**金华市中心医院网络安全服务采购项目**

**一、项目概述**

金华市中心医院医疗集团（医学中心）于2021年以金华市中心医院为核心组建，目前拥有金华市中心医院、金华市妇幼保健院2家主要成员单位，金华市中心医院始建于1910年，是浙江中西部地区集医疗、科研、教学、预防、保健、康复为一体的三级甲等综合医院。金华市妇幼保健院始建于1983年，是集预防、保健、医疗、科研为一体的二级甲等妇幼保健院。两院区实行网络部署一体化、安全管理同质化模式。

为确保金华市中心医院医疗集团相关业务系统稳定可靠地运行，建设金华市中心医院医疗集团安全大数据平台，完成互联网医院平台等外网环境部署相关系统的监测及其防护、威胁情报、重点部署流量安全分析、数据可视化以及7\*24小时的不间断的专业网络安全服务，保障医院业务的安全运行。

**二、项目内容**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 产品名称 | 数量 | 单位 |
| 1 | 安全分析管理平台服务 | 1 | 套 |
| 2 | 集成安全管理系统服务 | 1 | 套 |
| 3 | 流量威胁监测服务 | 1 | 套 |
| 4 | 网页防篡改服务 | 1 | 套 |
| 5 | EDR主机安全服务 | 1 | 套 |
| 6 | 云网站防护服务 | 1 | 套 |
| 7 | 勒索保险与理赔服务 | 1 | 套 |
| 8 | 高级安全与应急服务 | 1 | 套 |
| 9 | 扩展检测与响应服务 | 1 | 套 |
| 10 | 下一代防火墙 | 1 | 台 |
| 11 | 上网行为管理 | 1 | 台 |

**三、技术参数**

**1、安全分析管理平台服务**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 监控中心 | 支持不同安全视角展示15个独立的大屏，同时能满足多种场景的监控，比如日常运维、攻防演练场景等。 |
| 支持安全基线配置监测，可监测到开放了禁用端口、协议、属性变更等，以IP地址、MAC地址、所属租户和检测到时间来判断是否处置。 |
| 支持快捷菜单悬浮控件，平台全部功能可根据使用习惯自定义添加到快捷控件，方便使用，提高运维工作效率 |
| 支持流量实时识别漏洞分析，页面上支持展示业务脆弱性风险分布、漏洞类型分析、漏洞态势与危害和处置建议，并支持导出脆弱性感知报告。 |
| 脆弱性管理 | 弱密码检测技术基于UEBA学习技术，提取登陆成功的特征，通过UEBA技术对响应体内容和登录跳转路径进行持续学习训练登录成功特征，可实时自动生成学习到的登陆成功规则。 |
| 弱密码检测规则支持高度自定义，包括规则名称、生效域名、长度规则、字符规则、字典序、web空密码、账号白名单、密码白名单。 |
| 分析中心 | 可扩展挖矿检测增强分析模块，该模块变挖矿病毒的被动防御为主动探测发现，并提供根据本地和云端的日志分析提供实时检测播报，包括本地挖矿检测和云端挖矿检测。 |
| 支持挖矿威胁专项分析页面，具备挖矿全阶段的检测分析能力，综合运用挖矿病毒情报、漏洞利用规则和攻击行为分析技术，对挖矿进行分析和告警，并提供相关处置建议。 |
| 具备基于AI的webshell通信流量检测，可检出加密（如冰蝎）的通信流量。具备650+webshell规则检测，且覆盖webshell整个攻击阶段检测，包括webshell上传点探测、webshell上传下载、webshell通信。 |
| 具备规则检测引擎，通过异常行为分析结合各类机器学习算法完成高级威胁检测，包括内网穿透、代理、远控、隧道、反弹shell等场景。 |
| 平台内置挖矿知识库，对常见的挖矿如：Bluehero挖矿蠕虫变种、虚拟货币挖矿、EnMiner挖矿病毒、PowerGhost挖矿病毒、DDG挖矿病毒、Docker挖矿、DDG挖矿变种、GroksterMiner挖矿病毒、Linux挖矿木马等提供对应的背景概述、详细分析、IOC、解决方案。 |
| 报告中心 | 支持以PPT形式快速生成日报、周报、月报、季度报、年报，包含网络安全整体解读、网络安全风险详情、告警及事件响应盘点，帮助用户高效汇报，体现安全工作价值。 |
| 订阅方式支持邮件订阅、微信订阅和短信订阅。 |

