面向攻击面收敛的网络安全风险治理研究

沈　萍
（上海市教育委员会财务与资产管理事务中心，上海　200003）

摘　要：针对组织网络攻击面动态变化和防御者视角不能有效识别黑客攻击手段的特点，基于多维攻击者视角构建以“资产管理、攻击面识别与风险值计算、攻击面修复与闭环验证、网络流量采集与实时监控分析”为流程的攻击面收敛管理体系，有效实现“安全左移”。对已知资产、影子资产等计入纳管范围，融合风险量化分级与安全漏洞闭环验证，开启持续监控以实时感知资产异动并采取措施。实践结果证明，引入网络流量与威胁情报的协同分析后，威胁情报命中安全事件数量逐步下降；网址及端口非必要暴露面得到有效监控与响应，平均暴露时间显著缩短，从数天减少至1 h以内。攻击面管理技术有效缓解了攻防不对称性问题，提升了组织在网络攻击面的全局可见性与风险控制效率。

关键词：攻击面收敛；资产管理；风险值计算；闭环验证
中图分类号：TP393　　**文献标志码**：A　　**DOI**：10.19358/j.issn.2097－1788.2026.03.003

中文引用格式：沈萍. 面向攻击面收敛的网络安全风险治理研究［J］. 网络安全与数据治理，2026，45(3)：17－23.
英文引用格式：Shen Ping. Research on network security risk governance oriented to attack surface convergence［J］. Cyber Security and Data Governance，2026，45(3)：17－23.

Research on network security risk governance oriented to attack surface convergence

Shen Ping
(Shanghai Municipal Education Commission Finance and Asset Management Affairs Center, Shanghai 200003, China)

Abstract: In view of the dynamic changes of the organization's network attack surface and the fact that the defender's perspective can't effectively identify the hacker's attack means, based on the multidimensional attacker's perspective, an attack surface convergence management system with the process of "asset management, attack surface identification and risk value calculation, attack surface repair and closed-loop verification, network traffic collection and real-time monitoring and analysis" is constructed to effectively realize the "safe left shift". The known assets and shadow assets are included in the scope of custody, and the risk quantification and classification and closed-loop verification of security vulnerabilities are integrated. Continuous monitoring is enabled to detect asset changes in real time and take measures. The practice results show that after introducing the collaborative analysis of network traffic and threat intelligence, the number of security incidents hit by threat intelligence has gradually decreased; the non essential exposure surfaces of websites and ports have been effectively monitored and responded to, and the average exposure time has been significantly shortened from several days to less than one hour. The attack surface management technology effectively alleviates the asymmetry of attack and defense, and improves the overall visibility and risk control efficiency of the organization in the network attack surface.

Key words: attack surface convergence; asset management; calculation of risk value; closed-loop verification

0　引言

近年来，在数字化转型驱动下，人工智能、大数据、云计算技术处于高速发展阶段，广泛应用于专项领域和人们日常生活。新技术革新发展的过程中，也带来了新的安全问题。组织网络空间资产能被访问和利用的网络入口越来越多，攻击面不断变得更多、更分散、更动态，安全威胁不断增加，安全事件频繁发生，攻击面识别和收敛过程中面临诸多挑战。云服务、微服务架构、远程办公等导致资产分散化，形成攻击面的基础性扩张；员工私自部署的未授权的应用与设备，形成了难以监管的“影子资产”；复杂供应链中对第三方服务及开源组件依赖增加，相关漏洞也在不

断暴露；攻击者利用不断演变升级的自动化攻击工具，可以实现全网暴露资产分钟级扫描，从而将各类漏洞高效转化为武器化攻击入口。这些最终构成“资产分散—影子资产滋生—供应链传导—攻击自动化”的负向循环，形成数字足迹和攻击面更多、更分散、更动态的发展趋势，迫使防御体系向持续收敛范式演进[1]。

