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

2024 不止于安全

P15

第37期

2024 年 1 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。

安全创造价值

2023年11月，派拓网络（Palo Alto Networks）发布了一份研究机构Forrester撰写的报告《派拓网络Prisma Cloud的整体经济效益》。根据这个研究，部署派拓网络云原生应用保护平台（CNAPP）——Prisma Cloud平台的用户，可以在6个月收回投资，3年时间的投资回报将达到264%。

这种以数据为依据的量化安全投资回报的方法，无意是有益的尝试：不仅可以使安全负责人自信地做出符合需求的投资决策，更有利于获得更多的资源与投入。

长期以来，国内外的网络安全主管都面对证实安全投入价值的挑战——如何向老板们证实自己所花费每笔钱的价值与意义。尽管面对日益增长的合规高压，网络安全负责人依然难以证实自身价值，往往是“平时被遗忘，出事来背锅”。

这一矛盾的现象，与业界对网络安全的传统认识密不可分：传统上，网络安全建设作为合规的需要，一直被视为成本中心，被视为不得不花，又不太情愿的投入。

2023年的中央经济工作会议将高质量发展确立为新时代中国经济发展的鲜明主题。数字经济作为高质量发展的引擎，将以网络安全为基础，这意味着随着数字化转型的深入，网络安全将不再止于安全。当一切都在数字化之际，各行各业的数字化深入到业务、产品与服务，从业务的支撑变成业务的一部分。网络安全自然也已经深深地融入业务。

在数字经济时代，个人数据安全与隐私已经成为主流关注点。试想，如果支付系统没有强大安全的属性，智能汽车轻易可以被远程操控，国企云没有云原生的安全防护能力，数字藏品交易平台无法提供强大的资产保护，很难想象他们可以持续赢得用户的信赖。

将网络安全放在首位的企业往往更易赢得客户。对全球苹果迷来说，iPhone不仅是一种设备，还是安全性和可靠性的象征。毕竟在很多人眼中，相比其他操作系统的手机，iPhone用户成为漏洞受害者的可能性较小；在发生问题时，更有可能恢复数据。

以量化的形式来展示安全投资的收益和回报，不仅有利于安全从业者证实自身价值，也是扭转业界对网络安全认识的关键——网络不再是成本中心，而是一项重要的业务战略投资。它不仅仅可以降低安全风险，更可以为企业带来效率提升，是企业在数字时代的竞争优势，也是业务创新的加速器。

基于一段时间的梳理，我们筛选出一些能够展示出业务价值的安全创新应用案例，这些来自不同行业的用户，不再满足于降低风险，而将安全打造成企业与业务的显著标签，成为其市场竞争的明显优势。

希望更多的用户加入这些这些创新先行者，努力改变对安全的看法，向业界展示安全的业务价值。

总编辑

2024年1月1日

CONTENTS 目录

安全态势

月度专题

2024 不止于安全

P15

我国进入高质量发展时代，作为数字经济基石的网络安全，不仅要防范网络风险，还要兼顾业务价值的提升；在许多行业努力降本增效之际，网络安全需要证明其不再是成本中心，而是重要的业务战略投资，将会成为企业的利润中心、机构业务的加速器。2024 年乃至今后，安全将不再止于安全。

报告速递

专　栏

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：刘川琦
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 2123- L0058 号
编印单位：奇安信科技集团股份有限公司
发送对象：奇安信集团内部人员
印刷数量：4500 本
印刷单位：北京博海升彩色印刷有限公司
印刷日期：2024 年 1 月 26 日

政策篇

国内，关基安全屏障建设再获进展。财政部、工信部联合发布施行 7 项政府采购标准，对政府采购操作系统、数据库、通用服务器等主流软 / 硬件产品，作出了安全可靠等要求；交通运输部公布《铁路关键信息基础设施安全保护管理办法》，对铁路领域关基保护作出了进一步要求；

国际上，美国国防部发布关于承包商网络安全合规计划 CMMC 的拟议规则，要求承包商必须获得 CMMC 认证才能获得订单，初步估算，美国国防工业企业每年将为此增加超 40 亿美元的网络安全支出。

国内

《网络安全信息报送指南》等 5 项网络安全国家标准获批发布

1 月 5 日全国信安标委公众号消息，根据 2023 年 12 月 28 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 20 号），全国信息安全标准化技术委员会归口的 5 项网络安全国家标准正式发布。具体包括两项修订标准《信息安全技术 信息安全管理体系概述和词汇》《信息安全技术 射频识别（RFID）系统安全技术规范》，三项新标准《信息安全技术 网络安全信息报送指南》《信息安全技术 电子发现 第 1 部分：概述和概念》《信息安全技术 通用密码服务接口规范》。

十七部门联合印发《“数据要素 ×”三年行动计划（2024—2026 年）》

1 月 4 日国家数据局公众号消息，国家数据局、中央网信办、科技部等时期部门联合制定了《“数据要素 ×”三年行动计划（2024—2026 年）》，现公开印发。该文件共五章，包括背景介绍、总体要求、十二项重点行动、三项保障支撑举措、五项组织实施措施。该文件提出，到 2026 年年底打造 300 个以上示范性强、显示度高、带动性广的典型应用场景，数据产业年均增速超过 20%，推动数据要素价值创造的新业态成为经济增长新动力。在保障支撑举措“加强数据安全保障”中，该文件提出了落实数据安全法规制度、丰富数据安全产品、培育数据安全服务三方面内容。

《铁路关键信息基础设施安全保护管理办法》公布

1 月 3 日交通运输部官网消息，交通运输部公布了《铁路关键信息基础设施安全保护管理办法》，自 2024 年 2 月 1 日起施行。该文件共 6 章 30 条，包括总则、铁路关键信息基础设施认定、运营者责任和义务、保障和监督、法律责任、附则。该文件提出，铁路关键信息基础设施是指在铁路领域，一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生和公共利益的重要网络设施、信息系统等。铁路关键信息基础设施的网络安全保护等级应当不低于第三级。任何个人和组织不得实施非法侵入、干扰、破坏铁路关键信息基础设施的活动，不得危害铁路关键信息基础设施安全。

操作系统等 7 项政府采购需求标准发布施行

12 月 28 日财政部官网消息，财政部、工业和信息化部联合发布施行 7 项政府采购需求标准，分别是操作系统、数据库、通用服务器、工作站、一体式计算机、便携式计算机和台式计算机。该系列文件提出，对于既包含操作系统、数

据库、服务器等软 / 硬件产品也包含集成服务的采购项目，采购人应当合理划分采购包，尽可能将操作系统、数据库、服务器等软 / 硬件产品与集成服务分包采购。采购的操作系统、数据库、服务器等软硬件产品总额达到分散采购限额标准的，应当单独分包采购。该系列文件要求，乡镇以上党政机关，以及乡镇以上党委和政府直属事业单位及部门所属为机关提供支持保障的事业单位在采购相关产品时，应当将符合安全可靠测评要求纳入采购需求，其他单位可不在采购需求中提出此项要求。

十四部门联合印发《关于开展网络安全技术应用试点示范工作的通知》

12 月 18 日工信部官网消息，工业和信息化部、国家网信办、人力资源社会保障部等十四部门联合印发《关于开展网络安全技术应用试点示范工作的通知》，部署开展网络安全技术应用试点示范工作。该文件提出，将以新型信息基础设施安全、数字化应用场景安全、安全基础能力提升为主线，面向公共通信和信息服务、人力资源社会保障、水利、卫生健康、应急管理、广播电视、金融、交通运输、邮政等重要行业领域网络和数据安全保障需求，从基础网络安全、云计算安全、人工智能安全、大数据安全、信创安全、商用密码、车联网安全、物联网安全、中小企业数字化转型安全、网络安全共性技术、网络安全创新服务、教育技术产业融合发展联合体、网络安全“高精尖”创新平台等 13 个重点方向，遴选一批技术先进、应用成效显著的试点示范项目。

欧盟新《网络安全条例》正式生效

1 月 8 日欧盟委员会消息，欧盟新版《网络安全条例》于 1 月 7 日起生效。该条例规定了每个欧盟组织机构需要采取的相应措施，包括建立内部网络安全风险管理、治理和控制框架。该条例提出，设立一个新的机构间网络安全委员会（IICB）以监测和支持欧盟实体落实相关条例，并延长了欧盟计算机应急组织（CERT-EU）的任期。CERTEU 将作为威胁情报、信息交换和事件响应的协调中心、中央咨询机构和服务提供者。为了与其授权内容保持一致，CERT-EU 被重新命名为联盟内网络安全服务中心，其简称“CERT-EU”被保留。

美国防部发布关于承包商网络安全合规计划 CMMC 的拟议规则

2023 年 12 月 26 日美国联邦公报消息，美国国防部在《联邦公报》上发布针对网络安全成熟度模型认证（CMMC）计划的拟议规则，要求国防承包商必须获得 CMMC 认证才能获得订单。该规则确定了网络安全要求的分层模型，要求承包商根据信息的敏感性实施三级网络安全标准。其中，第 1 级针对涉及联邦合同信息（FCI）的合同，要求承包商必须遵守《美国联邦采购法规》52.204-21 规定的 15 项安全要求；第 2 级适用于涉及受控非机密信息（CUI）的合同，承包商除需遵守第 1 级要求外，还必须遵守《NISTSP 800-171 Rev2》中规定的 110 项安全要求；第 3 级旨在增强 CUI 抵御高级持续威胁的保护，承包商除在第 2 级基础上，还需遵守《NIST SP 800-172 Rev2》中选定的 24 项安全要求。据新规估算，美国国防工业企业每年将为此增加超 40 亿美元的网络安全支出。

美国 NASA 发布首版太空安全最佳实践指南

12 月 22 日 NASA 消息，美国国家航空航天局（NASA）发布首版太空安全最佳实践指南，以加强公共部门和私营企业太空活动的网络安全。太空安全最佳实践指南提供了安全实施任务的指导性原则和控制措施，旨在应对当今网络攻击者试图破坏任务所使用的战术、技术和程序（TTPs），保护航天器和地面段。指南采用美国国家标准与技术研究院 NIST SP 800-53 文件中“安全控制”的定义，并充当 NIST 术语与 NASA 飞行项目术语之间的翻译桥梁，适用于各种规模、范围和性质（国际、公司、大学）所有等级的任务、项目和计划。

事件篇

国家博弈与地缘政治交织下，网络对抗愈加激烈。俄罗斯安全公司卡巴斯基曝光，“三角行动”间谍软件利用了一个苹果硬件“后门漏洞”，俄情报部门认为攻击者为美国 NSA；我国国家安全部披露一起境外机构非法窃取我国航空数据活动，及时查获了数百套已在境内投放的设备。

美国证交会推特账号被黑并发布虚假市场消息

1 月 9 日 CyberScoop 消息，美国证券交易委员会（SEC）推特账号 @SECgov 当天下午约 4 点发布了一则虚假的市场消息，称批准比特币 ETF 上市交易。大约 15 分钟后，SEC 主席 Gary Gensler 在个人推特账号上声称，@SECgov 推特账号已被盗用，发布了未经授权的消息。SEC 发言人随后在一份声明中表示，在美国东部时间下午 4 点后不久，不明身份人士在短时间内对 SEC 的推特账号 @SECGov 进行了未经授权的访问和活动。目前黑客的访问“已被终止”。这则假消息发布后，比特币的价值暂时飙升至近 48,000 美元，然后又回落至 45,500 美元。

国家安全部披露境外机构非法窃取我国航空数据活动

1月6日国家安全部公众号消息，国家安全部发布文章《航空爱好者切莫变为“窃密志愿者”》称，发现多个境外机构以免费提供设备、共享航空信息为诱饵，依托网络社交平台面向境内航空爱好者精准招募“志愿者”，并跨境邮寄设备，指挥“志愿者”在我境内非法采集、向境外秘密传输我国飞行器飞行数据。这些境外机构在我国渤海、东海、南海周边省份大量投放此类设备，不仅窃取民用航空数据，甚至还能窃取军用航空器等敏感数据信息。经测算，每台设备每天可向境外发送约 1000 架次飞机的飞行数据和约 13 万条位置数据。按照覆盖半径 300 公里至 400 公里计算，仅需投放约 300 台设备，即可对我全空域飞机飞行数据实现监测覆盖。针对上述非法窃取我敏感数据的行为，国家安全机关会同有关部门在全国范围内开展了专项打击，及时查获数百套已在境内投放的设备，依法对有关人员进行处罚。

黑客攻击全国 21 个省市社保 / 医疗等系统，“爬取”公民信息获利 500 余万

1 月 5 日检察日报消息，四川省成都市新都区检察院公布了一起利用技术手段非法窃取公民个人信息案，法院近日以侵犯公民个人信息罪判处王某等人有期徒刑三年至十个月不等。经查，2021 年初至 2022 年 7 月，王某等人通过网络渠道委托黑客，利用搜集到的各种政府、企业网络平台的接口漏洞，通过对接口进行数据抓包、参数解析等，开发出 100 余款黑客软件。王某等人利用相关黑客软件，先后入侵全国 21 个省市的社保、医疗等共计 29 个行业的 51 个系统，“爬取”包括姓名、身份证号、手机号码、工作单位、家庭成员、社保缴纳等在内的公民个人信息，并贩卖给相关催债公司。被盗的公民个人信息被催债公司大规模用于数据画像，勾勒人物关系和活动轨迹，由此通过手机短信、微信、抖音等社交平台向欠款人的社会关系人发送催债信息。通过梳理固定涉案数据、司法鉴定意见及审计的获利情况，该院认定该团伙非法获利达 500 余万元。

电信巨头 Orange 西班牙公司关键账号被盗，导致国内大面积断网

1 月 3 日 Bleeping Computer 消息，国际电信巨头 Orange 西班牙公司的 RIPE 账号被盗，攻击者将其网络核心配置（BGP 和 RPKI）改为无效，导致全国互联网中断了大约 3 小时。Orange 是西班牙最大的移动运营商之一，此

次网络中断大约持续了 3 个小时。据悉，攻击者在信息窃取软件的数据集中发现了此次被利用的账号（未启用双因子认证），为了“找乐子”实施了此次攻击。

澳大利亚地方法院遭勒索攻击：敏感案件数据泄露 司法权威性被破坏

1 月 2 日 ABC 消息，澳大利亚维多利亚州法院系统遭受网络攻击，维多利亚州法院服务局（CSV）发言人表示，黑客侵入了法院系统的音视频存档区域。这意味着高度敏感案件的证人证词等听证录音可能已被访问或窃取。相关录音覆盖了 2023 年 11 月 1 日至 12 月 21 日期间的听证会，也可能包括 11 月之前的部分听证会。CSV 正在努力通知出庭记录遭黑客访问的人，并计划设立一个联系中心，向自认为受攻击影响者提供服务。有安全专家认为，攻击者是使用 Qilin 勒索软件的俄罗斯黑客。

杭州破获重大勒索病毒案：犯罪团伙借助 ChatGPT 进行程序优化

12 月 28 日新华社消息，杭州上城区网警近日破获一起重大勒索病毒案件，犯罪团伙成员均有网络安防相关资质，且在实施犯罪过程中借助 ChatGPT 进行程序优化。11 月 20 日，上城网警接到辖区某公司报案称，该公司名下相关服务器遭勒索病毒攻击，导致公司所有系统无法正常运行，对方勒索 2 万 USDT（泰达币）。警方随即组建技术攻坚团队开展侦查。专案组对被攻击服务器进行细致勘验、提取木马程序进行分析和对嫌疑人勒索使用的虚拟币地址进行多维度研判，成功抓捕 4 名犯罪嫌疑人。该团伙 4 人均有网络安防相关资质，且有供职大型网络科技公司经历。他们对分工负责编写勒索病毒版本、借助 ChatGPT 进行程序优化、开展漏洞扫描、渗透获取权限、植入勒索病毒、实施敲诈勒索的犯罪事实供认不讳。

卡巴斯基曝光疑遭 NSA 利用的苹果硬件“神秘后门”

12 月 27 日 Bleeping Computer 消息，卡巴斯基在年关时分披露了苹果处理器“后门漏洞”，为连载半年多的三角定位间谍软件行动收官。CVE-2023-38606 滥用苹果预留未公开的隐蔽硬件特性，绕过了系统保护措施，攻击者利用该漏洞对卡巴斯基、驻俄中国大使馆等多个组织实施了攻击。俄罗斯官方认为，美国 NSA 使用苹果提供的硬件后门发起了这次攻击，但尚无坐实这些指控的明确证据。卡巴斯基推测，这个未记录的硬件特性之所以包含在最终供消费者使用的 iPhone 版本中，可能是出于错误，或者是为了方便苹果工程师进行调试和测试。苹果通过更新设备树限制物理地址映射修复了这个漏洞。但是，仍然不清楚攻击者最初是如何发现这种如此隐蔽的可利用机制的。

意大利云服务商被勒索，导致上千个政府机构服务中断、数据丢失

12 月 19 日 Security Affairs 消息，意大利云服务商 Westpole 遭遇 Lockbit 3.0 勒索攻击，导致云上客户、政务服务商 PA Digitale 服务中断，PA Digitale 托管的大量地方政府组织和市政机构无法提供服务。有意大利媒体报道称，由于此次攻击，部分受影响政府机构将无法向员工发放 12 月工资。意大利国家网络安全局发布声明称，已恢复 700 多家与 PA Digitale 相关的国家和地方公共实体数据，但还有约 1000 家实体数据尚未恢复。

网络战场失利！伊朗全国大部分加油站数字崩溃，艰难转向手动运营

12 月 18 日路透社消息，伊朗石油部长 Javad Owji 表示，一起网络攻击导致境内约七成加油站无法提供服务，后来有一成多的加油站逐步恢复运营。据伊朗国家电视台报道，一家名为 Gonjeshke Darande 或“掠食麻雀”的组织声称他们是幕后黑手，以色列当地媒体也报道了这一声明。该组织在 Telegram 上发表声明：“我们以可控的方式实施这次网络攻击，避免对应急服务造成潜在伤害。”此前巴以冲突爆发后，“掠食麻雀”代表接受路透社采访，表示由于伊朗支持哈马斯，他们正在准备在未来对伊朗发动攻击，并“准备了一些攻击‘按钮’”。“掠食麻雀”组织此前曾网络攻击 UI；安加油站、铁路网络、钢铁厂等关基设施，并造成重大损害。

漏洞篇

热门产品 0day 漏洞在野利用猖獗。近一个月来，Google Chrome 浏览器两次披露有 0day 漏洞遭到在野利用，分别为 V8 越界访问、WebRTC 堆缓冲区溢出。Citrix 旗下 NetScaler Gateway 也曝出两个在野漏洞利用。建议用户尽快做好自查及防护。

Google Chrome V8 越界访问漏洞安全风险通告

1 月 17 日，奇安信 CERT 监测到 Google 发布公告 Google Chrome V8 越界访问漏洞 (CVE-2024-0519) 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，从而获取敏感信息或应用程序崩溃。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。

NetScaler ADC 和 NetScaler Gateway 多个在野漏洞安全风险通告

1 月 17 日，奇安信 CERT 监测到官方发布安全公告说明 NetScaler ADC 和 NetScaler Gateway 代码执行漏洞 (CVE-2023-6548) 与 NetScaler ADC 和 NetScaler Gateway 拒绝服务漏洞 (CVE-2023-6549) 存在在野利用。具有低权限的相邻网络的攻击者可通过管理界面访问 NSIP、CLIP 或 SNIP 后利用 CVE-2023-6548 在系统上执行代码；未经身份验证的远程攻击者利用 CVE-2023-6549 可以造成系统拒绝服务。鉴于这些漏洞影响范围较大，且已监测到在野利用，建议客户尽快做好自查及防护。

GitLab 密码重置漏洞安全风险通告

1 月 12 日，奇安信 CERT 监测到 GitLab 密码重置漏洞 (CVE-2023-7028)，未经身份验证的远程攻击者可利用该漏洞将用户账户密码重置电子邮件发送至任意邮箱。LDAP 用户不会受到影响，因为没有忘记 / 重置密码选项。此外，启用了双因素身份验证的用户很容易受到密码重置的影响，但账户不会被接管，因为需要第二个身份验证因素才能登录。鉴于该产品用量较大，建议客户尽快做好自查及防护。

Apache OFBiz 远程代码执行漏洞安全风险通告

12 月 29 日，奇安信 CERT 监测到 Apache OFBiz 远程代码执行漏洞 (CVE-2023-51467)，由于在 ofbiz 18.12.10 版本中官方仍未修复 CVE-2023-49070 漏洞中的权限绕过漏洞，导致未经身份认证的远程攻击者仍能够利用此漏洞绕过身份认证。远程未授权攻击者利用此漏洞结合后台相关功能可执行任意代码，接管目标服务器。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。

金蝶 Apusic 应用服务器 JNDI 注入漏洞 (QVD-2023-48297) 安全风险通告

12 月 22 日，奇安信 CERT 监测到金蝶 Apusic 应用服务器 JNDI 注入漏洞 (QVD-2023-48297)，金蝶 Apusic 应用服务器是一款企业级应用服务器，支持 Java EE 技术，适用于各种商业环境。由于金蝶 Apusic 应用服务器权限验证不当，导致攻击者可以向 loadTree 接口执行 JNDI 注入，造成远程代码执行漏洞。利用该漏洞需低版本 JDK。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

微软 2024 年 1 月补丁日多个产品安全漏洞风险通告

1 月 10 日，微软共发布了 49 个漏洞的补丁程序，修复了 .NET、Microsoft Office、Windows Server 等产品中的漏洞。值得注意的是，微软在 2023 年 5 月 9 日停止了 Windows 10 20H2 的安全更新和技术支持，建议您尽快升级系统。经研判，以下 10 个重要漏洞值得关注（包括 2 个紧急漏洞、8 个重要漏洞），如下表所示。鉴于这些漏洞危害较大，建议客户尽快安装更新补丁。

