极牛网络安全通讯 • 社群期刊

2024 年 8 月 第 38 期

网安观察

第38期

2024年8月

CONTEN

目录

安全态势

国际视野

P8 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

ONTENTS

专题报道

第 3 8 期

《网安观察》编辑部

主办　极牛网

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

公众号　小程序　网站

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

E m a i l：hi@geeknb.com
地　　址：深圳市龙岗区天安云谷2栋2层
邮　　编：518000
电　　话：0755-33228862

印刷数量：1000 本
印刷单位：深圳彩虹印刷有限公司

政策篇

国内，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。

红帽人才工程

Cyber Crime Governance Talent Training Project

工程简介

在“全国网络警察培训基地”的指导下，中国下一代网络安全联盟牵头发起「红帽人才工程」，联合华云信安、美亚柏科、高联通信等知名网络安全企业，围绕“网络犯罪治理、涉网犯罪打击”等相关网络安全课题，持续挖掘、培养、资助、赋能网络安全人才，构建红色基因的网络空间安全人才防线。

申报流程

课题征集 → 课题公示 → 立项评审

研究课题计划征集

研究课题信息公示

研究课题立项评审

申报说明

项目资讯

培养对象

政企单位在职人员、高校全日制在校生（含研究生）、互联网企业技术人员、网络安全企业技术人员以及社会网络安全人才...

核心课题

内网攻防、社工钓鱼、远控木马、免杀加壳、情报甄别、资金分析、调证溯源、取证固证、远程勘验、APP反编译、二进制逆向...

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

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。

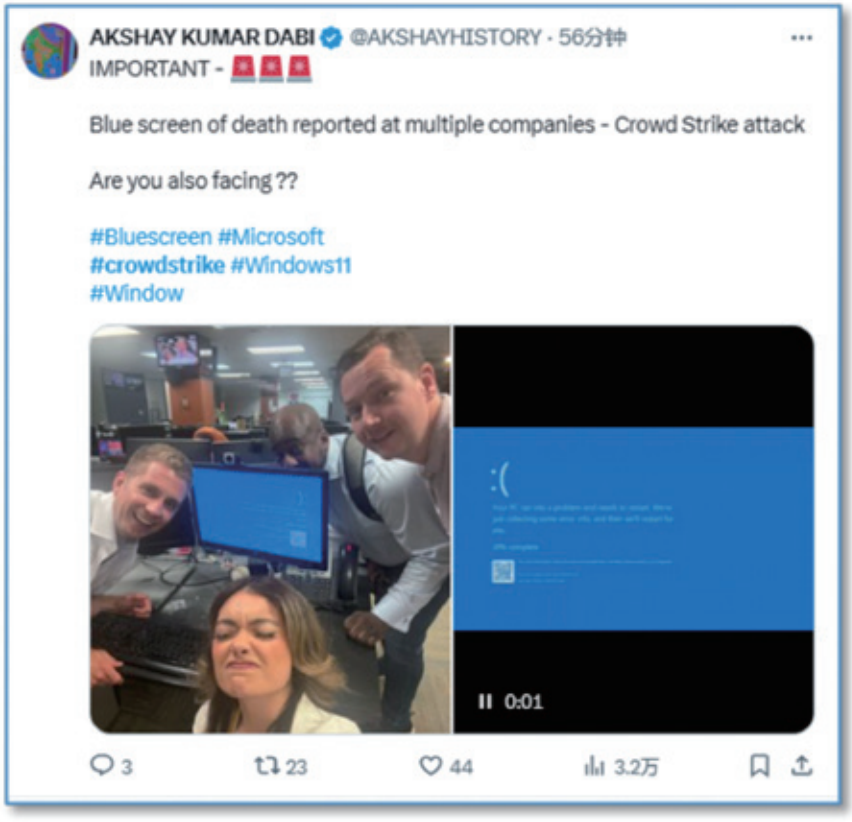
Falcon 平台是 CrowdStrike 的核心产品，它是一个完全基于云端部署的 SaaS 模型，能够提供实时的攻击指标、威胁情报和不断进化的对手手法技术。该平台通过一个轻量级的代理架构实现快速且可扩展的部署，并提供高级别的保护和性能。此外，Falcon 还集成了多种功能，如文件完整性监控、云安全、身份保护等。

