内部发行 免费赠阅

出版物准印证号：京内资准字 2122- L0058 号

SECURITY INSIDER

网安26号院

奇安信网络安全通讯 · 安全快一步

透视 RSAC 2023

P14

第29期
2023 年 5 月

奇安信
新一代网络安全领军者

打造新一代中国特色的安全托管服务

时刻守护您的网络安全

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

两种模式
模式随心选择

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

多种形态
全面助力建成

- 城市运营中心
- 行业安全运营中心
- 企业安全运营中心

两化融合
帮您真正实现

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

首创“云地结合”模式

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

7*24h实时持续监测

“地球不爆炸，我们不放假”——7*24h持续监测，充分保障常态化运营。

安全事件响应快一步

对APT攻击、网络攻击等长效监测，提前预警，响应快一步。

安全事件处置规范化

事前检测、事中分析、事后总结，真正实现闭环，并在实战中不断加固。

专家“一对一”指导

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

整合与 AI 将塑造网络安全的未来?

在已结束的安全风向标 RSAC 2023 会议上，整合与人工智能两大主题成为大会的焦点，被分析人士认为将会重塑网络安全的未来。

面对日益复杂的 IT 环境的风险，机构需要更高的效率、实时数据可见性和跨网络的端点、身份和资产的统一视图。作为这一需求的回应，包括 CrowdStrike、谷歌、Mandiant、埃森哲和 Palo Alto Networks 等领先安全厂商发布了数十个联盟和合作伙伴关系，比以往任何一届会议都要多，充分体现出本次大会的“Stronger Together”（携手更强大）主题。

与此同时，人工智能应对网络攻击的重要性也在会议上得到了强调。因为攻击者越来越多地使用该技术，同时基于大语言模型的生成式 AI 快速发展带来新的威胁和机会。

RSA Security 首席执行官 Rohit Ghai 在主题演讲时认为，AI 将对安全行业产生重大影响。（人工智能有助于改进身份管理和安全自动化）没有人工智能，零信任的目标则无法实现。Palo Alto Networks 董事长兼首席执行官 Nikesh Arora 也认为，需要“以 AI 对抗 AI”。

随着 ChatGPT 的爆炸式增长，每个人都想参与其中。人工智能在今年的 RSAC 上几乎达到了狂热的程度，安全厂商都争先恐后地发布基于人工智能的功能和工具。SentinelOne 和谷歌云在内的厂商发布了由大型语言模型支撑的新产品。有参会者发现，可能是因为时间紧张，一些厂商的产品资料甚至没来得及更新。难怪有安全分析师认为，我们现在正处于大型语言模型炒作曲线的顶峰。

RSAC 会议出现对 AI 近乎狂热的关注，今年 RSAC 创新沙盒竞赛的获胜者是一家专注于保护 AI 模型的初创公司也就不足为奇了。

超过 4 万名与会者之间的大部分对话都集中在 AI 发展对网络安全专业人员意味着什么，以及攻击者和防御者将如何使用新的人工智能技术。因此有分析人士评论，RSAC 2023 更像是观看科幻电影，而不是世界顶级网络安全专业人士的聚会。

现在复杂已经成为网络安全的大敌，网络防御人员在特定时间需要应对数十个安全工具。未来，要让 AI 成为游戏规则的改变者，我们需要重新思考安全防护的战略，以及如何整合纷繁复杂的安全工具。

总编辑

李建平

2023 年 5 月 1 日

CONTENTS 目录

安全态势

月度专题

透视 RSAC 2023

生成式人工智能不出意外地成为 RSAC 2023 的焦点，安全厂商竞相展示 AI 驱动的网络安全工具。在人工智能有望重新定义安全的时代，我们需要了解全球安全专家如何看待 AI 对安全的影响，以及 AI 之外的安全热点。

《网安 26 号院》编辑部
主办　奇安信集团

总　编　辑：李建平
安全态势主编：王　彪
月度专题主编：李建平
攻防一线主编：魏开元
安全之道主编：张少波
奇安信人主编：孙丽芳
安全叨客主编：王梦琪
奇安资讯主编：陈　冲

奇安信集团　虎符智库　安全内参

索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

索阅邮箱：26hao@qianxin.com
地　　址：北京市西城区西直门外南路 26 院 1 号
邮　　编：100044
联系电话：（010）13701388557
出版物准印证号：京内资准字 2122- L0058 号
印刷数量：4500 本
印刷单位：北京博海升彩色印刷有限公司
印刷日期：2023 年 5 月 26 日
发行对象：奇安信集团内部

政策篇

国内，全国首个自动驾驶示范区数据安全管理办法在北京发布，填补了国内自动驾驶示范区级数据安全管理的空白。

国际上，欧盟发布《网络团结法案》提案，以应对大规模网络攻击。官方称该提案发布标志着欧盟网络安全战略终于补齐了最后一块拼图，开始具备可操作性。

国内

《北京市智能网联汽车政策先行区数据安全管理办法（试行）》发布

5月12日北京市高级别自动驾驶示范区公众号消息，北京市高级别自动驾驶示范区工作办公室正式发布《北京市智能网联汽车政策先行区数据安全管理办法（试行）》。该文件填补了国内自动驾驶示范区级数据安全管理的空白，明确企业负数据安全主体责任，并提出一系列总则性的数据安全管理要求，包括全面厘清智能网联汽车产业数据安全管理的关键环节、详细梳理重点数据类型的合规风险、创新构建示范区数据安全能力建设机制。

《公路水路关键信息基础设施安全保护管理办法》公布，将于6月起施行

5月6日交通运输部官网消息，交通运输部公布了《公路水路关键信息基础设施安全保护管理办法》（简称《管理办法》），自今年6月1日起施行，切实保障公路水路关键信息基础设施安全，维护网络安全。《管理办法》共6章33条，包括总则、公路水路关键信息基础设施认定、运营者责任义务、保障和监督、法律责任、附则六部分，主要内容涵盖明确关基设施管理体制、建立关基设施认定机制、压实运营者主体责任、加强对关基设施风险隐患的应急处置、强化事前事中事后监管。

强制性国家标准《汽车整车信息安全技术要求》公开征求意见

5月5日工信部官网消息，工业和信息化部装备工业一司发布《汽车整车信息安全技术要求》（征求意见稿），公开征求社会意见。该文件规定了汽车信息安全管理体系要求、车辆信息安全一般要求、车辆信息安全技术要求、审核评估及测试验证方法，适用于M类、N类及至少装有1个电子控制单元的O类车辆，其他类型车辆可参考执行。该文件提出，车辆生产企业应建立车辆全生命周期的汽车信息安全管理体系，针对车辆的网络攻击、网络威胁和漏洞建立监测、响应及上报流程。

《信息安全技术 终端计算机通用安全技术规范》等3项国家标准公开征求意见

5月5日信安标委官网消息，全国信息安全标准化技术委员会归口的《信息安全技术 终端计算机通用安全技术规范》《信息安全技术 数据安全评估机构能力要求》《信息安全技术 机密计算通用框架》3项国家标准已形成标准征求意见稿，现公开征求意见。据了解，三份文件分别规定了终端计算机的通用安全技术要求与测试评价方法，数据安全评估机构的能力要求，包括核心组件、基础功能、安全服务以及服务接口类型四部分的机密计算通用框架。

《中华人民共和国反间谍法》修订审议通过，将于 7 月 1 日起施行

4 月 26 日新华社消息，十四届全国人大常委会第二次会议 26 日表决通过了新修订的反间谍法，将于 2023 年 7 月 1 日起施行。新修订的反间谍法将投靠间谍组织及其代理人，针对国家机关、涉密单位或关键信息基础设施等实施网络攻击等行为明确为间谍行为。根据实践中的情况，适度扩大相关主体窃密的对象范围，将其他关系国家安全和利益的文件、数据、资料、物品纳入保护。

《网络安全标准实践指南——网络数据安全风险评估实施指引》公开征求意见

4 月 18 日全国信安标委官网消息，全国信息安全标准化技术委员会发布《网络安全标准实践指南——网络数据安全风险评估实施指引》，公开征集意见。本指南给出了网络数据安全风险评估思路、流程和方法，明确了网络数据安全风险评估步骤和工作内容，基于数据安全管理、数据处理活动、数据安全技术、个人信息保护等方面识别、评估安全风险，适用于数据处理者自行开展安全评估或者有关主管部门组织开展检查评估。

国际

澳大利亚发布《关键基础设施资产类别定义指南》

5 月 12 日 IndustrialCyber 消息，澳大利亚网络和基础设施安全中心（CISC）近日发布《关键基础设施资产类别定义指南》，对关键基础设施资产认定提供了指导意见。该指南要求资产所有者和经营者参考澳大利亚《关键基础设施安全法案》和《关键基础设施安全定义规则》，确定他们的资产具体符合哪一项关键基础设施资产的定义，并给出了具体指引。澳大利亚关键基础设施涵盖了 10 大类别，共计 22 个行业。

欧盟议会内部委员会通过《人工智能法案》草案

5 月 11 日新华社消息，欧洲议会内部市场委员会和公民自由委员会通过《人工智能法案》提案的谈判授权草案，向立法严格监管人工智能技术的应用迈出关键一步。新文本将严格禁止“对人类安全造成不可接受风险的人工智能系统”，包括有目的地操纵技术、利用人性弱点或根据行为、社会地位和个人特征等进行评价的系统等。谈判授权草案还要求人工智能公司对其算法保持人为控制，提供技术文件，并为“高风险”应用建立风险管理系统。每个欧盟成员国都将设立一个监督机构，确保这些规则得到遵守。

这一草案将于 6 月中旬提交欧洲议会全会表决，之后欧洲议会将与欧盟理事会就法律的最终形式进行谈判。欧洲议会的声明说，一旦获得批准，这将成为全世界首部有关人工智能的法规。

五眼联盟联合发布智慧城市网络安全指南

4 月 19 日 CISA 官网消息，美国网络安全与基础设施安全局（CISA）、国家安全局、联邦调查局联合英国、澳大利亚、加拿大、新西兰等国国家网络安全中心发布《智慧城市网络安全最佳实践》指南文件。该指南概述了智能城市面临的风险，包括不断扩大和互联的攻击面、信息和通信技术供应链风险及基础设施运营日益自动化。为防范这些风险，指南提出了安全规划与设计、主动管理供应链风险及运营韧性三项建议，以帮助社区加强其网络态势。

欧盟发布《网络团结法案》提案，以应对大规模网络攻击

4 月 19 日 Euractiv 消息，欧盟委员会发布《网络团结法案》提案，希望促进欧盟范围内合作，为重大网络攻击做好应对准备。该提案提出，建立由欧盟各国与跨境安全运营中心共同组成的联盟级安全运营中心“网络护盾”，使用 AI 等技术监控和识别网络威胁，预计明年投入运营。该提案还提出，建立欧盟网络安全预备队，由可信赖和经认证的私营企业参与，加强网络应急制度应对重大网络事件。《网络团结法案》相关预算为 11 亿欧元（约合人民币 83 亿元）。

事件篇

网络攻击持续影响物理设施，瑞士工业自动化巨头 ABB、法国大型电子产品制造商 Lacroix、美国冷链物流企业 Americold 等多家企业近期均因网络攻击影响业务运营乃至行业供应链周转。

美国交通部 23.7 万名员工的个人信息遭到泄露

5 月 16 日路透社消息，美国交通部日前发生一起数据泄露事件，导致 23.7 万名现任或前任联邦政府雇员的个人信息被曝光。这次泄露事件影响的系统名为 TRANServe，是由交通部管理的电子旅行通行证系统，用于处理政府雇员的交通津贴、报销部分通勤费用。目前尚不清楚泄露的个人信息是否被用于犯罪的目的。美国交通部向国会报告了此次数据泄露事件，称其初步调查“已经将泄露事件隔绝在行政职能部门的某些系统中，如员工交通福利处理”。官方称，此次泄露事件并未影响任何交通安全系统。

丰田泄露超 200 万辆汽车敏感数据：实时位置暴露近 10 年

5 月 12 日 BleepingComputer 消息，丰田汽车公司披露了一起云环境数据暴露事件，从 2013 年 11 月 6 日至 2023 年 4 月 17 日的十年间，共有 215 万客户的车辆位置信息持续暴露。通告称，“由于云环境配置错误，丰田汽车公司委托丰田互联公司管理的部分数据已被公开。”此次事件暴露了 2012 年 1 月 2 日至 2023 年 4 月 17 日期间，使用丰田 T-Coneect G-Link、G-Link Lite 及 G-BOOK 服务的客户信息，包括车架号、车辆位置。该公司后续称，可能还暴露了 2016 年 11 月 14 日至 2023 年 4 月 4 日期间车外拍摄的视频记录。丰田公司承诺向受到影响的客户单独发送致歉通知，并设立专门的呼叫中心来处理这部分车主的查询和请求。

法国大型制造企业遭网络攻击，超三成工厂被迫关闭超一周

5 月 15 日 TechMonitor 消息，法国大型电子产品制造商 Lacroix 遭受网络攻击，致使其全球超三分之一的工厂暂时关闭。该公司称目前事件已经得到控制，但受到影响的生产工厂可能仍需继续关停一周。Lacroix 公司披露，本地基础设施已遭黑客加密，旗下 8 个制造工厂中有 3 个受到了影响，这 3 个工厂占公司总产量的 19%。在关闭期间，Lacroix 公司将实施备份，并通过分析检验是否存在数据泄露。目前尚不清楚该公司是否收到勒索要求或已经支付了赎金，但从其中涉及数据加密和泄露来看，此次事件很有可能属于勒索软件攻击。根据初步计划，各处工厂将于 5 月 22 日重新开放。

工业自动化巨头 ABB 遭遇勒索软件攻击，业务运营受影响

5 月 11 日 BleepingComputer 消息，国际工业自动化巨头 ABB 遭受了 Black Basta 勒索软件攻击，短暂影响了公司业务运营。据 ABB 多名员工透露，勒索软件攻击了公司的 Windows Active Directory，影响了数百台设备，ABB 被迫终于与客户的 VPN 连接，以防止勒索软件传播至其他网络，据称这次攻击扰乱了公司运营，推迟了项目并使工厂受影响。ABB 官方称，公司采取遏制措施控制 IT 安全事件，导致业务受到一些干扰，目前正在处理。ABB 绝大多数系统和工厂现在都处于运行状态。

英国最大外包公司因勒索攻击损失 1.75 亿元，股价大跌

5 月 10 日 TheRecord 消息，英国外包巨头 Capita 在今年 3 月遭遇勒索软件攻击。该公司前日表示，应对此次事件可能将花费高达 2000 万英镑（约合人民币 1.75 亿元），包括“专家服务费、恢复与补救成本及加强对 Capita 网络安全环境的投资等。”Capita 还表示，“客户、供应商和内部员工的数据可能已经被盗。”Black Basta 勒索软件团伙宣布对此次攻击负责。该团伙已经将 Capita 列入受害者名单，并公布了明显窃取自该公司的数据，包括家庭住址和护照照片。

美国德州达拉斯市遭勒索软件攻击，市政服务瘫痪

5 月 3 日 CBSNews 消息，美国德克萨斯州达拉斯市当天确认遭受了勒索软件攻击，导致多项市政服务中断。达拉斯市内部许多服务器被勒索软件破坏，警察局和市政厅网站已下线，以防止恶意软件进一步传播。根据勒索通知内容，勒索软件组织 Royal 似乎对此次攻击负责。Emsisoft 威胁分析师 Brett Callow 指出，勒索软件对美国地方政府的攻击已经非常普遍，平均每周都会发生一起类似攻击。

高通处理器被曝偷偷上传用户手机信息，官方回应

5 月 3 日 cybernews 消息，德国安全厂商 Nitrokey 4 月 27 日发布报告称，高通公司生产的硬件在未经用户同意的情况下，将用户个人数据（如 IP 地址、设备唯一 ID 等）上传至该公司服务器，且使用 HTTP 协议明文传输没有加密。高通公司回应称，上述数据收集符合高通 XTRA 隐私政策。此服务与辅助 GPS(A-GPS) 相关，有助于为移动设备提供准确的卫星位置。Nitrokey 公司称，研究人员使用索尼手机进行测试，但该结果同样适用于其他使用高通芯片的手机。

德国医疗 IT 巨头遭网络攻击，被迫关闭所有信息系统

5 月 1 日 TheRegister 消息，德国医疗保险 IT 巨头 Bitmarck 遭受网络攻击，被迫关闭了所有客户和内部系统，部分情况下甚至关闭了整个数据中心。Bitmarck 昨日在临时官网发布通知，称目前未发现任何客户、患者或受保人数据被窃取。但这家服务商还没有制定系统恢复时间表。通知称，各个系统会参考客户情况以不同速度重新上线，已经或即将恢复可用的服务包括无工作能力电子证明、电子病历。

美国知名冷链物流企业遭网络攻击：配送中断 临期产品可紧急配送

4 月 28 日 BleepingComputer 消息，美国知名冷链物流企业 Americold 自 4 月 25 日晚间遭遇网络入侵以来，持续受到 IT 中断问题困扰。据外媒看到该公司发给客 户的备忘录文件显示，公司称控制住了入侵活动并关闭了内部网络，以确保其他区域不受影响。Americold 要求客户取消本周内的所有入站配送，并重新安排除临期产品外的所有出站配送时间。该公司预计，至少要一周时间才能重新上线。

间谍软件厂商 NSO 去年至少使用了 3 个 iOS 0day 漏洞利用链

4 月 18 日 SecurityWeek 消息，公民实验室发布报告称，以色列商业间谍软件软件厂商 NSO 集团在 2022 年至少使用了三个此前未知的 iOS 零点击 0day 漏洞利用链。公民实验室在调查墨西哥人权主义者 iPhone 设备恶意软件感染事件时，意外发现了这些漏洞利用链。其中第一个被称为 PwnYourHome，针对 HomeKit 和 iMessage，至少从 2022 年 10 月起使用，用于攻击 iOS 15 和 16 设备。第二个被称为 FindMyPwn，针对 Find Me 和 iMessage，至少从 2022 年 6 月起使用，用于攻击 iOS 15 设备。第三个被称为 LatentImage，仅出现在一台设备上，至少从 2022 年起使用。苹果在 2022 年 10 月和 2023 年 1 月收到相关报告，目前已知与这起事件相关的漏洞有 CVE-2023-23529。苹果在去年修复了约 12 个 iOS 0day 漏洞。

漏洞篇

国产软件接连曝光多个高风险漏洞，包括泛微 E-Cology、宏景 eHR、Foxit PDF Reader 等，且均已成功复现，鉴于上述漏洞影响范围较大，建议客户尽快做好自查及防护。

泛微 E-Cology 身份认证绕过漏洞安全风险通告

5 月 16 日，奇安信 CERT 监测到泛微 E-Cology 身份认证绕过漏洞 (QVD-2023-11606)，在泛微 E-Cology9 部分版本中硬编码第三方登录密钥，攻击者可以利用该密钥计算出特定参数值，从而伪造任意用户接管泛微 E-Cology。目前奇安信 CERT 已成功复现该漏洞，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Linux Kernel 权限提升漏洞 (CVE-2023-32233) 安全风险通告

5 月 16 日，奇安信 CERT 监测到 Linux Kernel 权限提升漏洞 (CVE-2023-32233)，Linux Kernel 的 Netfilter nf_tables 子系统存在释放后重用漏洞，在处理 Netfilter nf_tables 基本操作请求时，由于匿名集处理不当，导致可以任意读写内核内存，拥有低权限的本地攻击者可以利用该漏洞将权限提升至 ROOT 权限。目前奇安信 CERT 已成功复现该漏洞，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Foxit PDF Reader 及 Editor 任意代码执行漏洞安全风险通告

5 月 15 日，奇安信 CERT 监测到 Foxit PDF Reader 及 Editor 任意代码执行漏洞 (CVE-2023-27363)，攻击者可通过诱导受害者打开特制的 PDF 文档，最终在目标系统重启后执行任意代码。目前此漏洞 PoC 已在互联网上公开，奇安信 CERT 已成功复现该漏洞，鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

宏景 eHR SQL 注入漏洞安全风险通告

5 月 12 日，奇安信 CERT 监测到宏景 eHR SQL 注入漏洞 (QVD-2023-11385)，未经过身份认证的远程攻击者可利用此漏洞执行任意 SQL 指令，从而窃取数据库敏感信息。目前奇安信 CERT 已成功复现该漏洞，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。宏景 eHR 人力资源管理软件是一款人力资源管理与数字化应用相融合，满足动态化、协同化、流程化、战略化需求的软件。

Windows MSHTML Platform 安全特性绕过漏洞安全风险通告

5 月 11 日，奇安信 CERT 监测到 Windows MSHTML Platform 安全特性绕过漏洞 (CVE-2023-29324)，在 Windows MSHTML 中，由于 Windows 处理路径函数 CreateUri 错误的转换了某些路径，导致攻击者可以构造恶意路径绕过 CVE-2023-23397 Microsoft Outlook 权限提升漏洞防护措施。目前奇安信 CERT 已成功复现该漏洞，鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

GitLab 代码执行漏洞安全风险通告

5 月 8 日，奇安信 CERT 监测到 GitLab 代码执行漏洞

(CVE-2023-2478)，经过身份认证的远程攻击者利用此漏洞可以通过 GraphQL 端点将恶意 Runner 附加到实例上的任何项目上，进一步利用可能造成代码执行或敏感信息泄露。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Linux Kernel 权限提升漏洞 (CVE-2023-0386) 安全风险通告

5 月 6 日，奇安信 CERT 监测到 Linux Kernel 权限提升漏洞 (CVE-2023-0386)，在 Linux Kernel OverlayFS 子系统中，当用户将一个具有权限的文件从 nosuid 挂载点复制到另一个挂载点时，未经授权的攻击者可以执行 setuid 文件，导致权限提升。目前奇安信 CERT 已成功复现该漏洞，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Windows HTTP.sys 权限提升漏洞安全风险通告

4 月 27 日，奇安信 CERT 监测到 Windows HTTP.sys 权限提升漏洞 (CVE-2023-23410) 的细节和 POC 已在互联网上公开，由于 HTTP.sys 在复制 ServiceName 时存在整数溢出漏洞，攻击者可以构造恶意程序触发该漏洞，成功利用此漏洞可实现权限提升或拒绝服务。目前，奇安信 CERT 已成功复现此漏洞，鉴于此漏洞影响较大，建议客户尽快做好自查及防护。

VMware Workstation 与 Fusion 多个高危漏洞安全风险通告

4 月 26 日，奇安信 CERT 监测到 VMware 发布安全通告，其中包括 VMware Workstation 与 Fusion 代码执行漏洞 (CVE-2023-20869)、VMware Workstation 与 Fusion 信息泄露漏洞 (CVE-2023-20870)。经过身份认证的本地攻击者利用这些漏洞可以执行代码或读取敏感信息。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

泛微 Ecology SQL 注入漏洞安全风险通告

4 月 24 日，奇安信 CERT 监测到泛微 Ecology SQL 注入漏洞 (QVD-2023-9849)，泛微 Ecology OA 系统对用户传入的数据过滤处理不当，导致存在 SQL 注入漏洞，未经过身份认证的远程攻击者可利用此漏洞执行任意 SQL 指令，从而窃取数据库敏感信息。奇安信 CERT 已成功复现此漏洞，鉴于该产品用量较多，漏洞影响较大，建议客户尽快做好自查及防护。

Apache Druid 远程代码执行漏洞安全风险通告

4 月 21 日，奇安信 CERT 监测到 Apache Druid 远程代码执行漏洞。Apache Druid 是一个高性能的实时大数据分析引擎，主要用于在线分析处理（OLAP）场景。在 Apache Druid 使用 Apache Kafka 加载数据的场景下，未经身份认证的远程攻击者可配置 Kafka 连接属性，从而利用 CVE-2023-25194 漏洞触发 JNDI 注入，最终执行任意代码。目前奇安信 CERT 已成功复现该漏洞，鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Google Chrome Skia 整数溢出漏洞安全风险通告

4 月 19 日，奇安信 CERT 监测到 Google Chrome Skia 整数溢出漏洞 (CVE-2023-2136) 存在在野利用，攻击者可通过诱导用户打开恶意链接来利用此漏洞，从而在应用程序上下文中执行任意代码。目前，此漏洞已检测到在野利用。鉴于此漏洞影响范围较大，目前官方已发布安全更新，建议用户尽快升级至最新版本。

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

对抗篇

国内攻防演习 4 月态势：哪些薄弱点最易被利用？

作者 | 奇安信安服团队

一、本月演习整体情况

2023年4月，奇安信Z-TEAM团队共承接攻防演习服务 28 场，其中地市级攻防演习 6 场，客户自主攻防演习 22 场。

本月承接的攻防演习数量与上月对比呈上升趋势（见图1）。

本月承接的攻防演习涉及政府部委、金融、企业行业较多，此情况与上月承接攻防演习涉及行业范围数据基本一致，行业占比略有不同（见图 2）。

本月攻防演习成果如表 1 所示：

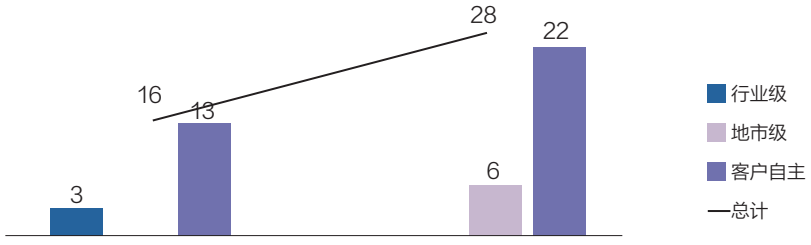


图 1　3-4 月 Z-TEAM 承接攻防演习数量统计

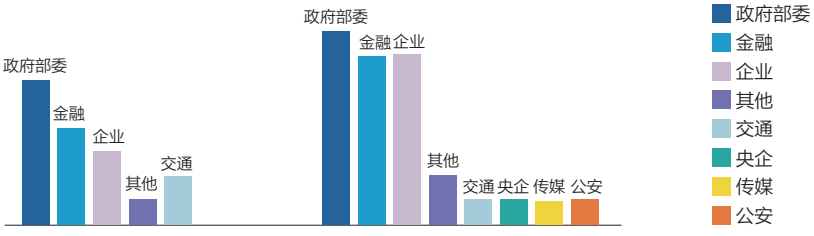


图 2 2023 年攻防演习涉及行业统计图

目标系统	靶标	强隔离内网	核心业务网	网站	堡垒机	安全设备	业务系统	服务器
数量	18	31	78	44	36	132	513	912

表 1

二、本月任务目标特点

本月攻防演习和评估任务行业比较分散，演习目标覆盖面比较广，涵盖了金融、政府部委、企业、交通、央企等行业。银行业的网络安全至关重要，因为银行业务涉及到大量的敏感信息、资金流转和交易数据等，如果遭到黑客攻击或者数据泄露，可能导致巨大的经济损失和严重的信任危机。因此，银行需要采取强有力的网络安全措施。银行业在本月攻防演习中的占比为 18%（见图 3）。

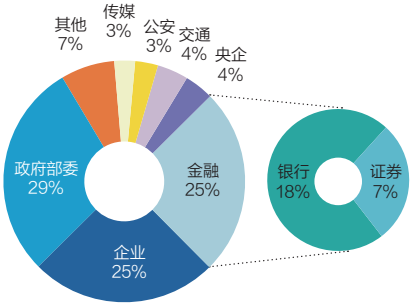


图 3 4 月攻防演习分布图

三、主要攻击手段分析

基于本月奇安信 Z-TEAM 团队实战成果分析，本月任务中对多行业不同目标网络进行攻击分析，总结了各个行业的攻击特点。政府部委、传媒、企业行业的外网安全防护相对较弱，容易被漏洞扫描利用和弱口令攻击等手段成功突破；央企、交通行业的外网安全防护相对较强，但仍需防范漏洞扫描利用和隐秘隧道外联、弱口令等手段的威胁；金融行业的外网安全防护最强，但也不能忽视漏洞利用、钓鱼攻击和 VPN 仿冒接入等手段带来的风险。本月攻击队突破目标安全防护使用的主要技术手段分布如下（见图 4）。

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

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

本月任务中银行业攻防演习任务占金融行业攻防演习任务的三分之二，通过针对该行业的演习数据分析发现，攻击者在外网纵向突破时，会寻找薄弱点并利用钓鱼进行攻击。然后以此为基础，在内网进行漏洞扫描利用、VPN 仿冒接入等攻击手段来实现横向拓展和渗透。在攻防演习中，攻击者往往需要多种攻击手段相互配合，才能成功地进行渗透和拓展。

四、典型攻击手段实现案例

银行网络安全工作的重要性不言而喻。随着技术的不断发展，银行业务日趋数字化和网络化，网络安全威胁也日渐繁多且复杂多样。保护银行的信息系统和客户数据免受黑客、恶意软件和其他网络攻击的侵害，已经成为银行最紧迫的任务之一。银行必须实施更加严格的安全防护措施和政策，如多层次身份验证、加密通信、定期漏洞扫描和红队 / 蓝队测试等，以确保其网络的安全性和可靠性。

案例：社工钓鱼结合 VPN 仿冒突破某银行隔离网（见图 6）

在针对某银行的攻防演练中，奇安信攻击队在前期的情报收集工作中发

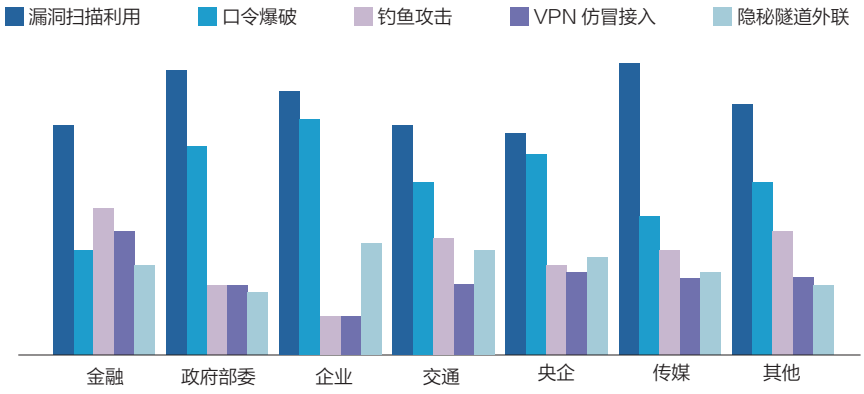


图 4 行业攻击手段分布图

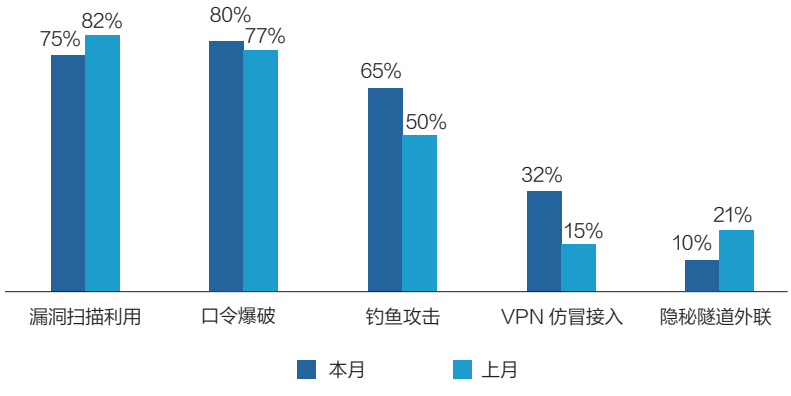


图 5 攻击手段对比图

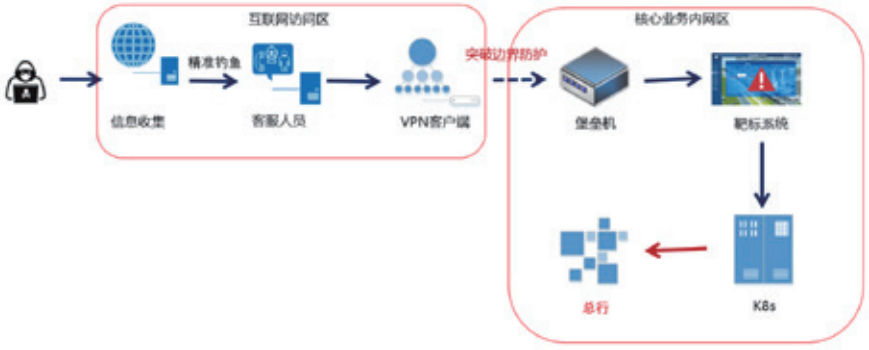


图 6 案例攻击路线图

现，该银行外部的网络安全防御体系比较健全，正面突破非常困难。为确保演习产出有效成果，经过多轮头脑风暴，大家终于达成共识——通过社工或 VPN 仿冒突破方法实现迂回入侵。

