ICS 35.030
CCS L 80

T/JQR

安 徽 省 机 器 人 学 会 团 体 标 准

T/JQR 21—2026

异构网络端边云协同主动防御技术要求

General technology requirements for heterogeneous network client-edge-cloud collaboration active defense

2026－4－7 发布　　2026－4－14 实施

安徽省机器人学会　　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。

本文件由安徽三实软件科技有限公司提出。

本文件由安徽省机器人学会归口。

本文件起草单位：安徽三实软件科技有限公司、安徽工业大学、北京交通大学、数据空间研究院、奇安信科技集团股份有限公司、天翼支付科技有限公司、安徽省质量和标准化研究院、安徽省电子产品监督检验所。

本文件主要起草人：吴宣够、王超、张焘、马韵洁、郑晓峰、刘奇、杨彬彬、刘吉强、陈爱华、王灿、张卫东、赵伟、刘翔宇、陈宇、王鹏、谢鲜桠、侯亚东、周恒宝、张志生、王东亚、季静、李红。

异构网络端边云协同主动防御技术要求

1 范围

本文件规定了异构网络环境下端边云协同主动防御系统的缩略语、系统架构与功能要求、技术要求和测试方法。

本文件适用于电子政务、能源、金融、工业等关键信息基础设施的异构网络端边云协同主动防御系统的设计、开发、部署、测试。

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 25069 信息安全技术 术语

3 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

异构网络 heterogeneous network

由多种不同厂商、不同类型、不同协议的网络设备和安全设备组成的复合网络环境，具有终端设备类型多元化、边缘节点分布泛化的特点。包括但不限于防火墙、入侵检测/防御系统（IDS/IPS）、Web 应用防火墙（WAF）、态势感知平台、终端检测与响应系统（EDR）等。

3.2

端边云协同 client-edge-cloud collaboration

在端侧（终端Agent）、边缘侧（数字化统一运营平台/边缘安全联动决策网关）和云端（智能研判与情报生产中心）之间，建立覆盖“发现→上报→研判→处置→验证”全链路的数据采集、威胁分析、策略编排和联动处置的多层级协同机制。

3.3

主动防御 active defense

区别于被动检测告警的安全防护模式，通过威胁主动感知、智能研判决策、深度强化学习驱动的策略编排与端边云联动处置，结合终端网络属性高频跳变等主动干扰手段，实现对已知和未知威胁的自动化闭环响应。

3.4

安全能力总线 security capability abstraction bus

通过定义统一的安全能力描述语义与标准化适配接口（软件定义安全接口），将多厂商异构安全设备的检测、阻断、审计等安全能力封装为可寻址、可编排的原子安全服务的中间件架构。

3.5

告警聚合压缩 alert aggregation and compression

以攻击源IP为核心视角，融合事件类型、目标端口、时间窗口、资产属性等多维特征，通过语义分析与关联聚类将海量离散告警归并为结构化威胁事件的过程。

3.6

端侧 Agent endpoint agent

部署于终端设备的轻量化安全代理软件，具备威胁事件查询、网络进程溯源定位、应急响应与联动阻断能力，实现安全事件在终端侧的“最后一公里”处置闭环。

3.7

加密流量威胁识别 encrypted traffic threat identification

在不对加密流量进行解密的前提下，通过融合流量统计特征、时序行为模式与协议握手元数据等多模态信息，识别加密流量中隐匿的恶意行为的技术方法。

3.8

深度强化学习驱动编排 deep reinforcement learning driven orchestration

以DRL算法为核心，根据当前网络威胁态势和资源状态自动生成全局最优防御策略，通过软件定义安全接口动态编排底层异构设备服务链的智能决策方法。

3.9

协同演化 collaborative evolution

通过跨域联邦学习、小样本知识蒸馏与持续学习机制，使分布式部署的端边云多层防御节点在数据不出域前提下共享防御经验，并持续适应新型威胁的能力演化过程。

3.10

联邦蒸馏 federated distillation

将知识蒸馏技术与联邦学习框架相结合的协同建模方法，通过在各参与节点之间传递模型软标签或中间表征（而非原始数据或完整模型参数），在数据不出域前提下实现轻量化的跨域知识聚合。

