ICS 35.110
L 70

团　　体　　标　　准

T/CERS 0117-2025

大数据平台网络攻击日志的交叉认证要求

The cross-certification requirements for network attack logs of the big data platform

2025-11-26 发布　　2025-11-26 实施

中国能源研究会　发布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》给出的规则起草。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本文件由中国能源研究会提出。

本文件由中国能源研究会标准工作办公室归口。

本文件起草单位：华中科技大学网络空间安全学院、国网湖北省电力有限公司武汉供电公司、西安电子科技大学网络与信息安全学院、广东电网有限责任公司信息中心、中国大唐集团数字科技有限公司、中国电力建设股份有限公司、山西省能源互联网研究院、中能国研（北京）信息通信科技有限公司、中能国研(北京)电力科学研究院。

本文件主要起草人：戴子城、韩兰胜、顾显俊、李新、孙海丽、秦泽青、朱东君、陈鹏、廖伟、尤伟、张行柯、杨帆、马铭芮、冯铭希、黄梦琦、田聪、黄冠杰、段彪、姚潮生、沈伍强、张小陆、张春林、常馨月、白敬强、梁志琴、黄慕夏。

本文件为首次发布。

本文件在执行过程中的意见或建议反馈至中国能源研究会。

相关意见反馈联系方式：中国能源研究会标准执行办公室（E-mail: cers@cers.org.cn；电话：010-56284696）。

引　言

由于攻击行为跨多个应用系统，其攻击数据存在于多个系统，不同系统间数据结构存在差异，单一数据的攻击行为不明显，单源证据证明力不足。针对单一证据证明力不足，进行跨系统多源证据的关联分析，并提出基于多源风险数据关联性证据的交叉认证方法，支撑大数据平台攻击证据的跨域交叉认证，提升证据证明的效力及可信度。

交叉认证本质是整合多源异构数据，为差分攻击、重标识攻击和统计推断攻击提供有效证据，在大数据安全领域可契合国际国内标准，为安全防护提供支撑。在攻击溯源中，它通过多数据源交叉验证推导更多证据与攻击信息，符合 ISO/IEC 27037:2012 对数字证据全生命周期管理的要求，能保障证据链完整有效。构建关联规则数据库时，将原始日志数据与关联规则结合，生成多类证据并形成证据库，助力安全分析与威胁情报研究，契合 GB/T 37988-2019 数据安全能力分级建设思想，推动数据安全分析能力升级。在攻击检测场景，对多类关联证据交叉认证以确定攻击行为，能加快攻击确认、缩短响应时间，既遵循 ISO/IEC 27037:2012 数字证据一致性原则提升检测精准度，又符合 GB/T 37988-2019 事件响应高效性要求，强化防护能力。

目前在网络仿真中，仍缺少证据交叉认证要求标准，异构证据交叉认证无法通用，因此，亟需制定相关标准予以规范。

大数据平台网络攻击日志的交叉认证要求

1 范围

本文件规定了大数据平台网络攻击日志的交叉认证工作流程和平台运维与安全审计团队的相关执行要求。

本文件适用于所有类型的大数据平台。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 37027-2025 网络安全技术 网络攻击和网络攻击事件判定准则