有同学首先想到了最常用的社工方法——邮件钓鱼，但此方法将会面临一个非常大的挑战，就是该银行完善的网络安全防御体系，其内网中大概率部署有邮件检测类的防御手段。如果简单地使用邮件钓鱼，很有可能会打草惊蛇，给后续的行动造成“大麻烦”。

随着情报搜集工作的深入，终于发现了让所有成员振奋的切入点。该银行使用了微信客服平台，且微信客服平台可以实时聊天甚至发送文件。考虑到客服人员一般技术功底不强，安全意识也相对薄弱，攻击队一致敲定：将社工对象确定为微信客服人员，并以投诉为话题尝试对客服进行钓鱼。果不其然，客服人员接收并打开了含毒压缩包，木马文件悄然执行。攻击队控制该客服计算机后，潜伏收集信息，经过大量信息甄别后，获得一大突破，成功获取到该计算机的 VPN 接入信息，最终拿到了目标内网接入的钥匙——VPN 账号口令。

攻击队登录 VPN 客户端软件后，以此作为跳板，连接到某银行内网的 VPN 服务器进行内网横向渗透拓展，获取到其自研堡垒机的服务器权限，控制了堡垒机里的测试环境和预生产环境的靶标及 Wiki、Kubernetes。在 Kubernetes 里找到连通总行的部分业务信息，成功实现跨网络隔离入侵总行。

五、防守加固建议

1、案例剖析

银行业网络安全边界防御体系普遍较健壮，社会工程学攻击则成为突破边界的首要手段。由于微信客服人员网络安全意识薄弱，攻击队通过钓鱼攻击微信客服人员，成功获取该人员的终端控制权限，并通过内网情报搜集和横向移动，获取了 VPN 的账号口令及堡垒机的控制权限，进一步入侵总行。

该案例暴露出，目标企业在安全防护上存在“安全风险意识薄弱”和“高权限设备安全防护能力弱”等问题。

2、防护策略

近几年金融机构网络安全态势呈现出攻击频率高、攻击手段复杂、内部威胁趋于严重、数据泄露风险大等特点。尤其是针对银行业的攻击事件通常都是复杂的组合攻击手段，常见手段包括社会工程学攻击、木马程序攻击、漏洞利用等。银行内部员工的安全意识和行为习惯成为影响网络安全的重要因素，员工可能因为疏忽、利益驱动、不当操作等原因，引发重大网络安全事件。因此，在安全建设中，人是安全的关键与核心，安全意识更是“人的因素”中的重中之重，金融机构应形成网络安全宣传教育常态化机制，不断地提升员工网络安全意识，形成安全习惯和行为，保护各类信息资产，有效地控制信息泄漏风险，进而全面地提高网络安全管理水平。

奇安信《网络安全意识服务解决方案》，通过宣传物料定制设计、意识培训、知识竞答、现场活动体验、知识展览及钓鱼邮件测试等服务，结合组织内部实际情况，为用户组织内开展全面、有序、定制化的员工网络安全意识宣传教育工作，让用户组织内部员工认识、理解、掌握网络安全知识和技能。

具体服务内容如下。

（1）网络安全意识视频：围绕各类网络安全风险隐患或真实事件展开，给出具体的安全防护最佳实践，强化员工对网络安全重要性的认识、获得网络安全技能。

（2）网络安全意识竞答：将知识内容以各种形式渗透到工作中的各个角落，通过在线答题方式，持续促进员工安全意识的提升。

（3）钓鱼邮件测试服务：基于社会工程学原理，精心构造极具迷惑性且含有恶意链接的邮件，向目标群体定向开展邮件钓鱼测试，评估用户组织内部人员信息安全意识，并为后续安全培训、技术防护手段升级提供依据。

（4）安全意识宣传材料：包括电子版及实物版的安全意识海报、月刊、长图、手册、屏保等内容。

（5）安全风险演示：以场景化的方式，多维度、多视角还原日常工作和生活中可能会遇到的网络安全威胁，从而警醒企业员工对网络威胁的感知，提升员工安全意识。

（6）网络安全意识培训：通过课堂演示、案例讲解、攻防模拟演练等多维度的授课方式将网安知识由浅入深、循序渐进地传递给企业员工。安

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

栏目主编　李建平

透视 RSAC 2023

生成式人工智能不出意外地成为 RSAC 2023 的焦点，安全厂商竞相展示 AI 驱动的网络安全工具。在人工智能有望重新定义安全的时代，我们需要了解全球安全专家如何看待 AI 对安全的影响，以及 AI 之外的安全热点。

RSAC 2023 热点与安全趋势
——奇安信安全专家全面解读

作者 | 周奕

RSAC 2023： 携手更强大

2023 年 RSAC 的主题是“Stronger Together”(携手更强大), 显然是从美国知名女作家、教育家、社会活动家海伦 · 凯勒的名言获取灵感，“Alone we can do so little; together we can do so much。”（单枪匹马，杯水车薪；同心一致，其力断金。）

“携手更强大”的主题首先反映在 RSAC 2023 庞大社区上：超 625 家供应商、700 位演讲者、26,000 名与会者参与了今年的 RSAC，规模超过了以往任何一届。同时，随着生成式 AI 的崛起 , 网络安全已从传统的人与人的对抗 , 逐渐演绎成人与机器的对抗，携手更强大”诠释的是超越传统意义上的人类力量聚合，还是产品、工具和平台间的互联互通，更是人员、工具、机器、自动化、AI 等在内的创造和组合 , 以最高的效率实现最佳结果。

人工智能席卷 RSAC，AI 将成安全防护基础?

人工智能与机器学习无疑是本届 RSAC 的热点话题， 旧金山莫斯克尼会议中心到处充斥着 “AI” 的味道。

这里既有坚信 AI 的追捧者，相信 AI 能深度落地到网络安全的诸多领域；这里也有 AI 的怀疑论者，过去 20 年机器学习和人工智能在信息安全领域起到决定性作用的场景依然有限。

今年的 RSA 创新沙盒比赛中，致力于保护 AI 模型的初创公司 HiddenLayer 被评为“最具创新性的初创公司”。事实上，除了 HiddenLayer，还有两家 AI 标签的安全初创公司入选创新沙盒比赛 10 强。HiddenLayer 提供 MLMDR (机器学习检测和响应) 平台，用于监测机器学习算法的输入和输出，以发现异常活动。行业观察人士认为，这一结果表明了网络安全创新的前景和创业生态系统的有趣转变：风险投资人从炒作 AI/ML 安全工具转向投资保护 AI 模型的初创公司。

RSAC 会议的所有研讨环节（Session）都会涉及 AI 话题，AI 安全产品发布也成为大会的热点。大大小小的安全公司都在努力与生成式 AI 结合，推出包含生成式人工智能的新产品，为自己的产品贴上 AI 标签：包括 RSA 安全在内的近 12 家主要安全供应商及 50 多家初创公司发布了人工智能驱动的网络安全产品。

谷歌云宣布推出 Security AI Workbench 平台，将谷歌云 Sec-PaLM 的新型安全大型语言模型 (LLM) 与 Mandiant 情报结合，使合作伙伴能将生成 AI 扩展到自己的产品。

SentinelOne 则推出使用生成人工智能和强化学习功能的威胁搜寻平台，帮助企业检测、阻止和自主修复攻击。BigID 推出人工智能引擎 BigAI，加速数据安全、治理和风险管理计划。SecurityScorecard 宣布推出与 OpenAI 的 GPT-4 系统集成的安全评级平台，让安全团队更容易理解威胁并采取行动。

在 RSAC 召开前，就有多家企业进行了 AI 安全产品的发布。4 月，Veracode 和 Recorded Future 也宣布将生成 AI 引入其自己的产品中。Veracode 生成式 AI 产品建议修复代码和开源存储库中的漏洞；Recorded Future 则训练 GPT 以帮助威胁分析师更好地解释安全风险。3 月下旬，微软宣布推出基于 OpenAI’s GPT-4 生成式 AI 的 Microsoft Security Copilot，通过易于使用的 AI 助手，提高安全团队的整体效能。

安全厂商在 RSAC 的 AI 产品发布没有改变”智者”疑虑，不少“智者”仍持观望态度。Cybrize 首席安全官兼战略官 & 联合创始人戴安娜·凯利，在主题演讲“炒作与现实：如何评估网络安全中的 AI/ML”中表示，人工智能和机器学习在网络安全的应用日益普遍，这些技术有望大大提高安全防御的质量，但也是容易被过度宣传的流行语。生成式 AI 都是在大量图像和数据上进行训练的，非常适合集思广益，但它还不是完全可信的系统，并非所有结果都是准确的。

与其他行业相比，网络安全公司将生成式 AI 应用于安全防护的速度要慢一些：安全公司只是在自己的情报和攻击数据中训练自己的大型语言模型。一些安全公司另辟蹊径，为 AI 安全提供防护。例如，赛门铁克在内部使用和研究生成式 AI，包括如何从 PB 级安全情报中获取更多价值，并针对 AI 使用中数据可能被滥用的风险，还推出了专门的解决方案，帮助企业安全地采用生成式 AI 应用，将数据安全控制应用于生成式 AI 对话。

在演讲中，RSA 首席执行官 Rohit Ghai 表示，人工智能将成为网络安全的基础。我们需要人工智能来阻止利用人工智能发起的攻击。但他也表示，安全领域的 AI 并不意味着要取代人。目前安全公司推出的大多数 AI 解决方案都是“副驾驶”类型的解决方案。很多行业的工作将会因为人工智能而消失，但在网络安全方面，人工智能将使决策变得更容易，即使人退出自己的角色，仍需要对 AI 进行

> RSA 首席执行官 Rohit Ghai 表示，人工智能将成为网络安全的基础。

RSA CEO Rohit Ghai：我们需要用好 AI 打败坏 AI

教育、监督和规范。

演讲者提供的题材的热度前三名分别为智能分析响应 (Analytics, Intelligence and Response)，威胁和攻击 (Hackers and Threat)，风险管理 (Risk Management & Governance) 。

智能、分析与响应：攻击面管理与主动狩猎更受关注

智能、分析与响应领域没有出现预料中的 AppSec 与安全运营，或者 IT 基础架构与安全运营等融合趋势的探讨，更多还是聚焦在一些单点技术的尝试和突破。

技术趋势方面，在攻击面管理方面有了更深入、更广泛的探讨。网络漏洞和弱点无处不在，但我们首先需要修复什么？Mitre ISA (Infrastructure-Susceptibility-Analysis-and-Assessments 基础设施敏感性分析) 是一种旨在将弱点或漏洞缓解工作集中在最有可能被利用的系统和架构上的方法。ISA 扩展并升级了当前的威胁情报方法，在威胁风险等级评估时，将情报中攻击者的能力 (Capability) 演进成目的 (Objective)，将攻击者使用的技术 (Technology) 演进成攻击成功后的后果 (Effect)，从而更好地用风险等级指导组织对运营环境中的风险隐患进行优先级排序。

主动狩猎呈上升趋势。当面对威胁进行狩猎建模时，不同的方法、理念和与风险指标应运而生，不仅仅是技术工具的演进，团队工作模式和信息共享方式，以及工作汇报的结构和方法都会随之变化。狩猎的技术方面，在机器学习技术的推动下，构建在知识图谱上的主动式威胁狩猎被多次提及。基于端及流量日志数据，结合内网资产数据形成的资产图谱，构造行为关系图谱；使用机器学习技术训练图自编码器 (Graph Auto-Encoder)，将知识图谱空间映射到多维的数值向量空间；利用图自编码器将同一类的行为映射成数值向量，通过设置与正常的向量的距离阈值推测是否为异常行为；再在资产图谱上对历史异常行为数据通过机器学习方法进行分析溯源或建立预测模型，从而对恶意行为如攻击的横向移动构建攻击路径预判或进行预测。

安全运营的流程趋势或创新倒是没有特别提及，相反更多强调的是网络安全从业者的责任感。在重压之下，我们应该学习如何像社会应急人员、救火队员、反恐小组成员等在突发事件到来时的责任和担当，更好地管理

压力和心理健康，并将高压下的训练和反应常态化。

威胁与攻击：勒索、钓鱼和账户接管（ATO）仍是主要威胁

历年的 RSAC 都会对威胁攻击事件进行预测总结，没有例外。所谓无威胁，不 RSAC。

宏观趋势方面，勒索软件、网络钓鱼和员工账户接管（ATO）仍然是最主要的威胁。网络安全领导者应投入足够的精力应对这些重要威胁并关注相关的微观趋势。勒索软件微趋势主要包括数据窃取或破坏较数据加密更易实施且更省时，利用企业设备、云存储和安全工具中的错误配置，二次赎金流行导致支付赎金法律风险增加。网络钓鱼微趋势方面，BEC 类型的钓鱼邮件仍然难以检测，钓鱼邮件仍是恶意软件传播主要途径，网络钓鱼即服 务（phishing-as-a-service）增加，钓鱼攻击仍是数据丢失的主要原因。对于员工账户接管（ATO），微趋势包括密码仍然是最流行的身份验证方式，多因素认证（MFA）易受钓鱼攻击影响，SMS 或语音身份验证可能遭受 SIM 交换、恶意软件和针对电信公司基础设施的攻击，提示轰炸或 MFA 疲劳攻击增长迅速，针对一次性密码（OTP）的中间人（MITM）攻击，可绕过身份验证的传递 cookie（PTC）攻击，利用账户恢复漏洞的攻击。

容器安全不能代表云安全，但对容器的集中攻击确实是今年的热门话题，尤其是公开的容器镜像的安全问题。虽然容器安全扫描正在被越来越广泛地采用，但从安全角度来看，每个容器镜像的目的，镜像中包含的复杂的开发组件及他们之间的依赖关系，导致容器安全最终的攻击面大于其漏洞总和。同时容器的全生命周期，新漏洞的发现、新版本生产环境的发布和部署都增强了其复杂度。而综合容器镜像安全的最佳实践，了解你的镜像，持续自动的优化容器，消除漏洞，以及非必要的组件，开销。最后，只上线你必须要的部分。

风险管理：API 风险热度超过多因素认证、零信任和漏洞管理

风险管理方面， API 风险被屡次提到，热度甚至超过多因素认证，零信任和漏洞管理。新型的无代码和低代码平台，以及并购安全风险也在本次大会的风险管理关注度中排名靠前。

API 风险

API 已成为应用前后端、应用间交互数据的主要方式，是组织业务和数据能力对外提供服务的主要形式。针对应用和数据服务 API 的攻击在数量和频率上呈倍数增长趋势，手法也日趋复杂。

与会专家认为，API 面临的主要风险包括：绕过访问控制机制的 API 未授权与越权使用；利用开源组件漏洞、脆弱性配置、管理不善的 API 等

风险管理方面， API 风险被屡次提到，
热度甚至超过多因素认证，
零信任和漏洞管理。

非法窃取数据；利用机器人和 AI 技术进行拒绝服务攻击和边界渗透；应对日益增长的 API 风险的措施：利用 WAAP 和内部分段进行纵深保护；开发与运行阶段结合发现 API 并做好生命周期管理与安全测试；对 API 进行分类结合数据分级保护；持续对 API 进行态势管理、安全监控、快速响应。

无代码 / 低代码 (No/Low Code) 风险

低代码或无代码平台方式开发应用软件带来的效率提升，开发门槛降低等好处已被广泛认可，与此同时这种新型生产模式带来的风险也被更多人认知。大量应用程序无法集中监管，从而产生的应用是否符合安全与合规标准难以评判。进而，应用程序的身份仿冒，数据泄露风险无法被定级评估。应对风险的措施主要还是对低代码或无代码平台进行审计并对生产的应用进行统一管理，统一进行风险评估并利用自动化剧本进行风险治理。

公司并购风险

在应对公司的并购活动中新公司的加入带来的网络安全风险中，今年提出了一些新的框架来预防并购过程中可能犯下的一些错误。通过并购过程中，场景→问题→方案 的沙盘推演，来解决 M&A 过程中准备不足，盲目冒险，不当整合，保护不足等问题。比如，对新并购公司的 SaaS 应用资产台账不清楚（场景），导致重要信息泄露的风险（问题），将 SaaS 应用的发现和台账信息获取纳入尽职调查流程。

初创公司：安全右移势头在上升

初创公司是伟大创意的发源地，通常也具备更好的执行力。很多网络安全从业人员都深受哈佛商学院教授克莱顿 · 克里斯坦森《创新者的窘境》（Innovator's Dilemma）的影响。

> 过去几年大家都在谈论安全左移。从相关初创公司的产品介绍来看，“右移”的势头却在上升。

今 年 RSAC 的 Early Stage Expo 给 52 家初创公司提供了集中展示的舞台。在候选企业中，有超过 20% 的企业从事应用安全 (AppSec) 相关的领域。过去几年大家都在谈论安全左移。从相关初创公司的产品介绍来看，“右移”的势头却在上升。厂商的产品价值普遍关注应用运行时的性能、弹性和可靠性。即使云原生模式的转变也同样需要兼顾左移和右移策略。初创公司除了提供更好的 CI/CD 工具，产品能力也在兼顾更好的可见性、扩展性和安全性。此外，在开源趋势的背景下，对 SBOM 的关注，越来越多以应用系统为目标的攻击，也促使相关的产品方案会兼顾对开源代码和其依赖的检查，以及开源代码的操弄、攻击和权限变更行为的检测。

以下我们也挑两家代表着 AppSec 未来的新生代厂商做个简要分析。

（1）OXEYE：全面的静态和运行时分析

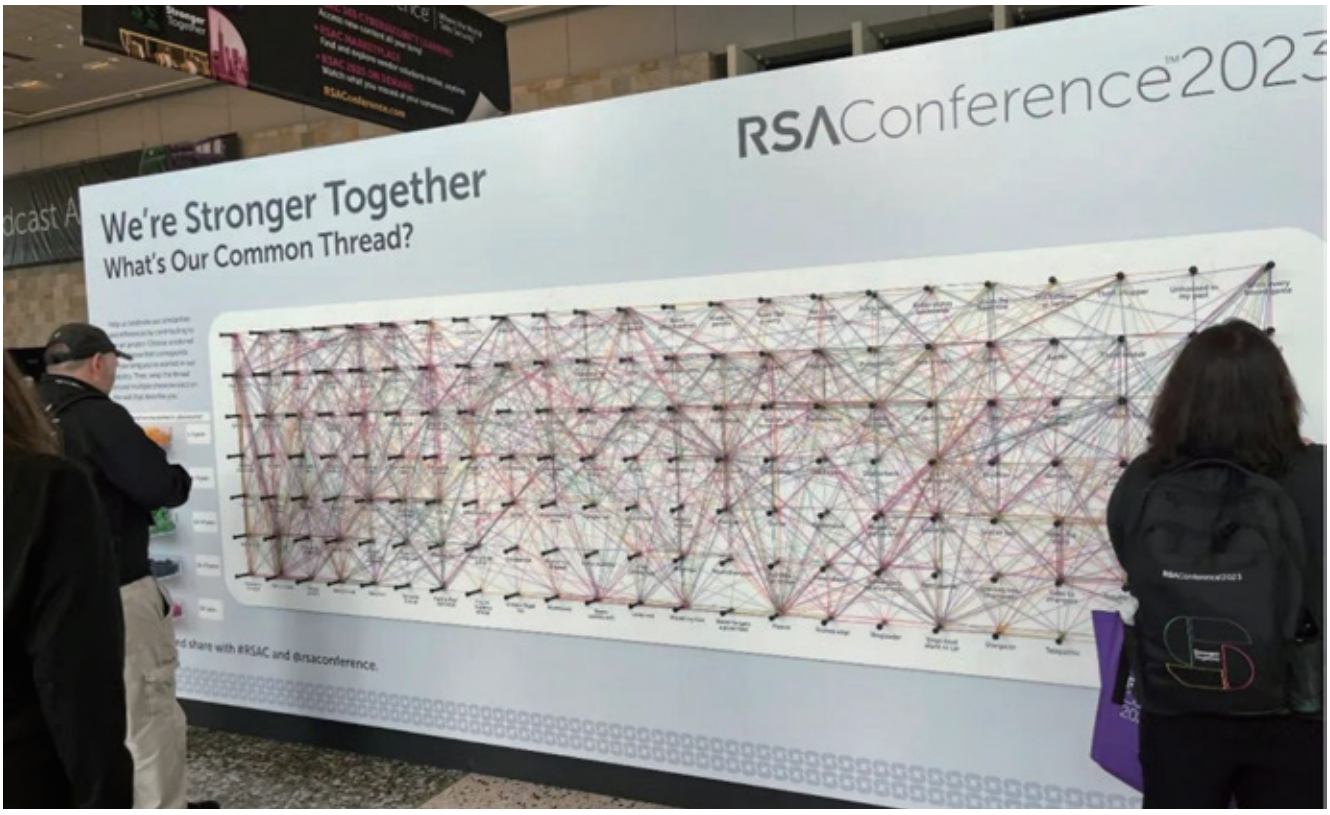
Oxeye 结合了 5C（代码、容器、集群、云及其连接 / 通信）的静态和运行时分析，以查找现代分布式应用程序的漏洞并确定其优先级。通过将静态和运行时分析及 SAST、DAST、SCA、 ASOC 和 ASPM 的功能组合到一个工具中来提供上下文化的漏洞结果。Oxeye 找到所有自定义代码、开源和第三方包漏洞，然后执行以下操作以消除无法利用的漏洞，以便更有效地进行修复：

- 查找并确定加载和使用了哪些易受攻击的开源和第三方包，并过滤掉那些没有的。
- 过滤无法从 Internet 直接或间接访问的漏洞。
- 通过添加基础架构配置数据进一步优化。
- 通过对可利用的 API 进行模糊测试来执行主动验证。

（2）ArmorCode 打破安全孤岛（ASPM+UVM+ASOC）

ArmorCode 结合应用程序安全状态管理 (ASPM)、统一漏洞管理 (UVM) 和应用程序安全编排与关联 (ASOC)，提供单一的 AppSecOps 平台。该平台统一了应用程序安全和基础架构漏洞管理，以提供洞察力、敏捷性和跨安全性和开发人员的协作团队。

ArmorCode 能够统一和关联数百种安全工具（从主机到云再到代码）的发现并统一漏洞管理，在单个工作流程



社交网络

中对 DevSecOps 管道、云和本地资产中的漏洞进行分类和优先级排序，通过优化分类工作和改善安全与开发团队之间的协作来缩短漏洞响应时间。

RSAC 最吸引人的部分还是见到老朋友、结识新朋友，建立公司及自己的朋友圈。井井有条的结构化会议日程固然高效，在没有刻意安排的早餐、咖啡、茶歇和会议间隙的五分钟休息中，能和来自全世界的网络安全从业人员彼此认识、相互学习，是很多 RSAC 忠实参会者的主要目的。

在今年 RSAC 中，我们偶然结识了 10 几位来自世界各地的网络安全从业者，在或长或短的聊天、讨论，辩论甚至是碰撞中，彼此尊重，相互理解。

印象最深的有两位，一位是 Dolby 的 CISO 并兼职湾区 CISO 社区的顾问。在 15 分钟的早餐闲谈，同时也是脑力激荡过程中，他听到中国 CISO 坚持业务导向、价值导向而非传统的最佳实践导向，给他带来巨大的震撼；同时，他也分享了指标驱动安全运营、安全建设的实操难度。来自 VMRay 的产品副总裁，在奇安信展台听到了来自中国网络安全发展的声音。

RSAC 参会人数已恢复到疫情前的水平。作为立足北京、辐射全球的世界级网络安全产业及技术交流与合作平台，2023 北京网络安全大会 (BCS) 也将恢复线下会议，中国网络安全人迎来自己的社交与深度沟通的机会。2023 年 7 月，北京网络安全大会 (BCS) 见!

重新定义安全运营“平台”
——从 RSAC2023 看安全运营技术发展趋势

作者 | 叶蓬

2023 年 RSAC 大会落下帷幕。毫无疑问，这场主题为“携手更强大”（Stronger Together）的大会展示了空前的盛况：超 625 家供应商、700 位演讲者、26,000 名与会者，规模超过以往任何一届。全球网络安全产业一片繁荣景象。

“携手更强大”主题除了反映在 RSAC 庞大社区上，还体现在安全产品、工具和平台的互联互通上。尽管各种市场调研显示客户对碎片化安全解决方案的忧虑。Gartner 表示，75% 的组织希望安全供应商能够整合。但当你看完创新沙盒 10 强赛，再浏览完早期厂商展厅的 48 家早期安全公司，你不会相信未来的安全供应商会减少。这或许验证了 Gartner 的那句话：“安全厂商永远在整合，但永远也整合不完”。

碎片化的安全解决方案及产品的出现源于层出不穷、永不止境的新安全威胁，这是无法改变的网络安全的本质决定的。但碎片化造成的安全运营的复杂度和难度急剧上升则是可以想办法予以缓解的。最简单的方法就是整合。这里的整合不仅包括狭义的供应商产品合并和数量减少，更包括基于平台的跨供应商产品集成与组合。整合的目标就是要让用户在安全运营的时候感到简单，并降低整个运营周期的维护成本。

未来安全运营的一个重要技术发展趋势主要就是围绕整合，也让安全运营变得更简单来展开。

生成式 AI 给安全运营带来深远影响

以 ChatGPT 为代表的生成式 AI 无疑是本次大会的最大噱头，几乎每个演讲都要提及。即便是与生成式 AI 应用最无关的议题，演讲者也有办法将其与之联系起来。譬如会说“我在写这个议题的胶片时，询问了 ChatGPT 应该从哪几个方面进行阐述”，然后

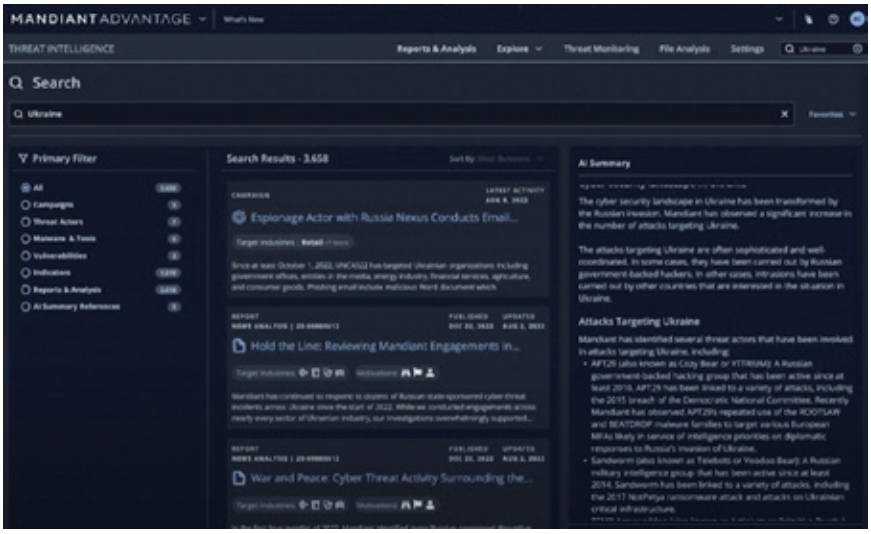
未来安全运营的一个重要技术发展趋势
主要就是围绕整合，
也即让安全运营变得更简单来展开。

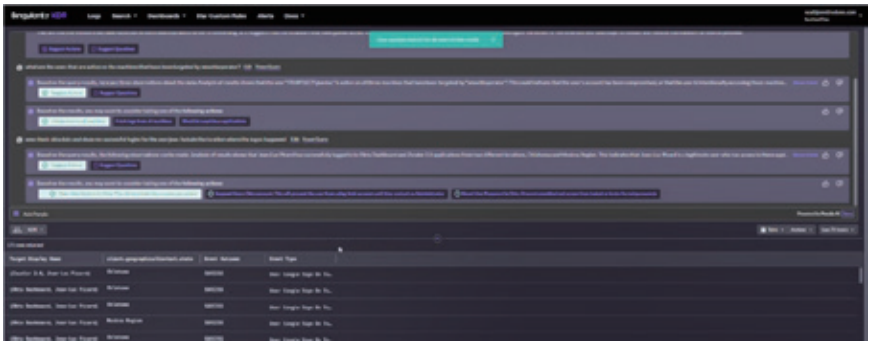
引来台下一片大笑。

纵观具体谈及生成式 AI 的议题，基本可以分为如何应用生成式 AI 进行防御、如何应用生成式 AI 进行攻击，以及讨论生成式 AI 自身的安全问题。

对于如何应用生成式 AI，目前的焦点基本都放到了安全运营上。目前生成式 AI 在网络安全领域的最佳应用场景几乎都来自安全运营，并涵盖从事件检测、调查、响应到汇报的各个环节。

2023 年 3 月底，微软抢先发布了基于生成式 AI（GPT4）的 Security Copilot（安全副驾），为用户提供了安全运营智能助理。在发布会上，微软演示了 3 个应用生成式 AI 的安全运营场景，分别是基于 Promptbook 的威胁猎捕、事件响应和出具安全报告。





在 RSAC 大会上，谷歌发布了基于安全领域专用的 LLM（称作“Sec-PaLM”）的谷歌云安全 AI 工作台（Google Cloud Security AI Workbench），赋能客户、伙伴和自身的安全产品，实现智能化安全运营。笔者观看了功能演示，主要应用场景包括基于 AI 的恶意代码检测，生成情报洞察摘要报告，基于自然语言的事件查询与调查，智能化检测规则生成，以及基于生成式 AI 的事件摘要和攻击图摘要说明。

在 RSAC 大会上，SentinelOne 也推出了自己的安全专用生成式 AI——Purple AI，通过基于自然语言的多轮对话形式，协助用户进行威胁猎捕、分析与响应。

有趣的是，这些厂商发布的安全专用生成式 AI 产品无一例外都仅提供有限预览，何时正式发布还没有确切的时间。这一方面体现了生成式 AI 的火爆导致厂商纷纷抢占山头，另一方面也说明该项技术在网络安全（主要是安全运营）领域的应用尚不成熟。

可以肯定的是，专门面向安全领域的生成式 AI 对安全运营必将产生深远的影响，正如微软安全业务的副总裁 Vasu Jakkal 在《Defending at Machine Speed》演讲时所说，“AI 应用于安全的拐点已来”在战略层面要高度重视生成式 AI。

微软描绘了应用于安全领域的 AI 的三个基本要素：AI 技术自身（尤指生成式 AI）、超大规模的安全数据及威胁情报。简单说就是：安全领域的 AI= 算法 + 数据 + 知识。谷歌的 Sec-PaLM 的底层逻辑基本上也是如此，思科亦是如此。

生成式 AI 对安全运营的深远影响核心就体现在简化二字上。它通过全

新的用户体验（微软称为新的生产力范式），也就是基于自然语言的最“人性化“的方式，简化了人与机器（工具）之间在安全运营时的交互过程，也简化了人与人的专业知识传承过程。未来不再需要人去做事件标准化，去写机读的查询语句、规则、脚本和剧本。