编号	漏洞名称	风险等级	公开状态	利用可能
CVE-2024-20674	Windows Kerberos 安全特性绕过漏洞	紧急	未公开	较大
CVE-2024-20700	Windows Hyper-V 代码执行漏洞	紧急	未公开	一般
CVE-2024-20683	Win32k 权限提升漏洞	重要	未公开	较大
CVE-2024-20698	Windows Kernel 权限提升漏洞	重要	未公开	较大
CVE-2024-21307	Remote Desktop Client 代码执行漏洞	重要	未公开	较大
CVE-2024-20652	Windows HTML Platforms 安全特性绕过漏洞	重要	未公开	较大
CVE-2024-20653	Microsoft Common Log File System 权限提升漏洞	重要	未公开	较大
CVE-2024-20686	Win32k 权限提升漏洞	重要	未公开	较大
CVE-2024-21310	Windows Cloud Files Mini Filter Driver 权限提升漏洞	重要	未公开	较大
CVE-2024-21318	Microsoft SharePoint Server 代码执行漏洞	重要	未公开	较大

金蝶 Apusic 应用服务器 JNDI 注入漏洞 (QVD-2023-48476) 安全风险通告

12 月 22 日，奇安信 CERT 监测到金蝶 Apusic 应用服务器 JNDI 注入漏洞 (QVD-2023-48476)，金蝶 Apusic 应用服务器是一款企业级应用服务器，支持 Java EE 技术，适用于各种商业环境。由于金蝶 Apusic 应用服务器权限验证不当，导致攻击者可以向 createDataSource 接口执行 JNDI 注入，造成远程代码执行。利用该漏洞需低版本 JDK，且需要服务器上有数据库驱动。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Google Chrome WebRTC 堆缓冲区溢出漏洞安全风险通告

12 月 21 日，奇安信 CERT 监测到 Google 修复 Google Chrome WebRTC 堆缓冲区溢出漏洞 (CVE-2023-7024)，该漏洞存在在野利用，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或导致浏览器崩溃。目前，此漏洞已发现在野利用。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

金蝶天燕远程代码执行漏洞安全风险通告

12 月 20 日，奇安信 CERT 监测到金蝶天燕远程代码执行漏洞 (QVD-2023-48081)PoC 及 EXP 在互联网上流传，该漏洞允许未授权的远程攻击者上传任意文件，最终可能导致远程执行恶意命令，控制服务器等。目前，奇安信 CERT 已复现此漏洞，经研判，该漏洞攻击利用难度低，且 EXP 已公开，被恶意利用的可能性增大。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 Dubbo 多个反序列化漏洞安全风险通告

12 月 18 日，奇安信 CERT 监测到 Apache Dubbo 发布新版本，修复了 Apache Dubbo 反序列化漏洞 (CVE-2023-46279) 与 Apache Dubbo 反序列化漏洞 (CVE-2023-29234)。攻击者通过向系统发送恶意数据包利用这些漏洞，成功后可以读取敏感信息或执行恶意代码。鉴于此产品用量较大，建议客户尽快做好自查及防护。

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

对抗篇

国内攻防演习 12 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12月，奇安信Z-TEAM团队共承接攻防演习服务 25 场，其中，行业级攻防演习 1 场，省级攻防演习 2 场，地市级行业攻防演习 1 场，客户自主攻防演习 21 场。

本月承接攻防演习数量与上月对比呈明显上升趋势（见图 1）。

本月承接的攻防演习涉及金融、政府部委、企业行业较多，此情况较上月承接攻防演习涉及行业范围数据变化显著，金融、企业、央企行业攻防演习数量明显增加（见图 2）。

本月攻防演习成果如表 1 所示：

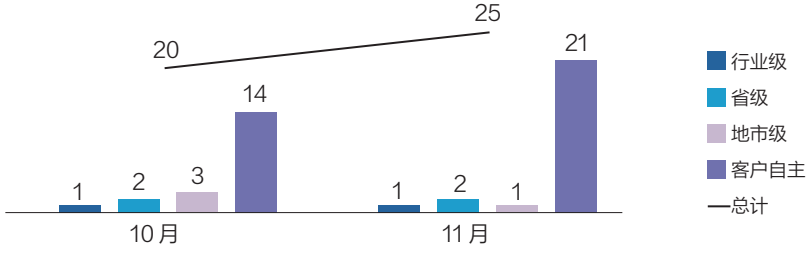


图 1 11-12 月 Z-TEAM 承接攻防演习数量统计

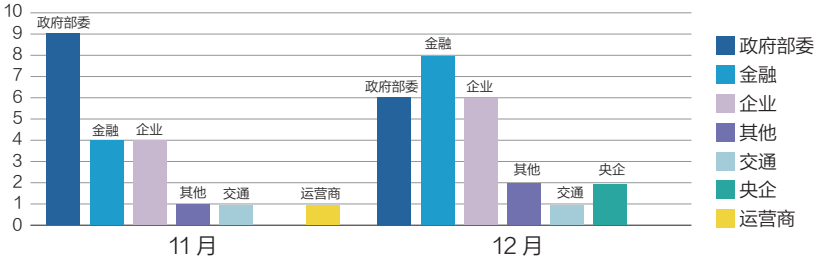


图 2 2023 年攻防演习涉及行业统计

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	42	56	61	108	37	146	413	14250

表 1

二、本月任务目标特点

随着计算机网络技术的不断发展，企业的业务系统也越来越依赖于互联网和内部网络。网络是开放的、系统的，同时也是共享的、复杂的，由于其边界和路径都存在不确定性，所以网络容易受到来自外界的入侵、攻击和破坏，影响数据信息的完整性和保密性，然而，随之而来的安全问题也日益严重，黑客和病毒等威胁不断增加，企业信息网络系统面临着越来越大的安全风险。因此，保障企业信息网络系统的安全性，已成为企业信息化建设所必须考虑的重要问题之一。在本月攻防演习中企业行业占比为 24%（见图 3）。

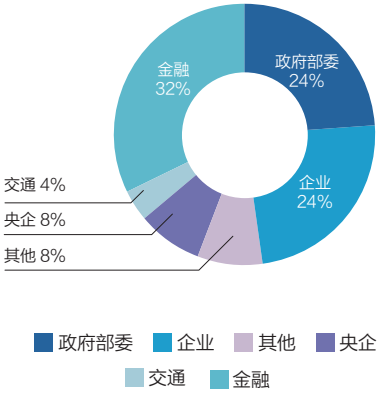


图 3 12 月攻防演习分布

三、主要攻击手段分析

基于本月奇安信 Z-TEAM 团队实战成果，对本月任务中多个行业的网络目标进行了攻击分析，对不同的行业目标使用不同攻击手段，如政府部委、交通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、金融行业主要是钓鱼攻击、漏洞扫描利用和 VPN 仿冒接入等；央企、其他行业外网突破的主要手段包括漏洞扫描利用、隐秘隧道外联等。本月各个行业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包括漏洞扫描利用、钓鱼攻击、口令爆破、VPN 仿冒接入、隐秘隧道外联等。

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

本月任务中企业行业攻防演习任务占比为三分之一，通过对该行业的演习数据分析，发现攻击队的外网纵向突破重点是寻找薄弱点，并利用历史漏洞和钓鱼攻击手段结合实现突破。内网横向移动则采用弱口令爆破、VPN 仿冒接入、隐秘隧道外联等攻击手段来实现横向拓展和渗透。在攻防演习中，攻击者通常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

随着互联网技术的不断演进，信息技术在企业运营中的地位日益凸显。计算机作为企业运营的关键要素，发挥着不可或缺的作用，而企业信息网络的安全性也因此变得至关重要。企业的业务系统在互联网和内部网络的支撑下，愈发依赖信息技术以实现

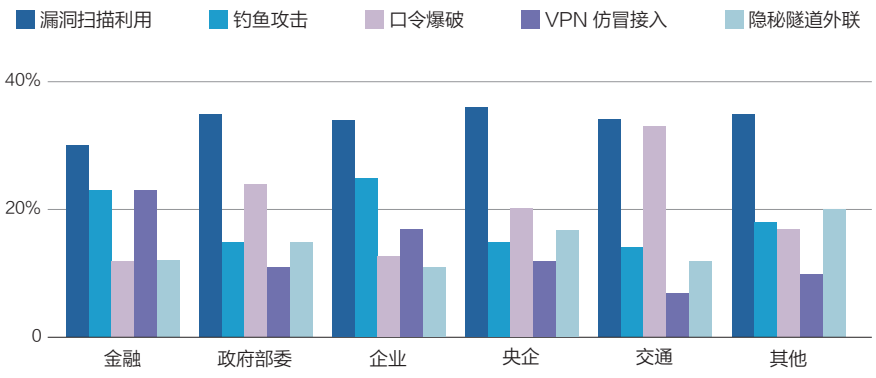


图 4 行业攻击手段分布

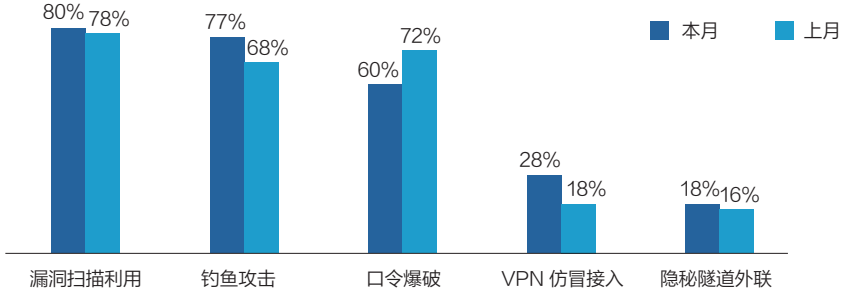


图 5 攻击手段对比

高效、稳定的运营。随着科技的飞速发展，企业信息网络系统的安全问题也日益凸显。黑客攻击、病毒传播等威胁不断涌现，给企业的正常运营带来了严重的影响。因此，保障企业信息网络系统的安全已成为企业发展中不可或缺的重要环节。只有采取有效的安全措施，才能确保企业信息网络系统的稳定、安全和可靠。这对于企业的发展至关重要，必须给予足够的重视。

案例：钓鱼攻击协同多漏洞突破目标核心网络。

在某企业近期举办的攻防演练中，奇安信攻击队伍经过初步的情报收集工作，对目标企业的外部网络安全防御体系进行了全面的评估。经过分析，该防御体系表现出较高的严密性。在现有的条件下，如果攻击队伍决定通过互联网作为主要的攻击途径，只有两种可行的方式：利用 0day 漏洞或实施钓鱼攻击，这两种方式均具有较高的可行性。考虑到企业对外沟通的常规渠道，攻击队经过慎重评估，决定采用招聘场景作为实施钓鱼攻击的切入点。经过内部讨论，团队成员达成共识，认为此举能够实现事半功倍的效果。

为确保行动的有效性，攻击队运用某招聘软件对目标企业招聘需求进行调查，并成功获取了招聘负责人的个人微信信息。在进一步的沟通中，攻击队将精心设计的诱饵文件伪装成个人简历的 exe 格式，诱导招聘负责人进行点击操作。

经过多轮的交流与诱导，招聘负责人的心理防线逐渐被突破，最终打开了带毒的压缩文件。该行为导致招聘负责人使用的终端设备成为攻击队打入目标内网的第一个安全缺口。

经过对受控终端的有效利用，攻击队顺利进入了目标企业的内部网络。他们利用一个尚未修复的系统漏洞，成功获取到一些关键设备的控制权。同时，结合内部网络的信息收集路径，攻击队进行了持续的试探性攻击。最终，他们成功获取了管控平台的服务器权限，并进一步拓展对内部网络的渗透。

在受控的服务器环境中，攻击队通过隧道技术对目标企业的内网进行了细致的探测。在全面收集内网安全信息的基础上，攻击队经过严格的安全审查，发现了云平台系统和内网堡垒机存在潜在的安全漏洞。针对这些漏洞，攻击队采取漏洞利用和口令爆破攻击手段，并成功地进入了目标企业的云后台和内网堡垒机。

经过周密的计划和准备，攻击队决定针对目标核心业务内网展开行动。在成功突破目标某云平台和堡垒机的基础上，攻击队通过读取服务器上部署的数据库配置文件，进行了深入的分析和测试。通过口令复用测试，成功获取了目标内网大量业务应用部署的关键信息。结合先前从数据库中提取的域用户账号信息，攻击队进行了严谨的爆破操作，并成功获取了域账号密码。在获取域账号密码后，进一步利用域管账号权限，成功控制了多个核心业务系统，包括 OA 系统、运维管理和 VPN 等。

五、安全加固建议

1. 案例剖析

随着攻防演习不断深化，企业客户在网络边界的防护能力不断完善，但是随着业务数字化转型发展，数字化资产也越来越多，导致内部数字化资产的攻击面也越来越多。随着边界防护能力不断提升，企业客户也应加强自身内网数据化资产的风险治理，从而全面提升自身的安全防护能力。

案例暴露问题：人员安全意识不足，通过社工攻击手段突破网络边界进入内部网络；同时内部重要资产的隔离与受攻击面多，导致内部全面失陷。

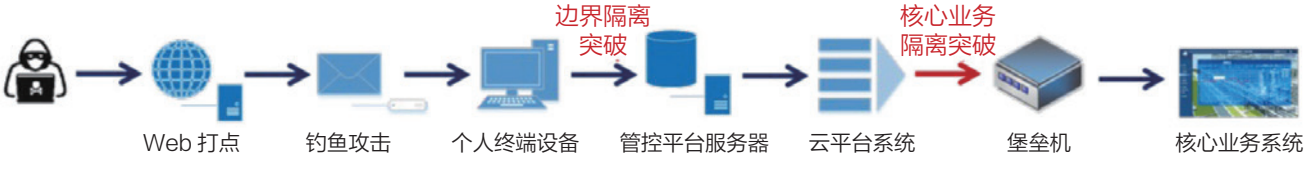


图 6 案例攻击路线图

2. 防护策略

结合案例暴露出的安全隐患，需从几个方面加强自身的防护短板。

・提升网络安全防范意识

通过技术、管理和人员教育等多维入手，提升内部员工网络安全防范意识。包括但不限于：

1）安全意识教育：定期开展内部全员的网络安全意识培训，同时结合终端桌面、内部展板等形式，夯实员工网络安全防范意识，为网络安全防护构建第一道防线；

2）开展网络安全意识技术演练：定期开展内部网络安全意识演练，模拟钓鱼邮件、微信钓鱼等技术手段，验证内部员工安全意识能力，并针对网络安全意识淡薄的员工有侧重的教育与培训；

3）在技术方面，应加强恶意邮件检测与防护、终端恶意代码检测与防护，以及内部员工上网的访问控制等技术措施，全面提升社工攻击防护能力。

・加强内网访问控制

企业客户重点办公区域应做到上网终端与业务环境的物理隔离。同时，针对内部业务系统，也应该做到办公系统与生产系统的严格隔离，并在各个子网中实现多级子域划分，实现不同重要等级业务系统与数据的隔离访问控制。特别是一些重要、集权的 IT 系统，需落实严格的白名单访问控制措施。

・构建内网数据化资产治理，借助平台 + 服务，开展互联网资产攻击面管理，包括但不限于：

1）建立网络资产攻击面管理（CAASM）平台，通过聚合 IT 资产、配置、漏洞、补丁、漏洞情报等数据，持续监控信息系统的资产状态，进行多维度数据碰撞分析、关联分析，发现资产安全问题，驱动资产发现、配置采集、风险持续监测和资产安全整改等安全运行工作。

2）常态化互联网资产发现，基于 IP 或域名，采用 Web 扫描技术、操作系统探测技术、端口的探测技术、服务探测技术、Web 爬虫技术等各类探测技术，对客户信息系统内的主机 / 服务器、安全设备、网络设备、工控设备、Web 应用、中间件、数据库、邮件系统和 DNS 系统等进行主动发现，全面、精准解决互联网资产边界盲区问题。

3）常态化应用系统安全检测，通过渗透测试及众测的方式，对全量应用系统的安全做深入的探测，发现系统最脆弱的环节，充分挖掘业务系统可能被攻击者利用的安全漏洞。

网络安全的本质在对抗，攻击面管理是攻防实战和对抗下的一种主动防御的思想与理念，奇安信的《网络资产攻击面管理解决方案》，是站在攻击者的视角来不断审视与管理资产和薄弱环节的持续过程。致力于打通“资配漏补”安全运行流程与 IT 服务流程，形成跨团队、跨组织的协同运营机制，将传统事件驱动的、临时抱佛脚资产安全运营模式，转变为以数据驱动的常态化运行模式，实现系统资产安全控制措施落地。安

规划一步

奇安信

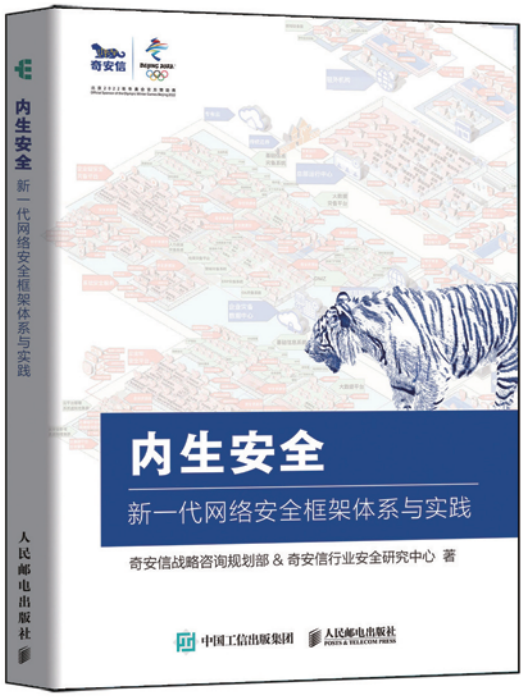
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

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

2024
不止于安全

我国进入高质量发展时代，作为数字经济基石的网络安全，不仅要防范网络风险，还要兼顾业务价值的提升；在许多行业努力降本增效之际，网络安全需要证明其不再是成本中心，而是重要的业务战略投资，将会成为企业的利润中心、机构业务的加速器。2024年乃至今后，安全将不再止于安全。

网络安全：从成本中心到业务助推器

高质量发展时代，网络安全不仅要防范风险，还要兼顾业务价值的提升，成为业务发展的加速器。

高质量发展是新时代我国经济的重要特征。2023 年中央经济工作会议提出“必须把坚持高质量发展作为新时代的硬道理”。由高速增长阶段转向高质量发展阶段，这是新时代我国经济发展的一个重要特征。数字经济作为经济高质量发展的核心，将为中国经济的高质量发展提供有力支撑。

高质量发展新时代，网络安全需要在确保网络与数据安全的同时，考虑如何为业务发展赋能。作为数字经济的基石，网络安全一直被视为成本中心，其对业务发展带来的往往被看作限制与桎梏；政企机构的安全负责人一直面的是对如何证实自身价值的问题。

对政企机构来说，需要改变对网络安全的传统认识，不应再将其视为成本中心，而应视为业务投资一项内容。数字化早已在路上，网络安全需要迫切跟上。正在如制装与培训的投资，可以让个人获得新工作，数字经济时代的网络安全就是业务投资的一部分。面对日益增长的安全风险，为了确保业务连续性和资产安全，需要持续增加对网络安全的投资和从整体上进行安全规划，而非简单地将网络安全视为成本中心，零打碎敲地增加安全能力。

对于网络安全行业及行业安全负责人来说，面对持续恶化的网络安全态势、日益增加的暴露面、攻击者日益增长的能力，但安全支出却无法显著增长的挑战，需要通过理念与范式的转变、技术与应用的创新，确保安全不能止步于安全。

如何通过模式创新、技术创新和应用创新，让安全成为业务的赋能器、加速器？国内一些政企用户基于业务发展需求，推动多种创新应用，打造安全能力的同时实现业务赋能，践行了让安全创造价值的理念。

我们选取了一些具有代表性的技术创新应用案例，作为创新先行者。

- “国资云平台”发展内生安全能力，打造显著的差异化优势，加速了各国企上云、用云的进程；
- “某国家信息中心”利用流量编排解决方案，确保威胁检测无盲区，并兼顾业务的连续性，显著提高设备利用率的同时，大幅降低运维成本；
- 某智能汽车公司实现汽车端到端安全防护，让安全成为亮眼标签。
- 某数字化智能工厂构筑整体工控安全体系，全面控制风险，实现了管理提效和安全保障“双同步”。
- 海关总署部署可信浏览器作为办公基础软件，满足不同业务系统的访问需求，实现对终端浏览器统一管控，同时清晰掌握业务系统访问服务质量。

这些创新应用案例显示，网络安全在夯实经济高质量发展基础的同时，同样可以为政企机构创新业务价值，成为业务的赋能器与加速器。

创新应用 1

安全、降本、提效，某信息中心如何“一箭三雕”？

作者 | 戎泽麟

“作为下属两千余家单位的组织，我们的数据中心经常要同时考虑多个方面，既要保障系统的安全可靠性，还要兼顾业务的连续性，以及提高设备利用率的同时降低运维成本。”某国家级信息中心相关负责人这样表示。

某信息中心是中华人民共和国国务院直属的综合性科研机构，是国内领先的信息化研究和战略咨询组织，下属两千余家单位。其主要任务是为国家发展战略和决策提供科学化、信息化的决策支持和智力支持，旨在推动我国信息领域的发展和建设。该信息中心的主要研究领域包括国家信息化战略与规划、信息资源开发与利用、电子政务、数字经济、智慧城市等，对推动国家信息化加速发展起到非常重要的作用。

近年来，为了加速数字化转型，该信息中心以“两地 + 四中心”方式新建数据中心网络，并严格划分内外网数据中心，为上千家单位提供互联网出口服务，建设信息中心整体网络安全防护与安全运营体系。与此同时，来自加密流量攻击的威胁，以及新旧品类安全设备的整体提效降本，成为最迫切的挑战。

为了解决这些问题，该信息中心通过与奇安信合作，由后者提供了以流量解密编排器（SSLO）为核心，兼顾安全性、流量可视、平滑割接、设备利旧的综合解决方案，完美解决了该信息中心的多重需求。

安全、效率、成本，如何三者兼得?