3.11

资产指纹 asset fingerprint

通过主动探测与被动流量分析获取的目标资产特征信息集合，包括操作系统类型与版本、开放端口与服务、Web 应用框架、CMS 类型、中间件组件及其版本等。

3.12

移动目标防御 moving target defense

通过动态改变终端网络属性（IP 地址、端口号、协议栈特征等），增加攻击者侦察和利用难度的主动防御技术，可实现终端网络属性的高频跳变。

3.13

安全编排自动化与响应（SOAR） security orchestration, automation and response（SOAR）

安全编排自动化与响应（SOAR），一种通过预定义剧本（Playbook）实现安全事件自动化响应的技术框架，可驱动安全能力总线执行跨设备联动处置。

4 缩略语

下列缩略语适用于本文件。

CMS：内容管理系统（ Content Management System）

CNVD：国家信息安全漏洞共享平台（China National Vulnerability Database）

CNNVD：中国国家信息安全漏洞库（China National Vulnerability Database of Information Security）

CVE ：公共漏洞和暴露（Common Vulnerabilities and Exposures）

DDoS：分布式拒绝服务（Distributed Denial of Service）

DRL ：深度强化学习（Deep Reinforcement Learning ）

EDR：终端检测与响应（Endpoint Detection and Response）

MTD ：移动目标防御（Moving Target Defense）

IDS：入侵检测系统（Intrusion Detection System）

IPS：入侵防御系统（Intrusion Prevention System）

SDK：软件开发工具包（Software Development Kit）

SOAR：安全编排自动化与响应（Security Orchestration, Automation and Response）

TLS：传输层安全协议（Transport Layer Security）

WAF：Web应用防火墙（Web Application Firewall）

5 系统架构与功能要求

5.1 系统架构

5.1.1 架构图

异构网络端边云协同主动防御系统应采用“端—边—云”三层协同架构，覆盖“发现→上报→研判→处置→验证”五大环节，系统构架图见图1。

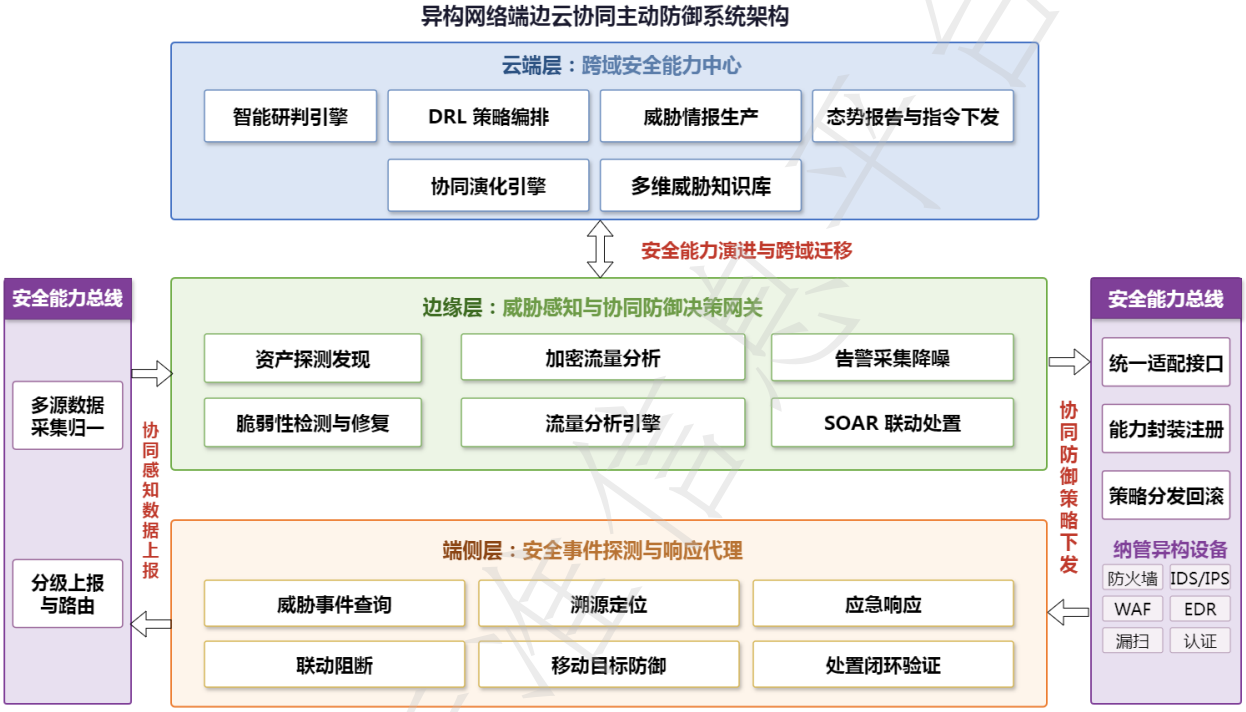

图1 异构网络端边云协同主动防御系统构架图

5.1.2 云端层

部署于中心数据中心或政务云，作为全局智能中枢，负责深度分析与决策指挥。核心功能应包括但不限于：

——数据汇聚：各边缘节点降噪聚合后的威胁事件统一上报云端；

——智能研判：AI 研判分析智能体与技术专家双重协同，AI 智能体负责机器学习模型驱动的模式识别与自动化分析，专家团队负责经验研判、威胁验证与决策支持；