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

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

ISO/IEC 29100:2024 信息技术 安全技术 隐私框架

3 术语和定义

下列术语和定义适用于本文件。

3.1

交叉认证 cross-certification

指通过多个独立来源证据数据集相互验证，协同印证网络攻击行为，确保攻击特征在不同维度证据链中具备一致性的过程。

3.2

原始日志数据 source log data

记录平台行为、可用于印证网络攻击行为的未经加工的原始数据。

3.3

证据 evidence

基于原始日志数据经校验规则处理后生成，用于印证网络攻击行为的各类数据与记录。

3.4

关联证据 correlative evidence

通过关联规则推导形成，具备行为标识与上下文关联特征的攻击凭证。

3.5

关联规则 association rule

用于匹配攻击相关证据间关联的确定性规则。

3.6

置信度模型 confidence model

通过概率统计或算法推导输出置信值，支撑决策判断，是量化预测结果或关联结论可靠程度的数学模型

4 网络攻击日志交叉认证工作流程规范

4.1 概述

证据的交叉认证工作流程应包含证据生成、关联规则设计、构建关联证据库、证据间交叉认证四个部分，其流程图见图 1。

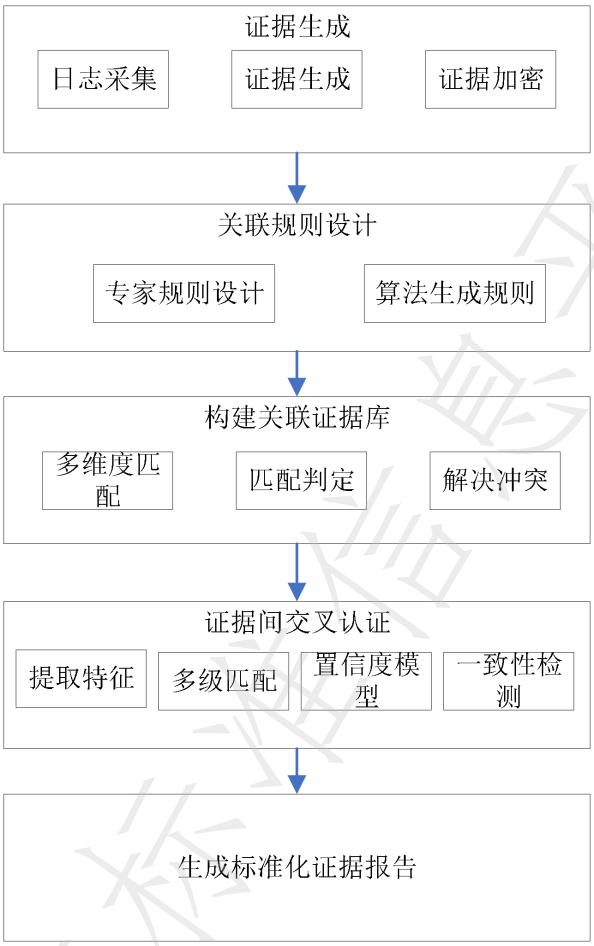

图1　网络攻击日志交叉认证工作流程图

4.2　日志采集流程要求

日志采集过程合规性要求如下：

a）　应留存日志原始载体，不应丢弃或篡改来源；若载体无法长期保存，须备份后再处理；

b）　生成原始日志电子副本时，应经哈希校验确保副本与原始载体哈希值一致，防范传输或存储环节数据篡改；

c）　采集日志应含秒级时间戳，并补充操作主体、操作对象等元数据，保障单条日志可独立追溯行为背景；

d）　若修正已采集日志，应记录改留痕，不应直接覆盖原始日志；修改记录单独存储，应包含修改人、修改时间、修改原因及修改前后内容对比，确保修改过程可审计；

e）　采集关键业务场景操作日志（如数据库敏感表修改、系统权限变更、核心业务配置调整、大规模数据导出等）时，应先明确判定标准（高业务影响、高数据价值、高安全风险），记录完整上下文，含操作前系统状态、操作过程及操作后结果，保障关键行为可完整复现，支撑交叉认证证据链闭环。

