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

安全漏洞如何管？

P15

第32期

2023 年 8 月

奇安信
新一代网络安全领军者

打造新一代中国特色的安全托管服务

时刻守护您的网络安全

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

两种模式
模式随心选择

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

多种形态
全面助力建成

- 城市运营中心
- 行业安全运营中心
- 企业安全运营中心

两化融合
帮您真正实现

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

首创“云地结合”模式

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

7*24h实时持续监测

“地球不爆炸，我们不放假”——7*24h持续监测，充分保障常态化运营。

安全事件响应快一步

对APT攻击、网络攻击等长效监测，提前预警，响应快一步。

安全事件处置规范化

事前检测、事中分析、事后总结，真正实现闭环，并在实战中不断加固。

专家“一对一”指导

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

漏洞修复为何成难以完成的任务?

2022 年，美国国家标准技术研究院报告了超过 23000 个新的安全漏洞，这是有记录以来一年内的最大峰值。令人担忧的是，这种上升趋势预计将持续下去。最近的研究表明，2023 年平均每月会出现 1900 个高危 CVE，比 2022 年增长 13% 。这源于工具、物联网设备和 SaaS 服务的增加，以及不断出现的人为错误风险。因此对于任何组织来说，漏洞管理对于信息安全都至关重要。

安全团队面临着安全预算减少和安全人才稀缺的问题，每年修补这一惊人安全漏洞浪潮简直是遥不可及的任务。大多数组织的漏洞修补能力有限，这受制于可用工具、流程和技能的影响。各类组织需要将有限的修复能力用于对降低风险最重要的安全漏洞。

实际上，盲目地修复漏洞是一项收效甚微的工作。在数十万个 CVE 中，只有 2% ~ 7% 曾经被利用。很多组织仅依靠 CVSS 评分来评估漏洞的风险。CVSS 评估机制仅局限于漏洞本身的技术威胁，与企业受威胁的实际情况脱节。这在安全专家看来，等同于随机选择漏洞进行修复。一边投入大量资源进行漏洞修复，一边却在为“不存在的威胁”买单，而真正的威胁却时刻暴露给攻击者，给组织的网络安全带来隐患。

随着攻击面的扩大，威胁形势不再像过去那样孤立。在大多数情况下，安全漏洞并不等于暴露面，对于意图渗透组织系统的攻击者来说，并不能带来足够的回报。现在攻击者利用登录凭证和错误配置等组合手段攻击组织关键资产、窃取数据。亨利·福特曾说过：如果你总是做你一直在做的事情，你只会得到你已经得到的。在网络威胁不断演变的今天，漏洞修复的思路需要改变——构建漏洞管理计划，基于风险来应对安全漏洞，对于组织保护其网络和数据至关重要。漏洞管理计划可以帮助组织在网络犯罪分子利用漏洞之前识别 IT 基础设施中的漏洞，确定优先级并进行修复。

在本期的《网安 26 号院》专题探讨了基于风险的漏洞管理，并分享了奇安信的安全漏洞管理实践，希望可以对漏洞管理带来一些启示。

总编辑

2023 年 8 月 1 日

CONTENTS

目录

安全态势

月度专题

安全漏洞如何管？

P15

随着攻击向量扩大和漏洞增加，漏洞管理成为安全解决方案的最前沿，成为风险管理的重要组成。安全漏洞数量激增、无处不在，简单的发现和修复模式已经难以为继 ，基于风险的漏洞管理成为未来趋势。

《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 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：2023 年 8 月 26 日

政策篇

国内，数据安全与隐私保护成为监管热门领域。国家网信办、中国人民银行、中国支付清算协会等机构接连公布规章或指导文件；

国际上，美国政府推进网络安全事件报告制度再落一子，证交会新规要求上市公司确认发生重大网络安全事件后，需在 4 天内进行信息披露。

国内

《信息安全技术 网络安全信息共享指南》等 4 项网络安全国家标准获批发布

8 月 11 日信安标委官网消息，根据 2023 年 8 月 6 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 7 号），全国信息安全标准化技术委员会归口的 4 项国家标准正式发布。其中有一项修订标准，为《信息安全技术 大数据服务安全能力要求》，三项首次发布标准，包括《信息安全技术 移动互联网应用程序（APP）生命周期安全管理指南》《信息安全技术 机器学习算法安全评估规范》《信息安全技术 网络安全信息共享指南》。

中国支付清算协会印发《个人支付信息保护指引》

8 月 9 日中国支付清算协会官网消息，中国支付清算协会修订发布《个人支付信息保护指引》，自发布之日起实施，原《个人信息保护技术指引》废止。本文件给出了个人支付信息的范围定义，提出了个人支付信息保护的基本原则、安全框架、安全保护范围、业务主体及主要义务、组织建设、人员管理、终端和业务系统安全等内容，并针对不同业务场景提出了典型的保护要求，适用于指导参与支付业务的机构信息系统处理个人支付信息的服务与活动。

国际标准《网络安全 工业互联网平台安全参考模型》正式发布

8 月 3 日信安标委官网消息，我国牵头提出的国际标准 ISO/IEC 24392：2023《网络安全 工业互联网平台安全参考模型》在今年 7 月正式发布。ISO/IEC 24392 作为首个工业互联网安全领域的国际标准，基于工业互联网平台安全域、系统生命周期和业务场景三个视角构建了工业互联网平台安全参考模型。该国际标准用于解决工业互联网应用和发展过程中的平台安全问题，可以系统指导工业互联网企业及相关研究机构，针对不同的工业场景，分析工业互联网平台的安全目标，设计工业互联网平台安全防御措施，增强工业互联网平台基础设施的安全性。

国家网信办公布《个人信息保护合规审计管理办法（征求意见稿）》

8 月 3 日国家网信办官网消息，国家网信办发布《个人信息保护合规审计管理办法（征求意见稿）》（以下简称《办法》）及配套的《个人信息保护合规审计参考要点》（以下简称《要点》），公开征求意见。《办法》是对《个人信息保护法》第五十四条“个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计”的细化。《办法》明确提出，处理超过 100 万人个人信息的个人信息处理者，应当每年至少开展一次个人信息保护合规审计。《要点》则直接列明个人信息保护法中各情形下的合规审计要点，

为企业提供了实操性指引，并首次明确外部独立监督机构、个人信息保护社会责任报告的具体要求。

中国人民银行发布《中国人民银行业务领域数据安全管理办法（征求意见稿）》

7月24日中国人民银行官网消息，中国人民银行发布《中国人民银行业务领域数据安全管理办法（征求意见稿）》（以下简称《办法》），公开征求意见。《办法》共八章五十七条，包括总则、数据分类分级、数据安全保护总体要求、数据安全保护管理措施、数据安全保护技术措施、风险监测评估审计与事件处置措施、法律责任、附则。《办法》约束的数据处理活动，主要包括货币政策业务、跨境人民币业务、银行间各类市场交易业务、金融业综合统计业务、支付清算业务、货币管理和数字人民币业务、经理国库业务、征信业务、反洗钱业务等领域。《办法》首次提出，数据安全工作遵循“谁管业务，谁管业务数据，谁管数据安全”基本原则。

《铁路关键信息基础设施安全保护管理办法》公开征求意见

7月18日国家铁路局官网消息，国家铁路局起草形成《铁路关键信息基础设施安全保护管理办法（征求意见稿）》，现公开征求意见。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运营者应当建立健全网络安全保护制度和责任制，保障人力、财力、物力投入。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。

国际

英国内阁发布《2023 年国家风险登记报告》

8 月 3 日英国政府网消息，英国内阁发布《2023 年国家风险登记报告》，警告严重网络攻击威胁正逼近国家关键基础设施。这份报告涵盖了恶意和非恶意风险，共列出了 9 大领域的 89 种风险，其中网络领域仅次于恐怖主义，位列第二。报告中，英国面对的潜在网络威胁前景令人担忧。该报告的主要依据是英国政府内部的国家安全风险评估。报告显示，未来两年内，关键基础设施有高达 5%~25% 的概率遭遇重大网络攻击。报告确定了一系列可能易受网络攻击威胁的目标，包括天然气基础设施、电力基础设施、民用核设施、燃料供应基础设施、政府机构、卫生保健系统、交通运输系统和电信系统等。报告还将人工智能标记为“长期风险”，首次将人工智能引入并视作战略风险。

美国国家网络总监办公室发布《国家网络人才与教育战略》

7 月 31 日白宫官网消息，美国国家网络总监办公室发布《国家网络人才和教育战略》，标志着美国开启为期数年的系统性培养网络安全技能和能力计划。该战略包括四大支柱：让每个美国人具备基础网络技能、转变网络教育、扩充与增强美国网络人才队伍、加强联邦网络人才队伍。每个支柱都包括教育、招聘、职业发展和联邦劳动力政策等方面应落实的多条措施，旨在帮助现有网络技能人员进一步提升能力、鼓励新员工和少数族裔员工进入网络安全领域。该战略承诺，将动用数十亿美元的联邦资金，改变政府、企业、学校和其他组织的劳动力发展方式。

美国证交会通过新规，上市公司重大网络安全事件需在 4 天内披露

7月26日SEC官网，美国证券交易委员会（以下简称“证交会”）通过了新规则，要求上市公司发生网络安全事件并确认属于重大级别后，在 4 天内要进行信息披露。如果立即披露会带来严重危及国家安全或公共安全，可由司法部致函证交会延迟披露。证券交易委员会主席 Gary Gensler 表示：“不论是公司失火导致工厂损失，还是网络安全事件造成数百万份文件丢失，都可能对投资者产生重大影响，新规将让信息披露更具有一致性，并令投资者、上市公司和交易市场受益。”新规还要求，上市公司每年披露网络安全风险管理、战略和治理的重大信息。

事件篇

大型政企机构频频因网络攻击导致业务受影响，造成巨额损失。如美国多州上百家医院和医疗保健机构运营被扰乱，船舶制造巨头因网络攻击停产多天损失超 6 亿元，专业医疗厂商心脏监测服务瘫痪数天等。

英国发生重大数据泄露事件，近 10 年选民数据全部曝光

8 月 8 日 BleepingComputer 消息，英国国家选举委员会披露了一起大规模的数据泄露事件，2014 年—2022 年，所有在英国注册的投票者，个人信息均遭泄露。据委员会发布的公告，他们在 2022 年 10 月首次检测到本次网络攻击，后续调查时发现威胁行为者早在 2021 年 8 月就已经入侵了他们的服务器，其中存储了该部门的电子邮件、控制系统及选民登记册副本，可能导致约 4000 万选民的数据被泄露。选民登记册副本具体包括姓名、家庭地址等信息，英国民众应避免进一步信息泄露，以免遭遇针对性网络钓鱼。

网络攻击扰乱美国多州医院和医疗保健机构运营

8 月 5 日美联社消息，美国大型医疗机构前景医疗遭到网络攻击，导致多州运营的医院和诊所受到影响，许多急诊被迫关闭，救护车被迫转移，许多初级保健服务持续关闭。前景医疗在加利福尼亚、德克萨斯、康涅狄格等州运营 16 家医院、166 家门诊中心与诊所，共同组成一个大型医院网络。美国医院协会的全国网络安全和风险顾问 John Riggi 指责“这是威胁生命的犯罪行为”，他表示恢复过程通常需要持续数周，期间医院将临时回归纸质系统，依靠人工完成设备监控、部门间病历传输等事务。美国国家安全委员会发言人 Adrienne Watson 表示，白宫一直在密切监控这次网络攻击。她表示：“卫生与公众服务部已经与该公司联系，提供联邦援助。我们已经准备好提供必要支持，以防此事件对患者护理造成任何干扰。”

美国船舶制造巨头因网络攻击损失超 6.1 亿元

8 月 3 日 The Record 消息，美国船舶制造巨头宾士域集团（Brunswick Corporation）首席执行官在财报电话会议上向投资者透露，公司因一次网络安全事件蒙受高达 8500 万美元（约合人民币 6.1 亿元）的损失。6 月 13 日，宾士域集团宣布遭受网络攻击，其系统和部分设施受到影响。官方并未确认这是一次勒索软件攻击，但在专家和执法部门处理该事件期间，部分地区的运营被迫停止。公司花费 9 天时间才恢复正常运营，造成了巨大的生产时间损失。据估计，这次攻击将使公司第二季度的收入损失高达 8500 万美元，全年损失可缩减至 6 千万至 7 千万美元。

加拿大专业医疗厂商被黑，心脏监测服务瘫痪数天

7 月 26 日 TechCrunch 消息，加拿大消费级和专业级心脏监测技术提供商 CardioComm Solutions 遭遇网络安全事件，导致服务中断。7 月 25 日该公司披露，由于“服务器遭遇网络安全事件”，业务运营将“受到数天甚至更长时间的影响”。CardioComm 官网持续无法访问，仅显示一条公告消息，称服务中断影响了 CardioComm 多款产品的使用，包括便携式心电图监测器 HeartCheck CardiBeat、医学专业软件 Global Cardio 3 和 Home Flex。目前尚不清楚服务中断范围究竟有多大，会对依赖这些设备进行家庭测试的消费者产生哪些影响。CardioComm 首席执行官 Etienne Grima 尚未回应相关提问。

武汉地震监测中心遭网络攻击，黑手疑来自美国

7 月 26 日环球网消息，武汉市应急管理局 24 日发布声明称，该局所属武汉市地震监测中心遭受境外组织的网络攻击，已封存报案处理。据专家组发现，武汉市地震监测中心部分地震速报数据前端台站采集点网络设备遭受网络攻击，初步证据显示网络攻击来自美国。武汉市公安局江汉分局随即发布警情通报，证实在武汉市地震监测中心发现了源于境外的木马程序，该木马程序能非法控制并窃取地震速报前端台站采集的地震烈度数据。该行为对国家安全构成严重威胁。江汉分局已对此案立案侦查，并对提取到的木马样本进一步开展技术分析。

这是继 2022 年 6 月西北工业大学遭受境外网络攻击后又一具体案例。有专业人士表示，地震烈度数据指地震的烈度和震级，这是衡量地震破坏力的两个重要指标，尤其是地震烈度代表对地质的破坏程度，烈度越大、破坏性越大，“地震烈度数据与国家安全息息相关，如一些军事防御设施就需要考虑到烈度等因素”。

外包服务商遭网络攻击，致使英国部分地区救护车系统瘫痪

7 月 26 日 The Register 消息，瑞典医疗软件公司 Ortivus 遭受网络攻击，导致托管数据中心环境中的客户系统受影响，多家英国国民健康服务（NHS）的救护车机构难以记录患者数据，或将数据传递给其他医疗服务提供商。受影响的英国西南救护车服务信托、中南救护车服务信托，为英格兰西南部 1200 万常住人口及 2300 万游客提供服务。据透露，事件发生后，中南救护车服务信托工作人员无法使用计算机，被迫用纸和笔工作。

因统一政务系统 0day 漏洞遭利用，挪威十余个政务平台敏感数据或泄露

7 月 24 日 Bleeping Computer 消息，挪威政府警告称，黑客利用第三方软件的 0day 漏洞发动网络攻击，12 个部委使用的信息通信技术平台受到影响。挪威政府安全和服务组织在发现网络攻击后通知了挪威国家安全局，并协同警方进行调查。挪威数据保护局已收到有关网络攻击的通报，表明黑客可能已经访问和 / 或窃取了信息通信技术系统中的敏感数据，导致数据泄露事件。尽管受到攻击的平台在政府的日常运作中扮演着关键角色，但这次网络攻击不会导致工作活动陷入停滞。据悉，此次曝出的 0day 漏洞（CVE-2023-35078），来自美国软件巨头 Ivanti 旗下 Endpoint Manager Mobile（EPMM）。除总理办公室、国防部、司法与公共安全部、外交部外，挪威其他所有部委均使用该平台。

今年最大规模网络攻击：受害机构数量逼近 400 家，影响人数超 2 千万

7 月 20 日 The Register 消息，美国 Progress Software 公司旗下产品 MOVEit 的 0day 漏洞遭利用曝光已近两月，据网络安全厂商 Emsisoft 统计，目前已公开的受害机构逼近 400 家，超过 2 千万人受到影响，其中不乏美国能源部等政府机构、能源巨头壳牌、德意志银行、普华永道、零售巨头 TJX 等知名公司机构，以及向大量下游机构提供服务的服务商。今年 5 月下旬，俄罗斯勒索软件组织 Clop 开始利用 MOVEit 文件传输软件的 0day 漏洞发动攻击，由于 MOVEit 拥有大量企业机构用户，此后受害者数量和损失持续攀升。

网络犯罪盯上 ESG 领域！挪威资源回收巨头被黑，导致部分系统瘫痪

7 月 18 日 The Record 消息，挪威再生资源回收和矿业公司陶朗集团（Tomra）遭受 “大规模”网络攻击，公司系统受到影响。陶朗集团在 17 日发布声明称，“公司遭受了一次大规模网络攻击，直接影响了部分数据系统……为了限制攻击影响，我们立即断开部分系统。目前，陶朗集团正在评估，客户和员工在使用我方服务时是否会遇到稳定性下降的问题。”陶朗集团没有回答此次攻击是否为勒索软件攻击，表示首要任务是“尽快恢复所有系统的正常运行”。目前尚无黑客组织声称对此次攻击负责。

漏洞篇

近期，全国各地接连举办网络安全攻防演练活动，奇安信 CERT 监测到多家厂商发布安全更新，修复多个安全漏洞，建议相关产品用户尽快做好自查及防护。

Smartbi Token 回调地址漏洞安全风险通告

8 月 10 日，奇安信 CERT 监测到 Smartbi 官方发布安全更新，修复了 Smartbi Token 回调地址漏洞 (QVD-2023-18159)。由于 QVD-2023-17461 漏洞未修复完全，Smartbi 在特定场景下仍存在 Token 回调地址漏洞，未经身份认证的远程攻击者利用该漏洞获取管理员 Token，从而以管理员权限接管后台，进一步利用可实现任意代码执行。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

WPS Office 代码执行漏洞安全风险通告

8 月 9 日，奇安信红雨滴高级威胁研究团队捕获 WPS Office 代码执行漏洞 (QVD-2023-17241) 在野利用样本，同时奇安信 CERT 监测到 WPS Office 官方修复 WPS Office 代码执行漏洞 (QVD-2023-17241)。攻击者通过诱导用户打开文档中嵌入的远程链接，即可触发此漏洞执行任意代码。鉴于此漏洞目前处于在野利用状态，现实威胁较大，建议客户尽快做好自查及防护。

Smartbi 身份认证绕过漏洞安全风险通告

8 月 2 日，奇安信 CERT 监测到 Smartbi 身份认证绕过漏洞 (QVD-2023-17461)，未经授权的远程攻击者可利用该漏洞获取管理员 Token，从而以管理员权限接管后台，进一步利用可实现任意代码执行。利用此漏洞需目标可出网。鉴于此漏洞影响较大，建议客户尽快做好自查及防护。

Linux Kernel 权限提升漏洞安全风险通告

8 月 1 日，奇安信 CERT 监测到 Linux Kernel 权限提升漏洞 (CVE-2023-3269)，又名“Stack Rot”。在 Linux 内核的内存管理子系统存在释放后重用漏洞，本地低权限用户可以利用此漏洞提升至 ROOT 权限。目前，此漏洞技术细节、POC 及 EXP 已在互联网上公开，奇安信 CERT 成功复现此漏洞，鉴于此漏洞现实威胁上升，建议客户尽快做好自查及防护。

Apache Shiro 身份认证绕过漏洞安全风险通告

7 月 26 日，奇安信 CERT 监测到 Apache Shiro 身份认证绕过漏洞 (CVE-2023-34478)，当 Shiro 在 API 或基于非规范化路由请求的 Web 框架中使用时，攻击者可能利用此漏洞绕过身份验证。目前，奇安信 CERT 已复现此漏洞，鉴于此产品用量较大，建议客户尽快做好自查及防护。

Metabase 远程命令执行漏洞安全风险通告

7 月 25 日，奇安信 CERT 监测到 Metabase 官方发布安全更新，修复了 Metabase 远程命令执行漏洞 (CVE-2023-38646)。未经身份认证的远程攻击者利用该漏洞可以在服务器上以运行 Metabase 服务器的权限执行任意命令。目前，奇安信 CERT 已复现此漏洞，鉴于此漏洞利用简单、影响较大，建议客户尽快做好自查及防护。

Apple kernel 安全特性绕过漏洞安全风险通告

7 月 25 日，奇安信 CERT 监测到 Apple 官方发布安全更新，其中包括 Apple kernel 安全特性绕过漏洞 (CVE-2023-38606)。攻击者使用恶意应用程序利用该漏洞能够修改敏感的内核状态，从而可以控制设备。鉴于此漏洞影响范围较大，且已发现在野利用，建议客户尽快做好自查及防护。

Spring Security 身份认证绕过漏洞安全风险通告

7 月 20 日，奇安信 CERT 监测到 Spring Security 身份认证绕过漏洞 (CVE-2023-34034)，在 WebFlux 的 Spring Security 配置中使用 "**" 作为匹配模式，会导致 Spring Security 和 Spring WebFlux 之间模式不匹配，并可能导致身份认证绕过。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Atlassian Confluence Data Center&Server 远程代码执行漏洞安全风险通告

7 月 20 日，奇安信 CERT 监测到 Atlassian Confluence Data Center & Server 远程代码执行漏洞 (CVE-2023-22508)，经过身份验证的远程攻击者可以利用此漏洞在 Confluence Data Center & Server 上执行任意代码。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

OpenSSH ssh-agent 远程代码执行漏洞安全风险通告

7 月 20 日，奇安信 CERT 监测到 OpenSSH ssh-agent 远程代码执行漏洞 (CVE-2023-38408)，开启 ssh-agent 转发时，拥有转发到的服务器权限的攻击者可以利用该漏洞在 ssh-agent 上执行任意代码。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Citrix ADC 及 Citrix Gateway 远程代码执行漏洞安全风险通告

7 月 19 日，奇安信 CERT 监测到 Citrix ADC 及 Citrix Gateway 远程代码执行漏洞 (CVE-2023-3519)，Citrix ADC 及 Citrix Gateway 中存在远程代码执行漏洞，远程未授权攻击者可利用此漏洞在目标设备上执行任意代码。目前已监测到在野利用。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

厂商安全更新提醒

近期，全国各地接连举办网络安全攻防演练活动，奇安信 CERT 监测到多家厂商发布安全更新，修复多个安全漏洞，经不完全统计如下表所示，建议相关产品用户尽快做好自查及防护。

厂商名	发布时间	相关链接
思迈特 SmartBI	2023-08-08	https://www.smartbi.com.cn/patchinfo/
金山办公 WPS	2023-08-09	https://security.wps.cn/notices/35
用友 Yonyou	2023-08-10	https://security.yonyou.com/#/noticeList
新华三 H3C	2023-08-10	https://www.h3c.com/cn/Service/Online_Help/psirt/security-notice/detail_2021.htm?Id=111
泛微 Weaver	2023-08-10	https://www.weaver.com.cn/cs/securityDownload.html#
深信服 Sangfor	2023-08-10	https://www.sangfor.com.cn/sec_center/details/70df3b537b2549db86f3f31bda4ec850
帆软 FineReport	2023-08-11	https://help.fanruan.com/finereport/index.php?doc-view-4833.html

注：发布时间为近期首次发布安全更新日期，部分厂商后续仍在持续发布安全更新。

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 7 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 7 月，奇安信 Z-TEAM 团队共承接攻防演习服务 37 场，其中省级攻防演习 1 场，省级行业攻防演习 2 场，地市级攻防演习 5 场，客户自主攻防演习 29 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政府部委、金融、央企行业较多，此情况与上月承接攻防演习涉及行业范围数据有所变化，央企行业攻防演习数量增长明显（见图 2）。

本月攻防演习成果如表 1 所示。

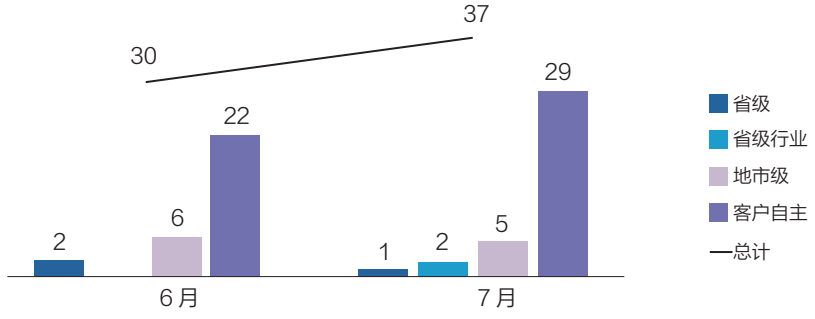


图 1 6-7 月 Z-TEAM 承接攻防演习数量统计

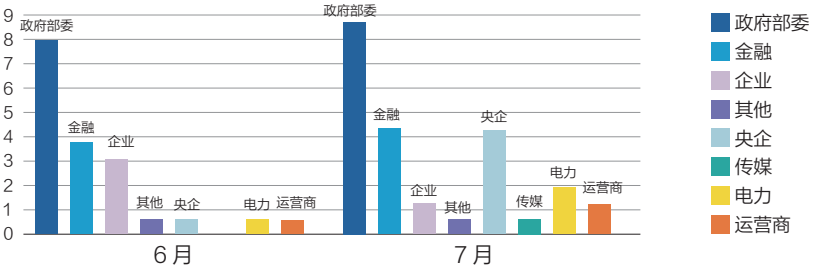


图 2 2023 年攻防演习涉及行业统计图

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	62	77	69	103	127	215	733	12859

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，涵盖了政府部委、金融、央企、电力、企业、传媒、运营商等行业。

随着信息通信技术的快速发展，计算机病毒、系统安全漏洞和网络违法犯罪等网络与信息安全问题日益严峻，网络安全已经成为运营商必须重视和关注的重要方面。只有通过加强网络安全措施，及时应对网络安全事件，确保用户隐私与数据安全不受侵害，才能赢得用户的信任，保护自身业务的稳定运营。网络安全攻防演练通过对运营商的网络平台和信息系统进行全方位渗透测试，以发现可造成数据泄露、资产受损、系统篡改等风险的漏洞，帮助用户提早发现网络空间中的安全隐患，未雨绸缪。运营商行业在本月攻防演习中占比为 5%（见图 3）。

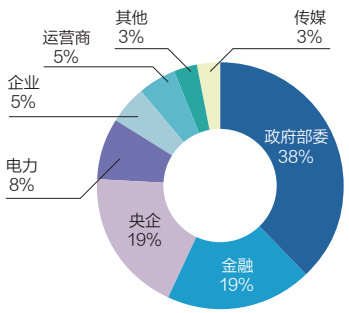


图 3 7 月攻防演习分布图

三、主要攻击手段分析

基于奇安信 Z-TEAM 团队实战成果，在本月任务中对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。例如，政府部委、企业、运营商行业外网突破的主要手段包括口令爆破和漏洞扫描利用等；传媒、电力行业主要是漏洞扫描利用和隐秘隧道外联等；金融和央企行业外网突破的主要手段包括漏洞利用、钓鱼攻击和口令爆破等。因此，我们建议各个行业加强外网安全管理，定期检测和修复漏洞，加强口令策略，增强员工安全意识，以防止攻击者利用外网攻击内网。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、隐秘隧道外联等。

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

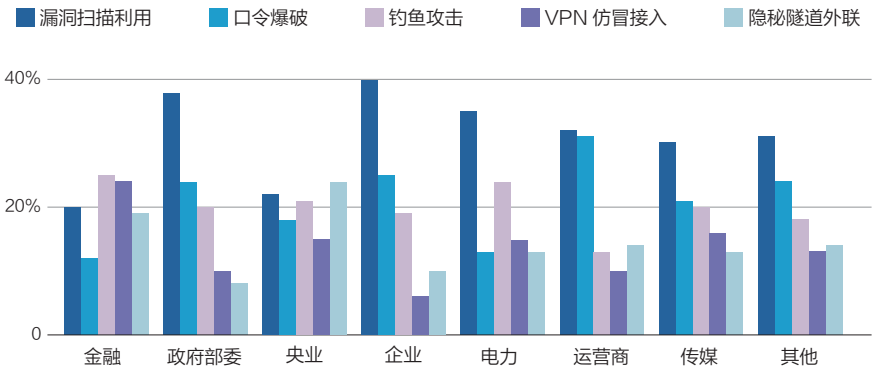


图 4 行业攻击手段分布图

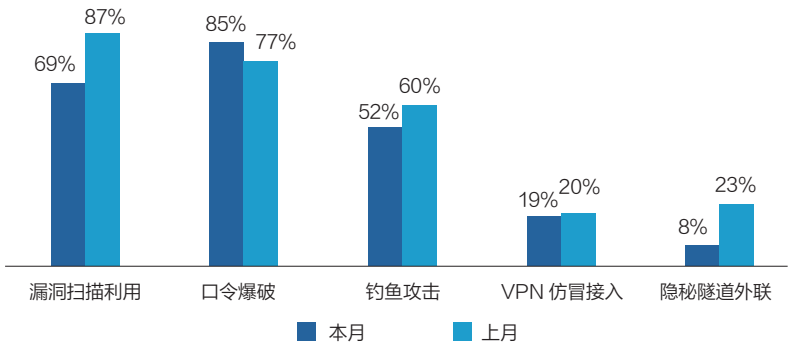


图 5 攻击手段对比图

通过对本月运营商行业攻防演习任务的数据分析发现，开源情报搜集到诸多如企业员工内部邮箱、联系方式、企业架构、供应链名录、产品代码等关键情报信息，这些信息都可以为进一步的攻击提供支撑。根据情报收集围绕薄弱点利用弱口令、历史漏洞等攻击手段实现突破；以突破点为基础进行内网横向移动，利用钓鱼攻击、隐秘隧道外联攻击手段，在内网以点带面实现横向拓展遍地开花。