——情报生产：构建威胁数据集，提炼高价值威胁 IP，生产威胁情报库、处置指令与态势报告；

——指令下发：研判后事件标记自动下发，触发边缘层联动处置；

——协同演化引擎：基于联邦蒸馏与持续学习机制，实现跨域防御知识聚合与模型迭代更新。

5.1.3 边缘层

5.1.3.1 部署于用户侧网络边缘或区域汇聚节点，承担数据处理、安全检测与联动控制的枢纽角色。核心功能包含两个方向：

——脆弱性发现方向：资产自动探测发现（内外网资产）、联动安全组件检测脆弱性、脆弱性修复与验证闭环；

——威胁联动治理方向：采集现场所有安全设备数据、降噪聚合识别高价值威胁事件、接收云端指令联动设备执行处置。

5.1.4 端侧层

端侧Agent部署于终端设备，通过“获取事件→溯源定位→上报数据→执行指令→验证闭环”处置流程解决安全事件闭环的“最后一公里”问题。核心能力应包括但不限于：

——威胁事件查询：联动边缘平台查询终端存在的威胁事件；

——溯源定位：溯源定位相关网络进程，通过网络分析、进程监听、行为溯源、文件扫描等手段完成内部溯源定位，实现事件验证与威胁定位；

——应急响应：下沉到事件最末端，形成处置闭环；
——联动阻断：执行网络隔离、进程封禁等阻断动作，快速隔离与阻断攻击路径。

5.1.5 安全能力总线

贯穿“端—边—云”三层，通过软件定义安全接口统一纳管防火墙、IDS/IPS、WAF、漏洞扫描、上网认证、EDR 等异构安全设备，将其安全能力封装为可编排的原子服务。

5.2 功能模块

在“端—边—云”各层系统功能应至少包含以下模块：
——云端层；
- 智能研判与情报生产模块；
- 指纹规则库与漏洞库管理模块；
- 联邦蒸馏与协同演化模块；
- 深度强化学习驱动编排与自动响应模块；

——边缘层
- 资产发现与指纹识别模块；
- 加密流量分析与威胁识别模块；
- 异构设备统一适配与纳管模块；
- 联邦蒸馏与协同演化模块；

——端侧层
- 多源告警采集与聚合归并模块；
- 端侧 Agent 威胁感知与溯源阻断模块；
- 移动目标防御模块；
- 深度强化学习驱动编排与自动响应模块。

5.3 协同工作机制

“端—边—云”三层架构之间应形成紧密的数据与指令流转闭环，整体形成“端侧精准定位→边缘汇聚研判→云端智能决策→指令逐级下发→端侧执行验证”的完整安全运营闭环。整体工作机制按表1执行。

表1 端边云协同工作机制要求

层级	核心职责	上行数据	下行指令
云端	智能研判、情报生产、全局决策、协同演化	—	处置指令、威胁情报、模型更新、态势报告
边缘	数据采集与降噪、安全检测、联动控制	高价值威胁事件上报	接收并执行云端指令，下发至端侧与安全设备
端侧	威胁定位、溯源取证、联动阻断、主动防御	溯源数据上报	接收处置指令并执行

6 技术要求

6.1 风险感知

6.1.1 资产识别覆盖率

6.1.1.1 系统应支持对目标网络范围内存活资产的自动化发现与识别，采用主动探测与被动流量分析相结合的方式，主动探测应支持基于多协议（TCP/UDP/ICMP/SNMP 等）的端口扫描与服务探测，被动分析应支持从镜像流量中提取资产特征信息。覆盖资产类型应包括但不限于服务器、网络设备、安全设备、终端主机、物联网设备、Web 应用等，在线资产识别覆盖率应≥95 %。

