 DOI: https://doi.org/10.12349/iser.v7i3.9471

Construction of a High-level Persistent Threat Monitoring System for the Natural Resources Database

Xiaojuan Ma[1] Nan Su[2] Zhipeng Tian[3] Shanshan Ye[1]

1. Natural Resources Information Center of Ningxia Hui Autonomous Region, Yinchuan, Ningxia, 750000, China
2. National Computer Network Emergency Response Technical Team/Coordination Center Ningxia Branch, Yinchuan, Ningxia, 750000, China
3. Ningxia Hui Autonomous Region Ecological Environment Information and Emergency Center, Yinchuan, Ningxia, 750000, China

Abstract

Advanced Persistent Threats pose a severe challenge to the secure operation of natural resource databases. Their characteristics of concealment, persistence, and destructiveness can easily lead to data leakage, tampering, and system paralysis, threatening national resource security and the effectiveness of ecological governance. To build a scientific and efficient monitoring system, it is necessary to integrate multi-source data fusion, intelligent recognition algorithms, and dynamic protection mechanisms to achieve real-time perception, precise positioning, and rapid response to threat behaviors. By establishing a multi-dimensional monitoring indicator system, integrating various types of information such as network traffic, data access logs, and system behaviors, and combining intelligent analysis technology to identify abnormal patterns, a closed-loop management of "perception - analysis - response - optimization" can be formed. This system can effectively enhance the defense capabilities of natural resource databases against advanced persistent threats, ensuring data integrity, confidentiality, and availability, and providing security support for the digital transformation of natural resource management.

Keywords

Natural resource database; Advanced Persistent Threat; Monitoring system; Data security; Intelligent protection

自然资源数据库构建高级持续性威胁监测体系

马晓娟[1] 苏楠[2] 田志鹏[3] 叶姗姗[1]

1. 宁夏回族自治区自然资源信息中心，中国 · 宁夏 银川 750000
2. 国家计算机网络应急技术处理协调中心宁夏分中心，中国 · 宁夏 银川 750000
3. 宁夏回族自治区生态环境信息与应急中心，中国 · 宁夏 银川 750000

摘 要

高级持续性威胁对自然资源数据库的安全运行构成严峻挑战，其隐蔽性、持续性及破坏性特征，易导致数据泄露、篡改与系统瘫痪，威胁国家资源安全与生态治理效能。构建科学高效的监测体系，需融合多源数据融合、智能识别算法与动态防护机制，实现对威胁行为的实时感知、精准定位与快速响应。通过搭建多维度监测指标体系，整合网络流量、数据访问日志、系统行为等多类信息，结合智能分析技术对异常模式进行识别，形成“感知-分析-响应-优化”的闭环管理。该体系可有效提升自然资源数据库对高级持续性威胁的防御能力，保障数据完整性、保密性与可用性，为自然资源管理数字化转型提供安全支撑。

关键词

自然资源数据库；高级持续性威胁；监测体系；数据安全；智能防护

1 引言

在数字化技术深度融入自然资源管理领域的进程中，数据库已然成为承载、管控与解析资源数据的核心平台，其稳定运行直接影响着资源治理的科学性与公信力。高级持续性威胁持续迭代，令数据库直面隐蔽入侵、长期潜伏、深度破坏等一系列风险，传统安全防护方式难以匹配其复杂特性与持续威胁态势。构建契合自然资源数据库特质的高级持续性威胁监测体系，成为保障数据安全、维系资源管理秩序的核心任务，亟待从技术与管理两个维度开展系统性探究。

【基金项目】宁夏自然资源科技创新资金支持“宁夏自然资源业务系统被攻击画像识别技术研究”（项目编号：ZRZYTKY202501004）。

【作者简介】马晓娟（1989–），女，回族，中国宁夏同心人，本科，高级工程师，从事信息化网络安全研究。

2 自然资源数据库高级持续性威胁的现存问题

2.1 威胁行为隐蔽性与持续性加剧监测难度

高级持续性威胁针对自然资源数据库的攻击具备显著的隐蔽渗透与长期潜伏特性，其行为轨迹和正常业务操作高度重合，很难依靠单一特征匹配来识别。攻击者常利用合法的资源管理系统接口、数据交换协议或第三方工具，凭借零日漏洞或未授权访问手段逐步渗透，在数据库系统内搭建隐蔽控制通道，达成数据的长期窃取与篡改 [1]。这类威胁的持续性不只是攻击周期的延长，更体现在对数据库底层架构的深度植入，攻击者通过修改存储过程、植入恶意脚本或调整数据索引，让威胁行为在不触发明显告警的情况下持续存在，形成“潜伏 - 探测 - 破坏”的渐进式攻击链条，对监测体系的实时表现与精准程度提出极高要求。