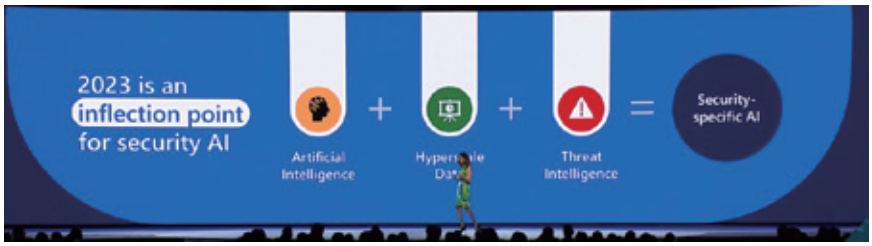
思科的 Jeetu Patel 在题为《威胁响应需要全新思维》的演讲中也提出了同样的观点：用 AI 简化安全。

思科虽然尚未发布自己的 LLM，但也畅想了一番 AI 加持下的全新安全运营用户体验。

但是，无论我们如何在战略上重视安全专用生成式 AI，都不要忘记一点：安全对抗的本质还是人与人的较量。笔者认为，在可见的未来，AI 技术依然无法改变这点。正如微软的 Vasu Jakkal 所说：“在安全领域，要讨论的不是（AI）技术能做什么，而是人在（AI）技术加持下能做什么”。即便是 Trellix 的 CEO Bryan Palma 提及未来 SOC 将由机器人来操作的时候，也没有忘了说这些机器人是在人的领导下，受人指挥调度和监督的。

在战术层面，必须清醒地认识到，当前生成式 AI 技术在安全运营领域的应用还比较初级，并应充分挖掘可以发挥生成式 AI 基本特长的安全运营应用场景。当前的核心是如何将自然语言翻译为机读指令（规则、策略、脚本、剧本等），最终安全运营平台和工具执行的还是原来那些机读指令。然后，再使用生成式 AI 对结果进行解读，并开启新一轮人机交互。

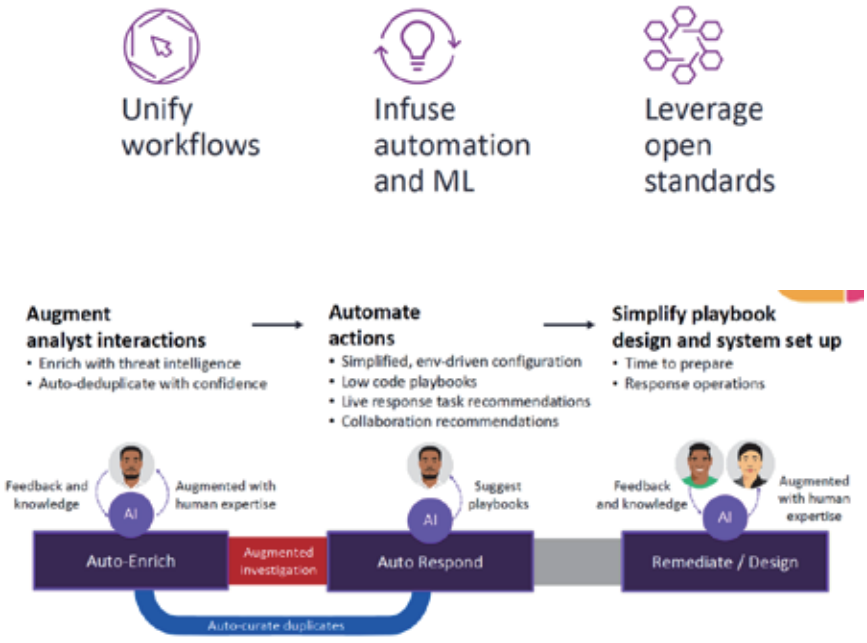
因此，安全领域的生成式 AI 不仅依赖于算法和数据，还严重依赖于安全知识（经验、流程、情报等）。在从海量安全数据中找寻隐匿的威胁方面，还需要灌输人类的知识，尚无法



实现自主检测。笔者认为，在生成式 AI 一统 AI 之前，包括知识图谱在内的分析型 AI 依然还有用武之地。

智能自动化是安全运营的必由之路。

在某种意义上，安全运营自动化的本质上是简化。安全运营自动化通过对使用者提供一种简化的交互模式，来提升安全运营的效率，降低运营的复杂度和成本。



聆听与会大咖们的发言，可以明显地感受到，安全运营的自动化正在从传统的机械式自动化向 AI 加持的智能自动化、认知自动化，或者说超自动化方向演进。

如果生成式 AI 让我们获得了空前的思考力，AI 加持的智能自动化将让我们获得空前的行动力。对于安全运营而言，行动才是一次运营活动闭环的标志。

在关于未来安全趋势的演讲中，Akami 的首席安全官 Boaz Gelbord 将自动化列为第一个大趋势。他认为，安全想要赶上数字化时代的业务发展速度（speed of business），要赶上攻击者的速度(speed of adversary)，不能再依靠人工操作，而必须借助自动化，用机器速度(speed of machine)来对抗机器速度。

IBM QRadar的产品经理们在《从孤岛到整合：安全分析体验的经验》”演讲中，提出了改善分析体验的三个基本策略：统一工作流、融合 AI 和自动化、利用开放标准。

下图展示了一个用 AI 赋能的自动化安全事件调查过程。通过这套智能自动化过程，简化了安全运营的流程步骤，缩短了调查和响应时间，提升了分析师体验。

重新定义安全运营的“平台”

企业和组织都迫切希望降低安全（不仅是安全运营）的复杂性、提升效率。在安全的各大领域纷纷出现了旨在整合该领域安全技术的平台。如果说整合是安全发展的内在驱动力，那平台就是这个驱动力的具象化。

未来安全厂商之间的竞争将从产品的竞争发展到平台的竞争。这时的平台已不再是传统的平台。这里的平台既包括单一安全厂商提供的全家桶式平台，也包括跨厂商的开放式平台。这些领域包括整合边缘网络安全的 SASE，整合数据安全的 DSP，整合身份安全的 CIP（下一代身份平台），整合云安全的 CNAPP，整合检测与响应的 XDR，当然也包括整合不同安全运营技术的未来 SOC。

在介绍当前身份管理面临的危机时，RSA 的 CEO Rohit Ghai 提到了身份管理平台的三次发展浪潮。笔者认为，身份平台发展的三个阶段同样适用于其他平台，包括安全运营平台。

第一代平台：核心是通过各种 API 将各种碎片化的安全能力组装到一起。这时候关心的是“能组装到一起吗？”

第二代平台：核心是形成一个全

景图，获得对目标的可见性。这时候关心的是“这个图长什么样子？”

第三代平台：核心是形成洞察，做出决策。这时候关心的是“这幅图代表了什么含义？我该做些什么？”

如果我们采用上面的代际划分方法论，随着 AI 应用于安全的拐点到来，安全运营的平台开始迈入第三代。鉴于不同的人对安全运营平台的代际划分可能不同，笔者姑且将这个新时代的安全平台称作“未来安全平台”，而将新时代安全运营平台称作“未来 SOC”。

未来 SOC 具备什么核心特征？对此，业界现在还没有统一答案，但 RSAC 大会上的演讲发言给我们一些启发。

思科的 Jeetu Patel 在演讲中提出了跨域原生遥测的概念，强调未来平台要能够采集和集成多种原生的遥测数据。

思科的另一位副总裁 Tom Gillis 则进一步阐释了未来平台应该是预先集成和组装好的，用户开箱即用的，而不能是用户买回来一堆零部件自己组装的。

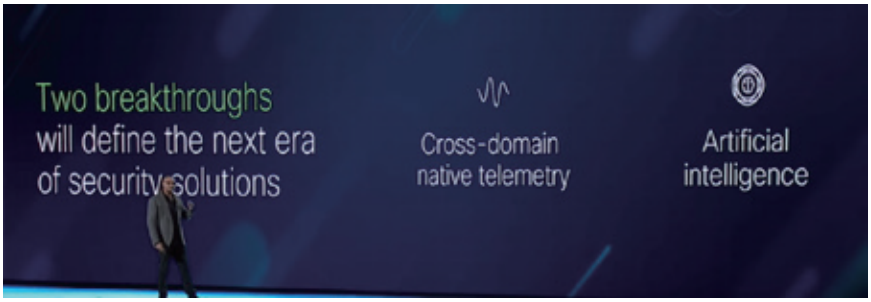
派拓网络的首席产品官 Lee Klarich 则将原生集成作为未来平台的关键能力。这一提法跟思科的思路大体一致。他表示，以前的集成往往做不到被集成的能力都是同类最佳的，而新的原生集成将可以做到“既要又要叒（还）要”。

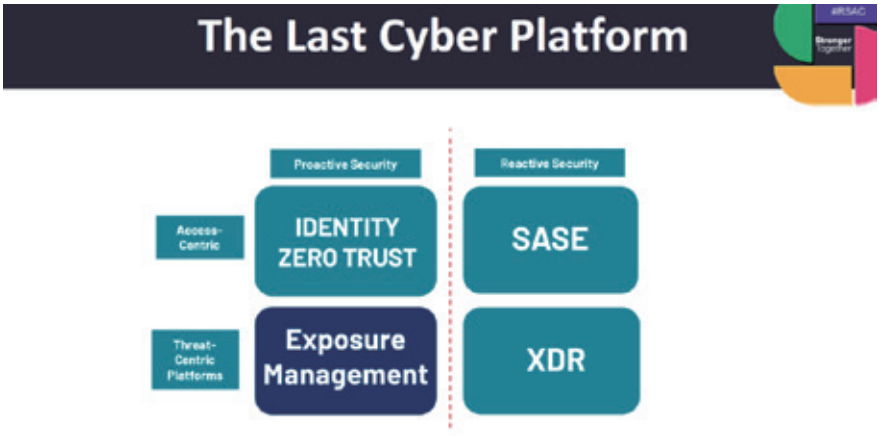
安全运营平台的核心能力是威胁的检测与响应，但已经属于事中和事后阶段了。因此，需要增加一些事前的主动安全的手段。

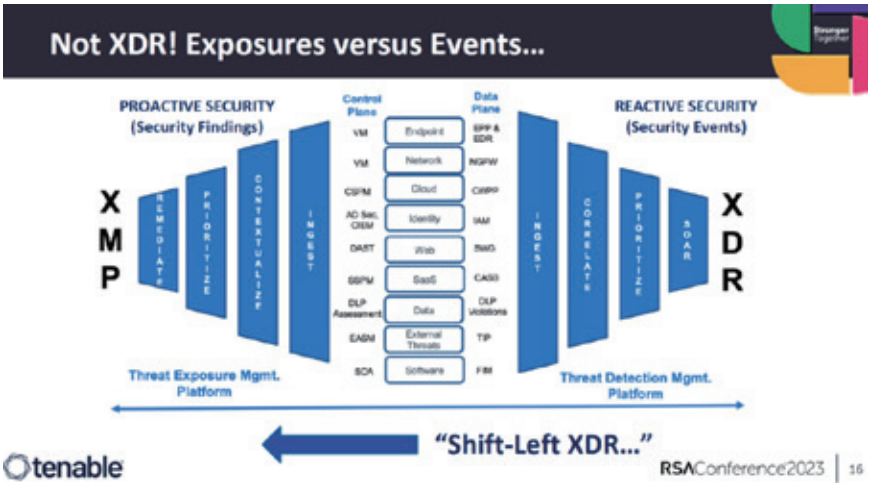
Tenable 的首席产品官 Nico Popp 介绍了将暴露管理纳入主动的网络安全平台的理念和框架。

Nico Popp 表示，暴露面管理补齐了以威胁为中心的（安全运营）平台缺失的一块内容，并进一步提出了 XMP（威胁暴露面管理平台）的概念。

除了以上大部分人都在讨论的未来安全运营的技术点，还有专家在







RSAC 上就未来的安全运营发表了更加激进的言论。

Trellix 的 CEO Bryan Palma 在《现在开启安全运营变革》的主题演讲中，提出了未来 SOC 的三个关键倡议：1）能回击对手的 SOC，强调先发制人（strike first）回击攻击者，使出扫堂腿（sweep leg），改变交战规则；2）游戏化的 SOC，强调构建一种高度游戏化的靶场或者攻防演练实景，借鉴游戏的奖励机制来激励人员，培养安全运营人才，并能快速平战转换；3）机器人运行的 SOC，强调构建一个在人类指挥调度和监督下的自主 SOC 或认知自动化 SOC。

考虑到 Trellix 脱胎于大量服务于军方的 FireEye 的背景，笔者可以理解这番表述。前两个倡议在军用级别和国家级别的 SOC 行得通，但对于民用级的 SOC，恐怕不现实。

选 XDR 还是选 SIEM？

笔者在 2 月份跟 Gartner 分析师 Pete Shoard 沟通时，他表示 XDR 更多是一种技术，并不是一个（产品）市场，也不会编写 XDR 的市场指南或者魔力象限。XDR 跟 SIEM 在应用场景上有重叠，但不会取代 SIEM。

业内知名的安全运营专家 Anton Chuvakin 在参加完此次 RSAC 大会后发表博客表示，相较于 2022 年的喧嚣尘上，今年 XDR 明显降温，并且有一些 XDR 厂商已经转型 SIEM。

我们可以看到，思科还在大力推广他们的 XDR 组合式（全家桶）解决方案，并且在大会上表示“XDR 不是 SIEM，可以跟 SIEM 联合工作”。笔者认为，在集成的和简化的检测与响应

理念大行其道的当下，思科所描述的 XDR 与 SIEM 的差别基本上都不是技术层面的，而更多是业务模式上的。

实际上，包括思科 XDR 在内的技术架构跟现代 SIEM 越来越趋同，尤其跟现代 SIEM 的 TDIR 应用场景相比较时，如下图所示。

此外，在赞助商的产品简报环节，Elastic 和 Cybereaon 还在讲 XDR。当你看完他们描述的内容，跟现代 SIEM 并无二致。

ESG 在大会上展示的调研报告凸显了用户侧对于 XDR 认知的分歧。55% 的受访者认为 XDR 是 EDR 的扩展【笔者注：这跟当今大部分依然奋战在 XDR 领域的厂商都是前 EDR 厂商高度一致】，28% 的受访者认为 XDR 是单一厂商提供的检测与响应套件（全家桶），还有 16% 的受访者认为 XDR 是一种集成的和异构的，用于威胁阻断、检测和响应的协作性安全产品架构（这类客户通常是大型客户，他们更倾向于通过采购 + 定制开发的方式自己搭建 XDR 体系）。显然，不同规模的客户，不同安全成熟度的客户，对 XDR 的诉求各不相同。

笔者认为，对于厂商而言，选 XDR 还是选 SIEM 更多是一种业务策略；对于用户而言，XDR 的定义不重要，选 XDR 还是选 SIEM 也不重要，关键是要实现集成的、简化的、高效的威胁检测与响应。

总结

回顾此次 RSAC 大会，安全运营已成为网络安全的焦点。安全运营技术则正处在 AI 应用落地的拐点，各种安全专用的生成式 AI 将对未来的安全运营平台产生深远影响。生成式 AI 跟编排自动化技术相结合，将创造出全新的交互模式，以及随之而来的极简和高效的用户体验。

一直处于碎片化的安全技术，正在通过集成化、智能化的网络安全平台进行有机整合，进而涌现出更多的应用场景，创造出更高的安全价值。

在安全创新的路上，我们始终要记住，复杂是安全最大的敌人。

四项技术重塑安全行业
——硅谷投资人解读 RSAC

作者 | 蔡新华

RSAC 2023 汇聚世界各地的顶尖网络安全专家、风险投资者和初创企业，探讨安全行业的发展趋势与技术热点；同时还展示了为应对数字化和分布式工作环境安全挑战而开发的前沿创新技术。

会议展现了大量安全创新技术和趋势，未来将深刻影响安全行业，其中，最值得关注的是人工智能成为大会讨论的焦点。第一天上午的会议包括由主要网安风险投资者主持的“网络安全风险投资现状”讨论，介绍安全领域的主要风险投资和并购活动与动态。创新沙盒比赛及 10 强企业的演示，反映出人工智能、区块链和机器与机器通信领域的重要发展趋势。HiddenLayer 从众多强大和成熟的竞争对手中脱颖而出，获得 RSAC 创新沙盒“最具创新性的初创公司”，符合了最近人工智能的火爆趋势。作为今年主题“携手更强大”（ Stronger Together ）的重要体现，Palo Alto Networks、Snowflake、Jupiter One 等头部网络安全企业在 RSAC 上展示了通过技术合作，实现对网络数据、流量、资产和 API 等的统一管理。

> 2023 创新沙盒比赛集中体现出四个领域的网络安全趋势，包括应用于人工智能（ AI ）和大语言模式（ LLM ）的网络安全、区块链技术、机器与机器通信，和远程工作。

安全行业风投趋于谨慎，投资兴趣仍持续不减

2021–2022 年，网络安全行业的风险投资环境出现明显变化。2021 年是一个蓬勃发展的市场，共发生 1048 笔融资，总金额达 304 亿美元，新增独角兽企业超过 30 家。2022 年则是总融资量下降的一年，共发生 1037 笔融资，融资金额 185 亿美元，融资量比 2021 年减少了 38.9%。这可能由于风险投资行为出现变化，特别是后期投资者在 2022 年下半年日趋谨慎，发现公开市场的价格和资产更具吸引力。然而，2022 年仍有 95 轮的融资超过 5000 万美元。此外，2022 年新增 15 家独角兽企业，包括 Vanta、Devo、Material 和 Sonar，这表明对创新网络安全解决方案的兴趣仍然持续存在。季度数据对比分析显示，2021 年第 4 季度融资金额 96 亿美元，2022 年第 4 季度降至 35 亿美元，而 2020 年第 4 季度的金额为 39 亿美元。这一下降趋势可能预示，在经过一段时期快速发展和投资增长后，市场开

始出现冷却。网络安全初创企业则需要控制支出，确保具有较高市场契合度的产品，并能实现收入增长。

另一方面，2022 年的并购活动则日益活跃，同比增长 48%，发生 263 笔交易，金额达 1190 亿美元。并购活动最活跃的细分领域包括托管安全服务提供商 (MSSP)、安全和风险管理，说明专业知识和资源整合成为这些领域的战略重点。2022 年发生 13 笔超过 10 亿美元的并购，包括 Keseya 以 62 亿美元收购 Datto，KKR 以 40 亿美元收购 Barracuda，Thoma Bravo 以 28 亿美元收购 Ping，以及 Vista 以 43 亿美元收购 KnowBe4 等并购案例。这些并购显示，业界对网络安全行业的兴趣和投资持续。大型私募股权玩家及领先的网络安全企业，为网络初创企业的整合和退出创造了重要的机会，如在过去 5 年，Palo Alto Network 共收购了 13 家安全企业。

人工智能、API、区块链与远程工作重塑安全行业

网络安全是一个由基础技术和社会趋势驱动的行业。由于技术创新、社会行为及监管的变化，新的机遇不断涌现。2023 创新沙盒比赛集中体现出四个领域的网络安全趋势，包括应用于人工智能（AI）和大语言模式（LLM）的网络安全、区块链技术、机器与机器通信，和远程工作。

人工智能 (AI) 和大语言模型 (LLM)： AI 可以算作 RSAC 的非正式主题。RSA 安全的首席执行官 Rohit Ghai 表示，零信任部署需要由 AI 来驱动。各类技术平台和应用持续集成 AI 和 LLM，这将彻底改变多个行业的

> 并购活动最活跃的细分领域包括托管安全服务提供商 (MSSP)、安全和风险管理。

发展。赢得创新沙盒大奖的 Hidden Layer，其机器学习检测与响应平台（MLDR）解决方案，就像 EDR 与 WAF 的组合，致力于保护企业的重要资产——AI 模型。OpenAI 公司发布的 ChatGPT，让许多人意识到 AI 的力量。大语言模型（LLM）可以实现人类自然语言交流和理解。鉴于最近不断曝出有企业的专有数据被贴入 ChatGPT，如三星公司曾有 3 名员工发生此类行为。许多企业都渴望可以确保自己的数据不被贴入 ChatGPT 这类面向公众的系统。为避免数据泄露和无意间披露，企业有必要打造私有模型 / 隔离版大语言模型。

网络安全企业对 AI 和 LLM 的利用还处于早期。但在 RSAC 2023 上，众多安全公司发布了基于 AI 的安全解决方案。Security Scorecard 公司展示如何使用 ChatGPT-4 来改进平台的人机交互问答，如询问平台上最危险的 10 个供应商是哪些。SentinelOne 则推出了自己的生成式 AI 解决方案，可以利用其自然语言有助于更好应对复杂威胁和对手狩猎问题。SentinelOne 首席执行官 Tomer Weingarten 表示：“网络安全人才严重短缺，我们解决方案可以提升安全从业人员的能力，使组织能够快速晋级，以保护云的安全，规避攻击者利

> 攻击者可以利用 AI 生成高级的恶意软件，实施自动化网络攻击或更精确地进行数据操纵。

用生成式 AI 快速发起自动化的攻击风暴。”正如 AI 可以用来撰写文章、生成照片和视频，为创意产业的人士带来高效一样，AI 也可以为网络安全人才带来更高效率。

尽管 AI 技术有许多好处，但也带来新的网络安全挑战。攻击者可以利用 AI 生成高级的恶意软件，实施自动化网络攻击或更精确地进行数据操纵。过去一年，我们已经看到黑客组织 LapSus$ 利用社会工程攻击，对微软、Okta 和 T-Mobile 等头部企业带来的巨大影响。这个黑客组织的成员年龄在 16~21 岁之间。想象一下，如果黑客像 Auto-GP 一样，24/7 地持续改进攻击工具，实施自动化网络攻击、社工攻击（使用人类语言进行交互），AI 赋能的黑客将会给社会带来什么样的危害？正如 SANS 数字情报高级主管 Heather Mahalik 所指出的那样，ChatGPT 可能会成为社工钓鱼攻击的工具。网络防御企业和专业人士需要未雨绸缪，为这些潜在风险做好准备。同样，安全防护人员也可以利用 AI 和 ML 改进威胁检测、自动化安全响应和大规模数据实时分析，从而可以实现网络安全防护能力的提升。为了防范不断出现的新兴威胁、不断演变的攻击，网络安全公司需要持续开发 AI 驱动的创新安全工具和解决方案。

API 和机器与机器 / 应用与应用通信：API、物联网设备的激增及远程工作方式的增长，导致机器与机器 (M2M)、应用与应用通信，以及 API 调用的增加。互联的网络环境扩大了网络的攻击面，现在攻击者可以利用 API 和机器相关资产（如密钥）中的漏洞实施攻击。

保护这些组件提供的综合安全解决方案的需求日益增长。根据《福布斯》最近的报道，研究机构 IT-Harvest 称目前美国市场就有 27 家 API 安全企业。创新沙盒 10 强入选企业 Astrix Security 就代表了这一趋势，该公司专注于应用的身份，将身份安全延展到了非人类身份的安全。

正如特权账户（PAM）负责管理组织高层的身份、密码和访问控制，机器也需要自己的专门治理系统。企业中 AI 应用和自动代理的兴起，将推动机器间通信的治理需求。如同传统的 PAM 一样，API 防护同样需要实现可见性、威胁检测、特权账户（包括机器）行为监测和快速响应。

远程工作和数字化转型：新冠疫情加速了远程工作的转变，迫使组织迅速采用数字解决方案。这种转变扩大了网络犯罪分子的攻击面，因为企业越来越依赖云服务、远程访问工具和在线通信平台。对综合安全解决方案的需求出现激增，如安全访问服务边缘 (SASE)、零信任架构和端点安全解决方案。这一趋势为网络安全公司开发和提供尖端产品和服务创造了机会，只有这样才能有效地保护远程劳动力和数字基础设施。

特别是今年，笔者看到许多企业级浏览器初创企业和解决方案。Island 和 Talon 是这一领域较为知名的两家，此外还有笔者投资过的 Mammoth Security，以及至少另外四家早期初创公司，它们都专注于从浏览器提供安全服务，今年在 RSAC 都有各自的展位。企业级浏览器重要，原因是加密的网络流量使行为分析更加困难，VPN 只能保护连接而无法进行监测。

然而，浏览器天然可以观测、检测、记录和识别异常的或有风险的行为，如下载大量内部代码或将文档粘贴到 ChatGPT 中。这一技术方向的重要性未来可能会继续增加。

Web3/ 区块链：以去中心化和分布式特性著称的区块链技术，在各个行业获得了重大发展机遇。它虽具备数个安全优势，但它并不能免于网络威胁。区块链具有各种攻击面，以及代币的大量资产。2022 年发生了针对区块链的重大黑客攻击，如以太坊跨链桥（Ronin Bridge）黑客事件（损失超过 6 亿美元）和蠕虫桥利用漏洞（损失超过 3 亿美元）。区块链生态系统的网络安全可谓至关重要。Anchain 入选 RSA 创新沙盒决赛 10 强，是 RSAC 认可区块链安全重要性的第一步。

最近，像 SEC 等政府机构加大对加密资产执法和监管，提供链上情报、监测、检测和调查的网络服务将会非常重要。除了基于钱包的多方安全和欺诈交易检测，也出现了智能链合约，协议审计与形式化验证，以及恶意地址库等安全工具。与通用网络安全相似，Web3 网络安全领域也将迅速成长出一体化和拥有单项优势的安全企业。

值得注意的是，Anchain 不是创新沙盒 10 强中的唯一 Web3 安全公司。Zama AI 的完全同态加密可以通过在智能合约中保持输入和输出加密，并在转换过程中解密，来实现更私密的区块链交易。在演示时，公司首席执行官提到与 ZK(零知识证明) 的集成，使端到端加密和解密成为可能。这可以帮助保护交易隐私。

合作与平台化大行其道 前景依然充满光明

正如 RSAC 2023 的官方主题“携手更强大”（ Stronger Together ），大型技术平台企业和网络安全企业正努力成为主要平台，来管理数字基础设施的关键要素，如身份、数据、网络流量、资产和 API，并通过产业合作，提供全面的安全和管理能力。RSAC 2023 上多家安全企业展示了合作成果。Zscaler 展示其统一云访问和事件流平台，与北极狼的托管安全运营服务、开放 XDR 平台的整合，同时可以接入其他的平台。Snowflake 与 Hunters 合作，展示了其单一源数据平台，提供网络安全为核心的数据管理层，用于即开即用的安全分析和数据。Tines 与 JupiterOne 达成合作，以利用其 API 连接能力和 JupiterOne 的资产管理技术。未来，网络安全行业将继续需要实现流网络量、资产、API 等各类数据的各自统一管理，安全企业正通过合作实现这一目标。

RSAC 2023 展示了网络安全行业的最新趋势和创新，其中 AI、区块链技术和远程工作的影响不断增加。RSAC 透露出风险投资和兼并收购活动的变化，显示安全行业的风险投资行为发生了变化，后期投资者将更趋谨慎。

尽管如此，网络安全行业将继续见证新独角兽企业的出现，未来安全行业也将仍然是战略性收购的重要领域。由于技术平台、创新、社会行为和监管的持续变化，网络安全也将不断演进。

随着 AI、LLM、API、M2M 通信、远程工作和区块链技术重塑安全行业，新的机遇和挑战将会不断涌现。大型技术平台企业和网络安全企业正努力发展成为主要的平台，负责管理数字基础设施的关键要素，如身份、数据、网络流量、资产和 API 等。

网络安全的未来前景依然充满光明，安全企业将会持续开发创新解决方案，并加强合作，只有这样才能应对不断变化的威胁，保护互联世界的宝贵数字资产。

> 大型技术平台企业和网络安全企业
> 正努力成为主要平台，
> 来管理数字基础设施的关键要素，
> 如身份、数据、网络流量、资产和 API，
> 并通过产业合作，提供全面的安全和管理能力。

创新沙盒背后的安全热点

4 月 24 日，RSAC 宣布 HiddenLayer 成为年度 RSAC 创新沙盒比赛的获胜者。作为今年的“最具创新性的初创公司”，HiddenLayer 主打 AI 安全，其 HiddenLayer MLsec平台可以检测对抗性 ML 攻击，保护模型免受攻击，而无需访问任何原始数据或算法。北京网络安全大会创客汇评委直击 RSAC 现场，对创新沙盒冠军与 10 强进行深度解读。

HiddenLayer 联合创始人兼首席执行官 Chris Sestito 与创新沙盒评委

HiddenLayer获冠军，AI 安全成行业热点

每年的创新沙盒比赛都会结合当年的热点，数世咨询的创始人李少鹏表示，去年创新沙盒比赛的热点是云原生安全，今年则是 AI 安全。

今年的创新沙盒中凸显出人工智能技术的热度——十强企业中有三家企业：HiddenLayer、AnChain.AI、Relyance AI，分别致力于 AI 模型防护，区块链安全的 AI 应用，以及利用机器学习进行隐私管理、治理数据和合规运营。

知名安全专家、赛博英杰董事长谭晓生表示，今年 ChatGPT 的出现，让 AI 安全成为热点。RSAC 会议的所有研讨环节（session）都会涉及 AI 话题。企业也都在尽量贴上 AI 标签。AI 出现过热的现象。

IDC 预计，2023 年企业在人工智能方面的支出将增长 27%，达到 1540 亿美元。ChatGPT 及后续版本持续爆火，也深刻影响到网络安全行业。随着 ChatGPT 等人工智能服务的大量应用，将成为越来越有吸引力的攻击目标，黑客可以对模型进行逆向工程或使用“对抗性”数据对模型进行篡改。

普华永道预计，2030 年人工智能将发展成为 15.7 万亿美元的市场，这预示着 AI 安全防护领域将存在巨大的市场需求，这或许也是

BCS 安全创客汇专家直击 RSAC 创新沙盒

HiddenLayer 被评为创新沙盒冠军背后的行业背景。

尽管 AI 安全备受关注，但对话嘉宾对于创新沙盒冠军 HiddenLayer 的商业模式存在疑虑。元起资本联合创始合伙人万熠认为，这取决于未来的应用模型数量。如果大量公司都拥有自己的模型，就可能会存在较大需求。

奇安信集团副总裁张聪表示，ChatGPT 表现出的理解力是过去的模型所不具备的。3 年前 OpenAI 发布 GPT-3 时就受到安全行业关注。奇安信目前主要关注 ChatGPT 技术在网络安全领域的应用，以及广泛应用之后的安全防护问题。目前奇安信已经基于 ChatGPT 相关技术和自身积累的海量安全知识和数据，训练奇安信专有的类 ChatGPT 安全大模型。奇安信天眼小助手推出的 3 年来，显著提高了安全人员的工作效率。

对于 ChatGPT 等模型在安全行业中的未来应用与影响，谭晓生预测，在很近的未来，初中级的网络安全工作人员或将会被人工智能所替代。

创新沙盒背后的网络安全热点与趋势

2023 年创新沙盒 10 强中，除了 3 家人工智能相关的创新企业，入选的初创安全公司还涉及供应链安全、云安全、云身份安全、可信通信平台、安全自动化、密码应用与隐私安全。

50 家十强企业主要集中在
云安全、数据安全、软件供应链安全、身份安全
四个热门赛道。

BCS 安全创客汇专家认为，除了了 Web3，国内的安全创客汇 50 强，对于目前业界主流的安全热点都有较为全面的覆盖。

奇安信集团产业发展研究中心通过创新沙盒近五年（2019—2023）年十强赛道分析，发现 50 家十强企业主要集中在云安全、数据安全、软件供应链安全、身份安全四个热门赛道。

与创新沙盒 10 强专注细分领域创新不同，安全创客汇 50 强的初创公司有着更大的梦想，反映出中外安全创业公司的区别。对此，作为资深行业专家兼投资人，谭晓生每次看到创新沙盒 10 强的初创企业，往往会倍感焦虑，因为国内初创安全企业专注于细分领域通常会难以生存。这凸显出国内网络安全行业创新创业中的不健康局面。