6.1.1.2 应支持资产组件级识别，对已识别资产的操作系统类型与版本、开放服务与端口、Web 框架与中间件及版本、CMS 类型等组件信息识别准确率应≥90 %。
6.1.1.3 对新入网资产应支持持续发现与更新，发现周期应≤24 h（周期扫描模式）或≤10 min（实时流量分析模式）。
6.1.1.4 应建立"资产—漏洞—威胁"动态关联图谱，支持脆弱性自动关联与风险量化。
6.1.1.5 端侧 Agent 应支持终端资产信息主动上报，包括主机软硬件配置、已安装应用、开放服务等信息，补充边缘层资产发现盲区。

6.1.2 加密流量威胁识别率

6.1.2.1 系统应支持在不解密条件下对 TLS/SSL 加密流量进行威胁识别，采用多模态融合分析方法，融合流量统计特征（包长分布、包间隔、流持续时间等）、时序行为模式与 TLS 握手元数据（密码套件、扩展字段、证书链特征等），识别准确率应≥97 %，误报率应≤3 %，支持识别的加密流量威胁类型应≥10 种。
6.1.2.2 应支持基于深度学习的加密流量分类，涵盖但不限于加密恶意通信识别、匿名网络流量识别、加密隧道检测、DDoS 攻击流量识别等场景。
6.1.2.3 应支持模型增量更新与在线微调，适应加密协议版本演进和新型攻击变种。
6.1.2.4 加密流量分析结果应与资产指纹关联，定位受威胁的具体终端与服务。

6.1.3 流量分析支持速率

6.1.3.1 系统应支持对网络流量的实时采集与在线分析，采集方式应支持镜像流量、分光采集和 NetFlow/sFlow 等模式。流量分析引擎应支持并行处理架构与横向扩展，并满足以下要求：

a) 单节点流量分析处理速率应≥10 Gbps（基础配置），通过集群扩展应支持≥40 Gbps；
b) 流量元数据索引写入延迟应≤5 s，检索响应时间应≤3 s（千万级记录条件下）；
c) 额定处理速率下丢包率应≤0.1 %。

6.1.3.2 应支持流量元数据的结构化存储与快速检索，支撑事后追溯分析。

6.1.4 告警聚合压缩比

6.1.4.1 系统应支持对多源异构安全设备产生的原始告警进行统一采集、标准化解析与智能归并，同一攻击行为的告警归并准确率应≥90 %，处理延迟应≤30 s。
6.1.4.2 告警归并应以攻击源 IP 为核心视角，融合事件类型、目标端口、时间窗口、资产属性等多维特征，采用语义分析实现跨设备、跨类型的告警关联聚类，原始告警到结构化威胁事件的压缩比应≥10:1。
6.1.4.3 应支持自适应时间窗口，根据攻击场景（扫描、暴力破解、持续渗透等）动态调整聚合策略。
6.1.4.4 归并后的威胁事件应保留原始告警关联链，支持向下钻取还原。
6.1.4.5 边缘层应完成告警降噪与价值筛选后，仅将高价值威胁事件上报云端。

6.2 协同防御

6.2.1 攻击扫描命中率

6.2.1.1 系统应支持对网络环境中的攻击扫描行为（端口扫描、漏洞扫描、Web 扫描、弱口令扫描等）进行检测与识别。
6.2.1.2 攻击扫描检测应融合流量特征分析、行为基线偏离检测和威胁情报匹配等多维手段，并满足下列要求：

a) 攻击扫描命中率：对已知攻击扫描行为的检测命中率应≥95 %；
b) 攻击研判准确率：对攻击事件研判分析的准确率应≥92 %；
c) 扫描行为识别类型：应支持识别的攻击扫描类型≥8 种。

6.2.1.3 云端智能研判应支持 AI 研判分析智能体与技术专家双重协同，AI 智能体负责模式识别与自动化分析，专家团队负责经验研判与威胁验证。
6.2.1.4 应支持攻击者 IP 历史行为画像关联，辅助误报过滤与攻击意图判定。
6.2.1.5 端侧 Agent 应支持对终端上发生的攻击扫描行为进行本地检测与上报，补充网络层检测的盲区。