2.2 监测指标体系覆盖不全存在识别盲区

自然资源数据库融合地理信息、资源权属、生态环境等多类敏感数据，威胁场景复杂多样，但当前监测体系存在指标覆盖不全问题。数据层面上，攻击者会通过窃取、篡改、伪造等手段破坏数据完整性，或借权限提升、越权访问获取敏感资源信息，需依托数据访问日志、操作审计记录、数据哈希校验等多维度指标开展监测；系统层面上，数据库运行状态、网络流量、进程行为等参数出现异常波动，可能暗示攻击者已实施渗透或破坏行为，需搭建实时系统状态监测指标。现有监测手段仅关注单一网络流量或权限管理维度，缺乏对数据全生命周期、系统底层架构及业务逻辑的多维度指标整合，使得对高级持续性威胁的识别存在明显盲区。

2.3 传统防护手段难以应对高级威胁

传统安全防护手段像防火墙、入侵检测系统、访问控制列表等，在应对高级持续性威胁时有着明显局限。防火墙与访问控制列表依靠端口、地址等静态规则开展访问控制，很难识别动态策略攻击行为；入侵检测系统依托已知攻击特征库，对零日漏洞或变种攻击的识别能力不足，容易出现漏报或误报。自然资源数据库的业务特性要求数据具备高可用性与实时性，传统防护手段的部署会增加系统负载，影响数据查询与分析效率，造成“安全与效率”的矛盾。高级持续性威胁的攻击行为有着强适应性，能够绕过传统防护机制、修改攻击特征持续发起攻击，使得传统防护手段无法形成有效防御闭环，难以满足数据库长期安全运行的需求。

2.4 数据泄露篡改对资源管理影响加剧

自然资源数据库中的数据涉及土地资源、矿产资源、水资源等核心资源的权属信息、分布情况、开发利用规划等敏感内容，一旦出现数据泄露或篡改，会直接影响资源管理的科学性与权威性。高级持续性威胁的攻击目标包含数据窃取，还涵盖恶意篡改，修改资源权属信息、伪造生态环境监测数据等，这类行为会造成资源管理决策失误，甚至引发社会矛盾。数据泄露的隐蔽性让相关事件往往难以被及时察觉，等到察觉时攻击者已完成数据转移与销毁，形成不可逆损失。数据泄露还可能使国家资源安全面临风险，尤其是跨境资源数据、战略资源数据等敏感领域，高级持续性威胁的攻击行为会对国家资源安全与生态治理效能构成严重威胁。

3 自然资源数据库高级持续性威胁监测体系构建路径

3.1 搭建多源数据融合监测指标体系

监测指标体系是构建高级持续性威胁监测体系的核心基础，需结合自然资源数据库业务特性与威胁场景，构建多维度、全链条的监测指标体系 [2]。数据层指标涵盖数据访问日志、数据修改记录、数据传输流量、数据哈希值等，对数据全生命周期开展监测，实现对数据窃取、篡改、伪造等行为的识别；系统层指标包括数据库运行状态、进程行为、网络流量、权限配置等，对系统底层架构开展监测，实现对攻击者渗透、植入恶意脚本等行为的感知；业务层指标涵盖资源管理业务操作流程、数据查询频率、业务逻辑异常等，对业务逻辑开展监测，实现对攻击者利用业务漏洞攻击的识别。通过数据访问日志与系统权限配置的关联分析，识别未授权访问、越权访问等异常行为；通过数据传输流量与业务操作频率的关联分析，识别数据窃取、批量导出等异常行为。结合威胁情报数据，对监测指标动态调整，及时纳入新的威胁场景与攻击特征，确保指标体系的全面性与时效性。

3.2 智能识别机制构建

为实现对高级持续性威胁的精准识别，需构建基于智能分析的异常行为识别机制，通过多源监测数据分析，识别与正常行为存在显著差异的异常模式。该机制以多源数据融合指标体系为基础，整合网络流量、系统日志、业务操作等多类信息，形成覆盖数据、系统、业务的立体化监测维度。智能识别机制的核心在于构建异常行为特征库，通过对历史威胁数据的深度分析，提炼出未授权访问、数据篡改、恶意脚本植入等典型攻击行为的特征参数。该机制引入自适应分析算法，对实时监测数据进行动态比对，通过算法对数据访问、系统运行、业务操作等维度的参数进行实时分析，快速识别偏离正常行为模式的异常信号 [3]。为提升识别效果，需建立特征库动态更新机制，结合威胁情报的最新动态，及时将新型攻击行为的特征参数纳入识别体系，确保机制能够适应高级持续性威胁的演化趋势，有效弥补传统监测手段的识别盲区。

3.3 动态防护机制设计与部署

动态防护机制是实现对高级持续性威胁快速响应的核心，需结合监测体系运行状态，设计并部署具备自适应能力的动态防护机制。防护策略制定遵循“最小权限”“最小暴露”原则，通过优化数据库权限配置，限制用户访问权限，规避因权限过大引发的安全风险。动态防护机制拥有实时响应能力，监测到异常行为后会自动触发防护策略，阻断威胁行为持续发展。监测到未授权访问行为时，系统自动锁定相关账

