内部资料 免费交流

出版物准印证号：京内资准字 2122- L0058 号

SECURITY INSIDER

网安26号院

奇安信网络安全通讯

四个故事
聊清数据安全风险

P13

第30期
2023 年 6 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。

超级 IP《西游》遇到数据安全

6 月初的 Gartner 安全与风险管理峰会上，Gartner 分析师兼副总裁尼尔·麦克唐纳（Neil MacDonald）表示，75% 的安全用户在寻求供应商整合。他特别告诫：不要把一堆孤立的安全工具堆在一起，用户想要更少的供应商，想要更好的效果。

作为这一趋势的体现，安全产品逐步整合。他认为网络安全产品将整合为包括数据安全平台在内的 10 个主要平台。

目前，数据安全保护成为大多数安全团队的首要任务，推动了数据安全领域的产品技术创新。2023 年，中国信息通信研究院发布的《数据安全产品与服务图谱 2.0》，合计收录了 116 家企业的 488 款数据安全产品及服务信息。部署多种单点数据安全工具带来的挑战也日益明显：不同数据安全工具孤立运行，不仅效率低下，无法支持数据风险评估，以及涉及数据的创新和协作，更糟的是会带来看不见的安全风险与漏洞。

2021 年下半年，Gartner 在《2021 数据安全技术成熟度曲线》对数据安全平台（DSP）进行定义，认为孤立单点的产品正走向整合。此后，行业和客户对数据安全平台（DSP）的兴趣呈爆炸式增长。

对于数据安全平台的核心功能，不同供应商有不同的定义。研究机构 Gartner、Forrester 及 ESG 研究集团都有少许差别的定义与功能界定。Forrester 对全球数据安全平台提供商进行评估时，主要能力标准包括：数据发现、数据分类、数据使用洞察、数据威胁和风险可见性、数据访问控制、数据防泄密、数据脱敏或编写、数据加密、权限管理、标记化、隐私用例、数据和信息治理用例、调查、可管理性和支持、零信任集成和供应商风险。这些长达 16 项的功能，也可以按照核心功能分为数据发现与分类、数据访问控制、数据安全防护，数据安全态势管理及数据合规等，这与奇安信发布的奇安天盾所强调的四项核心能力——看清风险、管好防控、防好攻击，以及实现合规——不谋而合。数据安全平台的功能还处于不断演进中，而政企机构企业转向完整的数据安全平台架构需要时间，但尽早开启数据安全功能整合却是不容忽视的需求。

本期《网安 26 号院》在风格上进行了创新尝试，用四个真实案例改编的西游漫画，轻松聊聊数据安全风险： 看清篇——偷瞄同事薪资单，险酿数据安全事故，如何预警？管好篇——家贼难防，竞争对手窃取企业标书；防护篇——数据被加密，企业遭遇巨额勒索；合规篇——企业数据泄露，总裁遭处罚。

超级 IP《西游》遇到数据安全，能迸发出怎样的火花？期待您的反馈。

总编辑

李建平

2023 年 6 月 1 日

CONTENTS

目录

安全态势

月度专题

偷瞄同事薪资单，险酿数据安全事故；家贼难防，竞争对手窃取企业标书；数据被加密，企业遭遇巨额勒索；企业数据泄露，总裁遭处罚。四个来自业务场景的鲜活故事，充分展示了数据安全的主要风险，以及如何看清风险、管好访问、防住攻击和实现合规。

奇安资讯

《网安 26 号院》编辑部

主办 奇安信集团

总　编　辑：李建平
安全态势主编：王　彪
月度专题主编：李建平
攻防一线主编：魏开元
安全之道主编：张少波
安全叨客主编：魏开元
奇安资讯主编：陈　冲
报告速递主编：闫　延
专　栏主编：李建平

奇安信集团　虎符智库　安全内参

索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

索阅邮箱：26hao@qianxin.com
地　　址：北京市西城区西直门外南路 26 院 1 号
邮　　编：100044
联系电话：（010）13701388557

出版物准印证号：京内资准字 2122– L0058 号
编印单位：奇安信科技集团股份有限公司
发送对象：奇安信集团内部人员
印刷数量：4500 本
印刷单位：北京博海升彩色印刷有限公司
印刷日期：2023 年 6 月 26 日

栏目主编　王彪

政策篇

国内，《商用密码管理条例》自 7 月 1 日起施行，相关组织应及时做好商用密码应用安全性评估。

国际上，欧洲议会通过人工智能法案草案，该法案已进入立法最终程序。欧洲议会声明，该提案获得批准后将成为全球首部规制人工智能的法规。

国内

金融业三大协会分别发布行业公司网络和信息安全三年提升计划

6 月 9 日综合消息，中国证券业协会、中国证券投资基金业协会、中国期货业协会同日分别发布《证券公司网络和信息安全三年提升计划（2023—2025）》《基金管理公司网络和信息安全三年提升计划（2023—2025）》《期货公司网络和信息安全三年提升计划（2023—2025）》。

《证券公司安全提升计划》阐明了未来三年全面提升证券公司网络和信息安全的指导思想、基本原则、总体目标、主要任务及实施路径，包括六类 31 项主要任务要求，形成了 32 项具体任务清单。《基金管理公司安全提升计划》主要包含发展现状与形势、总体要求、重点任务、保障措施及附件等 5 个部分，提出了“6 体系 1 落实 7 保障”的工作思路与具体建议，设定了 33 项量化指标。《期货公司安全提升计划》主要包括导语、总体要求、主要任务和保障措施四方面内容，提出了 20 项工作任务，并配套制定了五方面保障措施。

国家密码管理局《商用密码检测机构管理办法》和《商用密码应用安全性评估管理办法》公开征求意见

6 月 9 日司法部官网消息，国家密码管理局研究起草了《商用密码检测机构管理办法（征求意见稿）》和《商用密码应用安全性评估管理办法（征求意见稿）》，现公开征求意见。《商用密码检测机构管理办法（征求意见稿）》提出，从事商用密码产品检测、网络与信息系统商用密码应用安全性评估等商用密码检测活动，向社会出具具有证明作用的数据、结果的机构，应依法取得商用密码检测机构资质。《商用密码应用安全性评估管理办法（征求意见稿）》规定了商用密码应用安全性评估的总体要求，以及规划、建设、运行各阶段的具体要求。

国家网信办发布《个人信息出境标准合同备案指南（第一版）》

5 月 30 日网信办官网消息，国家互联网信息办公室编制发布《个人信息出境标准合同备案指南（第一版）》，对个人信息出境标准合同备案方式、备案流程、备案材料等具体要求作出了说明，以指导和帮助个人信息处理者规范、有序备案个人信息出境标准合同。该文件要求，个人信息处理者通过与境外接收方订立个人信息出境标准合同的方式，向境外提供个人信息，应当根据《个人信息出境标准合同办法》规定，按照备案指南向所在地省级网信部门备案。

《政务网络安全监测平台技术规范》等 19 项网络安全国家标准获批发布

5 月 31 日信安标委官网消息，根据 2023 年 5 月 23 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2023 年第 2 号），全国信息安全标

准化技术委员会归口的 19 项网络安全国家标准正式发布，包括 10 项修订标准和 9 项新标准。

10 项修订标准包括网络安全审计产品技术规范、网络安全事件分类分级指南、信息安全风险管理实施指南、网络入侵防御产品技术规范、反垃圾邮件产品技术规范、云计算服务安全指南、云计算服务安全能力要求、信息安全管理体系指南、行业间和组织间通信的信息安全管理、电子政务移动办公系统安全技术规范。

9 项新标准包括边缘计算安全技术要求、区块链技术安全框架、区块链信息服务安全规范、可信执行环境服务规范、网络身份服务安全技术要求、个人信息处理中告知和同意的实施指南、移动互联网应用程序（APP）个人信息安全测评规范、政务网络安全监测平台技术规范、电子凭据服务安全规范。

李强签署国务院令，公布修订后的《商用密码管理条例》

5 月 24 日新华社消息，国务院总理李强签署第 760 号国务院令，公布修订后的《商用密码管理条例》（以下简称《条例》），自 2023 年 7 月 1 日起施行。《条例》共计九章六十七条，主要围绕“科技创新与标准化、检测认证、电子认证、进出口、应用促进、监督管理”等六个方面进一步明确了规范要求，包括完善商用密码管理体制、促进商用密码科技创新与标准化建设、健全商用密码检测认证体系、加强电子认证服务使用密码和电子政务电子认证服务活动管理、规范商用密码进出口管理、促进商用密码应用等。

国际

欧洲议会通过人工智能法案草案，立法进入最终程序

6 月 14 日欧洲议会官网消息，欧洲议会全体会议表决通过了《人工智能法案》授权草案，该法案进入欧盟立法严格监管人工智能技术应用的最终谈判阶段。欧洲议会投票决定，禁止实时远程生物识别技术，如不能在公共场合进行实时人脸识别，并对 ChatGPT 等生成式人工智能工具增加更多安全控制措施，提出新的透明度要求，以确保人工智能的研发和应用符合欧盟权利和价值观。按照立法议程，欧洲议会将就这一授权草案，与欧盟委员会和成员国进行“三方”谈判，欧洲立法者希望在今年年底前就法案的最终版本达成共识。欧洲议会声明，这部提案如正式获得批准，将成为全世界首部有关人工智能的法规。

美国 CISA 发布强制操作指令，降低联邦机构设备的公网暴露风险

6 月 13 日 CISA 官网消息，美国网络安全与基础设施安全局（CISA）发布了今年首个约束性操作指令 BOD 23-02，要求暴露在互联网上的联邦民事机构设备网络管理界面 / 接口，如果无法禁止公网访问，那么必须采用零信任架构实施访问控制。CISA 将扫描互联网上的设备和管理系统，如发现暴露设备将向对应机构通报。联邦机构需在发现问题后 14 天内，采取措施确保配置错误或暴露在互联网上的设备的安全性。

美国 NIST 发布《联邦机构漏洞披露指南建议》

5 月 24 日 NIST 官网消息，美国国家标准与技术研究院（NIST）发布《对联邦漏洞披露指南的建议》（NIST SP 800-216）。该文件就建立联邦漏洞披露框架、正确处理漏洞报告，以及沟通漏洞的缓解和 / 或修复提出了指导建议。联邦漏洞披露框架不仅提供了联邦监督，还提供了本地解决方案支持，适用于联邦控制下的所有软件、硬件和数字服务。

美国防部向国会提交《2023 年美国防部网络战略》

5 月 26 日美国防部官网消息，美国国防部向国会提交了机密级文件《2023 年美国防部网络战略》，并计划未来数个月内公布非机密版战略摘要。该战略基于此前美军网络行动和俄乌战争网络战的现实经验，提出三项网络领域指导原则：一是美军将最大限度地发挥其网络能力，以支持综合威慑，并与其他国家力量工具协同运用网络空间行动；二是美军将在低于武装冲突水平情况下在网络空间中和通过网络空间开展活动，以加强威慑和挫败对手；三是美国的全球盟友和合作伙伴是必须保护和加强的网络领域基础优势。

事件篇

我国《数据安全法》执法进入密集期，浙江、江西等多地监管单位接连公布相关案件处罚案例。勒索软件全球持续肆虐，美、德、法、日等多国重要企业不断中招。

今年最大规模网络攻击：0day 漏洞击穿防线，美国近百家大型政企遭勒索

6 月综合消息，美国网络安全与基础设施安全局（CISA）称，俄罗斯勒索软件组织 Clop 在 5 月 27 日开始，利用 MOVEit 文件传输软件的 0day 漏洞发动攻击。目前确认的知名机构受害者包括美国能源部下属机构、美国农业部、俄勒冈州和路易斯安那州的机动车部门等，海量政府、企业和公民数据遭勒索。安全厂商 Emsisoft 的威胁分析师 Brett Callow 称，已统计 63 名已知 / 确认受害者和数量不详的政府机构。据悉，美国财政部、国防部、NASA 等众多机构均采购了 MOVEit 软件。CISA 局长 Jen Easterly 表示，此次大规模入侵的对象具有“高度随机性”，危害等级低于 2020 年的 SolarWinds 事件。

浙江一公司涉数据安全违法，当地警方依据数据安全法处以 100 万罚款

6 月 16 日公安部网安局公众号消息，浙江温州公安网安部门近期在查处一起涉数据安全违法案件时发现问题。浙江某科技有限公司为浙江某县级市政府部门开发运维信息管理系统的过程中，在未经建设单位同意的情况下，将建设单位采集的敏感业务数据擅自上传至租用的公有云服务器上，且未采取安全保护措施，造成了严重的数据泄露。浙江温州公安机关根据《中华人民共和国数据安全法》第四十五条规定，对公司及项目主管人员、直接责任人员分别予以罚款 100 万元、8 万元、6 万元的行政处罚。

勒索攻击致使德国知名大学 IT 设施全瘫痪，近半年该国已有多所高校被黑

6 月 12 日 TheRecord 消息，德国卡尔斯鲁厄应用技术大学（HS Kaiserslautern）披露遭受勒索软件攻击。该学校通过紧急网站宣布“整个 IT 基础设施”已经下线，其中包括学校电子邮件账户和电话系统。学校表示，几乎所有面向学生的设施和服务都遭到波及，超过 6200 名学生受到了影响。电脑机房乃至图书馆都将“暂时关闭，具体开放时间另行通知”。学校还在官网向学生和员工发出警告，不要打开他们的工作电脑：“这是一次加密攻击，员工工作场所的工作站可能也会受到影响。”此前数月，德国至少有六所类似的机构也遭遇了类似事件，包括汉堡应用技术大学、哈尔茨应用技术大学、杜伊斯堡 – 埃森大学等。

江西某公司疑遭黑客攻击，当地网信办依据数据安全法处以 50 万罚款

6 月 7 日网信南昌公众号消息，南昌市网信办于 4 月 13 日接到上级网信部门通报，江西某股份有限公司运营的网络智能办公系统疑似遭黑客组织攻击并植入木马病毒，主机存在受控的风险。经立案调查查明，该公司的 OA 系统和服务器内存储了大量敏感数据，但该公司履行数据安全保护义务不到位，OA 系统感染了可获取服务器文件管理权限和命令执行权限的木马程序，相关行为违反了《中华人民共和国数据安全法》第二十七条规定；该公司开展数据处理活动未加

强风险监测，在发现数据安全漏洞风险和事件时未采取补救措施，未履行风险监测、补救处置等义务，相关行为违反了《中华人民共和国数据安全法》第二十九条规定。

5 月 30 日，南昌市网信办依据《中华人民共和国数据安全法》第四十五条规定，对江西某股份有限公司处以警告、罚款 50 万元，对直接负责的主管人员处以罚款 5 万元的行政处罚。

日本制药巨头遭勒索攻击：内部系统被迫大面积断网 运营受影响

6 月 8 日 BleepingComputer 消息，日本制药巨头卫材（Eisai）披露了一起勒索软件事件，攻击者加密了部分服务器并导致运营受到影响。受勒索攻击事件影响，卫材公司被迫将大量 IT 系统断开网络，包括物流系统等多个系统被迫下线并停止服务，预计调查结束后才能恢复。卫材表示正在调查数据泄露的可能性，目前无法排除这一潜在风险。目前尚无勒索软件团队宣布对此负责。

法国海外省疑遭勒索软件攻击，政务网络已瘫痪数周

6 月 6 日 TheRecord 消息，位于中美洲加勒比海的法国海外省马提尼克岛疑似遭遇勒索软件攻击，致使互联网访问与多项政务民生服务已中断大半个月，目前仍在处理中。马提尼克岛管理委员会发布公告称，此次网络攻击开始于 5 月 16 日，当地官员被迫隔离受影响的系统，制定计划逐步恢复正常运行。公告提供了教育、金融等多类服务无法使用网络的替代方案，但恢复进度远不尽人意。该岛政府和法国外交部、网络安全部门没有回应置评请求。

俄罗斯指责 NSA 利用苹果后门监控境内 iPhone，中国大使馆亦受影响

6 月 1 日 BleepingComputer 消息，俄罗斯联邦安全局、国家 CERT、卡巴斯基今天分别发布消息，披露了一起针对俄 iPhone 用户的网络间谍事件。卡巴斯基报告称，未知攻击者利用苹果 0day 漏洞，在员工 iPhone 上安装远控软件，莫斯科及多国分部员工均受影响，并公开了多个 IoC 信息。俄联邦安全局公告称，美国情报部门利用苹果提供的漏洞监控了数千台 iPhone 设备，受害者包括俄罗斯公民、以色列、中国及多个北约成员国外交人员。俄罗斯 CERT 发布警报，将这两份报告归并为一起事件。苹果公司否认了“政府后门”指控，NSA 对此不予置评。

希腊教育部遭遇最严重网络攻击：全国考试被干扰 引发政治动荡

5 月 31 日美联社消息，正值希腊全国高中期末考试期间，希腊教育部“学科库”国家题库平台在 5 月 29 日、30 日连续两天遭到大规模 DDoS 攻击，导致教师无法从题库平台抽取考题，部分考生不得不在教室等待数小时。此次网络攻击共计超过 114 个国家的计算机共同发起，导致高中考试出现中断和延迟，但未能使系统瘫痪。希腊教育部表示，“这是希腊公共机构、政府机构有史以来遭遇的最严重攻击。”希腊主要反对党左翼激进联盟发言人 Popi Tsananidou 称：“到目前为止，新民主党政府一直在傲慢地推卸责任。四年来，他们未能针对学科库平台采取足够的数字保护措施，无力保障学校考试顺利进行。”

特斯拉 100GB 数据泄露，或面临 35 亿美元罚款

5 月 29 日界面新闻消息，据德国《商报》报道，特斯拉未能充分保护客户、员工和业务合作伙伴的数据而造成泄露，并收到了数千份关于该公司驾驶员辅助系统的客户投诉。报道援引一名举报者泄露的 100GB 机密数据，这些数据包含超过 10 万个离职和在职员工姓名，以及私人电子邮件地址、电话号码、员工工资、客户的银行信息和生产的秘密细节的多个表格，其中更是涉及特斯拉 CEO 埃隆 · 马斯克的社保号码。特斯拉柏林超级工厂所在地勃兰登堡的数据保护办公室将此次数据泄露描述为“大规模”。这一行为违反了欧盟的《通用数据保护条例》（GDPR）。如果证明确实存在此类违规行为，特斯拉可能会被处以高达其年销售额 4% 的罚款，即 32.6 亿欧元（35 亿美元）。

漏洞篇

国产软件漏洞利用层出不穷地在互联网上公开，近期金蝶云星空远程代码执行漏洞（QVD-2023-14179）、畅捷通 T+ 反序列化漏洞 (QVD-2023-13615)、畅捷通 T+SQL 注入漏洞 (QVD-2023-13612) 等影响较大，建议客户尽快做好自查及防护。

金蝶云星空远程代码执行漏洞安全风险通告

6 月 15 日，奇安信 CERT 监测到金蝶云星空远程代码执行漏洞（QVD-2023-14179），该漏洞是由于金蝶云星空管理中心的通信层默认采用的是二进制数据格式，需要进行序列化与反序列化，在此通信过程中未做签名或校验，攻击者可以恶意修改传输的数据，导致执行任意代码执行。奇安信 CERT 已成功复现该漏洞，鉴于该漏洞的 PoC 已在互联网上公开，现实威胁上升，建议客户尽快做好自查及防护。

Nuxt 远程代码执行漏洞安全风险通告

6 月 14 日，奇安信 CERT 监测到 Nuxt 远程代码执行漏洞 (CVE-2023-3224)，Nuxt 中存在代码注入漏洞，当服务端以开发模式启动时，远程未授权攻击者可利用此漏洞注入恶意代码并获取目标服务器权限。Nuxt 是一个 Web 应用开源框架。目前此漏洞 PoC 已在互联网上公开，同时奇安信 CERT 分析并复现此漏洞，鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Apache NiFi 多个高危漏洞安全风险通告

6 月 13 日，奇安信 CERT 安全研究员发现 Apache NiFi 反序列化漏洞 (CVE-2023-34212)，经过身份认证的远程攻击者利用该漏洞可以执行代码或造成崩溃。Apache NiFi 新版本修复的还有另一高危漏洞 Apache NiFi 代码执行漏洞 (CVE-2023-34468)，经过身份认证的远程攻击者利用此漏洞可以执行代码。Apache NiFi 是一个易于使用、功能强大而且可靠的数据处理和分发系统。鉴于这些漏洞影响较大，建议客户尽快做好自查及防护。

Openfire 身份认证绕过漏洞安全风险通告

6 月 14 日，奇安信 CERT 监测到 Openfire 身份认证绕过漏洞 (CVE-2023-32315)，由于 Openfire 的路径名限制不恰当，未经身份认证的远程攻击者可以构造恶意请求利用该漏洞，成功利用此漏洞可以绕过身份认证登录管理界面。目前此漏洞的 PoC 与技术细节已在互联网上公开，漏洞的现实威胁进一步上升。鉴于此漏洞影响较大，建议客户尽快做好自查及防护。

Fortinet FortiOS SSL-VPN 远程代码执行漏洞安全风险通告

6 月 12 日，奇安信 CERT 监测到 Fortinet FortiOS SSL-VPN 远程代码执行漏洞 (CVE-2023-27997)，在 Fortinet FortiOS SSL-VPN 中存在一个基于堆的缓冲区溢出错误，允许未经身份验证的远程攻击者通过特制请求使设备远程崩溃，并可能执行任意代码。鉴于此漏洞影响较大，建议客户尽快做好自查及防护。

畅捷通 T+ 多个高危漏洞安全风险通告

6 月 12 日，奇安信 CERT 监测到畅捷通 T+ 反序列化漏洞 (QVD-2023-13615)、SQL 注入漏洞 (QVD-2023-13612)。基于 QVD-2023-13615，未经过身份认证的攻击

者可以通过构造恶意的请求在目标服务器上执行任意命令；基于 QVD-2023-13612，远程未授权攻击者可利用此漏洞在目标系统执行任意 SQL 语句，最终实现远程命令执行。奇安信 CERT 已成功复现上述漏洞，鉴于上述漏洞的技术细节或 PoC 已在互联网上公开，现实威胁上升，建议客户尽快做好自查及防护。

Windows Win32k 权限提升漏洞安全风险通告

6 月 9 日，奇安信 CERT 监测到 Windows Win32k 权限提升漏洞 (CVE-2023-29336) 的技术细节和 PoC 已在互联网上公开，由于 Win32k 中存在释放后重用漏洞，经过身份认证的本地攻击者可以构造恶意程序触发该漏洞，成功利用此漏洞可以提升权限至 System 或造成系统崩溃。目前，奇安信 CERT 已成功复现此漏洞。鉴于此漏洞影响较大，且存在在野利用，建议客户尽快做好自查及防护。

GeoServer SQL 注入漏洞安全风险通告

6 月 9 日，奇安信 CERT 监测到 GeoServer SQL 注入漏洞 (CVE-2023-25157)，由于系统未对用户输入进行过滤，远程未授权攻击者可以构造特定语句绕过 GeoServer 的词法解析，从而实现 SQL 注入，成功利用此漏洞可获取敏感信息，甚至可能获取数据库服务器权限。由于 GeoServer 在默认配置下内置图层存放数据在文件中，则未使用外置数据库的场景不受此漏洞影响。奇安信 CERT 已成功复现该漏洞，鉴于该漏洞的 PoC 已在互联网上公开，现实威胁上升，建议客户尽快做好自查及防护。

Google Chrome V8 类型混淆漏洞安全风险通告

6 月 7 日，奇安信 CERT 监测到 Google Chrome V8 类型混淆漏洞 (CVE-2023-3079) 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，建议客户尽快做好自查及防护。

Nacos 集群 Raft 反序列化漏洞安全风险通告

6 月 6 日，奇安信 CERT 监测到 Nacos 集群 Raft 反序列化漏洞 (QVD-2023-13065)，在 Nacos 集群处理部分 Jraft 请求时，攻击者可以无限制使用 hessian 进行反序列化利用，最终实现代码执行。奇安信 CERT 已成功复现该漏洞，鉴于该漏洞仅影响集群间通信端口 7848（默认配置下），若部署时已进行限制或未暴露则风险可控，建议客户做好自查及防护。

