

面向多源异构数据的网络安全威胁智能分析与动态响应：研究综述与展望

刘 柳

江西工业工程职业技术学院信息工程学院，江西 萍乡

收稿日期：2026年8月7日；录用日期：2026年9月7日；发布日期：2026年9月18日

摘 要

随着网络攻击手段复合化与防御孤岛化，如何基于多源异构数据实现网络安全威胁的智能分析与动态响应，已成为态势感知与主动防御的核心议题。多源安全数据在来源、结构与质量上高度异构，其冗余、误报与标注稀缺构成框架性能的上限约束。围绕“感知-识别-响应”闭环，D-S证据理论与模糊/贝叶斯推理仍是融合不确定、不完备证据的主流范式，机器学习与知识图谱分别从数据驱动与语义推理维度予以补充；事件定级、自动化缓解、访问控制与平台化协同共同构成动态响应链条。当前框架的可信落地仍受数据质量治理、模型可解释性、自动化误伤与对抗鲁棒性四重挑战制约，未来应从追求更高自动率转向追求可验证的可信度。

关键词

多源异构数据，网络安全，威胁识别，态势感知，动态响应

Intelligent Analysis and Dynamic Response of Cybersecurity Threats for Multi-Source Heterogeneous Data: A Review and Prospect

Liu Liu

School of Information Engineering, Jiangxi Vocational College of Industry & Engineering, Pingxiang Jiangxi

Received: August 7, 2026; accepted: September 7, 2026; published: September 18, 2026

Abstract

As cyber attacks grow increasingly composite and defense devices remain fragmented into isolated silos, how to achieve intelligent analysis and dynamic response of cybersecurity threats based on

文章引用：刘柳. 面向多源异构数据的网络安全威胁智能分析与动态响应：研究综述与展望[J]. 人工智能与机器人研究, 2026, 15(5): 1242-1249. DOI: 10.12677/airr.2026.155113

multi-source heterogeneous data has become a core issue in situational awareness and active defense. Multi-source security data is highly heterogeneous in origin, structure, and quality; its redundancy, false positives, and label scarcity set a hard upper bound on any fusion or detection model. Around the sense-identify-respond loop, D-S evidence theory and fuzzy/Bayesian reasoning remain the dominant paradigms for fusing incomplete and uncertain evidence, while machine learning and knowledge graphs progressively contribute data-driven detection and semantic attribution. Event grading, automated mitigation, access control, and platform-centric collaboration form the dynamic response chain. Yet the current framework's trustworthy deployment is constrained by four challenges: data-quality governance, model interpretability, false-positive misinjury in automated response, and adversarial robustness. In the future, efforts should shift from pursuing higher automation rates to achieving verifiable credibility.

Keywords

Multi-Source Heterogeneous Data, Cybersecurity, Threat Identification, Situational Awareness, Dynamic Response

Copyright © 2026 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

随着网络规模持续扩张与攻击技术的快速演化，网络安全防御面临的困境日益突出：攻击者采用多阶段、多维度的复合攻击手段，而防御方依赖的入侵检测系统、防火墙、流量监控等安全设备各自为战，形成一个个“安全信息孤岛”。实践中，单个入侵检测系统产生的报警信息往往包含大量误报与冗余，安全管理人员难以从海量报警中识别真实的入侵事件。与此同时，安全设备之间的数据格式、检测规则与情报库互不相通，针对同一攻击事件，不同厂商的检测系统可能给出完全不同的判断。如何从多源异构的安全数据中提炼可信的威胁认知，并在此基础上形成快速、准确的响应机制，已成为网络安全研究的核心议题[1]。在车联网等专用场景，也有学者综述了大数据时代下的安全加密认证技术架构与面临的挑战[1]。

