ICS 35.030
CCS L 80

团 体 标 准

T/CEATEC XXX—2026

网络空间跨域协同安全数据融合与关联分析技术规范

Technical specification for cross-domain collaborative security data fusion and correlation analysis in cyberspace

2026-X-XX 发布 2026-X-XX 实施

中国欧洲经济技术合作协会 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》的规定起草。

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专利的责任。

本文件由中国欧洲经济技术合作协会提出并归口。

本文件起草单位：。

本文件主要起草人：。

本文件为首次编制。

网络空间跨域协同安全数据融合与关联分析技术规范

1 范围

本文件规定了网络空间跨域协同安全数据融合与关联分析的总体要求、数据分类与标识、数据融合要求、数据关联分析要求、安全与隐私保护要求、测试与验证、运维管理。

本文件适用于跨域协同场景下安全数据的融合处理、关联分析与应用实施。

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 5271.1 信息技术 词汇 第1部分:基本术语

GB/T 17969.8 信息技术 对象标识符登记机构操作规程 第8部分：通用唯一标识符（UUIDs）的生成及其在对象标识符中的使用

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25069信息安全技术 术语

GB/T 35273 信息安全技术 个人信息安全规范

GB/Z 41290 信息安全技术 移动互联网安全审计指南

GB/T 41818 信息技术 大数据 面向分析的数据存储与检索技术要求

GB/T 42460 信息安全技术 个人信息去标识化效果评估指南

GB/T 43697 数据安全技术 数据分类分级规则

GB/T 44886.1 网络安全技术 网络安全产品互联互通 第1部分：框架

GB/T 45994 信息技术 大数据 跨域数据可信共享参考架构

3 术语和定义

GB/T 5271.1、GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

跨域协同 cross-domain collaboration

不同管理边界、安全域、组织、行业或网络环境下，为实现统一安全目标开展的数据共享、能力互通、流程协同的活动。

3.2

关联分析 association analysis

基于规则、统计、模型、知识图谱，对融合后数据进行时序、空间、因果、行为、威胁链关联，识别异常与攻击的过程。

3.3

数据不出域 data without leaving the domain

跨域协同过程中，数据提供方在自身域内完成数据的计算、脱敏和特征提取，仅将非原始数据结果对外提供，原始数据不跨域传输的共享模式。

4 总体要求

4.1 基本原则

4.1.1 合规性原则

跨域协同安全数据的融合、关联分析及共享利用应符合GB/T 22239、GB/T 35273、GB/T 41818的要求。

4.1.2 可信协同原则

建立跨域身份互信、权限互认、行为可审计、责任可追溯的可信协同机制，符合GB/T 45994的跨域数据可信共享要求。

4.1.3 数据最小必要原则

跨域协同过程中,应仅采集和处理实现安全分析目标所必需的最少数据,对敏感数据应优先采用“数据不出域”处理模式。

4.1.4 技术中立原则

融合与关联分析技术应兼容主流的网络安全数据格式、通信协议和软硬件架构，符合GB/T 44886.1的要求，不依赖特定的技术平台或产品，支持技术方案的迭代和扩展。

4.1.5 实时性与准确性原则

安全数据融合应保证数据的时效性和完整性，关联分析应保证结果的准确性和可靠性，满足跨域协同安全事件快速发现和处置的需求。

4.2 总体架构

4.2.1 数据接入层

网络空间跨域协同安全数据融合与关联分析总体架构分为数据层、融合层、分析层、应用层、管控层五个层级：

a）数据层：包含各跨域安全域的原始安全数据源，如防火墙日志、IDS/IPS告警、流量监测数据、资产信息、漏洞数据、威胁情报、业务系统日志等；

b）融合层：负责跨域数据采集、预处理、标准化、集成、归并与存储，实现多源异构数据的统一化处理；

c）分析层：基于融合数据集，开展规则关联、统计分析、机器学习、知识图谱推理等关联分析，识别威胁、评估风险；

d）应用层：面向跨域协同防护场景，提供威胁感知、攻击溯源、态势可视化、协同响应、预警通报、应急处置等应用功能；

e）管控层：覆盖身份认证、权限管理、安全审计、隐私保护、质量管控、运维管理等全流程管控，保障系统安全稳定运行。

4.3 性能要求

跨域协同安全数据融合与关联分析系统应满足表1规定的性能指标。

表1 系统性能指标要求

指标类别	具体指标	数值要求	适用场景
数据处理性能	数据融合吞吐量	≥10Gbps	跨域海量安全数据实时处理
	单条数据处理延迟	≤200ms	实时威胁监测
	数据接入协议支持率	≥95%	兼容主流安全设备/系统
关联分析性能	威胁检测率	≥95%	攻击事件检测