4.3　证据生成流程要求

为确保能够有效实现关联证据的交叉认证，证据生成要求如下：

a）　证据的基本信息应包含时间、IP地址、用户身份信息、具体系统或服务器名称或编号、攻击类型等；

b）　在生成证据过程中应适当保留日志与证据的关联关系，如时间戳、唯一标识符、来源标识、关键属性等参数；

c）　应保证生成证据的可靠性和保密性；

d） 数据处理应包含去噪、清洗、格式标准化、数据脱敏四个环节。

4.4 证据加密要求

含敏感信息的证据类日志应明确保密性技术实现标准，其要求如下：

a） 证据加密：采用SM4算法对敏感字段加密存储，SM2算法用于数字签名验证,并符合ISO/IEC 29100标准，对日志敏感字段加密存储；

b） 密钥管理：对称加密密钥轮换周期不应超过90天，非对称加密密钥轮换周期不应超过180天；建立密钥生成、分发、存储、销毁全流程管控机制；

c） 传输安全：日志数据在采集端至存储端、存储端至分析端传输时，采用 TLS 1.3 协议加密传输，传输过程采用双向证书认证，密钥协商算法选用加密套件。

4.5 关联规则设计要求

交叉认证关联规则分专家设计和算法生成两种，需按攻击类型差异化构建：高优先级的网络层、应用层攻击，聚焦流量、请求参数等核心维度关联；中高优先级的主机层、数据层攻击，侧重进程行为、数据访问等特征关联；中低优先级的身份认证、供应链 、物联网攻击，结合行为特征与算法挖掘隐性关联。

4.5.1 专家设计关联规则要求

其中专家设计的基础关联规则应包含以下几种：

a） 属性关联规则：基于日志属性相似性构建，如 IP 地址相同、访问时间临近、目的 IP 一致等；

b） 访问模式关联规则：基于访问模式特征构建，如访问来源一致、访问频率固定等；

c） 用户行为关联规则：基于用户行为特征构建，如多次登录失败、测试访问权限等；

d） 专家设计关联规则：含定义时间窗口阈值（如短时高频攻击设为5分钟内，低频潜伏攻击设为24小时内）与地理围栏范围（如同一城市IP段、企业内网IP区间）的时空关联、预定义高危行为模式库的行为序列、设置网络标识权重及时间敏感系数的属性权重等维度。

4.5.2 算法生成关联规则要求

算法生成规则要求应包括：

a） 采用基于支持度阈值和置信度阈值的频繁项集挖掘关联性算法；

b） 采用基于大规模样本训练的自动化规则生成深度学习模型；

c） 采用多规则权重投票策略的冲突解决机制。

4.6 关联证据库构建要求

构建初始证据集后，应结合专家规则与算法规则开展多维度比对，将日志属性与规则库逐项比对并触发匹配判定，具体要求如下：

a） 采用预设基础关联规则与算法生成关联规则开展对比分析；

b） 将初始证据集中待认证证据的属性，与关联规则库规则逐一比对；

c） 若待认证证据日志属性中某属性项，与关联规则库中某规则完全吻合，即判定该证据与对应初始证据集匹配；

d） 建立规则匹配度量化指标：完全匹配（所有属性符合）、强匹配（关键属性符合阈值）、弱匹配（基本属性符合阈值）；

e） 设定规则冲突解决机制，专家规则优先级高于算法生成规则。

4.7 证据间交叉认证流程要求

证据间交叉认证流程分三步：

a） 从原始日志提取攻击特征指纹，包括网络会话哈希、进程行为签名、异常操作模式编码；

b） 在关联规则库中执行多级匹配，优先匹配时空约束的专家规则，再用机器学习规则进行行为模式扩展匹配；

c） 构建攻击行为置信度模型，采用0-100分权重量化规则：直接关联证据赋予80-100分权重；间接关联证据赋予30-60分权重。

4.8 证据间交叉认证要求

对于已匹配的初始关联证据集，执行以下分析认证要求：

a) 攻击行为一致性检查：分析集中所有证据，确认是否存在指向待认证证据同一攻击行为的证据；
b) 认证结果判定：存在指向同一攻击行为的证据则认证成功，反之则认证失败；
c) 交叉认证过程：根据待认证证据所指证的攻击行为，遍历全部证据，如各类日志数据、关联规则衍生证据、网络流量记录等；
d) 在遍历过程中，若某关联证据指向的攻击行为与待认证证据所指完全一致，即视为交叉认证成功。