攻击面的识别和收敛是网络安全主动防御[2]的发展趋势。在考虑系统安全、系统复杂性、资源需求和管理成本等因素下[3]，传统的资产发现、风险评估、漏洞管理、网络空间测绘等流程在企业网络稳定和集中的情况下效果显著，但无法响应当今网络中新漏洞和攻击媒介出现的速度[4]。攻击面管理作为近些年来的研究热点，深刻影响到当下资产与漏洞管理模式，其持续工作流程和黑客视角为防御者提供了攻击者视角下的企业外部攻击面数据，帮助减少攻防信息差，支持安全团队在不断增长和变化的攻击面背景下建立更主动的安全态势，促进企业攻击面的收敛和管理，为安全团队提供了实时可见性的解决方案。

1 攻击面管理现状

在大型软件系统中，按照攻击流程通常将攻击面评估指标细化为入口点、通道、数据 3 个维度[5]。近年来，攻击面管理逐渐成为安全领域的研究热点。在移动目标防御方面[6]，其核心机制在于通过持续动态地改变系统攻击面，不断提高攻击者发掘和利用系统漏洞的难度。Zhang 等人[7]通过建立攻击面元素所需权限与通用漏洞评分系统（Common Vulnerability Scoring System，CVSS）中权限指标的映射关系，将攻击面分析扩展至网络结构层面，为该方向的实际应用提供了新的研究思路。2021 年，Gartner 在安全运营技术成熟度曲线报告中首次提出了攻击面管理的两个新兴技术[8]，即面向网络空间内部资产的网络资产攻击面管理和面向互联网暴露资产的外部攻击面管理。随后两年 Gartner 持续发布相关内容，明确了攻击面管理由网络资产攻击面管理、外部攻击面管理和数字风险保护服务三个主要功能支持[9-10]。国内通常倾向于将攻击面管理分为外部攻击面管理和网络资产攻击面管理，数字风险保护服务并入外部攻击面管理。张睿[11]在研究中指出，攻击面管理应从攻击者视角构建覆盖内外资产的统一治理体系，并提出“风险闭合框架”以实现攻击面管理与传统风险控制的协同，但缺少具体的实验场景结果。毕亲波等人[12]结合 5G 网络特点梳理攻击面并进行网络安全威胁建模，核心流程包含识别资产、识别威胁参与者或威胁因素、分解系统定义攻击面、威胁行为分类、威胁评估和评价、威胁控制措施 6 个步骤。顾兆军等人[13]综合各资源组件的端口、协议、数据进行资源节点的攻击面建模并为资源间的相互关系建立资源图，融合各资源攻击面与在资源图约束下的脆弱性严重程度形成系统攻击面组合，以表征三维度的威胁程度，计算网络结构的整体风险，其研究范围在空管信息系统。外部攻击面管理和网络资产攻击面管理技术分别聚焦内网资产可见性与互联网暴露面监控，已成为当前关键研究路径，二者协同构建覆盖全域的攻击面治理体系，为动态防御提供核心支撑。

研究面向攻击面收敛的网络安全风险治理，目的在于消除或降低攻击面对系统的影响，达到组织可接受的范围。攻击面动态收敛过程如图 1 所示。

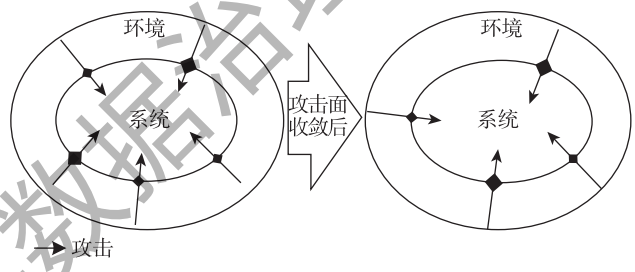

图 1　攻击面动态收敛过程

基于上述攻击面管理现状和现实网络环境常态化监控的实际需求，本文构建了“资产管理、攻击面识别与风险值计算、攻击面修复与闭环验证、网络流量采集与实时监控分析”为流程的攻击面收敛管理体系，适用于多种信息系统环境，强调攻击面修复的闭环验证与攻击面复发的持续监测，以保障安全状态的可持续、可动态评估。