攻防演练过程中，各种攻击手段的运用往往不是孤立的，而是相互交叉配合的，一个渗透拓展步骤的成功，往往需要两种，甚至两种以上的手段共同配合才能成功。

四、典型攻击手段实现案例

运营商需要处理大量的用户数据，包括个人身份信息、通信记录等。如果网络安全存在防护漏洞或未经授权的访问，这些数据可能会被窃取、篡改或滥用，给用户和运营商带来严重的风险和损失。网络安全问题不仅会给运营商的业务连续性、用户信任及企业声誉造成严重威胁，还必将导致法律风险和额外成本增加。因此，运营商需要高度重视网络安全，并采取有效措施来防范和应对安全威胁。

案例：利用弱口令结合历史漏洞直达某运营商核心内网。

奇安信攻击队在某运营商攻防演练中，根据攻击队前期的情报信息，在进行目标资产信息搜集时，尝试在各种互联网资产探测引擎上查找目标信息，最终发现各种 SQL 注入及反序列化等可以简单 GetShell 的方式，全部没有用，该运营商的办公网络及核心工业控制系统得到了非常严密的安全防护，对互联网暴露的业务系统很少，而且业务系统做了安全加固及多层防护，同时也拥有较强的日常网络安全运维保障能力，防守固若金汤。想要正面突破，难之又难，仿佛是一场不可战胜的战斗。

就在大家一筹莫展之际，一位同事提出侧面出击，既然正面无法突破，那就围绕目标周边寻找契机。一些队员便开始通过某些开源社工库或互联网痕迹中收集目标企业的信息。功夫不负苦心人，终于搜索到了一批工作人员邮箱列表。掌握这批邮箱列表后，便根据已泄露的密码规则、123456、root、admin123 等常见弱口令、用户名密码相同或用户名 123 等多种弱口令生成了一份弱口令字典。利用 hydra 等工具进行爆破，成功破解一名员工的邮箱密码。

攻击队根据已破解的邮箱密码成

> 攻防演练过程中，
> 各种攻击手段的运用往往不是孤立的，
> 而是相互交叉配合的。
> 一个渗透拓展步骤的成功，
> 往往需要两种，甚至数种手段共同配合才能成功。

图 6 案例攻击路线图

功登录了该员工的邮箱，通过查找其中关键敏感信息，利用所收集到的信息成功登录采购管理系统。当攻击队为这一重大突破高兴时，一盆冷水悄然而至。攻击队发现这是旧版采购管理系统，核心网段的关键信息很少。无奈之下，攻击队只能放弃这条路。

柳暗花明又一村，攻击队接着根据爆破的邮箱从其他信息入手，发现某运营商新版报表系统，由于业务需求，报表系统往往提供文件上传或下载功能，攻击队发现报表系统未对上传、下载的文件类型进行严格的验证和过滤，就容易造成不受限制的文件类型上传或敏感文件下载，可确定存在文件上传、下载的历史漏洞。攻击队利用该漏洞成功地获取了管理员权限，通过报表系统权限进入堡垒机，并成功打入该运营商的核心内网，为本次演习画下完美的句号。

五、安全防护建议

1. 攻击案例剖析

运营商企业网络安全边界有较完善的防御体系，并对互联网暴露面进行了排查收敛，攻击队采取互联网敏感信息搜集 + 社工 + 弱口令爆破，打开了突破口。由于没有有效的技控手段，当出现安全意识薄弱的员工时，很难避免出现弱口令、信息泄露等安全隐患。攻击队以此为突破口，获取员工账号口令信息，登录重要业务系统，再利用系统漏洞获取系统权限，突破网络边界，入侵核心内网。

2. 弱口令检测与防护策略

该案例企业在人员安全意识、弱口令治理与防护等工作方面存在不足，具体建议如下。

(1) 强化全员网络安全意识

① 网络安全意识培训：通过课堂演示、案例讲解、攻防模拟演练等多维度的授课方式将网安知识由浅入深、循序渐进地传递给企业员工。

② 安全意识宣传材料：包括电子版及实物版的安全意识海报、月刊、长图、手册、屏保等内容。

③ 网络安全意识竞答：以碎片化、长周期的企业员工意识的提升为目标，将知识内容以各种形式渗透到工作中的各个角落，通过在线答题方式，促进员工安全意识的提升。

④ 钓鱼邮件测试服务：基于社会工程学原理，结合客户网络环境、邮件使用习惯和特征，以热点事件为主题，精心构造极具迷惑性且含有恶意链接的邮件，模仿用户组织内部人员 / 部门向目标群体定向开展邮件钓鱼测试，进而评估用户组织内部人员信息安全意识，为后续安全培训、技术防护手段升级提供依据。

(2) 开展弱口令安全隐患排查

针对企业所有环境（含生产、开发、测试、灾备、预生产环境、机构云），及第三方部署环境所有的应用系统、基础设施的账号密码，包括但不限于以下内容：

- 所有应用系统前后台的用户、管理员账号，包括只读账号等；
- 操作系统、中间件、数据库、网络和安全设备、语音和视频设备等基础设施账号；
- 各种内部 FTP、SVN，开发框架及各类监控平台、网管平台，备份平台、云管理平台、自动化运维等各类管理工具、管理控制台的登录账号；
- 部署在第三方的应用系统和基础设施账号；
- 个人计算机登录账号。

持续主机口令风险排查：利用奇安信椒图云锁主机防护系统，定期对主机操作系统、中间件、数据库等软件系统进行弱口令及服用口令排查（根据企业特性，制定弱口令字典）；

实时流量监测分析弱口令行为：利用奇安信天眼威胁检测与分析系统，对告警及流量日志进行分析，通过弱口令监测模块发现网络内的弱口令登录行为。安

奇安信

北京2022年冬奥会官方网络安全赞助商

奇安信威胁情报中心

中国威胁情报行业领军者

威胁情报中心

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

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

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

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

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

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

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

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

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

安全漏洞如何管？

随着攻击向量的扩大和漏洞的增加，漏洞管理成为安全解决方案的最前沿，成为风险管理的重要组成。安全漏洞数量激增、无处不在，简单的发现和修复模式已经难以为继，基于风险的漏洞管理成为未来趋势。

基于风险的管理：漏洞管理破局之道

作者 | 李渊

一、背景

1.1 漏洞及威胁的发展趋势

物联网、云服务与移动设备等新设备与应用不断增加，不可避免地伴随众多漏洞，机构的攻击面不断增加，网络安全威胁日益严重。

安全公司 Skybox Security 发布的《2022 年漏洞和威胁趋势报告》显示，过去的十年间，安全漏洞数量增长了近三倍，创历史新高。其中，2021年公布的新漏洞共有20175个，比 2020 年增长了 10%，比 2017 年增长了 37%（见图 1）。

图 1 2017 年—2021 年发布的漏洞数量 (CVE)

传统中型企业整个生态系统平均面对 20 万个漏洞，其安全分析师常常陷入不知道从哪儿开始的窘境。大型企业的 IT 安全漏洞数量可达数百万的数量级。漏洞数量在不断积累，而漏洞的平均修复时间却在增加，根据 WhiteHat Security 2021 年发布的报告《AppSec Stats Flash》，修复关键网络安全漏洞所需的平均时间已经从 2021 年 4 月的 197 天增加到了 2021 年 5 月的 205 天。

旧的漏洞没有修复，新的漏洞不断涌现，巨大而快速的漏洞数量积累，使企业背负了高额的漏洞负债。

1.2 传统漏洞管理发展现状及问题

1.2.1 传统漏洞管理发展现状

回顾传统漏洞管理的发展历程，企业从没有安全扫描手段，补丁随意管理，到实现了自动化漏洞扫描，开展定期评估；从无法发现安全隐患，到能够发现隐患并采用固定的评估方式，进行漏洞和安全隐患评估。

传统漏洞管理已经从“问题即解决”的管理模式进入到基于合规的“定期评估”的结构化管理模式，并形成了相对固定的套路。进一步说，是将漏洞管理分为“识别 – 评估 – 处理 – 报告”四个阶段。在漏洞评估阶段，采用漏洞扫描工具发现漏洞，漏洞信息基本源自公共漏洞库；在漏洞评估

阶段，多数做法是直接沿用通用漏洞评估系统（Common Vulnerability Scoring System，CVSS）评估标准，按照通用评估标准将漏洞划分为高危、中危、低危；在漏洞处理阶段，按照高、中、低的顺序进行漏洞修复；在漏洞修复完成后形成漏洞修复和评估报告。

1.2.1 传统漏洞管理现存问题

漏洞修复的工作量日益庞大，企业面临的网络威胁千变万化，时刻对企业安全产生威胁。这种情况下，传统的漏洞管理模式暴露出了明显的问题。

传统漏洞管理将重点放在高CVSS的严重漏洞上（以漏洞为中心的模式），而CVSS的评估机制仅仅局限于漏洞本身的技术威胁，与企业受威胁的实际情况脱节。即无论其评估有多么严重，对于企业来讲，如果没有暴露出来或者不能被攻击者利用，都是极其安全的。反之，即使是中低风险的漏洞，如果很容易被攻击者接触并被利用，那么该漏洞都是极其危险的。

企业一边投入大量资源进行漏洞修复，一边却在为“不存在的威胁”买单，而真正的威胁却时刻暴露给攻击者，给企业安全带来隐患。使漏洞管理工作陷入困境，难以破解。

二、漏洞管理成熟度模型

漏洞管理难题之所以陷入困境，是因为我们没有站在更高的角度看待问题，不了解企业漏洞管理所处的阶段，不清楚未来的发展方向。

早在2016年，著名网络安全公司CoreSecurity提出了漏洞管理的成熟度模型（见图2）。这个模型在业内得到了广泛的认可，在这个模型中，企业漏洞管理是一个从盲目走向成熟的过程。模型像一张地图，清晰展示了企业安全漏洞管理的发展路径，也为我们破解当前漏洞管理难题提供了指引。

从大的分类来看，漏洞管理成熟度可以分为三个阶段：无意识的初级阶段、意识觉醒的中级阶段、基于商业风险及环境的高级阶段。更细致地分，漏洞管理可分为六个层级（L0 ~ L5）。

Level 0 无管理阶段（NON-EXISTENT）。该阶段没有安全扫描，缺乏自动化手段，漏洞补丁管理随意，依靠人工进行安全设置和评估，这个阶段不存在漏洞管理概念。

Level 1 扫描阶段（SCANNING）。该阶段主要是以问题为导向，开展漏洞扫描，发现安全隐患和漏洞，但是不知道从哪里开始补救。生成大量扫描数据，但是不知道该如何使用，企业缺乏对扫描数据利用的指导。

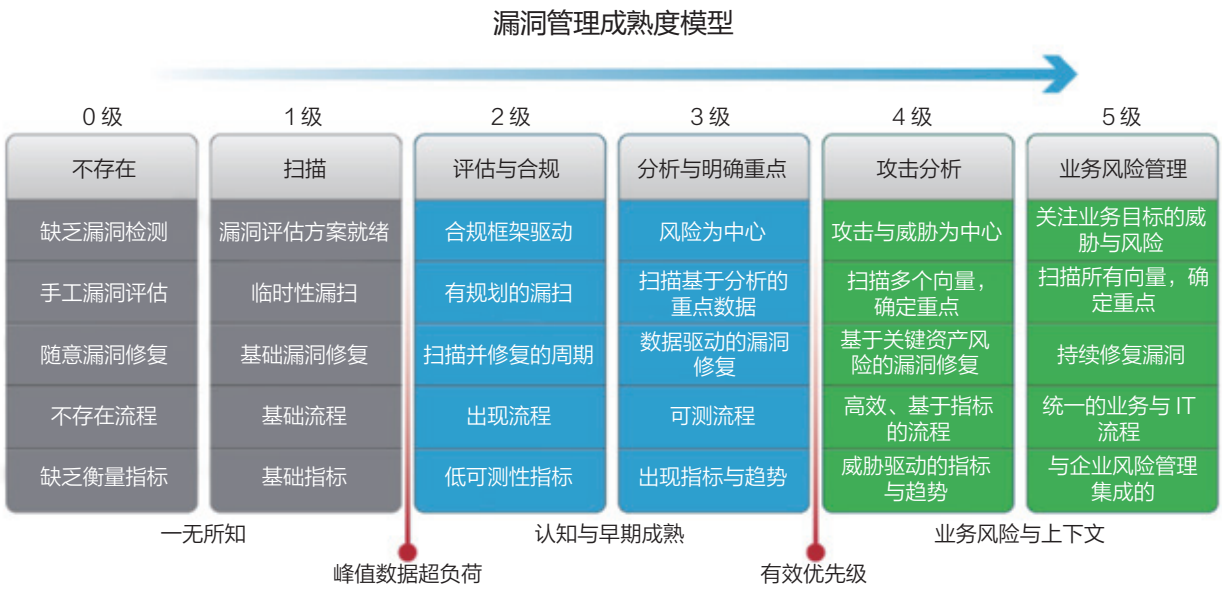


图2 漏洞管理成熟度模型

Level 2 评估和合规阶段（ASSESSMENT & COMPLIANCE）。该阶段开展了有计划化的安全评估，从第一阶段的“问题即解决”的管理模式跃迁到第二阶段的“定期评估”的结构化管理模式是一个巨大的转变。企业可以使用合规性要求作为框架，围绕该框架构建漏洞管理计划。

Level3 分析和优先顺序阶段（ANALYSIS & PRIORITIZATION）。一旦进入该阶段，漏洞处理的优先顺序就不是基于合规，而是基于风险，一旦达到这一级别，优先顺序就不再基于合规标准，而是由风险决定。然而，尽管这一级别包含了基于风险的优先级划分，但其更关注局部而非整体。它根据攻击者是否可以在某一个攻击步骤中利用漏洞获得访问权限来划分优先级。

Level4 攻击管理阶段(ATTACK MANAGEMENT）。这个阶段更关注整体，不再将漏洞和修复视为独立的实体，而是视为一个完整的生态系统。攻击管理使用扫描和渗透测试数据来进行攻击识别，关注威胁参与者如何在系统中移动，并利用漏洞访问业务关键资产。该阶段通过对这些关键资产的风险分析来确定漏洞修复的优先顺序。

Level5 商业风险管理阶段（Business-Risk Management）。这是所有组织都应该努力达到的水平，依据商业风险开展漏洞和风险管理。该阶段具备全面发展的管理计划，考虑企业的整体环境，分析漏洞扫描和渗透测试的数据，检查指标、确定趋势，使用特定的流程和补救技术。

通过与漏洞成熟度模型的对比，不难发现，国内大多数企业还处于漏洞成熟度发展的初、中级阶段（即L0~L2 阶段），而当前面临的种种问题，正是这个阶段必然遇到的问题。

发展中的问题要靠发展来解决。要想解决当前问题，漏洞管理就要尽快迈入 L3 阶段（分析和优先顺序阶段），通过建立更科学、更成熟的漏洞管理模式，解决低层次管理中遇到的问题。按照漏洞管理成熟度模型的描述，L3 阶段的核心思想是基于风险进行漏洞的优先级排序，再按照漏洞的优先顺序进行漏洞修复。从而将企业的关注点放在最有威胁的漏洞上，极大降低漏洞管理人员的工作量。

三、基于风险的漏洞管理（RBVM）

3.1 RBVM 的诞生和内涵

近年来，一种新的漏洞管理方法兴起，这就是基于风险的漏洞管理（RBVM），这种思想与漏洞管理成

> 基于风险的漏洞管理（RBVM）思想与漏洞管理成熟度模型中 L3 阶段的管理思想不谋而合。

熟度模型中 L3 阶段的管理思想不谋而合，也为企业进入 L3 阶段提供了科学的方法。

RBVM 的内涵是根据漏洞给组织带来的风险，来检测、修复和控制漏洞的过程。通过自动、持续地识别安全弱点，全面了解攻击面，从而根据风险严重性和业务影响确定补救的优先级。借助基于风险的漏洞管理计划，安全团队可以有效地管理风险，避免浪费时间修复对组织威胁很小或没有威胁的漏洞。

Gartner 在 2020 年“安全与风险管理峰会”上，将 RBVM 提上 2020 年十大安全项目，Gartner 认为应该采用基于风险的方法来管理补丁程序，重点关注具有较高风险的系统和漏洞。Gartner 认为“2022 年，采用基于风险的漏洞管理方法，组织将减少 80% 的入侵”。

图 3 传统漏洞管理和基于风险的漏洞管理方法对比

3.2 RBVM 聚焦真正的风险

越来越多的漏洞被推高到重要的高评级，给企业带来一个问题，即有太多的漏洞需要立即修复，使企业分散精力和资源，从而使得问题变得更糟。所以，适当地确定优先级或降低优先级，这是漏洞管理中的一项关键需求。RBVM 解决了这一需求，它提供了一种清晰的方式来解释需要解决的漏洞总数、最迫切需要解决的风险，它可以以更广阔的视野审视业务风险，聚焦真正的风险，关注最重要的漏洞和资产，提升安全防御的效率和精准度。

1. 全面评估风险。评估企业业务风险和 IT 环境，全面了解整个攻击面，消除风险管理盲区，并根据风险确定要优先考虑哪些漏洞，以进行补救。

2. 提升管理精准度。不在被利用可能性较低的漏洞上浪费时间，以最少的努力减少最大数量的风险，聚焦真正的业务风险，提升安全管理的精准度。

3. 建立动态管理模式。不断发现和评估与攻击面上所有的业务关键资产相关的风险，对漏洞、威胁和资产关键数据开展动态分析，建立动态漏洞管理模式。

4. 提升管理效率。给组织提供一种理性的漏洞管理方法，可以识别哪些行动可以推迟或完全忽略，使得组织能将精力投入到最重要的事情上，以提升管理效率。

3.3 RBVM 与传统方法的区别

传统漏洞管理方法并不是为应对现代攻击方法和随之而来的日益增多的威胁而设计的，它还局限于漏洞自身的风险，从而使安全团队浪费大量时间寻找和处理与业务并不相关的漏洞，却忽略了许多对业务构成最大风险的、最关键的漏洞。

传统的漏洞管理是基于 IT 合规的，目标是满足合规要求的，然而合规仅仅是最基本的要求，仅满足合规的漏洞管理存在诸多风险。这种管理方式往往只关注传统 IT 资产，对于漏洞的认识是静态的，对漏洞的分类参照 CVSS 进行纯技术层面的评价，不考虑漏洞与业务的关系。

对比传统的漏洞管理方式，RBVM 具有以下特点：

（1）RBVM 是面向风险的，其管理目标在于最大限度的降低风险。

（2）RBVM 更关注整个攻击面，它认为漏洞的风险是在随时变化的。

（3）RBVM 更关注业务环境，需要结合业务和攻击面对漏洞进行等级评定。

3.4 攻击面管理（ASM）的重要支撑

攻击面管理（ASM）指的是以攻击者的角度对企业数字资产攻击面进行检测发现、分析研判、情报预警、响应处置和持续监控的一种资产安全性管理方法，其最大特性就是以外部攻击者视角来审视企业所有资产

可被利用的攻击可能性。从 2018 年 Gartner 首次提出攻击面管理的概念以来，ASM 的理念迅速被整个安全行业所接受。RBVM 与 ASM 关系紧密，不可分割，RBVM 是 ASM 的重要支撑，RBVM 的发展，客观推动 ASM 理念的落地实施，而 ASM 理念被广泛的认可又带动了 RBVM 的发展。

（1）ASM 与 RBVM 的管理理念具有统一的管理对象。ASM 追求的攻击面管理是指未经授权即能访问和利用企业数字资产的所有潜在入口的总和，包括未经授权的可访问的硬件、软件、云资产和数据资产等；同样也包括人员管理、技术管理、业务流程存在的安全漏洞和缺陷等，即存在可能会被攻击者利用并造成损失的潜在风险。RBVM 也不是针对某一部分 IT 资产，而是企业或组织内部所有管辖的 IT 资产。因此，二者具有统一的管理对象。

（2）RBVM 的核心技术是 ASM 的重要技术支撑。RBVM 的核心技术是漏洞优先级排序（Vulnerability Prioritization Technology，VPT）。Gartner 在《Hype Cycle for Security Operations，2021》中共有 5 个相关技术点：外部攻击面管理（EASM）、网络资产攻击面管理（CAASM）、数字风险保护服务（DRPS）、漏洞评估（VA）、弱点 / 漏洞优先级技术（VPT）。可见 VPT 技术是 ASM 技术的关键支撑，RBVM 的应用带动 VPT 技术的发展，而 VPT 技术又推动 ASM 的发展。

（3）RBVM 是实施 ASM 的核

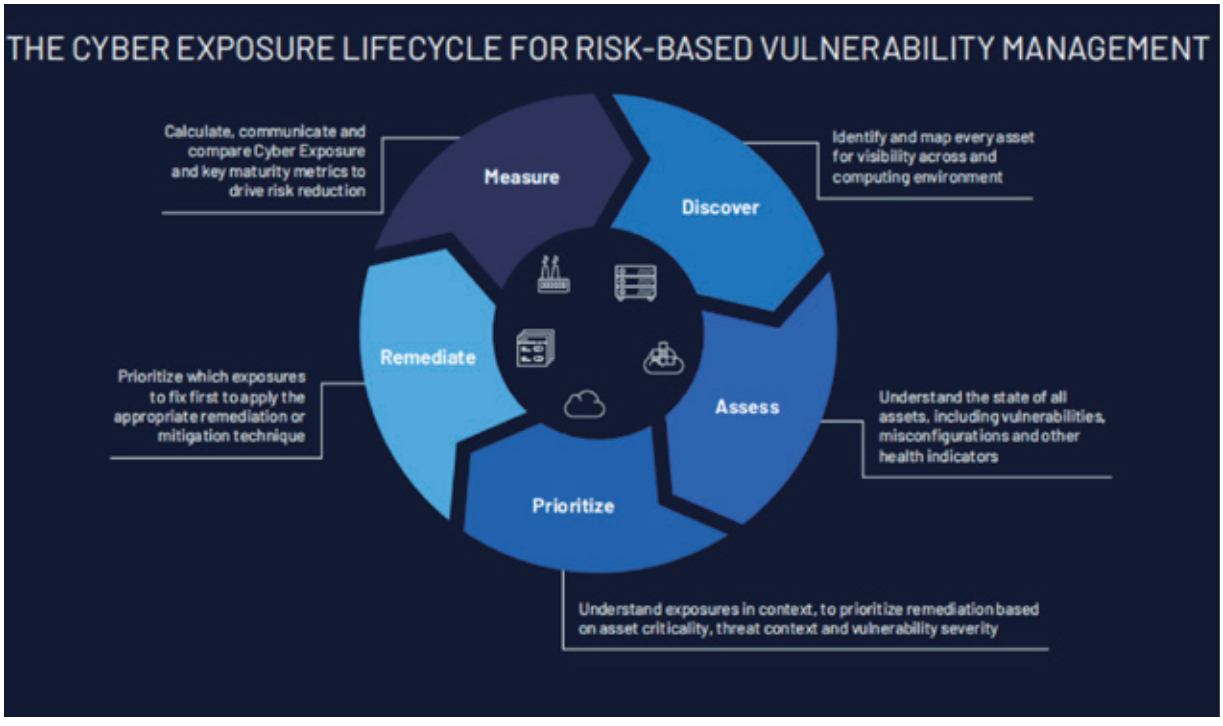


图 4 基于风险的漏洞管理生命周期

心流程之一。ASM 由四个核心流程组成：资产发现、分类和优先级排序、修复及监控。其中漏洞优先级排序即 RBVM 是 ASM 的关键实施步骤。

3.5 RBVM 的实施路径

相比传统的漏洞管理方法，基于风险的漏洞管理策略是更全面的解决方案。如图 4 所示，主要分为五个步骤：发现（Discover）、评估（Assess）、优先级排序（Prioritize）、修复（Remediate）、度量（Measure），每一个步骤使用一组特定的工具和技术。

3.5.1 资产发现（Discover）

（1）识别企业的业务状况。通过识别企业的业务状况来确定服务的关键性和应用程序的优先级。同时，还要建立、评估现有系统的安全性，选择合适的 IT 策略和流程。

（2）部署合适的网络扫描设备，编制实施策略。考虑到 IT 环境的复杂性、多样性（如局域网、公有云、OT、容器环境），应注意选择合适的扫描设备（如在局域网络中使用的漏洞扫描设备可能无法在云环境使用）。同时，因为基于风险的漏洞管理策略是一个组织性工作，而不是 IT 部门一个部门的工作，因此在编制实施策略时，应注意将企业的全部相关部门都纳入进去。

（3）总揽全局。应尽量全面的将整个攻击涉及到的所有资产全部纳入扫描范围，扫描策略应覆盖到所有子网。

3.5.2 风险评估（Assess）

这一步的核心是开展全面风险评估，就是要对整个攻击面的漏洞进行评估，包括云、OT 和容器环境中的任何资产（包括瞬时资产），同时应注意 3 方面问题：

（1）不能仅仅满足于行业监管的合规要求，因为通过行业监管的审核并不意味着企业就安全了，评估的标准是安全，而不是合规。

（2）评估计划中应包括整个攻击面，同时应该有足够的评估频度，因为攻击者会时刻扫描我们的网络环境，一旦发现薄弱环节，马上开始攻击。

（3）时刻记住威胁是动态的、不断变化的，因此所有的策略、情报、计划都应该是动态适应的。

3.5.3 确定优先顺序（Prioritize）

（1）对漏洞和资产排序

传统的漏洞管理方法是使用通用漏洞评分系统（CVSS）来优先修复哪些漏洞，这种方式的最大问题是没有考虑到对业务的风险。此外，大多数企业只使用 CVSS 的基础得分，而不管威胁环境的变化如何。在基于风险的漏洞管理方式中，在关注漏洞的同时，要充分了解受关键漏洞影响的资产，因为，一旦在最重要的 IT 资产上发现最高风险的漏洞，那么它必然是最高优先级的。

（2）评估风险

要有效地对风险最大的漏洞进行优先排序，就需要了解每个漏洞的完整上下文，可以在 CVSS 标准使用之前结合其他因素，比如，威胁情报（攻击源、当前攻击者的活动情况、可疑的 IP 地址）、漏洞详情（漏洞持续时间、漏洞被利用的程度、威胁被发现的频率）等，有了每个漏洞的完整上下文，安全团队就能够专注于最重要的资产和漏洞。

以 IBM 的安全团队 X-Force Red 为例，X-Force Red 要从每天发现的数十万个漏洞中找出哪些漏洞需要首先修复。图 5 是 X-Force Red 的漏洞排序示意图，其中最关键的漏洞处于金子塔的顶端，排名基于漏洞是否被武器化、暴露资产的价值和关键程度。

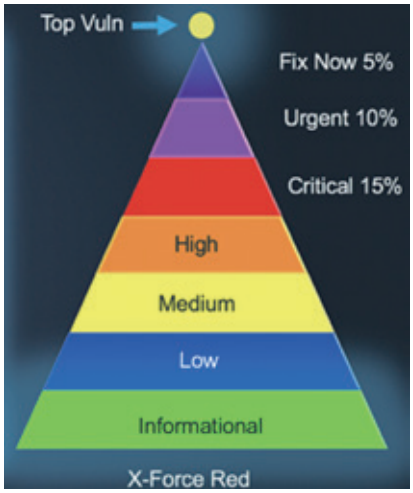


图 5 X-Force Red 的漏洞排序示意图

3.5.4 修复（Remediate）

通过上一阶段制定的措施管理风险，开展漏洞修复工作。一旦确定了哪些漏洞是最高优先级，就需要采取适当的行动来有效地管理风险。对于每个漏洞，都有 3 个响应选项——补救、减轻或接受。

1. 补救。通常情况下，可以使用补丁安装的方式进行漏洞修复。但需要注意的是，补丁只是修复漏洞这项工作的一部分。修复漏洞工作还可能是资产撤销或重建，操作系统或特定的软件组件可能需要升级，或者可能存在需要纠正的配置错误。一旦漏洞被验证已被完全修复，与漏洞相关的风险将完全从环境中消除。

