内部发行 免费赠阅

出版物准印证号：京内资准字 2122- L0058 号

SECURITY INSIDER

网安26号院

奇安信网络安全通讯 · 安全快一步

关基保护最全解 P10

第26期
2023 年 2 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。

俄乌网络战一周年，关基保护进入深化期

2023 年我国首个关基标准将于 5 月正式实施，关基保护落实进入新阶段。

与此同时，俄乌冲突也迎来一周年。期间发生的激烈网络战，正在重塑现代战争中的形态，令现实的军事冲突与虚拟的网络攻击密不可分。

2022 年 2 月 24 日爆发冲突以来，俄罗斯对乌克兰的政府和关键服务进行了多次网络攻击。常用策略包括 DDoS 攻击、虚假信息活动和大规模擦除器攻击，试图通过网络攻击来摧毁关键基础设施，如针对电信服务商和能源供应商的攻击。这表明网络战将在未来战争中发挥重要作用。未来战争将既通过常规手段进行，也将越来越多地在无边界的网络空间领域进行。

俄乌冲突期间，基础设施成为了网络攻击首要目标：政府、能源、金融、交通、通信与制造六大行业攻击居前。根据截至 2022 年 9 月的统计，在 447 次行动中，针对政府行业的高达 134 次。战争期间攻击政府机构，中断和瘫痪政务服务，将会造成巨大的社会混乱。还值得注意的是，俄乌冲突期间，全球参与网络战组织达 89 个，为历史最高（截至 7 月 14 日）。全球参与的黑客人员达数十万之多，防护难度空前。

网络战的真实状况，或许如微软总裁 Brad Smith 所指出的，“比许多报告所披露的更为复杂和广泛”。我们需要记住的是，一场真正的全球网络战会是什么样子：电力和通信等关键基础设施部门相互依存，一次严重网络攻击可能会同时摧毁许多部门，包括摧毁重要基础设施并引发连锁反应，产生与自然灾害类似的影响。

俄乌网络战作为现代战争的重要组成，为我们的关基保护带来前所未有的启示：关基设施需要具备应对大规模、高强度、新型网络攻击的能力。

这意味着我们不仅需要构建全面的安全防护体系，还要不断借助各种创新技术，通过增加协同，才能防护住各种未知攻击；同时，做好应对现代网络战的准备，还意味着提升网络系统的弹性，尽一切可能将潜在损害降到最低。

不过，令人欣慰的是乌克兰在网络战中的表现。在俄乌之间长期的网络对抗中，乌克兰提升了自身的安全能力：面对前所未有的网络攻击，乌克兰关基设施显示出来强大的网络弹性，设法维持住绝大多数地区的基本公共服务。这说明，面对强大的网络攻击，成功的防守并非是完全不可能。在北京冬奥防护中所取得的“零事故”成绩，同样可以成为我们关基防护所追求的目标。

在本期，奇安信安全专家从标准解读、关键业务识别、风险评估、APT 检测防御及行动建议等多个角度，对关基保护进行深度解构，希望可以为关基防护提供一些参考。

总编辑

李建平

2023 年 2 月 1 日

CONTENTS 目录

安全态势

月度专题

关基保护全解读

2023 年我国首个关基标准将正式实施，关基保护落实进入新阶段。从标准解读、关键业务识别、风险评估、APT 检测防御以及行动建议，奇安信安全专家对关基保护进行深度解构。

《网安 26 号院》编辑部
主办 奇安信集团

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

奇安信集团　虎符智库　安全内参

索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

索阅邮箱：26hao@qianxin.com
地　　址：北京市西城区西直门外南路 26 院 1 号
邮　　编：100044
联系电话：（010）13701388557
出版物准印证号：京内资准字 2122-L0058 号
印刷数量：4500 本
印刷单位：北京博海升彩色印刷有限公司
印刷日期：2023 年 2 月 26 日
发行对象：奇安信集团内部

政策篇

国内，数据安全监管持续趋严，工业和信息化部公布《工业和信息化部行政执法事项清单（2022 年版）》，新增 15 条数据安全相关行政执法事项，国家邮政局审议并原则通过《寄递服务用户个人信息安全管理规定（送审稿）》；

国际上，比利时发布国家协调漏洞披露政策，提出上报者严格遵循相关要求发现并上报漏洞，即可豁免法律责任，以保护白帽黑客群体，专家称该政策对白帽黑客保护范围达到了欧盟迄今为止的最高水平。

国内

公安部和科技部联合部署推进科技兴警三年行动计划

2 月 15 日公安部官网消息，公安部、科技部联合印发通知，部署推进科技兴警三年行动计划（2023—2025 年），旨在构建公安战略科技力量体系，优化公安科技创新平台布局，增强公安重大业务需求科技支撑能力，完善公安科技人才梯队培育体系，形成科技兴警协同工作格局，提升科技创新支撑平安中国建设的水平。通知指出，要深入推进重大项目实施行动，在反电信网络诈骗技术、物证全息勘验技术、视频图像智能技术等领域布局，组织科技创新主体系统开展科研攻关。

证监会发布《证券期货业信息系统渗透测试指南》金融行业标准

2 月 7 日证监会官网消息，证监会发布《证券期货业信息系统渗透测试指南》金融行业标准，自公布之日起施行。该标准提供了一套通用的信息系统渗透测试框架，为在渗透测试策划、设计、执行、结果及风险管理等环节，保障测试质量、控制安全风险提供了操作指南。标准的实施将有利于规范行业机构安全、稳定地开展渗透测试工作，强化信息系统安全运行保障，提高行业网络安全防护能力，助力资本市场平稳运行。

数据安全列入《工业和信息化部行政执法事项清单（2022 年版）》

2 月 8 日工业和信息化部官网消息，工业和信息化部公布《工业和信息化部行政执法事项清单（2022 年版）》，新增了数据安全相关工业和信息化部行政执法事项清单共计 15 条（第 247—261 条）。其中包括：对工业和信息化领域数据处理者落实数据安全保护责任义务及管理措施落实的监督检查；对工业和信息化领域数据处理者开展数据处理活动，未加强风险监测，发现数据安全缺陷、漏洞等风险时，未立即采取补救措施的行政处罚；对工业和信息化领域数据处理者未经主管机关批准向外国司法或者执法机构提供存储于境内的数据的行政处罚等。

国家邮政局审议《寄递服务用户个人信息安全管理规定（送审稿）》

2 月 6 日国家邮政局官网消息，国家邮政局召开局长办公会，审议并原则通过《寄递服务用户个人信息安全管理规定（送审稿）》等。会议强调，邮政快递领域用户个人信息保护事关国家安全、公共安全和人民群众生命财产安全。要会同有关部门依法严厉打击泄露、买卖寄递服务用户个人信息等行为，落实好邮政管理部门监管责任，督促寄递企业加强网络安全数据安全和个人信息保护工作。要认真组织抓好规定宣贯落实，健全完善企业信息安全保护责任制，积极推进有效技术手段应用，强化个人信息安全实时监测能力，严密防范和遏制重大安全风险、事件发生。

国家能源局印发《2023 年电力安全监管重点任务》

1 月 30 日国家能源局公众号消息，国家能源局综合司于 1 月 17 日印发《2023 年电力安全监管重点任务》，要求杜绝出现重大安全事故，确保电力系统安全稳定运行和电力可靠供应，保持电力安全生产形势稳定。该文件提出了两项网络安全相关任务，包括推进电力行业网络与信息安全工作，开展电力行业关键信息基础设施安全保护专项监管。具体内容如下。

推进电力行业网络与信息安全工作。组织开展网络安全五年行动计划中期评估，持续推进电力行业网络安全“明目”“赋能”“强基”行动。加强网络安全态势感知能力建设，推进国家级电力网络安全靶场建设，组织开展年度攻防演练。修订行业网络安全事件应急预案，建立完善网络安全监督管理技术支撑体系，推动量子计算、北斗、商用密码等在电力行业的应用。

开展电力行业关键信息基础设施安全保护专项监管。制修订电力关键信息基础设施安全保护政策性文件，动态开展认定。对电力行业运营者落实关键信息基础设施安全保护要求的有关情况开展专项监管，印发《电力行业关键信息基础设施安全保护专项监管报告》。

国际

比利时发布报告 IT 漏洞的新法律框架，以保护白帽黑客

2 月 15 日 CCB 官网消息，比利时网络安全中心（CCB）发布报告 IT 漏洞的新法律框架国家协调漏洞披露政策，概述了不存在欺诈或伤害意图的个人或企业，该如何合法发现并上报比利时境内网络和信息系统的漏洞，无论易受攻击的系统属于私营或公共组织。该法律框架规定了数项基本原则，包括研究人员证明漏洞存在的行为应严格遵循必要性，发现漏洞必须尽快报告 IT 系统负责人，并按照规定程序报告给比利时网络安全中心等。比利时法律官员 Valéry Vander Geeten 表示，该政策对白帽黑客保护范围的全面性达到了欧盟迄今为止的最高水平。

美国 NIST 宣布轻量级密码学标准算法 Ascon，适用小型物联网设备

2 月 7 日 NIST 官网消息，美国国家标准与技术研究院（NIST）宣布，选中 Ascon 算法作为轻量级加密算法标准，以保护小型物联网设备产生的数据。Ascon 是一组轻量级认证加密和哈希算法的统称，包括 7 种算法，由格拉茨科技大学、英飞凌科技、拉马尔安全研究中心和拉德堡德大学的密码学家团队开发。NIST 后续将与 Ascon 算法开发者合作，起草新的轻量级密码学标准，征求公众意见并实施标准化。

美国 NIST 正式发布《人工智能风险管理框架》

1 月 26 日 NIST 官网消息，美国国家标准技术研究院（NIST）发布《人工智能风险管理框架》，旨在提供设计、开发、部署和使用人工智能系统的指南，降低应用人工智能技术的风险。《人工智能风险管理框架》主要内容分为两部分。第一部分介绍了组织如何界定与人工智能相关的风险，并概述了可信赖人工智能系统的特点。第二部分描述了四个具体功能：治理、映射、测量、管理，以帮助组织在实践中应对人工智能风险。

欧盟通过跨境获取电子证据法规和指令草案

1 月 25 日央视新闻消息，欧盟理事会发布公告称，欧盟理事会和欧洲议会就跨境获取电子证据的相关法规和指令草案达成协议。相关规定将使欧盟当局可直接向其他成员国相关数据提供方发送获取电子证据的司法指令。欧盟轮值主席国瑞典司法部长表示，新规则使法官和检察官能在证据消失前快速获取它们，无论这些证据存储在何处。

相关司法指令可涵盖各种类别的数据，包括用户、交易和内容数据，但只适用于满足特定条件的罪行，包括在指令发起国可判处最高监禁刑罚为 3 年以上，或与网络犯罪、儿童色情、伪造非现金支付方式或恐怖主义有关。

事件篇

国内发生重大数据泄露事件，45 亿条个人信息泄露并通过 Telegram 机器人提供公开查询服务，泄露数据包大小达 435GB，疑似电商或快递物流行业数据。用户仅需输入手机号，即可通过该机器人查询到姓名、手机号和详细的收货地址等隐私信息，引发各界关注。

因供应商遭勒索攻击，半导体巨头应用材料将损失超 17 亿元

2 月 17 日 The Record 消息，全球最大的半导体制造设备和服务供应商美国应用材料公司（Applied Materials）在财报电话会议上透露，有一家主要上游供应商遭到勒索软件攻击，将对公司第二季度出货造成影响，预计相关损失达 2.5 亿美元（约合人民币 17.17 亿元）。据多位行业分析师表示，该上游供应商应为美国公司 MKS Instruments，该公司在勒索攻击两周后仍处于“恢复阶段”。

勒索攻击迫使国际帆船之都奥克兰进入紧急状态

2 月 15 日 BleepingComputer 消息，因勒索软件攻击导致城市所有 IT 系统离线，新西兰奥克兰市临时行政官 G. Harold Duffey 宣布该市进入紧急状态。该起事件影响到了城市大量非紧急服务，当时离线的多个系统一周后仍未恢复，不过如 911 警务调度、消防及应急资源等紧急服务未受到影响。尚不清楚攻击者是哪个勒索软件团伙。宣布进入紧急状态后，奥克兰市加快政令实施、材料与设备采购，并在必要时召集应急工作人员。

疑似 45 亿条国内个人信息被泄露，输手机号可查询历史收货地址

2 月 14 日 21 世纪经济报道消息，2 月 12 日晚，Telegram 各大频道突然大面积转发某隐私查询机器人链接。网传消息称该机器人泄露了国内 45 亿条个人信息，数据包大小达 435GB，疑似电商或快递物流行业数据。用户仅需输入手机号，即可通过该机器人查询到姓名、手机号和详细的收货地址等隐私信息，引发各界关注。另据上海证券报，受此消息传播影响，2 月 15 日开盘，快递板块集体下挫，截至当日收盘，申通快递、顺丰控股、韵达股份跌幅均超过 2%，圆通速递跌幅近 6%。

以色列理工学院遭勒索攻击，被索要超千万元赎金

2 月 13 日 CyberScoop 消息，一个声名不显的网络犯罪团伙 DarkBit 在周末入侵了以色列理工学院，索要价值 170 万美元（约合人民币 1167 万元）的比特币。院方称该校“处于严重网络攻击威胁之下”“主动封锁了全部通信网络”。该团伙声称，这笔钱是要让以色列政府为其在侵占领土、战争罪及技术裁员等行为中的“谎言和罪行”付出代价。以色列理工学院（Technion）成立于 1912 年，被誉为中东的 MIT。

北约网站遭黑客攻击，包括“北约特种作战司令部”网站

2 月 13 日环球网消息，据《欧洲新闻周刊》援引德新社报道称，北约一名消息人士透露，包括“北约特种作战司令部”在内的多个北约网站于 12 日遭到黑客攻击。该消息人士透露，据称网络安全专家正在积极调查此事。北约方面没有提供其他

任何细节，只是表示该组织经常面临黑客威胁。据德新社消息，当天早些时候在社交网络上，特别是在推特上，有指控称亲俄黑客组织“killnet“的活动人士是此次黑客攻击的幕后黑手。

伊朗总统在国庆日电视直播的讲话遭黑客中断篡改

2 月 11 日 HackRead 消息，黑客组织“阿里的正义”（Edalat-e Ali）声称，对入侵伊朗国家电视台及广播电台的现场直播负责。该次攻击中断并篡改了伊朗总统易卜拉欣 · 莱希在革命日仪式上的演讲画面。当日，易卜拉欣 · 莱希在首都德黑兰阿扎迪广场发表直播演讲，与民众共同庆祝国家成立 44 周年。但黑客干扰了国家电视台的正常直播，转而放送“哈梅内伊去死”等口号。此外，他们还鼓励公民参加定于 2023 年 2 月 16 日举行的反政府抗议活动。

因网络攻击造成近亿元损失，英国半导体材料厂商股价大跌

2 月 7 日 The Record 消息，英国半导体材料厂商摩根先进材料（Morgan Advanced Materials）日前披露，1 月发生的网络攻击可能造成高达 1200 万英镑（约合人民币 9799 万元）的损失。该消息公布后，摩根先进材料的股价立即下跌超 5%，收盘时跌幅为 4.91%。此次事件的性质尚未得到证实，但从投资者公告来看，事件影响部分的描述基本可以断定是勒索软件攻击。该公司表示，旗下所有制造工厂均在正常运营。“只是在系统恢复期间，部分制造工厂临时转为手动操作流程。”

VMware 老漏洞遭大规模勒索利用：欧洲多国预警 已有数千个系统受影响

2 月 6 日 The Record 消息，法、意、芬等欧洲多国网络安全监管机构警告称，勒索软件攻击者正在“大规模主动利用”一个已存在近 2 年的 VMware ESXi 漏洞（CVE-2021-21974）。这次攻击被命名为 ESXiArgs，原因是勒索软件加密文件后，会创建一个扩展名为 .args 的附加文件。安全大数据公司 Censys 发现，欧洲和北美已有数千台服务器遭到破坏。奥地利计算机安全应急响应小组也发出警告，称“至少有 3762 个系统”受到了影响。据悉，意大利、法国、芬兰、美国、加拿大等国均遭到攻击。美联社报道称，勒索攻击发生时，意大利电信公司出现大规模互联网中断，意大利总理办公室已就勒索攻击发布了公告。

欧洲汽车经销商巨头遭勒索攻击，客户个人数据全部泄露

2 月 2 日 SecurityWeek 消息，英国汽车零售商 Arnold Clark 日前通知客户，其个人信息可能因网络攻击而失窃。该公司称在 2022 年 12 月 23 日沦为网络攻击目标。Play 勒索软件团伙表示对此负责，并声称掌握了数 GB 敏感信息。调查显示，恶意黑客可能已经窃取到客户个人数据，包括姓名、联系方式、出生日期、车辆信息、护照 / 驾照、国民保险号和银行账户等详细信息。据悉，Arnold Clark 在英格兰和苏格兰拥有 200 多家销售门店，销售超过 25 家汽车制造商的车辆，号称欧洲汽车零售行业中的龙头企业。

英国政府大臣要求地方政府掩盖勒索软件事件“灾难性”影响

1 月 31 日 The Record 消息，在英国国家安全战略联合委员会（JCNSS）日前举行的听证会上，雷德卡与克利夫兰自治市议会的领导人玛丽 · 拉尼根表示，某位政府大臣曾经要求她，对两年前当地发生的勒索软件攻击带来的“灾难性”影响保持沉默。她表示，来自中央政府的不讨论压力“给我们带来了很多问题”，致使最终承受了约 700 万英镑的损失，耗时 8 个月才重回原有状态。JCNSS 正在调查，英国的国家安全战略能否有效应对勒索软件引发的威胁。

俄罗斯外交部：美国正在入侵其网络空间

1 月 28 日央视新闻消息，塔斯社报道称，俄罗斯外交部副部长瑟罗莫洛托夫表示，美国正在网络空间实施自己的侵略计划。美方招募黑客雇佣兵，利用受其控制的盟友和私营公司的人工智能系统不断对俄罗斯的信息基础设施发动攻击。与此同时，美国利用间谍软件入侵个人通信设备和计算机，在全世界范围内盗取个人信息。

漏洞篇

微软邮件服务软件 Exchange Server 披露 3 个高利用可能性的远程代码执行漏洞，奇安信 CERT 已经确认其中 2 个可公开复现，鉴于这些漏洞影响较大，建议客户尽快做好自查及防护。

Microsoft Exchange Server 多个远程代码执行漏洞安全风险通告

2 月 17 日，奇安信 CERT 监测到微软发布 2 月补丁日安全更新，修复了多个 Microsoft 产品中的漏洞，其中包括 3 个利用可能性较高的 Microsoft Exchange Server 远程代码执行漏洞：CVE-2023-21707、CVE-2023-21706、CVE-2023-21529。经过身份认证的远程攻击者可利用这些漏洞在服务器账户的上下文中执行任意代码。微软将这些漏洞标记为“Exploitation More Likely”，奇安信 CERT 已确认 CVE-2023-21706、CVE-2023-21529 漏洞影响，鉴于这些漏洞影响较大，建议客户尽快做好自查及防护。

HAProxy 请求走私漏洞安全风险通告

2 月 16 日，奇安信 CERT 监测到 HAProxy 官方发布 HAProxy 请求走私漏洞 (CVE-2023-25725) 通告。通过构造特殊的 HTTP 请求可能导致绕过基于 HAProxy 的访问控制。由于此漏洞在解析 HTTP/1 的请求时可能丢弃部分重要的请求头字段，这在特定场景下可导致鉴权绕过等危害。鉴于此产品部署量较大，建议客户尽快做好自查及防护。HAProxy 是一个基于 TCP 和 HTTP 协议的开源应用程序代理。

Windows NTLM 权限提升漏洞安全通告

2 月 15 日，奇安信 CERT 监测到 Windows NTLM 权限提升漏洞 (CVE-2023-21746) 技术细节、PoC、EXP 在互联网上公开，国外研究人员将其称为“LocalPotato”。Windows NTLM 在进行身份验证时存在漏洞，允许拥有低权限的本地攻击者通过运行特制程序将权限提升至 SYSTEM。奇安信 CERT 已复现此漏洞，经研制，此 PoC 稳定有效，漏洞的现实威胁进一步提升。鉴于此漏洞影响较大，建议客户尽快更新至最新版本。

Apple 产品多个漏洞安全风险通告

2 月 14 日，奇安信 CERT 监测到 Apple 官方发布了多个安全漏洞，包括：Apple WebKit 任意代码执行漏洞 (CVE-2023-23529)、Apple Kernel 权限提升漏洞 (CVE-2023-23514)、Apple macOS Ventura 敏感信息泄露漏洞 (CVE-2023-23522)。

其中，CVE-2023-23529 较为严重，此漏洞允许未经身份认证的远程攻击者诱骗受害者访问其特制的恶意网站，使 WebKit 处理网页内容时触发类型混淆错误，最终在目标系统上实现任意代码执行。另外，攻击者可组合利用 CVE-2023-23529 和 CVE-2023-23514 提升权限并逃逸 Safari 沙箱。目前，已发现 Apple WebKit 任意代码执行漏洞 (CVE-2023-23529) 的在野利用，鉴于这些漏洞影响范围较大，建议客户尽快做好自查及防护。

Apache Kafka Connect JNDI 注入漏洞安全风险通告

2 月 9 日，奇安信 CERT 监测到 Apache Kafka 官方发布 Apache Kafka Connect JNDI 注入漏洞 (CVE-2023-25194) 通告，当攻击者可访问 Kafka Connect Worker，且可以创建或修改连接器时，通过设置 sasl.

jaas.config 属性为 com.sun.security.auth.module.JndiLoginModule，进而可导致 JNDI 注入，造成 RCE 需低版本 JDK 或目标 Kafka Connect 系统中存在利用链。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。Kafka Connect 是一种用于在 Apache Kafka 和其他系统之间可扩展且可靠地流式传输数据的工具。

IBM WebSphere Application Server 远程代码执行漏洞安全风险通告

2 月 8 日，奇安信 CERT 监测到 IBM 官方发布 IBM WebSphere Application Server 远程代码执行漏洞 (CVE-2023-23477) 通告，此漏洞允许未经身份验证的远程攻击者可通过构造特制序列化对象序列发送至目标服务器，从而在系统上执行任意代码。鉴于该漏洞影响范围较大，建议客户尽快做好自查，及时更新至最新版本。

Jira Service Management Server 和 Data Center 身份认证绕过漏洞安全通告

2 月 6 日，奇安信 CERT 监测到 Atlassian 官方发布 Jira Service Management Server 和 Data Center 身份认证绕过漏洞 (CVE-2023-22501) 通告，当 Jira Service Management 开启用户目录和邮件外发的写入权限时，攻击者可获取尚未登录过账户的用户注册凭证，最终攻击者可冒用这些用户身份获得对 Jira Service Management 实例访问权限。值得一提的是，大部分机器人账户容易被利用。鉴于该漏洞影响较大，建议客户尽快做好自查及防护。

ImageMagick 多个高危漏洞安全风险通告

2 月 3 日，奇安信 CERT 监测到 ImageMagick 信息泄露漏洞 (CVE-2022-44267) 和拒绝服务漏洞 (CVE-2022-44268) 的技术细节及 PoC 在互联网上公开，远程攻击者可通过制作恶意的 PNG 文件并上传至受影响的使用 ImageMagick 解析图片的网站来利用这两个漏洞，当网站或应用使用 ImageMagick 对恶意的 PNG 文件进行解析时将触发这两个漏洞，从而造成敏感信息泄露或拒绝服务。目前奇安信 CERT 已成功复现这两个漏洞。鉴于这些漏洞影响范围较大，建议客户尽快做好自查及防护。

F5 BIG-IP 格式化字符串漏洞安全风险通告

2 月 3 日，奇安信 CERT 监测到 F5 官方发布 F5 BIG-IP 格式化字符串漏洞 (CVE-2023-22374) 通告。经过身份认证的远程攻击者通过在 GET 请求参数中插入格式化字符串 (如 %s 或 %n)，可使得 iControl SOAP CGI 进程崩溃，或可能执行任意代码。目前，此漏洞技术细节及 PoC 已在互联网上公开，奇安信 CERT 复现此漏洞 PoC，经研判，漏洞利用影响有限，鉴于漏洞影响产品部署量较大，建议客户尽快做好自查及防护。

Adobe Acrobat 和 Reader 任意代码执行漏洞安全风险通告

2 月 3 日，奇安信 CERT 监测到互联网上公开 Adobe Acrobat Reader 任意代码执行漏洞 (CVE-2023-21608) 技术细节及 PoC，攻击者可以利用该漏洞制作恶意的文件，诱导受害者打开特制的文件，在当前用户的上下文中执行任意代码。目前，奇安信 CERT 已在 32 位版本程序中已复现此漏洞，经研判，在 Adobe Acrobat Reader 64 位版本上进行漏洞利用实现远程代码执行的难度较大。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

QNAP QTS 和 QuTS hero SQL 注入漏洞安全通告

2 月 1 日，奇安信 CERT 监测到 QNAP 发布 QNAP QTS 和 QuTS hero SQL 注入漏洞 (CVE-2022-27596) 通告，QNAP QTS 5.0.1 和 QuTS hero h5.0.1 中存在 SQL 注入漏洞，未经身份认证的远程攻击者可利用此漏洞注入恶意代码。此漏洞仅影响 QNAP QTS 5.0.1 和 QuTS hero h5.0.1，建议客户尽快做好自查及防护。安

注：使用公司邮箱发送公司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。

关基保护最全解

2023 年我国首个关基标准将正式实施，关基保护落实进入新阶段。
从标准解读、关键业务识别、风险评估、APT 检测防御以及行动建议，
奇安信安全专家对关基保护进行深度解构。

不止合规
—关基设施保护发展历程及行动建议

作者 | 黄凯

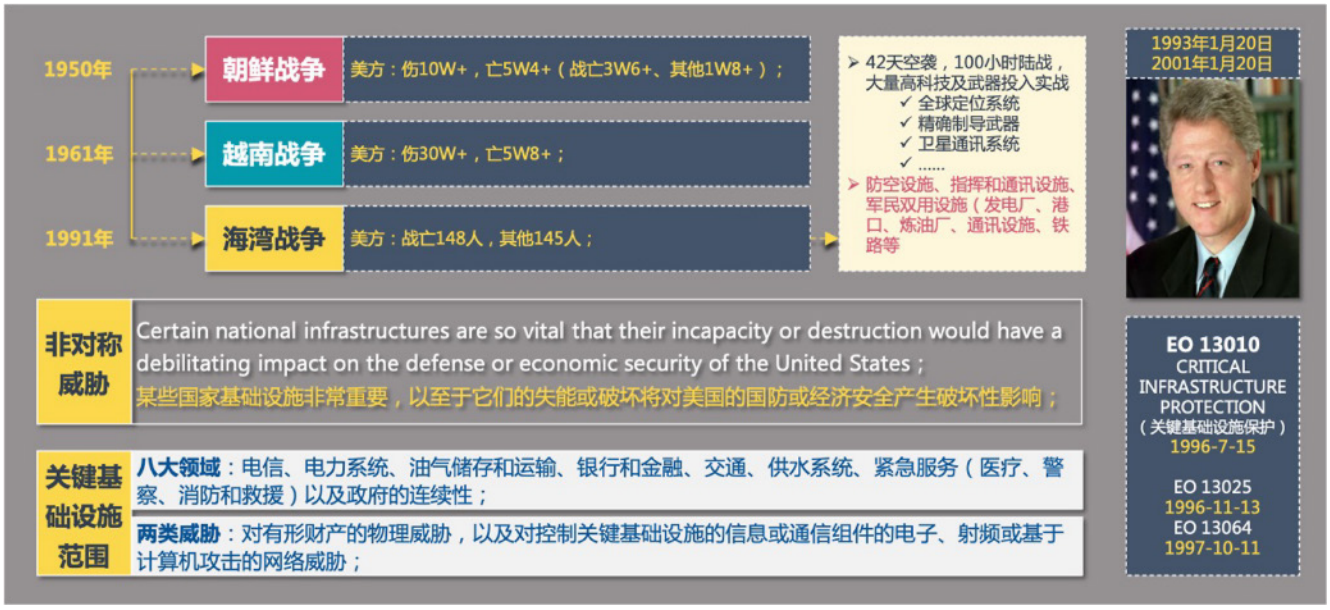
一、概念诞生

1991 年海湾战争，经过对伊拉克防空设施、指挥和通信设施、军民双用设施（发电厂、港口、炼油厂、铁路）等历时 42 天的空袭，美国领导的联军部队最终以轻微的代价取得了决定性的胜利。

海湾战争结束后，美军首次正式提出非对称作战理论，随着理论的外延和内容不断的扩大，美国意识到某些国家基础设施的重要性，一旦遭受破坏将对美国的国防或经济安全产生破坏性影响。基于此，美国总统克林顿于 1996 年 7 月 15 日发布关键基础设施保护总统行政令。“关键基础设施”的概念由此诞生。

二、美国关基设施保护发展历程

从 1996 年开始，美国关键基础设施保护涉及的行政令、总统令、网络空间安全国家战略、国家基础设施保护计划、信息系统保护国家计划、改善关键基础设施网络安全框架、网络安全国家



行动计划等共计近 30 余项，总体可分为三个阶段。

1、评估阶段（1996 年 7 月～ 2001 年 9 月）

克林顿总统在 1996 年 7 月份发布 13010 号《关键基础设施保护》，定义了关键基础设施的概念及相关领域范围。同时行政令中明确要求设立总统关键基础设施委员会，该委员会的具体职责涉及评估关键基础设施的脆弱性及威胁、建议针对关键基础设施保护的相关国家政策及实施战略。基于此，历时 15 个月时间，总统关键基础设施委员会在 1997 年 10 月发布了《保护美国基础设施》的报告，核心内容是风险威胁很多，有效的防御措施很少，并且从建立伙伴关系、法律行动、研究开发、意识教育等方面给出行动策略。

为了落实“保护美国基础设施”报告内容，深化关键基础设施保护工作，克林顿总统在 1998 年 5 月发布 63 号总统令《关键基础设施保护》，强调了针对关键基础设施的保护工作，将会采取一切必要措施，并要求委员会提交一份国家基础设施保障计划的时间表，包含“保护美国基础设施”报告中提到的部分行动策略。

