼攻击发生数据泄露	22 年 9 月
Dropbox	因网络钓鱼攻击发生数据泄露	22 年 10 月

表 1 人为原因是引发安全事件的重要因素

二、网络安全意识从未如此重要

人为错误是迄今为止安全事件的最大原因，解决这一问题将是减少安全事件和数据泄露的关键。一份调查显示，全球 97% 的人无法识别网络钓鱼邮件；74% 的人会下载潜在的恶意文件，因为他们缺乏发现和预防的网络安全意识。

在确保组织数字资产的安全和保障时，网络安全意识培训仍然是最好和最有价值的投资回报。

安全研究人员不断利用人工智能、机器学习和区块链进行技术创新，以对抗不断增加的网络威胁。但是，仅靠技术是不够的。网络安全意识和教育仍将必不可少。了解最新的威胁和漏洞，并采取必要措施保护自己对个人、企业和政府来说至关重要。

现在，网络安全意识被安全人士视为应对安全问题的最简单、最快捷和最经济的方式，网络安全意识是个人和组织为保护自己免受威胁而学习的知识和采取的行动，也就是利用安全意识活动和网络安全意识培训——提高 “人工防火墙”的能力和发展具有网络安全意识的文化。

在联系日益紧密的世界中，网络安全意识的重要性从未如此重要。安全意识被视为消除网络安全攻击风险的最佳方法之一和消除人为错误的最好起点。通过对员工进行培训，帮助其掌握识别和应对网络威胁所需的信息，可以从源头上消除风险，并立即从源头上防止网络攻击行动的演进。

2022 年发生了一系列通过社工攻

击和人为错误发生的安全事件，影响到优步和知名游戏开发商 R 星等多家大型组织后，许多安全领导者开始强化安全意识培训，以更好地教育员工注意行为的安全性。

网络安全意识的重要性其实超越个人和企业保护。它也是国家安全和公共安全的关键要素。政府和组织有责任保护公民和利益相关者免受网络威胁。政府可以通过支持研发为个人和组织提供指导和资源，以及执行法律和法规追究网络罪犯的责任来提高网络安全意识。

组织可以通过投资网络安全培训、实施最佳实践和进行定期安全审计，来提高网络安全意识。通过合作，个人、企业和政府可以为每个人创造更安全的数字环境。

除了网络攻击的风险，物联网 (IoT) 和其他新兴技术的发展也带来了新的网络安全挑战。这突出表明需要持续的网络安全意识和教育，以领先于最新的威胁和漏洞。

安全意识培训应是所有组织的首要任务，最终让意识成为关键词。通过对全体员工进行安全意识教育，使其能够在攻击的初期关注到恶意活动，安全地创建和存储密码，并识别和减少社会工程尝试。

> 人为错误是迄今为止安全事件的最大原因，解决这一问题将是减少安全事件和数据泄露的关键。

奥斯特曼（Osterman）研究报告显示，近五分之四的 IT/ 安全决策者和影响者认为，技术和培训在应对安全威胁方面同等重要。当问及这两种方法的单独作用时，超过一半的人认为，培训是将网络安全风险降至最低的更有效的方法。

人通常被认为是信息安全中的“最弱一环”。通过提高网络安全意识，个人和组织可以采取主动措施来保护自己免受在线威胁，将成功攻击的风险降至最低，将最弱一环打造成最强资产。

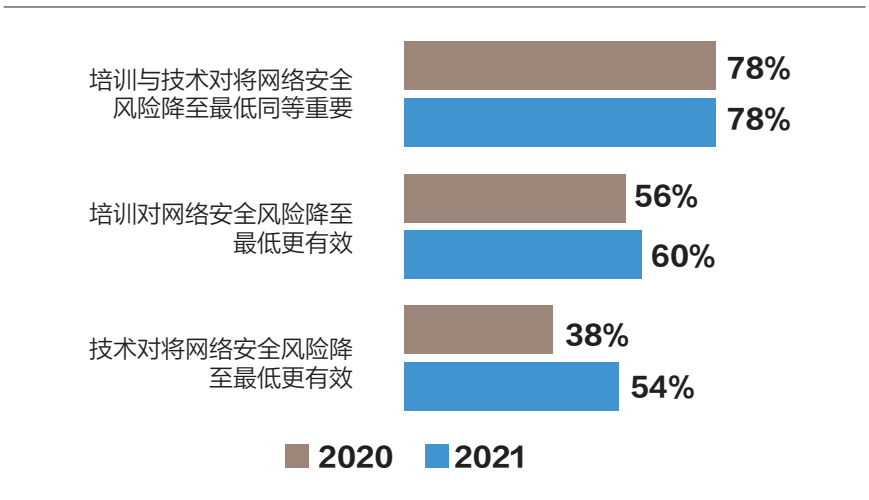


图 1 用户对培训重要性的认识逐年提升

三、网络安全意识从未如此重要

网络攻击的风险很大，后果可能很严重。安全意识在当今的数字世界中至关重要，而且其重要性只会越来越大。采取积极措施和提高安全意识可以降低网络攻击得逞的可能性，并最大限度地减少网络攻击造成的损害。未来随着技术的进步，网络攻击的威胁只会增加。这意味着未来对网络安全意识培训的需求将变得持续增加。

但真实情况却不容乐观：SANS 2022 安全意识报告分析了世界各地一千多名安全专业人员的数据，以确定组织如何管理其人为风险。报告发现，超过 69% 的安全意识专业人员是兼职的，他们花在安全意识上的时间还不到一半。

提高网络安全意识的一种方法是通过教育和培训计划，这可以帮助个人和员工了解网络攻击的风险，以及如何采取必要措施来保护自己。但对组织来说，开展安全意识和培训需要

找到更好的方法，不仅要对员工进行网络安全教育，还要通过可衡量的方法来降低风险。

根据《PC Magazine》2019 年进行的一项调查显示，即便经过十多年的敦促、警告、安全意识月、企业安全意识培训等，大多数美国人仍缺乏基本的网络安全知识，得分只能达到 D（等级）。

安全公司 Proofpoint 称，尽管 99% 的组织声称提供网络安全意识计划，但员工仍然不具备基本的网络安全知识，47% 的组织仍然缺乏对“网络钓鱼”概念的理解。

在过去五年左右的时间里，尽管“针对人的网络”产品开始激增。但这些项目的存在是为了满足“意识培训”的监管要求。

临时的、分散的员工培训尝试是行不通的。如果想要充分的内部防御来抵御复杂的网络钓鱼威胁，应该每月对 100% 的员工进行培训。

Cyber Guru	意大利网络安全意识培训平台	21 年 6 月获 360 万欧元 A 轮融资
SoSafe	德国初创公司，提供游戏元素的网络安全培训平台	22 年 1 月，获得 B 轮 7300 万美元融资
HacWare	美国初创公司，与 Office 365 集成，提供网络安全培训	22 年 4 月，获得 230 万美元种子资金
Hoxhunt	芬兰发展最快的游戏化 SaaS 网络安全培训平台	2022 年 5 月获得 4000 万美元 B 轮融资
CybSafe	英国初创公司，提供订阅模式，SaaS 化“行为安全”平台	22 年 6 月，获得 2800 万美元 B 轮融资
Hack The Box	英国初创公司，提供游戏化网络安全培训平台	23 年 1 月，融资 5500 万美元
Riot Security	美国初创公司，提供安全意识培训	23 年 2 月获 1200 万美元 A 轮融资

表 2 安全意识培训初创公司受到投资机构关注

企业在硬件和软件上花费了数百万美元，却忽视了对员工进行适当的安全实践培训这一简单行为。教导员工识别威胁、遏制不良行为，并遵循基本的安全习惯可能是最好的投资回报。

为实现这一目标，安全领导者需要针对不安全的行为制定基于风险的意识培训计划，为员工提供一种引人入胜且实用的以人为本的安全意识培训方法。

四、从安全意识到安全文化

保护组织免受网络攻击始于建立安全文化。网络安全意识培训会形成一种重视网络安全、使安全成为日常业务行为一部分的文化。大多数情况下，这是网络安全意识培训的最后阶段，也是网络安全成熟度的最终阶段。

在当今的现代工作场所，几乎所有员工都使用联网设备，这些设备使工作更轻松，但也为入侵者创造了无数的入口点。

Juniper Research 认为，所有企业都必须意识到网络攻击的整体性质，需要从整体上采取防护措施。随着社会工程学的不断发展，以人为中心的安全策略需要在企业安全中占据一席之地。

因此，组织必须了解，文化也可以用作网络安全的策略和工具，是降低网络风险的最佳方法之一。任何组织的目标都应是培养网络安全文化，以确保组织的弹性，并在面临网络攻击时最大限度地减少损失。

1. 为何文化是关键

塑造人类行为和减少人为错误是一个长期而复杂的过程，不能通过不

定期的行动来解决。只有强大的安全文化才能塑造员工在网络安全方面的行为、规范、态度和思维。我们可以从高危工作环境机构（如发电站、石油平台和铁路）看到安全文化的价值。

在过去的 30 年里，高危行业努力使商业文化与安全目标保持一致，最终真正减少了安全事故的发生。

这些面临高危环境的机构一直努力培训员工，但却发现员工的行为改善并没有持续多久。20 世纪 70 年代，社会学家巴里 · 特纳 (Barry Turner) 开始寻找培训失败的原因，结果发现文化是改变问题的关键。

20 世纪 80 年代发生的几起引人注目的事故，例如，自由企业先驱号沉没、切尔诺贝利爆炸和挑战者号航天飞机事故，使特纳的理论得到了更多的理解和接受——组织的组织架构、文化、政策和管理流程直接影响工业事故的发生。

现在，各类组织可以借鉴这些高危行业的经验教训，构建自身的网络安全文化，这是降低网络风险的最佳方法之一。与组织坚持的其他企业价值观一样，网络安全必须融入业务之中。这需要组织对员工进行培训，将安全融入员工的思维之中。在员工最终形成一种心态，即风险是真实存在的，他们的日常行为会影响网络风险。

因此，对组织来说，最重要的是转变企业文化，使其成为能够在整个业务流程中提高人员安全意识的推动力。在 2017 年重大网络安全事件之后，Equifax 公司开始积极改变其安全文化，并取得了显著成果，凸显出网络安全中“人的因素”的重要性。

> 组织的组织架构、文化、政策和管理流程直接影响工业事故的发生。

2. 什么是网络安全文化

网络安全文化的概念是指组织的员工队伍对网络安全的态度、知识、假设、规范和价值观。这些由组织的目标、结构、政策、流程和领导层决定。

良好的网络安全文化是一种文化的组织决定因素（政策、流程、领导、社会规范等）和文化的个人决定因素（态度、知识、假设等）与组织的网络安全方法保持一致的文化，体现在网络安全意识行为中。

技术和市场研究公司 Forrester Research 首席分析师 Jinan Budge 将网络安全文化定义为一种工作环境，每个人在其中都对网络安全感到兴奋，并有动力使其变得更好。人们理解为什么网络安全很重要，他们将自己视为解决方案的一部分。

因此，安全文化不仅仅是网络安全意识。它要求员工了解安全风险和避免风险的过程。“网络安全文化”概念让安全意识行为成为组织文化的一部分，从而让组织中的人员成为强大防御的组成部分。

Forrester Research 认为，组织现在应该关注意识、行为和文化，而不仅仅是安全意识课程和培训，前者才是降低人的风险的基础。安全意识现在是无国界的，灌输无处不在的安全文化至关重要。创建有影响力的网络安全文化的核心和关键是认识到，人而不是技术让组织变得安全。人既是网络安全链中最薄弱的环节，也是网络攻击的最佳应对者，代表抵御网络攻击的第一道防线。营造让员工具备成为第一道防线的知识和本能的环境至关重要。