2 攻击面收敛管理

2.1 攻击面收敛管理流程

攻击面收敛管理的一般流程分为资产管理、攻击面识别与风险值计算、攻击面修复与闭环验证、网络流量采集与实时监控分析。资产管理为攻击面收敛的初始阶段，通过多样化技术手段发现与监测全网存活资产，构建动态更新的资产指纹知识库。攻击面识别与风险值计算通过采用主动扫描、自动化渗透测试[14]等方式全面识别信息系统可利用风险并量化。攻击面修复与闭环验证通过工作流引擎驱动漏洞处置方案下发与执行、漏洞处置结果有效性验证、漏洞处置过程归档等闭环治理工作。网络流量采集与实时监控分析则是建立实时感知响应变换机制以维持攻击面收敛态

势，部署内核级探针监控资产变更事件，结合威胁情报触发风险监测与处置闭环流程。其流程如图 2 所示。

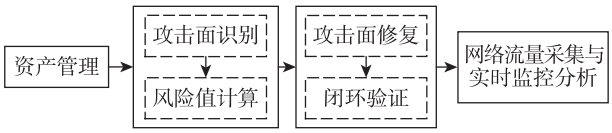

图 2　攻击面收敛管理流程

2.2　关键技术分析

2.2.1　资产管理

资产管理构成攻击面收敛的底层基础，将传统静态、碎片化的资产信息转化为动态、可操作的防御知识图谱。现代各类组织的网络环境中，数字资产增长、防御能力滞后于技术迭代、供应链等信任体系崩塌等均会引起资产模糊，导致攻击面扩大，需要有效的资产管理实现攻击面可视化[15]。

在资产发现维度上，通过动态采集为主、静态采集为辅的方式，全面探索与识别面向互联网的硬软件、云资产、数字资产等。动态采集主要有基于 Nmap 等工具的适用于内网及公网 IP 段的主动发现和基于网络设备与流量分析工具的被动感知，依据 ICMP/TCP SYN 进行存活判定，并对 HTTP（S）、SSL/TLS、SSH 等应用层协议进行精准识别。通常需要配置采集的范围、周期、采集异常处理等。威胁情报关联也是资产发现的有效手段[16]，通过将外部威胁情报与内部流量日志、终端日志等进行实时匹配，有效适用于发现已失陷或与恶意地址通信的资产，快速定位传统扫描难以察觉的主动威胁关联资产。

资产发现范围包括但不限于以下方面：已知资产，即组织了解并主动管理的所有 IT 基础架构和资源；未知资产，即在 IT 或安全团队不知晓的情况下使用网络资源但“未清点”资产；第三方或供应商资产，即组织不拥有但属于组织 IT 基础设施或数字供应链部分的资产；附属资产，即属于附属单位网络的任何已知、未知或第三方资产，通常安全团队对附属单位的资产关注度较低；恶意资产，即威胁行为者为攻击组织而创建的冒充组织品牌的网络钓鱼网站、窃取后在暗网上共享的被盗敏感数据等。

在资产分类的维度上，为业务系统添加关键性标签：核心系统、支持系统与一般系统；为暴露风险评级，互联网暴露面风险等级最高，DMZ 区暴露面风险等级次之，内网暴露面风险等级最低。

在资产监控维度上，通过自动化监控程序实时掌握公网非必要暴露面画像，监控域名/IP + 端口 + 后缀，自动检测非必要开放服务。

在资产退役维度上，自动标记 180 天无流量的资产为僵尸资产，进行释放或关闭访问。

资产管理流程如图 3 所示。

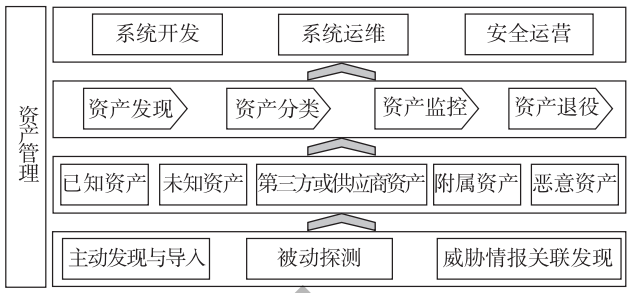

图 3　资产管理流程

资产的发现、分类、监控与退役组成了资产的全生命周期管理，进一步利用配置管理数据库（Configuration Management Database，CMDB）整合数据源、调和多数据源字段、同步联合数据源的更新情况、映射与可视化资产数据[17]，实施有效的资产识别与管理，帮助资产责任人能够快速定位目标资产，及时进行资产排查和分析。

