**本项目采购预算最高限价：15万元整**

1. **采购内容及要求**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 使用单位 | 级别 | 数量 | 服务内容 | 服务期限 |
| 1 | 安全态势感知平台服务 | 瑞安市人民医院 | 三级 | 1套 | 基础安全服务 | 1年 |

* 1. 基础安全服务

3.1.1三级医院基础安全服务技术要求及指标：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 服务类型 | 名称 | 技术服务内容 | 数量 | 单位 |
| 1 | 硬件设备 | 综合日志审计设备租用服务 | 详见具体服务功能要求或配置描述 | 1 | 台 |
| 2 | APT网络战预警设备租用服务 | 详见具体服务功能要求或配置描述 | 1 | 台 |
| 3 | 态势感知综合平台功能服务 | 等级化保护的实时动态监测服务 | 详见具体服务功能要求或配置描述 | 1 | 项 |
| 4 | 网络流量攻击分析能力服务 | 详见具体服务功能要求或配置描述 | 1 | 项 |
| 5 | 人工安全服务 | 新系统上线检查服务 | 详见具体服务功能要求或配置描述 | 1 | 项 |

3.1.2三级医院硬件设备功能要求：

1）综合日志审计设备

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 品牌要求 | 产品获得公安部计算机信息系统安全产品销售许可证产品获得国家保密科技测评中心检测并获得涉密信息系统产品检测证书产品取得软件著作权登记证书 |
| 工作模式 | 独立完成审计日志采集，不依赖于设备或系统自身的日志系统；审计工作不影响被审计对象的性能、稳定性或日常管理流程；审计结果存储于独立存储空间；自身用户管理与设备或主机的管理、使用、权限无关联；提供全中文WEB管理界面，无需安装任意客户端软件或插件 |
| 硬件规格 | 4个电口，1个console口，内存：32GB，磁盘：6T\*4，双电源，可扩展项：内存可扩展至128GB，单个磁盘可扩展至4T(8个盘位)，支持HBA卡扩展,支持扩展光模块产品CF卡化：产品操作系统存储在CF卡中，日志数据存储在磁盘，提供可靠性。（提供第三方检测报告） |
| 处理性能 | 平均处理能力（每秒日志解析能力EPS）：15000EPS；峰值处理能力（每秒日志解析能力EPS）：14000EPS。 |
| 功能扩展 | 要求采用解决方案包上传对产品进行功能扩展，无需代码开发。 |
| 日志收集 | 支持Syslog、SNMP Trap、OPSec、FTP协议日志收集支持使用代理(Agent)方式提取日志并收集；支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等；设备厂家包括但不限于：Cisco(思科)，Juniper，联想网御/网御神州，F5，华为，H3C，微软，绿盟，飞塔(fortinet)，Foundry，天融信，启明星辰，天网，趋势，东软，Nokia，CheckPoint，Hillstone(山石)，安恒，珠海伟思，BEA，中国电信，安氏，帕拉迪，apc，arbor，clam，戴尔（dell），digium，东方电子，EMC，中国电力科学研究院，Eudora，google，冠群金辰，linksys，Mcafee，netapp，NAS（美国国家安全局），永达，sonicwall，vigor，天存，西岭，Symantec（赛门铁克），Hardened-PHP，foundertech(方正)，三零盛安，allot，蓝盾，IBM，金诺网安，网威，nortel(北电)，citrix(思杰)，watchguard，中兴，阿帕奇，WINDOWS系统日志，Linux/UNIX syslog、IIS、Apache等；支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等 |
| 日志分析 | 可以以日志等级进行过滤；应该可以通过自定义配置将用户不关心的日志过滤掉；支持对收集到的重复的日志进行自动的聚合归并，减少日志量；支持可由用户定义和修改的日志的聚合归并逻辑规则;支持将收集到的日志转发，当原始日志设备无法设置多个日志服务器时，可以通过本系统的日志转发功能将日志转发到其他日志存储设备；支持对收集到的日志进行解析（标准化、归一化），解析规则可以根据客户要求定制扩展。可对日志进行细粒度解析，解析后的日志根据具体日志包含但不限于：日期、发生时间、接收时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议、地理信息（公网情况）支持基于内存的实时关联分析，跨设备的多事件关联分析；支持自定义条件都事件进行聚合；进行关联分析的规则可定制；支持根据资产价值、资产漏洞、针对漏洞的威胁事件三者进行威胁的自动关联分析（三维关联），所有的三维关联算法和准则以CVE、Bugtraq、OWASP公开协议和标准为为基础（提供第三方检测报告） |