除了第二次世界大战时日本偷袭美国海军基地珍珠港，美国本土并未遭受恐怖袭击或军事攻击事件，美国的敌人很少有能力严重威胁美国的心脏地带，网络空间领域也同样如此，由于美国的信息和通信技术处于世界顶尖水平，美国的关键基础设施也是世界上最好的，虽然知道通过网络发起攻击对关键基础设施造成伤害的能力真实存在，但是并未能清晰的识别具体的攻击手段及造成的破坏性影响，所以在这个阶段很大一部分的内容都是在针对关键基础设施开展脆弱性评估工作。

2、体系初现（2001 年 10 月～ 2014 年 2 月）

911 恐怖袭击事件后，美国国会认为，美国遭到恐怖攻击的原因是情报单位之间的竞争，造成国家安全情报无法正确快速地传达给重要决策人士，为消除部门间无法彼此协调的问题，布什总统在 2001 年 10 月 8 日第 13228 号

行政命令中要求建立国土安全办公室和国土安全委员会，其使命是保护美国及其关键基础设施免受恐怖袭击，并于2002年11月25日签署美国参议院通过的《国土安全法案》，国土安全部正式成立。

2003年2月，美国国土安全部发布《网络空间安全国家战略》，作为《国家国土安全战略》的重要组成部分，其战略目标与国土安全战略保持一致，并明确提出了五个国家优先事项（建立国家网络空间安全响应系统、国家网络空间安全威胁和漏洞减少计划、国家网络空间安全意识和培训计划、保障政府网络空间安全和国家安全和国际网络空间安全合作），给出了体系化的行动建议，有助于预防、威慑和防范针对关键基础设施的攻击。

之后相继发布的7号国土安全总统令《关键基础设施识别、优先排序和保护》、54号国家安全总统令/23号国土安全总统令《网络安全政策》及其配套的《国家基础设施保护计划》和《国家网络安全综合计划》等，都在不断完善关键基础设施保护体系，包括但不限于细分保护对象、明确组织架构、完善指标标准、制定保护计划、定义风险管理框架等内容。

2013年2月，奥巴马总统在13636号行政令《改善关键基础设施网络安全》明确要求NIST美国国家标准与技术研究院领导制定降低关键基础设施网络风险的基线框架（Cybersecurity Framework网络安全框架），并且在在一年内发布网络安全框架的最终版本，以帮助关键基础设施的所有者和运营商识别、评估和管理网络风险。2014年2月，《改善关键基础设施网络安全框架》正式发布，该框架侧重于使用业务驱动因素来指导网络安全活动，是基于风险的网络安全风险管理方法，并将网络安全风险作为组织风险管理流程的一部分，旨在减少和更好的管理网络安全风险。自此，以识别、保护、检测、响应和恢复的关键基础设施保护体系初步形成。

3、完善执行（2014年2月～至今）

2015年12月18日，奥巴马总统签署了《2015年网络安全法案》，从立法层面加强了网络安全保护，明确了国土安全部在网络安全领域的主责地位，确立了政府和私营企业信息共享、应急响应、风险评估、人才培养等工作的法律责任和义务。2016年奥巴马政府发布《网络安全国家行动计划》，明确指出要增强关键基础设施的安全性和抗打击能力。2017年5月特朗普签署EO13800号行政令《加强联邦网络和关键基础设施的网络安全》，加强关键基础设施网络安全保护。该行政令明确了风险评估报告的基本要求，重点关注信息通信系统、电力系统网络安全能力的评估。2018年NIST美国国家标准与技术研究院发布《改善关键基础设施网络安全框架》V1.1版本，为关键基础设施提供了更细粒度的指导。在燃油管道勒索事件后，拜登政府发布《改善关键基础设施控制系统网络安全》的国家安全备忘录，提出建立工业控制系统网络安全倡议和推进工业控制系统网络安全计划等内容。历经五任总统二十六年时间，关键基础设施保护体系已经逐步完善，更加强化落地执行。

> 2015年7月1日通过的《国家安全法》明确提出关键基础设施的概念：
> “国家建设网络与信息安全保障体系，
> 提升网络与信息安全保护能力，
> 加强网络和信息技术的创新研究和开发应用，
> 实现网络和信息核心技术、关键基础设施
> 和重要领域信息系统及数据的安全可控”。

三、我国关基设施安全保护进展

中国关键（信息）基础设施的概念最早可追溯到七年前。

2015年7月1日通过的《国家安全法》，“第二章 维护国家安全的任务”中第二十五条明确指出“国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控”。自此，关键信息基础设施安全保护的相应动作开始显现。

2016年4月19日，习近平总书记《在网络安全和信息化工作座谈会上

的讲话》中明确指出，要“加快构建关键信息基础设施安全保障体系”“关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标”，必须深入研究，采取有效措施，切实做好国家关键信息基础设施安全防护。

为贯彻落实习近平总书记“4·19讲话”中关于“加快构建关键信息基础设施安全保障体系”的重要指示精神，指导关键信息基础设施网络安全检查工作，中央网络安全和信息化领导小组办公室在2016年7月发布《关于开展关键信息基础设施网络安全检查的通知》（中网办发【2016】3号文），要求进行全国范围内关键信息基础设施的摸底和检查工作，各地区各行业纷纷发文开展关键信息基础设施网络安全检查相关的工作。

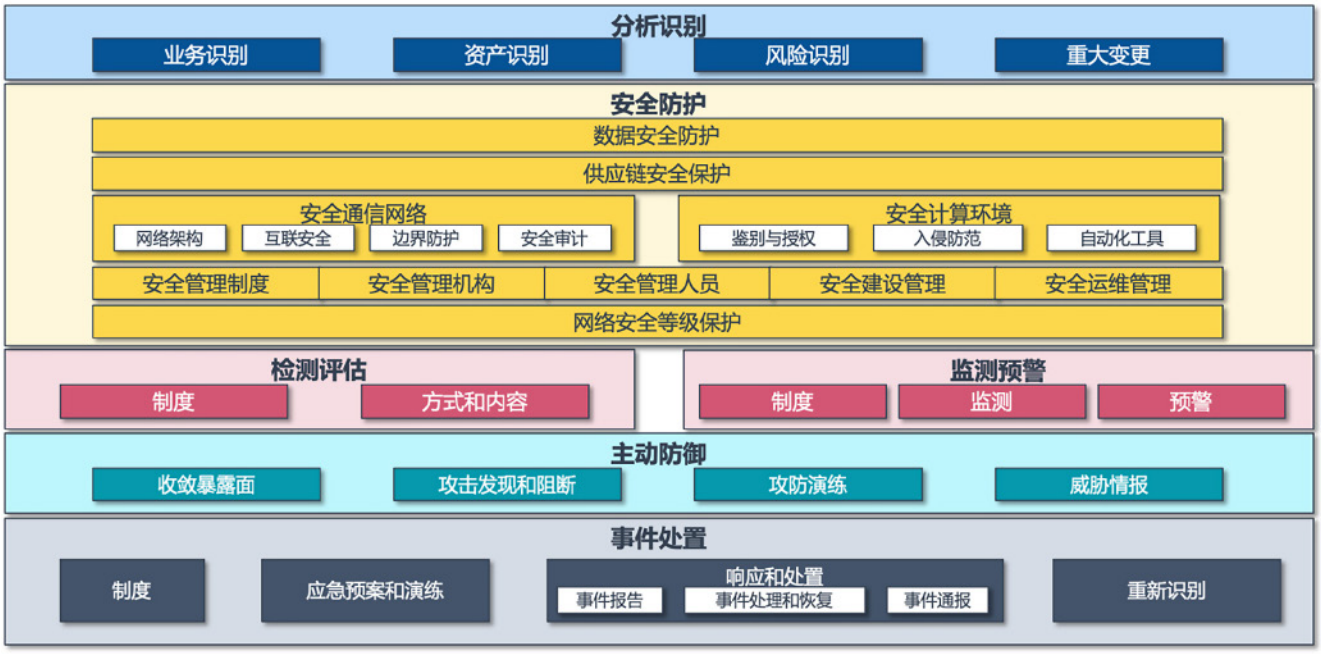
2016年11月7日通过、2017年6月1日起正式施行的《网络安全法》，强调在网络安全等级保护制度的基础上对关键信息基础设施实行重点保护，明确关键信息基础设施的运营者负有更多的安全保护义务，并配以国家安全审查、重要数据强制本地存储等措施，确保关键信息基础设施的运行安全。

2017年7月11日，国家互联网信息办公室发布了关于《关键信息基础设施安全保护条例（征求意见稿）》公开征求意见的通知。作为《网络安全法》的重要配套法规，《关键信息基础设施安全保护条例（征求意见稿）》对关键信息基础设施的范围、各监管部门的职责、运营者的安全保护义务，以及安全检测评估制度提出了更加具体、操作性也更强的要求，为开展关键信息基础设施的安全保护工作提供了重要的法律支撑，自此，与之配套的关键信息基础设施安全保护标准体系开始制定，并逐步开展关键信息基础设施安全保护的试点工作，验证关保基本要求内容的合理性和可操作性，为标准推广实施积累经验，为关键信息基础设施安全保护工作提供技术支撑。

2021年7月30日，《关键信息基础设施安全保护条例》正式签发，2021年9月1日施行。从支持与保障、关键信息基础设施范围、运营者安全保护、产品和服务安全、监测预警、应急处置和检测评估、法律责任等诸多方面，对于关键信息基础设施保护相关的一系列制度要素作了更为具体的规定，保护条例的发布也意味着我国关键信息基础设施保护工作从规划走向落实，与之配套的《关键信息基础设施安全保护要求》（GB/T 39204-2022）（以下简称《保护要求》）于2022年11月7日正式发布，该标准作为关键信息基础设施安全保护标准体系的构建基础，将于2023年5月1日正式实施。

作为我国第一项正式发布的关键信息基础设施安全保护的国家标准，《保护要求》提出了以关键业务为核心的整体防控、以风险管理为导向的动态防护和以信息共享为基础的协同联防的安全保护三个原则，针对六个方面提出了111条安全要求，用于指导运营者开展关键信息基础设施安全保护相关工作。

> 作为我国第一项关基保护的国家标准，《保护要求》提出了以关键业务为核心的整体防控、以风险管理为导向的动态防护和以信息共享为基础的协同联防的安全保护三个原则。



四、《保护要求》要点解读

《保护要求》包含分析识别、安全防护、检测评估、监测预警、主动防御、事件处置六个方面。

（一）分析识别

在关键信息基础设施安全保护施行前，国内网络安全合规遵循的最多的是等级保护相关的制度进行建设，它的前身是基于美国 IATF 信息保障技术框架，是建立在信息基础设施的概念上。伴随着信息化发展及 IT 变革数字化转型，安全的本质是要解决业务连续性和安全风险相关的问题，脱离业务就很难让安全达到很好的效果，所以关键信息基础设施安全保护更多是从业务视角出发，是面向业务的安全治理，需要识别关键业务，针对关键业务与其相关联的外务业务开展依赖性识别、重要性识别，并梳理关键业务链，基于关键业务链依赖的资产清单去开展风险评估的工作。

（二）安全防护

《网络安全法》《关键信息基础设施安全保护条例》均要求对关键信息基础设施在等级保护的基础上实行重点保护。根据已识别的关键业务、资产、安全风险，在安全管理制度、安全管理机构、安全管理人员、安全通信网络、安全计算环境、安全建设管理、安全运维管理、供应链安全、数据安全等方面实施安全管理和技术保护措施，确保关键信息基础设施的运行安全。

（三）检测评估

《网络安全法》中“关键信息基础设施运行安全”一节第三十八条明确提出要求“关键信息基础设施每年至少进行一次检测评估”，《关键信息基础设施安全保护条例》第十七条要求“运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估”。与之配套的《保护要求》重点讲的是安全防护前的业务、资产、风险的分析识别及安全防护后的监测

预警和事件处置，重心是在分析面临的安全威胁及发现安全问题，分析威胁及问题带来的安全风险，用于运营者提升安全保护水平和能力，本质上是把关注安全的建设过程牵引到关注业务的结果导向，在满足合规性的同时更多地去考量有效性，提升应对大规模网络攻击及 APT 攻击能力。

（四）监测预警

《信息安全技术 网络安全监测基本要求与实施指南》（GB/T 36635-2018）给出了网络安全监测框架和实施指南，《信息安全技术 网络安全预警指南》给出了网络安全预警的分级指南与处理流程，保护要求从制度、监测、预警三个方面，从制定并实施网络安全监测预警和信息通报制度、针对发生的网络安全事件或发现的网络安全威胁提前或及时发出安全警示给出了细化的指导。结合正在进行中的关键信息基础设施安全监测预警要求，将监测场景分为三类，常态监测在互联网出入口、内外网连接处、内网重要节点等进行实时监测；如果接受到授权机构的预警信息、或在重点时期、或监测发现异常，则需要升级到重点监测；如果监测发现疑似安全事件，则升级为事件监测。常态监测、重点监测、事件监测的监测强度是逐级增加的，切实加强关键信息基础设施安全保护。

（五）主动防御

《保护要求》的制定经历了四个阶段，从最早没有该部分内容到新增“对抗反制”环节，继而调整为“技术对抗”，最终发布的是我们现在看到的“主动防御”，该部分内容更加强调积极防御的能力，以对攻击行为的监测发现为基础，主动采取收敛暴露面、诱捕、干扰和阻断等措施，开展攻防演习和威胁情报工作，提升对网络威胁与攻击行为的识别、分析和和主动防御能力。

（六）事件处置

事件处置要求：运营者对网络安全事件进行报告和处置，并采取适当的应对措施，恢复由于网络安全事件而受损的功能或服务。

五、行动建议

1、落实关键信息基础设施安全保护责任

确立网络安全总策略，制定适合本组织的网络安全保护计划，结合关键业务链的安全风险，明确关键信息基础设施安全保护工作的目标、安全策略、组织架构、管理制度、技术措施等内容，加强机构、编制、人员、经费、装备、工程等资源保障，支撑关键信息基础设施安全保护工作。在次过程中明确六大关键要点：一是将网络安全确定为关键信息基础设施建设的“底板工程”，将安全工作纳入企业工程管理范畴；二是开展专项规划，通过工程和任务设计，明确安全预算在 IT 预算的占比，建议不低于 10%；三是设置专门的网络安全管理机构，任命首席安全官，明确网络安全责任制，并确保机构负责人和关键岗位经过背景审查。网络安全团队人数在 IT 团队总人数的占比，建议不低

《保护要求》包含
分析识别、安全防护、检测评估、
监测预警、主动防御、 事件处置六个方面。

于 8%；四是加强全周期安全管控，将安全工作融入到信息化建设的需求评审、架构设计、编码、集成、测试、部署、发布等环节；五是开展安全需求控制和安全系统建设架构管控，确保网络安全立项建设的内容与安全规划相符合；六是建立面向成效的安全考核指标机制，编制安全成效考核指标，以数据为安全管理工作提供依据，为安全能力建设提供决策支持。

2、强化关键信息基础设施技术防护措施

结合自身数字化业务发展情况，开展网络安全体系化防护。一是加强关键信息技术设施资产安全管理，针对关键信息基础设施的资产情况和安全保护状况要做到底数清、情况明，全面掌握关键信息基设施的软 / 硬件设施、重要业务系统和重要数据的资产情况。应定期清查与关键信息基础设施及与其相关的资产底数，根据关键业务链所依赖资产的实际变化等，建立资产档案并及时动态更新。二是落实关键信息基础设施重点防护措施，在现有安全保护措施的基础上，梳理关键信息基础设施网络结构和数据流向，合理分区分域，完善边界防护策略，收敛互联网暴露面，加强网络攻击威胁管控；加强供应链安全管理，定期梳理、更新供应链企业、产品、人员清单，掌握供应链底数，定期对供应链企业和产品开展安全检查和技术检测，开展源代码安全审计及开源代码和第三方组件安全检测，及时发现处置重大问题隐患；开展数据安全治理，梳理数据资产，建立面向数据生命周期的安全管控与防护能力；推进信创工程，建立自主可控的信息化基础设施底座。建立基于自己的 IT 底层安全架构和安全标准，从底层生态解决国外产品存在未知后门和非法监控。三是建设监测预警体系，结合自身业务特点，在网络关键节点，对关键信息基础设施涉及的网络、系统等网络流量进行监测，部署攻击检测设备，发现网络攻击和未知威胁，在流量监测的基础上全面收集网络安全日志，构建违规操作模型、攻击入侵模型、异常行为模型，强化监测预警能力。

> 关键信息基础设施保护工作涉及到国家指导、行业保护、网络服务机构、运营者落实等多方协同，需要落实责任、强化技术防护措施、构建保障体系。

3、构建关键信息基础设施安全保障体系

一是加强网络安全教育培训，树立科学正确的网络安全观。常态化开展全员网络安全意识教育培训和技能考核，配置适当的关键信息基础设施从业人员和网络安全关键岗位从业人员的年度培训时长，教育培训内容应包括网络安全相关制度和规定、网络安全保护技术、网络安全风险意识等。二是开展攻防演习，通过实战化的攻防演习展示网络安全状态。使运营者能够直观看到目标系统面临的网络安全威胁，同时促使关基运营单位用户对网络安全的风险认知从基于安全漏洞类型、数量和严重程度等方面的风险认知过渡到基于损失程度以及危害程度的影响认知，提升网络安全的实战化能力。不具备实战环境的情况下，可通过网络安全实验室，建设网络安全仿真平台，工业控制领域建立测试床等仿真环境。开展网络安全攻防模拟演练，依托实验环境，开展新技术研究。模拟场景化网络安全环境，提出适用于关基运营单位的网络安全方案，提升实战能力。三是建立运行保障体系，针对性设置技术、监测等安全人员岗位，确定安全监控、安全分析、安全响应等各类角色，明确岗位职责，通过制定标准工作流程，设计安全事件监控、发现、分析、通告、响应、处置、复核等全周期的安全运营流程，确保安全运营工作闭环管理，针对安全事件的响应、处置等工作的时效、质量等进行评价。定期开展资产管理、安全监测、威胁分析、关联规则优化等工作，通过安全运营做到问题早发现、快响应、早根除，确保关键信息基础设施安全稳定的运行。

结束语

数字化转型前，信息化是支撑工具，数字化转型过程中，IT 逐步成为生产力引擎，业务与信息化深度融合后，网络安全风险等同于业务风险。运营者需要结合自身关键业务情况，健全关键信息基础设施安全保护体系，在满足合规的基础上保证有效性，继而保障业务安全运行，为我国数字强国之路保驾护航。

数字经济下的关键信息基础设施监管

作者 | 宗剑

我国已经在中央层面最开始进行数字经济的系统化布局，在全国大市场的基本原则的下，正在建设基于数据要素的社会经济系统基础规则体系，通过传统要素的数字化改变现有经济要素的配置方式，引发行业、市场和体系的创新，同时通过产业数字化转型，逐步改变数据资产和相应的运营方式，以及数字空间与实体空间的相互作用，提升数字治理能力，加速数字技术与实体经济的融合。

数字经济是指以使用数字化的知识和信息作为关键生产要素、以现代信息网络作为重要载体、以信息通信技术的有效使用作为效率提升和经济结构化的重要推动力的一系列经济活动。

随着数字经济的不断发展，数字基础设施的概念不断扩展，在原有云计算、移动互联网、物联网等信息基础设施的基础上，也包括公路、建筑、电网、油气管道等传统的基础设施的数字化改造。因此，在数字经济的大背景下，提升关键信息基础设施安全的监督和管理水平，是网络安全是产业数字化和社会数字化转型的管理基础，同时也对于关键信息基础设施的管理、分析能力和协调指挥体系的构建上有更新的要求。

一、完善关键信息基础设施的管理体系

在数字经济时代和新基建的战略举措下，对于中国数字经济的进一步发展、传统产业的数字化提升奠定了基础，在传统的基础设施行业数字化转型所形成的新型基础设施，尤其是人们创造财富所应用的数字化工具（硬件、软件、算法等），数字对象（数据、信用等）将构成新形态下的关键信息基础设施，使得在数字化功能和传统能力相叠加，从而能够提升传统业务的数字化水平。

但是当前管理现状存在大量的监管盲区，对于数字化系统的备案、认证、上 / 下线、变更、日常运营等全生命周期的管理，特别是上线前的代码审计、风险评估，运行中的敏感数据检查、日志审计等一系列的资产准入、合规和安全性检查缺乏有效的运行管理机制。

因此，数字经济下的关键信息基础设施管理强调四个层面的管理。

1、 基础信息维度，包括相关的管理责任单位、系统关联资产、网络拓扑等一系列基础信息。

2、 安全监测维度，包括系统脆弱性、受攻击情况、受威胁情况、攻击者

> 在数字经济的大背景下，
> 提升关键信息基础设施安全的监督和管理水平，
> 是网络安全是产业数字化和社会数字化转型的
> 管理基础。

情况及系统相关安全防护措施等数据。

3、 安全生态维度，包括系统的设计、建设、支撑、运维单位，域名解析、运营服务商、系统监测服务商等数据。

4、 管理业务维度，汇聚展示系统备案信息、域名注册信息、通报处置记录、安全检查记录、攻防测评等数据。

此外，特别是需要加强对关键信息基础设施针对性的软件供应链管理、测评、备案和验证等，加速提升关键信息基础设施供应链的透明度，对供应商的供应链安全管理能力进行量化，达到成份级的精细化管控力度。通过结合威胁情报运营能力，监测供应链相关安全事件，使安全管理部门及时应对供应链安全事件预警、自查、定位、响应、处置、溯源能力。

二、强化攻击者视角的研判分析

随着数字化功能和传统能力相叠加，数字化转型重塑 IT 架构，大多数组织的网络资产数量和复杂性前所未有的增加，攻击面急剧扩大，网络攻击手法将更加层出不穷，安全挑战指数级增长。除漏洞攻击外，利用社会工程学、泄露的代码和敏感信息、盗用的凭证、影子资产、数字供应链等弱点，通过分子公司网络、供应链（或网络）、VPN、运维员工违规外联通道和第三方接入的系统作为突破口的攻击，令人防不胜防。

在监管部门的指导和要求下，很多单位看似购买了很多先进的武器，然而很多单位连知己都做不到，或者只是以防御者视角构建的安全防御体系，更多聚焦在已知 IT 资产的漏洞发现与修复上。这些传统的方法，往往过于碎片化、维护成本高，信息孤岛、缺乏上下文信息，造成效率低下，安全分析人员往往淹没在大量的告警、漏洞和事件中不知所措。这就要求以威胁主体进行攻击者分析的研判模式，从分析威胁主体的客观行动，到进一步分析威胁主体的主观意图，从而能够在海量的数据中发现真正攻击行为，主要包括如下分析能力。

1、基于攻击特征的同源分析

据大量分析经验可知，攻击者通常使用了大量代理 IP、网络出口 IP、秒拨技术、多地进行配合行动等，造成海量告警经常呈现出独立、碎片化、过程缺失的状态。因此需要根据不同的方法从攻击者视角将属于同一事件，但不同源 IP 的事件信息进行同源分析：

・静态特征同源

提取攻击者的静态特征痕迹，如 C2 域名、Mac 地址、邮箱、手机号、Cookie、恶意文件 MD5、后门地址、XSS 平台地址、DNS 地址等。

・行为模式同源

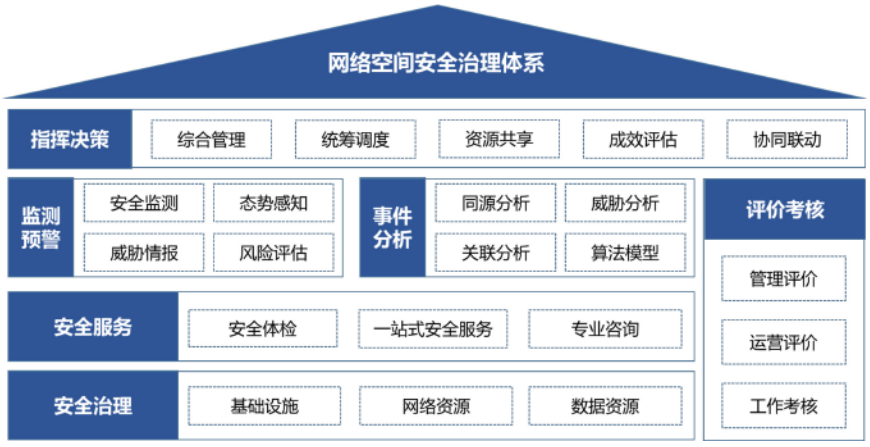
提炼攻击者的行为模式，将攻击者的行为转化为攻击者向量，当向量在一定时间窗口内存在行为模式相似性，则视为存在同源关系并进行进一步的研判识别。

2、攻击者属性分析

通过对于攻击者行为的属性识别，包括自动化扫描器识别、安全公司识别、白帽子识别、黑客（团伙）识别、扫描器识别等属性分析能力。

3、攻击者威胁评估分析

通过攻击者能力维度、攻击手法维



度、攻击危害维度等，最终得出事件得分情况，进而决定此事件是否应该作为系统推荐的重点研判事件。

因此，强化攻击者视角的研判分析，特别是针对暴露的资产（包括互联网、云、物联网、智慧城市等环境下的资产与风险），通过攻击者视角与情报来进行分析，能够更早启动研判的能力，通过消减传统研判模式的滞后性，在攻击链靠前的阶段研判并识别攻击事件和攻击者，通过早研判、早发现、早处置的能力，提升整体关键信息基础设施的安全水平。

三、构建数字化网络空间安全治理体系

随着数字化转型的加快，数据将成为人、物、服务的表现形式和连接方式，呈现海量、动态、多样的特点。通过数据技术，有效地打通社会间、区域间、部门间壁垒，实现网络安全治理流程的再造和联动治理。按照“谁主管谁负责、谁建设谁负责、谁运行谁负责、谁使用谁负责、管业务必须管安全”的原则，充分利用网络安全监管单位、各行业主管单位和安全企业的服务协同配合。通过科学合理的角色分工，充分发挥各相关单位的能力，形成网络安全的合力，提升整体网络安全管理水平。

安全治理，建立网络安全档案，按照统一标准对于数据资源、网络资源和基础设施进行全面数据采集和梳理，围绕安全数据全生命周期管理构建网络安全数据资产地图和数据分布地图。

监测预警，强化关键信息基础设施管理机制，制定关键信息基础设施安全防护技术标准和技术防护方案，通过安全监测预警、态势感知平台等基础平台，进一步提升威胁情报，获取和一体化监测预警管理能力。

事件分析，强化网络安全事件的分析能力，基于网络安全专家经验和建立数据分析模型，通过算法模型和人工相结合的方式，从更深层次、更广维度对网络安全情况进行综合研判。

评价考核，制定网络安全管理评价、安全工作运营考核和对应的奖惩机制，对网络安全事件进行问责处罚，并依据安全标准和方案实施整改。

安全服务，为网络安全运营者提供网络安全体检和一站式网络安全服务，发布网络安全服务评价，引导网络安全科技创新和提升安全产品服务水平。

指挥决策，对网络安全预警、响应、处置流程的全方位支撑，对各类资源的统筹调度、情报共享、协同联动，全面支撑在网络安全事件通报、预警、应急、信息发布、联动处置和综合管理。

因此，通过数据驱动的网络空间安全治理体系，要求在数字治理的框架下，不能仅靠单纯的数据或工具，同时需要统筹人员、流程、技术和服务在内的各项活动，将安全数据进行汇聚整合、挖掘利用和研判分析，形成安全协同指挥闭环，将数字化安全从社会层面实现政府、企业、个人的群体智慧，也是政府数字化、产业数字化和社会数字化的重要内容。

关基设施保护基础：关键业务分析识别

作者 | 张靖雯

《关键信息基础设施安全保护条例》是根据《中华人民共和国网络安全法》制定的条例，是面向公共信息和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域出台的专门保护制度，保障关键信息基础设施安全及维护网络安全。随之发布《信息安全技术 关键信息基础设施安全保护要求（GB/T 39204-2022）（以下简称《关基保护要求》）是关键信息基础设施安全保护标准体系的构建基础。

《关基保护要求》标准将关键信息基础设施安全保护活动分为分析识别、安全防护、检测评估、监测预警、主动防御和事件处置六个方面。其中“分析识别”是保证安全控制措施落地的基础工作。主要围绕关键信息基础设施承载的关键业务，开展业务依赖性识别、关键资产识别、风险识别等活动。

“分析识别”阶段面临的四个挑战

业务识别不清

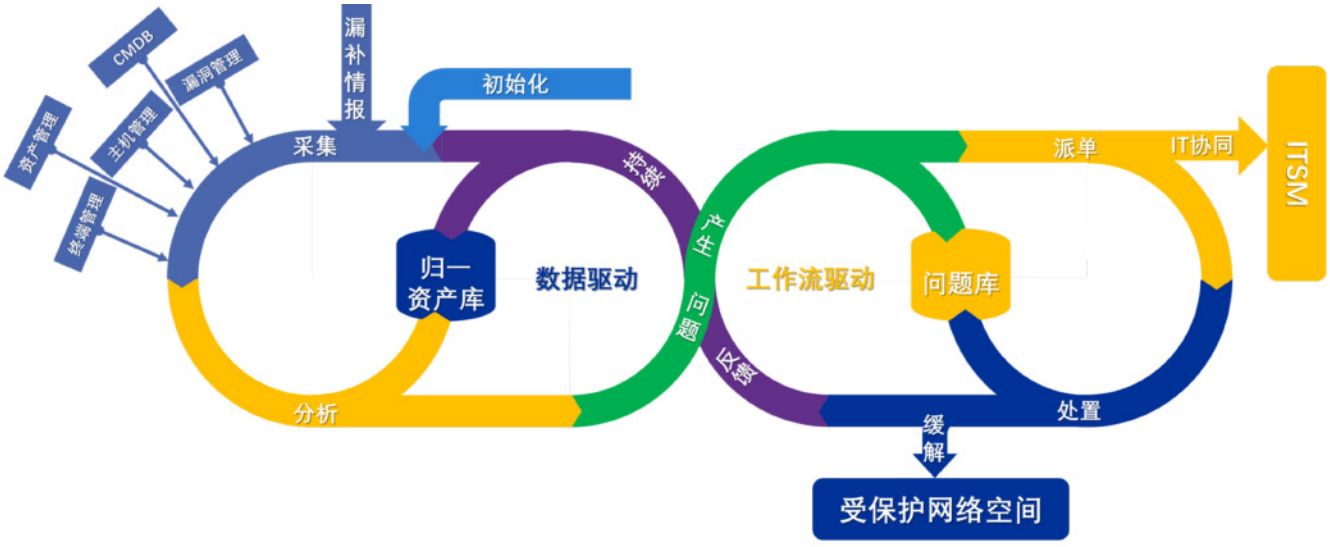
大部分组织的安全主管部门通过线下台账的方式管理关键业务信息，信息来源主要依赖于人工维护或分支机构上报等方式，数据质量无法保证，错报漏报时有发生。受限于人工维护的局限性，造成业务信息梳理的全面性、准确性和实效性方面存在诸多问题。