Apache RocketMQ 远程代码执行漏洞安全风险通告

5 月 31 日，奇安信 CERT 监测到 Apache RocketMQ 远程代码执行漏洞 (CVE-2023-33246)，在 RocketMQ 5.1.0 及以下版本，在一定条件下，存在远程命令执行风险。RocketMQ 的 NameServer、Broker、Controller 等多个组件暴露在外网且缺乏权限验证，攻击者可以利用该漏洞更新配置功能，以 RocketMQ 运行的系统用户身份执行命令。此外，攻击者可以通过伪造 RocketMQ 协议内容来达到同样的效果。奇安信 CERT 已成功复现此漏洞。鉴于该漏洞影响较大，建议客户尽快做好自查及防护。

GitLab 目录遍历漏洞安全风险通告

5 月 24 日，奇安信 CERT 监测到 GitLab 目录遍历漏洞 (CVE-2023-2825)，当嵌套在至少五个组中的公共项目中存在附件时，未经身份验证的恶意用户可以利用该漏洞读取服务器上的任意文件。目前奇安信 CERT 已成功复现该漏洞。鉴于该漏洞影响较大，建议客户尽快做好自查及防护。

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

对抗篇

国内攻防演习 5 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5月，奇安信Z-TEAM团队共承接攻防演习服务 26 场，其中省级攻防演习 1 场，地市级攻防演习 2 场，客户自主攻防演习 23 场。

本月承接攻防演习数量与上月对比呈下降趋势（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大体相同，部分类型活动数量略有不同（见图 2）。

本月攻防演习成果如表1所示。

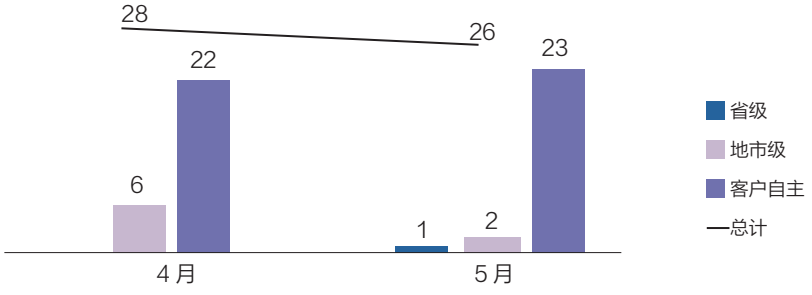


图 1 4-5 月 Z-TEAM 承接攻防演习数量统计

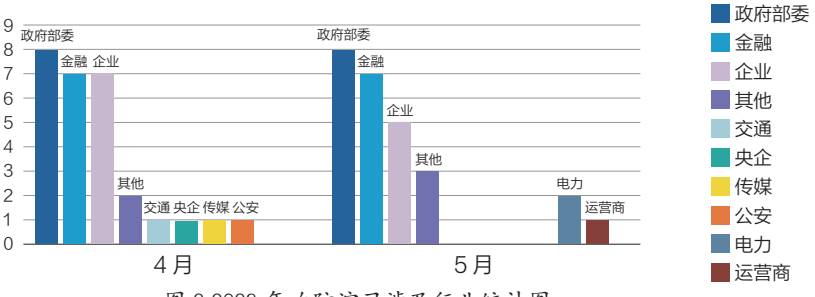


图 2 2023 年攻防演习涉及行业统计图

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	26	44	71	57	64	102	601	1712

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、电力、运营商、物流等行业。随着经济全球化的发展，物流业发展迅速。在国民经济中发挥着越来越重要的作用，近年来我国物流业迅猛发展，企业数量不断增加，业务规模不断扩大。同时，由于互联网和信息技术的迅速发展，物流行业网络安全问题日益凸显。物流行业作为网络安全问题较为突出的行业之一，其网络攻击面较广、攻击手段多样、隐蔽性强，给网络安全带来了极大的挑战。因此，物流行业需要采取强有力的网络安全措施。物流行业在本月攻防演习中占比为 4%（见图 3）。

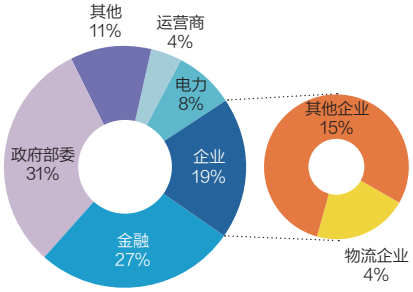


图 3 5 月攻防演习分布图

本月攻防演习服务中，攻击队使用的攻击手段主要有：漏洞扫描利用、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 VPN 仿冒接入利用率基本趋同，口令爆破有明显下降趋势，钓鱼攻击和隐秘隧道外联手段有明显上升趋势（见图 5）。

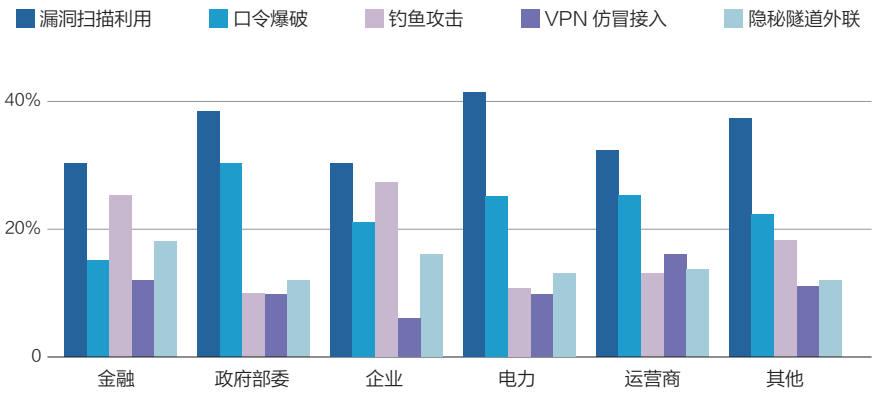


图 4 行业攻击手段分布图

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，本月任务中主要针对多行业不同目标网络，使用的攻击手段也有所不同，如政务、电力、其他行业外网突破的主要手段包括漏洞扫描利用和口令爆破等；企业行业主要是钓鱼攻击和隐秘隧道外联等；金融、运营商行业外网突破的主要手段包括漏洞利用、钓鱼攻击和 VPN 仿冒接入等。各个行业使用的主要技术手段分布如下（见图 4）。

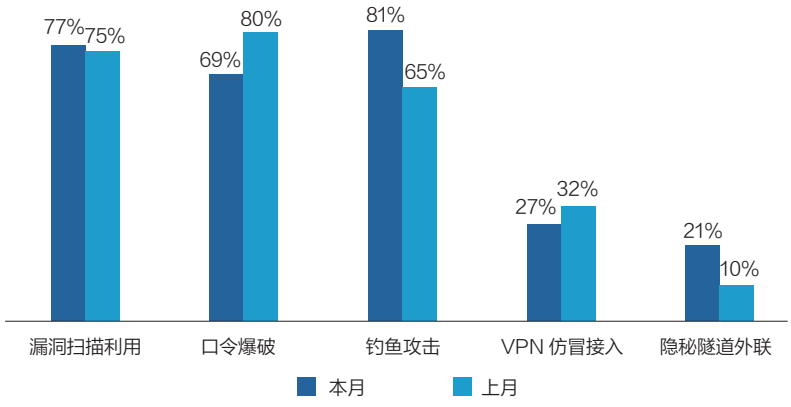


图 5 攻击手段对比图

本月任务中物流行业攻防演习任务占企业行业攻防演习任务的四分之一，通过针对该行业的演习数据分析发现，攻击队外网纵向突破重点寻找薄弱点，围绕薄弱点利用历史漏洞攻击手段结合钓鱼攻击实现突破；内网横向移动以突破点为支点，利用反向代理攻击手段在内网以点带面实现横向拓展遍地开花，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、安全防护建议

在上述攻击案例中，我司攻击队员充分利用水坑攻击、供应链攻击等手段，突破了防守单位层层安全防线，最终控制了核心业务平台和整个办公域。

通过此次水坑攻击实践，物流公司除了应加强自身网络和应用系统安全防护建设（如供应链安全防护、漏洞安全检查、账号口令管理等），亟须对水坑攻击开展安全风险排查工作，避免水坑攻击防护成为安全防御体系的短板。水坑攻击安全防护建议如下。

· 安装终端防护软件

安装终端防护软件，监测、阻断不可信的网络安全访问行为；及时更新升级应用程序，修复已知 / 未知漏洞。

· 网络流量全面监测

传统基于特征签名的安全监测类设备，无法有效监测复杂的水坑和其他攻击，建议部署高级威胁监测类设备，监测水坑攻击网络传输流量，经大数据分析、威胁情报等技术，清晰描述攻击路径、定位到终端，形成威胁告警信息。

· 提升安全防范意识

对全员开展社工攻击安全意识培训，了解社工攻击类型、危害及防护措施，提升全员安全防范意识。必要或条件允许的情况下，可开展模拟社工攻击测试，如水坑攻击测试、钓鱼邮件测试等。安

四个故事
聊清数据安全风险

偷瞄同事薪资单，险酿数据安全事故；家贼难防，竞争对手窃取企业标书；数据被加密，企业遭遇巨额勒索；企业数据泄露，总裁遭处罚。四个来自业务场景的鲜活故事，充分展示了数据安全的主要风险，以及如何看清风险、管好访问、防住攻击和实现合规。

看了同事薪资单，结果触碰了数据安全红线，冤不冤？

作者 | 魏开元

“我就把号借给 xxx 玩了一次，然后就被盗了。”相信大多数游戏玩家即便没有以上经历，也听说过类似的故事。显而易见，将账号随意借给他人使用，将大幅提高账号内资产、数据失窃的概率，不法份子可以不借用任何技术手段，即可轻易达成目标。针对海量的数据泄露事件的研究表明，因凭据的失窃或滥用已经成为近年来数据失窃的最主要因素。

但对政企机构而言，针对敏感系统账号、权限的管控却并非易事。随着信息化、数字化建设的不断深入，企业数字资产不断增多，相应地，账号登录权限也随着员工的流动不断发生变化，非常容易出现监控的盲点，导致账号滥用和越权访问寻行为的出现。

敏感系统的违规访问

出于便利性的原因，国内某家具备一定规模的电商直播公司，一直存在着域账号共享的现象。然而在某月工资发放之后，网络安全部在日常运营监测过程中发现，个别员工登录了其他员工的域账号，并在内网系统中查看了他人的薪资单。

“我们通过日志，很快就定位到了违规登录他人域账号、查看他人工资单的员工。”该公司网络安全部运营工程师表示，结合多源日志分析，其中一位违规员工使用私人电脑，在家里连接 VPN 访问了其他员工的薪资单，并

在薪资单页面停留了较长时间；另一位员工则是在公司内部登录了他人的域账号，并访问了薪资单。

众所周知，许多公司都将薪资单设置为内部的数据安全红线，禁止员工私自共享薪酬信息。而在此次事件中，违规员工就通过共享的域账号，违规访问了他人的薪资单，触碰了公司数据安全红线。

尽管从结果来看，该事件并没有造成较为严重的后果，但域账号如果在共享过程中被外部攻击者窃取，就有可能会造成很严重的数据泄露事件。因此，除了完善相关的规章制度、提升员工的数据安全意识，还应当采取适当的技术手段，及时发现并阻断违规访问等高危行为。

全链路监测应对数据安全高危行为

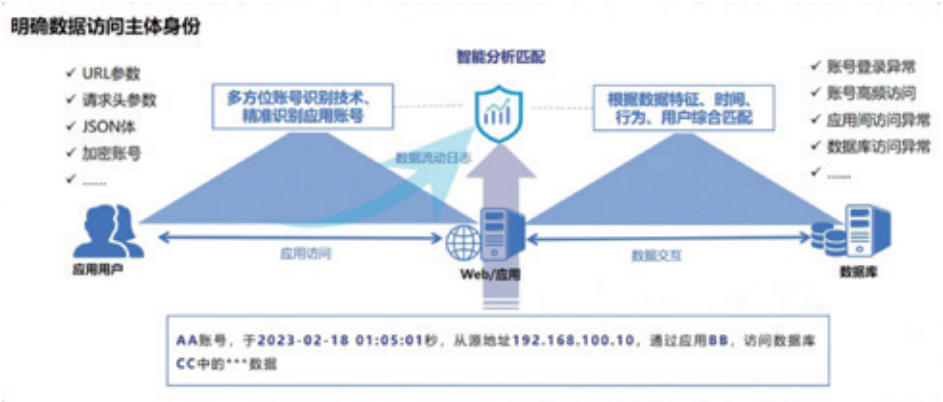
不久前，奇安信发布了奇安天盾数据安全保护系统（以下简称奇安天盾），它基于“全链路监测、全穿透识别，全兵种协同、全闭环处置及全天候控制、全场景防护”的六全框架，以“数据资产”为核心，将“事件监测、风险分析、策略调整、访问控制”融为一套完整闭环体系，做到了三能：数据安全风险能看清，内鬼能管好，攻击能防住。

在此次事件中，奇安天盾展现了强大的风险监测能力，能够通过多种监测组件，帮助安全运营人员看全数据流转和访问的完整路径，明确数据访问主体身份，及时发现数据流转各个环节的潜在风险和针对敏感数据的异常访问行为。

正因如此，安全运营人员才能第一时间掌握是谁违规访问了他人的薪资单，并且知道是通过什么渠道访问的。

当然，针对账号和权限的监测与管控并非数据安全的全部。奇安信数据安全产品总监王弢表示，作为一种新型生产要素，数据的流转在管理者、经营者、使用者的不同的载体上处理，数据涉及到个人数据、商业数据、公共数据，甚至是机密数据，数据复杂的流转带来更多的安全风险，而奇安天盾弥补了对于数据保护的事件监测、风险分析、策略调整、访问控制一体化能力的缺失。

显而易见，薪资单泄露仅仅是数据安全风险的冰山一角，数据安全是一项极其复杂的工作，只有一套体系化的安全保护能力，才能应对新技术新场景下的新威胁和新挑战。 安



图：对多源数据进行关联分析，实现全链路数据流动监测

办公室深夜惊现神秘黑影，2 天后公司重要数据丢失，谁是真凶?

作者 | 张少波

“千防万防，家贼难防”。因为内部人员故意或者无意将重要数据泄露给商业竞争对手，导致商战中满盘皆输的例子，屡见不鲜、比比皆是。此前，奇安信曾分享过一个真实的数据泄密案例，国内某家大型地产公司，一位管理 AD 域的员工离职后，将账号密码贩卖给竞争对手，然后竞争对手用这个账号登录到该公司内网，把这家地产公司的经营数据一股脑儿全部拿走，最终给这家地产公司造成了重大损失。

2022 年，中国裁判文书网披露的一起华为前员工数据泄露刑事案件也引发了舆论关注。刑事裁定书显示，华为某员工调离岗位后未清理 ERP 登录信息，利用 bug 越权访问，将所获得数据透露给华为供应商、上市公司金信诺，最终因非法获取计算机信息系统数据罪被判处有期徒刑。在该案中，由于企业数据权限管理上的漏洞，导致了整个数据泄露事件的发生。

根据 Verizon 近日发布的第 16 份年度数据泄露调查报告 DBIR 显示，所有违规行为中有 74% 属于人为因素，人们通过错误、特权滥用、使用被盗凭据或社会工程参与其中。其中，内部员工的违规操作成为重要原因之一。

近年来，数据泄露越发猖獗，因内鬼造成的数据泄露所造成的损失也在不断走高。奇安信认为，随着数据的流动性不断加强，数据作为重要资产，不仅在内网，也在外网、云上、数据库里。接触数据的人变多，监控范围和身

份验证难度加大，“内鬼”管控难度随之提升。

奇安天盾，用体系化能力应对数据泄露难题

奇安信数据安全产品总监王弢表示，在安全风险复杂、合规性要求越来高的背景下，需要一套体系化的安全能力应对新技术新场景下的新挑战。

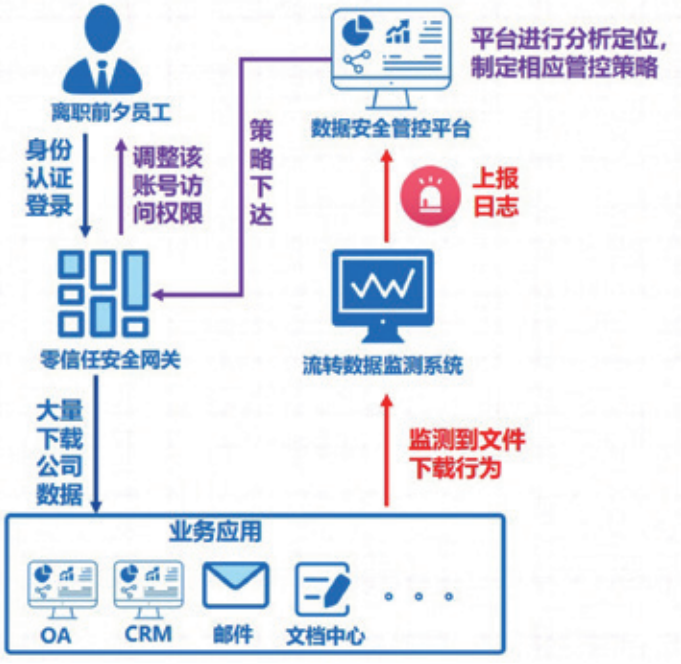
不久前，奇安信发布了奇安天盾数据安全保护系统（简称奇安天盾），它基于“全链路监测、全穿透识别，全兵种协同、全闭环处置、全天候控制、全场景防护”的六全框架，以“数据资产”为核心，将“事件监测、风险分析、策略调整、访问控制”融为一套完整闭环体系，做到了三能：数据安全风险能看清，内鬼能管好，攻击能防住。

在事件监测方面，奇安天盾实现了数据安全的全链路可视。在风险分析方面，奇安天盾能基于场景的建模，多源数据的关联分析，对用户登录活动、访问行为、数据库查询、API 调用等监测数据进行关联分析。在策略动态调整方面，奇安天盾面向 5W1H 的细颗粒度访问控制策略，提升风险响应实时性。在访问控制方面，奇安天盾将丰富的管控手段和安全防护能力内置到了数据流转的各个环节，帮助客户实现全天候控制、全场景防护。

拿一个案例来说，某公司员工准备跳槽到友商，离职前夕，利用合法的身份账号，访问公司业务系统，大量下载公司核心业务文件。针对这些问题，奇安信通过奇安天盾的流转数据监测系统，发现该账号的数据下载异常行为，及时向数据安全管控平台上传告警信息，平台进行分析后制定针对该账号的管控策略，并下达给零信任安全网关，零信任安全网关调整该账号访问权限，限制访问。

在这个过程中，奇安天盾的监测、分析、调整、控制等四项核心能力都得到充分使用。通过奇安天盾的数据流转链路可视，及时发现可疑的数据泄露行为和违规操作行为，降低了用户发生数据安全风险的概率。同时，风险事件发生后，第一时间进行告警并指定策略进行管控，避免损失扩大。

数据安全是一项极其复杂的工作，只有一套体系化的安全保护能力，才能应对新技术新场景下的新挑战。通过部署奇安天盾，可以对内鬼实现有效的管控，最大程度降低数据外泄的风险。 安



图：对离职员工的数据泄露风险防范

数据被“绑架”！工资不能按时发，这家企业该不该支付巨额赎金？

作者 | 闫延

今年 3 月，“高大上”的法拉利（Ferrari）遭遇勒索攻击。黑客入侵其系统并窃取了部分用户数据，包括姓名、地址、电子邮箱和电话号码等，借此勒索高额赎金。而类似戏码半年前就在该公司上演过一次。无独有偶，去年底国内某新派造车企业被破解了员工数据、车主用户身份证数据 40 多万条，遭到 225 万美元等额比特币勒索。车企遭遇的勒索事件，就是数据安全外部攻击频发的一个缩影。

目标：数据资产成为攻击重点

目前，工业互联网、智能系统等都需要数据互联互通，一旦勒索病毒进入攻击阶段，管理员处理攻击的窗口非常短，勒索病毒很快会蔓延开来，导致整个数据资产遭到威胁，后果非常致命。

更为雪上加霜的是，数据安全面临的攻击往往是复合的、激烈的，在人工智能技术的推波助澜下，黑客的水平跃升，攻击手法不断升级翻新、变幻莫测。比如，勒索攻击者正在大量应用间歇性加密来快速加密受害者的文件，更快的加密速度越快更难被检测与拦截；间歇性加密还可以有效规避统计分析的检测。此外，还要注意数据 API 化带来的安全风险，许多核心业务数据、个人身份信息等由 API 传输，流动性大为增强，外部恶意攻击者会利用 API 接口批量获取敏感数据。数十家全球顶级汽车制造商生产的车辆和车联网服务中，发现了

奇安天盾

能看清、能管好、能防住

数据安全保护系统全面上市!