2.2.2　攻击面识别与风险值计算

攻击面识别为基于资产识别结果分析业务系统、端口、后台及与外部链接上的薄弱点，了解资产可能面临的风险、风险暴露的原因以及黑客可能通过这些风险暴露执行的攻击类型，并按“可攻击性”划分优先级，帮助组织缩小攻击面，收缩攻防战线。采用主动扫描、基线合规扫描、弱口令检查、从攻击方视角组织人力配合工具从外部对信息资产进行脆弱性测试等技术手段，进一步将各类技术检查结果通过 Python 框架转化为自动化渗透测试的输入参数，设定触发规则并限制测试深度与范围，实施自动化风险利用。技术手段的融合机制适用于攻防演练及重要系统上线前的安全验证场景，以实现对高危漏洞的快速武器化利用演练。

基于风险识别结果，采用通用漏洞评分系统 CVSS 量化风险，计算攻击面风险值。通用漏洞评分系统 CVSS 4.0 由基础指标、威胁指标、环境指标和补充指标四个度量标准组成，各自都包含了评估所需要的相关属性。基础指标评估漏洞本身固有的、与时间和环境无关的特征；威胁指标衡量漏洞被攻击利用的可能性，该指标会随时间变化；环境指标进一步将结果严重性分数细化到特定的计算环境；补充指标描述并测量漏洞的额外外在属性，但不参与最终分数的计算。CVSS 4.0 评估指标如图 4 所示。