指标类别	具体指标	数值要求	适用场景
	误报率	≤5%	降低无效告警
	MTTD	≤5min	威胁快速发现
	关联分析规则并发数	≥1000 条	复杂威胁多规则分析
系统可靠性	系统可用性	≥99.9%	7×24 小时连续运行
	数据丢失率	≤0.01%	数据完整性保障
	故障恢复时间	≤30min	应急故障处置

5 数据分类与标识

5.1 数据分类

按照GB/T 43697的规定，结合跨域安全场景，将安全数据分为7大类、17子类，具体分类见表2。

表2 跨域安全数据分类表

一级分类	二级分类	数据内容	典型来源
安全日志数据	设备日志	防火墙、IDS/IPS、WAF、路由器、交换机运行日志、操作日志、告警日志	网络安全设备
	系统日志	服务器、终端、数据库、中间件的登录、操作、异常、审计日志	主机/业务系统
	应用日志	业务系统、Web 应用、APP 的访问、交易、错误、安全事件日志	业务应用系统
网络流量数据	原始流量	网络报文、流量五元组、流量大小、通信时长、协议类型	流量监测设备
	流量统计	流量峰值、均值、异常流量、DDoS 流量特征	流量分析平台
安全告警数据	入侵告警	恶意代码、漏洞利用、非法访问、暴力破解等入侵告警	IDS/IPS、EDR
	异常告警	异常登录、异常流量、异常操作、异常访问告警	安全监测系统
	合规告警	违规访问、违规操作、数据泄露、权限越权告警	数据安全系统
资产数据	硬件资产	服务器、终端、网络设备、安全设备的型号、IP、MAC、位置、配置	资产管理系统
	软件资产	操作系统、数据库、中间件、应用程序的版本、漏洞、授权	资产管理系统
	数据资产	核心数据、敏感数据、业务数据的存储位置、权属、分级	数据管理系统
漏洞与风险数据	漏洞数据	系统漏洞、应用漏洞、配置缺陷的编号、等级、影响范围、修复方案	漏洞扫描系统

一级分类	二级分类	数据内容	典型来源
	风险数据	安全风险评估结果、风险等级、风险影响、处置建议	风险评估系统
威胁情报数据	内部情报	内部攻击事件、恶意样本、攻击 IP、域名、特征库	安全运营平台
	外部情报	全球威胁情报、漏洞情报、恶意代码库、攻击组织信息	威胁情报平台
协同数据	共享数据	跨域共享安全告警、威胁、漏洞、处置信息	跨域协同平台
	响应数据	协同处置指令、处置结果、反馈信息、应急日志	应急响应系统

5.2 数据分级

依据数据重要性、敏感程度及泄露影响，将跨域安全数据分为4级：

a）一级（核心数据）：涉及国家秘密、核心业务、关键基础设施的安全数据，泄露会导致特别严重危害（如核心资产信息、高级威胁溯源数据）；

b）二级（重要数据）：涉及行业敏感、用户重要信息的安全数据，泄露会导致严重危害（如用户敏感日志、重大漏洞数据）；

c）三级（一般数据）：普通安全运行、监测数据，泄露会导致一定危害（如常规设备日志、普通告警数据）；

d）四级（公开数据）：可公开的安全统计、态势、合规数据，泄露无实质危害（如安全态势汇总数据、公开威胁情报）。

5.3 数据标识

跨域安全数据应采用统一全局唯一标识（UUID），格式遵循GB/T 17969.8，编码规则为[域编码]-[分类编码]-[分级编码]-[时间戳]-[序列号]：

a）域编码：3位字母，代表跨域类型（如ZW=政务域、JR=金融域、NY=能源域）；

b）分类编码：2位数字，对应表2一级分类（如01=安全日志、02=网络流量）；

c）分级编码：1位数字，对应5.2分级（如1=核心、2=重要）；

d）时间戳：14位数字，格式为YYYYMMDDHHMMSS；

e）序列号：6位数字，同一时间戳下的顺序编号。

示例：JR-01-2-20260413102030-001234（金融域、安全日志、重要数据、2026年4月13日10时20分30秒、序列号001234）。

6 数据融合要求

6.1 数据采集

6.1.1 采集方式

支持以下采集方式，适配不同跨域数据源：

a）主动采集：通过API接口、JDBC/ODBC、FTP、SFTP主动拉取数据，支持定时、增量、全量采集；

b）被动采集：通过Kafka、MQTT、Syslog等消息队列接收跨域系统推送的实时数据；

c）旁路采集：通过流量镜像、分光方式采集网络流量数据，不影响业务系统运行。

6.1.2 采集协议

支持主流采集协议，至少包括：Syslog、SNMP v3、HTTP/HTTPS、RESTful API、WebSocket、Kafka、MQTT 3.1.1/5.0、NetFlow v9/IPFIX。