据介绍，该信息中心在数据中心建设中，主要面临了三个方面的挑战。

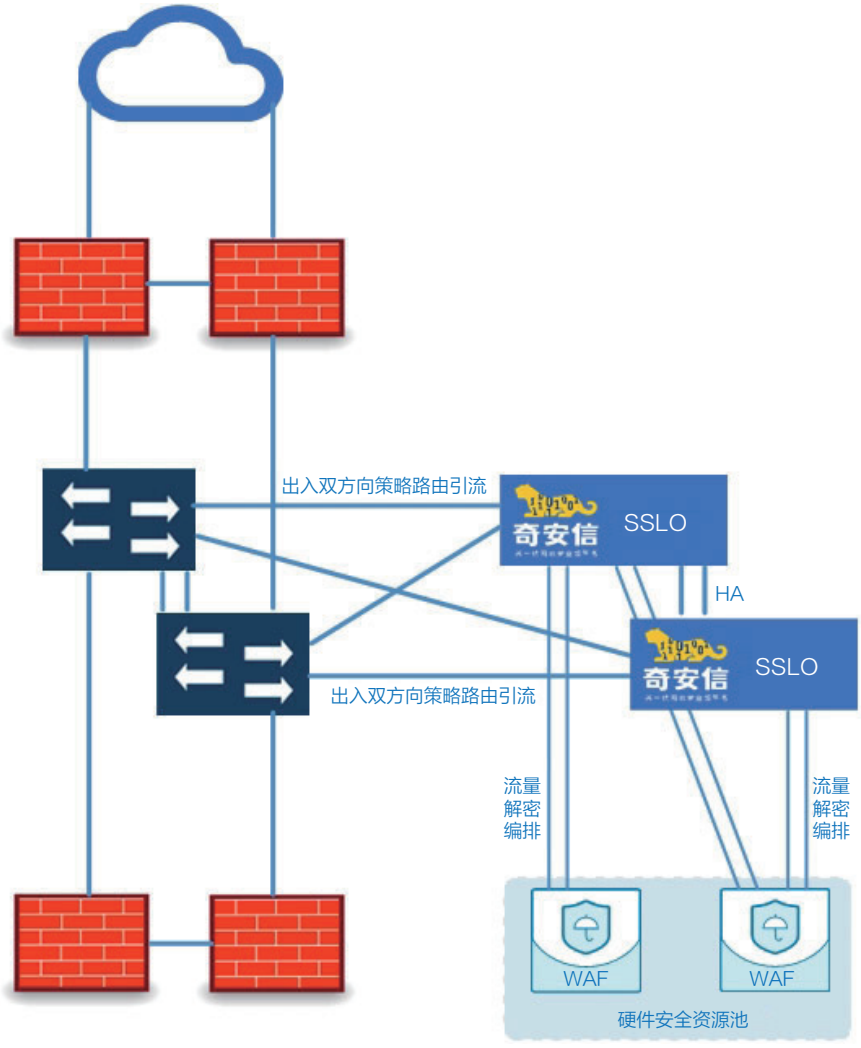
首先是来自加密流量的威胁，很多检测设备处于“半盲”状态。众所周知，基于网络安全合规要求及保障用户数据和系统安全实际需求，越来越多的网站使用加密技术保护数据传输安全，据谷歌统计，目前在互联网上使用 HTTPS 加密流量已经超过九成。而数字化程度越高的企业，加密流量占比往往越高。

奇安信在对信息中心进行风险分析过程中发现，中心内有超过 60% 的系统采用 HTTPS 访问，互联网出口流量有 30%~40% 是加密流量，并且这一比例还将不断增长。可以看出，通过 SSL 或 TLS 加密技术用于保护数据在网络中安全传输成为广泛共识，但是加密后的数据，却增加了威胁检测的难度，加密技术在保护用户数据的同时，也为黑客攻击提供了“隐蔽”通道，导致网络监控实际处于半盲状态。因此，黑客对加密网站的攻击将无法在网络侧进行监测，这是网络安全的重要风险。

第二是新旧安全设备并存，性能被浪费，利用率偏低。目前信息中心已经拥有多厂商、多型号的老旧安全产品，如果全部用新的安全产品替换，无疑会带来很大的成本压力。而且安全产品利用率低，当两台硬件设备做了 HA 之后，只有一台设备正常工作，等于另一台的性能被白白浪费。如何充分提升新旧安全设备的利用率，成为该信息中心的最紧迫课题。

> 以流量解密编排器（SSLO）为核心，兼顾安全性、流量可视、平滑割接、设备利旧的综合解决方案，完美解决了多重需求。

第三是建设过程中设备割接频繁，严重影响业务连续性。数据中心的建设过程是长期过程，而不是一蹴而就的。信息中心新建业务流量编排区域，未来会新增不同的安全产品，就会需要新设备的割接。然而，网络割接可以被视为一项相对复杂且具有挑战性的任务，尤其是当涉及到数据中心的核心网络时。每个割接动作都必须极其谨慎，因为如果操作失败，可能会带来严重后果。因此，该信息中心希望减少新设备上线的割接时间，将对业务的影响降低到最低。



解密与编排一体 奇安信 SSLO 实现三大价值

为了解决以上三大问题，该数据中心在核心交换机旁新增流量解密编排区，采用了奇安信 SSLS 流量解密编排器（SSLO）作为组网核心，该产品与其他安全设备组成解密与编排一体的解决方案，通过重构安全设备部署，构建硬件安全设备资源池，根据业务按需引流，SSL 解密流量编排等技术手段，实现了集成 SSL 解密和按需引流的流量编排方案。

在具体实现上，两套解密编排器物理旁挂在信息中心核心交换机上，业务流量在核心交换机上通过策略路由引流方式，将所有业务流量都引流到解密编排器中。解密编排器再将引流流量发回核心交换机，组网方面实现了物理旁挂，三层路由引流方式接入网络，同时两套解密编排器配置 HA 主备模式，确保设备冗余。

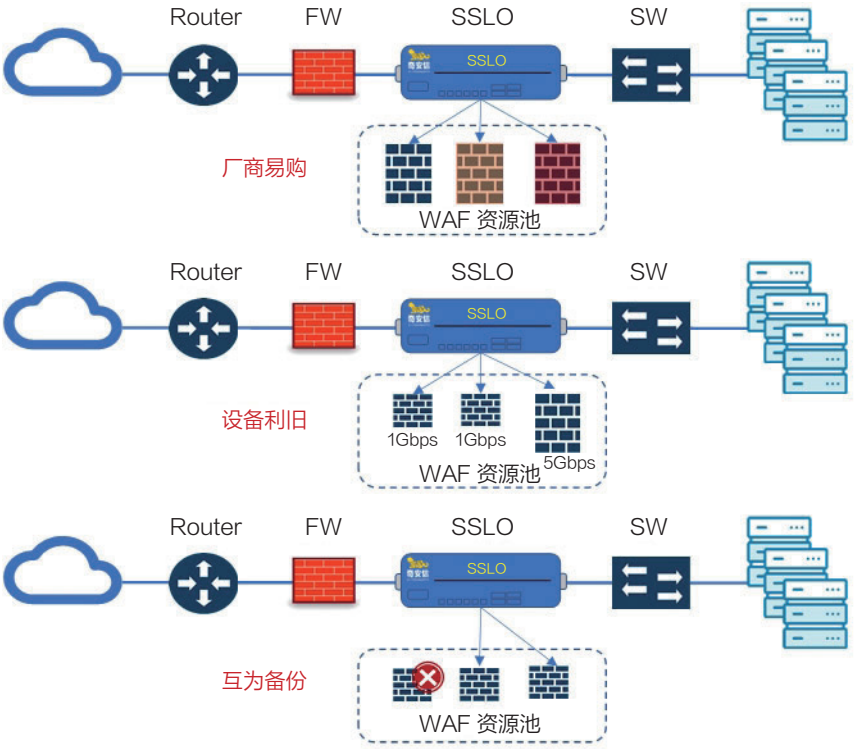
通过解密与编排一体的解决方案，奇安信帮助该信息中心实现了三大价值。

首先是高效解密，一次解密多台设备使用，实现威胁检测无盲区。

数据中心将两套 SSLO 旁挂核心交换机及两套 WAF 与 SSLO 互联，通过核心交换机实现所有业务流量穿行 SSLO，此时加密流量即可解密为明文并编排给 WAF（Web 应用防火墙）和天眼新一代威胁感知系统实现防护与检测，未来还可以给更多新安全设备提供明文流量。这种集中式 SSL/TLS 解密的方式，可以实现一次解密给多种设备使用，显著降低安全设备解密压力。配合精细化流量编排，精细到 IP 和协议的流量匹配，按需将指定流量给到指定安全设备。

凭借流量解密编排器强大的服务链编排能力，奇安信为信息中心规划设计了旁路链和串接链。旁路链是将所有解密后的流量以复制报文方式发送给天眼威胁分析平台，实现加密流量威胁检测；串接链是将识别的 HTTP 明文和 HTTPS 解密后流量通过服务链技术发送给 WAF 设备，WAF 无需再次解密直接进行检测防护，过滤后送回给流量解密编排器，然后重新加密封装，按照原路径进行发送。实现一次解密多次使用的能力，大大提高处理效率，降低网络延时，并且提供了全栈的网络安全检测与防护能力。

在实战攻防演习期间，流量解密编排器与天眼、WAF 协同联动，灵活将指定解密流量给多款旁路检测设备，实现深度检测。解决了以往威胁攻击隐藏在加密流量中安全设备无法检测过滤的问题，极大的增强了现网安全防护能力，使加密流量中的威胁无处可藏，助力该信息中心防守队取得佳绩。



图：安全资源池化部署

其次是硬件资源利用高，设备利旧更简单容易。

该解决方案通过多台安全设备构建安全资源池，提升设备利用率。安全资源池设备基于旁挂部署，不影响接入网络，并支持厂商异构，支持不同性能规格型号，支持带宽、权重等负载方式，方便实现设备利旧。并且，安全资源池设备互为备份，设备异常自动移除下线，流量负载至其余存活设备。

最后是简化安全运维，业务割接不断网。

新设备上下线不影响当前业务，出现异常会自动 bypass，日常运维与割接随时处理，真正实现“零打扰”，运维利旧、扩展升级简单便利。据介绍，在故障排查或割接时，传统网络部署方式，往往可能需要断网，继而导致业务中断。该信息中心最新采用的三层旁路引流方式，由于会话保持在编排器上，被编排的网元可以通过配置实现 bypass，之后所有业务流量流经编排器时，只是路由多一跳；当出现故障需要旁路掉流量解密编排器时，只需在核心交换机上通过简单操作，就可以将编排器进行旁路，整个过程对业务基本不造成影响，最大程度保证业务的平稳进行。安

入选理由

部署以流量解密编排器(SSLO)为核心的解密与编排一体解决方案，兼顾安全性、流量可视、平滑割接、设备利旧需求，完美解决了该信息中心的多重需求，实现精细化防护，简化网络，提升安全设备利用率，降低运维压力，真正实现了安全、提效、降本“一箭三雕”。

创新应用 2

安全能力也能创收变现？运营商行业威胁情报运营最佳实践

作者 | 魏开元

电信运营商作为我国云计算与通信网络基础设施提供商，对网络安全的重视程度相对较高，通常情况下具备相对较为完善的基础安全建设，包括网络边界的防火墙、WAF；流量侧的全流量分析、态势感知；云上的云安全管理平台、云工作负载保护平台等。

但随着新技术的快速落地，云网融合、算网融合加速发展，任何缺乏统一规划、缺乏联动、数据孤岛林立的安全建设，绝不足以应对愈演愈烈的安全威胁。

在这一背景下，基于威胁情报建设统一的安全运营平台，打破不同网络安全设备之间割裂的现状，实现情报共享、统一运营，成为了最佳选择。

一、普遍面临五大安全难题

与很多企业一样，运营商在网络安全建设中，同样会存在明显的“信息孤岛”现象，不同的安全设备之间各自为战，统一运营管理能力不足，主要包含以下五个方面。

第一是“烟囱”林立。

随着网络安全建设的深入，产品类型不断丰富，系统复杂度也在显著增加，这就带来了协同联动的难题。通常情况下，网络攻击并不会局限于系统的某一点，而是一旦得手便会在内部进行不断地横向系统渗透。但对于体量庞大的运营商企业而言，不同的系统通常分属不同部门进行管理，这些系统、网络之间往往存在着一定的安全隔离策略限制，因此无论是产品之间的数据联动还是跨部门的人员协作，都存在一定的困难。

第二是被动防御。

网络安全本质是攻防的对抗，因此新的攻击手段总是层出不穷。依靠被动的静态特征匹配技术处置已知威胁效果十分显著，但难以识别新型攻击手法和未知恶意样本。想要做到主动发现未知威胁，只能依靠安全专家的判断，如此一来不仅费时费力，还会消耗大量人力物力，显著增加了安全运营的成本。

第三是海量告警。

随着安全设备的逐渐增多，巨量的告警日志成为了摆在所有安全运营人员面前的一道难题。为了确保真正的网络攻击不被漏掉，安全运营人员不得不花费大量时间去查看并分析这

些告警背后的真实原因。但面对海量告警，有限的人员在有限的时间内很难完成处置。

第四是视野受限。

由于不同的安全设备能看到的数据视野十分有限，安全运营人员无法基于全量数据进行威胁分析，比如，终端侧产生的告警就只能看到终端侧的攻击行为，无法看清攻击全貌，也就无法做到端到端溯源，对于某些特定的威胁组织，攻击 IP、域名、样本等分析能力相对薄弱。另外，面对内部产生的大量数据，如何利用这些数据产生有价值的情报从而指导威胁分析，也是亟需解决的一个问题。

第五是安全成本居高不下。

在威胁与合规的双轮驱动下，作为国家关键信息基础设施的关键一环，运营商企业不得不投入更多的资源，建设网络安全体系。尽管网络安全建设能够降低网络攻击造成的损失，但毕竟安全能力的建设并不能直接产生短期可见的收益。对于任意一家企业，如何降本增效、开源节流是一个必须解决的问题。

二、化被动为主动，威胁情报成为破局关键

显而易见，传统安全防护手段的弱点在于对于威胁毫不知情，不能料敌于先，无法精准判断对手的动向，从而制定统一的、积极的防护策略，只能被动应对，各个模块之间的协同联动也就无从谈起。

而想要化被动为主动，情报起到的作用将会是至关重要的。众所周知，威胁情报的价值就在于解决攻防不对等，将企业安全建设、安全运营变被动为主动，实现知己知彼。作为新时代网络安全的“血液”，威胁情报能够将所有安全设备有机的结合在一起，为网络安全防护提供必要的“营养”。

显然，威胁情报能力的建设，成为破局的关键。

需要注意的是，威胁情报能力建设并非简单的威胁情报消费，即使用现成的 IOC 做失陷检测这么简单。事实证明，在高水平的网络攻击中，攻击者会搜集目标大量信息，并制定针对性的入侵计划和针对性的攻击武器，想要发现这些定向攻击，单独的情报消费远远不够。

因此，建设自有威胁情报中心，打通威胁情报生产、共享和消费全生命周期的必要性，被凸显出来，即在企业内部部署完整的威胁情报工具平台、基础数据、运营流程和分析人员，建设基于本地数据和外部情报联动的情报运营体系。

而云、网、数据和算力，正是运营商企业的优势所在，因此在建设自有威胁情报中心方面，有着先天的优势。

对此，奇安信威胁情报运营系统 TIOS 能够满足客户需求。

该系统是奇安信推出的一站式情报内生解决方案，包含威胁情报平台（TIP）、威胁情报运营平台（TIM）、邮件检测系统、样本同源分析系统、文件样本鉴定平台等安全组件，能够提供威胁研判、攻击定性、黑客画像及威胁持续跟踪等服务，同时提供多维度的威胁情报数据和分析应用，实现威胁情报的数据接入、生产、处理、运营与消费的闭环建设。

基于奇安信 TIOS 建设的威胁情报中心，能够聚合分析多源互联网安全情报数据，以及奇安信独有的千万级终端的遥测数据、十亿级互联网资产及应用数据、万亿级历史 Passive DNS 数据，同时结合运营商骨干网、城域网等大网流量数据，生产运营商高价值私有安全情报，为自有安全产品及公司自有业务威胁监测进行安全赋能。

在完成先期的威胁情报中心建设后，企业能够在下面两个方面有较大提升。

首先是海量恶意文档并行分析能力，奇安信威胁情报沙箱深度集成了多个威胁检测引擎，可进行恶意代码特征深度检测，同时支持 50+ 分析器对恶意样本进行并行分析，日均检测样本数量超过一万个，完全能够满足日常乃至实战攻防演习期间的恶意样本鉴定需求。

其次是全网威胁研判和溯源分析能力，通过优化威胁情报事件研判、攻击定性分析能力，完善私有威胁情报库及档案库内容管理，从而具备安全数据实时报送、攻击特征实时监测及历史溯源分析等能力。

> 鉴于运营商行业的特殊性，其自有威胁情报中心除了能对内提升网络安全防护水平，还可以实现对外赋能，为客户提供高质量威胁情报。

情报赋能，构建网络安全协同防护体系。

基于奇安信 TIOS 构建的自有威胁情报中心，能够与运营商企业现有安全体系的深度融合，无论是防护体系的任意一点发现入侵痕迹，都可以基于自有威胁情报中心的海量情报数据进行全网分析比对，然后快速定位公司内部所有失陷主机，同时通过安全运营中心统一下发应急处置策略，第一时间将威胁消弭于无形，从而打破了传统网络安全体系互相割裂的现状，消除烟囱和孤岛现象，形成公司网络安全共同体。

所有检测到的恶意样本和攻击行为，又会形成新的威胁情报，经由自有威胁情报中心下发到各个安全设备。就像心脏一样，把血液送到全身各个器官，从而形成一个有机的生命体。

其价值主要体现在几个方面：

第一，主动防御。通过威胁情报的生产、消费的闭环，实现主动的威胁狩猎、一体化的响应处置及精准的威胁溯源，同时在攻击发生之前提前采取防御措施的方式，降低新型威胁带来的实际业务损失。

第二，告警降噪。针对巨量的告警，可利用威胁情报对告警进行智能化筛选，极大降低噪音告警数量，提升有价值告警的分析效率；统计数据显示，威胁情报中心投入运营后，公司误报率整体降低约 30%。

第三，APT 追踪。基于威胁情报大数据积累的样本、IP、域名等已有的 APT 组织特征，第一时间追踪到特定 APT 组织的攻击信息。

第四，内外赋能。建立威胁情报中心后，除了可对内部安全系统进行赋能来提升安全运维效率，也可以对已经产生的情报数据实施对外能力提供，针对政企客户提供威胁情报库碰撞，威胁风险评估等服务，可直接把威胁情报中心的能力转化为创收，实现安全能力变现。

三、内外兼修，构建威胁情报闭环运营

值得注意的是，鉴于运营商行业的特殊性，拥有大量的云、网络安全和网络基础设施客户，其自有威胁情报中心除了能够对内提升网络安全防护水平，还可以实现对外赋能，为客户提供高质量威胁情报。

运营商企业拥有业内最全的骨干网、城域网流量数据，这是任何其他类型企业都无法比拟的，这也是运营商威胁情报能力可以实现对外创收的关键。

在完成威胁情报中心基础能力建设后，企业还可规划新增云端 SaaS 服务，以在线服务的方式对外提供新型样本威胁分析、VPC 环境回连检测、用户业务资产失陷检测、互联网 DNS 威胁检测等引擎能力，并对异常威胁检测分析引擎进行扩容，有效提升面向安全产品、内部业务和外部客户的安全赋能能力。安

入选理由

发挥运营商先天数据优势，实现威胁情报闭环运营。
该运营商公司通过建设本地化威胁情报中心，打通了威胁情报的生产、共享、消费的各个环节，实现内部情报数据和外部大网数据的联动，创新性做到了在内部提高威胁检测与响应基线能力的同时，实现对外部客户赋能，甚至可将能力转化为创收，实现安全能力变现，堪称威胁情报能力在行业应用的最佳实践。

创新应用 3

国企数字化转型全面提速，云安全如何实现内生融合？

作者 | 于水情 梁阳旭 方建国

北京能源、北京燃气、北京水务、北京公交、首农食品……作为国民经济的“稳定器”和“压舱石”，北京国企在保障首都水、气、热、路、运、环、食等方面发挥着不可替代的重要作用，承担了几乎全部的公共交通服务、70% 的城市供水量、96% 的污水处理量、95% 的燃气供应量、40% 的供热面积、60% 的垃圾处理量等。可以说，2000 多万首都人民的衣食住行、日常工作生活，背后都离不开北京国企的强大支撑。

“建设全球数字经济标杆城市”是北京市“十四五”规划提出的战略目标，目前，数字经济占北京市 GDP 比重已超过 40%，位列全国第一。作为数字化转型的“先锋队”和“主力军”，北京国有企业近年来全面加速上云、用云的进程，带头引领以云计算为代表的新一轮科技革命，成为北京数字经济发展的重要力量。

