内部资料 免费交流

出版物准印证号：内资准印证 京内资准字 2124-L0058 号

SECURITY INSIDER

网安26号院

奇安信网络安全通讯

微软“蓝屏事件”深度复盘

P13

- 全球数千航班取消
- 多国银行服务中断
- 政府、医疗业务受到影响

第44期

2024 年 8 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。

别忘了墨菲定律：可能出错的事都会出错

一次简单的配置文件更新让数百万台 Windows 系统瘫痪。CrowdStrike 引发的大面积 IT 故障，肯定会在人类重大技术故障史占据重要地位。

这次事件的灾难后果是令人震惊的——全球数千架航班被取消，大量医疗和银行服务中断。这再次提醒我们，智能融合时代的数字基础设施是多么脆弱，单点故障就会带来大面积的灾难后果。

但值得警惕的是，软件企业匆忙发布更新，并将其直接推送到全球环境已成为主流，这意味着任何软件供应商都可能再次制造此类混乱。

我们分析一下导致这次故障的一系列责任方。

首先，微软把责任推给了网络安全公司 CrowdStrike，但微软应承担一部分责任。长期以来，全球用户把 IT 鸡蛋放在微软 Windows 篮子里。篮子被打翻导致鸡飞蛋打的后果难以避免。CrowdStrike 用户少，中国 Windows 用户受影响较小，但这不是我们庆幸的理由。一方面推动国产操作系统的 Windows 替代，可以避免鸡蛋都放在“微软 Windows 篮子里”的风险，但少数本土操作系统软件主导同样会面临可靠性挑战。毕竟国产化仅仅实现了可控目标，而非安全与可靠的保障。

其次，CrowdStrike 是此次故障的罪魁祸首，凸显出网络安全公司在速度和质量间的艰难平衡。作为以技术卓越和速度而闻名的企业， CrowdStrike 深受用户信任，但很少人会想到，本来用以避免混乱的安全公司会成为史上最大 IT 故障的肇事者。

安全形势瞬息万变，安全企业每天都会发布更新。CrowdStrike 可能为保持敏捷性而牺牲了一些步骤，或者对风险评估松懈了。部署任何更新前，都应进行彻底测试，尤其是在软件对关键系统组件具有最高程度的访问权限时。未在临时或测试环境中进行充分测试，就把更新部署到生产环境，无疑会制造灾难性后果。对于 CrowdStrike 这样规模的企业来说，这种根本性错误是不可原谅的。

网络安全从业者应警醒：在保护用户免受威胁时，不应忽视自身可能造成的风险。较高的开发质量、严格的测试、应对故障的安全机制和适度的谦逊必不可少。对政企用户来说，在选择安全供应商时，也应将具有较高开发质量保障和是否有充分测试作为重要标准之一。

CrowdStrike 制造的系统故障，可以被视为墨菲定律的典型实例——任何可能出错的事情最终都会出错。对微软蓝屏事件的教训，我们需要进行深入总结。毕竟，网络安全的下一个重大威胁可能只是一次更新。

总编辑

李建平

2024 年 8 月 1 日

CONTENTS 目录

安全态势

月度专题

微软“蓝屏事件”深度复盘 P13

——几行代码引发的全球性混乱

只需要几行代码，就让全球数百万台计算机死机，引发全面的社会混乱。这种只在科幻电影中出现的场景，真实发生了。

7 月 19 日凌晨 4 点，网络安全巨头 CrowdStrike 向其 Falcon 产品发送例行的内容配置更新。

随后，一场严重程度和规模都空前的全球 IT 系统故障爆发，全球 850 万台 Microsoft 设备受到影响，全球的重要航空公司、医院、银行、医疗机构、政府等机构随之出现业务中断，引发了巨大的混乱。事件影响超过了之前所有的黑客攻击和系统故障，成为有史以来最大的网络事件。

《网安 26 号院》编辑部
主办　奇安信集团

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

奇安信集团　虎符智库　安全内参

索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

索阅邮箱：26hao@qianxin.com
地　　址：北京市西城区西直门外南路 26 院 1 号
邮　　编：100044
联系电话：（010）13701388557
出版物准印证号：内资准印证 京内资准 2124-L0058 号
编印单位：奇安信科技集团股份有限公司
发送对象：奇安信集团内部人员
印刷数量：4500 本
印刷单位：北京博海升彩色印刷有限公司
印刷日期：2024 年 8 月 26 日

政策篇

国内，各行各业深化部署网络安全。就智能网联汽车安全，工信部、自然资源部均发布文件规制，国家发改委就《电力监控系统安全防护规定》修订版公开征求意见，财政部修订印发《会计信息化工作规范》强化会计信息化安全；

国际上，全球首部全面监管人工智能的法规，欧盟《人工智能法案》正式生效。该法案将不同人工智能系统可造成的风险分为四类，风险等级越高，管控越严格。

国内

财政部修订印发《会计信息化工作规范》《会计软件基本功能和服务规范》

8月7日，财政部修订印发了《会计信息化工作规范》及《会计软件基本功能和服务规范》，自2025年1月1日起施行。《会计信息化工作规范》共6章50条，与原规范相比强化了会计信息化安全，全面要求单位统筹考虑会计信息化的系统安全、网络安全、涉密安全、跨境安全等，强化会计数据在生成、传输、存储等环节的安全风险防范。《会计软件基本功能和服务规范》共8章47条，与原规范相比加强了会计软件及服务对会计数据的多维度保障，要求会计软件应当保证会计数据的真实、完整、安全传输，能够完整接收和读取电子凭证，并通过验签等方式检查电子凭证的合法性和真实性，应当满足数据保密性的要求，支持对重要敏感数据的加密存储和传输，保障会计数据不被篡改。

《网络安全标准实践指南—互联网平台停服数据处理安全要求》公开征求意见

8月7日，全国网络安全标准化技术委员会秘书处组织编制了《网络安全标准实践指南—互联网平台停服数据处理安全要求（征求意见稿）》，现公开征求意见。该文件提出了互联网平台停服数据处理基本要求，规定了重要数据处理的要求，适用于指导互联网平台数据处理者开展数据安全保护工作，也可为主管监管部门实施安全监管或安全评估提供参考。

三部门印发《加快构建新型电力系统行动方案（2024—2027年）》

8月6日，国家发展改革委、国家能源局、国家数据局制定并公布了《加快构建新型电力系统行动方案（2024—2027年）》。该文件多处涉及安全，包括优化加强电网主网架，保障电力安全稳定供应和新能源高质量发展；推进构网型技术应用，提升系统安全稳定运行水平；制定修订一批配电网标准，推动构建系统完备、科学规范、安全可靠的配电网标准体系；建设一批虚拟电厂，完善虚拟电厂的市场准入、安全运行标准和交易规则等。

《标识密码认证系统密码及其相关安全技术要求》等两项国家标准公开征求意见

8月2日，全国网络安全标准化技术委员会归口的国家标准《网络安全技术 标识密码认证系统密码及其相关安全技术要求》和《数据安全技术 数据接口安全风险监测方法》现已形成标准征求意见稿，现公开征求意见。其中，前者规定了标识密码认证系统的系统组成架构，及其密钥生成、管理及公开参数查询等服务的技术要求，适用于标识密码认证系统的设计、开发、使用和检测。后者给出了数据接口安全风险监测的方法，包括方式、内容、流程等，明确了数据接口

安全风险监测各阶段的监测要点，适用于指导各类组织开展的数据接口安全风险监测活动。

两部门《关于进一步加强智能网联汽车准入、召回及软件在线升级管理的通知》公开征求意见

8 月 1 日，工业和信息化部装备工业一司联合市场监管总局质量发展局组织编制了《关于进一步加强智能网联汽车准入、召回及软件在线升级管理的通知（征求意见稿）》，现公开征求意见。该文件正文共 4 章 10 条，包括总体要求、加强组合驾驶辅助准入与召回管理、强化汽车软件在线升级协同管理、保障措施。该文件要求，企业要落实智能网联汽车产品质量和生产一致性、产品安全主体责任，持续确保汽车数据安全、网络安全、OTA 升级、功能安全和预期功能安全等保障能力有效，严格履行 OTA 升级管理和备案承诺，以及事件、事故报告要求。

自然资源部印发《关于加强智能网联汽车有关测绘地理信息安全管理的通知》

7 月 26 日，自然资源部印发《关于加强智能网联汽车有关测绘地理信息安全管理的通知》。该文件共 10 条，包括依法开展智能网联汽车相关测绘活动，加强智能网联汽车涉测绘行为管理，严格涉密、敏感地理信息数据管理，从严审核把关导航电子地图，落实地理信息数据存储和出境要求，强化地理信息安全监管，鼓励地理信息安全应用探索，优化地理信息公共服务，营造安全发展的良好氛围，强化工作落实。

《中国人民银行关于进一步加强征信信息安全管理的通知》修订版公开征求意见

7 月 26 日，中国人民银行拟对《中国人民银行关于进一步加强征信信息安全管理的通知》部分条款进行修改，起草了《修改＜中国人民银行关于进一步加强征信信息安全管理的通知＞有关公告（征求意见稿）》，现公开征求意见。该文件要求加强征信信息查询管理，人工查询实现查审分离，自动查询要严格设置规则、专人管理，查得的数据要按照高敏感型数据进行全流程安全管理。该文件提出，建立征信信息安全监管走访机制，根据监管走访情况由运行或接入机构调整其用户管理权限。

两部门《国家网络身份认证公共服务管理办法》公开征求意见

7 月 26 日，公安部、国家互联网信息办公室起草了《国家网络身份认证公共服务管理办法（征求意见稿）》，现向社会公开征求意见。该文件共 16 条，主要包括四个方面的内容：一是明确了国家网络身份认证公共服务和“网号”“网证”等概念；二是明确了公共服务的使用方式和场景；三是强调了公共服务平台和互联网平台的数据和个人信息保护义务；四是明确了公共服务平台和互联网平台违反数据和个人信息保护义务的法律责任。该文件提出，对自愿选择使用“网号”“网证”的用户，除法律法规有特殊规定或者用户同意外，互联网平台不得要求用户另行提供明文身份信息，最大限度减少互联网平台以落实“实名制”为由，超范围采集、留存公民个人信息。

国家发改委《电力监控系统安全防护规定》公开征求意见

7 月 25 日，国家发展改革委组织修订了《电力监控系统安全防护规定》（发改委 2014 年第 14 号令），形成《电力监控系统安全防护规定（公开征求意见稿）》，现向社会公开征求意见。该文件共 6 章 38 条，包括总则、安全技术、安全管理、应急措施、监督管理、附则。该文件提出，电力监控系统安全防护应坚持“安全分区、网络专用、横向隔离、纵向认证”结构安全原则，强化安全免疫、态势感知、动态评估和备用应急措施。该文件细化了安全分区保护粒度，强化了安全接入区设置及防护要求，补充了业务横纵向交互、设备选型、安全加固、态势感知等技术要求，以及应急备用等管理措施。该文件首次提出电力监控系统专用安全产品目

录及技术规范，以强化供应链管理。

李强签署国务院令，公布修订版《中华人民共和国保守国家秘密法实施条例》

7 月 22 日，国务院总理李强日前签署国务院令，公布修订后的《中华人民共和国保守国家秘密法实施条例》，自 2024 年 9 月 1 日起施行。该文件共 6 章 74 条，包括总则、国家秘密的范围和密级、保密制度、监督管理、法律责任、附则。该文件要求，县级以上人民政府应当加强保密基础设施建设和关键保密科学技术产品的配备。该文件提出，涉密信息系统按照涉密程度分为绝密级、机密级、秘密级，机关、单位应当按照国家保密规定，对绝密级信息系统每年至少开展一次安全保密风险评估，对机密级及以下信息系统每两年至少开展一次安全保密风险评估，涉密信息系统中使用的信息设备应当安全可靠，以无线方式接入涉密信息系统的，应当符合国家保密和密码管理规定、标准。

国际

《联合国打击网络犯罪公约》顺利通过

8 月 9 日，联合国打击网络犯罪公约特委会一致投票通过了《联合国打击网络犯罪（使用信息和通信技术系统实施的犯罪）公约》。该文件系网络领域首个由联合国主持制定的普遍性国际公约，将在全球范围内为打击网络犯罪国际合作提供法律框架，对网络空间国际法发展也有重大意义。该文件规定，在调查任何根据国家法律可判处至少四年监禁的犯罪时，成员国可以向其他国家当局要求提供与该犯罪相关的任何电子证据，也可以向互联网服务提供商索取数据。

欧盟《人工智能法案》正式生效

8 月 1 日，欧盟《人工智能法案》于今日正式生效。该法案是全球首部全面监管人工智能的法规。欧盟介绍，制定《人工智能法案》的目的，在于在维护民主、人权和法治的同时，推动普及值得信赖的人工智能。根据使用方法而非技术本身造成的影响风险进行分类。风险分为四类，风险等级越高，管控越严格。其中，风险最高的情况包括：为唆使犯罪而利用人工智能技术操纵人的潜意识；使用高级监控摄像机等，将人脸识别等生物识别技术实时应用于犯罪搜查等。这些情况是被“禁止”的。第二高风险的情况包括：基于犯罪心理画像的犯罪预测、在入学考试和录用考试测评中应用人工智能。人类有义务保存和管理使用人工智能技术的历史记录。许多国家和地区正在制定人工智能管制规则，欧盟新规则可能为后来者提供重要借鉴。

美国白宫发布《联邦风险和授权管理计划现代化》备忘录

7 月 25 日，美国白宫管理和预算办公室（OMB）发布《联邦风险和授权管理计划（FedRAMP）现代化》备忘录（M-24-15），以应对云市场变化和各机构对多样化任务交付的需求，推动联邦政府加速安全采用云服务。FedRAMP 是美国联邦机构采用云服务必须遵守的安全合规项目。该备忘录从多个方面加强 FedRAMP，从而改革云安全授权计划。包括规定 FedRAMP 需实现“严格审查”功能，并要求云服务提供商（CSPs）快速缓解任何安全架构中的弱点，以保护联邦机构免受最“突出的威胁”。应建立自动化流程，用于输入、使用并重用安全评估和审查，以减少参与者的负担，并加快云解决方案的实施进度等。

美国海军陆战队发布新版《人工智能战略》

7 月 10 日，美国海军陆战队发布《人工智能战略》，将指导其整合人工智能技术工作。该战略提出改善海军陆战队态势的五个关键目标，包括全面了解可由人工智能提供解决方案的特定任务问题；提高部队各级人员在建立、支持和维护人工智能系统及相关技术方面的专业技能；改善基础设施并制定和发布标准；建立人工智能政策、管理和沟通渠道；加强与国防部其他部门、国际盟友、工业界和学术界合作等。该文件是海军陆战队推进数字现代化的重要里程碑。

事件篇

7 月 19 日中午开始，网络安全厂商 CrowdStrike 的问题更新，导致全球 Windows 大面积蓝屏死机，致使航班停飞、火车晚点、银行异常、巴黎奥运服务受影响等，全球至少二十多个国家受到波及。据悉，此次事故导致全球近千万台 Windows 蓝屏死机，超过了 2017 年永恒之蓝勒索病毒事件的影响。

特朗普竞选团队在大选期间被黑，部分敏感数据外泄

8 月 10 日 Politico 消息，美国前总统唐纳德 · 特朗普的竞选团队日前确认，其部分内部通信资料已被黑客获取。特朗普竞选团队引用微软 8 月 9 日发布的一份报告的说法，将此归咎于“对美国怀有敌意的外国势力”。该报告称，伊朗黑客“在 2024 年 6 月向一名美国总统竞选的高级官员发送了一封鱼叉式网络钓鱼邮件，成功入侵其邮箱账号。”微软并未确认邮件针对的是哪一家竞选团队，也拒绝发表评论。此前，多家知名媒体收到来自一个匿名账号发送的电子邮件，其中包含了特朗普竞选团队内部的文件。

巴黎奥运会比赛场馆遭勒索软件攻击

8 月 6 日 Politico 消息，巴黎检察官办公室披露，法国国家博物院网络的 IT 系统上周日遭到勒索软件攻击。该网络内共有约 40 个博物馆，其中包括被改造为巴黎奥运会击剑和跆拳道比赛场馆的巴黎大皇宫。巴黎检察官办公室表示，奥运赛事未受到此次攻击影响。官方称，自奥运会开赛以来，法国已经阻止了数十起网络攻击。

美国金融巨头因勒索攻击损失近 2 亿元，超 1600 万用户数据泄露

8 月 7 日 SecurityWeek 消息，美国抵押贷款巨头 LoanDepot 通过 SEC 报告披露，今年 1 月曝光的勒索软件攻击相关的费用总计 2690 万美元（约合人民币 1.92 亿元）。公司当时遭受勒索软件攻击后，为了应对攻击导致数据被加密的情况，选择将一些系统下线。几周后，LoanDepot 通知当局，超过 1600 万人的个人信息可能已被泄露，泄露的信息包括姓名、地址、电子邮件地址、电话号码、出生日期、社会保障号码和金融账号。LoanDepot 最新财报显示，该事件给公司造成了 2690 万美元的损失，包括“调查和补救网络安全事件的成本、客户通知和身份保护的成本、专业费用（包括法律费用、诉讼和解费用及佣金担保）”。

勒索软件致使数百家印度小型银行支付系统瘫痪

8 月 1 日路透社消息，因技术服务提供商 C-Edge Technologies 遭受勒索软件攻击，近 300 家印度本地小型银行的支付系统被迫暂时关闭。负责监管支付系统的印度国家支付公司（NPCI）表示，为避免攻击影响扩大化，已临时禁止 C-Edge Technologies 访问 NPCI 运营的零售支付系统，期间使用 C-Edge 服务的银行的客户将无法使用支付功能。有消息人士称，受影响的大多是小型银行，仅有约 0.5% 的 NPCI 交易会受到影响。

美国知名电子大厂因勒索攻击损失超 1.2 亿元，此前曾停运两周

8 月 5 日 BleepingComputer 消息，美国知名电子制造服务提供商 Keytronic 披露，由于 5 月的一次勒索软件攻击，该公司遭受了超过 1700 万美元（约合人民币 1.2 亿

元）的损失。Keytronic 在 SEC 文件中表示，此次攻击影响了支持机器人操作和公司功能的业务应用程序，导致其墨西哥和美国站点受干扰被迫暂停运营两周。Keytronic 称，“由于这一事件，公司产生了约 230 万美元的额外费用，并推测在第四季度损失了约 1500 万美元的收入。这些订单大部分是可恢复的，预计将在 2025 财年内完成。”虽然 Keytronic 尚未将此攻击归因于特定的威胁团伙，但 Black Basta 勒索软件团伙在 5 月下旬声称对此负责，并泄露了他们所说的从公司系统中窃取的所有数据。Keytronic 是全球最大的印刷电路板组件（PCBA）制造商之一，在美国、墨西哥、中国和越南均设有工厂。

近 30 亿人个人数据遭暗网售卖，美国一背调公司被起诉

8 月 2 日 BloombergLaw 消息，一份在佛罗里达南区美国地方法院提交的起诉文件显示，今年 4 月，一家以“国家公共数据业务”（National Public Data）为名的背景调查公司 Jerico Pictures Inc. 发生了数据泄露事件，暴露了近 30 亿人的个人信息。此前 4 月 8 日，一家名为 USDoD 的网络犯罪团伙在一个暗网论坛上发布了名为“国家公共数据”的数据库，声称拥有 29 亿人的个人数据，并将该数据库以 350 万美元的价格出售。如果确认，这次泄露可能是有史以来影响人数最多的一次。2013 年雅虎的一次泄露事件曾暴露了大约 30 亿人的数据。根据投诉，为开展业务，国家公共数据从非公开来源抓取了数十亿人的个人身份信息，这意味着原告在不知情的情况下向该公司提供了他们的数据。一些被曝光的信息包括社会安全号码、现居地址、几十年来的曾居地址、全名、亲属信息，其中一些亲属甚至已去世近二十年。截至提交投诉时，Jerico Pictures Inc. 仍未向受影响的个人发出通知或警告。

美国重要血液中心遭勒索攻击，数百家医院启动“血液短缺”应急程序

7 月 31 日 The Record 消息，因勒索软件攻击关闭部分系统，美国大型血液中心 OneBlood 的运营能力骤降。OneBlood 发布声明称，“为了维持运转，我们已经实施了手动流程和程序。手动流程执行起来不仅需要耗费长得多的时间，还会影响库存可用性。为了进一步管理血液供应，我们已要求 250 多家接受我们服务的医院启动关键的血液短缺程序，并在一段时间内保持该状态。”OneBlood 表示，目前正在与网络安全专家及联邦和州官员合作解决这一危机。OneBlood 向美国东南部多个州的数百家医院提供血液及其他医疗物资。

史上最高！一财富 50 强企业向勒索软件支付了超 5.4 亿元赎金

7 月 30 日 The Stack 消息，美国安全厂商 Zscaler 发布报告称，2024 年年初发现一家财富 50 强企业向勒索软件团伙 Dark Angels 支付了 7500 万美元（约合人民币 5.42 亿元）。Zscaler 未透露受害者的名字，加密货币情报公司 Chainalysis 在社交平台上证实了这一消息。成功索要赎金的黑暗天使一跃成为今年最值得关注的勒索软件团伙。这一金额是此前公开报道的勒索软件赎金最高记录的近两倍。2021 年 3 月，美国保险巨头 CNA Financial 遭受勒索软件攻击后被迫支付 4000 万美元（约合人民币 2.89 亿元）。

美国政府最大 IT 服务商发生数据泄露事件

7 月 24 日彭博社消息，知情人士透露，黑客泄露了从美国联邦政府最大 IT 服务提供商之一的 Leidos Holdings Inc. 公司窃取的内部文件。Leidos 发言人表示：“我们已经确认，这是源于之前第三方供应商 Diligent 的数据泄露事件，所有必要的通知已在 2023 年发出。此次事件并未影响我们的网络或任何敏感客户数据。”根据 2023 年 6 月在马萨诸塞州提交的文件显示，Leidos 使用 Diligent 系统来托管内部调查中收集的信息。Diligent 发言人表示，这次泄露的数据似乎源自 2022 年其子公司 Steele Compliance Solutions 遭遇的黑客事件。该子公司于 2021 年被收购。当时包括 Leidos 在内的客户不到 15 家。Leidos 主要客户如美国国防部、国土安全部和 NASA 未立即回应置评请求。

乌克兰一城市供暖系统遭网络攻击被关闭，部分居民在寒冬下停暖近 2 天

7 月 23 日 TechCrunch 消息，美国工控安全公司 Dragos 发布报告，披露了一种旨在攻击工业控制系统的新型恶意软件 FrostyGoop。Dragos 表示，经与乌克兰当局沟通，在今年 1 月下旬，FrostyGoop 曾被用于攻击乌克兰利沃夫市的暖气系统，导致超 600 栋公寓楼停暖近 2 天，当时室外温度低于零度。据悉，FrostyGoop 恶意软件通过 Modbus 协议与工控设备交互，该协议被广泛用于工控环境，这意味着 FrostyGoop 也可被用于攻击其他公司和设施。Dragos 称，FrostyGoop 是该公司已发现的第九款专门针对工控系统的恶意软件。

墨西哥 ERP 软件巨头云泄露超 7 亿条记录，内含密钥等敏感信息

7 月 23 日 HackRead 消息，安全研究员 Jeremiah Fowler 发现，墨西哥最大的 ERP 软件提供商之一 ClickBalance 旗下一个云数据库暴露在公网，未设置任何认证措施，导致 7.69 亿条记录被泄露，恶意威胁行为者可以轻而易举地访问这些数据。Fowler 向 WebsitePlanet 报告了这一问题。该报告指出，该数据库包含了潜在的敏感信息，如访问令牌、API 密钥、密钥、银行账号、税号和 381224 个电子邮件地址。目前尚不清楚数据库暴露了多长时间，也不清楚是否有其他人访问过。Fowler 发送了负责任的披露通知，几小时后该数据库限制了公共访问。

CrowdStrike 更新导致全球近千万台 Windows 蓝屏死机

综合消息，7 月 19 日中午开始，CrowdStrike 问题更新导致全球 Windows 大面积蓝屏死机，致使航班停飞、火车晚点、银行异常、巴黎奥运服务受影响等，全球至少二十多个国家受到波及。由于事件发生时亚太地区在白天，欧美在夜晚，初期社交媒体上的反馈集中在亚太地区，主要是日本、澳大利亚。随着时间的推进，欧美用户也大量出现服务中断反馈。大量的机场、医院、媒体与银行由于系统的崩溃，导致服务中断，数以万计的航班延误取消，有些医院不得不转移病人，很多受影响企业的不得不提前放假。CrowdStrike 于当天下午发布相关通知承认了这一问题，并承诺将在 45 分钟后修复。微软官方后续表示，估计 CrowdStrike 的更新影响了 850 万台 Windows 设备，占所有 Windows 设备不到 1%。奇安信表示，基于其数据视野估计国内的 CrowdStrike 软件装机量在万级，相关单位数在百级，用户主要集中在北上广深等发达地区。受影响的主要是外企、外企在华分支机构及合资企业，大量这类机构中招，有反馈某个在华外企大量终端中的 40% 崩溃。

美国家具巨头遭勒索攻击：工厂被迫关闭 业务受到严重影响

7 月 17 日 The Record 消息，美国最大的家具公司之一巴西特家具（Bassett Furniture）表示，本月 10 日遭遇勒索软件攻击后被迫关闭部分 IT 系统，导致制造设施停运多天。该公司在 15 日公布的 SEC 文件中写道，“黑客通过加密某些数据文件扰乱了公司的业务运营”，迫使公司启动事件响应计划关闭部分系统。“公司的零售店和电子商务平台仍然开放，客户可以下单并购买现有商品。然而，公司目前的订单履行能力受到了影响。”巴西特家具罕见地承认，此次攻击已经并且可能继续对公司的业务运营产生重大影响。

重大事故！美国电信巨头 AT&T 几乎所有用户的电话记录泄露

7 月 12 日 TechCrunch 消息，美国电话电报公司（AT&T）披露，将向约 1.1 亿客户通知发生了一起新的数据泄露事件。该公司发言人表示，网络犯罪分子窃取了“几乎所有”客户的电话记录。被盗数据包含从 2022 年 5 月 1 日至 2022 年 10 月 31 日期间移动电话和固定电话客户的电话号码，以及 AT&T 网络内的通话和短信记录，如谁通过电话或短信联系了谁。被盗数据还包括 2023 年 1 月 2 日以后的小部分客户的较新记录，但未具体说明数量。AT&T 在 4 月 19 日得知该事件，由于事涉重大，美国司法部和 FBI 两度同意推迟在 SEC 披露文件中公开事件。

漏洞篇

8 月上旬，微软官方披露修复了 Windows 远程桌面许可服务远程代码执行漏洞（CVE-2024-38077），未经身份认证的攻击者可利用漏洞远程执行代码，获取服务器控制权限。目前网信办旗下漏洞平台 CNVD、工信部漏洞平台 NVDB 均发布预警，建议受影响的用户即刻升级到最新版本。

微软 8 月补丁日多个产品安全漏洞风险通告

8 月 14 日，微软本月共发布了 91 个漏洞的补丁程序，修复了 Windows WinSock、Microsoft Project、Windows Power Dependency Coordinator 和 Azure 等产品中的漏洞。经研判，以下 22 个重要漏洞值得关注（包括 7 个紧急漏洞、14 个重要漏洞、1 个中等），如下表所示。鉴于这些漏洞危害较大，建议客户尽快安装更新补丁。