| 日志备份 | 可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；支持日志备份自动传送到远程服务器； |
| 日志查询 | 支持B/S模式管理，支持SSL加密模式访问；支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询；支持用任意关键字对所有事件进行高性能全文检索支持可指定多个查询条件进行组合查询支持将查询的条件存储为查询模版，方便再次使用极高的日志高查询性能，支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果。 |
| 应用性能监控（APM） | 性能监控：通过在目标主机上安装agent程序，支持监控目标主机的CPU利用率、内存使用率、磁盘使用情况、流量等信息，并支持设置报警阈值。支持如下应用的性能监控（Windows、Linux、Aix、FeeBSD、HP-UX/Tru64、Max OS、Sun Solaris）、数据库（mysql、oracle）、应用服务器（weblogic、tomcat）、web服务器（apache）。（提供第三方检测报告）支持应用性能历史详情回溯查看支持如下性能监控参数支持监控Windows操作系统如下参数：cpu使用率、内存使用率、磁盘使用率、网络发送流量、网络接收流量、网络发送接收总流量、交换区使用率、磁盘总使用率、进程数、线程数；支持监控Linux操作系统如下参数：一分钟系统负载、5分钟系统负载、15分钟系统负载、cpu使用率、内存使用率、磁盘使用率、网络发送流量、网络接收流量、网络发送接收总流量、交换区使用率、磁盘总使用率、进程数、线程数支持监控Mysql如下参数：查询缓存命中率、键缓存命中率、立即获得锁数、连接数、线程数、每秒SQL查询数、每秒发送字节、每秒接收字节；支持监控Oracle如下参数：库缓存命中率、内存排序比率、词典缓存命中率、SGA数据缓存命中率、重做日志缓存命中率；支持监控Apache如下参数：总访问数、写日志次数、每秒发送字节数、长连接数、关闭连接数、空闲活动数、查询DNS数、正在发送数、请求完成数、负载、等待连接数、总数据量、读操作数、工作线程数、空闲线程数、CPU占用率支持监控应用服务器（tomcat、weblogic）如下参数：活动线程数、堆内存（已用）、守护线程数； |
| 脆弱性管理 | 弱点管理：支持导入安恒明鉴弱点扫描器、绿盟极光扫描器等扫描报告，可进行统一检索，并支持计算威胁等级。（提供第三方检测报告）支持从IBM Rational AppScan导入资产弱点漏洞信息支持从安恒明鉴Web应用监测工具导入网站弱点漏洞信息支持从安恒明鉴数据库弱点扫描器导入数据库弱点漏洞信息支持从NetSparker Web应用扫描器导入网站弱点漏洞信息支持从Nessus网络扫描器导入网络弱点漏洞信息支持从OpenVAS扫描器导入弱点漏洞信息内置73000+条CVE漏洞数据知识库内置数十项符合OWASP的Web漏洞数据知识库 |
| 地理安全系统 | 内置GeoSec地理安全子系统，内置世界以及中国安全GIS地图支持用地理地图展示来源威胁的趋势支持用地理地图展示目的威胁的趋势支持在地理地图上标注威胁事件的发生分布内置IP地址到经纬度的转换库支持以地理信息类进行统计的数据报表支持切换Google地图（需要连通互联网） |
| 告警功能 | 可预设置安全告警策略；支持数据阀值设置，超过阀值将产生告警;可以通过邮件、短信和屏幕显示进行告警；支持自动防止报警信息在短时间内大量发送(告警抑制)；具备报警合并和在一个时间段内抑制报警次数的能力。 |
| 综合查询及报表管理 | 内置合规性报表1000+种；内置SOX、ISO27001、WEB安全等解决方案包内置完善的等级保护合规报表内置综合性自动化审计报告支持用户自定义报表；自定义的报表支持多个统计维度的数据集合。数据报表支持数据趋势预测功能，根据历史规律数据对未来数据的发展趋势进行预测报表支持详单数据钻取支持报表导出为PDF和Word格式文件。 |
| 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，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。系统自带自身管理日志注册用户资产时，提供自动发现识别能力。提供一键式故障排除功能。提供自助式的升级接口，支持对产品升级、规则升级。 |
| 部署方式 | 支持分布式部署；支持集中式管理和升级模式；支持分级管理模式；采用B/S架构操作方式，无需客户端安装。支持监控设备自身CPU、内存、磁盘等工作运行状况 |
| 售后服务 | 提供不少于五年产品原厂商质保服务； |
| 提供不少于五年的原厂商上门7\*24小时现场服务支持； |

