团　　体　　标　　准

大数据平台网络攻击日志的交叉认证要求

（征求意见稿）

编制说明

XXXX-XX-XX

《大数据平台网络攻击日志的交叉认证要求》
（征求意见稿）编制说明

1 任务来源、协作单位

1.1 任务来源

2024 年 8 月 12 日，根据中国能源研究会下达的《关于 2024 年第一批中国能源研究会标准立项的通知》(中能研标〔2024]3 号)，团体标准《大数据平台网络攻击日志的交叉认证要求》予以立项，由中国能源研究会提出并术归口。

1.2 协作单位

牵头公司：华中科技大学网络空间安全学院

参编单位：西安电子科技大学网络与信息安全学院、国网湖北省电力有限公司武汉供电公司

牵头单位简介及与本标准相关的工作介绍：

华中科技大学网络空间安全学院是中国首批独立建制的网络空间安全学院之一，依托学校计算机科学与技术、电子信息等学科优势，聚焦网络攻防、数据安全、系统安全等核心领域。学院拥有国家级网络空间安全实验教学示范中心、教育部重点实验室等平台，牵头承担多项国家重点研发计划、国家自然科学基金项目，并与华为、360、安天等企业建立联合实验室，推动产学研深度融合。学院以“实战化、工程化”为导向，在威胁检测、攻击溯源、安全大数据分析等领域具有显著技术积累。

参编单位简介及与本标准相关的工作介绍：

西安电子科技大学网络与信息安全学院是国家首批获批“网络空间安全”一级学科博士学位授权点的单位之一，以密码学、数据安全、系统安全为核心方向，依托综合业务网理论与关键技术国家重点实验室（ISN 国家重点实验室）、信息对抗技术国家级实验教学示范中心等平台，形成了“密码技术为根基、攻防实战为特色”的学科优势。学院承担了多项国家重大科技专项、重点研发计划，并与华为、中兴、中国电科等企业共建联合实验室，在网络安全领域具备深厚的技术积累和行业影响力。

国网湖北省电力有限公司武汉供电公司是国家电网公司下属的大型供电企业，负责武汉地区电网规划、建设、运营及电力供应服务，是保障华中地区能源安全的核心单位之一。公司深度参与电力系统智能化、数字化转型，在电力信息物理融合系统（CPS）安全防护、工控网络安全等领域处于行业领先地位，拥有电力行业网络安全攻防实验室、能源互联网安全创新中心等平台，并牵头承担多项国家电网科技项目，聚焦电力关键基础设施的网络安全威胁监测、应急响应与取证溯源。

2 编制工作组简况

2.1 编制工作组及其成员情况

1.科研院所：华中科技大学网络空间安全学院

编写组成员情况：

韩兰胜：教授，华中科技大学国家网安基地创新与实践中心主任。

戴子城：博士生，华中科技大学网络空间安全学院。

李新：硕士生，华中科技大学网络空间安全学院。

孙海丽：博士生，华中科技大学网络空间安全学院。

秦泽青：硕士生，华中科技大学网络空间安全学院。

朱东君：博士生，华中科技大学网络空间安全学院。

陈鹏：博士生，华中科技大学网络空间安全学院。

廖伟：博士生，华中科技大学网络空间安全学院。

张行柯：硕士生，华中科技大学网络空间安全学院。

杨帆：硕士生，华中科技大学网络空间安全学院。

马铭芮：硕士生，华中科技大学网络空间安全学院。

冯铭希：硕士生，华中科技大学网络空间安全学院。

2.科研院所：西安电子科技大学网络与信息安全学院

编写组成员情况：

尤伟：讲师，西安电子科技大学网络与信息安全学院信息安全系。

3.检验认证机构：国网湖北省电力有限公司武汉供电公司

2.2 标准主要起草人及其所做的工作

张行柯、杨帆、马铭芮、冯铭希等人负责大数据平台网络攻击日志的交叉认证要求第一章的适用范围讨论；

朱东君、陈鹏、廖伟等人负责第三章术语和定义的讨论与规整；

李新、孙海丽、秦泽青负责第五章交叉认证工作流程规范的梳理；

戴子城、韩兰胜负责全文整理、编撰，并完成第四章、第六章和第七章的总结与概述。

3 起草阶段的主要工作内容

2023 年 6 月，根据中国能源研究会下达的《关于 2023 年第一批中国能源研究会标准立项的通知》，随后组织开展前期调研，召开专家研讨会，对标准的范围、深度、主要内容等进行初步讨论。

