**一、采购需求清单**

## 1、项目采购清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **技术规格及配置要求** | **数量** | **单位** |
| 1 | **防毒墙** | 《**详细参数见技术参数要求》** | 1 | 套 |
| 2 | **日志审计** | 《**详细参数见技术参数要求》** | 1 | 套 |
| 3 | **堡垒机** | 《**详细参数见技术参数要求》** | 1 | 套 |
| 4 | **态势感知平台** | 《**详细参数见技术参数要求》** | 1 | 套 |

## 2、技术参数要求

1. **防毒墙技术要求**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| 硬件参数 | 硬件外形：软硬一体化1U标准机架式设备；CPU：2核，内存≥16GB；硬盘容量≥1T；板载自带接口≥2GE+4GE Bypass ；电源：单电源；扩展插槽≥2个。 |
| 性能参数：网络层吞吐率≥3Gbps，防病毒吞吐率：≥200Mbps。 |
| 部署方式 | 部署模式支持桥接、路由、监控 (旁路模式) 模式。 |
| 威胁可视化展示 | 能够对威胁进行可视化展示，展示维度应包括威胁类型统计（至少包含勒索、挖矿、病毒、APT、漏洞利用威胁事件）、近30天威胁事件趋势、攻击源IP TOP5、受影响主机TOP5、勒索&挖矿事件拦截统计、热门威胁事件TOP5、自定义黑名单TOP5等。 |
| 提供防病毒功能 | 1.支持多种协议的解析, 至少包括 |
| HTTP/SMTP/POP3/FTP/SMB/TFTP/TCP/UDP/NFS/SNMP/ICMP/RTMP/DNS/IRC。 |
| 2.能够对SMBv1/SMBv2/SMBv3文件共享协议进行病毒检测与查杀。 |
| ★3.提供对压缩文件解压并进行病毒查杀，支持解压层数不少于20层。 |
| 4.能够防御多种类型的恶意软件，包括但不限于病毒、木马、蠕虫、后门、间谍软件、灰色软件、Rootkits等。 |
| 5.提供文件扫描优化，可自定义文件扫描的大小范围，最大不小于2G。 |
| 6.提供三年病毒库升级服务 |
| 提供入侵检测虚拟补丁功能 | 1.能够提供包括但不限于防止漏洞利用和SQL注入、命令注入、 Webshell 攻击、XSS 攻击、CSRF 攻击的能力。 |
| ★2.提供虚拟补丁功能，可通过CVE编号搜索对应的防护规则，在网络层面对漏洞攻击进行阻断。 |
| 3.提供用户自定义IPS规则，支持设置严重等级、规则种类、源/目的IP地址、源/目的端口、协议类型（至少包含HTTP、TCP、UDP协议）等。 |
| 4、提供3年入侵检测虚拟补丁库升级服务 |
| 联动防护 | ★提供与本次采购的态势感知、态势感知探针等系统联动，实现已知、未知威胁全方位的发现、拦截、病毒查杀。 |
| 提供威胁情报 | 1.提供威胁情报能力，以覆盖更大范围的威胁检测，且可根据需求进行开启或关闭。 |
| 2.提供黑/白名单自定义，包括支持URL黑白名单、邮件收发件人黑/白名、基于SHA1的文件黑/白名单。 |
| 可靠性 | 1.为确保管理安全，须支持通过加密的SSL协议访问管理控制台。 |
| 2.支持自动、手动硬件BYPASS功能，在断电时能自动实现直通功能恢复通讯。 |
| 3.支持特征码最新版本检测和提示功能，以便管理员及时维护，提升设备的可维护性。 |
| 系统升级 | 支持自动/手动在线升级，且可配置自动升级周期。 |
| 服务要求 | 提供三年7\*24小时全天候原厂商质保，30分钟内响应；需提供针对本项目的原厂商授权书和售后服务承诺原件； |