然而，国企数字化平台大都承载着关乎国计民生、社会稳定的业务和数据，一旦遭受黑客攻击或数据泄露和破坏，都会引发不可估量的严重后果。近期以来全球频发的云基础设施频繁遭受攻击，更体现了这种严峻形势。如何在云体系建设过程中，提供安全可靠、自主可控的网络安全保障，成为摆在北京国资委和各国企面前迫切要解决的问题。

一、构筑国企云平台，赋能市属国企数字化转型

“切实加强合规管理，注意防范风险；高标准构建信息安全保障能力，系统提升数据、算法、算力集约化整合能力，力争建成数字化转型示范标杆。”为推动北京市国企数字化转型，并构筑自主可控的数字中国底座，北京市国资委对市属国有企业提出了以上要求。

其中，国企数字协同创新云平台（以下简称“国企云”）是北京市属国企数字化转型工作的助推器。建成后，将成为北京市属国企首朵可规模化运营、全栈可控的信创云，赋能市属国有企业数字化转型工作。

据国企云的建设方北控数科（北控集团全资成立的二级企业）相关负责人介绍，北控数科将发挥国资企业主力军作用，联合行业龙头企业，建

设和运营国企数字协同创新云平台，以首善的标准，集约化建设安全可信的国企云平台，打造首都国企高质量发展的坚强数字化底座。

国企云建设坚持高标准、集中化的要求，兼顾云平台的功能齐全、运行高效、使用灵活、维护方便、安全稳定、易于扩展等优势。云平台建成后，不仅面对北控集团控股公司，更面向广大的北京市属国企，为客户提供行业私有云、混合云和大数据等整体解决方案。

二、国企上云用云加速，安全风险愈发复杂严峻

近年来，全球范围以云平台为目标的网络攻击事件频发，愈演愈烈。2023 年 8 月，拥有 8 万台服务器的全球云服务商 Leaseweb 遭遇安全事件，导致一些关键系统被迫关闭，部分客户的云停止服务。12 月，意大利云服务提供商 Westpole 在 12 月 8 日遭受网络攻击，上千个政府机构服务中断、数据丢失。

国企云安全面临以下四个方面的挑战。

首先是云计算给现有安全架构带来了严峻挑战，安全隐患无处不在。

云计算弹性化带来了便利，同时带来了大量僵尸主机、不当暴露的端口、不当安全配置、弱口令等。有数据统计，政企 90% 安全事件和不当操作有关。而 2023 年 Verizon 数据泄露报告显示，74% 数据泄露事件涉及人为因素。

同时，云计算导致传统安全域划分逐渐失效，东西向流量不可见、横向移动无法及时发现等成为主要的安全问题。云上业务的复杂化导致更多暴露面，无文件攻击、供应链攻击等

新型攻击方式出现，竖井式的安全设备无法及时发现问题。

其次是外部的网络攻击日益专业化、趋利化，对关键基础设施威胁加大。

云上算力高度集中、数据高度集中、以经济为目的，勒索、挖矿、数据窃取等攻击方式大行其道。数字货币起推波助澜作用。云数据中心作为关键基础设施，以政治为目的，专业APT 组织日益猖獗，国家关键基础设施成为主要攻击对象。

再次是虚拟化引入给云基础设施带来新的风险。

国企云基础设施防护包括构建云计算环境所需的云操作系统（云业务及云基础设施管理）、虚拟化层（Hypervisor）、基础设施（网络、计算、存储）的安全防护。云基础设施一旦被攻破将威胁到云平台所承载的所有应用安全。

由于云计算与虚拟化环境自身的特性，企业需要充分考虑虚拟化的引入为企业带来的相应的风险，根据各个风险点带来的问题及威胁建设针对性的防护方案，以保障企业数据的安全及业务系统的平稳运行。

最后是提供国企云服务的企业，普遍面临来自 Web 安全、内容安全、应用安全等业务应用层的风险。

其中在 Web 安全方面，企业云上业务系统多采用 HTTP/S 应用协议（Web）对外提供服务，因而其面临的各种攻击可能都会转嫁至云应用上，攻击者利用 Web 服务可能存在的诸多漏洞进行攻击，窃取业务系统数据或权限等；在内容安全方面，云上业务系统数据可能遭受病毒、蠕虫、木马攻击，在传输过程中存在被中途窃取或篡改的风险，造成数据完整性和机密性受到影响；而在应用安全方面，对于将应用迁移至云上的企业而言，在迁移过程中可能会涉及迁移安全、风险评估等诸多问题。

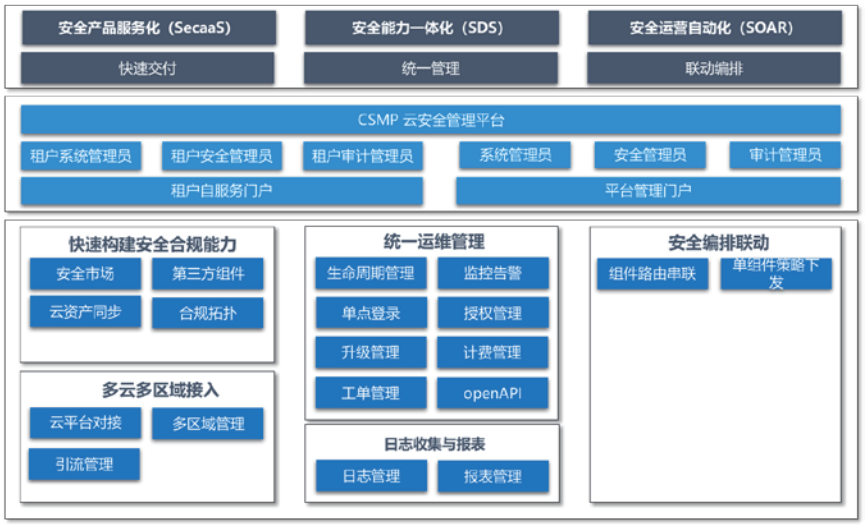
三、云平台与云安全同步建设，实现数据驱动的内生安全

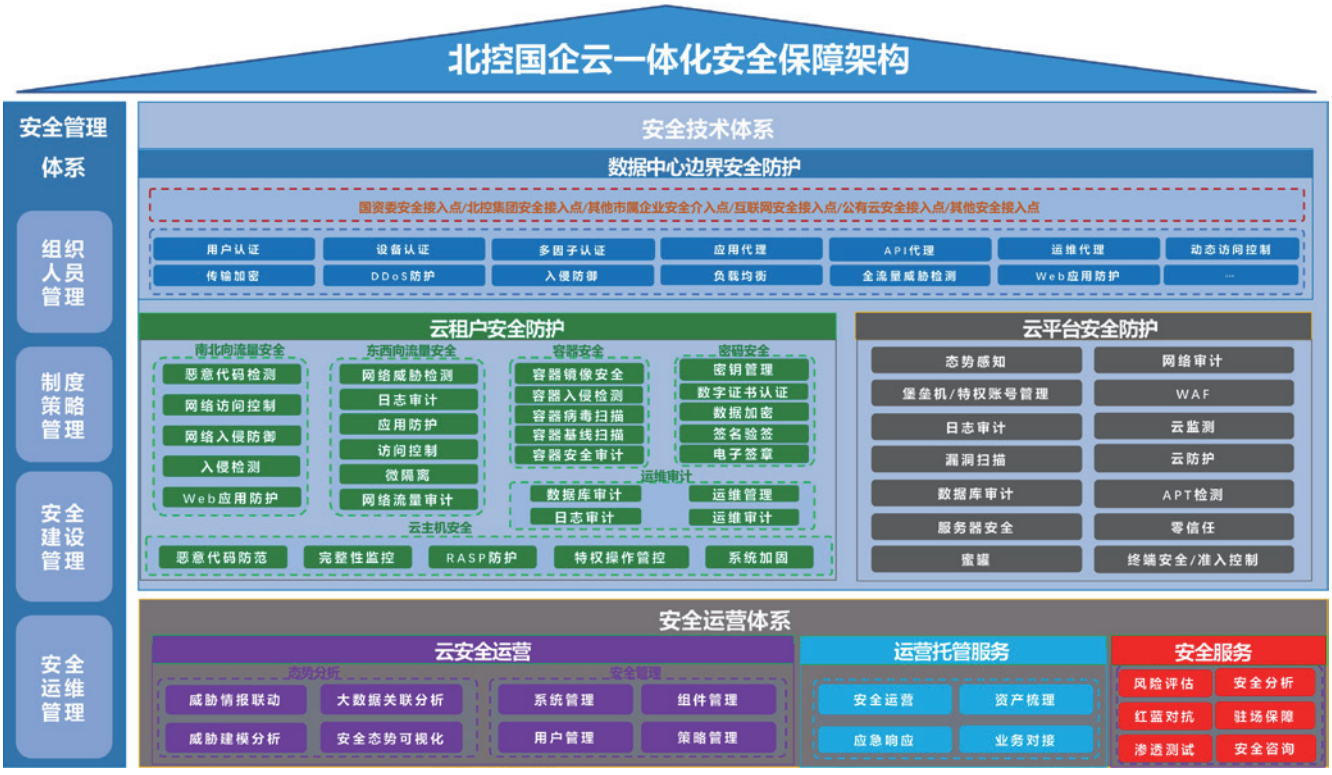
面对市属国有企业迫切的数字化转型需求和面临的网络安全挑战，在市国资委指导下，北控数科（北控集团全资成立的二级企业）履行使命担当，构建国企数字协同创新云平台（以下简称“国企云”），目标是打造一流的数字基础设施、一流的数据分析中心、一流的数字化服务中心，为市属国企提供一流的数字化服务。

在安全保障方面，北控数科联合奇安信，共同建设和运营国企云，保障国企云安全，赋能市属国企数字化转型工作。以国企云核心能力为驱动，打造“北京方案”、创造“北京模式”、塑造“北京样板”用数字化手段助推北京全球数字经济标杆城市建设。

“作为促进央国企数字化转型重要底座，云平台在引入云、大数据等新技术的同时，也面临着新的安全风险，而传统安全模式已难以适应快速的变化，对此，我们提出了用新一代网络安全框架来保护国企云安全，获得了客户和相关合作方的普遍认可。”奇安信相关负责人表示。

更具体来说，新一代网络安全框架引入内生安全的理念。所谓内生安全，就是把安全能力与业务系统和相关流程紧密结合起来，进行深度融合，





把原来静态的、局部的、外挂式的安全策略，升级为动态的、系统的、内生的防护措施，从而建立自适应的安全免疫体系。因此，国企云选择数据驱动的内生安全体系来构建国企云安全立体防护架构，保障自身安全。

首先，通过奇安信云安全管理平台为北控数科云搭建云基础安全防护体系，并通过三项核心功能，满足云计算数据中心安全需求。

① 安全产品服务化：通过将安全产品资源池化，支持多资源池弹性部署，从而解决客户快速构建安全合规能力，和多云多区域接入的需求，实现快速交付；

② 安全能力一体化：通过将安全能力整合在云安全管理平台，进行统一运维管理和数据展现，从而解决客户统一运维管理和日志收集报表展现需求，实现统一安全管理；

③ 安全运营自动化：通过在平台整合安全组件的网络能力，支持如防火墙 WAF 的路由编排和策略下发，从而解决客户的安全联动需求，实现安全能力联动。

其次，云安全管理平台提供两类门户入口，支持租户通过自服务门户进行安全组件的创建和业务管理，也支持管理员通过平台管理门户进行统一管理，租户和管理员都支持三权分立模式，默认平台管理门户支持系统管理员，租户自服务门户支持租户系统管理员、租户审计管理员，开启三权后，支持系统、安全和审计三个角色。

针对云计算环境特性及安全需求分析，奇安信云安全管理平台遵循国家信息安全等级保护第三级要求和相关安全建设标准规范，构建了一套体

系化的云计算环境安全保障体系，全面提升云计算安全管理水平及运营水平，并具备自适应、弹性伸缩、敏捷性等管理优势，以适应云计算动态变化的安全需求。

此外，国企云安全中心基于新一代网络安全框架，以及内生安全理念，着力构建体系化、集约化的安全能力，以保障国企云、市属国企云上业务安全，并提供定制化安全服务。通过部署奇安信态势感知与安全运营平台等产品，全面感知市属国企云数据中心的安全态势，为国企用户业务的统一安全监测提供技术支撑、数据支撑。

得益于双方的深度信任和默契合作，国企云安全中心在云平台建设之初就深度融入其中，从而把安全能力与业务系统和相关流程紧密结合起来，进行深度融合，将原来静态的、局部的、外挂式的安全策略，升级为动态的、系统的、内生的防护措施，从而建立自适应的安全免疫体系，真正实现内生安全“自适应、自主、自生长”的目标。

在技术创新方面，该项目兼顾了项目的安全自主可控和未来可扩展性。国企云安全体系通过打造基于信创技术的新型网信架构，实现了网信基础设施的集约化建设、集约化管理、集约化运营，并且为市管企业数字化转型和信创替代提供全面技术支撑和服务保障。

同时，所有的网络安全产品，软、硬件也实现了全面信创。截至目前，国企云已全部支持 IPv4 与 IPv6 双栈协议，具备 IPv4 和 IPv6 转换平台，无论是网站群、移动办公应用上云后，从基础网络到安全防护都能满足企业 IPv6 改造要求。

安全人才短缺是市属各国企上云过程中的突出矛盾。为此，北控数科联合奇安信共同运营国企云安全，各自派出强大的技术支撑团队、人员，形成国企云安全中心的安全运营团队、安全服务团队，保障国企云自身安全的同时，还能够为市属国企提供专业的增值网络安全服务。

四、塑造国企云新标杆

奇安信和北控数科共同构建的国企云安全体系，不仅是北京市国资委国企云安全建设的重要抓手，同时这种模式为国内广大国企、央企等探索了一条可落地实践的标杆示范，对全国各地国企云建设及联合运营模式有非常强的借鉴参考复制意义和价值。

2023 年中关村数字经济产业联盟发布《2023 全国数字经济典型场景与解决方案》，北控数科“国企云安全案例”被评为 2023 数字化应用场景十佳解决方案之一。 安

入选理由

成功打造安全内生的国企云，树立国企云建设新标杆。
该项目的创新性在于，国企云平台建设之初，安全中心就深度融入其中，实现安全能力与业务紧密结合，将原来静态的、局部的、外挂式的安全策略，升级为动态的、系统的、内生的防护措施，真正实现内生安全“自适应、自主、自生长”的目标，真正加速了国企上云、用云等数字化转型的进程。

创新应用 4

新能源车企如何应对网络安全挑战？赛力斯“安全之路”分享

作者 | 付海涛

发展新能源汽车是我国从汽车大国迈向汽车强国的必由之路，是应对气候变化、推动绿色发展的战略举措。我国坚持纯电驱动战略取向，使得新能源汽车产业发展取得了巨大成就，成为世界汽车产业发展转型的重要力量之一。当前，全球新一轮科技革命和产业变革蓬勃发展，汽车与能源、交通、信息通信等领域有关技术加速融合，电动化、网联化、智能化成为汽车产业持续发展的潮流和趋势。作为中国企业 500 强，以新能源汽车为核心业务的科技型制造企业，赛力斯集团致力于推动汽车能源变革，实现创享智慧移动生活的使命。

赛力斯集团 IT 与网络数据安全总部雷相其部长表示：“赛力斯一直以习近平新时代中国特色社会主义思想为指引，推进以数据为纽带的‘人—车—路—云’高效协同，基于汽车感知、交通管控、城市管理等信息，构建‘人—车—路—云’多层数据融合与计算处理平台，开展特定场景、区域及道路的示范应用，促进新能源汽车与信息通信融合应用服务创新。”在面对技术深化发展、多种风险层出不穷的情况下，赛力斯着眼于构建完整的网络安全管理体系，推动密码技术深入应用，强化新能源汽车数据分级分类，健全新能源汽车网络安全管理制度、标准、流程和规范，完善风险评估、预警监测、应急响应机制，保障‘车端—传输管网—云端’各环节信息安全。

车辆智能化网联化大势所趋，安全风险随之而来

随着全球联网车辆的数量的高速增长，预计将从现在的 2.5 亿辆增长到 2040 年的 10 亿辆以上，车辆网络安全挑战正在成为热点议题。根据研究机构 Upstream 发布的《2023 年全球汽车行业网络安全报告》显示，全球汽车行

业在过去 5 年中因网络攻击而遭受的损失超过了 5000 亿美元，而近 70% 的汽车安全威胁都是由远程网络攻击行为引发的，仅仅是 2021 年到 2023 年全球公开发布的汽车网络安全事件就超过了 1300 多起。因此，汽车行业构建更牢固可靠的网络安全防线已迫在眉睫。

雷相其部长表示：“在过去，我们更多地着眼于车企的整体信息安全，随着车辆智能网联化的进一步发展，带来了更多便利的同时，也增加了更多的安全风险。

对于目前车企面临的主要信息安全问题，雷相其部长归纳了三个方面。

首先是智能化网联化带来的网络安全技术与合规风险。

开放发展和安全往往是对立统一的矛盾，新技术和新业务的持续应用，可能会不断地导致新安全漏洞的产生，车辆互联使得车辆能够实现与外部通信，比如，远程诊断和升级功能使得车辆生产商可以在线更新软件和固件，但这也会让黑客入侵系统和破坏车辆变得更为容易。

同时，随着新技术和业务的不断推进，监管机构持续制定政策法规以确保车辆安全和隐私的全生命周期的保护，这可能会对企业造成合规压力。

汽车企业需要密切关注这些风险，并采取必要的策略和技术措施来保护数据和车辆的安全，保障业务的持续发展和运营。

其次是供应链网络安全合规风险。

汽车的研发和生产制造过程涉及大量的供应商提供的产品，而这些供应商提供的产品有可能存在网络安全漏洞，这将会成为汽车供应链安全攻击的潜在入口。与此同时，汽车制造企业作为汽车产品责任人，需要对消费者、监管机构和社会承担网络安全合规的主体责任，此形势下汽车制造企业如何加强汽车的产业供应链安全管理，确保所有供应商企业都符合统一且明确的安全合规标准，这些方面将面临巨大的挑战。

最后是车企出海面临的合规风险。

汽车企业出海之前，需要注意网络安全及数据安全合规风险，不同国家和地区会有不同的市场监管法规和标准，企业需要了解并遵守当地法规和标准，尤其是进入国外成熟市场将面临非常严苛的合规监管挑战，如欧盟的车辆产品网络安全合规准入认证等。因此，海外业务运营过程中持续满足合规要求是车企出海制胜的关键。

强强联手、稳步推进，共同破解网络安全难题

作为国内领先的智能汽车制造商和国内领先的网络安全企业，赛力斯和奇安信在 2023 年重庆智博会同期举办的新能源汽车智能座舱生态论坛上，共同签署战略合作协议，双方约定将在智能网联汽车领域网络与数据安全威胁检测防护、监测预警、威胁信息共享、应急处置协同等方面开展深入合作，按照“长期合作，优势互补，互利共赢，共同发展”的原则，建立长期稳定的战略合作关系。

近日，在赛力斯生态网联车端安全检测项目中，通过多方方案的比较和深入考察，赛力斯最终选择奇安信作为生态网联车端安全检测项目的安全技术服务提供商，随着项目合同的正式签署，赛力斯与奇安信立刻启动项目团队组建，迅速展开项目实施各项工作。

项目启动会中，双方项目团队明确了项目时间点、分项负责人、项目质量管理、项目沟通机制等，后续双方项目经理按照工作计划表逐项推进。

奇安信车联网安全团队负责完成车辆入侵检测模块和安全运营平台的开发和搭建，主要工作包括以下几个方面：

其中在 CAN 入侵检测方面，重点

工作包括检测整个车载网络的负载率和信息熵，定义安全阈值，防止如泛洪攻击、重放攻击等异常行为发生；根据 DBC 文件，检测单帧报文是否符合 DBC 定义；定义报文序列管理、信号关系等正常场景和 UDS 探测等攻击场景；

在主机入侵检测方面，包括检测应用操作行为、文件行为、进程行为、系统 API 调用、系统 root 行为、系统资源占用等，可对非法网络连接、提权攻击、敏感信息窃取等攻击行为进行告警；可对车机系统、应用、进程、文件等 10 类 100 多种日志数据进行采集上报、威胁分析和溯源；

在以太网入侵检测方面，工作包括实时监控统计车端应用流量，发现异常流量消耗行为，基于 IP 五元组、APP、URL 进行访问控制，可识别 HTTP、DoIP、DNS 等协议内容，可检测文件传输、空车指令、隐私数据泄露等应用层攻击行为。

当然，网络安全不是部署好设备就可以高枕无忧了，告警需要研判、日志需要分析、事件需要处置、策略也需要执行，这是一条永无止境的安全运营之路。为此，奇安信为赛力斯量身打造了适合智能网联车企的安全运营平台。

据介绍，该运营平台基于 Gartner 自适应安全架构，以安全风险管理为关键流程，以 AI 算法及大数据计算能力为核心，融合车端、产线端等探针数据，对汽车网络安全事件、漏洞等进行关联分析、风险识别、威胁预警、风险评估及应急响应处置，包含了系统管理、资产管理、风险管理、应急响应、态势感知、规则运营等功能模块，为赛力斯开展安全运营提供了强大的工具平台。

在项目具体实施过程中，因项目所涉及的人员多，部门跨度广，各方之间的需求和期望不统一，给项目协调和推动工作带来很大难度，但通过前期建立的项目流程和团队，双方项目经理及时拉通部门负责人，建立合作和信任的氛围，以及有效的沟通策略解决各种分歧，共同推动项目成功。