随着各类业务系统的建设，系统之间的集成关系错综复杂，而系统间的集成调用关系通常记录于技术部门的设计文档中，如果没有建立完善的系统集成备案机制，对于安全主管部门难以厘清与关键业务关联的外部业务，更无法分析关键业务对外部业务的依赖性和重要性。

资产识别不全

大部分组织通过资产探测系统和资产管理系统、或利用终端安全类产品、SoC、SIEM 系统的资产管理模块、CMDB 系统，采集和管理资产数据。资产探测类产品通过主动发包探测资产信息，数据准确性依赖于指纹能力，用于发现未被管理的资产，但易受到网络环境或安全策略限制导致探测失败，且无法采集组件等细粒度的资产元素。终端安全管理类产品通过代理客户端采集资产数据，依赖于产品的资产识别能力，

> “分析识别”是保证安全控制措施落地的基础工作。主要围绕关基设施承载的关键业务，开展业务依赖性识别、关键资产识别、风险识别等活动。



利用资产的本地权限，可以采集全面准确的资产信息，但无法发现未被管理的资产。SoC 和 SIEM 类产品通过从流量中解析资产信息，数据的全面性依赖于流量探针部署的覆盖程度，用于发现未被管理的资产，但流量加密或流量较少时，难以采集细粒度的资产元素。CMDB 系统的资产数据主要依赖于人工运营，存在资产物理属性缺失或管理属性久未维护等情况，使数据的准确性和实效性无法保证。

在当前网络环境复杂，云服务、虚拟化等资产类型众多的场景下，资产信息变化频繁，资产关系盘根错节，受限于单一技术手段的局限性，仍无法全面掌握资产信息。

风险识别不准

《关基保护要求》在分析识别方面明确要求应按照《GB/T 20984-2022 信息安全技术 信息安全风险评估方法》（以下简称“GB/T 20984 风险评估方法”）等风险评估标准，对关键业务链开展安全风险分析，识别关键业务链各环节的资产、威胁、脆弱性，确认已有的安全控制措施，分析主要安全风险点，确定风险处置优先级，形成安全风险报告。

采用 GB/T 20984 风险评估方法进行风险识别时，需要对资产、威胁和脆弱性进行赋值。资产赋值主要来源于业务识别和资产识别过程中的重要性评估结果。威胁赋值需要参考日常威胁监测和威胁运营工作结果。脆弱性赋值需要结合漏洞情报和资产的安全防护措施综合评估。

而大部分组织在风险识别过程中，由于资产、威胁和脆弱性数据分散在不同的系统中（如 CMDB、SoC 和 VM），系统之间没有打通，数据难以相互关联，需要人工进行风险评估计算，增加了风险识别过程中的人力投入，且评估结果准确性无法校验。

重大变更不知

随着资产承载业务的变化日新月异，使资产的系统配置、服务状态、责任归属等信息变化频繁，人工方式难以对资产变化及时更新。当发生安全事件时，经常出现无法定位目标资产、资产责任人信息失效等问题，拉长了安全事件从发现到响应的时间窗口，加大了安全事件造成的损失。

创新“数据 + 运行”双核驱动模式破解“分析识别”难题

为了落实《关基保护要求》，解决当前大部分组织面临的业务识别不清、资产识别不全、风险识别不准、重大变更不知等问题。需要建立以关键业务为核心的资产安全运营体系，将资产安全管理的“白账”和“探查账”进行汇聚并碰撞分析（“白账”是指在人工台账中维护的资产数据，“探查账”是指通过各种资产发现、漏洞扫描工具获取的资产信息）。通过对多源异构资产及其配置、漏洞、补丁等安全状况数据进行治理与碰撞分析，一方面可以发现“白账”中未登记的资产及登记错误的数据，另一方面驱动人工运营补全“探查账”中未核实的资产信息。

这种基于多源数据融合和碰撞分析的资产安全运营体系，将传统依赖人工的定期检查模式转变为数据驱动

运行的常态化运营模式。通过数据的周期性接入和更新，驱动运营人员对资产数据持续校准。结合漏洞情报，判定资产安全状况与脆弱性缓解优先级，建立组织的动态资产清单，实现关键业务资产安全闭环管理。

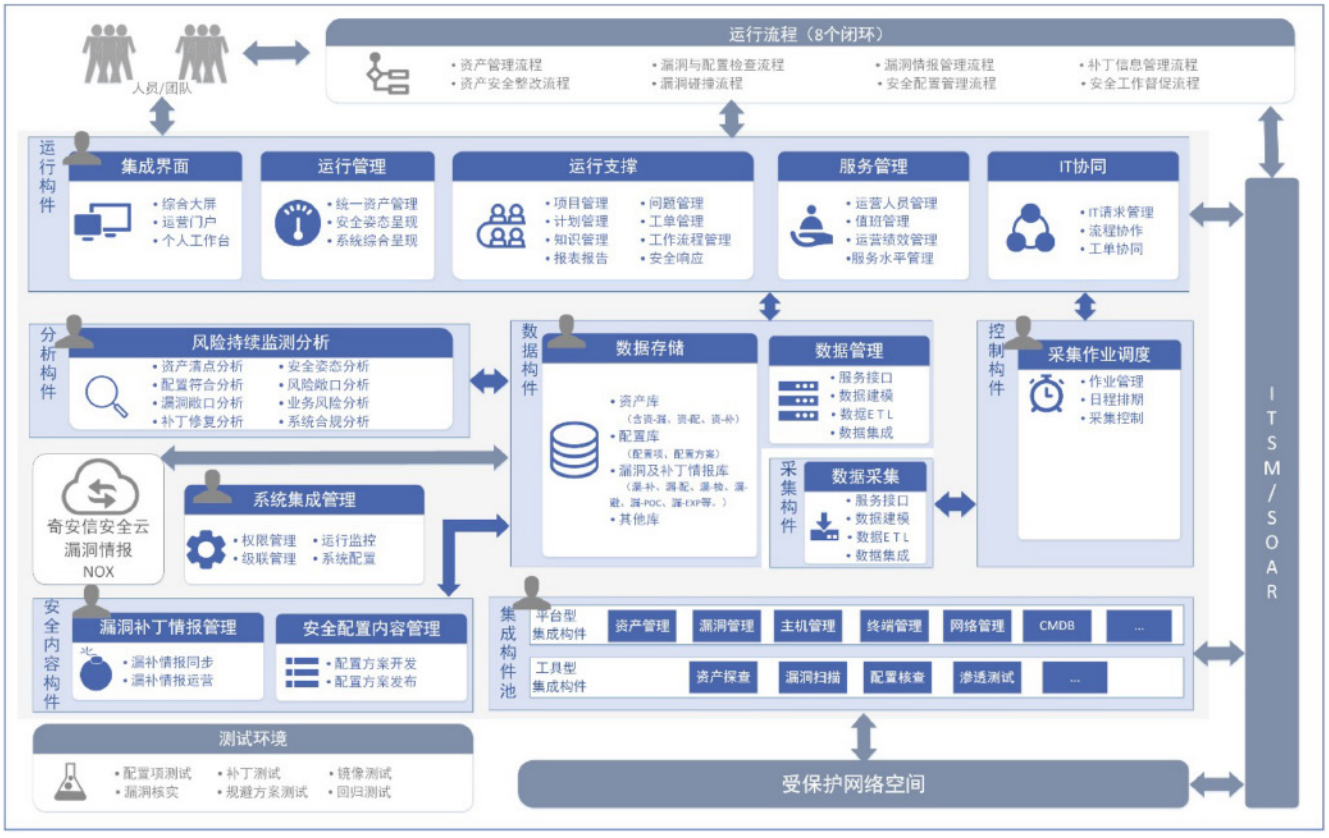
面向关键业务的资产安全运营平台建设思路

面向关键业务的资产安全运营平台（以下简称“平台”）将多源异构的资产数据进行融合，形成时空动态的资产画像信息。通过“数据 + 运行”双核驱动的常态化运营模式，盘清企业网络资产，明晰资产安全状态，持续收敛资产风险敞口。

平台是由若干个不同的构成系统（以下简称“构件”）有机整合起来的一个复杂系统。构成系统是指具有独立架构与功能，能够开展运行并完成独立应用目标的自主系统。这些构成系统组合起来的形成的新系统称为SoS（系统之系统，也称为“复杂系统”），具有涌现效应，能够产生原来各个独立的构成系统单独存在时所不具备的能力（即 1+1>2 的效应）。

如下图所示，平台架构包括 7 大构件（构成系统）。

集成构件池：主要是具备对受保护网络空间进行资配漏补管理的各类构成系统，这些构成系统既在网络资产攻击面管理系统之外，但也在系统安全体系之中，各自承担了本应有的应用场景，但从系统安全体系的视角出发，需要复用其安全功能或数据，因此需要被集成。在现实环境中，用户往往或多或少已经具备了一种或多



种此类构件，从系统工程的角度出发，应尽可能地复用这些能力，将其作为集成构件纳入到整体解决方案中。

安全内容构件：包括漏洞补丁情报管理和安全配置内容管理。漏洞补丁情报管理能够采集包括奇安信云端情报在内的多源漏洞及补丁情报信息，结合自身的安全内容运营和漏洞研究，采用漏洞补丁情报持续管理闭环流程，对内持续输出漏洞补丁情报，通过情报驱动系统安全运行。安全配置内容管理则通过安全配置内容管理流程，实现资产安全配置信息的开发与发布，驱动系统安全的运行。

采集构件：实现对多源异构的资配漏数据的采集与收集，包括对采 / 收集到的数据的语法校验、预处理、数据映射关系配置等。采集构件具有开放式架构设计，具备良好的可扩展性和适应性。

数据构件：实现全局资配漏补的数据集成、存储与管理。数据集成是指将分散的纳管构件的要素信息集成起来送入大数据管理层的过程。数据构件应采用大数据技术实现对系统安全所需的要素信息的统一集中管理，包括对采集构件送上来的数据按照预先构建的数据模型进行 ETL 处理，存储到内置的数据仓库中，继而应用分析构件中的各种分析算法对这些数据进行运算，发现系统安全问题，并将分析后的资配漏补数据和各类系统安全问题，通过对外封装的数据服务输出给运行构件。数据构件具有灵活的可定制性，包括数据可建模、ETL 可视化定义、数据服务可自定义等。数据构件具有良好的伸缩性，从单机部署到多机集群部署，以满足不同级别的客户的不同处理性能需求。

分析构件：在系统安全运行流程的驱动下，预置分析规则，通过数据分析引擎，实现资产信息分析、配置符合性分析、漏洞敞口分析、漏洞修复分析，并支持根据用户的运营需求，自定义扩展分析规则。

控制构件：包括系统安全策略管理、采集作业调度、编排响应与控制。安全策略是指系统安全运行所需的各种策略制定、发布与存储。采集作业调度聚焦于对采集构件的控制与调度，驱动采集构件按照预定的日程排期执行工作。编排响应与控制包括各类控制剧本、脚本和应用的管理与执行，实现自动化的资产安全事项响应与控制。编排响应与控制聚焦于对集成构件进行控制操作，包括下发策略，改变集成构件的工作姿态。此外，编排响应与控制也能作用于受保护网络空间的各类设施和 ITSM，以调整受保护网络空间的安全姿态。

运行构件：通过运行构件将各类运行人员和相关团队协同起来，与各类构件进行交互，最终实现资配漏补的运行闭环。运行构件包括运行管理、运行支撑、服务管理、IT 协同、集成界面等。运行管理实现面向用户的统一资产安全管理，包括资产画像、攻击面、配置、漏洞和补丁情况的管理，帮助用户获悉全网整体资产的安全姿态与合规性。运行支撑从项目视角出发，采用事项驱动工单的形式，实现体系化、常态化的系统安全运行。服务管理实现对运行人员、服务水平和绩效的管理与度量。IT 协同实现系统安全与用户侧 IT 大运维（ITSM）的双向协同，主要是数据与流程的协同。集成界面具备面向各级管理人员的综合展示大屏，以及面向各角色运行参与者的个人工作台。

整个平台还包括系统集成管理，实现各构件权限的集成，进行各种配置管理，对各构件及其分子系统进行运行监控，实现系统的级联。

结束语

构建体系化、常态化和实战化的企业级资产安全管理体系，融合主流资产管理系统、安全工具、安全设备、IT 基础设施、漏洞情报提供的资产、配置、漏洞、补丁、安全防护、应用发布、人员、组织和情报等类型数据，借助于平台提供的数据处理、数据分析和任务流转等能力，发现资产安全问题，触发安全运营流程，驱动运营人员对问题进行处置。形成“平台 + 运营 + 数据”三方协同的运行机制，将《关基保护要求》中分析识别相关的控制措施落地。

> “平台 + 运营 + 数据”
> 三方协同的运行机制，
> 将会确保《关基保护要求》中分析识别相关的
> 控制措施落地。

以关键业务为核心的风险管控必经之路

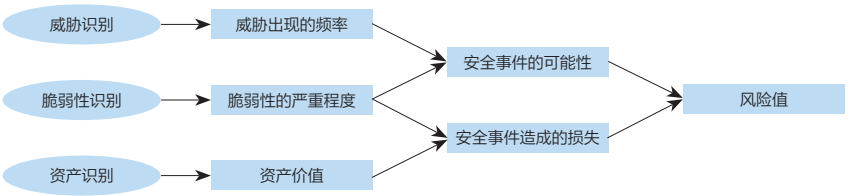
——关基设施安全风险评估

作者 | 施啸天

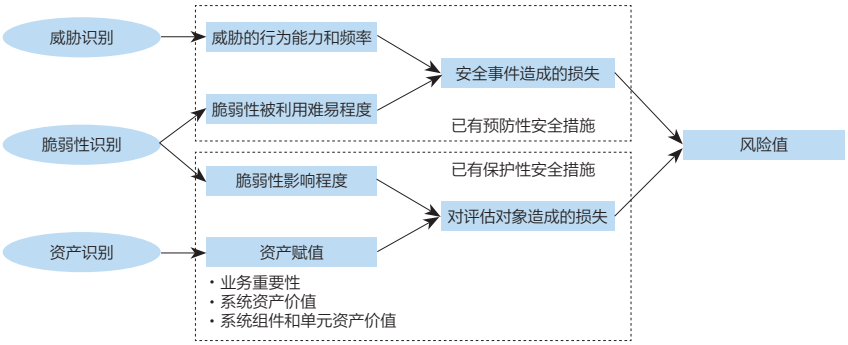
如果说互联网和信息化建设改变了我们的生活方式，那么关键信息基础设施就是在各个领域默默的支撑着我们的衣食住行和国家发展。随着《网络安全法》《关键信息基础设施安全保护条例》《关键信息基础设施安全保护要求》等法律法规和国家标准的发布实施，开展关键信息基础设施建设，推动安全保护工作落地更加意义重大，不断识别风险并降低风险成为新的网络安全任务目标，风险评估则是开展关键信息基础设施安全保护的基础，也是安全风险管理不可或缺的重要环节。

从国家标准和要求来看，关键信息基础设施安全保护的分析识别方面明确要求应按照《GB/T 20984-2022 信息安全技术 信息安全风险评估方法》（以下简称“GB/T 20984 风险评估方法”）等风险评估标准，对关键业务链开展安全风险分析，识别关键业务链各环节的资产、威胁、脆弱性。在检测评估方面要求运营者对关键信息基础设施安全性和可能存在的风险，每年至少进行一次检测评估。从信息化建设的意义来看，确保网络安全是为关键信息基础设施建设提供保障，关键信息基础设施的稳定运行最终是为了确保关键业务的顺利开展。所以关键信息基础设施的安全风险评估更应该注重风险发生对业务安全造成的影响。

GB/T 20984 标准在 2022 年发布了新的版本，并于 2022 年 11 月 1 日起正式实施，这也是 GB/T 20984 标准自 2007 年发布以来的第一次更新。主要优化了风险评估流程，细化了风险要素识别过程，并且改进了风



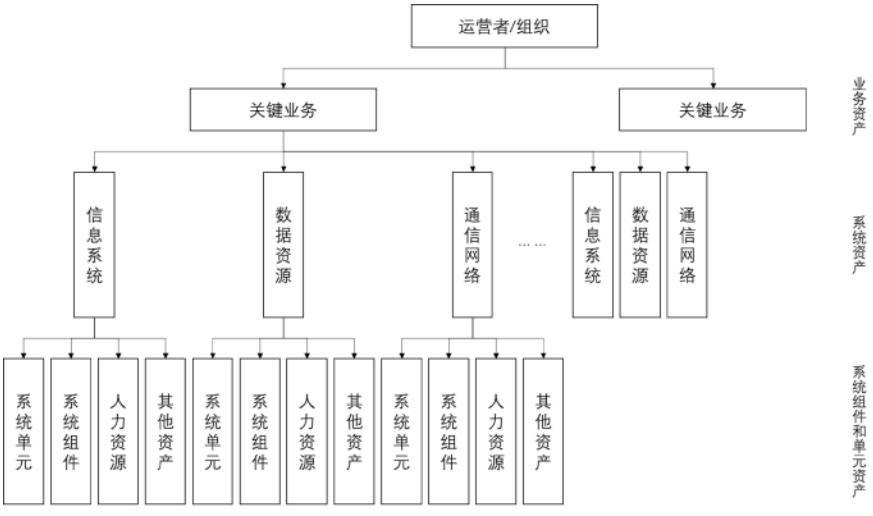
《GB/T 20984-2007 信息安全技术 信息安全风险评估规范》风险分析原理



《GBI 20984-2022 信息安全技术 信息安全风险评估方法》风险分析原理

险分析和计算原理。更新后的标准中对脆弱性的赋值分为被利用的难易程度和影响程度两个方面，这样一来解决了曾经对某个影响较大但几乎不会被利用的脆弱性赋值高低的矛盾问题。

关键信息基础设施风险评估在GB/T 20984标准的风险评估方法的基础上围绕保障关键业务的安全开展，对风险要素的识别和分析须包括资产、威胁、脆弱性、安全措施等，对风险计算和风险分析须考虑风险是否直接或间接对业务造成影响，不存在的业务场景或对业务不构成影响的风险不是评估的重点内容，同时风险分析的方向应该考虑风险发生后信息安全和网络安全问题是否影响信息化设施稳定运行，信息化问题是否影响对关键业务的支撑能力。如果不造成影响，那么就只是网络安全风险或信息化风险，而非业务安全风险。同理，如果某个网络安全风险或信息化风险直接或间接对业务安全造成影响，则应该将其上升为业务安全风险，进行重点分析和关注，在风险处置和整改工作中也应提高相应的优先级。



资产识别

关键信息基础设施的认定和边界确认过程需要识别关键业务信息、关键业务信息流，以及各关键业务信息流上资产分布情况。在开展关键信息基础设施的风险评估活动时，识别资产可按GB/T 20984标准的风险评估方法提供的方法论，识别为业务资产、系统资产、系统组件和单元资产，这种方法识别的资产范围也符合关键信息基础设施从业务到资产的识别和认定过程，可以协助运营者更好地厘清关键信息基础设施边界。此外，对资产的赋值可采取更加贴合业务的方法，将业务、系统、组件和单元等资产分别采取更为精准的评价标准进行赋值，而非“一刀切”的考虑所有资产的可用性、完整性和保密性，同时赋值分析时要考虑关键业务生存周期中各资产的价值变化情况。更加细分的资产赋值可以使风险分析和计算结果更为精准，也更加符合业务为重的风险评估目标。

威胁识别

威胁识别可根据外部环境威胁、内部意外故障和人为威胁等不同来源，划分自然环境、物理损害、信息损害、功能损害、网络攻击、供应链失效、误操作等多个类别。关键信息基础设施安全风险评估的威胁识别应结合日常监测预警工作开展，更加关注国内外及所在行业发生和面临的安全事件和发展趋势，尤其是将我国作为网络空间战略对手的敌对国家和黑客组织，而这些敌对势力的攻击目标正是国内各行业的重要业务部门及军工和科研单位。对此，识别到此类威胁应当重点关注，或提升其评价等级，分析此

类威胁发生频率时，不能只依靠历史数据和威胁监测数据，还应充分考虑风险评估时是否处在或即将进入网络安全重保等特殊时期，进而优化和调整威胁分析结果和评价等级。

脆弱性识别

脆弱性是资产自身存在的，如果没有被内外部威胁利用，或威胁不具备利用条件，脆弱性本身不会对资产造成影响，而威胁没有可利用的脆弱性，也不会构成安全风险。关键信息基础设施风险评估中脆弱性的识别，除了考虑技术和管理两个方面，还应考虑运行管理的合规要求，将不合规作为脆弱性的一种进行识别，尤其是保护工作部门或行业制定的合规要求，包括行业发布的关键信息基础设施保护标准、指南、规划等文件要求，以及行业数据安全保护、供应链保护、信创和国产化要求等。脆弱性赋值按照 GB/T 20984 标准的风险评估方法将脆弱性被利用的难易程度和影响程度分别赋值，并得出相应的评价等级用于风险计算和分析，但开展关键信息基础设施脆弱性管理时应对影响程度高的脆弱性保持同等的关注度，即便是该脆弱性处在难以被利用的评价等级。

已有安全措施识别

安全措施是关键信息基础设施运营者为开展安全保护已经采取的风险控制措施。根据安全措施的控制方式方法不同，作用于风险控制点也不相同，安全措施可以是降低风险发生可能性的预防性措施，此类措施通常根据存在的威胁情况进行设置，也可以是减轻风险发生对业务和资产造成影响后果的保护性措施，此类措施通常根据脆弱性的情况进行设置，或采取转移、替代等策略降低资产本身的价值。在风险评估中，不需要单独对已有安全措施进行赋值，而是与威胁识别和脆弱性识别同步开展识别工作，并且验证已有安全措施的有效性，根据有效的安全措施属性对应降低或调整已识别的威胁或脆弱性赋值。安全措施对威胁或脆弱性赋值的影响应在合理范围，必要时可以采取专家打分的方式进行评审。同时，在识别和分析安全措施的时候也需要考虑其是否引入了新的脆弱性。

风险分析和评价

关键信息基础设施风险分析主要是对风险要素进行模型计算，得出风险值和风险等级，并将风险归纳整理的过程。风险值和风险等级通常采取矩阵法计算得出，包括两个风险指标：一是风险事件发生的可能性，由脆弱性被利用的可能性和威胁对应的赋值进行计算得出。二是风险事件发生后对资产或关键业务造成的损失，由脆

信息系统风险评估风险矩阵

风险值=R[事件可能性,事件损失]		低风险（风险值1-4）	一般风险（风险值5-9）	较大风险（风险值10-15）	重大风险（风险值16-25）
可能性 \ 损失	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

关键信息基础设施风险评估风险矩阵

风险值=R[事件可能性,事件损失]		低风险（风险值1-3）	一般风险（风险值4-8）	较大风险（风险值9-15）	重大风险（风险值16-25）
可能性 \ 损失	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8 *	10
3	3	6	9	12	15 *
4	4	8	12	16	20
5	5	10	15	20	25

”*“ 标记的风险处于相对高损失低可能性区间，采取升级措施加强风险事件关注度

弱性影响程度和资产自身价值对应的赋值进行计算得出。对风险的评价需要与关键信息基础设施的单元资产、系统资产及业务资产相对应，而且应当注意的是，在风险矩阵中存在两种风险值一致但是两个风险指标相反的风险，这种情况由于关键信息基础设施和关键业务无法承受任何一次严重打击的特殊性，即便是风险值相同但更应该关注高损失低可能性的风险事件，在风险等级评价方面也应高于低损失高可能性的风险事件。

关键信息基础设施风险评估实践

对关键信息基础设施面临安全风险的改进和风险处置措施制定，以及安全建设方案、实施计划的编制过程，不仅要结合风险等级、风险类别的分析情况，还须要围绕关键信息基础设施运营者整体信息化建设规划和安全建设规划进行统筹考虑，解决高等级高优先级的安全风险时应一并解决同类型的低等级安全风险。在关键工程和关键项目落地过程中，还应全面推进以实现“三化六防”为目标的技术、管理、运行体系建设，相关平台和工具的建设，并且按照国家和行业要求同步开展信创建设等。

> 关键信息基础设施风险评估并非是一项“机械性”或“应试”工作，而应该做的有价值，在必要时不限于每年一次的风险评估频率，应当将风险评估和风险管控工作“常态化”。

风险评估的方法并非一成不变，很多运营者在对关键信息基础设施开展安全建设和运行维护过程积累了大量的风险处置经验，对关键信息基础设施在不同的生命周期面临的安全风险具有相对明确的认知，这种情况下，为了更加高效地开展风险评估，也可以采取故障树分析等方法直接定位到风险事件，对风险事件采取鱼骨分析等方法进行风险因子和要素的识别，在对各风险因子和要素进行计算得出风险值和风险等级评价。在关键信息基础设施安全风险评估实践中也多次得到验证，贴合实际业务场景和安全建设需求的方法才是好的评估方法也是更为合适的方法。同理，大而全的安全风险评估也并不是都能起到良好的风险管控成效，在相对专业的领域内开展如数据安全、供应链安全、云计算环境安全、工业控制安全等专项安全风险评估往往会得到更好的效果，更有助于对关键信息基础设施安全风险的精细化管理。

结束语

在关键信息基础设施安全保护的工作中，风险评估的方法论有据可依，风险识别和分析的过程相对灵活，具备较强的目标导向能力。关键信息基础设施风险评估并非是一项“机械性”或“应试”工作，而应该做的有价值，为运营者开展风险管控提供充分依据，在必要时不限于每年一次的风险评估频率，应当将风险评估和风险管控工作“常态化”，同时通过持续的风险管控策略逐步优化风险评估过程，避免重复开展烦琐的评估内容，追求更高的投入产出比，用最快的响应速度来应对日益多变的信息化和网络安全挑战，以强力支撑和更加安全的保障关键业务稳定运行。

关基设施安全治理下的 APT 攻击检测防御

作者 | 孙伟

一场 “精细策划”的持续隐蔽入侵渗透行动

2022 年 6 月 22 日，西北工业大学发布《公开声明》称，该校遭受境外网络攻击。陕西省西安市公安局碑林分局随即发布《警情通报》，证实在西北工业大学的信息网络中发现了多款源于境外的木马和恶意程序样本。美国国家安全局（NSA）在中国的网络安全渗透一时间成为热搜新闻头条。据相关事件调查报告称，此次攻击方是由美国 NSA 特定入侵行动办公室（TAO）策划实施。TAO 在入侵时，先后使用 41 种网络武器对西北工业大学发起攻击，其中一款名为“饮茶”的嗅探窃密类网络武器，是导致大量敏感数据遭窃的最直接“罪魁祸首”之一，引起了公众的高度关注。TAO 此次发起的网络攻击技战术针对性强，采取半自动化攻击流程，单点突破，逐步渗透，长期地潜伏窃密。TAO 在此次入侵中目标之明确、步骤之缜密、手段之丰富让人吃惊！

该事件入侵过程简述如下：

1. 单点突破、级联渗透，控制西

北工业大学网络

经过长期的精心准备，TAO 使用“酸狐狸”平台对西北工业大学内部主机和服务器实施中间人劫持攻击，部署“怒火喷射”远程控制武器，控制多台关键服务器。利用木马级联控制渗透的方式，向西北工业大学内部网络深度渗透，先后控制运维网、办公网的核心网络设备、服务器及终端，并获取了部分西北工业大学内部路由器、交换机等重要网络节点设备的控制权，窃取身份验证数据，并进一步实施渗透拓展，最终达成了对西北工业大学内部网络的隐蔽控制。

2. 隐蔽驻留、“合法”监控，窃取核心运维数据

TAO 将作战行动掩护武器“精准外科医生”与远程控制木马 NOPEN 配合使用，实现进程、文件和操作行为的全面“隐身”，长期隐蔽控制西北工业大学的运维管理服务器，同时采取替换 3 个原系统文件和 3 类系统日志的方式，消痕隐身，规避溯源。TAO 先后从该服务器中窃取了多份网络设备配置文件。利用窃取到的配置文件，TAO 远程“合法”监控了一批网络设备和互联网用户，为后续对这些目标实施拓展渗透提供数据支持。

3. 搜集身份验证数据、构建通道，渗透基础设施

TAO 通过窃取西北工业大学运维和技术人员远程业务管理的账号口令、操作记录以及系统日志等关键敏感数据，掌握了一批网络边界设备账号口令、业务设备访问权限、路由器等设备配置信息、FTP 服务器文档资料信息。根据 TAO 的攻击链路、渗透方式、木马样本等特征，关联发现 TAO 同时还非法攻击渗透中国境内的基础设施运营商，构建了对基础设施运营商核心数据网络远程访问的“合法”通道，实现了对中国基础设施的渗透控制。

这一系列令人“眼花缭乱”的入侵操作背后，突显出关键基础设施单位面对的网络攻击已不再是经济利益驱使的黑客个人的“炫技”行为，而是具有强大经济支援、成规模体系化、具备高超技术手段的国家级入侵组织团伙。此案件中的西北工业大学以航空、航天和航海研究而闻名，承担了我国大量的国防和科学研究，是典型的关键信息基础设施单位，而这类目标，正是 TAO 的核心攻击对象。不难想象，关键基础信息设施所掌握的数据价值对于国家安全的重要性有多高，境外政府不惜以网络犯罪为手段，对我国国家安全利益造成极为严重的影响。