1. **日志审计技术要求**

|  |  |
| --- | --- |
| **指标项** | **技术参数** |
| 硬件要求 | 机箱1U，内存≥16G，硬盘≥2T，网卡≥6个千兆电口；含3年及以上特征码升级和硬件保修服务。  日志源≥50个；日志处理性能≥1500EPS 。 |
| 日志采集 | 支持Syslog(UDP、TCP）、目录、远端软件（FTP、SFTP、HDFS、LOCAL）、WMI、SNMP（Trap）、数据库（ORACLE、DB2、MYSQL、SQLITE、POSTGRES、SQLSERVER）协议日志收集 |
| 日志分析 | 提供对设备日志查询和聚合分析； |
| 提供内置常见安全事件关联分析规则； |
| 提供基于策略的多日志源海量日志实时关联分析，发现安全事件实时告警； |
| 日志审计 | 提供SOX审计包含SOX登录事件、SOX对象访问、SOX账号管理、SOX策略更改； |
| 提供PCI审计包含PCI策略更改、PCI对象访问、PCI登录事件； |
| 提供ISO27001审计包含ISO27001对象访问、ISO27001策略更改、ISO27001账号管理、ISO27001登录事件； |
| 数据查询 | 提供按日期、时间、告警类型、日志来源、告警等级、受害IP地址、攻击IP地址、攻击结果、分析类型、地理城市等参数进行过滤查询； |
| 提供用任意关键字对所有事件进行高性能全文检索； |
| 提供可指定多个查询条件进行组合查询； |
| 用户管理 | 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； |
| 基于角色的权限管理机制，通过角色定义支持多用户访问； |
| 系统自身的健康状况监控，包括CPU、内存、磁盘的利用率； |
| 软件升级服务 | 防火墙AF-1000-B1120开通深信服云鉴订阅软件1年服务。（需提供针对本项目的原厂商授权书和售后服务承诺原件） |
| 服务要求 | 提供三年7\*24小时全天候原厂商质保，30分钟内响应；需提供针对本项目的原厂商授权书和售后服务承诺原件； |

1. **堡垒机技术要求**

|  |  |
| --- | --- |
| **指标项** | **技术参数** |
| 硬件要求 | 规格 1U；内存≥8G；硬盘≥ 2T；≥6千兆电口；USB口≥4个；可用扩展槽≥2；≥200个资产授权；含3年及以上特征码升级和硬件保修服务。 |
| 运维访问管理 | ★应支持远程应用单点登录的客户端水印，水印信息包括用户信息及运维时间； |
| 应支持可自定义个人运维资产组，便于快速搜索；设置优先展现资产收藏页或运维资产列表页； |
| 应提供运维人员使用的客户端工具管理，包括工具统一上传、统一下载等； |
| 应提供运维安全个人网盘，支持按用户开通个人网盘，开通后运维文件安全必须先上传至个人网盘，通过防病毒文件扫描的文件才允许上传，审计病毒文件拦截日志，支持从个人网盘批量上传至多个目标资产； |
| 认证管理 | 应提供用户忘记登录密码时，在登录首页申请密码重置；支持手机短信、令牌口令、邮箱三种方式重置密码； |
| 资产\资产组管理 | 应提供手工、自动方式发现目标资产，自定义配置IP地址段及自定义资产协议端口，精确识别是否在系统中存在，支持一键导入；应支持手工、自动方式采集主机资产上的帐号列表，精确识别是否在系统中存在，支持一键导入； |
| 应提供按第三方平台开通用户、资产、授权、审计、运维不同模块的API接口，调用记录可查询；支持API接口的熔断功能策略，单位时间超过调用阀值对该接口进行熔断； |
| 系统自防护 | 应提供内置Web安全组件，防护不因网络调整或内网绕行而失效； |
| 应支持SQL注入、XSS攻击的检测与防御能力，支持Web恶意扫描防护的检测与防御能力； |
| 应提供CSRF攻击检测与防御能力； |
| 应提供用户多次登录失败按策略提示输入验证码； |
| 支持提供自身防护DDOS攻击； |
| 资产巡检 | 应支持手工、定期、周期内自动发现资产，自定义配置IP地址段及自定义资产协议端口，精确识别是否在系统中存在,一键导入系统； |
| 主机防绕行 | 应提供按主机资产设置防绕行认证策略，认证方式支持不验证、令牌口令、短信口令、邮件口令 |
| 软件升级服务 | 防火墙AF-2000-FH2130B防火墙开通云威胁情报功能模块三年、开通SSL VPN授权功能模块，10个SSL VPN客户端许可、开通Web应用安全防护功能三年。（需提供针对本项目的原厂商授权书和售后服务承诺原件） |
| 服务要求 | 提供三年7\*24小时全天候原厂商质保，30分钟内响应；需提供针对本项目的原厂商授权书和售后服务承诺原件； |