API 应用缺陷，攻击者可利用缺陷非法窃取车主个人隐私信息，远程解锁车辆、监控车辆等。

后果：损失难以估量

据安全公司 Coveware 统计，2022 年勒索平均赎金高达 226,710 美元，同比增长 35%。事实上，除了支付“赎金”的直接损失，外部攻击带来的损失还应计入数据丢失、生产力下降、潜在收入损失甚至名誉损害等负面影响。比如，去年底某新派造车企业数据安全事件发酵为舆论事件，迅速在汽车圈里炸锅，引发车主群体的担忧。

更令人担忧的是，关键性基础设施仍是数据外部攻击的重点攻击目标。Check Point 发布的研究报告显示，包括能源、医疗保健和制造业在内的关键行业成为勒索软件的高度攻击目标。2020 年 2 月 18 日，黑客加密了美国某天然气管道运营商 IT 和 OT 系统中的数据，导致整个管道关闭了两天。可以设想，此次攻击事件将会给当地人的生活造成多大的不便。

奇安天盾方案：企业需要全链条防护能力

由于新兴技术越来越复杂、业务系统越来越复杂、数据种类越来越复杂数据流转越来越复杂，传统安全手段已难以抵御外部攻击，体系化的安全能力亟待实现。奇安信发布的“奇安天盾”数据安全保护系统，将丰富的管控手段和安全防护能力内置到了数据流转各个环节，无疑是实现这一能力的有效抓手。

实践中，“奇安天盾”的“三能”目标——能看清、能管好、能防住，其中“能防住”无疑是底线要求之一。实现“能防住”的手段，则是全天候控制、全场景防护，将安全能力内置到网络全链条中、内置到数据要素流动的各种场景中，第一时间发现各种各样的数据安全风险，依据场景进行针对性地风险分析，快速定位涉事主体，及时响应、快速处置，解决各种主要的数据外部攻击问题。

奇安信数据安全产品总监王弢表示，数据安全与网络安全是分不开的，做好数据安全，需要建立纵深防御的内生安全体系，当一道防线被突破，还有下一道防线来阻止威胁，整合监测、研判分析、处置、溯源等多层面的安全能力，配合多个数据安全保护组件，才能最大程度降低各种攻击带来的数据安全风险，更好地落实数据安全的全生命周期防护。

王弢认为，勒索攻击只是企业数据安全所面临的众多外在风险之一，只有依托奇安天盾构建体系化的数据安全保护能力，才能应对新技术、新场景、新合规要求下的全新挑战。 安

合规无小事，因为数据泄露，总裁竟然要被处分？

作者 | 张少波

数据安全千万条，坚守合规第一条。近年来，因数据安全不合规被重罚的案例屡见不鲜。不久前，脸书（Facebook）的母公司 Meta 因将用户信息发送至美国，被欧盟隐私监管机构罚款 13 亿美元。这笔罚款是根据欧洲标志性数据隐私法《通用数据保护条例》（GDPR）所征收的最高额罚款，这是迄今为止对科技公司处以的最大罚款。

而在 2022 年 7 月，国家互联网信息办公室依据《网络安全法》《数据安全法》《个人信息保护法》等法律法规，对国内某出行巨头处以人民币 80.26 亿元罚款，堪称国内个人信息保护的首单顶格处罚案例，充分体现了“合规不踩线”是企业经营的重要基石。

主体责任未压实是重要原因

面对复杂而严峻的数据安全威胁形式，当前我国各个行业的合规落地、仍存在诸多软肋和不足，而其中最核心的原因，表现在主体责任未压实。

2021 年 9 月 1 日《数据安全法》正式实施，该法律作为数据领域的“上位法”，确定了数据流转过程中组织、个人的安全责任和义务，明确了监管要求。同时，作为纲领性法规，为各部门、各行业、各领域在后续制定相关配套制度、措施、规范和标准过程中指明了方向，尤其强调了对主体责任的压实，推动合规建设进入快车道。

2023 年 1 月 1 日， 工业和信息化部出台的《工业和信息化领域数据安全管理办法（试

行）》（简称《管理办法》）正式实施。该办法明确了工业和信息化部和地方行业监管部门承担工业和信息化领域数据安全的监管职责，要求相关企业健全数据安全管理和技术保护措施及履行主体责任，全面提升数据安全的保护能力，助推数字经济高质量发展。

《管理办法》提出，涉及重要数据和核心数据的，应当建立覆盖本企业相关部门的数据安全工作体系，设置专门的数据安全管理责任部门，企业党委或领导班子对数据安全负主体责任，主要负责人是数据安全第一责任人，分管数据安全的负责人是直接责任人，明确各部门数据安全职责及人员，建立常态化沟通与协作机制。

奇安信集团副总工兼首席数据安全专家刘前伟认为，企业“一把手”成为数据安全第一责任人，对于压实责任具有非常重大的意义。组建“数据安全合规专项工作组”，数据合规通过一把手领导牵头，建立一个横跨公司管理、法务、技术、业务等多个部门的综合组织，才能将数据安全合规工作责任落到实处，满足监管需求，并避免安全和业务相脱节。

数据安全合规建设 需要系统性构建保护体系

做好数据安全合规建设，不仅仅是有一个产品，也不是简单的产品堆砌，需要基于数据访问生命周期风险分析，系统性地构建数据安全保护体系，解决各种数据安全的难题。

不久前，奇安信在 2023 数博会上重磅发布奇安天盾数据安全保护系统（简称奇安天盾），用“六全”框架实现“三能”：能看清、能管好、能防住；一个系统解决各种数据安全问题，并根据不同的场景化需求，实现“安全合规不踩线、业务数据不出事、预算投入不设限”。

以数据跨境传输为例，奇安天盾通过部署跨境数据监测系统组件，可以第一时间监测到高敏数据违规出境，将该告警信息上传到数据安全管控平台进行分析和策略调整，零信任安全网关调整该账号访问权限，限制其后续的访问，避免类似事件的发生。

刘前伟认为，数据安全要做到持续合规，除了产品技术和运营，管理、组织、制度流程也至关重要。由于数据在各业务系统之间流转，需要设立高级管理层参与决策的数据安全管理部门，统筹和规划多部门之间的工作；需要设立跨组织的数据管理协调部门，确保制度、流程、技术等方面的落地。

在这个过程中，除了企业和监管单位的努力，还需要充分借助外部的专业力量，依托专业数据安全公司，以及第三方法律机构的参与和支持，对合规制度流程不断完善，对人员技术能力不断提升，对各类安全风险持续跟踪及修复，才能从长远角度提升企业的数据安全水平，确保 “安全合规不踩线”，保障数字化行稳致远。 安

数据安全面临七大风险，应对需实现三大转变

作者 | 奇安信产研中心　产品战略市场部　陈华平　刘前伟　杜勇

一、数据要素成最活跃的新型生产要素，数据安全就是国家安全

数据要素作为兼具优化传统行业生产方式、促进新兴科技行业发展的基础性、战略性资源，已成为各国抢占数字经济发展机遇的重要抓手。

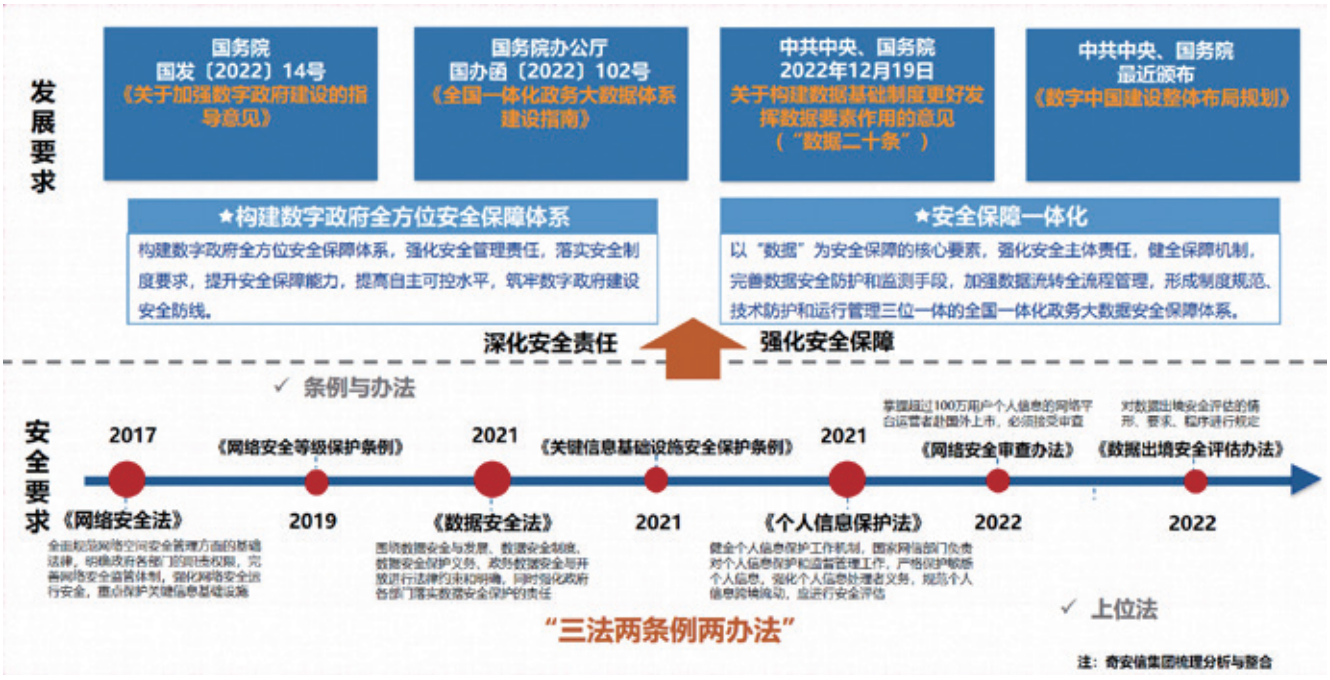
在全球数字化浪潮驱动之下，我国把深化政府数字化转型、打造数字化产业、产业数字化纳入到“十四五”整体战略部署及 2035 远景规划中，数字化理念、数字化战略、数字化基础设施、数字化产业在各地各行各业开枝散叶、落地实践，其中“数字中国”是总纲，与“数字政府、数字经济、数字社会、数字生态”共同构筑了中国数字化转型的“一体四翼”。

在加快数字中国建设的时代背景下，数据作为一种新的生产要素走到台前，数据要素作为基础性和战略性资源，被政府部门和市场主体寄予了推动产业升级、优化经济结构和创造经济增长点的厚望。据统计，2020 年我国“数字产业化”规模达 7.5 万亿元，占 GDP 比重 7.3%，“数字经济”规模突破 39 万亿元，而到 2021 年底，我国的“数字经济”规模就已增长到 45 万亿元，占 GDP 的比重也提升到了 39.8%，数字经济对我国 GDP 增长的贡献率达到 60% 以上。

在我国数字经济和信息产业蓬勃发展的同时，伴随着越来越多的数据产生和流动，数据应用范围更加广阔，应用场景更加丰富，数据安全面临的风险越来越高，数据泄露、数据滥用、数据损毁、数据篡改等威胁日益凸显，有的是个人隐私，泄露后会影响生活甚至生命财产安危；有的是商业秘密，如技术资料、经营数据、用户数据等，泄露可能让企业研发投资付之东流；有的是国家机密，泄露后甚至会危及国家安全。数据安全现已成为关系个人权益、公共利益和国家安全的重要因素。

与此同时，随着国际形势越发严峻，数据要素价值凸显，境外保护主义盛行，数据安全往往成为部分西方国家打击和遏制我国以数据为核心的数字经济新业态、新模式、新技术创新发展的借口和工具，针对以上情况，国家出台了一系列数据安全相关的法律法规，笔者认为，

> 数据资产成为国家的战略资源和核心资产，
> 数据安全脱离单独的个人或企业层面，
> 已经涉及影响国家安全的层面。



这些都体现了数据合规升级、数据监管趋严的宏观趋势。

目前，全国 31 个省（自治区、直辖市）均已结合政务数据管理和发展要求，制定了数据发展规划和政策措施。同时，组织实时政务数据采集、归集、治理、共享、开放和安全保护等工作，统筹推进数据资源开发利用。

二、数字安全面临七大主要风险

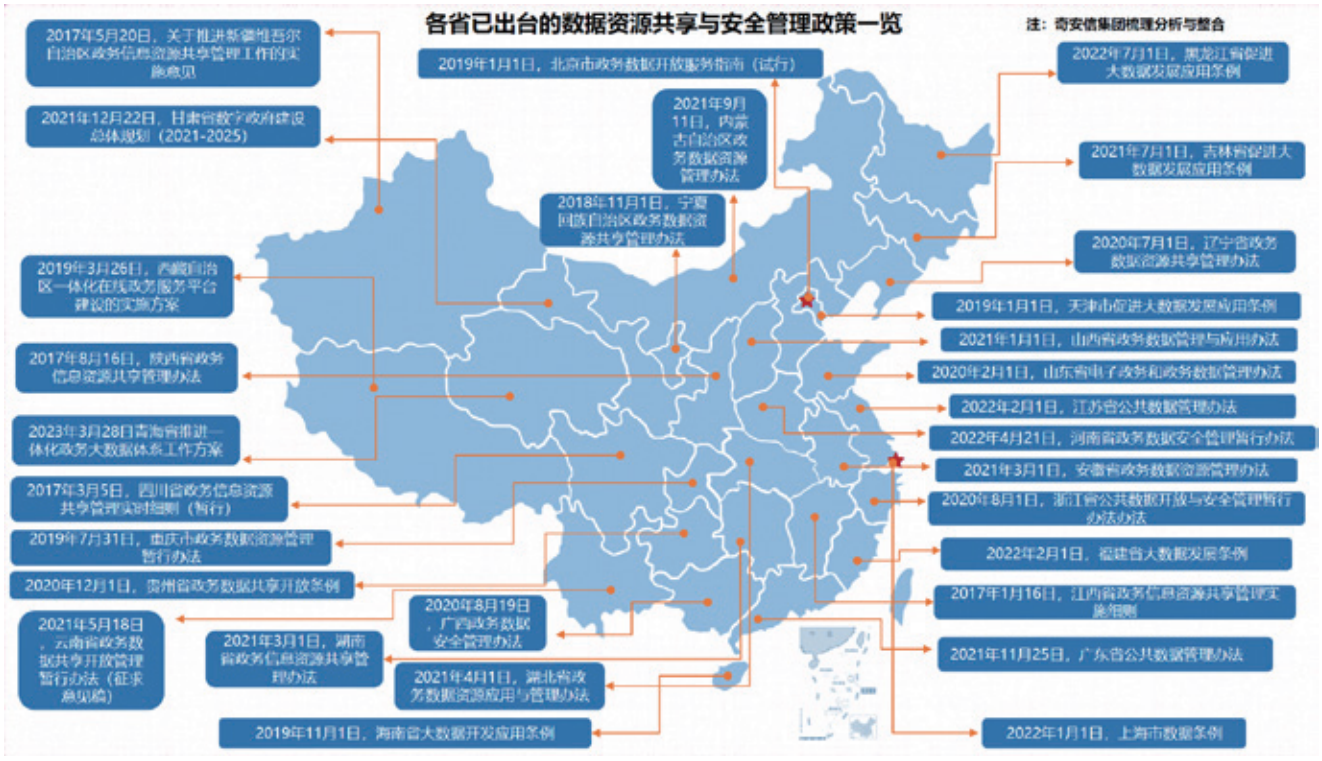
随着数字经济时代的到来，数据资产成为国家的战略资源和核心资产，数据安全脱离单独的个人或企业层面，已经涉及影响国家安全的层面。我们在数据释放价值的同时，如何应对严峻的数据安全形势，满足合规监管要求，笔者认为，需要明晰数据安全风险与问题有哪些。

（1）数据资产梳理不清和分级分类不准带来的安全死角问题

参与流通的数据形态日益丰富，数据资产梳理和分级分类难度加大，极易产生安全死角。传统的数据分析方法和工具，难以从非结构化数据中识别信息内容和重要程度。在规则制定方面，各地区各部门对数据分级分类制度的定位和规则存在差异，同时，数据的级别、类别需要结合业务场景进行动态调整，在不同场景下的等级认定及相应的管控或处理技术可能不同，数据分级分类的持续性难以保持。

（2）数据泄露风险是当今突出的数据安全问题

在数据使用过程中，数据泄露风险是目前重要的数据安全问题。在数据大量流动和使用的过程中，可能会因为网络安全漏洞或人为失误而导致数据泄露。例如，黑客或不法分子可能会通过攻击企业的系统，窃取企业活动数据和用户数据，并用于恶意目的。对个人来说，数据泄露可能会导致个人信息泄露，个人隐私遭到侵犯；对企业和组织来说，数据泄露可能会导致商业机密和交易数据泄露，进而造成经济损失或声誉损失。



（3）数据滥用风险是急需治理的数据安全问题

数据滥用风险也是当前数字经济发展急需治理的数据安全问题之一。数据滥用风险是数据收集者不当使用所收集的数据的风险。伴随着数字经济逐步渗透至各种生活场景，用户信息被大量收集。数据收集者利用收集的信息进行商业欺诈或不当广告投放，对个人隐私和用户利益造成严重损害，破坏了商业活动规律。

（4）场景化应用的数据安全风险

“场景化业务应用”作为推进数字化变革的重要应用载体，面向企业、大众提供各类服务，在“场景化”开发过程中常会碰到因为安全因素考虑不够周全或缺失，或者存在业务逻辑缺陷等导致的自身安全风险，同时也会带来诸如恶意破解、核心代码被窃取、恶意代码注入、数据泄露、内容篡改、互动关联、认证风险等一系列安全问题。

（5）数据共享交换的数据安全风险

数据要素市场建设加速推动了数据共享、交易和使用，尤其在数字政府建设过程中，数据来源多样、权属不同，且为了实现“让数据多跑腿、百姓少跑路”的目标，对数据共享的需求十分强烈。这导致在数据采集、共享、传输、应用过程中涉及非常多的主体，容易导致数据安全管理责任不清晰。而且由于各个政府部门，特别是基层单位的防护能力参差不齐，在共享过程中一旦薄弱部位被利用，就可能引发全局渗透风险。同时，由于数据流转链路增长，也进一步加大了数据流向和使用追踪难度。

（6）数据 API 化的数据安全风险

在共同建设信息基础设施、融合基础设施及创新基础设施的背景下，需要连通不同类型的设施和应用，使得各类

数据、算力和功能够在不同的区间内形成高效共享，API 作为能够支撑线上应用连接和数据传输重任的一种轻量化技术，其应用越来越普遍。由 API 传输的核心业务数据、个人身份信息等数据的流动性大大增强，因此这些数据面临着较大的泄漏和滥用风险，成为数据保护的薄弱一环，外部恶意攻击者会利用 API 接口批量获取敏感数据。从“数字生态”角度看，目前数据的交互、传输、共享等往往有多方参与，涉及到用户、应用方、关联方等多个主体，由此使得数据泄露风险点激增，风险环境愈发复杂。

（7）新技术应用的数据安全风险

由于 AI 技术的普及、算法的滥用和深度伪造等新技术带来的大量真假难辨的新闻事件，增加了辨别网络舆情真伪的困难度，增加了侵权案件、隐私泄露事件的发生，降低了恶意攻击成本、增加了隐蔽性，同时，增加了政府管理难度、危害国家社会民众利益。

三、夯实数字化时代数据安全防护体系的思考与建议

针对上述数据安全风险和问题，如何管好数据、用好数据、治理好数据、平衡好数据应用和安全防护、激发数据应用潜能，是我们夯实数字化时代数据安全防护体系的初衷，我们需要从传统的以数据承载环境为中心的“系统视角”向以数据全生命周期流转为中心的“业务视角”转变；我们需要从强调技术向“技术”与“管理”并重思路转变，把“技术”作为“管理”的延续，进而制定相应的管理机制；我们需要结合具体场景、行业特性、数据属性量等，综合制定数据安全目标和工作任务。

首先，先理后治、补短固底。“盘家底、补短板”，是数据安全的当务之急，是数据安全防护体系建设的基础。

（1）区别于合规要求的网络安全建设，数据安全防护体系应建立在事实依据的基础上，才能对自身业务最核心的数据安全风险采取技防监测、控制手段解决，所以第一步，即开展数据风险发现过程——数据安全治理评估。

（2）通过数据安全治理专家团队，从业务视角出发，对业务应用的现状、使用情况进行调研、分析，确定业务的关联关系、访问的关键路径、数据的流向及演变过程，结合对基础安全管控措施的分析，找出主要业务所面临的管理、技术及运营风险。

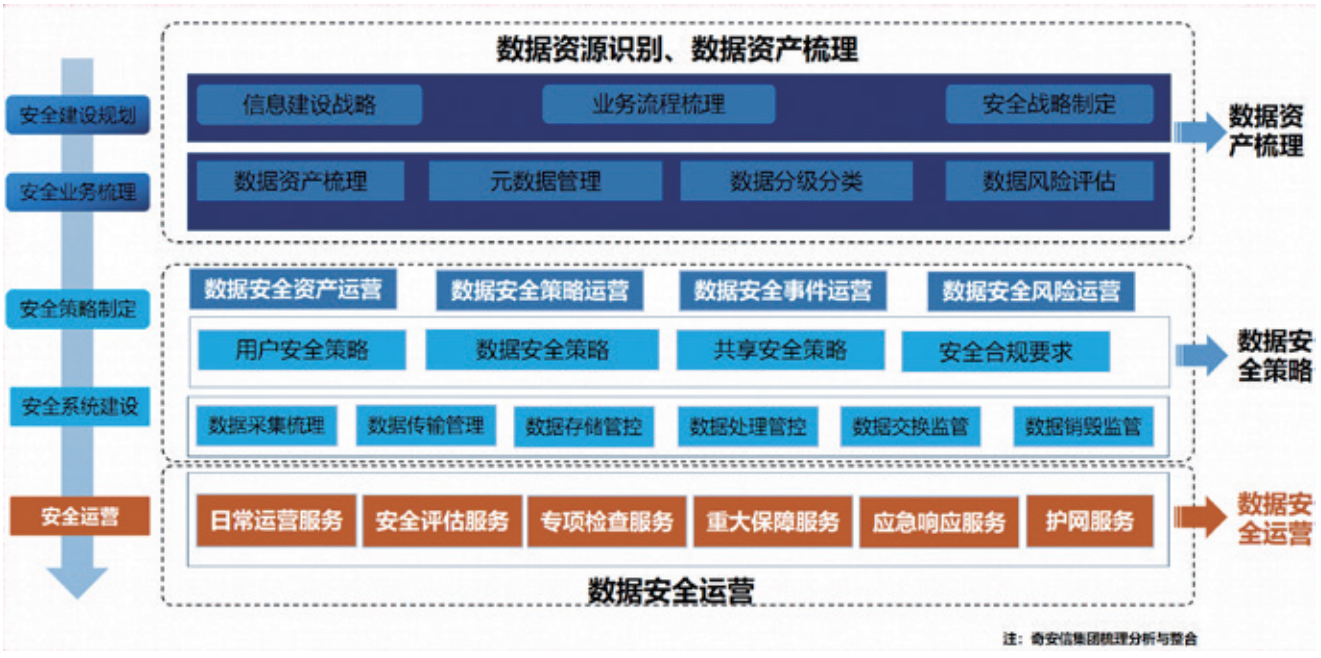
（3）集合多个业务系统的调研结果，找出系统间的共性问题，为制定业务的数据安全管理规范提供第一手的参考依据。针对业务各系统及数据资产全面开展评估梳理工作，形成《数据资产清单》，明确相关平台各系统的输入、输出，数据所在位置及其处理、共享、交换等使用过程中数据重要度等内容。

（4）围绕“重要数据资产”建立“高防区”，做访问控制设计、堡垒机、特权账号管理（含密码保险箱）、API 安全、数据库审计、数据安全态势感知、终端管控等，形成“急用先行”的落地方案，守住数据安全的第一道关口。

其次，系统治理、体系规划。开展数据安全治理和分级分类，建立制度、流程、规范等，以分级分类为基础，进行数据安全管理体系、技术防护体系、运营体系的规划和设计。

（1）数据分级分类的梳理是数据安全治理工作的核心，通过对数据资产进行分类和安全等级定义，支撑全生命周期过程、各业务场景下数据差异化的安全策略设置。基于分级分类结果并结合业务逻辑、数据流转，根据数据级别制定相应的分级管控与防护策略，包括管理策略和技术防护策略。

（2）数据安全防护体系的规划需



要从业务数据安全需求、数据安全风险控制需要及法律法规合规性要求等几个方面进行梳理，最终确定数据安全防护的目标、管理策略及具体的标准、规范、程序等。

（3）数据安全管理机制的设计是一项需要多方联动型的复合型工作，在开展组织架构建设时，需要考虑组织层面实体的管理团队及执行团队，同时也要考虑虚拟的联动小组，所有部门均需要参与到安全建设当中。同时，需要根据部门职责建立不同的数据安全角色，以满足数据安全建设的需求。

最后，有序建设、持续运营。依据整体规划和设计，分步骤、分阶段有序开展建设，持续运营，保障数据持续安全状态，包括数据资产安全运营、数据安全策略运营、数据安全事件运营和数据安全风险运营。

（1）依托专业业务团队 + 数据安全技术团队 + 平台支撑工具 + 数据运营流程 + 制度机制保障，构建“数据归心”的一体化数据安全运营体系，通过梳理明晰数据资源、实现数据资源资产可用、数据共享交换可信、数据传输环境可靠。

（2）针对公共服务数据、重要应用数据、关键基础设施数据在业务应用中的共享交换与流通，依托数据共享交换清单、权限管理、数据审计、数据安全态势感知平台、API 调用过程监测和数据安全运营团队，确保数据交换过程中的真实性、完整性、保密性，数据共享交换主体的专业与合规，以及实现全程可追溯和可审计。安

我们需要从传统的“系统视角”向以数据全生命周期流转为中心的“业务视角”转变；
从强调技术向“技术”与“管理”并重，思路转变；
结合具体场景、行业特性、数据属性量等，
综合制定数据安全目标和工作任务。

整合平台：数据安全的未来

面对不断增加的服务需求、快速变化的威胁形势和技术人才的不足，数据安全建设必然是从孤立的数据安全产品过渡到数据安全平台。

数据保护成为大多数安全团队的首要任务。随着数字化的深入与推进，机构的数据成指数级增长。在不断变化的架构中，数据分散在数以千计的应用程序、数据存储系统和 SaaS 提供商中。但大多数机构仍使用传统的安全技术来发现数据和保护数据。

目前机构部署了多种单点数据安全产品，由此带来的挑战日益明显。不同的数据安全工具孤立运行，这导致运营效率低下，无法支持数据风险评估，以及涉及数据的内部创新和协作，更糟的是会留下意想不到的（或看不见的）安全漏洞。因此，我们看到安全预算持续增加，但增加 IT 安全支出并不一定带来更好的数据安全，数据泄露事件也仍在继续增加。2023 年预计全球安全和风险管理支出将从 2021 年的 1580 亿美元增至 1880 亿美元，但数据泄露受害者人数继续增加，到 2022 年超过 4.22 亿，比上一年增加 1.28 亿。