关基单位面对 APT 入侵防御亟需解决的四类难题

纵观近些年国内曝光的多起 APT 入侵事件，可以看到，APT 攻击发起者具有很强的专业性，使用的攻击技术手法成熟、攻击策略较为先进。相对而言，目前对抗 APT 攻击的防御方案存在多方面的薄弱点，并缺乏完整的技术应对能力。我们认为，当前关基单位遇到的 APT 防御难题主要涉及四类，包括新型入侵渗透发现难；检测精度低；攻击溯源取证制困难；对新型攻击响应慢。

新型入侵渗透发现难，需要站在攻防两端对抗形势来看。攻击者始终处于“暗”处，新型入侵途径、新漏洞或新攻击技术的挖掘开发始终处于先机，造成防御方先天处于攻防两端弱势一方。相较于攻击者行动上的灵活多变，防御方始终处于明确标靶位置，存在检测技术滞后，应对策略僵化，威胁感知能力不全面等问题，难以达到攻防两端的平衡对抗。面对潜伏的攻击者，一个 0day 漏洞就可以在层层防御的安全纵深防御体系上轻松撕开一个“口子”，进而全面打开进入内部的通道。应对此难题，目前主要可以依赖的技术包括异常行为场景检测技术、主动攻击诱捕牵引技术、基于机器学习的钓鱼邮件检测技术等。

检测精度低，这里主要强调针对恶意变种样本的检测对抗。恶意代码对抗性是指恶意代码具有的可以遏制逆向分析，以及绕过杀软、穿透代理、防火墙及对抗 IDS 等防护手段。根据对抗类别的不同，恶意代码的对抗分为基于静态分析与检测的对抗、基于动态分析与检测的对抗及基于机器学习分析与检测的对抗等。恶意软件的对抗性使得恶意代码在系统设备中长期潜伏成为可能，这对系统资源和用户数据造成了严重的潜在威胁。

攻击溯源取证困难，这一问题直接造成对攻击事件中攻击目的、攻击途径、攻击手段等重要信息的缺失，导致无法看清攻击事件发生过程，难以精准查漏补缺，并在未来对安全防御无法做出合理反应。攻击溯源取证技术通过综合利用各种工具技术，如威胁狩猎技术、全流量原始数据关联分析技术等，主动明确网络攻击发起者、定位攻击源，还原完整入侵事件，结合网络取证和威胁情报，有针对性地减缓网络攻击，争取在造成破坏之前消除隐患。

对新型攻击响应慢，主要体现在日常应变 APT 事件反应上的不足。这样的反应既体现在人的意识逐渐淡化层面，也体现在安全防御力的实际效果减弱层面。由于 APT 事件的高隐蔽

特性，可能长期无任何威胁动作可被感知到。攻击者往往更有耐心等待下去，等待被攻击目标放松警惕，等待防御力的停滞，进而逐步展开深入行动。用户网络安全体系长期以“松弛”状态防御抵抗，难免出现失效、失职。应对此难题，目前可以依赖常态化的对抗防御效果评估手段，如入侵与攻击模拟 (BAS) 技术等，建立日常的关基单位防御体系抗攻击效果评估策略。

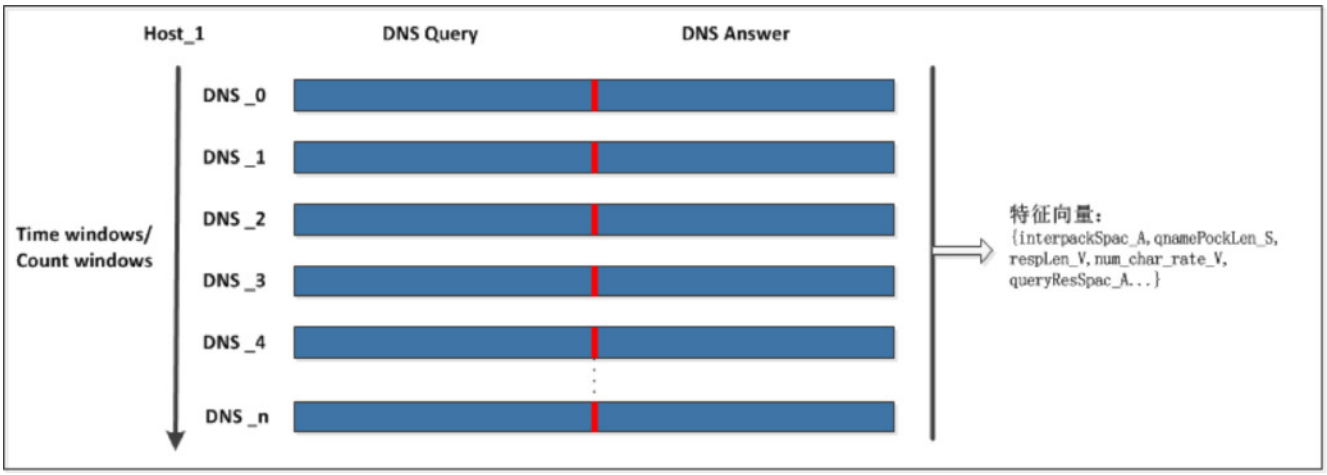
有效应对 APT 入侵攻击是一个较为复杂的难题。在攻防对抗的持续动态过程中，更重要的是的“技术策略”，而不仅是“技术方案”。解决上述四类难题，只有灵活、适当的应用“策略”，才能在高水平攻防对抗的态势下，依托多维度技术手段，有条不紊地开展 APT 安全防御工作。

安全攻防 BG 对抗 APT 入侵攻击防御关键技术盘点

从具体的技术层面来说，为了应对 APT 攻击，新的技术也是层出不穷。随着对 APT 攻击的研究不断深入，已经出现一些有效的防御技术来对抗 APT 攻击，其核心思想大多是针对APT“攻击链”的某一步骤展开防御。即从监测和检测的角度，针对 APT 攻击的各个环节 (侦查跟踪 – 武器构建 – 载荷投递 – 漏洞利用 – 安装植入 – 命令与控制 – 目标达成) 进行突破，任何一个环节能够识别，即可断开整个链条。本文限于篇幅有限，主要针对上述四类难题中提到过的技术点，重点选取介绍 5 项关键技术。

1. 异常行为场景检测技术

异常行为场景主要指网络中由攻击产生的异常数据流，这些行为特征有别于正常访问场景，并可经过异常行为模型匹配发现。在长期面对攻防特定场景的安全威胁分析背景下，经提炼出特定行为分析场景模型，可以达到对多种威胁类型的异常行为检测效果。比如 , 针对 0day 漏洞攻击这种无法直接检测的“核武”般攻击手段，基于 0day 漏洞攻击过程中附带产生的异常行为痕迹，可间接辅助对 APT 攻击的检测发现。此类异常行为检测模型包括 DNS 服务分析、非常规服务分析、Web 服务器行为分析、登录行为分析、数据库行为分析及访问行为分析等。选取三个特定异常行为场景为例：



・DNS 服务分析

DNS 服务分析包括可疑 DNS 分析（DGA 域名检测和 DNS Tunnel 隧道）、DNS 服务器发现、链路劫持等场景。DGA（域名生成算法）是一种利用随机字符来生成 C&C 域名，从而逃避域名黑名单检测的技术手段。DNS Tunnel 则是黑客利用 DNS 信道来传输数据的可疑隧道。链路层劫持是指第三方（可能是运营商、黑客）通过在用户至服务器之间，植入恶意设备或者控制网络设备的手段，侦听或篡改用户和服务器之间的数据，达到窃取用户重要数据（包括用户密码、用户身份数据等）的目的。如 DNS Tunnel 隧道，主要利用收集到的大量黑数据和白数据，生成用于分类 DNS 隧道和正常 DNS 数据的样本集合，利用基于窗口的 DNS 隐蔽隧道特征向量（DNS 隧道空间、回应包的长度、qname 中数字字符占比等），从而构建 DNS 隐蔽隧道检测模型。

・非常规服务访问分析

非常规服务访问分析主要完成常规行为分析之外的重要分析任务，包括可疑代理、远程工具和反弹 shell 等行为检测，让用户了解内部资产受到哪些代理工具、远程服务和反弹 shell 的威胁。可疑代理是指利用代理系统，中转客户系统的网络访问请求，并且可以过滤掉用户的指令，从而达到控制用户的目的。远程工具，主要用于主机远程控制，一般分为客户端程序 (Client) 和服务器端程序 (Server) 两部分，控制端上的 Client 与被控端的 Server 建立连接，完成各种操作。反弹 shell，表现为控制端监听被控端的 TCP/UDP 端口，被控端发起请求到该端口，并将其命令行的输入、输出转到控制端，实现客户端与服务端的角色翻转。这些非常规服务存在较大潜在威胁。

・异常 Web 访问行为分析

异常 Web 访问行为分析包含非常用请求方法、可疑爬虫和扫描和后门上传利用。非常用请求方法是指攻击者经常使用一些不常用的方法来获取服务器的敏感数据为后续的非法活动做准备，检测非常用请求可以用来来判断是否存在信息泄露事件。可疑爬虫和扫描主要指攻击者通过网络非法扫描、爬虫等多种攻击来扫描随机生成的 url 和随机方法来获取服务器数据。后门上传利用是指攻击者通过现有漏洞向服务器上传非法文件，以获取信息的行为。

2. 主动攻击诱捕牵引技术

主动攻击诱捕可以在攻防不对等的背景下发挥较大作用。主动攻击诱捕牵引技术指依托威胁检测设备检测

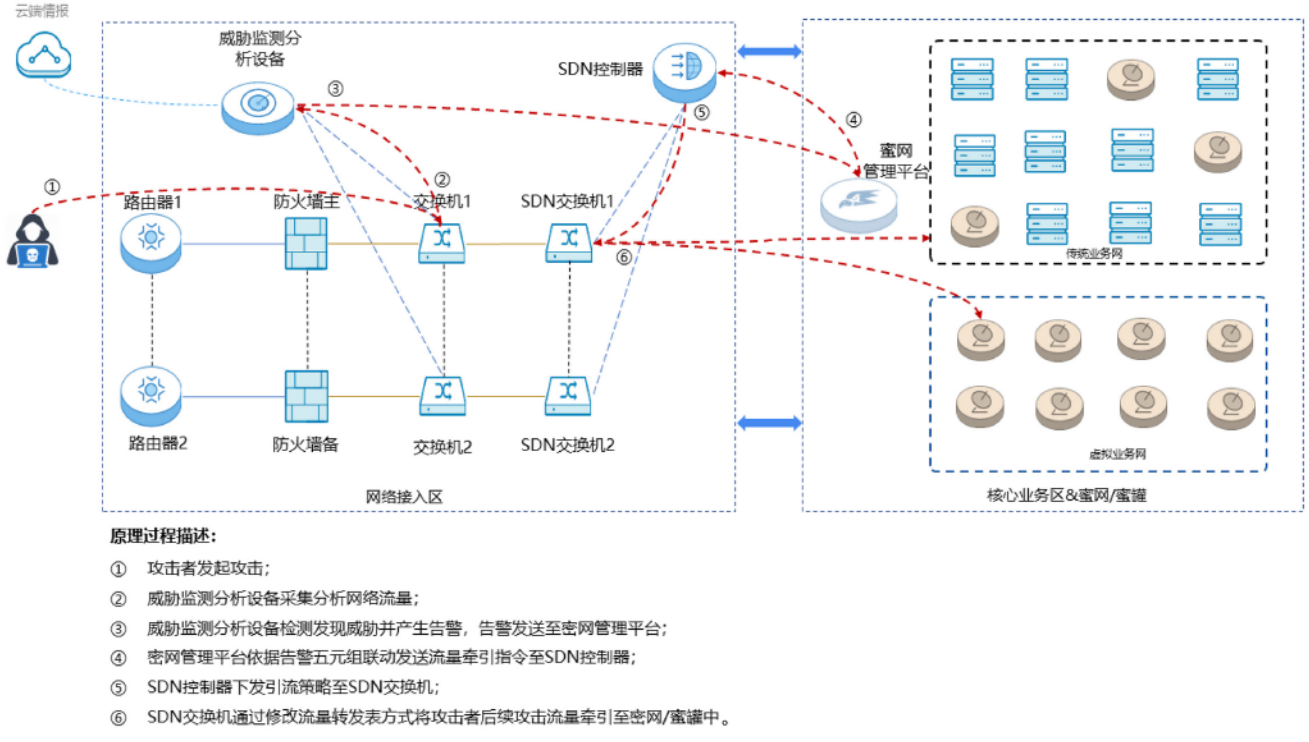


图 主动攻击诱捕牵引技术原理

规则对某些特定的流量进行检测，联动网络转发设备主动、智能化牵引攻击流量至蜜网系统中，达到欺骗捕获攻击者的效果。此技术实现，主要基于 SDN 技术的网络编排和网络威胁检测设备的联动技术能力，首先由网络威胁检测设备检测发现异常攻击，进而触发联动 SDN 设备对链路中指定威胁流量牵引至目标蜜网。由于流量牵引工作在网络层，可以达到不破坏攻击 IP 与受害 IP 间的联网结构，网络牵引过程对于攻击者无感。

3. 基于机器学习的钓鱼邮件检测技术

钓鱼邮件是目前 APT 攻击经常使用的手段之一，因其低成本、高成功率的攻击效果特点，被攻击者广泛使用。钓鱼邮件是指攻击者伪装成同事、合作伙伴、朋友、家人等用户信任的人，通过发送电子邮件的方式，诱使用户回复邮件，点击嵌入邮件正文的恶意链接或者打开邮件附件，以植入木马或间谍程序，进而窃取用户敏感数据、个人银行账户、邮箱账户和密码等信息，或者在设备上执行恶意代码实施进一步的网络攻击活动。当前针对钓鱼邮件检测，除钓鱼邮件域名、IP、url 等情报特征规则外，利用机器学习技术，在大量钓鱼邮件数据训练的基础上，形成钓鱼邮件检测模型可以一定程度上达到对鱼叉式钓鱼邮件的检测发现作用。钓鱼邮件机器学习检测模型主要针对链接式和仿冒式钓鱼邮件进行检测。模型借助还原出的邮件原文进行分析，提炼出基于邮件头部信息、主题、正文、链接、脚本等的多维度特征，然后输入到两阶段的机器学习检测模块“异常邮件检测模块”和“钓鱼邮件检测模块”中进行训练。机器学习检测模块利用随机森林、GBDT 等机器学习集成算法生成检测模型，基于生成的检测模型针对钓鱼邮件进行检测，根据实验结果统计，整体误报率可以有效控制到 1% 左右。

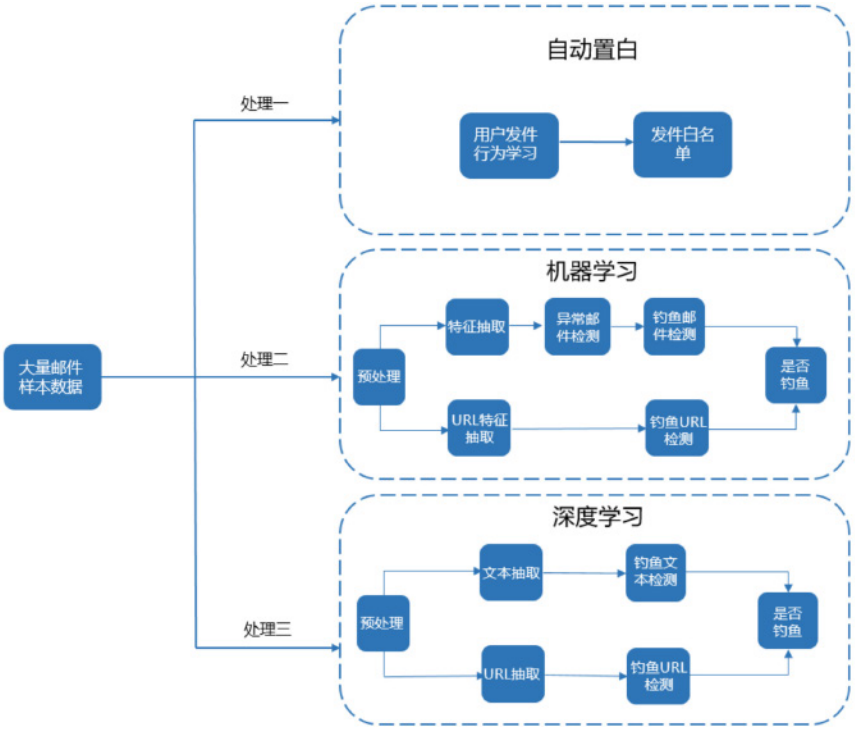


图 基于机器学习的钓鱼邮件检测模型

4. 恶意代码对抗检测技术

当今恶意代码病毒木马变种层出不穷，攻击者通过改变病毒木马的某一部分特征，实现对传统杀毒软件检测的绕过。在与恶意样本的对抗过程中，恶意代码对抗检测技术也在不断发展。基于静态分析的检测、基于动态分析的检测，以及基于机器学习的检测等技术不断涌现。基于静态分析的检测对非混淆样本更为准确；而基于动态分析的检测在检测混淆恶意软件方面表现更为出色；基于机器学习的检测则是通过对大规模恶意样本进行特征提取（如 API(application programming

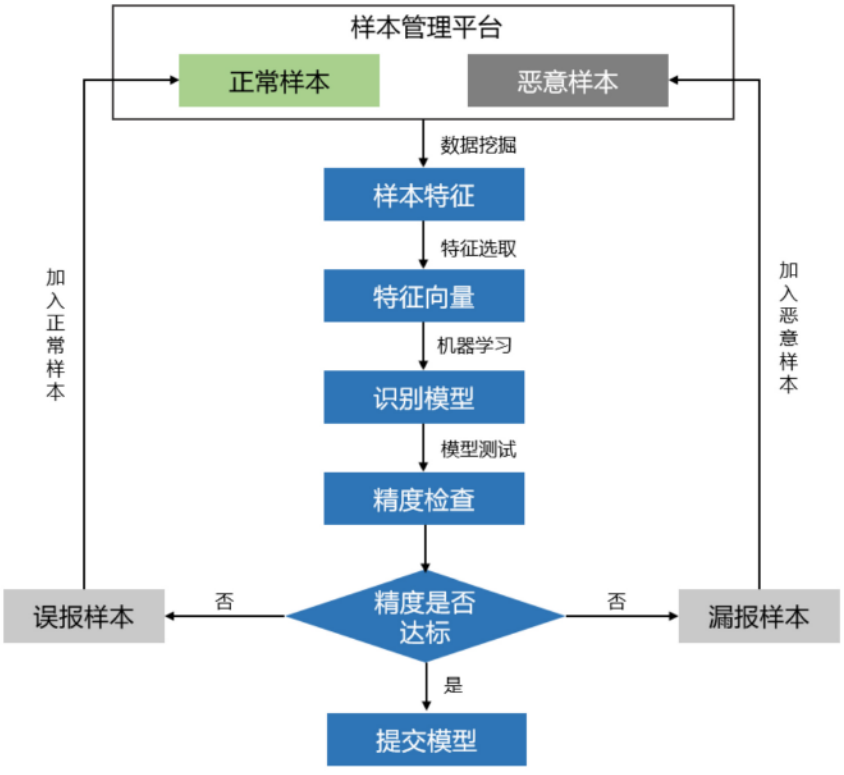


图 基于机器学习的恶意代码检测模型训练流程

interface)、CFG(control flow graph)、关键字符串值等），然后采用机器学习算法（例如分类或聚类）训练样本，以构建模型判断软件的恶意特性，有效地提高了大规模恶意软件的检测效率。

基于机器学习的恶意代码对抗检测技术主要根据已知的正常软件和恶意软件的大量样本，通过数据挖掘找出两类软件最具有区分度的特征，建立机器学习模型，使用机器学习算法，得到恶意软件的识别模型。通过获得的模型对未知程序进行分析判断，即可获得软件的恶意概率，从而在可控的误报率之下尽可能多的发现恶意程序。

5. 入侵与攻击模拟（BAS）技术

根据 Gartner 的调查，97%的入侵行为发生在已经部署适当网络安全防护系统的企业，99% 的攻击行为是使用已知并存在多年的攻击方式或者漏洞，95% 的绕过安全防护设备的入侵攻击行为是因为错误的配置造成的。

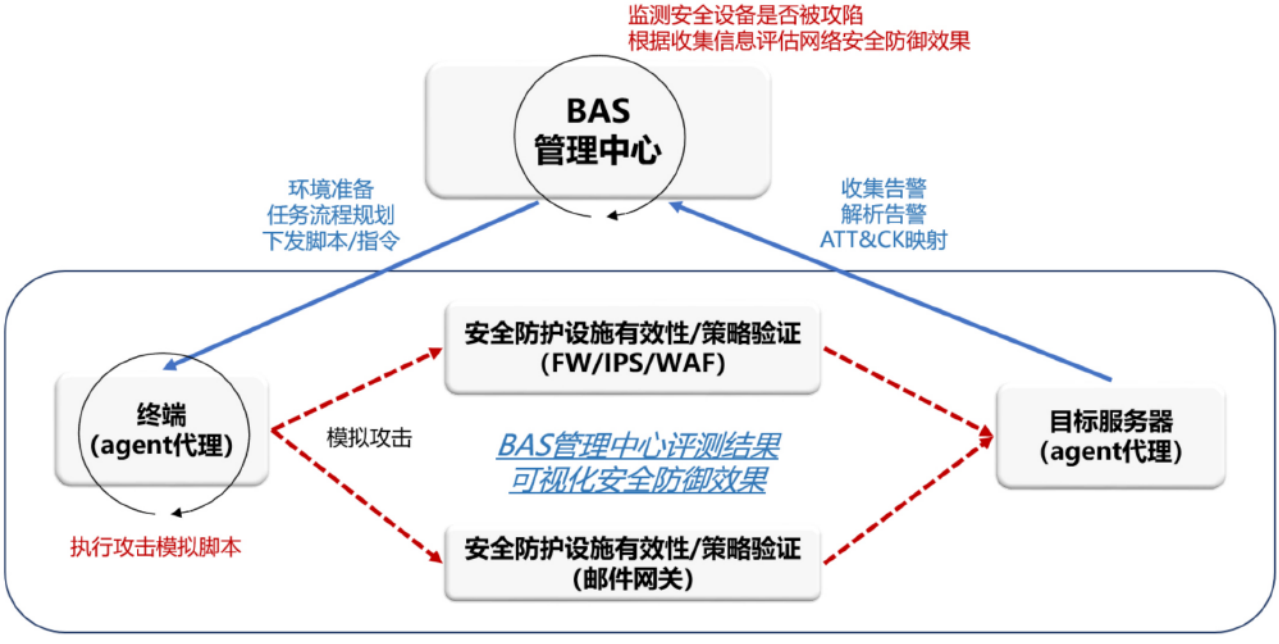


图 入侵和攻击模拟 BAS– 网络抗攻击效果评测原理

图 入侵和攻击模拟 BAS– 网络抗攻击效果评测结果

随着自动攻击数量的增长和严重程度的不断升级，攻击者在试图突破目标时，会尝试大量的漏洞并测试不同类型的弱点。攻击者会根据组织的安全防御状况调整攻击策略，以映射到这些系统的盲点和弱点。入侵和攻击模拟 Breach and Attack Simulation (BAS) 是一项新兴技术，主要目的是为企业和机构提供持续的安全防御体系评估能力，帮助用户建立常态化企业网络安全防御体系的测试评估及加固建议。它可以按需自动模拟企业的复杂网络来进行攻击，帮助测试企业系统的安全。BAS 和普通的自动化渗透测试工具不同，它可以自动模拟如 C2 攻击、对组织电子邮件系统的网络钓鱼攻击、对端点的恶意软件攻击，甚至是网络内的横向移动等攻击场景，可以执行各种破坏和攻击模拟。

结束语

APT 高级持续性威胁作为关键基础设施网络安全防御建设最为关心的焦点，对于我国目前新型攻击发现弱、检测精度低、溯源取证困难和对新型攻击响应慢等难题，需要形成针对性防御策略与防御体系。奇安信安全攻防 BG 始终将视角聚焦在攻防对抗领域，不断完善优化产品技术能力，以期保持对抗APT攻击的先进防御优势。安全攻防 BG 全系产品系统，借助对 0day 漏洞攻击技术的辅助检测与自学习进化等技术，持续升级攻防过程中检测防御能力，发现对抗各类 APT 威胁并降低误报、误杀等事件，力求帮助用户建设一套实战有效、具有高扩展性、且能够投入真实使用中的 APT 检测与防御策略及方案。安

重保能力常态化
——关键信息基础设施守护之道

作者 | 王千寻

自 2016 年公安部组织首次国家级实战攻防演练（简称“演练”）以来，网络安全重保（简称“重保”）成了安全行业的热词。重保的表面意义是保障关键时段关基业务的网络安全。其本质则是保障关键信息基础设施（简称“关基”）的网络安全。

如右图所示，重保常态化是指在纷繁复杂的实战化场景中持续保障关基可用性、时刻响应内外部攻击事件的综合实战能力。

1.1. 需求源于实战

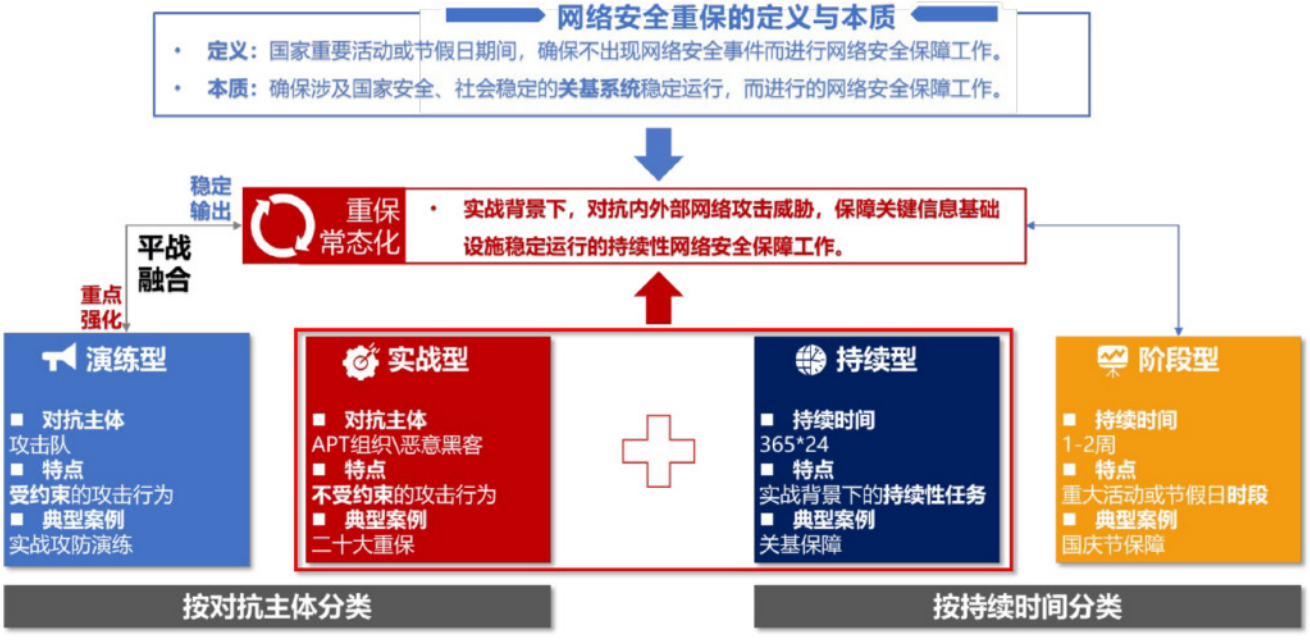
2022 是不平凡的一年，各种网络安全大事件向我们揭露了残酷的现实，网络空间的“虚假和平”被彻底撕破。

