**三、采购清单**

1、漏洞扫描服务器壹台，最低供货要求如下表所示（其中加★为关键条款，如不满足将可能导致报价被拒绝）：

|  |  |  |
| --- | --- | --- |
| **序号** | **技术指标** | **指标要求** |
| **1** | **硬件要求** | 授权：系统漏扫授权IP数：≥100，WEB漏扫授权URL数：≥20；性能指标：主机漏扫最大并发IP数：≥75，WEB漏扫最大并发URL数：≥5，内存大小≥8G，接口：≥6千兆电口+2千兆光口SFP。 |
| **2** | **系统要求** | 采用有自主知识产权的安全操作系统，采用B/S设计架构，并采用SSL加密通信方式，无须安装客户端，用户可通过浏览器远程方便的对产品进行管理。 |
| **3** | **风险统计** | ★支持全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息，并可查看详情。（需提供相关截图证明） |
| 支持从“高危”、“中危”、“低危”、“安全”四个安全级别展示资产的风险分布情况 |
| **4** | **资产发现** | 支持资产发现功能，可基于IP地址、IP网段、IP范围、URL等方式进行资产发现扫描，支持EXCEL格式批量导入。 |
| **5** | **系统漏洞扫描** | 支持检测的漏洞数大于19000条，兼容CVE、CNNVD、CNVD、Bugtraq等主流标准。 |
| **6** | **弱口令扫描** | 支持对多种服务协议的弱口令猜解，包括FTP、IMAP、Microsoft SQL、MySQL、PcAnywhere、POP3、SMB、Telnet、VNC、SSH、RDP、ORACLE、Rsync、SMTP、VMware等。 |
| **7** | **基线配置核查** | 支持对Windows、Linux等操作系统按照等保二级、等保三级要求实施基线配置核查。 |
| 支持对Oracel、MySQL、DB2、SQL Server、MySQL等数据库按照等保二级、等保三级要求实施基线配置核查。 |
| **8** | **合规自检平台** | ★支持域管理功能，系统默认内置数据域、终端接入域、运维管理域等九个域，可根据客户实际情况进行自定义管理。（需提供相关截图证明） |
| 支持业务系统登记功能，保护等级支持第二级和第三级，可根据不同域类别添加资产到业务系统中。 |
| ★按“一个中心、三重防护”的架构展示检测结果，每个检测结果呈现具体问题及整改建议，系统支持手动核查确认、整改后重新检测、以及手动导入全局分析和人工核查报告来对测评报告中的结果进行核查确认，其中手动核查确认支持单项核查确认和批量核查确认。（需提供相关截图证明） |
| **9** | **报告管理** | 支持报表过滤功能，支持从任务类型、任务/资产、风险等级、漏洞/基线类型等角度筛选和过滤报表生成条件。 |
| 产品支持对系统漏洞、WEB漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB漏洞扫描、基线配置核查、弱口令扫描结果的报表。 |
| **10** | **厂商资质** | 厂商研发体系应通过国际认证，取得CMMI5证书 |
| 厂商应为微软MAPP成员，需提供相关证明 |
| **11** | **产品资质** | 产品应具有公安部《计算机信息系统专用产品销售许可证》 |
| 产品应具有中国网络安全审查技术与认证中心颁发的《网络关键设备和网络安全专用产品安全认证证书》 |
| **12** | **售后要求** | 安装调试及售后服务人员应具有原厂高级认证资质，软硬件产品需提供不少于三年原厂免费售后质保证明、三年原厂工程师上门免费升级服务，三年免费质保期后应继续提供技术支持、维护维修（含升级）等售后服务（需提供详细服务方案及费用报价） |