为应对数据安全的挑战，必须从整体上看待和考虑数据安全保护，单独的数据安全功能和产品将合并到新的数据安全平台中，数据安全市场正进入融合阶段。自 2021 年下半年，Gartner 在《2021 数据安全技术成熟度曲线》对数据安全平台（Data Security Platforms，DSP）定义以来，行业和客户对数据安全平台（DSP）的兴趣呈爆炸式增长。Gartner 将 DSP 定义为一种统一的解决方案，整合了跨数据类型、数据存储位置和数据系统的数据保护要求。

Gartner 在其《2023 年数据安全平台融合战略路线图》中指出，成功的安全风险管理领导者可以通过从孤立数据安全产品过渡到数据安全平台，显著数据的业务利用和价值，从而实现更简单、一致的端到端数据安全。

在《路线图》中，Gartner 预计，到 2024 年，30% 的企业将采用数据安全平台（DSP），大大高于 2019 年低于 5% 的数字。这主要是由于对更高级别数据安全的需求，以及产品能力的快速提升的原因。

面对不断增加的服务需求、
快速变化的威胁形势和技术人才的不足，
数据安全建设必然是从孤立的数据安全产品
过渡到数据安全平台。

在网络安全领域，
孤立、单点的产品正走向整合。
数据安全平台是这一趋势在数据安全领域的体现。

打破数据安全孤岛

在网络安全领域，孤立单点的产品正走向整合。数据安全平台是这一趋势在数据安全领域的体现。在 2023 年 6 月的 Gartner 安全与风险管理峰会上，Gartner 分析师兼副总裁尼尔·麦克唐纳表示，75% 的安全用户正在推动供应商整合，其中 56% 的受访者特别重视数据安全平台整合。

在数据安全领域，与单点安全产品相关的挑战更加明显。鉴于数据在创建、访问、编辑、保存、复制、备份和 / 或存档时可能需要涉及大量异构系统，为应对不同需求的数据安全供应商如雨后春笋般涌现，分别提供诸如数据存储安全、用户和数据访问安全等不同的功能。

如果无法实现对数据的集中控制，也无法了解究竟是谁、出于什么目的来使用数据，数据孤岛就不可避免地会形成。这意味着数据没有得到妥善管理和保护，最终可能会使数据面临安全风险。它也可能使需要使用数据的人无法访问数据，从而丧失宝贵的增长机会。此外，使用多个解决方案提供商的数据安全产品会增加挑战，单点、孤立的数据安全产品将带来额外的成本和复杂性等问题。

因此，基于平台的数据安全方案受到越来越多 CISO 的欢迎。数据安全平台 (DSP) 可以更快、更轻松地进行部署和管理，提高对数据及其使用的可见性与控制能力，不仅满足合规目标，更使组织可以真正实现对数据安全的防护，从而可以让数据在个人、组织和政府之间安全流动。

数据安全平台的核心功能

对于数据安全平台的功能，不同的供应商有不同的定义。研究机构 Gartner、Forrester 及 ESG 研究集团对数据安全平台的定义与功能界定上也存在少量差异。

1、Forrester 数据安全平台

在《Forrester Wave™ 数据安全平台 2023 年第一季度报告》中，Forrester 对全球 14 家最重要的数据安全平台提供商进行评估，数据安全方面的主要标准包括：数据发现、数据分类、数据使用洞察、数据威胁和风险可见性、数据访问控制、数据防泄密、数据脱敏或编写、数据加密、权限管理、标记化、隐私用例、数据和信息治理用例、调查、可管理性和支持、零信任集成和供应商风险。

在 Forrester 的定义中，数据安全平台同样是将以前孤立的安全防护产品在同一平台工具中结合起来，从而使 DSP 成为数据安全建设的关键节点。

2、Gartner 数据安全平台

根据 Gartner 发布的数据安全能力融合成数据安全平台的演进图，2009 年，数据安全控制主要集中在数据库活动监控 (DAM) 上，然后是数据

1	数据发行（Data discovery）	5%
2	数据分类（Data classification）	5%
3	数据分类洞察（Data use insights）	5%
4	数据威胁与风险可见性（Data threat and risk visibility）	5%
5	数据访问控制（Data access controls）	10%
6	数据防泄漏（Data loss prevention）	5%
7	数据脱敏或编写（Data masking or redaction）	5%
8	数据加密（Encryption）	10%
9	权限管理（Rights management）	5%
10	数据标记化（Tokenization）	5%
11	数据隐私用例（Privacy use cases）	5%
12	数据与信息治理用例（Data and information governance use cases）	5%
13	数据调查（Investigations）	5%
14	管理与支持（Manageability and support）	10%
15	与零信任集成（Integrations for Zero Trust）	5%
16	供应商风险（Supplier risk）	10%

表：《Forrester Wave™数据安全平台报告》主要安全能力

库安全。2014 年，数据脱敏和标记化技术更加普遍。2021 年后的 DSP 市场则包括从数据加密、数据发现到数据访问治理 (DAG) 的一切功能。

根据数据安全能力融合成数据安全平台的演进图，DSP 平台主要能力及工具包括数据防泄漏（DLP）、数据发现和分类工具、数据访问治理（DAG）、数据活动监控（DAM）、数据脱敏（Data Masking）、静态数据脱敏（SDM）据库加密（字段/记录）、标记化、数据风险分析、隐私增强计算（PEC）技术。

根据 Gartner《2023 数据安全平台部署战略路线图》，目前有四个主要的数据安全平台 (DSP) 类别。

具有广泛功能的 DSP(bDSP)——为云端数据库中的结构化数据提供强大的整合；bDSP 将跨孤岛的数据发现和策略定义功能与统一的后期绑定访问控制相结合，超出了数据存储实施的范围和粒度。DSP 使用的流行的后期绑定访问控制是加密技术，如令牌化和格式保留加密 (FPE)、动态数据屏蔽（DDM）、隐私增强计算及专有连接器和代理。bDSP 通常提供数

图：数据安全能力融合成数据安全平台 来源 Gartner

据发现和分类、跨孤岛的策略定义功能、后期绑定访问控制、使用格式保留加密 (FPE) 对数据进行字段级加密、数据库活动监控等功能。

数据安全态势管理 (DSPM)——提供跨孤岛应用的态势管理和数据发现功能。具体来说，数据安全态势管理提供有关敏感数据位置、谁有权访问、数据使用方式及数据或应用安全态势的可见性。简单来说，DSPM 供应商和产品提供“数据发现 + 的能力，即深度数据发现能力，加上数据可观察性功能的不同组合。这些功能包括对数据流、风险和数据安全控制合规的实时可见性。数据安全态势管理 (DSPM) 的目的是发现安全漏洞和不当的风险暴露。

数据丢失防护（DLP）——DLP 技术用于阻止不合规的数据传输、使用或存储。DLP 技术已出现很长时间，很多安全产品都使用到它。DLP 技术不仅是企业 DLP 套件，也经常作为 DSP、SaaS 和 IaaS 环境的原生控制；同时也是安全 Web 和邮件网关、端点保护平台、云访问安全代理（CASB）和防火墙等安全产品的重要功能。

数据访问治理 (DAG) 产品——关注于为非结构化数据实施数据安全访问政策。以 DAG 作为主要关注点的数据安全平台（DSP），通常提供数据发现、数据分类、数据所有者身份识别、文件共享的活动监控和审计等安全功能。

3、ESG 数据安全平台

与 Gartner 一样，ESG 集团研究人员同样强调数据安全态势管理（DSPM）的作用，可以确保数据具有正确的安全态势——访问控制、加密、脱敏等——无论数据位于何处。此外，EDG 研究人员还特别强调数据检测和响应 (DDR) 功能，认为数据安全态势管理（DSPM）、数据检测和响应 (DDR)，与数据分类、数据访问控制一起构成复杂的数据安全平台。

数据检测和响应（DDR ）将端点检测和响应，以及扩展检测和响应的概念应用于数据领域：识别、分析和响应与敏感或关键数据相关的安全事件。DDR 的核心是检测潜在的数据泄露，或未经授权访问敏感数据，分析事件潜在影响并采取适当的措施进行补救，并防止未来类似事件的发生。

值得注意的是，Gartner 与 Forrester 都强调数据安全平台（DSP）与零信任的集成能力，支持零信任的数据控制对实现数据安全整合是必要的。零信任框架有助于保护用户、保护连接、保护数据。数据安全不是在真空中部署的解决方案。支持零信任的供应商，通过对所有可用源数据进行基于风险的分析来不断评估信任，能够更好地提供集成服务和安全功能，因为他们可以了解用户，应用和数据之间的交互，从而使客户能够进行数据控制的整合。

如何推进数据安全平台战略

采用数据安全平台具有不可否认的优势，且正在成为一种必然趋势。但是，企业过渡到完整的数据安全平台架构需要时间，部署和转向数据安全平台涉及组织的许多方面，不是简单 “按一下开关”就可以实现的，而是需要雄心勃勃、持续多年的过渡计划。拙劣的数据安全项目很容易导致持续数月的 IT 问题，甚至带来业务损失。安全和风险管理负责人必须了解这些风险，并将其传达给利益相关者和组织高管。

Forrester 在其报告中指出，不同

企业过渡到完整的数据安全平台架构需要时间，部署和转向数据安全平台涉及组织的许多方面，不是简单 “按一下开关”就可以实现的。

数据安全平台提供从数据发现、分类到数据控制的端到端功能，但彼此的功能差异很大，这取决于平台旨在保护的数据类型（结构化、非结构化或两者），以及平台涵盖的数据环境。因此，在企业环境中使用多种类型的数据安全平台是很常见的，尤其是在大型复杂的 IT 环境中，而且在可预见的未来，这种现象将继续下去。

Gartner 在《2022 数据安全成熟度曲线》中也指出，越来越多的数据安全供应商的产品可以支持不止一种功能，从而带来整合的可能性。目前，没有单一产品或单一供应商产品组合可以支持所有数据类型、数据位置或所有数据安全功能。

Forrester 建议，数据安全平台潜在用户应寻找具备以下条件的供应商:

- 可以降低持续运营的成本。供应商支持的质量和故障排除的响应能力、用户界面的设计，以及持续的特定产品学习和培训资源,对于成功至关重要。
- 实现数据安全控制，同时可最大限度地减少使用数据的摩擦。用户希望通过数据安全平台，实现一项或多项数据安全控制能力，因此在实施数据安全控制时，员工的经验非常关键。
- 具有稳健安全和风险管理实践，可以降低安全风险。 供应商对其产品应具备有力的安全软件开发生命周期管理。此外根据要求，向用户提供软件物料清单及 SCA 报告的情况也日益普遍。

在《2023 年数据安全平台融合战略路线图》的迁移计划中，Gartner 对更高的优先级的建议包括，在接下来的 12 到 24 个月内:

- 使用双管齐下的方法，利用 bDSP 和 DSPM 的各自优势：为基于云的数据库中的结构化数据实施 bDSP；针对云和本地数据中心中的非结构化数据评估 DSPM。
- 在零信任计划中包含数据安全。与零信任相关的数据安全功能是数据发现和编目、数据访问管理、数据加密和数据治理。
- 从高级控件开始。专注于高级控制的 bDSP 通常比专注于单一传统控制的 DSP 覆盖范围更广。
- 利用外部期望。外部期望（如合规性要求或法规）是加速为当前合规要求或法规范围内的数据存储部署数据安全平台的机会。
- 识别不适合组织环境的数据安全功能。
- 更新组织的数据安全策略和 DSG 框架,以确保它们不会停留在石器时代。重新评估现行政策、流程和标准的有效性和益处。安

> 不同数据安全平台提供从数据发现、分类到数据控制的端到端功能，但彼此的功能差异很大，用户应选择可持续降低运营成本，实现数据安全控制的供应商。

数据安全风险应当怎么“看”？

作者 | 魏开元

“看清安全风险，是实施安全防护的第一步。”在数博会期间，奇安信集团董事长齐向东总结了当前数据安全建设面临的三大难题，即风险难看清、内鬼难管好、攻击难防住。其中，作为数据安全的第一道难题，看清风险的重要性自然不言而喻，近些屡屡发生的重大数据泄露事件，都与防守方没有掌握风险全貌，有着或多或少的联系。

“数据能看清涉及到看数据内容，与过去的网络安全相比，没有黑名单，也建立不了白名单，想看清就很难。”齐向东明确指出了数据安全看清风险的难题所在，更具体来说，网络安全攻击面风险排查注重网络设备资产、配置、漏洞等方面的排查；与之相比，数据安全看清风险的手段更注重数据流动状态下数据安全风险的实时监测，一个偏静态，一个更加动态，尤其是随着数据流动的不断加剧，二者的难度自然不可同日而语。

> 看清数据安全风险的手段更注重数据流动状态下数据安全风险的实时监测，
> 相比网络安全更加动态，
> 尤其是随着数据流动的不断加剧，难度更高。

双视角看清数据安全风险

看清风险之前，首先看搞明白数据安全的风险到底是什么。对此，奇安信数据安全产品总监王弢认为，厘清数据安全的风险应从两个视角入手。

一是从业务的视角，即从业务的开展情况，看清从用户→终端→网络→应用→数据流转全链路上各个环节有可能发生的数据安全风险，如账号被窃取、账号弱口令、终端违规外发敏感数据、非授权设备接入网络、API 非授权访问、API 违规传输敏感数据、敏感数据明文存储、数据库遭恶意操作、特权账号滥用、敏感数据未脱敏使用等；

二是从数据生命周期视角，看清各个节点有可能发生的数据安全风险，如采集阶段的违规采集数据、超范围采集数据；存储阶段的数据未分类分级，敏感数据未加密存储、未进行针对性的数据访问权限设置、未进行统一运维收口；加工阶段的直接使用敏感数据加工、大量高频调取敏感数据、数据未授权访问；使用阶段的 API 违规传输敏感数据、应用 SQL 注入攻击、API 未授权访问；传输阶段的违规外

发敏感数据、敏感数据跨境传输；共享阶段的数据未脱敏使用、超范围共享等。

看清数据安全风险的三大难题

如前文所述，从相对静态的关注IT系统的资产、配置、漏洞及补丁等攻击面信息，到动态的观察数据的全生命周期及流转的各个环节，这其中面临着诸多难题，主要体现在以下三个方面。

首先是数据流转和数据访问的场景看不全。数据的生命周期涉及到数据的收集、存储、使用、加工、传输、提供、公开等各个环节，数据的流转可以涉及到不同的应用之间、不同的系统之间、不同的组织之间，甚至不同的国家之间，目前的解决方案很难将所有涉及到的环节全部看清。

比如，数据在不同应用之间流转，应用的种类多、数量多，相互间的依赖性强，不同的应用有不同的风险，也很容易被其他应用的风险牵连。并且应用之间的数据流转依赖大量的API接口，很多企业对海量API资产的识别不准确，脆弱性的发现能力也不足，从而导致API接口出现数据泄露问题。

二是数据流转的内容看不清。目前市面上的主流产品针对数据的识别能力不足，大量的敏感数据、重要数据识别不出来，导致企业难以分清到底哪些数据是重要数据、哪些数据是非重要数据，也就无法实现精准的数据分级分类和与之相配套的防护手段。

三是数据访问与身份账号的关系看不到。传统的监测手段只关注数据访问者的IP信息，具体到是“谁”？是什么账号访问了什么数据，访问身份和访问内容的关联关系无法看到，身份信息和访问数据的权限是否匹配也无从谈起。事实上，不同的用户在不同的时间、不同的地点，即便是访问了相同类型的数据，其潜在风险也有所不同。

打造全链路数据安全风险识别能力

面对上述挑战，奇安信发布的奇安天盾数据安全保护系统可以基于数据要素流动的各种场景，构建的数据安全保障体系。

王弢介绍，奇安天盾以“数据资产”为核心，将“事件监测、风险分析、策略调整、访问控制”融为一套完整的闭环体系，让数据安全风险能看清，内鬼能管好，攻击能防住。

针对看清数据安全风险，王弢强调，奇安天盾搭载了奇安信自主打造的三大业内领先的分析识别引擎，包括：

协议解析引擎，可对各类应用与API进行识别与深度解析，全面还原流量中传输结构化、非结构化，半结构化数据，为敏感数据识别提供基础数据，确保数据访问的安全性。

敏感信息识别引擎，通过文件类型识别、文件内容提取及分析、压缩文件内容提取及分析、图片文件内容提取及分析等，判断当前文件内容是否包含敏感信息，并产生敏感信息文件告警，为数据安全的进一步处理提供依据。

异常行为分析引擎，通过用户访问业务应用的请求，用户执行的操作、用户访问的内容、用户范围的时间、用户访问的地点等，关联上下文判断当前用户是否存在违背基线的访问行为、并产生用户异常行为事件，保护业务数据安全。

基于上述三大引擎，奇安天盾具备了行业领先的协议解析和数据识别能力，支持3000+的应用识别，2000+敏感数据监测、27种文件类型、4种图片类型还原；20多类1000+公共组件API识别、Restful、grpc等10+API还原，将终端流量、应用流量、运维流量、API流量、数据库流量的全流量覆盖及精准识别，看清所有数据内容。

因此，奇安天盾实现了数据安全的全链路可视，能够帮助客户精准识别各类数据资产，帮助建立数据资产台账；同时通过多种监测组件，例如，数据库审计监测系统、流转数据监测系统、跨境数据监测系统、终端访问监测系统、应用访问监测系统、API安全监测系统等，能够帮助客户看全数据流转和访问的完整路径，明确数据访问主体身份，及时发现数据流转各个环节的潜在风险和针对敏感数据的异常访问行为。

当然看清风险也只是数据安全防护的第一步。王弢表示，作为一种新型生产要素，数据的流转在管理者、经营者、使用者的不同的载体上处理，数据涉及到个人数据、商业数据、公共数据，甚至是机密数据，数据复杂的流转带来更多的安全风险，而奇安天盾的发布，弥补了对于数据保护的事件监测、风险分析、策略调整、访问控制一体化能力的缺失。安

史上最复杂的数据安全保障项目，如何实现“零事故”？

作者 | 张少波

60 多个核心技术系统，涉及全世界近百家供应商，服务 8 大类客户群，全球瞩目的体育盛事……如何保障2022北京冬奥数据安全“零事故”？没有能借鉴的行业成熟先例，更没有可参考的成功经验模式，奇安信通过在实践中的不断探索，寻找到了一条建设路径。

北京冬奥会之前，业界普遍认为网络安全不存在“绝对安全”的状态，数据安全更是如此。从历届奥运会来看，数据都是黑客、不法分子们觊觎的目标，2012 年伦敦奥运、2016 年里约奥运、2020 年东京奥运等都出现过不少数据泄露事件，这足可见数据安全保障的任务难度和艰巨性。

2022 北京冬奥堪称数字科技含量最高的一届冬奥会，对数据安全保障提出更苛刻的要求。作为北京冬奥网络安全官方赞助商，奇安信早在开幕前数百天，就作出了“合规不踩线、数据不出事、业务不中断”的“零事故”承诺。在具体实践中，奇安信以冬奥数据资产为核心，打造“监测—分析—调整—控制”的数据安全闭环体系，一方面，全面保障数据安全和隐私保护合规；另一方面，确保整个冬奥期间未发生一起数据泄露事件，圆满完成冬奥数据安全的保障任务并兑现“零事故”承诺。

第一步：梳理数据资产，做好分级分类，识别敏感数据

知己知彼，方能百战不殆。“相比终端、网络、数据中心等可见设备，数据总是无形和抽象的。尤其是北京冬奥会涉及的业务环境可以说空前复杂，各类数据在 60 多个技术系统中持续流动，如何在一团乱麻的数据资产中抽丝剥茧、理清思路，从而对症下药、量体裁衣，是冬奥数据安全面临的首要挑战。”奇安信冬奥保障数据安全负责人这样表示。

针对这些挑战，奇安信数据安全团队很早就进入场内，系统化梳理冬奥会的网络、信息系统及数据，并在收集、传输、存储、使用和销毁各个环节，掌握重要的数据存在哪、谁在使用、如何使用这三个核心问题。

图：北京冬奥会涉及业务环境

掌握了这些基础信息，团队进一步梳理已有安全措施情况，是否应用于重要数据资产的环境，从而形成详实、全面的数据资产梳理报告。依托该报告作为指导依据，团队全面开展数据分类分级。

其中在分类方面，冬奥数据安全保障团队根据来源和应用属性的不同，将个人数据、竞赛数据、业务数据、运行和安全数据依次分为 A 类、B 类、C 类、D 类四大类。在安全分级方面，根据流转场景和安全需求的不同，将其划分为公开级（L1）、内部级（L2）、敏感级（L3）、高敏感级（L4）四个等级。

“个人信息是冬奥数据最重要的部分。拿个人信息举例，它就可以分为四级：合法公开的某个运动员身高、生日，就是 L1 公开级数据；如果是内部公开的工作人员信息，如工作人员的职务、电子邮箱、工作电话等，就是 L2 内部级数据；而到了个人基本资料、网络身份标识信息、个人教育工作信息、个人通信信息等牵涉私人信息的话，就属于 L3 敏感级；如果是个人身份、生物识别、网络身份鉴权、个人健康生理、个人财产或其他隐私信息的话，就属于 L4 高敏感级数据了。”该负责人表示。

数据分类	数据分级			
	公开级（L1）	内部级（L2）	敏感级（L3）	高敏感级（L4）
个人数据（A）	个人公开信息（A1）	个人内部信息（A2）	个人信息（A3）	个人敏感信息（A4）
竞赛数据（B）	竞赛可公开数据（B1）	竞赛内部数据（B2）	竞赛敏感数据（B3）	竞赛保密数据（B4）
业务数据（C）	业务可公开数据（C1）	业务内部数据（C2）	业务敏感数据（C3）	业务保密数据（C4）
运行和安全数据（D）	运行和安全可公开数据（D1）	运行和安全内部数据（D2）	运行和安全敏感数据（D3）	运行和安全保密数据（D4）

图：冬奥数据分级分类

通过数据资产梳理和分类分级矩阵，任何数据都可以对应响应的类别和分级，并能快速识别敏感数据。

第二步：依据不同级别，识别敏感数据，制定管控策略

完成冬奥海量数据分级分类，并定位和识别敏感数据之后，相关的安全策略和措施就可以有的放矢了。

首先，加密是数据安全的最基础工作，针对不同级别的数据制定不同的加密策略。本次冬奥首个建设完成的专项，就是奇安信实施的冬奥密码专项。该项目遵循“冬奥网络安全总体规划”，是奥运历史上首次使用国密算法保护信息系统的核心数据，实现了高安全（等保三级、密评安全三级），高复杂环境（国内外、云与本地），以及密码与网络安全密切配合的密码服务能力。

同时，本着分层、精细化的原则，

图：冬奥风险关联分析及综合研判

建立了与数据级别相对应的分层数据权限管理体系。其中包括：根据数据级别制定相应数据授权审批流程，合理授予、管理数据权限；高敏感级和敏感级数据仅能通过高权限账户访问、提取和使用，高权限账户的数量应严格限制；采取措施保障数据细粒度访问控制。

第三步：基于管控平台 + 多种组件，实现数据流转全链路风险监测

只有全链路监测、全穿透识别，才能做到数据安全风险看得清。在冬奥数据安全专项上，奇安信部署了数据库监测、身份认证监测、流转数据监测、跨境数据监测、应用访问监测、API 访问监测、运维访问监测、终端访问监测等多种监测组件，采用多种监测方法，清晰地看全数据流转和访问的完整路径，直观了解数据的流转情况，能及时发现异常和风险，做到数据流转的全链路可视。