6.2.2 防御成功率

6.2.2.1 系统应支持基于 DRL 的全局防御策略智能生成，根据当前网络威胁态势与资源状态自动计算最优防御动作组合。对已确认威胁事件的端边云联动处置成功率应≥94 %，从研判结论产生到防御策略执行完成的端到端响应时间应≤60 s，关键场景应支持毫秒级联动响应。
6.2.2.2 应通过软件定义安全接口动态编排底层异构设备服务链，联动处置应支持跨设备协同执行，包括但不限于防火墙 IP/端口封禁、IPS 规则下发、WAF 规则更新、EDR 进程隔离/文件查杀、上网认证设备用户阻断等。
6.2.2.3 端侧 Agent 应支持终端级联动阻断，包括网络隔离、进程封禁、文件隔离等处置动作，实现威胁事件的末端处置闭环。端侧 Agent 接收处置指令后的执行成功率应≥95 %。
6.2.2.4 应支持移动目标防御技术，通过终端网络属性（IP 地址、端口号等）的高频跳变增加攻击者侦察与利用难度。
6.2.2.5 防御执行结果应逐级回传至云端管理平台进行效果验证，形成“发现—上报—研判—处置—验证”全链路闭环。已触发处置流程的事件应 100 %具有端边云全链路执行结果回传和效果验证记录。
6.2.2.6 应具备防御策略冲突检测与消解能力，避免跨设备策略矛盾导致业务中断。

6.2.3 防御策略分发耗时

6.2.3.1 系统应支持通过安全能力抽象总线向多台异构安全设备及端侧 Agent 并行分发防御策略。向单台安全设备或端侧 Agent 完成策略下发的耗时应≤3 s，向≤50 台异构安全设备并行分发同一策略的总耗时应≤10 s。
6.2.3.2 策略分发应采用统一语义描述，由设备适配层自动转换为各厂商设备的原生配置格式，端侧 Agent 自动解析为本地处置指令；
6.2.3.3 应支持策略下发的原子性保障,单台设备或单 Agent 策略下发失败不应影响其他节点的正常执行，并应自动触发重试或告警。策略分发的成功率应≥99.5 %
6.2.3.4 应支持策略的紧急撤回与回滚机制，在误封误阻场景下能够快速恢复业务，紧急策略撤回完成时间应≤5 s。
6.2.3.5 策略分发路径应覆盖云端→边缘→端侧三级传递链路，支持逐级下发与直达下发两种模式。

6.3 能力演化

6.3.1 新威胁识别率

6.3.1.1 系统应支持对零日攻击、新型变种恶意代码、未知攻击模式等新威胁的发现与识别。
6.3.1.2 应采用小样本知识蒸馏与个性化联邦学习相结合的协同建模方法，针对网络安全事件天然稀疏、跨域数据隐私约束的特点，在数据不出域前提下实现多源异构节点间防御经验的聚合。通过联邦蒸馏协同学习后的模型对新威胁样本的识别率应≥95 %，联邦协同模型检测精度较各节点独立训练应提升≥15 %。
6.3.1.3 应引入持续学习机制，保留历史知识并快速适应新威胁，新威胁学习收敛速度较全量重训练应提升≥ 40 %，避免“知识遗忘”（灾难性遗忘）。
6.3.1.4 应具备联邦学习投毒攻击防御机制，保障协同学习过程的可信性。
6.3.1.5 学习新威胁后，对旧有已知威胁的识别能力不应显著下降，学习新威胁后对旧有威胁的识别保持率应≥95 %。

6.3.2 胁知识跨设备迁移时间

6.3.2.1 系统应支持将云端更新的威胁检测模型、规则策略沿“云端→边缘→端侧”路径逐级同步迁移，从云端发起威胁知识更新到边缘网关完成加载并生效应≤5 min。
6.3.2.2 边缘安全联动决策网关应具备模型热更新机制，接收云端模型更新后快速加载生效；
6.3.2.3 端侧 Agent 应支持接收边缘层下发的轻量化模型或规则增量更新,从云端发起到端侧 Agent 完成更新应≤15 min
6.3.2.4 知识迁移应支持差量更新模式，仅传输模型参数差异或增量规则，降低带宽占用；
6.3.2.5 迁移过程应不中断设备正常防护功能，支持热更新机制，知识更新过程中防护功能中断时间应为 0（热更新），知识迁移完成后应自动校验完整性，校验通过率应达 100 %。

6.3.3 规则库

6.3.3.1 资产指纹库

6.3.3.1.1 系统应构建覆盖主流操作系统、Web 服务器、应用框架、CMS 平台、中间件组件、IoT 设备等的资产指纹规则库，资产组件级指纹规则总数应≥ 4000 种，覆盖国内外主流 CMS 系统指纹≥ 1500 种。