3. 文化的价值不至于安全

在员工中形成精通网络的思维方式和网络安全文化，这不仅仅可以防止网络攻击和破坏，也是给客户信心并建立信任。这同样是企业要承担的社会责任。

精通网络的思维方式和网络安全文化可以将整个组织凝聚在一起，专注于关注技术带来的增长机会；同时，也会让员工感到自豪，相信组织能够妥善保管客户的数据。

此外，精通网络安全知识作为一种重要技能，可以让员工应用到个人生活中，用来帮助其家人。

因此，拥有一支对数字信任和网络安全的影响有着深刻洞察和理解的员工队伍，可以降低组织的安全风险

并推动价值创造，可以更轻松地做出明智的决策与投资。

五．如何建立强大的网络安全文化

建立网络安全文化始于提高全体员工对个人风险和责任的认识，这包括从董事会到基层。

网络安全文化目标必须具有战略性、组织一致性和风险一致性。让网络安全文化成为规范日常行为的更广泛企业文化的一部分，鼓励员工在网上进行任何操作时，始终将组织的安全放在首位，做出符合安全政策的深思熟虑的决定。

至关重要的是，在对网络文化实施变革时，要不断倾听员工的意见，了解变革如何影响参与网络安全的方式，并进行调整。

网络安全文化具体建设不是一蹴而就的，涉及到多个关键要素。有媒体总结，网络安全文化包括 7 大要素。

⑴ 高层领导

培养网络安全文化的最关键的一点是必须从高层开始。领导层的支持对于安全文化至关重要。为了鼓励员工树立安全第一的心态，最高管理层要以身作则，将安全融入组织的方方面面。如果网络安全问题不是管理团队的首要任务，高管就不能指望员工会关注网络安全问题。

高管和董事会成员制定业务战略时，安全必须成为讨论的中心。高管还须积极通过虚拟或者线下方式向员工宣传关键信息。例如，向组织的每个人强调安全是企业价值观的内在组成部分，以确保全体员工了解行为安全的重要性。沟通对于建立参与度和培养网络安全文化至关重要。要促进安全文化变革，重要的是要用员工理解的方式进行沟通。

⑵ 跨职能工作组

由于每家机构的威胁、端点和漏洞的多样性，维持安全文化的一部分包括成立跨职能的工作组。该工作组应致力于识别风险和机会；弥合不同群体之间的安全优先事项；以及制定跨业务职能、团队和产品部署的具体保障措施。

跨职能工作组还有助于发现影响安全心态和最佳实践的文化障碍。例如，美国联合航空公司组建的意识和教育团队，在各个团队中选出“网络大使”和“安全之友”，以关注各自部门的安全问题。拥有主题专家和普通员工的观点，对于确保整个组织得到强化至关重要。

⑶ 教育与培训

奥斯特曼（Osterman）研究报告表明，培训是强大网络安全文化的基石。定期的培训可以显著提高用户检测网络威胁的能力。接受更多培训的员工也认为自己扮演着更负责任的角色，这是组织安全文化不可或缺的一部分。

与花费大量时间的员工相比，每月花很少时间在安全培训的员工，有三倍多的可能性认为自己对保护组织免受威胁的作用很小或根本没有作用。

安全意识培训对于文化发展至关

建立网络安全文化
始于提高全体员工对个人风险和责任的认识，
这包括从董事会到基层。

重要。但培训必须引人入胜、有趣、信息丰富且互动。网络钓鱼模拟练习是吸引用户并根据特定需求定制学习体验的好方法。对个人和部门在建立和维护数据保护和隐私法规方面的作用的认识应该是意识培训计划的组成部分。

调查显示，只有 50% 的受访者喜欢培训的写作质量；只有 45% 的人认为培训具有吸引力。这显示培训的质量和乐趣还有很大提升空间。

⑷ 员工相关性

安全意识的需求是普遍性的，但培养意识和教育员工不能一刀切。让员工了解自己的具体职责，以及如何帮助或阻碍组织的整体安全至关重要。这包括制定融入员工日常工作的网络安全流程，而不是要求进行烦琐或大幅的行为改变。学习工具和培训方式需要提供个性化内容。集成能够引起共鸣的场景，以及支持团队相关问题的解决方案等。

⑸ 态度和行为

组织的文化是员工的感受，包括信念、想法及其感知的价值观。这部分是为了让员工在发生错误时感到舒服，而不是惊慌失措。简而言之，员工积极为组织网络安全弹性做出贡献。

曾有组织专门聘请心理学家，以更好地了解如何让员工以易于接受的方式了解安全，包括提供各种培训方式——如通过使用游戏化、短视频和面对面讨论；同时为不同地区和语言的员工量身定制内容。

⑹ 生态系统

网络安全文化中经常被忽视的部分包括在公司的边界之外工作。应对数字威胁需要拥抱开放的文化。例如，在利益相关者之间共享威胁分析、使用开源代码或模型，以及将审计和问责制指标纳入采购和合作伙伴关系，



这些都有助于提高组织的安全性。

组织可以成立专门致力于安全问题信息共享的小组，其中包括各个行业的战略客户，以整合由外而内的观点。这不仅对公司推动自身的安全文化很有价值，也是以安全名义实现创新的直接途径。

⑺ 强大安全文化的指标

指标是监控培训有效性和整体价值的关键，可以使用多个指标来评估网络安全文化的发展和有效性。其中包括事件报告率、员工反馈流程等。它们对于向领导层阐明持续投资的价值，以及员工在取得成果上再接再厉也很重要。例如，安全和 IT 团队可以尝试将指标与生产力提高、员工激励、学习新技能的机会等联系起来。

建立强大的网络安全文化是一个持续的过程，需要组织中所有员工的参与与努力。通过关注高层的基调、安全测试、培训和教育、事件报告和无责备方法等关键要素，可以建立一种安全文化，不仅满足法规遵从性要求，还可以降低组织的网络威胁风险。

全员参与 渐进式培养企业的安全基因

——安全意识和能力培训实践

为了从源头上避免安全事件发生，网络安全意识和能力培训现已成为企业关注的核心问题。这一过程需要企业和员工共同努力，以达到提高全员网络安全意识和应对能力的效果。

奇安信集团以全员参与为目标，把网络安全意识渗透到日常工作中，通过渐进式培养员工安全基因，达到保障企业和客户的网络安全和数据安全的效果。

一、进阶培训课程设计体系

奇安信集团的网络安全意识和能力培训是一套分阶段开展的解决方案。



这个方案分为四个阶段——面向新入职人员的不踩红线阶段；针对年度普及的全面防护阶段；分角色的专岗专培训阶段； 面向“易感人群”的加强培训阶段。

1. 新入职人员——不踩红线阶段

新入职员工面对新的环境，短时间要接触各方面的信息，如果此时将安全体系的网络安全要求推给员工，可能会出现对网络安全知识和要求“消化不良”的现象，难以达到培训的效果。

但新入职场景下也是印象和意识导入从 0 到 1 的环节，一旦导入成功，将印象深刻。因此我们选择将网络安全最重要的内容推给新入职员工，达到新入职“不踩线”，给新入职员工留下网络安全在公司很重要的效果即可。

在员工新入职阶段，需要了解常见的网络安全威胁和入侵手段，并明确如何防范这些威胁和入侵手段。同时，培训需从公司的网络安全体系的角度出发，介绍公司的网络安全事件和数据安全事件，明确员工个人行为的安全要求和对数据安全的重视程度。最后，介绍公司的网络安全制度、流

程及培训的检索方式，以及如何在发现风险时及时联系网络安全部门上报风险。

2. 年度普及——全面防护阶段

年度普及培训是针对存量员工进行的定期性安全培训。通过安全培训，让员工全面了解网络安全相关的防范措施，鼓励职工养成正确的安全行为习惯，形成良好的安全管理机制，从而降低事故的发生率，提高职工安全素质，从而达到全面防护的目的。

年度普及培训需要制定具体的培训计划，包括培训时间、课程内容和培训方式等。同时，也需要对培训的目标和效果进行明确和评估。通过全员网络安全意识培训，提高员工的整体素质和技能水平，增强企业竞争力，推动企业发展。全员网络安全意识培训主要包含网络安全意识的重要性、典型案例、网络安全风险防护措施三方面内容。网络安全意识的重要性主要包含国家政策普及、集团四大驱动、网络安全意识和能力的培养及相关宣贯；典型案例主要包含集团的内部通报批评、网络安全事件案例、数据安全事件案例及集团的网络安全红线；网络安全风险防范措施主要包含终端安全、密码安全、数据安全（全生命周期的保护、办公文档的分类分级）、防钓鱼（社工钓鱼、邮件钓鱼、WiFi 钓鱼、IM 钓鱼、非官网下载钓鱼）、安全流程、风险上报。

全员网络安全意识培训主要是为了提高员工的整体素质和技能水平，增强企业竞争力，推动企业发展。年度普及培训通常包括以下几个阶段：

(1) 培训需求调研 在培训开始前，对员工的培训需求及常见的网络安全事件及数据安全事件进行调研，了解员工在工作中存在的问题和需要提高



的技能，制定培训计划和课程内容。

(2) 培训计划制定 根据调研结果，需要制定具体的培训计划，包括培训时间、课程内容、培训方式等。同时，也需要对培训的目标和效果进行明确和评估。

(3) 培训课程开发 在制定好培训计划后，企业需要开始制定培训课程内容，课程内容要结合实际工作情况，注重实用性和操作性，确保培训效果。

(4) 培训实施 培训实施是整个年度普及培训的核心环节，包括邮件和蓝信公众号通知、与各部门安全专员沟通、考核考试、建立合理的监督机制等。同时，也需要提供相应的培训辅助材料和技术支持，并不断收集学员反馈，及时进行调整和改进。

(5) 培训效果评估 经过培训，需要对培训效果进行评估和总结。评估可以主要从学员满意度、工作表现、业绩提升等多方面考虑，以评估年度普及培训的总体效果。 总之，年度普及培训是企业中比较重要的培训环节之一，由于在培训期间涉及多个方面的工作，需要在培训前做好计划，有序地部署和推进，以确保培训效果的最大化。

3. 分角色培训——专岗专培阶段

在组织中，不同的职务、角色所承担的安全责任是不同的。因此，分角色安全培训可以针对不同职务、角色所面临的不同安全风险，提供相应的安全防范能力培训，使得每个人能够更好地理解并履行自己的安全职责。并通过生动形象的工作场景案例分析、实际演练等方法，加深员工对安全问题的认识和警惕性，激发员工的安全意识。同时增强员工的安全意识和安全素养，有针对性地提高整体的安全防护水平。

分角色安全培训是根据员工的角色、职责、使用的系统及数据，为他们提供特定的安全培训内容和实践指南。不同类别的员工通常涉及处理不同类型的数据和信息，因此需要不同的安全培训。这种做法可以有效地提高企业员工的信息安全意识和网络安全技能，让他们更加了解自己在公司内负责的安全职责，并且帮助他们更好地理解和应对各种网络攻击和安全威胁。

奇安信集团的分角色安全培训课程包含了多个方面，如下所示。

系统管理员：深入讲解网站、服务器等设备的安全防护技术，以及围绕权限的提供、申请、授权、使用、回收的全生命周期，对各方提出了要求；

网络管理员：介绍常见的网络安全威胁，以及网络安全风险管理的方法，通过实践案例和模拟演练来加强

相关技术的掌握；

开发人员：针对开发过程中，为从编码层面减少由于使用 Android、iOS、PHP、JavaScript 等不同编程语言不规范造成的产品漏洞，减少后期漏洞修复及相关损失，让其在编写应用程序时更加注重安全；