北京冬奥是全球性的体育盛事，有 91 个国家和地区参加，存在广泛的数据跨境流动的场景。针对该场景，奇安信可以看清数据出境的数量、种类、范围、敏感程度，清晰掌握企业数据的出境情况，及时发现违规行为，对于出现数据出境违法违规的情况进行溯源取证。在发生数据违规情况后，通过数据安全管控平台与跨境数据监测系统、零信任安全网关的联动，及时制定处置策略，降低风险发生概率。

冬奥业务系统和网络部署多种监测组件，并依托数据安全管控平台，最终实现数据流转全链路风险监测。

第四步：风险关联分析，实现更精准的综合研判

能看见风险、看清风险固然重要，但如果安全策略过严，可能影响正常业务运行和数据流动，过松则会导致风险事件升级。因此，对风险进行关联分析，实现更精准的综合研判至关重要。

在冬奥项目中，安全团队基于复杂多样的业务场景特性，配置专有的风险分析策略，并构建风险分析模型，实现多源数据的关联分析。例如，对用户的登录活动、访问行为、数据库查询、API 调用等监测数据进行关联分析，一旦发生数据违规事件，及时

发现并告警；产生告警后，结合预置的各类检测规则和策略，实现告警归并和事件快速定位，同时综合敏感数据分布、数据流转情况、用户行为画像、异常行为监测等信息，对数据安全事件进行可视化呈现。

通过多维度、多规则、精细化的风险分析策略，以及强大的风险分析模型，安全团队能够用全局视角，及时发现“隐蔽”的数据安全事件，并进行精准的综合研判。

第五步：动态策略调整及控制措施下达

在访问控制上，奇安信为冬奥打造了多维访问控制模型，能对数据操作、特权访问、应用访问等不同颗粒度进行精准管控。这样一来，能及时制止高危数据安全行为，有效化解从内部“正常用户”对外泄露敏感数据的危机。

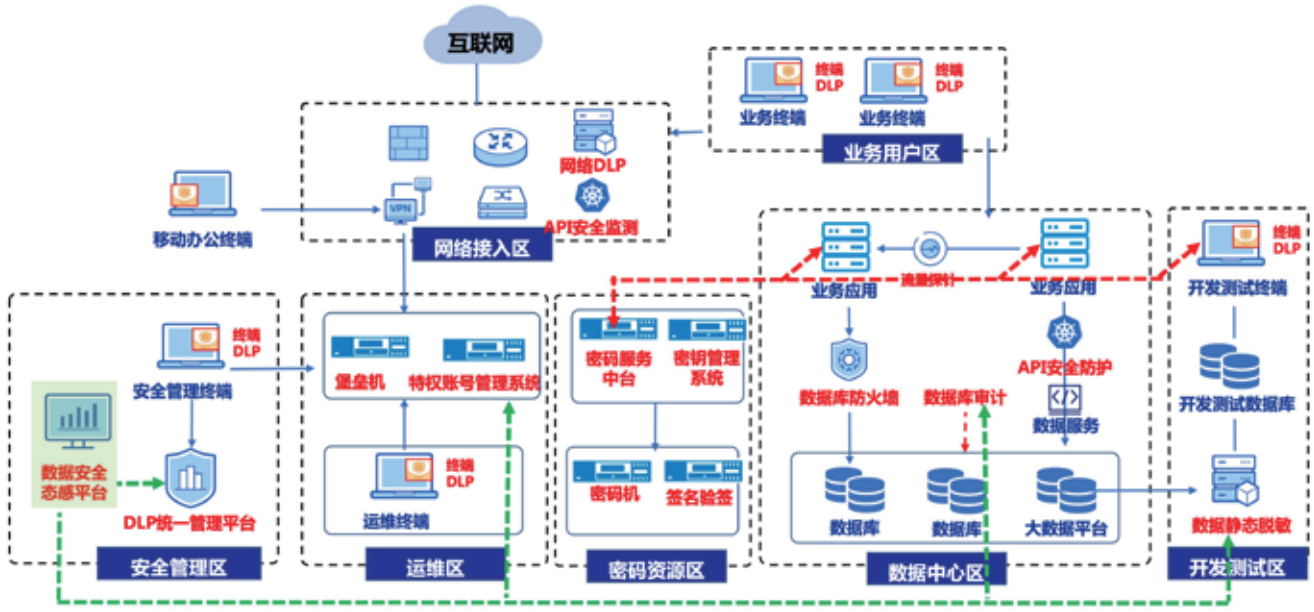
比如，通过数据安全管控平台，可以实现动态策略调整，并将调整后的策略下发到相应的控制网关，如在运维安全网关方面，调整运维操作权限，高危指令阻断，敏感操作二次授权；在零信任安全网关方面，通过调整身份账号权限，缩小数据访问权限范围；在 API 安全网关方面，针对高危 API 进行限流限速，紧急情况下阻断该 API；在终端安全网关方面，结合策略，阻断该终端敏感文件外发行为；在数据库运维网关方面，对数据库的操作进行细粒度审计和管控，并凭借强大的风险关联分析能力，发现数据库管理员针对数据库的恶意拖库、删库行为，并及时进行动态策略调整。

通过面向 5W1H 的细颗粒度访问控制策略，正确的人 (WHO)、正确的时间 (WHEN)、正确的地点 (WHERE)、正确的原因 (WHY)，用正确的方法 (HOW) 访问授权数据 (WHAT)，并基于多属性、多来源风险进行动态策略调整，覆盖端到端的全链路风险纳管与综合评估，提升风险响应实时性，确保冬奥数据资产安全。

结束语：

如果说 2022 北京冬奥网络安全保障是一张空前复杂的考试答卷，那么数据安全堪称这份考卷中复杂度最高的压轴大题。在北京冬奥数据安全保障中，奇安信基于体系化理念，制定了包括数据资产梳理 / 分级分类、制定管控策略、全链路风险监测、风险关联分析及综合研判、动态策略调整及控制措施下达等分步骤的完整方案，解决各种主要的数据安全问题，做到“能看清、能管好、能防住”，成史上最复杂的数据安全保障任务。

数据显示，整个冬奥防护期间，奇安信成功抵御了含社会面攻击超过 3.8 亿次，创造了包括数据安全在内的“零事故”记录。更重要的是，“零事故”让数据安全建设结果可评估、可衡量，为客户构建其全新的安全建设结果评价体系提供了范式，显著提升了行业竞争门槛，形成了公司差异化的竞争壁垒。 安



图：数据安全产品部署图

孙悟空一个筋斗十万八千里，为什么不直接让他取经?

作者 | 张少波

小时候看《西游记》，经常有一些疑惑的问题：

孙悟空既然一个筋斗云能十万八千里，从大唐长安到天竺灵山刚好十万八千里，让孙悟空一个筋斗翻过去取经回来，岂不更省事儿?

猪八戒、沙僧的武功稀松平常，还常拖后腿，为啥不找一个武艺高强的给孙悟空当搭档? 比如，黑熊怪、红孩儿……

唐僧手无缚鸡之力、胆小懦弱、人妖不分、固执迂腐，是不是取经团队的累赘?

……

但随着年龄的逐渐增长，再解读《西游记》，其实能发现，取经之路其实是团队每个成员不断成长、自我蜕变的过程。从初期的相互猜疑甚至拆台，到后期的众人齐心、相互补位，《西游记》其实描绘了从散兵游勇蜕变成优秀团队的成长历程。

孙悟空一个人完成取经可行么?

先回答第一个问题，让孙悟空一人去取经，是否可行?

先不考虑唐僧的前世是如来的大弟子金蝉子这层关系，假如没有团队，让孙悟空一个人去取经，合适么?

首先，孙悟空 500 年前大闹天宫、偷吃蟠桃金丹，罪孽深重，难道跑一趟快递，运送一次经书，就将功折罪了? 玉帝、太上老君、天庭诸臣等受害者能原谅么?

其次，如果孙悟空一个筋斗云取回真经，东土大唐这么容易就得到了大乘佛法，他们会珍惜么? 会给予足够重视么? 孙悟空适合当大乘佛法的最好代言人么?

最后，假如孙悟空轻松取回真经，获得刑满释放，他下一步去做什么? 去天庭、西天求职，肯定政审不合格，面试被 pass 掉。回花果山继续当猴大王? 但花果山已被二郎神烧毁了，猴子猴孙几乎被团灭了。孙悟空是否会旧仇新怨一起报复? 再次走上反抗

天庭、大闹天宫的老路?

可见，即便如来再偏爱，组织上再照顾，让孙悟空直接取经都是不可行的。《西游记》设定的西天取经任务，其实是给师徒四人一个自我救赎、蜕变成长的机会。如果由孙悟空直接取经，他就失去了九九八十一难的历练和实践，最终依然是顽劣不教，得不到任何成长和改变。

事实来看，整个取经之路，孙悟空从初期的我行我素、个人英雄主义，到后期懂得团队协作，能和唐僧猪八戒和睦相处，能虚心求助各界神通，和天庭、西天打成一片，充分体现了孙悟空的成长过程：个人能力再强，都离不开团队协作，都需要依托组织和平台，才能发挥最大价值。

唐僧真的是团队累赘么?

说完孙悟空，再说说唐僧。从能力来看，唐僧远不及孙悟空，但好在拥有了紧箍咒这个“调教武器”。猪八戒加入团队之后，唐僧又增加了一个制衡顽猴的“抓手”。因此，初期唐僧总有些偏袒猪八戒、打压孙悟空，而在《三打白骨精》中两人合力赶走孙悟空，就是最集中的表现。

到中后期，唐僧深刻意识到，完成取经大业，离不开孙悟空，他的管理方式更加灵活和柔性。对于孙悟空和猪八戒的态度也逐渐发生变化，不再一味的偏袒猪八戒，不再老用紧箍咒“高压”管理孙悟空。最终，大家的积极性、责任心都更强了，团队也更加和睦了。

唐僧的历程，体现了团队领导人的成熟和成长。对孙悟空的顽劣从不容忍、驱赶到耐心包容，对猪八戒、沙僧给予关怀和鼓励，最终提升了团队凝聚力。他虽是凡人躯体，但凭借

刚柔并济的团队管理能力，帮助大家共同成长，最终成为取经团队真正的领导者和灵魂人物。

猪八戒真的是“猪队友”么?

很多人对猪八戒的印象，就是好吃懒做，武功稀松，而且还经常挑拨唐僧和孙悟空的师徒关系，但其实，猪八戒在取经路上的进步，也是很大的。

早期猪八戒存在很多问题，比如，意志不够坚定、心猿意马还贪恋女色，是团队中负面形象的代表。随着团队磨合，猪八戒灵活调整了自己的定位，正确认识了自己作为孙悟空助手的角色，作战逐渐勇猛。例如，在联手孙悟空大战牛魔王时，一度将牛魔王打得招架不住。

同时，猪八戒扬长避短，将体躯笨重的短板化为了长板，主动承担脏活、累活。在“棘林吟咏五十二难”“稀柿衕秽阻五十五难”，他扫除荆棘，开山劈路，清理污秽，拱开通道，立下了大功，体现了担当。

能调节团队气氛，辅助孙悟空降妖除魔，能屈能伸、敢挑重担的猪八戒，是团队中不可或缺的角色。

沙僧只会说四句台词么?

《西游记》电视剧中，沙僧有四句经典台词：大师兄，师父被妖怪抓走了；二师兄，师父被妖怪抓走了；大师兄，二师兄被妖怪抓走了；大师兄，二师兄和师傅都被妖怪抓走了！一路上，沙师弟战绩少的可怜，没有存在感。

沙僧真的是打酱油、躺平熬资历的么？其实他最可贵的价值，是坚定的取经决心，以及遇到困难时沉着冷静的态度和情绪。可以说取经师兄弟三人中，唯一没有闹过散伙的是沙僧，无论取经团队遭遇何等困难，沙僧始终咬紧牙关，没有闹过半点情绪。

例如，在大战红孩儿时，孙悟空和唐僧出现重大分歧。孙悟空道：兄弟们，我等自此就该散了。猪八戒也附和：正是，趁早散了，各寻头路，多少是好。关键时刻，沙僧劝诫大家，“可不违了菩萨的善果，坏了自己的德行，惹人耻笑，说我们有始无终也。”最终，

沙僧在危难之际，稳住了团队。

沙僧虽然在四人中排在最后，但论大局观，沉着冷静的判断力，超高的情商，可以排在团队前列。

四人搭档才是最佳团队

由此可见，在西天取经团队的四人组中，孙悟空的能力最强，但缺少团队协同能力；唐僧是取经团队的领导，他逐渐成长并适应了角色，并能发挥出每个成员的优势；猪八戒虽有小毛病，但性格开朗，能屈能伸，中后期发挥作用很大；而沙僧一直是团队的稳定器，沉稳的性格让他不冲动，遇事冷静，也是取经团队的最后一道防线。

总而言之，四人搭档，最终形成了最佳团队。

> 做好数据安全，不能是简单的产品堆砌，
> 需要基于数据访问生命周期风险分析，
> 系统性地构建数据安全保护体系，
> 解决各种数据安全的难题。

做好数据安全，你需要一支能力互补的“取经团队”

做网络安全难，做数据安全更是难上加难。要为大型复杂机构做好数据安全，不亚于九九八十一难，要过很多道难关。比如，业务涉及面太广、数据资产体系庞杂、数据流转环节多、身份账号复杂如麻、访问控制策略难以一刀切……

要解决这些难关，仅靠一个神通广大的“悟空”，是远远不够的。比如说，即便这个“悟空”看到了威胁，但无法协同联动其他产品，无法准确分析评估风险、快速调整策略、确定访问权限，依然无法避免数据泄露事件的发生。同样，仅有“唐僧”“八戒”“沙和尚”，任何一个也都不够。

因此，做好数据安全，不仅是一个产品，也不能是简单的产品堆砌，需要基于数据访问生命周期风险分析，系统性地构建数据安全保护体系，解决各种数据安全的难题。

在这种情况下，不久前，奇安信在2023数博会上重磅发布“奇安天盾”数据安全保护系统（简称奇安天盾），用“六全”框架实现“三能”：能看清、能管好、能防住；一个系统解决各种数据安全问题。

在技术变革快，安全风险复杂，合规性要求越来高的背景下，数据安全存在着面临“难看清”“难管好”“难防住”等困境，奇安天盾能够基于“六全”框架，即全链路监测、全穿透识别、全兵种协同、全闭环处置、全天候控制、全场景防护，将“事件监测、风险分析、策略调整、访问控制”融为一套完整闭环体系，让数据安全风险能看清，内鬼能管好，攻击能防住。

举个例子，这就如同将一支优秀的取经团队，联合到一起来应对数据安全风险。

“孙悟空”火眼金睛，辨别世间妖魔鬼怪，对应奇安天盾的事件监测能力。它通过全面的识别和监测能力，实现数据安全的全链路可视，不遗漏任何潜在隐患和异常行为。

“沙僧”沉着冷静，及时洞悉内外风险，对应奇安天盾的风险分析能力。可以通过多源数据的关联分析，缜密判断，一旦发生数据违规事件，及时发现并告警。

“猪八戒”能屈能伸，战术策略动态调整，对应奇安天盾的策略调整能力。通过多属性、多来源风险进行动态策略调整，覆盖端到端的全链路风险纳管与综合评估，提升风险响应实时性。

“唐僧”管控徒弟，分分钟拿捏，对应奇安天盾的访问控制能力。颗粒度更精细的管控，实现全天候控制、全场景防护，在提升安全的同时满足业务连续性需求。

单个成员，谁都无法解决复杂的数据安全问题，但几个成员联动起来，形成闭环体系，就能解决几乎所有的数据安全问题。

数据安全，可以化繁为简，选择“奇安天盾”，一个系统就够了。安

《2023 年数据泄露调查报告》：五大要点

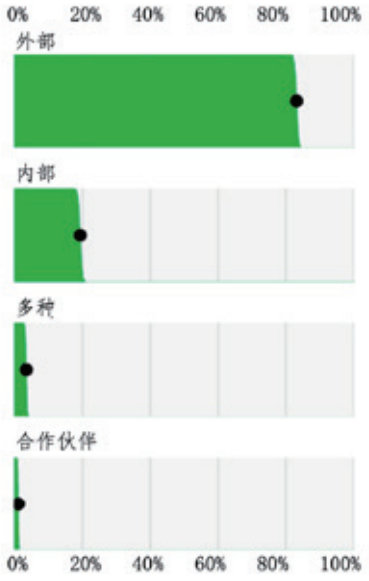
作者 | 姚磊

2023 年 6 月 6 日，美国通信运营商威瑞森发布《2023 年数据泄露调查报告》(DBIR)。在 2023 DBIR 中，威瑞森威胁研究咨询中心分析了 16,312 起安全事件和 5,199 起数据泄露事件，揭示了全球政企机构遭遇的数据泄露事件，以及面临的主要安全威胁。

报告显示，在近一半的数据泄露事件中，被盗凭证被用于对组织系统的初始访问；在动机方面，过去一年观察到的 95% 的攻击都是出于经济动机，只有一小部分攻击是间谍活动。

1、83% 的数据泄露事件是由外部攻击者造成的

根据 2023 DBIR，83% 的数据泄露事件涉及外部攻击活动。每 10 起数据泄露事件中，有 8 起是有组织的犯罪团伙和网络造成的。但不可否认的事实是，机构的一些员工也会出于恶意目的从而造成数据泄露。内部攻击造成数据泄露的最常见行为是滥用特权。勒索软件则成为攻击者首选的攻击武器。攻击窃取客户和财务数据的行为司空见惯。金融服务和制造业成为攻击者的首选目标。这些行业所属企业为了留住客户，必须按时交付产品和服务。



图：数据泄露事件中的攻击者

2、95% 的数据泄露是出于经济动机

数据泄露背后的主要动机依然是经济利益，今年这一比例高达 95%；2019 年，86% 的数据泄露是出于经济动机；此外，即使是滥用特权账号的内部攻击，其经济动机也高达 89%。

从地域来看，亚太地区的数据泄露事件中，61% 出于经济目的，高达 39% 是间谍活动；北美地区的数据泄露事件中 99% 是经济动机，间

谍活动仅占 1%。

图：数据泄露事件的动机

3、 24% 的数据泄露事件涉及勒索软件攻击，勒索作为主要攻击方式呈长期上升趋势

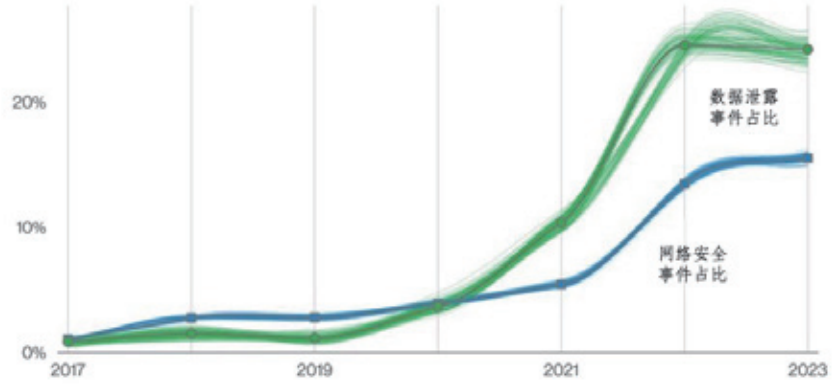
勒索软件依然是各种规模、不同行业的组织所面临的主要威胁，24% 的数据泄露事件中出现勒索攻击，这些事件中，94% 属于系统入侵。勒索软件已经普遍存在于各种规模和各个行业的组织中。目前，91% 的行业已将勒索软件列为三大威胁之一。

在有组织犯罪团伙实施的所有安全事件中，62% 出现勒索软件攻击；所有以经济利益为目标的安全事件中，59% 使用了勒索软件攻击。

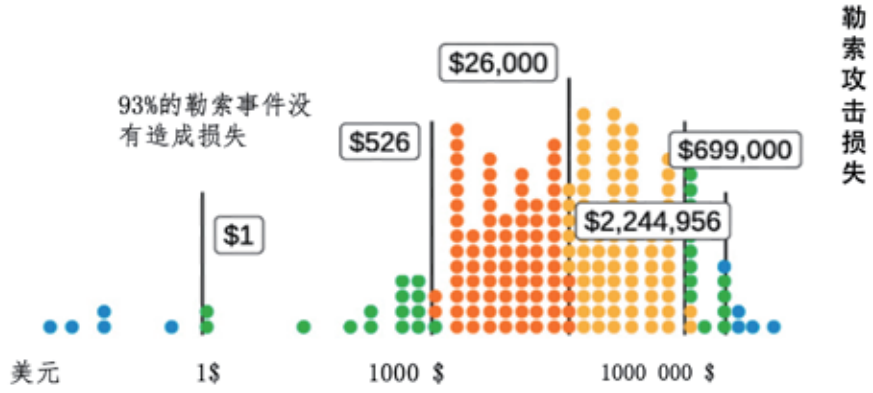
4、勒索攻击的平均成本增加了一倍多

勒索损失的中位数从 2021 年的 11,500 美元，激增至 2023 年的 26,000 美元；2020 年，勒索软件的平均成本为 8100 美元，而 2018 年仅为 4300 美元。五年内，勒索软件的平均成本增加了两倍。

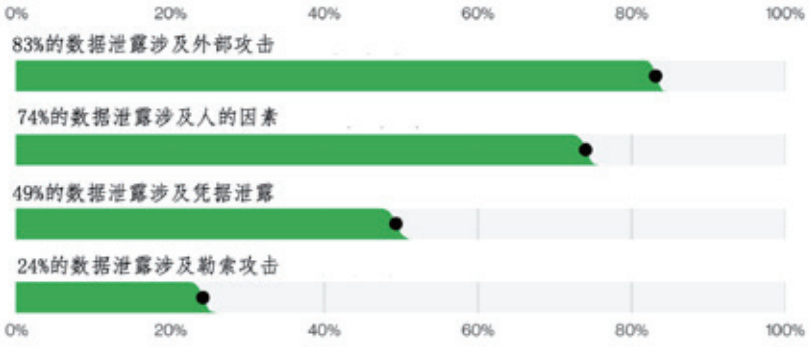
2023 年 95% 的勒索攻击造成的损失在 1 美元到 225 万美元之间。因勒索攻击停工而损失最大的行业，勒索攻击的损失继续创下记录。尽管勒索赎金的金额在降低，但从勒索攻击恢复的整体成本却在增加。



图：数据泄露事件中的勒索攻击占比



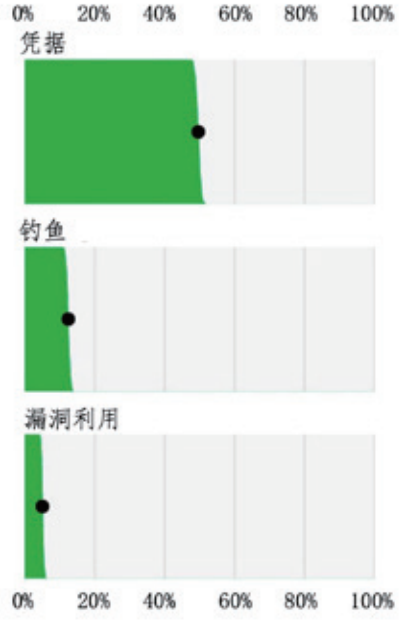
图：勒索软件攻击的成本



图：攻击者侵入组织的主要途径

5、特权账号或凭据的窃取、滥用是数据泄露的重要攻击手段

74% 的泄露事件是人为因素造成的，包括人为错误、滥用特权、使用被盗凭证或社会工程。攻击者进入组织的三种主要方式是窃取凭据、钓鱼和漏洞利用。窃取凭证已成为数据泄露事件中的最受欢迎的入口。过去的五年中，使用凭证的方式获得广采用。



Verizon Business 网络安全咨询总经理 Chris Novak 表示：“对许多企业而言，企业高级管理层自身就是重大安全威胁。因为这些高管不仅拥有一个企业最敏感的信息，而且往往是最不受安全控制的人群，因为许多企业的安全协议都为高管‘网开一面’。随着社会工程学的快速发展和日益复杂，企业现在必须加强对其高管的保护，以避免代价高昂的系统入侵。”