在赛力斯产品网络与数据安全部曹国华部长看来，项目团队是不分甲方乙方的，应该是一个团队，要共同奔着实现项目目标一起努力，奇安信团队在交付过程中表现出来的专业性、责任心，获得了赛力斯的充分肯定。同时曹部长也表示，虽然目前的重点是保障项目交付，但交流合作还需要持续深入，双方要发挥各自优势，为赛力斯和智能汽车行业发展贡献力量。

构建闭环安全体系，创造三大价值

在赛力斯生态网联车端安全检测项目启动会上，曹国华部长提到汽车出海是赛力斯业务发展重要一环，国内自主品牌车企在海外发展壮大，向全球展示中国汽车的领先技术，有助于提升中国汽车品牌形象，但想要真正实现高质量出海，企业首先要遵守当地的法律法规，譬如欧盟地区的 R155 法规，这需要汽

> 车辆的网络安全已成为汽车企业安全运营的关键一环，车辆网络安全成为汽车企业战略业务目标的重要部分。

车企业建立和完善车辆的网络安全管理体系和技术体系。

通过本次项目，奇安信协助赛力斯建设了涵盖整车及零部件深度威胁检测能力，基于 B/S 架构实现集中管理，对车辆安全形成检测、防护、响应、管理、分析、策略运营的闭环安全管理流程体系，给赛力斯提供了以下三大价值。

首先，符合 R155 的法规要求，让汽车出海有了“准入证”。目前搭建的安全运营平台可以覆盖约 20 万辆汽车，可以给 20 万辆车颁发“网络安全合格证”；赛力斯一直努力为客户打造舒适安全的驾乘体验，特别是现在攻击手段越来越复杂的情况下，网络安全更是汽车安全的重要部分，合规只是赛力斯在汽车网络安全走出的第一步；通过奇安信给赛力斯搭建的安全运营平台和体系，利用机器学习、模型匹配的方式实现异常数据检测，进行未知威胁能力持续分析，并通过算法和模型更新，确保系统能力可以不断升级，满足不断增长的安全威胁需要；而且可以有效的培养公司内部安全团队，持续为赛力斯的客户打造安全可靠的驾乘体验。

其次，能够做到监控、分析及应对汽车网络安全风险。项目以汽车资产为对象，以安全风险管理为关键流程，以 AI 算法及大数据计算能力为核心，打造实时的风险计算引擎及车载安全组件，对汽车网络安全事件、漏洞等进行关联分析、风险识别、威胁预警、风险评估及应急响应处置，赋能车企更好的看到威胁、看清风险、及时预警。

最后，提供了直观的安全运营工具，显著提升效率。平台能够对采集的各类安全数据、态势要素进行综合分析评判，通过多维度和指标化的形式来呈现整体安全运行态势和资产、漏洞、攻击、管理等专题态势，并进行可视化展示，帮助安全分析人员辅助决策和运维指导，同时赋予定量化的数据分析及实践能力，显著提升了安全管理和决策效率。

未来：网络安全更深度融入企业战略，助力企业发展

对于未来的发展，曹国华部长表示，车辆的网络安全已成为汽车企业安全运营的关键一环，车辆的网络威胁从技术问题转变为商业挑战，我们现在也看到了车辆网络安全的定位从基础技术到业务战略的转变，成为汽车企业战略业务目标的重要部分。

“车企的网络安全能力将会直接影响企业的商誉和品牌影响力”，雷相其部长谈到。一方面赛力斯将会加大网络安全领域的投入，开展各类安全合规管理和技术落地措施；另一方面，将加大车辆网络安全与企业原有安全业务的全面融合，实现企业及汽车网络安全的端到端内生安全防护，全面保障驾乘人员生命财产安全和企业信息安全。安

入选理由

正如曹国华部长所说的，车辆的网络安全已成为了汽车企业安全运营的关键一环，其定位也从基础技术升级到业务战略，并成为汽车企业战略业务目标的重要部分。随着安全成为赛力斯的亮眼标签之一，其旗下新能源汽车的出海战略、销售前景和用户口碑也势必将水涨船高。

创新应用 5

在数字化转型道路上乘风破浪，用安全点亮一座座灯塔工厂

——某大型机械制造企业工业互联网安全建设案例

作者 | 唐鹏程

“我们这个行业最大的痛点就是行业周期影响大，工程机械的发展受国家基建投资和宏观经济环境影响很大，这也是我们下定决心全面推进数字化与智能化转型的重要原因。”

在与某大型机械制造企业的信息化与智能化建设与网络安全的需求与目标沟通时，BP&IT(质量与流程 IT 管理部) 负责人和我们聊到了工程机械行业的痛点。并且告诉我们，除了面向行业的发展痛点，还面临伴随数字化与智能化转型过程中的工业互联网伴生的风险防御与检测需求，他表示，“从 2008 年开始我们发布《XX 集团制造技术方案大纲》以来，高度的工业互联场景下我们不得不考虑工业互联网与数据安全问题，因此进行一场彻底的面向工业互联网的安全规划与建设尤其重要。”

某大型机械制造企业试点工厂

数字化智能制造工厂率先启动，安全风险随之而来

2013 年开始，该机械制造企业开启流程信息化改造，深化信息化变革，开始建设数字化工厂平台。也就是在这个阶段，依托工信部支持的“国家两化融合智能制造专项”科技项目，该机械制造企业启动打造了首个全球数字化智能制造工厂——试点工厂，建设和实施了智能加工中心与生产线、智能化仓储与运输配送、计划与执行等 6 个子系统。

“试点工厂建成投产以后，生产方式从将传统的人工作业、机械作业、单点自动化转向高度集成自动化、数控化以及智能化设备转变，我们逐渐开始对智能化场景中的端、点设备安全变得敏感。尤其是一些进口的高端精密设备，一旦遭受网络攻击，损失会非常大，甚至威胁工厂正常生产。然而此时此刻我

们就发现工厂内的部分工控机有病毒存在。”BP&IT 网络安全组相关负责人向我们表达了原始诉求。

关键设备突破产能瓶颈是该机械制造企业提升效能的重要环节，而关键设备的保护，涉及控制设备与执行设备的漏洞风险、控制协议脆弱性风险、控制主机病毒入侵风险，以及网络通信风险急需得到有效处理。

在试点先行、同步规划的指导思想下，该机械制造企业选择以试点厂房为试点开始进行第一轮咨询与评估。针对试点厂房的下料、成型、机加、装配、涂装、AGV 物流、立库与焊装 8 大工艺系统进行现场技术和管理层面的评估。

评估结果显示，在工业控制系统运行的 11 大类、129 个细项的检查中，总体安全符合度有 77 项，占比 60%，去掉不适用部分 10 项 8% 之外，风险暴露部分占比超过 30%。其中以威胁和外联无法管控为主要部分。

根据该机械制造企业的网络安全管理办法，禁止一切不符合标准的工控机访问互联网，需要通过远程访问方式进入内网调试需通过堡垒机。在试点工厂的评估过程中，发现有工控终端设备通过私人远程工具对厂家提供远程桌面服务，且不受时间与监管限制，对此 BP&IT 部门提出强烈要求，必须禁止行为、严格管控、加强措施！

另外，该机械制造企业还通过流量分析技术，发现工控网络中存在安全威胁，经分析总结发现安全威胁 12 个，紧急风险 2 个，高风险 1 个，中风险 5 个。其中包括了挖矿蠕虫、Artemis Botnet C&C 活动事件及其他相关漏洞。

基于白名单防护理念，构筑整体工控安全体系

“我们做了大量的流程化管理设计，也将传统的 MES 升级成为 MOM 管理系统，皆在建立智能化工厂的统一管理平台，安全需要这样做。”

在集团统一的管理目标之下，结合已经发现的问题，当务之急便是充分理解该机械制造企业的业务现状及发展方向，制定出满足能面向全国包括 28 家灯塔工厂，以及近百座普通工厂的风险可控、威胁可视、流程闭环的安全管理平台。

时间线回到 2020 年，计算机病毒犹如 COVID-19 一样，开始在该企业试点工厂肆虐传播，对工厂一线生产造成了很大的困扰。问题初始，BP&IT 开始组织资源进行病毒处置工作，一方面要对病毒进行删除，对文件进行修复，另一方面还需要对操作系统进行保护，避免影响到重要的生产活动。然而事与愿违，BP&IT 同事在做了充分的准备情况之下，还是出现了因为病毒处置导致的操作系统蓝屏事件，而且多次出现，这就意味着面向工业控制主机的病毒处置任务失败。

“后来我们了解到，工业主机这类场景应该采用白名单的防护思路，于是我们进行了多家安全厂商的相关产品测试工作，最后奇安信的产品解决了我们的问题。”BP&IT 相关专家这样表示。

于是，该机械制造企业在选定的试点工厂，开始进行评估工作、病毒处置工作及规划建设工作。

建设内容主要包括：集团构建以工业安全管理与分析系统为中心的整体工控安全体系，形成以长沙为管控总部的工控安全运营中心；在总部与各分子公司的工厂汇聚交换机和接入工业防火墙和工业安全监测系统进行管理，同时对核心工业主机安装主机防护。工业安全管理与分析系统采集工业安全设备日志，进行安全状态的分析，同时对安全设备进行性能监测和设备基本管理。

为了实现良好的使用效果，奇安信工程师多次到现场交流，了解现场情况和问题，并特别提供了工业安全运营人员，协助现场运维工程师进行资产梳理和安全配置，并对运维工程师进行安全培训和赋能，使运维工程师能够完成工控安全的日常运营，处置安全事件。

在整体建设原则方面，以安全分区、主动防御、异常监测和集中管控为核心。

“安全分区”：根据评估结果和现有网络情况进行梳理，将办公网与工控网络分离开来，进行安全分区，工控网络内部再根据不同工序进行安全域划分，形成更为细致合理的安全区域。根据划分的安全区、安全域制定区间、域间防护措施，部署安全防护设备实现区域之间的安全隔离。

“主动防御”：结合安全区、安全域划分结果，在各安全区、安全域之间部署适当的安全防护设备，如工业安全网关，形成从办公网生产网的纵向安全隔离防护，同时形成生产网各车间网络之间的横向隔离防护，以及各网络内部安全区域之间的安全隔离防护，主动阻断来自网络上的病毒传播以及恶意入侵，并在安全区、安全域内各工业主机（包括上位机和服务器）上部署应用程序白名单安全防护软件，实现对异常行为、恶意代码的检测和防护，主动阻断已知未知病毒及恶意软件的感染入侵，多种技术手段结合形成从外到内、从点到面的主动防御体系。

“异常监测”：针对各安全区、安全域内工业控制设备的运行情况及数据交互、网络流量，持续进行网络流量采集和分析，实时掌握工控设备运行情况，以便出现问题时及时预警。

“集中监控”：针对各安全区、安全域的网络流量、工业设备运行情况、安全设备运行情况、工控设备资产分布情况建立数据采集机制，统一监测各网

络区域的工业控制系统的运营日志并进行综合分析，通过对包括全网流量、设备运行状态、数据交互、终端运行安全状态等海量数据的关联分析，发现生产网络存在的安全风险并及时告警，并给出详细的统计报表和攻击路径溯源，形成企业内部 的工业安全监控中心，将生产网络安全运行情况进行集中展示，提供资产威胁视图、安全告警视图、资产安全监控视图、资产统计视图等直观数据统计界面，协助用户全面掌握工业控制系统的安全态势并及时做出应对。

三现四表互联防护，全数转型管理提效

2016 年开始，该机械制造企业与树根互联共同打造工业互联网平台，实现从研发到后市场服务的全价值链数字化转型。依托树根互联“数字化转型新基座”，该机械制造企业完成了 5.5 万个“三现四表互联”。其中，“三现”是指现场、现实、现物，“四表”是指水、电、气、油表，而“互联”则是围绕以上 3 个现场，将“四表”的交流管理搬到树根互联的根云平台。

据介绍，现阶段安全防护实现了对全网的“三现四表”设备的状态监测与入侵攻击检查，有效避免来自信息网络的安全隐患对生产控制网络的威胁。通过两网之间的隔离措施，实现生产网内各业务系统之间的横向逻辑隔离和安全防护，阻止来自区域之间的越权访问，入侵攻击和非法访问；实现了对上位机、工程师站、各系统服务器系统的安全加固，通过白名单机制构建安全基线，防止病毒木马、恶意软件对系统的破坏；实现了对生产网络及生产设备的监测审计，及时发现网络或系统中是否存在违反安全策略的行为和被攻击的迹象；实现了对所有工控安全防护设备及系统的统一管理，降低运维管理成本；实现了对生产网络、生产设备、安全防护设备情况的综合运营管理，协助用户全面掌握工业控制系统的安全态势并及时做出应对。

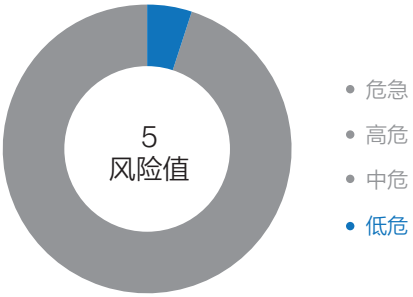
在集团数字化转型取得初步成功的基础上，该机械制造企业与奇安信一起，对数字化转型的工厂做了持续的检测与梳理。

其中在工业资产层面，按组织和生产工艺，划分为冲压车间、焊装车间、涂装车间、总装车间、动力总成和质检 VQ，并分网段进行管理。利用工业安全管理与分析系统将工业主机防护系统、工业安全监测审计系统，以及工业防火墙产品，作为资产识别数据源，并配置资产运营优先策略，经过人工审核和确认，形成一套资产台账，为后期运营打下良好基础。

在风险控制层面，运营过程中持续关注全网风险指数，根据平台量化的风险值，为了将风险控制在一定范围内，运营人员会及时对危害程度高的告警进行处置。目前经过近 1 年的安全运营，基本上不会出现中危和高危告警。

在管理方面，基于完整的资产台账列表，绑定资产风险与使用责任人，将风险处理方式与流程化工单进行结合，周期性对各分子公司信息安全负责人的风险事件处置率、处置量及风险发生的数量进行考核，极大的提升了管理效能。

通过以上一系列措施，该机械制造企业在推动全面数字化转型管理提效的同时，更夯实了网络安全基石，为未来持续发展提供了坚实底座。



风险值大大降低

十年矢志不渝，安全与数字化实现同步跃级

路虽远，行则将至。该机械制造企业作为一家国内领先的工程机械企业，从 2013 年就痛定思痛，探索数字化转型之路，积十年之功，咬定青山不放松，终于吃到了数字化的甜头，并以安全为基，点亮了一座座灯塔工厂。安

入选理由

数字化与智能化转型是制造企业产业升级的必经之路。只有坚定不移走安全与业务转型双同步路线，才能在新时代竞争激烈的数字化道路上越走越远，成为最终赢家。该大型机械制造企业结合生产环境、业务发展需求和安全风险，构建起整体工控安全体系，为数字化转型夯实基石。

创新应用 6

全国海关：夯实国产化替代工作，打造海关业务统一承载平台

作者 | 蔡佩宸

近年来，国产化替代一直是数字中国建设的热门话题。在 2023 年中共中央、国务院印发的《数字中国建设整体布局规划》，明确提出“强化数字中国关键能力”“构筑自立自强的数字技术创新体系”。国产化替代作为我国推动科技自立自强的重要举措，不仅为数字经济高质量发展打牢了安全基石，还解决了“卡脖子”问题，是数字中国建设的重要保障，目前已经在党政、金融、能源、通信等“2+8+N”行业全面展开。

中华人民共和国海关总署是国务院直属机构，正部级单位，负责全国海关工作，垂直管理全国海关。海关信息化发展多年以来，业务系统包括通关、征税、缉私、保税、物流、检验检疫、监管等近百余个，供全国海关系统十余万用户使用。

根据海关信息化建设规划，海关总署进行了应用系统及用户终端的替代改造。由于系统数多、用户体量大，在一定时间内存在 x86 终端环境、国产终端（国产 CPU+ 国产操作系统，以下统称国产终端）环境与新旧业务系统并行的情况。

根据全国海关系统实际情况，既要保障国产终端替代工作稳步推进应替尽替，能替尽替，也需要保障在替代过程中原有 x86 终端正常访问新替代系统，以及国产终端对原有系统的正常访问，保障替代工作与正常办公开展顺利进行。实现全国海关统一业务安全入口，保障全国海关业务安全访问。

国产化改造，终端、业务系统同步进行

随着海关信息化工作的持续深入，奇安信可信浏览器已适配海关新业务系统，同时海关总署已启动对全国海关办公终端替换工作，为了保障改造过程中

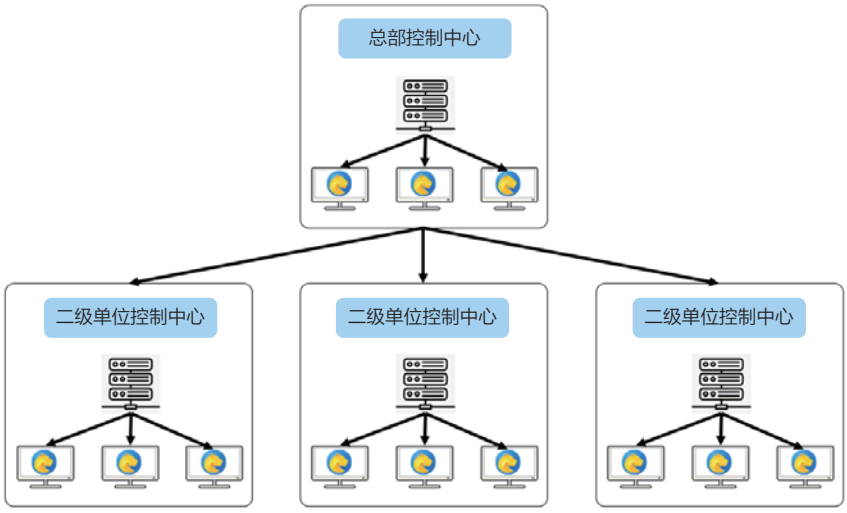
新旧业务系统正常使用，奇安信可信浏览器提供远程浏览解决方案，在无需改造老旧业务应用系统且用户无感的情况下，通过远程虚拟化的方式，依照管控中心配置和调用规则，实现用户在国产化终端访问原基于 IE 内核开发的业务系统，并解决未完成迁移的业务系统、插件和外设无法使用、客户终端替换后无法正常办公的问题。

加强终端级联管理，保障业务访问的一致性

根据海关总署统一规划、统一部署的施行策略，海关各类型系统后续将通过统一的服务工作登录入口进行业务访问。总署对 x86 终端、国产化终端实行同台管理模式，运维管理人员利用管控平台对员工访问业务系统时使用的不同内核做设定，满足不同业务系统的访问需求，实现总署对全国海关终端浏览器的统一管控，但是随着国产化终端数量的逐渐增多，衍生出各直属海关及地方隶属海关单位的个性化需求，在实现分级管理，赋予区域海关相关权限的基础上，由总署进行统一管控和同台管理，既满足区域海关的个性化需求，又积极落实总署统一调控策略。

应用数据分析，促进业务系统的深化完善

针对海关应用系统国产化替代的有效性和可用性，保障真替真用。奇安信可信浏览器数据分析软件，支持对产生的访问数据进行多层面的访问数据汇集分析和可视化管理，在浏览器客户端发起业务系统访问的同时，对访问质量进行实时检测与分析，将应用访问异常、应用性能、全链路性能等关键治标进行可视化管理，助力运维部门理清当前网内业务系统数量、访问热度及访问的质量，清晰的掌握多地域、多业务系统之间访问服务质量，助力运维人员进行业务系统成熟度和稳定性评估，进一步促进业务系统的深化完善。



本次项目奇安信可信浏览器覆盖了海关总署及 40 多个直属单位，部署包含终端总数超过 18 万点，保障原有 x86 终端及国产化终端安全访问的基础上，既能完成对基于 IE 设计的系统做平滑过渡，又能贯彻落实关基国产化政策，明确工作主体目标和替代路线，不断完善综合办公系统（OA、党群、门户等）的替代工作。所有这些工作，充分体现了奇安信可信浏览器作为办公基础软件，可以深入业务场景，持续为客户提供包括业务系统承载平台、统一安全管控、浏览器双内核及业务质量分析等丰富的产品价值。安

入选理由

在数字化办公中，企业浏览器除了作为统一业务承载平台，在安全方面越来越受到客户重视，逐渐成为业务访问安全的“第一道防线”。本次项目的实践，充分体现了奇安信可信浏览器作为办公基础软件，可以深入业务场景，持续为客户提供包括业务系统承载平台、统一安全管控等丰富的产品价值。

微软数据安全指数报告：自动化和 AI 是提升保护能力的可行途径

作者｜微软 &Hypothesis Group

近日，微软和 Hypothesis Group 发布的《数据安全指数：趋势、见解和数据安全战略》报告显示，随着数字化的发展，网络安全漏洞也在不断增加，网络威胁、数据泄露和内部风险变得越来越常见，也给我们的企业带来了很大的风险。

结论一：决策者认为他们受到了保护，但事实并非如此

从表面上看，决策者对其数据安全解决方案展现出高度的信心和满意度。大多数单位、组织认为其数据安全控制措施在防止数据泄露方面是有效的，“他们知道自己的大部分数据放在哪里，并且可以检测与数据相关的大多数风险”。

但事实上，政企单位（单位组织）却持续遭遇大量的数据安全事件，在过去 的 12 个月中，平均每家公司经历了 59 起数据安全事件，其中 20% 被视为严重事件，可能带来高达 1500 万美元的年度成本。

