

智慧校园背景下网络安全态势感知平台建设实践

马永新

天津商业大学, 天津 300134

DOI: 10.61369/ETR.2026210012

摘 要 : 随着信息技术的高速发展, 智慧校园建设已成为推动教育数字化转型的重要举措, 校园网络规模不断增加, 应用场景也逐渐变得更丰富, 其具有教学科研、师生服务等功能, 而网络安全风险也具有隐蔽性的特征。网络安全态势感知平台作为智慧校园安全防护体系的重要枢纽, 能够实现对校园网络安全风险的精准化监测, 从而为智慧校园健康发展奠定坚实的基础。基于此, 本文结合智慧校园建设的核心需求, 深入分析网络安全态势感知平台的内涵和建设价值, 深入分析当前校园网络安全态势感知建设的问题, 为各类智慧校园网络安全态势感知平台建设提供支持。

关 键 词 : 智慧校园; 网络安全; 态势感知; 平台建设

Practice on the Construction of Network Security Situation Awareness Platform Under the Background of Smart Campus

Ma Yongxin

Tianjin University of Commerce, Tianjin 300134

Abstract : With the rapid development of information technology, the construction of smart campuses has become an important measure to advance the digital transformation of education. The scale of campus networks continues to expand and application scenarios are gradually enriched, undertaking functions such as teaching and scientific research as well as services for teachers and students. Meanwhile, network security risks present obvious concealment characteristics. As an important hub of the smart campus security protection system, the network security situation awareness platform enables accurate monitoring of campus network security risks, thereby laying a solid foundation for the sound development of smart campuses. Based on the core demands of smart campus construction, this paper deeply analyzes the connotation and construction value of the network security situation awareness platform, explores the existing problems in the current construction of campus network security situation awareness, and provides references and support for the construction of similar platforms in various smart campuses.

Keywords : smart campus; network security; situation awareness; platform construction

前言

在教育数字化背景下, 智慧校园建设步入高质量发展的关键时期。云计算、大数据等多样化的技术手段应用于教育、管理的全方位, 形成了协同共联的校园生态体系。智慧校园的核心在于数据驱动, 校园网络作为数据传输、储存和交互的重要渠道, 以业务系统、终端设备作为枢纽, 其安全稳定运行也直接关系着教育的秩序, 影响着教育数字化转型工作的开展。网络安全态势感知平台能够通过校园网络中的各类安全数据, 运用大数据分析和人工智能技术, 对网络流量、终端设备和业务系统进行监测, 有助于精准识别安全风险, 为校园安全管理提供支持。

一、智慧校园背景下网络安全态势感知平台建设的价值

(一) 筑牢智慧校园安全屏障

智慧校园中的教学科研系统、学生管理系统、财务系统等核心业务系统, 涉及到大量的数据信息, 如果发生安全事件则会直接影响教学工作开展的秩序性。态势感知平台能够监测业务系统

的运行情况, 当发现恶意入侵和数据泄漏的问题时, 可以通过快速处置安全事件, 避免安全风险的扩散, 进而保障校园核心业务的有效运行, 为智慧教学, 智能管理提供保障^[1]。

(二) 实现安全风险精准管控

传统校园网络安全管理主要通过人工监控的方式进行, 效率不高, 并且无法发现隐蔽的风险。态势感知平台则可以通过智能化的技术对安全风险进行采集和分析, 从而识别到风险的源头、

风险的等级和其影响范围，帮助管理人员尽快聚焦高价值威胁，避免无效告警干预，大幅提升安全风险管控的精准度^[3]。包括部分高校的态势感知平台通过智能分诊技术，能够确保消除绝大多数的告警噪声，这也有效缓解了管理人员的告警疲惫。

（三）完善安全管理体系

态势感知平台能够充分整合校园各类安全资源，从而保障安全数据的有效管理，确保打破传统的信息孤岛局限，构建更加系统而完善的安全管理机制。在此期间，对安全数据展开分析，能够为校园网络管理提供数据上的支持，并掌握安全态势的变化情况，优化安全防护策略，进而推动校园网络安全管理实现转型升级，确保提升安全管理的有效性。

（四）保障师生信息安全

在智慧校园中，师生个人的信息、学术成果以及财务信息数据量相对较大，如果发生泄露问题将直接影响师生的合法权益，影响校园的稳定性。态势感知则能够通过监控数据的方式实现信息传输，在使用过程中如果出现安全风险，则需要及时发现数据泄露的问题，采取加密与拦截的方式，保障师生数据信息的敏感性，增强师生对智慧校园建设的信任度，并营造良好的校园氛围。