普通员工：培养员工的安全意识，教授网络安全基础知识、密码管理、社交工程等实用技能，帮助他们更好地防范网络安全风险。

4. 面向“易感人群”——加强培训阶段

“易感人群”可能会忽视或忘记安全问题，加强培训阶段可以加深他们对安全问题的认识和印象，提高他们的安全意识，避免类似事故再次发生。

针对数据安全事件和网络安全事件频发的组织进行，为易感人群提供定制化的、重点突出的网络安全培训。这种加强型的安全培训阶段可以使这些人员更加了解自己在公司内的责任，并学会如何应对各种网络安全威胁。这种培训包括但不限于以下几个方面。

⑴ 数据安全：数据安全背景（国内监管、企业内生需求、数据安全泄露风险）、数据安全事件案例（非必要采集、存储、传输、使用、外带 / 共享、删除销毁、账号权限）、数据安全要求（数据分级、数据事件、移动介质、账号权限、数据脱敏、终端安全、流程指引）。

⑵ 网络安全：网络安全事件案例（各类触犯网络安全红线的行为、集团内部通报批评）、网络安全制度规范（事件定级、原则及处置）、网络安全流程规范（终端安全、密码安全、安全流程）。

二、培训渠道

针对网络安全相关的培训，可以综合使用线下培训 – 现场宣贯、线下培训 – 课堂培训、线上培训、直播宣导、经验分享、海报及易拉宝、公众号及问卷、安全演练场景等不同方式，以确保培训的效果和广度。

不同培训渠道的优缺点对比及应用

培训渠道	培训特色
线下培训 – 现场宣贯	在社招员工的入职现场中快速的融入网络安全培训，以达到了解“安全红线”的目的
线下培训 – 课堂培训	在校招生集中培训中，用半天的时间体系化、全面化深入讲解网络安全，以提高知识性和互动性
线上培训	在全员培训中，尽可能多的触达学员随时随地学习网络安全培训，以提升培训的全员普及性
直播宣导	在非定向的加强培训中，利用直播的实时性、互动性和多样性，让学员能够更加深入地理解培训内容
经验分享	通过技术分享的方式，进行知识共享，增加团队凝聚力的同时，推动工作相关的提升和创新
海报及易拉宝	以润物细无声的宣贯方式，使网络安全的知识醒目易懂，让网络安全占领公司的每一个角落
公众号及问卷	利用蓝信公众号【网安快宣】专栏直白的规范在常见犯错的工作场景下的合规操作，避免事件的发生
安全演练场景	通过模拟真实的安全事件进行演习，让全员身临其境的实战网络安全的培训内容，促进培训效果

1. 现场宣贯

入职现场是针对新员工进行安全培训的重要机会，可以将安全培训或引导纳入入职流程当中，确保新员工对于企业安全政策和安全规范的充分理解和掌握。可以利用入职现场的投影仪和计算机进行安全演示，展示奇安信集团的网络安全制度和规范，以及涉及的各种网络安全威胁和风险。另外，重点介绍新入职员工可能会碰到的安全问题及应对策略，让新员工掌握必要的安全知识和技能，做到“防患于未然”。

2. 课堂培训

线下的课堂培训可以同样适用于较多专项网络安全教育场景，包括校招生、特定部门、特定岗位等。由网络安全专家逐一讲解网络安全知识，从基础到实践应用，再到案例分析。这种方式可以增加员工之间的互动性和参与性，同时能够提高员工对于安全知识的理解和掌握。

3. 线上培训

借助企业内部奇安学堂培训工具，开展线上培训，让员工在办公桌前或在家中就能够参与并学习。这是一种面向企业内部人员进行的网络安全知识普及活动，主要目的是提高员工对网络安全的认识和意识水平。此类培训通常采用集中授课的方式，由专业的安全从业人员给予讲解，包含网络安全基本概念、信息安全法规政策、网络攻击与防御等方面的内容。这种方式的优点是省去了线下面对面的时间和空间限制，员工能够自由学习，可以随时随地回看和巩固所学内容。线上培训可以保证每个员工都接受统一知识框架的培训，也具有较高的成本效益。



4. 直播宣导

通过网络以直播的形式进行的一种培训方式，它具有实时性、互动性和多样性等特点，让学员能够更加深入地理解培训内容。在开始直播培训之前，需要进行适当的宣传和推广，让学员提前了解培训主题和时间，减少缺席和麻烦。同时也要保证直播的接收质量，让学员能够顺利接收和参与直播，提高效果。直播培训结束后，可以通过学员反馈、考试成绩等方式，对培训效果进行评估。如果发现有问题，可以及时调整培训内容和方式，提高效果。同时，也需要针对培训课程进行效果监控、数据统计和分析，便于优化和改进。

5. 经验分享

企业安全专家或高管可以定期举办经验分享会议，分享企业内部安全体系的建设经历和实践案例，向员工们介绍如何遵守企业安全规范和准则。通过分享，网络安全人员可以获取来自同行或其他领域专家的知识。通过了解到其他团队在面对类似问题时所采取的解决方案，网络安全团队可以扩展他们的技能和知识范围。技术分享是促进新想法和创新发展的重要载体。分享可以鼓励开放思考，并引导团队思考如何将现有知识用于解决现有或未来的问题。

6. 海报及易拉宝

制作和张贴网络安全知识宣传海报和易拉宝、发布蓝信公众号、全员邮件，是一种较为传统和简单的宣传方式。海报应当醒目易懂、内容完整、简洁且具有针对性。通过海报，能够让员工从视觉上了解公司的安全政策和行为准则，提高员工对于安全风险的识别和应对能力。

网络安全周期间，网络安全部可以组织网络安全小游戏，针对新员工可能遇到的网络安全风险和问题，进行互动式教学。员工可以通过参与游戏和答题，来加深自己对于网络安全知识的掌握。



7. 公众号及问卷

利用蓝信公众号的网安快宣专栏对近期热点的网络安全事件、数据安全事件进行直白的宣贯，在常见犯错的工作场景下，规范违规行为，并提示合规的操作。

发布安全调查问卷，了解员工对于网络安全知识的掌握情况，大家所关心的安全问题和需求，以及培训提升的方向。然后，在此基础上做出针对性的安全培训和宣传，并设计更加有效的网络安全管理措施。

8. 身临其境的安全演练场景

网络安全部组织企业内部安全应急演练及内部的钓鱼演习。通过模拟真实的安全事件进行演习，对于团队成员而言，锻炼应急反应能力，并提高整体的协同配合水平，以更好地应对未来可能出现的安全事件；对于全体同事而言，提高员工对网络安全的认识和意识水平，为培训查缺补漏。

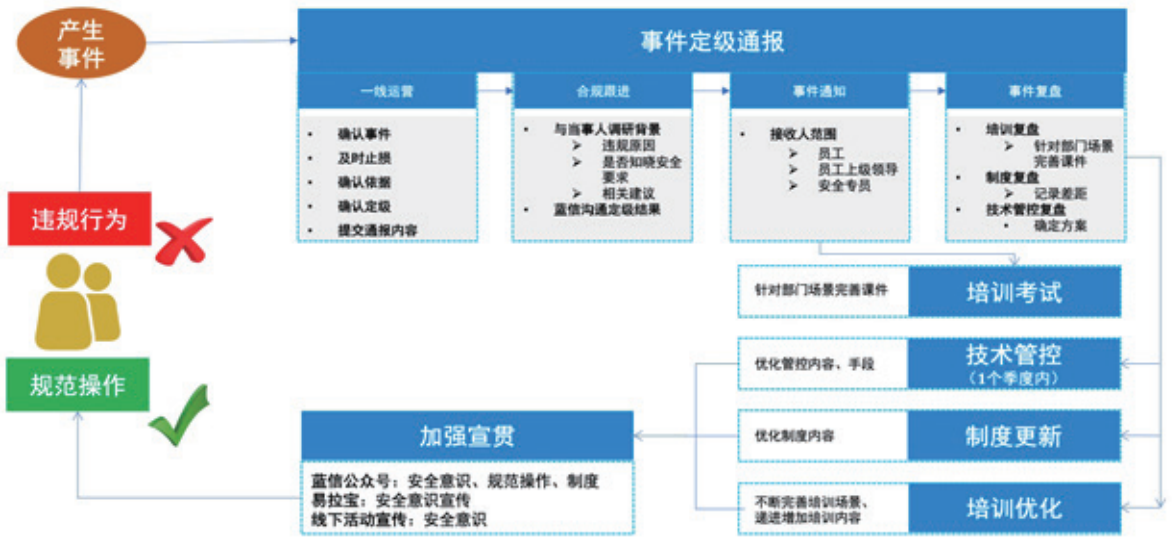
三、培训提升计划

网络安全培训应该从事件定级角度来提升，这可以让员工更好地理解网络安全事件的严重性和紧急性。网络安全培训提升计划的目的是提高员工的网络安全意识和技能，保障公司的信息系统安全，预防各种网络安全威胁。

从网络安全事件和数据安全事件的定级开始进行细化拆分，在一线运营确认事件后，合规跟进违规的原因及相关的建议，并通知相应同事进行培训考试。同时针对事件做技术管控、制度更新和培训优化三方面的复盘，针对每类事件进行技术、制度和培训三方面的优化和反思，最终加大宣贯力度，达到“规范操作”，减少安全事件的目的。

四、网络安全培训体系

综合上述的网络安全课程体系和培训的宣贯方式，汇总出一份全面的



培训 & 事件 & 制度闭环提升计划 V1



网络安全培训体系，从培训对象层、培训内容层、培训形式层、培训载体层和体系管理层等方面逐步构建。

培训对象层分析人员类型，从新员工阶段、在职阶段、提升阶段和持续教育阶段四方面实现不同岗位不同的网络安全需求和技能要求。培训内容层，根据集团特色分为安全意识、安全能力、政策合规三方面，并针对每一方面进行细化的知识图谱展开。培训形式层和培训载体层，根据人员类型、培训内容的性质及规模选择最合适的方式，同时最大限度地提升培训的互动性和趣味性。在体系管理层，将整个培训需要管理的内容进行划分，并建立有效的评估机制。

五、培训收益

通过以上的体系化、案例化的网络安全培训体系，不仅可以提高员工自身的安全资产价值，增强企业防御网络攻击的能力，还可以为企业带来其他收益。

（一）提高员工安全意识和保护能力。 网络安全意识培训可以让员工通过合理地使用安全技术手段，有效地保护自己的计算机和公司网络不受攻击。同时也可以提高员工对抵御和应对不确定、复杂的网络安全事件的框架、方法和技巧等方面的知识和技能，为企业提供了安全保障。

（二）减少网络安全威胁。 员工通过提高安全意识和保护能力，能够更好地察觉网络攻击的风险，减缓网络安全威胁对企业造成的巨大损失。因此，网络安全教育和培训能够降低员工的泄漏、外泄、盗用企业数据及资料的风险，增强企业网络安全。

（三）提高企业合规度。 合规对于企业已经是不容忽视的重要问题，网络安全意识和保护能力更是企业合规的基石。员工通过学习网络安全的基础知识和操作，规避一系列不利的企业合规事件，从而提高企业的安全能力。

网络安全意识培训和能力培养应作为企业网络安全治理的一项重要工作，能够提高员工的网络安全意识和保护能力，减少企业网络安全威胁，规避各种不利企业合规风险，并为提高企业整体防御水平奠定基础。

成为最厉害的白帽黑客，需要经历什么？

“你们觉得最厉害的黑客应该是什么样子？”笔者一本正经地问道。

正在鼓捣电脑的路人甲：“是什么样我不知道，但不是什么样我知道，比如我（笑出鹅叫）！”

一旁指手画脚的路人乙：“看过电影吧，给你个画面自己脑补——键盘噼里啪啦，屏幕滚滚而下，响指突然一打，系统全部拿下。”

话音未落，两位小哥又低下了头，钻进了属于他们的二人世界里，电脑屏幕左上角的补天平台 Logo 若隐若现。

突然，路人乙对路人甲兴奋地喊道：“我们上次在补天提交的 RCE（远程代码执行漏洞），奖金已经到账了。”