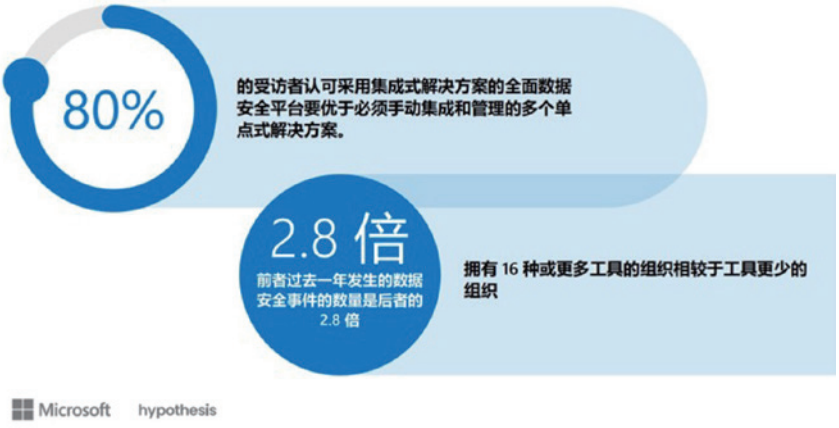
除了这些成本，40% 的决策者还表示，为了从数据安全事件中恢复过来，以及挽回因声誉受损而造成的业务损失，需要花费的运营成本也是很高的。高达 92% 的受访者表示面临挑战，主要是在成本、集成和实施时间等方面。

结论二：拥有更多工具并不意味着能够提高数据安全性或效率，情况恰恰相反

虽然大多数人认为一体化的解决方案更好，但数据安全工具的使用仍然很分散。企业通常使用大约 10 种不同的数据安全工具来降低数据安全风险，而在员工人数超过 5000 人的公司中，这个数字还会更多。

拥有更多的数据安全工具并不总是意味着更高的安全性。事实上，情况可能恰恰相反。一项调查显示，那些拥有 16 种或更多数据安全工具的单位组织，在过去一年中经历的数据事件数量平均达到了 133 起。相比之下，使用较少工具的单位组织平均仅发生了 48 起数据事件，这意味着前者的事件数量是后者的 2.8 倍。

为何会出现这种情况？报告分析指出，首先，各种各样的数据安全工具可能会导致一些盲区，使得某些问



题无法被发现，同时也会产生大量的“影子数据”。其次，每种工具都需要专门的人员来进行安装、维护和操作，这会增加工作的复杂性和成本。最后，使用更多的工具也意味着需要花费更多的精力，来整合这些工具提供的信息，制定补救计划，而且在信息传递的过程中可能会有遗漏。

结论三：来自内外部数据（尤其是业务数据）安全事件的压力持续给单位组织带来困扰

尽管数据安全事件的来源可能多种多样，但恶意软件或勒索软件等外部威胁无疑是最常见的。在接受调查的企业中，有一半的企业表示他们在过去的一年里至少经历过一次这样的攻击。此外，还有 41% 的企业表示，他们对未来一年如何防范恶意软件或勒索软件的攻击并没有做好准备。

防止内部风险也是决策者的重要工作。35% 的受访者表示，他们需要更好地保护自己的公司和账户不受内部恶意人员的侵害，还有三分之一的人担心无意中造成的内部问题。虽然恶意内部事件不是数据安全的主要问题，但却是决策者觉得最没有准备好应对的问题之一。

展望未来，有 77% 的企业认为他们的业务数据（如知识产权和源代码）是最容易受到攻击的。这些数据在建立竞争优势和经济收益方面起着关键的作用。然而，识别和分类这些数据是具有挑战性的，因此企业需要更先进的技术来帮助他们发现和保护这些容易受到攻击的敏感数据。

结论四：单位组织需要云和 AI 来推动数字化转型，但它们也是最容易受到攻击的数据位置

云服务和 AI 技术对现在的公司来说非常重要。一般来说，每个公司都在使用大约 147 种云服务，有超过一半的公司已经有了人工智能的发展计划，其中大约三分之一已经开始实施。但是，因为这些技术在发展，所以我们很难搞清楚数据在哪里，这就带来了很多不确定性和风险。

在过去的一年里，有 42% 的企业报告了他们在云存储中遇到了安全问题，而有 31% 的企业报告了他们在使用电子邮件、即时消息或在线会议工具时遇到了安全问题。在这些工具的使用频率和协作程度较高的地方，这些问题似乎更为常见。

与其他领域相比，AI 被认为是最有可能发生数据安全问题的领域，有 27% 的企业在这个领域遇到了安全问题。尽管人们对 AI 有所担忧，但决策者还是看到了它的潜力，尤其是在市场上的供应商正在开发创新的方法来帮助企业通过负责任地使用 AI 提高能力的情况下。

结论五：自动化和 AI 是提升保护能力的可行途径

由于资源和人力的限制，以及工作分配可能不太合理，企业正在寻找技术来帮助他们有更多的时间进行主动性的活动。自动化是一个很好的选择，它可以帮助企业腾出时间来采取更主动的数据安全策略。

74% 的企业希望能够实现半自动化或全自动化的风险缓解机制，这样安全团队就可以在潜在的数据安全事件发生之前，将其影响降到最低，而不需要手动进行审核。通过自动化这些任务，企业可以减轻数据安全团队的负担，让他们能够采取更主动的策略。

将 AI 应用于数据安全也可以帮助企业提高战略意识，更智能地应对未来的威胁。这项技术可以加快对检测到的事件的响应速度，从而为数据安全专业人员赢得更多的时间进行调查。通过利用 AI 和自动化的优势，并转向更加集成的解决方案，企业可以采取更主动的数据安全策略，为打造一个更安全的未来做好准备。

最终结论

1、采用集成式平台，加强数据安全状况

一个集成的数据安全平台应该能够让安全团队，无缝地完成所有这些关键任务：首先是在数字环境中发现和保护敏感数据；其次是检测与此数据相关的重大风险；第三是防止未经授权使用敏感数据，同时不影响合法的业务活动。通过实施综合的数据安全战略，单位、组织可以实现更高级别的保护，同时简化其安全基础设施。

2、采用深度防御方法，由外而内和由内而外防范数据安全事件

单位、组织可以采取深度防御的策略来保护他们的数据，就像博物馆保护珍贵的艺术品一样。例如，博物馆会使用带有威胁智能防御功能的先进监控摄像头来监控访客，票务系统来管理身份和进入博物馆的权限，以及严格的安全措施来保护艺术品。这与保护企业宝贵数据的数据安全控制措施非常相似。无论是来自外部的恶意行为者，还是已经在企业环境中的个人，这些措施都可以阻止潜在的事件发生。

3、利用 AI 和自动化技术升级你的数据安全战略

自动化和 AI 可以帮助组织在数据安全方面变得更加积极主动。比如，利用 AI 帮助识别敏感数据和应用保护策略，包括加密和权限管理。利用 AI 的强大功能来确定与敏感数据相关的重大风险，并战略性地分配资源，以处理潜在的高风险事件。使用 AI 和自动化技术，根据评估的风险自动量身定制防护和缓解控制措施，从而实施适应性更强、更具前瞻性的数据安全战略。安

组织更主动与更被动的结果对比	更主动	更被动
过去 12 个月的数据安全事件的平均成本影响	20.7 万美元	33 万美元
在平均不到一个月的时间内完成一项数据安全调查	80%	68%
相信防御控制措施足以防止数据泄露	77%	68%

大事记

齐向东委员出席政协北京市第十四届委员会第二次会议

1月20日，政协北京市第十四届委员会第二次会议开幕，政协委员齐向东立足自身工作经验，聚焦数字技术创新企业发展和智慧城市建设，带来了两份提案。

在《关于推动数字技术创新企业“走出去”，增强国际竞争力的建议》中，他提出，建议像支持中国产品“走出去”一样，支持中国数字技术创新企业“走出去”。针对数字技术创新企业出海精准施策，给予必要的财税优惠、金融支持和系统服务，进一步加快“走出去”步伐，加快建成北京全球科技创新中心，加快实现高水平科技自立自强。

在《关于进一步强化智慧城市网络安全韧性》的提案中，他提出，在实战攻防演练中发现，我国智慧城市的网络安全防线依然十分脆弱，建议北京在补足安全短板，增强安全韧性上下功夫，打造宜居、韧性、智慧城市，提升超大城市治理现代化水平。

控制超百万台设备 奇安信 X 实验室曝光潜伏 8 年黑产团伙

奇安信 X 实验室日前在技术博客上揭露了一个潜伏 8 年的黑产团伙 Bigpanzi，该团伙利用免费或廉价的视频 APP 或固件刷机，控制了全球超过百万台机顶盒，形成了一个庞大的僵尸网络，用于发动 DDoS 攻击，代理流量，提供盗版内容等。该团伙还可远程控制机顶盒播放任何不受法律约束的声音和图像，危害社会稳定。X 实验室与 Bigpanzi 的攻防战正在进行中。X 实验室表示，他们将不惜一切代价，与 Bigpanzi 进行斗争，保护网络安全，维护社会公益。

电力信息化专委会专题研讨会在奇安信举行

1 月 13 日，由中国电机工程学会电力信息化专业委员会网络与信息安全学组、发电学组与奇安信集团联合举办的“走进冬奥保障中心 共话网络安全攻防”专题研讨会在奇安信安全中心举行。50 余位电力信息化专委会专家及学组成员参与活动。

电力信息化专委会副秘书长兼发电学组组长董杰对奇安信的精彩分享和展示表示了感谢，并表示希望成员单位能够通过当天的内容分享，思考总结适合电力行业现状的安全规划与建设思路，实现行业安全建设的有效提升。

2024 年全国首批电子数据取证分析师认证在奇安信安全中心完成

2024 年全国首批电子数据取证分析师（四级 – 中级工）职业技能等级认定考试于 2024 年 1 月 6 日至 7 日在奇安信安全中心多功能厅完成，有 161 名考生通过考试认证。

奇安信根据北京市职业技能鉴定管理中心京职技鉴发〔

2023] 13 号要求，备案时，按照国家标准执行的从 2024 年 1 月 1 日起需按照新版申报条件对企业职工报考资质进行审核，并从考务流程、题库设置、人员分配、质量管理、考核监督等优化运营流程，并做好事后督导准备，圆满完成第二期电子数据取证分析师认证考核工作。

奇安信集团与 FESCO 签署战略合作协议

1 月 5 日，奇安信集团与北京国际人力资本集团股份有限公司（简称“北京人力”）下属北京外企人力资源服务有限公司（简称“FESCO”）签署了战略合作协议。双方将立足数字化、智能化服务与人力资源服务，开展业务创新合作，打造双赢和可持续发展的新型战略合作伙伴关系。

FESCO 与奇安信已有多年的合作基础，此次战略合作将聚焦人力资源服务、软件与数字技术服务、数字化运营服务、教育培训、出海服务、智能企服等业务，充分发挥双方在各自领域的行业生态、技术服务等方面优势，共同拓展数字化、智能化服务与人力资源服务的新模式，携手面向企业客户提供数字化创新服务。

黑龙江省教育厅与奇安信达成战略合作

1 月 4 日，黑龙江省教育数字化工作推进会议在哈尔滨召开。会上，黑龙江省教育厅与奇安信签署战略合作协议，双方通过共同设立“龙江高校网络安全培训虎符基地”、打造“龙江网安学科孵化联盟”、开展网络安全检查及攻防演练等多项合作内容，助力黑龙江教育数字化战略行动顺利实施。

此次合作是黑龙江省教育厅打造“一云四网”龙江教育数字化转型创新发展体系的重要举措之一。黑龙江省教育数字化战略三年攻坚行动中明确了“扎实筑牢教育‘安网’”的工作任务，与奇安信的深入合作将加快推进“扎实筑牢教育‘安网’”的工作落地。

奇安信入选智慧军工联盟 2023 年网信领域重点支撑单位

近日，中关村科创智慧军工产业技术创新战略联盟（简

称“智慧军工联盟”，英文缩写“ZASDI”）在京组织了2023 网信领域重点支撑单位入库评审会。经专家组严格评审，奇安信成功入选 2023 年网信领域重点支撑单位。

据悉，“2023 年网信领域重点支撑单位”是智慧军工联盟通过有关党政部门、军工集团公司、行业协会、产业联盟等多个渠道，开展的各类网信领域重点企业信息征集工作。本次评审会由核、航天、航空、船舶、兵器等领域及有关工业部门专家组成评审，从单位基本情况、核心技术能力、产品应用情况、自主安全水平等方面，对企业及产品进行遴选评审。

奇安信集团中原区域总部在郑州揭牌

12 月 26 日，奇安信集团中原区域总部、奇安信（郑州）安全技术有限公司、工业控制系统安全国家和地方联合工控实验室郑州分中心，在河南郑州正式揭牌。

据悉，奇安信集团目前已在河南省建成了中部大数据中心，组建了上百人的专业团队。未来，随着区域总部“1+2+3+N”的战略布局落地及战略地位的提升，将发展成为省内技术人员数量最多、配置最全、能力最强的网络安全服务商之一。

嵩山实验室与奇安信共建网络安全联合研究中心

12 月 26 日，奇安信集团与嵩山实验室在郑州签署战略合作协议，将共建“嵩山 – 奇安信网络安全联合研究中心”，研究中心将围绕网络安全前沿技术、重大专题项目、推动标准制定等多个领域，联合开展核心关键技术攻关，携手推动更多科研成果转化为新质生产力。

奇安信集团与福建联通签署网信安全共链合作协议

12 月 25 日，2023 年福建联通生态合作伙伴大会在福州举行。会上，奇安信集团与福建联通签署了“网信安全共链合作”协议，围绕此项计划，奇安信将与福建联通一起，在网信安全领域开展全方位、深层次合作，为数字福建发展建设筑牢网络安全底座。福建联通还为奇安信颁发了“年度特别贡献奖”和“年度网信安全共链合作奖”两项荣誉。

上海市公安局金山分局与奇安信共建打击治理新型网络犯罪联合实验室

12 月 22 日，上海市公安局金山分局与奇安信科技集团股份有限公司签署战略合作协议，共建打击治理新型网络犯罪联合实验室，并通过深度警企合作，汇聚专业技术资源，建立多场景下的涉网犯罪打击治理模型，助力打击治理各类新型网络犯罪活动。签署协议期间，金山公安分局与奇安信举行了打击治理新型网络犯罪联合实验室的揭牌仪式。

通过警企共建打击治理新型网络犯罪联合实验室，双方对打击治理新型网络犯罪的重要性有了全新的认识，奇安信作为一家专业从事网络安全技术研发和服务的国家队企业，将不断强化警企合作，形成工作合力，共同维护网络安全，为构建安全、和谐、美好的网络空间贡献企业力量。

齐向东：做好“四管四防”护航金融安全

12 月 22 日，2023 北京国际金融安全论坛在北京金融安全产业园成功举办。齐向东发表了《做好“四管四防” 护航金融安全》的主题演讲。他在演讲中表示，金融行业站在数字化、智能化转型的最前沿，安全风险与日俱增。要通过“管好资产、管好行为、管好技术、管好运营”这 4 个管好，来实现“防亏损、防泄露、防瘫痪、防丢钱”的目标，高效化解安全困境，最终实现行业高质量发展。

会上，奇安信集团与房山区人民政府正式签约，入驻北京金融安全产业园。未来奇安信将在房山区设立电子取证业务运营中心，建设金融网络与数据安全产教融合创新人才培养基

地，成立网络安全保险相关实验室并引入网络安全险业务，并统筹建设房山区网络安全运营中心，为智慧房山建设助力。

荣誉墙

奇安信获中国计算机行业协会数据安全专业委员会数据安全研究优秀贡献奖

1月17日，中国计算机行业协会数据安全专业委员会（以下简称“数专委”）在北京召开了年度工作总结会。会上，数专委总结了2023年年度工作，展示本年度所取得的成绩及2024年年度工作计划，表彰优秀支撑单位。奇安信集团获评“数据安全研究优秀贡献奖”。

软件供应链安全应用实践入选信通院优秀治理实践成果

近日，信息通信软件供应链安全社区公布2023软件供应链优秀成果案例名单。奇安信集团的“云原生场景下的软件供应链安全应用实践”入选“优秀治理实践成果”。

基于奇安信云原生应用保护平台CNAPP，该方案实现了从开发阶段到运行时的全生命周期防护，以应用为中心，贯穿一体系（DevOps）、两方向（安全左移与安全右移）、三环节（构建、部署、运行），将安全融于DevOps流程，提供云原生应用全生命周期的风险管理与卡点管控能力。


三、优秀治理实践成果

成果名称	获奖单位
云原生场景下的软件供应链安全应用实践	奇安信科技集团股份有限公司

取证技术新突破 奇安信再获公安部科学技术奖一等奖

近日，公安部公布了一批2023年科技信息化获奖成果，

奇安信集团参与申报的某电子数据取证技术研究及应用项目，获评 2023 年公安部科学技术奖一等奖。这也是奇安信继 2022 年凭借“关键信息基础设施安全保护关键技术与应用”获得公安部科学技术奖一等奖后，再次获此殊荣。

奇安信携手国家管网集团入选工信部 2023 年数据安全典型案例

近日，工业和信息化部网络安全管理局公布了 2023 年工业和信息化领域数据安全典型案例名单。奇安信集团携手国家石油天然气管网集团有限公司和北京移动打造的数字管网数据安全与共享流通一体化方案设计与验证案例，成功入选数据安全体系整体设计实施方向的典型案例。

据悉，本次 2023 年工业和信息化领域数据安全典型案例遴选工作，根据 2023 年“十六部门关于促进数据安全产业发展的指导意见”的要求，首次以“数据安全”为专题方向组织的部委级试点示范，面向工业领域、电信和互联网领域组织开展数据安全典型案例遴选。

2023 年工业和信息化领域数据安全典型案例名单

一、工业领域典型案例（共 34 项）

序号	申报方向	申报类型	案例名称	申报主体	联合申报单位	推荐单位
18		数据安全监测预警类	数字化管销系统 CDP 数据保护案例	重庆长安汽车股份有限公司	/	重庆市经信委
19		数据溯源类	国网安徽电力-国网安徽电力调度移动终端屏幕数据安全溯源解决方案典型案例	国网安徽省电力有限公司	安徽明生恒卓科技有限公司；合肥高维数据技术有限公司	安徽省经信厅
20		整体设计实施类	国家石油天然气管网集团有限公司-数字管网数据安全与共享流通一体化方案设计与验证典型案例	国家石油天然气管网集团有限公司科学技术研究总院分公司	奇安信科技集团股份有限公司；中国移动通信集团北京分公司	国家石油天然气管网集团有限公司
21	数据安全体系整体设计实施方向	整体设计实施类	大冶特殊钢有限公司——特钢企业数据安全体系构建	大冶特殊钢有限公司	/	湖北省经信厅
22		整体设计实施类	华晨宝马汽车有限公司-数据安全整体设计实施典型案例	华晨宝马汽车有限公司	/	辽宁省工信厅
23		整体设计实施类	全天安全基础，护航数字转型——中国商飞公司数据安全治理实践案例	上海航空工业（集团）有限公司	/	中国商用飞机有限责任公司

奇安信集团获 CCIA 2023 年度先进会员单位、技术支撑单位两项荣誉

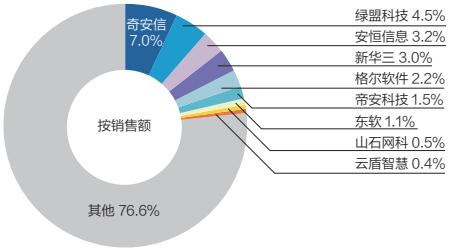
1 月 4 日，2023 年度中国网络安全产业联盟会员大会（CCIA）暨理事会在京举行。会上举行了“中国网络安全产业联盟技术支持单位”授牌仪式，并对会员单位进行表彰。奇安信集团获评“2023 年度先进会员单位”“中国网络安全产业联盟技术支持单位”两项荣誉。

五连冠！奇安信位列赛迪云安全报告榜首

近日，赛迪顾问发布《2022~2023 年中国云安全市场研究年度报告》（以下简称“《报告》”），《报告》指出，2022 年中国云安全市场整体规模达到 176.9 亿元，同比增长 46.7%，奇安信作为云安全、云原生安全的领导者，凭借深厚的技术积累，以及业界最完整的云及云原生安全体系，以 7.0% 的市场份额位居报告首位，连续 5 年夺冠，继续领

跑云安全市场。

2022 年中国云计算安全市场品牌结构



数据来源：赛迪顾问，2023.02

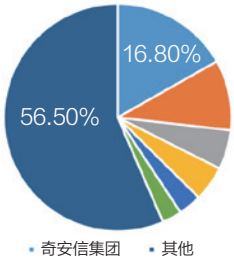
奇安信集团获数据安全共同体计划年度杰出贡献单位

12 月 22 日，由中国信息通信研究院安全研究所主办，大数据应用与安全创新实验室承办的“数据安全共同体计划成员大会（2023）”在京举办，会上公布了 2023 年数据安全“星熠”案例入选名单。奇安信集团申报的“奇安天盾数据安全保护系统”获评“数据安全技术与产品应用优秀案例”，同时，奇安信集团连续两年获评数据安全共同体计划“年度杰出贡献单位”。

奇安信夺得国内 EDR 市场头名

近日，赛迪顾问发布《中国终端安全检测与响应产品市场研究报告》（以下简称“《报告》”），奇安信以 16.8% 的市场份额，位居 2022 年中国终端安全检测与响应市场第一，超过第二、三名市场份额总和。