编号	漏洞名称	风险等级	公开状态	利用可能
CVE-2024-38193	Windows 辅助功能驱动程序 WinSock 权限提升漏洞	重要	未公开	在野利用
CVE-2024-38189	Microsoft Project 远程代码执行漏洞	重要	未公开	在野利用
CVE-2024-38107	Windows Power Dependency Coordinator 权限提升漏洞	重要	未公开	在野利用
CVE-2024-38106	Windows 内核权限提升漏洞	重要	未公开	在野利用
CVE-2024-38213	Windows Web 查询标记安全功能绕过漏洞	中	未公开	在野利用
CVE-2024-38063	Windows TCP/IP 远程代码执行漏洞	紧急	未公开	较大
CVE-2024-38109	Azure Health Bot 权限提升漏洞	紧急	未公开	较小
CVE-2024-38140	Windows 可靠多播传输驱动程序 (RMCAST) 远程代码执行漏洞	紧急	未公开	较小
CVE-2024-38160	Windows 网络虚拟化远程代码执行漏洞	紧急	未公开	较小
CVE-2024-38159	Windows 网络虚拟化远程代码执行漏洞	紧急	未公开	较小
CVE-2024-38206	Microsoft Copilot Studio 信息披露漏洞	紧急	未公开	较小
CVE-2024-38166	Microsoft Dynamics 365 跨站点脚本漏洞	紧急	未公开	较小
CVE-2024-38150	Windows DWM 核心库权限提升漏洞	重要	未公开	较大
CVE-2024-38144	Kernel Streaming WOW Thunk 服务驱动程序权限提升漏洞	重要	未公开	较大
CVE-2024-38141	Windows 辅助功能驱动程序 WinSock 权限提升漏洞	重要	未公开	较大
CVE-2024-38163	Windows Update Stack 权限提升漏洞	重要	未公开	较大
CVE-2024-38148	Windows 安全通道拒绝服务漏洞	重要	未公开	较大
CVE-2024-38147	Microsoft DWM 核心库权限提升漏洞	重要	未公开	较大
CVE-2024-38133	Windows 内核权限提升漏洞	重要	未公开	较大
CVE-2024-38125	Kernel Streaming WOW Thunk 服务驱动程序权限提升漏洞	重要	未公开	较大
CVE-2024-38198	Windows 打印后台处理程序权限提升漏洞	重要	未公开	较大
CVE-2024-38196	Windows 通用日志文件系统驱动程序权限提升漏洞	重要	未公开	较大

微软 RDL 服务远程代码执行漏洞安全风险通告

8 月 9 日，奇安信 CERT 监测到官方修复 Windows 远程桌面授权服务远程代码执行漏洞 (CVE-2024-38077)，该漏洞存在于 Windows 远程桌面许可管理服务（RDL）中，成功利用该漏洞的攻击者可以实现远程代码执行，获取目标系统的控制权，可能导致敏感数据的泄露及恶意软件的传播。该漏洞影响所有启用 RDL 服务的 Windows Server 服务器，特别是未及时更新 2024 年 7 月微软最新安全补丁的系统。需要注意，RDL 服务并非默认启用，但出于扩展功能等目的，许多管理员会手动启用它，如增加远程桌面会话的数量。在

一些特定的场景中，如堡垒机和云桌面 VDI 环境，RDL 服务的启用也是必需的。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Google Chrome ANGLE 越界访问漏洞安全风险通告

8 月 7 日，奇安信 CERT 监测到 Google 修复 Google Chrome ANGLE 越界访问漏洞 (CVE-2024-7532)，Chrome 使用的 2D/3D 图形渲染引擎 ANGLE 中存在越界内存访问漏洞，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或导致浏览器崩溃。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Roundcube Webmail 多个 XSS 高危漏洞安全风险通告

8 月 6 日，奇安信 CERT 监测到官方修复 Roundcube Webmail 跨站脚本漏洞 (CVE-2024-42008) 和 Roundcube Webmail 跨站脚本漏洞 (CVE-2024-42009)。Roundcube Webmail 在处理 HTML 和 SVG 等附件的过程中存在跨站脚本漏洞。未经身份验证的攻击者可以窃取电子邮件、联系人和密码等敏感信息。鉴于之前的 Roundcube Webmail 漏洞曾多次在 2023 年被 APT28、Winter Vivern 等 APT 组织利用，建议客户尽快做好自查及防护。

Apache OFBiz 授权不当致代码执行漏洞安全风险通告

8 月 5 日，奇安信 CERT 监测到官方修复 Apache OFBiz 授权不当致代码执行漏洞 (CVE-2024-38856)，该漏洞允许未经过身份验证的攻击者绕过原有的安全机制执行代码。攻击者可能利用该漏洞来执行恶意操作，包括但不限于获取敏感信息、修改数据或执行系统命令。目前该漏洞技术细节与 PoC 已在互联网上公开，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

JumpServer 多个高危后台漏洞安全风险通告

7 月 19 日，奇安信 CERT 监测到官方修复 JumpServer 后台文件写入漏洞 (CVE-2024-40629) 和 JumpServer 后台文件读取漏洞 (CVE-2024-40628)。攻击者可以利用 Ansible 脚本读取或写入任意文件，从而导致 Celery 敏感信息泄露和远程代码执行。奇安信鹰图资产测绘平台数据显示，该批漏洞关联的国内风险资产总数为 124,880 个，关联 IP 总数为 22,031 个。目前该漏洞技术细节与 PoC 已在互联网上公开，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Nacos Derby 远程命令执行漏洞安全风险通告

7 月 19 日，奇安信 CERT 监测到官方修复 Nacos Derby 远程命令执行漏洞 (QVD-2024-26473)，由于 Alibaba Nacos 部分版本中 derby 数据库默认可以未授权访问，恶意攻击者利用此漏洞可以未授权执行 SQL 语句，最终导致任意代码执行。奇安信鹰图资产测绘平台数据显示，该漏洞关联的国内风险资产总数为 40,575 个，关联 IP 总数为 8171 个。目前该漏洞 PoC 已在互联网上公开，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

泛微 e-cology9 WorkflowServiceXml SQL 注入漏洞安全风险通告

7 月 15 日，奇安信 CERT 监测到泛微 e-cology9 WorkflowServiceXml SQL 注入漏洞 (QVD-2024-26136) 在野利用行为，在默认配置下，未授权攻击者可利用该漏洞执行任意 SQL 语句，从而造成任意命令执行。奇安信鹰图资产测绘平台数据显示，该漏洞关联的国内风险资产总数为 51,855 个，关联 IP 总数为 8761 个。目前该漏洞 PoC 已在互联网上公开，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

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。

规划快一步

奇安信

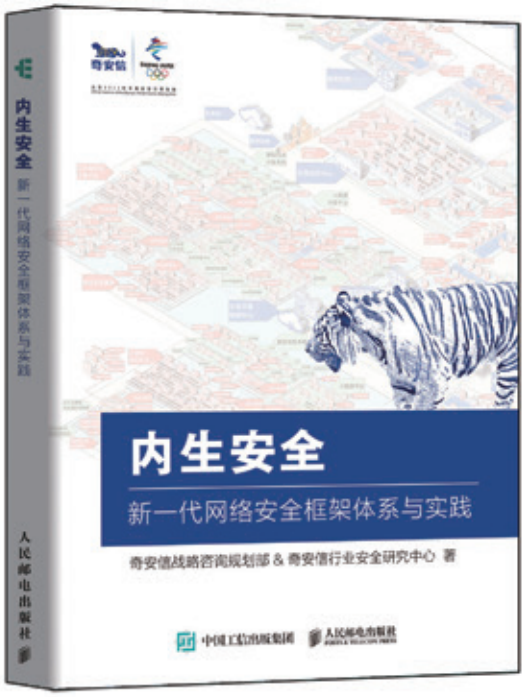
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

新书发布

内生安全权威解读

19支团队、37位专家倾力打造

政企“十四五”网络安全规划必读书籍



- 什么是内生安全
- 内生安全从何而来
- 为什么要内生安全
- 内生安全如何落地
- 新一代网络安全框架
- “十工五任”建设要点

扫描二维码
专享内购价

微软“蓝屏事件”深度复盘

——几行代码引发的全球性混乱

全球数千航班取消

多国银行服务中断

政府、医疗业务受到影响

只需几行代码，就让全球数百万台计算机死机，引发全面的社会混乱。这种只在科幻电影中出现的场景，真实发生了。

7 月 19 日凌晨 4 点，网络安全巨头 CrowdStrike 向其 Falcon 产品发送例行的内容配置更新。

随后，一场严重程度和规模都空前的全球 IT 系统故障爆发，全球 850 万台 Microsoft 设备受到影响，全球重要航空公司、医院、银行、医疗机构、政府等机构随之出现业务中断，引发了巨大的混乱。事件影响超过了之前所有的黑客攻击和系统故障，成为有史以来最大的网络事件。

CrowdStrike 致全球 IT 基础设施中断事件分析

本文撰稿　奇安信 CERT

北京时间 2024 年 7 月 19 日中午开始，CrowdStrike 问题更新导致全球 Windows 大面积蓝屏死机，致使航班停飞、火车晚点、银行异常、巴黎奥运服务受影响等，全球至少二十多个国家受到波及。

基于奇安信的独有数据视野，我们估计国内的 CrowdStrike 软件装机量在万级，相关单位数在百级，用户主要集中在北上广深等发达地区。受影响的主要是外企、外企在华分支机构及合资企业，大量这类机构中招。有反馈，某个在华外企大量终端中的 40% 崩溃。

01 CrowdStrike 公司及产品概况

CrowdStrike 公司成立于 2011 年，由两位传统杀毒软件 McAfee 的高管创立，团队成员主要来自信息安全产业，如微软和亚马逊等。该公司是全球知名的下一代终端安全厂商，其核心产品包括基于云的 Falcon 平台及其多个模块，这些模块涵盖了端点保护、威胁情报、IT 资产管理和恶意软件搜索等多个领域。目前市值超 800 亿美元，仅次于最大的网络安全公司 Palo Alto Networks。

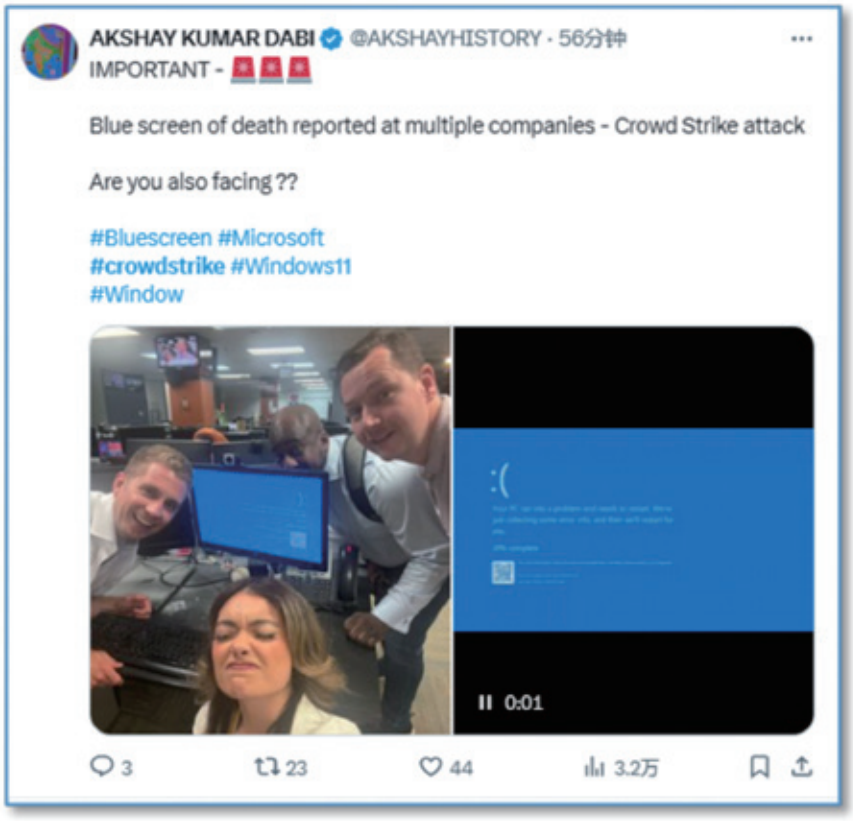
Falcon 平台是 CrowdStrike 的核心产品，它是一个完全基于云端部署的 SaaS 模型，能够提供实时的攻击指标、威胁情报和不断进化的对手手法技术。该平台通过一个轻量级的代理架构实现快速且可扩展的部署，并提供高级别的保护和性能。此外，Falcon 还集成了多种功能，如文件完整性监控、云安全、身份保护等。

CrowdStrike 目前的客户数超 24000 个，覆盖了大部分全球 500 强企业，导致本次事故的就是其 Falcon 平台的核心组件驱动程序部分的功能。

02 IT 服务中断情况

北京时间 2024 年 7 月 19 日周五下午 2 点多开始，全球大量 Windows 用户在社交媒体上晒出电脑蓝屏画面，出现了大量 Windows 电脑崩溃、显示蓝屏死机、无法重新启动的案例。

由于事件发生时亚太地区在白天，欧美在夜晚，初期社交媒体上的反馈主要集中在亚太地区，主要是日本、澳大利亚。随着时间的进展，欧美用



户也大量出现服务中断反馈。大量的机场、医院、媒体与银行由于系统的崩溃，导致服务中断，数以万计的航班延误取消，有些医院不得不转移病人，很多受影响企业不得不提前放假。

事件还影响到了微软的云服务，主要应该是微软云服务上运行了大量的基于 Windows 系统的应用程序实例，其中部分安装了 CrowdStrike 的软件，所以连带着这些虚拟机也崩溃了。当然，也可能有部分原因在于微软的管理云的应用系统也受到了 CrowdStrike 的影响。

在国内，“微软蓝屏”迅速登顶微博热搜，成为热议话题。随后，蓝屏问题被确认与 CrowdStrike 的软件更新有关，导致 Windows 用户出现了蓝屏现象。

CrowdStrike 于 7 月 19 日下午发布相关通知承认了这一问题，并承诺将在 45 分钟后修复。

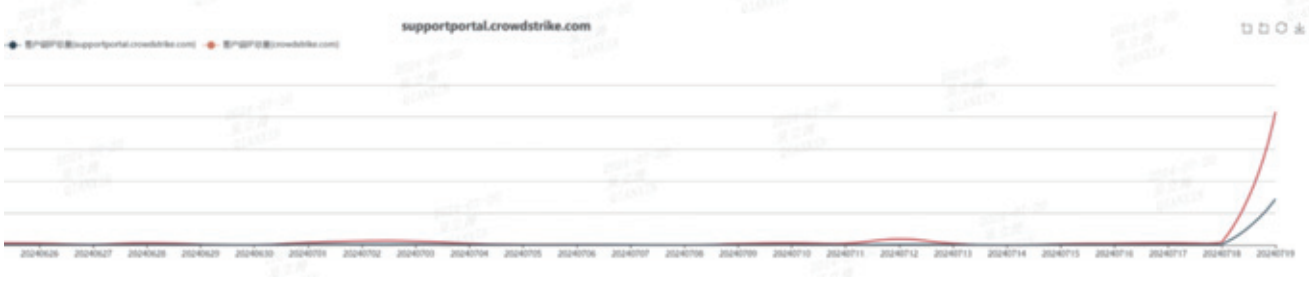
CrowdStrike 本次 IT 系统中断事件的影响一定会被记入史册，与 2017 年的 WannaCry 勒索蠕虫事件可相提并论，所幸由于安全软件生态一定程度的隔离，中国所受的影响不大。

03 软件系统影响面

Falcon sensor for Windows version 7.11 在线时间北京时间 7 月 19 日中午 12 点 09 分 ~13 点 27 分，下载了问题更新的系统会遭遇崩溃。

基于奇安信的独有数据视野，估计国内的 CrowdStrike 软件装机量在万级，相关单位数在百级，用户主要集中在北上广深等发达地区。受影响的主要是外企、外企在华分支机构及合资企业，大量这类机构中招。有反馈，某个在华外企大量终端中的 40% 崩溃。

奇安信网络研究院对于 CrowdStrike 相关网站的访问监测显



示，7 月 19 日国内对于 CrowdStrike 支持网站的访问量出现了上百倍的增长，可见国内对此事件的关注度与处置力度也很高。

至于国内的其他类型单位，特别是党政央企、大型的民企公司，使用量极少。奇安信收到的相关应急响应需求很少，此次事件对国内的政府、央企及绝大部分的大型民企影响不大。

以当前 Falcon 软件的安装量，初步估计导致数以百万到千万计的 Windows 系统不可用，由于问题导致计算机只要启动就会蓝屏崩溃，因此没有自动化的措施可以执行批量集中修复，只能一台台手工操作解决问题，所以恢复过程会非常消耗时间和精力，估计完全恢复需要的时间将以周计。

04 技术细节相关的讨论

Falcon 是安全软件，有其特殊性，需要获取操作系统底层权限来更好地实现保护能力，所以组件很多以驱动程序形态出现。这回导致系统崩溃的 CSAgent.sys 是 CrowdStrike 客户端的一个核心的驱动，驱动程序由于工作在内核态，一旦执行上出现问题，就直接会导致操作系统不可用，启动时加载驱动直接蓝屏，这是它跟一般工作在应用层的应用程序不一样的地方。

按 CrowdStrike 给出的解释，程序在增加处理新观察到的利用命名管道进行 C&C 通信的恶意代码活动时，更新相应的配置文件（“C-00000291-”开头的文件）触发了一个代码中的逻辑错误，在内核态形成非法内存访问，触发操作 Windows 系统蓝屏。因此，导致问题的更新应该被视为某种“规则”的更新，而不是直接驱动程序本身，这也就可能解释了数据的下发如此快速而“随意”，但依旧无法解释如此能导致明显危害的更新如何通过了发布前的测试环节。

05 事件的启示与建议

此次事件暴露出 CrowdStrike 公司在产品开发测试发布环节中存在严重问题，存在质量缺陷的软件通过了测试，以看起来并没有灰度机制的方式被推送出来，直接导致了数以百万计的系统不可用。作为一个国际主流的大安全厂商，会出现这样的低级错误，这是整个事件中最不可思议的地方。

目前，主要有两种阴谋论的说法浮出水面，引起了人们的热烈讨论。

> 一次软件更新引发全球 IT 事故，
> 提醒了业界和广大用户，
> 即使是非常成熟的技术平台也可能遭遇意外故障，
> 再次凸显了“零事故”保障（业务不中断、
> 数据不出事、合规不踩线）的重要性和必要性。

第一种说法认为，这起事件可能是美国政府进行的一种压力测试，目的是为了检验在遭受网络战攻击时的社会现象和应急恢复能力。然而，对于这一说法，有人认为其代价过于巨大。据估计，此次事件造成的直接和间接损失高达数十亿美元。尽管如此，仍有部分人坚持认为，这与历史上的某些事件相似，例如 911 恐怖袭击，他们认为这可能是政府的某种策略。

第二种说法则指向了 CrowdStrike 公司，认为有黑客入侵了该公司，并修改发布了恶意代码，导致了此次计算机崩溃事件。对于这一说法，普遍认为可能性相对较大。尽管 CrowdStrike 公司否认了遭受网络攻击的说法，但考虑到公司可能出于维护形象的考虑，这种否认也是可以理解的。然而，如果这一说法属实，公司将不得不面对可能的诉讼和赔偿问题。值得注意的是，目前还没有组织或个人宣称对此次事件负责。

在这两种说法中，尽管各有其支持者，但真相究竟如何，目前尚无定论。

其实终端软件安全厂商由于自己的开发运营能力问题搞出破坏客户系统的事件绝不新鲜，大多影响范围较小而不被公众所感知。2010 年，当时的 McAfee 就因为发布了错误的病毒定义，删除了 Windows XP 的系统文件而导致系统反复重启不可用。巧合的是当时 McAfee 的 CEO 就是现在 CrowdStrike 的 CEO，可以说是传统艺能。因此，运营错误导致问题的可能性还是远高于阴谋论。

抛开阴谋论不提，一次软件更新引发全球 IT 事故，提醒了业界和广大用户，即使是非常成熟的技术平台也可能遭遇意外故障，再次凸显了“零事故”保障（业务不中断、数据不出事、合规不踩线）的重要性和必要性。

此次微软蓝屏，导致全球大量主机无法使用，包括终端和一部分服务器主机，对全球航空、金融等重要业务产生重大影响，大量重要政府企业无法对外提供服务，再回想 2017 年的永恒之蓝勒索病毒，同样导致了全球大量主机无法使用，大量政府企业无法提供服务。说明网络安全行业，已经和水电煤气一样，就是整个社会的关键基础设施行业，无论是没有防住网络攻击，还是升级更新出现问题，都会导致重大的社会影响。

因此，网络安全行业，真正要追求的目标是重要环境“零事故“，零事故的第一个标准就是“业务不中断”，从奇安信参与的 2017 年永恒之蓝的应急处理，和 2022 年北京冬奥的“零事故”安全保障，客户没有出现过勒索和蓝屏，核心业务都没有受到中断影响。

零事故的核心是对安全的持续投入和重视，是一个体系化建设工程，如果没有足够多、足够长时间的投入，“零事故”目标就无从谈起。对客户来说，应该以“零事故”为标准，做好业务弹性规划，以随时应对勒索软件攻击、员工失误或意外 IT 故障的威胁。

综上可见，业务稳定和网络安全不仅是技术问题，更是管理和战略问题，需全面综合考虑各种因素，主要体现在以下几点。

对于安全厂商

· 首先是把好质量关。正所谓“能力越大责任也越大”，涉及系统稳定性的软件厂商需要对自己的软件有更严格的质量管理。否则，这种意外故障导致的业务连续性问题比恶意的网络攻击还要大。

· 其次是做好升级策略。在产品升级时，要控制影响范围，俗称“爆炸半径”，掌控好升级策略，确保灰度升级，控制放量节奏。逐步测试，逐步增加覆盖。

· 最后是态度需要积极主动。在出现事故时，平台厂商和安全厂商，都需要本着客户至上原则，最短时间给出客户相应的解决方案，并积极与公众沟通，避免因信息差等导致的恐慌。

安全产品用户

· 选择有实力有信用背书的安全厂商，尤其基于当前复杂的国际环境，优先国内的能力厂商。

· 在部署终端安全软件，要对资产做好分类、分级，对关键资产设置单独的管理单元或分组，并设置灰度或延迟更新的策略。

对于国家相关主管机构

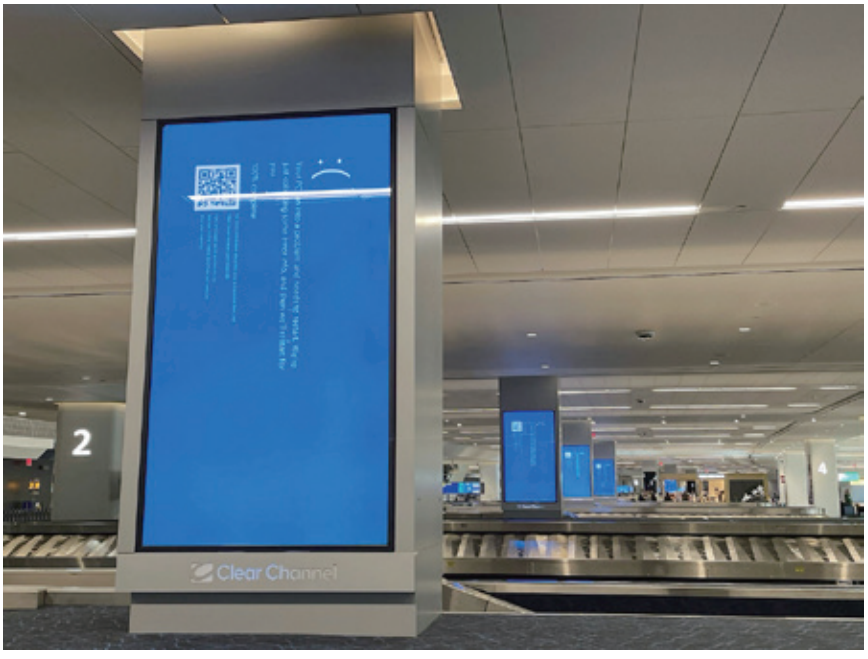
· 持续推进国产化，安全软件工具平台与操作系统一样有特殊的影响和意义，必须确保自主可控。

· 使用面巨大的软件应该作为关基一样的重点关注目标，鼓励国产化操作系统及流行软件的漏洞挖掘及风险消除的行动。

· 进一步加强关键基础信息系统的保护，切实执行相关的法规，落实相应的能力建设。

CrowdStrike 故障引发全球性混乱与巨额损失

作为最大的网络安全公司之一，CrowdStrike 的软件在全球非常受欢迎。正因为如此，更新造成的系统故障影响范围十分广泛，被称为“历史上最大的 IT 故障”。全球的多家航空公司、医院、银行、医疗机构、政府机构随之遭遇业务中断，引发了巨大的混乱。



图：航空业受 IT 故障影响最大

全球性混乱影响多个行业

航空

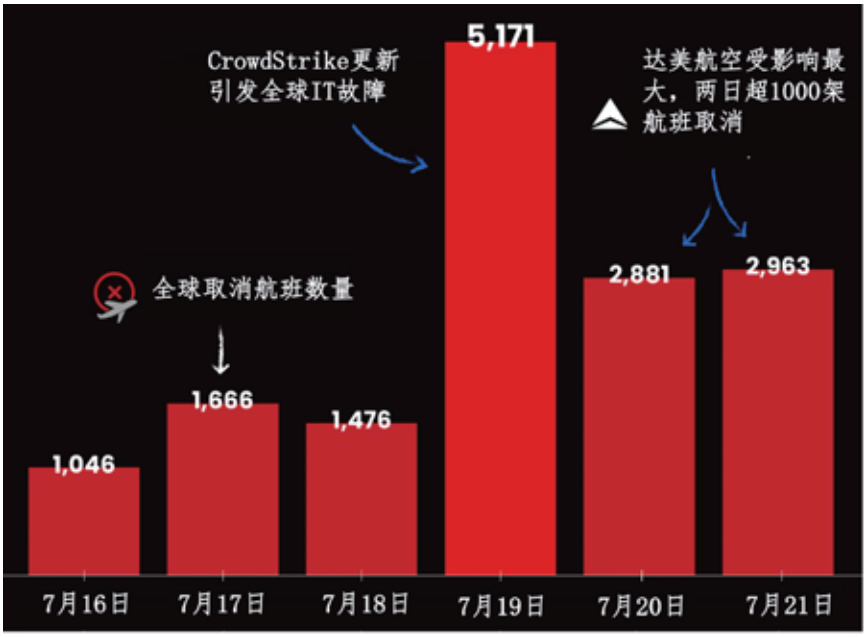
根据航班跟踪与数据平台 FlightAware 的数据，7 月 19 日超过 5,000 个航班被取消，比过去三天的平均取消数量高出 270%。

美国联邦航空管理局因系统宕机关闭运营。因通信问题，达美航空、联合航空、美国航空等美国航空公司宣布停飞航班，机场陷入混乱。航空数据公司 Cirium 称，达美航空及其地区附属公司取消了 1300 个航班，占其航班计划的 1/4 以上。联合航空和联合快运则取消了 550 多个航班，占其航班计划的 13%，美国航空网络取消了 450 多个航班，占其航班计划的 8%。

在全球主要航空旅行市场中，英国、法国和巴西的航班取消率约为 1%，加拿大、意大利和印度的航班取消率约为 2%。

印度航空、荷兰皇家航空、香港国际机场、柏林勃兰登堡机场和伦敦斯坦斯特德机场等多家航空公司和机场也报告了故障情况，其中一些航空公司不得不依靠人工办理登机手续。

部分铁路交通也受到影响。美国首都华盛顿特区的地铁系统出现延误。



图： IT 故障导致 5000 个航班取消

纽约市地铁系统管理机构 MTA 表示，“由于全球技术故障，部分 MTA 客户信息系统暂时离线。”

英国最大的通勤铁路网络 GTR 表示，其泰晤士河铁路和南部铁路列车因通信系统故障而中断。西南铁路表示，其所有售票机都已停止工作。西米德兰兹铁路、阿凡提西海岸干线、大西部铁路和奔宁特快也受到影响。