兴趣使然

3 月 28 日，补天平台如期举行了自己的十周年生日会。

四面八方的白帽黑客纷至沓来，他们中的大多数有着略显稚嫩的脸庞，却充满了年轻人独有的自信心，仿佛在告诉所有人，未来的赛博世界是属于自己的。

讲台上，补天平台负责人正眉飞色舞地讲着补天平台的辉煌过往：“补天平台始终把漏洞的快速响应放在首位，以打造一个健康、繁荣的白帽子社区为中国的网络安全做贡献为己任，成立十年来，共有超过十万名白帽黑客齐聚于此，提交了一百多万个漏洞。”

“那你知道最厉害的黑客应该是什么样子的吗？”笔者迫不及待地再次问出了这个问题。

“啊，我前年刚入行，这个话题离我还有点遥远。”一名补天 ID 叫作 BugMaker 的白帽子回答道，“不过你可以参考一下补天发布的‘实战化白帽人才能力图谱’（简称图谱），那里总结了不同阶段的白帽黑客所应掌握的实战化技能。”

“你说的是这张图么？”笔者拿起手机给他看。

“对，就是这张。你看，从最初级的 Web 漏洞利用到高阶的内网渗透和底层的漏洞挖掘，都在上面了。”BugMaker 点了点头。

笔者数了数，总共 14 大类、85 项具体技能。如果是最厉害的黑客的话，不敢说全都会，至少也掌握了绝大部分吧。

“我看这张图把技能分成了三个阶段，你大致在一个什么样的位置？这上面列的这么多技术，你都会去学

> 兴趣是指引白帽子前进的最佳“导师”，
> 也是白帽子进步的不竭动力。



习吗？”笔者接连发问。

“我撑死也就算是初级阶段呢，跟着学长和补天上的大神们在学习各类漏洞的利用方法。至于再往后学习，主要还是看兴趣吧。其实像我们大部分人入行都是因为兴趣，一次机缘巧合就对这玩意来了兴趣。”

听到这句话，笔者本着“社牛”的姿态四下问了一圈，得到的答案算是大同小异吧，有学长带着上道的，有社团一起打网络安全比赛的，还有自己账号被盗突发奇想的……

总之一句话，兴趣一直在路上。

后来 BugMaker 告诉笔者，大二的时候他写的代码出了一个小 Bug，不管自己怎么调试都无法运行，后来还是请教了很多人，才发现哪里出现了 Bug，后来就慢慢的对漏洞感兴趣了。

BugMaker 的 ID 也是来源于那里，意在靠自己的经历鞭策自己，撸代码的人都会制造一个又一个 Bug，但自己从当上白帽子的第一天起，目标就是将这些 Bug 和漏洞揪出来，确保不会受到坏人的侵扰。

从“脚本小子”开始

相比 BugMaker，与之年龄相仿的 Tracy（补天 ID）明显拥有更长的白帽子职业生涯。

他成为白帽子的年龄非常早，大概也就十四五岁，当时还在上初中。一个燥热的周六，他惊奇地发现自己的 QQ 账号被盗了。腾讯游戏玩家当然知道这意味着什么，这让本就只有

“脚本小子”并非贬义词，
站在前辈的肩膀上学习，
能够帮助初学者迅速掌握漏洞的基本原理，
树立强大的自信心。

假期才能玩一两个小时游戏的 Tracy 心凉了半截。

果不其然，他辛辛苦苦积攒的游戏装备，被盗号者“能毁尽毁”。那两年，他对盗号者恨得牙痒痒。

所以 Tracy 立志要成为白帽子。在他心里，干盗号这行当的肯定都是黑客，而网上说，白帽子是好黑客，极富正义感，是对抗坏黑客的生力军。

在做完这个决定之后的第一个周末，Tracy 像往常一样，被父母允许玩两个小时的电脑。出乎意料的是，他直接删除了他最爱玩的游戏，反手就在搜索引擎栏里输入了“白帽子”三个字。

面对网上五花八门的教程、科普文章，Tracy 一时间呆住了，不知道该从哪里开始。

直到一篇叫作《避免成为“脚本小子”》的帖子，出现在他的眼前。大概意思就是绝大多数白帽子都是从使用脚本工具入门的，但有些初学者学会使用一些自动化的漏洞扫描、利用工具之后就沾沾自喜，失去了继续学习的动力，成为只会用脚本的“小子”。

不过，Tracy 倒是没有在意很多人对脚本小子的不屑，他只有一个想法：打游戏有人开脚本就会变得很厉害，当白帽子岂不是也差不多？

“你听说过SQLMap吗？”Tracy反问笔者。

“当然听过，你看这里就有。”笔者指了指手机里图谱上的基础能力方格。

白帽子同学都知道，SQLMap 是一个自动化的 SQL 注入工具，其主要功能是扫描、发现并利用应用程序中的 SQL 注入漏洞。

Tracy 说，他学会使用的第一款安全工具就是 SQLMap，它的意义丝毫不亚于他玩的第一款电脑游戏，亦或者是篮球爱好者上脚的第一双高档篮球鞋，钓鱼爱好者手上的第一根鱼竿……

借助这款工具，Tracy 很快就学到了白帽子生涯的第一项技能——SQL 注入。

SQL 注入是指在原先正常的 SQL 语句上添加额外的非法 SQL 语句，以此来实现欺骗数据库服务器执行非授权的任意查询，从而进一步得到相应的数据信息。

“在入门阶段，当‘脚本小子’真的很酷，它让我也成为了当时同学们心中遥不可及的‘黑客’。”Tracy说，他用了酷这个词。SQLMap 可以让他批量测试 SQL 注入漏洞，每次成功利用都让他有一种不可名状的满足感。

在他那些还只会打游戏的同学们眼中，他就是很酷。

有意思的是，在笔者沟通过的若干个白帽子当中，大部分学会使用的第一款工具都是 SQLMap。

类似 SQLMap 的脚本工具还有很多，比如某些偏执狂最钟爱的 BurpSuite，能够自动化抓取数据包，便于批量收集目标情报信息；再如同样以 SQL 注入见长的啊 D 注入工具、

名小子等……

挖洞有一定的门槛，对新手并不友好，所以利用老旧漏洞练习是每一位白帽子的必修课。自动化脚本工具可以让漏洞利用的门槛降到很低，而且能够帮助用户快速掌握各类漏洞的原理和利用方法，几乎是所有白帽子入门必备。

很多人觉得“脚本小子”是一个贬义词，但 Tracy 并不这样觉得，他崇拜的一位大神就常以“脚本小子”自居。而且，使用脚本并不是新手的专属，强大便捷的工具谁会不爱呢?

逃离舒适区

和很多人不同的是，科班出身的 Enjoy（补天 ID）并非是从当脚本小子开始的。作为网络安全专业的学生，他在大一、大二两年期间就打下了优秀的编程基础，C/C++、Java、Python、Go 等主流编程语言都有广泛涉猎。

“大二的时候，我发现我们社团有个学长时不时就会在补天或者各大 SRC 提交漏洞，后来就带着我一起搞 Web 安全了。”Enjoy 说，因为代码写得多，一上手就和另一位伙伴一起学着搞搞代码审计。

比很多人都幸运的是，Enjoy 很快就拿到了开门红：在学长的帮助下，他通过审计源代码，发现了某一线软件厂商旗下某款办公软件的前台 RCE，甚至这还是一个高危 0day 漏洞（即从来没人发现过的漏洞）。

在提交给相关软件厂商后，Enjoy 拿到了人生的第一桶金，这对于当时还是学生的他，简直是一笔巨款。

相比之下，Kamelo（补天 ID）要更加励志一些。作为编程和黑客的重度爱好者，大学期间除了和同学一起打篮球、看球赛，他有事没事都泡在学校的计算机实验室。

Kamelo 尤其喜欢研究各种黑客小工具，并叹服于前辈大神怎么能开发出这么多功能强大、使用便捷的小玩意。

“该说不说，当‘脚本小子’真的很爽。”Kamelo 说。想象一下，一杯茶，一包烟，一个脚本跑一天的躺平生活，几乎不用动什么脑筋，他就是从这里一步步开启白帽子生涯的。

但 Kamelo 并不止于此，他最喜欢周杰伦《听妈妈的话》这首歌里面的一句歌词：将来大家看的都是我画的漫画，大家唱的都是我写的歌。

所以他有自己的小目标：有一些自己首发的 0day 漏洞，网上能流传着自己写的安全工具和攻防渗透科普文章。

从基础能力向进阶能力过渡，并不是一条坦途。Kamelo 几乎每天都会花费大量的时间研究编程技巧及各类漏洞的成因，这样才能知道什么样的代码会产生漏洞，这些漏洞到底该怎么利用。

甚至，他会针对自己写的漏洞进行复现，同时尝试编写漏洞利用的代码（EXP）。

尽管直到现在，Kamelo 离自己当初定下的小目标还有一定的距离，但在补天攻防社区，他写的渗透技巧攻略文章有着很高的关注度，很多都有大几千上万的阅读量，同时也收获了一批忠实的粉丝和白帽朋友。

“在参加补天校园行活动的时候，我很喜欢一位嘉宾分享的这样一句话。”Kamelo 说，“白帽子从入门到精通，编程能力是一道最明显的分界线。”

在他看来，掌握一种或多种主流编程语言可以帮助白帽子更轻松地阅读和理解源代码，确实有助于提升漏洞挖掘能力，通过深入理解目标应用程序的代码和底层架构，白帽子可以更容易地发现潜在的漏洞，并尝试利用它们进行攻击。

在图谱的中间层进阶能力方格，尽管编程能力只是作为其中的一项被单独列出，但无论是编写 PoC（漏洞验证过程）还是 Web 漏洞挖掘，编程能力都是核心。

主流队伍的大洞，几乎都是通过代码审计进行挖掘的。

向更底层前进

那么，什么是大洞?

> 躺在前人的成果上，
> 是白帽子的隐形杀手。
> 想要更进一步，逃离舒适区，
> 自立门派研发出“独门绝技”是必经之路。

> 系统底层的奥妙是所有白帽子攀登的最高峰，
> 其漏洞的争夺是黑白之间
> 乃至国家之间网空竞争的“战略要地”。

危害大？影响面广？其实好像也没有一个明确标准的定义，姑且把漏洞触发后危害大、漏洞影响用户多的漏洞叫作大洞吧。

那么，什么样的漏洞会同时满足这两个条件呢？肯定有人立马想到了 2017 年爆发的永恒之蓝。

说起永恒之蓝，这个漏洞有一个明显的标志，它位于微软 Windows 操作系统之上。相对于各类软件应用，操作系统要位于计算机更底层的位置，因此通常情况下，系统层的漏洞破坏性要更强，更容易成为一个大洞。

这么说是有原因的。

如果把整个 IT 系统比作一个水桶，那么在上层的 Web 应用上捅一个洞，只有最上面的那部分水会流出来；但如果在下面的操作系统上捅一个洞，那么可能整桶水都会流出来。

所以，这种来自底层的漏洞，更容易成为国家之间网空对抗的网络军火。

只不过，系统层漏洞不是谁都能挖的。顺着图谱往下看，在高阶能力方格，系统层漏洞挖掘赫然立于其中。如果你能干这个，至少也得是一个高阶白帽子了。

换句话来说，如果想成为一名高阶白帽子，在摆脱脚本小子的舒适区之后，还得继续往更底层前进。

以安全老炮自居的 TheSky（补天 ID）很有话说，一头浓密的黑发让人很难将他与十几年白帽子的身份联系起来。

总结十几年的挖洞经验，他认为与 Web 应用的漏洞挖掘相比，系统层的漏洞挖掘难度主要体现在以下几个方面。

复杂性：系统层漏洞的挖掘需要对操作系统、网络协议、系统内核等底层技术有深入的了解，而这些技术本身就非常复杂。此外，系统层漏洞往往牵涉到多个组件和模块之间的交互，因此调试和定位问题的难度也更大。

