# 日志审计系统参数

**(★**为必须满足的参数，若不满足废标处理, 要求所有**★**必须提供截图，如发现功能造假招标方有权取消资格并追究责任）

|  |  |  |
| --- | --- | --- |
| **日志审计系统** | | |
| **指标项** | | **功能描述** |
| **整体概述** | **系统要求** | 标准机架式硬件设备，支持50个采集源，日志处理速率<=1000 EPS，日志容量：2亿条，无需在被采集目标系统上安装任何软件；产品功能的实现无需额外增加服务器等设备。采用B/S架构操作方式，无需安装客户端软件。 |
| **安全性要求** | 通过SSL加密对数据传输等进行处理；  采用B/S架构，HTTPS访问； |
| **部署** | 支持集中和分布式部署；  采用B/S架构操作方式，无需安装客户端软件。  ★支持采集器扩展部署。 |
| **资产管理** | **资产管理** | 资产管理：可以添加、修改、删除资产；对资产的基本属性进行维护；资产可以增加自定义属性。  资产支持组织管理、网络管理  ★系统支持对IP对象的自动发现功能；对自动发现的设备可以转资产或删除，提供功能证明。  **★**事件流程处理：支持对事件的处理流程管理，对事件处理进行任务分配，对事件处理流程进行监控，事件流程处理完成后进行入库。 |
| **日志采集** | **采集对象** | 系统满足设备的信息采集要求，主要包括：   1. 安全设备：启明WAF防火墙、绿盟IDS、华为防火墙、Juniper防火墙、天融信防火墙等； 2. 操作系统：Linux、Windows、Window server、Uinx等操作系统； 3. 数据库：Oracle、MySQL、SQLServer等； 4. 应用系统：如Apache、Tomcat、IIS、weblogic等； 5. 网络设备：主流的路由器、交换机、负载均衡等网络设备等，如Cisco、华为、juniper等。 |
| **采集接口** | 系统需支持Syslog、Syslog-ng 、SNMP Trap、文件、WMI、FTP、数据库 等协议采集日志；  ★被采设备无需安装任何代理；  日志采集器可实时或按设定的时间将指定的日志送到审计中心；  日志采集器在将日志送往审计中心的时候，可以制定传送策略，仅传送符合条件的日志；  审计中心可以支持多个日志采集器。 |
| **标准化** | 对日志格式进行标准化操作时，将不破坏原始日志内容。  系统从不同设备或系统中所获得的各类日志、事件中抽取相关片段准确和完整地映射至安全事件的标准字段  对安全事件重新定级。能根据统一的安全策略，按照安全设备识别名、事件类别、事件级别等所有可能的条件及各种条件的组合对事件严重级别进行重定义  系统能够将标准格式的事件写入存储设备  系统的标准化策略具备良好的可扩展性，可通过配置文件或界面实现管理功能 |
| **日志处理** | **过滤** | 1. 系统既可以完全收集采集对象上的日志信息，也支持在安全事件收集引擎上设置过滤条件，可过滤出无关安全事件，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，从而减少对网络带宽和数据库存储空间地占用。 2. 系统需可在关联分析引擎上设置过滤条件，可以过滤掉该类型的安全事件的实时显示，而该安全事件仍需要保存到安全事件数据库中。既要给管理员的实时监控提供了方便，又要在以后需要的时候查看分析这些安全事件数据。 |
| **归并** | 1. 系统需具有归并技术，安全事件收集代理会在一段时间内比较收到的安全事件，如果安全事件相同，则只需发送一条安全事件，该安全事件应包括安全事件详情及该安全事件发生的次数，这样可以减少安全事件通信量； 2. 对单位时间内发生的大量安全事件，按照维护要求和实际管理情况，对指定安全设备进行告警安全事件归并；可以通过安全事件严重程度级别、安全事件类别、安全事件标题等安全事件属性进行归并。 |
| **日志分析** | **日志查询** | 1. 支持根据设备类型，按日期展示日志的接入情况，包含不同级别日志数量统计； 2. 支持简单易用的日志查询普通模式，根据系统预置的查询条件，根据用户需求查询对应的日志，并且支持查询条件的保存，供后续快捷使用； 3. ★支持更加精确的专家模式查询，根据页面的指导提示，通过组合查询表达式完成精确查询。 |