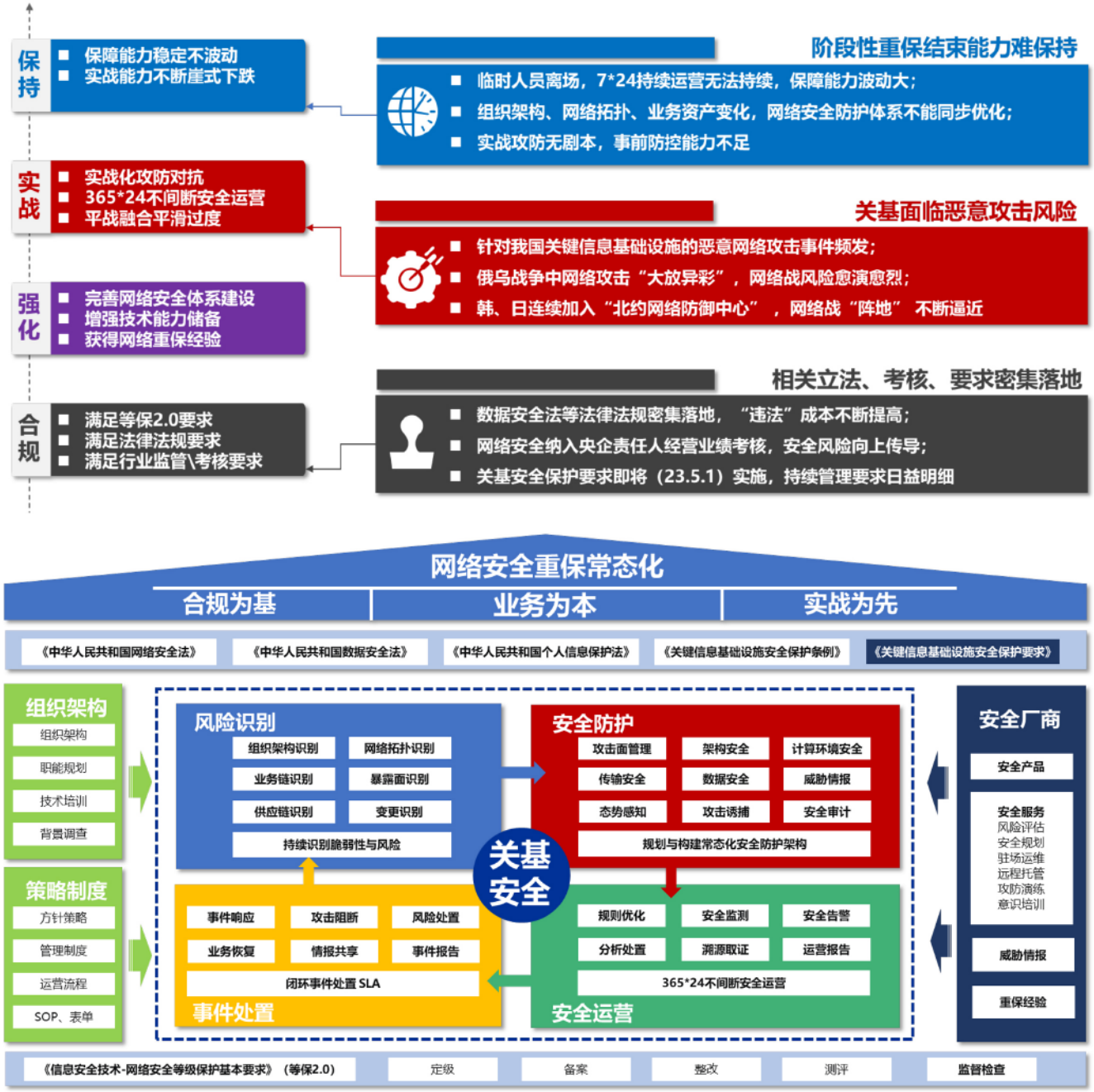
- 年初，北京 2022 冬奥、冬残奥会期间，冬奥资产受到全球网络攻击约 3.8 亿次。奥运会作为和平的象征，讽刺的成为攻击者的重点攻击目标；
- 4 月，北京市健康宝遭境外团伙 DDoS 攻击。这种对关键业务链（北京市正常运转）的关键节点（健康码）进行的突袭、点穴式攻击，令人浮想联翩；
- 10 月，伊朗的国家广播公司在直播中被黑客攻击，攻击者劫持信号播放了政治抗议内容；
- 11 月，乌克兰网军盗取俄罗斯央行 2.6G 共 27000 个文件并进行公开。目的是影响用户对俄罗斯银行系统的信任，破坏卢布的币值稳定。

事实证明，关基长期面临实战安全风险。恶意攻击者不会约束攻击时间和目标，也不会约束对业务的破坏性操作。因此，网络安全重保的本质应是实战背景下对关基业务持续性的安全保障能力。

1.2. 能力建设思路

常态化重保作为一种体系化能力，其建设过程切忌无脑投入、一拥而上。业务的经济价值、政治价值和社会价值都是衡量安全投入的核心因素。





图：重保常态化能力模型

安全风险是业务的天然伴生品，业务价值决定风险量级，对风险的有效识别是重保常态化能力建设的基础。通过业务及风险识别，我们将构建组织的重保常态化能力模型。从业务保障（可用性、业务数据安全等）视角出发，完成从风险识别到持续运营能力建设的闭环过程。

1.2.1. 重保常态化能力模型

奇安信重保常态化模型通过平台、流程和服务进行 365*24 不间断的闭环安全运营，可落地、可操作性是它的基本原则。

如上图所示，其要点如下：

1. 业务为本：业务价值是安全能力建设的前提，一切安全能力建设，都应该以保障业务安全为基本原则。

2. 实战为先：先救命，再治病。

以风险为导向量体裁衣，将资源优先投入最严重的问题，随时随地应对内外部安全威胁。

3. 合规为基：等保等合规要求，都是对共性风险、共性经验的总结。在我国，完成等保合规是基本要求。

无论现有安全能力处于何等水平，都可以对标安全、平稳、零事故的常态化安全保障目标进行评估与优化。对于任何类型的机构而言，要做好常态化重保都必须做到 3 个到位。

1. 防护到位：确保没有特别明显、易被利用的脆弱性暴露；

2. 监测到位：确保安全监测全覆盖，没有明显的监测盲区；

3. 人员到位：确保岗不离人，时时有响应，事事成闭环。

1.2.2. 风险识别、评估与规划

能力规划与建设的前提是看清，看清自己、看清“敌友”、看清风险。

价值定位	• 某地方公立三甲医院，提供公共卫生服务，关系国计民生的关键基础设施。 • 日均门诊量 XX 万、手术 XX 台（三、四级手术占比 XX%）。 • 其 HIS、EMR 等系统属于关键信息基础设施
风险现状	• 完成部分核心系统等级保护评测工作。 • 上了态势感知系统，但未实现对底层日志、流量全覆盖。 • 终端及服务器安全软件未能全覆盖。 • 内外网存在网络隔离打通问题，存在文件违规传输问题。 • 网络收口不严，攻击暴露面大。 • 缺少专业人员，由安全集成商人员 7*8 驻场运维
风险接受能力边界	• 无法接受因勒索病毒等因素导致核心业务系统服务中断的风险。 • 无法接受病历等医疗数据泄露的风险。 • 无法接受网络安全事件触发的违法违规风险
强化思路	• 明确党政一把手对医院网络安全的主要责任，参照《党委（党组）网络安全工作责任制实施办法》。 • 进行整体安全规划，包括但不限于目标、架构、阶段性强化等内容。 • 在技术层面上，通过策略配置等手段强化网络收口和安全隔离。通过终端、服务器安全软件全覆盖等措施弥补最紧急的脆弱点。通过托管运营等手段，将安全运营能力覆盖到 7*24 全时段，不留安全空窗。 • 参照国卫规划发〔2022〕29 号《医疗卫生机构网络安全管理办法》，综合考虑预算、风险与合规要求，分阶段强化网络安全能力建设

• 看清自己

1. 业务是关键信息基础设施么？

2. 涉及大量公众用户数据或其他敏感数据么？

3. 业务链有哪些关键节点，上下游风险可控么？

4. 安全能力现状如何？

• 看清“敌友”

1. 遭遇过哪些安全事件，同类风险受控么？

2. 国内外同行有什么事件经验可借鉴么？

3. 我会被纳入“演练”清单么？

4. 谁能为我提供能力补全？可靠么？

• 看清风险

1. 面临哪些内外部风险？能自行弥补么？

2. 面临哪些合法合规风险？

3. 面临的风险和业务价值对等么？能否承受这些风险？

看清后，即可明确业务价值定位、风险现状与风险承受能力边界，并开始考虑强化路线。

例如（下表）：

1.2.3. 系统性保障能力建设

一、对于安全能力建设成熟度不高，还不能满足基础要求的关基运营者，应先对基础安全能力进行补全。

1. 网络收口

通过分区分域、设备部署和策略优化进行网络收口，通过 SD-WAN、零信任、网络准入等控制方式加强内外部双向收口。

2. 终端与服务器安全

终端、服务器作为人与业务、业务与业务的交互节点，是风险高度汇聚点。应该做好终端、服务器安全软件的安装和管理，确保做到全覆盖。

3. 资配漏补

资产不清则威胁不明，资产即是业务的载体也是风险的来源，应通过持续资产及变更管理明确有什么、是什么、有什么风险、谁是责任人等信息。

4. 安全监测全覆盖

对相关日志、流量进行全面监听，不留监测盲区。

5. 情报共享

充分利用威胁情报，并做好组织内、组织间的情报共享与应用。

6. 态势感知类运营平台建设

态势感知类系统作为风险监测及事件处置的汇聚调度点，是常态化安全运营体系的核心节点。

7. 人员配置

部署驻场值班人员，或采用专业的安全托管服务。

通过以上几点能力建设，可以实现基础的常态化保障运营能力。

二、在此基础上，还可根据组织所面临的风险级别和保障场景进行专项安全能力增强，包括但不限于：

1. APT 攻击检测及防控能力建设

2. 攻击诱捕能力建设

3. 数据安全能力建设

4. 防勒索能力建设

5. 供应链安全能力建设

6. 威胁预测及前置处置能力建设

三、对于安全防护建设成熟度高、能力强的用户，也可参考常态化运营模型，确保演练等重点时段度过后，依然能保持较高的持续保障能力。

1.2.4. 常态化运营能力建设

“岗不离人”是确保重保常态化能力落地的关键点之一，能力落实所需包括但不限于：

1. 岗位划分明确

应根据组织业务规模、编制规模进行岗位划分，包括但不限于监测岗、分析岗、处置岗、追溯岗等不同岗位。可一人兼多岗，也可多人并一岗，应根据重保时段进行灵活调整。

对于关基单位安全运营人员，需遵守关保安全要求中的“安全背景审查”制度。

2. 运营流程等体系性内容明确

明确运营操作流程、规范，编写策略、流程手册、SOP 进行正式发布。体系规范是常态化标准运营能力的有效指导，应对其进行周期性优化。（可参考北京冬奥四级文件体系）

3.SLA 规划

根据自身业务特性和行业要求设置合适的 SLA，并与岗位、流程设置等环节进行匹配。

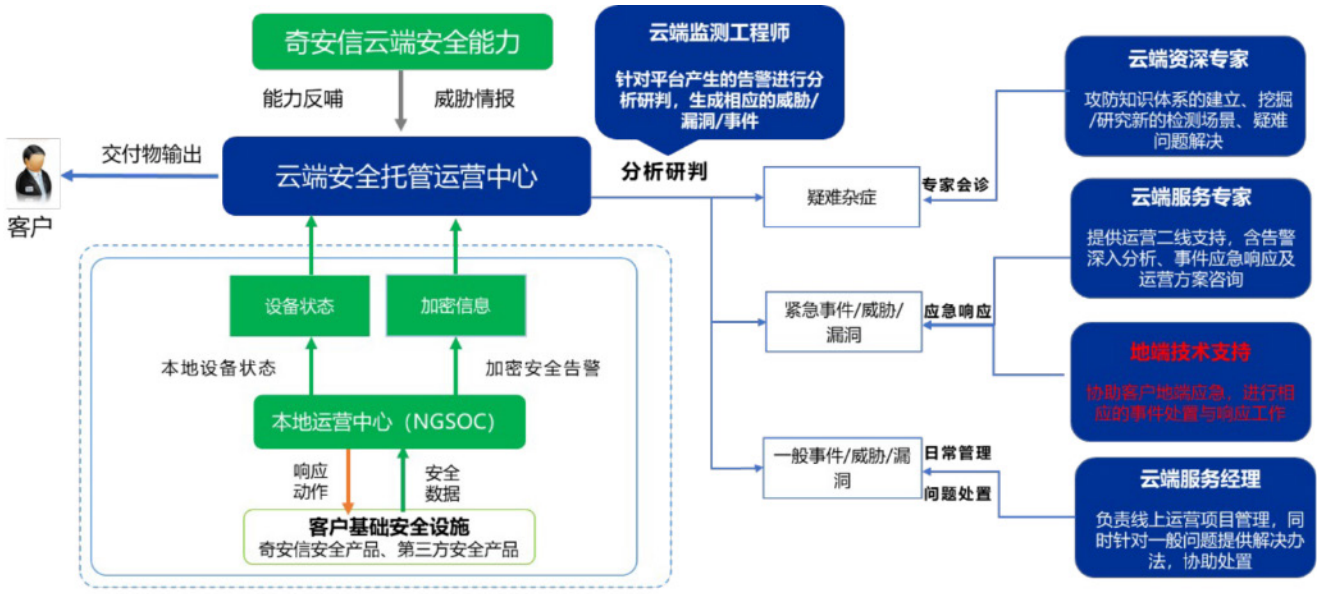
4.“岗不离人”

通过部署驻场值班人员或远程托管服务实现不间断安全运营。通过人的分析应变能力，解决自动化调度方式无法处理的问题。

5. 应急响应调度机制明确

对于 DDoS 攻击、勒索软件攻击等重大风险事件形成标准化应急机制，明确各角色在应急响应中的责任，控制风险窗口期。

特别要明确业务人员、IT 人员在



图：奇安信 MSS 7*24 安全托管服务

应急流程中的定位和作用。

6. 沟通汇报机制明确

明确日报、周报、事件报告等报告沟通机制，及时总结安全态势向管理岗进行汇报。对机构而言，应明确向保护单位的事件报告机制。

1.3. 成功案例

1.3.1. 冬奥网络安全零事故

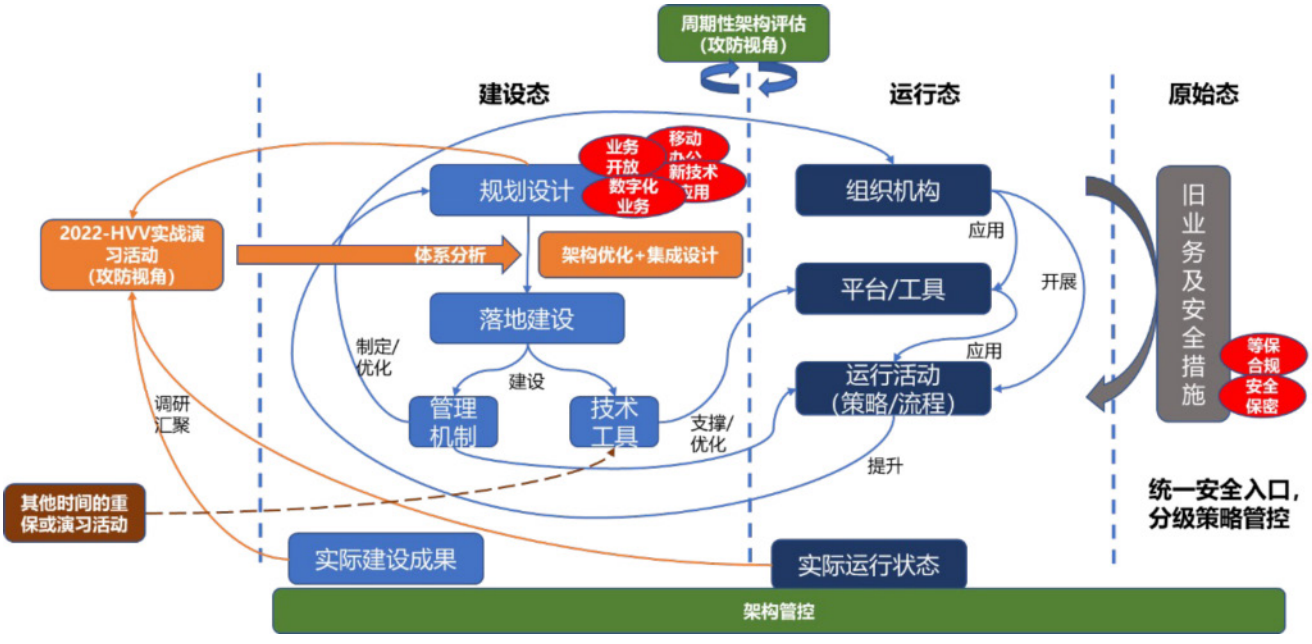
奇安信作为冬奥网络安全独家赞助商，从 2019 年年底到 2022 年一季度进行了长达两年半的冬奥安全防护体系建设与重保运营。

奇安信对冬奥网络安全承担完全、彻底、端到端的责任，面临来自全球海量攻击，取得了零事故的出色成绩。既上交了令人满意的答卷，也为未来奥运及其他重大活动的网络安全保障工作提供了值得参考和借鉴的标杆。

1.3.2. 中国电子（CEC）网络安全运营中心

CEC 安全运营中心参照冬奥零事故经验，通过 SD-WAN 等技术手段将 CEC 旗下数百家下级单位纳入集团一体化安全运营体系，解决了集团风险评估中发现的散、乱、虚、弱等切实问题。

通过集团一体化重保运营，取得了 2022 演练成绩优秀、二十大重保零事故的出色效果。



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

奇安信威胁情报中心

中国威胁情报行业领军者

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

威胁情报中心

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。

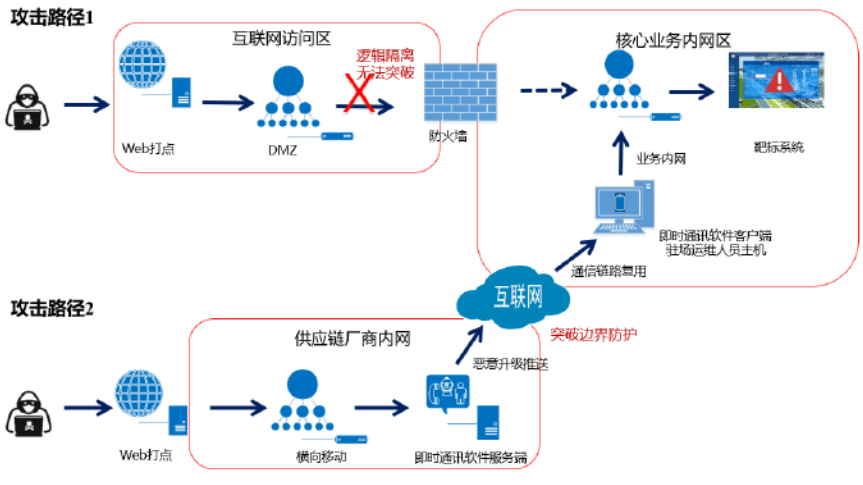
奇安信威胁情报中心：
ALPHA网址：https://ti.qianxin.com
雷达网址：https://r.ti.qianxin.com
扫描关注我们的微信公众号
邮箱：ti_support@qianxin.com

网络安全正面防守固若金汤？别忘记供应链攻击侧面迂回

能源领域的大型和特大型企业，以央企、地方国企居多。以石油、电力、煤炭、新能源等为代表的基础资源开发、流通，再到稳定可靠的供给和使用，关乎国计民生，是经济社会健康稳定运行的重要基石。能源企业的高水平、健康、可持续发展，离不开科学有效的现代化管理手段，离不开网络安全的有力支撑。能源行业的网络安全形势依然严峻，网络风险和安全事件十分严重。石油、电力、水利等能源行业作为国家关键基础设施通常具备较强的网络安全意识和防护能力，传统 Web 攻击和社工钓鱼方式已经很难取得正面突破。即使偶有突破进入内网，由于其内部网络采取安全分区措施，导致攻击队员在面对防火墙、网闸等安全防护设备时，很难在较短的时间内从技术上形成有效突破。

但众所周知的是，能源行业供应链规模上全球性的、大量的业务系统，需要借助厂商提供运维支撑。同时，由于厂商运维身份的特殊性，其具备访问目标内网的合法身份，以及掌握目标众多业务系统的管控权限。因此，如果能够“借用”厂商运维身份，进入目标内网开展横向移动，很可能会取得事半功倍的效果。

下面通过一个实战攻防演练的案例来具体说明。



攻击路径示意图

案例：巧借供应链厂商运维直达目标核心业务内网

在对某能源企业的攻防演练中，攻击队通过信息探测逐步摸清了目标互联网侧 Web 资产并收集了少量企业员工的邮箱、手机号、微信等联系方式。攻击小队根据前期收集的网情信息制定了以 Web 打点为主、社工钓鱼为辅的网络攻击方案。详细攻击路径如左图所示。

在攻防演练期间，能源企业的目标人员安全意识尤为警觉，导致社工钓鱼手段并未取得理想进展。而在 Web 打点中，攻击队利用前期储备的漏洞武器顺利撕开了目标网络外部防线，获得了目标内网访问权限。但是，在开展内网横向渗透时，由于目标内网实行了严格的内网安全分区策略，攻

击队所在 Web 网段与核心业务网段之间部署有某型号防火墙实现逻辑隔离。只有设法突破防火墙隔离才能访问部署在核心业务网段的靶标系统。时间紧迫，硬刚防火墙显然不是最优策略。

柳暗花明又一村，攻击队在内网信息收集中获得了重大发现，该目标核心业务内网区部署有某厂商的信息系统，且由厂商驻场人员提供信息系统日常维护服务。由此攻击队迅速调整攻击方案，将供应商驻场运维人员作为下一步攻击的重点对象。在征得多方授权的前提下，攻击队针对目标供应链厂商开展渗透攻击。

首先对供应链厂商开展信息收集，发现该供应商网络安全防护能力较弱。攻击队很快发现该厂商 OA 系统存在历史漏洞，通过漏洞利用成功进入供应链厂商内网，经过一系列内网拓展最终控制该厂商自研即时通讯软件服务器权限。进一步分析即时通信软件聊天记录，攻击队获得了重要线索，即通过聊天日志和访问 IP 定位到厂商外派到目标企业的驻场运维人员，因此下一步要做的就是如何搞定驻场运维人员。既然已经获得厂商的即时通信软件服务器控制权限，利用服务器进行恶意软件推送不失为一个好办法。

接下来，攻击队迅速组织人力对即时通信软件版本升级服务、软件推送机制开展逆向分析，功夫不负有心人，后方技术团队很快破解了软件秘钥，实现了恶意软件推送，并通过链路复用技术一举解决了目标核心业务网段出网流量白名单限制问题。攻击队利用技术手段向目标驻场运维员推送即时通信软件更新服务，诱导运维人员点击更新，成功上线多台运维主机。通过上线运维主机可以直达企业靶标系统，最终攻击队利用储备漏洞顺利打下靶标系统，成功获取靶标系统权限，为本次演习画下完美的句号。

> 传统 Web 攻击和社工钓鱼方式
> 已经很难取得正面突破，
> 但“借用”厂商运维身份进入目标内网
> 开展横向移动很可能会取得事半功倍的效果。

防守加固建议——面向供应链攻击的安全防护策略

1、案例剖析

由于供应链厂商的 OA 系统存在历史漏洞，案例中攻击者通过漏洞利用成功进入供应链厂商内网，并最终控制该厂商自研的即时通信软件服务器权限，再通过对供应链厂商外派到目标企业的驻场运维人员进行 OA 软件恶意升级推送，成功上线多台运维主机，最终以供应链攻击的手段拿下目标企业的靶标系统。

这暴露出目标企业在供应链安全防护上存在“安全风险意识薄弱”和“管理措施不到位”等问题。

2、防护策略

近几年，供应链攻击呈上升趋势，Gartner 预测，到 2025 年全球 45% 的企业机构将遭遇软件供应链攻击，相比 2021 年增加了 3 倍。供应链攻击深度和广度的延伸，也给组织的网络安全带来了更大的挑战，传统的防御手段聚焦在组织自有业务数据资产。为有效应对供应链攻击，组织需通过实施供应链安全防护专项来“发现全链路安全隐患”并进行有效整改和能力提升。

奇安信的《供应链安全服务解决方案》，通过“供应链的资产及网络连接梳理、供应商暴露面排查、供应链信息系统与产品的漏洞风险排查、供应链安全事件应急及情报共享”四步走，能为客户提供“快、准、全”的供应链全生命周期闭环检查，及时发现供应链存在的风险并进行有效整改，帮助客户严守供应链安全阵线。

具体服务内容如下：

（1）供应链的资产及网络连接梳理：涵盖供应链企业梳理、供应链系统产品梳理、供应链网络连接梳理等内容，帮助客户形成清晰可见的资产清单。

（2）供应商暴露面排查：涵盖网络暴露面风险排查、集权设备风险排查、敏感信息风险排查等内容，帮助客户减少攻击面，防微杜渐。

（3）供应链信息系统与产品的漏洞风险排查：涵盖源码及开源组件安全检测、漏洞评估、漏洞发现处置等内容，帮助客户提前发现漏洞，降低风险。

（4）供应链安全事件应急及情报共享：涵盖情报共享、应急响应、教育培训等内容，帮助客户建立情报体系，在攻击事件发生后能有效应对。安

路虽远，行则将至

——京东方安全运营中心的 5 年探索路

作者 | 研究员 张少波

“京东方不仅仅是传统认知的一家科技制造企业，而且扩展出很多的业态，既包括小课屏、画屏等面向 C 端的创新产品，也包括互联网医院、移动健康等智慧医疗服务。这就意味着我们的信息系统和数据开放性更强，暴露面更广，因此网络安全面临的挑战也越来越严峻。”京东方安全中心负责人李楠这样表示。

京东方科技集团股份有限公司（BOE）创立于 1993 年 4 月，是一家领先的物联网创新企业，形成了以半导体显示为核心，物联网创新、传感器及解决方案、MLED、智慧医工融合发展的“1+4+N+ 生态链”业务架构。目前京东方在全国多个城市拥有制造基地，子公司遍布全球 20 个国家和地区，服务体系覆盖欧、美、亚、非等全球主要地区。

更开放的业态拓展，更广泛的全球布局、更庞大的 IT 系统规模……都给京东方信息系统的网络安全提出了严峻挑战。在这种情况下，从 2018 年起，京东方就启动安全运营中心（SoC）

建设，是国内最先部署 SoC 类产品的大型企业之一。经过多年建设，SoC 的成熟度已经走在了行业前列，并屡获权威机构的推荐。

启动篇：以资产为抓手破解“安全孤岛”难题

据李楠回忆，京东方从早期就非常重视网络安全，并在各个模块都有齐全的防护措施，如数据安全方面有特权账号管理，终端防御、网络防御、主机防御都有安全部署，可以应对常规的病毒木马、数据泄露、非授权访问等常规威胁。

然而，随着集团信息化建设不断深入，业务系统资产及漏洞暴露面越来越大、大量日志数据孤岛丛生，缺少关联及分析、安全措施各自为战、难以协同等问题也日益凸显。同时，随着各类安全产品的不断部署，海量安全日志无法得到合规存储，不仅存在合规风险，也存在日志无法有效利用的运营瓶颈。

面对千丝万缕、纷繁庞杂的集团网络安全状况，该如何破题？李楠团队给出的答案是“着眼资产”，即以资产为抓手，盘清家底、统揽全局。

面对千丝万缕、纷繁庞杂的集团网络安全状况，该如何破题？
李楠团队给出的答案是“着眼资产”，即以资产为抓手，盘清家底、统揽全局。

“选择资产为切入口，基于两层原因，首先是 2016 年 4 月 19 日习近平总书记主持召开的网络安全和信息化工作座谈会中，重点提到‘要全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改。’另一方面，就是京东方在终端安全方面已经有了良好的基础，将终端资产作为安全管理的切入口，就变得顺理成章、水到渠成。”

在这种情况下，奇安信刚推出不久的态势感知与安全运营平台（NGSOC），走进了京东方的视野。尤其是该平台在资产发现、日志收集、关联分析、服务器脆弱性管理等功能方面，吸引了京东方的极大关注。

图：京东方 SoC 第一阶段态势感知展示

在李楠看来，资产是网络安全运营管理非常重要的环节，第一阶段的核心工作，是以资产为中心收集资产、脆弱性、日志、流量等基础数据，并对数据进行分类梳理，对安全事件进行管理，以实现基础运行，为运行可控打好基础。从 2018 年到 2019 年，京东方依托态势感知平台完成了 SoC 建设的第一阶段。

第一阶段的建设从几个层面展开：在资产层面，通过人工录入、模板导入、流量探针、主机安全管理、漏扫等措施，实现了梳理资产、摸清家底；在漏洞层面，通过定期脆弱性扫描、漏洞与资产自动匹配、资产风险评估等机制，找出漏洞并有效管理；在日志留存层面，通过态势感知平台完成日志汇聚、资产安全事件回溯分析、审计合规等基础性工作；在威胁发现层面，通过建立有效而全面的流量分析，有效发现大量透过防御体系的安全风险；而在事件管理层面，通过大数据处理技术及威胁情报匹配，以及资产数据信息查询责任人等，大大提高了安全事

件的分析处置效率。

该阶段建设的效果可谓立竿见影：在运营方面，实现了所有已知资产对应责任到人，高危漏洞有效管理，资产、漏洞、告警有效关联，关键安全事件闭环解决率 100%，安全事件响应时间节约 90% 以上，并可通过仪表板、大屏等方式数字化展示集团网络安全各维度关键指标。在合规方面，实现日志留存 6 个月以上，完全符合法规及等保要求，并支撑 HR、ERP、画屏及邮箱等系统顺利完成等级保护测评。

完善篇：“多平台互联互通 构建安全中枢大脑”

“第一阶段建设显著提升了集团的安全水平，但随着 SoC 发挥的作用越来越大，我们也发现了新的问题，例如，部分告警资产无法找到责任人，子公司告警无法有效定位，告警量大，告警流程手工处理慢等。”李楠表示。为此，从 2019 年开始，集团决定启动 SoC 第二阶段，即功能完善建设阶段。

根据规划，SoC 第二阶段的任务，主要是完善并实时了解资产属性信息变化，属地公司部署流量探针，集团完成平台扩容，和周边设备做数据打通，对关联规则告警进行优化降噪，网络安全数字化展示等，进而支撑资产、事件、漏洞全生命周期管理。主要围绕以下几个方面：

首先是更精细化的资产管理。一期工程尽管实现了有效的资产发现及资产管理，但由于所管理的组织过于庞大，资产责任部门及责任人时常动态变化，故存在一些在网设备无法实时准确对应责任部门及责任人的问题。同时资产缺少入网、退网状态管理。该阶段，京东方通过定制化开发完成 SoC 平台和 CMDB（资产管理系统）数据的实时打通，给每个资产赋予 BMC 编号，并通过 API 接口完成态势感知平台及 CMDB 资产数据之间的实时同步，以应对组织及人员变化对资产准确性的影响。通过自定义资产属性字段增加入网、退网标签，并通过“资产发现确认”流程，对入网 / 退网资产进行管理。真正实现了从看见发现，到清晰识别和实时掌控。

其次是建立集团化安全运营。作为分支机构遍布全国各地的大型集团企业，京东方对于大型属地公司和小型属地公司采取不同的部署、运营和账号权限策略。集团可通过级联管理及分权分域管理向属地单位下发针对性关联分析规则及预警通报，以对下级单位进行赋能。基于平台计算存储所需资源，态势感知平台服务器集群也在随着数据量的增加而增加。