点评：政企单位应加强对内部特权人员和特权账号、凭证的管控

随着《网络安全法》的颁布和实施，政企单位在网络安全的投入是在逐年增加的，但往往更多的关注在终端、网络、云基础设施的安全建设上，《数据安全法》颁布和实施时间较晚，政企单位在数据安全的投入相对较少，这其中更是很少会优先关注内部特权人员的安全管理。

大规模的数据泄露事件，往往都是由于一两个内部特权人员的一次恶意操作导致的，所以在数据安全建设方面优先加强对数据访问权限特别是对特权账号和特权行为的管控，是解决数据安全问题最快、最有效的方式。建议政府政策端帮助各重点领域部门、企业树立数据安全防护意识。安

图：数据泄露的主要方式

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

大事记

2023 安全创客汇复赛重庆站落幕 20 强企业名单出炉

6 月 16 日，2023 安全创客汇复赛在重庆两江新区圆满结束，经过为期两天的精彩角逐，20 强企业名单正式出炉。据相关负责人介绍，安全创客汇将于 2023 年在北京网络安全大会期间举行。20 强企业还需通过半决赛、决赛环节，面临更加专业、严格的评审，以决选最终的获奖企业。

奇安信集团与中国传媒大学达成战略合作 共建网络安全“传奇班”

6 月 12 日，奇安信集团与中国传媒大学正式签署战略合作协议。双方将共建“传奇”班，培养高端网络安全人才，并在科学研究、学科建设、行业合作等方面开展深入合作。

此次合作重点内容之一是开展“传奇”班高精尖网络安全人才培养。该项目将由校企双方共同建设，打造提升网络安全能力的教学体系，积极探索改进和融合，鼓励基于网络安全生态的教学课程体系建设，实现基础课程到实训教学到场景实战的贯通，培养具有实战能力的应用型、创新型、特色型网络安全人才。此外，双方还将在网络安全技术创新、产学研贯通合作、行业应用合作、人才交流培养等方面开展深入合作。

全国高等职业学校校长联席会议：奇安信网络安全产业学院申报正式开始

现代高等职业技术教育网日前正式发布《关于推荐申报“奇安信网络安全产业学院”合作项目的通知》，根据全国高等职业学校校长联席会议要求，奇安信网络安全产业学院申报正式开始。

产业学院建设将基于国家网络安全发展趋势和战略定位，依托奇安信集团网络安全行业龙头的资源和能力，聚焦区域产业带优势资源，协力推动区域一体化人才培养。未来计划与院校共建立足区域数字经济发展的网络安全产业学院，支持院校高水平专业群建设，培养复合型、应用型、创新型、国际型高素质人才，助力区域数字产业发展。

千万级边界安全大单！奇安信中标国家电网旗下南瑞集团信息安全设备项目

近日，奇安信中标国家电网旗下南瑞集团信息安全设备框架项目，中标产品包括防火墙、入侵检测及防御等，中标金额超过千万。这是继不久前中标中国移动防火墙集采项目之后，奇安信边界安全产品的又一个千万级大单。

据介绍，本次入围产品将全面部署于智能电网发电、输

电、变电、配电、用电、调度各环节的信息安全防护，针对智能电网信息安全点多面广、技术复杂的特点，将“双网双机、分区分域、安全接入、动态感知、精益管理、全面防护”的主动防御策略进行全维度贯穿，切实将网络安全防护工作进行扎实落地。同时，本项目严格遵循国家电网信息安全现状，采用适合国家电网边界安全防护策略，从而更好地满足智能电网信息安全防护需求，适用性和扩展性强。

奇安信集团与华东空管局签署战略合作协议

6 月 6 日，中国民用航空华东地区空中交通管理局（简称华东空管局）与奇安信集团正式签署战略合作协议。双方将充分发挥各自领域优势，共同探索空管领域网络安全的中国方案，打造民航网络安全新标杆。

据悉，2020 年奇安信集团协助华东空管局编制了网络安全专项发展规划，确定了网络安全管理、保障、运行三大体系发展蓝图，为后续网络安全工作开展提供依据，并已在安全运营、制度建设等领域开展多项合作。此次签署战略合作协议，将为建设“四强空管”、推动民航空管高质量发展进一步筑牢根基，为新时代民航强国战略贡献力量。

奇安信与广东电信签署战略合作协议

5 月 30 日，在中国电信股份有限公司广东分公司（简称广东电信）举办的 2023 数字科技生态大会暨颁奖典礼上，奇安信集团与广东电信正式签署战略合作协议。双方将建立深入全面的业务合作，打造广东省网信安全、数字化建设的新标杆。

此前，奇安信已与广东电信在云安全、代码安全、数据安全、实战攻防、终端安全等领域进行过多次合作。此次战略合作的达成，双方将进一步发挥各自在产业、技术、资源等方面的能力与优势，共同探索在网络安全、5G 安全、安全运营等领域的新方案、新技术和新产品。

齐向东接任全国工商联大数据运维（网络安全）委员会主席

5 月 29 日，全国工商联大数据运维（网络安全）委员会轮值主席交接仪式暨数字中国建设整体布局规划解读会在

京召开。根据《全国工商联行业委员会工作规则》，全国工商联副主席、奇安信集团董事长齐向东接任全国工商联大数据运维（网络安全）委员会主席团主席。

齐向东对全国工商联的认可和信任表示由衷感谢，并深感使命光荣、责任重大。他表示，委员会自成立来，工作内容和使命紧紧围绕党和国家的战略需求，以服务国家战略方针为己任，屡创佳绩；未来两年，也将带领委员会继续奋斗，更好地服务于国家，服务于数字产业、网络安全产业发展，力争让委员会的规模更加壮大，社会影响力更加广泛，促进委员会成员更加团结。

盘古实验室最新手机芯片安全研究成果入围“BlackHat USA 2023”

近日，奇安信旗下盘古实验室最新研究成果《Core Escalation: Unleashing the Power of Cross-Core Attacks on Heterogeneous System》成功入围BlackHat USA 2023。

盘古实验室的研究成果此前也曾多次入选 BlackHat。作为国内乃至全球移动安全领域的引领者，盘古实验室研究成果丰硕，在各类主流操作系统和重要应用程序中发现过大量高价值安全漏洞，也多次在极具影响力的工业安全峰会和顶级学术会议发表前沿研究成果；盘古实验室秉承“以攻促防”的理念，协同移动设备厂商一同捍卫用户隐私与设备安全。

奇安信亮相 2023 中关村论坛 为数字经济安全发展建言献策

5 月 25 日——30 日，2023 中关村论坛在北京举行。奇安信集团深入参与平行分论坛、中关村国际技术交大会、科技合作项目主题推介会、中关村论坛展览（科博会）等环节，围绕数据安全、智能城市、科技创新等层面，深度解读网络安全及数据安全，在推动北京建设全球数字经济标杆城市、推动数字经济稳步发展过程中的重要作用。

在 2023 中关村论坛“雄安智能城市分论坛”上，奇安信集团董事长齐向东表示，雄安新区领跑智能城市建设，网络安全能力也需要与时俱进。并提出，以“零事故”为目标，建立一体系、一中心、一平台，为我国智能城市的网络安全防护树立样板。

在 2023 中关村论坛“北京银行 GBIC2 组合金融论坛”上，奇安信集团董事长齐向东表示，风险投资是科技创新的催化剂。在投资等五大驱动力推动下，网络安全行业已进入发展的黄金时代，以数据安全为核心的网络安全产业将迎来爆发式增长。

奇安信亮相 2023 数博会 “奇安天盾”数据安全保护系统正式发布

5 月 26 日——28 日，2023 中国国际大数据产业博览会在贵州贵阳举行。奇安信集团董事长齐向东在参加“东数西算”高端对话时表示，数据安全是“东数西算”战略稳步向前的首要前提，当下“东数西算”存在三大场景风险和三大来源风险。他建议用“零一三”体系，牢筑安全之盾，保护数据安全。

2023 贵州数博会期间，奇安信集团数据安全分公司正式揭牌成立，奇安信集团董事长齐向东出任总经理，同时，奇安信对外发布“奇安天盾”数据安全保护系统。这些举措标志着网络安全国家队全面发力数据安全领域，帮助客户破解“难看清”“难管好”“难防住”等难题，开拓市场新蓝海。

数博会期间，奇安信“网络空间安全态势感知与协调指挥平台”获评 2023 数博会领先科技成果奖“优秀科技成果”；奇安信集团“基于数据沙箱技术的数据安全流通平台”入选 2023 数博会“十佳大数据案例”。

首届“盘古石杯”全国电子数据取证大赛暨数字取证高峰论坛圆满落幕

5 月 26 日——27 日，首届“盘古石杯”全国电子数据取证大赛暨数字取证高峰论坛成功举办。来自全国各地的 101 支精英队伍和超过 300 名取证专家同台竞技，同时，来自产学研各领域的权威专家，聚焦电子数据取证领域热门话题，进行了深度解读和研讨。

首届“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，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发展。

奇安信与贵州联通签署全面战略合作协议

5 月 27 日，在 2023 中国大数据产业博览会上，奇安信科技集团股份有限公司与中国联通贵州省分公司（简称贵州联通）签署全面战略合作协议，未来双方将全面深化业务合作，为中国式现代化的贵州实践提供强有力技术支撑。

协议明确，双方将在产业链培育方面强化技术攻关、加强人才培养；在政企安全市场围绕区域政务云安全、教育行业云安全展开合作；在安全产品孵化层面，积极探索适合贵州本地需求的标准化自研安全产品；在自身安全保障层面，共同开展创新应用树立行业标杆。

吴云坤出席全国信安标委 2023 年第一次“标准周”全体会议

5 月 29 日上午，全国信息安全标准化技术委员会（简称信安标委）2023 年第一次“标准周”全体会议在云南昆明召开。奇安信集团总裁吴云坤出席并发表主题演讲。他建议，从开发、开源、运行部署、自动化渗透测试及软件供应链风险管理上五方面构建关键能力，体系化治理软件供应链安全。

他透露，上述思路、方法和能力建设，奇安信已与多个行业客户一起，在多个重要项目和工程中对软件供应链安全治理进行了实践——北京冬奥组委应用系统生命周期管理及奇安信内部开源软件安全专项治理就是两个典型的成功案例。

全国工商联副主席安立佳莅临奇安信集团调研

5 月 22 日，全国工商联副主席安立佳一行就大中小企业融通发展情况，莅临奇安信集团调查研究。安立佳一行实地参观了奇安信安全中心展厅、工控实验室、司法鉴定所、星舆车联网安全实验室，了解企业科研创新、平台建设、人才培养、生态产业建设等情况。

安立佳对奇安信的发展态势及对网安行业的生态推动给予了高度评价。他表示，很高兴看到奇安信的每一步都紧跟

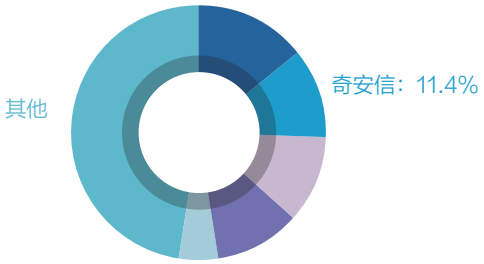
国家发展，安全能力和效果有目共睹，实现了国家网络安全和企业发展的“双赢”。通过今天走访调研，也对我国的网络安全发展有了更大信心。希望奇安信深刻认识大中小企业融通发展对建设现代化产业体系的重要意义，发挥龙头企业的示范引领作用，与网络安全产业生态伙伴一道，为数字中国建设保驾护航。

荣誉墙

IDC 报告：奇安信工业互联网安全管理平台市场份额名列前茅

近日，IDC 发布了首份《中国工业互联网安全管理平台市场份额》调研报告。《报告》显示，奇安信在 2022 年持续进行产品技术能力创新，并在石油石化、电力、轨道交通、智能制造等多个行业落地标杆案例，同比增长达 46.1%，达到行业平均增速的两倍以上，并以 11.4% 的市场份额位列前茅。

中国工业互联网安全管理平台市场份额，2022



数据来源：IDC《中国工业互联网安全管理平台市场份额，2022》报告

2022 年万得 ESG 评级：奇安信集团评为 AA 级行业第一

据知名金融信息服务商万得 ESG 评级（Wind ESG Rating）最新排名，奇安信集团的 ESG 表现被评为 AA 级，成为信息技术服务行业 ESG 综合得分最高、排名第一的企业，也是该行业唯一一家获得 AA 级的企业。

Wind ESG 评级指标体系是参考国际主流 ESG 体系架构，结合中国资本市场发展情况、监管政策和公司 ESG 实践，形成的本土化特色指标体系，能综合反映企业的 ESG 管理实践水平及重大突发风险。此次奇安信的 Wind ESG 评级，反映了资本市场对奇安信履行社会责任、践行可持续发展的高度认可。

奇安信获 SAE 汽车网络安全创新技术奖

2023 年 6 月 7——8 日，由 SAE 国际汽车工程师学会主办的 2023 国际汽车安全大会在上海召开。在汽车网络安全技术评选活动中，奇安信星舆实验室展示的相关安全技术获得广泛好评，在国内外众多竞争对手中脱颖而出，获得了汽车网络安全创新技术奖。

领航云原生安全 奇安信 CNAPP 荣获云原生安全技术创新奖

近日，由工业和信息化部主办的第 31 届中国国际信息通信展览会在京盛大召开，“ICT 中国 · 2023 高层论坛 – 云原生产业发展论坛”在展会同期举行。论坛公布了云原生优秀案例评选结果，奇安信 CNAPP 云原生安全管理平台凭借在云原生安全领域领先的技术架构和出色的实践效果，荣获云原生安全技术创新大奖，继续领跑云安全 & 云原生安全时代。


证　书

奇安信科技集团股份有限公司：

经专家评审，贵公司选送的『奇安信 CNAPP 云原生安全运营平台』荣获：

2023 年度云原生安全守护先锋

-云原生安全技术创新

特发此证，以资鼓励。

2023 年 6 月

奇安信入选全球《静态应用安全测试全景图》代表厂商

近日，国际权威咨询机构 Forrester 发布《Static Application Security Testing Landscape, Q2 2023》报告，评选出全球 22 家静态应用安全测试 (SAST) 代表厂商。凭借过硬的产品、技术和市场能力，奇安信成为亚太区少数入选的三家厂商之一。

奇安信集团获首批 CCRC 数据安全管理认证证书

5 月 19 日，中国网络安全审查技术与认证中心（CCRC）公布了数据安全管理认证名单，奇安信在通过技术验证和现场审核后，正式获得认证证书。


CCRC

数据安全管理认证证书

中国网络安全审查技术与认证中心

作为首批通过数据安全管理认证的企业，获得此项认证是对奇安信在数据安全管理水平方面的全面认可。在认证有效期内，奇安信将为客户提供全面满足合规与治理需求的数据安全服务与解决方案。

齐向东获评“北京市有突出贡献的科学、技术、管理人才”

日前，中共北京市委、北京市政府对第十四批“北京市有突出贡献的科学、技术、管理人才”进行表彰，并颁发荣誉证书。奇安信集团董事长齐向东获此殊荣。

“北京市有突出贡献的科学、技术、管理人才”是以北京市委、市政府名义评选表彰的北京市人才专项奖励项目，每 3 年评选表彰一次，旨在表彰首都经济社会发展中作出突出贡献的科学、技术、管理人才，加强创新型、领军型高层次人才队伍建设，营造“尊重劳动、尊重知识、尊重人才、尊重创造”的良好社会氛围。


荣誉证书

齐向东同志：

被评为“北京市有突出贡献的科学、技术、管理人才”。

特发此证。

奇安信威胁情报入选 Gartner《2023 安全威胁情报产品和服务市场指南》

近日，Gartner 发布了《安全威胁情报产品和服务市场指南》（简称《报告》），奇安信凭借漏洞情报、APT 档案库、邮件检测及基于云端的威胁情报建设入围《报告》。

目前，奇安信威胁情报中心通过极有特色的全量漏洞情报数据和关键漏洞深度分析报告服务引领国内漏洞情报服务，为客户提供真正基于威胁情报的漏洞风险缓解服务。在本次《报告》中，奇安信是国内唯一一家在漏洞情报市场被认可的代表性厂商。

奇安信入选国资委《中央企业科技创新成果推荐目录》

近日，国务院国资委发布了《中央企业科技创新成果推荐目录（2022 年版）》，经过严格审查与专家评审，奇安信态势感知与安全运营平台成功入选。

《中央企业科技创新成果推荐目录》旨在加快科技创新成果的应用推广，本次科技创新成果目录共涉及核心电子元器件、关键零部件、分析测试仪器、基础软件、关键材料、先进工艺、高端装备等七个领域，包括 369 项技术产品，态势感知与安全运营平台是唯一入选的网络安全产品。

奇安信再获 CNNVD 多项重磅大奖

5 月 24 日，国家信息安全漏洞库（CNNVD）2022 年度工作总结暨优秀支撑单位表彰大会在中国信息安全测评中心隆重举行，奇安信作为 CNNVD 一级技术支撑单位，凭借在漏洞报送数量和质量等方面的突出贡献，在 167 家技术支撑单位中脱颖而出，荣获“优秀技术支撑单位”“ 高价值漏洞优秀贡献单位”“高价值通报优秀贡献单位”三项大奖。

作为 CNNVD 最早的技术支撑单位之一，奇安信已经多次获得 CNNVD 年度优秀技术支撑单位等荣誉，充分体现了国家机构对奇安信技术能力、支撑工作的高度认可和肯定。

社会责任

2023 心安助学首个项目启动：“中国传媒大学——奇安信助学基金”正式设立

6 月 12 日，“中国传媒大学——奇安信助学基金”启动仪式在中国传媒大学明德楼举行。传媒大学教育基金会秘书处秘书长杨鹏与北京奇安信公益基金会秘书长齐子昕签署捐赠协议，宣布成立“中国传媒大学 – 奇安信助学基金”，该基金将为中国传媒大学计算机与网络空间安全学院家庭经济困难的学生提供社会实践支持、紧急救助、实习奖助学金等帮助。

据悉，“心安助学 · 高校教育助学”项目自 2022 年正式设立以来，已累计资助 7 所高校、实施资助学生 98 名，其中发放奖学金 58 人、助学金 20 人、疾病救助 3 人、支持社会实践 17 人。今年，基金会已经确定将新增资助约 30 所高校，总资助高校数量将达到 40 所，总捐赠额将超过 860 万元。

基金会秘书长齐子昕获北京青联 2022 年度优秀提案建议奖

近日，北京市青年联合会第十二届委员会第三次常委（扩大）会议在北京会议中心召开，通报表彰北京市青联 2022 年度委员优秀提案和建议。

北京市青年联合会第十二届委员会经济界别工作委员会副秘书长、北京奇安信公益基金会秘书长齐子昕提交的《关于推动北京数字经济高质量发展的建议》获评北京市青年联合会 2022 年度“优秀提案建议”。


荣誉证书

齐子昕：

您的《关于推动北京数字经济高质量发展的建议》被评为北京市青年联合会 2022 年度

优秀提案建议

特发此证，以资鼓励！

北京市青年联合会

二〇二三年四月

奇安信基金会积极开展“我认领 我服务”路口文明引导志愿服务活动

为积极响应首都精神文明办《“我认领 我服务”路口文明引导志愿服务活动》的倡议，近日，北京奇安信公益基

金会正式启动“我认领，我服务”路口文明引导志愿服务项目。今年 5 月——9 月，每单周周五下午 4——5 点，志愿者将在展览馆路和车公庄大街交叉口开展志愿服务，并持续招募志愿者。

基金会负责人表示，道路安全、交通文明不仅体现着城市文明，更是对人民群众生命负责的一种体现。此次“我认领，我服务”路口文明引导志愿服务活动，是奇安信基金会勇担首都社会治理责任的一次有益实践。今后，基金会将继续探索更多的志愿服务模式，举办类似活动，为建设文明和谐社会做出贡献。

京蒙协作结新对 奇安信公益基金会与巴林左旗正式签约

5 月 23 日，“‘百家民企（商协会）结对百个乡村振兴示范村’暨‘京蒙民营企业进边疆行动’”正式启动。启动仪式上，民营企业、商协会代表分别与乡村振兴示范村、乡村振兴重点帮扶旗县、边疆旗县签约，奇安信公益基金会作为“京蒙协作”企业奇安信集团的委托代表，与内蒙古巴林左旗签约，正式结对帮扶。

奇安信基金会负责人表示，基金会受奇安信集团委托，积极贯彻落实党中央、国务院关于倾斜支持国家乡村振兴重点帮扶县的决策部署，积极响应全国工商联《“万企兴万村”行动倾斜支持国家乡村振兴重点帮扶县专项工作方案》，与巴林左旗正式结对帮扶后，基金会也将从巴林左旗本土实际需求出发，着眼特色产业深化、组织和人才培育、人居环境改善等方面，充分发挥民营企业的优势和公益的力量，带动当地群众致富，推动京蒙协作取得更大成果。

奇安信基金会在安徽省舒城县捐资助学

近日，全国政协常委、经济委员会副主任，国务院发展研究中心原党组书记、副主任马建堂率调研组赴安徽舒城开展调研，奇安信公益基金会秘书长齐子昕随队参与调研。

基金会在考察走访过程中发现，杜店中学位于山岗地区，在万佛湖环湖大道开辟之前，地理位置相对偏僻。该校有近 1800 名学生，其中大部分是留守少年。为帮助杜店中学的学生获得更好的学习环境，奇安信基金会决定向舒城县杜店中学捐款 10 万元。

创客汇七大网络安全技术创新方向

作者｜奇安信集团产业发展研究中心

国际知名的网络安全大会 RSAC 已经落下帷幕，其中创新沙盒的板块引领了网络安全创新创业的风向。我国北京网络安全大会（BCS）的创新创业板块“创客汇”也已经选出今年的 50 强企业，并将于本月展开复赛。本文梳理了本次创客汇七大技术创新方向，从中体现出我国网络安全创新既紧跟国际主流方向，同时又贴合我国网络安全需求；技术创新与迭代的节奏也更加快速。

创新方向 1：数据安全

数据安全是近年来国内外安全创新的焦点，随着我国数字化产业进程的加快和安全合规要求的落实，推动数据安全创新更加密集和细化。

（1）合规依然是数据安全的主要驱动力

数据全生命周期安全监测和管控：基于内核级可观测的可编程工具，用以监视和控制系统中发生的各种事件。

数据安全治理：加强大语言模型在数据安全垂直领域的应用，实现敏感数据发现、数据分级分类、数据行为分析、数据安全报告。

数据恢复：满足多种异构云平台的备份需求，做到快速容灾。

数据安全运营：一体化、自动化，安全与价值融合，安全与治理融合。

（2）面向业务的数据安全闭环整体解决方案

数据安全闭环解决方案：数据安全咨询、管理体系建设、技术能力体系建设，深度学习的敏感数据的自动识别和分类算法，包括图片、敏感文本等识别已经产品化；基于深度学习的风险识别和异常监测算法。

业务数据安全：为业务数据流转各个阶段提供数据转发精细化控制，将数据流转安全进行统一编排和专属保护。

（3）AI 技术在数据安全领域的应用

基于 AI 的数据安全引擎：统一编排、自适应、身份智能化、决策动态化。

数据访问治理：基于 AI 规则学习的隐私合规管理。

（4）区块链和隐私计算与数据安全的结合

区块链安全服务平台：包括区块链系统全生命保护周期解决方案，智能合约安全审计服务，链平台安全检测服务，虚拟资产追踪溯源和调查取证

数据安全是近年来国内外安全创新的焦点，
随着我国数字化产业进程的加快和
安全合规要求的落实，
推动数据安全创新更加密集和细化。

服务。

区块链全生命周期版权保护：保护高价值数字资产，防止逆向工程何自动攻击。

区块链平台和应用产品：软 / 硬件协同数据安全流通解决方案，数据全生命周期安全管控和流通。

隐私计算：开源开放的生态，实现数据安全与价值流通。

> 得益于生成式 AI 的爆发，
> 今年安全智能化与自动化成为大热门，
> AI 应用于网络安全的各个领域，
> 大幅提升安全能力。

创新方向 2：安全智能化

得益于生成式 AI 的爆发，今年安全智能化与自动化成为大热门，AI 应用于网络安全的各个领域，大幅提升安全能力。

（1）AI 用于云原生安全

用 AI 构建高级防御框架体系，对攻击行为的机器学习，利用深度学习发掘：合法程序的行为特征、攻击过程中攻击行为的关联，利用经过训练的模型在实际部署环境中自学习，检测未知威胁。