2. 多源异构安全数据的特征分析

2.1. 数据来源的多样性与结构异构性

网络安全数据的来源呈现出显著的多点分布特征。从采集主体看，既包括部署在网络边界的流量传感器、入侵检测系统，也包括主机与设备产生的系统日志、应用日志，还包括 SNMP 协议采集的网络设备管理信息以及外部威胁情报。王峥等设计的网络安全态势评估系统将多源数据挖掘应用于采集与评估环节，通过统一的预处理把异构安全事件转化为可度量的态势要素[2]。钱斌等在计量自动化系统的研究中进一步细化了数据来源谱系，涵盖防火墙、IDS、网络准入与 IPS、正反向隔离阵列、堡垒机等多类安全设备[3]。陈锴据此设计了基于多源异构传感器的网络安全态势感知系统，由信息采集层、多源数据融合层与态势感知层构成，验证了传感器层标准化接入对提升感知符合度的作用[4]。

数据来源的多样性直接导致了结构的异构性。黄智勇等在研究多源网络安全数据融合时发现，流量传感器、主机日志、防火墙日志三者的识别框架完全不同：流量传感器关注弱口令、APT 事件、XSS 攻

击等攻击类型,主机日志记录错误事件、用户越权、审核事件,防火墙日志则体现端口扫描、SYN 洪泛、拒绝服务等形式,必须针对不同信息格式分别建立识别框架[5]。李斌等从数据交互的视角指出,多源网络大数据的频繁交互与存储打破了传统数据“孤岛”,实现了跨区域与跨组织的数据访问,但同类型数据在不同用户标注下呈现出不同的访问安全性[6]。此外,从数据形态看,多源安全数据还可划分为结构化、半结构化与非结构化三类,进一步加剧了融合处理的难度。

2.2. 数据质量的现实约束

多源安全数据在质量层面存在三重约束。其一是冗余度高。安全设备产生的原始数据量庞大且重复,何璘琳等利用前馈神经网络与遗传算法构建清洗模型,先剔除冗余数据再利用深度学习完成特征提取,验证了去冗余对提升态势要素质量的必要性[7]。其二是误报与漏报普遍。黄智勇等指出,主流入侵检测系统反馈的报警信息中仅约 10%是有用的,大量误报、漏报不仅淹没真实入侵事件,还会挤占传输负载与存储空间,使真实事件无法审计[5]。钱斌等在计量自动化系统的调研印证了这一点:各安全分区的 IDS 每天可产生上百万条记录,误报率高,若不加以挖掘分析,管理人员无法直接利用这些检测信息[3]。其三是标注稀缺。多源安全数据普遍缺乏统一标注,给后续监督式识别带来根本困难。

2.3. 数据的时空关联特性

多源安全数据的价值不仅在于单条记录的内容,更在于记录之间的时空关联。在时间维度上,攻击事件往往表现为持续一段时间窗口内的行为序列,黄智勇等据此将警报的时间向量纳入相似度计算,利用欧氏距离度量两条警报的时间接近程度,并指出网络攻击在一段时间内被多个设备检测到,可以为报警信息的准确性提供多方位支撑[5]。在空间维度上,不同端口、协议、网段的流量在等时间间隔采样点上形成多主题时序,郭鹏等提出的多源异构网络安全数据可视化融合分析方法,通过对异构日志的协同可视化揭示僵尸网络、DDoS 等攻击的多源关联特征[8]。赵洪芳等进一步从数字政府基础设施的角度指出,多源数据接入在提升效率的同时也放大了数据隐私、完整性与访问控制方面的关联风险[9]。

2.4. 数据预处理与标准化路径

针对上述特征,预处理与标准化形成了较为成熟的技术路径。在数据清洗环节,何璘琳等提出基于前馈神经网络与遗传算法的清洗模型,先剔除冗余数据再利用深度学习构建属性多样的安全态势要素集合[7]。在特征处理环节,程广振针对无线网络安全漏洞信息提出基于多源数据融合的检测方法,通过特征提取与融合降低数据集冗余度并提升模型泛化能力[10]。在统一表示环节,黄宏杰探索了智慧校园场景下的多源数据融合动态感知方案,以标准化接入与融合分析支撑跨域态势感知[11]。李舒畅的学位论文系统梳理了多源数据分析融合技术在态势感知系统中的应用,通过为十余种应用日志开发统一解析器,将应用日志与系统日志格式标准化为多源威胁检测的标准输入[12]。