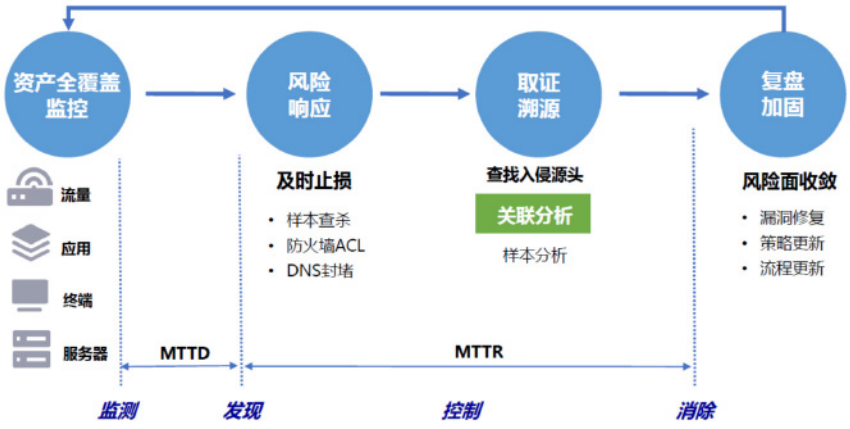
再次是和周边设备完成数据拉通，夯实安全大脑定位。通过定制化开发及 API 接口的对接，京东方先后完成和多个产品间的数据打通。例如，和主机 CWPP 对接自动获取服务器资产及配置基线数据；和资产管理系统对接完成全集团资产数据信息的实时同步；和漏扫设备对接，实现直接在态势感知平台调用漏扫设备下发扫描策略进行扫描并自动导入漏扫结果；和第三方威胁情报平台对接，完成双威胁情报匹配，为自动化处置打下基础；和 ITSM 系统对接，实现手动或部分确认性告警及脆弱性风险自动派单，缩短人员处置响应时间；和用户中台对接，从用户中台同步用户信息实现 SoC 平台的单点认证登录；和短信及移动门户平台对接，实现告警及风险的消息提醒；和工控安全产品对接，实现 IoT 设备数据一体化分析、管理和展现等。

再者是更加持续优化的安全运营。李楠做了一个比喻，NGSOC 在整个安全运营中就如同“大脑中枢”，它一方面“眼观六路、耳听八方”，打通集团各类平台并汇聚分析集团资产、漏洞、日志、流量、告警等各类数据。另一方面，要“知行合一”，通过新增“告警处理流程”“漏洞处置流程”，实现对告警处理闭环和漏洞生命周期管理，避免对安全风险出现“跟丢跑飞”的情况。对于告警量过大的通病，京东方通过各种技术手段进行筛选，结合长时间的风险修复运营，告警量已从最初的每日上万级下降到每日上百级，达到人工可逐一分析处理的水平。

最后是更为灵活多维的安全态势展现。一期工程由于缺少相应数据及功能支撑，仅有外部威胁态势、内部威胁态势、资产风险态势、安全运营态势等部分大屏。持续优化之后，增加了包括资产态势、全网脆弱性态势、攻击者态势、业务外联态势、威胁预警态势、攻防演练态势、综合安全态势、漏洞生命周期态势、全球 BOE 设备及流量监控态势、应用系统安全态势等大屏展示场景，从而更加数字化、专题化、精细化的展示京东方整体网络安全态势。

通过该阶段的功能完善，京东方 SoC 的资产管理更加契合自身安全管理属性，并实现了告警处理闭环和漏洞生命周期管理。尤其在告警准确及风险闭环方面，京东方走在了国内前列。

图：京东方资产安全运营可视化平台架构图



图：SoC 第三阶段建设的关联规则优化

优化篇：深入业务威胁建模 夯实风险管理屏障

阶段一和阶段二建设完成后，整体安全运营框架搭建完毕，安全运营体系基本形成。但随着集团数字化转型的持续开展，业务系统和安全要素的融合越来越密切，各类新的问题也开始出现，比较明显的主要是两方面：基于业务场景的关联规则分析能力不足，SoC 特定的告警处置占用了安全人员大量时间。

“安全人员不懂业务，业务建模有难度，是红蓝双方共同的痛点。”京东方 SoC 建设负责人张森对打通安全和业务的难度，有着深刻理解。为了强化基于业务场景的关联规则分析能力，京东方开展业务建模工作，通过深入分析业务安全需求，实现了业务指标和 IT 指标的深度绑定。

以钓鱼邮件为例，过去仅有钓鱼邮件告警这一粗粒度的 IT 指标，业务建模之后，细化为钓鱼邮件收取率、打开率、URL 点击率等业务指标；同

样，边界安全的防火墙 IP 阻断 / 允许次数，转化为关键业务攻击量。基于业务场景制定了大量关联分析及基线分析规则，包括账号新增、账号锁定、钓鱼邮件、运维审计等。通过该项工作，最终实现了以资产、业务为核心的全集团风险管理并积累了大量安全运营知识库。

除了推动业务建模，京东方运营团队和奇安信一起，重点推动了海量告警的合并降噪。具体采取了定期梳理资产、告警归并、告警降噪、建立运营模式等多项措施，通过明确责任人以治降噪，对具有相同属性的告警数据根据特定逻辑进行归并，过滤明显的无效数据，通过威胁情报进行二次校验，对运营知识积累形成知识库等措施，大幅度减少低价值告警数量，实现了运营效率的显著提升。

效率篇：NGSOC+SOAR 双剑合璧 自动化响应提质增效

完成前三个阶段之后，京东方 SoC 已经具备了体系运营的基础，在成熟度层面逐渐成为行业翘楚。从 2022 年开始，京东方将安全自动化响应提上了日程。“安全运营人员的精力和时间是宝贵的，我们希望他们从繁琐事务中解放出来，投入到事件研判、溯源追踪等更高价值、更高技术含量的工作之中。”

具体实现上，京东方针对通用的、大批量的、固定流程的告警，以及运维人员告警处置过程等形成 SOP。并在 NGSOC 基础上，通过定制安全自动化编排与响应工具（SOAR），集成多类自动化通知，将人工处理的过程定义成剧本，实现告警自动化处理。

通过 SOAR 剧本的编排，最终大幅度缩短了 SoC 响应和处置时间，提升了效率。从实际效果来看，自动化处置和人工处置相比，在 NGSOC 中发现同类告警，时间从 3 分钟缩短到不到 10 秒钟；根据告警查询文件信誉 / 文件信息，时间从 5 分钟缩短到 5 秒钟；下载文件和上传文件检测内容，时间从 5 分钟缩短到 10 秒钟以内；而发送告警处置结果通知，时间从 2 分钟缩短到 5 秒钟以内），整体的响应处置时间从 15 分钟缩短至 30 秒钟，效率提升幅度达到 96.7%。

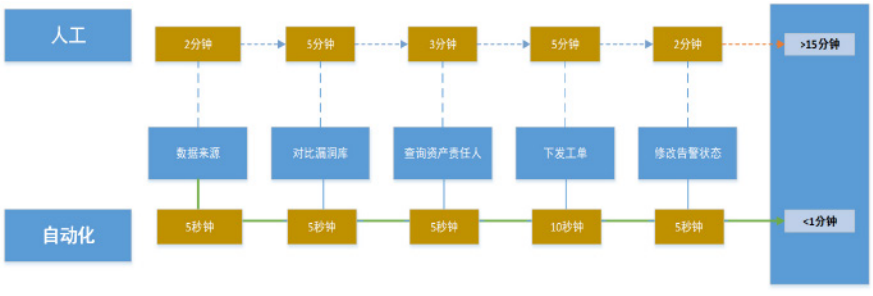
更重要的是，NGSOC 和 SOAR 的强强联合，可形成“采集 – 分析 – 响应 – 复盘 – 总结”的持续动态闭环，解决了安全运营的最后一公里落地问题。对于漏洞管理可以实现全流程闭环管理，能够追责到资产漏洞责任人，并进行告警状态调整。针对自动工单派发，在 NGSOC 中产生的告警，由人工派单转换为自动下发处置工单，并可通过邮件、短信、内部通信工具等方式通知资产责任人，加快整体派单效率，相关方可持续跟踪工单处置状态。

李楠总结道：“通过自动化响应、自动派单的安全运营模式，我们可以在实践中不断的复盘整改，让运营人员腾出精力去做更隐蔽的攻击行为分析或漏洞研究，反哺平台的告警分析规则，最终形成一个‘告警处置越来越智能，平台运营越来越省心，风险识别越来越精准’的良性循环，推动 SoC 真正迈入高成熟度的体系运营阶段。”

结束语：

根据赛迪顾问发布的《2021—2022 中国安全运营中心调研分析报告》（简称：《报告》）显示，国内企业安全运营中心建成率已接近九成，但有高达 65.5% 的受访企业仅处于一、二级成熟度区间”，大多数企业安全运营中心的成熟度还比较低。《报告》重点推荐了京东方的安全运营中心的建设案例，按照赛迪顾问的成熟度模型，京东方已接近实现了四级的体系运营，并向最高级——五级的深度运营逐步靠近，在国内大型企业中处于领先水平。

“路虽远，行则将至；事虽难，做则必成”。京东方 SoC 能取得安全运营成熟度行业领先的成绩，归其原因，不仅仅是布局早、规划清晰，更重要的是将规划目标的每一项任务分解都落到了实处，每一个细微工作都做到了极致，拾级而上、聚沙成塔，经过 5 年持之以恒、日积月累的分阶段建设、分步骤实施，京东方的安全运营中心，最终成为全行业的重要标杆。安



图：NGSOC+SOAR 实现响应效率的显著提升

规划快一步

奇安信 | BEIJING 2022

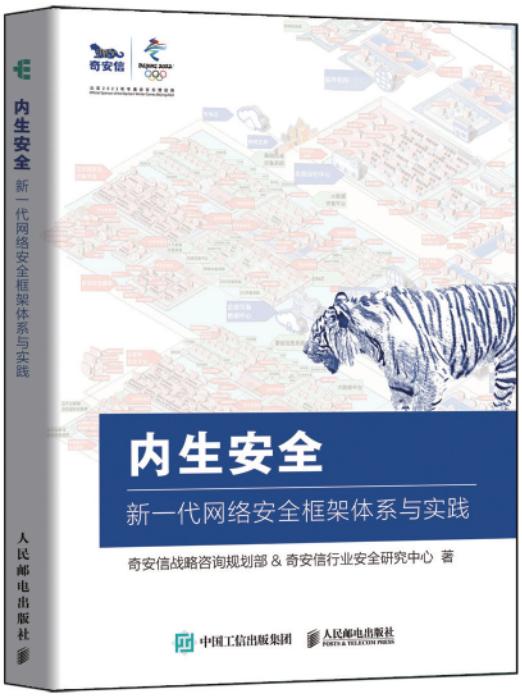
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

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

狂拽酷炫的科幻与流浪的网络安全

长度突破 9 万公里的太空电梯、算力突破天际的550系列量子计算机、动力足以推动地球流浪的行星发动机……癸卯兔年的大年初一，导演郭帆再次将中国式科幻搬到了大银幕上，数字生命、脑机接口、阵列爆炸等新鲜名词，让刚从疫情阴影之中走出不久的观众们应接不暇。

在《流浪地球 2》的世界观里，诞生了两大主要的对立阵营：其一是“躺平派”，面对几乎无法反抗的地球灭绝危机，这一派主张将人类数字化，即将人类信息通过脑机接口传输至另一个平行的数字世界，从而达到虚拟永生的目的；另一派则是“反抗派”，作为流浪地球计划的主体，中国提出的“移山计划”想要建造 1 万座行星发动机，从而推动地球走向新家园。

尽管“躺平派”的数字生命计划最终被 UEG 伦理委员会禁止，但两派之间的“明争暗斗”，在巨大的地球危机面前，还是酿成了一次次的网络安全危机。

从服务器入侵，到“反水的”无人机

为了破坏“流浪地球计划”“数字生命计划”的反叛者们入侵了基地的控制系统，控制了大量原本负责守卫基地安全的无人机，对基地进行无差别攻击。

出于无奈，技术员们只好使出杀招，利用新一代量子计算机 550C 覆写了系统，重新取得控制权。

大概是由于基地内部庞大的服务器集群和数以百万行计的代码量，即便是拥有顶级算力的量子计算机，也难以在短时间内完成全部的代码覆盖。过长的响应时间使得基地损失惨重，大量人员当场命丧。

视频画面带来的视觉冲击，让身处现实世界的观众难以想象：保卫人类家园的最先进武器，竟然在黑客攻击下，残忍地收割了一条又一条无辜者的性命。

一个略带讽刺的事实是，为了避免频繁的网络攻击，在太空电梯危机之后，联合政府下令断开了全球互联网。

很多人看到这里，可能会发出疑问：按常理来说，如此重要的系统理所应当会受到很好的保护，从数据加密到流量检测应有尽有。可即便是这样，在具有深厚背景的黑客组织面前，那些看似固若金汤的网络安全防线，

竟然显得如此脆弱。

难道面对隐藏在暗处、有组织的网络攻击，真的束手无策么？其实，网络攻击从来不是一蹴而就的，只要知己知彼，就能将损失降至最低。

通常来说，攻击者从寻找突破口到篡改代码，再到下发最终的攻击指令，需要不断变换攻击手法，同时躲避一个又一个网络安全设备的检测，如同小偷从踩点到最终打开保险柜，这个过程肯定需要消耗大量的时间，这段时间对于基地来说，是异常珍贵的。只要发现攻击行为，更容易将网络攻击消弭于无形。

同时，和攻击者赛跑，完成“发现－响应－阻断－预防”闭环，是防守方的必备技能。想要将所有网络攻击都挡在外面，是一件不可能做到的事情，攻击者总是可以找到无处不在的漏洞和风险暴露面，所以用最短的时间、最全面的防护体系发现攻击者的行踪，并及时阻断才是最关键的。

想要达到这个目标，基地的网络安全体系应至少包含以下几点：

第一，在网络边界部署必要的边界防御设备，如奇安信新一代智慧防火墙，通过适当的访问控制策略，阻断大部分的外部非法访问和病毒木马入侵；

第二，在网络的关键节点部署流量检测与响应设备，如奇安信天眼新一代安全感知系统，识别网络流量中隐藏的网络攻击行为和恶意文件；

第三，在关键服务器上部署服务器安全软件，如椒图服务器安全管理系统，能够及时发现并服务器内部的恶意行为；

第四，整个防御体系应该是协同联动的。当其中任意一点出现异常时，能够及时联动所有防御节点，阻断攻击链条。

《流浪地球 2》这个控制无人机攻击给了现实世界一个重要启示：5G 网络、IPV6 让万物互联逐渐走进现实，在万物皆可互联的背景下，智慧交通、智慧医疗、智慧能源等，或许都会由城市大脑的服务器进行控制，谁又能保证太空电梯危机不会走进现实呢？

从身份窃密到炸毁空间站的太空电梯

与控制无人机同时进行的，是一次针对太空电梯的入侵。

作为“流浪地球计划”的核心，“数字生命派”的反叛者们势必要击毁“方舟号”空间站，因此他们提出了这样一个计划：在基地被大量无人机攻击的空挡，趁乱利用太空电梯将爆炸物送上空间站，将空间站与太空电梯同

时摧毁。

想要实现这个计划，夺取太空电梯的控制权就成为了关键。

来看看电影中反叛组织是怎么做的。

第一步，攻击者利用各种社会工程学等欺骗手段，伪造了刘培强和韩朵朵的身份信息，骗过了地面门禁后成功进入太空电梯。

第二步，攻击者利用 AI 换脸技术，骗过了系统的身份验证机制，成功登录后实现了对太空电梯的控制。

最终，“数字生命派”支持的恐怖分子采用自杀攻击的形式，引爆了紧贴轿厢的导弹，“方舟号”空间站轰然倒塌。

那么这其中就有两个问题。

其一，系统的身份验证机制明显不够强壮，以至于在量子计算时代，凭借一个在目前已经不算新鲜的 AI 换脸技术就足以绕过。

量子时代的事情现在还说不清楚，但目前对用户的身份验证机制主要包括这么几种：静态口令认证、动态口令认证（短信验证码、动态口令生成器等）、生物识别认证（指纹、人脸）等。

其中，静态口令认证是现阶段使用最为广泛的手段，用户输入账号、密码即可完成身份验证。

但这种方法也是最不安全的。攻击者能够使用网络钓鱼、暴力破解、撞库攻击等多种手段来破解登录口令。而且在强大的算力支持下（尤其是量子计算），任何看似复杂的登录口令，都有可能分分钟被破解，即便是只有图丫丫才能记住的那个长达三万位的动态口令也并非万无一失。

事实上，对于太空电梯这个级别的关键信息基础设施而言，无论单独采用任何一种验证方式，都是不够安全的。

从理论上来说，多因素认证拥有更高的安全性。按照概率计算，假设一种身份验证机制的破解几率是 5%，那么同时破解双因素认证的概率就是 5%*5%，有 n 个身份认证因素，破解概率就是 5% 的 n 次方。

当然考虑到易用性等因素，认证因素也不是越多越好，否则攻击者拦没拦住先不说，倒是把自己人搞得够呛。

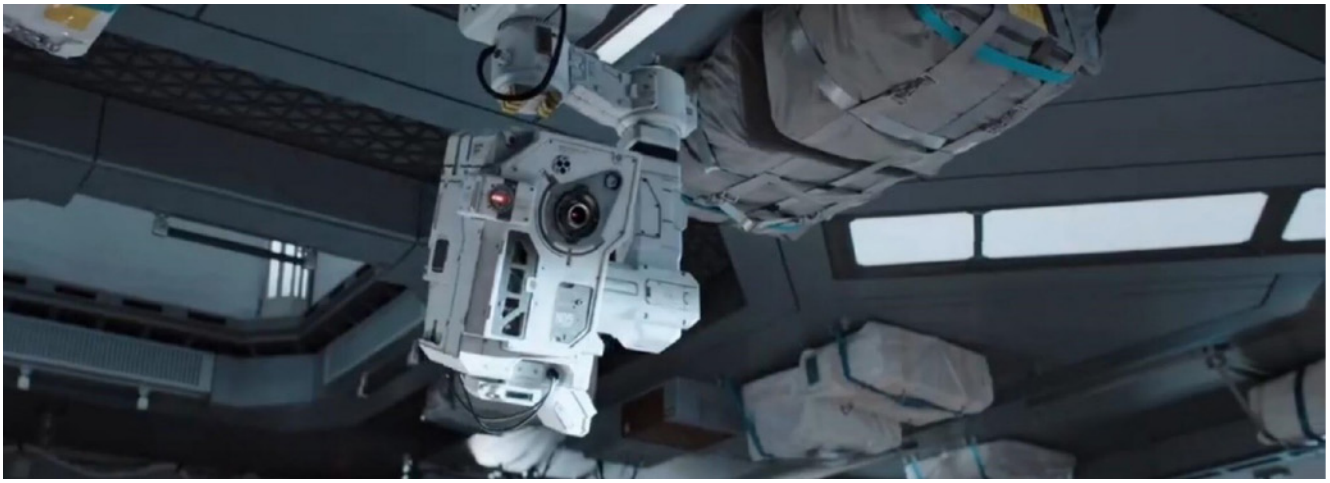
其二，相关账户的权限过高，以至于攻击者在登录后可以随意操控太空电梯。

相对于普通账户，特权账户因其拥有较高的权限，更容易成为攻击者的入侵对象。但是对于一个复杂系统而言，想要确保所有特权账户都不被入侵，几乎是不可能做到的事情。

并且，即便是账户没有失窃，内部员工也不见得不会吃里扒外。如果有了内鬼的支持，恐怖分子或许大可不必费尽周章攻击基地。

因此要想解决上述两点问题，真正需要的是一种动态的、实时的、刚刚好的身份认证和访问授权机制，通过统一身份管理、权限管理、单点登录、自适应多因子认证、身份分析与治理等多维度核心能力，对访问主体进行持续感知和验证，对访问上下文进行持续评估，最终实现端到端的动态细粒度身份认证和访问控制。

而这正是奇安信零信任体系的核



心。

当然，为了进一步降低账号失窃的风险，关键信息基础设施运营者还应通过技术手段（如奇安信网神特权账号管理系统）建立完整的特权账号台账、制订特权账号密码轮换、存储与备份机制、完善的机机交互能力，实现对各类基础设施资源账号的全生命周期管理。

细思极恐的 moss

随着全球互联网踩点重启成功，电影《流浪地球 2》也进入了尾声。但在长达数分钟的演职人员字幕之后，导演郭帆还拍了一段小小的彩蛋：人工智能 moss（也就是量子计算机 550W）与图恒宇的对话。

有一小段对话大致是这样的。图恒宇：是你毁掉了月球发动机；Moss：包括但不限于 2044 年太空电梯危机；2058 年月球坠落危机，以及未来的 2075 年木星引力危机和 2078 年太阳氦闪危机。

在电影刚上映的那几天，或者是由于电影院在演职员表出现以后就提前开灯，导致有部分观众并没有看到最后的彩蛋。

郭帆或许希望以这样的方式告诉观众，拥有意识的人工智能竟然具有如此巨大的破坏力。除了碳基生命，硅基生命也就是机器人，同样能成为地球的主宰。

细思极恐！

但在技术还不那么发达的今天，人工智能还远未如此先进，但人工智能算法受到网络攻击也并非什么新鲜事。

这对于网络安全从业者来说，又是一个巨大的挑战。

地球的流浪计划还在继续，网络安全可不行了，木星引力危机和太阳氦闪危机，还需要保驾护航。安

《补天漏洞平台报告》：2022年漏洞增长15%

摘　要

- 2022 年全年，补天漏洞响应平台共收录白帽子报告的全国各类网站安全漏洞约 16.8 万个，较 2021 年的 14.6 万个增长了约 15.0%；漏洞共涉及网站约 9.0 万个，较 2021 年的 11.5 万个减少了约 21.7%。
- 从行业分布来看，2022 年，补天平台收录的 IT 信息技术类网站漏洞数量最多，共有 32088 个，占比约为 19.1%；其次是制造业网站，共收录漏洞 15456 个，占比约为 9.2%；生活服务类网站排名第三，共收录漏洞 12264 个，占比约为 7.3%。
- 2022 年全年，补天平台收录网站漏洞数量最多的十个省级行政区，相关漏洞占到了漏洞收录总量的 74.6%。其中，IP 地址在广东省的网站漏洞最多，占比为 14.8%，其次为北京市，占比为 10.8%。
- 从漏洞的风险等级来看，在补天平台 2022 年全年收录网站安全漏洞中，高危漏洞 4.7 万个，占比约为 28.1%；中危漏洞 9.2 万个，占比约为 54.8%；低危漏洞 2.9 万个，占比约为 17.1%。
- 从技术类型来看，补天平台 2022 年全年收录的网站漏洞中，SQL 注入漏洞最多，占比约为 31.8%；其次是信息泄露类漏洞，占比约为 23.1%；配置错误排第三，占比约为 17.1%。
- 2022 年，补天平台收录漏洞的平均确认率约为 97.2%，未确认率为 2.8%。从已注册厂商确认的漏洞修复情况来看，2022 年，补天平台收录的漏洞修复率可达 69.8%。

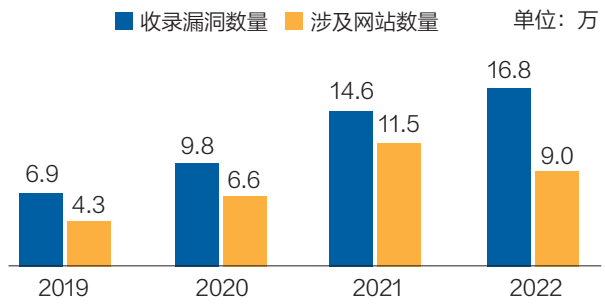
第一章 漏洞收录情况

一、 漏洞收录增长 15.0%

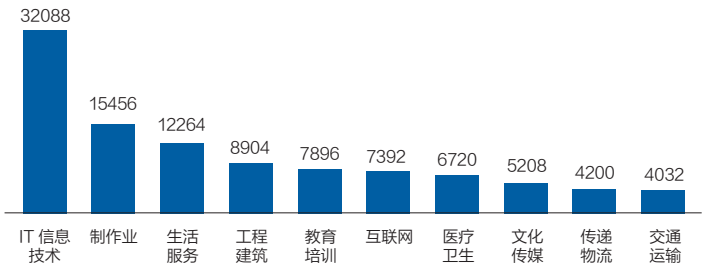
2022 年全年，补天漏洞响应平台（以下简称：补天平台）共收录白帽子报告的全国各类网站安全漏洞约 16.8 万个，较 2021 年的 14.6 万个增长了约 15.0%；漏洞共涉及网站约 9.0 万个，较 2021 年的 11.5 万个减少了约 21.7%。

下图给出了 2019 年以来，补天平台每年收录网站漏洞的情况对比。总体来看，补天平台每年收录网站漏洞的数量持续高速增长，这与国内机

补天平台历年收录网站安全漏洞情况



2022 年补天平台收录网站安全漏洞行业排行 TOP10



构日益重视、白帽子群体不断扩大、挖洞水平日益提升等多种因素有关。同时，优质白帽资源也正在不断的向那些愿意投入资源做好 SRC 的企业集中，这是导致挖洞数量增长、漏洞涉及网站数量却不升反降的重要原因。

左上图给出了 2022 年补天平台每月收录漏洞数量的情况。受新年和疫情等因素影响，第一季度收录漏洞数量相对较少，月均 3000 个左右。12 月收录的漏洞数量最多，近 3.4 万条。

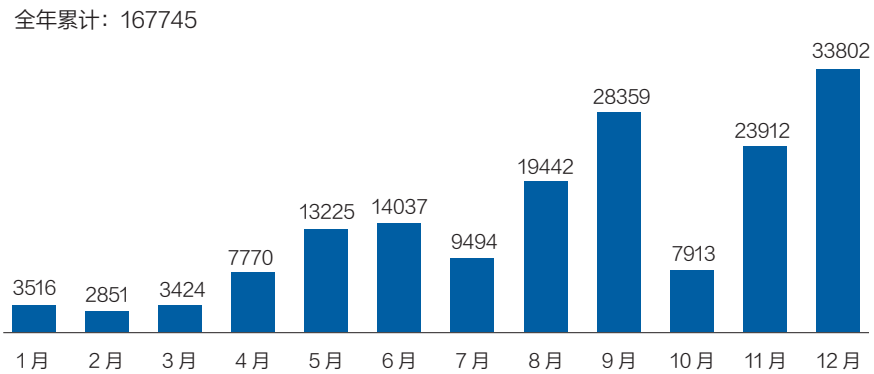
二、 IT 信息、制造与生活服务业漏洞居前

从行业分布来看，2022 年，补天平台收录的 IT 信息技术类网站漏洞数量最多，共有 32088 个，占比约为 19.1%；其次是制造业网站，共收录漏洞 15456 个，占比约为 9.2%；生活服务类网站排名第三，共收录漏洞 12264 个，占比约为 7.3%。此外，工程建筑、教育培训、互联网、医疗卫生、文化传媒、快递物流、交通运输等行业网站，被报告的漏洞数量也相对较多，排入 TOP10，详见右上图。

三、广东、北京漏洞占比居前

本报告中，对网站漏洞进行地域划分的主要依据是通过网站 IP 地址查询其网站服务器归属地，这可能与网站实际运营机构的行政归属地存在一定的差异。2022 年全年，补天平台收录网站漏洞数量最多的十个省级行政区，相关漏洞占到了漏洞收录总量的 74.6%。其中，IP 地址在广东省的网站漏洞最多，占比为 14.8%，其次为北京市，占比为 10.8%。具体如下图所示。

2022 年补天平台收录网站安全漏洞数量月度分布

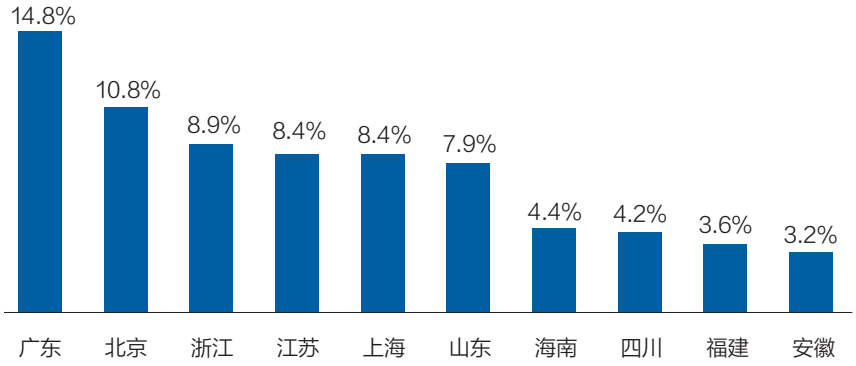


第二章 漏洞特征分析

本章主要从漏洞等级和类型分布来分析网站安全漏洞形势。

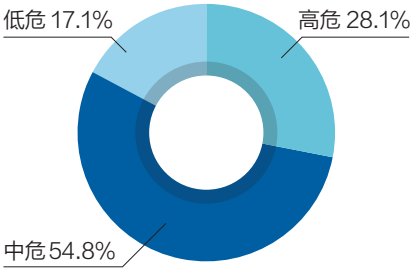
一、 高危漏洞占比近 30%

2022 年补天平台收录网站安全漏洞地域排行 TOP10



从漏洞的风险等级来看，在补天平台 2022 年全年收录网站安全漏洞中，高危漏洞 4.7 万个，占比约为 28.1%；中危漏洞 9.2 万个，占比约为 54.8%；低危漏洞 2.9 万个，占比约为 17.1%。详见下图。

2022 年补天平台收录网站安全漏洞危险等级分布



二、 SQL 注入漏洞占比最多

从技术类型来看，补天平台 2022 年全年收录的网站漏洞中，SQL 注入漏洞最多，占比约为 31.8%；其次是信息泄露类漏洞，占比约为 23.1%；配置错误排第三，占比约为 17.1%。此外，弱口令、代码执行、文件上传等漏洞也比较常见。具体漏洞类型分布请见下图。