户，限制其访问权限；监测到数据篡改行为时，系统自动恢复数据原始状态，并触发告警机制。动态防护机制具备自适应能力，能够依据威胁行为演化趋势，自动调整防护策略，增强防护的针对性与有效性。防护机制部署进程中，结合数据库业务特性，采用分层防护策略，在网络层、系统层、应用层等多个层面部署防护措施。网络层部署入侵检测系统、防火墙等设备，实现网络流量的实时监测与过滤；系统层部署终端防护软件、漏洞扫描工具等，实现系统漏洞的及时修复与防护；应用层部署数据加密、访问控制等技术，实现数据的安全保护。

3.4 闭环管理体系构建

为实现对高级持续性威胁的全生命周期管理，需构建“感知 - 分析 - 响应 - 优化”的闭环管理体系，形成监测体系的持续改进机制。感知层是监测体系的基础，通过多源数据融合与智能识别机制，实现对威胁行为的实时感知；分析层是监测体系的核心，对感知到的异常行为进行深度分析，确定威胁的类型、来源、影响范围等信息；响应层是监测体系的关键，根据分析结果采取相应防护措施，阻断威胁行为进一步发展；优化层是监测体系的保障，对监测体系的运行效果进行评估与优化，提升监测体系的性能与安全性。同时建立监测体系评估机制，定期对监测体系的运行效果进行评估，包括识别准确率、响应时间、防护效果等指标，根据评估结果对监测体系进行优化与改进，提升监测体系的性能与安全性。

4 监测体系的应用成效

4.1 威胁识别能力与响应效率显著提升

监测体系的构建与应用，让自然资源数据库对高级持续性威胁的识别能力与响应效率实现显著提升。该体系依托多源数据融合与智能识别机制的协同运作，能够精准捕捉隐蔽性强、持续性久的威胁行为，实现对未授权访问、数据篡改、恶意脚本植入等典型攻击行为的有效识别，有效弥补了传统监测手段的识别盲区。在响应效率层面，体系可实现对异常行为的实时感知与快速处置，在威胁行为初期阶段即可阻断其进一步发展，大幅缩短了威胁处置的时间周期，有效降低了数据泄露与系统瘫痪的风险，提升了数据库安全防护的时效性与主动性。

4.2 数据安全防护能力全面增强

监测体系落地实施，全面增强了自然资源数据库的安全防护能力。数据安全层面，体系覆盖数据采集、传输、存储、使用等全生命周期环节，通过对数据访问、修改、传输等行为的实时监测，有效防止数据窃取、篡改与伪造，保障数据的完整性、保密性与可用性。系统安全层面，体系可实时监测数据库运行状态与系统漏洞，及时发现并预警潜在风险，助力相关部门快速修复漏洞，避免攻击者利用漏洞实施渗透攻击。权限管理层面，体系通过对用户权限的精细化管控，实现最小权限原则的落地，有效规避因权限过大引发的安全风险，构建起多层次、全方位的数据安全防护屏障。

4.3 资源管理业务稳定性与可靠性提升

监测体系的应用为自然资源数据库的安全稳定运行提供了坚实保障，显著提升了资源管理业务的稳定性与可靠性。业务稳定性方面，体系实时监测数据库运行状态，能够及时发现并处置系统异常，有效避免因系统故障导致的业务中断，保障了资源管理工作的连续性。业务可靠性方面，体系通过对数据完整性与准确性的严格把控，有效防止数据篡改与伪造，确保资源管理业务决策依据的真实性与可靠性，为资源规划、权属管理、生态治理等工作提供了精准的数据支撑。体系构建的安全运行环境，进一步提升了业务处理的效率与质量，推动资源管理工作的规范化与高效化。

4.4 应急处置能力与风险预警水平提高

监测体系的应用，大幅提升了自然资源数据库的应急处置能力与风险预警水平。在应急处置方面，体系可快速响应威胁事件，通过自动化防护策略的触发，及时阻断威胁行为的蔓延，有效降低事件造成的损失。在风险预警方面，体系能够实时监测数据库运行状态与威胁行为演化趋势，提前识别潜在安全风险并发出预警，为资源管理部门提供及时的风险提示，便于相关部门提前制定防护措施，实现从被动应对到主动防御的转变，有效提升了数据库的安全防控能力。

5 结语

自然资源数据库作为资源管理的核心基础设施，其安全防护能力直接关乎国家资源安全与生态治理效能。高级持续性威胁的复杂性与隐蔽性，对监测体系的构建提出了更高要求。本研究构建的监测体系通过整合技术与管理手段，实现了对威胁行为的全生命周期管理，有效提升了数据库的安全防御水平。未来，需持续关注威胁演化趋势，推动监测技术的创新与应用，不断完善体系的闭环管理机制，为自然资源数字化管理提供坚实的安全支撑，助力资源治理能力的现代化发展。

参考文献

[1] 韦峻峰,陈晨,杨莉.面向运营商网络的APT一体化监测体系研究[J].邮电设计技术,2025,(09):63-69.

[2] 《2024年全球高级持续性威胁研究报告》发布[J].中国信息安全,2025,(02):84.

[3] 庞九凤,张亚昊,胡威,等.高级持续性威胁（APT）攻击检测与防御的深度学习方法研究[J].办公自动化,2024,29(14):73-76.