医疗服务

系统故障对医疗行业造成了严重的影响，一些医疗机构和医院推迟了全部或大部分手术；医生无法访问电子病历，只能改用纸和笔。

在英国、德国和以色列等国，患者的医院预约在最后一刻被取消。其中，位于英格兰南部的皇家萨里国民保健服务信托机构宣布发生危急事件，取消了原定于 7 月 19 日早上的放射治疗预约。 英国诊所通过社交媒体报告称，无法访问患者记录或预约系统。以色列和美国的一些医院也遇到无法访问电子病历的问题。

更为严重的是，医院和 911 调度团队等重要应急服务也受到了影响。麻省总医院就此次中断对其运营的影响发表了以下声明：“全球范围内的重大软件故障影响了麻省总医院的许多系统。由于问题的严重性，今天（7 月 19 日）之前安排的非紧急手术、程序和医疗就诊均被取消。”美国阿拉斯加部分地区的 911 紧急电话线路中断，官员在社交媒体上发布了备用电话号码。新罕布什尔州和俄亥俄州等其他州也报告了类似问题。

金融服务

航空公司因故障而不得不取消航班，大多数市场和支付系统却仍在运行。但世界各地银行机构的大量服务也都受到严重影响——从 ATM 到移动银行应用和呼叫中心。

据监控应用程序 Downdetector 的数据，美国阿维斯特银行、美国银行、第一资本、查尔斯 · 施瓦布、道明银行、全美银行、富国银行受到影响。

据 CNN 报道，澳大利亚、南非、新西兰和英国的银行也都遭遇了服务中断。

英国银行桑坦德银行和大都会银行表示，周五的停电事件导致他们的 ATM 服务受到影响；新西兰的一些银行服务也受到干扰；南非的 Capitec 也遭遇了同样的问题。巴西主要金融机构布拉德斯科银行通过其应用通知用户，由于全球网络中断，数字服务存在不稳定。

媒体机构

世界各地的主要广播公司都遇到技术问题。NBC News、MSNBC 和英国天空新闻台（Sky News）等电视台都出现播出中断的问题。

澳大利亚广播公司，包括 Sky

News Australia、ABC、SBS、Channel7 和 Channel 9 也报告了技术问题。

商业运营

英国各大超市均报告了在线服务问题，包括乐购、英佰瑞、Asda、莫里森超市和维特罗斯连锁超市。一些超市甚至只接受现金。

德国地区性连锁杂货店 Tegut 则因收银系统受到影响，7 月 19 日暂时关闭了 340 家门店。

日本大阪环球影城表示，全球系统故障将影响周末园区的门票销售。7 月 20 日、21 日停止售票。

图：CrowdStrike 股价下跌超过 20%

54 亿美元的惊人损失

CrowdStrike 引发的系统瘫痪给相关机构带来巨大的经济损失。专家指出，系统瘫痪会造成收入损失、运营费用增加及巨大的修复成本。

IDC 研究部门副总裁 Duncan Brown 认为：此事带来的成本最有可能来自系统不可用导致的交易损失。此外还会导致生产力和运营成本的损失，然后是解决宕机问题的修复，其中大部分都需要人工干预。

微软公司估计，受影响的 Windows 机器超过 850 万台，研究公司 J. Gold Associates 预计仅修复成本就高达 7.01 亿美元，这基于内部技术支持团队修复机器所需的 1275 万个小时来计算。平均而言，每台受影响的机器，由内部员工修复将花费公司 82.50 美元。如果聘请外部帮助，成本可能会增加三倍。

美国云监控和保险服务提供商 Parametrix 估计，CrowdStrike 引发的宕机事件给美国财富 500 强公司（不包括微软）造成的直接经济损失达 54 亿美元。由于许多公司的风险自留额较大，且相对于潜在宕机损失的保单限额较低，网络保险单承保的损失部分可能不会超过 10% ~ 20%。这意味着相关企业将自己承担大部分费用。

根据 Parametrix 发布的《CrowdStrike 对世界财富 500 强的影响分析》报告，约有 25% 的财富 500 强企业因 CrowdStrike 故障而发生业

务中断。财富 500 强企业中，受影响最严重的行业是航空业、医疗行业和银行业，其中医疗行业的直接损失达 19.38 亿美元，银行业和航空业紧随其后，分别损失 11.5 亿美元和 8.6 亿美元。据估计，这三个行业每家机构的平均损失分别为 6460 万美元、7180 万美元和 1.4338 亿美元。但相关专家认为，实际数字可能要高得多。值得注意的是，100% 的航空业都受到了影响。

除了直接损失外，系统瘫痪造成的隐性成本可能还包括服务中断而支付给客户的赔偿及违规罚款。

此外，客户品牌还会蒙受声誉的损失。CrowdStrike 本身就遭受了严重打击，股价下跌超过 20%，股东价值损失超过 150 亿美元。

影响深远的 IT 故障频发

信息技术主导的现代社会，每隔一段时间似乎就会遭遇一次影响深远的 IT 故障。事实上，过去数年中，全球曾爆发出数起类似的宕机事件，重大 IT 故障的规模越来越大，发生频率也越来越高，凸显出全球互联系统的脆弱性。

根据影响范围，总结出史上十大 IT 宕机事件。

1. CrowdStrike IT 故障

2024 年 7 月 19 日，错误的 CrowdStrike 更新，导致 Windows 10 及更高版本崩溃，从而造成医院和航空公司等关键服务领域的全球 IT 中断。

2. 亚马逊云服务 (AWS) 中断

2021 年 12 月 7 日，亚马逊云服务 (AWS) 因网络设备过载，发生严重中断，持续数小时。自动容量扩展引发了意外行为。包括 Netflix、迪士尼、Spotify、DoorDash 和 Venmo 等众多知名企业遭遇运营中断。

3. Facebook 服务中断

2021 年 10 月 4 日，Facebook 及其子公司 Messenger、Instagram、WhatsApp 和 Oculus 遭遇全球宕机。Facebook 的数据中心与网络断开连接，全球数十亿用户服务中断数小时。

4. Fastly 服务器宕机

2021 年 6 月 8 日，内容交付网络 (CDN) 提供商 Fastly 的一项服务配置问题，引发了全球网络中断，影响到英国政府及 CNN、Reddit 和纽约时报等主要网站。

5. 谷歌全球宕机

2020 年 12 月，谷歌出现全球性宕机。Gmail、谷歌日历和 YouTube 等服务均出现故障，持续约 45 分钟，影响了全球数百万用户。问题是由于该公司身份验证工具的存储容量不足造成的。

6. Microsoft Azure 服务 中断

2020 年 3 月 3 日，Microsoft 至关重要的美国东部 Azure 区域大部分服务中断超过 6 小时。楼宇自动化控制故障引发的温度飙升影响了存储、计算、网络和相关服务。

7. T-Mobile 网络故障

2020 年 6 月，T-Mobile 网络经历 12 小时的中断，影响了其 4G、3G 和 2G 网络。此次故障导致拥塞，超过 23,000 个 911 呼叫失败。此次中断是由光纤链路故障和其他因素造成的。

8. Equinix 数据中心宕机

2018 年 3 月 2 日，弗吉尼亚州阿什本的 Equinix 数据中心宕机，部分中断了 AWS 连接，影响了 Atlassian、Twilio 和 Capital One 等客户。该地区的东北气旋导致了东海岸的电力中断，影响了 Equinix 数据中心。

9. 英国航空 IT 故障（2017 年）

2017 年 5 月 17 日，英国航空公司在最繁忙的周末遭遇重大 IT 故障。据新闻报道，约有 7.5 万名乘客受到影响，672 架飞机停飞，造成超过 1 亿美元的损失。一名工程师拔掉了数据中心的电源，导致大规模停电。

10. Dyn 遭 DDoS 攻击

2016 年 10 月，互联网域名系统 (DNS) 服务商 Dyn 公司遭遇分布式拒绝服务 (DDoS) 攻击，导致美国数百万个主要网站瘫痪数小时，其中包括 Twitter、亚马逊、GitHub、BBC、CNN、纽约时报等。

全球网安领导者如何看待微软蓝屏事件

全球网络安全企业的领导人分享了对此次事故的看法，并为其他组织提供了相关建议。

Palo Alto Networks 董事长兼首席执行官 Nikesh Arora

Palo Alto Networks 的产品更新方法是部署 1% ~ 3% 的样本测试队列，以确保不会发生问题；接下来，会分阶段发布内容更新。此外，Palo Alto Networks 还启用了控件，以便客户可以管理更新流程，并对其进行控制。

我加入 Palo Alto Networks 时的首要任务就是确保公司的产品“不断改进”。公司产品以最佳方式为客户解决问题，同时也在解决新问题。换句话说，Palo Alto Networks 的成功取决于产品组合和质量。基于 Palo Alto Networks 的产品，客户可以采用同类最佳的产品，并最终发展为平台模式。

奇安信集团董事长 齐向东

网络安全部署上的几个关键差异，让中国可以避免类似 CrowdStrike 的恶性事故。

首先，中国政企机构倾向于采用本地私有化部署，并和安全厂商的云进行可控的连接，这样即便出现问题，影响范围也仅限于单个单位或企业，不会像公有云那样一出问题就波及一大片。

其次，中国政企机构使用的终端安全软件与普通民众使用的计算机安全软件是完全分开的，其升级更新和维护策略也完全不同。

再次，中国政企机构的操作系统并非完全依赖微软 Windows 视窗系统。麒麟等信创操作系统已占据了相当大的市场份额，这减少了对 Windows

系统的依赖，从而降低了因软件更新导致的风险；操作系统多元化，可以形成异构的弹性机制，不容易集中性、大面积地统一出问题。

奇安信集团在保障政企机构业务连续性方面拥有丰富经验。每次软件升级都会进行灰度测试，先在小范围内升级，确保无误后再逐步扩大范围。这种渐进式的升级策略和一整套的体制机制保障，可以有效避免因软件更新而导致的大规模宕机事件。

Trustwave 首席信息安全官 Kory Daniels

“最近的 CrowdStrike 事件凸显了一个日益严重的问题：大范围的自然或数字灾难都有可能成为犯罪活动的催化剂。经验告诉我们，这些混乱时刻往往伴随着犯罪行为的激增。我们必须认识到，数字环境与物理世界一样，容易受到不可预见事件的影响，我们必须做好准备，防范可能随之而来的犯罪行为。

为了增强准备和恢复能力，组织必须优先考虑强大的事件响应和恢复计划，包括模拟关键系统和人员不可用的场景。这需要全面的战略来应对自然灾害和网络攻击。定期测试和模拟演习对于让团队有效应对危机至关重要。培养一种恢复力文化可以提高整个组织的警惕性和准备程度。

SecurityScorecard 首席执行官 Aleksandr Yampolskiy

我以前在高盛工作时，采购政策是从多家供应商购买工具。如果一家供应商的防火墙出现故障，还有另一家供应商可用。全球系统故障提醒我们，影响日常生活的技术存在脆弱性和系统集中风险。

系统故障只是安全事件的另一种形式。在这种情况下，反脆弱性来自于不把鸡蛋放在一个篮子里。你需要拥有多样化的系统，知道单点故障在哪里，并通过桌面演习和中断模拟主动进行压力测试。考虑一下“混乱猴子”的概念，故意破坏自己的系统——例如，关闭数据库或让防火墙发生故障，看看计算机会如何反应。

UpGuard 首席信息安全官 Phil Ross

CrowdStrike 故障不是第一次影响全球行业的技术中断，也不会是最后一次。为了避免和减少 CrowdStrike 更新导致的 IT 故障影响，必须对影响区域进行分类，并采取策略以尽量减少宕机。

对于最终用户计算设备，组织应推迟对操作系统、软件代理和应用的补丁和更新，直到在代表性设备上经过测试。此外，实施紧急更新的快速测试流程至关重要，尤其是针对安全软件。为了防范广泛使用的软件中的漏洞，组织需要清晰地了解其软件供应链。

黑莓网络安全英国及新兴市场副总裁 Keiron Holyome

鉴于此次故障影响了世界上一些最关键的系统、网络和应用，必须快速、准确、负责任地做出响应。关键事件管理 (CEM) 解决方案可以提供实时可见性，以确保在危机发展时快速做出明智的响应。

复杂的 EDR 和重型端点代理会带来重大的基础设施风险，且毫无必要地复杂。在端点上使用轻量级 AI 可以避免此类故障，因为它可以保护您的环境，而无需重型代理和定期更新，从而避免运营面临风险。

从更广泛的角度来看，此次全球 IT 故障是一个明确的提醒：最好的防守就是进攻。通过定期测试，了解漏洞和风险至关重要。为了防范试图利用 IT 故障的威胁行为，结合使用 AI 支持的内外部渗透测试评估仍然至关重要。

最大规模宕机事件的 10 个教训

网络安全公司 CrowdStrike 旗下的猎鹰传感器（Falcon Sensor）的一次软件更新引发了一场全球危机，导致全球安装有 Windows 系统的计算机出现大规模的蓝屏死机（blue screen of death, 即 BSOD），结果数千架航班被迫停飞、医院陷入混乱、支付系统崩溃，直接影响了数百万用户，成为历史上最大的 IT 故障。初步统计，宕机事件给财富 500 强企业造成高达 54 亿美元的损失。

此次宕机是由于 CrowdStrike 猎鹰传感器的更新中存在缺陷而引发的，相关更新出现一个逻辑错误，进而导致系统崩溃，特别是 Windows 设备。

IT 管理员被迫通过手动方式解决该问题，同时微软公司发布了相关工具进行系统恢复。CrowdStrike 公司也部署了一个修复程序，并向受影响的客户持续提供更新和补救措施。

尽管做出了这些努力，CrowdStrike 公司的股价仍然遭受重创。CrowdStrike 公司本可以采取哪些措施来避免这类事件发生？他们采取的哪些措施值得推荐？

下面是此次 CrowdStrike 引发的宕机事件中得出的 10 个重要教训。

1、确保开展严格的部署前测试

在软件发布到生产环境之前，开展严格的部署前测试，以识别和减轻潜在的漏洞影响是非常必要的。这一测试阶段涵盖各项全面评估，包括单元测试、集成测试、系统测试和用户验收测试。

此次 CrowdStrike 宕机事件凸显了开展全面部署前测试的必要性。导致大规模系统崩溃的猎鹰传感器更新中包含的逻辑错误，本可以通过更严格的测试来加以识别和纠正。此外，

在软件发布到生产环境之前，
开展严格的部署前测试，
以识别和减轻潜在的漏洞影响是非常必要的。
这一测试阶段涵盖各项全面评估，包括单元测试、
集成测试、系统测试和用户验收测试。

严格的测试程序可以模拟各种场景，包括边缘情况和压力条件，以保障软件在不同情况下的鲁棒性。

有效的部署前测试会在软件部署之前识别出错误的配置更新，从而避免用户遭受重大的运营中断。这种全面的测试方法不仅提高了软件的可靠性，还增强了用户的信任程度，并减少了昂贵的部署后修复费用和声誉受损风险。

2、优先考虑事件响应培训

事件响应培训在网络安全中至关重要，因为它使组织能够有效地处理和减轻安全事件带来的影响。这种培训为人员提供了必要的技能和知识，以迅速有效地应对各种网络威胁，如恶意软件攻击、数据泄露和系统中断。

这是 CrowdStrike 猎鹰平台做得好的一点，由于该公司对逻辑错误的快速识别和纠正，减少了系统遭受停机和负面影响的程度，这显示了有准备充分的事件响应团队的重要性。适当的事件响应培训涉及制定一个全面的事件响应计划、演练和随时掌握最新的威胁情报。

这些措施能够确保团队快速发现并处理威胁，减少组织遭受的潜在威胁。此外，事件响应培训培养了组织的安全意识和准备文化，鼓励采取积极的措施以防止事件的发生。培训还包括了沟通程序，确保在事件发生期间团队能告知并协调所有的利益相关者。

3、促进国际网络安全合作

由于网络威胁具有全球影响的属性，因此国际合作在网络安全中至关重要。网络攻击者通常不受国界影响，因此组织协调全球响应对于有效打击这些威胁至关重要。这种合作包括在国家和组织之间共享威胁情报、最佳实践和事件响应策略。

此次 CrowdStrike 宕机事件影响了全球系统。这些受影响组织之间的国际合作和信息共享，对迅速有效地解决这种全球问题至关重要，能够帮助不同国家的组织增强其整体的网络安全态势，提高其发现和应对威胁的能力，并降低网络事件造成的威胁风险。国际合作还促进了全球网络安全标准和框架的发展，促进了在安全实践方面的一致性和互操作性。

此外，研发团队的联手合作能够研究出应对新兴网络威胁的创新解决方案，进而使所有参与的国家受益。因为各国通力合作来应对共同挑战，这种协作方式还有助于建立信任和加强外交关系。总体而言，加强网络安全的国际合作对于为全球个体创造一个更安全的数字环境至关重要。

4、开展定期审计和测试

开展定期审计和测试是健全网络安全策略的关键组成部分。定期审计包括系统地审查和评估组织的安全政策、程序和控制措施，以识别弱点并确保符合行业标准和法规。

测试包括漏洞评估、渗透测试和安全扫描等活动，以在可疑漏洞被利用之前得到发现和解决。

此次 CrowdStrike 宕机事件显示了开展定期审计和测试的重要性。本可以通过更频繁和更彻底的测试程序来识别到导致系统崩溃的错误更新。通过开展定期审计和测试，组织可以识别并纠正安全漏洞，确保其系统的完整性，并维持高水平安全。

这些实践还有助于不断提高组织的网络安全态势，提升其抵抗网络威胁的韧性。此外，定期审计和测试促进形成了主动应对网络安全的方法，使组织能够领先于潜在威胁并降低数据泄露和业务中断的风险。

5、网络安全专业知识和资金

随着网络威胁变得越来越复杂，网络安全专业知识和资金的重要性不言而喻。熟练的网络安全专业人员对于开发、实施和管理有效的安全措施至关重要。充足的资金对于支持这些工作至关重要，能够允许组织投资于先进的安全技术、开展定期培训和随时获取最新的威胁情报。

此次 CrowdStrike 宕机事件，凸显了快速识别和纠正问题所需的高水平专业知识和资源。网络安全威胁的复杂性、管理及减轻这些威胁的复杂性，对网络安全专业知识和资金的投入增加，对开发健全的系统和防止类似事件再次发生至关重要。随着网络攻击的发生频率和复杂性增加，组织必须优先考虑组建和维护一支强大的网络安全工作队伍。

这不仅包括雇佣熟练的专业人员，还包括投资于对人员的持续教育和培训。充足的资金确保这些专业人员能够获得必要的工具和技术来有效地保护组织的资产。此外，一个资金充足的网络安全计划使组织能够实施全面的安全措施、开展定期审计和测试、制定健全的事件响应计划。

6、在效率与安全之间取得平衡

在当今快节奏的数字环境中，能够在效率与安全之间取得平衡至关重要。虽然运营效率对业务成功很重要，但不应以牺牲安全为代价。虽然快速部署各项更新很重要，但此次 CrowdStrike 宕机事件表明，优先考虑速度而不是彻底的安全检查可能会导致严重后果。

确保在追求效率的过程中不绕过或忽视安全措施，是防止漏洞不被网络攻击者利用的关键。这涉及执行已被无缝集成到组织工作流程中的安全程序和控制措施，使同时实现效率和强大的保护成为可能。

各组织应该培养一种安全被视为运营流程的基本要素而非障碍的文化。通过这样做，组织可以实现在保持高水平安全的同时高效运营的一种平衡。此外，定期审查和更新安全政策和程序能够确保这些政策和程序的有效性，并且确保其不会妨碍业务运营。

7、在事件期间保持透明沟通

有效和快速的沟通对于科技公司至关重要，尤其是在发生网络安全事件期间。及时的沟通能确保客户、员工和合作伙伴在内的所有利益相关者，都了解到事件情况以及处理步骤。

此次 CrowdStrike 宕机事件，凸显了快速和透明沟通的重要性，与客户的及时更新和清晰沟通有助于减轻事件影响，并指导客户完成补救措施。及时的沟通可以防止错误信息的传播、减少恐慌和维护信任。还能使所有人都意识到他们在减轻事件影响中承担的职责和责任，从而协同各方努力。

科技公司应该建立清晰的沟通程序和渠道，确保信息快速和准确地传播。这包括为不同类型的事件准备模板和指南，定期开展沟通演练，并更新所有利益相关者的最新联系名单。通过优先考虑快速沟通，科技公司可以增强其事件响应能力，降低安全事件的影响，并保护公司声誉。

8、分阶段推出更新

分阶段推出更新是管理新软件或系统变更部署的有效策略。通过分阶段发布更新，组织可以在全面部署更新之前观察小规模更新所带来的影响。这种方法能够较早地发现和解决问题，降低产生大规模宕机的风险。

此次 CrowdStrike 宕机事件，同时影响了很多系统，凸显了分阶段推出更新的潜在优势。如果分阶段部署更新，逻辑错误可能在影响大量系统之前就被识别和纠正。

分阶段推出更新还使组织能够从较小的用户群体中收集反馈，进而开

展改进和优化。这种方法不仅降低了主要问题的发生风险，还提高了软件的整体质量和可靠性。

采用多云策略（multi-cloud strategy）也可能有所帮助。这涉及使用多个云服务提供商来分配工作负载，降低停机时间和数据丢失风险。这种方法增强了冗余和韧性，确保如果一个服务商遭受服务中断，组织可以继续使用另一个服务商来运营。

> 通过反思 CrowdStrike 公司做得好的地方和可以改进的地方，组织可以加强自身的网络安全措施，防止类似的事件未来再次发生。

9、通过备份服务器和替代数据中心来确保业务连续性

备份服务器和替代数据中心是全面 IT 策略的关键组成部分，特别是对于那些严重依赖数字运营的企业。它们作为防止数据丢失和系统故障的保障措施，确保了业务连续性并减少停机时间。CrowdStrike 事件凸显了对于制定稳健的灾难恢复计划的需求，以快速恢复受影响的业务并减少对企业运营的影响。

备份服务器是用于存储关键数据和系统配置副本的专用服务器。它们的主要功能是在主系统遇到故障或数据损坏时提供恢复选项。定期备份能确保快速恢复近期的数据，降低因硬件故障、软件故障或网络攻击导致数据丢失的风险。可以配置备份服务器使其自动优化存储空间的使用并加快恢复时间。

替代数据中心是企业可以复制其 IT 基础设施和数据的备用设施。它们通过在地理位置不同的地点托管主要数据和应用程序的副本来提供额外的保护。在发生如自然灾害或重大技术故障等灾难的情况下，业务运营可以切换至替代数据中心，确保服务正常运营、数据保持完整。

10、自动化日常 IT 流程，将人为错误降至最低

将备份、更新和系统监控等日常 IT 任务进行自动化处理，对于保证效率和可靠性至关重要。自动化可以帮助将人为因素导致的错误最小化。例如，那些可能导致此次 CrowdStrike 更新中逻辑缺陷的错误。通过将日常 IT 流程自动化处理，组织可以确保更加一致和可靠地开展系统管理。

自动化系统降低了人为错误的可能性，确保流程的一致性，并使 IT 人员能专注于更有战略性的任务。例如，自动化备份解决方案可以安排并执行定期备份，无需人员手动干预，确保了备份的及时性和全面性。同样地，自动化工具可以管理更新和补丁安装，无需持续监督即可保障系统的安全性和及时更新。

有效的网络安全流程和措施本可以显著减轻此次 CrowdStrike 宕机事件带来的影响。在大规模部署之前定期开展测试更新，可能会较早地识别出有缺陷的更新。实施我们已经讨论过的其他推荐做法也能阻止我们现在面临的状况。

重要的是要承认并非一切事情都是负面的。CrowdStrike 公司在事件响应和快速沟通方面处理得非常好。希望这一事件可以作为一个经验教训，提醒企业优先考虑网络安全，因为即使是小问题也可能产生重大的连锁反应。通过反思 CrowdStrike 公司做得好的地方和可以改进的地方，组织可以加强自身的网络安全措施，防止类似的事件未来再次发生。

奇安信终端产品为何不会引发类 CrowdStrike 事故?