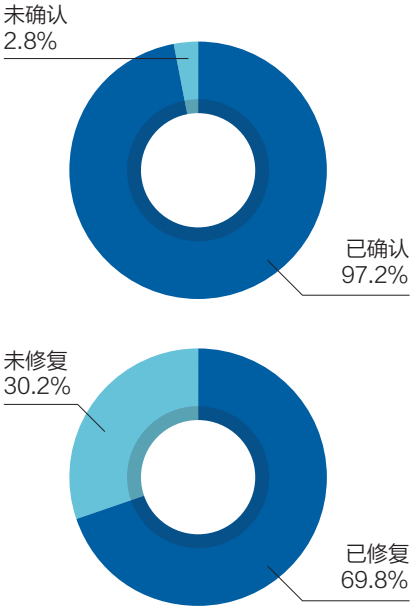
三、 复漏洞修复率达 69.8%

漏洞本身是无法完全避免的，被发现存在安全漏洞也并不可怕，关键是要进行及时的修复。检测显示，2022 年，补天平台收录漏洞的平均确认率约为 97.2%，未确认率为 2.8%。从已注册厂商确认的漏洞修复情况来看，2022 年，补天平台收录的漏洞修复率可达 69.8%。这表明，目前国内绝大多数网站都能及时确认安全漏洞，但修复情况还有待提高。

补天漏洞响应平台

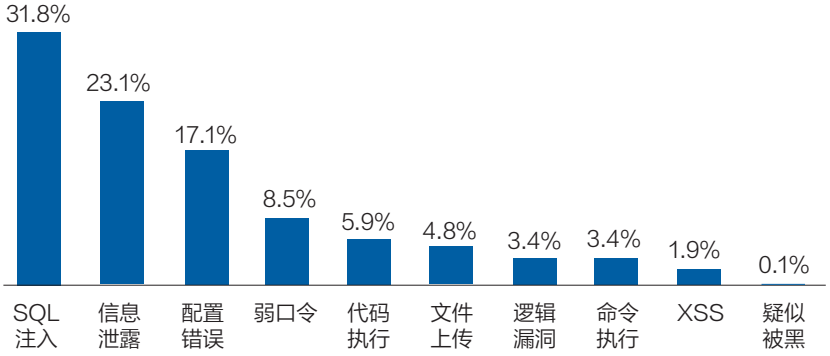
补天漏洞响应平台（https://www.butian.net），成立于 2013 年 3 月，是国内专注于漏洞响应的第三方平台。补天平台通过充分引导民间白帽力量，实现实时的、高效的漏洞报告与响应。成立 10 年来，补天平台已经成为全中国影响力最大的漏洞响应平台之一，同时也是最活跃的网络安全从业者交流平台之一。安

2022 年补天平台收录网站安全漏洞的确认与修复情况



（注册厂商修复情况）

2022 年补天平台收录网站安全漏洞类型分布



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

大事记

2023 中国互联网发展座谈会在京召开

2 月 17 日，2023 中国互联网发展座谈会暨中国互联网协会新春茶话会在京召开。中国工程院院士、中国互联网协会咨询委员会主任邬贺铨，工业和信息化部相关司局负责同志，中国电信邵广禄，百度李彦宏、滴滴程维、奇安信齐向东、搜狐张朝阳、腾讯马化腾、网易丁磊、新华网申江婴、小米雷军、亚信田溯宁、用友王文京等企业负责人参加会议。

与会嘉宾重点围绕数实融合、科技创新、网络安全、平台发展等方面进行交流，探讨互联网行业发展中面临的热点、难点问题，提出企业发展所面临的困惑、诉求和建议，解放思想，畅所欲言，真诚对话，共叙发展。

市通管局 工业和信息化部人事教育司赴奇安信开展主题党日活动

2 月 16 日，北京市通信管理局第一、五党支部和工业和信息化部人事教育司党支部赴奇安信集团联合开展主题党日活动，北京市通信管理局局长苏少林、工信部人事教育司副司长傅建奇及同行的支部党员，与奇安信集团就行业发展、党建和人才培养等工作进行了交流。奇安信集团党委书记、董事长齐向东、党委副书记、副总裁蒋虎参与了交流。

北京市通信管理局党组书记、局长苏少林充分肯定了奇安信以党建引领企业高速发展取得的成绩，特别是北京冬奥、冬残奥会网络安全保障服务“零事故”成就。并对奇安信提出两点建议：一是要政企协同、并肩作战，共同完成好今年的网络安全保障任务；二是继续加强体系化、实战化安全能力锻造，把“零事故”能力落实到更多场景。

吴云坤：构建四大关键能力 体系化治理软件供应链安全

2 月 16 日，在首届 ICT 软件供应链安全治理论坛上，奇安信集团总裁吴云坤表示，软件供应链系统生命周期的各个环节都可能存在供应链安全风险，需要用系统工程方法体系化、全局性治理。

吴云坤指出，软件供应链安全需要用系统工程方法体系化、全局性治理，从组织、流程制度、场景、能力四个层面出发，抓好四个关键点；在技术能力建设上，必须涵盖开发生产、集成交付、使用运行各阶段。

奇安信与中兴通讯签署战略合作协

2 月 13 日，中兴通讯股份有限公司与奇安信科技集团股份有限公司在奇安信安全中心签署战略合作协议。双方将在信息通信技术、网络安全等领域开展深入合作，共同推动技术创新和场景融合。

自 2020 年起，奇安信已与中兴通讯开始合作，在 5G 应用安全创新示范中心建设、内生安全远景白皮书、WSIS 项目奖等领域初见成果。此次战略合作协议的签署是中兴通讯与奇安信合作历程中的重要里程碑，标志着双方将开展更加全面和紧密的合作。

奇安信首批入选“人工智能安全可信护航计划”合作伙伴单位

在 2 月 13 日召开的北京人工智能产业创新发展大会上，奇安信作为首批合作伙伴单位，正式加入“人工智能安全可信护航计划”，（以下简称“护航计划”）。

据悉，“护航计划”将面向不同行业和地区设立“生态发展中心”。奇安信相关负责人表示，此次入选“护航计划”首批合作伙伴单位，是对奇安信在人工智能安全可信治理方面的充分认可。奇安信将积极履行责任，充分发挥自身技术和产品优势，推动人工智能安全可信技术落地应用，打造人工智能安全可信生态。

人工智能安全可信护航计划首批合作伙伴单位
（排名不分先后）

序号	单位名称
1	
2	
3	奇安信科技集团股份有限公司
4	
5	
6	
7	
8	
9	
10	

奇安信：正在训练公司专有的类 ChatGPT 安全大模型

近日，奇安信人工智能研究院负责人表示，公司正在基于 ChatGPT 相关技术和自身积累的海量安全知识和数据，训练奇安信专有的类 ChatGPT 安全大模型。未来将广泛应用于安全产品开发、威胁检测、漏洞挖掘、安全运营及自动化、攻防对抗、反病毒、威胁情报分析和运营、涉网犯罪分析等领域。

ChatGPT 是使用互联网数据及部分由标注人员人工编写的对话数据，利用人类反馈强化学习（RLHF）技术及自有的 GPT3.5 大模型进行训练而成的。奇安信团队对于相关的强化学习、大语言模型等技术，已经有长时间的实践，并取得了多项成果。

提效 50%！奇安信发布椒图服务器防勒索专版

1月30日，奇安信集团举办“椒图服务器安全管理系统－防勒索专版”产品发布会，推出针对勒索攻击防护的服务器端安全产品。

新产品针对勒索病毒的攻击链、行为特征提供多维度的防护方案，对勒索攻击的防护效果更好、针对性更强；并提供针对不同操作系统、业务环境的场景化配置模版，让产品能快速上线运行；同时，新版本还深度优化了系统资源配置，让管理中心对 CPU/ 内存等资源的配置要求降低 50%，支持的服务器数量增加 50%，让产品的部署门槛大幅度降低。

北京数据特区概念发酵 奇安信推出三方面举措

日前，北京市人民政府印发的《2023 年市政府工作报告重点任务清单》文件中提到，着力建设全球数字经济标杆

城市，落实北京数字经济促进条例，推动北京数据特区建设，开展数据基础制度先行示范。

齐向东透露，针对北京数据特区建设相关政策，奇安信推出了三方面举措。（1）聚焦应用场景，解决更多数据安全的新场景问题，为政企机构提供全方位的网络安全能力支持；（2）成立零信任专班，守好数据安全的第一道防线，“大概会接入十几条产品线，更好地为客户解决网络信任问题”；（3）奇安信将把研发平台上大量高水平的研发人员向产品线转移，进一步提升产品对研发平台的使用效率。

奇安信出席 G20 工商峰会议题工作组会议

1 月 24 日，由印度作为轮值主席国主办的二十国集团工商峰会（Business20）“数字化转型”议题工作组第一次会议在线上举行，作为 G20 峰会重要的配套活动，来自谷歌、微软、IBM、西门子、沃尔玛、波士顿咨询公司等 160 余名全球顶尖企业代表出席会议。奇安信集团作为中国唯一一家网络安全公司入选本届工作组并出席会议。

荣誉墙

奇安信实战化态势感知获 2022 数字经济优秀解决方案

近日，由国内知名科技媒体赛迪网和《数字经济》杂志主办的“2022 数字经济领航者峰会暨 2022 创新影响力年会”于线上召开。会议期间，主办方公布了“2022 数字经济竞争力创新成果”，奇安信实战化态势感知解决方案凭借强大的实战攻防能力和冬奥重保零事故的表现，荣获“2022 数字经济优秀解决方案”奖。

奇安信首次获得广东省科技进步一等奖

近日，2022 年广东省科学技术奖拟奖项目公示，奇安信集团与鹏城实验室等联合申报的“大规模网络仿真验证平台（鹏城靶场）关键技术与系统”项目通过评审，荣获 2022 年度广东省科技进步一等奖。

广东省科学技术奖是广东省在科技成果奖励方面的最高荣誉，是激励自主创新、激发人才创造活力的一项重要举措。这也是奇安信首次获得广东省科技进步一等奖。

奇安信云原生安全成果首获信通院权威认可

近日，云原生产业联盟（CNIA）年会上，六项奇安信云原生安全重磅成果亮相。奇安信作为《云原生应用保护平台（CNAPP）能力要求》标准核心参编单位受到联盟的认可与感谢，还一举拿下信通院云原生安全成熟度（云原生基础架构安全域 L4）、CNAPP 云原生应用保护平台（代码安全、镜像安全、云工作负载保护、网络微隔离、环境适配五大模块）这两大技术向权威评估认证，收获了云原生安全技术创新案


荣誉证书

奇安信网神信息技术（北京）股份有限公司：

贵单位『奇安信网神云安全运营管理系统』荣获：

2022年度云原生安全技术创新案例

特发此证，以资鼓励。

2023年01月

例这一重要荣誉。

这不仅是奇安信在云原生安全领域首次获得中国信通院的权威认可，更标志着奇安信对云安全的探索已经正式进入了云原生安全这一“新阶段”。

奇安信 Q-SASE 荣获 2022 云安全创新产品奖

近日，由 51CTO 主办的 IT 印象 · 激扬创新动能，掘金数字时代 | 2022 年第十七届中国企业年终评选榜单正式揭晓，奇安信网神边缘安全接入运营平台（Q-SASE）凭借专业成熟的运营服务和助力客户，以相对轻量的投入等众多优势，荣获“2022 云安全创新产品奖”。

作为国内首个在超大央企完整落地的 SASE 方案，奇安信 Q-SASE 2.0 以更简易的部署、更全面的服务、更广泛的合作以及更高效的运营，迎来了全方位的能力升级。作为奇安信在云安全领域的重要创新成果，Q-SASE 在央国企、运营商、教育等领域有众多客户。

奇安信斩获网络安全领域 2022 年度技术卓越双料大奖

近日，知名媒体 IT168 公布了“技术卓越奖”获奖名单。经过多方评审，奇安信网神特权账号管理系统 V6.0(PAM) 与奇安信网神终端安全管理系统 V8.0 在数据安全和信创安全领域表现突出，分获 2022 年度技术卓越奖和 2022 年度创新解决方案奖。

奇安信国密安全密码应用中间件获得商密产品二级认证

近日，奇安信网神国密安全密码应用中间件（Quick CSP，简称密码应用中间件）正式获得了国家密码管理局商用密码检测中心颁发的《商用密码产品认证证书》，并以密码应用组件的形式完成了与云安全管理平台（CSMP）的深度集成，可为云下、云上提供合规的密码基础设施建设，助力信息系统密评改造达标。

安

产业观察：八大重点领域将成新增长点

作者 | 陈华平

2022 年是国际形势格外动荡的一年，诸多因素影响网络安全产业，引入了不确定因素。随着疫情防控政策的调整和经济的复苏，2023 年开年多项重大利好政策密集发布，产业创新更加活跃，市场机会多点爆发，网安产业有望取得新的突破。

1. 宏观环境：网络安全产业受国际局势的影响叠加对冲，总体保持平稳发展

在宏观环境方面，国际局势的不稳定性对网络安全产业产生双方面的影响。一方面，安全形势不稳定对数字产业造成重大影响，使得可用于数字化乃至网络安全的资金捉襟见肘，相应的，产业投资也急速萎缩。另一方面，全球政治、经济、军事、民生全方位的不确定性使得安全需求急剧增加，各国建设网络安全防护能力的需求更加迫切。保卫网络空间国家主权、保护关键基础设施安全运行、保障数字化产业健康发展是网安行业的核心价值。

二十大的胜利召开为我国网安产业长期稳定发展指明了方向：安全与斗争成为时代强音，经济建设全局统筹下网络安全趋向集中化发展，中央网信机构调整体现统一部署、高效执行，合规体系快速细化、逐步落地。我国网络安全产业正在走上中国式现代化之路，创新方向更为多样化，符合我国产业特色的网络安全创新方向和创新企业大量出现，为产业持续高速增长注入新的动力。

2. 产业发展：短期波动不影响长期向好的基本面

在产业发展方面，2022 年全球经济普遍面临严重的下行风险，经济增速放缓程度高于预期。2022 年全球网络安全市场的预期增速也将降至 2020 年以来最低点，但是维持了高于 7% 的增长水平。中国网络安全市场 2022 年增速也有所放缓，但五年复合增长率仍超过 20%。Gartner 预计 2023 年后，全球网络安全产业将进入复苏期，到 2026 年市场规模将达到 2617.37 亿美元。2022 年网安头部企业市值受宏观环境影响较大，2023 年首个交易日相比 2022 年多数呈现下降，资本寒冬尚未过去，但营收依然实现较为稳定和快速的增长。

过去的五年里，中国网络安全市场复合增长率超过 20%，2021 年全球网络安全市场规模为 1354 亿美元，到 2025 年达到 2233 亿美元。其中，美国市场 1031 亿美元，中国市场 215 亿美元；美联邦政府一直保持高强度网络安全投入，将网络安全认定为数字化发展的“命门”；美国白宫公布的 2021 财年预算，其 IT 总预算为 922 亿美元，其中网络安全产业预算为 188 亿美元，占 IT 总预算的 20.4%，比 2020 财年高出 14 亿美元；根据 IDC 统计数据，我国网络安全投入占信息化的比重仅为 1.87%，比例不及美国水平的十分之一，低于全球 3.74% 的平均水平，增长潜力巨大。

3. 创新趋势：创新创业活跃，方向多样化，热点集中化

在细分赛道方面，2022 年网络安全产业创新活力依然强劲，方向更加多样化，热点趋于集中。国外优秀创企聚焦热门赛道、填补生态位。创新厂商聚焦热门创新赛道：主要集中在云安全、数据安全、身份安全和软件供应链安全领域，与头部企业热门领域基本一致；创新厂商着重核心技术与产品研发：与头部厂商形成良好互动，填补头部厂商生态体系，并有大量创新企业被头部厂商收购。

我国网安创企紧跟国际先进趋势，结合国情持续创新，热门赛道与国际市场基本相同，但更为多样化，千行百业的安全需求使我国网安行业创新方向更多、更加与业务相结合，网络攻防、安全运营、SOAR 等具实战化的技术与产品方向更受欢迎，数据安全一直是热点，符合我国行业对网络安全的需求。我国网安产业有足够的成长与创新空间，“十四五”网络安全市场空间预计超 6000 亿。热点赛道规模快速增长，成为网安产业发展的新动力。当前全球网安产业仍呈现碎片化态势，没有绝对强势的行业巨头，创业公司有机会脱颖而出。

4. 热点领域：八大重点领域将成为新增长点

2023 年关基市场、数字化产业市场、数据安全市场、云原生安全市场、合规市场、信创市场、国家安全市场和海外业务市场为八大热门市场：（1）关基市场：随着全球网络安全形势的恶化，对关键信息基础设施的攻防对抗成为热点。同时受法律政策驱动的影响，关基市场逐渐实现重点行业全覆盖，安全投入占比高，在网安整体市场的位置更加重要。（2）数字化产业市场：我国政企机构业务数字化转型驱动，覆盖速度很快，在网安整体市场占比快速提升接近与传统网安市场规模。（3）数据安全市场：数据安全监管要求和数字化业务数据保护驱动数据安全市场快速发展，2022 年市场规模已超百亿增速持续加快。（4）云原生安全市场：云原生安全是 2022 年国际网安市场热点，随着我国东数西算战略的部署，国家与地方政务云和企业云建设加快，数字化业务往云上迁移的步伐也在加快，云原生安全需求正在快速增长。（5）合规市场：国家战略与法律驱动，等保、关保、分保、密评等，在网安整体市场占比迅速提升。（6）信创市场：覆盖重要党政机构、重要行业和央企国企，当前占比较低但市场空间广阔。（7）国家安全市场：保卫国家安全和网络国防能力建设，未来具有很大的市场空间。（8）海外业务市场：国家扩大国际影响力，以及海外利益保护的要求，带来巨大的市场空间。

5. 发展前景：2023 年开年利好政策密集发布，网安产业迎来好开局

随着疫情防控政策的调整和经济的复苏，2023 年开年多项重大利好政策密集发布，网安产业有望取得新的突破。

全国一体化政务大数据体系建设启动数据安全体系化建设时代，带来数据治理与数据安全业务机遇，包括数据资源盘点及目录系统建设，数据质量咨询服务及系统建设，数据管理、数据安全治理、数据安全保护系统建设及合规服务。“数据二十条”推动数据要素活起来、动起来、用起来，从数据产权、流通交易、收益分配、安全治理四个方面初步搭建我国数据基础制度体系，提出二十条政策举措。国资委央企新一轮改革统筹发展和安全、防范化解重大风险。2023 年组织开展新一轮国企改革深化提升行动，更好地统筹发展和安全，有效地防范化解重大风险，压实企业主体责任，增强风险处置精准性、有效性，切实提升企业安全生产水平。证券行业网络和信息安全三年提升计划启动提出六大方面、33 项任务清单。持续提升科技治理水平，建立科学合理的科技投入机制，增强信息系统架构规划掌控能力，强化系统研发测试管理能力，夯实系统运行保障能力，健全网络和信息安全防护体系。

总结：2023 年预期网络安全产业将进入新一轮高速增长阶段。产业将更加注重体系化创新，以保障国家重大网络安全项目和工程的建设为主要任务。国资和资本市场将进一步加大网络安全投入，持续助推网安产业发展。网络安全与产业应用的深度融合发展将成为带动未来网络安全产业的关键增长点。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。

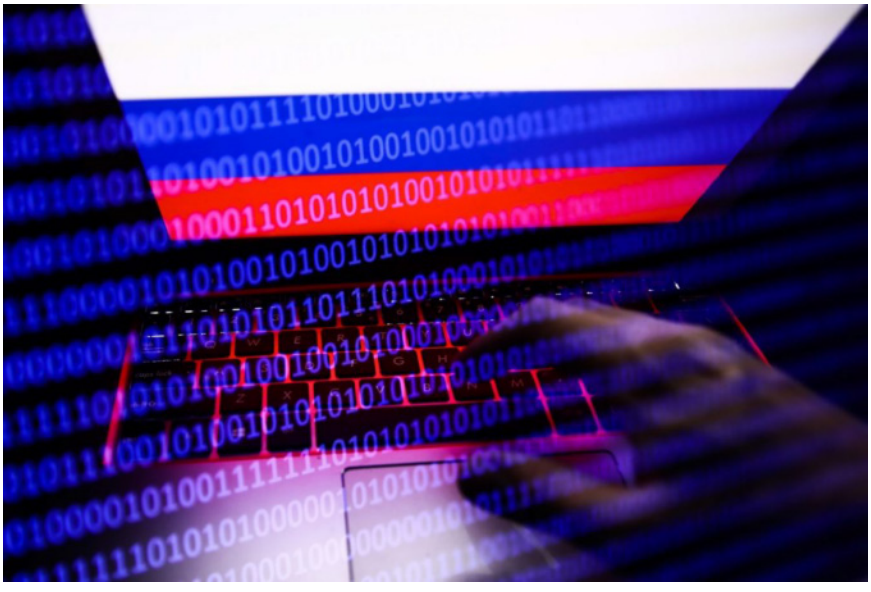
俄罗斯网络战的经验教训

作者 | 赵慧杰

乌克兰国家特殊通信和信息保护局局长尤里·希霍尔 1 月 31 日在美国大西洋理事会网站发文提出，乌克兰在应对俄罗斯网络威胁方面的经验既可为国际社会提供宝贵的经验教训，还启示出未来战争将日益结合常规手段和网络行动同时开展。

文章总结了乌克兰从俄罗斯网络战中吸取的经验教训：一是俄罗斯常规行动和网络行动之间存在明显联系，网络攻击经常先于或伴随着更常规的军事行动，网络战线将在未来战争中发挥重要作用；二是网络攻击处于“军事灰色地带”，避免了常规手段引发直接军事反应的风险，这使得网络攻击成为有吸引力的选项；三是数字环境的无国界性使得网络攻击的影响已远超实际的边界，随着网络战能力的不断扩展，未来无法避免将出现类似场景；四是网络攻击较传统军事行动需要更少的人力资源；五是网络攻击需要时间和知识来准备，较常规军事行动更难展开。

俄罗斯对乌克兰的全面入侵已近一年时间，但攻击实际更早，俄罗斯坦克部队 2022 年 2 月 24 日越过边界一个多月前就已开始。2022 年 1 月中旬，俄罗斯发动了一场针对 20 多个乌克兰政府机构的大规模网络攻击，旨在削弱乌克兰抵御莫斯科迫在眉睫的军事攻击的能力。



1 月 14 日的攻击未能对乌克兰的数字基础设施造成严重打击，但这表明网络战线将在未来战争中发挥重要作用。一年过去了，再也无法将网络攻击与俄罗斯侵略的其他方面区分开来。乌克兰官员目前正在寻求说服位于海牙的国际刑事法院（ICC），调查俄罗斯的网络攻击是否构成战争罪。

对过去一年俄罗斯在乌克兰使用的网络战战术的分析表明，常规行动和网络行动之间存在明显联系。乌克兰在应对这些网络威胁方面的经验可以为国际社会提供宝贵的经验教训，同时让我们得以一窥未来——战争将既通过常规手段进行，也将越来越多地在无边界的网络空间领域进行。

2022 年 1 月的俄罗斯网络攻击并非史无前例。相反，自 2014 年春季俄罗斯侵略克里米亚以来，乌克兰

一直是遭攻击目标。一年后，乌克兰成为世界上第一次针对国家能源系统的重大网络攻击发生地。2017 年夏天，乌克兰遭受了许多评论人员认为是历史上最大规模的网络攻击。这些引人注目的事件伴随着源源不断的、规模较小但意义重大的攻击。

在俄罗斯发动全面入侵后，网络攻击经常先于或伴随着更常规的军事行动。例如，在俄罗斯对乌克兰民用基础设施发动空袭前，乌克兰能源公司经历了数月来不断升级的网络攻击。

这些策略，对于俄罗斯在其不宣而战的战争中是一个具有吸引力的选择。更常规的侵略行为可能会激起压倒性的反应，但网络攻击存在于军事灰色地带，这使得其成为克里姆林宫的一个方便选择，因为其试图在欧洲和北美造成最大的混乱，而不冒直接军事反应的风险。俄罗斯可能还没有准备好对西方使用坦克和导弹，但莫斯科对部署在乌克兰磨练出来的网络战战术不会有太多保留。

除扰乱和破坏政府机构及重要基础设施外，俄罗斯对乌克兰的网络攻击还试图操纵公众舆论并通过受感染的电子邮件账户传播恶意软件。乌克兰当局发现，与公众协调努力并与广泛的利益相关者共享信息，对于及时反击攻击至关重要。

针对乌克兰的网络攻击的影响已经远远超出了乌克兰的边界。在俄罗斯入侵的初始阶段，乌克兰武装部队使用的卫星通信系统遭到一次攻击，对包括个人和公司在内的整个欧盟数以千计的用户造成了严重破坏。鉴于数字环境的无国界性质，随着网络战能力的不断扩展，类似的场景在所难免。

从俄罗斯的角度来看，网络战特别有吸引力，因为它比传统军事行动需要更少的人力资源。虽然莫斯科正在努力寻找足够的人员和军事装备来弥补入侵第一年在乌克兰遭受的毁灭性损失，但克里姆林宫应该不费吹灰之力就能找到足够多的技术人才来对乌克兰以外的许多国家发动网络攻势。

俄罗斯可以从一大批潜在的新兵中吸取力量，包括受克里姆林宫宣传的激励的志愿者，上述宣传将入侵乌克兰定位为与西方进行文明斗争的一部分。此类网络已经对西方目标开展了众多单独攻击。

与此同时，乌克兰过去一年的经验表明，网络攻击需要时间和知识来准备。这有助于解释为什么在 2022 年春季，俄罗斯的入侵战略最初失败后，高复杂性的网络攻势减少了。俄罗斯根本没想到乌克兰能经受住第一波网络攻击，也没有足够的计划来应对这种可能发生的情况。

乌克兰已经对俄罗斯的网络战进行了广泛的研究。由于这种强大的经验，我们对自己抵御进一步攻击的能力越来越有信心。为了最大限度地发挥防御能力，整个西方世界必须共同努力。必须怀着紧迫感来完成这项工作。为了寻找获得主动权的方法，可能在网络战线上尝试大胆的新攻势。从更长的周期来看，出现网络战争也只是时间问题。

全球亟待调整军事学说，以应对基于网络空间的威胁。网络攻击必须以与常规军事侵略相同的方式对待，并且应该受到同样的毫不妥协的回应。还必须努力防止相关政权获得随后可能被用来对付西方的技术。

俄罗斯入侵乌克兰，在许多方面是世界上第一次网络战争，但不会是最后一次。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。

威胁狩猎：基于假设的安全防卫能力

作者 | 张晓兵

一、威胁狩猎基本模式

威胁狩猎最重要的是要从一个“假设（hypothesis）”开始，不断搜查这些潜在的风险，跟踪网络中的可疑行为的一个迭代过程，建立这种假设有三种模式：

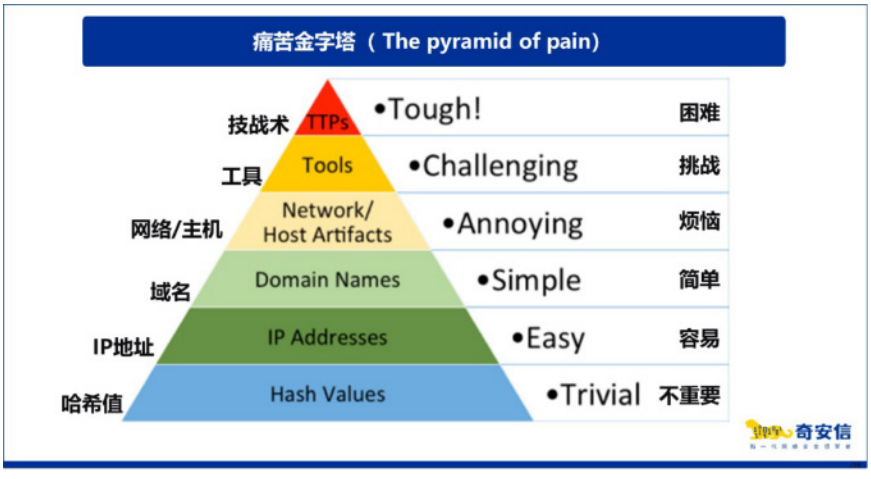
分析驱动（Analytics-Driven）模式是利用机器学习（ML）、用户实体行为分析（UEBA）等开始威胁狩猎的假设。

情境意识驱动（Situational-Awareness Driven）模式是利用 MITRE 公司的皇冠宝石分析法（Crown Jewels Analysis，CJA）和组织风险评估、公司或员工层面的趋势等开始威胁狩猎的假设。而“皇冠宝石”，指的是关键任务的网络资产（mission-critical cyber assets）。

威胁情报驱动（Intelligence-Driven）模式是利用威胁情报报告、威胁情报反馈、恶意软件分析、漏洞扫描等开始威胁狩猎的假设。

威胁狩猎最大的价值在于：能够确认环境中存在敌手，能够提供黑客没有入侵成功的证明，能够检验安全防护体系的有效性，能够发现未知的基础设施、应用程序和数据存储，能够发现组织新兴技术中存在的问题。

因此，当组织没有能力大规模组织红蓝对抗的时候，可以构建一个威胁狩猎体系是非常经济的做法。



图：痛苦金字塔模型

二、威胁狩猎安全模型

痛苦金字塔（Pyramid of Pain）是威胁狩猎和威胁情报领域里一个重要而优雅的概念。金字塔解决了一个问题：即攻击者改变其攻击的某些特征到底有多困难？同时它也显示了组织找到这些特征到底有多困难。

痛苦金字塔将威胁狩猎与威胁情报（Threat intelligence）联系起来。威胁情报提供了关于金字塔各层攻击者的相关信息。TTP（Tactics, Techniques, and Procedures）即攻击策略、技术和处理流程，是攻击者使用的攻击方法，在威胁狩猎的搜查中最为重要。

威胁狩猎与威胁情报的关系也颇为密切，如果没有威胁情报的基本知识，威胁狩猎中的一些概念很难解释。情报是猎杀的起点，情报是猎杀的背景和动力，猎杀以产生威胁情报，这三点对于威胁狩猎来说，尤为重要。

猎杀成熟度模型（Hunting Maturity Model）是度量组织威胁狩猎能力的一个评价模型，它着重于威胁狩猎的三个重要概念：组织需要注意他们收集的数据的质量、用于访问和分析数据的工具，以及进行猎杀的分析人员的技能。

猎杀成熟度模型提出了一个组织的猎杀能力的五个不同类别：起步 (Initial)、基础 (Minimal)、流程化 (Procedural)、创新 (Innovative) 和领先 (Leading)，如右图所示。