BCS 安全创客汇专家对云安全、Web3 安全等热点趋势进行了点评。

云原生与 AI 的安全都是基于新场景需求出现的技术。对此，张聪表示，云开发模式的变化，导致安全响应方式发生变化。云原生安全不能简单等同于容器，它是一套对云原生应用的端到端保护的一套完整逻辑和思想。

此外，Web3 作为吸引众多投资等领域，其安全问题也备受关注，国内也出现了多家专注区块链相关安全的创业企业。

专家激辩创新驱动力，产业发展依赖更严监管

针对网络安全领域的创新驱动力，BCS 安全创客汇专家有着类似却又不同的见解。

元起资本联合创始合伙人万熠认为，相对其他产业，网安产业是一个三边产业，涉及厂商、甲方和监管方。推动网络安全发展的动力从根本上是解决黑产的问题。攻击方技术的提升促使网络安全的技术创新与发展。

谭晓生认为，中美的网络安全创新背后都是需求驱动。但中美两国在监管上的不同造成了安全需求不同。美国对于安全事件的巨额处罚带来了巨大的网络安全需求，这推动了美国在网络安全领域的更多创新。

谭晓生建议，对于网络安全，应该参考消防领域，将其作为公共安全进行监管。与国内火灾每年造成损失数十亿人民币相比，国内因网络攻击造成的经济损失达到数百亿美元(2021 年 600 亿美元），国内网络安全市场规模与此不成正比。

据悉，安全创客汇作为我国网络安全领域的专业创投大赛，目前已连续举办七届。2023 年第八届安全创客汇于 2 月份启动，近期将公布本届安全创客汇初赛 50 强晋级名单，将在 2023 BCS 期间举办总决赛。

威胁情报与人工智能的碰撞融合效应

作者 | 张宇

RSAC 2023 共有 500 余场高峰论坛、主题演讲和研讨会，涵盖了多方面的热点话题，除历年备受关注的“创新沙盒大赛”外，还有如漏洞攻击、高级持续威胁（APT）研究、安全分析 / 情报及响应、黑客和威胁、云安全及运营、机器学习 / 人工智能及自动化等热点话题。

通过奇安信产业发展研究中心对近 5 年创新沙盒发展和变化的分析，除云安全、数据安全、软件供应链安全、身份安全四个热门赛道热度持续外，智能应用和自动化异军突起。随着 ChatGPT 风靡全球，以及创新沙盒冠军 HiddenLayer 的诞生，AI 安全成功杀出重围，似乎是一夜间就占据各大主流媒体的头版头条，成为炙手可热的创新赛道。

自上个世纪起，依赖于规则引擎发展的“人工智能”就在不断给我们的生活带来惊喜和变革，直到其进入机器学习和深度学习阶段，广泛应用于图像识别、语音识别、自然语言处理等领域，开始不断给网络安全产业带来“惊喜”。如今，人工智能和机器学习技术已经广泛应用在威胁情报、威胁检测、响应和修复等各个方面。

2023年（智能与自动化）			2022年（云原生安全）			2021年（数据安全）			2020年（供应链安全）			2019年（云安全）		
公司名称	国家	技术领域	公司名称	国家	技术领域	公司名称	国家	技术领域	公司名称	国家	技术领域	公司名称	国家	技术领域
AnChain.AI	美国	智能SOC	Araali Networks	美国	云原生安全（威胁管理）	Abnormal Security	美国	邮件安全	AppOmni	美国	云安全（SaaS应用安全）	Arkose Labs	美国	身份与访问安全（身份滥用）
Astrix	以色列	云身份安全	BastionZero, Inc.	美国	身份与访问安全（零信任）	Apiiro	以色列	软件供应链安全（代码安全）	BluBracket	美国	软件供应链安全（代码安全）	Axonius	美国	网络安全资产管理
Dazz	美国	安全自动化	Cado Security	英国	云原生安全（数字调查与取证）	Axis Security	美国	身份与访问安全（零信任）	Elevate Security	美国	安全意识教育	Capsule8	美国	云安全（容器安全）
Endor Labs	美国	软件供应链安全管理	Cycode	以色列	软件供应链安全（代码安全）	Cape Privacy	美国	数据安全（隐私计算）	ForAllSecure	美国	软件供应链安全（代码安全）	CloudKnox Security	美国	身份与访问安全（IDaaS）
HiddenLayer	美国	AI攻防对抗	Dasera	美国	数据治理与运维（DataGovOps）	Deduce	美国	身份与访问安全（零信任）	INKY Technology	美国	邮件安全	DisruptOps	美国	云安全（云管理平台）
Pangea	美国	云安全平台即服务	Lightspin	以色列	云原生安全（云安全平台CNAPP）	Open Raven	美国	数据安全（数据治理）	Obsidian Security	美国	云安全（SaaS应用安全）	Duality	美国	数据安全（密码应用）
Relyance AI	美国	智能数据治理与隐私安全	Neosec	美国	API安全（XDR）	Satori	以色列	数据安全（隐私合规）	SECURITI.ai	美国	数据安全（数据治理）	Eclypsium	美国	硬件及固件威胁预防
SafeBase	美国	可信通信平台	Sevco Security	美国	云原生安全（资产管理）	Strata	美国	身份与访问安全（IDaaS）	Sqreen	美国	软件供应链安全（开发安全）	Salt Security	美国	云安全(API保护)
Valence Security	以色列	安全自动化	Talon Cyber Security	以色列	安全浏览器	Wabbi	美国	软件供应链安全（开发安全）	Tala Security	美国	数据安全（隐私保护）	ShiftLeft	美国	软件供应链安全（开发安全）
Zama	法国	密码应用与隐私安全	Torq	以色列	安全运营（无代码自动化平台）	WIZ	以色列	云安全（无代理云安全平台）	Vulcan Cyber	以色列	云安全（漏洞管理和修复）	WireWheel	美国	数据安全（隐私计算）

创新沙盒 2019—2023 年十强赛道分析

人工智能技术通过与威胁情报的深度融合，可以极大地提高运营人员的分析效率、增强预测能力、提高精度和准确性、实现自动化分析。

威胁格局正在不断演变

今年的 RSAC 大会上，多位行业专家围绕人工智能发表了主题演讲，包括 SentinelOne、谷歌云、IBM 等在内的众多知名厂商都发布了基于生成式 AI 技术的网络安全工具。

抛开“人工智能是否被过热推崇”的争论，以及人工智能引发的“人工焦虑”不谈，不得不承认，人工智能确实又一次引发了新技术浪潮，根据 IDC 预测，2023 年企业在人工智能技术上的投入将达到 1540 亿美元，增长 27%，暗示了今后人工智能巨大的市场需求。

当今全球的网络安全形势变幻莫测，地缘政治因素引发的各种 APT 攻击活动持续加剧，网络威胁将更加智能化、复杂化、多样化、全球化，因此，组织需要采用更加先进和综合的安全措施，以应对不断增长的网络威胁。同时，受宏观经济的不确定性影响，导致众多安全公司都在不同程度上削减网络安全预算，失业率上升也增加了网络犯罪的风险。而据奇安信威胁情报中心预测，“2023 年，受地缘政治冲突影响，APT 攻击活动持续加剧；对受害国本土软件的漏洞利用愈加频繁；瞄准关键基础设施的破坏越发泛滥；各类新型钓鱼攻击活动将频繁出现。”

近年来，人工智能技术通过与威胁情报的深度融合，可以极大地提高运营人员的分析效率、增强预测能力、提高精度和准确性、实现自动化分析，这使得企业可以更快速地识别和应对网络安全威胁，降低运营成本，增强安全防御能力；Palo Alto Networks 高级副总裁 Kumar Ramachandran 在 RSAC 2023 的主题演讲中称，威胁格局正在不断演变，利用机器学习可以阻止高达 95% 的未知威胁。

但二者的不断发展也使得网络安全面临着诸多挑战和威胁，人工智能技术助推了攻击者不断演化和更新攻击手法，制定针对性的攻击策略，并更加难以被发现和防御，大大降低了网络犯罪的门槛。

SANS 的安全专家在本次会议上分享了《五种最危险的新型攻击技术》，对抗性人工智能攻击和 ChatGPT 驱动的社会工程学攻击被重点提及。在对抗性人工智能攻击中，攻击者可以操纵 AI 工具来加速勒索软件活动，并可以识别复杂系统中的 0day 漏洞，从简化恶意软件编码过程到普及社会工程，对抗性人工智能已经改变了攻击者的游戏规则。而风光无两的 ChatGPT，也在逐步沦为攻击者进行社工攻击的一把利刃，SANS 的研究员 Heather Mahalik 在交流中表示，这种发展意味着用户现在比以往任何时候都更容易受到攻击，只要误点一个恶意文件，不仅会使整个公司面临风险，还会影响受害者的生活。

威胁情报与人工智能的融合效应

在 2023 年 RSAC 大会上，谷歌

云正式宣布推出行业首款由专业安全的 Sec-PaLM 大语言模型（LLM）驱动的可扩展平台——Google Cloud Security AI Workbench，这种新型的安全模型包含了该公司威胁态势洞察，以及 Mandiant 关于漏洞、恶意软件、威胁指标和攻击者信息的一线情报。谷歌云 Security AI Workbench 已经为其多款新产品提供支持，解决其企业客户的安全挑战。

威胁情报与人工智能的深度融合，利不可抛，弊不可弃：

1. 威胁情报的时效性和上下文信息

时效性和上下文信息是影响威胁情报实际应用效果的两个重要属性，人工智能和机器学习技术的发展，改变了依靠人工获取和处理威胁情报的传统，通过算法和模型自动化地处理和分析大量的文本、语音和图像等数据，自动识别数据中的关键信息，发现网络资产中存在的漏洞，并快速提供分析报告和上下文信息，减少人力成本的同时，也极大的减少了漏报和误报，威胁情报分析和处理的速度和准确度得到了提高，进一步增强了威胁情报的时效性和有效性。

2. 实时精准的自动化检测和响应

目前人工智能技术已经可以实现对海量数据源的数据进行监控和分析，及时发现异常流量，快速识别和定位潜在威胁，通过机器学习算法对网络数据进行自动分类和识别，并对识别出的恶意软件和网络攻击进行自动化检测和拦截，保护企业和组织网络资产的安全。

3. 风险评估和风险预测

人工智能技术可以通过数据挖掘和分析，快速识别和评估各种威胁，减少漏报和误报。通过机器学习算法和模型分析网络日志，发现异常行为，多个角度对未来的风险进行分析，预测出未来可能的攻击类型和攻击目标，提高决策的可靠性和准确性，帮助企业和个人更好地制定应对策略。例如，人工智能技术可以对网络漏洞进行扫描和评估，预测漏洞被利用的可能性和影响范围，从而提高漏洞修复的效率和准确性。

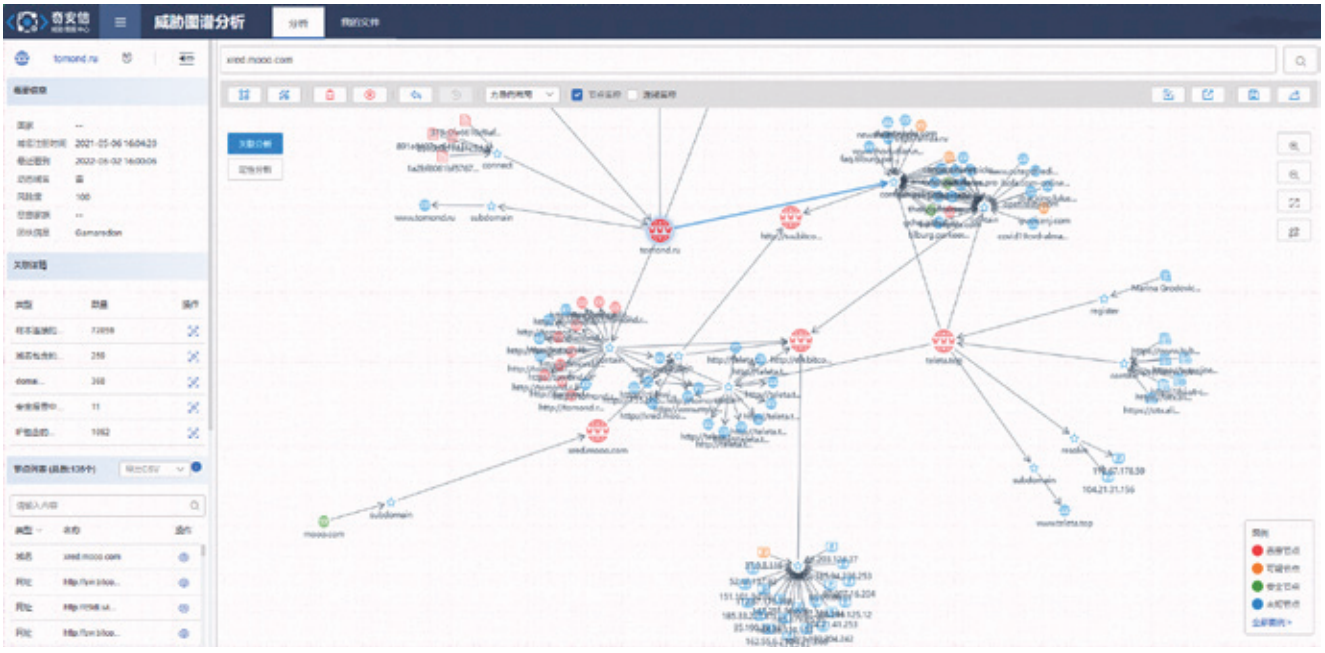
4. 无处不在的网络攻击和无法避免的漏报、误报

随着人工智能技术与威胁情报领域的融合越来越深入，其在威胁情报分析和应用中的不利影响也越来越显现：

1）人工智能虽然已经大幅度减少了漏报、误报的可能，但因为人工智能算法的训练数据可能不够全面或者存在偏差，导致算法出现错误的判断，这就需要人工进行二次研判，以最大程度减少误报。同时，人工智能处理威胁情报时，往往只能处理结构化数据，而无法处理非结构化数据，这就导致了信息不全面，从而产生漏报。

2）人工智能算法本身也存在着被

> 人工智能技术已经应用于奇安信威胁情报生产运营流程的各个环节，
> 也应用于威胁情报中心推出的多款安全产品中。



攻击的风险，黑客可以通过注入恶意数据或攻击算法模型，来干扰算法的判断，从而影响威胁情报的分析结果。

3）伴随着人工智能技术的发展，一些新型的攻击方式也层出不穷，使得网络攻击更加普及和难以应对。一些黑客可以利用机器学习算法进行网络钓鱼，还可以利用人工智能技术对网络进行扫描，发现网络漏洞，对攻击进行自适应等。

人工智能在威胁情报领域的典型应用

目前，人工智能技术已应用于奇安信威胁情报生产运营流程的各个环节，也应用于威胁情报中心推出的多款安全产品中，其中，ALPHA 威胁分析平台的“威胁图谱分析”模块尤为典型。

知识图谱是结构化的语义知识库，通过将各种实体、概念和关系以图形化的方式表达出来，从而构建出一个涵盖了丰富知识的结构化数据集。知识图谱的构建需要大量的数据积累和处理，人工智能技术可以通过自然语言处理、机器学习、图像识别等技术，对非结构化数据进行分析和处理，将其中的实体、概念和关系与知识图谱中的实体、概念和关系进行关联，将海量的数据转化为可用的知识图谱。

ALPHA 威胁分析平台——威胁图谱分析，是一款面向安全运营分析人员的可视化威胁分析工具，是知识图谱的高级可视化呈现，通过构建知识层级的威胁情报查询系统，针对某个单一的威胁实体，提供基于该实体的基本属性、关联关系、关联节点属性的结果数据集。

威胁图谱分析支持对 IP、URL、Hash、Domain、Email 等多类型数据实体的单个查询及批量查询，采用多种人工智能领域优化算法，自动化进行快速、精准的数据解析匹配，分析各类实体之间的关联关系和各种行为之间的因果依赖关系，基于威胁发现能力模型，展示数据实体间的关联关系，并提供多方位下钻查询、拓线溯源能力。该功能模块可以实现攻击者溯源及画像，使得安全运营人员快速、高效地提取高价值威胁情报、挖掘异常行为、提升安全响应效率。

结语

RSA Security 首席执行官 Rohit Ghai 在 RSAC 2023 大会的开幕式上说：“恶意黑客将在复杂的网络钓鱼活动中使用 AI 工具，并创建恶意 GPT 以伪造身份。网络安全专业人士必须借助 AI 的力量才能消除这些威胁。”由此可见，人工智能席卷整个行业的同时，人类必须要做的不仅是依靠 AI 获取更高的价值，还必须学会正视它的威胁，最大程度的驾驭这个行业“武器”，使“人类智能”与“人工智能”相辅相成。

RSAC 10 款新一代安全新品

作者 | 张宇

安全厂商在 RSAC 2023 上发布了一系列安全新品，其中包括 SentinelOne、谷歌云、埃森哲、IBM 等，整合应用生成式 AI 技术成为新一代网络安全产品的主打特色。

研究人员收集整理了在大会期间发布的 10 款新一代网络安全工具，对其主要应用特点进行了分析和介绍。

1. SentinelOne Threat Hunting Tool

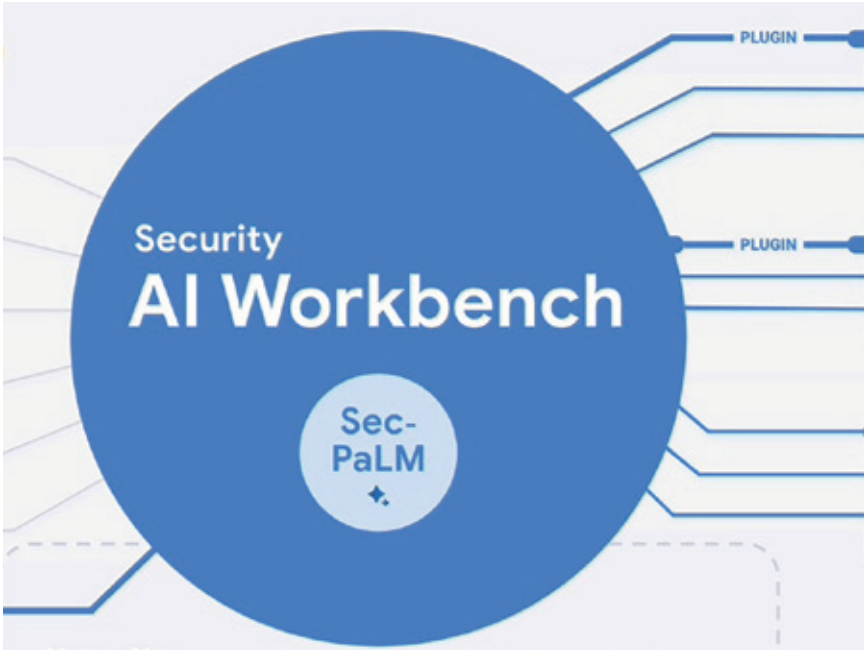
SentinelOne 公司在今年的大会上发布了一款新的网络安全威胁搜索工具，并表示这是生成式 AI 技术在网络安全领域应用的一项重大进展。该工具充分利用了大型语言模型(LLM)，相比传统模式，大幅提高了安全分析师的工作效率。SentinelOne 将这款基于生成式 AI 的新型威胁搜索工具称为“Purple AI”。

安全分析师能够在 Singularity Skylight 分析平台中使用新的生成式 AI 工具，并针对其组织环境中的安全威胁提出问题。通过使用自然语言查询系统，将为安全分析师大大节省威胁处理的时间，从而有更多的时间去响应更多的安全警报，并识别更多攻击。生成式 AI 技术还可以为分析师提供更简洁的事件分析报告，优化安全分析工作的效率。

据 SentinelOne 公司介绍，以这种方式实施生成式 AI 技术的主要目的是简化威胁搜索复杂度。整合这种生成式 AI 技术后，可以有效地帮助企业的安全运营团队扩大威胁搜索活动的规模。新的 SentinelOne 威胁搜索工具最初将作为 Singularity Skylight 平台的附件来提供，目前已处于有限试用阶段。

2. Google Cloud Security AI Workbench

谷歌云也发布了最新的 Security AI Workbench 产品，旨在帮助企业用户缓解威胁数据和使用众多安全工具所带来的日常安全运营压力。Security AI Workbench 基于一种名



为 Sec-PaLM 的新型安全专用大型语言模型。该模型充分结合了谷歌云丰富的威胁数据及 Mandiant 在漏洞和恶意软件方面的情报数据。

据了解，使用谷歌云 Security AI Workbench 的客户，目前只能在特定时间向 Security AI Workbench 平台输入可供模型学习的隐私数据，以保证数据使用中的安全性。谷歌云将会把 Security AI Workbench 率先部署在其新产品 VirusTotal Code Insight 上，该新产品使用这项技术分析各种可能存在恶意的脚本，并向安全分析师解释其异常行为，最终有助于客户改进检测流程、增强威胁发现能力。该产品目前还处于试运行阶段，使用 Security AI Workbench 技术的更多产品和方案将于今年夏天正式推出。

3. Accenture MDR

埃森哲公司在今年的大会上正式宣布，将通过与谷歌云合作，推出新的 MDR（托管式威胁检测和响应）服务，其中，主要的 AI 功能将会基于谷歌云最新发布的 Security AI Workbench 产品来实现。该服务将充分利用云原生的安全信息事件管理平台和 Mandiant 的威胁情报，并通过 Security AI Workbench 提升安全分析师的工作效率。

为了让用户可以更快地访问 Mandiant 威胁情报，新的 MDR 服务系统会充分利用生成式 AI 的分析能力和总结能力。比如，可以利用生成式 AI 系统让分析师更快地确定新的威胁活动模式和特征，从而更快速、更有效地识别出未知威胁。

4. Cisco XDR

思科在今年的大会上正式发布了最新的扩展检测和响应（XDR）平台，这是一个全新设计的多功能威胁检测和响应平台，不仅融合了传统网络检测和响应（NDR）与端点检测和响应（EDR）能力，还具有独创性的跨域遥测数据能力。此外，新 XDR 平台利用循证自动化技术，几乎实现了可实时检测威胁，并确定威胁响应优先级，大幅提升了安全团队的运营效率。

此外，Cisco XDR 的独特之处在于，不仅可以轻松整合旗下众多安全工具的高保真数据，还可以整合市场上主流的第三方安全产品，包括 Microsoft Defender、Cybereason、Palo Alto Networks Cortex XDR、SentinelOne Singularity、Trend Micro Vision One 及 ExtraHop Reveal NDR 等。

5. IBM Security QRadar Suite

IBM 公司在大会上针对安全运

营团队推出了新的产品套件：IBM Security QRadar Suite。QRadar Suite 一直是 IBM 多年深耕威胁检测和响应领域的成果。在新发布的版本中，最主要功能特色也是基于 AI 的创新设计，如基于 AI 的警报筛选、自动化威胁调查及智能化的威胁搜索。

通过 AI 技术的应用，新的产品升级主要体现在统一的分析师体验、SaaS 化交付模式及与 900 多个第三方工具集成。IBM Security QRadar Suite 的核心产品包括：面向云原生日志管理和安全可观察性的 QRadar Log Insights、QRadar XDR、QRadar SOAR 以及 QRadar SIEM。

6. CrowdStrike CrowdStream

在今年的大会上，CrowdStrike 公司和可观察性初创公司 Cribl 共同推出了一项新产品 CrowdStream，旨在实现更加快捷和准确的网络安全数据采集与分析，该产品基于 Cribl 研发的开放可观察性平台来实现。

据介绍，CrowdStream 平台可使用 Cribl 可观察性管道将任何数据源直接连接到 CrowdStrike Falcon，大大简化并降低了将数据采集的成本和时间。该产品最终可以帮助用户提升对 XDR 和 SIEM 等工具的应用效果，同时有助于汇集用于训练 AI 和机器学习模型的数据。

7. Zimperium Mobile-First Security Platform

专注移动安全的创新厂商 Zimperium 在大会上宣布，已成功实现了对移动设备防护和移动应用程序防护的能力整合。Zimperium 最新发布的 Mobile-First Security Platform 方案将其原有的 Mobile Threat Defense 产品与 Mobile Application Protection Suite 产品主要功能相结合，简化了企业安全团队的应用复杂性，实现了端到端的移动安全防护能力融合。

Mobile-First Security Platform 方案的优点之一就是为移动访问和管理两款安全产品提供了集中式界面，其他主要功能还包括：实现了设备端的威胁检测，无需再将数据上传云端；增加了阻止逆向工程的应用程序保护机制。

8. Flashpoint Ignite

Flashpoint 公司在今年的大会上发布了最新的情报平台 Ignite，旨在帮助组织更好地防御网络威胁和物理威胁。该平台的最大特点在于，可以通过跨组织的多个不同团队来采集情报信息，并提供可以充当团队之间协作桥梁的情报数据。

最新版 Ignite 的主要功能包括，Flashpoint Cyber Threat Intelligence，可以通过搜索数千个情报来源，同时监控不同威胁分子之间的联系，并获取来自 Flashpoint 分析师的威胁情报分析报告。方案其他重要功能还包括：可以帮助团队区分和修复漏洞的管理功能、监控和警报物理安全威胁的 Flashpoint Physical Security Intelligence 功能，以及面向特殊任务的 Flashpoint National Security Intelligence 功能。

9. Cybersixgill Attack Surface Management

网络威胁情报服务商 Cybersixgill 今年发布了一种新的攻击面管理解决方案，可以帮助用户的安全团队更快地区分和响应威胁。新方案充分利用该公司的威胁情报数据，帮助用户消除资产可见性盲点，并提供未知资产的持续映射和分类。这种持续的外部资产发现能力全面包括了识别域及子域、IP 及主机、已知漏洞、软件以及证书。

新方案的其他主要功能还包括：资产库存管理，可以帮助用户深入了解资产关联、位置和资产类型；以及与威胁情报相关的资产监控，便于用户快速了解潜在风险和相关警报。

10. Torq Hyperautomation Platform

初创型安全公司 Torq 在今年大会上也发布了最新的 Torq Hyperautomation Platform 方案，有望帮助企业组织自动管理大规模环境下的超复杂安全基础设施。新平台可以针对组织常见的安全运营工作任务，将自动化能力充分引入到整个流程和工作流。

据公司介绍，Torq Hyperautomation Platform 主要功能包括：能够跨所有基础设施环境（包括 Slack、Zoom 和 Microsoft Teams）连接所有应用程序和堆栈；支持任何命令行接口或编程语言，以实现“自带代码”；编排容器化操作（支持 Docker、Kubernetes、AWS 和 Azure），以实现“自带容器”。

此外，Torq Hyperautomation Platform 还通过 ChatGPT API 整合了 OpenAI 技术，初步拥有了生成式 AI 功能。该平台可以通过 Slack、Teams、Discord 和 Zoom 中的聊天机器人界面，为用户解答问题，以帮助用户加快解决所遇到的安全问题。安

奇安信 | BEIJING 2022

北京2022年冬奥会官方网络安全赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

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

规划快一步

奇安信

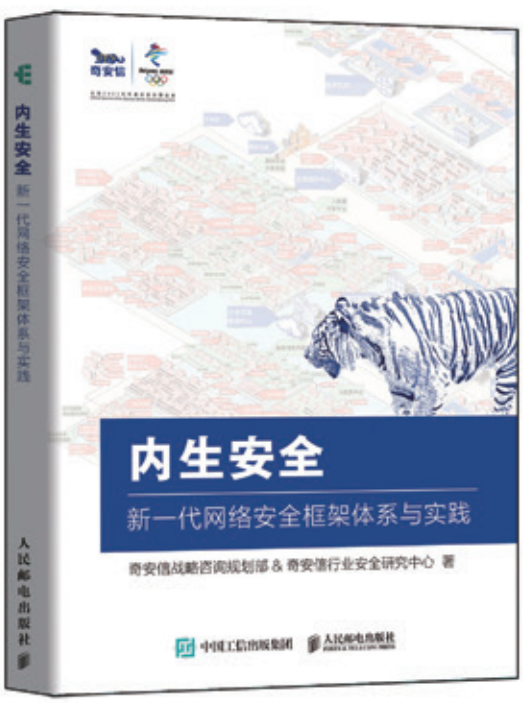
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

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

为了做好这件事，他们在漏洞堆里挖呀挖呀挖

作者 | 魏开元

“你觉得这么些年总共 30 万个漏洞很多吗？”奇安信威胁情报中心负责人汪列军反问道。

略作思考，笔者回答道：“应该挺多的吧。按照咱们奇安信 CERT 发布的数据来看，2022 年收录了 26000+ 条漏洞信息，也要十多年才能达到这个数量级。”

“话是这么说，但却不是这么个算法。我们收录的也只是已经公开的漏洞，其实很多软件包含的漏洞状态是未知的，随便拿一个有点规模的网络应用软件过来，对其做一下漏洞挖掘，发现个数位的中高危漏洞（命令执行、SQL 注入、文件泄露等），十位数的低危漏洞（跨站脚本执行类）是极其常见的。所以我保守估计，即便是在去掉所有重复漏洞（即多个软件使用了含有相同漏洞的开源组件）的情况下，现有漏洞总量至少比 30 万高一到两个数量级。”

“这么多吗？”

“只多不少，我们做漏洞情报的意义也就在这儿，能够为用户提供基于实际风险的漏洞处置优先级排序。”汪列军话锋一转，假如是你，三两个人的团队每天要看七八十个漏洞，今天搞不定明天又有新的七八十个来了，这事儿闹不闹心？

既然不能全部搞定，就得有所取舍。

一、收集器、过滤器和富化器

笔者首次领略漏洞情报的魅力还是在 2017 年。

3 月 14 日，微软在例行补丁日发布了数十个安全更新，其中有一个被微软官方标记为 MS17-010 的漏洞被正式修复。

根据微软官方的描述，此安全更新程序修复了 Microsoft Windows 中的多个漏洞。如果攻击者向 Windows SMBv1 服务器发送特殊构造的消息，那么其中最严重的漏洞可能允许远程执行代码。

对于 Microsoft Windows 的所有受支持版本，此安全更新的等级为“严重”。

无独有偶，一个月后的 4 月 14 日晚，Shadow Brokers（影子经纪人）公布了一大批黑客工具，其中“永恒

之蓝”可以利用上述微软漏洞获取系统最高权限。经过技术验证，已经确认利用这个漏洞能够形成蠕虫式的攻击传播，可惜当时没有足够大的声量把这个认定传播开来引发最大程度的重视。

最终最坏的结果还是沿着技术逻辑的必然导向发生了，攻击者打了所有人一个措手不及。当年的 5 月 12 日爆发了迄今为止最严重的安全事件，利用“永恒之蓝”工具制作的勒索病毒 WannaCry 开始广泛传播，数以百万计的机器中招下线。

事后回想起来，中招的群体无非就这么三种情况：

第一，压根没看到此次安全更新。谁没事会盯着微软官网，恐怕大多数人连微软的补丁日都不是特别关注。至于影子经纪人对外披露的黑客工具，那更是不知道躲在哪个网页里。

第二，看到了此次安全更新，但对于漏洞的危害一无所知。可以看到的是，除了打上一个“严重”的等级标签，微软官方对于该漏洞并没有过多的细节描述。

事实上，在每年新增的数万个漏洞里面，被标记为“严重”的漏洞多如牛毛，如果没有点特殊技能，根本处理不过来，多一个少一个压根不会激起半点水花。而安全团队向来是人少事多，一个漏洞就这么被放过去了。

第三，什么都清楚，但由于各种原因不方便处理。对于该漏洞，微软官方给出的解决办法就是安装补丁。但补丁安装是有风险的，可能会出现蓝屏、卡顿、不兼容等各种各样的问题。

出于对风险的顾虑，以及对于漏洞的“侥幸”，很多组织干脆就听之任之了。

综合以上三点原因，表面上看，微软都已经把肉（补丁）送嘴边上了，还有人要么没看到，要么装作没看到，或者嫌弃不好吃，所以才有了后面发生的事情。

> 基于漏洞情报的新型漏洞管理模式，
> 能够在企业安全运营过程起到收集器、
> 过滤器和富化器的作用，
> 帮助企业摆脱漏洞处理的泥潭，
> 更加高效地进行漏洞处置和管理。