2. 缓解。缓解是指采用其他技术来降低特定脆弱性的风险。例如，可以使用防火墙规则进行阻断，防止攻

击者利用漏洞访问敏感数据。

3. 接受。风险接受是指有意识地决定不采取任何行动。这样做可能有多种原因，例如，修复的成本大于漏洞被利用的成本。在这种情况下企业选择接受风险，但风险并未被消除，它依然存在。

3.5.5 度量（Measure）

最后，需要制定能够衡量流程完整性的关键性能指标，以及业务指标，以评价基于风险的漏洞管理程序的价值。具体如下。

1. 过程完整性指标：扫描覆盖率、扫描频率、扫描深度、平均评估时间（MTTA）和平均补救时间（MTTR）等指标。

2. 业务风险指标：需要长期跟踪组织的总体风险指标，并为每个区域、办公室、业务单元或资产组维护单独的指标。

3. 评估成熟度指标：为了确保风险度量基于高度可信的数据，需要了解安全程序的成熟度。如果安全评估缺乏足够的广度或深度，那么网络中很可能存在盲点，从而导致关键资产上的漏洞被忽视。

4. 标杆指标：将风险水平与行业同行进行比较，从而帮助安全团队真正了解其工作状况。

这些指标的好处是有两方面的。首先，它们帮助安全团队更深入地了解他们的安全计划的有效性，并突出需要改进的地方。其次，可以用来定期向管理层报告团队的进展，并能够清晰的表现出工作的情况。简言之，提高安全团队的工作效率，提升工作效果，赢得管理层的信任。

四、RBVM 带来三大转变

RBVM 方法的正确性和实用性已经得到验证，随着它在业界的普及，将会给企业的漏洞管理带来以下转变:

1. 漏洞优先级排序将成为解决当前漏洞问题的关键。基于风险的漏洞管理将被越来越多的企业所接受。通过使用最新的威胁情报、自动化、机器学习等手段，将使得漏洞管理更加精确、快捷，可以确定在恶意软件或有针对性的攻击中，攻击者最有可能使用哪些漏洞。

2. 资产重要性分析将成为漏洞管理的必然要求。在新的漏洞管理理念中，如果不了解受威胁资产的重要性，就无法准确评估风险，资产管理和资产的重要性分析成为漏洞管理的必然要求。

3. 制定个性化的漏洞管理计划将成为漏洞管理的目标。每个组织应该制定个性化的漏洞管理目标，比如，减少补救工作量、降低风险、减少数据噪音，提高自动化和进行实时洞察。安

> RBVM 方法的正确性和实用性已经得到验证，
> 随着其普及，
> 将会给漏洞管理带来转变。

奇安信的漏洞管理实践

作者 | 武鑫

随着攻击向量扩大和漏洞增加，漏洞管理成为安全解决方案的最前沿，成为风险管理的重要组成。安全团队面临两难：安全漏洞数量激增、无处不在，安全预算却在减少和安全人才持续短缺，修补每年发现的惊人安全漏洞简直遥不可及的任务，简单的发现和修复模式已经难以为继。

奇安信经过多年总结与实践，针对已知漏洞和未知漏洞风险管理，形成了自己的完善的体系。

1 背景介绍

安全漏洞一直被视作企业的入口，以各种形式存在于企业信息资产的方方面面，稍有不慎，安全防线就可能被击破。通过从组建漏洞管理团队、在现有大流程中设计漏洞管理流程、增加漏洞发现方法、建立漏洞管理闭环流程、形成漏洞复盘机制、构建漏洞评价体系、推动漏洞发现转向漏洞预防等 7 个方面，对企业的安全漏洞进行全面、深度的治理。

2 管理实践

2.1 漏洞管理团队

漏洞涉及的范围广泛，故管理难度也非常大。通过建立专项工作组、部门 BP 制度、安全团队内部分工等方式，为漏洞管理提供最有力的支撑。

2.1.1 集团级管理团队

· **专项工作组：**无论是建立虚拟或实体的工作组，都应该自上而下，需要包括产品、开发、测试、运维、安全等不同角色的人员。各企业中相关岗位可能已经有一定的组织，那么在建设专项工作组时优先考虑将其纳入或联系其主要成员加入，如下图所示的研发委员会、安全委员会等。明确该岗位的工作目标与工作职责，比如，研发需要对自己所写程序的安全质量负责，主动学习安全人员提供的开发安全规范、进行开发安全考试、在编码时安装安全 IDE 插件进行安全检查、编码完成后触发静态代码安全扫描工具进行安全检测、针对安全检测结果联动安全人员进行漏洞确认与修复、在运营阶段若是发现产品编码相关漏洞需要及时响应与修复。

· **部门 BP 制度：**建立部门的安全接口人，负责对接安全人员上传和下达消息、在本部门落地相关安全要求。建立的机制依旧是从上往下，通过专项工作组发通知给各部门的负责人，由负责人亲自指定并声明该部分工作的重要性，争取对接口人有一定的考核权，让安全工作正式成为接口人职责的一部分。前期可对接口人的配合情况和工作质量进行排名、正向反馈，最终需要落

实到绩效考核上。安全接口人需要对部门内部的产品、研发、测试人员进行联动、驱动，承接部门漏洞的管理职责。

2.1.2 部门级管理团队

为了保证各项安全活动有效落地，安全团队内部可根据安全活动不同的方向设置团队，包括安全防护、安全运营和产品安全团队，内部的漏洞管理工作也主要是由这三个团队负责。

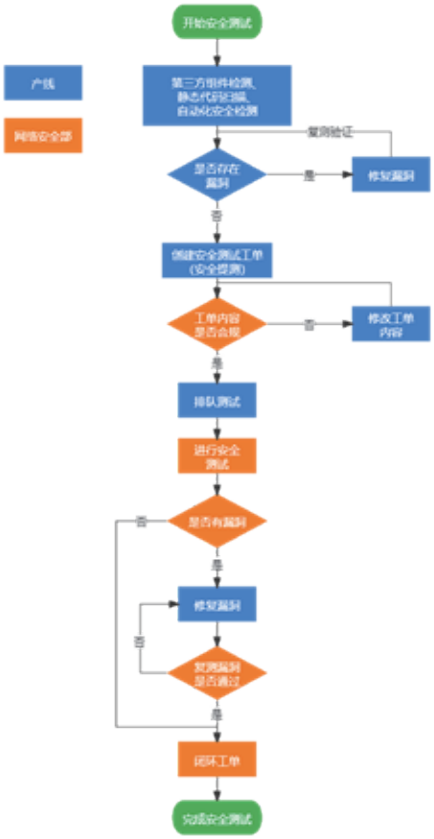
- 在安全防护团队中，设置专岗人员进行资产信息收集与识别、最新漏洞跟进分析、编写 POC、执行漏洞扫描等工作；
- 在安全运营团队中，安全运营人员通过日常安全设备的告警，发现漏洞并提交漏洞工单；
- 在产品安全团队中，负责产品上线前的安全测试及 SRC 运营，通过引入白盒测试、黑盒测试和灰盒测试等方法发现并推动漏洞修复。

2.2 漏洞管理嵌入流程

因为漏洞很多，故发现的方式也比较多。但如何才能持久、高效、有效地发现并管理漏洞呢？在经过长期实践之后，总结出以下两点漏洞管理方式，最核心的思想就是“嵌入现有的一切流程”中。

2.2.1 漏洞管理融入开发流程

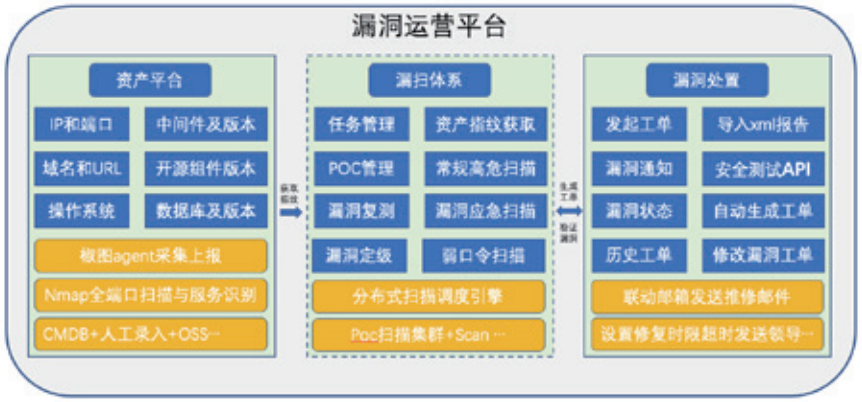
为进一步提升产品与信息系统的自身安全能力，防止产品与信息系统带严重、高危和中危漏洞上线，有效减小集团信息安全事件发生的概率。在产品发布节点上设置安全卡点，未经过安全提测或安全提测结果不达标的产线，将被禁止发布上线。同时由于安全人员有限，将部分安全测试能力融入到产品中，交由产线来完成，以此保障该措施能够落地。基于开发流程的安全测试流程，如下所示。



最开始的节点始于产线，在完成自主安全测试并漏洞修复后，可进行安全提测；产线提交安全提测工单后，进入排队待测试状态；安全测试人员分配到安全提测工单后，进入测试中状态；安全测试完成后，由产线进行漏洞修复，提测工单状态为修复中；漏洞修复完毕并经过安全测试人员验证，提测工单状态为安全测试通过。

2.2.2 漏洞管理联动资产管理流程

> 安全漏洞一直被视作企业的入口，
> 以各种形式存在于企业信息资产的方方面面，
> 稍有不慎安全防线就可能被击破。



无论是漏洞的发现，亦或是漏洞的修复，均需要明确存在漏洞的资产归属情况，故资产管理是漏洞管理的另一个基础。基于资产（操作系统 / 应用 / 组件）进行漏洞扫描，可以提升扫描效率、降低网络流量；基于资产（重要级别 / 网络位置）进行漏洞修复判断，可以提高必修的漏洞修复率；基于资产（使用人 / 运维负责人 / 安全负责人）进行漏洞修复推动，可以提高整体的漏洞修复率。以下为漏洞运营平台结构图，清晰地展示了与资产管理的紧密联系。

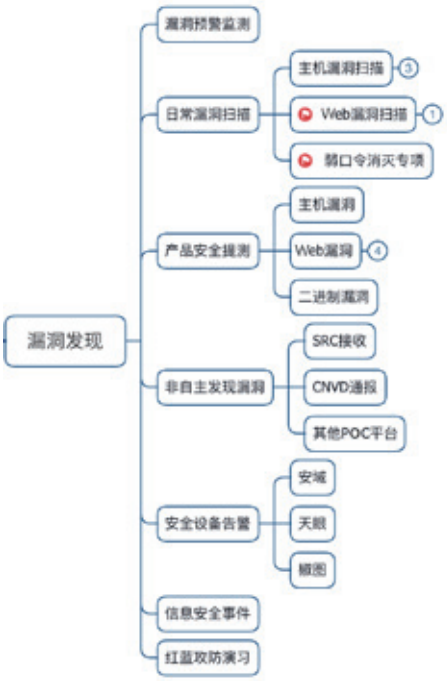
2.3 漏洞发现方法

2.3.1 漏洞预警监测

通过从安全媒介、软件官网、国内外漏洞平台、社交软件等途径，实时获取漏洞情报信息、漏洞利用信息等，结合公司的信息资产对内进行预警。对于银行、证券、运营商等行业，还会收到来自上级监管单位的漏洞预警通知。常见的漏洞监测情报包括 CNVD、CNNVD、CVE Details、CVE 等漏洞平台；可以是 freebuf、安全脉搏等安全媒介；还可以是微信朋友圈、twitter 等社交软件。

对漏洞情报的处理，是接收到漏洞情报后应立即开展的工作，也是对安全人员对自身资产熟悉情况、对新漏洞理解的考验。通常若漏洞有 CVSS 评分，则可以直接关注 7.0 分及以上的漏洞，进一步还需要结合以下几个维度进行综合评估。

- 漏洞利用危害程度：漏洞被利用后造成的直接危害；
- 漏洞利用难易程度：有无公开 POC、EXP，是否需要登录等；
- 受漏洞影响资产的属性：资产所在网络位置（公网或内网）、资产重要程度（重要系统或一般系统）；



- 监管或上级单位发文通知的漏洞（非普适）；
- 漏洞修复成本和对业务的影响。

2.3.2 日常漏洞扫描

定期使用扫描器对资产进行主机漏洞和 Web 漏洞扫描，是较为常见发现线上系统安全漏洞的方式之一。扫描频率和扫描规则决定漏洞的发现能力，扫描频率原则上在能覆盖所有资产的基础上越频繁越好，扫描规则需要根据漏洞情报或厂商及时更新。在常见的漏洞工具中，无论是系统还是 Web 层面，一般都支持登录扫描，但以此带来影响业务的风险也随之增大，特别是实时性要求很高的业务系统对扫描比较敏感，所以在进行扫描前需要注意以下事项。

- 扫描器地址加白：扫描器的地址加白包含两层意思，一是在一些特殊的网段或业务系统放行扫描请求，实现覆盖率全局覆盖；另一方面是在安全防护设备上添加白名单，防止被安全设备拦截导致扫描无果，同时也减少扫描时产生的大量告警，避免给安全运营带来巨大的工作量，已知的扫描告警淹没掉有真正攻击的有价值的告警。
- 设置扫描时间窗口：从扫描类型（系统 /Web 漏洞）和扫描目标（内网 / 外网系统）进行区分，设置每天扫描开始和结束的时间，每月 / 每季度的扫描频率，在制定的时间内进行扫描工作。
- 扫描前通知业务方：将制定的扫描任务与计划在开始前，同步到业务方并获得其统一，可以提高扫描时出现线上故障的处置效率。另外有一些业务系统也会反馈不能扫描，需要添加扫描的白名单。
- 留意加白业务系统：针对扫描加白的业务系统，可以通过进一步确定扫描作业开始时间、加大扫描周期、扫描

一比一的测试 / 预发环境、根据系统架构等基础信息进行精细化扫描等多种方式来发现漏洞，防止因为加白而导致的扫描盲点。

• 多款扫描器交叉扫描：不同扫描器的规则（能力）不一致，对漏洞的检出能力也有所差异。从黑客攻击、上级单位扫描检查等角度出发，需要将常见的扫描器加入到扫描武器库中，实现漏洞在被人发现之前先发现，掌握一定主动权。

• 对扫描器的操作进行审计：由于在网络和防护层面都对扫描器开放，扫描器上已知漏洞也属于公司的重要资产信息，需要对扫描器的登录、登出、扫描任务制定等关键操作进行审计，做到事后可取证追溯。

2.3.3 产品安全提测

业务上线前进行安全测试，基本已经成为拥有安全人员的企业必做安全工作之一，也是漏洞发现的主要来源。通过建立安全提测流程，设置业务上线卡点和安全质量要求，促使业务上线前都来进行安全测试并进行漏洞修复。

下面介绍几种常见的安全测试模式，不同企业一般都是有一种或几种搭配组合的。

• 黑盒主动漏扫：这应该是最常见的发现漏洞方式，也常常作为安全测试中的安全基线，使用工具通过爬虫获取待检测系统的 API，加载各类 payload 进行漏洞扫描，包括主机漏洞扫描和 Web 漏洞扫描。主机漏洞扫描器基本都是商用的，如 Nessus、绿盟 RSAS 等；Web 漏洞主动式扫描工具种类较多，包括耳熟能详的 AWVS、w3af、Nikto、OWASP_ZAP 等，大多都可通过开源方式获得。黑盒主动漏扫能发现常见的漏洞，但是在覆盖面方面存在一定的不足，就 Web 漏扫而言，针对单个链接的孤岛因为爬虫找不到路径、使用防重放一次失效 token 的页面等，通常会检测不到。

• 黑盒被动漏扫：相对于主动方式的漏洞扫描而言，被动漏扫最大的区别就是获取的 URL 来源不同，一般包括通过流量提取和日志解析。在功能测试时或者线上环境产生的流量中，提取待测系统的 URL、去重、加载 payload、重放进行安全测试，从而覆盖到用户能接触到的所有系统功能。至于工具方面，以商业和大型互联网公司自研两种形态为主；另外也出现一些社区版的产品，如 xray；半自动化的工具 Burpsuite + 自研漏洞插件进行漏洞扫描。

• 白盒安全测试：在安全测试领域，静态代码扫描通常作为安全测试在开发安全生命周期中左移一步的重要标识。通过对代码进行安全扫描，可丰富被发现的安全漏洞的种类，比如，除了常见的 SQL 注入、XSS、CSRF 等 owasp top10 类型，还能检出硬编码密码、不安全的随机数、日志伪造、路径操纵等类型的漏洞。

• 手工安全测试：无论是黑盒还是白盒安全测试，工具发现的漏洞总是有限的，都需要人工的参与。在逻辑漏洞、敏感信息泄露类、有一定防范但可被绕过类漏洞方面，检出率存在短板，往往需要人工根据经验、结合实际的业务场景进行手工分析测试。

• 交互式安全测试：IAST 技术将

> 漏洞管理难度非常大。
> 通过建立专项工作组、部门 BP 制度、
> 安全团队内部分工等方式，
> 为漏洞管理提供最有力的支撑。

白盒和黑盒安全测试的能力进行融合，能将漏洞定位到代码层面，漏洞检出率高、误报率极低，甚至能做到不产生脏数据（IAST 的 Passive 插桩技术）。在 DevSecOps 日益推行的今天，IAST 必将是安全测试技术的发展方向。

2.3.4 非自主发现漏洞

漏洞悬赏最开始流行在国外的 HackerOne、Bugcrow 等平台，到国内主要以漏洞平台和 SRC 的形式落地。各大互联网公司也纷纷建立 SRC，对外收集自家产品与信息系统及主流产品的 0day 漏洞，往往也能收到不少高价值的漏洞。

SRC 作为企业安全团队对外宣传、接收漏洞的官方渠道，既能够起到沟通桥梁的作用，又可以通过接收到的漏洞反向优化安全防护策略。建设 SRC 早的企业，各类规则完善、人气高，基本拥有一群稳定的白帽子为其挖洞，白帽子也对业务越来越熟悉，也能发现更多有质量的安全漏洞。对于新建的 SRC，则需要通过不断的运营活动来提升行业影响力，吸引更多的白帽子加入。

• SRC 建立：包括门户建立、漏洞接收范围确定、奖励机制确定等。

一是门户的建立，作为一个对外的门户，可以自研也可以通过国内的一些漏洞平台建立企业 SRC，漏洞平台的好处是有一定的白帽子基础、运营机制，相比较自研会更加高效快速上线，但也存在定制化功能和效果不佳的弊端。若是自研，可借助开源的程序进行修改，如 SRCMS、腾讯 xSRC（开源版）。值得注意的是，如果使用开源方案，则需要持续关注平台本身的漏洞情况，目前已经被发现不少安全漏洞。

二是确定漏洞接收范围，仅限于主域名的子域名，还是包括所有与公司相关的资产漏洞？ SRC 经常会接收到内部已知管理资产外的资产漏洞，白帽子的能力不容小觑，为避免发生争执需要提前明确。

三是设置有明显区别的漏洞奖励机制，可根据资产重要性、漏洞利用直接造成的影响、漏洞利用条件等进行评判。比如，核心系统可利用前台 SQL 注入漏洞的评级，应该比核心系统管理员之后可利用的 SQL 注入和一般系统前台可利用 SQL 注入高，对应的奖励机制也会更高。对于奖励机制，直接进行 RMB 奖励会更吸引白帽子的参与度。

• SRC 活动：漏洞接收数量直接取决于参与白帽子的数量，衍生开可能涉及平台影响力、奖励机制等因素。白帽子拉新、白帽子促活、每逢佳节奖金翻倍、月 / 季 / 年度额外奖励……需要有规划、有吸引力的发起线上或线下活动，保持与白帽子的联系。

• 其他事项：把跟白帽子的关系处理当做一项正式运营工作，给予白帽子感谢与尊重；注重在安全圈内的品牌，加入生态圈，与其他 SRC 一起活动，能吸引更多白帽子；制定内部漏洞审核和修复效率，别让线上漏洞暴露太久，也别让白帽子等待太久。

2.3.5 安全设备告警

企业一般都会部署安全设备，常见的有安全审计类，如堡垒机、日志审计系统、数据库审计系统；主动防御类，包括漏洞扫描系统、配置核查系统、IPS 等；被动防御类，有 WAF、IDS、主机安全防护软件……这些设备产生的告警除了能发现有人攻击，还能通过告警信息分析出信息系统的漏洞。以内部流量分析系统，举例进行说明：在镜像到流量分析系统前进行 SSL 证书卸载，一切将变得透明化。网络中的攻击、请求包中的弱口令，在流量系统上将得到还原，通过其可以发现应用层之外的网络攻击情况。下图为通过流量分析的方式发现系统存在弱口令。

2.3.6 信息安全事件

信息安全事件的发生，往往是最不愿意看到的，但也是不得不直面与不可避免的。通过复盘信息安全事件来发现漏洞，进行同类漏洞纵向（比如，信息安全事件由 redis 未授权访问导致，在进行复盘时对全网的 redis 服务进行未授权访问和弱口令排查）和横向（比如，信息安全事件还是由 redis 未授权访问导致，则可以扩展到对 resync、memcache、ftp、Jenkins、solr 等可能存在的服务进行排查）治理，发挥事件的最大价值。

2.3.7 红蓝攻防演习

类似于信息安全事件，红蓝攻防演示目标则更明确，偏重于漏洞链的组合利用，通过漏洞不断向目标一步步靠近，对于蓝队来说是很大的挑战，也是一次

不错的对防守能力、应急处置能力的检验。

红队即攻击发起方，通常会通过网站、VPN、邮件系统、Web 应用漏洞打开入口，结合对内部员工发邮件、即时通信的钓鱼攻击，以及物理攻击、供应链攻击等方式进入内网并获取权限，在内网攻击域控、堡垒机、云平台、单点登录系统、集中运维管理平台等重要系统，以点打面扩大战果。

对于蓝队，则需要通过各安全设备监测到的异常进行快速处置和分析，尽可能早的发现红队的攻击，制止并掐断攻击路线。在整个攻防过程中，漏洞的利用不可或缺，通过红蓝攻防演示也能收到很多不错的漏洞利用链。

2.4 漏洞验证与闭环

2.4.1 漏洞验证

漏洞验证主要是指对从外部接收到的漏洞进行测试，判断是否真的存在，由安全工程师进行，需要业务方配合提供环境、协作、确定及评估漏洞影响程度。

为保证漏洞的真实性和有效性，在发现漏洞之后进行验证十分有必要，可避免将不存在的漏洞直接推送给业务方，给安全团队带来不专业、权威性削减等负面影响。通常已经确定不需要进行验证的情况包括安全测试、漏洞情报、漏洞扫描，需要进行漏洞验证的场景有以下几种。

> 无论是漏洞的发现，亦或是漏洞的修复，均需要明确存在漏洞的资产归属情况，故资产管理是漏洞管理的另一个基础。

- 安全设备告警：一次漏洞挖掘与利用攻击会带来很多数据包及告警信息，根据 SourceAddress 和 DisnationAddress 进行聚合分析，结合 response 情况判断出存在漏洞的参数、payload、漏洞类型，并在对应的环境中进行验证。
- 信息安全事件：从安全事件中提取防护体系中的漏洞，可能是技术上的也可能是管理上的，针对技术层面的漏洞发现需要分析日志来确定，并从攻击者的角度对漏洞进行还原，确定漏洞真实存在。
- 红蓝攻防演习：红蓝对抗中的漏洞也一样，除了分析各类日志，由于是公司自己的红队，还会提供详细的漏洞报告，在此基础上验证漏洞更加快速、有效。
- 外部提交漏洞：外部提交的漏洞存在描述信息不详细、逻辑思维混乱、截图不全等情况，在安全人员进行验证时比较苦恼，为避免出现该类情况，需要和白帽子沟通补全信息，在制定 SRC 奖励规则时也需要将提交高质量报告考虑进去。然而，对于从 CNVD 上、其他 POC 平台上收到的漏洞信息，较难以控制。

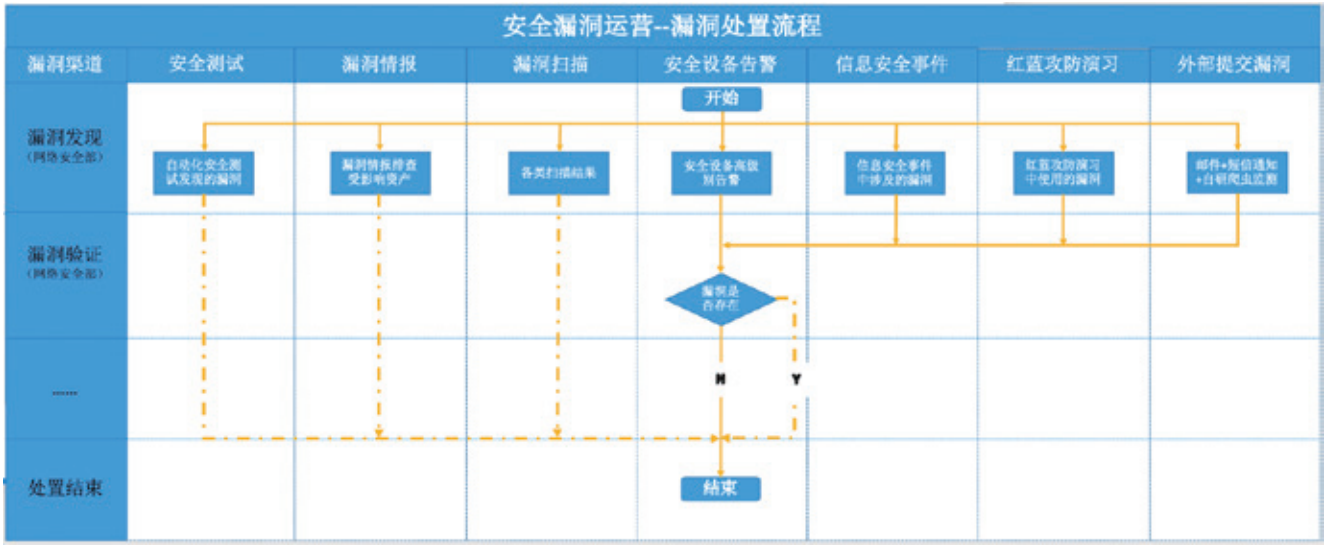
在漏洞验证前，充分理解 POC，尽量做到无损，避免影响线上业务的正常运行。在漏洞验证时，尽可能排除本机 POC 运行环境、网络环境等因素带来的干扰。

2.4.2 漏洞闭环

漏洞的管理重点在发现方法，难点在漏洞闭环，只有当漏洞被修复才是最终目的。当业务方完成修复的反馈后，安全人员接下来要对漏洞进行复测验证。

在进行漏洞复测时，需注意：

- 要求在漏洞相应处备注修复方法



甚至贴修复代码截图；

• 关注修复方案或补丁可能带来的安全缺陷；

• 确认修复后的代码已经提交到仓库，并且更新到待验证的环境；

• 把开发说的话当作不可信的输入，不能不验证就关闭漏洞；

• 严重与高危漏洞，须在生产环境中跟进验证。

2.5 漏洞复盘机制

漏洞复盘主要是指通过对漏洞产生的原因进行分析、验证安全防护检测的有效性及漏洞修复情况，从而将漏洞的价值发挥到最大化，以此提升纵深安全的防护能力。

2.5.1 复盘范围

通常的复盘工作，大多是由于信息安全事件触发，关注范围仅是造成安全事件或通过外部渠道接收的漏洞，却忽视了内部主动发现的漏洞。然而，内部发现的漏洞往往是最多的，复盘价值高，很有必要性。

2.5.2 复盘关注点

对漏洞产生的根本原因进行分析，应该考虑系统安全基线是否存在问题、安全配置是否正确，安全开发规范落实情况、安全设计培训效果等。从需求设计、功能实现、配置上线等程序开发的最初环节进行分析，相比较设置的各个安全活动，并细化到每个安全活动的落地情况。

当漏洞被发现时，就意味着安全策略的绕过或失效。以被外部发现安全漏洞为例，追溯到漏洞产生的源头，回顾漏洞被触发的整个过程，并寻找预期与实际情况的差距。

• 基础安全加固：漏洞所在服务器的系统服务、所使用 Web 框架是否按照安全基线要求进行配置？若无，则应分析出具体原因并进行覆盖；若有，则要查看执行细节、反馈完善现有安全基线模板。

• 应用安全测试：漏洞发生的系统，在上线前是否经过安全提测？若无，需要分析出被旁路的原因并重新规划设置卡点；若有，则关注漏洞是否已经被发现（包括已发现未修复的原因、未发现的原因）并制定补强措施反馈到现有工作。