**2、集成安全管理系统服务**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 产品形态 | 产品支持软、硬件一体化与软硬件解耦两种部署方式，并支持网桥、路由、旁路模式部署 |
| 平台要求 | 平台包含数据库审计、运维审计、日志审计等安全功能组件 |
| 在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑的编排，并且可以连接、开启、关闭虚拟网络设备。 |
| 为了提供更好的排障手段，支持在平台内节点抓包分析功能，能够设置抓包的网口、过滤条件、文件大小等参数 |
| 平台支持关键安全组件双机功能，保障安全组件高可用；在双机场景下，管理平台要支持双机配置同步，在硬件故障时保障无感知切换。 |
| 支持双因素认证功能，用户需在登录时进行双重认证，以此提高用户的安全性。 |
| 支持禁用默认超级管理员账号，防止特权账号被滥用。 |
| 支持针对安全组件账号的三权分立管理，实现平台管理员账号与安全组件账号权限的对应，防止平台管理员对安全组件进行越权操作。 |
| 集中管控 | 支持基于一体化平台的安全管理中心功能，能够对设备进行统一纳管，包括规则库与补丁包的统一升级、策略的统一配置、客户端补丁包统一升级等 |
| 支持等保2.0安全管理中心要求自评功能，能够进行完整度评估 |
| 支持安全管理中心交付模板，帮助用户快速交付安全管理中心各项功能 |
| 支持对一体化平台上的虚拟安全组件和外部接入安全硬件的统一管理 |
| 数据库审计功能要求 | 本次提供16个数据库实例数授权。 |
| 审计性能：峰值SQL处理能力≥16000条/秒；硬件最大吞吐量2000Mbps；双向审计数据库流量200Mbps；标配日志存储数40亿条；审计日志检索能力≥1500万条/秒。 |
| 支持多种数据库类型的审计，支持Oracle数据库审计、SQL-Server数据库审计、DB2数据库审计、MySQL数据库审计、Informix数据库审计、达梦数据库审计、人大金仓数据库审计、postgresql数据库审计、sysbase数据库审计、cache数据库； |
| 支持白名单审计，系统使用审计白名单将非关注的内容进行过滤，不进行记录，降低了存储空间和无用信息的堆砌，白名单内容包括以下4个维度:SQL模板、业务系统、URL地址及数据库条件 |
| 支持自动基线学习数据库语义语法，并支持提取参数自动生成SQL模板，可以减少审计日志的重复写入和节省磁盘的存储空间 |
| 支持基于SQL命令的webshell检测，提供webshell日志查询；  可通过查看webshell攻击的时间、源IP、业务系统、webshell规则发现威胁； |
| 运维审计功能要求 | 本次提供20个内网运维授权数和10个外网运维授权数 |
| 审计性能：峰值SQL处理能力≥16000条/秒；硬件最大吞吐量2000Mbps；双向审计数据库流量200Mbps；标配日志存储数40亿条；审计日志检索能力≥1500万条/秒 |
| 内置配置管理员、密码管理员、审计管理员、系统管理员、系统审计员、普通运维用户等管理角色 |
| 针对RDP、VNC、X11等图形终端操作的连接情况进行记录及审计；记录发生时间、发生地址、服务端IP、客户端IP、操作指令、返回信息、操作备注、客户端端口、服务器端口、运维用户帐号、运维用户姓名、审批用户帐号、审批用户姓名、服务器用户名等信息； |
| 能够记录RDP协议中的活动窗口名称、删除文件等动作，并能记录RDP会话中的键盘输入信息； |
| 日志审计功能要求 | 本次提供100个日志资产授权数量；日志处理能力EPS：4000/秒 |
| 系统从不同设备或系统中所获得的各类日志、事件中抽取相关片段准确和完整地映射至安全事件的标准字段 |
| 对安全事件重新定级。能根据统一的安全策略，按照安全设备识别名、事件类别、事件级别等所有可能的条件及各种条件的组合对事件严重级别进行重定义 |
| 系统既可以完全收集采集对象上的日志信息，也支持在安全事件收集引擎上设置过滤条件，可过滤出无关安全事件，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，从而减少对网络带宽和数据库存储空间的占用。 |