6.1.3 采集质量要求

应满足以下要求：

a）数据采集覆盖率：关键安全数据源采集覆盖率100%，一般数据源≥95%；
b）采集完整性：数据字段完整率≥99%，关键字段（时间、IP、告警类型）完整率100%；
c）采集时效性：实时数据采集延迟≤100ms，批量数据采集延迟≤5min。

6.2 数据预处理

6.2.1 数据清洗

应按照以下方法进行：

a）缺失值处理：关键字段缺失直接丢弃，非关键字段缺失采用均值、中位数、插值法补全，缺失值处理率≥99%；

b）噪声数据处理：过滤异常值、重复值、乱码数据，重复数据去除率≥98%；

c）不一致数据处理：统一时间格式（YYYY-MM-DD HH:MM:SS）、IP格式（IPv4/IPv6 标准化）、协议名称、告警等级，不一致数据标准化率≥99%。

6.2.2 数据标准化

内容包括：

a）统一字段名称：如将“告警时间”“发生时间”统一为“event_time”；
b）统一数据类型：数字型（整型/浮点型）、字符型、日期型、布尔型标准化；
c）统一枚举值：告警等级统一为“紧急、高、中、低、提示”5级。

6.2.3 数据脱敏

针对一、二级敏感数据，按GB/T 42460实施脱敏：

a）核心数据采用加密脱敏（SM4算法）；
b）重要数据采用掩码脱敏（如IP：192.168.XXX.XXX、手机号：138****1234）；
c）脱敏后数据可用性≥90%，不可还原率100%。

6.3 数据融合

6.3.1 融合层级

分为三级融合：

a）数据级融合：对原始数据进行对齐、归并、关联，形成统一数据集（如同一IP的多源告警合并）；

b）特征级融合：提取数据特征（攻击特征、流量特征、行为特征），进行特征组合与优化，形成特征向量库；

c）决策级融合：基于多源分析结果，通过投票、贝叶斯推理、集成学习，形成统一威胁决策结论。

6.3.2 融合算法

应包括以下算法：

a）时空对齐算法：按时间戳（±1s）、IP/资产ID进行数据匹配，匹配准确率≥98%；
b）数据归并算法：对重复告警、同源告警、关联告警进行归并，归并压缩率≥60%；
c）异构数据映射算法：建立跨域数据语义映射关系，映射准确率≥95%。

6.3.3 融合存储

应按照以下方法进行：

a）结构化数据：采用关系型数据库（MySQL、PostgreSQL）存储；
b）非结构化/半结构化数据：采用分布式存储（HDFS、对象存储）存储；
c）索引数据：采用Elasticsearch、Redis构建索引，数据查询响应时间≤1s；
d）数据存储周期：一级数据≥3年，二级数据≥2年，三、四级数据≥6个月。

7 数据关联分析要求

7.1 关联分析框架

关联分析分为规则引擎、统计分析、智能分析、知识图谱推理四大模块，流程为：数据输入→特征提取→关联匹配→威胁识别→风险评估→结果输出。

7.2 规则关联分析

7.2.1 规则分类

分类如下：

a）基础规则：单维度告警匹配（如单IP1分钟内暴力破解失败≥5次触发告警）；

b）复合规则：多维度跨域关联（如“异常登录+敏感数据访问+境外IP”复合告警）；

c）攻击链规则：覆盖攻击全生命周期（侦察→入侵→植入→控制→横向移动→数据渗出）；

d）协同规则：跨域联动规则（如A域发现攻击IP，自动关联B域该IP访问记录）。

7.2.2 规则参数要求

规则应包含：规则ID、规则名称、规则类型、关联维度、触发条件、阈值、告警等级、处置建议、适用域，参数完整率100%。

7.2.3 典型规则示例

跨域关联分析典型规则见表3。

表3 跨域关联分析典型规则

规则 ID	规则名称	关联维度	触发条件	告警等级
R001	跨域暴力破解攻击	IP、账号、时间、域	同一账号 1 小时内≥3 个域登录失败≥10 次	紧急
R002	APT 横向移动	资产、账号、端口、时间	2 小时内跨 3 个以上网段异常登录，访问敏感端口	高
R003	数据泄露行为	用户、文件、流量、域	非工作时间跨域下载≥1GB 敏感文件，且加密传输	高
R004	DDoS 协同攻击	IP、流量、时间、域	同一 IP 段同时向≥2 个域发起流量攻击，流量≥5Gbps	紧急