（2）AI 用于业务安全

基于专家规则和 AI 分析的业务安全解决方案。通用大模型中积累了多个用户大量业务安全场景的经验，可以检测通用安全隐患，实现了多业务场景的经验迁移。专用小模型可以实现“小数据”建模，应对特定业务的异常场景，提供更为精准的的分析能力。场景化策略可以高效沉淀业务专家的经验，用成本最低、效率最高的方式检测已知异常场景。

（3）AI 用于软件供应链安全

使用 GPT 模型对代码进行自动审计，生成代码审计缺陷报告。识别有效缺陷，减少误报，并给出缺陷等级和优先级。对有效缺陷进行修复建议，指导用户改进修复代码，提高代码安全性。使用 GPT 模型代码片段溯源检测的准确率和检测速度。

（4）基于 AI 的智能攻防

AI 漏洞挖掘：挖掘未知漏洞 & 完善漏洞特征库，AI 缺陷修复，缺陷解释，生成修复代码。

（5）基于 AI 的安全运营

利用人工智能和机器学习，获得各种风险模型和场景，提升自动化检测和响应能力、智能报告和决策，极大提升分析师人效。

（6）AI 用于安全测试

基于 AI 模型的特征匹配意见反馈：使用 AI 模型，结合业务和漏洞库生成修复建议，帮助修补目标增强网站防御能力。

创新方向 3：实战化网络安全攻防

得益于关键基础设施和重要行业对实战化攻防的重视，实战化网络安全攻防成为具有我国特点的网络安全热点创新方向。

自动化渗透测试：提供连续性和及时性的渗透测试服务，先于攻击者发现并最大限度发现风险。学习不断进化的智能决策引擎 主动式漏洞优先级（VPT）技术 自动化敏捷协同技术 基于智能博弈的攻击决策技术 基于模型的动态可视化技术。

网络安全靶场：面向行业应用的全栈数字靶场平台。

攻击者情报共享平台：SAAS 化形态情报平台汇聚所有采集的攻击者原始数据，经匹配、分析，形成情报网络，共享情报，指导联防联控。

安全风险评估自动化：BAS 实战防御体系有效性评估，防御设施短板 & 风险链路全面可视，非接触式评估，无损业务生产。

攻击面管理 + 自动化模拟攻击：提供全方位覆盖式安全建设。

创新方向 4：网络安全管理与运营

网络安全管理与运营是我国网络安全长期以来的创新方向，同时，热点技术不断演进发展。

资产暴露面检测与管理：信息系统和域名暴露、移动端应用暴露、邮箱和人员安全、文档和代码暴露、暗网和匿名社交社群监控、VIP 数字风险检测。

主动安全运营：基于人工智能知识图谱的攻击面技术，更好地梳理清楚资产、漏洞、攻击与防御之间的关系，具体资产数量、资产之间有哪些访问

路径、哪些资产上有漏洞，有哪些利用路径、资产会被哪些攻击技术攻击、攻击成功以后会对网络和系统造成多大的影响、如何收敛攻击面来减少黑客攻击的机会。

多平台统一的身份安全（ITDR）：事前加固——全面了解身份攻击面并削减身份威胁面，事中监控——全面监控身份攻击活动，实时了解身份攻击态势，事后阻断——快速响应阻断身份威胁。

智能化、自动化安全运营：安全协同响应，全攻防运营服务， AI 持续赋能主动安全免疫、智能攻防运营、集成 soar 的安全自动化协同处置管理、自动化攻击渗透、自动化防御。

SAAS 化网络安全运维：多云环境下的安全运维新模式。

创新方向 5：汽车网络安全

得益于智能网联汽车产业的大发展，汽车网络安全成为具有我国特点的网络安全创新方向。

纵深防御：智能网联汽车信息安全纵深防御体系建设。

嵌入式安全：汽车智能座舱芯片研发。

机器学习在汽车网络安全中的应用：使用机器学习算法进行安全架构模式匹配，利用机器学习算法对大量的网络架构和攻击过程进行处理、分析和训练，创建未知协议模型和未知漏洞画像，通过对网络协议、数据流、软件和硬件的逻辑或者物理连接进行分析，准确的匹配出漏洞或者威胁，并自动修复或给出修复建议。

创新方向 6：软件供应链安全

软件供应链安全是国际网络安全热点创新方向，在我国同样具有很高的热度。

开发安全：自研和外包开发场景下的安全管控系统，开发安全与数据安全融合，面向开发态、测试调试态、运行态代码，率先引入 AI 技术，对白盒、灰盒和黑盒安全技术进行变革。

全生命周期代码安全治理：自动化能力、全面的治理能力，代码逻辑的智能解释，自动生成修复代码，智能的安全代码编写建议。

代码安全检测：检测自研代码的安全和质量缺陷、检测引入开源组件的漏洞、检测开源组件 license 合规性、检测引入开源代码的风险、检测代码自研率、检测代码中隐私和敏感数据、检测成品软件开源组件漏洞，人工智能技术应用于软件供应链安全。

创新方向 7：身份安全与零信任

身份安全与零信任是国际网络安全热点创新方向，在我国同样具有很高的热度。

高级身份威胁检测：身份安全云 -ITDR 身份威胁检测与响应，全场景、一体化的身份认证 + 高级身份威胁检测的平台。

零信任 + 云原生安全：通过云、网、安、服深度融合的 SASE 云服务平台交付一系列零信任核心能力。

我国庞大的工业和数字化产业为网络安全提供了更为多样化的创新方向，除上述七大创新方向外，工控安全、API 安全、密码应用、网络安全保险、网络安全网格架构等，也是国内较为热门的创新领域。安

关于作者

奇安信集团产业发展研究中心是奇安信集团的产业研究团队。专注网络安全领域，跟踪国内、外产业发展现状与趋势，研究网络安全各细分领域，包括产品技术、市场、投融资和产业生态，为网络安全从业人员提供新视角，为企业决策提供依据，推动网络安全产业发展。

陈华平

奇安信集团副总裁，产业发展研究中心负责人。

乔思远

产业发展研究中心研究员，主要负责宏观分析和产品技术研究。

万物皆可“DR”：威胁检测与响应缘何热度不减

作者 | 李栋

如果生成式 AI 是 RSAC 2023 的一个焦点，XDR（可拓展威胁检测与响应平台）可以称为会议的另一焦点话题。会议期间，思科、CrowdStrike 等多家顶级安全厂商均发布了 XDR 新产品，从 2022 年持续火热至今的明星产品热度仍然不减， RSAC 2023 见证了 XDR 营销活动的激增。思科高级副总裁兼安全总经理 Tom Gillis 表示，XDR 成为 RSAC 2023 的焦点话题。你很难找到一个不谈 XDR 的安全供应商。

AT&T 的安全专家 Rakesh Shah 认为：端点数量的增加、攻击面放大、勒索攻击增加等因素成为 XDR 产品继续大热的推动因素。

XDR 成为安全的前沿和中心

早在 RSAC 2022 上，XDR 这个缩略词就已成为热点，遍布在大会的展厅，终端安全与 SIEM 厂商发布了各自的 XDR 方案。

XDR 宣称可以融合多个来源的数据，实时检测恶意活动，实现及时的响应。没有 XDR，我们就无法与日益复杂的攻击者作战。身处混合网络环境、面对多个安全供应商的用户，面对虚假威胁警报的困扰，以及日益增加的安全威胁，对扩展检测和响应 (XDR) 有着较高的期望，期待其能实现更高的安全可见性，简化安全运营。

2022 年度安全运营技术成熟度曲线（Hype Cycle），XDR 达到 Peak of Inflated Expectations 的顶端。这也难怪 XDR 的热度在 RSAC 2023 上持续，成为安全的前沿和中心。

对于 XDR，业界却依然没有公认的定义。作为由分析师创造的术语，XDR 被安全厂商广泛采用，但对其含义仍未有完全的共识。每家安全企业对 XDR 都有不同的定义。推广 XDR 的企业表示自己的方案包括各种功能，如终端保护、EDR、MDR、遥测、AI/ML、NDR、邮件、Web、威胁情报等。

在其关于什么是 XDR 的页面中，

> 身处混合网络环境、面对多个安全供应商的用户，
> 面对虚假威胁警报困扰，
> 日益增加的安全威胁，
> 期待扩展检测和响应 (XDR) 能实现更高安全可见性，
> 简化安全运营。

思科公司指出 XDR 跨邮件、端点、服务器、云工作负载和网络收集和关联数据，实现对高级威胁的可见性和掌握上下文。从而可以对威胁进行分析、确定优先级、狩猎和应对，避免、数据丢失和安全漏洞。简而言之，XDR 利用最新技术收集和关联威胁信息，实现较高的可见性；同时，采用分析和自动化技术帮助检测当前和潜在的攻击。

Gartner 给出 XDR 的定义是：XDR 是一个基于云交付的平台，可以将不同安全防御、检测和响应组件的数据和警报进行整合、关联，并进行上下文分析。由于包括多个单点解决方案和高级分析技术，可将多个来源的警报与安全事件进行关联，从而实现更准确的检测。

在技术模型中，XDR 结合了安全信息和事件管理（SIEM）、安全编排自动化和响应（SOAR）、端点检测与响应(EDR)及网络流量分析(NTA ）等多个第三方安全产品，既可以获取多点安全能力与多源安全数据，又能将多维数据关联分析、编排及自动化响应。

在本次 RSAC 中，有安全专家对 XDR 的核心能力做了概括，如聚合 & 关联多个数据源、对告警进行优先级排序、对恶意行为做出响应等。

IDC 安全与信任集团副总裁 Frank Dickson 表示：“XDR 的真正衡量标准是它能够为组织带来实际的安全成果、真实且可衡量的好处——早期检测、影响优先级排序及有效且高效的响应。”

XDR 不是 SIEM

对于 XDR 和 SIEM 存在很多混淆。许多 XDR 供应商声称用户不需要 SIEM，他们的 XDR 可以替代 SIEM。对此，思科高级副总裁兼安全总经理 Tom Gillis 表示，XDR 的用途不同于传统的安全信息和事件管理（SIEM）。没有响应的安全检测是不够的，但没有检测的安全响应是不可能的。思科希望提供的是自动化、云优先的单一检测和响应平台。借助 XDR，安全运营团队可以在威胁造成重大损害之前做出响应和补救。

因此，尽管 XDR 与 SIEM 有众多相似之处，SIEM 和 XDR 都收集、关联和分析数据，以发现和应对威胁。但 SIEM 解决方案仅限于向 IT 团队发送安全警报，因为其无法跨端点自动对安全事件进行响应。XDR 解决方案则可以自动调整网络和端点的保护措施，仅提醒安全运营团队调查重要的安全事件。

传统 SIEM 让组织管理以日志为中心的数据并在数天内分析出结果。XDR 强调使用以遥测为中心的数据，在几分钟内发现异常。也就是 XDR 旨在解决 SIEM 过于关注日志收集、合规和传统关联规则而无法有效阻止网络攻击的问题。

XDR 可与已有的安全工具配合使用，包括 SIEM。或许 SIEM 仍将继续成为您安全运营的一部分。我们要做的是如何扩展 SIEM 以使其变得更好。

未来 XDR 的功能可能将被 SIEM 集成，或者两者将集成一个平台，无论它被称为什么，将继续成为安全运营的核心。

万物皆可“DR”：X 成为“所有”

本次推出新型 XDR 的安全厂商思科和 CrowdStrike，均把接入 EDR、邮件安全、防火墙、SASE、身份安全等更多第三方安全工具作为产品卖点，这也充分展示了 XDR 万物皆可“DR”的产品特性。在 Cisco 的 XDR 解决方案中，“X”甚至代表

“所有”，而不是通常所说的“扩展。

思科 XDR

思科推出的新型扩展检测和响应（XDR）平台，融合了网络检测和响应（NDR）及终端检测和响应（EDR），并提供 "跨域遥测"，在提供威胁检测和优先次序方面，该产品还通过 "接近实时 " 的方式从安全信息和事件管理（SIEM）产品中脱颖而出。

此外，思科 XDR 的与众不同之处在于提供了来自各种安全工具的 "高保真数据"，如用于终端的 Cisco Secure Client（以前的 AnyConnect）。XDR 平台集成了大量主要的第三方安全产品。其中包括 EDR 工具（Microsoft Defender、Cybereason、Palo Alto Networks Cortex XDR、SentinelOne Singularity 和 Trend Micro Vision One）；电子邮件安全（Microsoft Defender for Office、Proofpoint）；Palo Alto Networks 的下一代防火墙；Microsoft Sentinel 的 SIEM；ExtraHop Reveal(x) 的 NDR。据思科表示，这一次是这段时间以来思科最大规模的一次安全产品发布，这代表着思科在实现其安全云愿景的道路上迈出了重要一步，即为现代安全提供一个全面、统一的平台。

CrowdStrike XDR

CrowdStrike 新的管理型 XDR（扩展检测和响应）产品——Falcon Complete XDR，沿用了 CrowdStrike 流行的管理型检测和响应（MDR）服务的模式，整合了 CrowdXDR 联盟中关键领域的供应商的工具，如安全服务边缘（Cloudflare、Netskope、Zscaler、Skyhigh Security、Menlo Security）；身份安全（Okta、ForgeRock、Microsoft Azure Active Directory、Ping Identity）；电子邮件安全（Mimecast、Proofpoint、Microsoft 365、Cisco Secure Email、Abnormal Security）；网络检测和响应（Corelight、ExtraHop、Vectra）；以及防火墙（所有主要的防火墙供应商，如 Palo Alto Networks 和 Cisco）。

> 无论 XDR 与 SIEM 形态如何演进，
> 检验它的指标只有一个——
> 如何让组织更早地发现和响应安全威胁。

XDR 在国内如何落地?

业界给了 XDR 很高的地位，Gartner 2020《顶级安全和风险管理趋势》报告还将其列为第一大安全趋势，但这个概念也一直饱受争议，主要问题是需要兼容多维度安全设备，并实现联动，落地难度大。

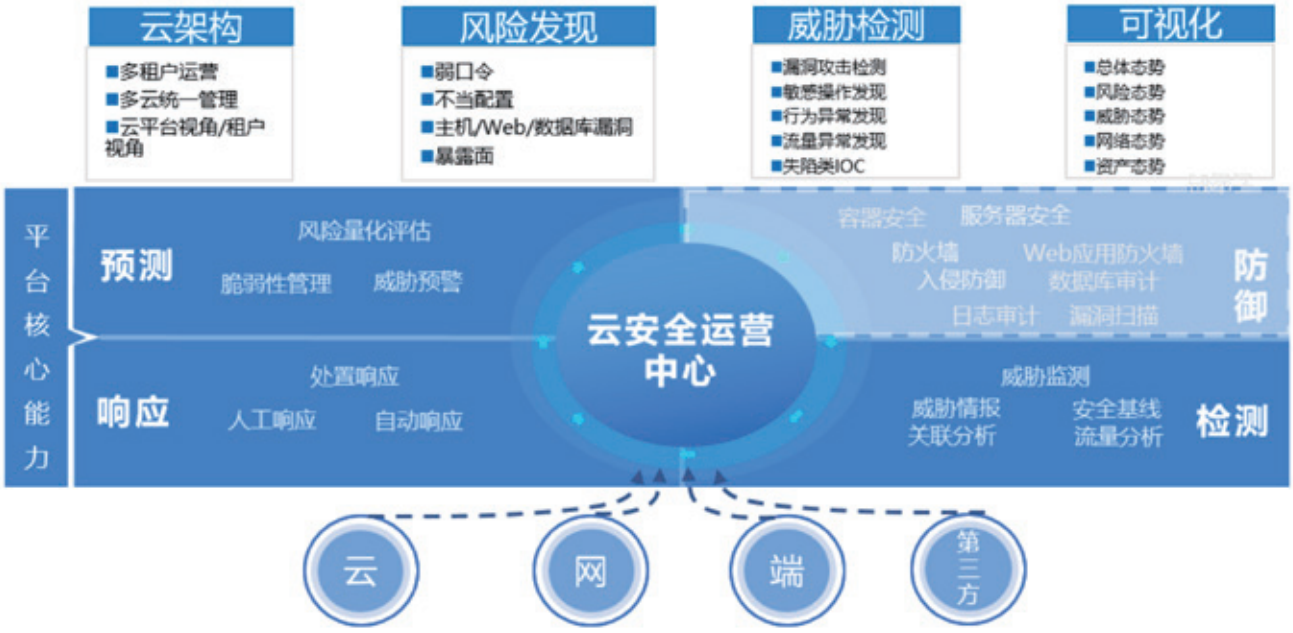
笔者认为，奇安信云安全中心（CSC）是一款面向云安全运营管理的威胁检测与响应系统（XDR），通过对资产、配置、漏洞清点，资产脆

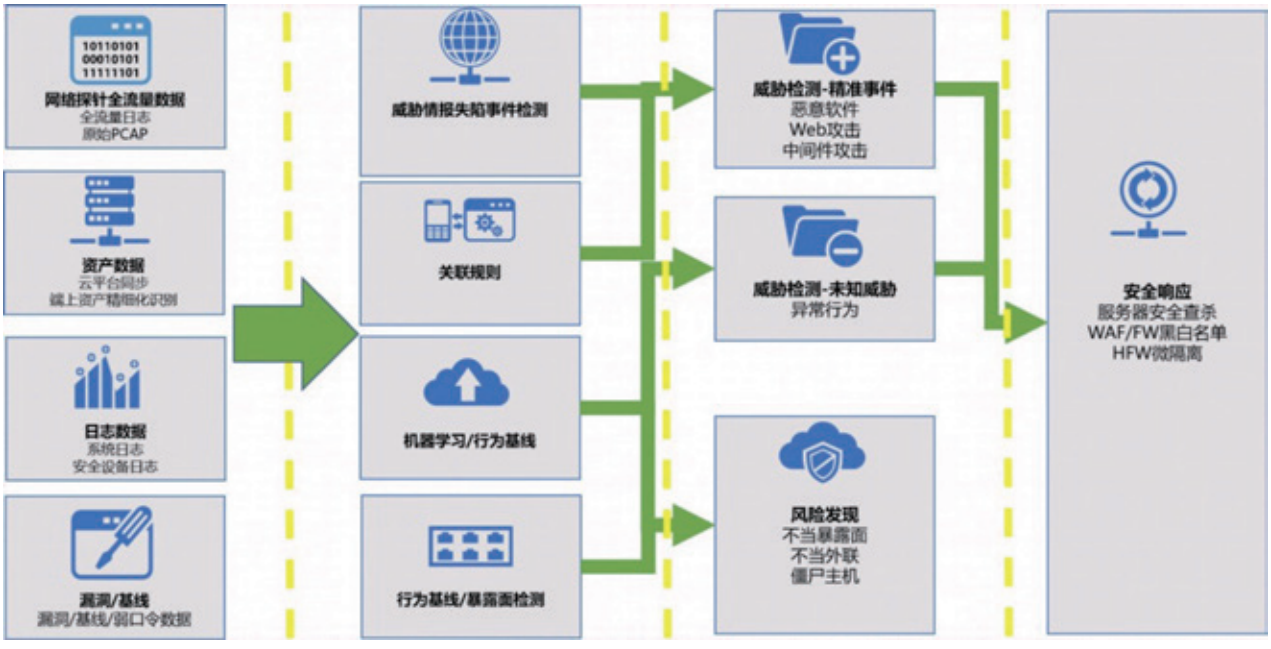
弱性评估，东西向流量威胁分析，云上安全能力联动等能力，帮助用户实现威胁预警、风险识别、攻击链还原、联动响应的自动化安全运营闭环。

XDR 要成功落地，至少需要具备以下三项核心能力。

1. 多源数据采集

奇安信云安全中心（CSC）针对云化数据中心场景设计，能够精准地获取云内资产信息，对来自云、网、端、第三方的全流量进行采集分析和威胁检测。



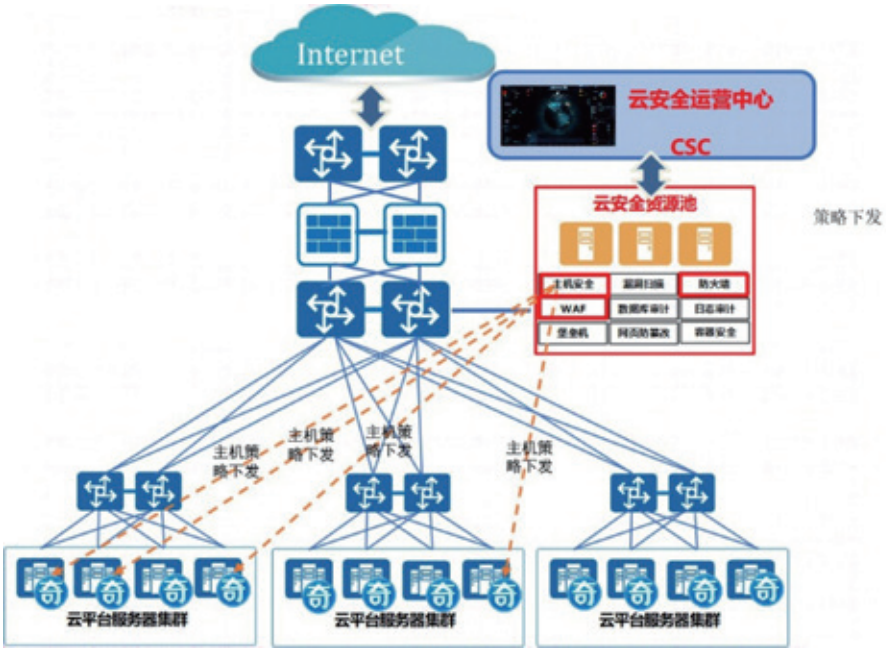


2. 威胁建模分析

威胁建模是各类安全产品实现威胁检测能力的关键环节，奇安信云安全中心（CSC）自主开发的 SABRE 引擎，可以实现对多日志来源关联分析的能力，对安全事件进行有效的去误报降噪和分级分类，同时产品采用了分布式架构，性能按需扩展，解决了传统威胁建模性能难以扩展的问题。

3. 响应处置

奇安信云安全中心（CSC）可联动防火墙、WAF、主机安全设备等云安全组件，进行快速响应处置，形成检测与响应的闭环。



结语

RSAC 作为网络安全的风向标，XDR 在本次大会继续保持热度，将会吸引更多的客户关注，也会让更多的厂家进入这个领域，这意味着安全运营已经成为安全的痛点，成为网络安全的必争之地。

无论 XDR 与 SIEM 形态如何演进，检验它的指标只有一个——如何让组织更早地发现和响应安全威胁。安

关于作者

李栋

奇安信资深云安全专家，网络安全老兵。

美军迈向战术云的九个步骤

作者 | 赵慧杰

编者按：

美国陆军第 112 信号营指挥官瑞安·肯尼、陆军特种作战司令部 G6 首席信息官保罗·斯帕克斯及陆军系统集成官员韦维尔·威廉姆斯联合撰文提出迈向战术云的九个步骤。

奇安网情局编译有关情况，供读者参考。

美国防部正在考虑采用云解决方案为战术指挥控制系统实施零信任原则。战术云解决方案的部署，将提高灵活性、可扩展性和互操作性。此外，上述解决方案还将支持任务合作伙伴环境的开发，并帮助国防部实现具有联合数据结构的统一网络。

云环境的好处有据可查。云解决方案具有可扩展性和弹性，这意味着美国防部可以根据需要添加或删除计算和数据存储资源。美国防部采用云解决方案变得更加敏捷，并部署新功能以快速响应不断变化的需求。