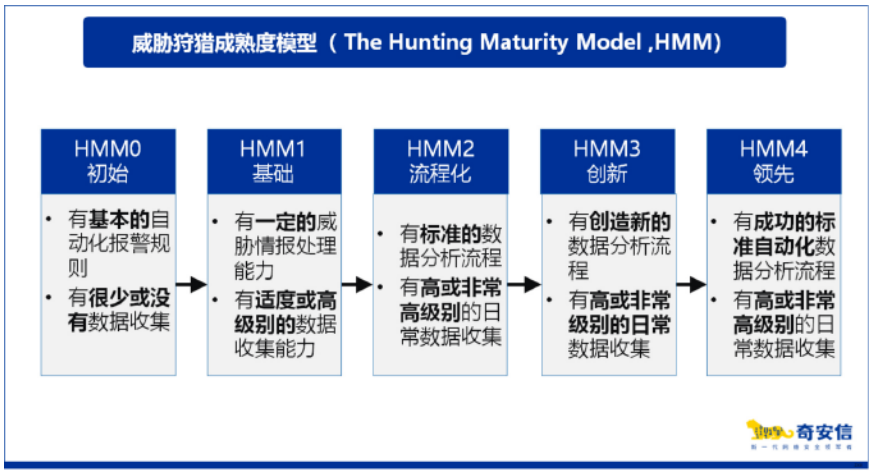
从这个模型中得到的主要启示是，威胁狩猎不是一个单一的状态，而是一个处理过程。组织应该尝试最大限度地收集数据，有效地分析数据，然后适当地利用他们的分析人员。

网络安全滑动标尺模型（Sliding Scale of Cyber Security）在许多方面与猎杀成熟度模型相似，但它定义了组织为了促进网络安全而进行投资的五个阶段，是组织网络安全建设成熟度的度量模型。

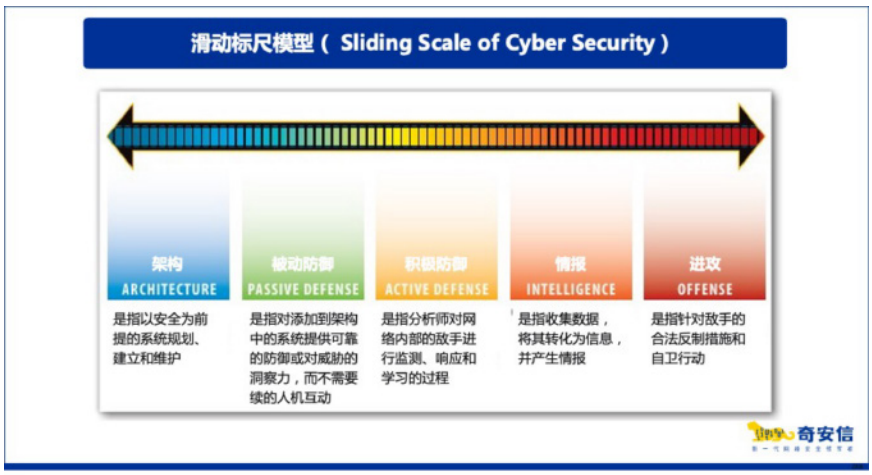
威胁狩猎包含在积极防御类别中，并整合了一些最好的情报产品。

积极网络防御周期（The Active Cyber Defense Cycle）是一个通过生成和消耗情报来应对威胁的一个持续过程。它是将网络杀伤链和入侵分析的钻石模型这两种模式产生的威胁情报，放入积极防御的上下文环境中的过程模型，也是威胁狩猎的主要支撑模型。它将网络杀伤链（Cyber Kill Chain）和入侵分析的钻石模型（Diamond Model of Intrusion Analysis）整合在一起，能够有助于识别入侵，并超越单一入侵的概念，转向识别和了解敌手的活动。

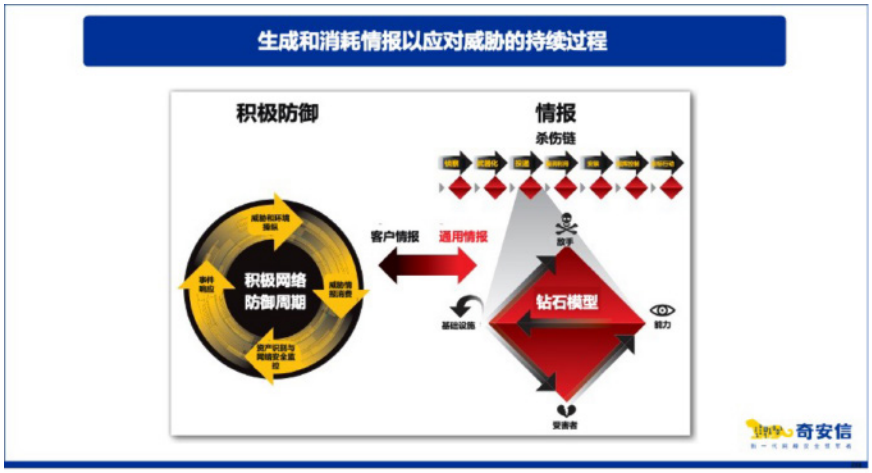
TaHiTI 是一种整合了威胁情报的威胁狩猎过程模型，分为三个阶段：启动、猎杀和定案。该过程总共有 6



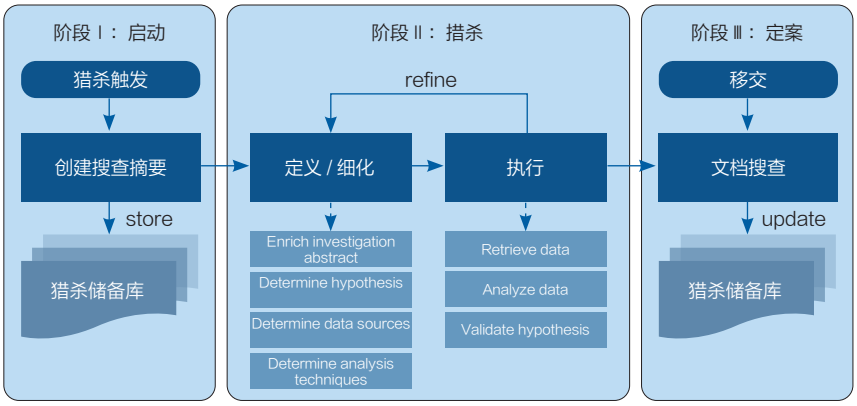
图：猎杀成熟度模型



图：网络安全的滑动标尺模型



TaHiTI 过程 (TaHiTI process overview)



图：TaHiTI 威胁狩猎过程

个步骤，如上图所示。

启动阶段是处理威胁狩猎输入的地方。首先有一个初始触发器（Trigger）来启动猎杀过程，这个过程被称为“猎杀触发”。接下来，触发器被转换为“创建搜查摘要”，并存储在猎杀储备库(Hunting Backlog)中。

威胁狩猎的第二阶段是进行实际搜查的地方，这个阶段有两个活动。狩猎阶段的第一个活动被称为“定义 / 细化（define/refine）”。第二个活动被称为“执行（execute）”，是狩猎的实际进行活动。

威胁狩猎的第三阶段是威胁狩猎小组必须处理执行步骤的结果，并记录搜查结果。

三、威胁狩猎度量标准

度量对于确定威胁狩猎过程的效率和有效性及显示其对组织的附加价值非常重要。有两种基本类型的指标：定量（数字）和定性（价值）。其中有发现的停留时间（Dwell Time）、事件响应数量、安全监控用例数量、由于威胁狩猎新产生的威胁情报、安全建议、漏洞数量等六个指标。

威胁狩猎效果的度量有十大指标：

- 按严重程度划分的事件数量
- 按严重程度划分的被攻击主机的数量
- 发现的任何事件的停留时间
- 填补检测空白的数量
- 确定并纠正的日志差距
- 发现漏洞数量
- 发现并纠正不安全的做法
- 已过渡到新的分析的猎物数量
- 过渡性狩猎的假流程率
- 获得的任何新的可见性

四、威胁狩猎组织建设

开展威胁狩猎活动需要考虑三点：人员、流程和技术。其中，对于人员的规划，需要考虑招聘、培训及服务外包三种方式。整个威胁狩猎的团队组织架构如下：

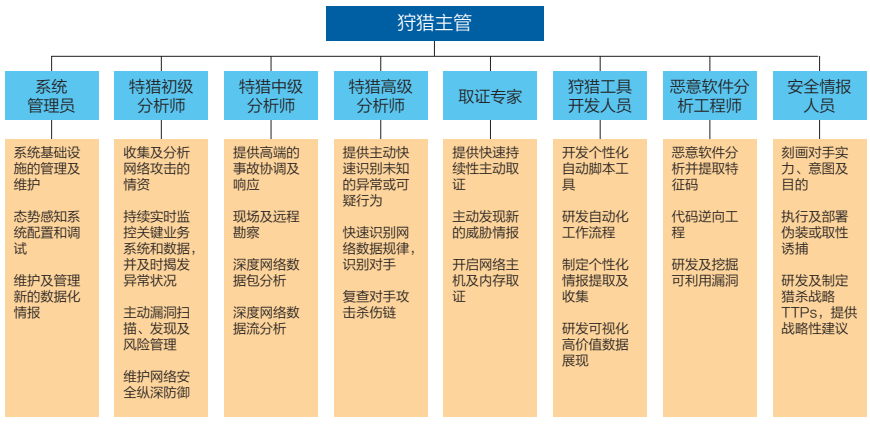
威胁狩猎团队的人员组织，需要 8 种角色，有些角色可以合并为一个人，其中包括：系统管理员、狩猎初级分析师、狩猎中级分析师、狩猎高级分析师、取证专家、狩猎工具开发人员、恶意软件分析工程师、安全情报人员等。

五、威胁狩猎参考架构

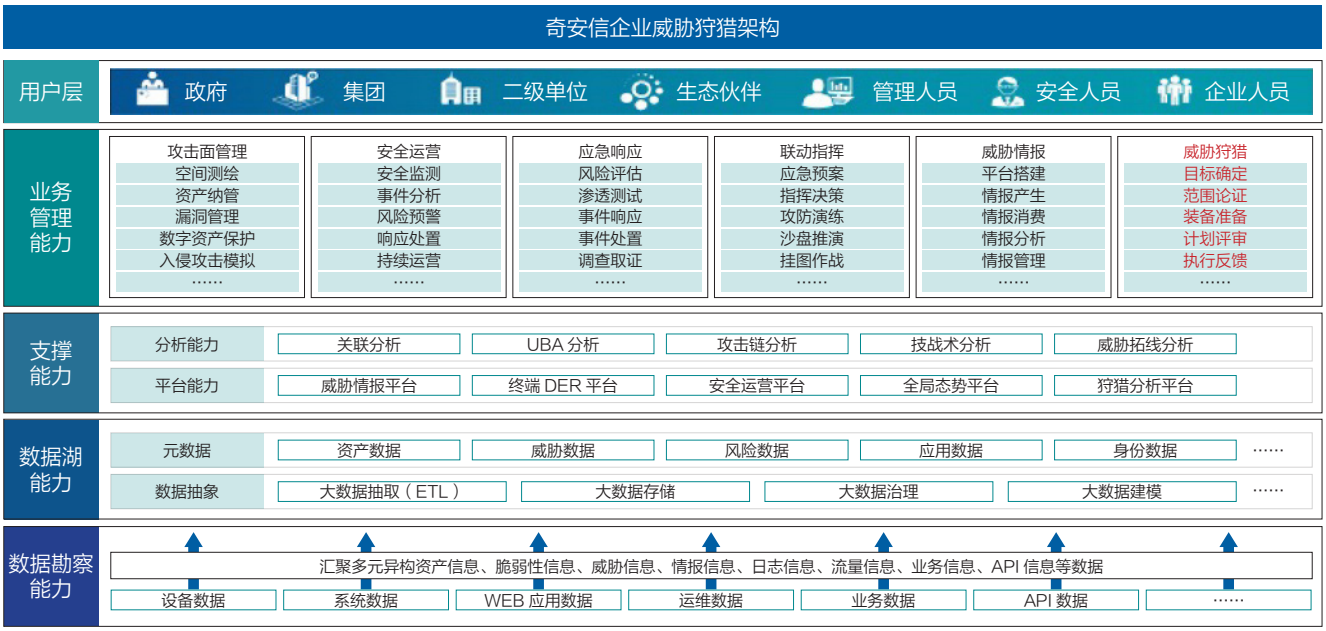
一个威胁狩猎体系的构建，离不开一个好的建设架构，如果只是散点式的建设，最终会让该项工作流于形式，无法真正发挥价值，从而让该项目负责人承受更多的非议。整个威胁狩猎的参考架构如下图所示。

威胁狩猎体系需要数据、工具、人才、制度和流程的配合，因此整个架构分成数据探查能力构建、数据湖能力构建、支撑能力构建、业务管理

威胁狩猎的组织架构



图：威胁狩猎的组织架构



图：威胁狩猎参考架构

能力构建四大部分。

数据探查能力构建指的是原始数据的探查能力；数据湖是一个安全大数据的基础设施； 支撑能力本身分为平台能力支撑和分析能力支撑两大方向，这里组织需要检验自身是否有足够的平台，而且这些平台是否有足够的分析能力；业务管理能力指的是站在组织管理的维度上，对“安全”这个业务如何进行有效管理。

六、威胁狩猎发展趋势

威胁狩猎既是一种安全的积极防御体系，又是一种利用威胁情报进行反击的安全防卫体系。因此我们必须了解入侵发展趋势与敌手（Adversary）的发展趋势，最终才能看到威胁狩猎本身的发展趋势如何。

入侵行为发展趋势主要以互动式入侵（Interactive Intrusion）、电子犯罪（eCrime）、针对性攻击（Targeted）、黑客活动（Hacktivist）为主。

敌手发展趋势主要以无文件攻击为主，这主要跟有效凭证被大量滥用、新漏洞的披露速度提升有关。

另外可以看到，云计算已经成为知识产权盗窃、数据勒索、赎金软件或简单破坏的新舞台，因此积极建设其云狩猎能力，将是未来威胁狩猎发展的一个重要趋势。

威胁已来，安全体系需要威胁狩猎。安

作者简介

张晓兵

奇安信集团 解决方案中心 / 科研管理部 高级总监 / 研究员

病毒分析师、系统程序员、信息安全领域资深专家，复杂系统解决方案专家。中国计算机学会（CCF） 计算机安全专业委员会会员；慧智库资深卓越专家；虎符名师堂特聘专家。是归一化细粒度反病毒引擎、云安全与大数据安全的倡导者。出版有《病毒杀除不求人》《由 0 晋身 200% 防毒高手》《由 0 晋身 200% 系统高手》《内生安全》等安全著作，在多家媒体发表了大量的安全技术文章，并在多家电视台向广大用户积极传播安全理念，被称为“网络安全的播种者”。

重新定义 SOAR

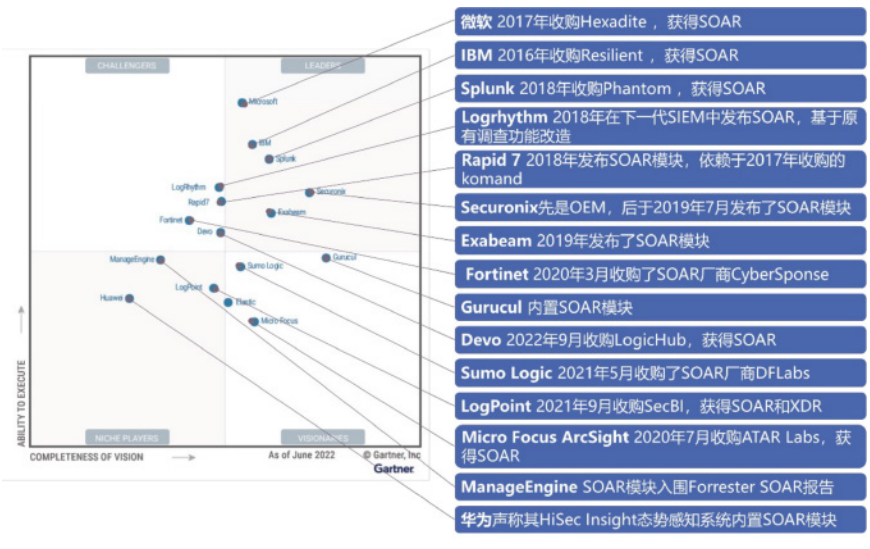
作者 | 叶蓬

SOAR 的全称是 Security Orchestration, Automation and Response，意即安全编排自动化与响应。从 Gartner 最早提出 SOAR 这个概念到现在已经过去了 7 年，期间伴随着国内外 SOAR 领域的不断实践，SOAR 的概念持续不断地在演变中。特别是中国网络安全市场因其技术和应用发展的特殊性，逐步形成了对 SOAR 的特有认知，并促成对中国 SOAR 市场的重新定义。

如果用一句话来概述 SOAR 的特性，可以解读为：人员是根本、协作是使命、流程是基础、编排是核心、自动是手段、响应是场景、提效是目标。

SOAR 发展方兴未艾，新应用场景不断涌现

近几年，在国际上，我们看到很多 SIEM 厂商纷纷加码 SOAR，或者通过收购，或者通过自研，将 SIEM 的功能扩展到 SOAR 领域，有的将 SOAR 作为 SIEM 的一个功能，有的将 SOAR 与其 SIEM 甚至 TIP 等系统打包成安全运营套件。笔者做过分析，几乎所有 2022 年 Gartner SIEM 魔力象限中的厂商都具备 SOAR 功能或产品，纷纷发起对独立 SOAR 厂商的收购。



微软 2017年收购Hexadite，获得SOAR

IBM 2016年收购Resilient，获得SOAR

Splunk 2018年收购Phantom，获得SOAR

Logrhythm 2018年在下一代SIEM中发布SOAR，基于原有调查功能改造

Rapid 7 2018年发布SOAR模块，依赖于2017年收购的komand

Securonix先是OEM，后于2019年7月发布了SOAR模块

Exabeam 2019年发布了SOAR模块

Fortinet 2020年3月收购了SOAR厂商CyberSponse

Gurucul 内置SOAR模块

Devo 2022年9月收购LogicHub，获得SOAR

Sumo Logic 2021年5月收购了SOAR厂商DFLabs

LogPoint 2021年9月收购SecBI，获得SOAR和XDR

Micro Focus ArcSight 2020年7月收购ATAR Labs，获得SOAR

ManageEngine SOAR模块入围Forrester SOAR报告

华为声称其HiSec Insight态势感知系统内置SOAR模块

但无论如何，大部分 SOAR 提供商都同时是 SIEM/ 安管平台 / 态势感知平台提供商，并且多是同一个团队在后面进行研发。

因此，很多人可能不禁会问：是否未来 SOAR 将成为 SIEM/ 安管平台的一个部分？独立 SOAR 厂商 / 产品是否会消亡？其实，如果有心的话，可以看到这几年独立的 SOAR 厂商依然像雨后春笋般涌现。并且，这些新兴厂商开发了很多应用场景，已经超越了 SIEM/ 安管平台所能覆盖的范畴。

笔者认为，在 3 到 5 年内，SOAR 会不断与 SIEM/ 安管平台进行多种形态的整合，甚至还会跟其他多种产品（譬如 XDR、数据安全平台、零信任平台）进行整合，发展为“嵌入式 SOAR”，但独立的 SOAR 会依然存在，能够中立地跟第三方系统（如 SIEM/ 安管平台、数据安全平台、零信任平台）集成，发展为“开放式 SOAR”，并且会与 SIEM/ 安管平台越来越不相同。但无论如何，SIEM/ 安管平台和 SOAR 都是安全运营中心的组成部分，这一点不会变。

正如 Gartner SOAR 报告所言，SOAR 与 SIEM 是一个交集的关系，二者的交集在于威胁检测与事件响应。也就是说，SOAR 的应用场景除了威胁检测与响应，还有其他超越 SIEM 的应用场景。

可以说，只要是安全运营工作，都可以通过编排和剧本去实现（部分）自动化。譬如员工入职后的各系统开通，员工离职时的各系统账号清除，堡垒机账号梳理，零信任中的持续行为评估，攻防演练，安全中台的能力编排，等等。

从这个角度来说，在把 SOAR 局限于安全事件响应显然是小看 SOAR 了。对 SOAR 而言，SOA 的重要性越来越凸显。所以笔者一直强调，响应是 SOAR 的一个场景，尽管是最重要的场景，但也仅仅是一种场景。编排才是 SOAR 的核心，编排让 SOAR 具备了更多的可能性。

国内 SOAR 独特性显现

目前，中国客户（尤其是头部客户）对 SOAR 正在迅速从旁观者向参与者转变。越来越多的中国用户开始落地 SOAR，越来越多的中国厂商发布 SOAR 产品或者模块。近两年，赛迪咨询都对用户使用 SOAR 的情况和意愿进行过调研，SOAR 已经成为安全运营建设时考察的关键能力之一。而根据 Gartner 对中国的安全运营市场进行的调研，以及数世咨询、安全牛、嘶吼等发布的安全全景图，都能发现，提供 SOAR 能力的厂商大幅增加。

根据笔者对中国市场的观察及深入实践，发现中国 SOAR 市场逐步呈现出一些不同于国际市场的特点：

1）SOAR 在国内落地的时候，基本上将 TIP（威胁情报平台）作为一个外部系统进行集成而非作为一个内在的功能集合。国内客户基本上都将 TIP 看作一个独立的基础性、支撑性产品 / 平台，为 SIEM、安管平台、态势感知、SOAR，甚至安全设备等提供情报赋能。因而，客户在考虑威胁情报的时候，通常不会咨询 SOAR 产品厂商，甚至都不会咨询安管平台 / 态势感知平台的提供商。这并不是说 SOAR 与 TIP 之间没有关系。一方面，SOAR 在进行告警和安全事件调查的时候需要利用威胁情报进行辅助研判，并可以将这个研判过程编排化、自动化；另一方面，也是往往容易忽略掉的，在于 SOAR、尤其是编排自动化有助于提升 TIP 自身的运营水平，譬如内生情报的产生。可以说，目前国内的 TIP 的运营化水平都还比较初级。因此，基于国内的现状，国内的 SOAR 平台更多是与 TIP 进行松耦合的解决方案集成，而非将 TIP 作为 SOAR 的一个 / 组模块功能。此外，Gartner 将 TIP 植入 SOAR 还有一个原因，就是美国政府（包括民事和军事）在实践 SOAR 的时候，首先从威胁情报的共享和基于情报的响应这个应用场景开始的。

2）中国的平均安全运营水平低于国外（尤其是美国），在落地 SOAR 的时候有些理念存在不同。一般来说，客户要想使用 SOAR，首先应该有相匹配的安全运营成熟度，尤其是存在固化的安全运营流程，譬如有 SOP（标准操作规程），有相对固定的运营人员。一旦客户具备前述条件，对 SOAR的需求就是自然而然的一件事，使用 SOAR 的过程就是将现有的流程转移到 SOAR 中，形成剧本，提升现有运营人员的工作效率。Gartner 反复强调这点，并建议低运营水平的客户去寻求 MSS 的帮助，购买效果导向的服务而非 SOAR 产品。笔者认为，上述观点没有毛病。但国内的客户就应该先闷头提升运营流程和人员，再考虑 SOAR 吗？或者说，SOAR 的应用能否为部分客户的运营水平提升提供帮助？其实，这个问题的答案就跟我们经常说的“三同步”是相通的。对于那些注定需要自建安全运营能力的客户而言，如果他们已经有了运营团队（尽管可能很小），有了宏观的安全流程并且运营团队实际在开展运营工作（尽管可能没有 SOP），此时距离使用 SOAR 所需的成熟度还有一些差距，但这时候使用 SOAR 得当的话，是有助于反向提升运营水平的。譬如，在对安全告警进行响应的时候，尽管没有现成的 SOP，但有基本的流程（尤其是岗位和部门间职责界定相对清晰），就可以借鉴 SOAR 厂商提供的剧本模板和样例，借鉴业界的最佳实践，结合自身的需要，创建或者完善某个具体的事件响应流程。或者，还可以不从剧本入手，而从使用应用（App）、快速调用 App 的动作入手，降低工具切换的时间成本，先稍

微缓解告警处理疲劳；然后再从实战中总结这些动作 / 操作的规律和经验，提取剧本，从而降低后续同类工作的时间成本。再者，可以先通过工具化的 SOAR 将一些简单的重复性工作自动化，形成几个经典实战化应用场景，真正提升运营团队的工作效率，拿出看得见的效果和度量指标，进而说服管理层提升对安全运营工作的重视程度，加大流程建设、队伍建设、自动化运营建设的投入。

重新给 SOAR 一个中国定义

对国内外 SOAR 最新发展和应用动态的分析，笔者提出一个全新的 SOAR 定义：

安全编排自动化与响应（SOAR）系统是一系列提升安全运营效率的技术集合。它在安全运营流程和规程的指引下，将与安全运营相关的第三方工具通过编排整合到一起，以自动化和高交互的形式辅助安全运营人员开展安全运营工作，并内建对安全事件的采集、分诊与响应。

这个定义的核心是“提升安全运营效率”，这是 SOAR 的目标，而安全运营流程和规程的牵引体现了 SOAR 的基础，编排是 SOAR 的核心和抓手，自动化和交互式响应（譬如基于 Chatbot 的作战室）则是多样化的运营辅助手段，而整个过程都围绕安全运营人员展开，体现了人的根本地位。最后，对安全事件的采集、分诊与响应是 SOAR 内置的一个应用场景。

在我国通信行业标准《安全编排自动化响应系统评价方法》的征求意见稿中，笔者也积极参与，阐述观点，得到了标准组各厂商成员的认可，将 SOAR 定义为：

SOAR 是一系列技术的合集，它能够帮助企业和组织收集安全运营团队监控到的各种信息（包括各种安全系统产生的告警、单点资产的状态信息、各类产品的操作日志信息等），基于这些信息进行事件分析与告警分诊，并将运营过程中涉及的的第三方工具、能力通过编排形式进行集成，从而显著地为常见安全运营工作带来效率提升，如威胁检测、安全事件响应、威胁情报调查等。

总结

SOAR 以安全编排和自动化为核心，以安全事件响应为必备应用场景，充分利用威胁情报，辅助安全运营人员高效开展各项安全运营工作。SOAR 在现有以数据为中心的安全运营框架基础之上，增加了一个以流程为中心的编排层，进一步完善和丰富了安全运营的体系，将人、流程、技术和工具整合到一起，提升了安全运营的实战化水平。

未来，随着超自动化（hyperautomation）技术不断应用到安全领域，以及诸如 ChatGPT 等基于 AI 的 Chatbot 技术的成熟，SOAR 除了在自动化运营方面继续上台阶，还能提供更智能的交互式运营手段，SOAR 的应用场景将更为广阔。

SOAR 引领的安全运营新时代已经到来。安

关于作者

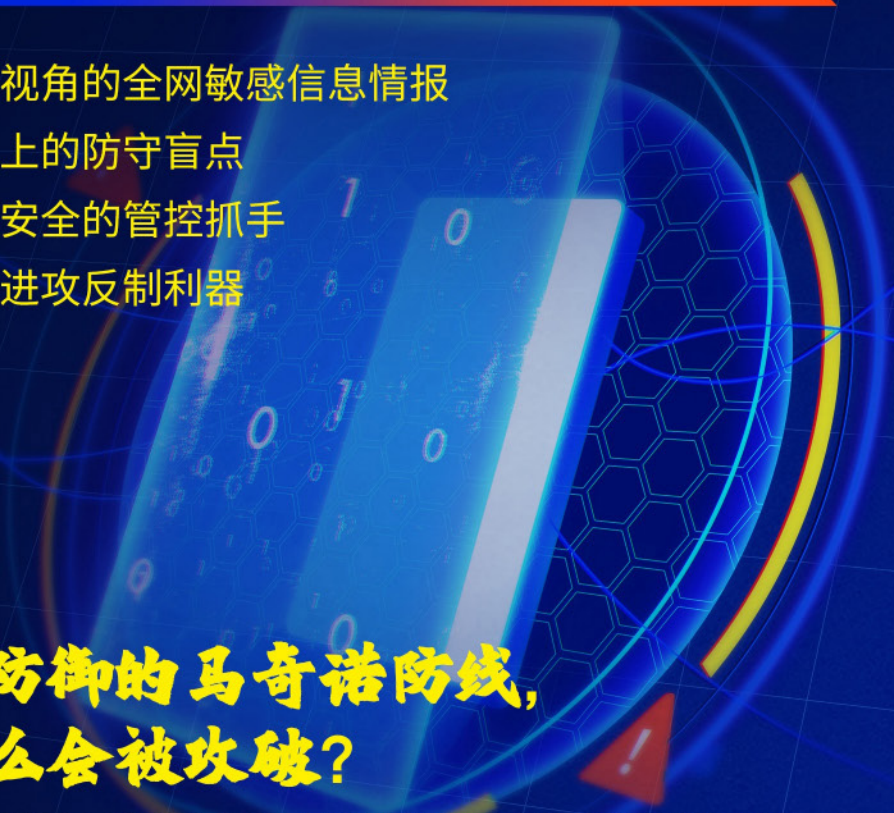
叶蓬

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。

奇安信

敏感信息泄露情报服务

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



纵深防御的马奇诺防线，为什么会被攻破？

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

服务定位 SERVICE POSITIONING

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

奇安信安服团队

奇安信蝉联“中国网安产业竞争力50强”第一名

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


奇安信科技集团股份有限公司

CCIA 50强

2022年中国网安产业竞争力50强

编号：CCIA-2022JZL-01

中国网络安全产业联盟
2022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	天融信科技集团股份有限公司
5	华为技术有限公司
6	绿盟科技集团股份有限公司
7	腾讯云计算（北京）有限责任公司
8	阿里云计算有限公司
9	新华三技术有限公司
10	杭州安恒信息技术股份有限公司
11	360政企安全集团
12	亚信安全科技股份有限公司
13	成都卫士通信息产业股份有限公司
14	杭州迪普科技股份有限公司
15	山石网科通信技术股份有限公司