2023 年 7 月，召开项目启动会，成立编制工作组，正式启动本标准编制工作。

2023 年 8 月-2024 年 3 月，编制工作组开展多轮研究讨论，编制标准各部分内容，以腾讯视频会议方式组织开展标准内部审查会议，形成标准初稿。

2024 年 7 月，中国能源研究会信息通信专业委员组织专家对初稿的形审和内容开展审查，根据评审专家意见进行修改。形成征求意见稿初稿。

2024 年 9 月，中国能源研究会信息通信专业委员会以函审的形式组织召开公开征求意见稿前审查会，对公开征求意见稿进行评审。

2024 年 9 月-2024 年 10 月，中国能源研究会信息通信专业委员会将征求意见稿挂网，

广泛征求意见，根据相关领域专家意见和建议进行修改，形成送审稿。

在大数据平台网络攻击日志交叉认证要求标准的编制过程中，我们遵循了科学、严谨、公正的原则，确保标准的适用性、前瞻性和可操作性。首先，根据大数据安全领域的实际需求，提出了编制该标准的立项申请，成立了标准编制小组，并明确了编制任务、时间表和人员分工；在充分调研和资料收集的基础上，标准编制小组开始编制标准的初稿；初稿内容涵盖了交叉认证的定义、使用场景、所需要素、认证流程以及数据和规则信息等各个方面；初稿完成后，标准编制小组内部进行了多次审查，对标准中的关联规则设计、日志证据生成、证据间交叉认证等进行了反复修改和完善。

关于交叉认证的定义主要争议问题的处理情况，我们调研了现有法律认证的基本规范、认证规则等相关知识，并了解了国内外在该领域的最新进展和技术成果，对交叉认证工作流程规范进行了相应的修改和完善。此外，我们邀请了行业内的专家学者进行咨询和论证，听取他们的意见和建议。通过专家的指导和帮助，我们对关联规则的制定有了更深入的认识和理解。

在标准征求意见阶段和审查阶段，专家们提出了许多宝贵的意见和建议，我们根据审查意见对标准进行了进一步的修改和完善，确保标准的科学性和合理性。根据专家意见绘制最终的送审稿，确保标准内容的完整性、准确性和清晰性。

4 标准编制原则及与国家法律法规和强制性标准及有关标准的关系

4.1.1 标准编制原则

4.1.1.1 统一性原则

对网络安全领域的日志管理能力进行全面、系统的评价，统一评价的尺度和标准，以便不同企业之间进行比较和分析。

4.1.1.2 协调性原则

与网络安全领域其他相关标准相互配合，共同构建完整的网络安全领域的标准体系，避免标准之间的冲突和矛盾。

4.1.1.3 适用性原则

充分考虑网络安全领域实际情况和特点，确保标准具有广泛的适用性。评价指标和方法应易于理解和操作，能够为不同规模、不同类型的能源企业提供有效的指导和参考。

4.1.1.4 一致性原则

标准的编制过程中，充分征求各方意见，确保标准内容与行业发展需求和企业实际情况相一致。

4.1.1.5 规范性原则

严格按照标准化工作的规范和要求进行编制，确保标准的格式、内容和表述符合国家标准的规范。

4.1.1.6 目标性原则

通过标准的实施，推动网络安全领域加强安全防护体系建设，提升安全防护管理水平，保障企业日志管理的顺利进行。

4.1.2 确定技术要素的原则

4.1.2.1 目的性原则

技术要素的确定应紧密围绕网络安全领域日志管理能力评价这一目的，明确评价的对象、范围和重点，确保技术要素能够全面、准确地反映安全防护能力的各个方面。

4.1.2.2 可证实性原则

能够通过实际的数据、案例或其他客观证据进行验证和评价，评价方法科学、合理，经专家多次评审能够确保评价结果的真实性和可靠性。

4.2 与法律法规的关系和强制性标准的关系

4.2.1 与法律法规的关系

本标准符合现行法律、法规、政策及相关标准相关规定。

本标准的编制和实施严格遵守国家相关法律法规，如《中华人民共和国网络安全法》《中华人民共和国数据安全法》等。这些法律法规为网络安全领域的日志管理方法提供了基本的法律框架和要求。

