**附件1**

**数据中心设备采购与安全服务集成项目需求书**

|  |  |  |
| --- | --- | --- |
| **名称** | **详细描述** | **数量** |
| 电子病历服务器 | 2\*英特尔至强E5-2660 v4(2.0GHz/14-core/25MB/85W)处理器(带散热器)，2\*600G硬盘，128G内存，2个8G HBA卡，1个万兆光纤网卡，冗余电源，冗余风扇 | 3 |
| 虚拟服务器 | 4\*6142 Gold（16核心，2.6GHz）512GB 2\*300GB硬盘4\*千兆网卡2\*独立万兆光纤网卡2\*独立16Gb HBA 卡 原厂三年服务 | 1 |
| 服务器内存扩容 | 原服务器有32G内存，扩容到256G，，原有2\*E7 4820v2cpu，现在扩容2颗cpu | 2 |
| PACS生产存储扩容 | 扩容9\*4T 7.2K 3.5寸，21\*900G 1OK 2.5寸，3\*200G 2.5寸SSD硬盘,增加1个25\*2.5寸槽位扩展柜 | 1 |
| PACS发布存储扩容 | 扩容9\*4T 7.2K 3.5寸，扩容11块1.2TB 10K 2.5寸磁盘增加1个25\*2.5寸槽位扩展柜 | 1 |
| PACS原图存储扩容 | 扩容38\*1.2T 1OK 2.5寸，增加2个25\*2.5寸槽位扩展柜 | 1 |
| 上网行为管理 | 适用于出口带宽250M，具备用户认证、流量控制、上网行为管理、上网行为审计、Ipsec VPN功能，原厂三年服务 | 1 |
| 态势感知平台 | 详细需求见《态势感知平台参数》 | 1 |
| 安全服务 | 详细需求见《安全服务内容》 | 1 |
| 集成服务 | 详细需求见《集成服务内容》 | 1 |

