林业网络安全态势感知中渗透测试数据融合与威胁预警模型研究

王敏杰*

黑龙江林业职业技术学院　黑龙江牡丹江

【摘要】随着林业资源监测、生态环境评估、智慧林业管理等系统的数字化与联网化程度不断提高，网络攻击手段日益多样化和隐蔽化，传统的安全防护模式难以及时、准确地发现潜在威胁。渗透测试作为评估系统脆弱性的重要技术手段，在态势感知体系中扮演着核心角色。然而，不同来源、不同格式的渗透测试数据在融合分析过程中面临标准不统一、数据冗余和信息孤岛等问题，限制了预警模型的有效性。本研究结合数据融合技术与智能分析方法，构建适用于林业领域的威胁预警模型，以提升风险识别的准确度与响应速度，为林业网络安全保障提供技术支撑。

【关键词】林业网络安全；态势感知；测试数据融合；威胁预警模型

【基金项目】中国（北方）现代林业职业教育集团 2024 年林业科学研究项目《渗透技术在林业网络安全领域的研究与实践》，课题编号：LZJB2024KY010

【收稿日期】2025 年 10 月 15 日　【出刊日期】2025 年 11 月 15 日　【DOI】10.12208/j.sdr.20250275

Research on data fusion and threat alert model of penetration testing in forestry network security situation awareness

*Minjie Wang**

Heilongjiang Forestry Vocation- Technical College, Mudanjiang, Heilongjiang

【**Abstract**】With the increasing degree of digitalization and network of forestry resource monitoring, ecological environment assessment, smart forestry management and other systems, network attack means becoming more and more diversified and concealed, and the traditional security protection model can hardly detect potential threats timely and accurately. Penetration testing, as an important technical means to evaluate vulnerability, plays a central role in the situation awareness system. However, in the process of data integration and analysis, penetration testing data from different sources and in different formats are facing such as inconsistent standards, data redundancy and information islands, which limits the effectiveness of the early warning model. In this study, data fusion technology and intelligent analysis method are combined to construct threat early warning model suitable for the forestry field, so as to improve the accuracy of risk identification and the speed of response, and to provide technical support for the security guarantee of network.

【**Keywords**】Forestry network security; Situation awareness; Test data fusion; Threat early warning model

近年来，随着智慧林业、生态监测与资源管理等信息化系统的广泛应用，林业行业正逐步迈入高度数字化与网络化的新阶段。然而，随之而来的网络安全风险日益凸显，针对林业信息系统的攻击手段呈现出高隐蔽性、强针对性和多样化趋势，涵盖数据窃取、系统入侵、服务中断等多种形式。尤其在分布式感知设备、卫星遥感平台和物联网节点的大规模部署背景下，林业数据链路和管理平台面临着更为复杂的安全威胁。传统的防护机制多依赖静态规则与被动响应，难以及时识别和预警新型攻击。渗透测试作为主动发现系统脆弱性的重要技术手段，在林业网络安全态势感知体系中具有不可替代的作

*通讯作者：王敏杰（1978-）女，本科，副教授，研究方向：计算机网络技术，网络安全。

用，但现有方法在数据融合、信息提取与威胁预测方面仍存在不足，亟需构建更高效的融合分析与预警模型以保障林业信息系统的安全运行[1]。

1 林业网络安全态势感知工作的主要开展意义

林业网络安全态势感知工作的开展，对于保障林业信息化建设的稳定运行与数据资源的安全利用具有重要意义。一方面，林业生产管理、生态监测与资源调配高度依赖网络化平台与数据传输链路，任何安全漏洞都可能导致关键业务中断、敏感数据泄露，甚至影响生态环境保护与林业决策的科学性；另一方面，通过态势感知技术能够实现对网络运行状态、潜在威胁和安全事件的实时监测与综合分析，为管理部门提供可视化、安全态势全局化的决策依据。同时，态势感知还可提升安全防御体系的主动性与智能化水平，从被动应对转向主动预防，有助于及时发现并处置新型网络攻击，降低安全事件发生的概率和危害程度，从而为智慧林业的可持续发展提供坚实保障。