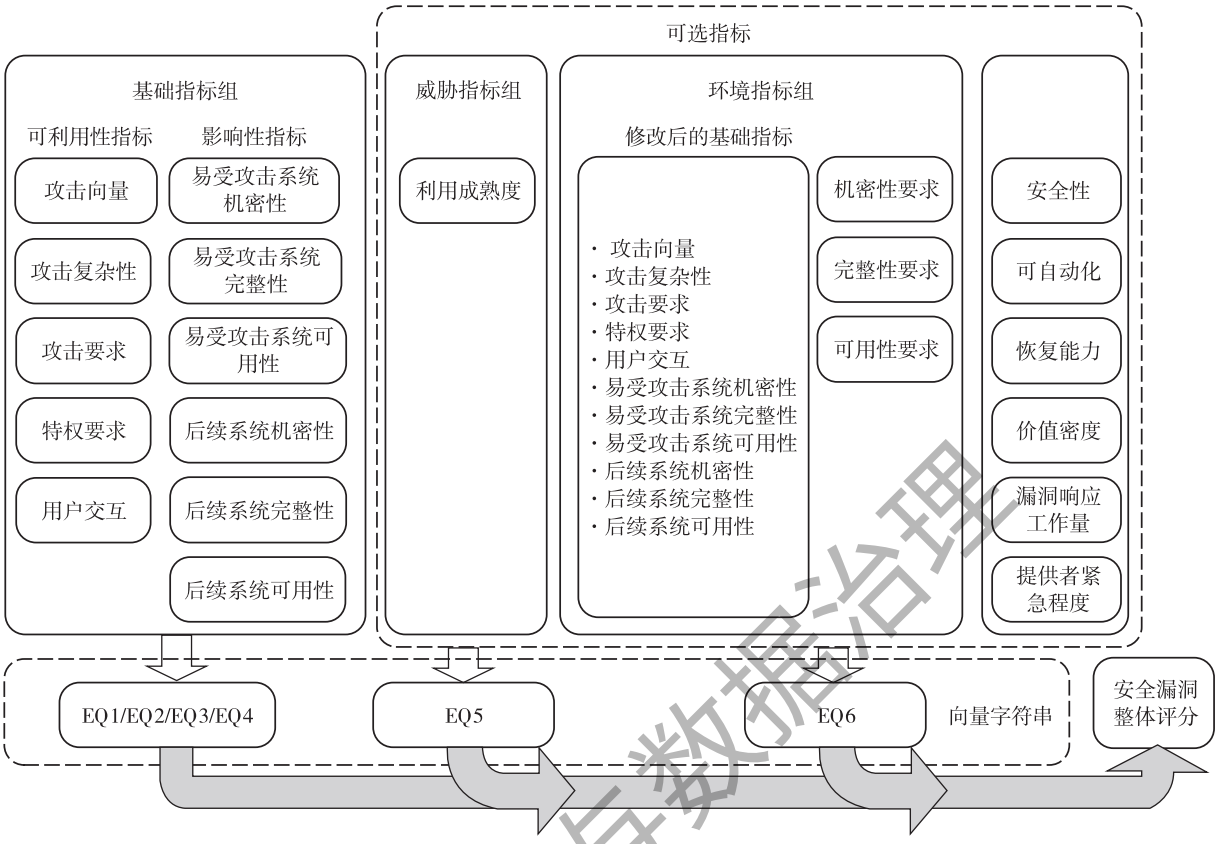

图4　CVSS 4.0 评估指标

CVSS 4.0 中指标分为 6 个等价类（Equivalence class，EQ），每个 EQ 对应不同的指标组合，构成指标子组，其级别由指标值决定。经指标赋值后得到每个 EQ 的向量，组成有效的 CVSS 4.0 向量字符串。向量的集合记为 MacroVector，所有 MacroVector 和相关分数可以通过配置文件 cvss_lookup. js 查询。已知两个向量之间的严重性距离为将一个向量转换为另一个向量所需的连续逐个指标变化的次数。MacroVector 的深度是 MacroVector 的最高严重性向量和最低严重性向量之间的最大严重性距离。

CVSS 4.0 得分计算过程如下：

（1）对于每个 EQ：

①确定当前 MacroVector 和相邻较低 MacroVector 之间的最大评分差异。

②确定待评分向量的严重性距离，即待评分向量与相同 MacroVector 中的最高严重性向量之间的距离。

③计算距离比例，即待评分向量的严重性距离除以 MacroVector 的深度。

④计算最大评分差异与距离比例的乘积。

（2）计算上述得出的比例距离的平均值。

（3）计算 CVSS 4.0 得分，即最高严重性向量的分数减去比例距离的平均值。得分四舍五入到一位小数。

上述计算结果为 CVSS 4.0 安全漏洞基础评分值，取值范围为 0～10，定义得分为 0 表示无漏洞，得分区间 0.1 ～ 3.9 为低级漏洞，4.0 ～ 6.9 为中级漏洞，7.0～8.9 为高级漏洞，9.0～10.0 为严重漏洞。依据相应评估分数判断漏洞威胁优先等级，可用于判断安全漏洞的修复顺序。

2.2.3　攻击面修复与闭环验证

在攻击面收敛管理体系中，风险识别与风险值计算是关键基础，其最终目标在于攻击面的有效修复与闭环验证。基于风险值计算的优先级排序制定修复计划，从技术与管理层面实施系统性的加固，采取有针对性的处置措施，可以有效降低因处置方案难以落实、缺乏根本原因分析、未验证修复效果等导致攻击面重新打开或持续暴露的情况。在主观修复已发现攻击面后，通过回归测试、代码审计、工具复测、功能测试、日志分析等多维度技术手段进行系统性验证，验证通