• 安全设备能力：漏洞在被测试及利用时，现有设备是否产生告警，包括 waf 攻击事件告警、流量分析系统告警、主机安全防护事件告警？若无，需要检测安全设备的覆盖情况并进行部署与安装；若有，则需验证安全设备真实的检测能力并通过新增规则、开启功能等进行防护。此外安全设备产生告警的运营及处置及时性也特别重要，应设置完善的 SOP 进行管理。

2.6 漏洞评价体系

CVSS（Common Vulnerability Scoring System，通用评估漏洞方法），是业界公认的漏洞评估方法，通过对漏洞进行打分将其分为严重（Critical）、高（High）、中（Medium）、

漏洞等级	计算分值	备注
严重（Critical）	9.0~10.0	重点关注
高（High）	7.0~8.9	需要关注
中（Medium）	4.0~6.9	无需关注
低（Low）	0~3.9	无需关注

低（Low）四个级别。

但在实际的漏洞管理工作中，除非是客户或合作伙伴有所要求，一般会由于考量指标过多、企业安全人员能力有限等诸多因素而难以落地。从攻击者的角度出发，通常可以结合漏洞利用难易程度（包括 POC/EXP 是否公开，漏洞触发条件，如是否需要登录认证后才能触发漏洞）和漏洞风险等级（指漏洞被利用时，对其所在主机产生的直接影响，比如 CVE-2020-1947 ShardingSphere 4.0.0 及以下版本存在反序列化漏洞，直接导致远程命令执行，造成影响较大）。对漏洞分为如下四个等级。

- 严重（Critical）：漏洞利用条件简单、单个漏洞直接影响大；
- 高危（High）：漏洞利用条件有一定门槛，如需要登录、单个漏洞直接影响大；
- 中危（Medium）：漏洞利用条件较难，须在一定环境下、单个漏洞直接影响大；或漏洞利用条件简单、单个漏洞直接影响不大；
- 低危（Low）：漏洞利用条件苛刻、单个漏洞直接影响小；或漏洞利用简单、单个漏洞直接影响极小。

在漏洞的推动修复过程中，往往还应加上资产属性这一维度。资产属性包括互联网侧资产、内网重要信息系统、内网其他信息资产，在进行加固修复时优先级依次降低。

2.7 漏洞管理转向预防

在造成安全事件前，发现漏洞并修复成本会降低；在引入或开发过程前期，发现漏洞并修复漏洞成本会更低。此外切断漏洞的利用链，也是漏洞管理中降低成本的常见有效方法之一。因此对于在引入漏洞前或当时，制定一些消减措施变得十分有必要。

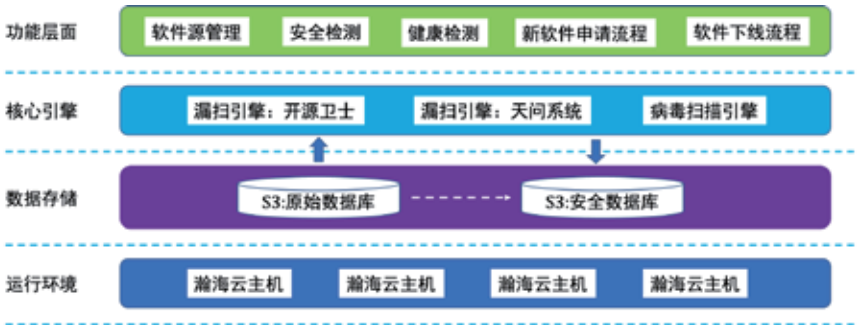
2.7.1 制定安全基线

尤其是第三方开源软件，存在较多的未授权、默认口令和已知可利用的 CVE 漏洞。在使用前，依据 CIS 制定企业级的安全基线，提供给产品线或直接定期维护软件库、镜像源，保障初始状态是默认安全的。在实践中，内部建立了开源软件运营平台来实现这一功能，架构图如下所示。

2.7.2 引入安全组件

在安全测试中，经过对安全测试的结果进行分析发现：漏洞主要集中在几类安全漏洞，包括 SQL 注入、XSS、文件上传、OGNL 表达式注入、OS 命令注入、Nashorn 引擎脚本（任意

> 在造成安全事件前，
> 发现漏洞并修复成本会降低；
> 在引入或开发过程前期，
> 发现漏洞并修复漏洞成本会更低。



开源软件运营平台

代码执行）、csrf、XXE、不安全的解压缩等。为了提升产线的漏洞修复效率，在漏洞修复阶段给其提供相关的安全组件，从而减轻开发的工作量。但最主要的还是要求产品线在编码时，引入这些安全组件，在静态代码时进行检验，确保正确使用安全组件，在编码阶段解决常见的漏洞。

3 风险控制

3.1 漏洞扫描事故

3.1.1 Web 漏洞扫描邮件通知

至少保证在进行漏洞扫描的前一天，对资产 owner 进行邮件通知，并标明扫描资产和联系方式。

3.1.2 弱口令消灭专项蓝信群报备

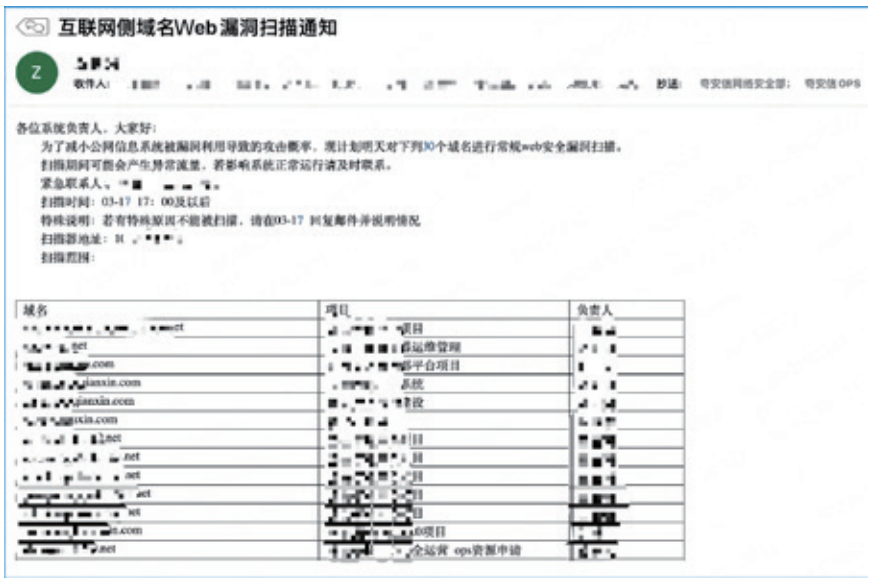
为了防止网络设备被扫描并进行账密枚举而导致账号被锁，在安全运营、OPS+SEC+IT 联署等蓝信群进行报备。

3.2 漏洞验证事故

禁用对系统或服务有严重攻击行为（影响业务连续性）的 exp 在生产环境验证或利用漏洞。

4、结语

漏洞管理是每个企业必定会遇到的安全工作之一，做好漏洞运营工作能在极大程度上减少攻击。本文就漏洞的发现、验证、修复、复测、复盘进行了详细阐述，基本覆盖了漏洞治理生命周期中的各个阶段。将“发现－推修－验证－复盘”闭环机制融入开发流程和资产管理运营体系，收敛已知漏洞安全风险；将安全左移至源头，引入安全组件、安全基线实现内部环境的默认安全，降低未知的漏洞风险，实现漏洞从被动救火转向主动防御阶段。最终，实现消除网络攻击入口，降低核心资产漏洞风险的目标，提升政企机构应对各类网络攻击的能力。安



零信任向前：数字工作未来已来

作者 | 魏开元

众所周知，信任可以决定很多事情。

如果家长信任一名老师，会想方设法把孩子送到这名老师的班上；如果患者信任一名医生，会准点守在挂号软件上，抢这名医生的专家号；如果领导信任一名下属，会把相对重要的工作交给这名下属去完成……

但信任不会凭空出现。通常情况下，信任可以来源于一纸身份证明，如身份证、教师资格证、机动车驾驶证；可以来源于资历年限，高年资的主任医师总是更容易受到患者的信任；可以来源于评价口碑，从电商平台刷单、刷评论就可见一斑；甚至可以来源于一道“墙”，墙内的网络会被认为是可信的，而墙外的互联网被认为充满了危险。

这道墙把网络划分成为外网和内网，由防火墙、IDS、WAF 等一众“保安”把守，墙外面被称作是外网，谁能进来不能进来，要看保安信任与否；墙里面则是内网，核心业务、核心数据都在这儿。

不法者的“自助餐”：信任危机

2004 年，安全圈出现了一个“奇怪”的声音——“去边界化”：以防火墙为代表的传统边界安全设备已经成为网络发展的阻碍，应该将企业网中的边界消灭。

此言一出，立即引起了不小的争议。很多人都觉得，边界没有了，企业网络那不是谁想进来就进来了？

这话要放在当时那个个人 PC 还没有普及的年代，确实有点超前。没有云计算，没有移动互联网，甚至连信息化都是一个非常新鲜的玩意。企业内部网络就是一个封闭的局域网，上班老老实实来公司就行，远程办公？想都没想过。

在广泛的质疑声中，这件事情也就不了了之了。至少在没有新技术可以取代的情况下，应当维持现状。

但大家其实都心知肚明，信任不总是正确的，尤其是这种靠网络位置来区分信任度的办法。保安不可能长着一双火眼金睛，无法识别出所有不值得信任的家伙。

2009 年，一次名为“极光行动”的网络攻击打疼了谷歌：攻击者利用钓

鱼攻击等手段，向内部植入了木马软件，从而监听、窃取关键账户的登录凭证，攻击者则利用这些窃取到的凭证登录到敏感系统中，执行最终的窃密工作。

这就像开自助餐厅的老板，只要顾客交钱（取得信任）就可以进来随便吃，至于食客有没有浪费食材、有没有私底下打包，这些事情确实很难限制。偶尔一次两次可以睁一只眼闭一只眼，数量多了餐厅非倒闭不可，必须加以限制。

但企业不一样，数据安全泄露事件有一次就受不了，这件事也在事实上引发了谷歌对于网络访问的信任危机，并逐渐蔓延至网络上的各个角落。

信任就像一面镜子，碎掉了是难以重圆的，零信任的魔盒就此打开。

从不信任，持续验证

2010 年，分析机构 Forrester 正式提出了零信任理念，其核心在于“Never Trust，Always Verify”，从不信任，持续验证，不再以内外网来区分信任度。

“网络攻击手段日新月异，针对身份和权限的攻击手段日渐成为主要形式。”奇安信零信任事业部总经理张泽洲表示，传统安全模型基于网络制定安全策略，难以应对针对身份、应用和数据的安全威胁。

与此同时，谷歌绝对属于给力的行动派。

从 2011 年开始，谷歌花费数年时间，打造了其内部的零信任项目 BeyondCorp，成为了行业内第一家“吃螃蟹”的公司。用户必须使用由谷歌提供且持续管理的设备，通过身份认证，且符合访问控制引擎中的策略要求，才能通过专门的访问代理访问特定的公司内部资源。

很难想象，一个 10 年前就上马的项目，时至今日依然是最成功的零信任落地项目之一，成为众多企业争相学习的对象。

但话又说回来，BeyondCorp 或者说零信任的成功，有着独特的历史背景。

其一，云计算尤其是公有云的成功，改变了企业 IT 资源的部署方式，业务系统除了部署在内部网络，还会部署在公有云上，靠城墙把所有关键业务和数据围起来已经难以实现。

谷歌更不用多说，云计算就是 2006 年谷歌自己提出来的；而现在大家熟知的云计算 3A（亚马逊 AWS、微软 Azure 和阿里云）也先后走上正轨。

其二，移动互联网的普及，改变了员工的办公习惯，移动设备办公逐渐被人们接受，没有人会一直呆在公司里使用内网，单纯依靠网络位置区分信任度，已经成为制约办公效率的绊脚石。

上述两点大大削弱了网络边界对于信任的影响力，不管是作为访问者的人，还是作为被访问者的核心业务系统或者数据，都在内外网之间“反复横跳”。

随着 BeyondCorp 的成功，零信任作为保护企业网络安全的重要力量，正式登上了历史舞台。

> 零信任策略强调以数据为中心，
> 以身份为基石，基于多维属性构建动态策略；
> 同时实现多点精细检控，
> 进行持续评估并实时调整。

破局：安全从 0 开始

短暂的喧嚣过后，市场重新静了下来。

相比零信任，彼时安全圈有一个“更靓的仔”，叫检测与响应。

这是有原因的。实施零信任道阻且长，相比之下部署几台设备、安装几个软件要容易很多。

更何况，网络安全的本质是攻防双方的对抗，没有一位防守专家会认为，自己的技术就是不如攻击者，凭什么你的攻击手法我就检测不出来?

那几年，几乎所有的安全公司，都希望在检测与响应技术上取得突破。

变化出现在 2018 年。

2018 年，奇安信干了两件事情。第一，提出安全从 0 开始，对于 0 的解释有很多，零信任就是其中一个，并正式面向市场发布了奇安信零信任安全架构与整体解决方案；第二，旗下身份安全实验室翻译了《零信任网络：在不可信网络中构建安全系统》这本书，首次在国内全场景展现了零信任架构的独特魅力。

“零信任策略强调以数据为中心，以身份为基石，基于多维属性构建动态策略；同时实现多点精细检控，进行持

续评估并实时调整。”作为 Forrester 认证的国内首位零信任战略专家，张泽洲的身影在内部培训、客户现场、会议中心之间“闪转腾挪”，为奇安信零信任战略站台。

奇安信的入局，仿佛推倒了第一块多米诺骨牌，打破了国内零信任市场的宁静，国内安全厂商纷纷下场。

与此同时，在太平洋的另一边，零信任市场的火热程度也不遑多让。

2019 年，RSAC 上主打零信任的厂商就逐渐开始增多，大致有 39 家。而到了 2020 年，RSAC 上打着零信任标签的厂商就已经有 91 家之多，零信任也因此成为了 RSAC 2020 热度增长最快的热词之一。

分歧与失败：谁才是零信任正统

很快，蜂拥而入的厂商们开始各显神通。

有人发现账号密码这种静态的身份认证方式不安全，所以打算在身份认证方面大做文章；有人觉得黑客在内网的横向渗透太过简单，所以希望在内网里，也加入足够细颗粒度的隔离和信任机制，避免黑客入侵由点及面迅速扩散……

美国国家标准与技术研究院 NIST 在其发布的《零信任架构》中，对实施零信任的常见技术路线进行了总结。

第一是软件定义边界 SDP。

早在 2013 年，云安全联盟 CSA 就提出了 SDP 的概念。SDP 强调在没有经过身份验证和授权之前，存储应用和数据的服务器都会隐藏在代理服务器后面，与此同时，代理服务器可以进行动态授信，只有通过验证才可以与服务器建立通信。

第二是增强型身份认证。

零信任强调总是验证。过去的身份验证偏向于静态单次验证，简单来说就是输入账密，验证通过后即可建立信任关系。增强型身份认证则不在局限于静态账号密码，而是基于大数据等技术，对用户的各类行为数据进行动态分析，综合判定用户身份是否合法。

第三是微隔离。

通俗来讲，微隔离就是将隔离的颗粒度无限缩小，小到每一个应用、每一个进程之间都应该隔离开，而应用与应用之间的每一次通信，都应该被验证是可信的，从而确保加入某个应用被攻破，不会迅速传播至其他应用。

从市场来看，上述三种技术路线都涌现了大批追随者。许多原本生产单一技术产品的厂商纷纷宣称自己为零信任产品供应商，而类似零信任就等于几种技术的叠加的误解也让零信任市场还没有真正成熟就陷入到了不少争议之中。

总之，在铺天盖地的炒作下，迅速掀起了一股零信任替代的热潮。

首当其冲的就是 VPN。

VPN 全称虚拟专用网络，其意义

就在于在内网和外网之间，搭建一条专用的虚拟网络，方便身处外网的用户可以访问内网资源。

显而易见，VPN 是外网用户与内网资源建立信任的关键。作为边界信任时代的产物，当企业对内外网一视同仁的时候，VPN 就成了一个可有可无的角色。

还是在 2019 年，Gartner 就预测到 2023 年，有 60% 的企业将逐步淘汰大部分 VPN，转而使用 ZTNA（零信任网络访问）。

或许是受到了这句预言的刺激，在相当一段时间内，用所谓的新技术、新产品搞 VPN 替代，似乎就成为了零信任的同义词，仿佛零信任的终极目标就是干掉 VPN。

黎明：内生安全

干着干着，逐渐有人发现了问题。

比如，替换了传统的 VPN，却迎来了一个新的“VPN”，而所谓的零信任项目也只是在网络访问上，保证了内外网信任的一致性，并没有进一步根据实际业务需求，赋予动态的访问权限，这就和传统 VPN 别无二致；再如，过度追求对访问用户身份的反复验证，却忽略了用户的实际使用体验，使得员工对于零信任策略产生抵抗心里……

“ZTNA 当然可以被说成是更好的网络访问产品，但 ZTNA 不等于就是零信任，而搞所谓的 VPN 替代，并不是零信任。”张泽洲说，技术本身可以解决很多单点问题，但零信任是网络安全信任模型新范式，并不是单点技术问题，更不是搞所谓的 VPN 替代。”

如果应用几个新技术、装几套新软件就是零信任，谷歌压根不用玩五六年。被单点技术、单一产品一叶障目，零信任就变味了。

一位不愿透露姓名的 CSO 解释道：“我们实施零信任战略的目标，是为了解决边界信任模型下，因业务开放和内网的过渡信任所带来的安全风险，而不是向我们的员工展示，你看公司用的这个新技术到底有多炫酷。”

很多产品都声称可以帮助客户实现零信任，但事实上，每家企业的业务相差甚远、IT 环境各不相同、工作方式也不一样，如果不能清晰地了解自身的零信任建设需求，零信任项目自然难以取得成功。

说直白一点，技术是技术，业务是业务，这俩根本没穿一条裤子。技术再好，跟业务没穿一条裤子，也遮不住时代进步在业务身上留下的伤疤。

为了解决这个问题，2019 年，奇安信在北京网络安全大会期间正式提出了内生安全，其核心就是业务安全和网络安全合一，确保业务持续稳定。

张泽洲认为，零信任架构聚焦身份、信任、访问控制、权限等维度的安全能力，而这些安全能力也是任何信息化业务系统不可或缺的组成部分，所以零信任本应该是内生的。

基于内生安全理念，奇安信形成了以身份为基石、业务安全访问、持续信任评估、动态访问控制这四大核心零信任能力。

2020 年 8 月，奇安信牵头发起的国家标准《信息安全技术 零信任参考体系架构》正式获得立项，这是零信任领域的首个国家标准。

数字工作，未来已来

就在奇安信提出内生安全后不久，一个席卷全球的黑天鹅事件强行改变了零信任的发展进程。

对大多数人来说，对数字化变革的切身体验从未像 2020 年新冠疫情爆发以来这般强烈。居家办公、远程访问成为新常态，各类“无接触”新业态争相冒头。

站在网络安全的角度，每上线一个新的系统，就等于为攻击者多提供了一个攻击目标，尤其是因为远程办公导致业务系统不得不对外开放。

这对于尚未准备好的公司来说，是一次艰难的选择：前进一步，网络安全

没有保障；退后一步，正常业务便难以为继。

而且，即便是有良好的网络安全和零信任网络访问基础，这事儿也不是一路绿灯。

比如，以前只要管一朵云，现在需要适配多云和复杂终端环境；以前的业务应用相对单一，现在需要覆盖本地应用、小程序、API、微服务等复杂应用形态；以前业务系统上线时间以年计算，而现在需要按月甚至按周计算……

“时至今日，零信任的外延依然在不断向外扩展。”张泽洲强调，数字化工作成为新常态，应用场景、IT 环境的变化，零信任要做的事情远不止其内涵强调的“从不相信，始终验证”这么简单。

如果站在业务视角去重新思考网络安全挑战，零信任架构将重点去解决三个方面的问题。

首先是“重”。对于任何一家企业而言，一味追求反复的身份验证，只会使得身份认证流程过于“沉重”，员工登录不同的系统需要多次重复输入账号密码，用户体验极差。如果身份验证策略强度过高，会导致员工对相关制度的反感甚至抵抗；而强度如果过低，则极易导致账户被破解。

其次是“乱”。不同的工作会使用不同的软件，比如，报销使用财务系统、招聘使用人力系统、销售使用 CRM 系统……不同的员工使用不同的系统，其权限分配十分复杂；而且使用非可信来源工具、应用也屡见不鲜，员工自行下载安装各类工作软件，来源不明，容易导致恶意软件入侵，给企业数据造成极大安全隐患。

最后是“险”。传统的边界信任模型自然不必多说，静态的安全策略、粗颗粒度的管控手段，很难对业务数据进行有效的管控和安全防护。而且即便是企业采用零信任架构，如果不能全面覆盖新应用和新业务，如微服务、API 等，依然会导致企业面临着巨大的数据泄露风险。

在这一点上，奇安信率先迈出了一步：基于零信任构建安全的数字化工作入口，发布“奇安天信零信任工作系统”。

用张泽洲的话来说，奇安天信是真正构建在业务系统之上的，零信任本该长成这个样子。

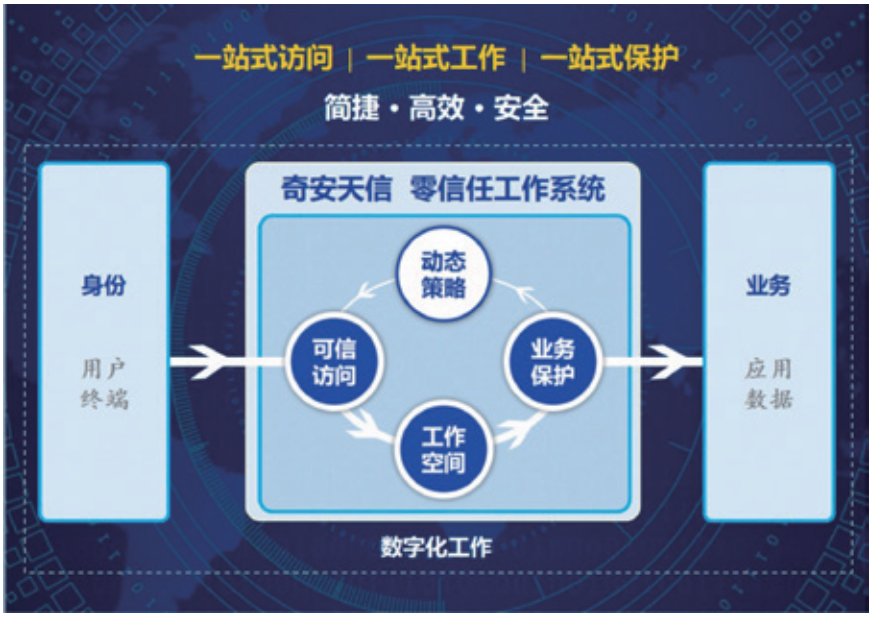
第一是通过一站式访问，告别烦复。奇安天信改变了过去反复登录、多次认证的复杂工作模式，通过自适应多维身份认证，确保人员可信；通过安全终端管控，持续环境感知评估，确保设备可信；通过全场景业务流量代理，确保流量可信；通过动态最小权限业务访问，确保访问可信。

第二是通过一站式工作，告别杂乱。奇安天信基于场景化、集中式工作环境，通过统一资源访问门户，实现业务访问简便易用；而轻量化应用商店更让工作软件随手可得。在协同方面，通过对接业务信息流，实现业务协同高效便捷；通过对各类终端、各种操作系统的全面兼容，使得工作体验无缝跨屏，满足远程、移动等各种场景需求……一系列一体化、协同化的设计，让企业的数字化工作拥抱轻简、效率倍增。

第三是通过一站式保护，告别风险。奇安天信在业务保护方面，在遵循零信任四大关键能力的基础上，全面应用奇安信在终端、应用、数据安全等多个方面的安全能力，如终端管控、代码审计、高级威胁检测等，围绕工作空间构建隔离、加固、纵深管控的全链条业务安全保护能力。

这正是数字工作的未来，未来已来。

在2023年北京网络安全大会上，奇安信集团董事长齐向东表示，数智安全要以内生为本，自我进化，从关注 IT 转变成关注业务、从关注设备转变成关注“人”、从关注建设转变成关注运营，而这正是零信任不断前进的方向。安



规划一步快一步

奇安信 | BEIJING 2022

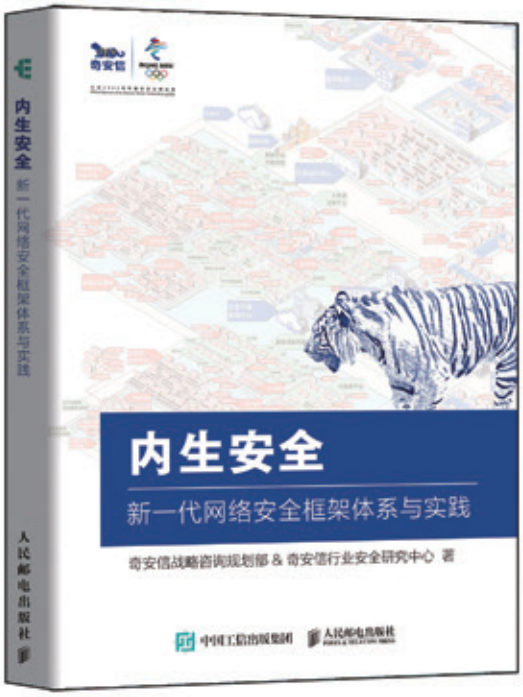
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

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

复盘：奥运史上最复杂数据安全项目实践之路

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，服务八大类客户群，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 年伦敦奥运会、2016 年里约奥运会、2020 年东京奥运会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。“相比于终端、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，其可以分为四级：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。

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。

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

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类分级，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，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。

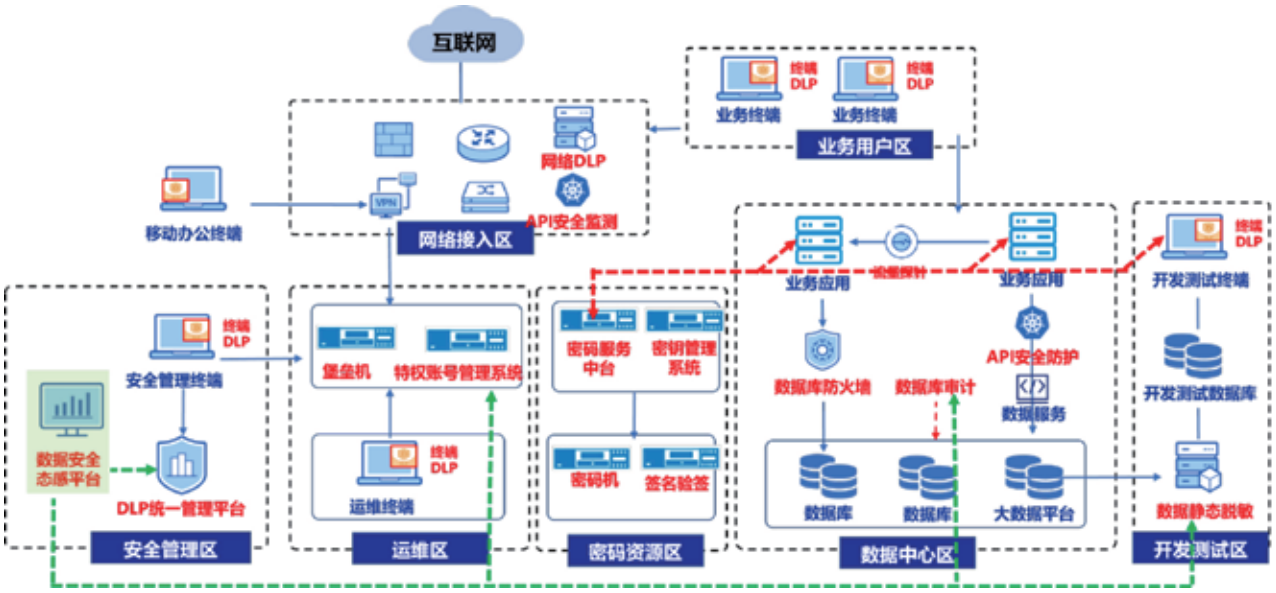
冬奥业务系统和网络部署多种监测组件，并依托数据安全管控平台，最终实现数据流转全链路风险监测。

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

图：冬奥风险关联分析及综合研判



图：冬奥数据安全产品部署图

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，确保冬奥数据资产的安全。

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”，成为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