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。

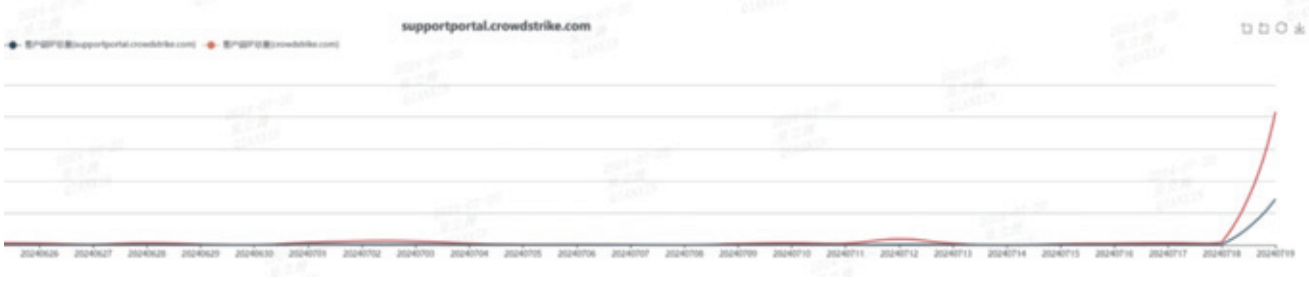
CrowdStrike 本次 IT 系统中断事件的影响一定会被记入史册，与 2017 年的 WannaCry 勒索蠕虫事件可相提并论，所幸由于安全软件生态一定程度的隔离，中国所受的影响不大。

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

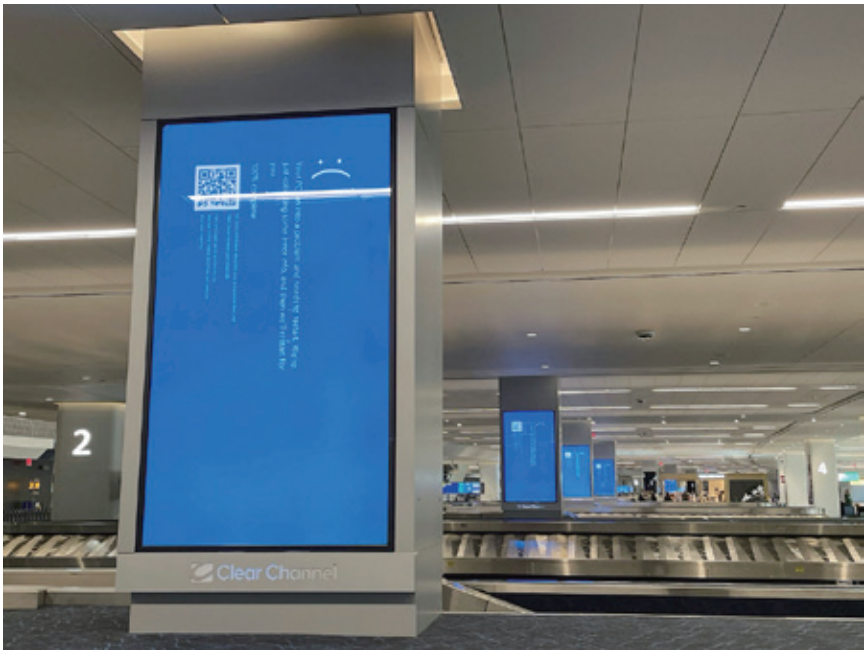
· 持续推进国产化，安全软件工具平台与操作系统一样有特殊的影响和意义，必须确保自主可控。