作者　任润波

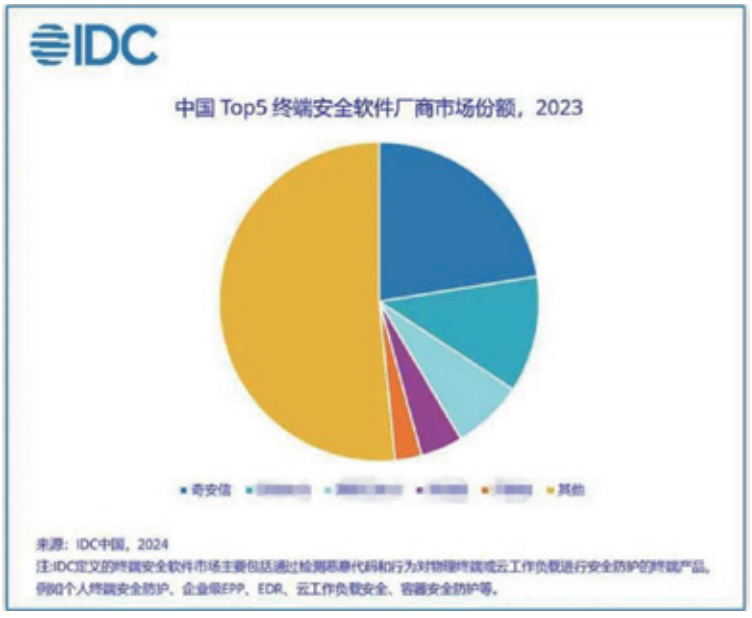
一次终端安全软件的更新引发全球 IT 事故，提醒了业界和广大用户，即使是非常成熟的技术平台也可能遭遇意外故障。“此次 Windows 全球蓝屏事故给我们带来的最大启示是，质量是安全软件的底线和红线。”奇安信集团副总裁、终端安全负责人张庭第一时间表示。

蓝屏事件发生后，从奇安信 XLab 实验室等独有数据视野观测到，国内 CrowdStrike 软件装机量在万级，受影响的主要是北上广深等发达地区的外企、外企在华分支机构及合资企业。由于 CrowdStrike 在中国市场的渗透率不高，特别是党政央企、大型的民企公司使用量极少，因此，此次事件并没有显著影响到国内的企业和机构组织。

国内企业在应用终端产品时，奇安信终端安全管理系统（天擎）无疑是头部选项。IDC 数据显示，2023 年奇安信终端产品正以 22.48% 的份额继续扩大该领域的市场优势。奇安信终端安全产品已连续 6 年稳居 IDC《中国 IT 安全软件市场跟踪报告》领头羊地位，多年蝉联赛迪顾问《中国网络信息安全市场研究年度报告》终端安全产品市场榜首。

在奇安信参与的 2017 年永恒之蓝应急处理、2022 年北京冬奥“零事故”安全保障，以及其他国家级 / 世界级重大活动网络安全保障工作中，均未出现过勒索和蓝屏事故，核心业务都没有受到中断影响。数次实战检验表明，奇安信终端产品能够在极端的复杂环境和严苛的安全要求下，确保系统的稳定运行和数据的安全保护。

作为国内领先的终端安全管理软件，奇安信天擎（终端安全管理系统）



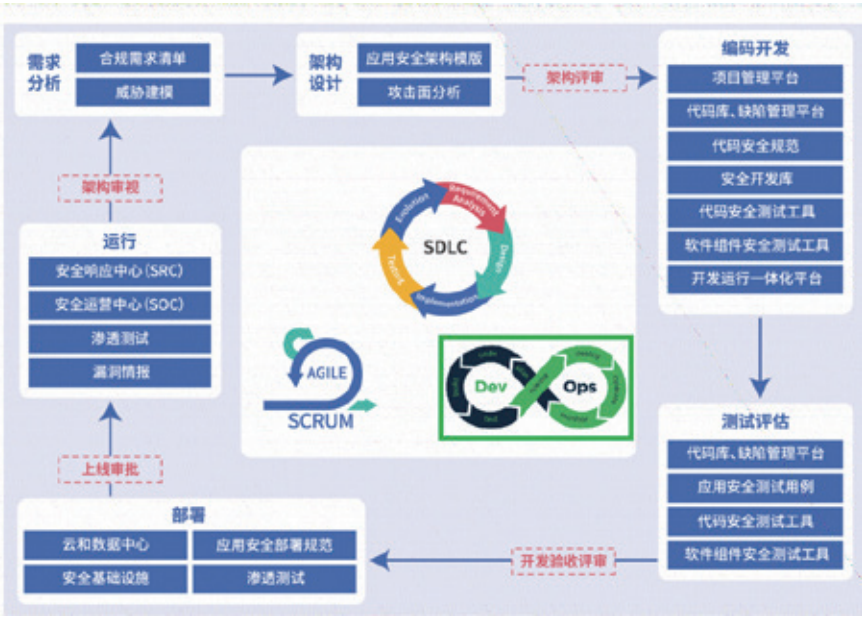


图 奇安信 SDLC 流程图

坚持“安全第一”的核心哲学，始终遵循严格的质量管理体系，从架构设计、产品开发、安全测试到灰度发布，每一步都将“零事故”保障（业务不中断、数据不出事、合规不踩线）作为执行标准，保障产品的质量、安全及用户满意度。

开发流程：践行全链路、端到端的安全检查

奇安信终端安全管理系统（天擎）参考安全开发生命周期（SDLC）、软件保证成熟度模型（OpenSAMM）、开发安全运维一体化（DevSecOps）等软件安全开发实践，构建了奇安信的软件安全开发体系，不仅提升了软件的稳定性和安全性，还保障了功能的完整性和可靠性，为用户带来了更加平滑和无忧的使用体验。

奇安信的软件安全开发体系覆盖安全需求、安全设计、安全开发、安全测试和安全部署运维等各阶段工作。

· **业务需求阶段，**通过产品方案评审，确保安全需求被明确纳入产品规划之中。这一阶段不仅考虑产品的功能需求，还特别关注安全需求，包括合规性要求、数据保护策略及用户隐私保护等方面，从而在源头上奠定坚实的安全基础。

· **技术方案评审阶段，**技术团队会对设计方案进行全面的安全评估，确保采用的安全技术和架构能够抵御潜在的安全威胁。这一阶段还涉及威胁建模和攻击面分析，以便识别和缓解潜在的安全风险点。

· **编码开发阶段，**通过严格执行代码安全规范，利用安全开发库和工具，如代码安全测试工具和软件组件安全测试工具，确保代码的质量和安全性。应用项目管理平台跟踪和管理开发进度，保证项目按照既定的安全标准进行。

· **测试评估阶段，**通过 QA 全面测试，包括自动化测试和人工测试相结合的方式，确保软件在不同环境下都能达到预期的安全性能。此外，通过安全响应中心 (SRC) 和安全运营中心 (SOC) 监测运行时的安全状况，及时发现并响应安全事件。

· **产品部署阶段，**应用程序签名验证技术确保软件的真实性和完整性，防止未经授权的修改。同时，通过内部研发流程管理确保整个流程的一致性和可追溯性，使安全成为产品的一部分，而非事后附加。

在全新的奇安信软件安全开发体系的指引下，产品研发从业务需求到产品交付实施，实现全链路、端到端的安全检查，整个流程确保产品安全防护能力不断提升，为软件植入安全“基因”。

架构设计：极致安全、更高可靠

奇安信天擎部署架构具有更强的安全性、更高的可靠性及非凡的性能表现。技术完全自主可控，对系统进行了强化设计及全面的安全性评估；产品支持云原生和微服务的部署架构，

关键组件服务支持高可用性（HA）。

奇安信天擎终端采用多进程结构，多同业务进程运行相互隔离，保障关键核心进程稳定运行，避免一个问题引起所有业务进程雪崩的现象发生；设置了“连续蓝屏异常自智能避机制”，驱动程序在遇到特殊兼容性问题时，如果连续多次蓝屏，驱动会智能识别此类场景，并做应急规避，暂停驱动加载，以优先保障系统业务进行。

当极端案例出现，例如，天擎大面积出现严重故障，常规手段无法令天擎恢复正常时，可启用“急救通道”修复方案。只要客户端和服务端仍可通信，客户端的文件系统运行正常，小助手进程仍可运行，即使操作系统无法接收鼠标键盘等外部输入、无显示器的图像输出，该方案通常也能正常执行，并且运行时不会受到其他业务功能的干扰。相对于常规版本升级的修复方式，急救通道具有更好的时效性，管理员可以快速解决终端出现重大 / 极端问题，急救通道具有完善的校验机制，不会被第三方恶意利用。

测试体系：专业全面，强化安全防御力

软件发布之前，天擎采用了一套专业而全面的测试体系，以及模拟各

种恶意攻击手段的高效安全测试。这确保了软件在实际使用中能够稳定且高效运行，并有效地防御潜在的安全威胁，为用户的数据和隐私提供了坚强而可靠的保护。包括但不限于以下测试：

· **单元测试，**通过伪造、打桩、交互测试的方式进行校验；

· **性能测试，**监控客户端资源占用、服务端资源占用、服务端接口性能情况，包括 CPU 占用、内存占用、磁盘 IO，页面错误等；

· **稳定性测试，**监控客户端及服务端的运行情况，客户端至少运行 7*24 小时，服务端运行时长超过 30 天，确保系统无蓝屏、卡死、重启等异常；

· **兼容性测试，**对各终端操作系统、服务器系统、主流浏览器、硬件设备、主流软件，以及不同版本进行兼容性测试。

……

这一系列举措不仅强化了软件的稳定性和性能，还极大地提升了用户体验，让用户在不同环境下都能享受流畅、安全的软件服务。

灰度升级：自动化编排，保障用户稳定体验

灰度升级即从局部开始，先针对少量终端优先升级，通过观察一段时间稳定性后，再自动对全网终端升级，以降低升级新版本可能引入的问题风险，可最大程度减少升级后程序 bug 引起的后果。

张庭表示，在产品升级时，一定要控制影响范围，俗称“爆炸半径”，掌控好升级策略，确保灰度升级，控制放量节奏，逐步测试、逐步增加覆盖，从而最大程度控制意外问题导致的风险范围。奇安信引入了一项先进的终端设备灰度发布自动化编排机制，这使得根据不同的版本和员工群体，软件能够在灰度环境中自动化地进行分批发布。

> 奇安信天擎终端采用多进程结构，
> 多同业务进程运行相互隔离，
> 保障关键核心进程稳定运行，
> 避免一个问题引起所有业务进程雪崩的现象发生。

奇安信更新终端程序，依次遵循内部生产环境验证、小批量用户测试、正式发布阶段三个流程。简单来说，在新功能开发测试完成后，会先在奇安信内部近 2 万台终端的正式环境中更新；版本稳定后，将选取小批量有直接需求的用户，在其终端测试环境中进行试用；经过相应调整，最后才会对外正式发布，用户可以配置升级时间。

此外，由于奇安信天擎病毒库每日更新，同样设置了针对库的灰度放量规则，以避免升级新库可能引入问题的风险。

该灰度发布自动化编排机制不仅确保了新版本软件在上市前能够得到充分的测试，而且为用户提供了更加及时、稳定的更新体验。

在信息安全领域，每一次的挑战都考验着技术团队的专业能力和应对策略。奇安信作为新一代网络安全的领军者，在终端安全产品研发、测试、部署、升级等一套流程机制中，始终秉持着“步步为营”的严谨设计态度，确保每一环节都达到最高标准的安全防护效果，才能在复杂的网络环境中真正为用户提供坚实的安全保障。安

奇安信

奇安信威胁情报中心

中国威胁情报行业领军者

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

威胁情报中心

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

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

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

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

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

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

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

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

揭秘：网络活动操纵各国大选

作者　裴智勇

随着网络空间“形态”的持续进化，简单的窃取或破坏已经无法满足攻击者的欲望和野心。网络战又进化出了一种新的形态——社会认知和政治生态攻击、破坏和诱导。其中最为典型的就是利用各种网络攻击手段，对各国大选活动干预和操纵。

近期，美国总统竞选团队成为网络攻击的目标。2024 年 8 月 12 日，埃隆 · 马斯克与前总统唐纳德 · 特朗普的直播连麦助选活动遭遇网络狙击，波次多、时间长，僵尸网络攻击致特朗普直播中断 40 分钟。

至此，利用网络战操纵各国政治的问题再次受到各国政治家和网络安全工作者的高度关注。

本文结合《安全内参》近两年来收录的公开新闻信息，介绍近年来比较典型的，利用网络战操纵各国政治和大选的案例总结。

一、希拉里“邮件门”事件将特朗普送上王座

马斯克与特朗普连麦直播被干扰推迟的事件，只能算是针对美国大选的一次小型狙击战，可能并不会真正影响大选的走势和最终结果。但这并不意味着网络战没有能力改变政治的走向。

要说迄今为止哪一次网络战事件对政治走向产生过决定性的影响，“希拉里邮件门事件”肯定当之无愧排名第一。这一事件直接改变了美国大选的结果，其直接受益者正是美国第 45 任总统唐纳德 · 特朗普。

希拉里邮件门事件要从 2009 年至 2013 年说起。根据 FBI 的调查显示，希拉里担任美国国务卿的这段时间里，使用私人电子邮箱和位于家中的私人服务器收发公务邮件，其中包括一些涉及国家机密的绝密邮件。这批邮件一共约 6 万封。此事于 2015 年 3 月被曝出。2015 年 7 月，美国联邦调查

局 FBI 启动了对此事调查程序。

但是，在 FBI 的调查工作开启之前，即将被调查的 6 万封邮件中，就有 3 万多封已经被希拉里团队以涉及私人生活为由删除了，只剩下另外约 3 万封邮件可供调查。此事被媒体披露后，引发了公众对希拉里更多的质疑。不过，当时还远未到美国大选的关键时刻，此事件对希拉里即将参加的美国总统大选的影响甚微。

然而，事态在 2016 年 7 月，也就是美国总统大选最为热闹、最为激烈的关键时刻，却发生了急剧的变化。自 2016 年 7 月 23 日起，维基解密逐步公开了与民主党全国委员会（DNC）有关的 19,252 封电子邮件及 8034 份邮件附件，这些邮件主要是 2015 年 1 月 ~2016 年 5 月，DNC 高级职员间往来的电子邮件，涉及的账户主要包括民主党的一些高层官员，如通信主管、国家财务主管、财务负责人、数据与战略行动部的财务主管等。事件发酵后，有多名希拉里团队的高级官员引咎辞职。

2016 年 8 月 12 日，此前声称对 DNC 遭黑客攻击事件负责的黑客组织 Guccifer 2.0 也再次放出大量机密文件，涉及美国民主党国会竞选委员会（DCCC）的大量数据。

实际上，这些 DNC 泄漏出来的邮件主要揭示了这样一个问题：早在 2016 年 2 月民主党内初选开始前，DNC 就已经开始暗中支持希拉里争夺党内提名，同时排挤希拉里在党内的最大竞争对手伯尼 · 桑德斯。此外，邮件内容还显示了希拉里竞选团队操纵媒体、涉嫌洗钱、有意抹黑特朗普等党内丑闻，此事引起美国政坛的巨大震动。

DNC 邮件泄露事件把希拉里邮件门推向了高潮。事件持续发酵并对美国社会和大选舆情产生了微妙的影响，最终使本来民调一直相对领先的希拉里在最后关头败下阵来。特朗普成功当选美国总统。

二、特朗普竞选团队被黑，2016 历史重演?

2024 年 8 月 10 日，美国前总统唐纳德 · 特朗普的竞选团队确认，其部分内部通信资料已被黑客获取。此前，外媒 POLITICO 陆续收到来自一个匿名账号发送的电子邮件，其中包含了特朗普竞选团队内部的文件。

特朗普竞选团队引用微软发布的一份报告的说法，将此归咎于“对美国怀有敌意的外国势力”。该报告称，“伊朗黑客在 2024 年 6 月向一名美国总统竞选团队的高级官员发送了一封鱼叉式网络钓鱼邮件。”

特朗普竞选团队发言人 Steven Cheung 表示，“这些文件是从对美国怀有敌意的外国势力那里非法获取

近期，美国总统竞选团队成为网络攻击的目标。2024 年 8 月 12 日，埃隆 · 马斯克与前总统唐纳德 · 特朗普的直播连麦助选活动遭遇网络狙击，波次多、时间长，僵尸网络攻击致特朗普直播中断 40 分钟。

的。他们意图干扰 2024 年大选，并在我们的民主进程中制造混乱。8 月 9 日，微软的一份新报告发现，2024 年 6 月，伊朗黑客入侵了美国总统竞选中一名‘高级官员’的账号，这与特朗普总统选择副总统候选人的时间接近。”

据 POLITICO 介绍，7 月 22 日，他们开始收到来自一个匿名账号的电子邮件。在过去几周里，发件人使用了一个 AOL 电子邮件账号，并仅以“Robert”的身份出现，传达了看似来自特朗普竞选团队高级官员的内部通信。

文件中包括竞选团队对特朗普的竞选搭档、俄亥俄州参议员 J.D. 万斯进行的研究档案，档案日期为 2 月 23 日。两位熟悉这些文件的人士指出，这些文件是真实的。POLITICO 向他们保证，他们对内部通信的描述将匿名发布。其中一人将认为这卷档案是万斯审查档案的初步版本。

这份基于公开可用信息的研究档案长达 271 页，涉及万斯过去的记录和声明。匿名账号还发送了部分关于佛罗里达州参议员马可 · 鲁比奥的研究文件，鲁比奥也是副总统候选人的最终入围者之一。

尽管黑客所获取信息的范围尚不清楚。但这说明特朗普竞选团队出现了重大安全漏洞。

美国东部时间 2024 年 8 月 12 日晚 8 时（北京时间 13 日上午 8 时），埃隆 · 马斯克将对第 60 届美国总统大选候选人唐纳德 · 特朗普进行一次连麦直播访谈，并在 X 平台上通过马斯克和特朗普的个人账号进行现场直播。然而，当直播时间开始用户访问两人

特朗普与马斯克直播连麦

的直播间时，系统却提示“此直播间不可用”。直至 40 多分钟后，直播平台才恢复正常。

调查显示，这次直播延时事故，并非简单的技术故障，而是一次有针对性的网络攻击活动。访谈结束后，马斯克在其 X 平台账号上发文，称 X 平台遭受了大规模的 DDoS 攻击。

对于马斯克关于 X 平台遭到 DDoS 攻击的说法，英国路透社与美国有线电视新闻网（CNN）持谨慎的态度，认为目前尚不清楚马斯克所说的“攻击”是否真的有幕后黑手，或仅仅是因为听众过多所造成的。

网络安全公司 Check Point Software 的实时网络威胁地图未记录到异常活动。NetScout 的实时 DDoS 地图也仅记录到针对美国的小规模攻击。

正当西方媒体和安全公司纷纷对马斯克提出质疑之时，来自中国奇安信集团旗下的一个同样以 X 命名的实验室 XLab（X 实验室），却在第一时间对 X 平台遭 DDoS 攻击事件予以了确认，并公布了部分关键证据。XLab 的大网威胁感知系统于第一时间捕获了本次针对 X 平台的攻击活动。

XLab 发现：有 4 个 Mirai 僵尸网络主控参与了此次攻击。另外，还有其他攻击团伙使用反射攻击、HTTP 代理攻击等方式也参与了此次攻击事件。监测显示，4 个僵尸网络主控发动了至少 34 波 DDoS 攻击。4 台控制服务器主要集中在英国（2 个）、德国（1 个）、加拿大（1 个）。攻击时间从北京时间 8 点 37 分持续到 9 点 28 分，攻击时长 50 分钟，这与访谈延迟时间基本吻合。

XLab 的进一步分析指出：攻击时间特别长，这是本次攻击呈现出的一个显著特点。统计显示，绝大多数的 DDoS 攻击，持续时间在几分钟以内，有些甚至短到几秒钟，仍然可以给目标系统造成巨大伤害。但本次攻击持续时间长达近一小时，如此之长的攻击时间，表明攻击者明显有备而来，针对性极强。

据悉，为 X 平台提供安全服务的 Cloudflare 公司的相关负责人已经与奇安信 XLab 取得联系，希望协助提

供威胁情报信息以协助溯源。

三、网络虚假信息干扰非洲多国大选

2024 年，18 个非洲国家准备进行大选。与此同时，针对非洲国家和驻非洲国际组织的网络虚假信息攻击正在急剧上升，网络安全专家们亟需寻求解决方案，来应对这一不断加剧的问题。

根据美国国防部下属学术机构国防大学非洲战略研究中心的数据，2023 年，非洲至少发生了 189 起有记录的虚假信息攻击活动，这一数字是前一年的四倍。英国杂志《经济学人》报道称，2024 年，至少有 18 个非洲国家将举行大选。对于依赖经济稳定的现有政府和企业来说，虚假信息已经成为主要威胁。

非洲战略研究中心研究助理 Mark Duerksen 指出，随着这些威胁的扩散，网络安全专家需要探讨保护策略，但不能期望通过单一解决方案解决所有问题。

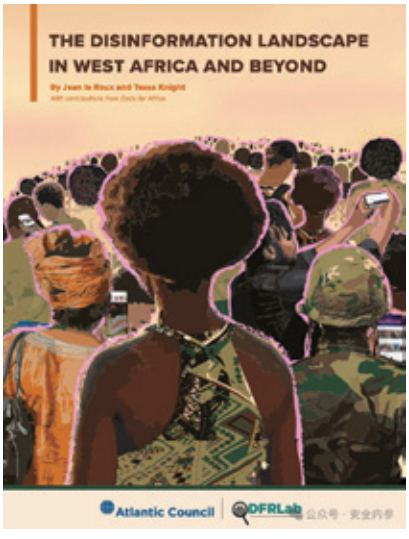
Duerksen 表示：“虚假信息不仅是技术问题，更是社会和政治问题。我们需要采取多层次的应对措施来增强韧性。因此，网络专家的工作只能是解决方案的一部分。然而，虚假信息攻击活动正日趋复杂，它们利用网络攻击来放大、洗白和煽动虚假信息。”

2024 年，预计将有超过 50 个非洲国家在不同程度上会继续提升和改进其网络安全水平。例如，拉各斯大学和肯尼亚女性网络安全机构 Shehacks Ke 等组织，致力于提升该地区的网络安全人才水平。然而，许多非洲国家在网络安全方面仍然相对落后。

根据非洲战略研究中心的最新报告，虽然全球都面临虚假信息问题，但非洲同时面临来自外国和国内的虚假信息双重打击。报告显示，外国政府主导了大部分针对非洲的虚假信息攻击活动。2023 年，约 60% 的攻击活动归咎于俄罗斯、阿联酋、沙特阿拉伯和卡塔尔。

大西洋理事会旗下的数字取证研究实验室（DFRLab）的报告显示，在 23 起针对某个非洲国家的攻击活动中，有 16 起来自与俄罗斯有关的团体。特别是法国从马里和其他萨赫勒国家撤军后，非洲国家面临的 189 次攻击活动大多数得到了俄罗斯的幕后支持。

报告引用了俄乌战争作为例证。Duerksen 表示，当时，一些尼日利亚记者的社交媒体账户被黑客攻击，用于传播亲普京的标签和虚假信息，制造出非洲支持俄罗斯的假象。



DFRLab 报告：西非及其他地区的虚假信息景观

当前，非洲有 6 亿互联网用户，其中 4 亿是活跃的社交媒体用户。非洲公民是全球最热衷于社交媒体的用户之一，尤其是尼日利亚和肯尼亚的用户在社交媒体上花费的时间最长。根据大西洋理事会 /DFRLab 的报告，非洲国家的互联网普及率不同，中非共和国的普及率最低，仅为 7%，而尼日利亚的普及率最高，达到了 51%。

2024 年年初，卡内基国际和平基金会发布了题为《有效对抗虚假信息：基于证据的政策指南》的报告，指出要保护公民和企业免受虚假信息攻击，需要采取一系列措施，包括支持本地新闻和媒体素养、提高选举的网络安全，以及检测、报告和移除不真实的社交媒体用户。

四、AI 伪造虚假信息干扰各国大选

2024 年 1 月，南亚研究通讯发表文章认为：孟加拉国大选明显受到 AI 虚假信息和深度伪造视频的影响，尤其体现在时任总理谢赫 · 哈西娜和反对党孟加拉国民党之间的激烈斗争中。

在科技治理和内容管控过程中，与 AI 工具滥用等技术性问题相比，孟加拉国在治理过程中更面临如何管控跨国平台和外国科技公司的挑战。由于本国市场规模小，监管能力不足，美国网络平台往往对孟加拉政府的管控要求置若罔闻，而美国科技公司利用 AI 工具低成本生成的虚假内容则持续影响孟加拉的国内选举，凸显出南方国家在网络与科技治理方面的困境，也同时为科技大国介入别国政治提供了抓手。

孟加拉国前总理谢赫 · 哈西娜

2023 年年底至 2024 年年初，随着南亚多国选举临近，使用 AI 生成虚假信息的问题日益严重。全世界的决策者都在担忧，AI 生成的虚假信息将在选举前被用来误导选民、煽动分裂。在孟加拉国，上述隐忧已经成为现实。

2024 年 1 月初，这个拥有 1.7 亿人口的南亚国家举行了全国大选，时任孟加拉国总理谢赫 · 哈西娜（Sheikh Hasina）与反对党孟加拉国民族主义党（Bangladesh Nationalist party）展开激烈的权力争夺。在选举前的几个月里，孟加拉国内亲政府新闻媒体与意见领袖一直在大肆宣发由人工智能初创公司所提供的廉价 AI 工具制作的虚假信息。

在一段所谓的“新闻片段”中，一名由 AI 生成的主播大肆批评美国，而哈西娜政府曾在选举前对美国表示不满。另一段已被删除的深度伪造视频显示，一名反对党领导人在巴以问题上含糊其辞，而这种模糊态度在这个穆斯林占多数的国家可能招致毁灭性的结果，毕竟公众对巴勒斯坦人抱有强烈的同情。

在孟加拉国，虚假信息加剧了 1 月大选前的紧张政治气氛，数以千计的反对派领导人与活动人士被逮捕，这也促使美国公开向孟政府施压，以保证选举的自由公平性质。正是在这样的背景下，AI 制造的深度伪造视频登场了。

在线新闻网站“BD Politico”于 2023 年 9 月在推特（现“X”网站）上发布了一段视频，该网站“世界新闻”栏目的一名新闻主播在演播室播放了一段视频，指责美国外交官企图干预孟加拉国的选举并且制造政治暴力，视频中间还穿插了骚乱现场的画面。

该视频由洛杉矶一家名为“数字人”（HeyGen）的人工智能视频生成公司制作。在“数字人”的宣传内容中，可以看到一个名为“爱德华”（Edward）的主播，这是可供该平台用户使用的数个 AI 主播形象之一。这些虚拟主播皆是由真实演员形象生成的。目前 X 网站、BD Politico 和“数字人”均未回应置评请求。

另外一个例子，在 Facebook 上发布的针对反对派的深度伪造视频，其中一个视频谎称是孟加拉民族主义党（BNP）领袖塔里克 · 拉赫曼 (Tariq Rahman) 录制的视频。视频中的拉赫曼建议 BNP 对加沙问题“保持沉默”，以免得罪美国。全球科技研究所（Tech Global Institute）和媒体非盈利组织“Witness”均认为，这段内容很有可能是 AI 生成的深伪视频。

孟加拉民族主义官员瓦希杜扎曼（AKM Wahiduzzaman）表示，他的所属党派要求 Facebook 移除此类内容，但该平台“大多数时候不屑一顾”。在《金融时报》（FT）联系 Facebook 要求其置评之后，Facebook 火速删除了这些视频。

另一个广为传播的深度伪造视频

由总部位于特拉维夫的人工智能视频平台 D-ID 制作，该视频声称孟加拉民族主义青年团领袖拉舍德·伊克巴尔·汗（Rashed Iqbal Khan）谎报了年龄。全球科技研究所鉴定称，该视频旨在抹黑拉舍德的信誉。

人工智能生成的内容在斯洛伐克的议会选举、阿根廷总统选举中带来重大的影响。

2023 年 9 月，基于生成式人工智能的政治干预，破坏了斯洛伐克的议会选举。在选民投票前两天，一段带有生成内容标记的音频在社交媒体上广泛传播，该选举影响到斯洛伐克对乌克兰的军事援助和对北约的支持。据悉，这段音频中出现了亲北约的斯洛伐克进步党领导人 Michal Šimečka 和一名记者的声音，他们在讨论如何操纵选举并从该国少数民族罗姆人手中购买选票。

在斯洛伐克等国，媒体封锁限制了新闻界在选举前讨论与竞选相关的内容，这对揭穿病毒式传播的内容构成了明显的挑战。

人工智能生成的内容在阿根廷 2023 年总统选举中也发挥了意想不到的作用。第一轮投票前几天，网上开始广泛流传丑闻录音。据称，这些录音中，时任总统候选人帕特里夏·布尔里奇的经济部长人选卡洛斯·梅尔科尼对女性恶语相向，并以政府职位换取性好处。

这一事件被称为“梅尔科尼门”。这些音频片段是否真的是人工智能生成的深度伪造，还有待证实。不过，这一事件凸显出，即使是人工智能生成的潜在内容，也能以意想不到的方式塑造选举竞争的轮廓。

2024 年 5 月 9 日，瑞士日内瓦安全政策中心（GCSP）网络安全部门负责人加兹门德·胡斯卡伊（Gazmend Huskaj）撰文《未来选举与人工智能驱动的虚假信息》。

文章总结了人工智能驱动的虚假信息行动，影响政治和选举活动的九种策略。所有这些滥用 AI 干预政治的方法都非常值得警惕。具体如下。

具体策略	具体方法
传播“热爱”情绪	传播虚假的积极信息，如强烈亲和力、忠诚度或爱国主义内容，营造一种联系或忠诚感
传播“仇恨”情绪	煽动对特定群体、种族或国家的仇恨或愤怒。包括散布虚假信息以加剧种族紧张局势或制造敌意
传播“恐惧”情绪	传播可引发恐惧或恐慌的虚假信息。如散布夸大威胁或捏造危机的谣言
传播“骄傲和自负”情绪	奉承或抬高目标群体自尊心的网络活动。虚假信息被用于使一个群体自感优越，操纵其感知和行动
传播“沮丧和自我贬低”情绪	传播虚假信息以削弱目标群体的信心或自尊。通常涉及散布贬低或羞辱目标群体的虚假叙述
传播“徒劳”情绪	散布虚假信息，让目标受众觉得反抗或异议是徒劳的，助长了对某些问题或行动的绝望或冷漠情绪
持续审问	在各种平台上反复传播相同的虚假信息或叙事
快速打击	用大量虚假信息快速轰炸受众，旨在混淆视听
假借名义	伪装成不同的实体或团体开展网络行动，旨在误导信息来源或诋毁被冒名的实体

五、结语

由于网络本身已经渗透至我们生

活的方方面面，利用网络进行思想控制、舆论干预、甚至是操纵选举的行为也越来越多。随着攻击手段、操纵方法的日渐成熟，网络空间必将成为所有大型选举活动的“兵家必争之地”。

未来，不论是在发达国家还是发展中国家，网络战之于选举活动，都呈现出以下几点明显的趋势。

1、针对选举活动的窃密是长期的、持续的

针对选举参与者及其团队、政党的网络窃密活动将会是长期的、持续的。被窃取的信息有很大概率被作为“撒手锏”，在关键时刻被用来舆论造势或暗中威胁。同时，如果参选者不能得到国家级的网络安全防御能力，那么其使用的信息系统被内外势力渗透成“筛子”，将是必然的。在未来的“西式”选举中，双方可能都不会再有什么真正的“秘密”。网络空间中的“水门事件”将会无时无刻、永不停息的发生。