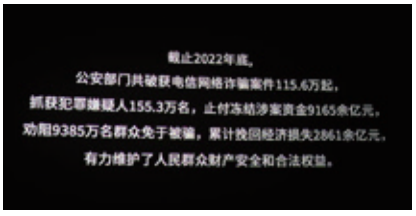
揭秘《孤注一掷》中的黑产现实图景，电子数据鉴定助力反诈！

作者 | 奇安盘古司法鉴定 徐子颖

近期，电影《孤注一掷》上映。影片中，受害者与犯罪者的界限变得模糊，每个人都在赌局中“孤注一掷”，希望能够赢得那仅存的一线生机。

反诈警察的一句“风险比贩毒小，利润比贩毒高，能不嚣张吗？”，对当前的跨境诈骗情况作了极为尖锐的描绘。

在传统情境中，一个赌桌上可能仅容纳 10 人，但在互联网时代，赌局规模可以无限扩大、更能跨越国界。互联网带来了时代的进步，也滋养了诈骗的天堂。据统计，公安机关仅一年内就破获了高达 115.6 万起电信网络诈骗案，逮捕犯罪嫌疑人 153.6 万人，并冻结了近万亿元的涉案资金。



图源《孤注一掷》片尾

诈骗背后隐藏的产业链深度和复杂度，已远超大多数人的想象。鉴于此，电子数据司法鉴定显得至关重要，它能帮我们追踪犯罪者、识别涉案网站并深入分析交易数据。奇安信司法鉴定曾深度参与众多赌博、诈骗与传销案件中的鉴定工作，我们希望通过本文，向大众深入展示跨境诈骗产业链的真实运作模式，并分享我们的实践经验，助力社会更好地认知与应对。

01 起底跨境诈骗产业链

近年来，我们所面对的不再仅仅是孤立的赌博或诈骗事件，而是一个系统化、产业化的跨境诈骗链条，从前期的人员招募，到信息搜集、资料制作、实施诈骗，再到后期的资金洗白、持续推广，每个环节都经过精心设计和高效执行。同时，新型技术与专业人才的加持，极大程度地提高了其隐蔽性与运作效率。接下来，将详细介绍产业链的各个环节，揭露其背后的

运作逻辑和策略。

1、缅北电诈园如何招募人员？

缅北与中国云南接壤，有着长达2000多公里的边界线，语言、生活方式与云南几乎如出一辙：汉语是官方语言，人民币在市场上流通，连电信网络使用的都是中国的，完美匹配了电诈团伙的需求。正因如此，缅北的电诈产业园如雨后春笋般涌现，以缅甸的妙瓦底KK园区为例，仅这一个园区就占地10平方公里，聚集了超过200家赌场和数万雇员。

图源网络

据媒体报道，除了KK园区，还有AA园区、14园区、亨利园区等众多园区散落于缅甸各地，参与这一行业的人数，达到了惊人的10万之众。

问题来了，这近10万的从业人员是怎么召集起来的？

通常，电诈团伙会以免费的出入境服务、往返机票、住宿、休闲旅游及诱人的高薪工作为饵，招揽国人出境参赌或为境外赌博服务，进而通过暴力、毒品等方式控制其人身自由，胁迫其参与违法犯罪。

在电影《孤注一掷》中，程序员潘生和模特安娜的遭遇，就是这种悲剧的生动写照，他们受到了海外高薪工作的诱惑，却不料落入了缅北诈骗工厂的深渊。

2、“千门八将”如何实施诈骗？

缅北的诈骗网络工厂以其严格的组织架构和明确的工作分工著称。千门八将「正、提、反、脱、风、火、除、谣」有条不紊地进行着“诈骗业务”：情报员风将搜集目标关键信息，程序员正将编写专属骗局程序，布局者提将用“内幕消息”获得受害者信任，而火将则用武力确保整个团队的“业务”顺利进行。

影片中，程序员潘生和模特安娜为了脱身，以赌博引诱大学生阿天陷入骗局，致使其损失近千万。接下来将详细介绍影片中的潘生和安娜在这场骗局中所扮演的角色：正将与提将。

· 正将：创造诈骗网站

正将，是诈骗工厂中的技术核心，主要负责创建和维护伪装为合法的赌博网站或钓鱼网站。为了进一步混淆视听，这些网站常常被伪装成线上棋牌游戏，其中涉及的资金流转都被伪装为游戏充值，从而极大地增强了其隐蔽性，使监管机构难以发觉。

图源网络

影片中，无论是博彩、赌球，还是虚拟币交易平台，都是由潘生这样的“正将”精心构建的。而背后的所有赔率、胜率都被人为操控，保证平台始终获利。此外，提现门槛被故意设定得很高，即使玩家赢得赌局，也难以从平台提取资金。

· 提将：引诱赌徒入局

有了网站，就需要有人去操作、去与受害者建立信任，这就是提将的

工作，他们精于人心，擅长通过对话读懂受害者的需求和心理状态。

影片中的安娜就是一名“提将”，其通过长时间的互动与赌徒阿天建立了信任，并利用这份信任声称自己拥有赌博网站的“内部信息”，从而诱骗阿天进行大额投注。这种策略的初期，为玩家提供一些小额胜利，使其放松警惕，然后在玩家投入大额资金时，就把钱尽数套走。

3、违法资金如何“人肉”洗白？

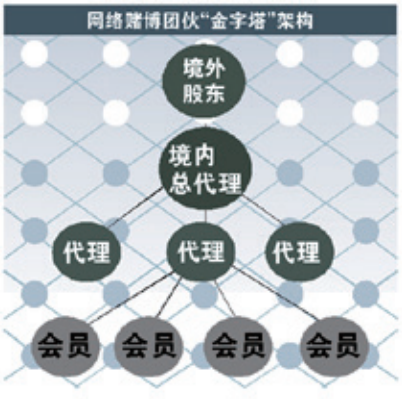
当受害者被骗取大量资金后，如何迅速且不留痕迹地转移这些资金就成为了诈骗团队的首要任务，这就是“洗钱”。随着科技的发展，洗钱的手段也日趋科技与隐蔽，通常包括“人头取款”“直播打赏”“话费慢充”等途径。

自动化控制手机转账，图源网络

影片中，随着赌徒阿天的 800 万转账到达，诈骗团伙头目一声号令“干活了”，随即，这笔巨额被迅速拆分到多个小额账户，通过“车手”前往 ATM 机进行取现，以规避警方的追踪，这种操作被称为“人头取款”。其中，技术组确保资金被自动分散到众多账户；刷机组将非法资金伪装成正规的营业收入；而取款组则专注于从银行取出现金，并从中抽取千分之五的提成。

4、参赌人员如何持续扩大？

近年来，网络赌博团队为追求更大的利润，采取了与传销类似的拓展策略，形成了一个层层递进、蔓延开来的参赌网络。



图源网络

这种模式下，赌博平台鼓励赌客成为代理，层层招募下级代理，进而构建起一个“金字塔”式的结构。为进一步激发代理的积极性，平台引入了返点制度，即代理能从其下线的赌资中提取一定比例的收益；而在多级代理链条中，上层还可以从其下层的提成中分得一杯羹。“金字塔”式的策略使得新的“下家”不断地被吸引进来，从而显著地扩大了参赌人员的规模。

02 电子数据鉴定助力打击

在网络诈骗产业链的迅速扩张中，其犯罪模式已形成一个错综复杂的网络结构，将诈骗、赌博和传销三者融为一体。同时，基于网络技术的专业性、便捷性，网络诈骗变得愈发复杂，呈现出无边界、跨国界分布等特点，给传统取证策略带来极大的挑战。

在此背景下，电子数据司法鉴定的引入尤为关键。网络赌博大部分活动均在数字领域内展开，包括但不限于交易流水、通信记录、资金转移轨

迹等，这些都可能是查明真相的关键证据。电子数据司法鉴定不仅可以助力执法部门高效、准确地锁定和分析这些证据，还确保这些数据在司法程序中具备法律效应。本文将结合奇安信司法鉴定的实践案例，分享电子数据取证鉴定在其中的应用场景。

1、剖析诈骗软件，锁定罪犯身份

在网络诈骗案件中，诈骗软件常是关键证据，通过深入分析诈骗软件、服务器地址等信息，可以为追踪罪犯提供线索。

例如，在上海警方侦办的一起“空气币”诈骗案中，受害人向警方报案，称经微信群讲师推荐下载了某虚拟币交易 APP，并进行了大额投资，但无法提现。奇安信司法鉴定正是从这款诈骗 APP 入手，提取其签名文件并计算其 MD5 值。利用这一标识，团队成功追踪到与其关联的其他 APP，并进一步定位到开发者；同时通过分析涉案 APP 的后台控制网站后，确认了登录者的 IP 地址，最终帮助警方确认了涉案犯罪团伙身份。

2、网站及代码鉴定，提供关键证据

追踪到开发者仅是线索的开始，为确凿地证明其涉及犯罪还需要更具决定性的证据，通过对网站功能、代码、工单系统等进行分析鉴定，可确认网站是否涉及诈骗、赌博或其他非法行为，从而为调查提供关键证据支撑。

例如，在“空气币”诈骗案中，奇安信司法鉴定通过对“虚拟币”交易平台、工单系统、代码服务器及聊天记录鉴定分析，确认该平台交易功能不涉及实际交割，该涉案企业参与平台开发且事先知晓其用于诈骗。

3、数据库解密统计，揭示层级关系

在传销式的诈骗活动中，常会呈现出清晰的层级和组织结构。通过数据库的解密和统计分析，可以揭示其背后的网络关系。

以一宗涉及百亿资金的传销案为例，奇安信司法鉴定成功地协助警方解读并深入分析了大量的数据库记录。经过数据库的完整还原、密文内钱包地址的解密、会员层级的计算，以及对虚拟货币和积分交易的统计分析等步骤，对包含百万账户及其附属层级和交易记录的涉案数据库进行了深入鉴定，成功揭示了这个传销网络的规模与运作方式，有效地辅助各地警方对超过 300 名涉案人员进行了准确打击。

4、充值与佣金分析，提供量刑依据

在诈骗和赌博活动中，经常涉及大量的资金流转。对这些资金的来源和去向进行分析，能够为公诉方在法庭上提供强有力的证据，并为量刑提供明确的依据。

以 2021 年信阳市特大跨境赌博案为例，奇安信司法鉴定对涉案赌博代理及跑分人员相关的账户进行了深入分析。针对赌博代理，梳理了超过百个账户的接收佣金总额及与下级会员的关联情况；针对跑分人员，梳理了充值、提现记录，并与警方提供的银行流水记录进行了仔细比对。经过这一系列的专业分析和鉴定，奇安信司法鉴定为公安部门编制并提交了超过百份的鉴定意见书，帮助警方确定犯罪分子非法获利的实际数额，为揭露涉案团队的组织架构、运营模式和资金流动路径，提供了有力的支撑。

结语

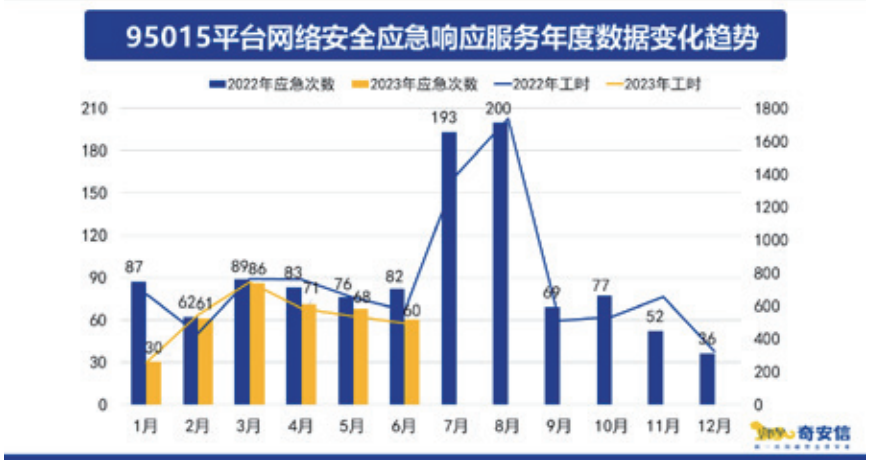
近年来，电信网络诈骗频发，诈骗的形式也日新月异，不断出现新的手法和新的变种，它们依托于现代科技与网络手段，深藏在复杂的网络交易中，极大地提升了侦查难度。

但幸运的是，在这个数字化时代，我们同样有更加先进的武器对抗这种犯罪。电子数据司法鉴定能够帮助揭示那些隐藏在数字背后的真相。其通过数据分析、功能鉴定等专业技术手段，协助警方追踪犯罪团伙、确定涉案金额、提供重要的证据支持，对于打击电信网络诈骗犯罪、保护公众权益具有巨大价值。

为了更有效地对抗日益猖獗的网络诈骗，奇安信司法鉴定将持续深化技术研究与应用，加强与执法部门的合作，为捍卫数字时代的公正与正义投入更多资源和智慧。安

《网络安全应急响应报告（上半年）》：国内政企机构安全运营能力严重不足

作者 | 奇安信安服团队



・政府部门、事业单位、金融行业是 2023 年上半年网络安全应急响应事件最为高发的行业。

・国内绝大多数政企机构在网络安全基础设施建设和网络安全运营能力方面存在严重不足。仅有 12.7% 的政企机构能够通过安全巡检提前发现问题，有 47.6% 的政企机构是在系统已经出现非常明显的入侵迹象后才进行报案求助的；有 33.8% 的政企机构是在被攻击者勒索之后才拨打 95015 的。

・内部人员违规操作触发的应急响应事件多达 98 起，约占 2023 年上半年 95015 服务平台接报事件总量的四分之一。

・以恶意程序为主要手段的网络攻击最为常见，占比为 34.3%。勒索病毒、挖矿木马、蠕虫病毒是攻击者使用最多的恶意程序类型，分别占到恶意程序攻击事件的 20.7%、12.0% 和 7.2%。

・弱口令是攻击者在 2023 年上半年利用最多的网络安全漏洞，相关应急事件多达 133 起，占比为 35.4%。其次是永恒之蓝漏洞，相关利用事件 84 起，占比为 22.3%。

第一部分 网络安全应急响应形势综述

2023 年 1-6 月，95015 服务平台共接到全国范围内网络安全应急响应事件 376 起，奇安信安服团队第一时间协助政企机构处置安全事故，确保了政企机构门户网站、数据库和重要业务系统等的持续安全稳定运行。

综合统计数据显示，在 2023 年上半年 376 起网络安全应急响应事件的处置中，奇安信安服团队累计投入工时为 3157.1 小时，折合为 394.6 人 / 天，处置一起应急事件平均用时 8.4 小时。其中，1 月份，因春节假期期间，应急响应处理量略有减少。

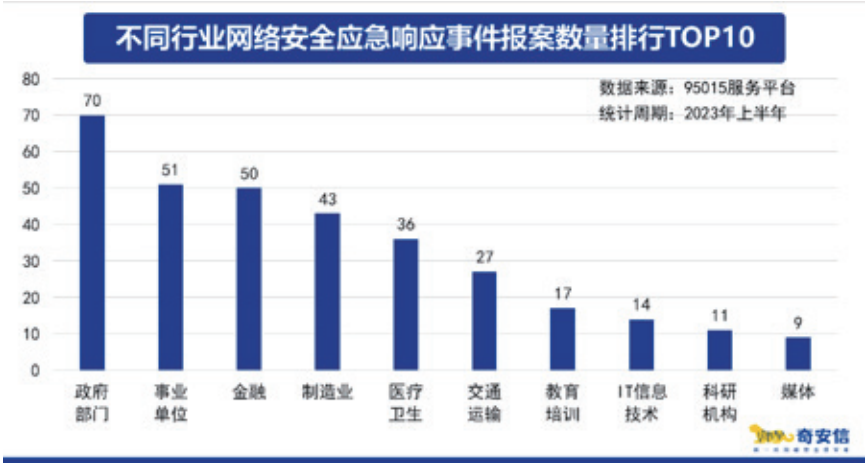
第二部分 应急响应事件受害者分析

本章将从网络安全应急响应事件受害者的视角出发，从行业分布、事件发现方式、影响范围及攻击行为造成的影响等几个方面，对 95015 服务平台 2023 年上半年接报的 376 起网络安全应急响应事件展开分析。

一、 行业分布

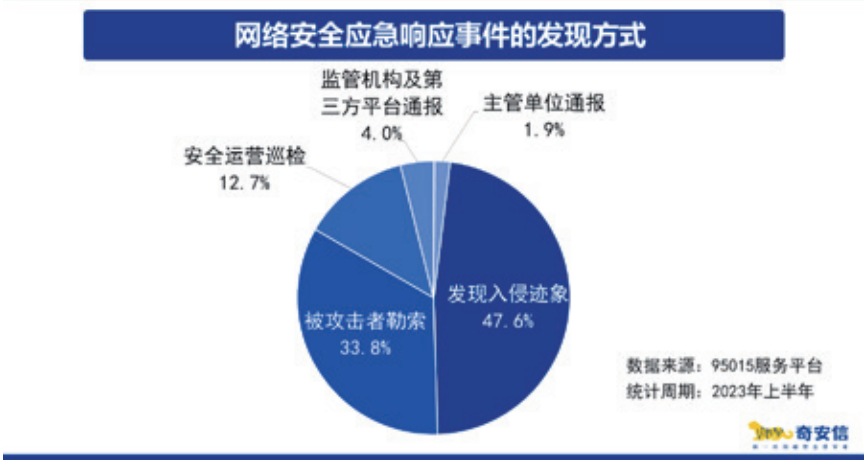
从行业分布来看，2023 年上半年，95015 服务平台接报的网络安全应急响应事件中，政府部门报告的事件最多，有 70 起，占比为 18.6%；其次是事业单位，有 51 起，占比为 13.6%；金融机构排第三，有 50 起，占比为 13.3%。此外，制造业、医疗机构、交通运输等行业也是网络安全应急响应事件高发行业。

下图给出了不同行业网络安全应急响应事件报案数量的 TOP10 排行。



二、事件发现

从安全事件的发现方式来看，有 47.6% 的政企机构才是在系统已经出现非常明显的入侵迹象后才进行报案求助的；有 33.8% 的政企机构是在被攻击者勒索之后才拨打 95015 网络安全服务热线的。这二者之和为 81.4%。



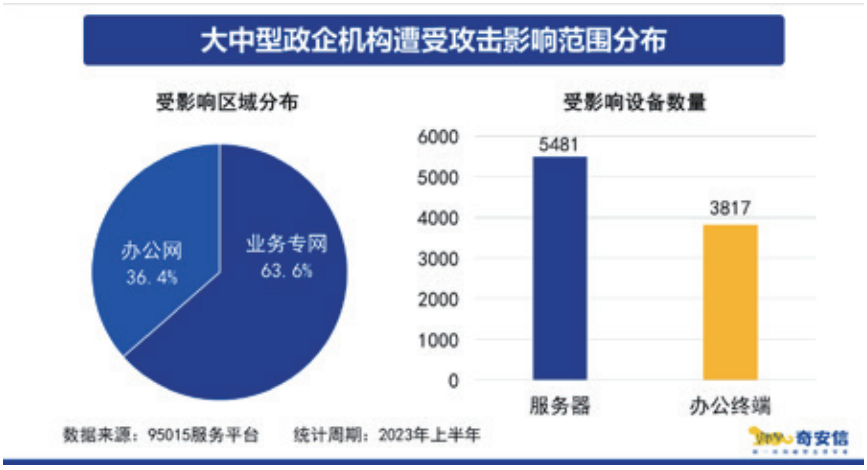
也就是说，八成左右的大中型政企机构是在系统已经遭到巨大损失甚至是不可逆的破坏后，才向专业机构进行求助。而真正能够通过安全运营巡检，在损失发生之前及时发现问题并呼救，避免损失发生的政企机构，占比仅为 12.7%。

此外，还有约 5.9% 的政企机构是在得到主管单位、监管机构及第三方平台的通报后才启动应急响应的。这些机构不仅严重缺乏有效的网络安全运营，也严重缺乏必要的威胁情报能力支撑，致使自己的主管单位或监管机构总是先于自己，发现自身的安全问题或被攻击现象。其中，某些通报可能还会使相关单位面临法律责任及行政处罚。这些被通报的政企机构都是潜在的定时炸弹，随时有可能爆发。

三、影响范围

网络安全事件往往会对 IT 及业务系统产生重大的影响。在 2023 年上半年 95015 服务平台接报处置的网络安全应急响应事件中，有 63.6% 的事件主要影响的是业务专网，而主要影响办公网的事件占比为 36.4%。从受网络安全事件影响的设备数量来看，失陷服务器为 5481 台，失陷办公终端为 3817 台。

2023 年上半年大中型政企机构遭受网络攻击事件的影响范围如下图所示。



在本报告中，办公网是指企业员工使用的台式机、笔记本电脑、打印机等设备组成基本办公网络，而业务专网泛指机构整体运行与对外支撑所需要的各种网络系统。

从影响范围和受影响设备数量可以看出，大中型政企机构的业务专网、服务器是网络攻击者攻击的主要目标。

大中型政企机构在对业务专网进行安全防护建设的同时，还应提高内部人员安全防范意识，加强对内网中办公终端、重要服务器的安全防护保障和数据安全管理。

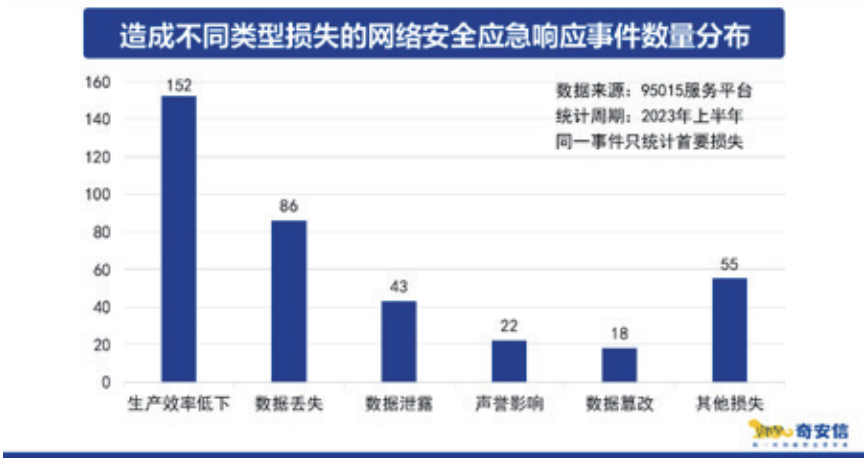
四、事件损失

网络安全事件通常都会引起政企机构不同程度、不同类型的损失。应急处置现场情况分析显示，在 95015 服务平台 2023 年上半年接报的 376 起报案中，有 152 起事件造成了相关机构的生产效率低下，占比为 40.4%，是排名第一的损失类型；其次是造成数据丢失的事件，有 86 起，占比为 22.9%，排名第二；造成数据泄漏的事件有 43 起，占比为 11.4%，排名第三；此外，造成政企机构声誉影响的事件有 22 起，造成数据被篡改的事件有 18 起。

特别说明，在上述统计中，同一事件只计算一次，我们只统计每起事件造成的最主要的损失类型。

造成生产效率低下的主要原因是挖矿、蠕虫、木马等攻击手段，使服务器 CPU 占用率过高，造成生产效率降低。也有部分企业是因为勒索病毒攻击造成了部分生产系统停产。

造成数据丢失的原因是多方面的，其中，因勒索病毒加密而导致数据无法恢复是首要原因。造成数据泄露的主要原因是黑客的入侵和内部人员的泄密。



第三部分 应急响应事件攻击者分析

本章将从网络安全应急响应事件攻击者的视角出发，从攻击意图、攻击类型、恶意程序和漏洞利用等几个方面，对 95015 服务平台 2023 年上半年接报的 376 起网络安全应急响应事件展开分析。

一、攻击意图

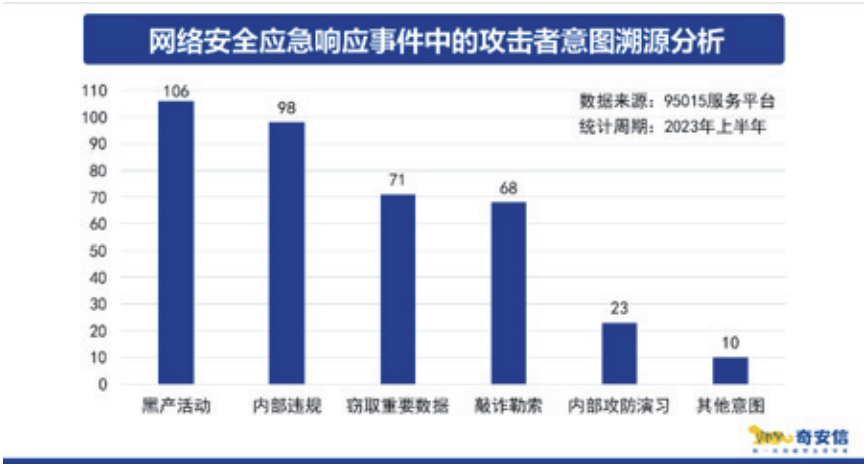
攻击者是出于何种目的发起的网络攻击呢？应急人员在对网络安全事件进行溯源分析过程中发现，2023 年上半年，内部人员为了方便工作等原因进行违规操作，进而导致系统出现故障或被入侵，触发应急响应的网络安全事件多达 98 起。这一数量仅次于

黑产活动（106 起）、超过了窃取重要数据（71 起）和敲诈勒索（68 起）等为目的的外部网络攻击事件的数量。

在这里，黑产活动以境内团伙为主，主要是指通过黑词黑链、钓鱼页面、挖矿程序等攻击手段开展黑产活动牟取暴利。

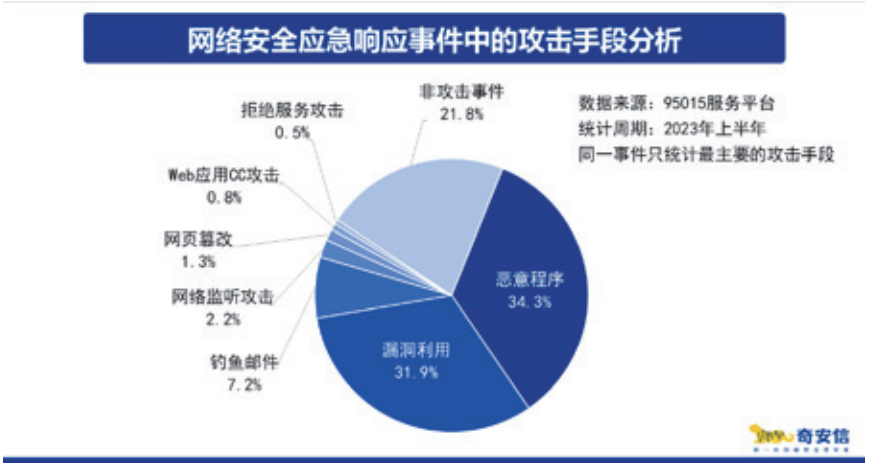
以窃取重要数据为目的的攻击，一般分为两种：一种是民间黑客非法入侵政企机构内部系统盗取敏感、重要数据，如个人信息、账号密码等；另一种则是商业间谍活动或APT活动。从实际情况来看，第一种情况更为普遍，第二种情况偶尔会发生。

敲诈勒索，主要是指攻击者利用勒索软件攻击政企机构的终端和服务器，进而实施勒索。此类攻击几乎全部是由境外攻击者发起，打击难度极大。



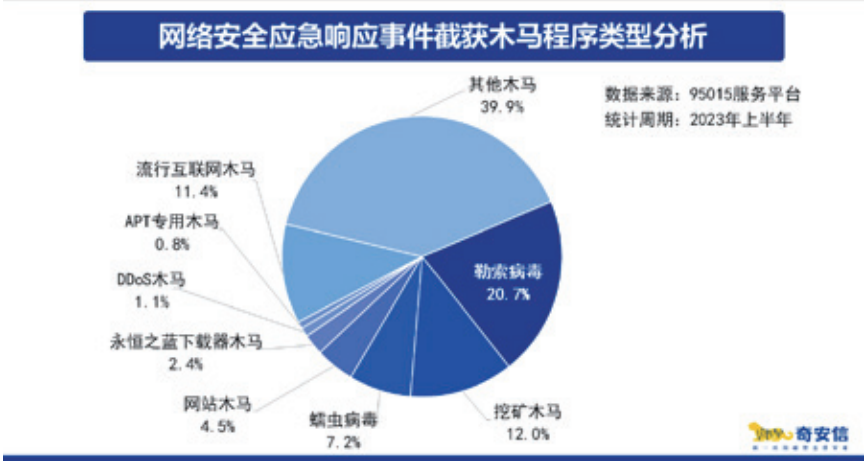
二、攻击手段

不同的安全事件，攻击者所使用的攻击手段也有所不同。通过对 2023 年上半年的网络安全应急响应事件分析发现，以恶意程序为主要手段的网络攻击最为常见，占比为 34.3%；其次是漏洞利用，占比为 31.9%；钓鱼邮件排第三，占比为 7.2%。此外，网络监听攻击、网页篡改、Web 应用 CC 攻击、拒绝服务攻击等也比较常见。还有约 21.8% 的安全事件，最终被判定为非攻击事件。也就是说，由于企业内部违规操作、意外事件等原因，即便没有导致系统被入侵，但同样触发了网络安全应急响应的事件也不在少数，值得警惕。