2、日志审计服务器壹台，最低供货要求如下表所示（其中加★为关键条款，如不满足将可能导致报价被拒绝）：

|  |  |  |
| --- | --- | --- |
| **序号** | **技术指标** | **指标要求** |
| **1** | **性能要求** | 默认包含主机审计许可证书数量≥50，最大可扩展审计主机许可数≥150，平均每秒处理日志数（eps）最大性能≥1200。  内存大小≥16G，接口：≥6千兆电口，≥2万兆光口SFP+。 |
| **2** | **系统许可方式** | 内置50个主机审计许可证书； |
| **3** | **日志采集** | 支持主动、被动相结合的数据采集方式，支持通过Agent采集日志数据，支持通过syslog、SNMP Trap、JDBC、WMI、webservice、FTP、文件\文件夹读取、Kafka等多种方式完成日志收集； |
| **4** | **日志传输与存储转发** | ★支持TLS加密方式进行日志传输，支持日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量。（需提供相关截图证明） |
| 支持设置日志存储策略，包括设置日志存储周期（天）、存储空间容量使用阈值等； |
| **5** | **日志分析** | 支持网站攻击、漏洞利用、C&C通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则，内置关联分析规则数量达到350条以上，支持自定义关联分析规则 |
| **6** | **日志告警** | ★日志进行归一化操作后，对日志等级进行映射，根据不同日志源统计不同等级下的日志数量（需提供相关截图证明） |
| **7** | **资产管理** | 支持资产全生命周期管理，资产入库审核、资产离线风险识别、资产退库、资产数据更新，责任人管理机制等，支持自定义资产标签、属性、 |
| 支持对IPv4/ipv6对象的自动发现功能，对自动发现的设备可以修改、删除或转为资产。 |
| **8** | **首页可视** | 支持自定义首页卡片，支持实时监控系统日志传输量和日志留存的合规情况。 |
| **9** | **系统管理** | 支持个性化定制，支持全系统更换logo与系统名称，支持一键恢复默认。 |
| 提供管理员账号创建、修改、删除，并可针对创建的管理员进行权限设置；支持IP免登录，指定IP免认证直接进入平台；支持只允许某些IP登录平台；支持页面权限配置和资产范围配置，用于管理账号权限，满足用户三权分立的需求；支持usb-key认证 |
| 支持网络连通性测试工具，至少支持ping、tracert route、telnet三种拨测方法； |
| **11** | **首页可视** | 支持可视化展示，包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等，可提供设备专项分析场景。如防火墙外部攻击场景分析、VPN账号异常场景分析、Windows服务器主机异常场景分析等，通过设备专项页面对每一台设备安全情况深度专业化分析 |
| **12** | **日志检索** | 支持将检索查询的条件收藏为查询模版，支持查询模版创建、导入导出、删除功能，支持历史搜索记录功能。 |
| ★支持通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属（可具体到外网、内网资产等）、IP地址、特征ID、URL进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件；（需提供相关截图证明） |
| **13** | **厂商资质** | 厂商具有国家信息安全漏洞库（CNNVD）技术支撑单位等级证书（一级）  厂商具有国家计算机网络应急技术处理协调中心颁发的网络安全应急服务支撑单位证书（国家级）  产品具有国家版权局《计算机软件著作权登记证书》 |
| **14** | **售后要求** | 安装调试及售后服务人员应具原厂高级认证资质，软硬件产品需提供不少于三年原厂免费售后质保证明、三年原厂工程师上门免费升级服务，三年免费质保期后应继续提供技术支持、维护维修（含升级）等售后服务（需提供详细服务方案及费用报价） |

备注：1、所提供的以上两款产品均需完成与采购方已有网络安全系统集成；2、漏洞扫描及日志审计服务器的参考品牌型号分别为:深信服漏扫：YJ-1000-B1075、日志审计：SIP-Logger-A600，如供应商提供其他品牌、型号产品，则需提供性能不低于参考品牌及型号产品的证明文件，并负责提供系统集成所需软硬件（需计算在总报价内）；3、针对每一款产品，均需提供详细技术参数及点对点技术条款应答表（格式自定）。