云解决方案提供了即插即用的容器化环境，各机构可以在其中快速安全地部署和拆除存储、服务器和服务。这使云解决方案成为建立具有不同访问控制和密级需求的任务合作伙伴环境的理想选择。美国防部可以使用云来管理可定制的、片断的任务合作伙伴环境，并在启用零信任原则的情况下，提供精细的设备、资源、应用程序和数据管理。

美国防部可以通过战术云更快地部署应用程序和服务。云提供了通用的应用程序协议接口（API），可以更轻松地在软件定义网络中集成新应用程序和自动化数据线程。这些 API 使开发人员能够快速向其应用程序添加新特性和功能。云服务通常提供全面的归档和支持，使开发人员更容易使用其服务。通过公共云环境，可以更轻松地实现统一网络和数据结构。

云解决方案可以消除对物理基础设施和人员成本的需求，同时促进跨多个部门和服务的资源共享，从而降低与基础设施和维护相关的一些成本。从长远来看，将这些资本投资成本从政府拥有的实体转移到商业实体，可以减少美国防部预算的开销，并为其他指挥、控制、计算机、通信、网络、情报、监视和侦察（C5ISR）投资腾出空间。

云解决方案还可以改善用户体验。云解决方案使得用户能够从任何位置

美国防部正在考虑采用云解决方案
为战术指挥控制系统实施零信任原则。
战术云解决方案的部署，
将提高灵活性、可扩展性和互操作性。

和设备访问数据和应用程序。开发美国防部战术云环境将使战术网络组合和最终用户设备通过商业蜂窝和互联网连接访问云托管应用程序成为可能。这将增加可用性和访问权限，同时提供新的战术用例。

以下步骤可以帮助美国防部提供战术云服务。

步骤一：确定战术云环境、战术 C5ISR 任务指挥系统和数据所有者的利益相关者和批准机构。谁承担任务风险最终将决定谁获准使用战术云。同样，各种利益相关者开发、操作和维护任务指挥系统。最后，流入和流出战术边缘的数据可能不仅仅存在于战术云环境中。通过美国陆军“融合项目”（Project Convergence）系列等活动与这些合作伙伴合作是解决集体 C5ISR 现代化和集成问题的好方法。

步骤二：确定各单位所需战术数据和工作负载的类型并确定优先级，总部应迁移至云端。首先确保它们适用于云环境。如果应用程序不是云原生的，则必须首先将其容器化并在云环境中进行测试。一些应用程序和服务可能不适合云。同样，许多业务流程应用程序不需要驻留在战术云环境中。用户的工作配置文件可以保持一致，但会根据他们当前扮演的角色而有所不同。

步骤三：在设计战术云解决方案时，考虑美国防部、联盟和任务合作伙伴间统一战术网络和联合数据结构的整体需求。让网络和数据工程师及早参与战术云解决方案的开发，有助于确定影响云工程的约束和限制。应在整个设计过程中解决跨域解决方案、数据共享限制和消息兼容性需求。此外，在网络连接可能面临拒止、断开连接、间歇性或带宽受限环境的战术环境中，云托管数据和工作负载可能不合适。在这种情况下，可能需要考虑云服务的前沿计算。

> 战术云解决方案的部署
> 有可能统一美国防部内的数据结构和网络。
> 相关解决方案还可以通过快速部署、
> 容器化安全措施和相对较低的成本
> 来支持任务伙伴环境。

步骤四：评估不同云服务提供商的安全能力，选择满足美国防部安全要求的供应商。美国联邦风险和授权管理计划（FedRAMP）计划管理办公室实施联邦风险和授权管理计划。该计划根据《美国联邦信息安全现代化法案》和美国行政管理和预算局（OMB）通告 A-130（标题：将信息作为战略资源进行管理）提供了一种标准化的云服务产品安全授权方法。根据这些要求，考虑企业合作伙伴和美国防部机构必须在各自的风险管理框架内运作的角色和责任。

步骤五：制定全面的安全计划，定义保护云中数据和工作负载的措施。该计划应包括访问控制、数据加密和事件响应协议。网络安全监督并没有在云环境中结束。它必须扩展到传输、网络和最终用户设备，云数据和工作负载最终将通过这些设备传输。战术云解决方案可能会交付给最终用户设备。因此，适当的安全措施必须识别这些相关风险并制定适当的控制措施。

步骤六：实施零信任、多因素身份验证和其他安全控制，以确保只有授权用户才能访问敏感数据和系统。设备及其战术云应用程序的合规连接可以限制风险。此外，通过零信任管理用户配置文件不仅通过控制用户可以看到的应用程序、服务和数据来降低风险，而且还提供了开发任务合作伙伴环境的新方法。最后，在战术云环境中，零信任协议的使用可以限制网络和环境中横向移动的风险，从而在其他风险管理控制失败的情况下降低潜在的网络风险。

步骤七：与云服务提供商合作，建立清晰的沟通渠道和事件响应协议。在军事危机时期使用战术云解决方案需要私营和公共机构间的合作。如果发生安全漏洞或其他问题，美国防部机构需要与行业合作伙伴密切协调。它们必须建立标准，以确定事件的严重程度和适当的响应措施。美国防部应为国防部和云服务提供商人员建立一个安全且专用的通信平台，以讨论事件、共享信息和协调响应活动。此外，各方都应制定预先制定的事件响应计划，其中概述在事件期间必须遵循的

特定角色、职责和流程。

步骤八：组织实施将需要更新的业务流程、C5ISR 治理模型和培训。云解决方案的使用将使跨员工职能的新用例成为可能。随着新用例的出现，将会发生中断，并且业务流程将需要修改。此外，正如不同网络的管理需要审批官员间的共同协议一样，云解决方案的使用也将如此，特别是在战术环境中。最后，美国防部用户将需要培训来交付和管理云基础设施，并管理其在这些解决方案中的驻留。

步骤九：云环境的监督必须解决几个挑战。如果美国防部采取所有必要的预防措施来开发安全的云解决方案，那么总会有一些风险。这是因为不可能消除所有潜在的安全威胁或漏洞。即使在美国防部采取措施保护其云环境之后，一些主要风险可能仍然存在，包括：

- 用户威胁：有权访问敏感数据或系统的用户可能有意或无意地危及安全。这可能是由美国军事人员或任务伙伴造成的。除监控云环境中的用户外，还应考虑端点检测和响应（EDR）措施以减轻最终用户设备的威胁。通过在端点遏制危险，EDR 有助于在危险传播前将其消除。
- 网络攻击：战术云环境的网络安全监督应包括多种措施，例如，实施强大的身份验证和访问控制措施，利用加密技术保护传输中和静态数据，以及实施全面的事件响应计划。此外，美国防部应该对用户进行最佳实践教育，使用自动化工具检测和响应恶意活动，并部署补丁管理流程。
- 数据泄露：敏感数据可能因人为错误或系统故障而无意中被暴露或访问。为减轻这些风险，美国防部应制定全面的数据安全政策，实施强有力的访问控制措施，并启用漏洞扫描和补丁管理。此外，美国防部必须监控系统是否存在可疑活动，并部署自动日志记录系统来跟踪用户活动，同时制定概述在发生泄露事件时应采取步骤的数据泄露响应计划。
- 合规性问题：美国防部可能需要遵守管理敏感和机密数据的使用和保护的相关法律、法规或政策。美国防部必须确保敏感数据在适当的位置安全存储和加密。这可能包括使用基于云的存储解决方案或本地数据中心。此外，美国防部必须确认只有授权人员才能访问和共享敏感数据。

战术云解决方案的部署有可能统一美国防部内的数据结构和网络。上述解决方案还可以通过快速部署、容器化安全措施和相对较低的成本来支持任务伙伴环境。为了在机器速度决策可能最重要的未来冲突中战斗并取胜，美国防部需要开始为战术指挥控制系统采用云解决方案。安

关于作者

赵慧杰

虎符智库专家、网络空间安全军民融合创新中心高级研究员。长期从事网络安全、互联网发展等领域研究工作，对外军网络战、国际网络安全态势、全球网络空间竞合及新技术新应用发展等具有深厚研究造诣，先后获得军内成果奖七项。

安全事件运营 SOP：钓鱼邮件

作者 | 武鑫

安全事件的种类繁多，但处理起来并非无据可循。经过大量的运营处置实践，总结出常见的处置标准操作程序（SOP）。

本文将从攻击、检测处置和防范三个维度，分别对应介绍钓鱼攻击方式、钓鱼邮件安全事件运营 SOP 及防范措施。

1. 钓鱼攻击

1.1 钓鱼攻击概述

利用社会工程学进行攻击，是实战攻击中出现率非常高的手法之一。

使用钓鱼的方式突破边界，也是实战攻击中出现频率非常高的手法。

将社工和钓鱼结合起来用，是实战中最为常见、高效、经典的攻击姿势。从目标来看，社工钓鱼主要可以分为以下几类。

- **信息获取类：**目的在于收集目标相关的账号密码、VPN 地址等敏感信息，如：1）通过联系客服，沟通目标及相关系统的试用，获取试用账号密码，登录系统后进行渗透测试；2）通过信息收集，获取目标相关的即时通信方式，混入 QQ 群、微信群获取试用系统地址相关信息、公司 VPN 等。
- **样本投递类：**制作能绕 AV 的样本，通过沟通、邮件等方式投递给目标相关的员工，如：1）针对 HR 通过微信发送绑有后门的简历；2）联系销售发送绑有后门的客户需求资料；3）通过伪造目标企业内部的邮箱发送钓鱼邮件。

1.2 钓鱼攻击要点

在开展钓鱼攻击前，需要针对目标公司、人员职务、企业邮箱及使用的终端杀软等进行尽可能多的信息收集，知己知彼方能提升中招率。其中有几个关键要素，需要精心准备。

- 钓鱼攻击方式：至少可以是邮件钓鱼、网页钓鱼、WiFi 钓鱼，也可以结合三者同时进行。笔者经历过比较厉害的一次是攻击队对某个开发人员进行钓鱼，先发带有恶意附件的钓鱼邮件让其通过 CS 上线，并在终端上翻看 IM，进行手机号等敏感信息收集，随后由于意外掉线。攻击队模拟公司安全人员，拨打其电话并告知已经被黑客控制，重新构造一封清除木马的木马工具给其使用，导致再次被远程控制。
- 钓鱼目标群体：常见的包括 HR、客户、销售、开发，广撒网的话就是针对全体员工。但后者对于有防护

> 将社工和钓鱼结合起来用，是实战中最为常见、高效、经典的攻击姿势。

措施的公司而言，很难攻击成功，因为有全员邮件需要流程审批、邮件网关在技术上实现自动拦截等原因。

• 钓鱼攻击原则：利用实事，吸引关注点；投其所好，抓住好奇感；史上最难，利用信任感。一切都是基于人性来攻击，成功率最高。

• 优质样本及工具：样本落地不被杀软查杀，这是第一步，也是最基础的。做的比较好的公司还会有异常进程、异常行为等检测规则。攻击队可以打时间战，比如，在非工作时间段动手、提升拿到据点后收集敏感信息自动化等方式。

1.3 钓鱼攻击矩阵

以攻击方式为列，攻击目标为行，再填上话术和技术实现方式，由此可以编织出针对性极强的攻击矩阵，大致如下所示。

攻击方式 / 攻击目标	邮件钓鱼	网页钓鱼	WiFi 钓鱼	+ 社工
HR	候选人简历 word、PDF 等漏洞利用制作木马文件			✓
客服	公司服务、产品售后问题 套取试用系统账号，登录之后渗透 发送文档类木马文件			✓
销售	订单 发送文档类木马文件			✓
软件开发工程师	网安通知 发送漏洞修复文件或工具			✓
全体员工	加薪福利、中奖 发送文档类木马文件	加薪福利、中奖发送恶意链接，诱导去钓鱼页面	最佳场景是 WiFi 接入认证账号体系与公司内网系统一致，如均为域账号	✓

2. 安全运营 SOP

邮件钓鱼是钓鱼攻击最为常见的方式，但其应用又会掺杂社工、网页钓鱼等招数，已跃然成为攻击成功率最高的方式之一。其表现形式多种多样，如携带恶意附件、内容中含有恶意链接、话术型邮件等，对于防护和检测的难度都比较大。当收到邮件告警时，不同类型的方式处置稍微有点差异，不过大致可分为以下步骤：

2.1 钓鱼邮件确认

根据告警信息人工判断是否为钓鱼邮件及其类型，在处理时有可能是垃圾邮件，也有可能是正常的业务来往的邮件，对于后者判断可能比较难以判断真实性，故需要与收件人确认。常见钓鱼邮件类型如下。

• 附件钓鱼邮件：邮件携带附件，附件一般以可执行的恶意文件、利用 word 宏病毒及其他已知漏洞为主，通过描述引导用户点击运行；

• 链接钓鱼邮件：邮件内容中包含链接，诱导用户访问链接，可能会下载文件（如上），也可能是克隆的钓鱼页面，套取账号密码等敏感信息；

• 话术钓鱼邮件：通过邮件内容引导用户到第三方平台或 IM 聊天群上，统一由专门人员通过聊天等方式进行钓鱼，直接传恶意文件或套取敏感信息均可能发生；

• 其他钓鱼邮件：指以上三类之外的或以上三类的综合使用，具体的处置方式随着攻击方式而变化，不过万变不离其宗。

2.2 恶意样本检测

针对样本投递类的攻击，钓鱼邮件可能是直接投递恶意样本，也可能间接投递（如在邮件内容中加入样本下载链接，通过话术加入 IM 群后引导在本机执行样本等）。按照钓鱼邮件类别分别进行以下处置。

• 所有钓鱼邮件：获取发件邮箱、发件人 IP、邮件内容中的 IP 或域名等，上传威胁情报平台判断是否已被标记为恶意，得到攻击地址；

• 附件钓鱼邮件：提取邮件附件，上传沙箱进行检测，分析出 C2 地址；

• 链接钓鱼邮件：访问邮件内容中包含的链接，下载获取样本上传沙箱进行检测，分析出 C2 地址。

若是信息收集类攻击，则仅需按照第一种操作即可。

2.3 恶意地址封禁

在邮件安全网关上拉黑发件邮箱；在公网防火墙上对已经分析出的恶意地址进行全面封禁（全面指防火墙是否同一进行策略管理），需要注意不能随意对发件人 IP、邮件内容中的 IP 进行封禁，除非已经被威胁情报标记或判断其为恶意地址，否则可能造成误伤；在 HIDS 和 EDR 上，将恶意样本的 MD5 加入黑名单。

2.4 确定影响范围

确定内部受影响范围的方式大致可分为 3 种，一是直接在邮件安全网关上根据发件邮箱确定收件人范围；二是在公网 FW、NTA 设备上查询钓鱼邮件内容中含有的 IP 或域名、C2 地址，根据访问情况来确定范围；三是在 HIDS 和 EDR 上查询是否存在恶意文件（md5），根据样本落地情况来确定范围。

2.5 推送内部通告

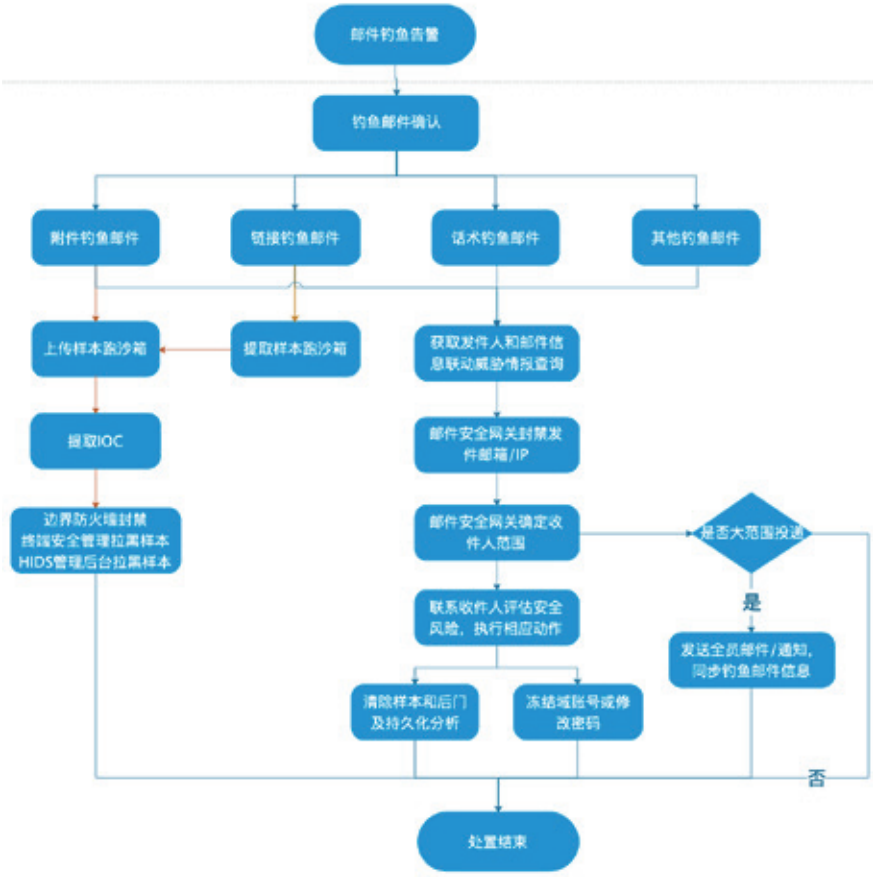
若钓鱼邮件是大范围投递，则需发送全员邮件或公众号进行防钓鱼提醒、用户已进行操作报备（如已点击恶意样本）；若仅投递少数人，则单点联系收件人并询问个人接收到后的操作情况。

2.6 人工清理后门

通知收到钓鱼邮件的人员，进行样本清除；在 NTA 设备上分析访问过 C2 的用户，并联系其进行域账号冻结、终端下线、样本清除、持久化排查等应急响应动作。

2.7 附 SOP 流程图

2.1–2.6 的处置流程，如下图所示。



3. 钓鱼邮件防范

在真实复杂的业务场景中，安全检测体系及安全设备大概率会出现漏报的情况。故在平时加强并持续进行全员安全意识宣贯、培训，打通内部员工与安全运营的互动通道，在条件允许的情况下对提供安全情报、反馈钓鱼邮件的员工进行物质奖励，会对漏报情况起到补充作用。

3.1 安全意识培训

在对员工进行安全意识教育时，生动的案例和必要的甄别方法能起到较好效果。常见的识别方法包括：

- 确认收件人名称和收件人邮箱地址一致：如果是公司邮件，发件人一定会使用工作邮箱，如果发现对方使用的是个人邮箱账号或邮箱账号拼写很奇怪，则需要提高警惕；
- 看邮件标题“系统管理员”“通知”“异常”“紧急”“账号锁定”“中奖”“积分”“<SPF Failed>”等，这类标题的邮件需要谨慎打开；
- 看正文目的：当心对方索要登录密码，一般正规的发件人发送的邮箱不会索要账密信息；对于公司和个人的信息和权限，做到未确认不提供；
- 看正文内容：若邮件内含有链接，须谨慎点击。若链接要求输入用户名和密码、下载文件，不要直接输入、不要直接下载或下载后直接运行。

3.2 钓鱼邮件演练

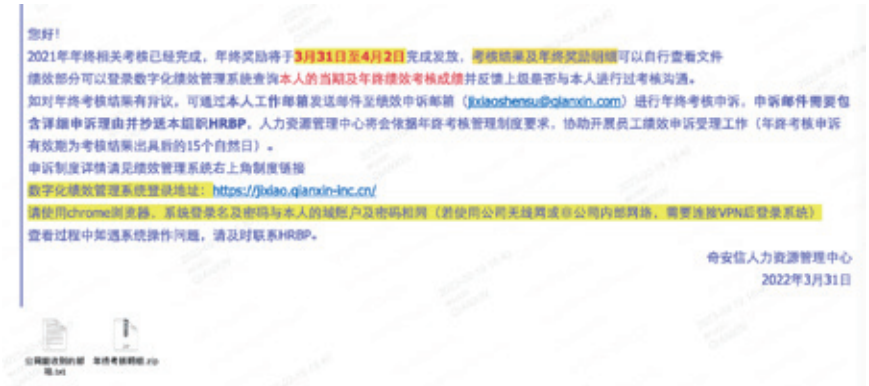
在安全意识培训及考试之后，再次发送钓鱼邮件验证培训效果。

亦可以常态化进行邮件钓鱼执法，中招人员参加安全意识培训。

在实施邮件钓鱼前，有以下两点事项需要注意。

- 提前向领导报备：包括话术、目标人群、时间等，邮件发送领导进行报备。涉及到针对某部门的定向钓鱼时，还应知会其部门负责人，避免事后产生不必要的麻烦。

您好！
2021年年终相关考核已经完成，年终奖励将于3月31日至4月2日完成发放，考核结果及年终奖励明细可以自行查看文件
绩效部分可以登录数字化绩效管理系统查询本人的当期及年终绩效考核成绩并反馈上级是否与本人进行过考核沟通。
如对年终考核结果有异议，可通过本人工作邮箱发送邮件至绩效申诉邮箱（jixiaoshensu@qianxin.com）进行年终考核申诉，申诉邮件需要包含详细申诉理由并抄送本组织HRBP，人力资源管理中心将会依据年终考核管理制度要求，协助开展员工绩效申诉受理工作（年终考核申诉



您好！
2021年年终相关考核已经完成，年终奖励将于3月31日至4月2日完成发放，考核结果及年终奖励明细可以自行查看文件
绩效部分可以登录数字化绩效管理系统查询本人的当期及年终绩效考核成绩并反馈上级是否与本人进行过考核沟通。
如对年终考核结果有异议，可通过本人工作邮箱发送邮件至绩效申诉邮箱（jixiaoshensu@qianxin.com）进行年终考核申诉，申诉邮件需要包含详细申诉理由并抄送本组织HRBP，人力资源管理中心将会依据年终考核管理制度要求，协助开展员工绩效申诉受理工作（年终考核申诉有效期为考核结果出具后的15个自然日）。
申诉制度详情请见绩效管理系统右上角制度链接
数字化绩效管理系统登录地址：https://jixiao.qianxin-inc.cn/
请使用chrome浏览器，系统登录名及密码与本人的域账户及密码相同（若使用公司无线网或非公司内部网络，需要连接VPN后登录系统）
查看过程中如遇系统操作问题，请及时联系HRBP。
奇安信人力资源管理中心
2022年3月31日

· 提前准备好环境：指自建 SMTP 邮件服务器（国内大厂云服务器默认禁用了 25 端口）、钓鱼域名（同形异构的字母）、伪造钓鱼网站、编写钓鱼话术、制作并测试后门文件等。不仅是要考虑绕过终端防病毒软件，还有 bypass 邮件安全网关的检测机制。安

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。

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

奇安信
新一代网络安全领军者

「零事故」安服团队重磅力作

900余次实战攻防演练的经验总结
从红队、蓝队、紫队视角全面解读攻防演练

扫码购买

奇安信连续三年位居
“中国网安产业竞争力50强”
第一名

6月20日，中国网络安全产业联盟（CCIA）
公布“2023年中国网安产业竞争力50强”榜单，
凭借扎实的技术实力和领先的市场表现，
奇安信连续三年高居榜单第一名。

“2022年中国网安产业竞争力50强”榜单

TOP15	公司名称
1	**奇安信科技集团股份有限公司**
2	深信服科技股份有限公司
3	启明星辰信息技术集团股份有限公司
4	华为技术有限公司
5	天融信科技集团股份有限公司
6	绿盟科技集团股份有限公司
7	腾讯云计算（北京）有限责任公司
8	新华三技术有限公司
9	阿里云计算有限公司
10	杭州安恒信息技术股份有限公司
11	三六零数字安全科技集团有限公司
12	亚信安全科技股份有限公司
13	中电科网络安全科技股份有限公司
14	杭州迪普科技股份有限公司
15	山石网科通信技术股份有限公司