**1.态势感知平台**

|  |  |  |
| --- | --- | --- |
| **序号** | **技术指标** | **指标要求** |
| **安全感知平台** |
| 1 | 性能指标 | 尺寸 | 2U架构 |
| 硬盘容量 | 32TB |
| CPU | 16核心 |
| 内存 | 96G内存 |
| 接口数量 | 4个千兆电口、1个串口、3个USB口 |
| 电源 | 冗余电源 |
| 2 | 大屏可视 | 综合态势大屏 | 支持以图形化大屏的综合监控展示，包括但不限于安全事件态势、安全事件TOP5、高危漏洞TOP5，最新攻击事件等； |
| 服务器与漏洞态势大屏 | 支持以图形化大屏的服务器与漏洞实时态势，包括但不限于漏洞等级分布、TOP5漏洞、服务器操作系统分布、影响服务器的数量、被访问服务器TOP5、实时漏洞发现更新、业务对外开放TOP5端口； |
| 业务风险外连大屏 | 支持以图形化大屏的方式展示业务外连的实时态势，包括但不限于外连业务风险TOP10、外连态势、外连地址TOP10、最新事件等，支持国际、国内地图自主切换； |
| 攻击态势大屏 | 支持以图形化大屏展示实时外部攻击态势，包括但不限于攻击事件、攻击源、危害级别等进行统计与展示。 |
| 横向威胁大屏展示 | 支持图形化大屏的横向威胁展示，包括但不限于横向威胁趋势，威胁类型分布、被访问业务TOP5、攻击源TOP5、违规访问源TOP5、可疑访问源TOP5、风险访问源TOP5； |
| 3 | 资产感知系统 | 资产自动识别 | 支持自动识别网络内部主机网段和外网网段；支持通过流量中的应用内容自动区分网络内部网段IP是属于PC还是服务器；  |
| 自动识别服务器信息 | 支持自动识别资产，在不影响内部网络的前提下，通过主动发送微量包的扫描方式探测潜在的服务器以及学习服务器的基础信息，如：操作系统、开放的端口号等； |
| 支持自动识别已知服务器，通过被动检测机制，对经过探针的流量进行分析，识别已知服务器对外提供的所有服务、已开放端口及端口传输的协议/应用等； |
| 设备运行监控 | 支持通过SNMP协议，获取待监测设备机器名、CPU负载、内存使用和流量情况，同时也支持OID定制（ |
| 4 | 脆弱性感知 | 脆弱性总览 | 支持页面展示业务脆弱性风险分布，不同严重级别业务分布，漏洞类型分布图，漏洞整体态势等，支持7天、30天统计 |
| 弱密码扫描 | 支持通过镜像流量检测数据包中存在的用户名和密码信息,通过分析密码的强度检测网络中存在的弱密码风险 |
| Web明文检测 | 支持通过镜像流量检测web流量中是否存在可截获的口令信息，分析web业务系统是否存在明文传输情况，避免因明文传输导致信息泄露的风险。 |
| 漏洞报告 | 支持流量分析实时发现操作系统、数据库、web应用等存在的漏洞风险，看清网络脆弱性，并支持生成漏洞检测报告。 |
| 5 | 高级威胁检测 | 僵尸网络检测 | 支持通过云端沙盒对全球威胁情报源进行验证，提取有效信息形成规则定期更新到僵尸网络识别库，增量提升检测能力； |
| 具备僵尸网络识别能力，行为规则35万条以上 |
| DNS协议深度检测 | 支持DNSFlow分析引擎，利用机器学习算法结合威胁情报，能够从大量的样本中进行学习，总结其伪装的规律，从而发现伪装的恶意DNS协议；  |
| SMB协议深度检测 | 支持SMBFlow分析引擎，利用机器学习技术,发现主机传输可疑文件、恶意软件行为、文件或关键目录的可疑操作行为以及SMB暴力破解等 |
| AD域控检测 | 支持对AD域控服务器安全检测，发现主机对域控服务器DNS探测、SMB会话枚举、账户探测、暴力破解等攻击 |
| 文件威胁深度检测 | 支持从流量中还原可执行文件进行深度检测，并展示主机所感染恶意文件名、病毒名称、传播协议、外部感染源等 |
| 邮件深度检测 | 支持SMTPFlow分析引擎，利用机器学习技术技术,发现主机发送可疑附件的邮件行为、伪造发件人发送邮件、发送钓鱼网站邮件和垃圾邮件等行为； |
| 支持检测恶意邮件检测，可定位具体的收件人账号、发件人账号、恶意邮件数量、邮件附件是否包含病毒。 |
| Webshell攻击检测 | 支持HttpFlow分析引擎，利用机器学习技术，发现绕过防御的webshell攻击，并能够大幅度降低传统检测技术带来的误判； |
| 失陷业务检测 | 支持检测业务的异常行为，从而识别业务是否已失陷被控制，并设立失陷等级和威胁等级展示当前业务的状态和产生的威胁程度； |
| 风险用户检测 | 支持检测网络内部用户的异常行为，要求能够基于僵尸网络识别库，检测用户是否存在风险，并通过可视化方式展示：风险用户对业务产生的影响、内部的横向攻击、风险/违规行为等； |
| 异常行为检测 | 支持NetFlow分析引擎，利用UEBA方式来检测服务器外发异常，包括是否正在进行DoS攻击、网络内部的横向探测：如IP扫描、端口扫描、数据收集（如到其他服务器下载）或数据传输（将数据传给其他服务器或外网）。 |
| 6 | 外联威胁检测 | APT C&C通信 | 支持检测主机与C&C服务器通信行为，支持区分国内外区域； |
| 可疑行为 | 支持检测访问恶意链接、使用IRC协议进行通信、浏览最近30天注册域名、下载文件格式与实际文件不符、基于行为检测的木马远控、比特币挖矿等可疑访问行为，支持区分国内外区域和显示可疑行为访问趋势； |
| 隐蔽通信 | 支持检测隧道、Tor暗网通信、端口反弹等对外通信方式，支持区分国内外区域； |
| 违规访问 | 支持检测违规访问策略黑名单或违反了白名单，或者违反了下一代防火墙中的应用控制策略的行为 |
| 风险访问 | 支持检测服务器对外发起的远程登录、远程桌面、数据库等风险应用访问 |