如果将微软发布的安全更新及影子经纪人公开的“永恒之蓝”工具两条信息放在一起，那么这就是一条在当时已经相当优质的漏洞情报。

但在漏洞情报已经相对成熟的今天，总觉得还缺点什么东西。

首先是漏洞信息的收集工作。对于微软来说，搞定自己产品的漏洞那就算齐活了，但是没谁只用微软的产品吧，还有甲骨文的数据库，谷歌的浏览器，或者谁谁谁的 ERP、OA 等，一个不小心，就把哪个漏洞给漏掉了。

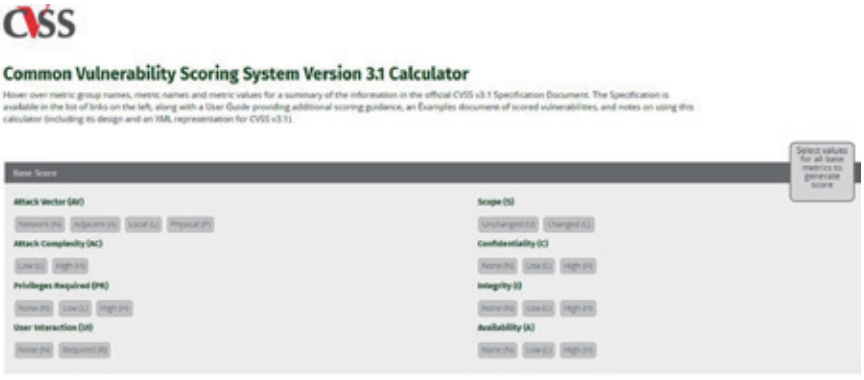
所以企业最好能有一个渠道能尽可能全的把和自己相关的漏洞信息收集起来集中管理，从而降低因没看到某个重要漏洞所造成的安全风险。

其次是漏洞的过滤工作。并不是所有漏洞都像“永恒之蓝”一样危害如此之大，甚至绝大多数漏洞并不会对网络安全造成实际危害。比如，有的漏洞听起来很唬人，甚至被微软这样的厂商标记为 Wormable（可被蠕虫利用），但触发或实现利用的难度非常大，需要在一些特别凑巧的情况下才能够形成现实的威胁。

来看一组统计数据：在 2022 年奇安信 CERT 漏洞库新增的 24,039 条漏洞信息中，监测到有公开 Exploit/PoC 漏洞数量为 721 个、有在野利用漏洞数量为 238 个、0day 漏洞数量为 41 个、APT 相关漏洞数量为 33 个，共标记关键漏洞 960 个，仅占新增漏洞总量的 3.99%。而如果只计算给组织造成实际危害的漏洞（即发现被攻击者成功利用），那么这个比例连 1% 都不到。

因此组织机构需要把一些真正能够造成威胁的漏洞给过滤出来重点关注，避免安全团队陷入到过多“无效”漏洞的海洋中无法自拔，反而对那些真正有威胁的漏洞视而不见。

最后是漏洞信息的富化工作。对于安全团队来说，一个“严重”的标签显然是远远不够的。影响漏洞实际危害的因素有很多，比如，这个漏洞



的影响范围有多大，有没有被发现已经成功利用了，有没有补丁，除了安装补丁还有没有什么别的应对方法等。

获取这些信息，除了参考官方发布的安全通告，就只能靠研究员对漏洞开展深入细致的研究了。只有综合尽可能全的信息，才好决定是应该优先修补还是可以暂时搁置，修的话是安装补丁还是用其他的缓解方法。

“漏洞信息的收集器、过滤器及富化器就是漏洞情报的三大使命。”汪列军说，漏洞情报的魅力就在于告诉用户哪里有漏洞，有什么样的漏洞，漏洞的实际危害如何，以及漏洞到底该怎么处置。

二、漏洞评分？评的是“人情世故”

在经过一系列复杂处理后，用户最终拿到的漏洞情报包含多个字段和标签，包括最基本的漏洞名称、漏洞编号、影响范围、危害程度、风险评分等，这些会为用户判断漏洞的具体风险带来实际参考。

下图是奇安信 CERT 输出的 Apache Log4j2 任意代码执行漏洞的情报信息。可以看到，除了下方的行业通用表格，上面还有奇安信 CERT 打上的密密麻麻的各种标签。

在所有这些标签或者字段当中，最直观也最有趣的当属漏洞评分了。目前最为流行的 CVSS（即通用漏洞评分系统，Common Vulnerability Scoring System），分数范围是从 0~10 不等，0 代表最不严重，10 代表最严重。

国际应急响应联盟组织（FIRST）论坛还贴心的给出了得分计算器。

上述的 Log4j2 漏洞在 v3.1 版本的 CVSS 评分标准下，直接被拉满到了 10 分，被认为是“永恒之蓝”后最危险的漏洞之一，应该排在漏洞修复的最优先位置。

毫无疑问，CVSS 为大部分漏洞的危害程度提供了一个非常直观的量化标准，对于漏洞情报和漏洞处置的优先级排序有着非常大的指导意义。

但是，如果一个“偷懒的”安全团队，完全按照 CVSS 分数的高低，来确定漏洞处置的优先级，那恐怕要掉进另一个坑里了。

“就实际的表现来说，当前漏洞的 CVSS 评分高低并不能客观反映

漏洞的实际风险。”汪列军说，无论 CVSS 有着再严格的评分标准或者计算公式，它归根结底只是一个主观的判断，不同的研究员或者研究机构，对同一漏洞给出不同的评分非常常见。

前段时间汪列军刚好在社交媒体上说过类似的事情。

事情大致是这样的，微软在发布安全更新时，将一枚漏洞评为 9.8 分，引得诸多机构跟风；但奇安信 CERT 深入研究后，在给客户推送的漏洞情报中将评分修改为了 8.8 分，引发了几家客户的询问。

“原因很简单，微软认为漏洞触发不需要用户交互，但我们认为漏洞的触发需要用户点击攻击者特制的一个文档，从而提升了难度，所以得分就稍微低一点。”汪列军解释到。

用他的话来说，升级到 v3.1 版本的 CVSS 评分系统，几乎将所有漏洞的评分都又提高了一大截。按照这个标准，半数以上的漏洞都成为了高危漏洞（即评分大于等于 7.0），如果一个组织的漏洞修补原则是高危必修，那么这和不评分没有区别，反正都是修不完。

评分拉不开差距，漏洞之间的危害程度，就很难在分数上体现出来。同样接近 10 分的漏洞，其实际危害可能有着天差地别。

而且，同样都是洞，破在不同的地方，所导致的实际风险也可谓是天差地别。

CVSS 基础得分主要反映的是漏洞本身的严重程度，并不代表现实的风险大小。

早在 2018 年，施耐德公司的安全负责人就曾公开表示，同样类型的漏洞（如拒绝服务漏洞，触发后可导致相关服务宕机），如果是在 IT 系统中，会被认为风险没那么高；而如果出现在工控系统中，则其风险可能是致命的。

这很好理解。同样一条牛仔裤，同样形状和大小的洞，如果破在膝盖处，那是年轻人追逐的时尚“破洞裤”；如果破在口袋，那你放进去的手机和钱包就得小心了；如果破在裤裆，不打上补丁我想你是不会穿着它逛街的。

除此之外，时间窗口对于漏洞情报的影响也非常大。

汪列军说，以下几个时间节点会渐次影响漏洞的实际危害：

第一，新的关键漏洞公开，潜台词就是赶紧看看影响不影响自己正在使用的产品；

第二，发现关键漏洞的技术细节，意思就是漏洞在技术上到底怎么出现的已经搞清楚了，估计很快就有人知道（甚至已经知道）这漏洞到底怎么用了；

第三，发现关键漏洞的 Exploit 或 PoC 公开，也就是说漏洞已经被证实可以在实际环境中利用，甚至已经出现了漏洞利用的代码，能修就赶紧修吧；

第四，发现关键漏洞的在野利用案例，已经发现有人成功利用了该漏洞，抓紧修吧，不修早晚打到你头上来；

第五，发现关键漏洞的新修补和缓解方案，照这些方法一步步来就行，总有一款适合你。

“这就是我们打标签的意义。”汪列军对笔者强调，我们打的标签多种多样，方便不同的客户按照标签去检索。仅仅是在野利用这一项，奇安信 CERT 已经标记了超过 4000 个漏洞。

有的标签还挺有意思。

“比如，关键信息基础设施的运营单位会关注是否有 APT 组织利用，我们会打上 APT 组织相关，并且标明是哪些组织利用了这个漏洞；

更多的组织会关注这个漏洞会不会像‘永恒之蓝’那样引起大范围传播，我们会标记是否被某些自动化脚本集成（如僵尸网络），从而在互联网上批量攻击……”

三、效率为王

有一点需要明确。如此多的漏洞标签并不是天上掉下来的，需要对漏洞进行持续的动态跟踪。

针对某个关键漏洞，奇安信 CERT 会连续发布一系列的安全通告，便于用户动态掌握漏洞所造成的的实

> 漏洞的分析过滤不仅要基于准确的技术判定，还要足够快速，这样才能抢在攻击者之前避免漏洞被利用，从而导致损失，需要及时地将与组织自身相关的漏洞风险通知到用户。

际风险。

就像下图这样。

动态跟踪需要一定的时间，如果再加上用户修补漏洞的过程，这段时间并不算太短。

但攻击者未必能给到这么多时间。大多数时候防御方是在跟攻击者抢时间，哪方先知道漏洞的存在及相应的细节，就决定了谁在对抗中获胜。

国外知名漏洞情报公司 VulnCheck 在官网首页公布了一组数字，2018 年，从漏洞变为网络攻击武器需要接近一年的时间，到 2023 年，时间直接缩短到了只有 8 天。

不论这组数据是真是假，但是漏洞从首次曝光到发现野外利用的时间窗口，已经在极速缩短。

“漏洞的分析过滤不仅要基于准确的技术判定，还要足够快速，这样才能抢在攻击者之前避免漏洞被利用，从而导致损失，需要及时地将与组织自身相关的漏洞风险通知到用户。”

汪列军说。

这里不妨将漏洞情报的生命周期，简单的抽象成为四个阶段（各阶段并非相互独立，有所交叉）。

第一是漏洞收集阶段。通常情况下，漏洞的收集渠道主要包括厂商自行发布（如微软、甲骨文等）、NVD/CNVD/CNNVD 等国内外主流漏洞库、独立漏洞研究机构、独立挖掘等，需要对这些渠道进行全面监测，才能掌握第一手漏洞信息。

“除了这些常规方法，我们还有独门秘籍。”汪列军故作神秘，“说穿了其实也没什么，就是我们有别人没有的补天平台。”

作为国内最大的漏洞收集平台之一，补天平台成立十年间，已经累计报送了超过一百万个漏洞。所谓的漏洞奖励计划无非就是平台发奖金，把白帽子手中挖到的漏洞“买”过来。而奇安信近水楼台，能第一时间拿到尽可能全的漏洞信息。

顺便提一嘴，从漏洞曝光到美国国家漏洞库 NVD 发布漏洞信息，有时候能长达七八天，按照 VulnCheck 发布的数据，漏洞都已经被做成网络武器了。

第二是漏洞的验证阶段。在拿到漏洞后，漏洞研究机构需要第一时间对漏洞验证进行复现，确认漏洞的实际危害。

汪列军表示：“漏洞的验证与复现最消耗时间的其实是涉及软 / 硬件环境搭建，好比是在沙盘上搭建一个一比一还原的战场，方便研究员在沙盘上进行兵棋推演。”

至于为什么需要搭建一个虚拟环境，那要直接在现实环境中测试漏洞还不乱套了。

奇安信有个明显的优势，那就是产品线足够丰富，服务的客户足够多，

复杂的产品线需要复杂的 IT 环境，这样漏洞研究员在面临任何漏洞环境搭建时，都显得游刃有余。

“所以我们很多时候能提前小半天发布一手漏洞情报。”汪列军说，别小看这小半天时间，有时候还真能挽狂澜于既倒。

第三是动态跟踪阶段，也就是客户喜闻乐见的“打标签”环节。

与其说是对漏洞的动态跟踪，不如说是对威胁的动态跟踪，掌握的是攻击者的信息。漏洞一经曝光就在那里，又不会变，变得只是攻击者到底可能会利用漏洞做什么。

不妨看看奇安信 CERT 给漏洞打上的标签，在野利用的意思就是已经发现有攻击者成功利用该漏洞发起了网络攻击，APT 相关的意思是被 APT 组织利用了，所有这些反映的都是攻击者的动态。

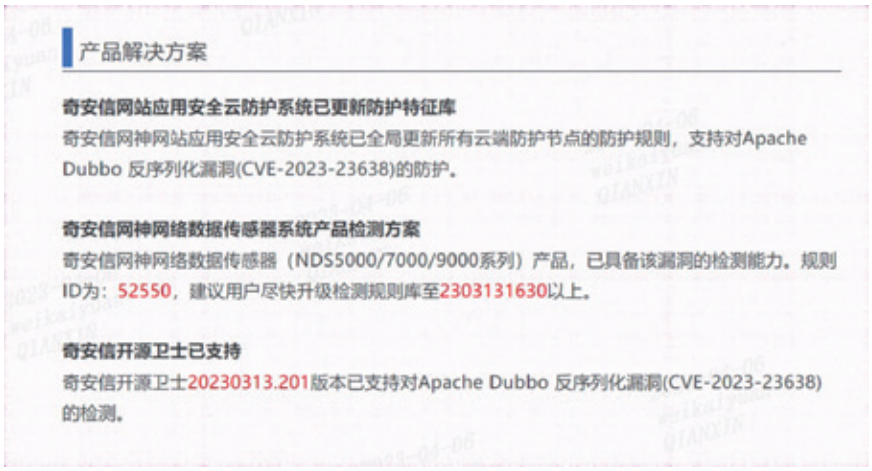
毫无疑问，这是威胁情报最擅长的事情。威胁情报与漏洞情报的联动，能够让奇安信第一时间捕获利用相关漏洞的海量攻击行为。在 2021 年年底 Apache Log4j2 漏洞曝光之后，奇安信威胁情报第一时间就检测到了数千起针对该漏洞的攻击行为，并第一时间打上了在野利用的标签。

第四是漏洞修补阶段。

对于组织来说，修漏洞不是点击“一键修补”就万事大吉了。上文笔者提到，考虑到补丁安全的风险，对业务连续性要求很高的组织，很多时候是不方便打补丁的，更何况有时候漏洞在曝光的时候厂商还没有发布补丁。

所以除了补丁安装，有其他临时的缓解措施是最好的，这一点软件厂商在发布安全更新时也会同时给出。

什么？官方发布临时缓解措施，不会操作怎么办？没关系，照着奇安信发布的操作步骤一步步来就行。



要是缓解措施也无效，奇安信还有最后的“撒手锏”，把安全设备的检测规则更新一下，这样就能及时阻断相关漏洞的利用行为了。

为了便于用户处置，在线数据获取的 API 接口及离线数据包，用户可以根据自己的需要集成到自有漏洞处理流程。

“去年我们又发了 280 多篇漏洞安全通告，差不多每个工作日一篇，另外还有接近 100 篇包含漏洞所有技术细节的深度漏洞分析报告。”汪列军粗略估算了下，在他眼里，处理 30 万漏洞也就那么回事，每天都标记一些，每天都向客户输出一些，不知不觉就有了一定的积累。

那 60 万呢？100 万呢？还需要坚持多少年？

“多长时间我不好说，但肯定不会太久。”汪列军坚定地说，“漏洞会越来越多，但我们的动作会越来越快！”安

全球 AI 独角兽，有了一双“安全眼”

作者 | 安全攻防 PBU　云娟

“人工智能是创造美好未来的高科技手段，但是要始终以安全保障为前提，才能促进智慧生活发展。”作为 AI“四小龙”之一的某人工智能公司网络安全部门负责人表示，当我们在享受人工智能技术带来的便捷与高效的同时，更有必要防止该技术被滥用的可能性，尤其是要重视黑客对人工智能公司发起的攻击，因为以“勒索病毒、信息泄露”为代表的网络攻击会给企业资产、企业声誉造成重大影响。同时，在《网安法》《数安法》《个保法》等法规之下，注重网络安全合规开展应该放在所有企业的首位。

作为全球 AI 独角兽，该公司拥有的人工智能算法、模型等核心技术都是公司的重要资产和竞争力所在。由于人工智能技术应用广泛，所涉及的数据量和信息也较为庞大，因此成为了黑客的重要攻击目标。同时，因为人工智能类公司通常需要使用不同的系统、应用程序及设备来处理数据和训练模型，复杂程度非常高，再加上供应链环节中供应商代码不可避免存在质量等问题，最终导致人工智能各业务及系统产生诸多漏洞和弱点，容易被攻击者利用。以上这些，都给该 AI 公司的网络安全提出了严峻挑战。

在这种情况下，该 AI 龙头企业选择与奇安信天眼达成合作。通过部署天眼系统，该 AI 公司数据中心及下属 9 个职场办公区实现内网全流量威胁监测、分析、处置为一体的可视化安全运营，进而提升了集团数据中心及各地职场的整体防护协同能力，确保及时发现各业务中隐藏的安全风险及威胁，准确快速地定位并阻断勒索病毒投递、挖矿木马外联、内外网渗透等各类恶意攻击。最终，保证人工智能业务相关的人脸、声音等关键信息数据传输安全、存储安全，保障业务稳定运行。

> 通过部署天眼系统，
> 该 AI 公司实现内网全流量威胁监测、分析、处置为一体的可视化安全运营，
> 提升了集团整体防护协同能力。

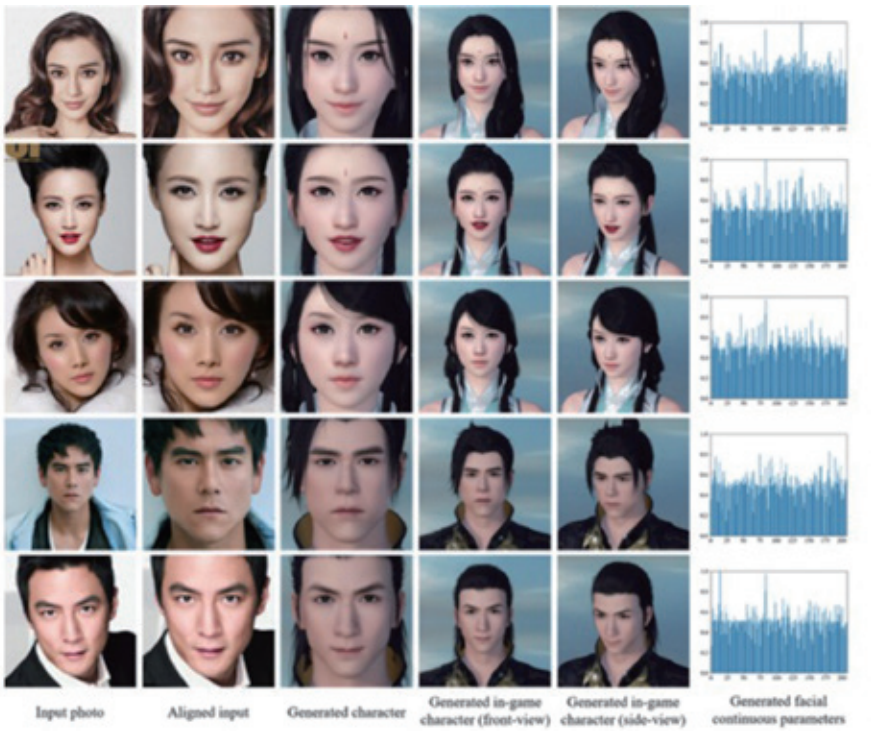
人工智能公司的数据，成黑客觊觎的目标

人工智能高度依赖海量数据的采集和训练分析，而海量数据意味着更复杂、更敏感的数据也会更多，大量敏感数据的汇集使得黑客在一次攻击中可能获得更多收益，从而导致 AI 公司面临更大的威胁。该 AI 公司网络安全部门相关负责人介绍，很多专业从事人工智能的公司业务覆盖都比较广，涉及教育、医疗、遥感、广电、商业、工业、金融等多个行业的数据，因此，黑客攻击人工智能类的公司，主要是看中了“数据”，想通过窃取数据来获得盈利，主要体现在以下几个方面。

首先，黑客通过非法手段进入 AI 公司内网，窃取大量数据和知识产权信息，这些数据和信息将被用于出售或者勒索钱财。例如，美国纽约的一家 AI 面部识别公司曾遭到黑客公司攻击，致使其全部客户名单及 30 亿张照片库被黑客窃取；某知名 AI 智能工业芯片制造商曾被勒索软件袭击，黑客要求支付 1300 万美元赎金。

其次，攻击者还可能对窃取到的数据信息进行“移花接木”，利用人工智能技术对人脸、声音等个人隐私敏感数据进行深度伪造，后利用其重新实施诈骗。例如，攻击者利用人工智能技术将窃取到的照片“活化”、合成动态视频，之后或直接骗过社交平台、支付宝账户的人脸核验机制，进行非法获利。

另外，除了获利，黑客还可能篡改内部数据，故意制造混乱，从而导致 AI 公司内的人工智能系统做出完全错误的决策。在这种干扰下，原本精确的人工智能，瞬间沦为“人工智障”。



> 从黑客的攻击手法来看，
> 过去的“小毛贼”已经鸟枪换炮，
> 升级为专业化的网络犯罪组织，
> 许多网络攻击来无影、去无踪，
> 更看不见，无法做溯源和调查分析。

例如，黑客攻击智能驾驶系统，导致明明是右转标志，自动驾驶系统却识别为左转，极其容易酿成交通事故。

安全响应滞后，AI 公司三大安全问题尤为突出

“很多数据安全事件都是出事之后，受害单位才知道，甚至还有很多公司受了攻击却并不知道。”该 AI 公司网络安全部门相关负责人表示，全世界的力量都在打击网络犯罪，但是从黑客的攻击手法来看，过去的“小毛贼”已经鸟枪换炮，升级为专业化的网络犯罪组织，许多网络攻击来无影、去无踪，更看不见，无法做溯源和调查分析，很多厂商都只能打掉牙齿往肚子里咽。

造成这种现象的原因就是，企业割裂式的安全建设，资产和未知风险看不全，碎片化的威胁检测，孤岛式的应急响应。在没有部署天眼之前，该 AI 公司面临的安全挑战主要也是体现在这几个方面：

首先，针对内网间传输的未知流量，以及来自外部的攻击流量不可视，这两部分流量就像“暗箱”，根本无法看清、看全威胁。

该 AI 公司网络安全部门相关负责人介绍到，内网间传输的未知流量，主要分为两个部分，一是职场和职场间互访的流量，这部分流量面临的威胁主要体现在，当攻击者拿到某个职场某台机器的权限时，他可以将这台主机视为跳板，进而对更多职场发起攻击；二是职场访问部署在公有云、数据中心、服务器等相关业务的流量，这部分流量面临的主要威胁多为攻击者窃取敏感口令信息后登录核心业务系统，窃取重要数据。

而来自外部的攻击，则主要是攻击者会利用各种手段尝试攻击企业内网，包括漏洞攻击、钓鱼邮件攻击、侦测踩点攻击等。

其次，部署在各职场办公区的不同防护设备之间数据相对割裂，碎片化的检测根本无法贯通攻击链数据，无法对攻击进行快速阻断和高效分析。

“和我们公司一样，大部分企业都有同样的困惑，那就是企业虽然有防火墙、有杀毒软件，但是就和瞎子一样，眼睛成了摆设。”该 AI 公司网络安全部门相关负责人表示，这也是导致目前各类网络攻击屡禁不绝的原因之一。

最后，不同职场分布在全国不同区域，威胁检测与分析的工作基本都是“各管各的”，异常线索无迹可寻，协同联动防护的能力差，无法满足对所有职场的全局态势进行掌控和分析。

由此看来，如何构建一套能够“看见风险、抵御威胁、制止攻击”的协

同联动体系，是该人工智能公司在数字化时代需要迫切解决的问题。

天眼助力 AI 巨头看见、看清、看全网络威胁

基于该 AI 公司的网络安全现状，以及各地职场单位的整体情况，该 AI 公司与奇安信天眼达成合作。天眼系统按照集群部署的方式，完成该 AI 公司数据中心及 9 个职场的整体威胁态势感知平台的搭建，将告警统一收集至数据中心进行集中展示和按需分析。

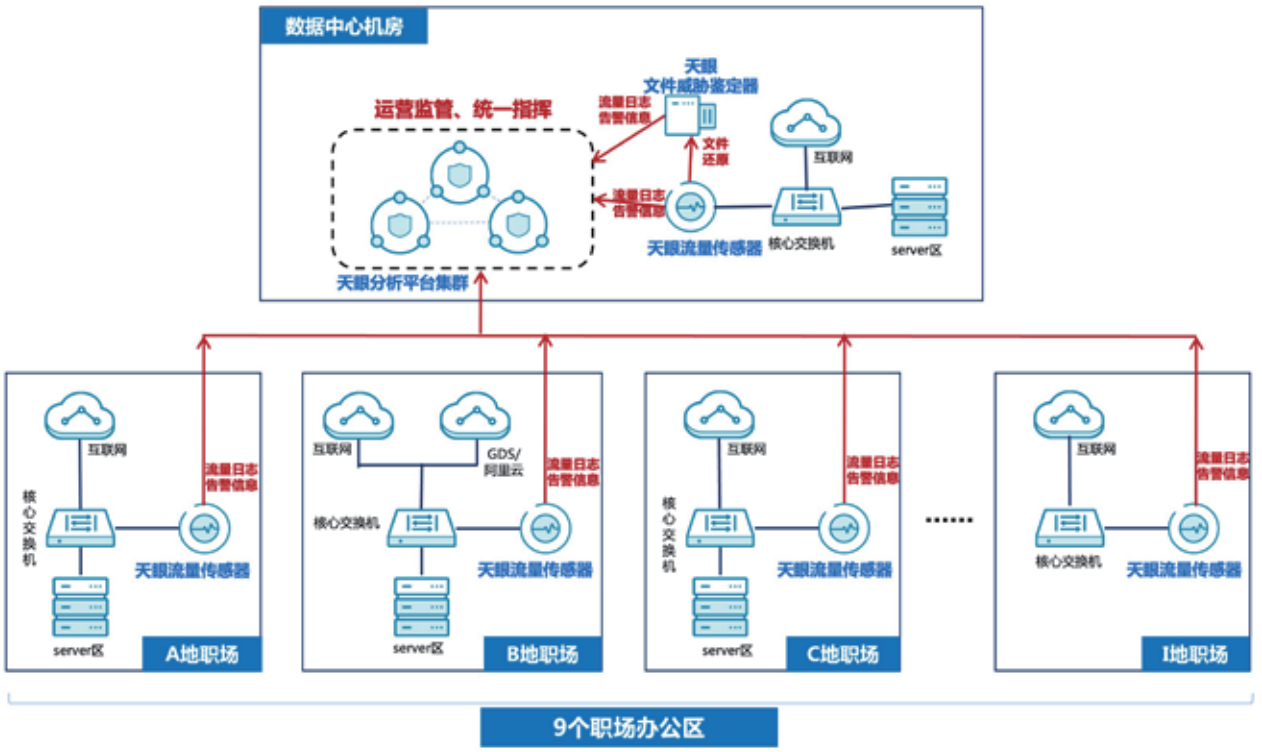
在各职场侧，通过在 9 大职场核心交换机侧部署天眼探针设备，把各地职场办公内网，以及内网访问互联网、阿里云等的流量日志和告警信息，全部上传到数据中心机房的天眼分析平台集群。分析平台通过对收集到的信息进行综合分析后，可精准发现数据中心及各大职场所存在的安全威胁。

在全局方面，以集群式部署在数据中心的天眼分析平台，既可以监测到各区域天眼探针上传的异常流量日志和告警信息，以及天眼文件沙箱传递的异常文件告警信息，还可以保证对其他 9 个职场的威胁情况进行全面掌控，并可根据需要呈现出数据中心、多地职场的各自安全态势，方便日常安全运营，确保威胁监测的全面性与稳定性。

“我们部署了天眼之后，公司内网互访，以及内外网互联的全场景、收发双向流量全部都能监测到，再也没有了盲区。”该 AI 公司网络安全部相关负责人表示，天眼基本做到了 100% 覆盖业务网络安全，将网络安全和 AI 业务运营紧密地融合到了一起，同时能快速定位各类已知、未知安全风险，联动其他环节，阻击潜伏在内外网的挖矿、勒索、APT 组织等，真正做到了看清、看全威胁。

该 AI 公司网络安全部相关负责人说：“现在打通 9 个职场之间的数据孤岛后，我们做到了对威胁进行智能关联，比如，根据某些职场的某些事件关联攻击者画像，模拟出攻击者的攻击路径，能看到攻击者是谁、使用了什么手段、进行到什么环节、做了哪些事情等，攻击过程知根知底。”

看清、看全威胁，对攻击过程知根知底之后，还需要通过可视化展现出来，这样对于日常运维的安全人员来说，才能真正做到让威胁“可见”。有了天眼之后，该 AI 公司网络安全部门相关负责人表示，公司安全运维人员既可以从整体综合安全态势来分析威胁，还能单独调取某地职场的态势来进行分析，同时还能按照外部威胁



> 奇安信天眼作为网络威胁检测与分析领域的领头羊，为各行业客户提供专业的集威胁检测、响应、溯源为一体化的网络安全解决方案，同时也积累了大量实践经验。

态势、外部访问状态、横向访问等多个角度来按需进行分析，提高对高级威胁的处置效率。

后记：

当前，人工智能已广泛应用于人们日常生产、生活的方方面面，对其安全可信的需要已经提升到前所未有的高度。人们不仅要关注人工智能应用暴露出的各种安全风险和挑战，更要关注人工智能公司内部的网络安全，毕竟 AI 技术源起于人工智能公司，一旦人工智能公司遭受网络攻击，那么人工智能算力基础设施将会受到破坏，人工智能发展蓝图的底色安全、可信、可靠将被摧毁。

奇安信天眼作为网络威胁检测与分析领域的领头羊，为各行业客户提供专业的集威胁检测、响应、溯源为一体化的网络安全解决方案，同时也积累了大量实践经验。未来，天眼将持续协助人工智能行业客户做好网络安全威胁风险监测防范工作，保障算法运行时的机密性与完整性，人工智能数据的安全传输与存储，携手 AI 公司打造可信、可用、好用的人工智能算力底座，共同营造安全、健康、合规发展的人工智能产业生态。安

图：天眼威胁感知系统

网络安全学院学生创新资助计划

在中央网信办指导下，中国网络空间安全协会、中国互联网发展基金会、10家一流网络安全学院、奇安信等多家网络安全企业发起“网络安全学院学生创新资助计划”，面向一流网络安全学院的全日制在读本科、硕士、博士学生提供项目资助。

让科技创新“最后一公里”更加顺畅
让科研创新与市场需求“零距离”

十所高校深挖人才“蓄水池”：山东大学、北京邮电大学、北京航空航天大学、西安电子科技大学、东南大学、四川大学、华中科技大学、武汉大学、上海交通大学、中国科学技术大学。
五大科研方向探索新突破：风险检测、识别分析、数据安全、新技术、情报响应。