2、虚假信息将成为各国选举活动的最大威胁

虚假信息本就是充斥在西式选举活动中的毒瘤。但随着社交网络逐渐深入人心、AI 语音与视频深度伪造技术日渐成熟和民用化，虚假信息的生产效率、制作品质和传播速度，都有可能陷入完全失控的状态，从而使选举活动本身更加“闹剧化”，民主和公平不再是“理所当然”的结果，信任危机、社会分裂都有可能因此加剧，最终给国家的发展和稳定带来不可逆的持续性伤害，直接危及国家安全。

3、针对选举活动的直接网络攻击将越发频繁

> 网络本身已经渗透至我们生活的方方面面，利用网络进行思想控制、舆论干预、甚至是操纵选举的行为也越来越多。

从目前的实践效果来看，无论是对助选演讲活动的网络袭击，还是对投票过程的网络攻击，对选举结果本身的影响，远不及“数据窃密”或“虚假信息”的传播，但这类攻击活动却很可能成为各类极端人士或组织对特定目标发泄不满的方法，也很可能成为境外敌对势力进行袭扰的“常规操作”。未来，一个国家元首的选举活动，会成为这个国家最需要网络安全保障的大型活动。

4、网络战组织将很快成为选举黑产成熟业态

通过网络战活动干预选举结果的方法已初步被证实是有效的，未来，无论是大国还是小国，无论是参选的政党、组织还是个人，可能都会迫不得已的拿起网络武器参与选举大战，由此必将催生出无数的，如“乔治小组”之类的，包装成“助选科技”公司的网络组织。这些组织在本质上就是一种以干预、操纵选举为目的的新型网络黑产。这种黑产也将迅速的进化为成熟业态。安

从“零基础”到全优，某医药巨头网络安全的跃迁之路

作者　张少波

某医药公司系世界 500 强直属企业，是一家以药品分销为核心的全国性现代医药供应链服务企业，经营规模超 2000 亿，经营中心网络遍布全国 25 个省市，覆盖全国 7 万多家终端医疗机构。

随着规模的不断扩大，该医药公司的业务范围已经覆盖分销、零售、贸易、物流等多个领域。与此同时，公司在加速数字化转型的过程中，对外信息服务平台规模和数据量更加庞大，随之带来了日益突出的网络攻击、业务中断、数据泄露等威胁。如何发现潜在风险、防范未知威胁，保障全集团加速推进数字化转型，成为该医药公司亟待解决的问题。

医药安全关乎健康生命，安全运营能力亟待提升

“公司作为健康事业‘国家队’，在不断推进全国战略、深化服务创新、加快产业突破的同时，也同样面临数字化转型时代的新型网络安全威胁。集团需与时俱进，一方面需要提升自身员工的安全意识能力，做好应对现代网络攻击战的准备；另一方面也要“打铁还需自身硬”，全方面提升集团的整体安全运营能力，将公司潜在的网络安全威胁降到最低，为客户提供更安全的健康服务。”该医药公司网络安全相关负责人表示。

纵观近些年国内外新闻曝光的多起网络安全攻击事件，可以看到，攻击者具有很强的专业性，使用的攻击手法尤为成熟，攻击策略也较为先进。而该医药公司在对抗网络攻击中存在多方面薄弱点，缺乏完善的体系化的技术应对能力。2017 年以前，整个集团只有终端安全的病毒防护能力，且防护较分散，难以做到全面的终端一体化管理，面对肆虐的勒索病毒攻击，

往往力不从心，更不用说更高维度的威胁监测及资产安全运营了。

同时，医药行业属于知识密集型、资产密集型和数据密集型行业，对于数字化系统依赖度很高，因此网络安全对公司医药业务的保障作用就显得至关重要，主要表现在以下几个方面。

首先，高价值的数据，往往容易成为攻击者的目标。医药企业往往拥有价值数十亿美元的数据，通常包括机密知识产权、药物进步和技术的研发数据、药物和开发的专有信息，以及患者和临床试验数据。访问此类关键和敏感信息，使制药行业成为网络犯罪分子极具吸引力的目标。不久前，印度制药巨头阿尔肯实验室（Alkem Laboratories）证实发生一起网络安全事件，导致旗下一家子公司向欺诈分子转账 5.2 亿卢比（约合人民币 4500 万元）。

其次，医药行业关乎社会民生，甚至公民的健康和生命，数字化平台的容错空间极小。“对于很多重危急病患者，医药的及时配送，就是和病魔在赛跑。”相关负责人表示，全市数千家的大大小小医院、卫生院、诊所等，都依赖于公司去配送药品，一旦公司系统遭到破坏，不能及时送药，轻则影响患者正常治疗，重则关乎危重患者的生命。例如 2020 年 9 月，德国杜塞尔多夫的一家医院遭勒索软件攻击，导致一位紧急入院病人在被迫转院途中耽误救治时间而亡。

最后是公司的庞大规模和快速发展的业务，其安全风险也是指数级攀升。公司以全国性的终端网络为基础，着力推进医院供应链服务，发展“新分销新零售”，构建新产业优势。庞大规模和多元化的业务模式，使得数字化系统也非常复杂和开放，这就带来了更多的暴露面和风险敞口，一旦某个分支机构被单点攻破，就可能影响整个集团系统，这对于医药公司是个严峻的安全挑战。

从终端切入到全局安全运营，集团总部率先取得成效

罗马不是一天建成的。面对纷繁复杂、防护孱弱的全集团网络安全状况，该从哪个切口入手？该医药公司给出的答案是：终端。

据介绍，在 2017 年的时候，集团经常遇到病毒的侵扰，由于集团终端量大，分布于不同的办公区，总部所有省区终端的安全状况，分部来总部的时候终端可以直接连上总部内部网络，存在很大的风险。现有的防病毒软件远远无法满足需求。

就在一筹莫展之际，奇安信走进了该医药公司的视野。尤其是奇安信天擎（终端安全管理系统）具有的病毒防护、补丁管理、终端管控、终端审计、勒索防护等功能，可以解决终端资产不清、防护能力薄弱等紧迫问题，获得了该医药公司的认可。

天擎和传统防病毒软件具有的最大不同在于，它充分体现了管理和运营的理念，它通过搭建一套集中统一的计算机终端安全管理平台，增强计算机终端面对复杂的新型威胁防护能力，真正实现终端的数字化安全运营。

终端安全建设的第一阶段围绕集团上海总部，截止到 2022 年，上海总

部终端安全产品安装率已达到 98%。在总部实现了终端资产信息实名化，资产可达到人、机实名对应的情况，总部所有终端安全产品均可做到版本及时更新、病毒库版本及时更新、补丁库版本及时更新。

总部终端安全建设的效果显而易见，该医药公司也正式借助奇安信的天擎，实现了初步的终端安全运营工作。随着终端安装杀毒软件数量的提升，终端的中毒类事件逐渐下降，安装后勒索事件未有发生。

终端安全运营工作取得的成绩，让该医药公司也充分感受到安全运营带来的价值。因此，从 2020 年年底开始，公司正式规划建设安全运营中心，将安全运营从终端运营提升到全局运营层面。在可研、规划及方案设计阶段，奇安信态势感知与安全运营平台（NGSOC）的专业性和全面性令该医药公司印象深刻，最终决定选择奇安信 NGSOC 作为集团总部安全运营中心的底座。

通过部署 NGSOC，实现覆盖全量资产的全面实时监测预警、事件快速响应，整个安全运营中心初见成效。目前公司已实现“平战结合”的实战化安全运营能力，具备网络资产全面细致、颗粒度管理，丰富安全事件的监测预警手段，进而提升安全事件发现与检测的效率与准确性，提升安全事件处置与应急响应的效率。

为了更近一步完善安全运营中心的建设，奇安信的终端安全准入、漏洞扫描、WAF、防火墙等陆续部署到集团总部，最终在总部建成了以 NGSOC 安全运营平台为中心的一套实时监测、及时预警、协同联动的统一安全运营体系。

从总部到全国，安全能力向全集团辐射

到了 2023 年，该医药公司在感受到总部网络安全建设成效之后，重点工作转移到第二阶段，即将总部成功的经验，向控股公司及各分支机构推广。

在该阶段，在安全运营层面，由于集团总部安全运营平台的系统整合建设已基本完成，所以重点工作是建立集团总部及多区域、多级联的安全运营平台，实现集团统一管控、统一管理，完成“一屏观全局”的安全愿景，持续优化安全防护策略。

在安全技防层面，主要包括持续完善集团公司与分支公司的网络纵深防御、流量威胁检测、主机安全加固措施；同时面向集团公司多场景提升综合防护能力；建设内部威胁防控体系；完善国产化密码基础设施建设；建设安全靶场、实战演练平台等。

截至目前，天擎终端安全方案已经全面推广到集团公司及各分支机构。接下来，集团计划重点将流量检测、安全准入等产品，逐步向各地推广，最终实现统筹分管、集约联动。包括横向打通集团各子系统，纵向贯穿集团、省平台、分支机构等，实现管理对象全协同，对各类资源的统筹调度、情报共享、协同联动，提升整个医药公司的整体网络安全运营能力水平。

“通过这两个阶段的建设，我们最大的收获在于，网络安全建设一定是一个体系化的工作，单一的产品和能力无法实现整体的安全，单点的安全防护无法实现整体安全防御能力。通过体系化的安全运营能力，引入不同节点的安全管控手段，联合作战，在功能和能力上互相弥补，才能实现保卫整体网络安全的目标。”该医药公司网络安全相关负责人表示。

步步为赢，集团安全建设的四年三大跃迁

实践是检验真理的标准，也是最好的老师，从 2019 到 2023 年，该公司不断在实践中探索，收获了三方面价值。

首先是从应对乏力到体系防御。

在项目建设之前，公司早期仅有基础的防病毒软件，在主机加固、虚拟化、应用、数据、密码等通用安全能力建设严重不足，下属单位也缺乏统一的终端威胁检测与处置等终端运营手段。面对日益复杂、新型的、专业的网络安全攻击和勒索病毒，公司在这些方面还有很多提升和改善空间。

随着天擎、安全准入、安全运营平台、智慧防火墙、WAF 等一系列产品的部署，在满足合规的同时，该医药公司的整体网络安全建设成效已经非常显著，安全运营能力水平提升显著。如防火墙实现边界访问控制、恶意代码防范；WAF 完成网站防护、防篡改；漏扫完成脆弱性管理；天擎完成终端管控、终端防病毒等，已经构建起一套叠加演进、持续兼容、务实高效的网络安全体系框架，实现了风险可视、态势可知、威胁可控、资源可用。

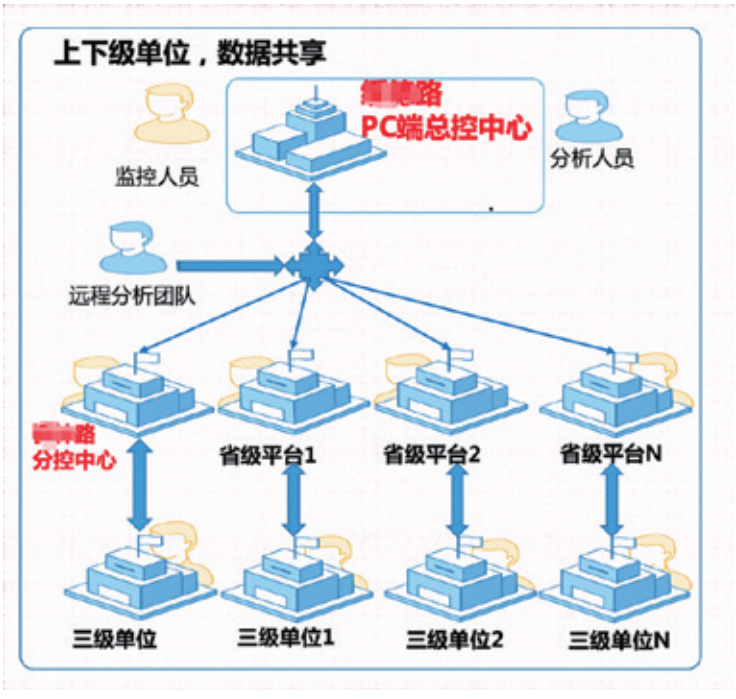
其次是分散到统一管控。

在初期，该医药公司面临终端资产不明、纳管不全，看不见风险、缺乏全局感知等难题，而终端往往又是黑客最热衷关注且最容易突破的窗口。例如，知道某个终端遭遇了勒索攻击，是哪个区域、哪个终端？终端资产归属人是谁？会给集团总部造成多大损害、多大影响？集团总部和分支机构的终端安全状况如何？这些问题都无法得知，更谈不上集中化的统一管控。

统一管控不是一项一蹴而就的工作，该医药公司先通过上线天擎，解决了资产台账的问题，实现了终端安全的持续运营和统一管控。之后，公

司通过上线安全运营平台，可以对天擎 /EDR、智慧防火墙、WAF、漏扫、椒图等 10 多种设备联动，实现处置命令、策略下发等。同时，通过安全运营平台的系统整合建设，在总部试运行；建立集团总部及多区域、多级联的安全运营平台，实现集团统一管控、统一管理。

通过网络安全运营中心的建设，不仅在等保合规、资产管理、脆弱性管理、事件管理、基础运行等基础能力，取得了建设成果，尤其是提供了综合安全态势、外部威胁态势、内部威胁态势、攻击者态势等多个维度大屏，实现了资产风险、网络攻击和业务漏洞等层面的全局可视，结合集团需要的不同展示场景，可以更加数字化、专题化、精细化的展示医药公司整体网络安全态势。



最后是聚焦总部到辐射全集团。

在前期，医药公司主要重点解决总部终端安全的问题。天擎、安全运营平台、安全准入、智慧防火墙、WAF 等均围绕集团总部来进行部署。这样带来的问题就是，各单位与集团之间的整体运营保障联动不足，下属单位数据采集不足，在数据、流程及安全工作等层面的打通和联动机制都亟待完善。加上集团公司二三级单位的安全管理人员严重不足，人员能力参差不齐，给整个公司埋下了安全隐患。

为了解决这些问题，目前医药公司已经将终端安全全面辐射到集团下属的各级单位，完成了全国终端一体化安全态势平台，实现全集团的终端统一监管。

对于下一步的规划，该医药公司计划将网络安全准入、安全运营平台等向集团下属各级单位普及，最终横向打通集团各子系统，纵向贯穿集团、二级单位、子公司等，实现管理对象全协同，对各类资源的统筹调度、情报共享、协同联动，提升网络安全事件应急响应能力水平。

结束语：

医药行业是我国国民经济的重要组成部分，不仅是推动经济增长的重要支柱，同时也关乎着亿万公民的健康和生命。当前，AI、物联网、大数据、云计算等新兴数字技术，也在医药行业得到越来越多的应用，推动着整个行业的高质量发展。而在医药行业的数字化转型过程中，迫切需要筑牢网络安全底座。该医药公司在网络安全建设中的探索与实践，无疑为同行树立了可供借鉴的建设范本。安

大事记

奇安信集团与视联动力达成战略合作

8 月 19 日，奇安信集团与视联动力信息技术股份有限公司（以下简称“视联动力”）签署了战略合作协议。双方将发挥各自优势，聚焦优势领域和行业场景，打造体系化的安全管控解决方案，并将边界安全、终端安全、密码安全等安全产品，与视联网场景形成融合方案，推动视联网赋能经济社会发展提供“新动能”。奇安信集团董事长齐向东、视联动力董事长杨春晖出席签约仪式。奇安信集团副总裁陈华平与视联动力副总裁王艳辉代表双方签署协议。

APT 攻击、勒索软件已成 2024 年最大网络威胁

8 月 19 日，奇安信威胁情报中心发布《网络威胁 2024 年中报告》（简称《报告》）。《报告》基于奇安信威胁雷达监测数据，同时结合全网开源 APT（高级持续性威胁）情报、勒索软件、互联网黑产攻击、漏洞情报等综合信息，对 2024 年上半年各种主流网络威胁进行了全面剖析。

《报告》显示，APT 攻击和勒索软件依然猖獗。从受影响行业来看，涉及我国信息技术、政府机构、科研教育、建筑、制造行业的高级威胁事件占主要部分，其次为医疗健康、能源、金融等领域。

在勒索攻击方面，2024 年上半年全球范围内活跃的勒索软件家族数量众多，新型勒索软件和变种不断出现，部分勒索团伙大多采用“双重勒索”的攻击模式。勒索软件攻击波及包括中国在内的多个国家，受害者中既有个人用户，也有各种规模的组织机构，政府、医疗、制造、能源等行业屡次遭到勒索攻击团伙染指。

奇安信天工实验室携虚拟化研究成果亮相 DEFCON

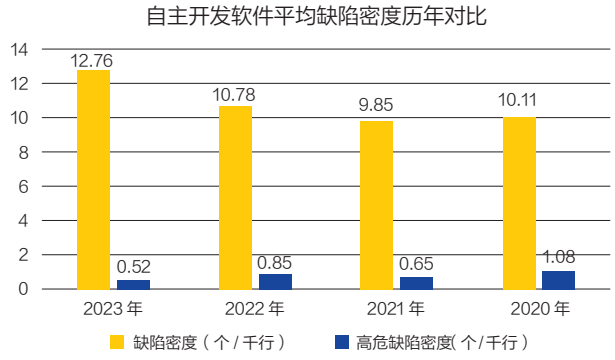
2024 年 8 月，全球顶级黑客大会 DEFCON 于美国拉斯维加斯拉开帷幕。8 月 12 日，奇安信天工实验室受邀线上参会，发表《Dragon Slaying Guide: Bug Hunting In VMware Device Virtualization》的议题演讲。本次分享着重介绍天工实验室对于 VMware Hypervisor 的相关研究成

果，详细讲解由实验室独立挖掘的多个与设备虚拟化相关的漏洞。

奇安信《软件供应链安全报告》：七成国产软件有超危漏洞

8 月 12 日，奇安信集团对外发布《2024 中国软件供应链安全分析报告》（以下简称《报告》）。《报告》显示，国内企业软件项目，开源软件使用率达 100%。目前，开源软件漏洞指标仍处于高位，软件供应链的安全问题并没有得到根本性的改善，20 多年前的开源软件漏洞仍然存在于多个软件项目中。

《报告》提出了三方面建议，一是建立国家层面统一的软件供应链安全保护基础设施；二是完善国家和行业级的软件供应链安全测评认证体系；三是健全关基软件供应商安全实践证明材料的备案机制。



吴云坤：培养网络空间安全高水平人才迫在眉睫

8 月 9 日，由中国网络空间新兴技术安全创新论坛、中国网络空间安全人才教育论坛、国务院学位办网络空间安全学科评议组主办，奇安信集团等单位协办的“2024 年网络安全技术创新与人才教育高峰论坛”在湖南长沙开幕。奇安信集团总裁吴云坤受邀出席，并做“新形势下网络安全人才培养模式创新与探索”的主题演讲。

他表示，网络空间对抗已经成为大国博弈和科技竞争的主战场，支撑网络空间对抗需要大批高层次拔尖人才和高水平实战人才，长期的科研和产业实践验证，建立人才培养、科学研究和产业应用三位一体的产教深度融合机制，是实现高水平科技创新和高质量人才培养的必由之路。

鹏银数据与奇安信签署战略合作 打造算力安全新高度

8 月 5 日，鹏银数据与奇安信集团在京就打造战略协同、优势互补、资源共享、共赢发展的算力安全业务生态链展开深入交流，并签署战略合作协议。鹏银数据董事长宋晓宇，奇安信副总裁陈华平出席会议并见证签约。鹏银数据副总经理戴京津，奇安信助理总裁、东北特区总经理李志鹏分别代表双方签署协议。

陕西西安洞鉴云侦声像资料司法鉴定所正式揭牌成立

7 月 27 日，陕西省电子数据司法鉴定应用研讨会在西安举行。会议期间，陕西西安洞鉴云侦声像资料司法鉴定所正式揭牌成立，这标志着奇安信洞鉴旗下的第三家司法鉴定机构正式投入运营，为西北地区司法鉴定事业注入了新的活力。

奇安信总裁吴云坤参加中国电子 2024 年中工作会议

7 月 26 日 ~27 日，奇安信集团总裁吴云坤参加了中国电子在深圳举行的 2024 年中工作会议。此次会议是对中国电子上半年工作的总结，更是对党的二十届三中全会精神的深入学习和贯彻。

吴云坤号召奇安信全体员工要深入学习领会年中工作会议精神，立足本职工作，紧跟国家政策步伐，持续开拓创新、发展新兴技术。奇安信也将积极履行社会责任和使命担当，为推动我国网络安全产业的健康发展和国家网信事业的繁荣进步贡献更大的力量。

湖南省副省长、公安厅厅长王一鸥会见齐向东

7 月 24 日上午，湖南省副省长、公安厅厅长王一鸥在长沙会见奇安信科技集团股份有限公司董事长齐向东一行。

王一鸥介绍了湖南锚定“三高四新”美好蓝图，加强新时代网络安全建设，护航高质量发展的情况。他指出，网络安全关系重大，湖南推动网络强省建设取得了新成效、迈出了新步伐。省政府和奇安信达成战略合作协议以来，双方在网络综合治理体系建设、城市网络安全、工业信息安全等多个领域重点开展合作，目前各合作事项正在有条不紊地推进中，已取得阶段性成效。希望奇安信持续加大在湘的人才、技术、研发等方面投入，不断创新业务模式、合作方式，与地方和部门增强交流借鉴互补，共同为湖南网络安全建设取得新的、更大的成效而努力。

奇安信中标证券行业某核心机构 2024 年重保服务

近日，奇安信集团中标证券行业某核心机构 2024 年网络安全重保服务采购项目。根据合作内容，奇安信将为该机构提供重保期间涵盖风险评估、攻防演习、实时监测、响应处置等的安全服务。这是奇安信在金融行业核心机构网络安全服务的又一个标杆项目。

齐向东：中国目前不会发生 Windows 全球性蓝屏这样的事故

近日，全球多地的计算机因美国计算机安全技术公司

CrowdStrike 的一款安全软件更新而遭遇宕机，导致“微软蓝屏”现象，影响波及航空、医疗、传媒、金融、零售、物流等多个行业。然而，中国政企单位似乎并未受到此次事件的严重影响。奇安信集团董事长齐向东表示：中国政企单位目前不会发生 Windows 全球性蓝屏这样的事故。这主要得益于中国在网络安全部署上的几个关键差异。

首先，中国政企机构倾向于采用本地私有化部署，与国外机构和企业普遍采用的公有云部署形成鲜明对比；其次，中国政企机构使用的终端安全软件与普通民众使用的计算机安全软件是完全分开的，其升级更新和维护策略也完全不同；再次，中国政企机构的操作系统并非完全依赖微软 Windows 视窗系统；最后，齐向东提到，奇安信集团在保障政企机构业务连续性方面拥有丰富经验。

荣誉墙

Gartner 最新报告：奇安信领跑八大赛道

日前，Gartner 发布《Hype Cycle™ for Security in China, 2024》（简称《报告》），本期报告中，奇安信除再次入围攻击面管理 ASM、软件组成分析 SCA、安全服务边缘 SSE、IoT 身份认证、安全接入服务边缘 SASE 五大领域外，同时入选零信任网络访问 ZTNA、数据安全平台 DSP、安全信息和事件管理 SIEM 三大领域代表供应商 (Sample Vendors)。

奇安信与阜职产教融合成果获安徽省教学成果特等奖

近日，《安徽省教育厅关于公布 2023 年度高等学校省级质量工程项目名单的通知》（皖教秘高〔2024〕55 号）公布，奇安信集团与阜阳职业技术学院联合申请的《面向皖北区域新一代信息技术产业应用型人才培养模式构建与实践》获得安徽省教学成果特等奖，这是奇安信集团深化产教融合、助力职业教育发展，联合培养实战型网络安全人才，积极探索教育、科技、人才“三位一体”协同融合发展的又一个标志性成果。


安徽省教学成果奖

证书

为表彰安徽省教学成果奖获得者，特颁发此证书。

项目名称：面向皖北区域新一代信息技术产业应用型人才培养模式构建与实践

奖励等级：特等奖

获 奖 者：林雪朝

二零二四 年 六月 二日

证书号：2023jxcgj482-3

六连冠！奇安信稳居中国云安全市场首位

近日，赛迪顾问发布《2023—2024 年中国云安全市场研究年度报告》（以下简称“报告”），报告指出中国云安全市场规模达到 184.2 亿元，同比增长 21.3%。奇安信作为


表 2 2023 年中国云安全市场品牌 TOP5 排名

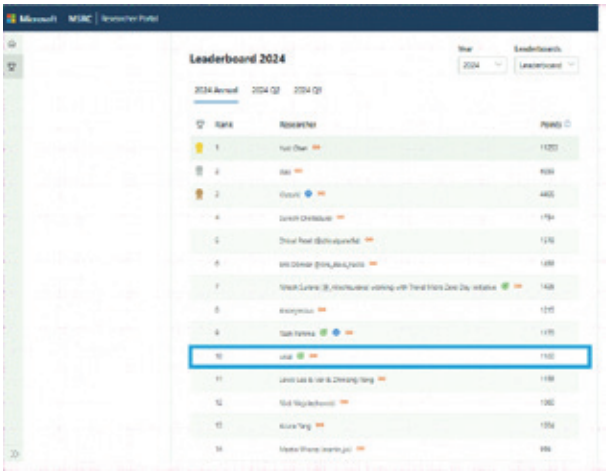
排名	厂商	销售额（亿元）
1	奇安信集团	9.04
2	[illegible]	[illegible]
3	[illegible]	[illegible]
4	[illegible]	[illegible]
5	[illegible]	[illegible]

数据来源：赛迪顾问 2024

中国云安全市场的领导者，凭借卓越的产品能力、深厚的市场积淀，以及完整的云及云原生安全体系，以 9.04 亿元的营业收入高居榜首，连续 6 年夺冠，稳坐中国云安全市场头把交椅。

奇安信代码安全实验室研究员入选“2024 MSRC 全球最具价值安全研究者”榜单

8 月 7 日，微软安全响应中心 (MSRC) 发布 2024 年度全球 Top 100 最具价值研究者榜单，奇安信代码安全实验室一名研究员凭借高超的安全漏洞研究能力入选该榜单，位列第 10 名；此外，微软还发布了 4 个特定技术领域的荣誉榜单，分别是 Windows 操作系统榜单、Azure 云榜单、Office 榜单、Dynamics 榜单。奇安信代码安全实验室该名研究员入选“MSRC 2024 最具价值研究者——Windows 操作系统榜单”，位列第 3 名。

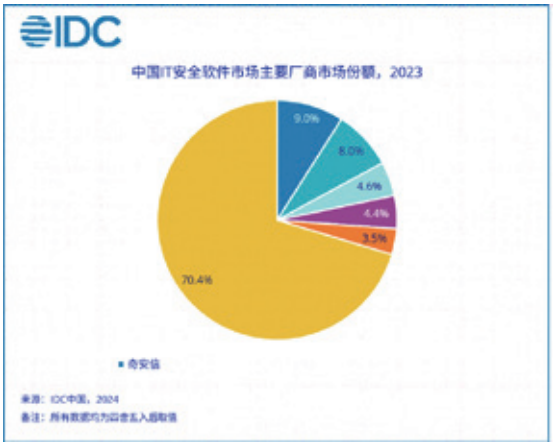


5 项满分！奇安信 CSMP 通过权威机构安全资源池技术能力评估

近日，IDC 发布《中国安全资源池技术能力评估，2024》（Doc#CHC52437524，2024 年 7 月），通过对国内市场中主要安全资源池技术服务提供商的综合技术评估，来帮助市场更加全面地了解中国安全资源池相关技术在过去的发展情况，以及未来的技术发展趋势。奇安信 CSMP 云安全资源池凭借卓越的产品能力和深厚的市场积淀，在众多产品中脱颖而出，获得了 5 项满分（总共 6 项维度）的优异成绩。