| 外连攻击 | 支持检测主机对外发起的攻击行为 |
| 7 | 基础检测能力 | 数据索引 | 支持记录用户网络当中南北向和东西向的访问信息，包括时间、五元组、具体应用、归属地、访问次数、流量大小等各类实时信息；  |
| 支持识别应用类型超过1100种，应用识别规则总数超过3000条；  |
| 支持自动识别所有访问关系，并能够将访问请求进行归类：正常访问、风险访问、违规访问等； |
| 依托于大数据检索能力，提供详细的日志查询功能，便于事后取证； |
| 支持自定义威胁情报，可自定义确定性等级、威胁等级、事件描述、危害描述和处理建议 |
| 漏洞利用攻击检测 | 支持对服务器、客户端的各种应用发起的漏洞攻击进行检测，包括20种攻击类型共9000+以上规则 |
| 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP等）和数据库软件（MySQL、Oracle、MSSQL等）的口令暴力破解检测功能。 |
| WEB应用攻击检测 | 支持检测针对WEB应用的攻击，如SQL注入、XSS、系统命令等注入型攻击；支持跨站请求伪造CSRF攻击检测；支持对ASP,PHP,JSP等主流脚本语言编写的webshell后门脚本上传的检测；支持其他类型的Web攻击，如文件包含，目录遍历，信息泄露攻击等的检测； |
| 要求具备独立的Web应用检测规则库，Web应用检测规则总数在3000条以上；； |
| 8 | 威胁感知监控 | 外部风险行为监测 | 支持展示外网对网络内部尝试（或已成功）进行的远程登陆、数据库访问等行为，可查看明细列表，内容包括但不限于外网IP、受影响网络内部主机IP、外部风险访问者数等； |
| 正常业务外连监控 | 支持对业务的外连行为进行监测，以可视化的方式展示业务外连的地域分布、是否存在风险、外连趋势等，并提供详细的外连日志查询； |
| 潜伏威胁黄金眼 | 支持基于可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，能够直观的看到失陷主机攻击了谁，被谁攻击了，帮助管理人员及时了解威胁的影响，并制定有效的处置动作 |
| 失陷主机举证 | 支持对风险业务、风险用户进行详细举证，详细举证为什么评判该主机为失陷级，并针对每个举证的安全事件进行详细的描述，如具体事件、该事件带来的危害、如何进行处置； |
| 威胁攻击链展示 | 支持基于威胁活动链的形式展现主机的安全状况，能够直观地展示主机正处于被黑客入侵的哪个阶段，是否已经被利用、以及威胁的程度； |
| 访问关系梳理 | 支持基于用户/业务维度的访问关系梳理，可呈现该用户/业务已经通过哪些应用、协议和端口访问了哪些业务，这些访问是否是攻击、违规、远程登陆等行为，IT人员可清晰的看出已对哪些业务存在影响，也能推导当前用户是否已失陷（或可疑）。 |
| 9 | 报表与日志管理 | 主机安全风险报告 | 支持从业务和主机的角度详细分析各主机的安全风险状况，提供危害解释和参考解决方案；适用于日常处理安全问题的运维人员 |
| 脆弱性感知报告 | 支持分析具体的业务系统存在的脆弱性风险，提供危害解释和参考解决方案；  |
| 摘要报告 | 支持提供PDF格式报表形式的摘要报告，包含总体摘要、安全感知详情、UEBA行为画像、安全规划建设建议等，从整体展示安全状况，快速了解业务和网络的安全风险 |
| 综合风险报告 | 综支持合分析具体的业务系统和终端的安全风险详情，提供危害解释和参考解决方案 |
| 安全告警 | 支持以邮件的形式及时将发现的失陷业务、失陷用户、攻击成功事件等安全事件进行告警，支持根据安全事件类型配置发送间隔和触发条件； |
| 安全日志检索 | 支持 TB级数据秒级查询;支持检索接入设备传输过来的所有安全日志，可基于时间、攻击类型、严重等级等选择项进行组合查询，可基于具体设备、来源/目的所属、IP地址、特征ID、URL进行具体条件搜索；支持通过syslog等接收、存储第三方设备的日志，并提供详细的字段搜索能力； |
| 访问日志检索 | 支持检索接入设备传输过来的所有访问关系日志，可基于时间、访问类型、应用类型等选择项进行组合查询，可基于具体设备、来源/目的所属）、IP地址、端口进行具体条件搜索； |
| 10 | 联动响应 | 安全组件接入展示 | 支持接入防火墙、上网行为管理、终端EDR、虚拟安全系统和潜伏威胁探针,并在页面中显示安全组件接入的数量和状态；  |
| EDR组件联动 | 支持与同品牌终端EDR组件联动响应，禁止攻击流量出站或入站，也可以实现被感染主机IP封锁隔离，防止风险扩展； |
| 防火墙设备联动 | 支持与同品牌防火墙进行联动响应，支持平台下发安全策略到防火墙上，阻断攻击IP； |
| SSL VPN设备联动 | 支持同步SSL VPN用户信息，实现与安全事件关联；支持同步管理日志，满足审计要求 |
| 上网行为设备联动 | 支持与同品牌上网行为管理设备进行联动响应，同步上网行为管理设备认证用户，实现与安全事件关联；支持通过浏览器推送用户提醒或冻结用户上网； |
| 11 | 设备管理 | 特征库升级 | 具备IPS漏洞特征识别库、WEB应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、URL库、应用识别库、恶意链接库、白名单库等，支持定期自动升级或离线手动升级 |
| 深度检测引擎升级 | 具备安全日志分析引擎、DnsFlow行为分析引擎、HttpFLow分析引擎、NetFLow分析引擎、MailFLow分析引擎、SmbFLow分析引擎、威胁情报分析关联引擎、第三方安全检测引擎、文件威胁检测引擎等，支持定期自动升级或离线手动升级 |
