附件：信息安全基础设施加固项目基础需求

本次采购项目拟分为6个标包，意向人可同时参与多个标包的市场调研。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 数量 | 需求描述 | 标包号 |
| 1 | 服务器主机安全软件 | 200-400用户 | 1．实现医院200台Windows及Linux主机的漏洞检查、主机基线检查、主机弱口令检查、主机命令执行跟踪、C&C回连进程定位、入侵轨迹记录、进程调用监控及高危行为阻止、WebShell后门检测查杀等全方位防护；提供不少于3年的特征库更新及软件升级服务；  2．软件支持部署在 RedHat、CentOS、Ubuntu、Suse、Windows Server等操作系统，同时支持中标麒麟、银河麒麟、统信 UOS 、BC-Linux等国产化操作系统。  3．支持自动清点容器镜像、容器实例、容器网络等多种容器相关资产，支持检测容器内应用的弱口令，并提供相关资产统计视图  4．支持检测发生在容器内部的入侵事件，如反弹 SHELL、WebShell、恶意命令等  5．支持检测 Radmin Server、TigerVNC、TightVNC、向日葵等远控软件弱口令  6．支持webshell拟态防护功能，能够有效诱导黑客webshell攻击并进行攻击溯源  7．支持暴力破解防护、异常登录防护、反弹Shell防护、WebShell防护、病毒防护、网络层防护  8．支持根据用户自定义策略对系统敏感端口的监听行为进行监控，并对恶意端口监听行为进行告警。 | 01 |
| 2 | 运维安全管理（堡垒机） | 1台 | 1．为医院运维提供集中身份认证、访问控制、操作全过程审计等，满足主机运维审计、权限控制、访问身份唯一性认证的等级保护要求。设备内存≧16G，硬盘可用空间≧8T，千兆电口≧2个，冗余双电源，最大支持1000字符并发、100图形并发，提供不少于800个资产可管理授权，提供不少于3年的硬件质保及软件升级服务，提供原厂安装实施服务。  2．支持SSH、Telnet、RDP、SFTP、RemoteAPP、Oracle、Mysql、MSSQL、DB2、B/S、C/S等常见运维协议。支持应用发布功能，需要的运维工具发布到外置服务中供调用，并支持自定义脚本适配账号密码代填；  3．支持多级审批模式，管理员可自定义各级审批人，相应工单逐级审批通过后后生效；针对已审批通过的工单，管理员可以一键撤销；  4．支持对命令行操作行为和数据库操作审计的100%文本审计，支持图形界面操作过程中的录像和键盘鼠标操作、剪贴板操作、标题栏操作三大类文本信息，保障任何场景下都不会缺审漏审；  5．为防止因会话负载过高而阻碍运维安全管理系统正常运行，应支持同类会话、单一会话的cpu、内存负载限制，限定用户通过运维安全管理系统发起的图形、字符、数据库三类操作分别可以占用的最大资源比例；  为适配集群等高可用部署资产的管理，应支持等价资产管理和等价账号管理，当等价关系设定后，其中一台资产内的账号密码发生变更，等价的资产、账号密码随之自动变更。 | 02 |
| 3 | 态势感知平台 | 1台 | 1．医院部署一套全新态势感知平台，实现南院及北院全网安全态势独立感知能力，同时与院内边界AF防火墙、上网行为管理等安全设备形成威胁联动处置。提供不少于3年的硬件质保及特征库更新服务，提供原厂安装实施服务。  2．态势感知平台存储容量≥36T，在带宽性能1Gbps时存储时长≥1800天/1Gbps，日接入日志量≥3.5亿条，千兆电口≥6个，万兆光口SFP+≥2个；  3．支持不同安全视角展示多个独立的大屏展示功能，包括全网安全态势感知大屏、分支安全态势、安全事件态势、通报预警态势、资产态势大屏等，同时能满足多种场景的监控，比如日常运维、护网场景等；  4．具备元数据行为分析引擎：httpflow、dnsflow、adflow、icmpflow、maillflow等, 通过异常行为分析，结合各类机器学习算法完成未知威胁检测。