2）APT网络战预警设备

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 产品资质 | 具备公安部颁发的《计算机信息系统安全专用产品销售许可证》 |
| 通过中国信息安全认证中心检测并获得证书 |
| 具有国家保密科技中心颁发的《恶意代码辅助检测系统》涉密信息系统检测证书 |
| 产品规格 | 软硬一体化2U标准机架式设备；  |
| 1+1冗余电源； |
| 可用磁盘空间不小于2T，带RAID1； |
| 6个千兆电口，4个千兆光口 |
| 产品性能要求 | 网络层：2Gbps，应用层：1Gbps HTTP最大并发数:7万/秒邮件处理数:150万封/24小时文件检测：5万个/24小时综合管理分析：支持管理节点10个 |
| 部署方式 | 旁路镜像模式部署，不影响服务器处理性能和网络架构； |
| 分布式部署 | 支持分布式部署，管理中心可实现告警统一管理；支持添加和删除探测器配置；支持根据添加探测器情况，配置探测器名称、发送时间、发送目录等信息支持显示不同探测器的IP、版本、状态和最近24小时的风险信息； |
| 自定义配置 | 管理中心和探测器之间的数据传输速率、时间、发送目录都可自定义；(提供功能截图证明) |
| 审计协议 | 支持审计http、ftp、smtp、pop3、smb、imap等协议报文提供审计协议类型的端口号配置，可根据需要变更端口号 |
| 检测风险类别 | 支持检测WEB攻击、异常访问、恶意代码攻击、访问黑IP黑域名、后门程序访问、发件人欺骗、邮件头欺骗、邮件钓鱼欺骗、邮件恶意链接、恶意行为、WEB渗透等风险 |
| 告警详细展现 | 可支持详细展现告警级别、时间、威胁名称、状态、客户端IP、服务端IP、报文、操作等信息，包含请求URL、请求类型、请求内容、请求头、Host、User-Agent、Accept、Accept-Language、Accept-Encoding、Accept-Charset、Keep-Alive、Connection、Cookie、请求参数、响应码、返回长度等信息 |
| 主机威胁分析 | 可根据不同威胁指数的主机实现攻击溯源和攻击过程的可视化分析 |
| 可通过攻击源、攻击目的对攻击路线进行统计，包括攻击的行为、告警，并以直观的图形化形式展示 |
| C&C URL配置 | 支持黑IP过滤，对危险IP可直接进行黑名单告警集成黑域名库，支持新增或删除黑白名单配置 |
| 木马回连分析 | 可自动学习网络流量中包含的各种可疑C&C IP/URL，包含各种可能对内网存在影响的IP和域名 |
| 快速识别网络中存在的恶意回连行为，包含回连主机IP、服务器IP、时间、行为等 |
| 对基于木马回连的非法数据传输等行为进行取证分析，包括回连主机IP、服务器IP、传输数据大小、协议类型等 |
| 攻击地图展示 | 可通过攻击源和目的的地理位置信息，以世界地图和中国地图的形式展示，并实现世界地图和中国地图自动切换直观展示攻击路径(提供功能截图证明) |
| HTTP解析 | 支持 HTTP协议解析，检测WEB攻击 |
| 双向审计 | 支持双向审计，对请求和响应都进行审计 |
| 攻击检测 | 支持SQL注入攻击检测支持命令注入攻击检测支持跨站脚本攻击检测支持代码注入攻击检测支持协议错误攻击检测 |
| WEBSHELL检测 | 支持WEBSHELL检测，可检测访问webshell的行为，包含具体对应的URL、返回码、返回数据包内容等(提供功能截图证明) |