1. **态势感知平台技术要求**

|  |  |
| --- | --- |
| **指标项** | **技术参数** |
| 硬件要求 | 1U； CPU≥6核；内存容量≥128GB；硬盘容量≥16TB；网口≥8个千兆电口；显示器接口≥1个HDMI；USB口≥3个；冗余电源；含3年及以上特征码升级和硬件保修服务。  1.性能：  (1)提供日志源数量≥100个  (2)数据采集和处理性能≥10000EPS  2.功能：  包含：大屏展示、监测中心、分析中心、响应中心、资产中心、平台管理、SOAR插件管理、情报中心、威胁狩猎、安全快照、5个SOAR剧本、3年威胁情报。 |
| 功能要求 | 提供通过TCP，UDP，Syslog，WebService、SSH、Telnet、JDBC、WMI、FTP、SNMP、FTP、SFTP、HDFS、目录、文件等采集协议，实现100+种常用设备的告警日志直接接入平台，无需单独部署日志采集设备； |
| 安全告警拆分成了网络告警和终端告警，增加了恶意文件、挖矿攻击的告警类型以及对终端告警的遏制、验伤处置操作。对于挖矿类告警，可以呈现挖矿阶段、挖矿币种图等信息。 |
| ★提供威胁狩猎功能，支持基于IP的威胁狩猎，实现风险钻取分析功能，可根据攻击者和受害者等不同纬度的风险要素对整网安全进行逐层分析和逐级追踪，可以从系统内所有的IP进行下钻分析，聚合关联与该IP相关的所有安全告警与访问信息，以时序方式呈现资产遭受的攻击全过程 |
| 提供资产探测任务，以IP或者IP段、端口或者端口段进行扫描，能够识别操作系统、开放端口、开放服务、MAC地址、资产名称，所得的资产数据可以自动或者人工确认装载到资产数据库进行统一管理。 |
| 基于性能和业务需求，可配置探针记录内容（文件，进程，网络，注册表和系统事件）的详细程度，支持“标准级”和“增强级” |
| 提供呈现资产风险打分和资产风险级别，该资产与异常信息联动安全告警、安全事件、脆弱性信息。 |
| 资产支持呈现组织机构、业务系统、安全域、资产组的风险评分、评分趋势和风险资产列表等。 |
| 提供全局提示待处理工单、待处理事件、待处理告警，不受当前页面限制 |
| 提供大屏轮播，可以指定轮播的大屏和时间；可批量或者单独设置大屏的过滤参数包括是否情报命中、安全域、组织机构。 |
| 设置事件类型、事件等级、处置状态、攻击阶段等查询条件，筛选出符合条件的安全事件； |
| 提供数据级联功能，可以通过前端页面配置，将本平台内的告警数据、安全事件、资产上报给上级平台； |
| ★联动防护功能要求 | ★提供与本次采购的防毒墙、态势感知探针等系统联动，实现已知、未知威胁全方位的发现、拦截、病毒查杀。 |
| 探针硬件要求 | 1U标准机架式设备；接口：≥4个千兆电口；吞吐量≥500Mbps；冗余电源；CPU≥4C；内存≥16G；硬盘≥2T；可扩展插槽≥2个；含3年及以上特征码升级和硬件保修服务。 |
| ★提供挖矿检测功能 | 提供多样性的挖矿检测手段，能够检测挖矿木马投递、挖矿木马横向移动行为、挖矿软件、矿池域名解析、矿池连接、矿池协议等。 |
| 矿池协议告警须提供虚拟币种类别。 |
| 挖矿告警须提供专项告警页面，独立于其它告警。 |
| 能够自动解析DNS响应的矿池及IP地址。 |
| 提供恶意文件侦测功能 | 具有文件威胁检测能力，能够准确识别300多种文件类型；支持恶意程序分类；针对检测出的恶意文件，能够给区分类型，如木马、勒索病毒等等。能够侦测各种文件型病毒，如勒索病毒、木马、僵尸、后门等， |
| ★提供恶意行为分析侦测 | 提供25000条以上攻击检测规则，涵盖Web攻击、漏洞利用、恶意软件、隐蔽隧道、黑客工具、内网安全等多种威胁类型 |
| ★提供暴力破解行为检测研判功能 | 提供分布式爆破、慢速爆破检测，且界面可配。 |
| 提供信息泄露检测功能 | 提供识别流量中的个人敏感信息，包括身份证、银行卡、手机号、港澳通行证等，并展示传输信息的协议、网站域名、URL、客户端IP、服务端IP，便于用户发现敏感信息的传输安全隐患和处置 |
| 告警和研判 | 能够按照预设的条件，对相同攻击源、攻击目标、攻击类型的事件告警进行聚合，减少不必要的重复告警。 |
| 告警智能化一键降噪 | 能够使用统计模型对产生的告警日志进行噪声分析。用户在分析日志时，可以根据噪声级别对日志进行实时过滤。支持对历史数据进行噪声标记。分析模型支持在线更新。 |
| 提供智能研判（风险主机）功能 | 能够提供攻击详情分析，包含风险信息概览，攻击链阶段，攻击关系图，风险主机涉及的告警列表详情，入侵检测攻击上下文等。 |
| 提供流量抓包与回放功能 | 提供pcap回放功能，对导入的pcap进行回放并进行威胁检测，回放产生的告警必须和生产网络流量的告警分页面展示，避免干扰正常安全运营。 |
| 服务要求 | 提供三年7\*24小时全天候原厂商质保，30分钟内响应；需提供针对本项目的原厂商授权书和售后服务承诺原件； |