3. 网络安全威胁的智能识别方法

3.1. 基于证据理论与统计推理的融合识别

证据理论因其处理不确定信息的能力,成为多源威胁融合识别的主流工具。黄智勇等基于 DS 证据理论建立多源网络安全数据融合模型,针对误报问题设计了动态的基本概率分配递推公式:若某传感器持续误报,则其基本概率分配随误报次数动态衰减,从而抑制不可靠证据对融合结果的干扰[5]。陈玉明在网络空间多源数据融合框架下研究 APT 攻击溯源方法,将告警、流量与威胁情报等多源证据统一建模,显著提升了复杂攻击链的关联识别能力[13]。

与证据理论并列, 模糊推理与贝叶斯方法构成了统计推理识别的另一分支。钱斌等基于层次分析和模糊综合评价构建态势评估模型, 从危险性、脆弱性、可用性、可靠性四个维度设置一、二级指标, 通过隶属度矩阵与判断矩阵计算系统风险等级, 在 $b_1 = 5$ 、 $b_2 = 6$ 的参数设定下检测率达 90.6%, 对关联攻击的检测成功率达 62.8%, 显著优于 SVM 与朴素贝叶斯方法[3]。高斐等在服务安全态势感知模型中先利用贝叶斯公式评估响应时间、负载能力、连接状态三个指标下服务处于正常、偏离、失效态势的概率, 再以 D-S 证据理论合成评估结果, 其对 DNS 服务评估的样本标准差仅为 0.117, 稳定性优于 PCA 模型[14]。

3.2. 基于机器学习的威胁检测与分类

机器学习方法为威胁识别提供了数据驱动的路径。在监督学习方向, 常利伟等以 BP 神经网络作为决策引擎分析各数据源的数据, 不同探测器对识别不同类型攻击各具优势: Netflow 数据源对 Analysis 类和正常流量识别准确率较高, Snort 数据源对 Backdoor、Worm 类攻击区分效果好, Suricata 则擅长识别 Dos 攻击, 多源融合正是通过集成这些差异化优势提升整体识别性能[15]。何璘琳等利用深度学习方法对清洗后的多源数据实施特征提取与分类, 据此建立属性多样的安全态势要素集合[7]。在无监督与新兴模型方向, 张雅瑄等提出融合多源数据与动态防御机制的智能检测架构, 通过跨域语义对齐与注意力机制实现深层特征融合, 并引入在线演进机制增强模型在对抗环境中的适应性[16]; 杨伟面向煤矿场景设计基于人工智能的入侵检测系统, 以多源数据融合支撑实时防御[17]。杨宏宇等基于无监督多源数据特征解析进行网络威胁态势评估, 以变分自动编码器-生成式对抗网络(V-G)缓解标注稀缺下的威胁表征问题[18]。谭保雄的学位论文系统研究了基于多源数据的入侵检测技术, 以 CNN-GRU 模型融合源流量数据, 使实际网络流下的入侵检测准确率显著提升[19]。

3.3. 基于知识图谱与本体的语义推理

统计与机器学习方法解决的是“识别”问题, 而理解威胁的语义上下文则需要知识层面的推理。张书钦等以 CAPEC 攻击模式为桥梁, 将 ATT&CK 矩阵中攻击者的战术、技术与 CWE 弱点、CVE 漏洞、CPE 受影响平台端到端关联, 整合后的图结构知识库存储于 Neo4j, 包含 29 万余条 CPE 条目、16 万余条 CVE 条目和 711 万余条关系链接; 在此基础上构建的 RIOTSCO 本体包含平台、漏洞、弱点、攻击模式、活动、事件六个顶级类, 通过 OWL 描述逻辑与 SWRL 推理规则, 能够自动标记高脆弱性平台、推理可采用的缓解措施、分离面临特定威胁的高危节点, 并描绘威胁事件波及上下游供应链的情报全景[20]。胡开明等进一步提出一种融合多源异构数据的图神经网络联合框架, 将异构信息网络与时空图卷积结合, 用于网络攻击溯源与态势感知[21]。在威胁情报层面, 尹彦等归纳了威胁情报在态势察觉、理解与投射三个阶段的应用, 指出多源威胁情报能显著提升对新型高级威胁的察觉能力[22]。