网络安全学院
学生创新资助计划
项目办公室

520“嗑 CP”，不妨看看这些

作者 | 魏开元

在古今中外的文学作品中，爱情与 CP 总是成为读者关注的焦点。

比如，中国古代神话爱情故事中的梁山伯与祝英台、金庸笔下的神仙眷侣杨过与小龙女、莎士比亚戏剧中罗密欧与朱丽叶的凄惨爱情……

除了人与人，网络安全产品也是具有明显 CP 属性的。

或许绝大多数用户已经习惯了，某些产品或者功能模块总是成对出现，相互之间功能互补、配合默契，可以明显发挥出“1+1>2”的效果，甚至有不少用户对于任意一方单独出现而感觉到非常奇怪。

恰在今年，RSAC 将“Strong Together”作为大会主题，不仅强调了人与人、组织与组织需要在一起，安全产品也应当更加紧密的结合，可谓是进一步鼓励了安全产品之间搞 CP。

细细数来，安全产品 CP 还真不少。

一、防火墙 &VPN：陪伴是最长情的告白

自上世纪 70 年代以来，互联网技术取得了飞速的发展。出于安全性和保密性的考虑，人们迫切需要对一些不受控的访问行为进行限制。

于是防火墙的雏形产生了，在实验室里，它能够实现简单的网络过滤功能。

在经过一系列的技术演变之后，1994 年，CheckPoint 创始人吉尔·舍伍德正式带来了世界上第一款可商用的防火墙，奠定了几十年来防火墙在网络安全产品中不可动摇的老大地位。

与防火墙相比，VPN 的出现要略微晚一些，但同样与互联网的发展有着紧密的关系。

20 世纪 90 年代，全球化趋势使得大量企业出现了各地甚至跨国分支机构网络互联的需求，但运营商提供的专线租赁的模式不仅价格昂贵，在安全性方面也没有加密传输的保证。

VPN 的出现解决了这样一个难题，它通过在各个机构之间建立一个虚拟专用的加密通信隧道，在大幅提升组网效率的同时，相对保证了访问的安全性。

随着防火墙的广泛应用，VPN 的需求也越来越多：当身处外网的用户想要访问内部网络时，就会被防火墙阻断，此时不得不通过 VPN 来达到访问内网的目的。

正因如此，防火墙和 VPN 的命运被紧紧捆绑在了一起，一个负责堵，一个负责疏，共同守护组织的网络边界，形影不离。

2004 年 9 月，IDC 首次提出了统一威胁管理 UTM 概念，将防火墙、VPN、邮件过滤等边界安全能力整合到了一起，防火墙与 VPN 从此结束

了“爱情长跑”，彻底走在了一起，几十年如一日。

时至今日，尽管 VPN 的地位受到了诸如 SD-WAN 等新技术的挑战，但防火墙和 VPN 依旧相互陪伴在一起。各类性能强大的防火墙，依然将 VPN 视作标配。

例如，奇安信新一代智慧防火墙，基于第四代高性能 SecOS 操作系统（鲲鹏平台），完美整合了传统防火墙、VPN、防病毒、防漏洞利用等，可在大流量、复杂场景、多安全功能开启的情况下保持高性能，为客户提供灵活组网、精细化访问控制、高效威胁检测等功能，连续三年在有着“中国含金量最高的防火墙测试”之称的中国移动防火墙集采测试中脱颖而出，并多次入围中国移动、中国联通等大型客户的防火墙集采项目。

二、EPP&EDR：你若不离不弃，我必生死相依

EPP 是终端安全保护平台，EDR 是终端检测与响应平台，二者本是不同时代的产物，却因同一块阵地而走在了一起。

最初的终端安全没有什么花里胡哨的概念，有的只是一个单纯的防病毒软件。那时，杀毒就是终端安全的全部。

很快，随着组织终端、应用数量的不断攀升，单纯的反病毒已经不能满足终端安全需要了，于是安全厂商把终端相关的反病毒、设备管理、应用管理、漏洞和补丁管理等功能进行了整合，为客户提供更强大的终端安全保护能力。

EPP 应运而生，直到现在 EPP 也一直是保护组织终端的主力产品。

但 EPP 并非没有缺陷。黑客的攻击手段是会不断变化的，免杀、白利用、逃逸、无文件攻击等技术层出不穷，这让依靠静态规则匹配的 EPP 防病毒模块难以招架。

2013 年 7 月，Gartner 分析师首次提出了 EDR 的概念，强调基于终端大数据同时结合外部情报进行分析检测，完成对可疑攻击行为的发现、响应和溯源。

由于在应对未知攻击方面的独到优势，EDR 一经问世就受到热捧，再加上各大安全厂商、分析机构及媒体的炒作，一度出现了 EDR 要取代 EPP 的论调。

但明眼人都知道，威胁发现仅仅是终端安全的一部分，EDR 看上去光鲜亮丽，但背后的设备管理、漏洞管理等脏活累活，还得靠 EPP 去打理。

所幸的是，EDR 并没有迷失在众星捧月的高光里，也没有嫌弃看起来已经不再时尚的 EPP，而是不离不弃，为终端安全添砖加瓦。

久而久之，EPP 和 EDR 就被整合在了一起，过上了“持证上岗”的生活。

奇安信天擎基于“体系化防御、数字化运营”的思想，全面整合了 EDR、EPP 等技术，能够为客户提供横跨 Windows、Linux、MacOS、移动平台的一体化终端安全能力，全面覆盖病毒防护、高级威胁检测与响应、调查溯源、资产管理及补丁管理等，帮助客户构建全覆盖、全统一、全协同的一体化终端安全体系；同时依托多元的基础数据、丰富的运营知识、统一的运营平台，保障终端安全效果。

IDC 报告显示，奇安信天擎已连续五年位居国内终端安全软件市场首位。

三、NDR& 蜜罐：两情若是久长时，又岂在朝朝暮暮

作为 EDR 的同门师兄弟，网络检测与响应技术 NDR 正式面世的时间要稍晚一些。

同样是在 2013 年，Gartner 分析师针对网络侧也提出了一个新概念——网络流量分析 NTA，检测网络

> EPP 是终端安全保护平台，
> EDR 是终端检测与响应平台，
> 前者负责防护与管控，后者负责检测与响应，
> 共同守护终端安全。

流量中隐藏的异常行为和威胁，弥补过去入侵检测系统 IDS 的不足。

但 NTA 依然存在很多问题：误报数量依然居高不下，并且没能解决发现威胁后的响应处置问题，因此不得不依靠人工处置。

所以，安全厂商们开展了对 NTA 类型产品的改进，比如，引入机器学习、威胁情报，提升检测准确率；引入设备联动能力，在发现威胁后，调用其他设备对威胁进行阻断。

与 EDR 类比，大家开始习惯将此类方案称为 NDR。

直到 2020 年，Gartner 正式将原 NTA 方案重新命名为 NDR 方案，并于 6 月 11 日发布了首份 NDR 市场指南，NDR 也正式面世。

由于NDR的概念早已不胫而走，因此它早已成为网络流量检测的核心。

与 NDR 相比，蜜罐出现的时间要早得多。

1988 年，Clifford Stoll 博士在论文中描述了蜜罐的构想：设置陷阱引诱攻击者，记录攻击者的痕迹，延误入侵的脚步，同时保护真实目标。

然而在接下来的十多年里，蜜罐技术也只是作为一种理想存在。

直到 2000 年前后，蜜罐产品才从开发者的手中诞生，能够模拟成虚拟的操作系统和网络服务，并对黑客的攻击行为做出回应。

蜜罐的商用，使得 IDS 有了最佳伴侣: 前者主动出击，后者则严阵以待。并且，蜜罐不像 IDS，对所有可疑行为都很敏感，它的属性就决定了只有攻击者才会触发蜜罐。

所以，蜜罐基本上没什么误报。

听起来一切都很美好，但从蜜罐出生那一刻起，供应商们就一直在解决两个问题：

一是仿真性问题，“一眼假”的陷阱无法欺骗攻击者；

二是安全性问题，决不能让攻击者利用蜜罐作为跳板，渗透到真实的业务系统中。

出于这两方面的考虑，蜜罐的应用一直受到很大的限制，无论是最早的 IDS、还是后来的 NTA、NDR，尽管互相爱慕，却始终没能走在一起。

不过好事多磨，技术的发展也不是一朝一夕的事情。

好在奇安信天眼解决了这个问题。

在流量检测与响应方面，奇安信天眼基于多个威胁检测引擎，可以精准发现网络流量中的攻击行为；利用本地大数据平台对全量数据进行查询，结合威胁情报和攻击链分析对事件进行分析、研判和回溯。

另一方面，天眼可与奇安信攻击诱捕系统（蜜罐）进行完美联动。借助天眼的全流量分析能力，蜜罐能够快速构建符合真实业务逻辑的“陷阱”，将攻击流量主动牵引至蜜罐中隔离起来，使攻击者相信已初步取得部分目标的控制权，并且不能横向渗透进正

> 奇安信天眼联动了 NDR 的网络流量检测与响应、蜜罐的欺骗检测，
> 不仅实现了对攻击流量的严阵以待，
> 还实现了对攻击者的主动出击。

常系统中。最终，蜜罐产生的威胁告警会发送至天眼分析平台中进行统一的告警管理。

四、SIEM&SOAR：一见倾心

SIEM 诞生于 2005 年，同样是由 Gartner 分析师提出的概念，中文全称是安全信息和事件管理。

从字面意义上来理解，SIEM 的初衷或许很简单，就是把系统中发生的和网络安全相关的信息和事件收集起来进行统一管理。

不过随着网络空间的攻防对抗越来越激烈，几乎所有的网络安全产品都会收到一份灵魂拷问：你能检测到网络攻击吗?

所以这十多年来，攻防对抗逐渐发展成为 SIEM 的核心，Gartner 更是在 2016 年直言攻防检测将成为推动 SIEM 发展的核心驱动力。

于是安全厂商不断将各类检测能力整合进 SIEM，如关联分析、威胁情报、用户实体行为分析……

但问题出现了。由于 SIEM 强大的数据整合能力，海量日志、数据汇集于此，从而产生了过量的告警，远远超出了人工可以处置的范围。

用户迫切需要一种方法能够对海量告警进行初筛，就像医院的分诊台。普通的安全事件可以按照既定的“剧本”，自动化完成响应处置流程，而分析师只需要关注那些系统无法判定的高级威胁。

SOAR 的出现使这个问题迎刃而解。

2017 年，Gartner 提出了现如今广为接受的 SOAR 的概念，即安全编排、自动化与响应，其核心目标是为安全运营人员提供机器辅助和自动化，以提升他们的工作效率，而这种自动化是通过对流程的编排（即剧本）来实现的。

很快，在 Gartner 的一手“撮合”下，SOAR 和 SIEM 可以说是“一见钟情”。

Gartner 在 SIEM 的最新定义中特别强调了 SIEM 应当基于 SOAR 的响应集成，并且将 SOAR 视作为 SIEM 产品的一个重要功能。

目前来看，SIEM 和 SOAR 结合方式主要包括两种：其一是 SIEM 产品中内置一个附加的 SOAR 模块；其二是将 SIEM 和 SOAR 打包成一个套件进行联动部署。

比如，奇安信态势感知与安全运营平台 NGSOC（核心平台是 SIEM）以大数据平台为基础，通过收集多元、异构的海量日志，利用关联分析、机器学习、威胁情报等技术，能够为安全运营人员提供威胁发现、调查分析及响应处置的安全运营工具。

在 SOAR 方面，奇安信 SOAR 可以与奇安信 NGSOC 或者第三方 SIEM 平台进行很好的联动，将分散的安全工具与功能转化为可编程的应用和动作，然后借助编排和自动化技术，将团队、工具和流程高度协同起来，从而将来自 SIEM 平台的告警处置效率提升十倍以上。

番外篇：除了 CP 还有什么?

有专情的，自然也少不了“滥情”的，也就是俗称的“海王”。

首先被想到的应该就是威胁情报。

威胁情报技术发展至今，已经成为提升所有安全设备检测效率和准确率的核心手段之一。因此，威胁情报不仅仅是见一个爱一个，也是人见人爱的“俊男靓女”。在前文所述的 CP 中，或多或少都有威胁情报出现的影子。

奇安信威胁情报检测引擎依托奇安信威胁情报中心多年的技术积累、海量的文件信誉库和 IP 情报库，支持细粒度的规则设置，具备微秒级威胁情报查询能力，检测准确率可达 99.9%。

为解决奇安信大客户的威胁情报应用痛点，奇安信对外发布了一站式本地化威胁情报运营系统（简称 TIOS）。TIOS 整合了多个威胁情报组件，融合了奇安信全面独有的数据视野，结合威胁图谱分析的关联视图展示，实现威胁情报数据接入、生产、处理、运营与消费的闭环建设。

另外一个则是奇安信的“关门弟子”——流量解密编排器。

尽管它相对陌生，但受欢迎程度却丝毫不亚于威胁情报，无论是防火墙、WAF、IDS，还是 NTA、NDR，都向其抛出了橄榄枝。

为了应对加密流量的威胁，所有处理网络流量相关的安全设备都需具备解密能力。在同时串联部署多个安全设备的情况下，由于解密能力参差不齐，导致流量处理效率极其低下。

奇安信发布的国内首款流量解密编排器则重点解决了这个问题：在流量解密方面，通过搭载硬件加速卡，并配合自研的异步调用技术，理论上可以将 SSL 解密性能提升 10 倍以上；在流量编排方面，奇安信首创了智能化服务链编排技术，能够将明文报文分发至服务链上的各个安全设备，从而实现“一台设备成功解密，多台设备成果共享”，大幅提升了加解密效率。安

《全球高级持续性威胁（APT）态势报告》：我国仍是主要受害国

作者｜中国信息安全测评中心

摘要

·俄乌冲突作为2022年最为突出的地缘政治事件，激化APT组织形成持续至今的攻击潮。

·APT呈现军事化、武器化、组织化、隐匿化等特征，APT组织与政府部门进一步深度绑定，“雇佣兵”性质更为凸显，获得国家级情报信息资源和攻击武器支持，0day漏洞、供应链入侵等高水平渗透手段利用呈现常态化的特征。

·中国是APT主要受害国，面临国家背景的超高能力威胁行为体的现实威胁，攻击者手法和目标持续更新升级，目标扩散，攻击深入，尤以美国发动的对华APT攻击最甚。

·传统APT组织“阳谋”尽显，不断升级战技术，实施新的对抗和反溯源技术；新兴APT组织“阴谋”涌现，攻击危害不容忽视。

·APT攻防向体系化方向发展，网络空间“对等打击”“相互制约”更趋激烈，围绕APT的政治对抗日益凸显。

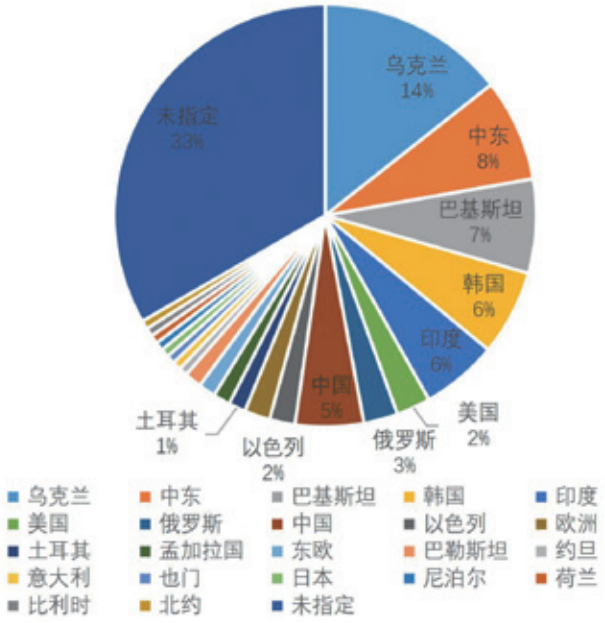
第一部分 2022年全球APT态势图景

一、攻击数量增长

APT是网络空间与地缘政治互动的产物，APT组织活跃趋势与全球热点问题密切相关。受地缘政治热点事件的影响，2022年全球APT活动进入新一轮活跃期。一是攻击总量增多。不仅纯APT攻击类型增多，APT与其他攻击形式融合的混合攻击也在不断增长，直接助推形成新攻击潮。二是攻击烈度增强。2022年，造成重大影响的APT攻击事件频发，既有攻破钢铁厂造成停产，也有攻击卫星通信系统造成“掉线”，还有直接参战影响战争进程的攻击事件。三是攻击形式多样。2022年，APT组织攻击形式有一个明显的变化，就是从原有的“破坏”到“攻心”地拓展，部分APT组织正在增多意图干扰认知、影响民众心理的攻击活动。

二、目标区域拓展

地缘政治目标一直是APT组织任务的核心，热点地缘政治事件持续驱动APT组织行动，2022年尤甚。一是冲突事件致攻击激增。俄乌冲突



2022 年度 APT 主要攻击目标国家分布

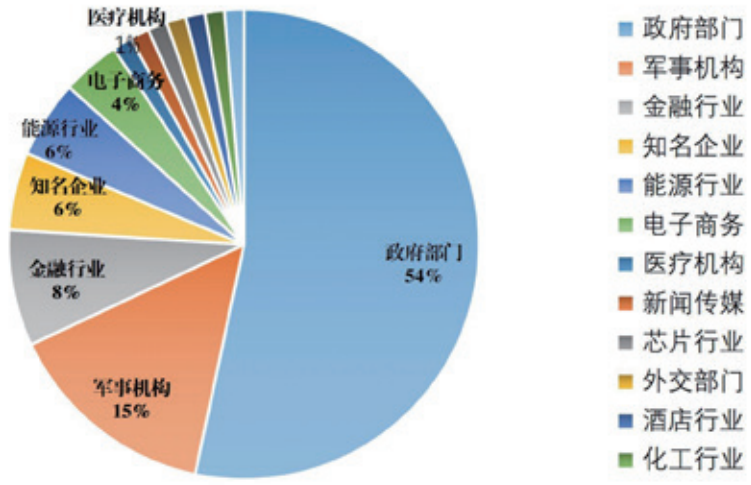
作为近年最典型的地缘事件，成为推动 2022 年 APT 攻击走高的导火索，交战双方及相关国家遭遇的 APT 攻击数量最为突出。二是热点区域形成攻击“高地”。中东地区、南亚地区、东北亚等热点区域现实冲突不断，网络空间的 APT 攻击相应配合，相关国家所涉 APT 攻击“高位运行”，如上图所示。三是非洲国家攻击事件开始增多。随着非洲国家在全球地缘政治中的重要作用不断凸显，针对非洲国家的攻击也开始出现在全球 APT 攻击版图中。

三、目标机构泛化

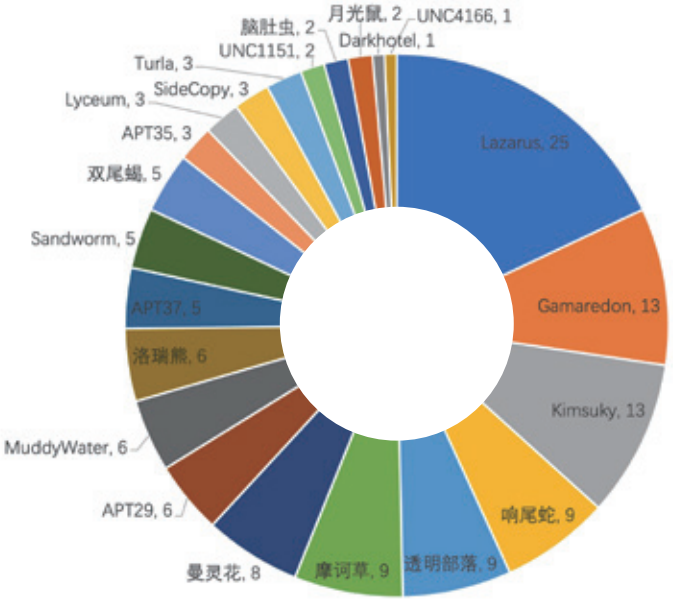
近年来，APT 攻击目标更趋泛化。在所有的攻击目标中，一是政府和外交机构、国防承包商等“高政治”领域依然是重点目标，情报数据窃密仍旧猖獗；二是金融部门、博彩机构等经济组织成为攻击热门，索取经济利益的攻击活动更为频繁。三是针对技术部门的攻击增多，特别是在当前科技博弈日趋严峻的形势下，芯片行业等科技部门成为攻击新领域。

四、攻击组织多源

在 APT 攻击战场中，传统组织与新兴组织更迭交替。一方面，“拉撒路”、Kimsuky（又名 Mystery Baby、Baby Coin、Smoke Screen、Black Banshe）、“摩诃草”（Patchwork）、“透明部落”（Transparent Tribe）等传统老牌 APT 组织在 2022 年持续活跃，不断精进攻击手法，仍然占据 APT 整体图景的“基本盘”。另一方面，新兴组织不断涌现。“穆伦鲨”（MurenShark）、Polonium、Metador 均为 2022 年新披露的组织，在攻击活动中展现了较强的对抗能力，成为新的威胁行为体，加剧形势复杂。



2022 年度 APT 主要攻击目标机构分布



2022 年度主要 APT 攻击组织分布

第二部分 我国是 APT 主要受害国

我国面临的 APT 网络攻击威胁是全方位的，风险源既有国家背景的超高能力威胁行为体，如美国国家安全局网攻组织 APT-C-40、“方程式”（Equation）、CIA（Vault7）等，又有周边地区组织的滋扰，如“海莲花”（Ocean Lotus）“毒云藤”等。攻击目标涵盖了我国政府、军事、教育、科研院所、海事机构、航空航天等关键信息基础设施和重要信息系统，活跃时间长达几年甚至十几年。

一、攻击数量持续增加

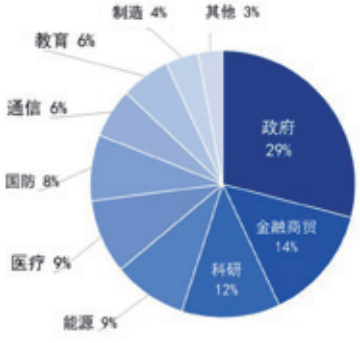
2022 年针对中国的 APT 攻击呈现持续高发状态，国内安全公司公开发布的受害目标涉及中国的活跃组织分析报告 22 份。值得注意的是，实际发生在我国境内的 APT 攻击事件远高于公开披露的数据，仅对我国攻击的 APT 组织就达数十之多。相关报告所涉及的 APT 组织除了美国安局“方程式”，其余大部分来自我国周边地区。近年还出现了在攻击活动中专门针对中国目标的 APT 组织，如“摩诃草”、TA575、“虎木槿”（OperationShadowTiger）、“蔓灵花”等。

二、攻击手段日益复杂化

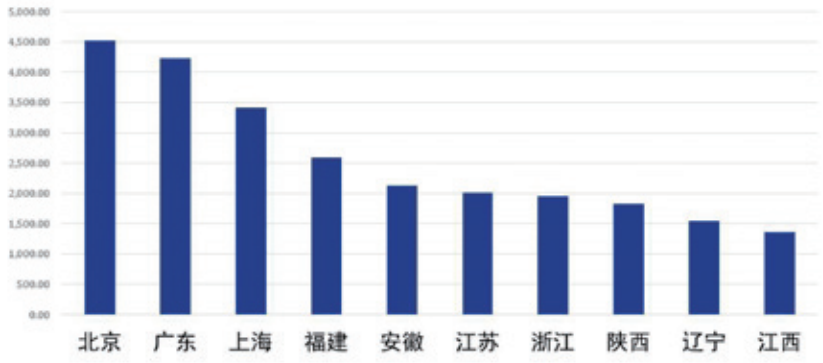
APT 组织“专门定制”对我国的网络攻击工具。各 APT 组织在长期针对我国网络攻击中逐渐“摸清”我国重要行业的薄弱点和风险点，定制相关 TTPs。如“海莲花”在 2022 年 5 月针对我国产化系统的定向攻击中专门基于我国产化系统的特点对其攻击载荷进行了定制，特别研发了针对 MIPS 架构的木马程序。“摩诃草”在对我国攻击活动中所使用的后门程序，在连接控制服务器之间会专门检测目标机器的时区设置是否为中国。AgainstTheWest（ATW）黑客组织早期主要针对 SonarQube 代码质量管理平台进行攻击，在 2022 年初其攻击目标又扩大到我国广泛使用的 Gitblit、Gogs 等代码存储管理平台。

三、攻击目标呈现弥散特点

涉华 APT 攻击活动中，目标涉及政府、金融、科研、能源、医疗、电力、电信等关键信息基础设施和重要信息系统，旨在进行敏感信息窃取、物理破坏，以影响系统正常运行。地域分布上，经济发达省份和政治中心仍是主要目标地区，其中，北京市是 APT 组织的重点目标地区，其次是广东、上海、福建、安徽等地区。



2022 年高级威胁事件涉及境内行业分布



2022 年中国境内疑似受控 IP 地域分布

四、美国对我网攻愈演愈烈

美国将中国视为最主要的“战略竞争对手”，在现实社会和网络空间中同步打压。自拜登政府上台以来，持续实施“前置防御”“前沿狩猎”等进攻性网络行动，瞄准目标国家，开展大量的数据窃取、后门部署、网络攻击等活动，其中 APT 是重要手段。2022 年曝光的美国对我 APT 攻击事件中，显示美对我开展大规模、长时间、系统性的网络攻击，潜伏时间长、“后门”利用多、跳板部署广，对我国国防安全、关键基础设施安全、金融安全及公民个人信息造成严重危害。

第三部分 趋势研判

随着近年来传统 APT 组织的持续活跃和大量新兴 APT 组织的不断涌现，APT 将作为网络空间重要力量持续塑造“网缘”政治，并呈现出以下趋势。

一、APT 攻击与国家战略方向同频共振

APT 组织俨然已成为实现国家战略目标的“先遣队”，是配合网络空间国家战略布局的重要力量，可以配合现实军事战争、上升为政治“筹码”，并且仍然以关基为重点目标。

二、APT 组织攻防较量更趋复杂

在长期地缘冲突中，APT 组织之间、APT 组织与安全企业之间的攻防较量更为复杂和激烈，主要表现为：敌对 APT 组织在攻击手段上对抗化发展、新老组织在攻击目标和手段上交织融合、网络安全企业逐渐成为攻防主体。

三、供应链成为 APT 攻击新目标

通过入侵软件供应商并污染上游软件代码的供应链攻击技术，具有隐蔽性高、影响面广、边界突破能力强、检测防御困难等优势，与 APT 组织的诉求高度吻合，因此越来越多的 APT 组织在谋求建立供应链攻击能力。

四、针对新技术新应用的 APT 攻击持续增加

APT 组织持续探索在新技术领域的攻击能力，区块链、人工智能、云计算等新技术逐渐成为 APT 攻击的目标。区块链方面，APT 攻击呈现生态化特征；云基础设施也正在成为 APT 新战场；空间技术领域是 APT 攻击的新目标。

五、APT 攻击“勒索化”趋势越来越明显

无论是 APT 攻击“勒索化”，还是勒索攻击“APT 化”，均是近年来的典型趋势。APT 组织使用复杂的手段攻击企业甚至关键基础设施，并植入勒索软件，在针对政府、医疗、交通、管道运输等关键基础设施的攻击中尤为凸显。

六、APT 事件调查呈现强烈的政治化趋势

作为网络空间中能够反映国家意志的攻击形式，APT 攻击政治化倾向目益明显。对 APT 的归因溯源、威慑响应及规范限制等均成为大国博弈的热点内容，“模糊归因”“点名羞辱”“精准制裁”等成为美西方网络霸权的新手段。安

大事记

奇安信“中国芯”防火墙中标中国移动集采大单

5月15日，中国移动公布2023年至2024年硬件防火墙产品集中采购（新建）中标候选人名单，全部采用中国芯的奇安信旗下网神智慧防火墙，在标包二（需求数量最多的防火墙品类）高价中标。这也是奇安信连续三年作为唯一专业网络安全供应商，入围中国移动硬件防火墙集采项目。

据悉，中国移动硬件防火墙集采测试项目共包含功能测试、性能测试、可靠性测试等共计40多个测试项目，是中国含金量最高的防火墙测试。该测试对防火墙硬件通信性能要求极高，因此向来都是数据通信巨头厂商的优势领域，奇安信是迄今为止唯一入围中国移动硬件防火墙集采项目的专业网络安全供应商。

奇安信出席首届武汉网络安全创新论坛

5月16日—17日，首届武汉网络安全创新论坛隆重举办。奇安信集团受邀出席，并深入参与学术报告、研讨会、成果发布等环节，聚焦网络安全技术创新和人才培养，展示网络安全领域的前沿创新成果。

论坛期间，举行了网络安全学院学生创新资助计划座谈会，奇安信安全专家、企业导师和资助学生面对面进行交流，展示第一期创新资助计划项目成果、分享师生参与感受。

同时，网络安全学院学生创新资助计划二期宣布启动，奇安信集团作为资助计划一期的参与支持单位，积极参与了资助计划二期项目。

奇安信集团2022年ESG报告正式发布

日前，奇安信集团正式发布《2022年度环境、社会及治理（ESG）报告》，这是公司自2020年上市以来发布的第二份ESG/CSR报告。该报告围绕公司治理、网络安全产品服务、价值链建设、人才成长、社会公益、绿色发展六大板块，全方位呈现奇安信在2022年的可持续发展成就与贡献。

“2022年，奇安信重点关注了22项环境、社会与治理议题，公司的发展离不开对行业布局的远见、产品价值的追求、安全运营的坚持、员工福利的保障等可持续发展理念与行动。”奇安信集团董事长齐向东表示，“道阻且长，行将致远，未来奇安信将持续加强ESG管理和信息披露，用数字包容与技术向善，为社会可持续发展注入动力。”

《数据跨境合规白皮书》发布

5月11日，普华永道发布《数据跨境合规白皮书》。该白皮书由普华永道与奇安信联合撰写，通过系统梳理全球及中国数据合规安全趋势与法规，分析典型数据跨境场景的风险和挑战，深度解读结合不同行业典型场景下的数据跨境合规应对之道，以期为企业数据合规和安全保障提供有力借鉴。

奇安信与华为联合发布天眼鲲鹏一体化解决方案

近日，鲲鹏昇腾开发者峰会 2023 在广东东莞隆重召开。奇安信受邀出席此次大会，并与鲲鹏联合发布“奇安信天眼鲲鹏一体化”解决方案，共同打造安全可靠、性能卓越的网络威胁监测与分析平台，助力各行业客户提升网络安全防御水平，更加安全地推动数字化转型。

此前，作为国内网络威胁检测与响应领域的龙头产品，奇安信天眼已基于国产海光、麒麟操作系统完成了国产化产品的上市发布。如今，奇安信天眼与华为深化合作，共同推进基于鲲鹏的网络威胁监测与分析自主创新生态高质量发展。

“强研发”优势凸显 奇安信中标某电网公司网络安全全域感知项目

近日，国内某头部电网公司公布了网络安全全域感知与自动化管理平台项目一期工程中标结果，奇安信凭借安全咨询规划、大型研建项目开发等综合实力，成功中标该项目。该项目标志着奇安信“强研发”战略不断显效，在大型央企集团复杂项目中体现了显著的竞争优势。

本次中标某电网公司网络安全全域感知项目，不仅体现了奇安信对于大型安全项目顶层规划和体系设计的战略咨询实力，同时也验证了公司流程性组织变革所带来的显著效果，尤其是大型研建项目中的综合优势，为大型安全系统建设探索出一条用企业架构方法论解决复杂安全问题的成功路径。

首届“盘古石杯”全国电子数据取证大赛线上晋级赛圆满落幕

5 月 6 日，首届“盘古石杯”全国电子数据取证大赛线上晋级赛圆满落幕！本次比赛共有 979 支队伍、超 3000 名选手同台竞技，共同角逐总决赛入场名额。比赛之外，本场大赛直播现场还邀请了来自产学研各领域的权威专家，分享电子取证行业洞察，围绕行业前沿技术趋势、创新案例分享与取证人才培育体系等话题进行深入交流。