· 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

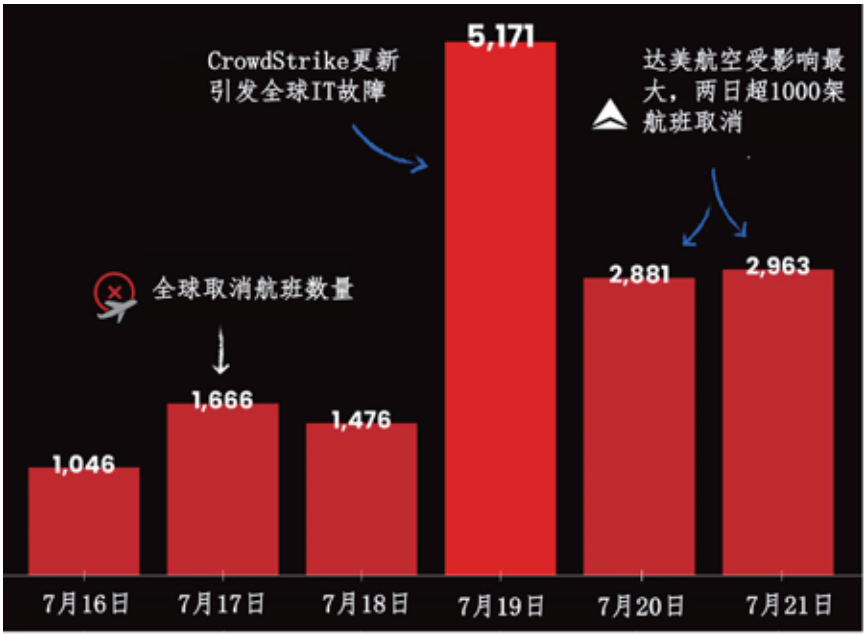
根据航班跟踪与数据平台 FlightAware 的数据，7 月 19 日超过 5,000 个航班被取消，比过去三天的平均取消数量高出 270%。

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。

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。

揭秘：网络活动操纵各国大选

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。

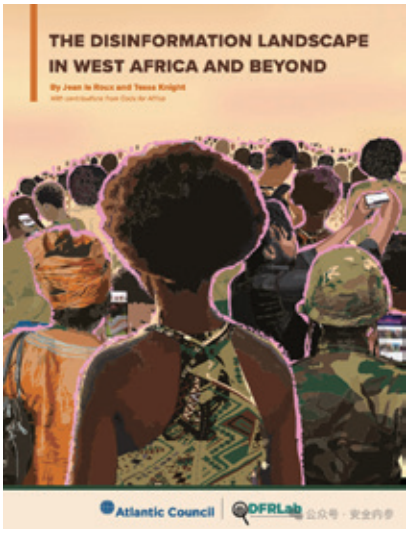
Duerksen 表示：“虚假信息不仅是技术问题，更是社会和政治问题。我们需要采取多层次的应对措施来增强韧性。因此，网络专家的工作只能是解决方案的一部分。然而，虚假信息攻击活动正日趋复杂，它们利用网络攻击来放大、洗白和煽动虚假信息。”