4.9 标准化证据报告要求

对已生成的标准化证据报告，应执行以下要求：

a) 交叉认证成功后生成标准化证据报告，作为攻击溯源、责任认定、司法取证的核心依据；
b) 报告应完整包含操作系统、应用程序、安全设备等各类日志原始信息，涵盖系统状态、用户活动、异常事件等关键信息，如攻击者 IP、访问时间、访问页面、攻击流量来源及目的端口等；
c) 报告应清晰呈现关联规则，包括原始日志数据中事件与数据的内在联系，交叉认证所依据规则，如特定网络流量模式与已知攻击手段的匹配规则，确保证据推导逻辑可追溯；
d) 报告需详细记录交叉认证过程，包括初始关联证据集遍历步骤、验证人员信息、验证发起时间、各项证据关联验证结果；
e) 报告存储于指定数据库，数据库应支持分布式存储方案，具备高可靠、高扩展、高查询性能，并通过加密保障报告安全与完整，同时需满足容灾备份要求，应采用异地多活架构，核心数据每日全量备份且每小时增量备份，非核心数据每日全量备份；
f) 攻击溯源应以报告中日志原始信息为基础，梳理攻击者从外部渗透至内部系统的完整路径；
g) 责任认定应依据报告中的关联规则与验证过程，明确各环节相关人员或系统的责任边界；
h) 若涉及司法取证，应确保标准化证据报告符合司法要求，凭借完整性、规范性与可追溯性作为有效证据，提升证据在司法采信度。

5 网络攻击日志交叉认证要求

5.1 原始日志收集范围

大数据平台原始日志应收集多系统关联数据，数据类型以系统运行日志为主，每条日志需记录 IP、时间、设备类型等可用于交叉认证的信息，具体日志收集要求：

a) 数据类型应包含：网络流量日志、系统事件日志、应用审计日志、安全设备日志，以及大数据平台关键组件日志；
b) 采集时间精度应包含记录时间、网络标识符、用户身份、操作参数等核心属性；
c) 数据质量应保障完整性保护、可靠性验证、空值处理机制。

5.2 日志要求

5.2.1 网络安全设备类日志要求

网络安全设备类应聚焦网络层攻击与连接管控，日志要求包括：

a) 防火墙日志应包含连接请求处理结果、源 IP、目的 IP、源端口、目的端口、连接时间、协议类型等；
b) 入侵检测系统和入侵防御系统日志应包含攻击类型、攻击源 IP、攻击目标 IP、端口号、包含攻击时间、匹配规则 ID、处理结果。

5.2.2 系统运行类日志要求

系统运行类日志应反映系统层面运行状态与进程行为，具体要求如下：

a) 操作系统日志应包含系统启停时间、用户登录账号、时间、IP、连接方式、进程创建或终止记录、进程 ID、名称、时间、终止原因、系统权限变更记录等；

b) 进程运行日志应包含进程 ID、名称、资源调用记录、进程间通信方式、通信对象、进程启停时间、异常退出原因等。

5.2.3 应用与数据类日志要求

应用与数据类日志应聚焦应用交互与数据操作，具体要求如下：

a) 数据库系统日志应包含操作账号、时间、类型、执行 SQL 语句、操作数据表、字段、结果、客户端 IP、数据库实例名等；
b) API 接口调用日志应包含 API 名称、版本、调用参数、调用方、被调用方地址、调用时间、结果、错误码。

5.2.4 用户操作类日志要求

用户操作类日志应记录用户身份与高风险操作，具体要求如下：

a) 用户登录日志应包含登录账号、系统、应用名称、时间、IP、设备标识、登录方式、结果、会话有效期等；
b) 操作审计日志应包含操作账号、时间、类型、操作对象、IP、结果；
c) 敏感操作应标注风险等级等。