本标准在安全防护能力评价的指标体系中，充分考虑了法律法规在网络安全、数据安全、隐私保护等方面的要求，确保企业的安全防护措施符合法律规定。

标准的实施有助于互联网企业更好地落实法律法规的要求，提高企业的法律意识和合规水平，降低法律风险。

4.2.2 与强制性标准的关系

本标准在编制过程中，参考了相关领域的强制性标准，如信息安全技术相关的国家标准等，确保在技术要求和评价方法上与强制性标准保持协调一致。

本标准在安全防护能力评价的指标设置和权重分配上，充分考虑了强制性标准的重点要求，在满足强制性标准的基础上，为进一步提升安全防护能力提供了指导。

本标准的实施不会与强制性标准产生冲突，而是作为一种补充和完善，帮助互联网企业更好地满足强制性标准的要求，提高企业的整体安全防护水平。

4.3 本标准与上位标准或其他相关标准相比较主要技术指标的不同点

1.编写要点：

与《信息安全技术数据安全能力成熟度模型》上位标准不同点

本标准是团体标准，其上位标准为国家法律法规及相关强制性标准。标准内容未与上位标准冲突，且在适用的范围内补充了上位标准的不足。

与《网络安全威胁信息格式规范》其他团体标准的关系

本标准与现行的团体标准《网络安全威胁信息格式规范》相比,重点解决了以下问题：

填补空白：针对现有《网络安全威胁信息格式规范》团体标准未覆盖的日志交叉认证领域进行了补充。

细化提升:《网络安全威胁信息格式规范》在现有技术要求的基础上，进一步提升技术指标。

优化完善：对现有《网络安全威胁信息格式规范》团体标准中未明确的条款进行了细

化，增强了标准的可操作性。
与行业标准的关系：
本标准与 YD/T 3865-2021《工业互联网数据安全保护要求》 相比，主要技术指标的不同点如下：
填补空白：本标准针对网络空间安全领域的日志交叉认证技术要求领域的空白问题，提出了创新性的技术要求。
提升指标：在日志管理方面，本标准的日志、证据数据要求技术指标高于行业标准。
细化要求：对日志的交叉认证技术的应用场景、操作流程等进行了细化，便于企业实施。
总结
本标准在满足国家法律法规和上位标准的基础上，结合行业实际需求，对技术要求进行了优化和提升，填补了行业的部分空白，具有较强的适用性和指导意义。
2.参考示例：

本标准充分考虑了大数据平台网络攻击日志交叉认证的实际需求，确保了标准在实际应用中的可行性和有效性；与现有法律法规、强制性标准及相关标准之间保持了良好的协调性，确保了标准的实施不会与现有规定产生冲突；并明确规定了编制的目标和目的，提高了大数据平台网络攻击日志交叉认证的准确性和效率，为大数据安全提供有力保障。

在法律法规方面，本标准在编制过程中，充分考虑了国家关于大数据安全、网络安全等方面的法律法规要求，确保标准的编制和实施符合法律法规的规定。

与其他相关标准相比，本标准在大数据平台网络攻击日志交叉认证方面填补了国内相关标准的空白，为大数据安全提供了新的技术支撑和保障。在日志证据的要求方面，本标准对日志数据的完整性、可靠性和保密性提出了更高的要求；在关联规则的要求方面，本标准强调了关联规则的制定应根据不同攻击类型有所变化，并采用了聚类、深度学习等先进方法构建关联规则。

5 标准主要技术内容的论据或依据；修订标准时，应增加新、旧标准水平的对比情况

5.1 标准主要技术内容的论据

5.1.1 理论依据
本标准提出《大数据平台网络攻击日志的交叉认证要求》的技术要求，主要基于以下理论支撑：
信息安全能力模型：参考 GB/T 37988-2019《信息安全技术数据安全能力成熟度模型》，设计标准化日志交叉认证，确保设备兼容性。
数据安全框架：依据 ISO/IEC 27037:2012《信息技术-安全技术-数字证据的识别、收集、获取和保存指南》，提出数据加密、权限分级等要求，保障交易隐私。
5.1.2 数据依据
基于《大数据平台安全审计与攻击溯源关键技术》重点研发测试数据制定技术指标：

数据来源：
重点研发《大数据平台安全审计与攻击溯源关键技术》提供日志数据。
统计结论：
行业标准未覆盖司法取证场景，本标准新增电子证据固定规则，在威胁信息共享场景中，将事件关联粒度从“IP 级”细化至“会话级”，并针对性补充了攻击证据链构建的实操规范。

5.1.3 技术思路总结

针对大数据平台日志数据的多样性和复杂性，本标准提出了一种基于多维度特征的日志交叉认证方案。该方案基于信息论特征冗余性与互补性原理，构建时间戳、IP 地址、事件类型等多维度特征向量，实现跨平台日志交叉认证，提取日志中的关键信息，如时间戳、IP 地址、事件类型等，构建日志特征向量，并进行相似度计算和匹配，从而实现对日志数据的交叉认证。为确保交叉认证结果的准确性和可靠性，本标准对日志数据的格式、存储、传输等方面提出了具体的技术要求。这些要求旨在确保日志数据的完整性、一致性和安全性，为交叉认证提供有力的技术保障。

我们搭建了多个大数据平台网络攻击模拟环境，并在这些环境中进行了日志交叉认证的试验验证。试验结果表明，本标准所提出的交叉认证方案能够准确识别出网络攻击事件，并实现对日志数据的交叉验证。