| 接入设备管理 | 支持管控接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级； |
| 对接入的安全组件实时监控，包括展示是否在线、日志传输模式、今日传输日志量、当前传输总量等； |
| 平台运行监控 | 支持对平台的CPU、内存、磁盘利用率进行实时监控，同时支持对核心进程的资源占用率进行实时分析 |
| **潜伏威胁探针** |
| 1 | 接口数量 | 6个千兆电口、4个千兆光口、2个万兆光口 |
| 2 | 性能指标 | 3Gbps |
| 3 | 部署模式 | 旁路部署，支持探针同时接入多个镜像口，每个口相互独立不影响 |
| 4 | 资产发现 | 具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等 |
| 5 | 基础检测功能 | 具备报文检测引擎,可实现IP碎片重组、TCP流重组、应用层协议识别与解析等,  具备多种的入侵攻击模式或恶意URL监测模式,可完成模式匹配并生成事件,可提取URL记录和 域名记录,在特征事件触发时可以基于五元组和二元组(IP对)进行原始报文的录制。 |
| 6 | 监测识别规则库 | 能够识别应用类型超过1100种，应用识别规则总数超过3000条，具备亿万级别URL识别能力。漏洞利用规则特征库数量在4000条以上，漏洞利用特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应CVE编号 |
| 7 | 异常会话检测 | 可实现对外联行为分析、间歇会话连接分析、加密通道分析、异常域名分析、上下行流量分析等在内 的多场景网络异常通信行为分析能力。 |
| 8 | 深度监测能力 | 可提供网络流量的会话级视图,根据网络流量的正常行为轮廓特征建立正常流量模型,判别流量是否出现异常,对原始流记录进行异常检测,可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP地址扫描，端口扫描，ARP欺骗，IP协议异常报文检测和TCP协议异常报文等常见网络异常流量事件类型;支持对节点检测节点内部主机外发的异常流量进行检测 支持对信任区域主机外发的异常流量进行检测，如ICMP，UPD，SYN，DNS Flood等DDoS攻击行为；支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解检测功能；可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测 |
| 9 | 高级检测 | 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 |
| 支持DNS审计日志，主要用于平台dns flow分析引擎进行安全分析；HTTP审计日志，主要用于平台http flow分析引擎进行安全分析；SMB审计日志，主要用于平台SMB flow分析引擎进行安全分析；同步SMTP、POP3、IMAP审计日志，主要用于平台Mail flow分析引擎进行安全分析，同步AD域协议审计日志，主要用于平台AD域分析引擎进行安全分析 |
| 10 | Web应用安全检测能力 | 支持HTTP 1.0/1.1，HTTPS协议的安全威胁检测；支持针对B/S架构应用抵御SQL注入、XSS、系统命令等注入型攻击；支持跨站请求伪造CSRF攻击检测；支持对ASP,PHP,JSP等主流脚本语言编写的webshell后门脚本上传的检测；支持其他类型的Web攻击，如文件包含，目录遍历，信息泄露攻击等的检测；产品应具备独立的Web应用检测规则库，Web应用检测规则总数在3000条以上； 支持敏感数据泄密功能检测能力，支持敏感信息自定义，支持根据文件类型和敏感关键字进行信息过滤；支持对被Web网站是否被挂黑链进行检测 |
| 11 | 僵尸网络检测 | 支持对终端种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为；具备独立的僵尸主机识别特征库，恶意软件识别特征总数在35万条以上；对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁特征； |
| 12 | 违规访问检测 | 能够针对IP，IP组，服务，端口，访问时间等策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单（哪些访问逻辑是正常的）和黑名单（哪些访问逻辑肯定是异常的）两种方式 |
| 13 | 流量记录 | 能够对网络通信行为进行还原和记录，以供安全人员进行取证分析，还原内容包括：TCP会话记录、Web访问记录、SQL访问记录、DNS解析记录、文件传输行为、LDAP登录行为。 |
| 14 | 抓包分析 | 支持通过设备对流量进行抓包分析，可定义抓包数量、接口、IP地址、端口或自定义过滤表达式 |
| 15 | 管理功能 | 能够支持时间同步支持设备内置简单命令行管理窗口，便于基础运维调试（需提供截图证明）能够提供网络管理功能，可进行静态路由配置多次登录失败将锁定账号5分钟内不得登录可支持在线升级和离线升级，并依托安全感知平台进行统一管控可支持用户初次登陆强制修改密码功能。可实时监控设备的CPU、内存、存储空间使用情况。能够监控监听接口的实时流量情况 |
| 16 | 集中管控 | 支持安全感知平台对接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级； |
| 17 | 部署 | 支持旁路部署，对镜像流量进行监听可以多台采集器同时部署于客户网络不同位置并将数据传输到同一套分析平台 |