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。

从 Gartner2024 年北美安全峰会看安全运营的技术趋势

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。

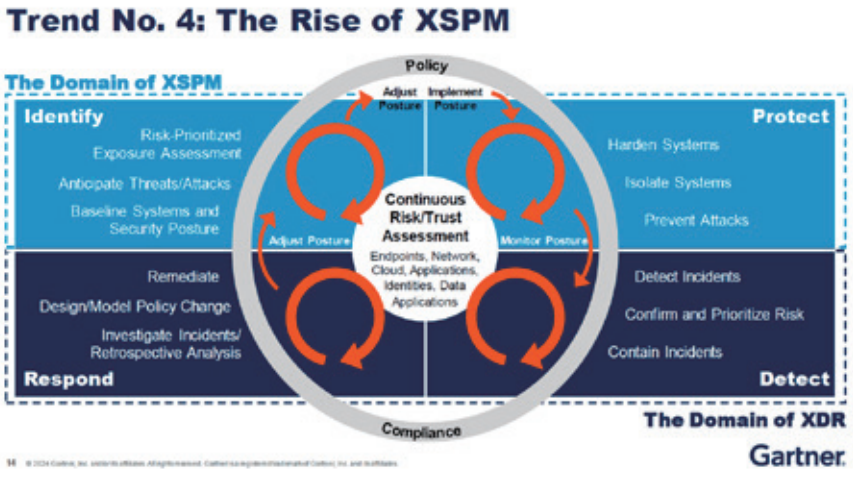


图 1

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

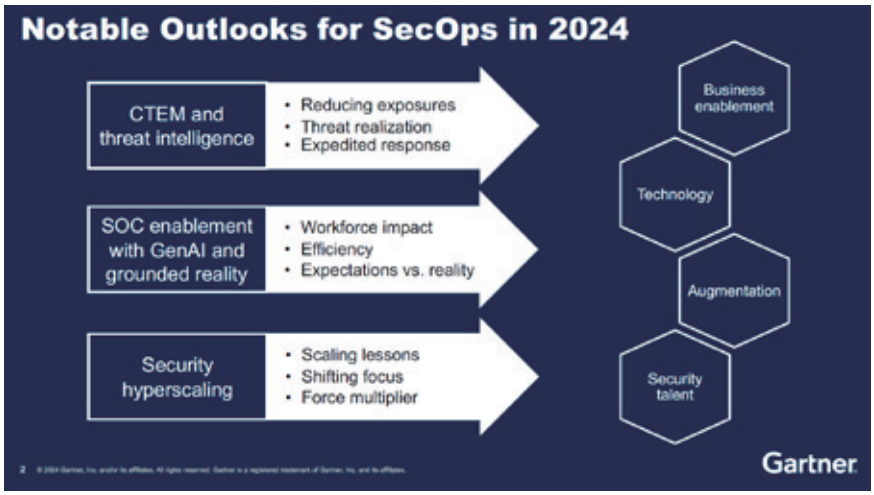


图 2

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。

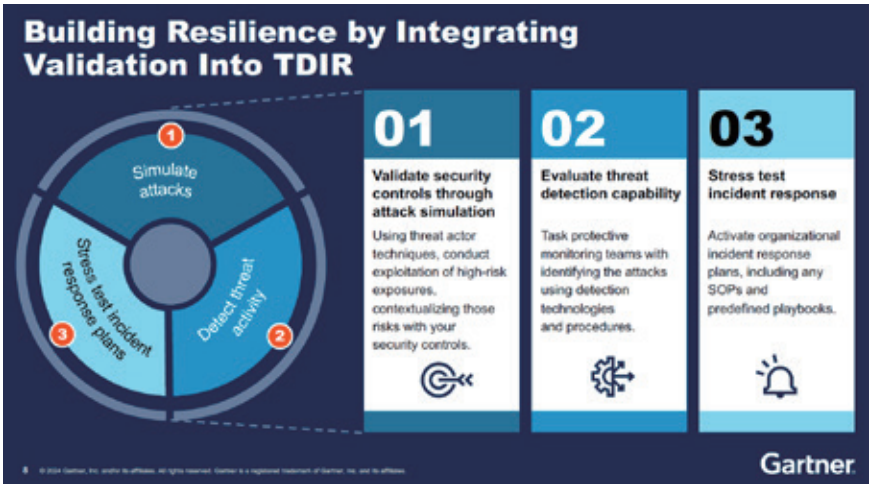