包括：内网穿透、代理、远控、隧道、反弹shell等事后检测场景；  5．文件威胁分析支持平台内置的静态文件检测引擎、AI智能引擎、SAVE查杀引擎、webshellkiller引擎，利用LSA, AutoEncoder, LogicRegression, SVM, 随机森林，XGBoost等多种机器学习算法组合进行综合研判。支持采用AI技术针对无文件落地的恶意脚本进行检测；  6．支持挖矿专项检测页面，具备挖矿攻击事前、事中和事后全链路的检测分析能力，综合运用威胁情报、IPS特征规则和行为关联分析技术，如检测发现文件传输（上传下载）阶段的异常，对挖矿早期的准备动作即告警；  7．实时检测到关注告警类型的威胁可以发出声音告警提醒用户。支持受害者IP/攻击者IP/代理服务器IP表头筛选支持复制IP,攻击者和受害者IP展示带上资产名片或区域信息，包括重点关注资产、威胁类型排行统计展示，复制告警支持自定义模板。 | 03 |
| 4 | 北院态势感知探针 | 1台 | 1．医院北院区配置1个威胁感知探针设备，可注册接入态势感知平台实现威胁的联动分析与大屏统一展示，探针设备性能要求如下：网络吞吐性能≥10Gbps，内存≥48GB，硬件≥960G SSD，冗余电源，千兆电口≥6个，万兆光口SFP+≥2个；  提供不少于3年的硬件质保及特征库更新服务，提供原厂安装实施服务。  2．内置URL库、IPS漏洞特征识别库、应用识别库、WEB应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、恶意链接库、白名单库；  3．支持SQL注入、XSS攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web整站系统漏洞、自定义WAF规则、WAF云防护等网站攻击检测；  4．支持Database漏洞攻击、DNS漏洞攻击、FTP漏洞攻击、Mail漏洞攻击、Network Device、Media漏洞攻击、Shellcode漏洞攻击、Scan漏洞攻击、System漏洞攻击、Telnet漏洞攻击、Tftp漏洞攻击、IPS云防护、Web漏洞攻击等服务漏洞攻击检测；  5．支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括3389、53、80/8080、21、69、443、25、110、143、22等；  6．支持HTTP未知站点下载可执行文件、浏览最近30天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC通信等僵尸网络行为检测；  7．支持敏感数据泄密功能检测能力，可自定义敏感信息，支持根据文件类型和敏感关键字进行信息过滤；  8．支持5种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求。 | 03 |
| 5 | 南院态势感知探针 | 1台 | 1．医院南院配置1个威胁感知探针设备，可注册接入态势感知平台实现威胁的联动分析与大屏统一展示，探针设备性能要求如下：网络吞吐性能≥2Gbps，内存≥8GB，硬件≥480G SSD，冗余电源，千兆电口≥6个，万兆光口SFP+≥2个；  提供不少于3年的硬件质保及特征库更新服务，提供原厂安装实施服务。 | 03 |
| 6 | 态势感知平台MSS托管服务 | 1年 | 1．为医院200个关键服务器资产提供1年7\*24 小时线上安全运营托管服务，以保障网络安全“持续有效”为目标，云端安全运营团队通过安全运营平台实时对医院网络安全事件进行监测，联合医院现场安全服务团队一同构建持续(7\*24 小时)、主动、闭环的安全运营体系。围绕资产、漏洞、威胁、事件四个要素，监测安全攻击和入侵攻击事件，通过自动生成工单，与用户现场的安全服务团队结合，及时进行分析预警和处置。  2．