| 自定义WEB审计规则 | 支持根据来源IP、MAC、HTTP请求方法、URL、请求头、请求参数、响应码等内容设置审计规则高、中、低等风险等级 |
| 动态分析 | 自动关联行为分析的详细展现，包含SQL注入取数据、表单破解、XSS测试、目录穿越读取文件、多人访问Webshell、APT攻击等 |
| 解析协议 | 支持解析webmail、SMTP、POP3类型报文 |
| Webmail攻击检测 | 支持基于webmail攻击类型检测，包括sql注入、跨站、命令注入等攻击检测 |
| 社工类攻击检测 | 对社工类攻击进行检测，检测内容包括：邮件头欺骗、邮件发件人欺骗、邮件钓鱼欺骗、邮件恶意链接(提供功能截图证明) |
| 恶意附件检测 | 支持邮件恶意附件行为检测 |
| 解析协议 | 支持 HTTP 、ftp、smb、SMTP、POP3等协议传输文件检测 |
| 文件类型 | 支持doc, xls, ppt, swf, pdf, java, rar, zip, rar, exe, vbs, scr, html等多种文件解析 |
| 自定义文件类型 | 可添加或删除指定审计文件类型 |
| 特征检测 | 对文件进行特征匹配，利用已知的特征库发现恶意可以执行代码对文件进行特征匹配，利用已知的特征库发现恶意的非可执行文件 |
| Shellcode检测 | 通过分析文件中的二进制代码，找到文件溢出攻击的代码，并能找到APT攻击中的0day攻击(提供功能截图证明) |
| 动态沙箱检测 | 对存在问题的文件输出完整的二进制动态分析报告可展示文件中版本信息、段信息、资源信息、导入表、字符串信息、删除文件信息等内容（提供截图证明） |
| 子文件扫描 | 对文件内部嵌入的子文件可进行二次扫描，分析安全性 |
| 攻击样本提取 | 可以提取出攻击的完整样本文件，并提供对该文件下载的能力 |
| **管理功能** |
| 三权分立用户管理 | 提供三权分立的用户管理能力：配置员、用户管理员、审计员相互独立，支持自定义管理用户权限和角色 |
| 风险处理 | 支持根据需要对风险状态进行选择处理中、处理完成、延迟处理、拒绝处理等 |
| 攻击追溯 | 支持IP地址追溯，迅速定位攻击 |
| 设备状态监控 | 支持对设备的CPU、内存等状态进行监控，并在设备界面中进行展示  |
| 知识库 | 根据不同的风险信息，提供风险分析知识库；根据不同的风险信息，提供风险处理建议知识库； |
| 告警与报表 | 告警可详细展示风险级别、发生时间、告警名称、客户端IP、服务器IP、报文内容（URL、请求头、请求参数、请求内容） |
| 可根据需要针对单个告警添加白名单 |
| 支持短信、邮件、syslog、snmp、ftp等告警方式 |
| 支持同时发送多人、单条发送、发送统计等高级告警功能；  |
| 报表能够支持WORD、PDF等格式导出； |
| 日志数据管理 | 审计数据保留策略应至少满足天数和百分比两个控制参数，且支持web界面可配置，且恢复数据不影响正常的审计功能 |
| 支持自动备份审计日志，备份完后通过FTP方式外送到外部设备；备份文件需要进行加密，且必须导入设备才能够进行恢复查看； |
| 当磁盘空间达到一定的阀值，支持自动清理最早的数据释放空间； |
| 售后服务 | 提供不少于五年产品原厂商质保服务； |
| 提供不少于五年的原厂商上门7\*24小时现场服务支持； |