6.3.3.1.2 指纹规则应支持多维度匹配，包括但不限于：HTTP 响应头特征、页面内容特征、端口服务 Banner、协议握手特征、SNMP OID 等。

6.3.3.1.3 应支持指纹规则的版本管理与增量扩展，支持用户自定义指纹规则导入。

6.3.3.1.4 指纹库应覆盖国产化软硬件生态，包括国产操作系统、国产数据库、国产中间件等，覆盖主流国产操作系统、数据库、中间件指纹≥500 条。

6.3.3.1.5 应支持基于指纹特征融合与增量学习的指纹库自动扩充机制。

6.3.3.2 漏洞库

6.3.3.2.1 系统应建立与 CVE、CNVD、CNNVD 等权威漏洞库对接的安全漏洞知识库，漏洞库收录漏洞总数应≥200000 条，对近 3 年公开披露的高危及以上漏洞（CVSS≥7.0）覆盖率应≥95 %。

6.3.3.2.2 漏洞信息应包含漏洞编号、影响组件与版本范围、危害等级（CVSS 评分）、漏洞类型、修复建议、关联 PoC/EXP 信息等结构化字段。漏洞记录中含影响版本、危害等级、修复建议等完整字段的比例应≥90 %。

6.3.3.2.3 应支持漏洞与资产指纹的自动关联匹配，实现“发现资产→匹配漏洞→评估风险”的自动化流程。

6.3.3.2.4 应支持漏洞的可利用性标注，区分理论漏洞与实际可利用漏洞。

6.3.3.3 威胁检测库

6.3.3.3.1 系统应构建覆盖网络层、应用层、主机层的多维威胁检测规则库，威胁检测规则总数应≥5000 条；

6.3.3.3.2 规则应覆盖应满足以下要求：

a) 覆盖网络攻击、Web 攻击、恶意代码、异常行为、数据泄露等≥5 大类威胁场景；
b) 覆盖 OWASP Top 10、MITRE ATT&CK 主要战术与技术、常见恶意软件行为特征等威胁场景；
c) 覆盖 MITRE ATT&CK 企业矩阵中≥80 %的战术阶段。

6.3.3.3.3 应支持基于 Sigma、YARA、Snort/Suricata 等通用格式的规则导入与转换；

6.3.3.3.4 应支持规则的优先级分层与场景标签管理，便于按行业（电子政务、能源、金融等）、场景进行规则集定制；

6.3.3.3.5 端侧 Agent 应支持加载轻量化威胁检测规则集，在终端本地执行主机层检测。

6.3.3.4 更新频率

6.3.3.4.1 系统应建立常态化的规则库更新机制，包括威胁检测规则、漏洞特征、资产指纹等的持续更新，威胁检测规则库应支持≥1 次/周的常规更新

6.3.3.4.2 应支持与外部威胁情报源（CVE/CNVD/CNNVD 等）的自动对接与增量同步，针对高危漏洞和重大安全事件的紧急规则应在公开披露后≤24 h 内发布。

6.3.3.4.3 云端情报生产中心应持续提炼高价值威胁 IP 和攻击特征，自动生成并下发新规则。

6.3.3.4.4 应支持基于实战攻防演练和用户自定义场景的定制化规则生产与导入。

6.3.3.4.5 规则更新应经过自动化兼容性测试后方可下发，避免规则冲突导致误报激增或防护缺失，新增/更新规则应 100 %经过自动化兼容性与误报测试。

6.3.4 安全设备适配类别

6.3.4.1 系统应通过安全能力抽象总线支持多厂商异构安全设备的统一纳管，设备以原子安全服务形式动态注册。

6.3.4.2 应提供标准化设备适配接口规范和 SDK，支持新设备类型的快速适配接入，基于标准 SDK 的新设备适配接入周期应≤5 个工作日，构建开放的安全生态。