5.3 证据要求

证据来源于原始日志，但原始日志常包含冗余信息或格式不统一问题，应通过标准化处理形成可用证据实体，具体要求：

a) 应对证据进行标准化处理，如：清洗、提纯、属性保留；
b) 证据标准化处理应保留高信息熵的属性值，形成可靠的证据实体，如保留时间戳、主题IP、客体IP、操作、所在域、攻击类型、调用进程等可用于交叉认证的属性；
c) 应构建证据专属数据库；
d) 证据库更新过程需保留完整变更日志，并进行数字签名，防止更新记录被篡改；
e) 应添加动态更新机制，将证据库与日志库同步更新；
f) 证据库与日志库同步失败时，立即触发告警通知，启动备份数据补传流程，补传完成后校验数据一致性，确保数据实时对齐；
g) 日常按小时增量更新，每周进行一次全量更新；日志量激增时（如遭遇大规模攻击）触发实时增量更新。

5.4 关联证据库数据模型要求

对关联证据库数据模型的要求包括：

a) 原始日志表：覆盖网络层、主机层、应用层、用户层等全链路节点日志，字段应包含日志唯一ID、日志来源标识、日志生成时间戳、日志类型、日志原始内容、标准化处理记录等；
b) 关联结果表：字段应包含证据链唯一ID、关联发起时间、参与关联的原始日志ID列表、关联生成的证据ID、关联结论、关联规则ID等；
c) 规则表：字段应包含规则唯一 ID、规则名称、规则类型、规则描述、规则创建时间、规则更新记录、规则启用状态等；
d) 审计表：字段应包含审计记录唯一 ID、操作人用户标识、操作时间戳、操作类型、操作对象、操作内容、操作结果等；
e) 原始日志表中用户身份、敏感IP等字段采用脱敏存储；关联结果表、规则表仅对授权人员开放访问权限，记录访问日志。

5.5 关联规则要求

对关联规则的要求包括：

a) 关联规则的制定应根据不同攻击类型有所变化，应符合攻击特性；
b) 关联规则应将同一事件在不同的层级留下的日志数据关联起来；
c) 关联规则应根据证据属性而分析；
d) 关联规则应采取聚类、深度学习等方法构建；

e） 应构建关联规则数据库用于交叉认证。

5.6 关联规则维护要求

关联规则维护应从匹配多源数据、识别安全事件更新入手，具体要求如下：

a） 规则有效性每月检测1次，通过模拟攻击场景、校验历史安全事件数据，验证规则对目标事件的识别准确性，针对攻击识别准确率低于95%、误报率高于3%的失效规则及时进行剔除或优化，确保规则的精准性与时效性；

b） 设定规则库单次更新比例上限，应分批次更新，每批次更新后开展小范围验证；

c） 模拟攻击场景的覆盖类型，需包含差分攻击、重标识攻击等特定隐私攻击场景；

d） 规则生命周期分“创建-验证-启用-修订-废止”五个阶段实施管理。

5.7 后期维护要求

交叉认证完成后，应保障规则与数据的安全性和可追溯性，后期维护要求如下：

a） 规则库版本应采用“主版本号.次版本号.修订号”标准化格式（如 V1.1.1），主版本号对应规则库架构重大调整，次版本号对应批量规则更新，修订号对应单条规则紧急修复；