图 3

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。

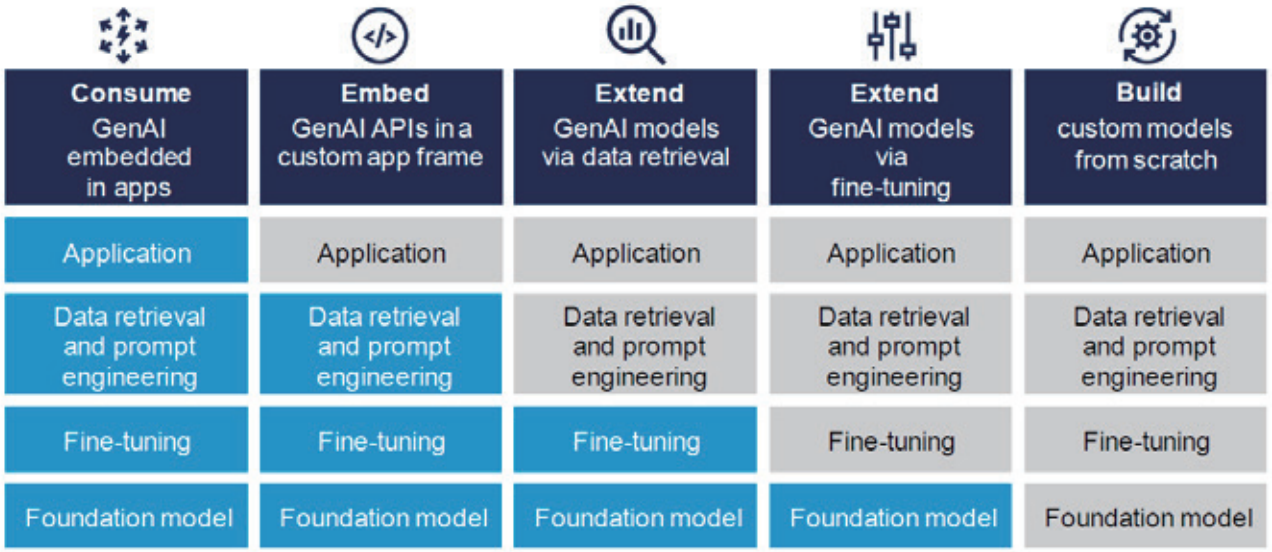


图 4

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。

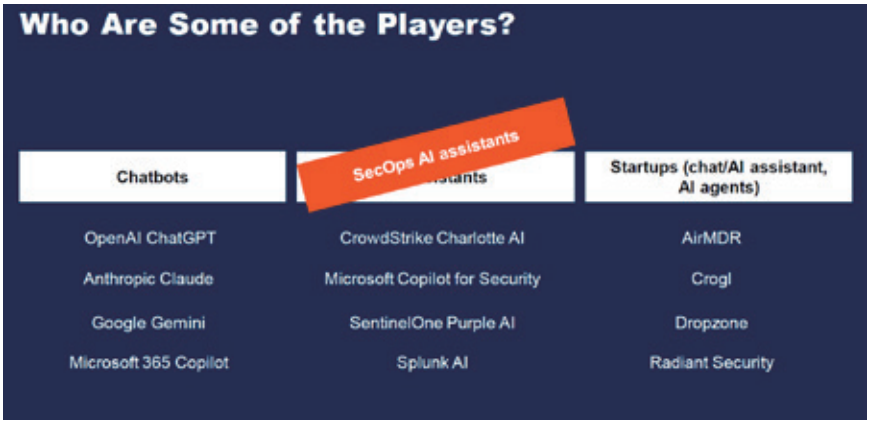


图 5

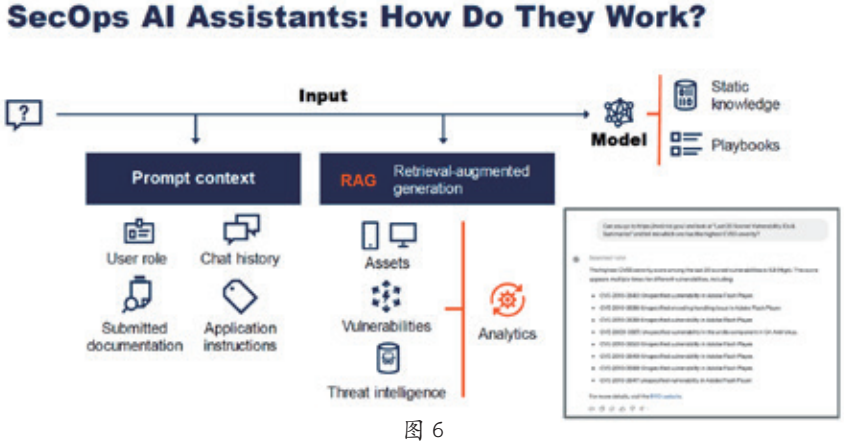


图 6

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。

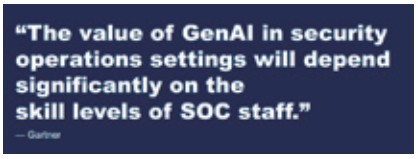