缺乏可利用性信息：系统层漏洞通常没有公开的渗透测试平台或漏洞利用工具可供使用，因此白帽子需要自己编写相应的利用脚本和工具。这一点让所有的脚本小子都望而却步。

需要更多专业技能：系统层漏洞挖掘需要掌握较为专业的知识，如二进制分析、汇编语言、内存管理等。这些技能对于许多白帽子来说可能是新颖而陌生的。

不确定性更强：由于系统层漏洞往往会导致更严重的后果，如拒绝服务、代码执行等，因此系统层的攻击面也更加保护严密。在挖掘系统层漏洞时，白帽子需要更加小心谨慎，以免引起安全问题。

正因为难度更大、破坏力更强，所以挖到一个操作系统的漏洞，拿到的漏洞奖金往往更高，备受白帽子群体的追捧。在黑客圈早已扬名立万的主，谁手里还没拿过几个操作系统的 0day 了。

“那你是高阶白帽子吗？”笔者忍不住问 TheSky。

“咳咳，那你说呢？”TheSky 抛来了一个自信的眼神。

面向实战

在修炼好一定内功之后，CTF（夺旗赛）往往是白帽子们进入的第一个实训场，它是目前世界范围内最为流行的网络安全竞赛。

大致流程是，参赛团队之间通过进行攻防对抗、程序分析等形式，率先从主办方给出的比赛环境中得到一串具有一定格式的字符串或其他内容，并将其提交给主办方，拿到相关赛题的分数，这个过程被形象的称为“夺旗”，有点拔得头筹的味道。

BugMaker、Enjoy、Kamelo 他们都曾多次参加过各类 CTF 比赛，也拿过不低的名次，都认为 CTF 对提升技术和经验大有裨益。

但话又说回来，CTF 毕竟只是比赛，主办方会预先布置虚拟的网络环境，选手们面对的也只是一成不变的赛题。

白帽子本身就是要与黑产战斗的，更需要在真实的环境中反复锤炼。

就此而言，CTF 比不了与近些年开始普及的大型实网攻防演习，也就是在真实的网络环境中，组织攻防双方展开较量。

在 Kamelo 看来，大型实网攻防演习与 CTF 比赛相比，对白帽子的要求更加全面和综合。白帽子需要掌握更广泛的知识和技能，具备团队协作和安全意识，并能够快速适应不同的情况和任务。

比如如何利用欺骗、钓鱼等手段使目标上当中招，当利用漏洞渗透进入目标内网后，如何迅速获取目标系统内部更大的权限，如何隐藏自己入侵的痕迹不被防守方的安全设备检测到，这些都是平常很难学到的知识。

“第一次参加实网攻防演习时，其实我还是很有点紧张的。”Kamelo 说。虽然他以渗透技术见长，但却选择了更具挑战性的角色，以防守队的身份首次参加，这比当攻击队员更让人感到紧张，因为攻击渗透失败了大不了再来一次，但防守队根本猜不到对方会用什么样的攻击手法。

历经多次实战的 Kamelo 褪去了学生时期的稚嫩，并且早已成长为某家企业安全团队的攻防箭头，他对于白帽子也有了更深的理解。

据他讲，一名最优秀的白帽黑客应该具备以下技能。

精通计算机网络和操作系统：掌握计算机网络和操作系统的原理、结构及其内部运行机制，充分了解网络结构和服务的功能，以便更好地识别潜在安全风险。

深入了解各种安全工具和技术：拥有广泛的知识体系，熟悉各种安全工具和技术，并能够灵活应用这些工具和技术，以发现和利用安全漏洞。

具备编程和脚本语言技能：具备编写程序和脚本的能力，可以自动化测试和审计过程，提高效率和准确性。

良好的逆向工程技能：能够理解和修改二进制代码，深入了解软件内部的工作原理，从而发现软件中的漏洞。

出色的漏洞挖掘和利用技能：能够通过各种手段发现未知漏洞，并利用这些漏洞入侵目标系统。

良好的沟通能力和团队协作能力：与其他人员合作，配合渗透测试、修复和排除故障。

“那你对想要成为最厉害的黑客的新手白帽子，有什么建议吗？”笔者追问道。

Kamelo 捏了捏鼻子，思考了一下说：“其实也没有什么，你手上拿着的图谱就是一份非常有价值的指导性材料，这份图谱基于实际需求，针对不同阶段和领域的技能和知识进行了详细的分类和解释，可以为从业者提供清晰的职业发展路径和技能提升方向。”

就在笔者准备收拾收拾离开的时候，Kamelo 突然又蹦出了一句话：“别忘记守法是所有白帽子的底线，技术本不能用来作恶。”

> 最厉害的白帽子是什么样不知道，
> 但想要成为最厉害的白帽子，
> 唯有持之以恒的学习和千百次实战的锤炼。

对当前 5G 应用安全的 5 点认识

5G 网络取代传统网络，有利于推动新业态发展，有利于加强行业应用安全能力。但 5G 安全是一项长期工作，需要以“零事故”为目标，进一步增强面向行业应用的安全能力，解决 5G 替代面临的关键安全问题，护航 5G 应用发展。

5G 网络将催生一批新兴业态

5G 行业应用已广泛开展。5G 在行业应用具有先进性和不可替代性，将催生一批新兴业态的出现和发展。

在智能制造领域，随着产业结构的转变，传统的大批量生产方式正在向柔性生产转变。由于生产设备需要在一定范围内移动，且满足网络实时性、稳定性的要求，5G 是最为合适的生产网组网方式。5G 特有的网络切片可以使不同厂家的业务系统独立运行，避免相互干扰和安全隐患，有利于传统制造业转型和培育新业态。

在智慧医疗应用中，5G 网络推动远程医疗发展，将核心城市的高水平医疗能力通过网络远程投放。该应用需要开展远程影像传输、诊断和处置，乃至开展远程手术，对网络的可靠性、实时性、带宽和移动性都有较高的要求， 5G 是最适合的网络。

在车联网应用中，车路协同与自动驾驶离不开 5G 网络的支持。在车路协同情况下，采用 5G 网络能够实现低时延、高可靠、高速率和大连接的能力，实现车辆间位置、速度、行驶方向和行驶意图的沟通，更有利于道路智能设备辅助车辆对环境进行感知。

云手机、AR/VR、元宇宙等云终端应用需要 5G 网络支撑。在基础设施云化、应用服务化和保障数据安全等多重背景下，云终端应用得以快速发展。所有的数据应用均在云端，终端仅通过加密通道进行音视频展示和交互。为保障云终端应用的用户体验，需要高带宽和实时性，因此 5G 网络配合边缘计算将是最适合的基础条件。

> 5G 安全是一项长期工作，
> 需要以“零事故”为目标，
> 进一步增强面向行业应用的安全能力，
> 护航 5G 应用发展。

5G 取代传统网络有利于加强行业应用安全能力

从发展的角度看 5G 更安全，也更适合应用于重要行业。5G 网络是一个体系化、组织化的网络，其终端实名认证、物理位置易定位，信令面有管理控制权而黑客难以直接进入，与分散无序的互联网相比能够实现更强的安全管控能力，与行业专网相比有更快的技术迭代能力。

5G 比互联网更安全：互联网是无序的，无法定位威胁的源头。互联网上的黑客隐藏在虚拟网络中，很难定位其攻击的源头。而 5G 网络是垂直管理的有序网络，可以追溯到每一片区域，每一个基站，甚至每一台终端，快速定位攻击源头，切断攻击传播路径。

5G 比现有的专网更安全：现有的专网多是封闭体系，建成之后专网专用，技术迭代缓慢甚至停滞不前。封闭体系只能解决当前的问题，解决不了发展的问题，从而导致封闭体系最终一定会落后。因此传统专网在一定的时间和范围内可以保证高安全，但不可持续。而 5G 是更先进也更灵活的网络，其技术进步是不断迭代发展的，应用的范围广，承受的攻击更多，改进也更快。虽然暂时可能还存在一定的安全问题，但从发展的眼光看，其前景是光明的。

但 5G 应用于行业需要进一步增强安全能力

5G 安全特性的增强，使得 5G 网络具备内在的安全基础能力。相比之前的移动通信网络，5G 网络在安全性方面做了切实的加强：

> 5G 网络在安全性方面的加强，
> 使其能够更好地应对传统威胁，
> 从行业应用的角度看，
> 5G 网络仍面临严峻网络安全挑战。

- 5G 实现了更好的空口安全，进一步支持用户数据的完整性保护机制，防范用户数据的篡改攻击。
- 5G 加强了用户隐私保护，用户永久身份 SUPI 以加密形式发送。
- 5G 实现了更好的漫游安全，在传输层和应用层对运营商间的信令进行端到端安全保护。
- 5G 实现了密码算法增强，以应对越来越强大的算力破解。

5G 网络在安全性方面的加强使其能够更好地应对传统威胁，但 5G 应用于行业是一个新课题，从行业应用的角度看，5G 网络仍面临严峻网络安全挑战：

- 攻击暴露面扩大

原来封闭的生产网络、业务系统开始向外界打开。网络、应用、数据有了更多的暴露面，带来了新的安全风险。

- 数据泄露风险加剧

数据的开放、共享和持续流动加剧了信息数据的泄露风险。5G 独有的边缘计算技术，产生了大量终端侧数据，数据的实时吞吐量很大，不仅

5G 行业应用需要解决的关键安全问题主要包括 3 个方面：需要开展双向防护；实现 IT-CT-OT 网络一体化安全监测；实现增强的身份认证与访问控制。

增加了攻击点、扩大了攻击范围，还更容易被篡改和窃取。

• 个性化安全需求剧增：

5G 是面向应用而生的，和场景关联性极强，5G 时代下，新业务场景的安全需求千差万别，需要针对不同行业的差异化需求、不同的业务场景量身定做个性化的网络安全解决方案。

5G 行业应用需要解决的关键安全问题

5G 应用面临的网络安全问题是一个系统问题，涉及网络安全、终端安全、数据安全、业务安全等问题。通常应用行业和企业不仅部署 5G，而是多网融合的信息和业务系统，因此需要在行业整体网络安全体系框架下解决 5G 安全问题。当前 5G 行业应用需要解决的关键安全问题主要包括 3 个方面：

（1）行业使用 5G 网络需要开展双向防护

5G 行业应用带来的新型网络边界需要重点进行边界阿防护，区别于传统边界，应从运营商侧和行业侧开展双向防护。做到任务清晰、责任明确。运营商侧边界防护，重点防御来自企业网络的流量攻击，以流量解析、隔离、DDoS 防护为主，防止黑客控制行业业务对运营商大网的稳定运行造成破坏。行业侧边界防护，重点防御来自运营商网络的 APT 攻击，以漏洞利用、间谍软件、深度威胁为主。防止黑客通过运营商网络渗透进行业网络，进而破坏行业业务。

（2）实现 IT-CT-OT 网络一体化安全监测

从业务应用和网络角度来看，信息化办公网络（IT 网络）、数字化生产网络（OT 网络）和面向行业应用的移动通信网络（CT 网络）一体化已成为必然趋势。因此要增强 5G 行业应用安全监测能力，需要打破孤岛，实现 CT-IT-OT 网络一体化流量分析。通过对信令安全监测、IT 基础设施的安全监测、工业应用的安全监测，面向行业网络流量进行综合分析，加强网络威胁发现能力并实现实时告警。

（3）实现增强的身份认证与访问控制

5G 业务应用需要做二次认证。即 UE 设备向核心网认证，而 UE 的应用向业务系统认证。将二次认证进行统一，可以绑定设备与应用，并增强行为分析能力，构建用户、终端、网络、服务之间统一的信任体系。进一步可以通过零信任打通 IT 与 CT 认证机制。将 CT 入网和漫游认证信息作为基础环境安全要素，对于运行在可疑设备上的业务应用进行重点监