三、恶意程序

应急事件分析显示：勒索病毒、挖矿木马、蠕虫病毒是攻击者使用最

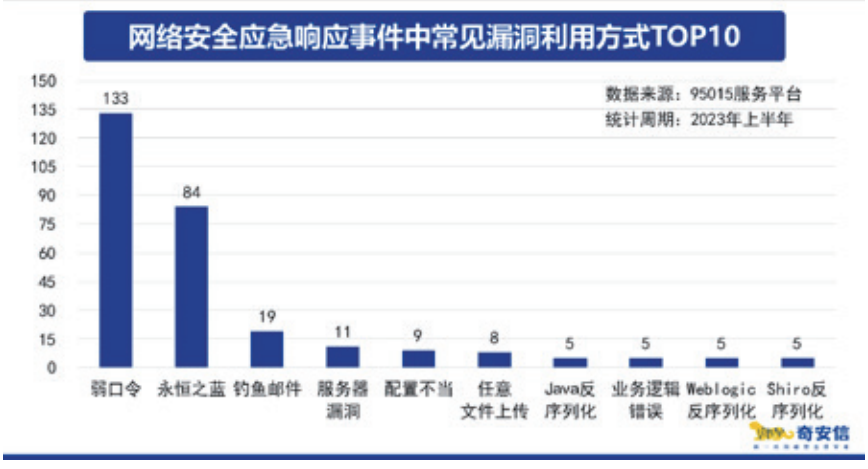


多的恶意程序类型，分别占到恶意程序攻击事件的 20.7%、12.0% 和 7.2%。此外，网站木马、永恒之蓝下载器木马、DDoS 木马、APT 专用木马等也都是经常出现的恶意程序类型。还有 11.4% 恶意程序攻击事件与比较常见的，针对普通网民的流行互联网木马有关。

表 1 给出了 2023 年上半年 95015 服务平台接报的网络安全应急响应事件中，出现频率最高的勒索软件排行榜 TOP10。可以看到，排名第一的是 Phobos 勒索软件，2023 年上半年触发大中型政企机构网络安全应急响应事件 12 次；其次是 LockBit 勒索软件 10 次，Wannacry 勒索软件和 Makop 勒索软件各 6 次。这些流行的勒索病毒，十分值得警惕。

表 1 遭受攻击勒索软件类型 TOP10

勒索软件名称	应急次数
Phobos 勒索软件	12
LockBit 勒索软件	10
Wannacry 勒索软件	6
Makop 勒索软件	6
Tellyouthepass 勒索软件	4
Mallox 勒索软件	3
BeijingCrypt 勒索软件	3
Gottacry 勒索软件	2
Devos 勒索软件	2
Elbie 勒索软件	2



四、漏洞利用

应急事件分析显示：弱口令是攻击者在 2023 年上半年最为经常利用的网络安全漏洞，相关网络安全应急响应事件多达 133 起，占 95015 平台 2023 年上半年应急响应事件接报总数的 35.4%。其次是永恒之蓝漏洞，相关利用事件有 84 起，占比为 22.3%。相比之下，其他单个类型的漏洞利用占比都要小很多，排名第三的钓鱼邮件仅有 19 起，占比为 5.1%。

弱口令的大行其道，完全是安全意识淡薄、安全管理松懈的体现。而永恒之蓝漏洞自 2017 年 WannaCry 病毒爆发后，已经成为广为人知必须修补的安全漏洞。时至今日仍然有大量的政企机构倒在永恒之蓝的枪口之下，说明这些政企机构严重缺乏最基本的网络安全基础设施建设，缺乏最基本的网络安全运营能力。预计在未来相当长的时间里，弱口令和永恒之蓝漏洞仍将是国内政企机构亟待解决的、基础性的网络安全问题。安

阅读报告全文
请扫描以下链接

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

全国政协副主席周强一行调研奇安信集团

8 月 17 日，全国政协副主席周强一行到奇安信集团进行走访调研。中央网信办副主任、国家网信办副主任赵泽良，工信部总工程师赵志国，全国政协委员张金英、张云泉、赵岩、张峰，中央网信办及工信部有关领导参加调研。全国政协委员、全国工商联副主席、奇安信集团董事长齐向东陪同调研。

周强对奇安信在数据安全领域的布局和成绩表示肯定。他表示，数据安全事关国家发展和安全大局。要坚持技术创新、系统规划，坚持数据安全与发展并重，突破数据安全领域关键核心技术，从根本上筑牢国家网络安全屏障，为提升网络治理体系和治理能力现代化水平提供坚实的技术支撑。

北京国际信托有限公司一行来访奇安信集团

8 月 11 日，北京国际信托有限公司（简称“北京信托”）总经理瞿纲一行来访奇安信安全中心，参观奇安信安全中心展厅、工控实验室，并与奇安信集团董事长齐向东进行座谈。双方就产业资本基金与高精尖企业如何深入合作推动科技创新、科技成果转化进行深入交流。

瞿纲表示，北京信托一直重点关注高精尖企业，奇安信在网络安全行业的贡献有目共睹。希望依托奇安信在网络安全行业龙头企业的行业地位、科技创新、前瞻视角，为产业投资起到资源“探照灯”作用，共同挖掘更多潜力企业并提升投资精准度；同时，依托奇安信的科技创新能力，推进知识产权信托发展，推动更多科研成果落地转化。

奇安信流量解密编排器中标某大型银行机构国密改造

近日，奇安信中标某大型银行机构征信系统所需安全网关设备采购项目，主力产品为流量解密编排器（SSLO）。该项目为奇安信流量解密编排器用于金融行业国密改造的典型场景，针对高性能国密加解密、流量编排的场景，流量解密编排器可以充分满足客户需求，解决客户痛点，为后续更多地落地金融应用场景奠定坚实的基础。

奇安信相关负责人表示，目前，国密改造在金融行业已经广泛展开，客户对于流量解密编排的需求越来越迫切，该项目的中标落地，不仅对金融行业加速国密落地具有重大意义，也对其他金融行业客户的同类采购具有重要示范作用。

商用密码与网络安全技术融合创新发展论坛顺利举行

8 月 10 日，由奇安信集团承办的 2023 商用密码大会“商用密码与网络安全技术融合创新发展论坛”在郑州举行。论坛围绕“技术融合 创新应用”主题，来自主管部门、高校、科研机构、网络安全企业、商密企业、应用单位的专家学者，就密码相关政策法规、应用实践及产业发展方向，进行了深入地交流和研讨。

活动上，奇安信对“密码应用中间件”的数据加密保护能力进行了升级发布。同时，为进一步促进商密生态发展、商密产业链产学研深入合作，会上进行了商密生态企业与产学合作签约仪式，奇安信、新疆 CA、数字认证、信安世纪、格尔软件等企业与北京交通大学、中国传媒大学共同签约，各方将共同携手，打造种类更加丰富、链条更加完整、安全适用更好的商用密码产品体系。

奇安信亮相第四届中国石油石化企业云计算、大数据与信息安全研讨会

8 月 9 日至 11 日，以“数智赋能石油石化企业创新发展”为主题的第四届中国石油石化企业云计算、大数据与信息安全研讨会在天津举行。会上，奇安信安全专家介绍了石油石化企业网络安全建设重点，同时带来多个石油石化业务场景的安全解决方案。

实践中，奇安信集团搭建仿真生产环境，研究工控安全核心技术，已持续为中国石油、中国石化、中国海油、国家管网等众多石油石化企业提供了工业互联网安全相关产品及服务，从油气生产、炼油化工、油气管输、成品油库四大场景进行安全设计，打造工业安全核心能力。

奇安信集团与南水北调水网智科签署战略合作协议

8 月 9 日，中国南水北调集团水网智慧科技有限公司（简称“水网智科”）一行赴奇安信安全中心参观交流，并与奇安信集团签署战略合作协议。

双方将依托各自技术和资源优势，在安全技术、安全运营、安全能力培养等多方面开展深入合作，共同推进南水北调集团数字化转型，为加快构建国家水网筑牢安全底座。

奇安信发布 APP 侵害用户权益检测报告

近日，奇安信病毒响应中心发布《2023 年上半年 APP 侵害用户权益检测报告》（简称《报告》）。这一时段内，该中心共收录全国应用市场新收录、新更新 APP 近 40 万个。《报告》将相关的国家法律法规作为检测标准依据，使用奇安信完全自主研发安卓动态引擎 QADE，对 2023 年上半年应用市场新收录新更新的头部主流 APP 抽样检测，评估当下 APP 侵害用户权益的问题。

《报告》显示，此次检测到侵犯用户权益的 APP 中（存在违规收集个人信息或者违规索取权限），有 6 款 APP 下载量在亿次以上，有 76 款 APP 下载量在千万次以上，297 款 APP 下载量在百万次以上。可见 APP 侵害用户权益问题的影响面非常广，至少影响到上亿用户。

齐向东：以网络安全为底板做好“三件事” 护航辽宁数字经济发展

8 月 3 日，在“全国知名民企助力辽宁全面振兴新突破高端峰会”开幕式上，全国政协委员、全国工商联副主席、

奇安信集团董事长齐向东表示，随着“数字辽宁、智造强省”战略的深入推进，辽宁需要进一步夯实网络空间安全屏障。奇安信将提供国内顶尖的网络安全产品和服务，护航辽宁数字经济发展、工业制造业数字化转型，服务好“数字辽宁、智造强省”建设。

齐向东表示，奇安信将做好“三件事”，助力辽宁加快推进“数字辽宁、智造强省”建设。一是筑牢网络安全底板，助力辽宁以数字经济引领高质量发展；二是发挥技术研发优势，助力辽宁以科技创新引领高质量发展；三是抓牢“一带一路”机遇，助力辽宁以对外开放引领高质量发展。

奇安信集团与辽河数码达成战略合作

8 月 3 日下午，辽宁地区油化企业“护航数字化”网络安全论坛在盘锦召开，论坛上，奇安信科技集团股份有限公司与盘锦辽河数码科技发展有限公司达成战略合作。双方将在网络安全人才培养、网络安全规划、咨询服务、产品技术开发等领域达成战略合作，发挥各自优势，为辽宁地区石油石化企业数字化和网络安全发展做出贡献。

奇安信与支流科技携手共筑 API 安全新生态

近日，奇安信与深圳支流科技宣布达成深度合作，奇安信 API 安全卫士和支流科技 API7 企业版将形成 API 联动安全方案，通过 API 生命周期管理 +API 安全监测分析一体化解决方案，为 API 业务提供便捷性与安全性，助力 API 安全生态建设，赋能企业数字化转型。

2023 第七届“蓝帽杯”全国大学生网络安全技能大赛报名正式开启

7 月 28 日，2023 第七届“蓝帽杯”全国大学生网络安全技能大赛报名正式开启。作为面向全国公安院校和普通高校大学生的实战技能大赛，本届“蓝帽杯”大赛将通过靶场演练模式，模拟真实涉网案件，全面考察选手对场景问题的发现和解决能力，并通过比赛及培训等多种形式，全面选拔、培养网络安全实战型专业人才。

奇安信亮相第六届石油石化数字化与智能化创新发展交流会

7 月 27 日，第六届石油石化数字化与智能化创新发展

交流会在贵阳开幕。奇安信集团受邀亮相，并发表《基于“零事故”实践的石油石化数智化转型网络安全保障思考》主题演讲，和与会的行业专家、机构代表、石油石化企事业单位代表一起，围绕石油石化行业数字化创新发展及智能化安全运营等话题进行交流分享。

齐向东：以数据安全为第一要务“零事故”为目标 助力聚数算数产业

7 月 26 日，2023 全国工商联主席高端峰会在郑州召开。全国政协委员、全国工商联副主席、奇安信集团董事长齐向东在“数聚中原 算好未来”平行专题活动上发表主题演讲时表示，数字经济全球竞争的下一个赛道已然聚焦于“数据”和“算力”，网络安全成为聚数算数产业的底板工程。

齐向东表示，聚数算数产业要以“零事故”为标准。首先要建设纵深防御的内生安全体系；二是建设全链条的数据安全防护体系；三是建设三级态势感知体系；四是建设一体化的网络安全运营中心。

奇安信发布《2023 中国软件供应链安全分析报告》

7 月 24 日，奇安信集团对外发布《2023 中国软件供应链安全分析报告》（以下简称《报告》），深入分析了过去一年来，国内软件供应链中开源软件应用的安全状况，并附以典型案例加以说明，总结了开源软件供应链风险的趋势和变化。

《报告》显示，2022 年开源软件生态依然繁荣。2021 年年底和 2022 年年底，主流开源软件包生态系统中开源项目总量分别为 4395386 个和 5499977 个，一年间增长了 25.1%；截至 2022 年年底，主流开源软件包生态系统中平均每个开源项目有 12.6 个版本，较前两年报告的 11.8 个和 10.2 个呈持续增长的趋势。

重庆网络与数据安全产业大会正式开幕

7 月 24 日，重庆网络与数据安全产业大会在重庆市璧山区盛大开幕。会议由市委网信办、市发展改革委、市经济信息委、市大数据发展局指导，璧山区人民政府、重庆广播电视集团（总台）、奇安信科技集团股份有限公司主办。

此次大会以“构建网络与数据安全产业大生态 打造成渝地区数字经济新名片”为主题，由大会主会及“数据安全”“网络与数据安全产业生态合作”“软件供应链安全”三场主题分会组成，邀请了数字领域政、产、学、研、用各界领导和嘉宾出席，呈现了一场聚焦网络与数据安全的数字经济巅峰盛会。

活动中，璧山区联合奇安信集团与浪潮云、超图软件、西部智数、中科网威等 18 家知名企业进行了生态合作战略

签约，共同构建更加完整的数字经济产业生态，打造更具竞争力的网络数据安全产业集群。

2023 网安人才报告：北京就业岗位多，西安求职者最多

7 月 24 日，奇安信行业安全研究中心联合牛客平台、网教盟、新安盟、广州大学、深圳信息职业技术学院等单位，共同发布了《2023 网络安全人才市场状况研究报告》。

该报告显示，在过去一年中，网络安全科技人才市场需求规模快速增长，但存在高等教育资源的分布不均，人才培养与市场应用的错配的情况，导致网络安全科技人才供求的地域性失衡问题十分突出。报告认为，应届网络安全科技人才毕业后跨地域就业迁徙将成为未来一段时间的常态。

奇安信亮相 2023 年网络安全技术创新与人才教育高峰论坛

7 月 24 日，2023 年网络安全技术创新与人才教育高峰论坛在长沙成功举办，奇安信亮相论坛并与各界嘉宾共同探讨网络安全领域发展新思路。颁奖仪式上，奇安信集团荣获论坛“优秀支撑单位”，吴云坤总裁获得“2022 年 CCSIA 杰出贡献奖”。

论坛上，“网安人才供需战略签约仪式”同步举行，奇安信与中国网络空间安全人才教育联盟达成战略合作。双方将在网络空间安全人才队伍建设方面充分发挥各自的优势，通过网络安全优秀人才挖掘、能力认证、人才培养、竞赛活动等多方向全面合作，共同推进网络空间安全高质量人才队伍建设。

齐向东：以网络安全护航内蒙古全方位建设“模范自治区”

7 月 21 日，全国工商联副主席、奇安信集团董事长齐向东在世界蒙商大会上发表“汇聚内蒙古力量 建设模范自治区”主旨发言时表示，作为从内蒙古“走出去”的企业家，希望通过网安服务、平台支持、携手“出海”等方式，为全方位建设“模范自治区”做出应有贡献，为家乡建设添砖加瓦。

齐向东表示，未来将充分发挥奇安信在网络安全领域的优势特长，通过助力内蒙古提升数字经济比重、以科技创新引领高质量发展、深度融入“一带一路”战略，助力“模范自治区”建设。

数字城市网络安全运营再升级 “星城”3.0 发布

在 2023 北京网络安全大会 · 长沙网络安全运营峰会上，“星城”城市网络安全运行平台 3.0 正式发布。奇安信集团副总裁、长沙研发中心负责人左文建介绍，在 2.0 版本基础

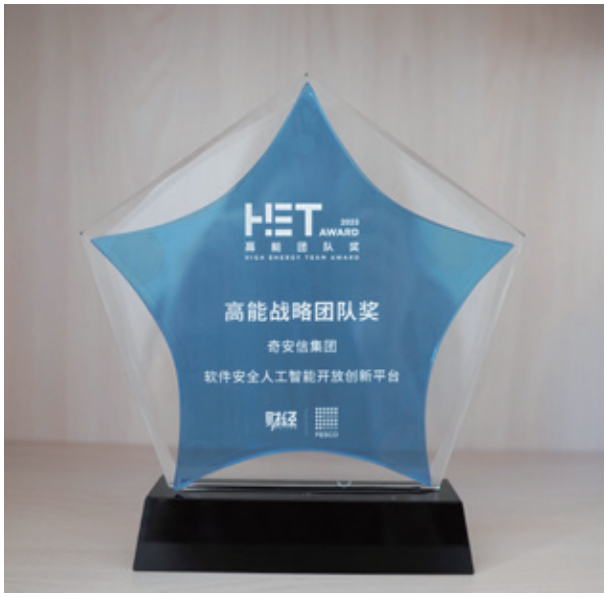
上，“星城”3.0 通过精简操作流程、降低信息干扰、聚焦重要信息等方式，全面提升了平台使用效率：资产运营效率提升 40%、重保信息传递效率提升 30%、漏洞管理效率提升 30%、漏洞知识匹配效果提升 100%，实现了深度资产运营管理、智能化漏洞管理、数字化重保管理等一系列优化，进一步为我国数字城市建设提供高效、稳定、安全的运营服务。

荣誉墙

奇安信软件安全人工智能开放创新平台团队获哈佛商业评论高能团队奖

8 月 18 日，《哈佛商业评论》（Harvard Business Review）中文版携手 FESCO 成功举办第九届人才经济论坛暨 2022—2023 高能团队奖颁奖典礼。论坛秉承前沿的全球视野及权威的管理理念，发掘并展示本土企业组织管理的最佳实践，并重磅揭晓第二届“高能团队奖”评选结果。奇安信集团“软件安全人工智能开放创新平台团队”从百余家优秀企业团队中脱颖而出，获评“高能战略团队奖”。

凭借突出的前瞻视角、扎实的科技创新能力和强大的战略执行力，奇安信成为本次获奖名单中唯一一家网络安全企业。

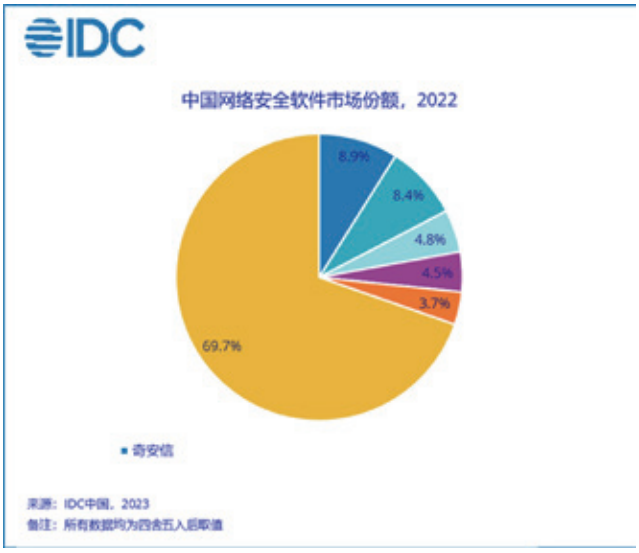


奇安信成为入选赛迪数据安全报告领域最多的企业

近日，赛迪顾问发布《中国数据安全防护与治理市场研究报告（2023）》（简称《报告》），作为国内领先的数据安全产品和服务供应商，奇安信共计入选 9 大类、38 小类数据安全各细分领域，全面覆盖数据全生命周期安全治理和数据流动各个环节安全防护，是入选该报告细分领域最多的企业。

份额和增幅双第一 奇安信连续两年位居网络安全软件市场头名

近日，全球领先的 IT 市场研究和咨询公司 IDC 发布了《中国网络安全软件市场份额，2022：增速放缓，主动变革，厂商探寻技术与市场新机会》，在网络安全软件市场整体增长不及预期的情况下，奇安信以 17.3% 的市场增长率，领先头部主要供应商（包括综合性安全厂商和大型云服务提供商），并显著高于行业平均水平，并以 8.9% 的市场份额，连续两年拿下网络安全软件市场头名。



盘古实验室连续三年荣获华为终端安全突出贡献奖

8月4日，在第五届华为开发者大会（HDC 2023）期间，华为正式公布了 2021 和 2022 年度华为终端安全奖励计划获奖名单，凭借在过去两年为华为终端在漏洞挖掘和安全应急等方面做出的贡献，奇安信旗下盘古实验室和研究员斩获华为终端安全多项大奖，成为获得奖项最多的团队。

奖项包括：盘古实验室获得 2021 年度突出贡献奖、2022 年度杰出生态合作伙伴。盘古实验室研究员闻观行在华为终端安全奖励计划英雄榜 2021、2022 年度排行榜斩获第一名，独家获得了 2021 年度安全奖励计划一等奖、2022 年度安全奖励计划一等奖。同时，奇安信旗下补天漏洞响应平台和奇安信网神则分获 2021、2022 年度优秀合作伙伴。

奇安信连续两年入选 Gartner® Hype Cycle™ 中国 CPS 安全代表供应商

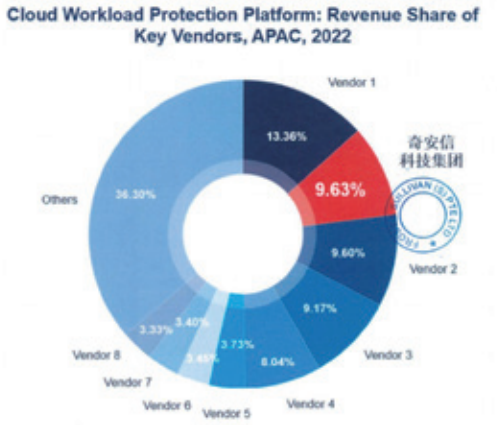
近日，Gartner 正式发布了《Hype Cycle for Smart City and Sustainability in China, 2023》报告。在中国信息物理系统（Cyber-Physical Systems，CPS）安全领域（2022 Hype Cycle 报告中为“智慧城市 CPS 安全”），奇安信连续两年被评为该领域代表供应商。

在城市安全运营中心建设方面，奇安信围绕数字城市相关主题，以城市运营中心为主体，以城市发展为目标，从实时洞察、精确感知、主动防御、联防联控、协同指挥、全城防御等方面梳理和设计城市安全运营架构体系，保障城市数字化改革的推进和发展。2023 数博会期间，奇安信正式发布了“零事故”城市安全运营中心 2.0。

Frost&Sullivan 发布 CWPP 全球云工作负载保护平台报告 奇安信排名中国第一

近日，Frost & Sullivan 发布 CWPP 全球云工作负载保护平台报告《Global Cloud Workload Platform

Growth Opportunities》（简称“报告”）。《报告》统计，由于中国区的强劲增长，亚太区已经成为全球第二大 CWPP 市场，占据 23.2% 的市场份额，其中，奇安信是全球规模最大的中国 CWPP 供应商，以亚太区 9.63% 的市场份额位列中国第一。



奇安信旗下两大鉴定所 CNAS 国际能力验证均获得满意结果

近日，由中国合格评定国家认可委员会（CNAS）与公安部第三研究所上海辰星电子数据司法鉴定中心联合发起的第二届电子数据提取、恢复和分析（MYSQL 数据库）国际能力验证计划公布了最新结果。

奇安信集团旗下的盘石软件（上海）有限公司计算机司法鉴定所和北京网神洞鉴科技有限公司司法鉴定所在此次全球范围内的能力验证中，均以卓越表现赢得“Satisfactory”（满意）的评价。

奇安信入选数据安全人才强基计划数据安全风险共治组成员单位

在 7 月 19 日举行的 2023 中国互联网大会“数据安全

论坛”上，中国互联网协会公布了“电信和互联网行业数据安全人才强基计划”数据安全风险共治组成员名单。经过专家函审、评定会议等流程，奇安信集团入选数据安全风险共治组成员单位，将参与数据安全关键技术研究、风险信息监测研判，为综合提升行业数据安全风险治理效能，有效保障国家各行业各领域数据安全提供力量。

社会责任

全国工商联社会服务部部长吴建辉与奇安信公益基金会座谈交流

8 月 18 日，全国工商联社会服务部（光彩事业部）部长吴建辉一行到访奇安信安全中心，先后参观了奇安信安全中心展厅、工控实验室、党建长廊等地，并与奇安信公益基金会开展公益及社会责任交流活动，了解基金会工作开展情况。

吴建辉对奇安信集团在践行社会责任、奇安信基金会在公益事业方面做出的成绩表示充分肯定。为缩小区域差距、城乡差距、收入差距，促进共同富裕做出贡献。

北京航空航天大学 – 奇安信助学基金正式启动

8 月 16 日，“北京航空航天大学 – 奇安信助学基金”启动仪式在奇安信安全中心举行。助学基金将为北京航空航天大学网络空间安全学院学生提供社会实践支持、紧急救助、实习奖助学金等帮助。

此次“北京航空航天大学 – 奇安信助学基金”项目为期 6 年，是目前为止“心安助学”项目资助时间最长、金额最多的项目。

雨季防汛救灾 奇安信基金会心安救灾在行动

面对北京今夏的雨季汛情，奇安信基金会积极应对，从防灾、减灾、赈灾等角度出发，通过捐建防洪渠、捐赠物资等方式，积极参与防汛救灾。

7 月，奇安信基金会与多家组织联合为北京市密云区山口庄捐赠建设防洪渠，并积极推进工程建设。在 7 月 29 日至 8 月 2 日的特大暴雨灾害中，新建成的防水渠成功经受住了暴雨的袭击，有效保护了山口庄的大棚等基础设施和田地，

帮助村里避免了更大的经济损失。

8 月 3 日，基金会收到北京市房山区慈善协会求助信息。基金会立即响应，第一时间组织捐款，支持房山区救灾和灾后重建工作；8 月 7 日，门头沟区雁翅镇田庄村向基金会发出求助，受灾群众急需米面等生活物资。奇安信基金会联合奇安信集团党委，迅速采购 300 套米面物资，并组织人力运力送往灾区，送达受灾群众手中。

心安助农 · 巴林左旗乡村振兴项目正式启动 专家团赴当地进行调研走访

近日，“心安助农 · 巴林左旗乡村振兴项目”正式启动，奇安信基金会组织专家调研团赴巴林左旗实地走访，深入了解当地实际发展情况和需求，为制定适合当地乡村振兴组织建设、人才培育、产业发展等各方面的可持续发展方案奠定基础。

奇安信基金会负责人表示，调研活动结束后，调研组正在抓紧形成调研报告，后续将向有关部门进行反馈和沟通，并组织巴林左旗政府各部门及乡村骨干开展研学、参与式学习互动，协同巴林左旗各相关部门及奇安信基金会共同制定具体、可执行、可落地、可持续发展的帮扶方案，为后续的帮扶措施奠定坚实的依据和基础。

北京奇安信公益基金会荣获“支持党建工作示范单位”称号

近日，中共北京市行业协会商会综合委员会在举办的学习贯彻习近平新时代中国特色社会主义思想主题教育“社会组织跟党走”文艺汇演暨“岗位双先、单位双示范”选树颁授仪式上，北京奇安信公益基金会荣获“支持党建工作示范单位”荣誉称号。

打造数智融合安全体系新范式

作者 | 陈华平

在过去 30 年，中国完成了数代技术演进，成功影响和带动了互联网、移动互联网、云计算、物联网等数化技术和应用的发展和演进，目前正进入智能化与数字化为特征的数智时代，给网络安全带来深刻影响。

数智化是必然趋势 AIGC 带来大量新问题

当前全球经济环境下，挑战重重，中国在下一个 30 年是否能够延续辉煌和成就，数字化升级和转型成效将起关键作用。数字化转型就是数字化、信息化体系向智能化、自动化演进。

• 技术有支撑。云计算、大数据、移动互联网等软件能力不断升级成熟，为电子政务数智化升级提供了落地手段和技术支撑。

• 运行成本持续降低。计算、存储、网络等硬件基础设施单位成本持续降低，是数智化电子政务大规模建设和运营的基础和前提。

• 多维需求产生驱动力。手机、PC、物联网终端及各类应用在线时长不断延长，运营管理体验优化。

• 可持续发展能力。政务上云，数据集中、移动支付、5G，“互联网 + 政务服务”为民众切实提供了便利，已体系化、规模化形成商业闭环，为新技术广泛应用和数智化电子政务可持续发展提供了生长环境。

我们在体验数智化带来便利的同时，也同样要面对数智化带来的安全问题，AIGC 作为数智化的典型代表应用，带来了大量新的安全问题。

• 新的对手。“科技霸权”升级带来的国家安全问题，对手升级为国家层面，中美对抗呈多元化、升级化趋势，以 AIGC 为代表的技术垄断向科技霸权发展，进而影响国家安全。