3.4. 威胁态势的量化评估与可视化表达

威胁识别的结果需要转化为可度量、可展示的态势认知。在量化评估方面, 常利伟等以 Snort 报警规则为标尺提炼威胁等级划分原则, 将权系数理论与等级划分相结合量化攻击威胁因子, 再采用层次化评估模型依次计算服务层、主机层、网络层态势[15]。高斐等从服务质量需求与服务可生存性两个维度量化服务态势[14]。在可视表达方面, 郭鹏提出的多源异构网络安全数据可视化融合分析方法, 将异构安全数据以融合视图呈现, 辅助分析人员快速把握全局态势[8]。黄达辉等基于多源传感数据融合构建医院网络安全态势测量与风险预警方法, 通过模糊集实现时序对齐与深度融合, 并以分级标准发出风险预警信号[23]。王新哲等构建动态时空图网络预警框架(DSTGN), 通过动态攻击图将多源告警转化为含时序与空间关联的图结构, 并以通道时空图神经网络捕捉攻击链时序演化, 在复杂场景下提升检测精度与早期预警

能力[24]。

4. 动态响应机制设计

4.1. 事件定级与响应触发机制

动态响应的前提是建立统一的事件定级标准，使响应资源按照威胁程度有序投放。常利伟等依据 Snort 规则提炼高、中、低三级威胁划分原则，发挥着响应触发阈值的作用[15]。王峥等在态势评估系统中专门设置事件威胁度评价环节，将高威胁度安全事件置于首位提醒管理人员重视[2]。定级完成后，响应动作依据威胁等级依次触发：对特别重大与重大事件启动跨团队协同处置，对较大与一般事件则交由自动化剧本优先处理。

4.2. 自动化缓解推理与处置机制

定级之后，响应动作的生成本身也可以智能化。张书钦等设计的缓解措施推理规则表明：当物联网环境中的高脆弱性位置已知时，可通过平台漏洞可能受到的攻击模式映射至攻击技术，利用已知威胁事件分析与该技术关联的恶意行为与战术，从知识库中自动化提取相关缓解措施；分离高危节点的推理规则则可查询存在特定弱点的平台，将可能被攻击者利用以达成战术目标的节点优先分离处理，大幅减少响应的时间与空间消耗[20]。胡开明等的图神经网络框架同样支持从融合特征到候选响应动作的映射，使推理规则能够依据实际环境特点自适应调整[21]。

4.3. 访问控制与协同防护机制

动态响应不仅作用于已识别的威胁，也应作用于数据访问这一威胁作用面。李斌等提出基于区块链的多源网络大数据安全访问权限认证方法：以相似关系度量数据在网络传输中的变化状态并计算访问概率，通过区块链建立数据安全访问合约，标定数据访问属性与交易密文，再根据访问目的的信度定制访问规则并认证具体权限；实验显示其认证响应时间保持在 20 至 30 毫秒，而传统跨域认证与差分隐私方法在常规模式下超过 400 毫秒、攻击模式下超过 700 毫秒[6]。黄银强等基于联邦学习研究智能电网多源数据安全共享，在不暴露原始数据的前提下完成跨主体威胁特征联合建模，为协同防护中的数据可用不可见提供技术路径[25]。

4.4. 平台化协同与响应效能评估

单体机制需要平台支撑才能形成规模化的响应能力。李嘉等基于多源异构数据的网络安全威胁分析技术，在电信运营商 SOC 场景中构建数据采集与预处理、多级数据融合与威胁分析模型，解决了传统单一数据源面临的“数据孤岛”、检测滞后与高误报率问题，省级核心网部署验证显示已知威胁检测准确率达 99.2%、误报率降低 85%、溯源与处置效率提升超 80% [26]。简玲等提出多源融合的大数据网络安全态势感知平台架构，通过统一的数据采集传输规范与多源分析算法共识机制实现平台级融合[27]。该实践表明，通过多级融合与严格误报控制可显著降低误报并提升处置效率，平台化协同是框架落地的关键支撑。