2022 年中国终端安全检测与响应产品市场份额



数据来源：赛迪顾问，2023.12

目前，奇安信帮助政府、运营商、金融等行业超过 5000 万终端，构建了多种混合场景下，针对终端威胁的检测、响应和鉴定的高级威胁对抗能力。对此赛迪顾问在《报告》中评价，未来奇安信集团还将依托自身对终端及应用、业务及环境、威胁及防御效果及效率的深入理解，以及超大规模项目的最佳实践经验，推出形式更为灵活、类型更为丰富、场景更为多元的终端安全解决方案，持续有效的帮助政企客户解决现在以及未来可能面临的各种终端安全问题。

2023 北京企业百强榜单出炉 奇安信集团连续两年登榜

近日，由北京市人民政府、天津市人民政府、河北省人民政府、中国国际贸易促进委员会共同主办的 2023 年京津冀产业链供应链大会在北京举行。北京企业联合会、北京市企业家协会在会上发布了 2023 北京企业百强榜及其发展报告。凭借扎实的科技创新能力和领先的企业综合实力，奇安信集团连续两年入选“北京企业百强”“北京高精尖企业百强”“北京数字经济企业百强”三大榜单。

车云一体！奇安信获评车联网安全代表厂商

近日，安全牛发布了《车联网安全技术应用研究报告》（以下简称“《报告》”）。凭借车 – 云一体化持续风险监测方案，奇安信成功入选该报告并被评为车联网安全代表厂商。

《报告》强调，随着车企数字化转型和车辆网联化发展的不断深入，围绕智能网联汽车生产、运营、维护、通信的各个环节都引入了不同程度的网络安全问题。从底层芯片到虚拟化、操作系统、中间件、上层应用、车端内通信，每一个层级出现安全问题都会对汽车产生很大安全影响。奇安信秉承内生安全的理念，从产品、测试服务等方面为智能网联汽车提供了对应的安全解决方案。

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

《安全事件报告》新规解读：事后问责制升级为国家接管风险管理

作者 | 汪列军

12 月 8 日，国家互联网信息办公室发布了关于《网络安全事件报告管理办法（征求意见稿）》（以下简称《办法》），其中提到，运营者在发生网络安全事件时，应当及时启动应急预案进行处置。按照《网络安全事件分级指南》，属于较大、重大或特别重大网络安全事件的，应当于 1 小时内进行报告。

《办法》提倡并鼓励有关单位及时、完整、准确地报告网络安全事件，对于迟报、漏报、谎报或者瞒报网络安全事件，造成重大危害后果的，应按照相关法律进行处罚，这对于网络安全事件发生后的报告工作具有重要意义，在很大程度上能够减少网络安全事件造成的实际危害。

具体而言，有以下四方面影响需要重点关注。

第一是界定了事件范围，并要求主动报告。

这里的网络安全事件并非狭义上所指的由网络攻击或者其他蓄意破坏所造成的安全事件，而是广义上所有对系统和网络安全造成影响的事件。《办法》第十二条规定，本办法所指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其中的数据造成危害，对社会造成负面影响的事件。

《办法》第十一条规定，发生网络安全事件时，运营者已采取合理必要的防护措施，按照本办法规定主动报告，同时按照预案有关程序进行处置、尽最大努力降低事件影响，可视情免除或从轻追究运营者及有关责任人的责任。

因运营者迟报、漏报、谎报或者瞒报网络安全事件，造成重大危害后果的，对运营者及有关责任人依法从重处罚。

第二是明确了报告对象，确立网信部门的监管作用。

《办法》第三条规定，国家网信部门负责统筹协调国家网络安全事件报告工作和相关监督管理工作。地方网信部

门负责统筹协调本行政区域内网络安全事件报告工作和相关监督管理工作。具体如下：

网络和系统归属中央和国家机关各部门及其管理的企事业单位的，运营者应当向本部门网信工作机构报告；网络和系统为关键信息基础设施的，运营者应当向保护工作部门、公安机关报告；其他网络和系统运营者应当向属地网信部门报告；有行业主管监管部门的，运营者还应当按照行业主管监管部门要求报告；发现涉嫌犯罪的，运营者应当同时向公安机关报告。

第三是强调了“1 小时”制度，安全事件应尽快上报。

显而易见的是，网络安全事件拖延时间越长，其危害性往往越大，后续的故障恢复及消除影响等工作也更加困难。因此对于网络安全事件报告的时效性要求非常高。

《 办法 》规定，运营者在发生网络安全事件时，应当及时启动应急预案进行处置。按照《 网络安全事件分级指南 》，属于较大、重大或特别重大网络安全事件的，应当于 1 小时内进行报告。

此外，《 办法 》还专门针对重大、特别重大网络安全事件做出了特别规定。《 办法 》第四条指出，属于重大、特别重大网络安全事件的，有关单位在收到报告后，应当于 1 小时内向上级部门报告。

第四是细化了报告内容，事件调查应全面、细致。

为准确评估网络安全事件造成的影响，为全面统筹后续的响应处置、溯源分析及故障恢复提供有力支撑，报告内容至关重要。《 办法 》第五条明确规定，运营者应当按照《 网络安全事件信息报告表 》报告事件，至少包括事发单位名称及发生事件的设施、系统、平台的基本情况；事件发现或发生时间、地点、事件类型、已造成的影响和危害；初步分析事件原因；下一步所需的线索及进一步采取的应对措施等。

值得一提的是，美国近 2 年也在制定相关法律法规。早在 2022 年 3 月，美国总统签署了《 2022 年关键基础设施网络事件报告法案 》(CIRCIA) ，要求网络安全和基础设施安全局 (CISA) 制定和实施法规，对关键基础设施部门发生的网络安全事件和勒索事件提出了明确的报告时间要求，其中网络安全事件要求在 72 小时内报告，涉及支付赎金的勒索事件在 24 小时内报告。根据法案要求，CISA 须在 24 个月内 (即 2024 年 3 月之前) 发布具体规则。

今年 2023 年 7 月，美国证券交易会员会 (SEC) 通过了网络安全事件披露规则，要求上市公司确定网络安全事件重大后 4 个工作日内提交。如果美国司法部长确定立即披露将对国家安全或公共安全构成重大风险，并以书面形式通知委员会该决定，则可以延迟披露。而就在今年 11 月初，ICBCFS 发生勒索攻击后，找美国安全服务厂商 MoxFive 进行帮助，并立即向执法部门进行了报告。

想要全面掌握上述网络安全事件相关细节、正确做出下一步处置行动并非易事。尤其是在某些高水平网络攻击中，攻击者通常会采用技术手段，隐藏甚至擦除入侵的路径、恶意样本、行为日志等，为事件调查带来非常大的挑战，要求运营单位必须具备准确的安全检测能力、全面的数据搜集能力、强大的关联分析能力。

前不久，奇安信发布的新版态势感知与安全运营平台 (NGSOC) ，可将相关联告警自动汇聚形成完整事件卷宗，自动补充上下文证据，自动映射 MITRE ATT&CK 攻击者战术和技术，自动解读攻击者意图、自动识别关键攻击痕迹、自动评估影响面并计算处置对象，1 分钟内即可完成事件定性、5 分钟完成影响面评估。

与此同时，奇安信威胁情报中心还拥有千万级终端的遥测数据、十亿级互联网资产及应用数据、万亿级历史 Passive DNS 数据及全量漏洞情报库，可进一步补充网络安全事件中有关的上下文信息，确保运营单位能在 1 小时内完成安全事件报告，并对运营单位下一步处置动作提供关键的技术支撑。 安

关于作者

汪列军

奇安信威胁情报中心负责人汪列军、网络安全事件响应专家，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。

CISO 的风险计算：划清偏执和警惕之间的界限

作者 | 奥默·科恩

我在以色列出生和长大，至今仍清楚地记得第一次“冒险”去美国购物中心的情景。停车场停满了车，人们在转来转去，但我却找不到入口在哪里。我过了几分钟才意识到，美国的购物中心与以色列不同，并非所有购物中心的每扇门外都设有武装警卫和金属探测器。

我经常分享这件轶事，以此来阐明网络安全领域中的“健康偏执”概念。正如以色列的政治现实让其公民对人身安全保持持续警惕一样，今天的 CISO 也必须在其员工中培养类似的精神，以做好准备，并保护自己免受不断变化的数字威胁的影响。

CISO 本质上别无选择，只能对所有可能出错的事情保持偏执。相反，组织中的其他人通常不会偏执，直到坏事发生。

有用的警惕和令人衰弱的偏执之间的界限在哪里呢?

偏执需要一个目标

用户要始终保持警惕状态显然既不现实，还会适得其反。在心理层面上，持续的警觉可能会让人精神疲惫，常常导致疲劳和倦怠。当个人始终被要求保持高度警惕时，他们的认知功能可能会下降，生产力会下降，且更容易犯错误，这种警觉疲劳最终会抵消警惕的好处。

在零信任时代，这些趋势只会加剧，我们被要求“永远不信任，永远要验证”。有些人将这一要求发挥到极致，模糊了健康的怀疑主义和令人衰弱的不信任之间的界限。

网络安全中的零信任原则提倡严格的验证和监控，但至关重要的是要将这种战略方法和可能阻碍运营、协作和创新的偏执进行区分。

考虑一下组织在如何保护系统和数据方面，将偏执推进到不健康程度的一些方式。

- **繁重的密码要求：**密码的不足之处如今已为大多数用户所熟知，但密码依然被广泛使用。因此，多数大型组织都要求员工使用并定期更改字符、数字和符号组合的复杂密码。然而，此类安全协议往往忽视了一个现实，即许多身份验证相关安全事件，并不是由于密码被破解，而是通过相对简单的社会工程攻击来实现的。此外，如果强密码在暗网上被泄露，再复杂的密码也无法阻止攻击者执行撞库攻击。
- **追求“零风险”：**与许多战略努力一样，风险缓解往往会经历收益递减规律。过于严格的安全措施可能会降低工作效率，并使用户感到沮丧，导致用户寻找可能引入新漏洞的解决

> 许多身份验证相关安全事件，
> 并不是由于密码被破解，
> 而是通过相对简单的社会工程攻击来实现。

方案。追求绝对安全当然值得称赞，但将资源分配到对降低整体风险最有效果的领域往往更为实际。

· 恐惧驱动的决策：我们常常根据基于恐惧和不确定性的情绪反应做出决策，而不是客观分析和理性判断。比如，员工不小心点击了网络钓鱼邮件的恶意软件，由此导致的恐惧驱动反应可能是严格限制所有员工的互联网访问，阻碍生产力和协作，而不是通过更好的培训或更细致的访问控制来解决问题。

强化人类防火墙

有时，我们忘记了偏执和焦虑在物种集体生存中所发挥的关键作用。我们早期的祖先生活在充满掠食者和其他未知威胁的环境中，适量的偏执使他们更加警惕，帮助他们发现并避免潜在的危险。

当今时代的挑战是如何区分真正的威胁和无休止的虚假警报噪音，确保我们遗传的偏执和焦虑为我们服务，而不是阻碍我们发展。它还要求我们承认并解决安全计算中的人为因素。

正如已故知名黑客凯文·米特尼克（Kevin David Mitnick）所说，“随着开发人员不断发明更好的安全技术，利用技术漏洞变得越来越困难，攻击者越来越多地转向利用人的因素。破解人类防火墙通常更容易。”

安全领导者可以采取哪些措施来更有建设性地利用这些本能，以便能够帮助用户警惕并应对这些现实世界的危险，而不至于不知所措呢?

以下是一些可以提供帮助的策略。

· 拥抱安全从设计开始的策略：宣称安全是每个人的责任，并倡导普遍的安全文化是常见说法，但真正的挑战在于如何运用思维方式并将安全措施整合融入产品和系统开发的各个环节。为了真正实现这一目标，安全原则必须无缝嵌入到流程和实践中，确保其成为本能行为，而不仅仅是强制任务。

· 强调边缘情况：边缘情况是指在预期的系统边界之外发生的情况或用户行为。比如，大多数 CISO 都会优先考虑防范数字威胁，但如果有人现场造访服务器机房会怎样？随着技术和用户行为的发展，今天被认为是边缘情况的，在未来可能会变得更加普遍。通过识别并应对这些异常情况，安全团队将能够更好地应对未来不确定的威胁。

· 安全培训必须持续：安全培训不应是一次性的举措。制定强有力的政策是至关重要的第一步，但指望人们会自动理解，并始终如一地遵守这些政策是不现实的。人的天性不能记住仅出现一次的信息并根据其采取行动。这不仅仅是提供信息，而是通过反复培训不断强化知识。时不时的推动或提醒，即使感觉像是唠叨，但对将安全原则放在首位，并确保长期合规，发挥着至关重要的作用。

正如作家约瑟夫·海勒在《第二十二条军规》中所写，“你偏执并不意味着他们不再攻击你。”这是一个很好的提醒，在这个不可预测的世界中，健康适度的偏执可能是防止自满的最佳方法。安

关于作者

奥默·科恩

Descope 首席信息安全官，在网络安全、研究、软件开发和系统管理方面拥有深厚的背景。

境外认知战作战力量及技术装备分析

作者 | 肖宁 曾华圣

认知对抗诞生至今，经过了多轮演化，从最早实体空间的谣言散播、传单投送，到现在网络空间的视频图像伪造合成、虚假新闻传播、信息茧房构建等，充分体现了机器学习、大数据等技术带来的重大变革。

为了更好地了解和掌握境外认知作战体系，以美国、俄罗斯等国家及中国台湾地区为研究对象，梳理了其作战力量与主要技术装备，将为我国认知域积极防御提供借鉴和参考。

一、作战力量

美国、俄罗斯、英国等国家，以及中国台湾地区都成立了相应的认知战指挥机构和认知战部队，其职能各具特色，能够有效地与其他军种、兵种进行联合作战。

1. 美国

美军在目前世界各国军队中信息化程度最高，它一直将认知战作为信息化时代的核心作战样式，相关队伍建设也走在世界前列。2010 年 5 月，美军成立网络战司令部，整合分散在美军各军兵种中的网络战指挥机构，并将网络媒体战部队列为其麾下的重要作战力量之一，2018 年升级为第十联合作战司令部。以美海军为例，其网络媒体战部队在电子战、网络战、心理战、军事欺诈和作战安全 5 大信息建设核心综合能力中占据了 3 项，充分反映了其对认知战的重视。

2. 俄罗斯

俄军一直致力于建设一支专业性强、体系完整的信息战部队。2017 年 2 月，俄军宣称组建信息作战部队，其主要职能是保护私有计算机网络和军事指挥通信系统免遭网络攻击。此外，信息作战部队还负责开展舆论战，以增强俄军的网络舆论掌控能力。该部队的规模在 1 000 人左右。2018 年，俄罗斯设立军事政治管理总局，通过重塑军队政治文化、强化信息传播职能等手段，提升俄军心理战、舆论战、信息战的作战能力。

除上述官方作战部队外，俄军还通过“巨魔行动”和僵尸网络（克里姆林宫“巨魔军队”）来执行心理战、舆论战、信息战任务。每个“巨魔”拥有 6 个 Facebook 账户和 10 个 Twitter 账户，每天能够发布 50 条推文，此外，每天还能发布 50 篇新闻报道。

> 随着人工智能、社会科学、虚拟现实、ChatGPT 等新技术的发展，技术装备也朝着智能化、人机协同、无人化方向发展。

3. 英国

英国作为最早开展心理战的国家，长期维持着一支在境外从事心理战的队伍。英军成立第 15 心理作战群，其角色定位于国内外联合作战的支援力量，通过支援区域性和地方性的作战任务，协助开展战场心理作战活动。

英军对其认知作战力量按照战略、战役、战术的层级进行划分。其中，第 15 心理作战群属战略层级，主要负责招募、训练、指导、规划等活动。下辖的心理作战支援分遣队、战术心理作战小组分别属于战役和战术层级。

4. 中国台湾地区

中国台湾方面认为，未来高新技术条件下的心理战是一种集军事行为、政治攻势、电子干扰于一体的全新作战样式，必须依托健全、专业的心理战作战机构来组织、协调和实施。为此，在“台湾地区防务事务主管机关”设立了“信息战策略规划委员会”，负责对包括心理战在内的信息战实施整体指导，并效仿美军的做法，成立心理战研究机构——“陆军心战装备中心”，其下设“信息心战”“计划指导”和“后勤支援”3 个分队，隶属于“陆军总部政治作战部”。

台军心理作战由“台湾地区防务事务主管机关”直接领导，“总政战局”主任统筹规划，一名“总政战局”副主任督导执行。“总政战局”设有“心理战总队”“心理战电视台”“心理战播音大队”“心理战情报大队”等机构。“心理战总队”下辖 3 个心理战大队，每个大队包含 3 个中队 。

二、主要技术装备

从业务层面，可将网络空间认知作战装备分为态势感知类装备、鉴定识别类装备、内容创作类装备、引导干预类装备、仿真评估类装备。

从业务层面，可将网络空间认知作战装备分为态势感知类装备、鉴定识别类装备、内容创作类装备、引导干预类装备、仿真评估类装备。

1. 态势感知类装备

外国军方研制了多款态势感知和战略预警工具，通过实时监控全球新闻媒体、社交媒体等目标，全面获取互联网信息，利用大数据技术分析、挖掘热点事件及敏感信息，实现全球热点网络态势实时监控和热点冲突实时预警。

1.1 美军心理作战自动化管理系统

美军心理作战自动化管理系统主要为心理作战计划制订、心理战实施和心理作战效果评估提供所需的各种信息，具备信息存储、信息分析、信息处理、信息分发等功能。系统包括外国媒体分析、心理战外国地区数据和心理作战效果分析 3 个系统。外国媒体分析系统主要收集目标地区网络媒体信息，并针对该地区的重要事件、公共人物等，提供详细的分析报告。心理战外国地区数据系统能够处理超 1600 个地区的信息数据，并支持动态自动更新。该系统不仅为美国国防部心理作战组织提供外国地区数据，还为参谋长联席会议主席和心理作战指挥机构提供辅助决策。心理作战效果分析系统主要提供对心理作战效果的分析评估能力。

1.2 “社交媒体战略传播”项目

“社交媒体战略传播”项目由 DARPA 发起，通过研究基于新技术的社交网络信息获取，帮助美军实时掌握网络上的热点事件，并跟踪事件的产生、发展、演化全过程，挖掘事件规律，支撑美军进行战略宣传。

1.3 “数据驱动的模型发现”计划

“数据驱动的模型发现”计划目的是让机器学习如何通过数据驱动进行建模。研究用于高效仿真加速计算架构及支撑平台，开发专为大型复杂体系的演化计算所设计的独立仿真处理系统，提供社会化仿真计算能力；研究智能图像分析、反向图像搜索等深度媒体数据挖掘能力，为美国国家安全局（National Security Agency，NSA）等机构认知域分析提供决策支持。

1.4 “开源指示器”项目

“开源指示器”项目（Open Source Indicator，OSI）由美国情报高级研究计划局（Intelligence

Advanced Research Projects Activity，IARPA）发起，旨在开发对开源数据进行连续、自动分析的方法，以检测和预测政治危机、人道主义危机、大规模暴力骚乱、大规模迁移、疾病暴发等重大社会事件。研究人员通过融合来自多个公开数据源和类型事件的早期指标，来对现实世界中的事件进行评估和分析。

1.5 “X 关键得分”计划

“X 关键得分”计划（XKeyScore）是 2013 年覆盖范围最广的网络信息窃取计划，由 NSA 发起。NSA 通过在全球 150 个地区，设置 700 余台服务器实现对普通用户一切网上行为（如邮件内容、网络访问和搜索记录等）的监控 。NSA 人员只需输入目标对象的邮箱地址，就能对其网上行为进行实时监控。

1.6 “混合预测竞赛”项目

“混合预测竞赛”（Hybrid Forecasting Com petition，HFC）研究项目由 IARPA 于 2017 年 8 月发布。该项目旨在综合利用人与计算机系统各自的长处，改进世界范围内地缘政治问题预测的准确度。竞赛过程中，HFC 将尝试各种人－机混合策略，在政治选举、国家冲突、重大疫情等一系列涉及真实世界事件的场景中，将传统新闻报道、社交媒体和财经数据等信息源与人的判断加以融合，对预测结果进行综合分析，以提升准确率。

1.7 Maltego

Maltego 是 Paterva 公司开发的一款交互式社交网络拓扑情报挖掘工具。只需要一个域名，便可对互联网上的资源自上而下地搜索，它可以枚举网络和域的信息，包括域名系 统（Domain Name System，DNS）、互联网协议地址（Internet Protocol Address，IP）等，可以搜集目标的电子邮件、网站、电话号码、组织、公司等信息。

2. 鉴定识别类装备

鉴定识别类装备帮助外国军方对监测到的敏感信息进行检测、识别，并提供本地文化、语言等参考，帮助其正确理解事件。

2.1 “文化感知信息作战防御”项目

“文化感知信息作战防御”项目是 DARPA 提出的重点 AI 项目，旨在形成人类语言能力，使机器能够理解文化背景、社会和情感背景，从而加深对突发事件的态势感知 。该项目能够帮助参战人员快速了解变化的战场情况。

该项目在 2022 年有 3 个计划：一是引入社会和文化背景模型框架，包括共享的价值观、社会规范和跨文化情感表达的差异；二是为新的自然语言处理（Natural Language Processing，NLP）能力制定方法，例如，解释实体、情感和紧迫性的本地化参考，以及叙事和事件的文化意义；三是建立文化上的专业能力，以理解在稳定作业中通常遇到的紧急事件类型。