控。将 IT 持续认证和行为分析结果反馈给 CT 作为用户入网控制的决策依据。对运行危害网络安全应用的移动接入设备做断网、限流等处理。

5G 应用安全建设应以“零事故”为目标

在行业应用领域，5G 替代传统网络是一个长期过程。行业应用不同于个人消费，受国内外供需关系、产业规模、利润率等多方面因素影响，其生产设备、网络的更新迭代需要更长的周期。我国工业总体规模庞大，数字化率相对较低，在很多行业和领域替换 5G 网络暂时还不是刚需，这些因素都会影响 5G 替代的进程，也同时影响 5G 行业应用安全工作的推进。

着眼于当前形势和未来发展趋势，5G 行业应用安全当以“零事故”为目标实现联合作战、精准防护、深度运营，在保障不出现重大网络安全事故的前提下，统筹发展与安全，融合形成统一的安全架构，护航 5G 应用发展。

（1）联合作战

全流量检测 + 态势感知实现联合作战：建立全面监控能力，实现网络安全能力的高效协同。

通过全流量威胁检测全面监测网络安全异常行为，防止终端恶意接入，及时发现隔离失效、非法访问、越权管理等安全事件；结合网络基础设施运行状态，对网络安全态势做出评估，提供针对性的预防建议。通过一体化安全态势感知将 CT 侧的信令安全、IT 侧的边缘计算平台安全和 OT 侧的工业应用安全相结合，通过网络行为与业务应用行为的对比分析，精准定位威胁。

（2）精准防护

构建用户、终端、网络、服务之间统一的信任体系。

通过零信任将用户的身份信息、地理位置信息、行为操作、终端信息等，和业务访问有机结合起来，构建用户、终端、网络、服务之间统一的信任体系。开展持续进行信任评估，持续提供主体信任等级评估、资源安全等级评估及环境评估等评估数据，确保合适的人、在合适的时间、以合适的方式，访问合适的数据。

（3）深度运营

用合规检测实现深度运营。定期开展实战攻防演习和安全测试，及时发现问题解决问题。梳理识别 5G 网络中的安全资产，分析安全威胁风险，并借助专业的 5G 仿真工具进行攻防测试，检测 5G 接入网、核心网和各种类型的攻击行为，及时消除隐患，不断提升安全防御能力。



关于作者

乔思远

奇安信集团副总工程师、产业发展研究中心总经理、工业和信息化部 5G 应用安全创新示范中心奇安信分中心负责人。从事网络安全相关产业研究和前沿技术创新与应用研究。

美国切换国家网络防御系统大脑的背后

面对新的威胁格局，传统基于特征和情报比对的爱因斯坦计划已经无法应对。美国宣布推出 CDSA（网络分析和数据系统），实现数据驱动的后端安全分析，同时探索全新的前端检测技术栈。

从 NCPS 到 CADS

2023 年 3 月，拜登政府公布了 2024 财年的预算申请，包括 262 亿美元的网空预算。其中，联邦民事机构占 127 亿美元、国防部占 135 亿美元。在联邦民事机构的网空预算中，DHS 下属的 CISA 就占了 31 亿美元，其中 4.25 亿美元用于名为网络分析与数据系统（Cyber Analytics and Data System）的新计划。

根据 CISA 公布的部门详细预算，从 2024 财年开始，将启用一个全新计划——联合协作环境（JCE）——来支撑未来联邦民事机构的态势感知能力。

预算申请书提到，在 JCE 中，CISA 将在遗留的国家网空安全保护系统（NCPS）计划（即爱因斯坦计划）的基础上，为新的网络分析和数据系统（CADS）提供 4.25 亿美元，以增强 CISA 的内部分析系统能力并使 NCPS 现代化。在 CADS 计划之下，CISA 能够开发一个一流的分析环境，集中与任务相关的数据，依托更高程度的自动化，实现更高效的分析。

在受到多年的质疑之后，美国政府终于开启了新系统（CADS）来重塑之前饱受诟病的 NCPS。让我们看看这些质疑，以及 CADS 的由来：

（1）2016 年 1 月，GAO 的一份审计报告直指 NCPS 进度严重偏离预期，且收效不佳。报告认为 NCPS 检测能力存在缺陷，检测种类缺失，未知威胁检测能力太弱，在各大联邦政府机构的部署范围和程度层次不齐，用户反馈普遍不高等。核心点是无法识别未知威胁。

（2）2017 年 3 月，GAO 在给美国众议院国安委的书面证词中，再次指出了 NCPS 和 CDM 项目存在的诸多问题（包括不能识别未知威胁），并促使 CISA 全面重新评估 NCPS 项目。

（3）2018 年，美国国会研究服务处在一份报告中指出爱因斯坦存在一个关键限制因素，即必须“事先

在受到多年的质疑之后，
美国政府终于开启了新系统（CADS）
来重塑之前饱受诟病的 NCPS。

看到并分析过恶意流量才能起效，无法在首次接触新的恶意流量时进行识别”。换句话说，就是无法识别未知恶意流量（未知威胁）。

（4）2020 年的太阳风攻击事件使得美国联邦政府蒙受损失。事后，人们纷纷质疑耗资将达 72 亿美元的爱因斯坦系统为何没能及时识别攻击，成为促成 NCPS 真正开始变革的导火索。譬如 Bruce Schneier 就认为，美国政府过于关注进攻（进攻性策略引发反噬，使美国遭受了更多的攻击，放大了自身防御的薄弱），却在网络防御方面做的太少。“2018 年就指出来的缺陷，（至今）未能修复。”

（4）2021 年 3 月，CISA 代理局长 Brandon Wales 在参议院听证会上表示，“最好能保留爱因斯坦系统中仍能发挥作用、提供重要价值的部分，并把那些缺乏实际作用的部分替换成新项目。”

（5）2021 年 6 月，CISA 代理局长 Brandon Wales 在给参议员 Ron Wyden 的质询回信中写道：“随着越来越多使用加密流量进出联邦网络，十年前发起的（基于签名）的爱因斯坦 E2（网络检测）技术已经不能再提供 CISA 所需的可见性。”

（6）2023 年 3 月 3 日，DHS 的监察总长办公室发布了一份审查报告，评估了 EO14028 的落实情况，认为“CISA 需要显著改进网络可见性和威胁识别技术”，并“建议 CISA 下面的 CSD（网络安全部）对 NCPS 数据分析能力的组织、运行和维护做出并实施一项长期计划”。也正是在这个报告中，CISA 表示 CSD 下面具体负责 NCPS 的能力交付部提出了一项 CADS 计划。其中的一个重点就是把原 NCPS 中的数据分析做强。

在 DHS 发布预算后，DHS 的前高级官员 Chris Cummiskey 表示，这份预算案是对过去几年间围绕爱因斯坦系统未来走向这一重大问题做出的回应。“当时的想法是，爱因斯坦系统终将转化成其他形态。我想我们现在已经有了答案。”

> 新的 CADS 系统将帮助 CISA“在破坏性入侵发生之前，快速分析、关联并行动以解决网络安全威胁和漏洞”。

CISA 负责网络安全的执行助理主任 Eric Goldstein 在一封邮件声明中表示，新的 CADS 系统将帮助 CISA“在破坏性入侵发生之前，快速分析、关联并行动以解决网络安全威胁和漏洞”。

Goldstein 解释道，该系统将整合来自多个来源的数据，包括“公共与商业数据馈送；CISA 自己的端点检测与响应传感器、PDNS（保护性 DNS），以及覆盖美国数千家注册组织的漏洞扫描服务；还有公共和私营合作伙伴共享的数据”。

CADS 还将为 CISA 的网络分析师提供统一的数据仓库，其提供的工具和功能有助于数据的摄取、集成、协调和自动化分析，将支持对恶意网络活动的快速识别、检测、缓解和预防。

CADS 计划介绍

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。

我们知道，NCPS 有四大核心能力：入侵检测、入侵防御、安全分析和信息共享。

根据 CISA 的计划，NCPS 的一部分能力将迁移到 CADS，剩下的能力则作为遗留 NCPS，继续存在。其中，遗留的 NCPS 将继续保留入侵检测和入侵预防功能，主要包括爱因斯坦入侵检测和预防传感器套件。而 NCPS 的信息共享能力、安全分析能力，以及核心基础设施则将转移到新的 CADS 计划中，并将在“网络任务 IT 基础设施”“网络行动工具”和“网络使命工程”的支撑下运行和维护。

经此一变，在未来，如果我们还把美国联邦民事机构的态势感知系统称作爱因斯坦的话，那么，（遗留）NCPS 继续充当爱因斯坦的前端传感器，而新的 CADS 将充当爱因斯坦的后端大脑。在未来，CISA 一方面会继

Non Pay Cost Drivers
(Dollars in Thousands)

	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)**

表 1：CADS 和遗留 NCPS 运行支撑的非支付性预算

续对传感器进行全栈升级，另一方面则会着力发展态势感知大脑。

通常 CISA 将每个项目的预算分为运行支撑和采购建设两个部分。

从 CADS 和遗留 NCPS 运行支撑的非支付性预算可以看出，从 2024 财年开始，原来 NCPS 的开发与工程、核心基础设施、分析、信息共享预算已经清零，不再申请，并转移到 CADS 中，改称为“网络使命 IT 基础设施”“网络行动工具”“项目管理办公室”和“网络使命工程”。加上其他此表未列出的运行支撑预算，2024 财年为 CADS 申请的总运行支撑预算为 2.58 亿美元。另外，作为遗留 NCPS 组成的入侵检测和入侵防御预算则继续有新申请，其中入侵检测预算同比上一年还有所增加。

从新 CADS 的采购预算可以看到，采购建设的申请预算是 1.67 亿美元。这其中最关键的是“网络运行工具”。这里的工具其实就是指网络数据的摄取、管理、分析，以及信息共享工具。这正是整个爱因斯坦计划的大脑，现在把他从 NCPS 中独立出来单独作为 CADS，也足见其重要性。“网络任务 IT 基础设施”是承载爱因斯坦大脑的计算与网络支撑，“网络使命工程”是爱因斯坦大脑运行的各种服务、标准和最佳实践等工程性支撑。

新态势感知系统分析

坦率地讲，爱因斯坦无法检测未知威胁这个问题至今依然是业界的难题，并没有被很好的解决。人们一直寄希望于 AI 和 ML 驱动异常检测技术，但正如 CISA 代理局长 Brandon

(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**

表 2：新 CADS 的采购预算

Wales 在给参议员 Ron Wyden 的质询回信所说：“尽管爱因斯坦也部署了一些基于 AI 和 ML 的网络异常流量检测技术（譬如 LRA 和 NEST），也依然没能及时检测到 SolarWinds 攻击。”CISA 同时表示，使用非基于签名的检测技术的商业能力同样没有检测到 SolarWinds 对政府和私营部门的攻击。反而，基于签名和指标的检测技术有时候更加有效，前提是以最快的速度获得相关的签名和指标，而这就是威胁情报要干的。爱因斯坦计划为了将“情报 + 检测”运行起来也是煞费苦心，包括建立广泛的情报社区和快速分享机制，不断强化自身的威胁猎捕团队和能力，加大高级恶意软件分析能力的投入，还大力建设保护性域名服务（pDNS）。事实上，在攻击曝光后，CISA 获得了很多相关的 IoC，并且通过爱因斯坦 E1 识别出了一些可能失陷的联邦机构，尽管为时已晚，但还犹未为晚。

因此，CISA 认为，仅仅依靠网络侧的威胁检测是不够的，因而“紧急将其检测功能从互联网出口转移到机构网络中以更多关注端点安全……额外的 6.5 亿美元将使 CISA 能够迅速实现这一转变”。在 SolarWinds 事件的教训下，2021 年 5 月美国政府颁布总统行政命令 EO14028，其中要求在联邦民事机构中部署 EDR。也正是从这个时候开始，EDR 技术变成了网红。