**3、流量威胁检测服务**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 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。 |
| 漏洞利用攻击检测 | 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漏洞攻击等服务器漏洞攻击检测 |
| 支持Application漏洞攻击、File漏洞攻击、Scan漏洞攻击、Shellcode漏洞攻击、System漏洞攻击、Web Activex等客户端漏洞攻击检测。 |
| 支持FTP、IMAP、MS Sql、Mysql、Oracle、SMTP、SSH、Telnet等协议的暴力破解检测。 |
| 异常流量检测 | 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。 |
| 支持ICMP、UDP、SYN、DNS等协议外发异常流量检测，支持自定义阀值。 |
| 僵尸网络行为检测 | 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。 |
| 审计白名单 | 审计白名单支持源目IP、源目端口、日志类型和来源。 |
| 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。 |
| 支持传输安全检测日志，包括网络攻击检测日志、漏洞利用攻击检测日志、僵尸网络检测日志、业务弱点发现日志。 |
| 支持传输访问检测日志，包括正常访问、风险访问和违规访问。 |
| 支持传输协议审计日志，包括https、http、DNS、邮件协议、SMB、AD域、WEB登录、FTP、TELNET、ICMP、SNMP、SSL、sip、onvif、NFS、SOCKS、全流量元数据、数据库协议等审计日志。 |
| 抓包分析 | 支持流量抓包分析，可定义IP地址、端口、包大小阈值、包数量阈值。 |
| 管理功能 | 内置命令行管理窗口，便于进行基础运维调试。 |
| 可实时监控设备的CPU、内存、存储空间使用情况，以及监听接口的实时流量情况。 |
| 部署 | 支持多台流量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。 |

**4、网页防篡改服务**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 数量要求 | 本次要求支持防护目录数≥20个 |
| 网站防护与恢复 | 支持国产化银河麒麟V10、中标麒麟V7操作系统网站，以及Windows、linux等主流操作系统网站防篡改； |
| 支持采用基于文件过滤驱动保护技术、事件触发机制相结合方式的网页防篡改功能； |
| 支持各类网页文件的保护，包括静态和动态网页以及各类文件信息； |
| 支持防护模式和监控模式两种模式的防篡改模式 |
| 支持Ipv4/IPv6网络环境下部署管理防篡改； |
| 支持对指定文件夹以及子文件夹的保护，避免上传非法文件及木马等恶意文件或插入恶意代码； |
| 支持在断线情况下对网页文件目录的防护功能 |
| 支持服务器网站异常检测(linux与windows双平台)，检测防护端所在服务器网站进程是否正常或存在 |
| 支持网页防篡改支持增加策略生效时间控制，可在防护端设置防篡改功能的启用与停用的时间 |
| 支持运行日志定时清除(Windows平台)，避免日志文件过大导致系统问题 |
| 支持防护端与管理中心连接监控功能(Windows平台)，发现连接异常则对防护端进行重启，并记录重启动作 |
| 支持IIS、Weblogic、Websphere、Apache、Tomcat等Web服务器； |
| 支持超过40GB以上网页防篡改保护和恢复功能，以适应医院业务发展需要； |
| 支持大规模连续篡改攻击防护； |
| 日志系统 | 支持对与系统自身安全相关的下列事件产生审计记录： |
| 支持对管理角色进行增加、删除和属性修改等操作行为； |
| 支持对网页篡改、添加、删除进行日志记录，并针对文件、进程、攻击类型进行详细记录； |
| 支持针对时间、主机名文件、进程、攻击类型等进行日志筛选查询； |
| 集中监控 | 支持防篡改管理中心通过统一的管理中心进行远程管理、策略下发和日志收集 |