6.3.4.3 适配层应屏蔽不同厂商设备的管理协议差异（SSH/SNMP/RESTful API/Syslog/NetConf 等），向上提供统一的能力调用语义，应支持≥ 4 种设备管理协议（含 SSH、SNMP、RESTful API、Syslog 等）。
6.3.4.4 应支持设备能力自动发现与注册，纳管后的设备应能参与 SOAR 编排引擎的联动处置流程。
6.3.4.5 联动对象应覆盖业务系统（OA 系统、监控平台、管理系统等）、网络设备（路由器、交换机、防火墙等）和安全设备（IDS/IPS、WAF、态势感知、防毒墙、EDR 等），应支持纳管的安全设备类别≥ 6 类（含防火墙、IDS/IPS、WAF、漏洞扫描系统、上网行为管理/认证系统、EDR）。
6.3.4.6 应覆盖国内主流安全厂商的核心安全产品，支持多部门、多厂商设备的联防联控。每类设备应至少适配≥3 家国内主流厂商。

7 测试方法

7.1 测试环境

7.1.1 网络

测试环境应搭建包含云端、边缘和终端三层架构的完整测试网络。云端部署智能研判与情报生产中心，边缘层部署数字化统一运营平台，终端部署≥10台安装端侧Agent的主机。接入≥3家不同厂商的安全设备（防火墙、IDS/IPS、WAF至少各一台），网络带宽≥10 Gbps。

7.1.2 数据

测试数据应包含：
a) 标注的加密流量数据集（含正常加密流量和恶意加密流量样本）；
b) 多源异构安全设备产生的原始告警日志（≥10 万条）；
c) 已知攻击行为与攻击结果的标注数据集；
d) 目标网络的资产清单基线（作为识别覆盖率验证的 ground truth）；
e) 新威胁样本数据集（不在系统初始训练集中的威胁类型）。

7.1.3 工具

测试应配备流量回放工具、攻击模拟工具、性能测试工具、日志分析工具和终端威胁模拟工具。

7.2 风险感知测试

7.2.1 资产识别覆盖率测试

资产识别覆盖率按如下方法进行测试：
a) 建立目标网络资产清单基线，记录全部在线资产数量 N_total（含已部署端侧 Agent 的终端）；
b) 启动系统资产发现功能（含边缘层主动探测与端侧 Agent 主动上报），执行完整扫描周期；
c) 记录系统识别到的资产数量 N_identified；
d) 计算资产识别覆盖率=（N_identified / N_total）×100 %；

7.2.2 加密流量威胁识别率测试

加密流量威胁识别率按如下方法进行测试：
a) 准备加密流量测试数据集，包含≥1000 条标注样本（正常样本与恶意样本比例不低于 3:1）；
b) 将测试数据通过流量回放工具注入测试网络；
c) 记录系统识别结果，与标注标签对比；
d) 计算识别准确率。计算方式为：（正确识别的恶意样本数/恶意样本总数）×100 %；
e) 计算误报率。计算方式为：（误报为恶意的正常样本数/正常样本总数）×100 %。

7.2.3 流量分析支持速率测试

流量分析支持速率按如下方法进行测试：
a) 使用流量发生器以 10 Gbps 的指定速率向系统发送混合流量；
b) 持续运行≥30 min，记录系统处理的流量总量和丢包数量；
c) 计算实际处理速率和丢包率；

d) 逐步提升流量速率，记录系统性能拐点。

7.2.4 告警聚合压缩比测试

告警聚合压缩比按如下方法进行测试：

a) 导入多源异构设备告警日志≥10 万条（应包含≥3 种设备类型的告警）；
b) 启动告警聚合功能，记录输出的结构化威胁事件数量；
c) 计算压缩比。计算方式为：原始告警数量/聚合后事件数量；
d) 随机抽取≥30 个聚合事件，人工验证归并准确性。

7.3 协同防御指标测试

7.3.1 攻击扫描命中率测试

攻击扫描命中率按如下方法进行测试：

a) 使用攻击模拟工具对测试网络发起≥8 种类型的攻击扫描行为(含端口扫描、漏洞扫描、Web 目录扫描等），同时在终端侧模拟主机层攻击扫描行为；
b) 记录系统（含边缘层网络检测与端侧 Agent 主机检测）检测命中的攻击扫描事件数量与攻击扫描总数；
c) 计算命中率。计算方式为：（检测到的扫描数/实际发起的扫描数）×100 %；
d) 对命中的攻击事件，验证研判结论的准确性。

7.3.2 防御成功率测试

防御成功率按如下方法进行测试：

a) 发起≥50 起模拟攻击事件（含不同威胁等级和攻击类型，覆盖网络层与终端层攻击场景）；
b) 记录系统自动触发端边云联动防御的事件数量和防御执行结果（含边缘层设备联动与端侧 Agent 阻断）；
c) 验证每起事件的全链路处置闭环状态(“发现→上报→研判→处置→验证”五环节是否完整)；
d) 计算防御成功率。计算方式为：（成功阻断的事件数/已确认威胁事件数）×100 %。