**2.安全服务内容**

* **定期安全检查**

**服务频次：每季度一次**

**服务内容：**

对医院的现网整体安全提供全面的巡检服务，巡检的内容包括但不限于：

* 安全设备品牌、设备型号、设备放置、设备性能参数、设备内存大小、设备槽位、设备序列号、设备购买年限、设备保修状态、设备备件状况、设备标签完善程度；
* 安全设备软件版本信息、当前IOS版本信息、最新IOS版本信息、设备持续运行时间、设备IOS备份情况、设备CPU利用率、设备内存利用率、设备模块运行状态、设备风扇及电源状况、设备端口数量、设备端口类别、设备端口类型、设备运行机箱温度；
* 安全设备连通性、冗余协议运行状态、VLAN信息、以太通道信息、路由协议、邻居关系、交换协议、生成树STP协议、NAT连接数状态、FLASH信息、设备配置信息分析、多余配置信息分析、配置精简建议、IOS安全建议、防火墙信息、防火墙策略、防火墙DMZ区检查、防火墙Xlate状态、应用业务、IP地址使用状况；
* 对设备性能、告警信息、被攻击和入侵情况（如入侵事件、入侵源、前十位攻击对象等）、安全威胁进行动态评估；
* 对安全系统瓶颈和资源竞争情况进行分析，找出潜在问题。
* 对服务器、终端做周期检查，主要内容是检查是否存在高危漏洞，杀毒软件病毒库是否最新。如果发现问题需要及时提供人工现场处理修复或者升级服务。
* **安全风险评估**