7.3 统计分析

7.3.1 频次分析

统计IP、账号、资产的告警频次、访问频次，识别高频异常主体。

7.3.2 趋势分析

分析安全事件日/周/月趋势，识别突发异常（如告警量突增3倍）。

7.3.3 对比分析

跨域对比安全指标，识别差异异常（如A域漏洞数量远超其他域）。

7.3.4 阈值分析

基于3σ原则、Z-score设定动态阈值，异常识别准确率≥90%。

7.4 智能关联分析

7.4.1 算法要求

支持以下机器学习算法：

a）监督学习：随机森林、SVM、XGBoost（威胁分类准确率≥92%）；

b）无监督学习：孤立森林、DBSCAN、K-means（异常检测准确率≥88%）；

c）深度学习：CNN、LSTM（时序流量分析、恶意代码检测准确率≥90%）。

7.4.2 模型训练

应满足以下要求：

a）训练数据集：跨域历史安全数据≥1000万条，标注准确率≥95%；

b）模型更新：每周增量训练，每月全量更新，模型准确率下降≤2%。

7.5 知识图谱关联分析

7.5.1 图谱构建

跨域安全知识图谱由实体、关系和属性三部分构成，具体如下：

a）实体：IP、域名、账号、资产、漏洞、恶意样本、攻击组织；

b）关系：攻击、利用、控制、访问、包含、同源、关联；
c）属性：实体特征、行为特征、时间特征、域特征。

7.5.2 图谱推理

通过路径分析、子图匹配、链路预测，实现：
a）攻击溯源：从告警反向追溯攻击源、攻击路径、攻击入口；
b）威胁扩展：识别关联威胁、潜在受害者、隐藏攻击节点；
c）团伙识别：发现协同攻击组织、恶意IP团伙。

7.6 关联分析结果输出

7.6.1 输出内容

应包含威胁ID、威胁类型、告警等级、涉及域、关联IP/资产/账号、攻击链阶段、风险值、处置建议、证据数据。

7.6.2 风险值

采用0～100分计分制：≥80分为极高风险，60～79分为高风险，40～59分为中风险，20～39分为低风险，＜20分为无风险。

7.6.3 输出格式

支持JSON、XML、CSV、PDF，兼容跨域协同平台接口。

8 安全与隐私保护要求

8.1 身份与访问控制

8.1.1 采用多因素身份认证（账号密码+短信/令牌/生物特征），认证通过率100%，防暴力破解（5次失败锁定10分钟）。

8.1.2 基于RBAC实施权限管控，分为管理员、分析师、审计员、普通用户，权限最小化，越权访问阻断率100%。

8.1.3 跨域数据访问应进行授权审批，一级数据双人审批，访问日志留存≥3年。

8.2 数据传输安全

8.2.1 跨域数据传输应采用TLS1.3协议，并使用国密SM4算法进行加密保护，加密强度不低于256位。

8.2.2 应采用SM3哈希算法对传输数据进行完整性校验，校验不通过的数据应予以自动丢弃。

8.2.3 传输过程应具备防重放、防篡改能力，相关攻击行为拦截率应达到100%。

8.3 数据存储安全

8.3.1 敏感数据应采用SM4算法加密存储，实行密钥分级管理，核心密钥应离线保管；

8.3.2 数据应定期备份，执行每日增量备份、每周全量备份策略，备份数据实现异地存储，数据恢复成功率不低于100%。

8.3.3 存储介质应具备防篡改、防泄露能力，所有访问轨迹应全程记录。

8.4 隐私保护

8.4.1 个人信息处理应符合GB/T 35273的要求，采取匿名化、去标识化措施，实现个人信息泄露率为0。

8.4.2 跨域数据共享应遵循“最小必要”原则，不得传输与业务无关的敏感信息。

8.4.3 隐私合规审计应实现全覆盖，审计合规率不低于100%。

8.5 安全审计

8.5.1 应对登录、访问、查询、修改、导出、删除等全操作行为开展审计，完整采集操作日志。

8.5.2 日志应包含操作人、时间、IP地址、操作内容、执行结果及操作对象，日志完整率不低于100%。

8.5.3 应对异常操作进行实时审计分析，审计告警响应时间不大于1分钟。

9 测试与验证

9.1 一般要求

系统的功能、性能及安全要求应通过测试验证，测试环境应模拟实际跨域协同运行场景，测试数据应具备典型性与代表性，测试步骤应可复现，测试结果应满足本文件的全部技术要求。