5. 框架面临的理论与实践挑战

5.1. 数据质量对框架性能的上限约束

多源异构数据驱动的威胁分析框架，其能力上限首先受制于输入数据质量。网络安全数据普遍冗余度高、标注稀缺且噪声大，而机器学习“垃圾进、垃圾出”的固有规律意味着，融合与识别模型无论如何

精巧，其性能都无法超越训练与评估所依赖的数据边界[7]。在威胁分类任务中，标注错误会被模型隐蔽吸收，导致检测边界偏移却难以在离线指标上暴露；不同安全设备识别框架不一致、样本分布随攻防演进而漂移，进一步放大训练集与真实流量之间的语义鸿沟。周景贤等提出的网络威胁情报质量评估方法，从及时性、活跃性、关联性、完整性等维度量化情报源质量，说明数据供应链的质量治理已成为框架可信度的基础环节[28]。因此，数据治理并非前置的工程琐事，而是决定整个框架效能上限的根本性约束：标准化采集、去冗余、标注质量控制与偏差校正，任何脱离数据质量讨论的准确率提升都可能是虚假繁荣。这也提示我们，在评价一个威胁分析框架时，应将其数据供应链质量纳入与算法精度同等重要的位置。

5.2. 模型可解释性与响应决策可信度

即便识别模型具备较高检测精度，若其决策逻辑不可解释，自动化响应所依赖的可信度便无从建立。深度模型在威胁识别中常表现为黑箱，安全运营人员只能获得告警而难以获知为何触发，这在误报频发时会迅速削弱人机协同效率。可解释人工智能通过特征归因、规则提取与反事实解释等路径，将模型判断转化为人类可理解的语义上下文，使分析人员能够核验攻击载荷的关键特征。胡开明等提出的图神经网络联合框架实现了多源异构数据的深层融合与攻击溯源[21]，但此类融合模型在面向动态响应时，其决策解释性仍有待加强，提示可解释性必须服务于“决策可信度”而非仅满足合规展示——只有当响应动作的触发依据能够被复盘与追责，自动化处置才具备被授权接入高危操作的正当性。

5.3. 自动化响应的“误伤”风险及其控制策略

动态响应机制的核心价值在于缩短响应时延，但“自动处置”天然伴随误伤风险，也就是将合法业务流量或运维行为误判为威胁后实施阻断、隔离或下线，可能造成业务中断乃至连锁故障。误报在静态告警阶段尚可交由人工甄别，一旦进入自动执行链路，其代价被指数级放大。控制误伤需采取分层策略：其一，在触发层设置置信度阈值与多源交叉验证，避免单模型低置信度判定直接驱动高危动作；其二，将自动化响应限定于告警升级、流量镜像、临时限速等可逆、低影响的动作，而主机隔离、账号禁用等高危动作保留人工确认；其三，建立灰度发布与回滚机制，对响应剧本进行离线仿真与线上小流量验证；其四，引入人在回路作为最终兜底。李强等构建的主动防护体系同样强调以动态行为分析与自主决策响应缩短时延，但需以可控的误伤代价换取防御收益[29]。

5.4. 概念漂移与对抗扰动下的鲁棒性

框架在封闭实验设定下的优异表现，往往难以迁移到持续演化的真实网络环境。攻击技术、正常业务模式与资产拓扑都处于动态变化之中，训练所得模型面临概念漂移，检测边界随时间退化而失效。与此同时，依赖深度特征的识别模型对对抗扰动高度敏感：在输入中施加难以察觉的微小扰动即可诱导模型做出错误判定，这类脆弱性在攻击者刻意构造的对抗样本面前尤为突出。更严峻的是，可解释接口本身也可能成为攻击面——针对解释机制的对抗性操纵可使分析师被“看似合理”的假解释误导。张雅瑄等的智能检测架构引入在线演进机制以应对模型退化[16]，但框架整体鲁棒性仍不能仅以静态数据集上的准确率衡量，而必须纳入持续学习、在线校验与对抗训练等机制，并将分布外检测与异常不确定性估计作为响应的前置闸门。