5.2 修订标准时，应增加新、旧标准水平的对比情况

相较于旧标准，新版《大数据平台网络攻击日志交叉认证》团体标准在技术深度、实施规范性和场景覆盖上实现显著提升。技术层面，新版细化证据分级（一级原始日志、二级合成证据、三级关联证据），并新增冲突解决机制（专家规则优先）；流程规范，新版要求证据生成需满足高性能指标，数据预处理强制包含脱敏与哈希保留，且证据库需动态同步更新；场景扩展，新增差分攻击、重标识攻击等特定隐私攻击的检测规则与验证流程，并引入对抗分析模型等动态规则；合规性，新增引用 GB/T 37988 和 ISO/IEC 27037 标准，强化数据安全与电子证据管理的合规要求。总体而言，新版标准从框架到细节均体现出更强的技术严谨性、操作指导性和安全防护能力。

6 主要试验（验证）的分析、综述报告，技术经济论证，预期的经济效果

6.1 主要试验（验证）的分析

我们设计了医疗、校园网、运营商等验证场景，模拟了包括大数据平台网络攻击日志数据生成与收集、证据生成、交叉认证流程等试验工作。在不同场景下，采用了多种技术手段进行验证，通过对比分析，我们验证了标准中提出的交叉认证方案的准确性和可靠性。

6.2 综述报告

回顾大数据平台网络攻击日志交叉认证的背景和意义，以及国内外相关研究和实践情况，本标准详细描述了交叉认证的制定过程、确定技术要求、开展试验验证等。并概述了标准的主要内容和特点，包括交叉认证的原理、方法、流程和技术要求等。

6.3 技术经济论证

在技术方面分析了标准实施所需的技术条件和资源，包括硬件设备、软件平台、技术人员等方面的要求。此外，通过计算和分析，本标准实施能够带来显著的经济效益，如帮助安全团队快速准确地确认攻击行为，并采取相应的应对措施，缩短安全事件的响应时间，降低安全风险等。同时，标准实施所需的成本也是合理的，可以通过提高效率和降低成本等方式进行分摊和回收。

6.4 预期的经济效果

随着大数据产业的不断发展，对数据安全性的要求也越来越高。标准的实施将有助于推动大数据产业的安全发展，提高整个产业的竞争力和创新能力。并带动相关产业链的发展，如网络安全设备、软件和服务等。

7 采用国际标准的程度及水平的简要说明

本标准深入研究了国际标准和国外标准中关于大数据平台网络攻击日志交叉认证的技术要求、测试方法和评估标准等内容，最终决定不直接采用国际标准或国外标准，而是基于国内实际情况和行业需求进行自主制定。本标准充分考虑了国内大数据平台网络攻击日志交叉认证的实际需求和行业特点，具有更强的针对性和实用性。

8 重大分歧意见的处理经过和依据

完成初稿后，内部审核专家旧标准的题目提出了修改意见，需要聚焦大数据平台攻击日志，因此修改标准题目为大数据平台网络攻击日志的交叉认证要求；此外，专家还建议增加交叉认证的工作流程规范方面的内容，因此修改团标编撰内容，增加交叉认证工作流程规范内容。

9 贯彻标准的要求和措施建议（包括组织措施、技术措施、过渡办法等内容）

建议由数据安全、网络安全及 IT 运维等部门联合成立大数据平台网络攻击日志交叉认证专项工作组，负责标准的制定、执行、监督及优化。建立跨部门的沟通机制，确保信息畅通，及时共享网络攻击日志交叉认证的相关信息和经验，并设立专门的反馈渠道，收集员工对标准的意见和建议，不断完善标准体系。

在技术方面，建议采用统一的日志收集工具，确保大数据平台所有网络攻击日志的完整性和准确性；开发或采用成熟的交叉认证算法，对收集到的网络攻击日志进行交叉验证，确保日志的真实性和可靠性；此外，还需建立日志交叉认证数据库，存储经过验证的日志信息，便于后续分析和追溯。

建议将标准贯彻工作分为多个阶段，逐步推进，初期可选择部分关键系统进行试点，积累经验后再全面推广。试点系统应对员工进行大数据平台网络攻击日志交叉认证标准的培训，包括大数据平台网络攻击日志交叉认证的基本概念、原理、操作流程及注意事项等，提高员工的认知和操作技能。

10　其他应予说明的事项，如涉及专利的处理等

专利名称：大数据平台攻击证据交叉认证方法、设备、介质和产品

变更原因：该专利涉及的技术是实现大数据平台网络攻击日志交叉认证的核心技术之一，从技术角度考虑无法避免涉及。

处理方式：我们已与专利持有人进行了沟通，并获得了其同意在标准中免费使用该专利的书面声明。