9.2 功能验证

9.2.1 验证内容

应对数据采集、数据预处理、数据融合、关联分析、分析结果输出等功能开展验证。

9.2.2 验证方法

在模拟跨域场景下，接入多源安全数据，启动系统各功能模块，通过运行日志、流程跟踪、结果回显等方式，观察功能执行过程与输出结果。

9.2.3 判定依据

各功能模块应正常启动、流程完整、无异常中断，输出内容应准确、完整，符合本文件相关功能规定。

9.3 性能验证

9.3.1 验证内容

应对表1规定的数据处理性能、关联分析性能、系统可靠性指标进行测试。

9.3.2 验证方法

在满负载运行条件下，采用流量测试仪、性能监测工具、计时统计工具等，连续运行不少于72h，记录数据融合吞吐量、数据处理延迟、威胁检测率、误报率、MTTD、系统可用性、数据丢失率、故障恢复时间等指标。

9.3.3 判定依据

全部测试结果应满足表1中对应的数值要求，任一指标不满足则判定性能不符合要求。

9.4 安全验证

9.4.1 验证内容

应对系统脆弱性与抗攻击能力进行验证。

9.4.2 验证方法

采用通用漏洞扫描工具开展漏洞扫描，按照典型网络攻击方法实施渗透测试，检查高危漏洞、越权访问、数据泄露等安全问题。

9.4.3 判定依据

系统不应存在高危漏洞，安全机制应有效，未出现越权访问、数据被篡改或泄露等情况。

9.5 兼容性验证

9.5.1 验证内容

应对系统与主流安全设备、安全系统的数据接入兼容性进行验证。

9.5.2 验证方法

接入不同厂商、不同类型安全设备，统计系统支持的协议种类与实际接入成功数量，计算协议支持率。

9.5.3 判定依据

数据接入协议支持率应不低于95%，数据接入稳定、无丢包、无解析异常。

10 运维管理

10.1 运维组织

应建立专门的跨域协同安全数据融合与关联分析系统运维组织，运维组织至少应设置以下岗位，并明确岗位职责边界、协同流程与责任认定机制：

a）运维负责人：全面负责系统整体运维策略制定、资源统筹、跨域协调、重大事件决策及运维质量监督；

b）系统管理员：负责系统基础设施、网络环境、计算资源、存储资源、中间件与数据库的日常配置、状态监控、故障排查与性能调优；

c）数据运维工程师：负责跨域安全数据接入质量监控、数据缺失核查、异常数据定位、融合任务调度管理、数据生命周期管理及存储资源扩容规划

d）安全分析师：负责关联分析规则、机器学习模型、威胁知识图谱的日常维护、效果验证、误报优化与漏报补齐；

e）安全审计员：依据GB/Z 41290开展全流程操作审计、权限行为审计、数据访问审计、跨域共享行为审计。

10.2 日常运维

10.2.1 每日巡检

每日对系统运行状态、跨域数据接入情况、性能指标及安全告警开展全面巡检，巡检覆盖率达到100%，异常情况及时记录并处理。

10.2.2 每周维护

每周进行数据清理、索引优化、分析模型更新和关联规则优化，保障系统高效运转。

10.2.3 每月评估

每月对系统性能、分析效果及安全状况开展综合评估，形成正式评估报告，为系统持续优化提供支撑。

10.3 应急运维

10.3.1 建立应急预案

针对系统故障、数据泄露、大规模攻击、跨域协同中断等场景制定专项应急预案，规范处置流程。

10.3.2 应急响应

故障响应时间不超过15分钟，一般故障处置完成时间不超过30分钟。

10.3.3 应急演练

每季度至少1次跨域应急演练，演练覆盖率100%。

10.4 版本管理

应满足以下要求：

a）对系统版本、规则版本、模型版本实行统一管理，建立变更申请、审批、记录与回溯机制；

b）功能版本每月更新一次，安全补丁根据漏洞情况及时更新，确保系统安全性与功能稳定性；

c）所有版本操作均留存日志，便于追溯与审计。