安全运营平台支持接入医院的态势感知系统，可在平台呈现接入设备或系统信息（包括设备类型、IP、在线状态等）且可在医院本地设备上查看同步云端的记录。  3．安全运营平台可对接入的设备或系统安全事件进行自动化分析，云端安全运营团队可在运营平台上对医院本地的态势感知系统及边界防火墙进行管理维护，支持下发封锁策略至边界防火墙实现联动应急处置。  4．安全运营托管服务面向医院的安全态势，提供可展示的用户界面，展示服务平台漏洞表、事件表统计情况，可按照资产类别、威胁类型进行定制化筛选查看，能直观呈现医院当前的风险态势情况。针对页面篡改、通报、断网、webshell、黑链等各类严重安全事件，医院安全管理员可在平台上直接发起技术咨询，云端专家进行紧急响应和处置。  5．线上安全运营托管服务可支持从服务平台生成、导出、下载各类安全报告，包括但不限于《安全服务值守日报》、《特殊时期值守报告》、《安全运营周报》、《安全运营月报》《安全运营季报》、《安全运营年报》，按需提供《勒索风险排查报告》、《敏感信息泄露排查报告》等。 | 03 |
| 7 | 虚拟专用网设备VPN | 2台 | 1.虚拟专用网SSL VPN设备，为医院提供端到端的安全接入通道，支持多种身份认证方式、细粒度访问权限控制等主要功能，保证远程系统接入的用户身份安全、终端安全、传输安全、应用权限安全和审计安全。  2.性能参数：加密流量≥400 Mbps，并发用户数≥6000，设备整机理论吞吐量≥1.5Gbps，设备整机并发会话数≥160w。内存大小≥8G，硬盘容量≥128G SSD，冗余电源，≥6千兆电口，≥4千兆光口SFP。最大用户数≥80000，最大用户组≥8000，最大角色数≥500，最大web资源数≥500，最大tcp资源数≥500，最大vpn资源数 ≥500。提供不少于3年的硬件质保及软件升级服务，提供原厂安装实施服务。  3．产品具备防中间人攻击功能，在用户登录SSLVPN时智能判断存在中间人攻击行为，断开被攻击的连接，并可提示异常现象；  4．产品应支持的密码算法包括：AES、DES、3DES、DH、RSA、RC4、MD5、SHA1  5．支持针对不同的web页面进行数据优化，支持动态压缩技术，针对B/S资源支持WebCache技术，动态缓存页面元素，提高Web页面响应速度。支持流缓存技术，提高访问速度。  6．支持与阿里钉钉、企业微信APP认证对接，移动端访问企业自建应用时可自动拉起VPN，实现其内置应用的安全接入。 | 04 |
| 8 | 南院数据中心防火墙 | 2台 | 1．企业级下一代防火墙，具备网络访问控制、漏洞入侵防御、网络文件病毒查杀、上网内容识别及防护等功能，支持基于源IP/目的IP，服务类型，应用类型，安全域，时间段等字段进行安全策略规则的配置，支持每IP、每用户的最大连接数限制；CPU、转发芯片为国产芯片；支持双机高可用架构部署。  2．防火墙吞吐量≥100Gbps，最大并发连接数≥3000万，每秒新建连接数≥100万，启用防火墙 +安全分析功能吞吐量≥50Gbps，启用防火墙 +安全分析功能吞吐量+IPS吞吐量≥40Gbps；100G光口≥2个，40G光口≥2个，25G/10G光口≥8个，万兆光口≥20个，配备100G多模光模块≥2个，万兆多模光模块≥4个，配置双电源。配置URL+IPS+AV 特征库升级许可≥3年；提供不少于3年的硬件质保及软件升级服务，提供原厂安装实施服务。 | 05 |
| 9 | 日志审计设备 | 1台 | 1．支持Windows、Linux等操作系统、支持网络设备（交换机、路由器、UTM等）、安全设备（防火墙、VPN、IPS、IDS、防毒墙、安全网关等）、数据库操作、网络行为、中间件（Tomcat、Webspere、weblogic等）应用系统（Web服务器、邮件服务器、OA、CRM等）日志集中管理与审计；  2．一体机设备，配置4块≥8TB硬盘，日志处理性能≥5000条/秒，≥4个千兆电口，不限日志审计授权许可数量；提供不少于3年的硬件质保及软件升级服务，提供原厂安装实施服务。 | 06 |