二、智慧校园背景下网络安全态势感知平台的整体架构

（一）数据采集层

作为平台的基础层，其核心功能是实现校园网络全场景安全信息的数据采集，消除监测盲区。采集范围涉及到校园局域网、无线网络、物联网终端、师生移动终端等所有网络节点，采集数据的类型包括网络流量数据、安全日志数据等。在采集的过程中，利用 Agent 采集 + 端口镜像 + API 对接相结合的方式，针对不同类型的设备进行采集，采用合适的采集方式，对终端设备、物联网设备采用 Agent 轻量化采集，降低对终端性能的影响。对网络设备、安全设备采用端口镜像采集，从而实现流量和日志的全面捕捉。对业务系统采用 API 实现全面的数据对接，确保信息的同步性。在此期间，建立统一的数据采集规范，明确不同类型数据的采集频率和格式标准，确保数据信息的完整性和精准性^[3]。

（二）数据预处理层

对采集到的数据进行有效处理，其原理是对数据进行清洗、标准化、融合与储存，为后续的态势分析研判提供精准的数据保障。首先，对数据进行清洗，去除无效数据、重复数据和异常数据，保障数据的精准性。其次，按照统一的数据标准，对不同格式、不同类型的数据信息进行有效处理，将非结构化的数据、半结构化数据转化为结构化数据，从而实现数据的有效统一。再次，通过数据融合技术，将来自不同采集渠道、不同类型的数据进行有效整合，解决信息孤岛的问题，挖掘数据之间的内在联系。最后，通过采用分布式储存 + 本地备份相结合的储存模式，利用分布式储存技术满足海量安全信息的储存需求，确保数据信息的有效获取。

（三）态势分析研判层

作为平台的核心层，其功能在于运用智能化技术，对处理后的安全数据进行有效分析，从而更好地实现安全态势的理解、风险识别和趋势预测。这个层次涉及到三个核心模块，主要包括以下几方面：一是基础分析模块，能够通过统计分析、特征提取等技术，对网络流量、中断状态和业务系统运行的情况进行常态化的分析，从而掌握网络的运行态势。二是风险识别模块。通过融入大数据分析、机器学习、关联分析等技术，结合 MITRE ATTCK 战术技术知识库与最新的威胁情报，构建多维度的风险识别模式，精准识别网络攻击、数据异常等问题，明确风险源头和其影响的范围^[4]。三是趋势预测模块。根据历史安全数据和威胁的情报，对当前的安全态势运用时间序列进行分析，提前识别潜在的安全风险，为防御提供支持。

（四）预警处置层

承接态势分析研判层的结果，核心功能是保障安全风险精准预警和快速处置，确保实现防护的闭环。预警模块应结合风险等级，采用分级预警机制。对一般风险通过平台消息、邮件等方式提醒管理人员进行关注。对高风险通过短信、平台弹窗的方式进行有效预警，要求管理人员限期进行处理。对严重风险应立即启动紧急预警机制，确保同步通知校园网络中心、保卫处等部门，启动应急处置流程。预警信息应明确其类型、等级和影响范围，为管理人员的快速处置提供帮助。

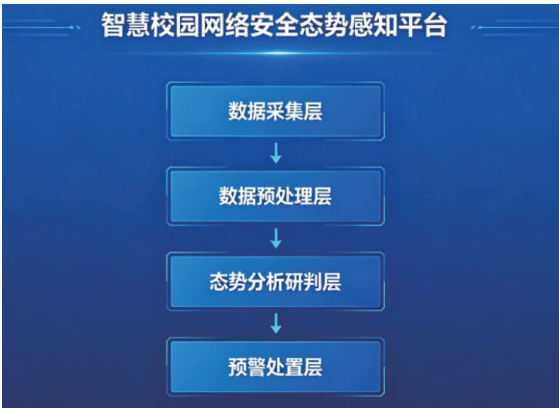


图 智慧校园网络安全态势感知平台

三、智慧校园背景下网络安全态势感知平台建设实践路径

（一）推动数据整合，实现全领域感知覆盖

打破传统的局限，构建统一的安全数据资源库，从而实现全面感知。一是拓宽数据采集的渠道，实现全面覆盖校园网络基础设施、终端设备、业务系统等场所，补充移动终端、师生上网行为和第三方威胁情报等数据采集。针对中小学物联网终端，数量较少的特点，采用轻量化采集方式，降低部署的成本。针对高校网络规模大、设备类型多的特点，优化和完善采集的策略，确保数据信息的有效性。二是统一数据标准，制定更加系统而完善的网络安全数据规范，明确数据的格式、采集频率等要素，推动不同部门、不同系

统的数据实现标准化改造。三是强化数据融合处理工作，引入数据融合技术，对采集到的数据进行关联分析，挖掘数据之间的内在联系和结构，确保更好地提升数据的使用价值^[5]。