本届“盘古石杯”全国电子数据取证大赛由公安部第三研究所、司法鉴定科学研究院、中华全国总工会 – 中国职工电化教育中心指导，奇安信集团联合南京信息工程大学、南京森林警察学院、江苏警官学院共同主办，由中国人民公安大学战略支持，旨在提升我国电子数据取证人才技术能力，培养更多行业电子数据取证人才，推动电子数据取证行业技术的发展。

奇安信参与“金融网络安全实验室”筹备启动仪式

4 月 27 日，由中国人民银行科技司指导，中国金融电子化集团有限公司主办的中国国际金融展 – 中国金融业网络安全大会在首钢会展中心召开。奇安信集团受邀出席，并作为筹建单位参与了“金融网络安全实验室”筹备启动仪式。

为进一步推进网络安全应急响应合作联动工作，提高金融机构对情报共享、网络安全新技术的应用，北京国家金融科技认证中心有限公司在中国人民银行科技司和中国金融电子化集团公司指导下建设“金融网络安全实验室”。奇安信集团积极参与实验室筹建，与金融机构、网络安全产业机构

联合，开展前沿网络安全理论、政策、标准和技术研究，探索金融业网络安全管理新模式，推动金融业网络安全技术和应用创新发展。

奇安信亮相数字中国建设峰会 为数字化建设建言献策

4 月 27 日—28 日，以“加快数字中国建设，推进中国式现代化”为主题的第六届数字中国建设峰会在福州举办。奇安信集团通过主题演讲、展览演示、产品发布等多种形式深度参与本次峰会。

数据安全：守护中国式现代化发展行稳致远

数据安全是数字政务的“生命线”，要做到“三要三不要”。在数字政务分论坛上，奇安信集团董事长齐向东表示，随着数字政务建设越来越深入，数据规模越来越庞大，一旦出事故很难人为控制大小，所以“零事故”目标是顺应时代要求的，必须迎难而上，做到“三要三不要”，为数字政务注入“安全力”。

数据安全治理是筑牢数字安全屏障的重要组成部分。在数字安全分论坛上，奇安信集团总裁吴云坤提出，数字化时代的业务系统、信息化环境、合规要求都发生了改变，对于数据安全防护提出了更高的要求和更大的挑战。

人工智能：“三个零”举措 守护人工智能时代安全底线

在“数字福建：数字政法”分论坛上，齐向东提出“三个零”举措，即以“零信任”为核心，解决“内鬼”安全隐患；以“零事故”为目标，建立纵深防御安全体系；以“零容忍”为原则，精准打击新型网络犯罪。他强调，我们必须坚持最严格的标准，为数字政法构筑坚实的网络安全底座。

在本次数字中国成果发布会上，奇安信还发布了“特权访问安全解决方案”。该方案可实现对各类基础设施资源账号和访问的全生命周期管理，帮助组织提升账号安全的主动防御能力，降低因特权账号、特权访问行为管理不善所带来的数据安全风险，是解决“内鬼”安全问题的重要工具。

体系化运营：数字安全建设的新目标、新思路、新方法

在“数字技术创新与安全”分论坛上，奇安信集团总裁吴云坤表示，数字中国需要构筑一个可信、可控的数字安全屏障，以“零事故”为目标，数字安全建设必须有新思路和新方法。

他建议从两方面发力强化网络、数据安全保障体系建设：一是建立“集中力量办大事”的组织机制，形成体系化作战；二是形成“打赢团体赛”的融合创新生态，由政企单位推动，国家队和综合性大型安全企业牵头，聚集细分领域的专精技术厂商，共同进行原创性技术和融合性技术创新攻关。

作为安全体系化运营的重要产品之一，奇安信天眼威胁监测与分析系统荣获 2023 数字中国“十佳解决方案”。据工作人员介绍，天眼以攻防渗透和数据分析为核心竞争力，

聚焦威胁检测和响应，为安全服务和分析人员提供一套在威胁监测、分析溯源、响应处置、威胁预警上得心应手的威胁检测平台和一体化解决方案。

共议金融数据新未来 奇安信与中央财经大学达成战略合作

4月26日，在第六届数字中国建设峰会“新数据 新动能”古厝私享汇上，奇安信集团与中央财经大学签署了战略合作协议。奇安信与中央财经大学将聚焦金融科技的人才培养及科研孵化，在金融科技新技术研究、投融资人才培养、高校网络安全建设等方面展开深入合作。

合作双方将充分发挥各自领域优势，围绕金融科技及网络安全领域展开合作，探索金融科技安全领域人才培养新模式。在智慧校园建设方面，双方也将共同探索金融类高校智慧校园网的网络安全体系建设。

DataCon 竞赛平台首次对外亮相

近日，由奇安信集团提供技术支持的第二届广东大学生网络安全攻防大赛成功落下帷幕。本次大赛首次使用了奇安信 DataCon 网络攻防竞赛平台（简称 DataCon 竞赛平台），该平台创新性地将 CTF 与电子竞技实现融合，将大赛竞技性与娱乐性提升到了新的高度。

这是 DataCon 竞赛平台首次使用于支持外部赛事。该平台在提供更接近真实攻防环境的同时，还全面实现全方面云化部署，告别繁重的现场布线与服务器搬运。现场选手仅需联网即可接入竞赛系统，大大降低了竞赛运维所需人力及物力成本，并保证竞赛高质量、高效率交付；DataCon 竞赛平台还实现了容器化的回合靶标管理，避免环境瘫痪后影响其他战队公平参赛；平台设置防止权限维持，也使得参赛选手可以专注于攻防赛事。

奇安信出席 RSAC 2023 C-SOC 解决方案于全球首次正式亮相

美国时间 4 月 24 日—27 日，全球网络安全行业的盛会——RSAC 大会在旧金山隆重举行。奇安信集团作为国内网络安全领军企业受邀出席，携全新打造的 QAX C-SOC 解决方案亮相 RSAC，展示网络安全的中国实力。

QAX C-SOC，即定制安全运营中心（SoC），以奇安信 SIEM 平台为核心，可根据客户业务与 IT 系统特点，灵活集成 EDR、NDR、VM、TIP 和 SOAR 等多个网络安全态势分析平台，可以实现统一的管理、统一的监控和统一的态势感知，为客户提供持续的威胁检测，数据获取、分析、实时协同和快速响应，从而达到更早感知潜在安全威胁，最大限度保障用户的网络安全。

这一集成多项平台的解决方案，与今年大会主题“Stronger Together”（携手更强大）不谋而合，既体现出集成化运营的需求，也展示出产业协同的趋势，将成为展会中备受关注的产品之一。

第八届安全创客汇初赛收官 2023 网安创业新锐 50 强名单出炉

近日，2023 第八届安全创客汇初赛专家评审会顺利召开，对参赛企业进行多维度、细致评审。最终，由安全创客汇、数世咨询、数说安全、安全 419、嘶吼、安全喵喵站、新安盟、通信世界全媒体、安全牛等多家机构联合，正式发布《2023 网安创业新锐 50 强》，公布本届安全创客汇初赛 50 强晋级名单。

荣誉墙

奇安信获得中国通信学会科学技术一等奖

近日，中国通信学会公布了 2022 年度“中国通信学会科学技术奖”。由奇安信科技集团牵头申报，董事长齐向东为第一完成人的“面向复杂网络攻击的检测与处置系统及产业化应用”项目，获得科学技术奖科技进步一等奖。

奇安信两项目获 2022 信息技术应用创新解决方案

近日，由工业和信息化部网络安全产业发展中心（工业和信息化部信息中心）、信息中心技术创新应用协作组牵头的 2022 年（第四届）信息技术应用创新解决方案名单正式公布。“奇安信态势感知与安全运营解决方案”“奇安信网神跨网文件安全交换管理解决方案”两项目获评网络人气最受欢迎 TOP30。

奇安信安全专家介绍，依托奇安信的技术和创新实力，两个解决方案均实现了信创 CPU、信创操作系统的兼容适配，已在金融、政企机构、医疗、交通等领域广泛应用，并获得好评。此次获选 2022 信息技术应用创新解决方案，也是市场及客户对相关产品服务的实力认可。

奇安信边界安全交互系统首批通过 GA/1788 标准符合性检测

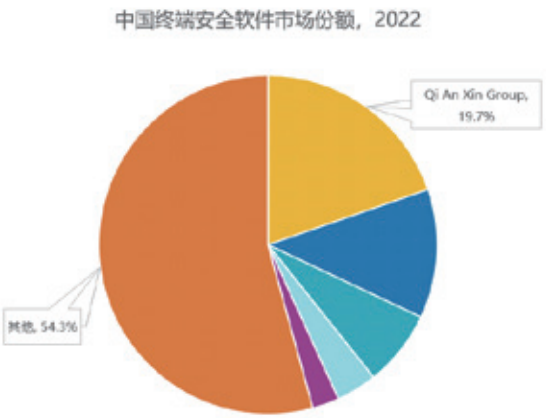
近日，奇安信边界安全交互系统成为首批次通过公安部安全与警用电子产品质量检测中心 GA/T1788 标准符合性检测的产品，其安全等级为增强二级（最高级）。

这标志着奇安信可以提供完全符合 GA/T1788 标准要求的相关产品和解决方案，为公安视频图像信息系统安全建设和运营提供保障。

唯一“三项全能”！奇安信连续多年领跑 IT 安全软件市场

近日，全球领先的 IT 市场研究和咨询公司 IDC 发布《2022 年下半年中国 IT 安全软件市场跟踪报告》（简称《报告》）。《报告》显示，奇安信连续 5 年稳居终端安全软件市场首位，连续 3 年稳居安全分析和情报市场首位，分别实现了市场份额的“五连冠”和“三连冠”。

与此同时，奇安信还首次拿下了数据安全软件市场份额头名，在国内整体 IT 安全软件市场 7 大细分领域中共摘得三项第一。



奇安信在 RSAC 2023 上斩获 CDM InfoSec Awards 2023 两项大奖

4 月 24 日—26 日，RSAC 2023 会议期间，国际领先的电子信息安全媒体 CDM(Cyber Defense Magazine，《网络防御杂志》) 颁发了 Global InfoSec Awards 2023 系列奖项，奇安信集团 SIEM、EDR 获评热门公司奖（Hot Company）。

奇安信集团荣获“2023 年首都劳动奖”

4 月 26 日，在“凝心铸魂跟党走 团结奋斗双提升”暨西城区 2023 年庆“五一”表彰座谈活动上，奇安信集团荣获由北京市总工会、北京市人力资源和社会保障局授予的 2023 年首都劳动奖状。

作为西城区科技企业，奇安信集团坚持以党建工作为引领、以技术创新为驱动，积极践行企业责任及社会责任。不仅圆满完成 2022 北京冬奥会、冬残奥会网络安全保障任务，还组织成立“冬奥央企网络安全救援队”，为政企机构网络安全保障提供及时、高质量的应急响应服务；在董事长齐向东的带领下，奇安信京区办公人员 150 余人注册成为西城家园志愿者，总志愿服务时长超 5400 小时。

社会责任

奇安信基金会秘书长齐子昕获评第六届“西城青年之星 – 志愿公益之星”

五四青年节来临之际，由北京市西城区委组织部、区委宣传部、区直机关工委、团区委联合举办的第六届“西城青年之星”颁奖典礼在天桥艺术中心举办。北京奇安信公益基金会秘书长齐子昕获评“西城青年之星 – 志愿公益之星”。

作为北京奇安信公益基金会秘书长，齐子昕不仅带领公益基金会开展的“心安工程”履行社会责任，还创造性地将网络安全工作与企业社会责任相融合，有效地提升了公益活动的覆盖度和影响力。

齐子昕表示，今年，基金会将继续围绕“心安助医”“心安助学”“心安救灾”“心安助农”四个方面开展公益活动，并发动更多员工参与其中，以实际行动履行社会责任，推动相关工作高质量发展。

奇安信

新一代网络安全领军者

聚焦安全运营，构建智能平台

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

国内领先的威胁情报能力

奇安信威胁情报中心在情报数量及数据覆盖度方面国内第一。

首款分布式关联分析引擎 - Sabre

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

将平战结合进行落地

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

重大安全事件的威胁预警

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

专业的安全运营服务

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

市场占有率NO.1

连续2年中国安全管理平台市场占有率第一——赛迪顾问认证

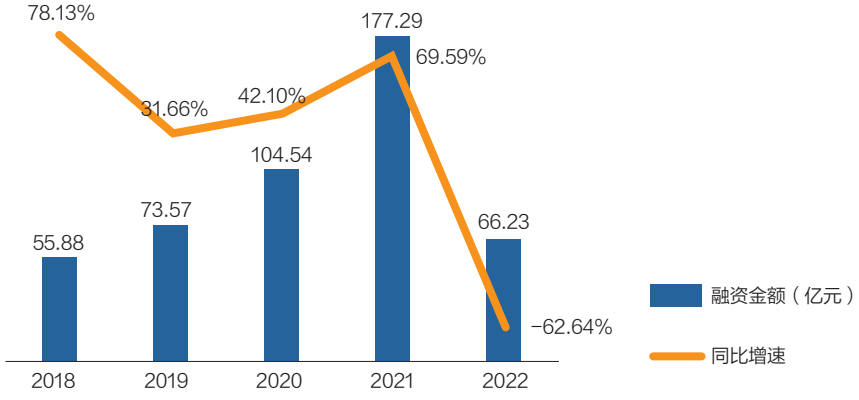
态势感知解决方案市场领导者——IDC认证

态势感知技术创新力和市场执行力双第一——数世咨询认证

产业观察：网安投融资呈现四大集中化特征

作者 | 陈华平 尹文鹏

科技创投领域的繁荣在 2022 年迎来了转折。受到外部宏观经济负面因素影响，2022 年中国和海外网络安全投融资市场波动明显，但是从长期来看，网络安全的国家战略属性赋予了行业在不确定的国际政治环境下发展的高度确定性。顶层制度设计的不断完善从外部推动了行业高质量发展，而安全事件导致的巨额损失则从企业内部驱动行业快速发展。



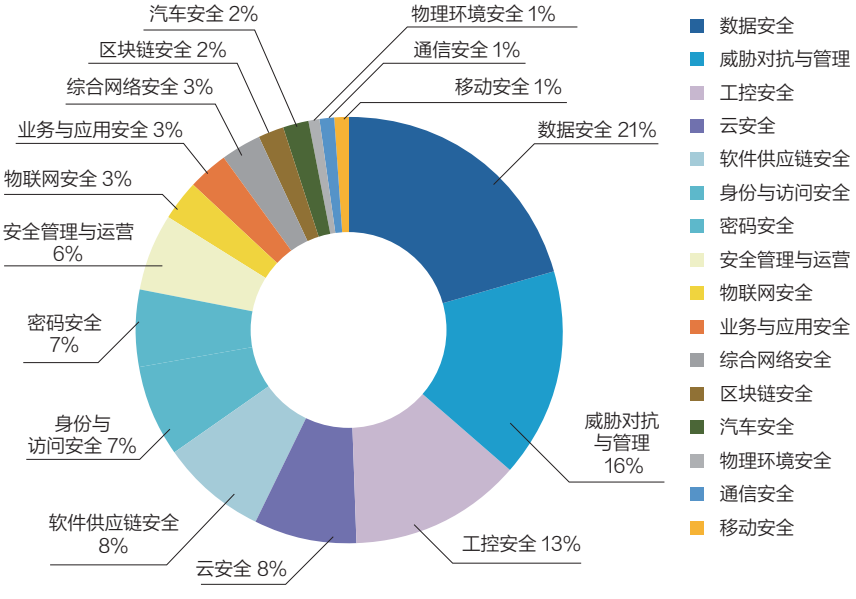
（数据来源：奇安信产业发展研究中心）

一、中国网络安全投融资市场热度下降，国有资本加速布局

受国内新冠疫情冲击和经济增速放缓的影响，中国网络安全投资融资市场在 2022 年出现明显降温。根据不完全统计，2022 年国内网络安全非上市企业披露的融资事件有 109 起，同比下降 26.85%，交易总金额为 66.23 亿元，同比下降 62.64%，共涉及 92 家网络安全企业，其中单笔融资规模大于 1 亿元人民币的融资交易有 26 笔，占总样本的 23.85%。

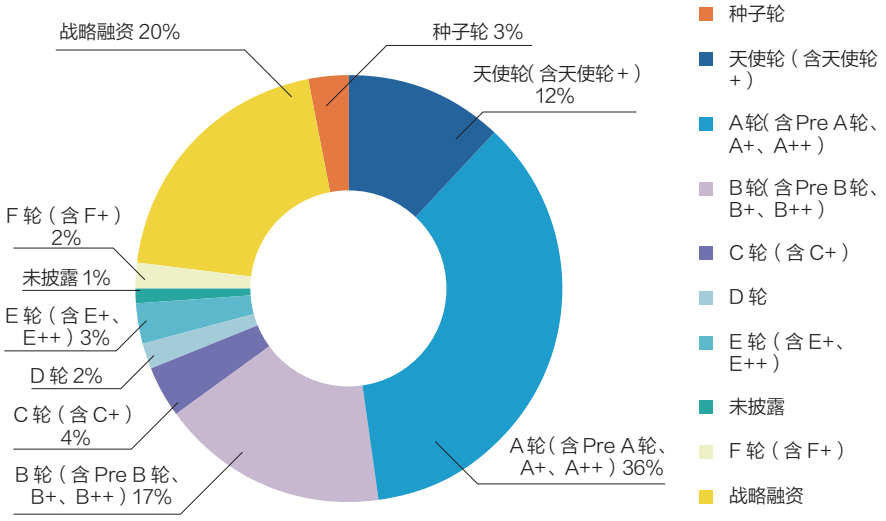
由于碎片化的特征，网络安全细分赛道繁多，从 2022 年的投资热度来看，数据安全（含隐私计算）、威胁对抗与管理、工控安全、云安全、软件供应链安全、身份与访问安全、密码安全、安全管理与运营、物联网安全和业务与应用安全等十大赛道在

2022 年网安非上市企业投融资赛道分布



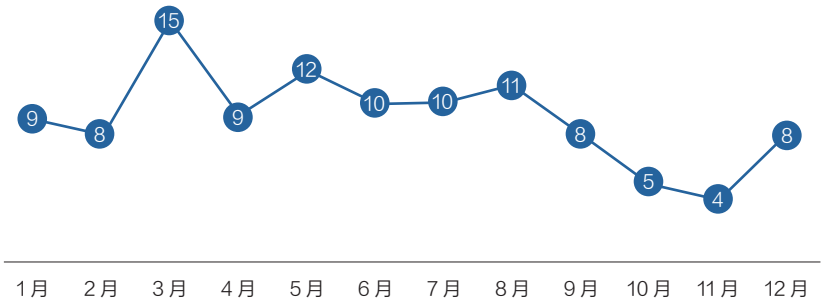
（数据来源：奇安信产业发展研究中心）

2022 年融资阶段分布



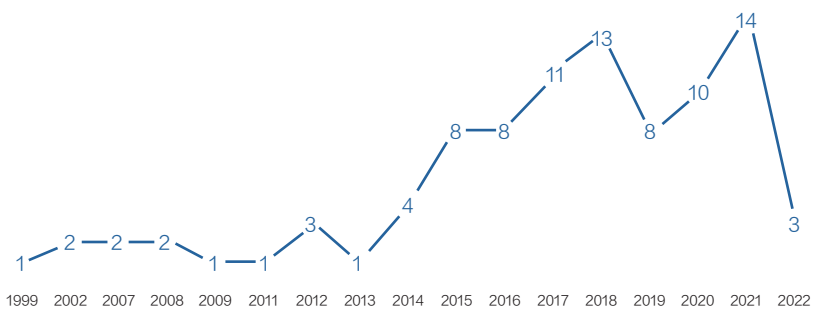
（数据来源：奇安信产业发展研究中心）

融资事件分布



（数据来源：奇安信产业发展研究中心）

2022 年网安非上市公司融资成立时间分布



（数据来源：奇安信产业发展研究中心）

一级市场投融资活跃度较高。

2022 年网络安全投融资呈现四个集中化特征，即投资阶段集中化、投资时间集中化、企业成立时间集中化、企业地域分布集中化。

• 投资阶段集中化：投资机构对网络安全一级市场的早中期项目关注度持续上升，早中期项目占比超过 67%，同比增加约 10 个百分点。

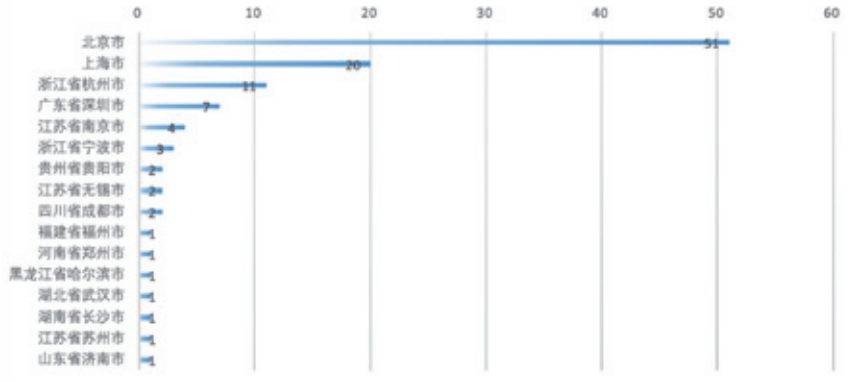
• 投资时间集中化：行业融资事件主要发生在上半年，总计有融资交易 63 起，约占全年的 57.80%，其中，3 月融资事件最多。

• 企业成立时间集中化：2022 年进行融资的网安非上市企业成立年限区间位于 1999—2022，其中 2015 年以后成立的企业（含 2015 年）有 75 家，占总样本容量的 81.52%。此外，92 家网安企业的平均成立年限为 6 年，而成立超过 10 年的企业仅有 11 家，行业不断涌入新兴力量。

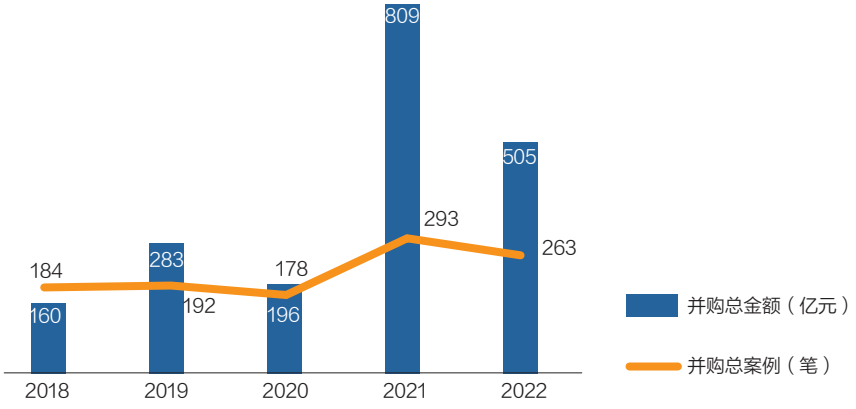
• 企业地域分布集中化：2022 年中国网安一级市场融资事件共有 109 起，其中北京地区有 51 起，占总样本的 46.79%，北京作为网络安全产业龙头，优势依旧明显；深圳、上海、杭州和南京在网络安全行业的区域影响力也在逐步增强。

国有资本加速对网络安全行业的布局是 2022 年行业投融资的重要特点。事实上，在地缘政治不确定因素趋强的背景下，网络安全的国家战略属性不断提高，政策端的不断完善使得行业获得了资本的高度关注。国资背景的投资机构的进入，一方面推动了行业的高速发展，另一方面也吸引了更多市场化投资机构的加入。当前行业投资机构可以根据投资目的粗分为两类，一类是战略投资机构，主要以头部网络安全企业和国资背景的投

2022 年融资事件地区分布



（数据来源：奇安信产业发展研究中心）



（数据来源：Momentum Cyber，奇安信产业发展研究中心整理绘制）

资机构为主，前者的投资目的在于补齐自身发展短板，因而投资多以早中期项目为主，典型企业有奇安信，而后者更多的是配合国家发展战略布局，偏好于中后期成熟的项目。另一类是市场化的投资机构，以追求财务回报为主要目的，偏好于专精特新的网络安全企业，代表机构有奇安投资和苹果资本。

二、风险 & 合规、数据安全、IAM 等八大赛道持续受到关注

在海外，除了新冠疫情、经济增长放缓等负面因素，2022 年发达经济体普遍收缩的货币政策无疑放大了风险投资机构交易的机会成本和压力，而这一压力在全球网络安全风险投资市场表现的非常明显。Momentum 数据显示，2022 年全球网络安全投融资交易总规模为 185 亿美元，与 2021 年 304 亿美元相比下降了 39.14%，交易数量 1037 笔，同比下降 1%。季度侧显示了更加强烈的下降趋势，交易数量从第一季度的 327 笔连续下滑到第四季度的 193 笔，下半年的交易金额不足上半年的 54%。单笔交易规模方面也出现一定程度下降，2022 年有 95 笔交易超过 5000 万美金，平均值和中位数为 2410 万美金和 600 万美金，而 2021 年则有 85 笔单笔交易超过 1 亿美金的交易，平均值和中位数为 3660 万美金和 760 万美元。从赛道来看，2022 年风险 & 合规、数据安全、IAM、网络 & 基础设施安全、安全运营 / 事件响应 / 内部威胁、应用安全、云安全、IOT 安全等八个赛道受海外投资机构注度较高。

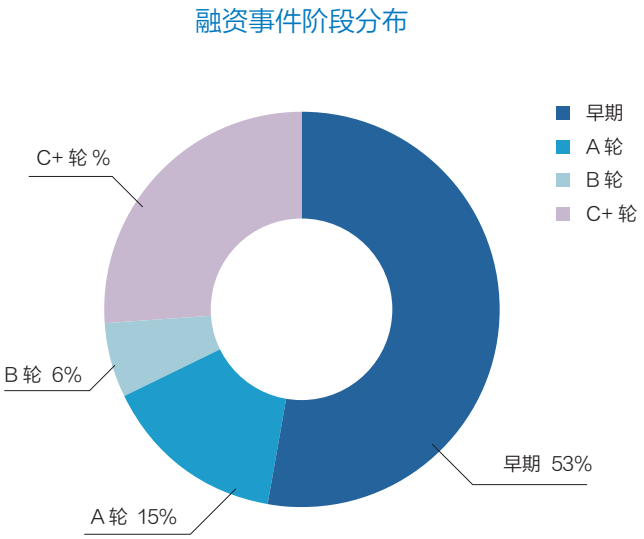
从投资阶段来看，2022 年全球网络安全投融资交易主要集中在早期和 c+ 轮。早期交易金额为 15.12 亿美元，同比增加 43.9%，交易数量为 516 笔，同比增加 21.7%，该轮次交易数量是各轮次中占比最高，且唯一保持正增长的投资阶段。C+ 轮交易规模最大，但是降幅明显，总计有 106.23 亿美元，同比下降 52.3%，交易数量为 247 笔，同比减少 18.5%。

并购交易方面，2022 年全球网络安全并购交易数量为 263 笔，同比减少 10.24%，由于欧盟暂停了博通对 VMware 的收购，行业并购规模出现明显下降，交易金额为 505 亿美元，同比下滑 37.58%。如果不考虑此影响，行业并购交易规模达到了 1198 亿美元，同比增加 48%，创 5 年来历史新高，其中收购上市公司 / 资产总计 1032 亿美元，占据总规模的 86.14%。分季度来看，并购交易主要集中在上半年，交易事件和规模占据全年的 59% 和 68%，而下半年交易数量和规模都出现较大下降，尤其是第四季度，并购金额仅有 71 亿美元，并购数量 49 笔，与高峰的第二季度相比，分别下降了 65.53% 和 35.53%。PE 的深度参与是海外网安行业并购的一大特点，其对网络安全行业并购参与逐渐扩大的过程正是网络安全高速发展的时期。与 2011 年相比，PE 由并购事件活动占比的 15% 扩张到 42%，由并购金额占比由 48% 上升到 68%。

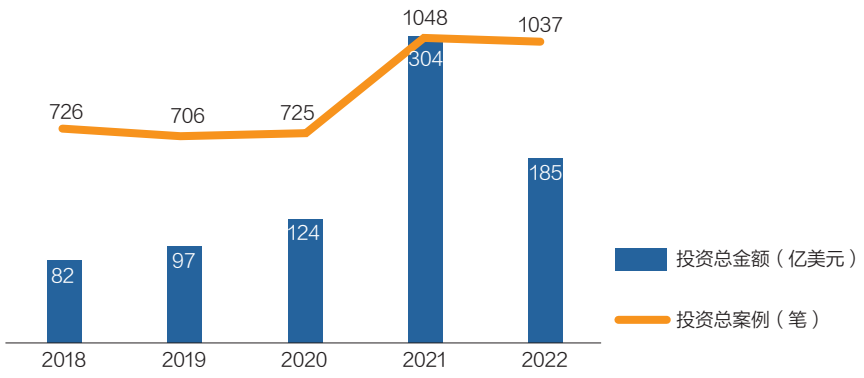
从并购金额中位数来看，2022 年全球网络安全行业并购交易规模的中值为 9020 万美元，略低于 2021 年的 1.085 亿美元，是近 5 年来第二高位。此外，2018—2022 五年并购中位数为 7700 万美金，与 2013–2017 五年并购规模中位数相比增加 76.61%。事实上，除去年外，2018—2021 年的并购规模中位数始终保持增长。从赛道来看，MSSP、安全 & 咨询、风险合规、IAM、网络 & 基础设施安全、数据安全、安全运营 / 事件响应 / 内部威胁、云安全、应用安全并购热度较高。

三、数字经济时代下，中国网络安全迎来行业发展的历史机遇

1. 网络安全和数据安全是数字经济持续健康发展的重要基石



（数据来源：Momentum Cyber，奇安信产业发展研究中心整理绘制）



（数据来源：Momentum Cyber，奇安信产业发展研究中心整理绘制）

数据是继土地、劳动力、资本、技术之后的第五大生产要素，是推动全球经济增长的主要动力，而以数据为基础构建的数字经济已经成为当代社会发展的主要方向。国家互联网信息办公室发布的《数字中国发展报告（2022 年）》显示，我国数字经济规模达 50.2 万亿元人民币，同比名义增长 10.3%，占 GDP 的比重提升至 41.5%，而这一占比在部分发达国家中更高。

事实上，脱离了安全的数字经济无法持续健康发展，更不用说数据本身就有安全属性，一旦泄露，则会造成重大损失。近年来，网络安全和数据安全已成为数字经济建设的底板工程，国家先后颁布了《网络安全法》和《数据安全法》，从立法层面强化和规范安全建设，工信部也明确表示电信等重点行业的网络安全支出占信息化投入的比例不能低于 10%。可以预见，在我国产业数字化和数字产业化的进程中，隐藏在数十万亿数字经济产业背后的网络安全和数据安全需求将逐渐得到释放，而这一释放的过程是长期和持续的。

2. 二十大的安全布局将进一步刺激中国网络安全潜能的释放

在 2022 年闭幕的二十大会议上，安全是大会的高频词汇，大会给中国网络安全及信息化、数字化产业的发展带来了深远影响，也直接刺激了去年年末我国网络安全二级市场板块的整体回暖。实际上，近几年，网络安全对其他国家战略产业的渗透越发明显，以信创产业为例，网络安全正在参与信创对我国信息化系统重构的全过程，并在其中与操作系统、终端、数据库等全要素同步规划、建设，全面覆盖并深度融合。随着信创产业加速从党政向金融、电信、电力、石油、交通、教育、医疗、航空八大关键行业渗透，并逐渐辐射至全行业，信创产业的规模在逐步增长，据艾瑞咨询统计，2021 年中国信创产业规模已经达到 13758.8 亿元人民币，2027 年有望达到 37011.3 亿元人民币，而信创产业与网络安全产业在共筑国家安全长城的同时，也进一步激发了网安产业发展的潜力。安