• 新的目标。数据成为攻击目标，网络攻击从瞄准网络与系统到瞄准数据与业务应用，数据安全变得尤其重要。

• 新的战场。数字化运行环境复杂，AIGC 大量使用“云大物移工”的数字基础设施和数字化环境，单一环境已是是传统安全灾区，复合环境下挑战呈指数级上升。

• 新的武器。攻击手段不断升级，勒索蠕虫、高级威胁 APT、供应链攻击，对安全缺乏系统性认识，原有攻击手段在 AIGC 加持下，攻击烈度提升。

• 需要新的监管体系。原有监管体系不能针对 AIGC 进行有效监管，监管、

数字化转型就是数字化、信息化体系向智能化、自动化演进。

法律法规理解需与时俱进，尤其是针对 AIGC 类新技术的监管需快速跟进。

数智化推动网络安全政策面和技术面发展

数据作为核心生产要素，贯穿于数字化系统的各个生产环节中，如果拧不紧数据“安全阀”，不仅会影响数字经济发展，甚至影响国家安全，将造成难以承受的后果。我国在数字化推进过程中需要平衡统筹安全问题，我们可以从政策和技术两个维度分析。

从政策面看，我国推出数安法、成立国家数据局、发布 AIGC 管理办法，说明我国在政策面的监管已完成基本布局，随着后续更多针对性政策的发布，将对网络安全产业带来深远影响。

- 加快数据基础制度的制定和完善，包括数据安全制度的制定和完善，推动数据安全相关投入的增加；
- 以四法、四条例、四合规为基础框架，针对网络安全相关的法律法规上将继续推进，人工智能、密码相关领域是重点；
- 数据安全从过去安全防护的细分组件跃升为安全防护的重心和主体，数据安全已包含网络安全；
- 大量数据大集中形式的数字化系统及平台（一体化政务 / 医疗 / 金融系统、云平台、大模型），需要提升防护等级；

从技术面看，数字化能力是经济发展的核心能力，数字化实力体现国家实力，我国处于产业升级的关键时期，外部环境恶劣，挑战巨大，数字化水平是网信产业龙头企业的实力晴雨表，数字化和智能化广义上代表了国家安全。同时数字化意味着开放和融合，涉及国家利益和商业利益之争，变化成为常态，唯一不变的是变化，发展与安全需要统筹。网络安全穿透数字化中各组件，是数字化产业中各成员不可或缺的生态组成，数字化转型是复杂的系统性工程，需要完整产业能力，产业龙头牵头，一同构建，充分融合，最终形成本质安全、防护安全和供应链安全的全体系安全，服务信息化和数字化，所以从这个维度看，要解决数字化安全问题，在技术面上将推动大量产业融合和生态融合，对数字化产业的健康良性发展起到积极推动作用。

> AIGC 运行在云计算、互联网和 IT 环境下，其网络安全问题将被无限放大。

网络安全长期驱动力来自“数智融合”

AIGC 运行在云计算、互联网和 IT 环境下，其运行环境天然就是网络安全问题频发的重灾区，注册用户已突破 1 亿，并在持续增长中，网络安全问题将被无限放大。微软发布首个与 ChatGPT 能力结合的网络安全产品 Security Copilot，说明网络安全本身就是 ChatGPT 的一个场景应用，且存在大量可被利用的攻击面，形成工具或产品聚合了大量攻防能力，但是显然对绝大多数用户而言，是不具备这种攻防能力聚合水平的，因此 AIGC 作为工具可为攻防两端同时提供“智力”赋能，用于降低攻击门槛，提升防守效率。在未来的某个时间点，攻防双方利用 AIGC 工具的方法将基本趋同，将达到攻守平衡，而在这之前，率先掌握并使用 AIGC 技术的一方，将在攻守对抗中获得压倒性优势。电子政务系统承担了大量对外服务业务，必然将面对被 AIGC 智力赋能的攻击挑战，就需要用 AIGC 智力赋能的防守来应对，达到某种动态的攻守平衡。

数据是 AIGC 的基本要素，数据安全将是未来的网络安全的主战场，一旦数据被窃取、篡改，将直接影响民生、舆情，甚至引发动乱。进入数智时代，数据已经被重新定义，数据将大范围流通、共享、交易，数据安全风险也将随着接触面的扩大而放大，这将推动网络安全防护模式向数值融合的新范式演进。

- 数据从“死”到“活”。数据既然作为生产要素，一定会流通，流通环节从最开始的数据产生、采集，然后到传输、存储、应用，整个过程中数据要活，只有活数据才能产生价值，所以数据在复杂的流动中会产生更大的风险，带来价值的同时也会产生更多的问题；
- 数据从“虚”到“实”。过去整个数据主要存在网络空间，基本不会影响现实的世界，但是在数智时代，数据和实体经济融合，边界变得越来越模糊，

也带来了更大的挑战；

• 数据从“贱”到“贵”。以前我们认为数据的价值有限，也没有进行体系化的挖掘，数智时代数据的价值越来越高，这些数据一旦被泄露、篡改带来的危害非常大，尤其是政务、金融、工业等行业，甚至影响国家和社会安全；

把网络安全产业的发展驱动力做简单分类，短期来自事件驱动项目，中期来自合规，驱动产业规模，长期来自创新，驱动核心能力养成。长期驱动力代表未来趋势，事实上网络安全从来都是一个高度智能化的产业，数智时代为网络安全高质量发展提供了更好的动力、环境和责任，也是网络安全企业发展壮大的长期驱动来源。

• 短期事件驱动项目，突发事件（棱镜门、窃听门、滴滴上市、俄乌战争）带来大量项目机会，助力有一定安全攻防、运营能力的小团队发展；

• 中期合规驱动产业规模，四大合规（等保、关保、密评、数评）提供了稳定市场容量，市场成熟，助力有一定规模的中大型企业发展；

• 长期研发驱动核心能力养成，安全核心能力将伴随 IT 架构及技术同步升级和技术融合（云原生、5G、web3.0、AIGC）养成，打造数智化的安全能力，助力龙头企业和技术创新创业企业发展。

打造数智融合安全体系新范式

得益于生成式 AI 的爆发，AI 应用在网络安全的各个领域，大幅提升安全能力。数智化将推动网络安全向前发展，但以 AIGC 为直接工具的网络安全能力养成还需要相当长的一段时间，应客观看待生成式人工智能对网络安全产业的影响 。

数智时代，网络安全同样要以“内生”为根本。在过去几年中，奇安信一直在强调内生安全，安全内生。内生安全的核心要义是“三个融合”：安全技术和 IT 技术的融合，安全数据和 IT 数据的融合，安全人才和 IT 人才的融合，这里的融合抽象出来就是数据 + 智力，只是在不同的维度，不同的场景，使用不同的技术和落地手段进行了不同程度的整合。在数智时代，这样的整合会越来越频繁，越来越体系化，最终形成体系化的数据 + 智力的安全体系新范式。

安全新范式包含了人、数据、工具和流程四要素。

• 人，这里的人更准确的定义是生态，既包含参与安全规划、建设、运营的个人，也包含个人所属的组织，不仅仅是安全厂商，信息化、数字化厂商都是生态伙伴，安全不能脱离于信息化和数字化，安全一定是融合内生于数字化的；

• 数据，这里的数据包含了个人数据、个人数据、单位数据、行业数据、国家数据等，是融合和内生的原料，是数智融合的前提；

• 工具，任何与网络安全有关的产品、技术和能力都可以作为工具使用，包括网络安全产品、机器学习、K8S、大数据、大模型、数字孪生等，都可以提升数智融合的安全防护效率；

• 流程，流程是规则，可以工单流转、运维服务、应急响应等流程，流程需要积累沉淀，动态更新，并形成制度，沁入到意识中；

未来 AIGC 和数智化的强势还会继续，随着生态、监管、技术等条件成熟，长期将驱动网络安全产业将朝数据 + 智能方向发展。同时也要看到，不管智能化的网络安全如何发展，网络安全防护体系的建设最终都是在合规、攻防、业务综合防护，以及安全意识养成这些方面下手，底层的方法论并没有发生改变。安

关于作者

陈华平

虎符智库专家，网络安全专家、安全创客汇评委会主任、奇安信集团公司副总裁。

趋势解读：SIEM 三个趋势与现代 SOC 四个要点

作者 | 叶蓬

2023 年 6 月 5 日 —7 日，Gartner 安全与风险管理峰会在美国召开。作为 Gartner 最重要的网络安全盛会，本次会议有 Gartner 的 71 位分析师登上讲台、240 家企业参展。Gartner SIEM 和 SOC 领域的关键分析师悉数亮相，分享了他们对于未来 SIEM 和 SOC 发展的见解。

SIEM 的生与死

SIEM 能否满足当前快速变化的安全需求？SIEM 是否已经不堪重负？面对新兴的技术和产品，SIEM 是否会走向消亡？

在二十多年的发展进程中，SIEM 产品曾多次遇到过类似的疑惑，但从来没有哪次像这两年一样面临如此巨大的挑战。在题为《安全运营展望 2023》的演讲中，Gartner 分析师 Eric Ahlm 将新技术和产品（尤其是 XDR）对 SIEM 的挑战比作天地大碰撞。

SIEM 会毁灭吗？还是在被撞击后重获新生？Eric Ahlm 表示，“好消息是，这不是一次 SIEM 灭绝事件，是时候重新掂量 SIEM 在 SOC 中的价值了。”

Gartner VP 分析师 Pete Shoard 在题为《SIEM 的未来和 TDIR 的演进》的演讲中，展示了多个 SIEM “被死亡”的节点。他坚定地认为，SIEM 还会好好活着！

Gartner 研究人员认为，SIEM 作为一个细分市场、一个术语不会消亡，但 SIEM 的内涵和外延却已不再似以前，而这也恰恰体现了 SIEM 自身所特有的与时俱进的能力。

重新定义和定位 SIEM

在大会上，Pete Shoard 给出了 SIEM 的最新定义：SIEM 平台提供一个可配置的安全记录系统，帮助组织识别和报告需要调查的感兴趣事项。并且协助组织对可能导致损害的已发现事项进行验证与响应。

Pete Shoard 表示会更新到今年的 SIEM 魔力象限报告中。作为对比，在 2022 年魔力象限报告中，对 SIEM 的定义如下：SIEM 将跨应用、网络、端点和云环境的各类监测、评估、检测及响应系统的事件数据聚合起来，以实现基于关联规则和 UEBA 的威胁检测，基于 SOAR 的响应集成，基于

> SIEM 作为一个细分市场、
> 一个术语不会消亡，
> 但 SIEM 的内涵和外延却已不再似以前。

TIP 的威胁内容持续更新和安全报表报告。

可以发现，之前的 SIEM 定义中对功能的描述较为具体，而新的定义则抓住调查、验证、响应三个关键能力进行简洁的概括，内涵较之前更为丰富。

进一步分析，多年以来 SIEM 定义的核心都是数据的采集与分析，即以数据为中心。从技术架构上来看，数据驱动安全没毛病。但正如 Gartner 所说，当前的实际情况表明，在经历多年的大数据时代后，更多的数据并不意味着更多的安全价值，数据的边际效益正在递减。同时，市场上出现了越来越多的具备检测和响应能力的产品种类。也就是说，检测与响应能力越来越分散到不同的安全系统之中。因此，对用户而言，数据分散问题虽依然存在，但重要性正在下降，而安全系统（尤其是安全检测与响应系统）的分散问题越发凸显。这就需要 SIEM 平台在保持大数据分析架构的前提下，大幅增加对异构安全系统的集成能力（Gartner 称之为相容性——Compatibility），而这也正是安全网格架构（Cybersecurity Mesh Architecture）产生的原因。总之，当前 SIEM 的外延已经从数据集成扩展到了系统集成。

既然 SIEM 被重新定义了，那么是否可以将新定义的 SIEM 命名为下一代 SIEM（NG-SIEM）或者 SIEMX.0 呢？对此，Gartner 的态度也是明确的。Pete Shoard 表示，那些不能从历史中吸取教训的人才会去不断发明所谓的下一代 SIEM。SIEM 就是 SIEM，它不会被取代，也不会变成 NG-SIEM。SIEM 定义的演进是 SIEM 内在的特征，SIEM 从一开始就被定义为具有极强的扩展性，能够随安全格局的演变而演进。SIEM 未来的定义还会继续变化。

在笔者看来，这种不断演进的 SIEM 定义正是 SIEM 的优势所在，因为 SIEM 代表了一种自顶向下的体系化安全运营建设需求。

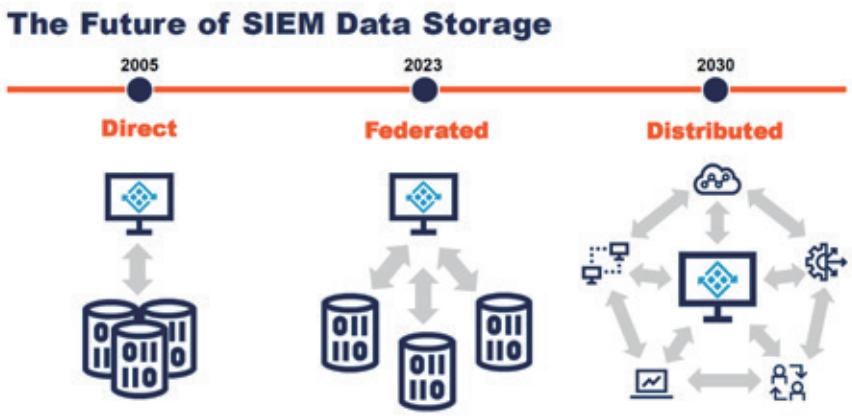
为什么 SIEM 能在与 XDR 等一众聚焦检测与响应领域的产品细分市场的竞争中存活下来呢？这里撇开 SIEM 领域日渐式微的合规性功能【笔者注：事实上这类功能越来越向 GRC 合规管理中心转移】不谈，Gartner 认为最关键之处还在于 SIEM 自身的开放性。从用户侧而言，发展到一定阶段必然需要一个统合全局网络安全监测与响应的、紧密结合用户自身业务实际的安全平台，而这个安全平台必然需要高度的开放性，包括可配置性和可定制性，而这正是 SIEM 所追求的。从这个意义上而言，XDR 及其他专项 DR 类产品都是可以与 SIEM 协作的。

可以说，开放性体现了 SIEM 区别于其他产品的独特性，也体现了 SIEM 的核心定位，即服务于有定制需求的客户。SIEM 产品肯定不止服务于有定制需求的客户，根据 Gartner 2022 年的《SIEM 关键能力》报告，SIEM 用例还包括开箱即用 SIEM 和作为 TDIR 平台使用。对于 SIEM 而言，真正受到挤压的是开箱即用 SIEM 用例所涵盖的市场。

凡事皆有两面性。SIEM 开放性的另一面正是其高度复杂性，以及由此带来的对 SIEM 落地实战能力的长期诟病。本质上，SIEM 作为应对客户复杂安全需求（将不断变化的异构数据和系统集成起来实现全局的监测与响应）的一个产物，必定也是复杂的。但是从产品和解决方案的角度，我们可以将 SIEM 的复杂性进行转移，尽可能地从用户侧转移到厂商侧。注意，这里说的是转移，不是消除！这种转移可以表现为 SIEM 产品中内置丰富的安全内容（包括策略、规则、报表模板、算法模型等），可以表现为 SIEM 产品提供更流畅的交互式设计和分析师体验，可以表现为提供丰

SIEM 未来趋势：
存储从联邦式向分布式转变；
安全内容市场逐步壮大；
出现新的、基于事态的用例。

富的产品附加服务（Gartner 称之为 VDSW——供应商交付的产品打包服务），也可以表现为托管安全服务。这些都是降低用户落地 SIEM 复杂度的良好实践，本质上是由厂商更多地承担起 SIEM 的落地复杂性，通过厂商丰富的安全经验，将这些复杂性工作打包成可传递的知识（包括易用的 UI、丰富的安全内容、有经验的服务人员等），提供给客户。



SIEM 的三个发展趋势

Pete Shoard 在大会上向大家介绍了三个 SIEM 未来发展的趋势：

1）存储从联邦式向分布式转变；2）伴随着社区的繁荣，安全内容市场逐步壮大；3）出现新的、基于事态（Event-Based）的用例（使用场景）。

对于第一点，Gartner 认为 SIEM 将从现在流行的联邦式大数据分析架构向更加完全的功能去中心化分布式架构方向发展。数据在哪里已不重要，功能的网格化才是重点，API 是关键。

对于第二点，本质上就是知识分享从过去的厂商与用户之间的单向传递，变成厂商、用户、第三方之间的双向分享。这是一种知识变现，会带来新的业务模式和商业机会。

SOC 建设的四个要点

安全运营需求、理念和技术的变化不仅带来了 SIEM 的变化，也促动了 SOC 的演进。随着云技术和远程办公的普及，Gartner 将 SOC 看作是一组安全运营能力的集合，而不再是一个地点。很多人坐在墙上挂着超大屏幕的屋子里盯着大大小小屏幕工作的场景正在成为过去。

在《你的 SOC 是不是现代 SOC》的演讲中，Gartner 分析师 Eric Ahlm 提出了建设现代化 SOC 的四个要点：采用混合运行模式、优化检测技术栈、聚焦日常自动化和施行基于度量的迭代演进。

1) 采用混合运行模式

随着网络安全的挑战日益严峻，用户方在资源和能力方面所面临的瓶颈越发明显，完全依靠自身的力量已经难以将 SOC 运行起来。Gartner 展望 2023，认为以后所有的 SOC 都将是混合型 SOC，即或多或少都要依靠外部力量，借助各种安全服务，弥补自身在 SOC 规划、建设和运行时的人员岗位缺口和能力缺失。此外，对于那些坚持采用单纯依靠自身运行的 SOC 的用户，Gartner 建议其运营团队人员应不少于 12 人，否则无法真正将 SOC 运行起来。

2) 优化检测技术栈

如前所述，用户要重新审视SIEM在SOC中的价值，SIEM不能在SOC技术平台中包打天下。Gartner建议用户在构建SOC技术平台的时候，将SIEM技术栈进行拆解，用其他技术替换掉SIEM中过时或低效的部分，同时引进一些新的功能（尤指XDR和暴露面管理），并更好地与其他技术协同起来。而分析师Neil MacDonald在《新兴安全市场趋势和增长机会》主题报告中就直接建议厂商引入多遥测数据融合分析技术，淘汰或升级旧有的SIEM，加入主动安全监测，还建议安全托管服务商增加暴露面管理和事件响应服务。

3) 聚焦日常自动化

Eric Ahlm表示，高大上的端到端的运营级流程自动化还太过遥远，当前用户更需要的是（较小粒度的）日常运行活动自动化。因为安全流程（Process）天生就是易变和动态的，存在很多分支情况，要完整进行描述十分困难，会耗费大量设计开发精力，而跨部门的流程更难。在当前管理和技术条件下，要实现全面流程级别的自动化代价太高。相反，对构成安全运行流程的安全活动（Activity）进行自动化则更切合实际且更高效。在流程层面，更适合通过人工和半自动化的方式将相关的活动串起来。对此，笔者完全赞同，笔者参与设计的SOAR系统正是秉持这个理念。

在实现流程和活动自动化方面，SOAR并非唯一选择，而是存在三种技术路线：从具备最高灵活度的SOAR平台，到SIEM和ITSM中嵌入的简化版自动化工具，再到XDR或其他DR类产品中预置的自动化功能。

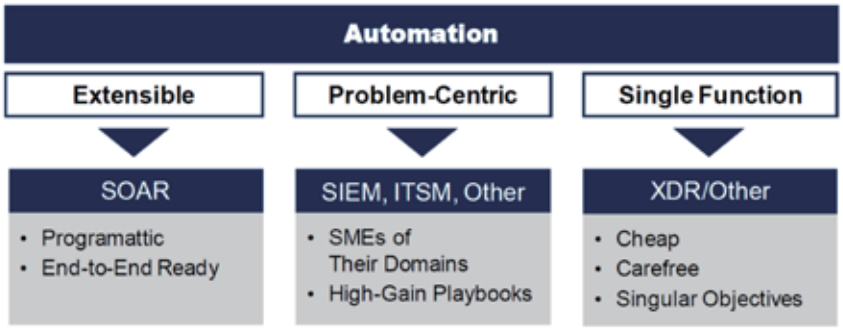
对于用户而言，选择哪种技术路线的产品和系统取决于自身的实际需求和未来发展规划。

4) 施行基于度量的迭代演进

Gartner反复强调，SOC建设是一个持续迭代的旅程，至少要在计划、排序、构建、运行、汇报、成熟6个阶段迭代三次。这个迭代旅程，是SOC能力不断增强，成熟度不断提升的过程。这个过程必须在量化的安全指标牵引下演进。

SOC的度量指标设计要跟当前的成熟度相适应。如下图所示，在进入“主动监测”阶段后就应该引入正式的指标体系去度量SOC有效性和价值。

此外，面向不同层级和职责的上级，汇报的指标应该具有针对性，切忌出现“鸡同鸭讲”。分析师Alex Michaels在《现代化高绩效SOC的



演进和期待》主题报告中就列举了一个悲催的示例，如上图所示。

Gartner 表示，对于单位高管级领导，要用他们听得懂的业务指标（而不是运营指标）和业务术语去汇报，对于 CIO 和更高级领导，要采用结果驱动的指标（Outcome-Driven Metric）设计方法论输出业务价值导向的指标。

结语

安全威胁形势越来越严峻，安全防御越来越强调实战化，强调结果导向，安全运营越来越重要。围绕网络威胁防御这个核心，SIEM 的内涵和外延正在不断演进，而 SOC 的方法论也在日渐成熟。包括 SIEM 和 SOC 在内的安全运营天然是一个复杂性问题，做好安全运营没有捷径，唯有持续迭代提升。这就好比唐僧师徒西天取经，孙悟空、筋斗云、金箍棒是取经路上拼杀的利器，但却无法让他们直接抵达西天。如果我们把 XDR、ChatGPT、AI 看作是安全运营的新利器，也依旧不能确保安全运营成功。

千里之行，始于足下，功在平时，贵在坚持。 安

关于作者

叶蓬

虎符智库专家、北京盛华安信息技术有限公司联合创始人、副总裁。具有 20 余年 SIEM、安全管理（SOC）平台和态势感知领域从业经验，并对 SOAR 有较深入研究。

“乌克兰 IT 军队”网络攻击情况分析

作者 | 赵慧杰

编者按：

美国外交关系委员会数字和网络空间政策项目的助理研究员凯尔·芬多夫近日发文称，诸多黑客行动主义团体在俄乌冲突中选边站队，发起 DDoS 攻击，窃取和泄露大量数据，并参与旨在诋毁对方的信息战活动；对比而言，“乌克兰 IT 军队”较为公开透明，其发布的信息展示了攻击者如何在战争期间在网络空间开展行动，并显示出其技术能力的界限，以及其偏离网络行动国际规范和攻击民用目标的意愿；“乌克兰 IT 军队”的主要攻击方式是 DDoS 攻击（占比在 90% 以上），比大多数其他西方国家采取网络行动的意愿更强，攻击了政府控制外具有民用功能的目标，显示出对美西方关于对军事目标开展网络攻击规范的漠视。

“乌克兰 IT 军队”在俄罗斯的战役动态

我们对网络行动的理解几乎完全由防御者驱动。来自网络安全公司、非营利组织和政府机构的报告提供了网络行动的目标和对象的观点，但这种观点是片面的，只抓住了总体行动的点滴。“乌克兰 IT 军队”，一个为应对俄罗斯军事行动而组织起来的并且可能与乌克兰政府有关联的黑客组织，提供了一个独特的视角来了解进攻方的决策和行动，以及如何在战争中利用网络空间。

“乌克兰 IT 军队”诞生于俄乌战争初期。该组织始于 2022 年 2 月 26 日乌克兰副总理兼数字转型部长米哈伊洛·费多罗夫的一条简单推文，他写道“我们正在打造一支 IT 军队。我们需要数字人才”，并包含一个 Telegram 频道的链接，访问者可以在该频道中找到要攻击的目标列表。该组织背后的概念很简单：该频道的运营者提供对俄罗斯网站开展分布式拒绝服务（DDoS）攻击的工具，并每周 2 ~ 3 次发布目标列表供志愿者攻击。这些志愿者使用频道中的工具，在某些情况下还运用自己的黑客技能，来关闭俄罗斯互联网上的服务，包括银行网站、税务处理器和军用设备商店。该组织攻击了著名的俄罗斯网站，甚至成功地将俄罗斯总统普京在圣彼得堡经济论坛上的演讲推迟了 1 个多小时。

“乌克兰 IT 军队”提供一站式黑

“乌克兰 IT 军队”的主要攻击方式是 DDoS 攻击（占比在 90% 以上），比西方国家采取网络行动的意愿更强。

客体验。该 Telegram 频道识别范围广泛的目标，并为用户提供攻击这些目标的工具。该工具将用户的计算机添加到乌克兰政府运行的僵尸网络中，使参与支持乌克兰的黑客活动就像下载单个程序一样容易。乌克兰当局降低了爱国黑客的进入门槛，并大规模实施，因为该 Telegram 频道在高峰期拥有超过 30 万名订阅者，个别信息被浏览近 100 万次。

黑客行动主义并非新概念，黑客行动主义团体在俄乌冲突的双方都频繁出现，包括 KillNet、Xaknet 和“匿名者”等团体。这些组织和其他组织发起了 DDoS 攻击，窃取和泄露了大量数据，并参与旨在诋毁对方的信息战活动。

相比之下，“乌克兰 IT 军队”是透明的，公开和详尽地记录了网络冲突的进攻方。该 Telegram 群组充当了共享宣传、被盗文件和俄罗斯人个人信息的渠道，并充当了试图在俄罗斯社会的不同部分制造混乱的代理人。有关网络活动的信息通常是保密的，尤其是国家资助的活动，大多数信息是从网络安全公司和具有防御任务的政府机构的报告中收集到的。“乌克兰 IT 军队”虽然可能不像其他国家支持的网络团体那样以同样先进的技术水平运作，但它提供了一个了解各国在战时如何使用网络攻击的独特窗口。

值得注意的是，乌克兰政府曾表示只有文职官员参与了“乌克兰 IT 军队”，并否认有军方或情报人员参与其中。然而，外部研究人员表示，乌克兰情报团队可能与该组织密切合作，至少部分原因是“乌克兰 IT 军队”的攻击有可能导致“战略混乱和对国防与情报部门自身行动的战术干扰”。2022 年 10 月，“乌克兰 IT 军队”频道还承认了与乌克兰特种作战部队

（SSO）的合作，当时运营者泄露了“由 IT 军队和 SSO 专家共同努力获得的”俄罗斯纳税人数据。

01、方法

“乌克兰 IT 军队”的攻击目标包含在米哈伊洛·费多罗夫在俄乌战争初期推文发布的 Telegram 频道中。该频道包含各种宣传公告、攻击特定目标的号召，以及源于“乌克兰 IT 军队”中执行更先进操作的较小型非公共团队行动的数据泄露。

重要的是要注意 2022 年 10 月“乌克兰 IT 军队”的瞄准方法发生了变化，这影响了对“乌克兰 IT 军队”行动的任何分析。在此日期前，该 Telegram 频道被用来散布“乌克兰 IT 军队”想要攻击的 IP 地址和网站。在 2022 年 10 月 2 日，“乌克兰 IT 军队”运营者分享称将使用 DDoS 工具来协调活动，以避免俄罗斯人使用频道中包含的信息来快速支持加强对受影响网站的防御。“乌克兰 IT 军队”表示，其将转向“在攻击结束后分享一份揭示结果的报告”。这种变化，加上“乌克兰 IT 军队”维护的内部团队实施的攻击，增加了整个战役的不确定性，并且需要使用部门而不是单个组织来细分“乌克兰 IT 军队”的行动。

对这些消息的分析根据两个标准，包括攻击方法和目标组织所在的经济部门，将各攻击呼吁或已经发生的攻击报告分为几类。攻击方法使用美国外交关系委员会（CFR）网络行动跟踪器的标准进行评估，该标准将行动分为 7 类，其中 4 类已被“乌克兰 IT 军队”使用，包括破坏、拒绝服务、人肉搜索和污损。经济部门根据美国普查局维护的北美行业分类系统（NAICS）进行评估，该系统将企业分为 20 个部门，其中“乌克兰 IT 军队”已攻击 10 个：金融和保险；信息技术；批发和零售贸易；运输；石油和天然气钻探、