奇安信领跑中国 IT 安全软件市场 安全大模型开辟跨越式发展新路径

日前，IDC 针对中国 IT 安全软件市场，再次发布《中国 IT 安全软件市场份额，2023：安全大模型在多类产品中展露锋芒》（Doc# CHC50964424，2024 年 7 月）（简称“IDC《报告》”）。从综合性网络安全厂商和公有云厂商视角，整体梳理了中国网络安全软件市场竞争格局。2023 年，奇安信集团以 25.1 亿元的安全软件市场规模、9.0% 的市场份额排名第一，市场规模较 2022 年增长 6.5%，彰显了客户对奇安信软件产品及优质客户服务的高度认可。



奇安信入选 Gartner®《2024 年私有移动网络服务成熟度曲线》

近日，国际市场研究与咨询机构 Gartner® 对外发布了技术成熟度曲线报告《Hype Cycle® for Private Mobile Network Services，2024》（《2024 年私有移动网络服务成熟度曲线》，以下简称“报告”）。奇安信入选为中国攻击面管理（ASM）代表厂商，充分证明了公司在该领域的领先技术优势和市场认可度。

奇安信安全 SD-WAN 荣获信通院“2023 年度 SD-WAN 优秀产品奖”

日前，中国通信标准化协会算网融合产业及标准推进委员会（CCSA TC621）在北京召开“2024 年算网融合发展大会 算力网络产业发展论坛”。会上，中国信通院公布了“2023 年度 SD-WAN 优秀产品奖”评选结果，经过专业评委的层层严格筛选和评估，奇安信凭借“海外运营商场景中完成大规模、智能、弹性 SD-WAN 组网实践”脱颖而出，荣获 SD-WAN 优秀产品奖。

奇安信一解决方案入围工信部 2023 年信息技术应用创新应用示范案例

近日，工业和信息化部网络安全产业发展中心（信息中心）通报了 2023 年信息技术应用创新解决方案征集遴选结果，本次共评选出典型解决方案 173 个。其中，奇安信和江苏省人社共同提报的“基于态势感知实战化安全运营解决方案”，以其创新性、前瞻性和实践性，成功入围了工业和信息化部 2023 年信息技术应用创新应用示范案例。此次入围工业和信息化部示范案例，不仅标志着奇安信在信息技术应用创新领域的实力得到了国家级的认可，也为整个网络安全行业树立了新的标杆。

2024 年万得 ESG 评级：奇安信集团荣获 AA 级并再获行业第一

近日，金融软件服务企业万得最新一期 ESG 评级（Wind

ESG Rating）显示，奇安信集团的 ESG 表现再度被评为 AA 级，是信息技术服务行业内 ESG 综合得分最高、排名第一的企业，这也是奇安信集团连续两年获得万得 ESG 评级行业第一。这一荣誉不仅是对奇安信 ESG 实践的充分认可，也是奇安信持续致力于可持续发展和社会责任的展现。

社会责任

“眼明心安”项目 2024 年进藏培训、义诊和带教活动在林芝圆满结束

7 月 20 日 ~23 日，以“提升西藏儿童盲及低视力诊疗能力”为核心目标的“眼明心安”项目在西藏林芝先后开展了“西藏儿童眼病诊疗技术二期培训班”（以下简称“二期培训班”）和爱心义诊与手术带教等公益活动，为来自西藏 7 个地市 16 个区县 26 家医院的 50 名医务人员提供了理论与实操带教培训，并在林芝市人民医院为 300 余名居民进行了爱心义诊， 为 12 名眼疾积患进行了公益手术。

从 Gartner2024 年北美安全峰会看安全运营的技术趋势

作者　叶蓬

2024 年度于 Gartner 北美安全与风险管理峰会于 6 月 3 日至 5 日在美国召开。这次峰会并没有在媒体（尤其是中国媒体和自媒体）上受到关注，可能是现在 Gartner 的安全峰会一年多次在全球举办分散了注意力，也可能是现在对于网络安全的创新点过于聚焦在 GenAI 之上，而显得各种安全大会缺乏差异而造成了思考疲劳，抑或是国内外的网络安全技术越来越多的分叉导致国内网络安全技术从业者越来越关注自身，而国内当前低迷的网络安全产业市场多少也对人们谈论网络安全的前瞻技术形成了阻碍。

1 重点的新兴技术领域

在《2024 年安全与风险管理新兴技术》议题中，Neil McDonald 筛选出了 5 类关键技术。

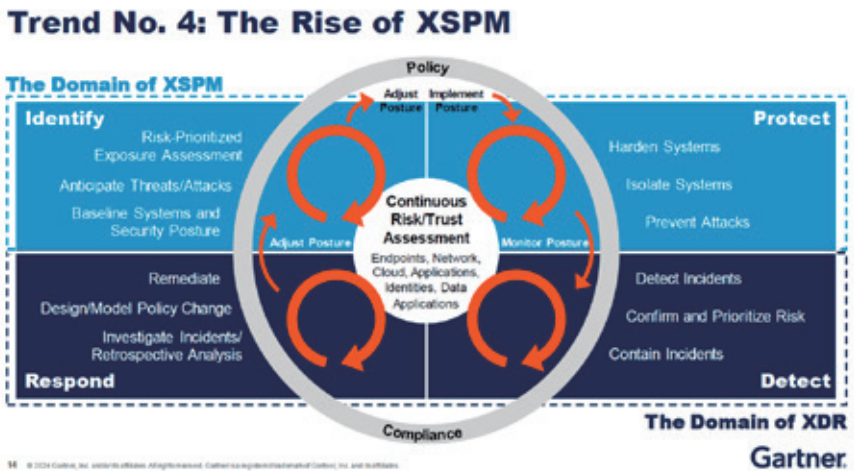


图 1

1）AI 和 GenAI：包括保护 AI 和利用 AI 两个方面。在保护 AI 方面，是 Gartner 重点关注的方向，涉及的新兴技术包括 AI TRISM（AI 信任、风险与安全管理）技术、LLM 防火墙、在 SASE/SSE 中增加对 AI 应用的保护技术，以及 AISPM（AI 安全姿态管理）。在利用 AI 方面，Gartner 显得十分谨慎，目前的建议就是，在现有的安全控制台中增加 GenAI 接口。

2）安全平台整合：这个已经谈了好几年了，主要集中在各个领域内的横向整合，包括面向云的 CNAPP，面向边缘接入的 SSE 和 SASE，以及面向安全运营领域的 SIEM/SOC 与 XDR、CTEM 的整合，此外还有身份安全平台的出现。Gartner 还指出，现在已经出现了跨多个领域的整合平台。

3）身份即关键基础设施：也即要保护身份这个关键基础设施。涉及的新兴技术包括 ITDR、ISPM（身份安全姿态管理）、机器身份管理及无口令认证。

4）xSPM 的崛起：xSPM（或者简称为 SPM，即安全姿态管理）代表了 Neil 自己提出的自适应安全架构的 I（识别）和 P（保护）象限【笔者注：最新的 Gartner 自适应安全架构的四象限分别是 IPDR，其中第一个

是 I（识别），而原来是 P（预测），仅修改了名称，内容未变，估计是为了与 CSF 的 IPDRR 中的 I 保持一致性】，而包括 XDR 等在内的 TDIR 则重点聚焦在 D 和 R 象限。在各种 SPM 中，新兴的 SPM 包括 ASPM（应用 SPM）、DSPM（数据 SPM）、AISPM（人工智能 SPM）、SSPM（SaaS SPM）。

5）CTEM：这个也谈了好几年了，新的变化主要是将 CTEM 从 IT 环境扩展到 OT 和 CPS 环境中。而新兴技术趋势包括 CTEM 下不同类型产品的相互融合，以及 SPM 厂商和 SIEM 厂商的纷纷介入（增加 EM 方面的功能）。而正是由于 SPM 厂商和 EM（暴露管理）厂商的互相渗透，使得 Posture（姿态）和 Exposure（暴露）两个概念之间的关系越发微妙。

从安全运营的角度来看，以上 5 个方面中，有四个方面都跟安全运营有关，包括：安全运营领域是利用 GenAI 的最佳场合之一；安全运营的平台整合正在塑造新一代的 SOC 平台；而 SPM 和 EM 也都正在融合到全新的 SOC 框架中。

2 安全运营领域的前景展望

在峰会上，Gartner 提出了三大方面的展望：CTEM 和 TI（威胁情报）助力安全运营、GenAI 赋能 SOC、超大规模安全运营。

其中，CTEM 和 TI 有助于帮助收敛攻击面，为安全运营做好事前准备，同时它们获取的信息可以作为后续检测和响应的情境（上下文）数据使用，以加速检测和响应。GenAI 能够从多方面赋能 SOC，但还很不成熟，存在

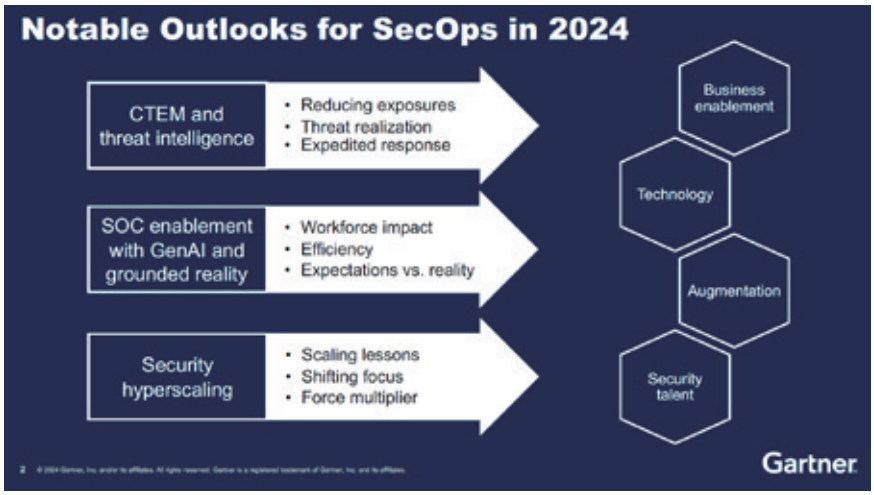


图 2

安全隐患，一定要慎重使用【笔者注：Gartner 对 GenAI 一直持谨慎态度】。而如何在现有（小）资源的条件下进行超大规模的安全运营工作，正成为越来越迫切的问题，必须有机结合 AI 与自动化技术。

以下笔者分别从 CTEM 助力安全运营、GenAI 赋能安全运营和超大规模安全运营三个方面进行深入分析。

2.1 CTEM 助力安全运营

2.1.1 CTEM 解析

结合 Gartner 观点，笔者认为持续威胁暴露管理 (Continuous Threat Exposure Management) 是一套包含技术、流程和人员在内的系统性、集成化、迭代性的方法和体系，让企业和组织有意识地、持续并一致地评估其数字资产和物理资产的可见性、脆弱性和可访问性，以持续优化提升安全姿态。Gartner 将 CTEM 看作是一个过程和方法，而将 EM（Exposure Management，暴露管理）或者 TEM（威胁暴露管理）【笔者注：Gartner 在 7 月底发布的 SecOps Hype Cycle 报告中，将 EM 改为 TEM】看作是支撑 CTEM 的技术集合。

EM 的核心能力是进行暴露评估和暴露验证，其中暴露评估包括攻击面评估（ASA）【注 1】【注 2】和漏洞评估与优先级研判（VA&VPT）【注 3】，暴露验证主要是使用破坏和攻击模拟（BAS）和自动化渗透测试等网络安全验证技术【注 4】。简单地说，EM = ASM + VM + CyVal。

【注 1：最新的 Gartner ASM 市场指南报告中指出 ASM 中的 M（管理）不是一个准确的定义，其实 ASM 的工作更多是 ASA（攻击面评估），由于历史原因也不会改名了，但有的场合会使用 ASA。】

【注 2：ASA 或者说 ASM 又包括三个技术，分别是 EASM、DPRS 和 CAASM。这里不再展开叙述。】

【注 3：这里的漏洞还包括安全配置缺陷和安全防御策略的缺陷。安全配置的缺陷通常使用配置核查工具来识别，而 xSPM 类产品也都提供相关能力。安全防御策略缺陷则包括了安全及网络设备的安全策略缺陷（譬如防火墙规则缺陷），甚至于安全运营体系（如 SOC）的检测、监测和响应

策略的缺陷，等等。】

【注 4：安全验证技术和工具不仅可以用于暴露验证，即验证暴露的有效性，还能用于安全漏洞及配置和防御策略缺陷的评估。】

必须指出，CTEM 的闭环并不是我们一般所理解的闭环，不是以暴露面的收敛（包括漏洞缓解）、暴露事项（issue）或者工单（ticket）的关闭为结束，而是以“动员”为结束。也就是说，Gartner 认为暴露面收敛的具体工作主要是 IT 和业务部门的事情，安全部门当然也要参与，但不属于安全部门自个儿的事情，因此不在 CTEM 闭环中。CTEM 的闭环最后就是能够将有效的暴露面事项或工单提供给专门的团队和人员，并协助和督促其整改。因此，不要想当然地认为 CTEM 会真正“管理”和收敛暴露面。

上述 CTEM 的工作内容也恰恰印证了安全运营工作中资产运行和漏洞运行的工作范围。其中最重要的是安全运营中的漏洞运行工作也是不包括漏洞缓解本身的（尽管有的漏洞缓解工作也能在安全运营团队内部实施），漏洞缓解系统应该另由安全部门、IT 部门和业务部门共同建设与运行。

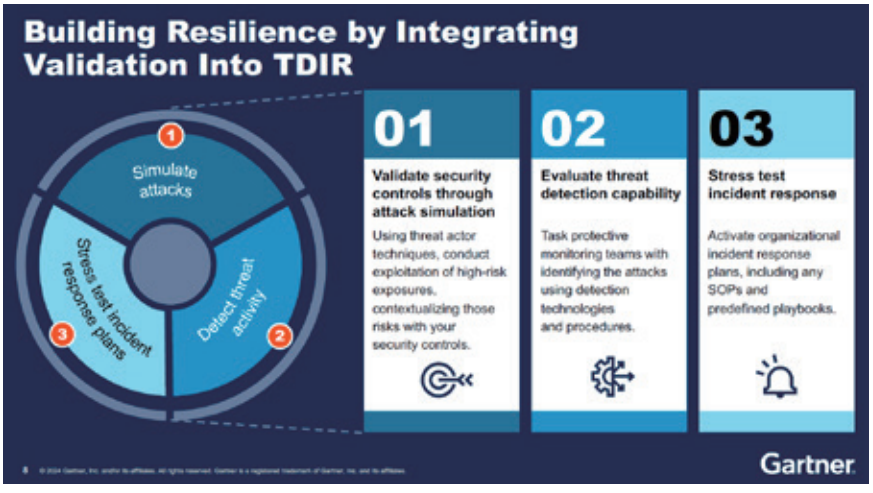


图 3

2.1.2 EM 为 SOC 提供上下文

EM 所代表的暴露评估和验证的结果对于 SOC 的检测和响应工作十分有价值。EM 可以为 TDIR 提供上下文（情境）信息，譬如：精准的资产和漏洞信息可以让分析师编写更加精准（包含资产和漏洞关联信息）的检测规则，并且这些规则可以真正用起来；可以生成更加丰富易懂的告警信息；有助于支撑威胁猎捕；而暴露验证获得的安全控制策略方面的缺陷有助进行威胁建模。总之，有了 EM 提供的上下文信息，TDIR 可以更加高效，也即安全运营更加高效。

2.1.3 EM 可以提升 SOC 自身弹性 / 韧性

EM 中的安全验证工具通过对安全漏洞、配置和防御策略缺陷的评估，以及暴露的验证，可以实现对包括 TDIR 在内的 SOC 有效性的评估，从而提升 SOC 自身的弹性。SOC 自身策略和安全内容的缺陷也是一种暴露，也需要被识别和验证，譬如发现针对某项不可修复的漏洞的补偿措施（虚拟补丁或者增强监控策略等）的缺陷，识别出低效（导致高误报）的关联分析规则，发现针对某种关键威胁的响应对策的缺失等。通过对这类缺陷的识别和验证，有助于提升 SOC 自身的强度。

2.1.4 从 SOC 的角度看 EM 和 TDIR

首先，安全运营（SecOps）是一个很宽泛的概念。如果我们把整个安全生命周期分为规划、建设、运营三个部分的话，安全运营的历程将伴随企业组织的一生。因此，可以把安全运营看作是持续不断地保障目标网络安全平稳运行，达成组织业务战略目标的永续过程。安全运营涉及的内容很广泛，从能力方面看，可以分解

为 IPDRR（识别、保护、检测、响应、恢复）或者类似的变体。从运营对象来看，可以分为工作负载、端点、应用、数据、身份等维度。Gartner 将安全运营定义为一个“通过一套人、流程和技术来识别和管理暴露、监测、检测和响应网络安全威胁与事件，以提升网络弹性”的过程。SANS 则将安全运营的使命定义为“保护业务运营的私密性、完整性和可用性，并最小化非预期事态造成的损失”。

安全运营中心（SOC）则比安全运营更加聚焦，虽然有很多定义，但通常都是指一个包含一系列流程、人员、技术等的组织单元，核心目标就是抵御网络安全威胁、保障目标网络安全平稳运行。围绕这个目标，通常会对目标网络实施持续的检测、监测、分析、调查、响应、报告、修复。

笔者基于自己的多年实践，认为安全运营中心可以分为威胁事件运营、资产暴露运营、安全漏洞运营、安全情报运营、防御策略运营、态势决策运营 6 个方面能力。其中，威胁事件运营是所有 SOC 的核心能力，就是指威胁事件的检测与响应，通常依托于 SIEM 或者 Gartner 新提出的 TDIR。而资产暴露运营和安全漏洞运营则跟 Gartner 的 EM 相匹配，以在事前掌握和完善自身安全防御的姿态，同时又与安全情报运营所依托的 TIP 一道为 TDIR 提供上下文（情境）信息，提升威胁事件运营的效能。防御策略运营则通过持续的评估、验证和改进来不断提升包括 SOC 自身在内的防御体系的有效性。最后，态势决策运营持续收集前面 5 大运营过程中的数据，进行指标计算和态势量化，形成决策，从而动态调整安全保障级别，调配安全防御力量。

在笔者看来，当前国内大部分 SOC 基本还处于基于 SIEM 所承载的威胁事件运营阶段。安全情报虽已普遍应用，但客户自身 TIP 建设及其上的安全情报运营还处于早期。资产暴露运营和安全漏洞运营则还处于初始、分散的阶段，相关信息处于不全、不准、滞后的状态，尚无法实战，难以赋能威胁事件运营，而这在全球范围内都是一个痛点，也因此 Gartner 近几年一直在力推 EM/CTEM。至于防御策略运营、态势决策运营（尤指宏观态势）则更多还停留在纸面上。以 2023 年发布的网络安全态势感知通用技术要求国标为例，更多还是描述了态势展示的内容，而态势信息的获取与分析则基本与 SIEM 重合。

2.2 GenAI 赋能 SOC

这已经是不争的事实了！从笔者分析的 RSAC2023 大会和 RSAC2024 大会的情况看，所有人都知道 GenAI 用在安全领域的首要场景就是安全运营和 SOC。因为 GenAI 恰好完美地击中了当下安全运营的三大痛点：人才短缺、工作倦怠（告警疲劳）、技能不足。不论是副驾、助理还是智能体，都试图让 GenAI 驱动的机器人充实到客户的安全运营团队中去。

Gartner 预计，到 2028 年，基于多智能体的威胁检测与事件响应工作将从现在的 5% 暴涨到 70%。同时，Gartner 认定届时 AI 主要还是增强而非替代员工。

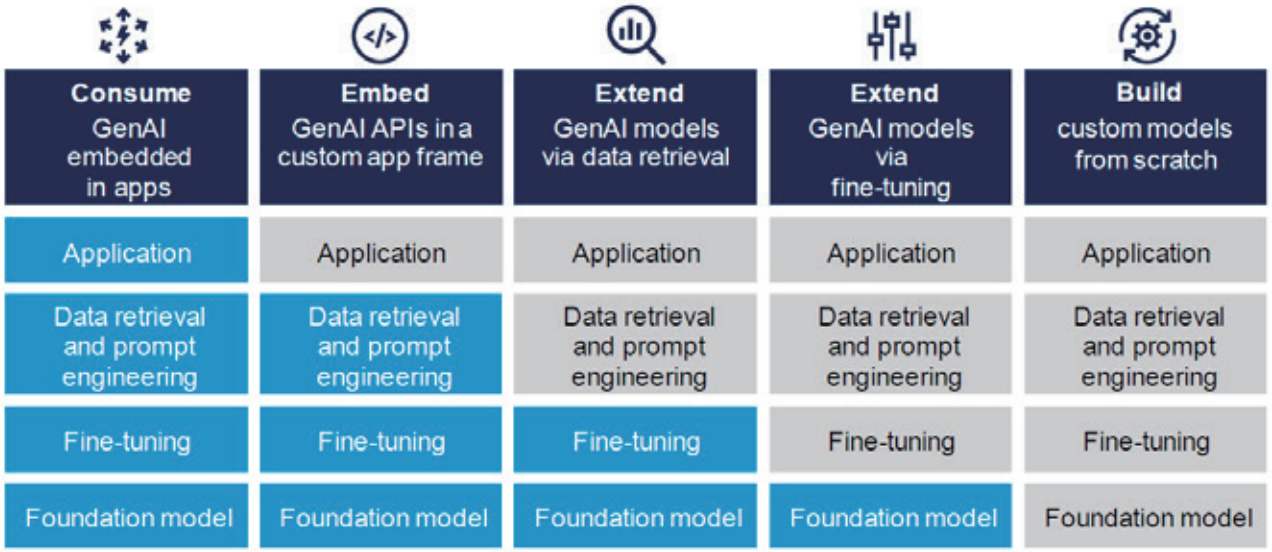


图 4

2.2.1 GenAI 应用部署模式

Gartner 将 GenAI 应用分为了四层：基础模型层、微调层、数据检索与提示工程层、应用层。对于使用 / 开发 GenAI 应用的人而言，可以采用五种部署模式：直接用第三方的 GenAI App、将 GenAI 嵌入到自己的 App 中、自己实现数据检索与提示工程、自己实现微调、自己从底层模型开始搭建。显然，从不同层次开始构建 GenAI App，成本和技术考量都是不同的。如图 4 所示，展示了 GenAI 的分层和五种部署模式，其中蓝色块表示采购自第三方的组件。

2.2.2 GenAI 应用类型

目前，仅就用于 SecOps 的 GenAI 应用而言，大体上可以分为三种类型：聊天机器人、AI 助理 / 副驾、智能体。三种类型的难度依次上升。目前，主流的 SecOps 厂商聚焦于 AI 助理 / 副驾（如微软的 Copilot、SentinelOne 的 Purple AI），而初创企业（如 Dropzone AI）则更多聚焦于智能体。图 5 展示了不同类型下的厂商示例。

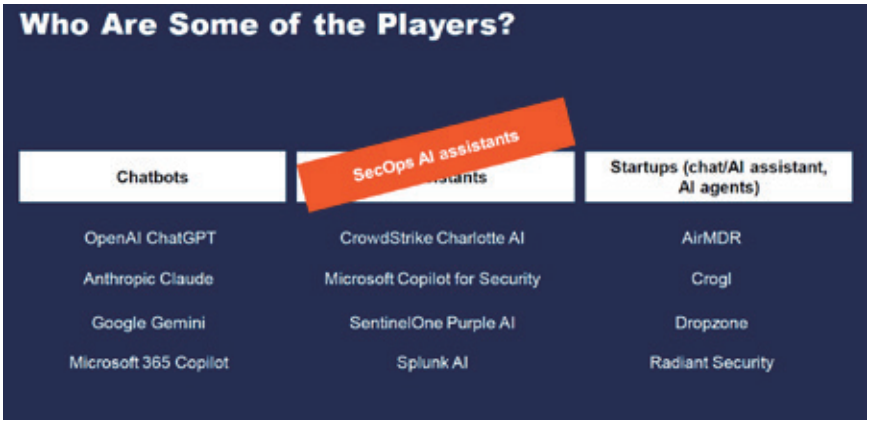


图 5

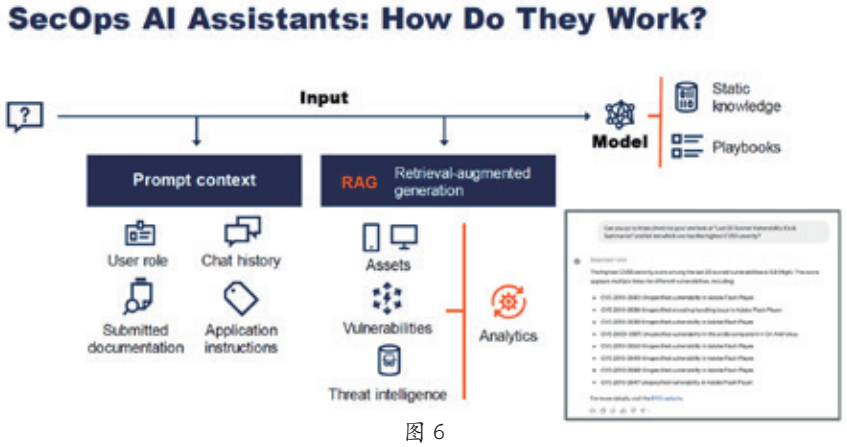


图 6

图 6 展示了当下主流的 AI 助理 / 副驾的工作原理，核心就是提示工程和 RAG。

Gartner 表示，以当前最重要的大语言模型（LLM）为例，它其实并不真的“智能”。在笔者看来，往深了讲，它的“智能”都基于你喂给它的语料和对它使用各种安全运营工作套路的训练，抑或各种静态知识库。此外，LLM 尚未真正取代现有的威胁检测引擎，大部分情况下都是 LLM 基于自然语言的输入生成检测规则或代码，然后还是由原来的检测分析引擎去跑。此时，大模型不会让你的检测引擎变好，而只是加速这个引擎的使用速度，降低引擎使用难度。而即便未来可以通过自然语言来生成检测 / 调查 / 猎捕的规则或代码，对于分析师的业务领域技能的要求依然不会降低，因为如果分析师不能问出正确的问题，也不会得到预期的结果。

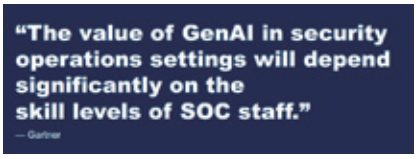


图 7

2.2.3 GenAI 赋能 SOC 的用例

在本次峰会上，多位分析师都列举了自己心中的主要 GenAI 赋能 SOC 的用例，以下是笔者综合多位分析师观点的一份用例清单。注意，以下用例主要都工作在 AI 助理 / 副驾模式下。

· 增强威胁检测能力：查询 / 规则生成、告警分析、告警信息解释、告警富化

· 简化检测工程：生成检测代码 / 规则

· 加速安全事件响应：事件解释、事件调查与信息增强、生成事件响应建议 / 计划 / 剧本

· 提升工作流程效率：GenAI 功能有机整合到现有 UI 中、工作流程提示

· 加速 SOC 度量：总结事件响应过程、生成资产 / 漏洞 / 事件报告、生成日报周报等报告

· 提供培训：培训新手使用本系统、安全运营实战教学、安全知识教学

· 助力攻击面管理：资产 / 漏洞识别、资产 / 漏洞去重与合并

· 简化情报分析：交互式威胁情报分析

· 辅助攻击演练：生成攻击场景、攻击模拟、桌面推演

2.2.4 SOC 使用 GenAI 的禁忌

Gartner 对 GenAI 一向特别谨慎，因为 GenAI 本身存在很多不确定性（如准确性、可解释性、可信度、隐私问题等）。Gartner 不断敬告大家，使用 GenAI 要以我为主，按需使用，不要彻底依赖 GenAI。把 GenAI 看作是增强人的一个工具，而不是替代人，要建立起合理的 GenAI 应用效果预期。如前所述，人的安全运营技能依然十分重要，不要降低这方面的投入和培训。此外，对于 GenAI 生成的结果，不要完全相信，要建立常态化的验证反馈机制。