### 3.1.4态势感知综合平台功能服务

1）等级化保护的实时动态监测服务

|  |  |
| --- | --- |
| 服务类别 | 服务能力要求 |
| 等保监测功能展示 | 根据等保合规事件对医院分平台整体态势展现，包括网络层设备和安全情况进行统计、主机安全资产和风险情况统计、应用安全攻击和威胁事件统计、TOP10风险管理统计等视图展现。 （提供截图证明） |
| 告警功能 | 可预设置安全告警策略；支持数据阀值设置，超过阀值将产生告警;可以通过邮件、短信和屏幕显示进行告警；支持自动防止报警信息在短时间内大量发送，告警抑制策略可自定义；（提供截图）支持告警处置建议。 |
| 综合查询及报表管理 | 支持用户自定义报表；自定义的报表支持多个统计维度的数据集合。数据报表支持数据趋势预测功能，根据历史规律数据对未来数据的发展趋势进行预测报表支持详单数据钻取支持报表导出为PDF和Word格式文件。 |

2）网络流量攻击分析能力服务

|  |  |
| --- | --- |
| 服务类别 | 服务能力要求 |
| 网络流量攻击检测服务 | 对可疑文件进行虚拟执行，有效识别恶意文件、病毒等威胁； |
| 支持Web攻击检测：包括HTTP解析、双向审计、Webshell检测、行为关联分析、DNS协议分析等，并能够与WAF，FW设备联动阻断； |
| 支持对全流量采集探针中的各种深度解析后的流量日志进行关联分析，可针对HTTP头部、DNS解析行为、邮件相关行为、文件传输行为、流量数据包进行关联分析，以发现潜藏在流量中的内外部威胁； |
| 支持邮件攻击检测：包括邮件协议解析、Webmail攻击检测、社工类攻击检测、恶意附件检测等； |
| 平台内置不低于1000种安全攻击检测规则，包括但不限于如下攻击检测：BashShellShock漏洞、Nginx文件解析漏洞、Struts2远程代码执行漏洞、XSS跨站脚本攻击 、SQL注入攻击、拒绝恶意脚本攻击等 |
| 平台支持多维安全关联攻击监测，包括但不限于如下攻击检测：扫描攻击、Webshell攻击、恶意文件攻击、暴力破解成功攻击、僵尸主机检测、漏洞利用成功事件、web页面篡改检测等 |
| 平台支持根据全流量关联分析，包括但不限于如下异常流量行为监测：异常流量攻击、DOS/DDos攻击CC攻击、UDP泛洪攻击、SYN泛洪攻击等 |
| 威胁情报管理及分析 | 支持云端获取威胁情报(支持在线实时更新和本地离线包导入两种方式),本地系统支持威胁情报关联分析，及时发现网络可疑安全事件，全面展现网络安全态势情况、动态提醒当前网络最新的安全威胁。此功能须支持按需选择使用，为防止数据泄露，当无需与云端互动时，须可屏蔽通信，将数据及安全分析能力控制在客户侧（需提供界面截图） |
| 支持第三方威胁情报数据的接入和离线威胁情报库的导入 |
| 支持基于威胁情报的0day漏洞监测和分析，支持0day漏洞数据导入并自动生成分析规则，支持本地网络中0day攻击详细信息查看和0day漏洞查询 |
| 支持安全威胁自定义添加，提供自定义添加入口和添加模板，不断丰富的安全威胁库（需提供界面截图） |
| 提供本地威胁情报库功能，支持本地威胁情报累计功能，实现对本地发现的高危安全事件、恶意IP、域名、病毒、木马等信息自动添加至本地威胁情报库，不断丰富威胁情报库的数据（需提供界面截图） |
| 提供知识库功能，可以根据不同的风险信息，提供风险分析知识库和风险处理建议知识库；（需提供界面截图） |

### 3.1.5人工安全服务要求

1）新系统上线检查服务

|  |  |
| --- | --- |
| 技术措施检查项 | 提供对技术措施的检查项必须包括：漏洞扫描、基线检查、渗透测试等三个方面 |
| 服务频次 | 12次/年，1-2个系统/次 |
| 输出报告 | 《新系统上线检查服务报告》 |