2 测试数据融合与威胁预警模型对林业网络安全态势感知的促进作用

测试数据融合与威胁预警模型在林业网络安全态势感知中发挥着关键的促进作用。通过对来自渗透测试、入侵检测、日志监控、流量分析等多源异构数据的融合处理，可以有效消除信息孤岛与冗余数据，实现对安全事件的全面、准确刻画；同时，融合后的数据能够为威胁预警模型提供更丰富、更高质量的输入，提升模型在攻击特征识别、风险等级评估和异常行为预测方面的精度与可靠性。借助机器学习、模式识别等智能分析方法，威胁预警模型能够提前发现潜在攻击链和隐蔽性安全风险，从而在态势感知体系中实现由事后响应向事前预防的转变。这不仅显著缩短了威胁处置的响应时间，还增强了林业信息系统抵御复杂网络攻击的主动防御能力，为林业业务的安全、稳定与高效运行提供了有力支撑。

3 林业网络安全态势感知中渗透测试数据融合与威胁预警模型构建难点

3.1 渗透路径复杂多样，数据融合困难重重

林业网络系统涉及众多设备与应用，渗透路径表现出高度的复杂性和多样性，涵盖物联网终端、云平台、传感网络等多层级结构。不同渗透路径所产生的测试数据格式、粒度和内容差异显著，导致数据融合过程中面临标准化不足和兼容性差的问题。数据来源的异构性使得对渗透行为的全面捕捉和分析变得极为复杂，往往出现信息碎片化与重复冗余。此外，渗透测试过程中的大量无效或噪声数据增加了后续融合与处理的难度，影响数据质量。如何在保持数据完整性和时效性的同时，有效整合多样渗透路径的测试结果，成为实现准确态势感知的首要技术挑战[2]。

3.2 攻击手法层出不穷，模型适配难以统一

网络攻击手段不断演进，从传统的漏洞利用到高级持续威胁，再到针对林业特殊环境设计的定制化攻击，手法多样且变化快速。威胁预警模型需应对不同攻击策略的多样化表现，这对模型的通用性和适配能力提出了严苛要求。统一构建一个既能覆盖多类型攻击，又能保持高识别率和低误报率的预警模型，面临显著困难。模型训练依赖大量标注样本，而新型攻击样本稀缺，使得模型更新和泛化能力受限。模型结构需具备高度灵活性，以适应不断涌现的攻击变种，但如何保证模型稳定性与适应性之间的平衡，仍是当前亟待解决的问题。

3.3 威胁特征动态演变，感知精度难以保障

网络环境及攻击手段的动态变化导致威胁特征不断演变，传统静态特征提取方法难以捕捉新兴威胁的微妙差异。林业网络系统中设备多样、运行环境复杂，使得威胁特征呈现高度时变性和非线性，给态势感知的准确性带来挑战。感知模型需持续学习和更新，以适应环境变化和攻击策略的演进，但实时更新机制受限于计算资源和数据采集效率。特征变化若未被及时捕获，容易导致误判或漏警，影响整体安全防护效果。实现对动态威胁特征的精准识别，是提升态势感知精度的关键所在。

3.4 异构数据时效不一，决策响应延迟明显

林业网络安全监测涉及多种异构数据源，其数据生成频率和传输时延存在较大差异，导致融合数据的时效性难以统一保障。部分关键数据如实时流量日志需秒级响应，而设备状态信息和历史记录更新频率较低，融合后信息的时序一致性难以保证。时效不一直接影响威胁预警模型的响应速度和决策准确性，延迟增加可能使安全事件发展为严重风险，削弱防御效果。构建高效的数据同步与融合机制，确保融合数据能够及时反映当前态势，是缩短决策响应时间的重要前提[3]。

3.5 安全场景边界模糊，预警标准尚待规范

林业网络安全覆盖面广，涉及生态监测、资源管理、设备维护等多个业务场景，安全边界界定复杂且常呈交叉重叠状态。不同场景对安全事件的敏感度和响应要求差异显著，缺乏统一的预警标准和评价体系，导致威胁预警结果难以实现跨场景的有效共享和对接。边界模糊使得预警模型在判定事件严重性和紧急程度时存在主观性，增加了误报和漏报的风险。同时，缺乏行业统一的安全指标体系限制了预警模型的标准化建设与性能评估，制约了态势感知能力的提升。明确安全场景边界，构建科学合理的预警规范成为提升林业网络安全防护水平的必经之路。