现在，主流的 SOC AI 助理厂商也都在尽力提升通过 GenAI 的回答结果的透明度和可解释性，包括给出结果的原始信息来源，给出分析的步骤等。

2.3 超大规模安全运营

随着日志量的不断攀升，数据存储量、告警量都在与日俱增。在现有本就短缺的安全运营资源投入条件下，如何处理海量日志告警并响应安全事件成为一个难题。目前为止的大部分方法都是采用上下文丰富、排序、分组等方式，让分析师聚焦到少部分重要的告警和事件上【注 5】，对于相对不重要的，就只能看着办，有时间就处理，没时间就忽略。现在，随着 AI 的火爆，业界产生了一种期待，能否对所有（或者大部分）的告警和事件都进行处理？

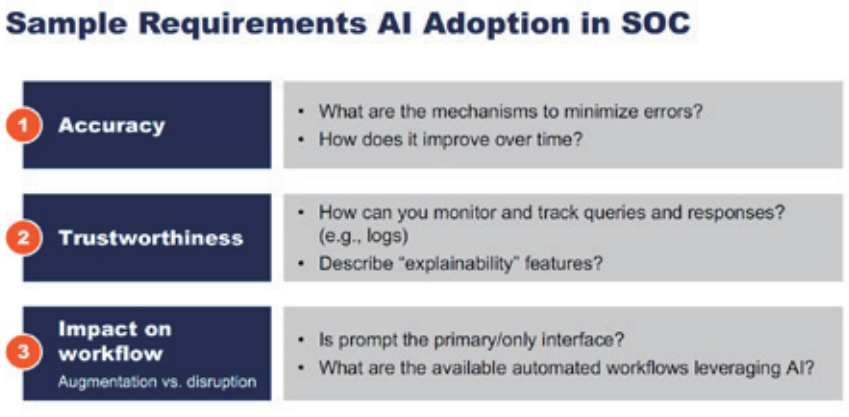


图 8

这就是笔者理解的所谓超大规模安全运营（hyperscale SecOps）。

超大规模安全运营是指综合采用自动化和 AI 等多种技术【注 6】，实现对超大规模日志量、告警量和事件量的安全运营。超大规模安全运营至少要使用自动化，但还必须使用 AI 等其他技术，即所谓的超自动化（hyperautomation）。

【注 5：有的厂商说，能够让用户一天就处理 10 条安全事件，并不是说只有 10 条，而是还有很多条疑似事件由于没有触发阈值（或者评分较低）而被忽略了。从安全的角度来说，可能恰恰问题就隐藏在其中。因此，如何把需要优先处理的安全事件降到最低，同时在概率上不遗漏重大的危害，就成为了各家的本事。】

【注 6：正如笔者以前就指出的，AI 不等于自动化！AI 也取代不了自动化，包括 SOAR，但 AI 可以赋予自动化以智能，让自动化更强大。】

要实现超大规模安全运营必须使用自动化。自动化尤其擅长将“低端”的重复性安全任务规模化。但是，SOAR 的发展路径提醒我们，不要试图去做全流程的、端到端的自动化！这样会适得其反！因此，真正实战化的 SOAR 都在不断提醒用户，先将剧本做小，然后再通过拼接的方式形成大的流程，同时要合理设计流程中人机交互的断点。

Gartner 显然也意识到了这个问题，表示对一个完整的流程实现规模化并不可取（也不现实）。同时，将某个岗位角色的工作过程简单的规模化也不可取，因为每个角色的不同活动性质各不相同，需要采取不同的规模化方式。综合比较，从构成流程的活动入手，实现规模化最为可行，同

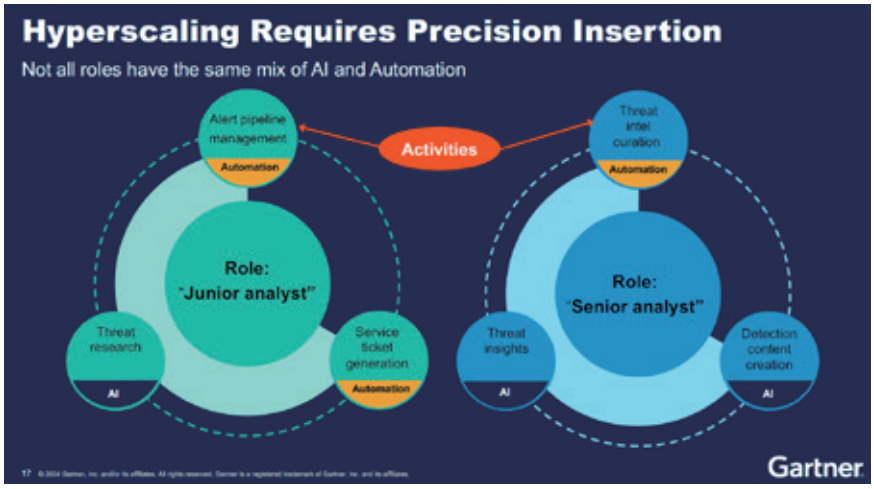


图 9

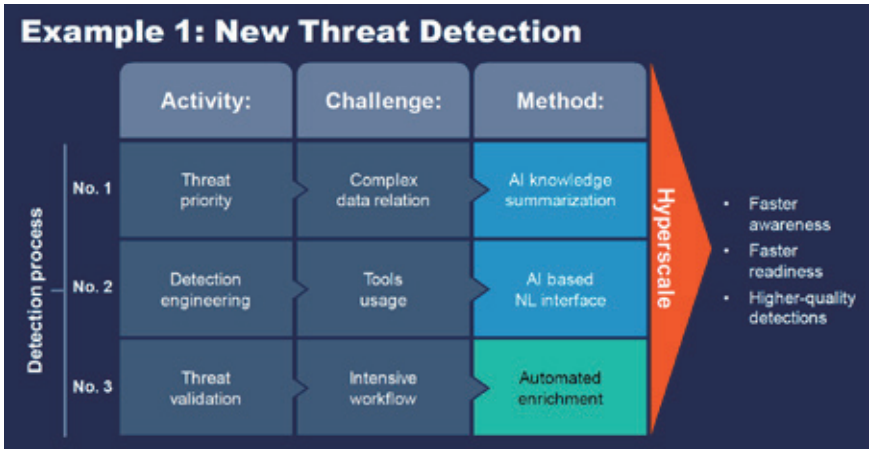


图 10

时有针对性地使用不同的规模化方法（自动化和 AI）。

自动化和 AI 各有所长。自动化擅长工作流执行、命令处理、知识编纂，而 AI 更擅长提出建议、提供指导，以及知识发现（尤其是总结）。因此，针对不同的安全运营目标，其分解出来的不同活动适用于不同的规模化方法。如图 10 所示：

以新威胁检测为例，威胁优先级排序使用 AI 技术，检测工程使用 GenAI 基于自然语言生成检测规则 / 代码，而威胁验证则使用采用自动化剧本。

2.4 安全运营技术展望小结

1） 将 CTEM 与 TIDR 技术结合，实现更完整的 SOC。

2） 实验试点 GenAI 赋能的 SOC 应用，同时保持合理预期，清醒地把 GenAI 作为一个能力的增强，而非取代现有的技术专家。

3） 综合使用自动化和 AI 技术迈向超大规模的安全运营。

3 总结

暴露管理正在借助实战化、真正面向运营的资产管理、漏洞管理和验证管理将 SOC 的实战性提升到新的高度。现有 SOC 中的资产管理、漏洞管理模块需要从设计理念、目标和架构上进行重构。同时，GenAI 正在深刻塑造未来 SOC 的运营方式，包括 GenAI 在内的 AI 技术，连同自动化技术，将大幅提升 SOC 的运营效能。

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。

北约人工智能战略举措与影响分析

作者 刘安

2024 年 7 月 10 日，北约更新了其《人工智能战略》（以下简称《战略》）。在 2021 年《战略》的基础上，纳入了人工智能技术的最新进展，如生成式人工智能和人工智能赋能的信息工具，进一步压紧、压实人工智能战略目标和预期实现的成果。

北约认为，鉴于人工智能技术的迅速发展，北约需要为成员国负责任地使用人工智能提供基础，推动将这些技术应用到能力发展中，并防止恶意使用人工智能。为此，北约从战略制定与落实、机构设置与分工、技术投资与创新等多个层面推进人工智能发展应用。

一、顶层规划，明确发展方向

近年来，随着人工智能技术的飞速发展，北约认识到其对全球竞争格局和未来战争形态的深刻影响，并开始进行顶层战略规划和前瞻性布局。因此，北约通过制定和更新《人工智能战略》，确立了在人工智能领域的发展方向和行动指南，并适时进行迭代更新，以满足最新发展需求，应对技术发展带来的挑战与机遇。此外，北约还制定了《数据开发框架政策》（《政策》），加速推动负责任的人工智能应用。

（一）发布《人工智能战略》，明确 AI 发展方向和行动指南

2021 年 10 月，北约在国防部长峰会上通过首部《人工智能战略》，不仅涵盖了技术的研发和应用，还包括了伦理、法律及治理等多维度的考量，确保人工智能技术的军事应用既高效又符合国际法规和北约价值观，以支撑其开展集体防御、危机管理和合作安全三大核心业务。

《战略》明确了北约和盟国承诺在开发和应用人工智能全生命周期遵循的六项原则：一是合法，即符合国际人道主义法和人权法等国际法及成员国的国家法律等。二是问责制，落实人工智能在开发和使用过程中人类的主体责任制。三是可解释性和可溯源性，人工智能应用应当具有可解释性和透明度，接受北约或国家层面的检查和评估。四是可靠性，人工智能应用的全生命周期均应当满足安全性、可靠性和稳健性，并且可以通过北约已认定标准测序的测试。五是可治理性，开发人工智能应当符合预期，并且在出现意外情况时，具有应对和解决问题的能力。六是降低偏见，人工智能应用程序和数据集的开发和使用过程应当避免偏见。

在上述原则的指导下，《战略》提出了四大目标：一是鼓励盟国以负责任的方式开发和使用人工智能，以实现盟友的安全和国防安全。二是为研发新的人工智能成果提供建议，以增强互操作性，加速推动人工智能的成果转化应用。三是明确负责任地使用人工智能的具体

要求，在安全的前提下促进技术创新。四是识别并防范国家和非国家层面行为者恶意使用人工智能带来的威胁。可以看出，北约将坚持贯彻负责任的开发和应用原则，提升人工智能的赋能作用，并最大程度地降低不利影响。

（二）适应当前需求，适时更新《人工智能战略》

2024 年 7 月，北约在 2021 年《战略》的基础上，结合最新发展态势和发展需求，对《人工智能战略》进行了更新。新版《战略》继续坚持六项负责任的开发和使用人工智能的原则，战略目标和期望实现的成果较上一版进行了调整，更加符合当前发展需求。

基本战略方向不变，战略目标进一步压紧、压实。新版战略的四项目标可总结为：负责任开发，以实现国防和安全目的；加速交付，增强互操作性；管控风险，坚持创新；防范对抗性使用人工智能带来的威胁。与 2021 版《战略》相比，战略基调保持不变，仍然以国防和安全为首要目标，继续强调技术创新与风险治理平衡，加速推动相关应用成果转化，突出强调防范人工智能被用于对抗性军事活动带来的安全风险。

预期成果进一步扩充，旨在快速提升人工智能准备能力。新版战略结合人工智能技术发展变化，除了建立人才队伍、加强公私合作、利用北大西洋国防创新，加速计划支持人工智能发展、防止恶意使用人工智能行为等，新增了四方面，以全面提升北约及成员国在人工智能领域的准备能力，主要包括：一是将人工智能能力纳入盟国军事能力衡量标准；二是通过测试、评估、验证等过程，促进负责任的人工智能使用；三是提升人工智能系统在联盟间的互操作性；四是加强在国防和安全中负责任地使用人工智能的规范和标准制定方面的贡献。

两版《战略》在技术发展考量、战略重点、预期成果等方面各有侧重，反映了北约对人工智能技术演进的适应性，以及其在维护成果国安全和推动技术创新方面的持续努力。

（三）制定《数据利用框架政策》，提供政策指导和基础支持

北约《数据利用框架政策》是其《人工智能战略》的重要组成部分，是实现该战略目标的重要基础，为北约及成员国实现负责任的人工智能应用提供了根本支持和政策指导。《政策》明确提出将数据视为战略资产，愿景是通过充分利用北约的数据，在各个层面实现信息优势和数据驱动决策，重点是提高军民领域及政治领域的数据利用能力。该政策从人、技、法三方面全面促进数据安全、可靠、可信、便捷应用：一是以用户为中心，使其能够从数据中获取最大价值；二是建立单一逻辑环境，保障数据安全；三是建立简洁连贯的流程作为指导框架，促进数据利用。

人工智能数据模型和算法开发离不开安全、可靠、可信的基础数据，数据质量、多样性、可解释性、合规性、可访问性、持续性等直接影响人工智能成果的性能，而确保数据的上述特征得到有效保障是构建安全、弹性、有效、可行人工智能系统的基础。因此，北约《数据利用框架政策》通过规范管理数据，为人工智能系统数据模型和算法开发提供安全可信的数据来源，将有效推动其《人工智能战略》中“负责任地使用人工智能”战略愿景的实现。

二、政策配套，推动细化落实

为确保人工智能沿既定原则发展，推动实现预期成果，北约先后成立了指导技术实施的数据和审查委员会、为技术创新提供指导的新兴和颠覆性技术咨询小组，以及促进技术合作的北约创新委员会等，这些机构各司其职，共同为推动北约人工智能技术创新和成果应用提供了必需的保障。

（一）成立北约数据和审查委员会，推动人工智能转化应用

2022 年 10 月，北约国防部长批准建立北约数据和审查委员会 (Data and Review Board，DARB)，推动落实《人工智能战略》中六项负责任的使用原则，指导负责任的人工智能应用，帮助北约与企业、终端用户及国际社会建立信任，该委员会将作为交流论坛，为盟友和北约企业分享经验和进行成果交流提供平台。该委员会将为“以相对速度应用人工智能”扫清障碍，帮助北

> 北约认为需要为成员国负责任地使用
> 人工智能提供基础，
> 在 2021 年《人工智能战略》的基础上，
> 纳入了人工智能技术的最新进展，
> 进一步压实人工智能战略目标和预期实现的成果。

约和盟友完善负责任的人工智能实践，提供更安全、可靠、可互操作的系统，先于对手实现竞争优势。

（二）成立新兴和颠覆技术咨询小组，指导创新与成果转化

北约指出，人工智能、自主系统和量子技术等正在改变北约的运作方式，带来了新的挑战和机遇。北约不断加强与公私部门、学术界和企业界的合作，加速开发和采用新技术，建立负责任的使用原则，并通过创新保持北约的技术优势。

2020 年 7 月，北约秘书长宣布成立新兴和颠覆性技术咨询小组，其核心职能是为北约如何快速采用新技术及促进技术成果转化提供建议，旨在提升整个北约的技术水平。该小组由来自学术界和工业界的 12 名专家组成，就北约如何最好地资助其创新工作、建立创新中心运营网络、推广成功的创新业务和运营模式及提高整个北约的技术素养水平提供建议。该小组发布的首份年度报告中，就北约应对新兴和颠覆性技术的方法提出了具体建议，并认为北约有潜力成为全球技术创新的推动者。

（三）成立北约创新委员会，引领前沿技术研究

北约创新委员会（NATO Innovation Board）是北约在人工智能等新兴和颠覆性技术领域进行研究和政策建议的重要机构，由 12 名来自北约私营部门及学界的专家组成，负责引领前沿研究，并为北约在这些领域的政策提供长期和短期建议。北约创新委员会是北约在职能机构部署中的重要组成部分，遵循对 9 项新兴和颠覆性技术的整体规划。这些技术包括大数据与高级分析技术、人工智能、自主性等，它们被视为对未来军事行动具有重大影响的关键领域。

北约创新委员会的成立，体现了北约对科技创新在军事领域应用的重视，以及其在促进跨大西洋盟国与学界、私营部门合作方面的积极作用。通过这样的合作，北约旨在提升互操作性，解决关键的国防安全问题，并推动负责任的人工智能政策的制定和实施。此外，北约创新委员会由北约副秘书长担任主席、盟国高级文职和军事领袖参与，致力于研究、讨论和促进来自组织之外的新想法。

三、加强投资，促进生态布局

北约在明确的政策指导和细化方针的牵引下，加大技术投资，多项举措齐头并进，全方位推动人工智能技术发展。其中，在北约对人工智能等新兴颠覆性技术的投资中，首当其冲的是大北西洋国防创新加速器和北约 10 亿欧元的创新基金，为北约推动技术创新、应对潜在挑战奠定了坚实基础。

（一）启动北大西洋创新加速器，搭建技术创新平台

2021 年，北约领导人在布鲁塞尔北约峰会上，启动北大西洋国防创新加速器（DIANA），设立跨国风险投资基金，旨在寻求整个联盟范围内的先进军民两用技术。北约明确地将人工智能、量子、生物技术和人因增强、太空、高超声速等九个领域列为重点创新领域，并为每个关键技术领域制定了具体的计划。DIANA 的创立为北约加速在上述领域的技术创新和成果转化开设了通道。

DIANA 通过发布挑战计划，支持优秀团队开发解决关键国防和安全问题的新兴技术。DIANA 的愿景是为拥有

先进技术的创业公司、系统供应商、研发人员等提供平台，推进具有深刻影响的军民两用技术发展。该计划具体的运作方式是为通过其挑战计划入选的公司提供资金和指导，以发展深度技术来解决关键的国防和安全挑战。这些公司可以获得补助金、访问联盟内的加速器站点和测试中心权限、获得北约创新基金的资助等。

（二）成立北约创新资金，提供技术发展保障

北约创新基金（NIF）是北约为推动创新和科技发展而设立的风险投资基金，于 2021 年在布鲁塞尔峰会中启动，旨在投资有助于国防和安全的军民两用技术，与北大西洋国防创新加速器一脉相承，为其提供了必要的资金保障。该基金于 2023 年 7 月在立陶宛维尔纽斯举行的北约峰会上正式启动，计划在未来 15 年内代表北约成员国投资 10 亿欧元，以填补欧洲早期资金的重要缺口。

基金将投资于人工智能、大数据处理、量子技术、生物技术和人类进步、新材料、能源、推进和太空技术等领域的创业公司和其他风险投资基金。北约创新基金是北约推动成员国在技术治理和应用方面制定的一套共同标准和原则，旨在保持北约在创新和科技前沿的领先地位。北约创新基金致力于推动联盟内部的创新，确保北约在未来几十年内能够应对不断变化的安全挑战。

四、影响与建议

北约近年来加紧布局人工智能顶层规划，大力投入资金、资源推动人工智能发展，促进军民融合，激活这一颠覆性技术对军民领域的使能作用，对我在人工智能领域的布局和实施具有一定的借鉴作用。

一是人工智能在改变全球政治局势和安全态势方面的影响不断加深，我应警惕重视，及早谋篇布局。从北约的人工智能战略规划中不难看出，北约锚定人工智能的变革性影响和军事潜力，决心发展安全可靠、可信的人工智能，并根据技术发展进度和趋势，实时调整战略目标，势必要在全球人工智能竞赛中占据先发优势。对于全球而言，北约的这一战略可能会推动全球在人工智能领域的合作与竞争，同时也可能加剧全球安全领域的紧张关系。人工智能技术的快速发展给全球带来了诸多的机遇和挑战，以及深刻的不确定性。我应立足自身需求、顺应发展大潮，在人工智能领域这一新赛道上继续走“中国道路”，推动创新主体加快资本、人才、技术、数据、算力等要素的汇聚，促进人工智能创新链、产业链深度融合，在全球竞争浪潮中跻身前列。

二是人工智能被用于军事用途后，将改变全球安全态势，我应促进军民融合、加强技术攻关。北约成立北大西洋国防创新加速器，促进私营部门、学术界和其他非政府实体与北约的合作，最终目的寻求先进的军民两用技术，解决国防和国家安全面临的关键问题。北约的该计划与美国的 DARPA 和 DIU 的作用极其相似，都是作为一个“中介”，促进先进技术研发和成果转化，使国防机构和军方部门始终保持技术领先。该计划与 10 亿欧元的北约创新基金全面“落地生花”后，将极大地提升先进技术对北约作战赋能水平，给全球安全带来新的不确定性，加之其与美国的亲密关系，或对地区安定构成新的威胁。为此，我国应继续加强在人工智能领域的技术攻关，促进军民融合深度发展，加强核心关键技术的突破，尤其是在算法、机器学习、自主无人系统等前沿技术领域，推动各类人工智能技术快速嵌入作战要素、作战流程，满足智能化作战需求，保护国家安全和国防安全。

三是全球人工智能技术治理竞争激烈，深刻影响未来人工智能技术的发展方向和应用范围，我应积极作为，把握话语权。全球人工智能技术治理的竞争日趋激烈，除了北约，还有其他国家和地区在人工智能治理方面做出了努力，释放出一个强烈的信号，即各国和国际组织都在积极推动符合自己利益和价值观的治理框架和标准。尤其是以美国为首的代表，作为全球科技和军事领域的领先国家之一，在当前的国际政治经济格局中，蓄意助推与一些国家之间的竞争，特别是在科技、经济和安全领域。美国与一些国家和地区在人工智能领域建立了广泛的合作关系，力图传播利美国价值观，打造以自身为中心的国际联盟。无论是拉帮结盟，还是单兵作战，各国的行动都体现了试图引领人工智能技术使用原则和治理标准的制定。我需要警惕以美国为首、包括北约在内的西方阵营，可能打造不利于我或旨在遏制我发展的标准和规则体系，应利用国际法和国际平台，掌握制定人工智能治理国际规则的主动性，提出具有全局观的治理倡议。

关于作者

刘安

虎符智库研究员，主要从事人工智能、网络空间等领域政策研究。

欧盟人工智能立法的特点与影响

作者　张熠天 王丹

深入探讨欧盟在人工智能治理立法方面的概况、原则与机制、特点与缺陷，以及未来的立法趋势，可以揭示欧盟如何在保障个人权利、促进数据安全和推动技术发展之间寻找平衡点。

自 2015 年以来，欧盟一直致力于推动构建针对人工智能技术应用的监管体系，旨在平衡技术创新与风险管理，确保技术进步与社会伦理、个人隐私的和谐共生。通过成立人工智能高级别专家小组（AI HLE）和发布《人工智能法案》（Artificial Intelligence Act），欧盟不仅在内部加快了人工智能治理的法律框架建设，也为全球人工智能治理提供了重要的规则参考。深入探讨欧盟在人工智能治理立法方面的概况、原则与机制、特点与缺陷，以及未来的立法趋势，可以揭示欧盟如何在保障个人权利、促进数据安全和推动技术发展之间寻找平衡点，为全球人工智能治理提供启示。

一、欧盟人工智能立法概况

2018 年，欧盟成立了人工智能高级别专家小组，以便在欧盟内部加快建立人工智能监管的法律框架。随着《人工智能法案》的发布，欧盟在全球范围率先制定了人工智能风险分类和对应监管措施的治理规则体系，或将成为全球人工智能治理生态重要的规则参照，对其他国家的政策法规制定和监管执法方式产生积极的影响。

欧盟开始关注人工智能监管的源起主要是基于对技术发展的期待和对潜在风险的担忧，并且期待在两者之间找到某种平衡。2015 年 1 月，欧洲议会法律事务委员会（JURI）成立研究处理机器人和人工智能发展法律问题的工作组。2016 年 5 月，欧盟法律事务委员会发布了《就机器人民事法律规则向欧盟委员会提出立法建议的报告草案》（Draft Report with Recommendations to the Commission on Civil Law Rules on Robotics），从民事视角为受人工智能控制的机器人设定了明确的权利和义务。尽管该法律文件因涉及机器人法律地位的争议而受到一些批评，但是作为欧洲首个专门针对人工智能的政策文件，其对欧洲的人工智能发展及治理产生了深远的影响。

针对人工智能技术的快速发展及应用引发的伦理挑战，欧盟将人工智能伦理与治理纳入立法工作的重要议程。2017 年 5 月，欧洲经济与社会委员会（EESC）发布名为《人工智能对（数字）单一市场、生产、消费、就业和社会的影响》（The Consequences of Artificial Intelligence on the (Digital)Single Market, Production, Consumption, Employment and Society）的报告，分析人工智能带来的机遇和挑战，特别关注伦理、安全、

隐私等 11 个核心领域，并倡导建立人工智能伦理准则，同时确立人工智能监控与认证的标准体系。同年 10 月，欧洲理事会强调欧盟需迅速回应人工智能的最新发展，保障数据保护、数字权利及伦理标准的卓越制定，并指令欧盟委员会于 2018 年年初提出应对策略。2018 年 4 月 25 日，欧盟委员会向欧洲议会、欧盟理事会、欧洲理事会、欧洲经济与社会委员会及地区委员会提交了题为《欧盟人工智能》（EU Artificial Intelligence）的文件，标志着欧盟在人工智能领域正式启动战略布局。文件提出“以人为本”的人工智能发展路径，旨在提升欧盟科研和产业实力，应对人工智能与机器人技术带来的技术、伦理和法律等挑战，更好地服务欧洲社会经济发展。同年 6 月，欧盟委员会继续采取行动，委任 52 名来自学术界、产业界和民间社会的代表，组成人工智能高级专家小组。该小组为欧洲人工智能战略提供支撑，推动欧盟在人工智能领域的持续创新与发展。2019 年，欧盟人工智能高级别专家组发布了《人工智能伦理指南》（Ethics Guidelines for Artificial Intelligence），为人工智能的发展和治理确立了“以人为本”的基本原则。该指南明确了可信人工智能的三大核心要素，即人工智能必须遵守相关法律法规，符合伦理准则和价值观要求，并在技术与社会层面展现稳健性。这些原则逐渐在全球范围获得了广泛的认可，成为评估人工智能的重要标准。同年，欧洲议会研究服务机构发布了《算法的可问责和透明的治理框架》（A Governance Framework for Algorithmic Accountability and Transparency），为人工智能算法的问责机制和透明义务制定了清晰的规则。这些文件的发布，标志着人工智能领域的伦理治理和法规建设迈出了重要的一步，为人工智能的健康、可持续发展提供了坚实的保障。2021 年 4 月，欧盟正式发布了《人工智能法案（提案）》（The Artificial Intelligence Act(Proposal)）。在经过深入审议和充分讨论后，欧洲议会于 2024 年 3 月 13 日正式通过了该法案。此举意味着欧盟在全球人工智能治理领域取得了显著进展。该法案通过引入风险分级监管、市场准入制度及监管沙盒等创新机制，致力于解决人工智能算法的不透明性问题，从而确保在欧盟市场运行的人工智能系统安全。该法案使欧盟成为规范人工智能技术与应用的引领者。

欧盟持续推进数据治理领域立法工作，旨在确立欧洲数据利用和流转的规范体系。欧盟相继推出了《数字服务法案》（DSA）、《数字市场法案》（DMA）和《数据治理法案》（DGA））。这些法案共同构成了欧盟数据战略框架的核心监管规则。这些规则从基础逻辑层面出发，旨在加强数据安全保护，促进欧洲数据的自由流动，并防范算法自动化决策可能带来的潜在风险。此外，这些法案还致力于建立相应的伦理价值标准，保障个人权益，实现监管与创新发展的平衡与协调。这些努力体现了欧盟对数据治理和人工智能发展的高度重视。

二、欧盟人工智能立法的原则与机制

欧盟在人工智能治理领域采取的策略，集中展现了两种风险治理理念，即基于风险的规制和坚持实验主义的治理。具体而言，欧盟在人工智能风险防范的立法设计上，以风险为基石，对风险进行分类，并针对各类风险制定相应的监管措施。此外，欧盟亦致力于在监管机构、科创企业和用户之间构建共治格局，通过平等协商与信息透明的方式，达成实验性“契约”，从而在推动科技创新的同时，实现社会效果的最大化。