7.3.3 防御策略分发耗时测试

防御策略分发耗时按如下方法进行测试：

a) 在测试环境中接入≥3 类、≥10 台异构安全设备及≥10 台端侧 Agent；
b) 触发安全事件，记录从研判结论产生到单设备/单 Agent 策略下发完成的时间；
c) 触发批量策略分发，记录≤50 台设备全部完成的总耗时；
d) 测试策略回滚功能，记录紧急撤回完成时间。

7.4 能力演化指标测试

7.4.1 新威胁识别率测试

新威胁识别率按如下方法进行测试：

a) 准备新威胁测试数据集（所含威胁类型不在系统初始训练集中）；
b) 记录联邦蒸馏协同学习前各节点独立模型的新威胁识别率；
c) 执行联邦蒸馏协同学习流程后，记录联邦模型的新威胁识别率；
d) 计算精度提升比。计算方式为：((联邦模型精度-独立模型平均精度)/独立模型平均精度）×100 %；
e) 验证学习新威胁后旧威胁识别保持率。

7.4.2 威胁知识跨设备迁移时间测试

威胁知识跨设备迁移时间按如下方法进行测试：

a) 在云端发起威胁知识（检测模型/规则策略）更新；
b) 记录边缘网关完成知识加载并生效的时间 T_edge；
c) 记录端侧 Agent 完成知识更新的时间 T_endpoint；

d) 验证更新期间防护功能是否中断；
e) 验证迁移完成后的完整性校验结果。

7.4.3 规则库测试

7.4.3.1 指纹规则库数量测试

指纹规则库数量按如下方法进行测试：
a) 导出系统当前指纹规则库全量数据，统计组件级指纹规则种类总数；
b) 验证指纹分类覆盖范围（操作系统、Web 服务器、CMS、中间件、IoT 等）；
c) 统计国产化组件指纹覆盖数量。

7.4.3.2 漏洞库数量测试

漏洞库数量按如下方法进行测试：
a) 导出系统漏洞库统计数据，核验漏洞总量；
b) 随机抽取近 3 年高危漏洞列表（CVSS ≥ 7.0）≥ 100 条，逐一核查系统覆盖情况；
c) 抽取≥ 50 条漏洞记录，验证信息完整性（影响版本、等级、修复建议等字段完整率）。

7.4.3.3 威胁检测规则库数量测试

威胁检测规则库数量按如下方法进行测试：
a) 导出系统威胁检测规则库统计数据，核验规则总量与分类；
b) 对照 MITRE ATT&CK 企业矩阵，验证战术阶段覆盖情况；
c) 核验规则是否覆盖网络攻击、Web 攻击、恶意代码、异常行为、数据泄露等主要类别；
d) 验证端侧 Agent 可加载的轻量化规则集数量。

7.4.3.4 更新频率测试

更新频率按如下方法进行测试：
a) 查阅系统近 3 个月的规则库更新日志，统计常规更新频率；
b) 模拟高危漏洞公开披露场景，记录紧急规则发布时间；
c) 验证每次规则更新的自动化测试记录。

7.4.4 安全设备适配类别测试

安全设备适配类别按如下方法进行测试：
a) 查阅系统已适配的安全设备类别和厂商清单；
b) 对每类设备至少选 1 台进行实际纳管操作验证（设备注册、能力发现、策略下发、结果回传）；
c) 基于标准 SDK 对 1 款新型设备进行适配接入，记录适配周期；
d) 验证支持的设备管理协议类型；
e) 验证联动对象是否覆盖业务系统、网络设备、安全设备三大类别。

参 考 文 献

[1] GB/T 25069—2022 信息安全技术 术语
[2] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[3] GB/T 39204—2022 信息安全技术 关键信息基础设施安全保护要求
[4] GB/T 20984—2022 信息安全技术 信息安全风险评估方法
[5] GB/T 36643—2018 信息安全技术 网络安全威胁信息格式规范
[6] GB/T 30279—2020 信息安全技术 网络安全漏洞分类分级指南
[7] MITRE ATT&CK 框架 (https://attack.mitre.org/)
[8] OWASP Top 10 (https://owasp.org/www-project-top-ten/)