4 林业网络安全态势感知中渗透测试数据融合与威胁预警模型构建路径

4.1 强化渗透测试体系，拓展数据采集维度

完善渗透测试体系是构建高效态势感知的基础。通过设计多层次、多类型的测试策略，覆盖林业网络系统中的关键节点与潜在薄弱环节，能够全面挖掘系统脆弱性。扩展数据采集的维度，不仅关注传统的网络层与应用层漏洞，还应涵盖设备层物联网节点与边缘计算平台的安全状况。多维度数据采集增强了对潜在攻击路径的感知深度，为后续数据融合和威胁分析提供丰富信息支持。建立标准化的渗透测试流程与数据格式规范，有助于提高测试结果的可比性和适用性，为融合分析奠定坚实基础。

比如，在“智慧林业安全评估”项目中，工作人员需要设计并实施覆盖林业物联网传感器、边缘计算节点、无线通信设备及核心管理平台的多层次、多维度渗透测试方案。该方案不仅包括网络层面的漏洞扫描，还针对设备固件、操作系统和通信协议开展专项安全检测，全面揭示潜在风险。项目中建立了标准化的数据采集流程，统一规范不同测试阶段产生的数据格式和内容，保证数据兼容性和完整性。通过扩展采集维度，项目有效挖掘了传统测试难以覆盖的薄弱环节，提升了测试深度与广度。同时，工作人员指导学生结合实际场景，灵活调整测试策略，实现针对性与全面性的有机融合，为态势感知系统提供了详实、丰富的基础数据支撑。

4.2 整合多源异构数据，构建融合分析框架

针对林业网络安全态势感知中的异构数据特点，应构建统一的融合分析框架。该框架需实现对来自渗透测试、流量监控、日志记录及入侵检测等多源数据的有效整合，通过数据预处理、清洗与格式转换，消除冗余和不一致性。融合过程强调语义关联和时序一致性的维护，确保不同数据间的协同分析。通过设计分层融合结构，将低层原始数据与高层抽象信息相结合，提高整体信息表达的准确性和完整性。该框架为威胁预警模型提供稳定、全面的数据支撑，实现信息价值的最大化利用[4]。

比如，在“林业网络综合安全监测”项目中，工作人员指导团队将来自流量采集设备、系统日志、入侵检测系统和渗透测试工具的多种异构数据进行融合。通过数据预处理模块对原始数据进行清洗、缺失值补全和格式统一，解决不同数据源格式不一致及时间戳错位的问题。项目构建了分层融合分析框架，将低层原始数据与高层抽象信息有机结合，实现多维度信息的协同表达和关联挖掘。该框架强调语义层次的统一和时序关联，提升融合数据的准确性和完整性。工作人员注重引导团队探索数据融合的关键技术，保证融合结果的质量和可用性，为后续威胁预警模型提供了坚实可靠的基础。

4.3 提炼关键威胁特征，优化模型输入结构

从融合后的数据中提炼具备代表性和区分力的威胁特征，是提升模型性能的关键环节。通过特征选择与降维技术，筛除无关或冗余信息，保留反映攻击行为本质的核心指标，增强模型训练的有效性。构建合理的模型输入结构，不仅应涵盖静态特征，还需引入动态变化的时序特征，以捕捉攻击演进的过程性信息。特征表达需兼顾多维度信息融合，提升模型对复杂威胁模式的识别能力。优化后的输入结构能够减少计算复杂度，提升预警模型的响应效率和准确性[5]。

比如，在“林业网络威胁识别优化”项目中，工作人员带领学生通过统计分析和机器学习方法，针对融合后的高维海量数据集提炼出具有强区分力的威胁特征。项目采用主成分分析、互信息法等降维技术，去除冗余与无关特征，保留反映攻击行为本质的关键指标。此外，构建了融合静态特征与动态时序特征的多维输入结构，以捕捉攻击的时间演进特征和行为模式。工作人员指导团队结合林业网络安全实际需求，设计模型输入形式兼顾多源信息融合与计算效率，确保模型训练时对复杂威胁的识别能力得到显著提升。优化后的输入结构有效降低了