采矿和其他开采；公用事业；教育；制造业；政府；艺术、娱乐和休闲业，其中包括新闻媒体组织。国有企业被算作各自行业的一部分，而不是政府的一部分。

02、“乌克兰 IT 军队”的目标

“乌克兰 IT 军队”攻击了俄罗斯经济的多个不同领域，尤其是那些高度数字化的领域。该组织对金融业发起的攻击次数最多，在 93 条消息中将金融业列为攻击目标，几乎总是使用 DDoS 攻击，但在少数情况下会泄露从金融机构窃取的数据。信息技术公司超过 57 次成为攻击目标。这些攻击主要集中在用作服务提供商的软件上。作为减缓供应链、阻碍纳税和阻止俄罗斯人获得国家福利的手段，在这些公司中，电子文件准备和验证公司 12 次成为攻击目标。该组织还 55 次将政府网站和网络列为攻击目标。这些目标通常是政府机构的网站，如俄罗斯联邦安全局（FSB）、执政的统一俄罗斯党、国防部和外交部。这些通常是 DDoS 攻击，会使网站在短时间内瘫痪。在少数情况下，“乌克兰 IT 军队”发起了更长时间的 DDoS 攻击活动，旨在致瘫许可系统，如 2022 年 6 月对用于认证待售动物产品的统一州自动信息系统（EGAIS）的攻击。

“乌克兰 IT 军队”还攻击艺术、娱乐和娱乐行业达 42 次，主要是攻击俄罗斯新闻和社交媒体平台。除两个案例外，包括“乌克兰 IT 军队”破坏了克里米亚新闻网站和某俄罗斯寡头经营的一个设计网站。针对该行业的攻击几乎都是 DDoS 攻击。自冲突开始以来，贸易公司已成为 42 次攻击的目标，主要是在线购物和送货公司及技术进口商。作为对贸易部门的攻击的一部分，“乌克兰 IT 军队”经常对第三方设备供应商开展 DDoS 攻击，以阻碍俄罗斯军队购买额外的装备、食品或补给品。

该组织对运输部门发起了 14 次攻击，其中包括战争初期针对航空公司票务系统的多次 DDoS 攻击和针对航运公司的多次 DDoS 攻击。在针对该行业的唯一的一次非 DDoS 攻击中，“乌克兰 IT 军队”于 2023 年 2 月泄露了莫斯科地铁支付系统的相关文件。在运输行业，“乌克兰 IT 军队”避开攻击铁路网络。这可能是由于俄罗斯军方依赖其铁路网络将部队、设备和物资运送到前线，这使得该部门对网络间谍活动价值非凡。

“乌克兰 IT 军队”还袭击了包括石油和天然气公司和采矿公司在内的采掘行业，共计 9 次。主要针对俄罗斯天然气工业股份公司（Gazprom）等俄罗斯石油和天然气巨头的网站。该组织曾两次泄露了 Gazprom 的文件，详细列出了其在伊尔库茨克地区的业务，以及大量财务和员工记录。最后，该组织已袭击制造业达 5 次，主要针对生产支持俄罗斯战争活动企业，包括大型武器制造商卡拉尼什科夫集团（Kalashnikov Concern），以及为俄罗斯军队供应靴子的公司。

03、“乌克兰 IT 军队”避开的领域

该组织特别避开攻击俄罗斯互联网的几个领域。这些遗漏可能是多种因素造成的，包括缺乏先进的黑客技术，乌克兰方面不愿透露对更敏感目标的了解，或试图避免损害由更高级行为者开展的其他网络行动。正如今年早些时候在 Discord 上泄露的文件所示，美国情报机构经常使用从俄罗斯网络收集的信号情报来为情报产品提供信息。“乌克兰 IT 军队”2022 年 10 月与乌克兰特种作战部队（SSO）的合作表明，部分乌克兰军方正试图维持在俄罗斯网络上的存在。

未归入北美行业分类系统（NAICS）但基本上未被攻击的领域包括军事和情报网络。“乌克兰 IT 军队”几乎完全绕过这些区域，几乎可以肯定是由于这些网络中包含的情报。有两个“乌克兰 IT 军队”攻击机密网络的实例，均发生在 2022 年 3 月 3 日，目标是俄罗斯联邦安全局（FSB）和俄罗斯国家近卫军（Rosgvardia）的内部通信渠道。目前尚不清楚这些渠道的用途，以及它们是否真的被破坏了。

包括电力系统和供水公司在内的俄罗斯公用事业公司也未受到“乌克兰 IT 军队”攻击的冲击，仅成为 3 起

> “乌克兰 IT 军队”攻击俄罗斯经济的多个不同领域，尤其是那些高度数字化的领域，其中对金融业发起的攻击次数最多。

攻击的目标。“乌克兰 IT 军队”只对电力公司发起过一次 DDoS 攻击：2022 年 2 月，对白俄罗斯国家电力集团公司（Belenergo）网站的攻击。“乌克兰 IT 军队”还在 2023 年 2 月泄露了俄罗斯一家自来水公司的数据，其中包括 38000 名客户个人信息。2022 年 10 月 15 日，“乌克兰 IT 军队”宣布了一次更严重的攻击，声称其内部团队已瘫痪圣彼得堡所在的列宁格勒州电网。该事件表明“乌克兰 IT 军队”可能试图攻击俄罗斯能源基础设施，但由于对这些网络开展攻击需要高度的技能和准备，因此攻击是有限的。

除了一个案例，“乌克兰 IT 军队”还避免攻击教育服务部门。除攻击俄罗斯一家酒店预订网站的案例外，“乌克兰 IT 军队”基本上避开住宿和餐饮服务。“乌克兰 IT 军队”避开建筑、房地产、管理和咨询及废物处理部门。

专业、科学和技术服务部门也没有受到攻击。此外，“乌克兰 IT 军队”的攻击基本上避开了农业、林业、渔业和狩猎部门。

最后，“乌克兰 IT 军队”还未攻击医疗保健和社会援助部门。长期以来，国际法将医疗系统划为非战斗人员，至少到目前为止，“乌克兰 IT 军队”似乎尊重这一区别。

04、结论

“乌克兰 IT 军队”的信息展示了攻击者如何在战争期间在网络空间开展行动，并展示了其技术能力的界限，以及其偏离网络行动国际规范和攻击民用目标的意愿。DDoS 攻击占“乌克兰 IT 军队”消息中提及攻击的 90% 以上，与其他网络攻击相比通常很容易发起，并且仍然具有破坏性。“乌克兰 IT 军队”的破坏性攻击展示了更深层次的能力。根据美国外交关系委员会（CFR）网络行动跟踪器的显示，每年成功的破坏攻击次数从未超过 7 次。

“乌克兰 IT 军队”通过其目标选择，突破了国际规范的极限。其攻击政府控制外区域的意愿，其中大部分具有民用功能，例如，对金融部门的 93 次攻击和对俄罗斯新闻媒体的每周攻击，显示出对由美国和志同道合国家发布的关于对军事目标使用网络攻击的一些规范的漠视。然而，“乌克兰 IT 军队”似乎并非完全不受限制地开展行动。该组织在 2022 年发动一次攻击后撤回了对教育部门的攻击，再加上它不愿攻击医疗部门的事实证明，尽管其比大多数其他西方国家更愿意采取网络行动，但至少，一些领域仍然是禁区。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。

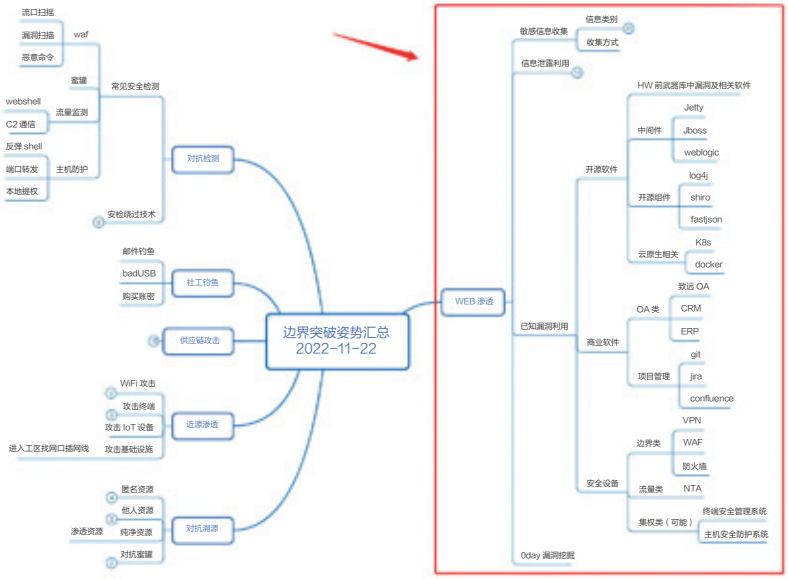
安全事件运营 SOP：网络攻击

作者 | 武鑫

在开篇《安全事件运营 SOP：安全事件概述》中，介绍了安全事件的定义、分级、处置原则及处置流程。当发生某类安全事件时，该如何快速处置，以及如何保证不同人员处置的效果都达标呢？

安全事件的种类虽然繁多，但是处理起来并非无据可循。为了解决上述两个问题，同时提升工作效率和降低安全风险，经过大量的运营处置实践，总结出以下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，分别对应介绍网络攻击方式、事件运营 SOP 及网络攻击防范措施。



1. 常见网络攻击

1.1 网络攻击概述

互联网上每天都充斥着各种网络攻击，如漏洞扫描、已知漏洞利用、DDoS 攻击、CC 攻击、网络爬虫等。本文介绍的网络攻击 SOP 主要指边界突破阶段，针对应用系统的一些攻击手法，如 Web 渗透、供应链攻击等。

1.2 网络攻击方式

就 Web 渗透而言，实际涉及到的漏洞，范围远不止字面意思上的应用系统层面。因为应用系统不可能单凭自身就可以运行，渗透又是一系列的操作，至少还包括如下内容。

- **敏感信息探测**：从外部视角来看，对攻击有用的信息，如端口开放扫描、源码备份文件扫描、应用服务框架识别、Swagger 存在敏感信息泄露；
- **已知漏洞攻击**：通常是使用漏洞扫描器（单一漏洞 / 综合漏洞）对目标系统进行扫描，根据漏洞检测规则发现已知漏洞，并进行利用导致系统被攻击。漏洞如果按照不同层面可分为基础层的系统及服务配置类漏洞，如基础环境的已知可利用漏洞、未授权类漏洞、弱账密类漏洞；应用层面的（即开发编写代码带来的安全问题），如 SQL 注入、Java 反序列化命令执行、文件上传等漏洞；基于业务场景的漏洞发现和利用，如已注册用户枚

举、任意账号密码重置、短信 / 邮件炸弹、短信 / 邮件纵向炸弹等。

在攻击技术日新月异的今天，供应链攻击成为最热门的方式，包括对人员账号、软件和硬件的攻击。此处，主要想提及软件投毒，由于软件产品基本都是开源组件 + 自研代码的组装，部分语言的存储仓库、社区管理不严格及 GitHub 自由开放等特性，攻击者可能上传恶意包并诱导他人进行下载。

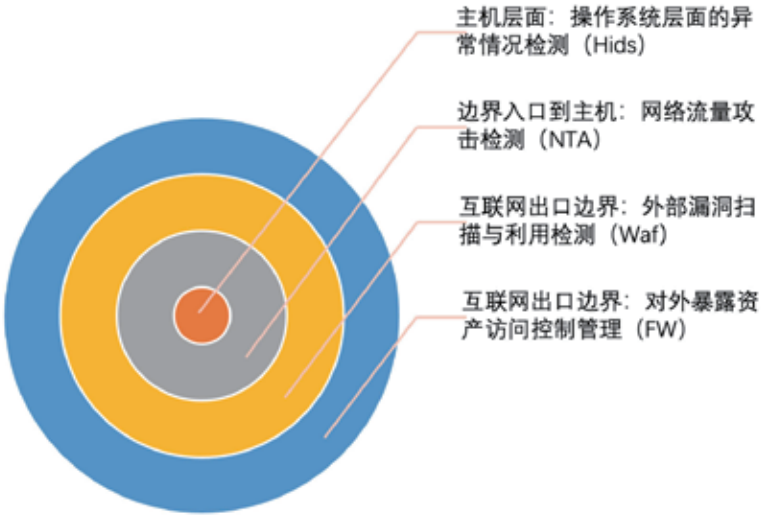
从安全运营的角度来看，最常见的攻击如下。

- **非法外连攻击：**开发使用的开源组件被投毒，应用所在服务器被远控，涉及到 metasploit 行为、CobaltStrike 行为等。

1.3 网络攻击检测

在攻击检测方面，除了传统的基于特征、异常、误用，机器学习和威胁情报等也得到了广泛应用。在企业的安全建设中不可或缺以上检测能力，通常体现在以下四类安全产品（每一类，列举一种产品加以说明）。

- **FW：**对应用上外网权限、对外暴露权限实现管控；
- **Waf：**对应用层的漏洞探测、利用进行检测及阻断；
- **NTA：**对网络流量进行安全分析，引入威胁情报提升已知攻击检测能力；
- **HIDS：**对主机层面如登录、进程异常等进行安全检测，往往作为最后一道防线。



2. 安全运营 SOP

网络攻击安全事件的处置，需要从攻击行为、攻击来源、攻击成功与否的状态等多个方面进行考量，不同情况的组合采取的措施略有差异。比如，在排除非公司资产的情况下，攻击源来自外网且发起大量扫描，则需在 FW 墙上进行封禁，再判断是否攻击成功；若攻击源是内网（已经被突破边界，如供应链投毒的场景），则应该进行网络、账号等权限的下线，并立即对源地址进行应急响应。简言之，在面对网络攻击事件时，有如下处置步骤。

2.1 攻击告警初判

从告警信息中提取攻击时间、源 IP（Sip）、目的 IP（Dip）、协议等基础信息，以时间为维度查看告警前后一段时间内，Sip 对哪些地址做过攻击或扫描，以及攻击是否成功。

2.2 攻击地址封禁

若 Sip 对一个或多个 Dip 发起大量攻击（如扫描），则需进行封禁处置。但在封禁之前，需要判断 Sip 是否为公司资产、是否在白名单中、是否为正常业务。若不是公司的资产，则在公网边界进行封禁并对 Dip 进行排查；若属于公司资产且在白名单中，则应检查是否为安全检测规则、安全运营策略等导致的误报。若属于公司资产但不在白名单中，则需联系业务或终端 Owner 确定是否为正常行为，若是正常或本人行为，则对业务进行加白或对相关 Owner 进行通报（尤其是在安全公司中，渗透测试需要授权，未授权的行为属于违规事件）；若是非业务或本人行为，则需立即开展业务故障排查、断网下线、溯源分析等应急响应动作。

2.3 攻击告警研判

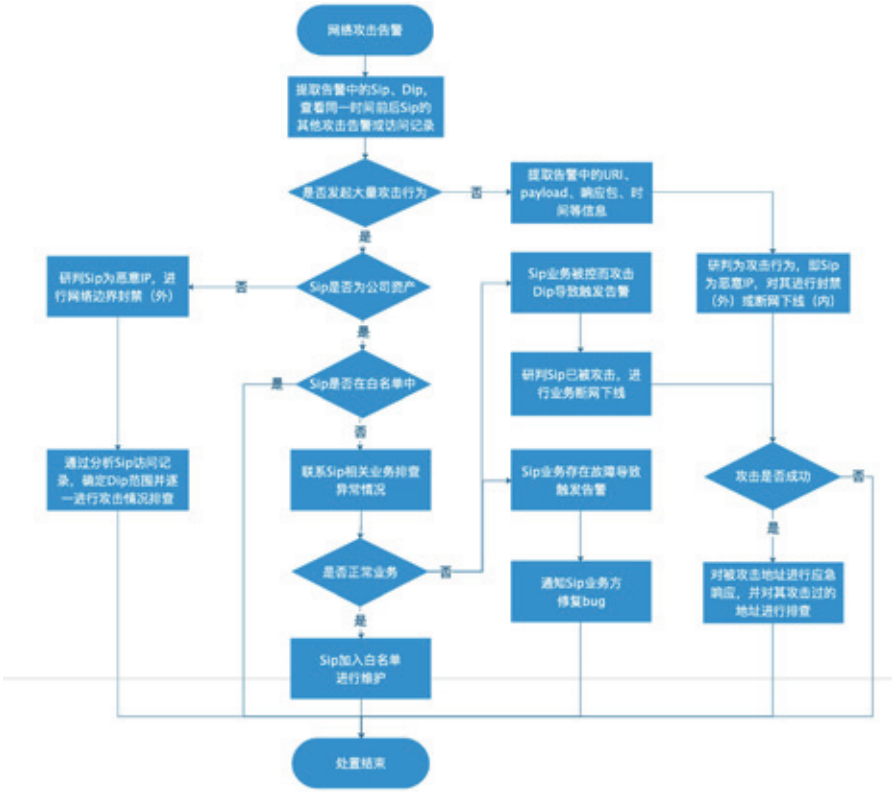
若 Sip 没有发起大量攻击，也需要对安全事件进行分析。从告警中提取URI、Payload、查看响应包状态等，甚至从日志、流量中提取更多上下文信息辅助分析攻击成功状态。

2.4 应急响应处置

若是攻击成功，则应立即断网下线，同时分别以 Sip 和 Dip 为基点，对整个攻击链进行溯源分析、后门清除等应急响应动作。

2.5 附 SOP 流程图

2.1~2.4 的处置流程，如下图所示。



3. 网络攻击防范

防范网络攻击是一门安全管理与技术融合应用的学科，涉猎范围较广，实现方法也有很多。但从 ROI 或仅从效果的角度来考虑，以下六种较为有效 & 高效。

3.1 减少对外暴露面

暴露面是指从互联网就能访问到的系统或使用的系统服务，具化为域名、IP、端口、API 等网络资产，减少它们对外的暴露情况，降低被攻击的可能性。

- **管住公网出口：**所有的内网地址均用 NAT 转化，统一形成几个出口对外暴露，通过使用负载均衡或防火墙进行收口管控。
- **互联网侧资产监控：**在外网部署资产扫描的节点，对公司所有的网段、域名和多级子域名进行全端口扫描及服务识别，7×24h 的进行资产监控。关于网段和域名的收集，实际的业务场景中除了传统 IDC，可能还有国内 / 外不同云厂商的地址，在最初的扫描前应该确定网段和域名范围。
- **互联网侧高危端口监控：**高危端口包括 21、22、23、873、1080、1433、1521、3306、6379、7001 等，其对应的服务可能存在弱口令、未授权、已知高危漏洞等风险，常常被攻击者所关注。需要注意的是，服务的端口号是可以修改的，在一些企业中懂技术的人员，通常会将远程连接的端口如 22 做映射为 2200，以逃过信

息安全部的限制或检测。

· 互联网侧高危 API 监控：敏感信息泄露、管理后台、密码找回、短信发送等接口，可能会存在安全问题，也常是攻击者喜欢寻找的点位。通过对应用日志进行关键字搜索，如管理后台可能的 url 为 /admin、/manage、/login 等。

3.2 系统上线前提测

在系统上线发布前嵌入安全活动，如白盒测试、黑盒测试和渗透测试，对系统进行安全自检，推进暴露出的安全漏洞或隐患修复。其中，比较关键的是安全卡点，通常没有业务方会花时间来进行安全测试，只有在发布流程中嵌入检查点才会有效。

· 内网发布系统：申请内网域名前，检查是否进行安全提测及是否通过；

· 外网发布系统：申请外网域名映射前，检查是否进行安全提测及是否通过；

· 已经发布系统：收集线上业务应用日志，对 API 资产进行监控。若出现 API 异常新增，就触发 Web 漏洞扫描器进行扫描。

3.3 供应商安全管理

供应链攻击的主要战场是其产品，对于安全水位高的企业而言，供应商的系统可能就是安全短板。例如：

· 服务部署在本地，中控服务在供应商侧，由于供应商中控服务失陷而导致被攻击；

· 服务部署在本地，与供应商系统无关联，仍旧会由于供应商被攻击而导致被攻击……

对于供应商产品的安全管理，业内其实已经有很多实践，如检查其产品的安全性报告（安全测试 / 代码审计 / 渗透测试）、要求其提供对外端口通信矩阵、提供系统框架及开源组件、系统上线前进行安全提测、签署应急响应协议保障其在运营阶段提供应急服务……这些都是有效的措施，但有时还是难以避免被攻击。目前做的比较好的应该是华为，对供应商进行赋能，并考量供应商自身的网络安全建设情况及产品研发流程的安全。

3.4 正确使用安全产品

想必每个企业都在使用网络安全产品，但是否会用或用得好，估计得

安全告警及运营有效性验证方案设计

验证类别	详细说明	实施方案	可行性判断
远控告警	使用多种远控以模拟多种钓鱼攻击	默认cobaltstrike（http/https/dns）	√
		具有伪装性的cobaltstrike（http/https/dns）	√
资产扫描告警	编写脚本进行资产扫描	IP/port 大规模扫描（常见端口）	√
已知漏洞POC扫描	已知漏洞POC扫描	log4j	√
		MS17-010	√
		OpenSSL heartbleed	√
用户名密码爆破	业务系统用户名密码爆破	对办公网段可以访问到的业务进行用户名密码爆破	√
ioc域名访问	模拟终端失陷后，数据回传行为	办公终端访问IOC域名	√
诱饵账号登录	模拟终端失陷后，黑客使用找到的密码登录并攻击业务	办公终端访问蜜罐节点	√
发送钓鱼邮件	模拟邮件钓鱼攻击	从外部定点定向发送钓鱼邮件（针对工作办公人员）	×
		从内部定点定向发送钓鱼邮件（针对工作办公人员）	×
端口穿透	模拟终端失陷后，黑客开启代理进一步攻击	开启内网端口穿透（如npc/frp）	√
		开启远程控制软件（如向日葵）	√

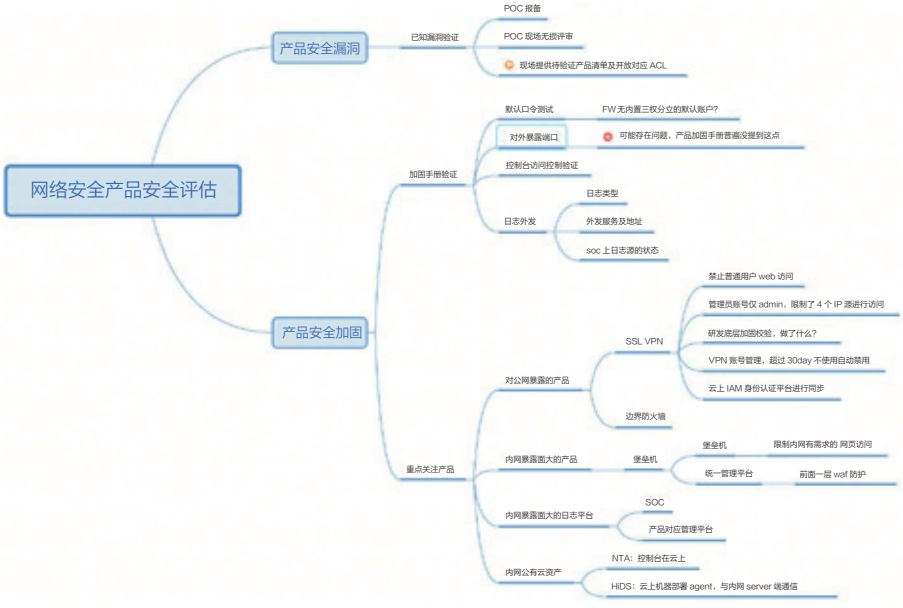
详细执行过程及检测效果评判

执行顺序	具体执行内容	检测效果评判	事件告警
1	打开向日葵软件	通过链接官方服务器的数据包成功检测	√
2	执行远控程序（直连）	通过IOC域名检测	√
	http方式通讯，执行指令有whoami/hashdump	有日志记录，但未触发告警	
	https方式通讯，执行指令有screenshot/hashdump/portscan	有日志记录，但未触发告警	
	dns方式通讯，执行的指令有whoami	通过dns请求域名判断	
3	通过向日葵远程控制其他主机	通过链接官方服务器的数据包成功检测	√
4	访问以下两个蜜罐节点	有日志记录	
	http://ip/ http://ip/		
5	使用ms17-010扫描一下c段ip/24	探针部署位置原因，没有日志产生	
6	执行远控程序（通过CDN转发）	有日志记录，但未触发告警	
	https方式通讯，执行指令有whoami/hashdump	有日志记录，但未触发告警	
	http方式通讯，执行指令有http/pwd	有日志记录，但未触发告警	
7	nmap -Pn 扫描c段 ip/24	探针部署位置原因，没有日志产生	
8	访问钓鱼域名 microsoft.com	通过IOC域名检测	√
9	nmap扫描c段 ip/24	探针部署位置原因，没有日志产生	
10	使用脚本扫描端口	探针部署位置原因，没有日志产生	
11	log4j poc请求蜜罐 ip	有日志记录，但没有告警	
12	开启npc，并进行端口映射配置	通过npc发送的数据包检测	√
13	对以下业务尝试进行用户名密码爆破	https流量不能解密	
	ip		
14	openssl heartbleed测试	NTA检测规则	√
	ip		

打个问号。从乙方中的甲方安全从业人员来看，常态化的使用安全产品、跟进告警并进行分析才是最好的打开方式，另外也别让安全产品带来额外的攻击面（尤其是边界类）。

·基于白盒产品安全能力验证：保证产品发挥效果的最佳实践方法。以安全告警及有效性运营为例，设计出关心 / 常用的安全功能并准备场景进行测试。

·产品自身安全加固能力验证：保障产品不被攻击的最佳实践方法。关注安全产品的历史漏洞修复情况、安全加固情况及重点产品（集控类 & 边界类）加强防护措施落地情况。



3.5 开设对外收洞渠道

SRC 作为企业安全团队对外宣传、接收漏洞的官方渠道，既起到沟通桥梁的作用，又可以通过接收到的漏洞反向优化安全防护策略。SRC 建设的早的企业，各类规则完善、人气高，基本拥有一群稳定的白帽子为其挖洞，白帽子也对业务越来越熟悉，也能发现更多有质量的安全漏洞。对于新建的 SRC，则需要通过不断的运营活动来提升行业影响力，吸引更多的白帽子加入。

·SRC 建立：包括门户建立、漏洞接收范围确定、奖励机制确定等。一是门户的建立，作为一个对外的门户，可以自研也可以通过国内的一些漏洞平台建立企业 SRC，漏洞平台的好处是有一定的白帽子基础、运营机制，相比较自研会更加高效快速上线，但也存在定制化功能和效果不佳的弊端。若是自研，可借助开源的程序进行修改，如 SRCMS、腾讯 xSRC（开源版）。值得注意的是，如果使用开源方案，则需要持续关注平台本身的漏洞情况，目前已经被发现不少安全漏洞。二是确定漏洞接收范围，仅限于主域名的子域名，还是包括所有与公司相关的资产漏洞？SRC 经常会接收到内部已知管理资产外的资产漏洞，白帽子的能力不容小觑，为避免发生争执需要提前明确。三是设置有明显区别的漏洞奖励机制，可根据资产重要性、漏洞利用直接造成的影响、漏洞利用条件等进行评判。比如，核心系统可利用前台 SQL 注入漏洞的评级，应该比核心系统管理员之后可利用的 SQL 注入和一般系统前台可利用 SQL 注入高，对应的奖励机制也会更高。对于奖励机制，直接进行 RMB

奖励会更吸引白帽子的参与度。

· **SRC 活动：**漏洞接收数量直接取决于参与白帽子的数量，衍生开可能涉及平台影响力、奖励机制等因素。白帽子拉新、白帽子促活、每逢佳节奖金翻倍、月 / 季 / 年度额外奖励……需要有规划、有吸引力的发起线上或线下活动，保持和白帽子的联系。

· **其他事项：**把跟白帽子的关系处理当作一项正式运营工作，给予白帽子感谢与尊重；注重在安全圈内的品牌，加入生态圈，与其他 SRC 一起活动，能吸引更多白帽子；制定内部漏洞审核和修复效率，别让线上漏洞暴露太久，也别让白帽子等待太久。

3.6 漏洞情报及预警响应

与攻击者比速度，在被已知 / 较新漏洞攻击前，自行先完成发现、修复或防护工作。主要涉及两部分工作：

· **预警监测输出高危漏洞 POC：**通过从安全媒介、软件官网、国内 / 外漏洞平台、社交软件等途径，实时获取漏洞情报信息、漏洞利用信息等，尤其应该关注重大保障活动前的“漏洞弹药”，并编写对应的 POC 在内 / 外部发起扫描。

· 联动资产优先发现互联网资产：无论是漏洞的发现，亦或是漏洞的修复，均需要明确存在漏洞的资产归属情况。基于资产（操作系统 / 应用 / 组件）进行漏洞扫描，可以提升扫描效率、降低网络流量；基于资产（重要级别 / 网络位置）进行漏洞修复判断，可以提高互联网侧的漏洞修复速率；基于资产（使用人 / 运维负责人 / 安全负责人）进行漏洞修复推动，可以提高整体的漏洞修复率。安

关于作者

武鑫

虎符智库专家，奇安信产品安全负责人，兼负责公司内部蓝军工作。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