b） 应保留近12个月的规则库历史版本，主版本号更新的重大版本永久保留。

5.8 更新管理要求

更新管理应避免认证中断或误判，具体要求如下：

a） 新增、修订应先在与生产环境数据结构一致的测试环境中验证，验证周期不少于3个工作日；

b） 部署前1小时关闭自动认证任务，在负载最低的时间段进行生产环境规则更新，部署完成后启动少量测试请求，确认规则正常生效且无异常报错后，再恢复自动认证任务；

c） 应采用分区域、分比例的发布方式，先在非核心业务区域全量部署，稳定运行24小时无问题后，再在核心业务区域按比例逐步扩大覆盖范围。

附 录 A
（规范性）
特定隐私攻击交叉认证标准示例

A.1 差分攻击交叉认证

检测特征：

a） 查询模式相似性检测：通过相似度算法分析连续查询的结构特征；

b） 响应数据分布异常监测：监控数据发布前后的信息熵变化；

c） 隐私保护机制失效检测：基于隐私保护算法输出的安全状态评估。

关联规则：

a） 专家规则：定义高频相似查询的时空模式特征；

b） 动态规则：采用时序模式分析模型识别查询序列的递进关联性。

验证流程：

a） 提取查询语义特征生成逻辑结构树；

b） 匹配历史攻击模式库中的敏感信息探测特征；

结合身份验证信息与数据分布异常特征综合判定。

A.2 重标识攻击交叉认证

检测特征：

a） 准标识符组合风险评估：基于唯一性计算模型分析字段组合强度；

b） 外部数据关联性检测：通过数据链接算法评估跨源匹配风险；

c） 匿名化机制有效性验证：基于去标识化算法的安全参数输出。

关联规则：

a） 专家规则：预定义高危字段组合模式库；

b） 动态规则：应用图结构分析模型构建身份关联概率网络。

验证流程：

a） 执行模拟攻击测试验证数据防护能力；

b） 监测数据使用中的跨源关联操作特征；

基于实际攻击成功率触发防御机制。

A.3 统计推断攻击交叉认证

检测特征：

a） 敏感属性关联性分析：通过多维关联算法评估数据维度相关性；

b） 统计单元安全检测：基于统计归并算法的最小单元保护验证；

c） 逆向推断风险监测：采用概率推断模型评估属性推测风险。

关联规则：

a） 专家规则：定义统计查询的维度叠加模式特征；

b） 动态规则：应用对抗分析模型模拟潜在推断路径。

验证流程：

a） 在数据发布环节植入可追踪特征标记；

b） 分析查询行为中的维度组合演进规律；

c） 基于标记特征还原概率触发主动防御。

A.4 常见攻击类型示例

检测特征：

a） 查询模式相似性检测：通过相似度算法分析连续查询的结构特征，适配差分攻击、重标识攻击、数据爬取等场景（如攻击者通过多轮相似查询推导敏感信息）；

b） 响应数据分布异常监测：监控数据发布前后的信息熵变化，针对性识别注入攻击、敏感数据泄露等导致的数据分布异常场景；
c） 隐私保护机制失效检测：基于隐私保护算法输出的安全状态评估，覆盖加密机制失效、访问控制绕过等导致隐私防护失效的攻击场景。

关联规则：

a） 专家规则：定义高频相似查询的时空模式特征，适配批量数据爬取、多账号协同探测等攻击的识别；
b） 动态规则：采用时序模式分析模型识别查询序列的递进关联性，对应 SQL 注入、权限提升等攻击的递进式操作特征。

验证流程：

a） 提取查询语义特征生成逻辑结构树；
b） 匹配历史攻击模式库中的敏感信息探测特征（含差分攻击、注入攻击、重标识攻击等典型场景特征）；
c） 结合身份验证信息与数据分布异常特征综合判定。

参 考 文 献

[1] 贾伟,张国瑜.基于代理机制的交叉认证模型研究[J].计算机应用, 2007, 27(12):3.DOI:CNKI:SUN:JSJY.0.2007-12-014.

[2] 应毅,任凯,刘亚军.基于大数据的网络日志分析技术[J].计算机科学, 2018, 45(B11):3.DOI:CNKI:SUN:JSJA.0.2018-S2-073.

[3] 王国杰.基于关联规则分析的网络安全态势智能评估方法研究[D].沈阳理工大学,2023.DOI:10.27323/d.cnki.gsgyc.2023.000758.

[4] 谷建光.关联规则算法研究综述[J].电子测试,2016,(14):41-42.DOI:10.16520/j.cnki.1000-8519.2016.14.020.