2.2 “计算文化理解”计划

2021 年 5 月，DARPA 发布“计算文化理解计划”项目，旨在利用人工智能技术，实现一种可以跨文化交流的自然语言处理技术，以协助美国国防部的海外行动。该技术不仅要阅读语言，还要能够理解和解释文化线索，并提供作战建议。

这项工作分为两个主要研究领域：一是解决目前限制人类语言和交流技术应用的一系列挑战，其中包括社会文化规范的发现、情绪识别和情绪变化的检测；二是开发对话协助服务，该服务可以自动检测社会文化背景并检测误解。

3. 内容创作类装备

外国军方综合运用虚拟现实、人工智能等技术，研制内容创作装备，生成多模态宣传制品，为信息引导提供“弹药”支撑。

3.1 动作捕捉系统

近年来，虚拟现实与增强现实技术被广泛应用于模拟各类极端、恶劣环境，提升军事训练环境的逼真度。与系统的行为交互由各类动作捕捉系统实现，其中 Facerig 软件能够实时读入用户的脸部表情和动作及音频输入；体感控制器有 Leap Motion、Kinect 等；Valve Index 手柄、诺亦腾 Hi5 手套等能实现手部动作捕捉；全身动作捕捉有 Xsens MVN 惯性动作捕捉系统，诺亦腾 Perception Neuron 动作捕捉系统等。

3.2 深度伪造系统

在 2022 年俄乌冲突中，DeepFake 首次被运用到军事活动中。由于 AI 技术日渐成熟，包括生成对抗网络（Generative Adversarial Network，GAN）的快速发展和网上各类深度伪造项目算法的开源，市面上大大小小的各种换脸 App 层出不穷，能达到以假乱真之效。

3.3 基于大语言模型的智能对话系统

以 ChatGPT 为代表的大语言模型对话系统，作为当前最强大的文本自动生成工具，凭借其强大的语言理解能力，不仅能够学习、理解人类的语言进行上下文互动聊天，还能够

根据上下文续写文章，并根据聊天内容进行逻辑推理，完成邮件撰写、代码编写、论文输出、图片生成等任务。除 OpenAI 公司的 ChatGPT 外，目前主流的大语言模型还包括 Google 公司的 T5，微软和英伟达公司的 MT-NLG，Meta 公司的 RoBERTa、LLaMA，BigScience 公司的 BLOOM，DeepMind 公司的 Chinchilla 等。

4. 引导干预类装备

外国军方在对目标身份定位的基础上，利用引导干预类装备，将定制化的“弹药”投送至特定的目标人群，实现认知“弹药”的精准释放。

4.1 社交网络舆论发布系统

社交网络舆论发布系统由美军中央司令部牵头研发，能够在社交媒体上以多个虚拟身份进行信息发布。通过伪造 IP 地址登录社交网站，制造虚拟网民是在不同国家和地区登录和发帖的假象，然后使用这些虚假身份发布信息，诱使极端分子接纳他们进入聊天室和论坛，从而渗透进一些组织（比如“基地”组织和塔利班等极端组织）中去散布假消息，干扰其行动。

4.2 “先进概念技术展示”计划

美军特种作战司令部“先进概念技术展示”计划（Advanced Concept Technology Display，ACTD）提出了研制综合信息推送系统，旨在解决禁入区域的心战制品分发问题，其中一项重要的研究内容就是开发基于不同通信设施的信息推送系统，包括卫星通信、手机、其他无线设备及国际互联网。

4.3 “剑桥分析”的政治竞选系统

“剑桥分析”公司在实际操作中融入心理学理论和影响模型，对各个不同的用户群体进行个性化推荐，进而做到悄无声息地影响用户选举行为。通过分析从社交媒体上获取的用户网络痕迹和发帖信息，分析用户行为，整合用户群体画像，分析出每个人的性别、年龄、宗教信仰、兴趣爱好、性格特征、政治理念、支持政党等。

在 2015 年美国总统大选中，“剑桥分析”公司利用数据模型挖掘中间选民，制造“共鸣信息”，实现广告的精准投放，长期向用户的社交媒体推送特定倾向性内容，从而影响他们的投票结果。

5. 仿真评估类装备

仿真评估类装备利用智能仿真技术对作战环境和作战场景进行模拟，并对各种决策效果进行评估，帮助指挥员进行决策。

5.1 “深绿”计划

“深绿”是 DARPA 研究的一套战前、战中一体，方案制订与分析评估一体的作战决策支持系统。“深绿”计划的技术本质是基于实时态势的动态仿真。

通过战场决策仿真和未来战场态势的超实时仿真，系统能够帮助指挥员针对性做出超前决策。

5.2 心理作战效果分析系统

心理作战效果分析系统属于美军心理作战自动化管理系统的一部分。通过分析信息接收者的抽样调查数据，实现对信息制品和作战计划的评估。

三、结语

作战力量的演进、技术装备的发展都是认知作战体系不断完善的过程，随着人工智能、社会科学、虚拟现实、ChatGPT 等新技术的发展，技术装备也朝着智能化、人机协同、无人化方向发展。本文通过归纳总结境外认知对抗综合情况，希望为我国认知防御体系构建提供参考和借鉴。安

（选自《信息安全与通信保密》2023 年第 5 期）

关于作者

肖　宁

高级工程师，主要研究方向为网络空间安全。

曾华圣

高级工程师，主要研究方向为网络安全。

第三次网攻断电：配合俄大规模袭击的乌克兰电网攻击

作者 | 赵慧杰

美国网络安全公司曼迪昂特 11 月 9 日发布报告称，隶属于俄罗斯联邦武装力量总参谋部情报总局（GRU）的 APT 组织“沙虫”（Sandworm）在 2022 年对乌克兰一处能源设施发动了复杂的攻击，导致其暂时停电，随后乌克兰各地的关键基础设施遭到广泛的导弹袭击。曼迪昂特表示，此次攻击是破坏目标设施物理运行的网络事件的罕见事例，入侵活动还包括一种前所未见的破坏工业控制系统（ICS）和操作技术（OT）的技术。

曼迪昂特公司新兴威胁和分析负责人内森 · 布鲁贝克表示，此次事件不仅是自俄乌战争开始以来第一起已知的因网络攻击导致断电的公开案例，而且还是首次与导弹袭击同时发生的此类事件。乌克兰政府网络官员曾就俄罗斯此前与导弹袭击协调进行的网络攻击发出警告，但从未详细说明这些行动是如何进行的或影响了哪些设施。曼迪昂特未透露目标能源设施所在位置、停电时间及受影响人数。

> 此次事件不仅是自俄乌战争开始以来第一起已知的因网络攻击导致断电的公开案例，而且还是首次与导弹袭击同时发生的此类事件。

一、伴随大规模导弹袭击的针对乌克兰变电站的网络攻击

曼迪昂特公司表示，2022 年年底该公司处置了一起破坏性网络物理事件，其中与俄罗斯有关的威胁组织“沙虫”针对乌克兰关键基础设施机构开展了攻击；该事件是一次多事件网络攻击，利用一种影响工业控制系统（ICS）/ 操作技术（OT）的新技术；攻击者首先使用 OT 级“离地攻击”（LotL）技术可能使受害者的变电站断路器跳闸，导致意外停电，同时乌克兰各地的关键基础设施遭到大规模导弹袭击；“沙虫”组织随后在受害者的 IT 环境中部署了恶意数据擦除软件 CADDYWIPER 的新变种，从而实施了第二次破坏性事件。

曼迪昂特表示，此次攻击代表了俄罗斯网络物理攻击能力的最新演变，自俄罗斯入侵乌克兰以来，这种攻击能力变得越来越明显；事件期间使用的技术表明俄罗斯进攻性 OT 武器库日益成熟，包括识别新的 OT 威胁向量、开发新功能，以及利用不同类型的 OT 基础设施执行攻击的能力；通过使用 LotL 技术，攻击者可能减少了开展网

络物理攻击所需的时间和资源；虽然无法确定最初的入侵点，但分析表明，此次攻击的 OT 部分可能是在短短 2 个月内开发出来的，表明威胁行为者能够快速开发针对来自全球不同原始设备制造商的其他 OT 系统的类似功能。

二、“沙虫”的网络物理攻击

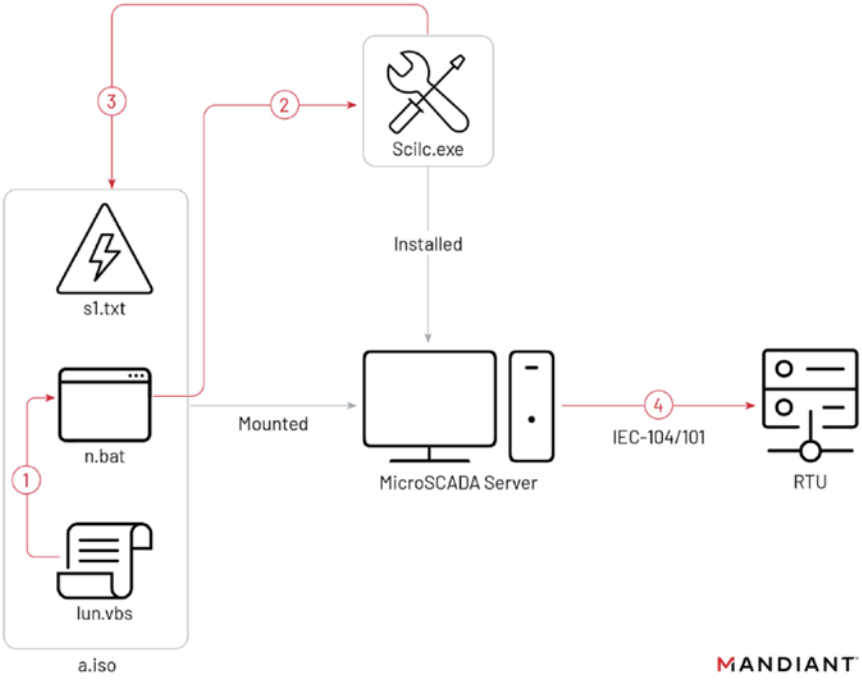
根据曼迪昂特的分析，此次事件的入侵始于 2022 年 6 月或更早，并在 2022 年 10 月 10 日和 12 日导致两次破坏性事件。虽然无法识别进入 IT 环境的初始访问向量，但“沙虫”通过虚拟机管理程序获得了对 OT 环境的访问权限，该虚拟机管理程序为受害者的变电站环境托管了监督控制和数据采集（SCADA）管理实例。根据横向移动的证据，攻击者可以访问 SCADA 系统长达 3 个月。

10 月 10 日，攻击者利用名为“a.iso”的光盘（ISO）映像执行本机 MicroSCADA 二进制文件，试图执行恶意控制命令来关闭变电站。ISO 文件至少包含以下内容：

- “lun.vbs”，运行 n.bat
- “n.bat”，运行本机 scilc.exe 实用程序
- “s1.txt”，包含未经授权的 MicroSCADA 命令

根据“lun.vbs”的 9 月 23 日时间戳，从攻击者首次访问 SCADA 系统到开发 OT 功能，大概有 2 个月的时间段。尽管曼迪昂特无法完全恢复二进制文件实现的 ICS 命令执行，但可以确定攻击导致了意外断电。

事件发生 2 天后，“沙虫”组织在受害者的 IT 环境中部署了恶意数据擦除软件 CADDYWIPER 的新变种，以造成进一步的破坏，并可能会删除取证工件。但是，曼迪昂特注意到该恶意软件部署仅限于受害者的 IT 环境，不会影响虚拟机管理程序或 SCADA 虚拟机。曼迪昂特表示，这是不寻常的，因为威胁行为者从 SCADA 系统中删除了其他取证工件，试图掩盖其踪迹，而恶意数据擦除软件活动会增强这种踪迹，这表明参与攻击的不同个人或操作团队间缺乏协调。

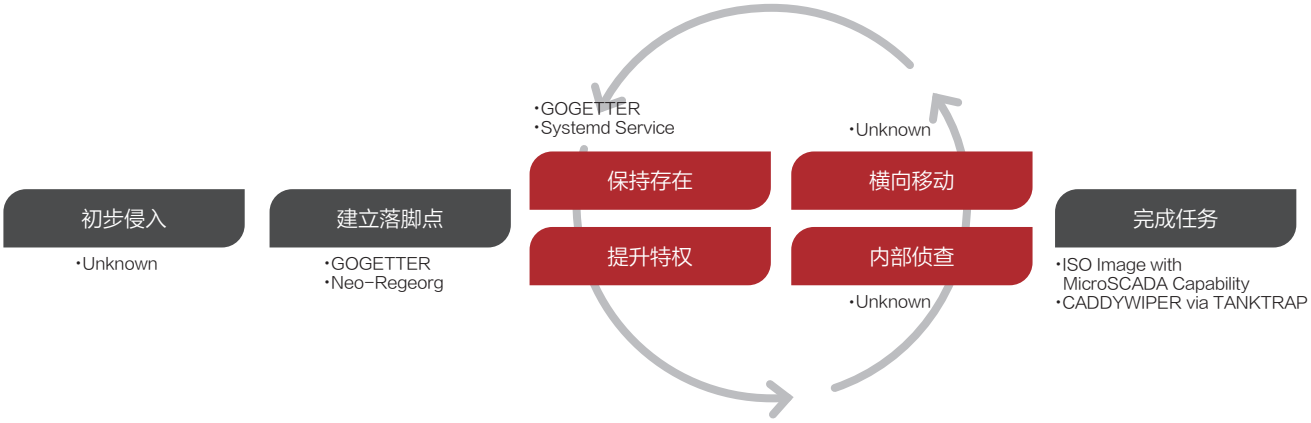


破坏性 OT 事件执行链

三、对俄罗斯进攻性网络能力的洞察

曼迪昂特表示，“沙虫”的变电站网络攻击揭示了俄罗斯持续致力发展面向 OT 的进攻性网络能力和攻击 OT 系统的总体方法；此次事件和 2022 年的 INDUSTROYER.V2 事件均显示出通过简化的部署功能来简化 OT 攻击能力的尝试，在分析一系列详细说明增强俄罗斯进攻性网络能力的项目要求的文件时也发现了同样的尝试。

曼迪昂特称，同样，疑似由俄罗斯联邦武装力量总参谋部情报总局（GRU）发起的 OT 攻击的演变表明，每次攻击的破坏性活动范围有所缩小；2015 年和 2016 年乌克兰断电事件均针对 OT 环境发生了多个离散的破坏性事件，例如，禁用 UPS 系统、破坏串行以太网转换器、对 SIPROTEC 继电器开展 DoS 攻击、擦除 OT 系统等；相比之下，INDUSTROYER.V2 事件



事件攻击活动周期

缺少许多相同的破坏性组件，并且该恶意软件不具有原始 INDUSTROYER 中的恶意擦除模块；同样，“沙虫”在 OT 网络中的活动似乎已简化为仅执行未经授权的 ICS 命令消息，而恶意数据擦除器活动仅限于 IT 环境。虽然这种转变可能反映了战时网络行动节奏的加快，但也揭示了 GRU 在 OT 攻击中的优先目标。

“沙虫”使用本地“离地攻击”二进制文件（LotLBin）来破坏 OT 环境，这显示了技术上的重大转变。使用比此前 OT 事件中观察到的工具更轻量级和通用的工具，攻击者可能减少了开展网络物理攻击所需的时间和资源。LotLBin 技术还使防御者难以检测威胁活动，因为他们不仅需要对引入其环境的新文件保持警惕，而且还需要对已安装的 OT 应用程序和服务中已存在的文件的修改保持警惕。还观察到“沙虫”在其更广泛的操作中采用 LotL 策略，以同样提高其操作的速度和规模，同时最大限度地减少检测的可能性。

曼迪昂特注意到此次网络攻击的时间与俄罗斯的动能行动重叠。“沙虫”可能早在事件发生前 3 周就开发出了破坏性能力，这表明攻击者可能一直在等待特定时刻来部署该能力。最终网络攻击的执行恰逢对乌克兰多个城市的关键基础设施进行了为期多天的协调导弹袭击，包括受害者所在城市。

四、“沙虫”攻击乌克兰变电站技术分析

1、初始渗透和维持存在

目前，尚不清楚“沙虫”最初是如何接触到受害者的。2022 年 6 月，“沙虫”首次在受害者环境中被观察到，当时攻击者在面向互联网的服务器上部署 Neo-REGEORG Webshell。这与该组织此前的活动扫描和利用面向互联网的服务器进行初始访问是一致的。大约 1 个月后，“沙虫”部署了 GOGETTER，这是一个用 Golang 编写的隧道器，使用基于 TLS 的开源库 Yamux 代理其命令和控制（C2）服务器的通信。

在利用 GOGETTER 时，“沙虫”使用 Systemd 服务单元来维护系统的持久性。Systemd 服务单元允许程序在某些条件下运行，在本事例中，它用于在重新启动时执行 GOGETTER 二进制文件。“沙虫”利用的 Systemd

```
[Unit]
Description=Initial cloud-online job (metadata service crawler)
After=
Requires=
[Service]
RestartSec=240000s
Restart=always
TimeoutStartSec=30
ExecStart=/usr/bin/cloud-online
[Install]
WantedBy=multi-user.target
```

Filename	Hash	Purpose
a.iso	Unknown	Contains attacker's files
lun.vbs	26e2a41f26ab885bf409982cb823ffd1	Runs n.bat
n.bat	Unknown	Likely runs native scilc.exe utility
s1.txt	Unknown	Likely contains SCIL commands

配置文件使该组织能够在系统上保持持久立足。在部署 GOGETTER 时，“沙虫”利用 Systemd 服务单元，伪装成合法或看似合法的服务。

2、横向移动到 SCADA 虚拟机管理程序和 OT 攻击执行

“沙虫”利用一种新颖的技术来影响 OT 环境，方法是在产品寿命结束（EOL）MicroSCADA 控制系统中执行代码并发出影响受害者连接变电站的命令。鉴于攻击者使用了反取证技术，无法恢复入侵中的所有工件。

为影响 OT 系统，“沙虫”访问了为受害者变电站环境托管 SCADA 管理实例的虚拟机管理程序，并利用名为“a.iso”的 ISO 映像作为虚拟 CD-ROM。系统配置为允许插入的 CD-ROM 自动运行。ISO 文件至少包含以下文件:“lun.vbs”和“n.bat”，因为这两个文件都在 D 卷中引用，因此包含在“a.iso”中。插入的 ISO 至少导致以下命令行执行:

- wscript.exe “d:\pack\lun.vbs”
- cmd /c "D:\pack\n.bat"

3、部署新 CADDYWIPER 变体破坏 IT 环境

OT 攻击活动 2 天后，“沙虫”在整个 IT 环境中部署了 CADDYWIPER 的新变体。此 CADDYWIPER 变体于 2022 年 10 月编译，包含一些较小的功能改进，使威胁行为者能够在运行时解析功能。

在俄乌战争期间，CADDYWIPER 被部署在乌克兰的多个垂直领域，包括政府和金融部门。CADDYWIPER 是一款用 C 语言编写的颠覆性恶意数据擦除软件，专注于使数据无法恢复并在环境中造成最大程度的损害。

“沙虫”在此次操作中使用 TANKTRAP 从域控制器通过两个组策略对象（GPO）部署了 CADDYWIPER。TANKTRAP 是一个用 PowerShell 编写的实用程序，它利用 Windows 组策略来传播和启动恶意数据擦除软件。安

关于作者

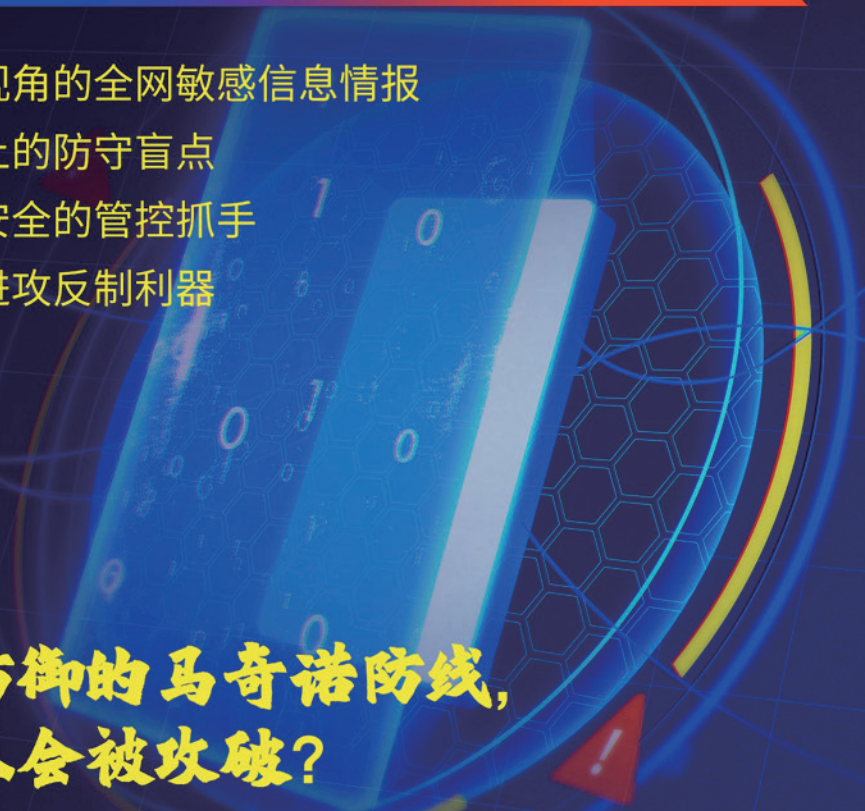
赵慧杰

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。

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

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。


奇安信科技集团股份有限公司

CCIA 50强

2023年中国网安产业竞争力50强

编号：CCIA-2023JZL-01

中国网络安全产业联盟

2023年6月

“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