**三、本项目集成要求**

## **3、内网安全建设集成要求：**

1. 本院预计通过购买安全设备后立即对安全等相关设备进行升级操作，解决存在的网络中的隐藏安全隐患，提高本院网络安全防护能力，确保院内的各业务系统安全稳定地运行使用。

## **4、外网及DMZ区安全建设集成要求：**

1、投标人需对新购态势感知系统根据我院网络安全情况进行评估后，部署在合理的位置，对我院网络安全态势进行全面的监控和分析。通过对网络的实时监控和信息分析，及时发现和预警网络中的威胁，并采取相应的措施进行防护和响应。供应商需提供网络安全应急响应服务，并定期对我院网络安全事件进行及时处理，提交处置报告。

3、投标人在项目实施前需按照信息安全等级保护三级、商用密码管理条例，对我院现有网络安全环境进行分析、规划，并提供符合我院的网络安全设备实施计划及详细的项目实施方案；

4、投标人需对我院此次所采购的安全设备进行安装调试工作，整个设备及相关软硬件安装调试完毕后，需配合完成我院信息安全等级保护测评；

## 5、网络安全**整改集成要求**

1、投标人需对我院机房内部线路整理，将院内机房内非成品网线更换为成品网络条线，机房内部对相关线缆进行打标签，提供机房内部设备技术文档。

2、投标人需调整院内现有网络安全设备位置，在现有网络安全设备上配置安全加固策略，调整安全设备部署位置使其设备发挥最佳功能及效果，提高院内整体网络安全能力。

# 二、售后服务要求

1. 投标人需对本次项目中软硬件产品需提供三年原厂免费质保服务，服务级别为：24\*7，30分钟现场响应；
2. 投标人针对本项目整体三年质保，服务级别为：24\*7，30分钟现场响应。投标人免费提供系统维护和故障排除；
3. 投标人必需提供本次项目的软硬件的技术支持工作。如果我院以设备出现故障或需要进行网络调整，投标人需做到随叫随到，3年内无偿提供以上设备及系统的技术支持工作；
4. 投标人提供三年每季度一次的巡检服务（本次所采购的软硬件），并提供巡检报告；