关于作者

陈华平

奇安信集团副总裁，产业发展研究中心负责人。

尹文鹏

产业发展研究中心研究员，主要负责投融资和市场研究。

延续还是改变？网络空间在未来武装冲突中的作用

作者 | 多米尼卡 · 齐维兹　布拉泽 · 赛杜克

编者按俄乌网络斗争四个主要洞察：一是俄罗斯未能在战争期间维持最初的快速和大规模网络攻击，表明在网络空间保持攻势极具挑战性；二是包括私营公司在内的西方国家协助在限制俄罗斯网络攻击的有效性方面发挥重要作用；三是俄罗斯战前的网络空间活动主要集中在通过虚假信息施加认知影响，未来将继续成为网络空间的重要用途；四是通过智能手机访问的 ICT 解决方案对于国防的重要性将会增加，此能力与国家和武装部队的信息系统相结合至关重要。

俄乌冲突被视为近三十年来的首次大规模常规战争，预计将给全球安全格局带来重大变化。这些变化不仅与战略和战术有关，还包括网络空间能力的利用。在乌克兰的敌对行动中，技术先进的行为者实际参与了冲突。值得注意的是，根据 2022 年国家网络力量指数，乌克兰在网络防御能力方面排名第二，而俄罗斯在拥有最重要的网络攻击能力方面排名第二。俄罗斯此前已经展示了其击败对手的能力，并被披露正在通过其秘密机构（在一家名为 NTC Vulcan 的私营公司的幌子下运作）不断开发进一步的攻击性网络工具。因此，俄乌冲突为未来战争中如何利用网络空间提供了独特的视角。

在 2022 年 2 月前，很多专家认为，俄乌冲突仍将处于灰色地带“闷烧”状态，网络空间将被广泛用于“处于战争边缘”的敌对活动。网络行动被认为是技术先进国家间激烈竞争的便捷替代选项。然而，俄罗斯对乌克兰的动能军事行动表明，当一方认为其切身利益受到威胁时，灰色地带的活动（包括网络行动）可能是不够的。俄罗斯的战略目标是实际占领乌克兰领土，事实证明网络空间的活动不足以实现这一目标。一旦跨过战争的门槛，网络空间进攻活动的作用也发生了转变。

关于此事，分析人士在 2022 年 2 月前设想了两种可能的情景，即在 21 世纪的武装冲突期间如何使用网络攻击。一些专家认为，网络攻击活动将被用作动能行动的补充或其局部替代。另一方面，其他一些专家强调网络空间活动与动能行动的同步，以提高后者的有效性。然而，对已披露的针对乌克兰的网络攻击活动及其与动能行动同时发生的分析表明，这两种假设都不成立。除对卫星互联网提供商 Viasat 的攻击外，没有任何旨在破坏物理基础设施的重大网络攻击的报道。此外，在同一地区协调动能攻击和网络攻击的情况很少见，对冲突进展没有产生重大影响。两种形式攻击的共存可归因于网络攻击的大规模性质，网络攻击因其规模似乎与其他领域的活动相关。

“五眼”联盟国家（美国、英国、加拿大、澳大利亚和新西兰）是关于网络空间在战争中当前和未来作用的宝贵知识来源。上述国家的网络安全机构于 2022 年 4 月底发表联合声明，警告犯罪集团在与乌克兰的战争中支持俄罗斯的行为，增加了这一消息来源的重要性。基于此，可以得出四个主要观察结果。

首先，俄罗斯未能维持最初的快速和大规模网络攻击，正如使用 6 到 9 个恶意软件家族所表明的那样。3 个月后，使用恶意擦除软件（破坏数据的计算机蠕虫）和其他类型的恶意软件的活动强度明显下降。

实际上，在网络空间保持攻势极具挑战性。开发有效的网络武器并使它们保持最新状态，比使用常规武器要困难得多。这是由于网络武器的“生命周期”，它需要更长的时间来检测新的漏洞并利用它发起攻击。当俄罗斯军队实际越过边界时，使用网络武器的优势被大大削弱，包括难以溯源、无国界性及避免人员伤亡以防止冲突升级。在这种情况下，大炮、火箭弹和无人机成为比网络攻击更有效的工具。因此，网络领域的使用不仅适用于俄罗斯的能力，还适用于任何必须在网络空间开展长期进攻活动的实体。需要一个计划周密的网络武器使用战略，网络武器在未来的大规模使用将主要是美国或中国（最有可能保持节奏和恢复能力的实体）的领域地盘。

其次，包括私营公司在内的西方盟友的协助，在限制俄罗斯网络攻击的有效性方面发挥了重要作用。美国网络司令部专家在战前访问了乌克兰，他们可能为乌克兰成功的网络防御做出了贡献。这种援助很可能是美国网络空间“前沿防御”防御“持续交战”战略的一部分。此外，乌克兰决定将关键数据迁移到云端并借助 Amazon Web Services 提供的 Snowball 设备对其进行保护，以及来自 Starlink 等公司的通信支持和来自卫星成像的数据支持，都在帮助乌克兰的安全方面发挥了至关重要的作用。因此，乌克兰的大部分敏感数据都被包括微软在内的西方实体转移和保护。

可以推断，在网络空间为盟友提供援助比在陆地等其他领域要简单得多。值得注意的是，西方领先的科技公司向乌克兰提供了大量支持。需要注意的是，这些公司并不效忠于国家当局，美国政府也不能强迫它们支持美国的盟友。然而，这引发了这些公司是否会以同样水平的承诺和决心支持其他美国盟友的问题。此外，美国公司发现援助乌克兰更容易，因为俄罗斯在战前并不是重要的经济伙伴。此外，从乌克兰获得的经验使网络安全公司能够更好地保护其所有客户。

再次，在战争爆发前，俄罗斯在网络空间的活动并不先进，主要集中在通过虚假信息进行影响。这种方法很可能会继续成为网络空间的主要用途。这符合英国引入的认知效应学说，该学说旨在操纵对手可访问的数据，

> 开发有效的网络武器
> 并使它们保持最新状态，
> 比使用常规武器要困难得多。

以创建和维持对现实的错误感知，然后可以利用这种感知为自己谋取利益。这一战略被西方情报机构用来对付“伊斯兰国”，很可能成为对抗俄罗斯的关键要素，因为信息战不仅直接支持军事行动，而且在战略沟通中发挥着至关重要的作用。

最后，乌克兰的国防活动包括组建由来自世界各地的志愿者组成的“乌克兰 IT 军队”。他们行动的有效性仍有待进一步分析。这项努力的一个成果是在 Diia 政府应用程序中添加了一项功能，用于报告俄罗斯行动造成的损失和敌军的位置。在美国的财政支持下，该系统可能会在其他国家普及。所有公民都可以通过智能手机访问的 ICT 解决方案对于国防的重要性将会增加。然而，将这些能力整合到战争期间的决策过程将是一项重大挑战。将这些能力与国家和武装部队的信息系统相结合至关重要，这项证明对北约国家具有挑战性。问题不仅在于网络安全和数据分析的水平，还在于确保通信符合在战时维持通信所需的标准。

在冲突进入白热化阶段前，
预计网络空间将保持重要地位，
因为它最适合处于战争边缘的活动，
而在军事行动中效果较差。

俄乌冲突证实了网络空间在战争中不断发展的使用，揭示了有关网络行动的专家假设。该领域活动的攻击性需要大量资源，只有少数国际行为者(包括私营公司)才能获得这些资源。在冲突进入白热化阶段前，预计网络空间将保持重要地位，因为它最适合处于战争边缘的活动，而在军事行动中效果较差。安

关于作者

多米尼卡 · 齐维兹

波兰雅盖隆大学学者、国家安全系副教授

布拉泽 · 赛杜克

波兰雅盖隆大学政治科学与国际关系学院副教授

如何基于威胁情报构建高效的网络威胁监测架构

声明：本文只代表笔者本人的观点，不代表所在公司和部门的意见。

作者 | 汪列军

通过网络层面开展基于情报的威胁监测，这是一种非常高效费比的技术方案，也是建设本地威胁情报中心的核心能力之一。然而，笔者研究过不少落地案例后发现，结果往往非常不尽如人意：要么检测不完全，数据能力没有充分利用；要么安全运营人员被淹没在一堆堆的垃圾告警中，连去看一下的兴趣都没有。为什么会造成这种结果？这源于尽管实现思路简单——无外乎数据的碰撞，但其中还是存在一些误区的：缺乏对威胁情报的深入了解和检测分析活动的实践，甚至有些从最初的架构设计上就决定了不太可能会有满意的效果。下面就笔者的实践和理解，剖析一下检测系统设计和运营的成功要素。

符合商业技术逻辑

作为基于威胁情报的监测系统的核心，威胁情报平台（TIP）一般来说是必要的组件，它负责汇集各种来源的威胁情报数据，赋能包括防火墙、IDS/IPS、NDR、SIEM/SOC 系 统在内各种检测设备和安全分析人员。TIP 汇集的情报数据中，直接可以用来执行检测和监测的数据就是 IOC（Indicator Of Compromise），还有各类可以支持分析研判的元数据和信誉信息。理想情况下，各种来源的数据以明文形式提供，TIP 平台可以方便地进行去重、验证、融合，这对于开源数据应该是可以的，但对于部分商业来源的重要数据则是有问题的。

这就涉及到商业逻辑：很多 TIP 厂同时也是情报数据厂商，与其他数据厂商很可能存在竞争关系。一般的开源数据也就罢了，数据厂商基本上不会愿意把自己的核心数据落到友商的 TIP 平台上，这再明显不过的道理会直接导致客户将来行事是事倍功半还是事半功倍。要知道数据服务不同于实现在产品里的逻辑功能，甲方可能觉得自己是出钱的，应该要什么就有什么，但实际上作为乙方的数据提供者天然占据信息优势，完全可以根据获得的商业收益决定输出的数量和质量。客户如果不同时进

> 理想情况下，
> 各种来源的数据以明文形式提供，
> TIP 平台可以方便地进行去重、验证、融合。

行多源采购，连个质量比较的机会都没有。由此导出，在检测架构的设计上需要允许安全厂商提供基于非明文数据的检测方案，然后对多家厂商输出的判定结果再做关联整合。如此的架构设计当然很不完美，因为检测数据层面的融合不再可行，大规模的批量关联拓展分析也不行了，但对于一个定位基于 IOC 做检测的系统来说至少是可用的，而且有望充分发挥多家厂商的数据能力。当然，如果客户预算足够多，全部明文也不是完全不可能，因为这符合价高者得的商业逻辑，但绝大部分客户不可能那样。

在技术限制的层面上，海量基础数据的本地化对绝大多数用户也不可行。被动 DNS、样本信息数据、Whois 数据条目量巨大且需要经常性更新，需要极大的存储计算资源。即便海量的数据在建设之初有个一次性的落地，日常更新的数据量也是巨量的；即使网络畅通也会消耗大量的带宽，更不用说很多物理和逻辑隔离的网络，基本不可能做到数据的及时更新，数据很快就会过时并与云端失去同步。基于以上这些限制，如果有些客户想在本地构建一个类似 VirusTotal 效果的系统，除非自身有海量基础数据的收集能力，最好不要轻易尝试，不然基本会以失败告终。

多源情报数据引接

基于威胁情报的检测系统必然涉及情报数据的引入，主要来源无外乎几类：开源采集、商业采购、联盟交换、用户自产。其中能起到核心作用的来源当然是商业采购。开源的数据一般会包括在商业数据中，因为没有一个情报厂商不把开源采集及其关联拓展纳入到自己的情报生产流程中。情报联盟由于能力不对等导致的贡献不匹配其实很难有效运作，用户自产只能起到非常有限的补充作用。

开源数据鱼龙混杂，收集容易研判难，一般用户不太可能同时有：

- 海量的历史被动 DNS 数据
- 海量的终端活动信息
- 海量的多来源文件样本
- 规模化的动静态自动化样本分析平台
- 看样本就像看一眼片子就知道啥肿瘤的医生那样的分析人员
- 数百万级别的商业基础数据采购
- 不可言说渠道来源的信息输入

事实上，如果用户自己具备如上的资源，那还要专业的情报厂商干什么？本质上，用户采购威胁情报购买的就是情报厂商打包后的基础数据及其分析研判能力。如果只是接入些甚至准确度都非常可疑的告警日志，提取 IP 和文件 Hash 当作威胁情报就太过家家了。

> 本质上，
> 用户采购威胁情报，
> 购买的就是情报厂商打包后的基础数据
> 及其分析研判能力。

各家大安全厂商都有自己独有的数据视野：有的自有安全产线齐全，能收很多特色数据；有的主动扫描收集能力强，能积累不少历史记录；有的蜜罐运营得不错，能及时发现新攻击活动；有的社区搞得热闹，有群众能提供线索和拓展；有的钞能力强大，能买不少基础数据；有的能依靠比较强的数据交换联盟支撑。以笔者对一些厂商数据能力的了解，数据存在相当大的非重合部分，所以，如果费用允许，强烈建议同时采购几家能力厂商的，但最好不要超过三家，因为市面上靠谱的情报厂商也没几家。这里又涉及到一个问题，如何评价各家厂商的威胁情报数据质量，笔者推荐现网流量环境下的测试，这当然也有很多坑，以后有机会单说吧。

另外，再说一下多源数据的融合，在笔者眼里这基本是个伪需求，有些 TIP 厂商号称用了什么 AI 的技术来融合多源情报，你可以想像两个不同厂商对于某个相同 IOC 定性矛盾的场景，有限的上下文信息使神奇的 AI 也不可能帮上啥忙，最终还是得依靠来源厂商的信誉做出取舍。

> 有效的威胁情报检测
> 应该基于事实型的原始元数据，
> 而不应该消费很不可靠的二手告警信息。

历史离线分析溯源

有效的威胁情报检测应该基于事实型的原始元数据，而不应该消费很不可靠的二手告警信息。鉴于目前流行的 IOC 数据类型主要是网络层面的，设备需要从网络流量中抽取如下元数据。

- DNS 请求和回应：最好是递归解析的流量，用于黑域名的检测，定位 C2 受害者。
- NetFlow：主要是 5 元组信息，用于检测不使用域名的直连 IP 的 C2 活动，确认 DNS 来源告警的真实性。
- URL：如果可以通过明文协调获取的话，用于黑 URL 的检测。
- 数字证书：直接定位使用了已知黑证书的网络基础设施或用于后续的关联拓展。
- Payload：一般收集的会话的前部的字节流，用于一些恶意代码的检测、确认和排除，确认 DNS 或 NetFlow 来源告警的真实性。
- 网络应用的指纹：结合漏洞情报定位一些存在漏洞的资产。
- 文件样本：配合后续的文件动静态的扫描检测。

IOC 的特性决定了它主要用于检测已知的威胁活动。一般的流量探针由于性能限制，只会最多加载数十万到百万级别的 IOC 数据，情报厂商出于显性效果的考虑，会优先输出流行度最高的数据，以预期产出最多的告警，但最流行的大概率并不是最重要的，因为涉及的攻击活动大多为非定向类型的威胁，而针对高价值目标的定向攻击往往比较聚焦，不太可能出现在高命中概率的优先输出 IOC 列表中。对于实时流量检测，Kill Chain 各个环节中可观测对象并非一直存在，结合加载 IOC 量的限制又进一步恶化了流量分析引擎中的实时检测效果。

应用 IOC，除了对当前的状况进行检测，更重要的是使用场景为追溯过往。作为尽最大可能捞取攻击线索的机制，全量离线异步的匹配计算必须考虑设计到整个检测架构中，元数据想当然的需要保留一定时间的历史记录，以备在新 IOC 被确认以后回溯过往的历史。在此类场景中，数据厂商的批量私有 IOC 数据可以通过某种单向 Hash 的形式，如布隆过滤器，提交到大数据平台执行批量的匹配，结果统一汇集到态势平台进行融合。当然，海量元数据会对存储、传输和计算带来极大的压力，设计策略和机制去除占大头的白数据可能是个缓解方案。这些元数据统一汇聚到一个大数据计算平台，可以被多个基于情报的检测引擎或设备共享，数据厂商对同一份现实数据给出自己的检测答案，也使评价厂商的现实能力成为可能。

重度数据运营投入

目前我所看到的威胁检测类产品项目中，“重初期建设数据、轻后期运营”基本是一种常态，这也是导致项目的安全效果不佳的主因之一。就笔者个人经验而言，威胁检测类项目

要出成果，数据采购费用应该在整个监测项目占到合适的比例，如 30% 以上。

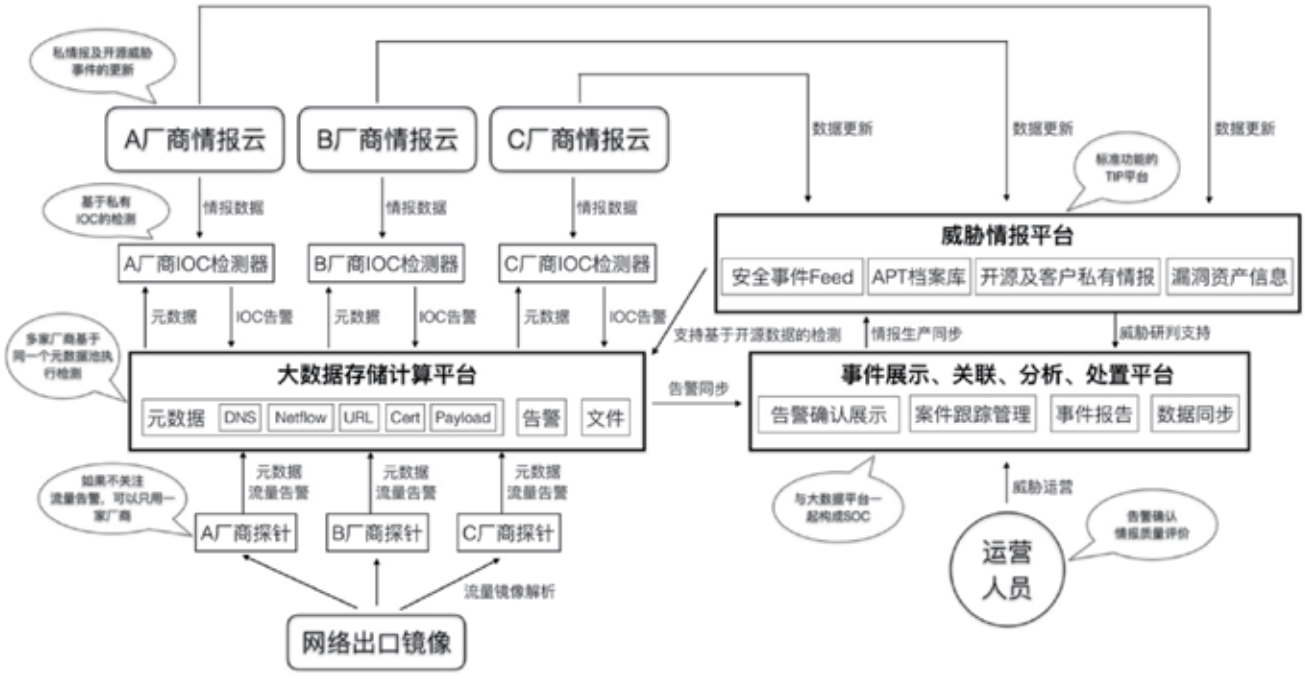
我们必须了解驱动安全检测设备或服务的核心是数据、规则、模型和人员，它们是整个系统的灵魂，没有这些，态势威胁感知系统就跟 OA 系统没有区别。对于情报数据厂商在实际环境下的检测能力表现需要有一个定期的评价机制。在情报数据费用总盘子内根据考核的结果进行倾斜分配，通过奖优罚劣，形成良性竞争，使客户自己的数据投入效果最大化。评价标准可以预先商定，然后根据自己业务方向的变化进行适时调整。威胁情报服务是乙方协助客户取得业务成功，反过来客户也需要学会牵引乙方，这当然也对客户本身的能力提出了更高的要求。多源数据引入的要义不仅仅在于互相补充视野，更在于通过对产出成果的比较来发现优秀的供应商，并通过赛马形成持续改进的压力，这样对于甲方和乙方都好。

需要强调的是，准确的 IOC 不等于准确的告警。典型的 IOC 类型，如 IP、域名、文件 Hash，都是些简单的原子化数据。域名之类的访问和非特定端口的 IP 连接，其实非常容易被正常的活动触发，引发不准确的告警。事实上，即便 IOC 集是 100% 准确，由此触发的告警可能还有 50% 以上是不准确的。基于 IOC 的告警只能作为威胁事件的线索，需要后期的分类分级，通过更多数据和行为的验证、人工经验的介入做进一步的确认，才能形成确定性的事件。

大多数没有得到正常运营的威胁监测系统，特别是 NDR 类设备，如果每天滚动着上万条的告警，其中至少 99% 是误报或不重要的。没有基本运营的检测系统只会是一个输出垃圾的机器，遗憾的是这样被荒废的系统，笔者见得实在太多了。如何避免呢？简单的应对是配备必要的运营人员。一个在客户侧运行的威胁监测系统，最少需要配备一个中低技能的驻场和一个高水平人员的远程支持和巡检。本地人员需要有基本的安全知识，进行明显误报的削减，发现自己处理不了的可疑线索转到远程寻求支持。高水平的人员永远都是缺乏的，笔者不认为 AI 能快速地解决这个问题，所以，必须在远程同时支持多个点上报的分析处理任务，如此才能在商业上做到支持成本可控。现在很多所谓的专家在提倡多利用 TTP 类型的威胁情报，在其指导下执行威胁狩猎。笔者想说的是，理想很丰满、现实更骨感。连准确的基于 IOC 的告警运营都没做到位，对于一般安全投入的客户来说，成本极高的本地威胁狩猎先就别想了，一点一点来吧。

总体来说，情报数据和运营人员的成本需要在项目总投入中划出来，理想情况应该占到总成本的 50% 以上。只有系统软 / 硬件的建设而没考虑后续运营投入的项目必定失败，不会有例外。

总体来说，
情报数据和运营人员的成本
需要在项目总投入中划出来，
理想情况应该占到总成本的 50% 以上。



总结

基于上述分析，监测系统的整体架构可以总结如下。这个架构只涉及最核心的威胁检测功能，溯源和打击都不在范围之内。

该架构的核心理念包括如下几点:

1、 实时流量检测与全量历史元数据异步检测结合。

2、 共享同一个元数据事实池，允许安全厂商进行背对背的基于私有情报的检测。

3、 多源数据采购和效果比较评价。

4、 必须的安全运营人员投入。

5、 高投入占比的数据和运营的安排。

聪明的客户需要知道细节，了解环境，懂得取舍，驱动改进，当然最好还要有预算。安

关于作者

汪列军

虎符智库专家 关注恶意代码分析、APT 攻击事件与团伙的跟踪与挖掘，实现安全威胁情报的运营与产品化。

安全事件运营 SOP：安全事件概述

作者 | 武鑫

在企业安全运营建设时，大致会经过依赖人工或安全公司提供服务、安全事件处置标准化、自动化响应三个发展阶段。

本文将聚焦介绍常见的安全事件及标准处置方法，即安全事件处置 SOP。

1. 安全事件概述

1.1 安全事件定义

这里引用《国家网络安全事件应急预案》中的定义，网络安全事件是指由于人为原因、软 / 硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件，可分为有害程序事件（MI）、网络攻击事件（NAI）、信息破坏事件（IDI）、信息内容安全事件（ICSI）、设备设施故障（FF）、灾害性事件（DI）和其他事件（OI），这些是比较官方的分类方法。

在实际的工作中，更多的是按照组织职能或工作内容加以区分，比如，安全部门中设置了反入侵团队和数据安全团队，则对应网络安全事件和数据安全事件日常运营。

• 网络安全事件：指由于人为操作、网络攻击、软 / 硬件故障、自然灾害等，对账号、信息系统或网络造成危害的事件。就企业安全建设和安全运营而言，可以细分为安全违规事件，风险操作违规、账号口令违规、私搭乱建违规等；网络攻击事件，扫描行为、IOC 告警、邮件钓鱼账号疑似被盗等；接收漏洞事件，SRC 接收漏洞、CNVD 接收漏洞、客户侧接收漏洞和行业监管单位接收漏洞。

• 数据安全事件：指将企业的机密、秘密或其他级别的敏感信息发布到外部环境中，一旦被不法分子利用，造成的安全事件。主要分为内部信息泄露和外部信息泄露两大类。其中内部信息泄露，如 U 盘文件拷贝、IM 文件外发、邮件外发敏感数据、U 盘文件创建 / 写入；外部信息泄露，如公网 github 信息泄露、敏感数据兜售监测。

> 在企业安全运营建设时，
> 大致会经过依赖人工或安全公司提供服务、
> 安全事件处置标准化、自动化响应三个发展阶段。

1.2 事件分级原则

• 事件分级以量化指标为优先原则，在主观量化损失时应按较高的量化损失或更严重的影响作为评估依据；

• 如判断准确量化存在较大困难或量化所消耗成本较高时，可基于主观判断；

• 在事件持续过程应根据事件进展动态更新事件级别。

1.3 安全事件运营

对于外部攻击导致的安全事件，每一次都需要进行深入分析，找到不足并补强。但针对内部人员导致的安全事件，从发生监测到事后运营，属于单事件运营，起到的防护或警示效果有限。为了进一步让事件发挥出更大的效果，对主机和数据安全事件进行统一化管理，建立以部门为单位的安全风险分数计算、公示机制，并组织违规个人及部门参与安全红线、安全意识培训和考试，以此降低再犯的可能性。

2. 安全事件处置

2.1 处置原则

1. 责任制原则

按照“谁主管谁负责，谁运行谁负责，谁使用谁负责”的要求，信息系统的业务主管部门、使用部门和运行部门是信息系统协调和处置的直接责任部门，部门负责人是第一负责人。各部门在处置中做好协调和沟通联系，在分工合作的基础上落实处置工作责任制，确保责任落实。

2. 快速恢复原则

发生需要跨部门协调处置的网络安全事件时，各部门应按照“解决问题优先，程序次之”的原则共同协作，力争快速恢复系统，使损失最小化。

3. 分级处置原则

按照事件的不同级别，应设置不同的响应时间、总结复盘及奖惩等要求。

• 响应时间：不同级别的信息安全事件，第一响应速度都应该是在分钟级甚至秒级的。但安全事件的级别越高，在限时内上报的领导级别就应该越高，比如，P5 事件仅需一线安全运营工程师或自动化处置，P3 事件就应该上报告网络安全部负责人，P2 事件就应该上报至网络安全委员会及最高领导；

• 总结复盘：在安全事件处置之后，应针对不同级别的事件做出不同级别的复盘要求，最低级别应该是涉事责任人，然后依次为涉事方部门反馈、网络安全部牵头复盘、网络安全委员会组织复盘并向最高领导做汇报；

• 事后奖惩：对事件进行定责与奖励。鼓励发现安全事件及在安全事件过程中表现优异的个人与行为，对造成安全事件的相关人员或部门进行处罚。安

全部门不具备行政处罚能力，需要联动人事部门按照公司要求进行执行。

2.2 处置流程

当发生信息安全事件时，及时止损与快速恢复业务是首要目标。及时止损包括控制或解决事件带来的不良影响；恢复业务需结合实际场景在事件得到有效的遏制或消除后，重新上线提供服务。无论是遏制或解决，按照处置流程进行操作均是标准的动作。常见的处理流程可以分为五个步骤。

> 对于外部攻击导致的安全事件，每一次都需要进行深入分析，找到不足并补强。

1. 告警响应

当收到告警信息时，一线安全运营人员需要对信息进行判断，按照相对应的 SOP 进行执行。但告警信息的来源非常广，可能是公司内 / 外部人员反馈、各类 Sensor 告警信息、上级监管单位通报、安全应急响应中心（SRC）接收等渠道，所有安全事件都先由一线安全运营人员处置，处置过程中发现问题或拿不准就上升到二线，二线再根据实际情况发起深入的安全响应措施。

2. 分析研判

事件分析是整个处置流程中的重点也是难点，安全事件种类较多，对安全运营人员的能力有较大的考验，可从实际安全运营工作内容及风险治理的角度，将安全事件按照处理的难易程度进行区分。

• 容易处置类：仅靠沟通就能完成处置，关键是需要相关责任人提供详实的证据，附在事件处置工单中才能当做闭环。包括主机安全事件中的违规事件、正常操作、误操作、重复事件、误报；数据安全事件中各类信息泄露。

• 验证处置类：主要是弱口令类数据，需要使用技术手段对事件进行验证。无论是 NTA 中的弱口令事件告警还是基于 HIDS 发现的弱口令，都需要进一步验证是否真实存在、是否从外部可利用并造成危害。前者是只要在 NTA 覆盖的流量范围内，传播弱口令，不管相关系统或服务是否真实存在弱口令，都会进行告警，所以误报可能性较大；后者是由于主机账号、服务可能仅本地使用，从非本地的地址访问存在不能利用的情况。

• 深入排查类：主要是指网络攻击类事件，需要对事件进行专业分析，对安全运营人员的技术能力有较高要求，且对于根因的发现、漏洞的排查与修复甚至溯源反制，都取决于安全人员的能力和经验。越是经过攻防实战的人，越能快速定位问题。

3. 事件上报

在对安全事件进行分析与判断后，需要对事件进行初步定论，并按照不同级别上报相关领导或安全组织，以获得更多资源支持与决策，推动该事件被更快速的处置。

网络安全事件处置报告单

事件名称			
事件 ID		事件级别	
报告日期		发现来源	
影响概述	事件影响级别		
	外部影响描述 内部影响描述		
系统信息			
系统 IP		影响时长	
负责人		负责团队	
事件关键时间			
发现时间			
安全初查时间			
漏洞修复时间			
安全复查时间			
事件处置过程			
处置过程	处置步骤		参与人员
1			
2			
影响分析			
法务影响	无		
业务影响	无		
数据影响			
安全风险	无		
其他	无		
原因分析			
原因分类	□设备设施 □应用系统 □人员 □流程 □外部因素		
原因分析			
后续改进			

4. 全面处置

主要从溯源取证、对外公关、业务止损与恢复三方面，对安全事件进行处置。

• 溯源取证：从各安全设备的告警、日志、流量进行分析，摸清攻击者的来龙去脉，还原攻击链；分析攻击者留下的样本、后门文件，进行内部横向排查和清除；

• 对外公关：当安全事件即将在特殊时期发生或已经发生时，且在外界产生不良影响，包括让客户的网络安全面临风险、用户信息遭到泄露等情况，需要联动公关部门对外做好舆情监测和应对策略；

• 业务止损与恢复：对相关业务系统及服务器进行安全加固，监测和发现可能存在的潜在后门并进行清理，为业务再次上线做准备。

5. 总结复盘

每一次事件，对于安全来说都应该是一次涅槃重生、建设更加安全网络环境的机会。深挖事件产生的原因、验证安全防护机制、检验安全监测策略，并做横向思考，根据剖析与总结事件，输出事件报告，其中比较重要的除了事件原因就是一系列可提升现有水平的后续改进项。以下为安全事件报告模板：

关于作者

武鑫

虎符智库专家，擅长从攻防视角进行甲方企业安全建设，在软件开发安全、供应链安全、攻防对抗方面有一定研究。

奇安信

敏感信息泄露情报服务

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

纵深防御的马奇诺防线，为什么会被攻破？

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

服务定位 SERVICE POSITIONING

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

奇安信安服团队

奇安信蝉联“中国网安产业竞争力50强”第一名

6月23日，中国网络安全产业联盟（CCIA）
揭晓“2022年中国网安产业竞争力50强”榜单。
凭借在网络安全领域领先的技术实力以及突出的市场表现，
奇安信蝉联第一名。

“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	天融信科技集团股份有限公司
5	华为技术有限公司
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	阿里云计算有限公司
9	新华三技术有限公司
10	杭州安恒信息技术股份有限公司
11	360政企安全集团
12	亚信安全科技股份有限公司
13	成都卫士通信息产业股份有限公司
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