> 欧盟在人工智能治理领域采取的策略，
> 展现了两种风险治理理念，
> 在人工智能风险防范的立法设计上，
> 以风险为基石，对风险进行分类；
> 亦致力于在监管机构、
> 科创企业和用户之间构建共治格局。

（一）算法可解释性和透明度原则

随着自动化决策技术的广泛应用，数据安全和隐私保护问题逐渐显现。欧盟通过制定《通用数据保护条例》（GDPR）等，规范了算法自动化决策，强调了透明度和算法问责原则的重要性。GDPR 第二十二条规定，数据主体有权拒绝仅基于算法自动化处理的决策。法国在 1978 年也提出了数据主体对自动化处理逻辑信息的知情权，并

赋予其拒绝自动化处理决定的权利。尽管产业界对这些法规仍存在争议，认为算法可能无法达到完全可解释的效果，披露算法运行机制无实际意义，并可能涉及商业秘密保护问题。因此，如何平衡数据主体权益、技术可行性和商业秘密保护，仍需要进一步探讨。

（二）风险分级分类与算法安全评估

《人工智能法案》详细制定了人工智能系统的监管框架，并特别突出了基于风险评估的分类分级监管策略。根据该法案，AI 系统被划分为四个风险等级，即不可接受风险、高风险、有限风险和低风险，每个等级均配有相应的监管措施。此外，该法案还明确了人工智能产品的全生命周期监管要求，从研发、上市到运营，均须确保符合法规标准。同时，数据保护和算法治理也受到了广泛关注。有专家建议将数据保护影响评估制度与 GDPR 的公私协同治理制度相结合，构建个人数据权利与算法治理相结合的影响评估机制。值得一提的是，欧盟的《算法的可问责和透明的治理框架》也提出了对公共机构实施算法影响评估的强制性要求，旨在提升公众对 AI 技术的信任度。

（三）人工智能治理的外部问责机制

算法决策在数字生活中发挥了重要作用，如搜索引擎、社交媒体、金融市场和政策制定等。欧盟颁布的《算法的可问责和透明的治理框架》明确了算法决策的规制路径和政策建议，重视算法决策，为全球算法监管提供参考。该框架要求公开算法的工作原理、数据来源和使用目的，确保透明度和可问责性，同时要求定期审查和评估算法，确保公正性和准确性。欧盟的《人工智能法案》从平台主体义务、监管机构职责、处罚措施等方面，构建了人工智能算法的外部问责机制。该法案要求平台主体遵守规定和标准，如数据来源合法、设计合理、决策过程透明等，并接受监管机构的监督和管理，定期提交审查和风险评估报告。违反规定将受到处罚。这些举措为算法决策监管树立了新标杆，有助于保护公众权益和利益，促进人工智能技术健康发展。然而，算法监管仍是复杂而艰巨的任务，需要各国政府和国际组织共同努力，不断完善和优化监管机制，确保算法决策的公正性、透明度和可问责性。

三、欧盟人工智能立法的特点与缺陷

剖析欧盟人工智能治理框架，可以看出，欧洲在人工智能监管和治理方面主要强调个人自治权与人格尊严的保护作为核心原则。欧盟致力于构建一个全面的人工智能监管体系，确保数据主体的基本权利得到充分保障。同时，欧盟也积极探索制定统一的监管规则，防范人工智能发展可能带来的潜在风险，并在促进创新发展与确保安全规制之间寻求平衡。

（一）特点

具体而言，欧洲的人工智能监管框架展现出以下几个显著特点。

一是欧盟在治理理念层面秉持“以人为本”的核心理念，坚持发展与规制并行。欧盟旨在防范风险的同时鼓励创新，并通过立法手段，确保人工智能技术在尊重人权的基础上获得公众的信任与支持。这种以人为本的治理理念体现在欧盟《人工智能法案》中。该法案强调人工智能应作为人类的工具，最终目的是提高人类福祉。

二是欧盟试图在治理主体方面建立统一的监管机构，实现和 GDPR 监管的有效衔接，实现数据治理和算法规制的有效统一。欧盟委员会确立了四项关键目标，包括确保人工智能的安全与合法、实现对人工智能的科学治理和有效执法、弥补法律空白，以及形成人工智能的单一市场。欧盟通过建立人工智能高级专家小组，加快建立统一的人工智能法律监管框架的步伐。

三是欧盟强调以风险预防为导向的治理内容和手段，通过事前评估、事中监测、事后救济的多元路径，分级监管人工智能系统并规避其可能带来的风险。同时，欧盟强调个人赋权和外部问责的协同治理。《人工智能法案》采用分类分级的风险规制路径，在规定统一监管框架的基础上，识别和评估 AI 系统可能引发的风险，将 AI 系统分成四个风险级别，并对不同级别的风险采取不同的监管措施。

（二）缺陷

在审视欧盟对人工智能市场进行规制的策略时，需要关注其在实施过程中面临的挑战和缺陷。尽管欧盟在立法和监管方面做出了前所未有的尝试，旨在确保人工智能技术的安全性、合法性和对公共利益的保护，但这些措施也引发了一系列担忧和批评。

一是在推进市场规制路径的过程中，欧盟的责任机制暴露出制度性不足。欧盟选择以监管产品的手段管理人工智能，被视为一种切实可行的方式。目前，各国在保护消费者权益和监管产品质量方面已建立了成熟的体系，将人工智能产品纳入现有的规制框架，并进行必要的调整和完善。为了执行人工智能法案，欧盟计划修订产品责任规则和行业安全法律规则。该法案遵循“效果主义”原则，实施“长臂管辖”，确保在欧盟区域内使用的人工智能产品符合法案要求，保护欧盟公民的权益。法案主要侧重对人工智能产品提供者的监管，要求进行风险评估，并坚持“谁提供谁负责”的原则。然而，鉴于人工智能产品的用户同样承担重要的责任，有必要将实际参与的运营者也纳入责任体系，强化他们在预防和规避风险方面的责任和义务。

二是欧盟超前性制定相关监管措施，引发了产业界对发展前景的担忧。以《人工智能法案》为例，尽管其旨在保护公共利益和确保人工智能技术的安全与透明，但是反对者指出，该法案可能导致欧洲人工智能企业面临过高的成本负担，且部分合规要求在技术上难以实现。OpenAI 公司的 CEO 萨姆·阿尔特曼（Sam Altman）于 2023 年 5 月 22 日在 OpenAI 总部接受采访时表示，若监管过度，将考虑把公司撤出欧洲市场。欧洲议会议员布兰多·贝尼菲（Brando Benifei）认为，欧洲在人工智能立法方面已超前于风险本身。然而，过度监管可能会阻碍产业的发展。

> 欧洲在人工智能监管和治理方面主要强调个人自治权与人格尊严的保护作为核心原则。欧盟致力于构建一个全面的人工智能监管体系，确保数据主体的基本权利得到充分保障。

2022 年 9 月 28 日，欧盟委员会发布了《人工智能责任指令提案》（Proposal for an Artificial Intelligence Liability Directive）。这一提案提及在 2020 年的一项针对使用人工智能技术的欧洲企业的调查中，欧洲企业视责任问题为其使用人工智能技术的前三大障碍之一。对于计划但尚未采用人工智能技术的欧洲公司来说，43% 的公司将责任问题视为最被关注的外部障碍之一。过度和超前的监管可能导致欧洲在人工智能领域落后，影响相关技术的开发进程。尽管欧盟委员会预测大部分人工智能应用属于低风险类别，但是事前监管仍然可能对开发活动产生负面影响。总体而言，该法案更多地倾向于规制型立法，对于促进产业发展的规定相对较少。因此，如何在确保技术发展与监管创新之间达到平衡，仍是欧盟需要继续探索和完善的重要议题。

三是欧盟过于倚重企业自治，规制的有效性受到质疑。欧盟《人工智能法案》虽规定了人工智能系统提供者需进行内部合规评估，却未确立外部监管机制。欧洲数字权利组织对此表示关切，认为这为企业赋予了过大的自我规制权力。欧洲数据保护委员会（EDPB）和欧洲数据保护专员公署（EDPS）发布的工作指南指出，监管机制的缺失可能削弱该法案治理工具的有效性和可执行性。此外，该法案在人工智能系统入市后的监管方面显得过于宽松，与入市前的严格监管形成鲜明对比，导致监管失衡。考虑到人工智能系统一旦被开发和应用后，传播和扩散速度极快，这无疑降低了规制的有效性。因此，为确保人工智能技术的健康发展，欧盟亟待建立更为全面、严谨的监管体系。

四是欧盟对人工智能的相关定义和分类，引起质疑和警惕。欧盟人工智能的监管试图通过列举监管对象的方式明

确范围，然而，由于人工智能技术的日新月异，这种列举方式很可能无法完全覆盖所有的应用领域。对人工智能的定义要么过于宽泛，包含太多非核心的概念，要么过于狭窄，滞后于技术的发展。此外，尽管法案尝试明确监管对象，但仍存在遗漏。例如，深度伪造技术作为一种高风险应用，却没有被明确纳入监管范围。深度伪造可以用合成技术生成和真实音频区分度很低的虚假音频，对社会稳定和个人隐私构成严重威胁。因此，将其纳入监管范围是十分必要的。EDPB 和 EDPS 发布的工作指南指出，法案的高风险清单还存在其他遗漏。例如，使用人工智能系统确定保险费或评估医疗方法适用于健康研究目的的场景，这些领域同样涉及大量的个人数据处理和隐私保护问题，因此，也应纳入监管范围。

四、欧盟人工智能立法的影响

欧盟在人工智能治理方面的立法趋势，不仅反映了对技术发展的前瞻性思维，也体现了在全球科技伦理和法律规范制定领域的领导力。人工智能作为新一轮科技革命的核心，对经济结构、社会治理，乃至国际关系，都产生了深远的影响。欧盟通过制定严格的法律政策，旨在确保技术进步不会以牺牲个人隐私和社会伦理为代价。

一是欧盟 GDPR 的实施，虽然在一定程度上限制了数据驱动的技术创新，但也为个人数据保护设立了全球性的高标准。欧盟在此基础上出台《人工智能法案》，试图在保护个人隐私和促进技术发展之间找到平衡。该法案的分级动态监管模式，不仅为人工智能系统的安全性和透明度设定了明确的标准，也为全球其他国家在人工智能立法方面提供了参考。

二是欧盟《人工智能法案》特别强调支持小微企业，表明欧盟意识到创新不仅仅来自大型企业，中小企业同样是推动技术进步的重要力量。通过监管沙盒等措施，欧盟支持中小企业广泛研发和应用人工智能技术，有助于创造一个更加多元和活跃的创新生态系统。同时，这也有助于防止大型企业形成垄断，确保市场的公平竞争。

三是尽管欧盟的人工智能治理框架在促进技术创新和保护个人隐私方面取得了一定的进展，但其严格的监管措施也可能给跨国企业带来挑战。全球企业都需要适应欧盟的法律法规。这不仅增加了企业的合规成本，也可能影响全球人工智能技术的交流与合作。此外，人工智能技术的快速发展和应用的多样性，使任何监管框架都需要具有一定的灵活性和适应性，以便应对不断变化的技术环境。

总体而言，欧盟的人工智能治理立法趋势，为全球人工智能治理提供了宝贵的经验。其强调了在促进技术创新的同时，必须考虑伦理道德、个人隐私和社会影响。随着人工智能技术的不断进步和应用领域的扩大，全球各国都需要在立法、监管和伦理指导方面进行深入的思考和合作，确保人工智能技术能够造福人类社会，而不是成为新的风险源。欧盟的这些努力，无疑为全球人工智能治理提供了启示和方向。

本文选自《中国信息安全》杂志 2024 年第 4 期

关于作者

张熠天 王丹

国家工业信息安全发展研究中心

浅谈勒索病毒原理及防范措施

作者 陈俊宇 姚文龙 黄子涵 陈艺文 李家志 李光宇

摘要：在人工智能时代的到来下，计算机信息安全与防护变得愈发重要。勒索病毒作为一种恶意软件，已经成为当前网络安全领域中最严重的威胁之一。文章以勒索病毒的案例作为研究对象，首先分析了勒索病毒的原理，然后介绍了这些勒索病毒攻击方式，接着以 wannacry 勒索病毒作为案例，解析其工作原理，最后又具体探讨了相应防范措施，以供参考。

引言

企业面临的最严重的问题之一是勒索软件。为了较好实现保障计算机网络安全，技术人员应该在全方位分析明确所有安全漏洞的基础上，了解存在的勒索病毒原理，进而基于这些常见勒索病毒进行防范，以求营造较为理想的计算机网络安全环境，相关研究极为必要。

一、什么是勒索病毒

勒索软件是一种恶意软件，通过加密阻止计算机用户访问他们的数据。网络犯罪分子利用勒索软件向其黑客入侵的个人或组织勒索钱财，并将数据作为人质，直到赎金支付。

如果网络犯罪分子不在规定的时间内支付赎金，数据可能会泄露给公众或被永久损坏。

近年来，企业、个人和政府组织都是勒索软件攻击的受害者，恢复其系统需要花费大笔资金。计算机是如何感染勒索软件的？勒索病毒作为一种恶意软件，起源于互联网时代的早期。从最早的文件加密型勒索病毒到如今的勒索软件即服务（RaaS）模式，勒索病毒不断演化和进化，威胁范围也越来越广泛。勒索病毒的付款方式通常采用加密货币，如比特币。这使得追踪和追诉不法分子变得困难，增加了受害者恢复被加密文件的难度。

在“新型冠状病毒肺炎”流行期间。威胁行为者甚至利用人们的恐惧心理在人们心理防备最脆弱的时候通过分发与冠状病毒相关的恶意应用程序，如冠状病毒跟踪器，症状识别器，冠状病毒分布地图等，或伪装成与 COVID-19（新型冠状病毒肺炎）相关的文件名、话题，诱导用户安装恶意程序。

二、勒索病毒的攻击策略

网络钓鱼是最常用的策略之一，攻击者会利用各类媒介传播勒索病毒，具体可分为以下几类：电子邮件网络钓鱼、网站弹窗、远程桌面、驱动捆绑安装。

电子邮件网络钓鱼：网络犯罪分子一直使用这种方法来发送勒索软件。电子邮件是精心构建的，目的是误导

受害者点击链接或打开附件。攻击系统的恶意文件包含在链接或附件中，点击后，它将获得对系统文件和数据的访问权限。当恶意软件感染计算机时，它会对文件进行加密，并在某些情况下锁定机器的所有者或用户。连接到网络的其他系统（计算机和服务器）将感染更复杂的勒索软件。

网站弹窗：当你点击随机网站上的恶意弹出窗口时，勒索软件会感染你的机器。尽管并非所有网站弹出窗口都是恶意的，但黑客还是会利用它们向受害者勒索钱财。勒索软件攻击者的弹出窗口通常会提示你更新计算机上的程序，或者让你相信你的系统感染了恶意软件，需要点击链接将其删除。

远程桌面：远程控制桌面旨在允许 IT 经理出于工作目的远程访问机器。尽管它是出于善意建立的，但黑客们已经把它变成了一个赚钱的计划。端口 3389 用于桌面控制。由于 3389 端口在许多系统上是开放的，黑客可以访问他们认为易受攻击的系统。他们将通过尝试使用暴力方法以管理员身份登录来获得访问权限。网络盗贼将可以完全访问计算机，并且一旦成为管理员，就可以对任何数据进行加密。一些网络犯罪分子甚至更进一步，禁用端点保护或破坏 Windows 文件备份。

驱动捆绑安装：这种破坏用户机器的方法是在用户不知情的情况下发生的——当用户访问被黑客入侵的网站时，就会发生勒索软件攻击。在病毒传播之前，用户不需要点击任何内容。合法网站上的免费下载通常被网络犯罪分子使用，尤其是在网站易受影响的情况下。另一方面，其他网络犯罪分子创建了一个网站，而不是闯入一个网站。当访问者访问一个感染了恶意软件的实际网站时，他们将被重定向到网络犯罪分子完全控制的另一个网站。一旦用户的计算机被黑客入侵，就会出现一封勒索信，要求支付系统解锁和文件解密的费用。

三、勒索病毒实例

通过对勒索病毒实际案例的分析，我们可以更加深入地了解其危害和影响。本章将选择一些具有代表性的勒索病毒案例，并从不同角度进行剖析，包括攻击手段、感染途径、受害者情况等。通过对这些案例的分析，读者可以更好地认识到勒索病毒对个人和组织所造成的巨大损失。

为此我们选取奇安信公司提供的勒索病毒 WannaCry 病毒样本进行勒索病毒代码解析，该病毒分为两个部分：一是蠕虫部分，用于病毒传播，并释放出勒索病毒。二是勒索病毒部分，加密用户文件索要赎金。

（一）蠕虫部分：蠕虫代码运行后先会连接某个设定好的域名，若该域名可以成功连接，则直接退出。这个域名实际上就是所谓的“Kill Switch”开关，也就是病毒中检测的网址是否可以访问的代码片段，如果可以访问则不会利用“永恒之蓝”漏洞继续传播。如果上述域名无法访问，则会安装病毒服务，服务的二进制文件路径为当前进程文件路径，并启动服务。释放资源到系统盘系统文件目录下的 tasksche.exe（该程序是勒索病毒），并将其启动。蠕虫病毒服务启动后，会利用 MS17-010 漏洞传播。传播分为两种渠道，一种是局域网传播，另一种是公网传播。

病毒会根据用户计算机内网 IP，生成覆盖整个局域网网段表，然后循环依次尝试攻击。

公网传播主要代码如下图，病毒会随机生成 IP 地址，尝试发送攻击代码。

蠕虫的 PE 文件中包含有两个动态库文件，是攻击模块的 Payload，分别是：x86 版本的 Payload 和 x64 版本的 Payload。两个 Payload 都是只有资源目录结构没有具体资源的无效 PE 动态库文件。病毒在攻击前，会构造两块内存，在内存中分别组合 Payload 和打开 Worm 病毒自身，凑成有效攻击 Payload。

之后病毒会使用 MS17-010 漏洞，通过 APC 方式注入动态库到被攻击计算机的 Lsass.exe，并

> 为了较好实现保障计算机网络安全，
> 技术人员应该在
> 全方位分析明确所有安全漏洞的基础上，
> 了解存在的勒索病毒原理，
> 进而基于这些常见勒索病毒进行防范，
> 以求营造较为理想的计算机网络安全环境，
> 相关研究极为必要。

```
while ( 1 )
{
  do
  {
    if ( GetTickCount() - time_1 > 2400000 )
      flag_1 = 1;
    if ( GetTickCount() - time_1 > 1200000 )
      flag_2 = 1;
    if ( !flag_1 )
      break;
    if ( a1 >= 32 )
      break;
    v8 = call_random(v7);
    v7 = (void *)255;
    random_a = v8 % 0xFF;
  }
  while ( v8 % 0xFF == 127 || random_a >= 224 );
  if ( flag_2 && a1 < 32 )
  {
    v9 = call_random(v7);
    v7 = (void *)255;
    random_b = v9 % 0xFF;
  }
  random_c = call_random(v7) % 0xFFu;
  random_d = call_random((void *)0xFF);
  sprintf(&random_ip_address, aD_D_D_D, random_a, random_b, random_c, random_d % 0xFF);
  ulAddr_1 = inet_addr(&random_ip_address);
  if ( call_connect(ulAddr_1) > 0 )
    break;
LABEL_23:
  Sleep(100u);
}
flag_1 = 0;
flag_2 = 0;
v21 = GetTickCount();
index = 1;
while ( 1 )
{
  sprintf(&random_ip_address, aD_D_D_D, random_a, random_b, random_c, index);
  ulAddr = inet_addr(&random_ip_address);
  if ( call_connect(ulAddr) <= 0 )
    goto LABEL_20;
  v15 = (void *)beginthreadex(0, 0, MS17_010, ulAddr, 0, 0);
  v16 = v15;
  if ( v15 )
    break;
```

```
int exec_worm()
{
  struct _STARTUPINFOA StartupInfo; // [sp+4h] [bp-54h]@1
  struct _PROCESS_INFORMATION ProcessInformation; // [sp+48h] [bp-10h]@1

  ProcessInformation.hProcess = 0;
  ProcessInformation.hThread = 0;
  ProcessInformation.dwProcessId = 0;
  ProcessInformation.dwThreadId = 0;
  memset(&StartupInfo.lpReserved, 0, 0x44u);
  StartupInfo.cb = 68;
  StartupInfo.wShowWindow = 0;
  StartupInfo.dwFlags = 129;
  if ( CreateProcessA(0, worm_file_path, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation) )
  {
    CloseHandle(ProcessInformation.hThread);
    CloseHandle(ProcessInformation.hProcess);
  }
  return 0;
}
```

执行 Payload 动态库的导出函数 PlayGame，该函数非常简单，功能就是释放资源“W”到被攻击计算机“C:Windows\mssecsvc.exe”，并执行，如上图所示。

被攻击的计算机包含病毒的完整功能，除了会被勒索，还会继续使用 MS17-010 漏洞进行传播，这种传播呈几何级向外扩张，这也是该病毒短时间内大规模爆发的主要原因。目前，攻击内网 IP 需要用户计算机直接暴露在公网且没有安装相应操作系统补丁的计算机才会受到影响，因此那些通过路由拨号的个人用户，并不会直接通过公网被攻击。如果企业网络也是通过总路由出口访问公网的，那么企业网络中的计算机也不会受到来自公网的直接攻击。但是，现实中一些机构的网络存在直接连接公网的计算机，且内部网络又类似一个大局域网，因此一旦暴露在公网上的计算机被攻破，就会导致整个局域网存在被感染的风险。

（二）勒索病毒部分

该部分主要包含如下四个模块。

1. 删除临时目录下的所有特定扩展名文件，即加密文件。2. 以任意 session 运行指定程序。3. 加解密程序。4. 通信模块。

解密加解密模块数据得到含有主要加密逻辑代码的动态库，通过其模拟的 LoadLibrary 和 GetProcAddress 函数调用该动态库中的导出函数执行其加密逻辑。勒索主逻辑执行时，先会导入一个存放在镜像中的 RSA 公钥，之后调用 CryptGenKey 生成一组 RSA 算法的 Session Key。之后将这组 Key 的公钥通过 CryptExportKey 导出，再写入到 00000000.pky 文件中。将 Session Key 中的私钥用导入的 RSA 公钥进行加密。

如果遍历到的文件扩展名在欲加密的文件扩展名列表中，则会将当前文件路径加入文件操作列表中，在遍历文件结束后一并进行文件操作，对于每个需要加密的文件，都会调

用 CryptGenRadom 随机生成 AES 密钥，之后使用 Session Key 中的 RSA 公钥对 AES 密钥进行加密，存放在加密后的数据文件头中，之后将原始文件数据用该 AES 密钥进行加密。

因为病毒是生成加密过的用户文件后再删除原始文件，所以存在通过文件恢复类工具恢复原始未加密文件的可能。但是因为病毒对文件系统的修改操作过于频繁，导致被删除的原始文件数据块被覆盖，致使实际恢复效果有限。且随着系统持续运行，恢复类工具恢复数据的可能性会显著降低。

四、勒索病毒的防治手段

基于对现有病毒标本、文献和数据的分析，现提出以下勒索病毒的防治手段。

个人层面：

1. 加强密码安全性：确保所有系统和服务都使用强密码，并定期更换密码。此外，禁用或限制远程登录功能，减少 3389 扫描弱密码登录的风险。

2. 更新和维护系统：及时安装操作系统和应用程序的安全补丁，以修复已知漏洞，并定期更新杀毒软件和防火墙等安全工具。

3. 数据备份与恢复：定期备份重要数据，并将备份数据存储在离线环境中，以防止勒索病毒感染后无法访问数据。同时，建立有效的数据恢复计划，以便在遭受攻击时能够快速恢复数据。

4. 网络监控与入侵检测：部署网络监控工具和入侵检测系统，实时监测网络流量和异常活动，并及时采取相应的响应措施。

5. 员工教育与培训：加强员工对勒索病毒等网络安全威胁的认识和意识，提供相关培训和教育，使其能够正确使用计算机设备并警惕潜在的网络攻击。

网络管理员层面：

1. 应监测和分析网络流量，及时发现和隔离疑似的勒索病毒活动。他们还应定期更新和修补系统漏洞，以防止勒索病毒利用这些漏洞入侵系统。

2. 对设定端口进行监控（非监听），理论上所有端口都可。主要是 3389 或者修改了远程连接的端口。为了及时发现和阻止勒索病毒的传播，我们需要对设定端口进行监控。这意味着我们需要实时监测网络中各个端口的活动情况，并及时发现异常行为。在理论上，我们应该监控所有端口，但特别要关注 3389 端口或者已经修改过远程连接端口的情况。

3. 设定监听频率（分钟），设置合适的监听频率对于及时发现勒索病毒感染至关重要。根据实际情况，我们可以根据网络流量和系统负载来设定监听频率。通常来说，较短的监听间隔能够更快地检测到异常活动，但也可能增加系统负担。因此，在设置监听频率时需要权衡考虑。

4. 设定推送地址，以便把连接服务器设定端口的 IP 地址投递到手机上。为了及时获取到连接服务器设定端口的 IP 地址，我们可以使用推送服务。

5. 自定义服务器姓名，以区分是哪台机器。

为了方便区分不同的服务器，我们可以为每台机器自定义一个独特的名称。这样，在应急响应流程中就能清楚地知道是哪台机器受到了勒索病毒的威胁或发现了异常活动。

6. 将 IP 地址转换成 mac 地址一并发到手机上。

除了获取连接服务器设定端口的 IP 地址，将其转换成可读性更好的地址形式也是有帮助的。通过将 IP 地址转换成 mac 地址，并将其发送到手机上，可以更直观地了解受到威胁的来源或异常活动发生的地点。

通过以上防治措施，可以有效减少勒索病毒的传播和感染，保护计算机系统和数据的安全。然而，需要注意的是，随着黑客技术的不断发展，我们应持续关注最新的安全威胁，并及时采取相应的防护措施来保护信息安全。安

关于作者

陈俊宇 姚文龙 黄子涵 陈艺文 李家志 李光宇

广西安全工程职业技术学院，广西 南宁 530100

基金项目：2021 年中国高校产学研创新基金——新一代信息技术创新项目“智慧校园中勒索病毒、挖矿木马安全分析与处置研究”（课题编号：2021ITA11010）

网安26号院 SECURITY INSIDER

征稿启事

当下，网络空间态势日趋严峻，关基设施成为重要攻击目标，因网络攻击导致的系统瘫痪、数据泄露现象频发。网络安全建设和运营需时刻因应形势变化进行创新。分享行业趋势、交流建设与运营之道成为提升安全防护水平的重要途径。

为此，奇安信《网安 26 号院》联合虎符智库、安全内参联合征稿。具体要求如下：

一、征稿对象：

投稿人为政企网络安全负责人、从业者，以及研究人员。

二、征稿时间：

本次活动活动长期有效。

三、征稿要求：

投稿论文应为投稿人原创，且尚未被任何期刊接受或发表。投稿人应对所投稿件的著作权及其他法律责任负责。

四、稿件说明：

来稿主题包括但不限于网络安全合规解读、网络攻防态势分析、网络安全建设经验、安全运营最佳实践，创新安全技术及应用等网络安全领域相关的议题。

稿件字数（含注释）原则上应控制在 4000 ~ 8000 字。

五、评选及奖励：

来稿经专家组评审入选刊登后，即获得相应的稿费（不低于 2000 元人民币）。

优秀获奖作者将有机会受邀参加 “BCS 北京网络安全大会”，发表主题演讲并分享研究心得。

六、其他荣誉：

长期供稿作者可以获聘“虎符智库”专家，授予聘书和徽章。

七、投稿方式：

投稿以附件形式通过电子邮件
发送至 lijianping@qianxin.com;
或者微信添加 security4 咨询联系。

扫码咨询

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