5.5. 人在回路与信任校准：走向可信自治

综合上述挑战，完全自治的“感知-识别-响应”闭环在可预见的时期内仍难以独立承担关键基础设施的安全职责。可信自治的可行路径是“人在回路”的人机协同：机器负责规模化感知、初筛与候选

响应生成, 人类负责高风险裁决、策略修正与责任认定。这要求对系统信任进行校准, 既避免对模型的过度依赖, 也避免对其价值的全盘否定; 可解释性、不确定性量化与可审计日志共同构成信任的工程基础。李嘉等的电信级实践表明, 多级融合与严格误报控制可显著提升处置效率[26], 但其在开放环境下的泛化仍需审慎评估。展望未来, 多源异构数据驱动的威胁分析与动态响应应从“追求更高自动率”转向“追求可验证的可信度”, 在数据治理、可解释决策、误伤控制与鲁棒性保障四个维度协同演进, 方能在复杂对抗环境中行稳致远。

6. 结语

基于学者们现有研究, 可以勾勒出一个“感知-识别-响应”的闭环框架: 在感知层, 多源采集与预处理机制解决数据的完整性与可用性问题; 在识别层, 证据理论融合、机器学习检测与知识语义推理形成互补的方法谱系, 分别回答“发生了什么”“是否为威胁”“威胁意味着什么”三个递进问题, 态势量化与可视化则把识别结果转化为决策者可用的认知产品; 在响应层, 事件定级触发、自动化缓解推理、访问控制与平台化协同构成动作的链条。从运行流程看, 该闭环按周期滚动执行: 每个评估周期内, 感知层汇总各传感器的原始记录, 经清洗与标准化后进入识别层; 识别层并行运行统计融合与机器学习方法, 输出威胁类型与概率; 响应层据此完成定级、缓解与协同, 并将效果反馈至下一周期。整体来看, 多源异构数据驱动的威胁分析已从单算法优化走向体系化机制设计, 但其可信落地仍取决于数据质量治理、模型可解释性、误伤控制与鲁棒性保障的持续协同。文献计量分析也表明, 多源数据驱动的安全分析正成为网络安全领域持续增长的研究热点, 其关注点由技术应用向战略与治理层面延伸[30]。

基金项目

江西省教育厅科学技术研究项目“基于多源数据的网络安全可视化系统的研究与应用”(GJJ2406808)的阶段性研究成果之一。

参考文献

- [1] 宋涛, 李秀华, 李辉, 等. 大数据时代下车联网安全加密认证技术研究综述[J]. 计算机科学, 2022, 49(4): 340-353.
- [2] 王峥, 崔冉. 基于多源数据挖掘的网络安全态势评估系统[J]. 吉林大学学报(信息科学版), 2025, 43(1): 143-149.
- [3] 钱斌, 蔡梓文, 肖勇, 等. 基于模糊推理的计量自动化系统网络安全态势感知[J]. 南方电网技术, 2019, 13(2): 51-58.
- [4] 陈锴. 基于多源异构传感器的网络安全态势感知系统设计[J]. 现代电子技术, 2020, 43(20): 74-78.
- [5] 黄智勇, 林仁明, 刘宏, 等. 基于 DS 证据理论的多源网络安全数据融合模型[J]. 现代电子技术, 2024, 47(7): 115-121.
- [6] 李斌, 何辉, 赵中英, 等. 基于区块链的多源网络大数据安全访问权限认证仿真[J]. 电信科学, 2024, 40(2): 107-115.
- [7] 何璘琳, 何月顺, 罗亚宾, 等. 网络多属性安全态势感知方法仿真研究[J]. 计算机仿真, 2024, 41(10): 333-336.
- [8] 郭鹏. 多源异构网络安全数据可视化融合分析方法[J]. 数智技术研究与应用, 2024, 30(22): 146-150.
- [9] 赵洪芳, 许峰, 陈立维. 数字政府基础设施中多源数据接入的网络安全风险防控策略[J]. 中国宽带, 2026, 22(6): 91-93.
- [10] 程广振. 基于多源数据融合的无线网络安全漏洞信息检测方法[J]. 桂林航天工业学院学报, 2025, 30(3): 433-440, 459.
- [11] 黄宏杰. 智慧校园多源数据融合动态感知方案探索[J]. 福建电脑, 2026, 42(3): 43-47.
- [12] 李舒畅. 基于多源数据分析融合技术的态势感知系统[D]: [硕士学位论文]. 北京: 北京邮电大学, 2023.
- [13] 陈玉明. 网络空间多源数据融合下的 APT 攻击溯源方法研究[J]. 软件, 2025, 46(9): 171-173.
- [14] 高斐, 王慧强. 基于多源数据特征的服务安全态势感知模型研究[J]. 武汉大学学报(理学版), 2011, 57(2): 165-169.