计算资源消耗，提高了预警模型的实时响应能力[6]。

4.4 引入智能算法机制，提升预警精准水平

应用先进的智能算法，诸如深度学习、强化学习及集成学习方法，能够显著提升威胁预警的精准度。算法需具备自适应能力，能够动态调整参数以应对攻击手法的多样化和演变。结合监督与无监督学习，增强模型对未知威胁的识别能力。引入注意力机制和多任务学习策略，有效挖掘特征间的复杂关联性，提升异常行为检测的灵敏度与鲁棒性。智能算法机制的引入推动预警模型从传统规则依赖向数据驱动转变，实现主动防御与精准预警的高度融合。

比如，在“林业安全智能预警”项目中，工作人员引导学生应用深度神经网络、集成学习和强化学习等多种智能算法，构建兼具鲁棒性和自适应性的威胁预警模型。项目结合监督学习与无监督学习技术，不断提升模型对新型未知攻击的检测能力。通过引入注意力机制，有效捕捉特征间的复杂关联性，增强异常行为识别的灵敏度和准确性。多任务学习框架帮助模型同时优化多个安全指标，降低误报和漏报风险。工作人员注重模型训练与调优的科学方法，推动预警模型由规则驱动向数据驱动转变，实现对林业网络环境中多样化、动态变化威胁的精准识别与响应[7]。

4.5 构建动态感知平台，实现联动响应闭环

构建集成化动态态势感知平台，实现从数据采集、融合分析到威胁预警和响应的闭环管理。平台需支持实时数据流处理，确保态势信息的时效性和连续性。通过模块化设计，融合多种感知手段和预警模型，提升系统灵活性和扩展能力。实现预警信息的自动传递与联动处置，缩短响应时间，增强安全事件的处置效果。动态感知平台应支持持续学习与自我优化，适应环境和威胁变化，推动林业网络安全防护由静态防御向智能化、动态化转变，保障林业信息系统的稳定安全运行。

比如，在“智慧林业动态安全感知平台”项目中，工作人员负责统筹设计一个集数据采集、融合分析、威胁预警与事件响应于一体的集成化平台。平台支持实时流数据处理，确保态势信息时效性与连续性，利用模块化设计实现各功能组件灵活组合和升级扩展。该系统建立了自动化预警触发机制，预警信息能够快速传递至防护设备和管理人员，形成闭环联动响应。工作人员指导团队开发持续学习与自适应优化模块，使平台能够根据环境变化和攻击演变不断调整策略，提升防护能力。该动态感知平台有效缩短安全事件的检测和响应时间，为林业信息系统提供了智能化、动态化的安全保障体系[8]。

5 结语

综上所述，本文主要研究了林业网络安全态势感知中渗透测试数据融合与威胁预警模型的构建方法。针对林业网络环境复杂多样、攻击手法多变等挑战，提出了强化渗透测试体系、整合多源异构数据、提炼关键威胁特征、引入智能算法以及构建动态感知平台的系统路径。通过多维度数据融合与智能分析，实现了对潜在威胁的高效识别和精准预警，提升了林业信息系统的安全防护能力。研究成果为推动林业网络安全防护由被动防御向主动感知和动态响应转变提供了理论基础和技术支持，具有重要的应用价值和实践意义。

参考文献

[1] 杨小漩. 人工智能在林业有害生物防治中的应用与效率提升研究[J].中国林业产业,2025,(05):107-108.

[2] 张颂.基于数据融合的森林地表凋落物含水率预测方法研究[D].东北林业大学,2024.

[3] 吴喜凯.基于 WSN 的林业土壤数据采集系统设计与实现[D].桂林理工大学,2023.

[4] 庞士军.基于双目视频数据融合的森林火灾监测研究[D].中南林业科技大学,2022.

[5] 孙晓宇.基于无人机影像与高程数据融合的煤矿矿区地物提取方法研究[D].北京林业大学,2021.

[6] 李健平.多源数据融合的低空无人机激光扫描平台自主定位定姿关键技术[D].武汉大学,2021.

[7] 陈东鹏.林业背包式激光雷达多传感器集成系统及数据融合的研究[D].东北林业大学,2021.

[8] 郑明智.基于数据融合技术的程控交换机温度无线监控系统研究[D].东北林业大学,2009.