图 7

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？

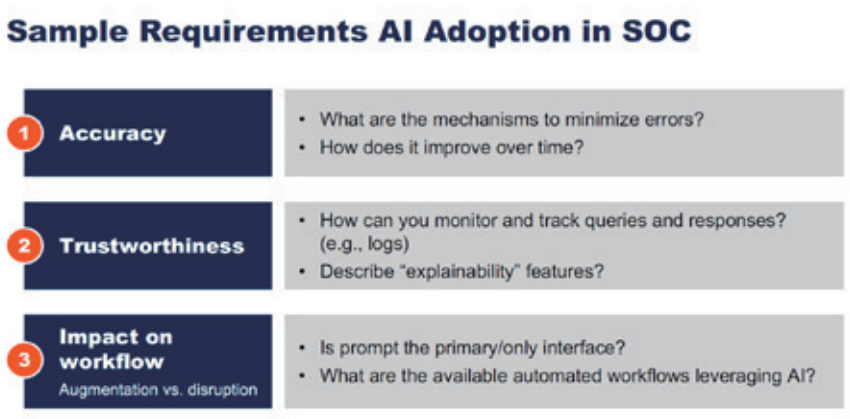


图 8

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

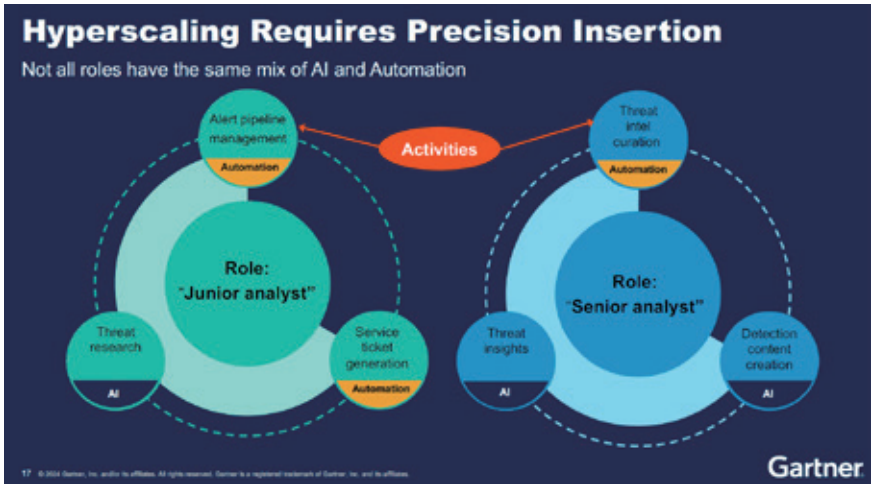


图 9

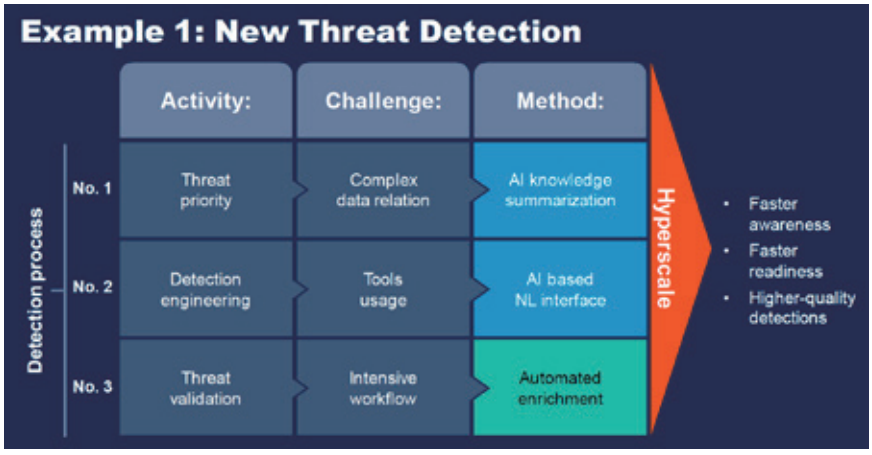


图 10

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。

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