过即构建了攻击面从发现、处置、有效收敛的完整闭环，真正实现组织攻击面收敛。

攻击面修复与闭环验证过程如图 5 所示。

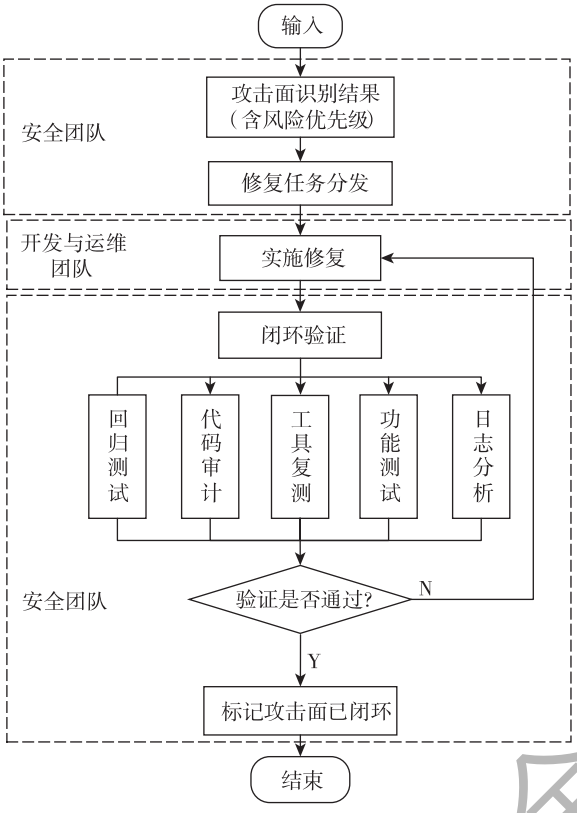

图 5　攻击面修复与闭环验证

2.2.4　网络流量采集与实时监控分析

依赖历史样本与人工经验的传统网络安全管理模式，安全问题定位高度依赖个人经验与直觉判断，存在响应滞后、误判率高、处置效率低下等问题。随后兴起的自动化分析方法，难以应对不断演化的对抗技术。网络环境中的攻击面发现与修复作为一项持续性工作，当组织内部的现有资产部署发生调整或新增等情况时，都会引起攻击面特征变化。为维持组织安全风险熵减态势，需要建立常态化监控机制。

采用功能可扩展的 Zeek 流量采集方式，结合组织网络流量采集需求，自定义多端口识别、采集时间间隔等功能，实现全网网络流量的实时采集。基于网络流量采集结果，汇总来自安全团队及受信任组织发布的威胁情报进行关联性智能化分析，建立基于威胁情报的大数据智能化分析体系。该体系下实时监控分析网络流量，降低信息检测时延，能够快速发现网络环境攻击面，并满足安全事件溯源分析和攻击面的系统化闭环管理需求。

3　攻击面收敛实践

3.1　基于威胁情报的大数据智能化分析

为有效应对海量、分散且非结构化的网络流量数据，组织采用基于威胁情报的智能化分析方法，将多源威胁情报与全流量数据进行关联分析，提升威胁检测与响应的精准性。自 2024 年 7 月起，该大数据智能化分析体系已正式部署并投入运行。系统启用以来的网络安全态势关键数据如表 1 所示。

表 1　网络安全态势关键数据

时间		安全事件数	威胁情报数	威胁情报命中数	威胁情报命中率/%	总网安事件率/%
2024 年	7 月	5	0	0	0.00	100.00
	8 月	0	8	2	25.00	25.00
	9 月	3	10	1	10.00	30.77
	10 月	3	13	2	15.38	31.25
	11 月	1	13	1	7.69	14.29
	12 月	0	8	0	0.00	0.00
2025 年	1 月	0	6	0	0.00	0.00
	2 月	0	6	0	0.00	0.00
	3 月	4	11	1	11.11	33.33
	4 月	3	5	0	0.00	37.50
	5 月	0	1	0	0.00	0.00
	6 月	0	3	0	0.00	0.00
	7 月	0	1	0	0.00	0.00
	8 月	0	8	1	12.50	12.50
	9 月	0	5	0	0.00	0.00
	10 月	0	8	0	0.00	0.00

基于威胁情报的大数据智能化分析体系启用至今的网络安全态势统计结果如图 6 所示。

基于威胁情报的大数据智能化分析通过将威胁情报与全网流量进行关联分析，在体系启用初期，检测能力提升使系统安全漏洞识别数量显著增加，是攻击面盲区消除的关键时期；经历 6 个月的调整与适应期后，安全事件发生频率逐步下降并趋于稳定。威胁情报通报的命中数呈现相同趋势，处置措施切断了攻击链条，同一类威胁情报在后续的重复命中数有效减少，少量、偶尔的命中主要来源于新增的、高质量的外部威胁情报以及内部首次出现的攻击手法。从信息安全管理体系安全策略来看，该体系提供了一种全面网络流量数据治理能力，具备对网络攻击面的防范能力，能够降低网络安全事件发生概率。