**服务频次：一年内不限次数**

**服务内容：**

在现网架构改动、新系统上线、配置变更的时候，对变动带来的风险进行识别和评估，提出风险预防和必要的整改措施。风险评估的对象包括但不限于以下内容：

（1）主机房环境，包括其环境、设备和设施等；

（2）存储被测系统重要数据的介质的存放环境；

（3）整个系统的网络拓扑结构；

（4）安全设备，包括防火墙、入侵检测设备、防病毒网关等；

（5）边界网络设备，包括路由器、防火墙和认证网关等；

（6）对整个信息系统或其局部的安全性起决定作用的网络互联设备，如核心交换机、汇聚层交换机、核心路由器等；

（7） 承载被测系统核心或重要业务、数据的服务器（包括其操作系统和数据库）；

（8）能够代表被测系统主要使命的业务应用系统；

（9）信息安全主管人员、各方面的负责人员；

（10）涉及到信息系统安全的所有管理制度和记录。

风险评估的方式包括人工访谈、工具检测、登录系统检测、文档分析，风险评估会涉及到物理安全、网络安全、主机系统安全、应用安全和数据安全、安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理等十个方面。

* **安全事件紧急响应**

**服务频次：一年内不限次数**

**服务内容：**

安全事件响应要求维护商在广州有总公司、分公司或办事处常驻有安全工程师，在接到医院的安全事件紧急救援服务请求后，本地安全工程师立即响应，通过预先确认的远程连接方式登录到相应的系统上，对安全事件进行排查，在发现远程登录无法解决的安全事件后，立即采用最快的交通方式赶赴客户现场，2小时内可达到医院的现场。每逢各大节假日和重要的国家政治事件提供工程师驻场服务。

当医院发生大规模的安全事件后，如信息系统中的计算机或网络设备系统的硬件、软件、数据因非法攻击或病毒入侵等安全原因而遭到破坏、更改，或已经发现的有可能造成上述现象的安全隐患，如非授权访问、信息泄密、系统性能严重下降、黑客攻击、蠕虫或大面积爆发病毒等，维护商常驻广州的安全团队将在2小时之内赶赴现场协助解决问题，必要时应提供入侵调查分析、安全审计预警与黑客追踪服务。

应急响应服务包括远程应急响应服务和本地应急响应服务，其主要内容如下：

1)消除潜在安全隐患： 通过日志信息和其他必要信息，检查后门程序和网络系统漏洞，消除其再次受到攻击的可能性，即消除今后的安全隐患，对系统的安全进行重新评估。

2)检查安全日志： 通过检查系统、防火墙、路由器等系统安全日志，为确认攻击来源和攻击手段以及调查取证提供必要的条件。

3)入侵者追踪： 通过所能得到的信息追踪入侵者，并记录其尽可能多的信息，为调查取证提供条件。

4)主机恢复： 在客户信息系统网络或主机受到攻击并且出现网页遭替换或系统丢失等恶性事件后，确认已经消除安全隐患，在系统网络管理人员的协助下，对应用系统或操作系统进行恢复，保证系统资源在第一时间内的可使用性。

5)网络恢复： 医院信息系统的核心交换机、路由设备等网络设备出现问题，在确定是受到攻击所造成的情况下，确认已消除安全隐患，在经过医院授权后，对网络设备进行恢复，保证医院信息系统网络资源在第一时间内的可使用性。