| **关联策略** | 1. 为了挖掘不同类型、来源于不同设备或系统的日志或安全事件之间可能存在的关联关系，系统提供了GUI方式的关联规则设置功能，关联的类型包括基于规则和基于统计的。 2. 支持基于因果式的状态关联分析 3. ★支持基于异常统计模型的检查分析功能，如：识别异常的流量攻击等，提供功能证明 |
| **关联事件** | 1. 若日志满足系统内置或用户定义的关联策略，将产生关联事件； 2. 关联事件管理可以统一监控事件的命中情况，包括来源的设备、事件类型、最近命中时间以及命中总次数等。 |
| **日志审计** | **审计事件** | 1. 支持显示审计事件分类统计列表，根据审计策略名称、审计事件类型、被审计人员、目标设备地址四个维度展现。 2. 通过事件总数查看具体的审计事件，并可以查看产生该审计事件的原始事件的详细内容和归并数量。 3. 支持导出PDF、WORD、EXCEL、CSV报告。 |
| **审计策略** | 1. 支持自定义审计策略。 2. 提供可视化方式进行策略制定。 3. 支持从审计策略模板直接创建策略。 4. 支持策略的导入导出。 5. 可通过事件的任意字段制定规则创建策略。 6. 审计策略命中后可以定义告警并通过相应方式转发，如：SYSLOG、邮件等。 7. 审计策略可以定义审计事件的名称、分类、级别以及命中后是否继续匹配其余审计策略。 |
| **审计策略模板** | 1. 提供预置审计策略模板，包括：Windows主机类审计策略模板、Linux/Unix主机类审计策略模板、防火墙类审计策略模板、扫描器类审计策略模板、IDS/IPS类审计策略模板、防病毒类审计策略模板、数据库系统类审计策略模板、萨班斯审计策略模版、等级保护审计模板等。 2. 支持从模板创建审计策略。 |
| **审计类型** | 1. 可自定义审计类型配合不同的审计策略。 |
| **审计对象** | 1. 支持审计对象的定义，包括：审计目标对象、审计行为对象、审计行为执行者对象、审计来源对象、审计时间段对象等。 |
| **审计人员** | 1. 支持定义部门和人员的对应关系。 2. 支持定义人员与账号的对应关系。 |
| **二级接入** | **接收下级审计系统转发告警** | 支持接收来自下级日志审计系统转发的告警日志进行二次分析、关联。 |
| **告警**  **管理** | **告警处理** | 对于告警的处理主要包括清除（认为不是问题）、确认（认为可能是问题）。 |
| **告警监控** | 1. 以列表的方式展示告警； 2. 告警声音设置 3. 告警过滤策略 |
| **告警策略** | 1. 系统支持通过GUI设置告警策略。 2. ★系统内置丰富关联/审计类告警策略，并灵活支持自定义策略。 |
| **全文检索** | **全文检索** | 为了便于操作，系统提供了一个全文检索功能。能对系统内的对象提供全文检索功能，对于海量数据的检索可限定检索时间段（主要针对安全事件）。全文检索提供一个输入栏，需要置顶，在任何页面都能够看到。 |
| **报表管理** | **报表管理** | 包括报表内置实例管理和报表任务管理 |
| **知识库管理** | **知识库管理** | 系统内置日志接入配置指导、典型日志事件介绍、安全经验等。并支持自定义创建增加知识库内容。 |
| **用户管理** | **用户管理** | 支持根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容；日志员只负责完成对系统本身的用户操作日志管理。 |
| **安全仪表板** | **仪表板** | 仪表板应内置支持下列内容：  ★整体安全概况（包括攻击地图展示，事件来源基于地域及组织）提供功能证明  安全资产概况  告警概况  安全事件概况  审计事件概况  还可以支持自定义仪表板，客户可以选择对应的微件，组成想要关注的仪表展现内容 |
| **IPV6支持** | **IPV6** | ★系统全面支持IPV6，提供功能证明。 |
| **系统配置管理** | **配置管理** | 1. 支持设置日志存储备份策略。包括系统日志保存期（天）、磁盘使用率百分比； 2. 支持日志文件备份到外部存储设备，包括FTP/NFS等； 3. 支持系统配置修改图形化（如修改主机名、IP地址等） |
| **资质** | **产品资质** | 1. ★产品具有公安部信息安全检测中心检验报告 2. 产品具有《销售许可证》 |
| **厂商资质** | 厂商具有中国信息安全认证中心颁发的信息系统安全集成一级服务资质  厂商具有信息安全等级保护安全建设服务机构能力评估合格证书 |