再进一步研究，我们发现通过在态势感知前端部署基于情报（IoC & IoA）驱动的传感器，并增加对端点的遥测，再在后端大脑部署一张强大的情报网，凭此要想战胜未知威胁依然不够。基于 AI/ML 的未知威胁检测能力虽不成熟，但方向正确，急需强化。这就需要升级前端的网络遥测能力，并着力强化后端对遥测数据基于 AI/ML 和情报（TTP）的分析能力，包括编排自动化分析和“人在回路之上”的分析。

CISA 寄希望于后端大脑的升级版分析能力能够在实战化级别实现未知威胁的检出与响应。因此，CISA 将原 NCPS 的分析部分分拆出来，单独成一个计划——CADS（网络分析与数据系统）。对 CISA 而言，这里的数据也空前的扩大化，不仅是网络遥测数据，还包括端点遥测数据，CDM 的数据，威胁情报数据，漏洞数据，以及其他各种情境数据。而这里的分析也不仅是算法，也包括人驱动的威胁猎捕。

从前端检测能力来看，CISA 表示，尽管目标是要替换现有的前端检测技术栈，但 2024 财年在检测这块重点是探索和试点新技术。

从后端分析能力来看，这也正是 CADS 所要做的。尽管大家看不到新的美国国家级态势感知架构，但肯定首先是基于云的。其次，既然说他是一个 system of system，就必然是一个多体系统，其核心在于如何整合其他既有或者新建的特定任务系统，实现涌现效果。然后，在能力方面，攻击面、漏洞、威胁情报应用与分享、编排自动化，几乎肯定会囊括其中。

总结

CISA 在爱因斯坦的基础上推出了 CDSA（网络分析和数据系统），大力运用云、AI/ML、编排与自动化技术，实现数据驱动的后端安全分析，同时探索全新的前端检测技术栈。

仅从现有信息来看，笔者并未发现在态势感知能力建设方面 2024 财年相较于 2023 财年有太大的变化。这次提出 CADS，倒是没看出跟 NCPS 近些年一直在做的有多大实质性的不同，更多可能是因为 NCPS 的名声已经无法支撑 CISA 未来的发展愿景了吧。



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。



CTFWAR.ORG

网络安全的本质是攻防对抗
讲百遍不如打一遍

---习近平

CTFWAR介绍

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

攻防答题模式

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

积分等级体系

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

极牛技术社群

网络安全技术社群

Cyber Security Technology Community

PLATFORM

网络安全技术社群

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

技术

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

管理

专注在帮助网安工程师在职业发展中，建立体系化的管理知识和技术管理转型路径。

圈子

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

极牛技术站

以沙龙、峰会、圆桌论坛等深度学习的形式进行，满足知识获取与社交需求。

管理加油站

面向管理者的闭门活动，前瞻性的思维和观点，成熟的管理模式与领导模型。

极牛知识变现

通过帮助工程师打造个人品牌，从出书、录课、企培等形式帮助知识变现。

极牛训练营

面向社群成员的线下课程，技术架构、团队管理、商业模式、塑造个人品牌等。

极牛众星计划

社群中优秀的工程师将会被受邀签约极牛众星计划，平台辅助进行品牌孵化。

更多内容敬请期待

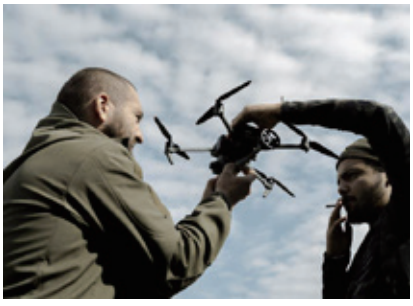
俄乌冲突：人工智能战争的试验场

编者按：前美国陆军网络司令部负责作战的副司令近日发文称，人工智能在俄乌战争各个领域得到应用，此场冲突已经成为人工智能技术的试验场，未来需要为将即将出现的新型“AI 战争”做好准备。

自俄乌战争以来，许多争论都集中在这场冲突是代表常规战争还是某种革命性的较量上。

《纽约客》2022 年 3 月的一篇文章将这场冲突描述为“第一次 TikTok 战争”。乌克兰数字化转型部长米哈伊洛·费多罗夫则称其为“技术战争”。数据分析公司 Palantir 的首席执行官亚历克斯·卡普表示，冲突中所用技术正在改变小国与大国的竞争优势。《华盛顿邮报》2022 年 12 月刊登了一篇内容是关于乌克兰和俄罗斯如何打“第一次全面无人机战争”的头版文章。





俄乌冲突正创造下一种战争形式

人们越来越多地谈论这场冲突如何加速全自动无人机和其他武器系统进入战场。人工智能在战争中的作用直接出现在此类评论中。无人机战争并不是直接的人工智能战争。乌克兰冲突在多大程度上具有人工智能的特征？中国创新工场首席执行官李开复，将人工智能武器系统称为继火药和核武器之后的“第三次战争革命”。这场革命是否正展现在我们眼前？乌克兰是否标志着战争性质的改变？答案是目前还没有。

俄乌冲突仍未改变战争的性质，但乌克兰是一个正在创造下一种战争形式的实验场。它不是一个边缘实验室，而是一个中心舞台，以微调、适

应和改进 AI 支持或 AI 增强的系统，从而可以立即部署。这一努力正在为未来的人工智能战争铺平道路。

这是一个预期的未来。在过去的几年里，人工智能战争的愿景比比皆是，并被贴上了不同的概念标签。美国退役海军陆战队四星上将约翰·艾伦和 SparkCognition 创始人阿米尔·侯赛因将其称为“超级战争”，这是一种人工智能控制的战争形式，几乎不涉及人类决策。前美国国防部副部长罗伯特·沃克和其他人将此称为“算法战”，在这类战争中，自主系统和武器会根据自己所处的情况独立开始选择行动方案。



美国国防高级研究计划局（DARPA）提出了“马赛克战”，这是一个更具战术性的术语，它将常规平台与无人驾驶系统相结合，以获得战场优势。

最近，美国中央情报局首席技术官南德·穆尔坎达尼和退役美国空军中将杰克·沙纳汉（联合人工智能中心首任主任）创造了“软件定义的战争”一词，软件将成为下一代作战系统所需的防御体系结构的关键部分。

所有这些概念的共同点是真正网络化战场的愿景，其中数据以光速移动，不仅将传感器与射手连接起来，而且还将所有部署的部队和平台连接起来。之所以设想这种未来情景，部分原因是技术发展日新月异，但也因为担忧地缘政治竞争及实力接近的竞争对手可能在不久的将来部署。

> 在过去的几年里，
> 人工智能战争的愿景比比皆是，
> 并被贴上了不同的概念标签。

俄乌冲突成人工智能前所未有的试验场

俄乌战争不符合这些未来情景。然而，这场冲突显然使这些未来主义的战争愿景更接近现实。这场冲突是人工智能前所未有的试验场。在一些领域，它的用途已经很明确了。例如，双方现在无处不在地使用无人机和巡航弹药，在飞行、瞄准和射击方面提供了人工智能增强的自主能力。游荡弹药（又称为神风敢死队、自杀式无人机或智能导弹）的使用受到了国际媒体的广泛关注，无论是作为重新定义战术战争未来的资产，还是作为道德和法律问题。

俄乌战争使用的无人机包括军用级无人机和商用无人机，例如，中国制造的大疆 Mavic 系列，这些无人机既廉价又易获得。

除航空系统外，自主舰船、用于



人工智能的重要用途是在网络战中，
尤其是在支持防御能力方面。
微软公司的报告表明，
乌克兰网络防御已被证明相对成功，
部分原因是人工智能增强威胁情报的进步。

扫雷的水下无人机和无人驾驶的地面车辆也得到部署。一些分析人士认为，在 2022 年 10 月对俄罗斯黑海舰队马卡洛夫海军上将号巡防舰的袭击中，联合使用空中和海上无人机可能是一种新型战争。

一般来说，人工智能大量用于将目标和物体识别与卫星图像集成的系统。事实上，人工智能在乌克兰战争中最广泛的应用是地理空间情报。AI 用于分析卫星图像，还用于地理定位和分析开源数据，如地缘政治敏感地点的社交媒体照片。例如，神经网络用于结合地面照片、无人机视频片段和卫星图像，以独特的方式增强情报，从而产生战略和战术情报优势。

这预示着在战场上招募 AI 进行数据分析的更广泛趋势。人工智能在俄乌冲突中越来越多地被结构性地用于分析大量数据，以生成有关冲突各方战略和战术的战场情报。这一趋势因其他发展的融合而得到加强，包括近地轨道卫星的可用性不断提高，以及来自开源的大数据前所未有的可用性。

此外，随着机器学习模型和系统的准确性不断提高，以及人工智能系统集成和交叉引用来自各种来源的数据的能力不断增强，人工智能本身也经历了巨大的技术改进。

俄乌冲突的独特之处在于，外国地理空间情报公司前所未有地愿意通过使用人工智能增强系统将卫星图像转化为情报、监视和侦察优势来协助乌克兰。美国公司在这方面发挥了主导作用。例如，Palantir Technologies 公司提供了其人工智能软件来分析战争的进展情况、了解部队调动和



进行战场损失评估。Planet Labs、BlackSky Technology 和 Maxar Technologies 等其他公司也在不断制作有关冲突的卫星图像。根据乌克兰的要求，其中一些数据几乎立即与乌克兰政府和国防军共享。

俄乌战争也可以被认为是第一次大规模使用人工智能增强面部识别软件的冲突。2022 年 3 月，乌克兰国防部开始使用美国公司 Clearview AI 生产的面部识别软件。这使得乌克兰能够识别死亡士兵，同时揭露俄罗斯袭击者并打击错误信息。

更重要的是，人工智能在电子战和加密方面发挥着重要作用。例如，美国公司 Primer 已部署其人工智能工具来分析未加密的俄罗斯无线电通信。这说明了人工智能系统正不断地重新训练和调整。

人工智能的重要用途是在网络战中，尤其是在支持防御能力方面。微软公司 2022 年 6 月份的一份报告表明，网络防御可能已被证明相对成功，部分原因是人工智能增强威胁情报的进步，以及保护软件向云服务和其他计算机网络的快速分发。

不利的一面是围绕冲突更明显地使用人工智能：错误信息的传播和作为信息战的一部分使用“深度造假”技术。例如，人工智能已被用于作为宣传活动使用的虚假社交媒体账户创建面部图像。虽然虚假信息的传播并不新鲜，但人工智能为扩大和发动此类活动提供了前所未有的机会，尤其是与社交媒体平台广泛结合。

同样，随着使用推荐算法以针对用户推送直接内容的使用越来越多，并且可以自主创建和传播消息的人工智能系统变得越来越复杂，出现了融合趋势。这是未来网络战的完美风暴，以 AI 为中心。



这些例子说明，俄乌冲突成为人工智能技术的试验场。当然，也有限制。各国正在测试现代人工智能增强系统，但仍不愿向乌克兰提供其最新和最先进系统的访问权限，部分原因是担心这些系统可能最终旁落。

为未来 AI 战争做好准备

作为一个人工智能实验场，这场冲突是独一无二的：前所未有的资金、国际参与和来自公共和私营部门的技术支持，可能会持续数年。冲突的持续时间使企业能够随时随地微调、调整和改进其人工智能系统。这就是人工智能增强型武器和系统与传统武器和系统明显不同的地方：它们部署的时间越长，可以收集的数据就越多，可以直接改进它们。这场冲突是通往网络化战场和未来人工智能战争的重要垫脚石。

关于 AI 增强型武器系统的媒体头条报道只是冰山一角。大多数人工智能已经并将部署在远离战场的系统中，如与规划、后勤和预防性维护等领域相关的云计算和数据分析系统中。这是人工智能驱动的战争革命的一个被隐藏领域，现在已经启动并且不会停止。

俄乌战争的性质可能尚未由 AI 决定，但此场战争类似于一个实验室环境，许多公司和政府能够在其中不断地训练和测试 AI 系统的各种能力、功能和应用。人工智能系统正在接受来自真实战场的真实数据的训练，不是为了停止苦难和结束战争，而是为了更有效地应对下一场战争：AI 战争。



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。

KnowBe4：百亿市值背后的安全意识生意

在美国网络安全行业有一家看似另类的独角兽公司：十余年专注于安全意识赛道，累计服务全球 5 .7 万多家客户，帮助企业有效解决“人”的安全风险问题。

这家名为 KnowBe4 的公司，号称全球最大的安全意识培训及钓鱼模拟演练平台提供商。它不是一家传统意义上的安全培训公司，而是将自己定义为一家领先的安全软件公司。KnowBe4 究竟如何在安全意识领域这一利基市场探索和领跑，发展成为全球唯一一家安全意识上市公司呢?