* **安全配置备份**

**服务频次：不定期备份，一个季度至少一次**

**服务内容：**

1、为了保证安全设备的健康运行情况，使得设备在失效或配置丢失时，能依靠备份尽快地恢复系统与配置，保护关键策略，保证配置不丢失，特制定本服务。

2、关键的网络安全设备的策略配置进行备份，防止策略的丢失与错误变更配置；涉及备份和恢复的事由专人负责备份工作，并认真填写备份日志。

3、备份数据应该严格管理，妥善保存；备份资料保管地点应有防火、防热、防潮、防尘、防磁、防盗设施。

4、一旦发生配置丢失或数据破坏等情况，要由负责人员进行备份数据的恢复，以免造成不必要的麻烦或更大的损失。

* **安全设备日志分析**

**服务频次：一季度一次**

**服务内容：**

1. 日志收集。定期收集各个安全设备的日志和报表进行存档以便分析。

2. 分析日志。跟据客户设备的具体情况，分析关键服务器、安全设备等设备的日志, 采取人工加工具的审计分析方法对日志信息进行综合分析,找到当前的系统及网络设备中存在的隐患和被攻击痕迹。

3. 生成报告。根据以上评估，生成具体的日志分析报告，服务商将会人工结合用户网络的构成及业务流程等，为客户量身定制出专业又极具可读性的报告，并会针对报告中的各项问题，为客户提供修补建议，使发现的问题能尽可能早的得到解决，避免引起更大范围的影响和损失。

4. 其它支持。客户得到服务商提交的日志审计报告后，可以根据报告的内容对系统进行检查和修补，在此过程中的所有疑问都可以通过客服热线与服务商安全专家取得联系，获得在线咨询和指导。

* **安全建设配合响应**

**服务频次：一年内不限次数**

**服务内容：**

在医院相关或上级部门提出安全建设、安全整改、安全加固等任务时，派遣专业安全技术人员指导配合进行安全相关工作，工作内容包括但不限于以下内容：

* 医院网站漏洞排查；
* 公安部门递送的安全检查或安全漏洞通知；
* 上级部门递送的安全检查或安全漏洞通知；
* 国家重大事件的安全保障检查；
* 突发性事件的检查通知或现场检查；

在上述事件发生的时候，医院需要有安全水平高的行业技术人员配合医院开展安全方面相关工作，维护商要根据约定的时间安排专业安全工程师提供远程或上门的安全相关服务，具体服务内容由医院和维护商根据具体要求商议决定。

* **安全设备配置适应性调整**

**服务频次：一年内不限次数**

**服务内容：**

在安全相关设备配置需要调整时，如：安全策略调整、新链路配置、产品参数调整等；维护公司必须派遣工程师进行配置风险评估、提出调整方案并实施。安全相关设备配置包括但不限于以下情况：

* 网络出口新增加，评估新网络出口的风险和安全防护措施；
* 防火墙、UTM等边界类设备的配置变更，详细记录变更内容，包括IP策略、端口策略、放通/禁止策略等；
* 网闸等隔离类设备的配置变更，详细记录变更内容，包括IP策略、端口策略、应用通道、转发模式等；
* 入侵防御、网络行为分析等旁路安全设备配置变更，包括协议监控、端口监控、联动策略等；
* 杀毒软件、准入控制等终端管理类软件的配置变更，包括扫描策略、准入方式、控制范围等；

维护商在协助医院进行安全设备或软件的配置变更时，要充分考虑到配置变更过程中和变更后带来的安全风险，采取一定的预防措施，将风险降低到最小，最小化对医院正常业务开展的带来的影响。

* **系统漏洞扫描与分析**

**服务频次：每季度一次**

**服务内容：**

维护商定期利用专业的技术工具对系统进行测试，包括基于网络探测和基于主机审计的漏洞扫描、网站漏洞扫描、数据库漏洞扫描等，扫描相关使用的专业工具版本由维护商提供，医院无需为该工具支持额外费用。