表 智慧校园网络安全态势感知平台建设实践路径及核心举措

建设路径	核心建设内容	关键建设目标	实施重点
数据整合与全域感知	拓宽采集渠道、统一数据标准、多源数据融合	消除监测盲区，打破信息孤岛	覆盖校园网络、物联网终端、业务系统、外部威胁情报
智能化技术升级	引入大数据与AI、优化预警模型、自动化处置	降低误报漏报，提升隐蔽威胁识别能力	机器学习建模、威胁情报联动、自动脚本处置
管理体系优化	完善制度、专业人才培养、常态化运维	实现技术与管理协同落地	岗位职责划分、安全制度建设、定期演练培训
全域协同防护	校内多部门联动、校外政企警联动	构建一体化联防体系	安全信息共享、应急资源互通、威胁同步预警

（二）强化技术升级，提升智能化分析能力

聚焦平台智能化建设的短板，加大技术上的支持和投入，提升分析预警和预警处置的智能化水平。一是注重引进先进的数据技术，融合大数据分析、机器学习等技术，构建智能化的分析研判机制，确保提升对隐蔽性、复杂性安全风险的识别能力。二是优化预警模型，并结合历史安全数据和威胁情报，不断训练和优化预警模型，尽量降低误报率、漏报率，确保实现精准预警。构建预警分级机制，并结合风险等级进行差异化的预警处理，确保提升预警工作的成效^[6]。三是推进处置流程自动化工作，针对常见的安全风险，开发自动处理脚本，实现病毒清除、账号锁定、异常流量拦截的操作，提升处置的成效。针对复杂的安全事件，提供处置流程指引和辅助工具，辅助管理人员进行有效地处置。

（三）优化管理体系，推动技术与管理融合

解决重视技术而轻视管理的问题，确保两方面的协同性。一是完善安全管理体系，根据校园的实际制定平台运行维护、管理

数据、应急处置等有关制度。明确各部门、各岗位之间的职责，确保平台操作的流程合理。例如，制定数据保密制度，规范安全数据的信息储存，确保数据信息有效使用^[7]。二是注重加强人才培养，构建校园网络安全管理团队，定期开展技术培训和应急演练，提升管理人员的平台操作、风险研判能力，提高应急处置能力。与高校、安全厂商进行合作，开展定制化的培训，引入外部的技术专家作为指导，提升团队的整体水平。三是构建常态化的运维机制，安全部门派专业运维人员对平台进行日常的监管和维护，及时发现平台存在的问题，确保平台运行的稳定性，提升平台的安全性^[8]。

（四）健全协同机制，提升全域联动防护能力

学校应注重建立协同性的防护体系，才能保障整体的安全性。一是加强校内协同，构建校园网络中心、教务处、学生处和保卫处等各部门之间的协同配合机制，明确各部门之间的安全职责，构建安全信息共享体系，确保实现安全态势、预警信息的有效处理。二是完善校外联动机制，与当地网络安全部门、运营商、安全厂商构建联动机制，及时获取全新的威胁情报，通过技术支持获取应急处置资源^[9-10]。

四、结语

综上所述，在智慧校园背景下，网络安全态势感知平台是完善校园安全防护体系，保障教育数字化转型的关键。其建设的质量直接影响着校园的网络安全。为此，这就需要加强智慧校园背景下网络安全态势感知平台的建设，构建完善的管理体系。在教育数字化的背景下，智慧校园网络架构将更加复杂，网络安全威胁也将持续增加，网络安全态势感知平台的建设也面临全新的挑战。这就需要不断优化和完善技术，建立健全协同防护机制，提升平台的智能化，分享建设的经验，为教育数字化转型建设网络安全的屏障。

参考文献

[1] 田文君, 王罕. 智慧校园网络安全运营体系的构建 [J]. 办公自动化, 2025, 30(06): 37-39.
[2] 袁策书, 蔡朝辉, 张传超, 等. 基于数据中台的智慧校园安全建设研究 [J]. 网络安全和信息化, 2025, (02): 115-117.
[3] 邵炜炜. 5G 物联网移动通信技术在安全智慧校园中的应用 [J]. 信息与电脑, 2025, 37(01): 83-85.
[4] 范俊. 构建智慧校园新生态——安徽医科大学信息化建设“八个一”工程实践 [J]. 教育信息化论坛, 2025, (01): 31-33.
[5] 辛亦轩, 邓谦, 刘姣, 等. 基于 5G 的智慧校园网络安全态势感知研究 [J]. 电信快报, 2024, (03): 39-43.
[6] 石莉. 基于 5G 的校园网络安全态势评估分析 [J]. 电子技术与软件工程, 2022, (22): 40-44.
[7] 李萌昕. 高校智慧校园建设中的网络安全建设现状与分析——以山东大学为例 [J]. 电脑知识与技术, 2022, 18(07): 31-33.
[8] 陈迎春. 基于智慧校园的网络态势指标体系研究 [J]. 青海科技, 2022, 29(01): 157-160.
[9] 曹鲁喆. 基于深度学习的校园网络安全态势要素提取与评估方法研究 [D]. 中国人民公安大学, 2021.
[10] 陈锴. 智慧校园环境中网络态势感知系统的构建 [J]. 电子技术与软件工程, 2018, (22): 17-18.