消除安全链条中最薄弱的一环

网络安全圈一直流传着关于“人的风险”的经典语句：“人是网络安全链条中最薄弱的一环”“网络安全中人的漏洞是最难修补的”“人是组织最宝贵的资产，也是最不可控的安全风险”等。

国外权威研究也支撑着这样的观点。“95% 的网络安全事件追根溯源是人为因素造成的”（世界经济论坛），“90% 的网络攻击始于一封钓鱼邮件”（波耐蒙研究所），“82% 的数据泄露事件与人为错误有关”（Verizon《数据泄露调查报告》）。

知名安全媒体 CSO Online 的一项调查显示，“企业平均部署了 75 款来自不同安全厂商的安全工具以期保障网络安全”。然而，任何企业，无论规模大小，无论买了多少安全产品，以“人”为目标的社会工程学攻击总是可以成功突破企业的安全防线。即便是当今全球市值最高的网络安全公司 CrowdStrike，其安全解决方案在应对社工攻击方面也是束手无策。既然人是黑客攻击的最佳突破口，是最大的攻击面，反过来，人也可以成为黑客攻击最难啃的一块骨头。



图 1 KnowBe4 首席黑客官数字创始人

> 任何企业，无论规模大小，
> 无论买了多少安全产品，
> 以“人”为目标的社会工程学攻击
> 总是可以成功突破企业的安全防线。

成立于 2010 年的 KnowBe4，借助其产品套件的创新安全意识培训方

法，可以提高人员对潜在威胁的认识，将最广大的员工群体的大脑武装起来，将“最薄弱的一环”打造为“最坚固的防线”，从而预防和阻止“以人为中心”的网络攻击，这是一种“尊重员工、赋能员工、依靠员工，将员工视为一道防线”的安全策略。

值得一提的是，很多产品是在其首席黑客官、前白帽黑客凯文 · 米特尼克 (Kevin Mitnick) 的帮助下设计的。米特尼克将其 30 多年的传奇黑客经验，转化为面向普通人的经典安全意识培训课程，教育人们如何有效防范社会工程学攻击。

灵活订阅模式与内容为王

与传统的线下安全意识培训不同，KnowBe4 实现了安全意识产品的标准化、上云化与订阅制。KnowBe4 的主要产品是其 SaaS 化的安全意识培训与钓鱼模拟集成平台。SaaS 产品既可供缺少 IT 部门和学习平台与钓鱼平台的中小型企业使用，同时也可扩展到业务运营遍布世界各地、拥有数十万员工的大型集团企业。

与传统的线下安全意识培训不同，KnowBe4 实现了安全意识产品的标准化、上云化与订阅制。

SaaS 化的安全意识产品能以较低的成本，帮助企业和员工树立安全意识，从而可以更加灵活地开展安全意识培训；同时集成的模拟钓鱼测试，可以确保培训效果可验证，从而显著降低人为错误造成的安全问题。

凭借业内最大的全职内容开发与设计团队，再加上不断收购的安全意识厂商、内容制作工作室，KnowBe4 在安全意识教育内容方面一直保持着绝对的领先地位。KnowBe4 拥有全球最大的安全意识教育资源库及钓鱼模拟演练邮件模板库。截至 2023 年 3 月，其资源库提供了超过 1300 多个原创的培训材料，素材类型包括图文海报、电子通信、互动课件、动漫视频、真人短剧、测评测试、安全游戏等，以不同的教育风格提供丰富的主题内容学习，包括一般性、随机性和有针对性的安全意识主题。且资源库每月不断更新，保持内容始终新鲜，支持 40 多种不同语言，不同级别的订阅客户可以访问不同的学习内容。其钓鱼演练平台提供了超过 20,000 个邮件模板，模板根据识别难易程度、员工岗位角色、知名品牌模仿、企业或行业定制等进行分类分级，目标是不断提升企业员工识别真实钓鱼邮件的能力，最大限度地减少钓鱼邮件的持续威胁。

作为产品战略和愿景的一部分，KnowBe4 每个月都会更新一些小的新功能，每个季度至少发布一个主要的特性功能或增强功能，最近两年不断地探索将人工智能、机器学习与安全意识教育相结合。

KnowBe4 引人注目的产品之一是由英国子公司 Twist & Shout 制作的“奈飞风格”网络安全剧集 The Inside Man 。该剧采用技术惊悚片的形式讲述网络安全故事。罪犯 Mark

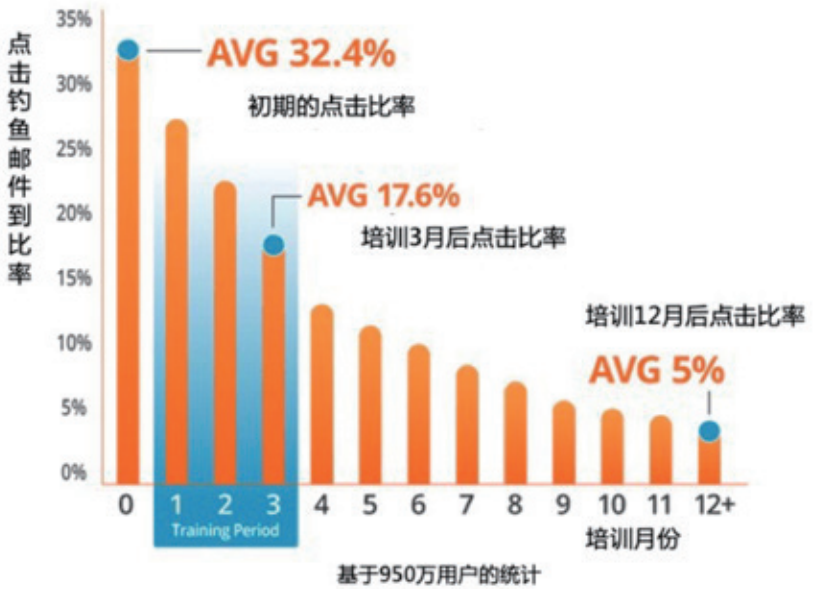


表 1　安全意识培训显著降低人为错误

Shepherd 和他的安全顾问组成的乌合之众团队，他们在挫败网络攻击的同时，就社会工程、密码卫生、社交媒体安全等主题提供可操作的课程。

在 KnowBe4 众多的技术创新中，最具特色的两个安全意识产品是 PhishER 和 SecurityCoach。

PhishER 是一款轻量级的安全编排和自动化响应 (SOAR) 平台，用于编排邮件威胁响应并管理员工上报的大量疑似恶意邮件。PhishER 在无需人工交互的情况下自动确定优先级排序，帮助企业安全团队消除邮件安全警告中的“信息噪音”，以便更快地应对最危险的邮件威胁。

SecurityCoach 是一款行为风险检测与响应 (HDR) 平台，通过将安全意识平台与传统的安全技术平台，例如，端点保护平台 (EPP)、邮件安全网关（ESG）、数据丢失防护 (DLP)、上网行为管理(IBM)、威胁情报平台 (TIP) 等形成联动，以“数据驱动”的方式来量化员工行为风险，并针对风险行为进行实时提醒和辅导，第一时间纠正和干预风险行为，从而显著提升安全意识培训的有效性，帮助企业安全团队进一步保护最大的攻击面——员工。

私有化的背后

自成立以来，KnowBe4 一直聚焦于中小型企业客户群（定义为员工少于 1000 人的组织），因为中小型企业越来越成为网络犯罪的攻击目标，它们比大型企业更容易被渗透。

根据其公布的 2022 年 Q4 财报数据显示，KnowBe4 服务的客户总数近 57,000 家，已经成为全球最大的安全意识培训和模拟网络钓鱼平台的提供商。尽管 KnowBe4 在安全意识领域也面临 Proofpoint、Infosec 等企业的竞争，但还没有一家公司的规模发展到被 KnowBe4 视为实质性竞争对手的地步。

业务蒸蒸日上的 KnowBe4 在上市仅一年半后欣然接受私募巨头 Vista equity Partners 的私有化。

KnowBe4 退市，并不代表退出安全意识市场。此次收购是网络安全行业安全意识创业成功的经典案例，对专注于安全意识领域的创业公司来说是值得鼓舞的一件好事，对于 KnowBe4 来说开启了一个新的发展篇章。

可以想象的是，Vista 这一操作背后酝酿着下一盘更大的棋。正如 KnowBe4 创始人兼首席执行官 Stu 在新闻稿中指出：“在完成私有化后，我们将获得 Vista 提供的额外资源和支持，这将帮助我们实现业务目标，并为客户提供更高的价值。”

作为安全意识赛道的长期主义者，KnowBe4 综合实力强、具有全球竞争力，相信其领导者地位短期不会动摇，并将在资金与资源双重加持下持续进化。期待 KnowBe4 未来在股市上“王者归来”，为安全市场带来更多惊艳。

告别唯技术论

从帮助企业提升员工安全意识，到改变员工风险行为，再到打造组织网络安全文化，是 KnowBe4 赢得用户认可和市场的底层逻辑。

“人的因素”仍是网络安全中最重要的方面。不论是满足合规，还是降低风险，员工安全意识教育与组织安全文化建设是高质量企业网络安全管理的“必修课”，是更广泛的企业网络安全治理生态系统中不可或缺的组成部分。

据市场研究机构 Global Market Estimates 预测，到 2027 年全球网络安全意识培训市场规模将达到 121.4 亿美元，2022 年 ~2027 年预期年均复合增长率 (CAGR) 为 45.6%。从调研数据来看，亚太区无疑是遭受网络攻击最多的地区之一，也就说，亚太区是互联网用户安全意识最为薄弱、对社工攻击最缺乏“免疫力”的地区之一。

在我国，网络安全意识、数字安全素养，在网络安全顶层设计和总体布局中是一个经常提及、却未被深入关注和深度理解的细分安全领域。从国内网络安全行业历史来看，安全意识培训或安全意识服务几乎一直是非主流，处于尴尬的“鸡肋”地位。

网络安全建设中，早日摆脱唯技术论，将网络安全意识培训，以及网络安全文化建设提到其应有的高度，是我们在应对网络威胁中必须要补的一课。这可以从国内何时出现 KnowBe4 规模的安全意识企业来进行验证。



关于作者

谢超首

易念科技首席专家，CEAC 网安意识工作组副组长

华云信安

以人才梯队为依托，以自主创新为核心，深耕网络空间安全产业

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

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

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

网络犯罪研究中心

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

极牛攻防实验室

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

涉网犯罪对抗　护网重保服务　安全咨询服务　安全保障服务　安全培训服务

丰富的解决方案

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

专业的团队服务

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

众多的行业案例

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

深入的厂商合作

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

全国范围的服务

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

公众号 小程序 官网

网安观察

没有网络安全就没有国家安全



7436084028