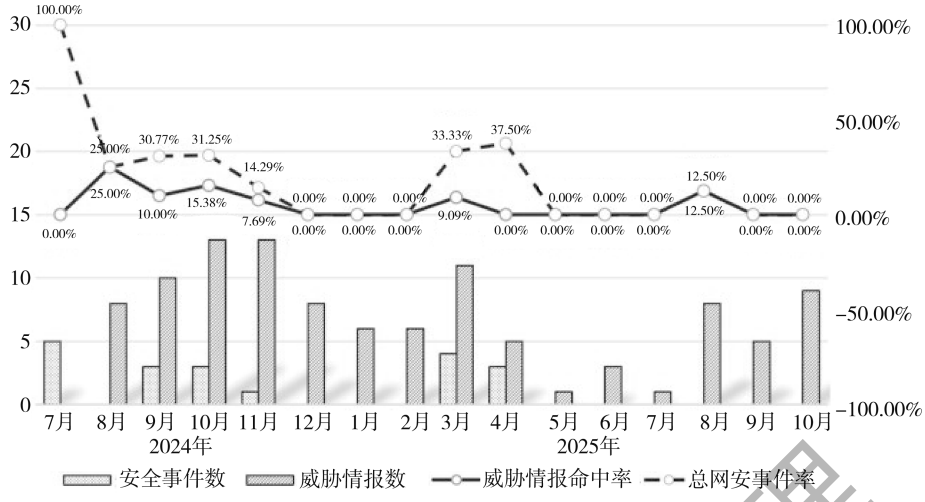

图 6　网络安全态势统计

3. 2　网址及端口攻击面的自动化监控与收敛

在数字化转型进程中，业务系统频繁出现测试网址、非必要对外访问网址、高危端口等未及时关闭的安全隐患，成为攻防演练攻方的有利突破口。为应对此安全隐患和实时监控需求，设计并部署了一套网址及端口攻击面的自动化监控收敛解决方案。该解决方案基于三维探测引擎（域名、端口、路径后缀）构建动态检测能力，通过风险量化模型实现精准威胁评估，依托分级响应机制驱动闭环处置，将轻量化代码设计实现与现有运维体系无缝集成。当检测到非必要暴露面开放即推送告警至安全责任人移动终端，直至在有效 1 h 处置时间段内完成非必要暴露面的闭环处理。

网址及端口攻击面自动化监控与收敛解决方案工作模式如图 7 所示。

图 7　网址及端口攻击面自动化监控与收敛解决方案

组织在 2024 年的攻防演练中因非必要暴露面触发了一起安全事件，事后经技术人员人工干预实现临时收敛。2025 年 3 月，同类问题再度发生。2025 年 4 月起，组织上线应用网址及端口攻击面的自动化监控与收敛方案。方案上线实施以来的网址及端口攻击面自动化监控结果如图 8 所示。

根据历史数据及方案实施以来的非必要暴露面与安全事件数对比，可以得出，网址及端口攻击面的自动化监控与收敛通过监控域名、端口、路径后缀，非必要暴露面得到系统性控制，由非必要暴露面引起的安全事件数显著减少并趋于零，同类漏洞复发率下降 100%，非必要暴露面的暴露时间从数天减少至规定的处置时间 1 h 以内。将网址及端口攻击面控制点由扫描发现实施补救左移至运维自动化环节，占主要组成部分的冗余测试端口等简单暴露可以在分钟级内完成闭环，此部分是原先整体暴露时间长的主要来源，少量复杂暴露基本实现在有效 1 h 处置时间段内完成闭环。从信息安全管理体系安全策略来看，该体系自动