维护商对发现的问题或安全漏洞提出整改建议，并配合相关客户做好整改工作。

* **安全培训服务**

**服务频次：按需求不定期培训**

**服务内容：**

配合医院展开安全建设和运维的工作，定期对医院信息科相关人员提供信息安全技术培训，提升医院信息安全意识和技术知识水平。

* 培训对象

医院系统管理员、网络管理员、数据库管理员、安全审计员等专业技术人员。

* 培训内容包括但不限于以下内容：

国家等级保护流程与相关内容

医疗行业等级保护建设案例分享

医疗行业内外网互联安全建设风险

医疗行业网站建设和漏洞防范介绍

医疗行业数据库安全和漏洞防范介绍等。

* **安全制度建设**

**服务频次：一年一次**

**服务内容：**

结合我院信息安全的实际情况，为我院提供信息安全制度建设服务，服务内容包括但不限定于：

* 计算机及软件备案管理制度
* 计算机安全使用与保密管理规定
* 用户密码安全保密管理规定
* 涉密移动存储设备的使用管理
* 数据复制操作管理规定
* 计算机、存储介质、及相关设备维修、维护、报废、销毁管理规定
	+ - 1. **集成服务**

为了提供最高的可靠性和安全性，最大限度降低生产环境的停机风险,投标人必须向采购人提供本项目采购的所有硬件的安装和维护服务的全部内容，并在需要的时候配合设备使用单位完成整个系统的联调工作。

▲本次采购的服务器需要替换电子病历原有业务服务器，供货商在将新服务器替换原有服务器的过程中，不能对原有业务系统的正常运行造成影响，在替换完成后原有的状态必须是正常运行。

▲本次新增虚拟化服务器需要接入医院现有的虚拟化平台，供货商负责提供虚拟化平台接入和优化服务，并且提供详细的接入和优化相关文档。

▲本次PACS存储扩容需要对PACS的原图、在线、发布等应用的存储空间进行扩展，在扩容过程中，不能对PACS原有业务造成影响，不能造成PACS系统的数据丢失，扩容后的存储性能不能低于原有PACS存储的性能。

**附件2**

**应急指挥系统功能扩展项目用户需求**

1. **应急指挥调度中心与院内信息平台对接**

1、应急指挥调度中心与信息平台对接，完成与院前急救、急诊与院内各相关科室的患者信息共享，电子病历共享。

2、卫生行政部门的信息对接，急诊科能够在患者送达前获取急救中心转送或基层医疗机构转诊患者信息，院内相关各科室在患者收住入院前获取病历资料，提高效率。

3、应急指挥调度中心可扩展或对接医院胸痛中心、脑卒中中心、创伤中心。

1. **无人机巡检系统**

1、定制化无人机，要求有热成像技术，突破光线和环境的限制，即使在黑夜、浓烟或树林中也可轻松辨识搜索目标。3分钟之内准备时间快速起飞，适合紧急搜救任务。采集到的图像可用于制作3D地图、3D建模和正射影像图，从而精确统计受损区域及受损程度。3.5 倍光学变焦镜头与2 倍数码变焦；有效像素不低于1240 万，支持4K 高清视频录制。配备高精度三轴云台。

最大起飞重量：≥3600g,工作环境温度：-10℃-40℃，

额定功率：≤100w,电池容量：≥5700mAh,

悬停精度（可安全飞行，有GPS）：≥垂直：0.5 m，水平：2.5 m；

最大旋转角速度：≥ 俯仰轴：300°/s，航向轴：150°/s ，

最大俯仰角度：≥ 35°，最大上升速度：≥ 5 m/s ，最大下降速度：≤ 4 m/s；最大可承受风速：≥10 m/s 最大航行速度 ：≥17 m/s （GPS模式下，无负载，海平面附近无风环境） 悬停时间：负载1 kg：≥16 min ，无负载：≥23 min 悬停精度（可安全飞行，有GPS）：≤ 垂直：0.5 m，水平：2.5 m

2、与应急指挥调度中心系统对接，可在系统内看到巡航音视频，及时掌控现场 拯救生命 在突发事件中，无人机能进行大范围监控和搜索，迅速传递现场情况，提升反应效率。

**（三）配置清单**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **品名** | **数量** | **单位** |
| 1 | 无人机 | 1 | 台 |
| 2 | 云台相机 | 1 | 台 |
| 3 | 连接件套件 | 8 | 个 |
| 4 | 视觉传感导航系统 | 1 | 套 |
| 5 | 充电器 | 1 | 个 |
| 6 | 备用电池 | 1 | 个 |
| 7 | PAD | 1 | 台 |