-
- [15] 常利伟, 田晓雄, 张宇青, 等. 基于多源异构数据融合的网络安全态势评估体系[J]. 智能系统学报, 2021, 16(1): 38-47.
- [16] 张雅瑄, 刘心声. 人工智能驱动的网络安全威胁检测系统[J]. 电脑知识与技术, 2026, 22(10): 85-87.
- [17] 杨伟. 基于人工智能的煤矿网络安全入侵检测系统设计与实现[J]. 电子元器件与信息技术, 2026(5): 154-157.
- [18] 杨宏宇, 王峰岩. 基于无监督多源数据特征解析的网络威胁态势评估[J]. 通信学报, 2020, 41(2): 143-154.
- [19] 谭保雄. 基于多源数据的入侵检测技术研究[D]: [硕士学位论文]. 南昌: 南昌大学, 2024.
- [20] 张书钦, 白光耀, 李红, 等. 多源数据融合的物联网安全知识推理方法[J]. 计算机研究与发展, 2022, 59(12): 2735-2749.
- [21] 胡开明, 陈建华. 一种融合多源异构数据的图神经网络联合框架[J]. 网络安全与数据治理, 2026, 45(4): 51-58.
- [22] 尹彦, 张红斌, 刘滨, 等. 网络安全态势感知中的威胁情报技术[J]. 河北科技大学学报, 2021, 42(2): 195-204.
- [23] 黄达辉, 钟伟华, 王欣霖, 等. 基于多源传感数据融合的医院网络安全态势测量与风险预警方法研究[J]. 国外电子测量技术, 2026, 45(1): 273-279.
- [24] 王新哲, 孙望舒, 罗晨, 等. 基于动态时空图网络的数据安全态势预警技术[J]. 计算机与现代化, 2026(8): 83-95.
- [25] 黄银强, 刘栋. 基于联邦学习的智能电网网络多源数据安全共享研究[J]. 智能物联技术, 2025, 57(2): 98-101.
- [26] 李嘉, 冯铭能, 伍铭坚, 等. 基于多源异构数据的网络安全威胁分析技术的研究与实践[J]. 通信与信息技术, 2026(3): 134-138.
- [27] 简玲, 叶天鹏, 林祥, 等. 多源融合的大数据网络安全态势感知平台研究与探索[J]. 信息网络安全, 2020(S2): 139-143.
- [28] 周景贤, 李其蔚, 程志棚. 基于多源异构数据的网络威胁情报质量评估方法[J]. 中国民航大学学报, 2024, 42(4): 29-36.
- [29] 李强, 李伟光, 李俊佳. 基于人工智能的网络安全智能防御系统构建与主动防护技术研究[J]. 网络安全和信息化, 2025(9): 52-54.
- [30] 黄冬. 网络安全教育领域热点及趋势分析——基于 CiteSpace 的图谱量化分析[J]. 信息网络安全, 2026, 26(3): 491-499.