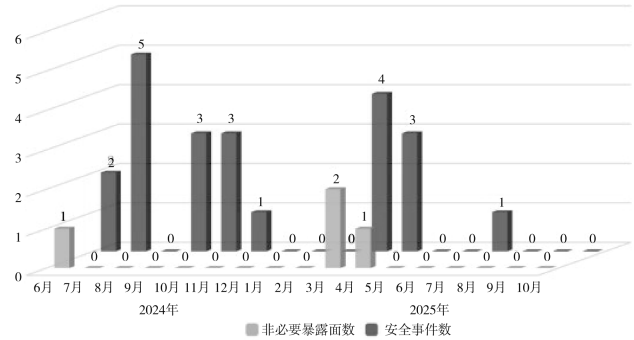

图 8　网址及端口攻击面自动化监控结果

化监测与告警机制主动识别非必要暴露面，阻断了其向实际网络攻击面的转化路径，显著降低了恶意攻击的成功概率。

4　结论

在网络空间对抗日趋激烈和数字化转型加速的背景下，应用系统面临着系统层、Web 应用层等多层攻击面利用威胁。作为系统所属组织的防御者，需采用攻击者视角，通过攻击面管理技术体系实现威胁早期识别与快速闭环处置，主动提高自身的主动防御能力，实现“安全左移”。基于“资产管理、攻击面识别与风险值计算、攻击面修复与闭环验证、网络流量采集与实时监控分析”的多维流程攻击面管理，以攻击面引发的安全事件率为导向，强调攻击面修复的闭环验证与攻击面复发的持续监测，为网络空间攻击面提供全时段持续监控，有效解决传统资产漏洞管理误报率高、处置延迟及覆盖盲区等核心缺陷，实现安全漏洞闭环处置的高精确度目标，成功构建了具备预测性防御效能的组织网络安全运营体系。

参考文献

[1] 邬江兴. 网络空间内生安全发展范式 [J]. 中国科学：信息科学，2022，52（2）：189－204.

[2] 王许培，王伟刚. 基于业务与安全融合的智慧煤矿主动防御技术与实践 [J]. 网络安全与数据治理，2022，41（12）：17－24，33.

[3] SENGUPTA S，CHOWDHARY A，SABUR A，et al. A survey of moving target defenses for network decurity [J]. IEEE Communications Surveys & Tutorials，2020，22（3）：1909－1941.

[4] ZHENG Y，LI Z，XU X，et al. Dynamic defenses in cyber security：techniques，methods and challenges [J]. Digital Communications and Networks，2022，8（4）：422－435.

[5] THEISEN C，HERZIG K，MURPHY B，et al. Risk-based attack surface approximation：how much data is enough? [C]//2017 IEEE/ACM 39th International Conference on Software Engineering：Software Engineering in Practice Track（ICSE-SEIP）. IEEE，2017：273－282.

[6] 周余阳. 基于网络攻击面的移动目标防御方法研究 [D]. 南京：东南大学，2021.

[7] ZHANG M，WANG L，JAJODIA S，et al. Network attack surface：lifting the concept of attack surface to the network level for evaluating networks’ resilience against zero-day attacks [J]. IEEE Transactions on Dependable and Secure Computing，2018，18（1）：310－324.

[8] SHOARD P，HANDA S. Hype cycle for security operations 2021 [R]. USA Connecticut：Gartner，G00747546，2021.

[9] DAVIES A. Hype cycle for security operations 2022 [R]. USA Connecticut：Gartner，G00770249，2022.

[10] NUNEZ J，DAVIES A. Hype cycle for security operations 2023 [R]. USA Connecticut：Gartner，G00787018，2023.

[11] 张睿. 整体安全视角下的综合攻击面管理 [J]. 工业信息安全，2023（5）：20－27.

[12] 毕亲波，赵呈东. 基于 STRIDE-LM 的 5G 网络安全威胁建模研究与应用 [J]. 信息网络安全，2020，20（9）：72－76.

[13] 顾兆军，杨睿，隋嵩. 面向网络架构的系统攻击面建模方法 [J]. 信息网络安全，2022，22（3）：29－38.

[14] 陈可，鲁辉，方滨兴，等. 自动化渗透测试技术研究综述 [J]. 软件学报，2024，35（5）：2268－2288.

[15] 杨显哲，尹毅峰，张宏涛，等. 教育系统网络资产探测与预警研究 [J]. 计算机应用与软件，2023，40（10）：322－328.

[16] 周颖，刘毅洲，黄微. 面向信息安全自主可控的网络空间风险情报源识别 [J]. 情报杂志，2025，44（6）：109－118.

[17] WU M S，CHIU N H，CHIN K Y. The cost/benefit strategic grid approach：a decision support method for design and improvement of configuration management databases [J]. International Journal of Information Systems and Change Management，2022，13（2）：95－113.

（收稿日期：2025－12－25）

作者简介：

沈萍（1999－），女，硕士，主要研究方向：网络安全、信息安全运营。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部