**5、EDR主机安全服务**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 数量要求 | 本次要求提供360个服务器端授权 |
| 产品形态 | 产品可以纯软件交付，包含管理控制中心软件及终端客户端软件，其中管理控制中心可云化部署；同时也支持硬件管理平台交付 |
| 多维度威胁展示 | 支持全网风险展示，包括但不限于未处理的勒索病毒数量、高级威胁、暴力破解、僵尸网络、WebShell后门、高危漏洞及其各自影响的终端数量 |
| 提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数 |
| 云端威胁分析 | 支持跳转链接至云端威胁情报中心，针对已发生的威胁提供详细的分析结果，包含威胁分析、网络行为、静态分析、分析环境和影响分析。 |
| 自动分组 | 支持终端自动分组管理，新接入的终端可以根据网段自动分配到对应的分组 |
| 资产管理 | 支持全网视角的终端资产统一清点，便于帮助用户快速发现风险面。清点信息包括操作系统、应用软件、监听端口和终端账户。 |
| 支持对单个终端运行状态的监控，包括但不限于进程、服务、网络连接、计划任务和开放共享信息 |
| 支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，支持统计最近一年未修改密码的账户 |
| 管理员管理 | 支持配置不同的权限角色，支持超级管理员、普通管理员（管理）、审计管理员（查看）三种权限，并配置可管辖的终端范围，支持管理员账号限制IP登录；支持管理员账号采用双因素认证 |
| 威胁检测 | 通过智能识别终端环境情况（低配硬件、老旧设备、虚拟化等）和当前终端资源占用，在闲时实时监控和病毒扫描场景，都可智能调整EDR的资源占用（CPU、IO等），为业务让出资源。 |
| 具备针对最新未知的文件，使用IOC特征（文件hash、dns、url、ip等）的技术，进行云端查询。 |
| 支持一键云鉴定服务，提供云端专家+沙箱+多引擎鉴定能力，结合云端威胁情报对已告警的威胁文件再次进行综合研判并给出100%黑白结果，用户可自助对管理平台告警的威胁快速判断是否误报和了解威胁详情。 |
| 文件实时监控 | 可实时监控文件的状态，在文件读、写、执行或者进入主机时主动进行扫描，支持根据用户性能偏好设置高、中、低3种防护级别 |
| Windows服务器加固 | 提供基于可信鉴定方式的进程防护方式，通过人工智能自学习机制，自动建立信任进程名单，阻断非可信进程的运行并提供配置指引，同时支持通过模板和手动的方式添加信任进程 |
| 支持windows服务器RDP远程登录保护，可开启RDP远程登录二次认证，以防止黑客对服务器的入侵 |
| 勒索病毒专项防护 | 基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御 |
| 支持监控诱饵文件，诱饵文件可被实时监控，当勒索病毒对该文件进行修改或加密操作时进行拦截 |
| 支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具 |
| 支持对勒索入侵的主流方式RDP暴破做全方位保护，包括RDP登录校验、RDP文件加白二次校验等功能 |
| 暴力破解检测 | 统计单个攻击源及分布式攻击源的暴力破解检测，支持按照RDP、SMB和SSH类型进行封堵并自定义爆破阈值，可对封停时间进行自设置 |
| 终端合规检查 | 一键式操作对指定Windows终端/终端组进行合规性检查，包括身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范，对不合规的检查项提供设置建议，并可视化展示终端的基线合规检查结果 |
| 一键式操作对指定Linux终端/终端组进行合规性检查，包括身份鉴别、访问控制、安全审计、SSH策略检测、入侵防范、恶意代码防范，对不合规的检查项提供设置建议，并可视化展示终端的基线合规检查结果 |
| 威胁处置 | 构建全网文件信誉库，当一台终端发现某一病毒文件，全网可进行感知并进行针对性查杀，支持处置病毒时选择是否在其它终端上同步处置 |
| 具备强力专杀云端下发通道，支持在管理端批量下发强力专杀工具到内网各终端快速响应终端威胁。 |
| 漏洞防护 | 支持流行Windows高危漏洞的轻补丁免疫防御，支持Windows补丁批量一键修复 |
| 微隔离 | 支持基于IP（组）、服务和角色维度进行配置项设置，并且支持对配置项的备份以及恢复操作 |
| 支持图形化显示业务系统、服务器及流量详情 |
| 流量线详情支持展示该流量线对应的控制策略；图形化显示服务器间流量关系，包括访问详情、流量趋势等 |

**6、云网站防护服务**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 数量要求 | 本次要求提供≥50个数目的web网站防护授权 |
| 部署形态 | 支持镜像和容器的方式部署在虚拟环境和云平台中。支持反向代理的部署方式，适应复杂使用环境的接入要求。 |
| Web应用防护 | 支持超过4900种Web应用防护规则，和超过1200种Web漏洞攻击特征识别规则。 |
| 支持防护SQL注入、XSS攻击、网页木马、网站扫描、Webshell、跨站请求伪造（CSRF）、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漏洞攻击等。 |
| 支持WEB登录弱口令检测。 |
| 支持自定义Web应用防护规则，通过正则表达式自定义规则匹配方向、动作、字符串、危险等级、动作、攻击影响、描述等。 |
| 语义分析 | 支持语义引擎用于检测Web攻击，能针对不同类型的Web攻击如命令注入攻击防护等，单独选择开启或关闭语义引擎检测。 |
| 支持自定义语义引擎白名单功能，包含通过Web应用防护规则、URL参数、IP地址、Webshell上传防护、SQL、XSS、后门扫描的方式排除。 |
| 机器人流量防护 | 产品原生支持BOT防护功能，可过滤机器人自动化流量，非联动其他组件或产品，并支持用户自定义保护阈值。 |
| 支持自定义BOT防护排除功能，支持通过IP地址白名单、User-Agent、URL前缀的方式排除。 |
| 界面展示 | 支持针对业务风险汇总，支持展示业务安全状态分布，包括已失陷业务、正在遭受攻击的业务、存在漏洞但暂时未被攻击的业务。 |
| 支持对业务详情进行展示，包括业务存在关键的风险，可以提供具体的攻击链过程并对攻击进行举证。 |
| 支持针对业务攻击事件汇总，展示攻击事件类型TOP5及当前业务命中的全网实时热点事件。 |

**7、勒索保险与理赔服务**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 保险对象 | 针对已经安装终端防护服务组件并且已配置勒索防护策略的资产。 |
| 勒索风险排查 | 投标方应面向招标方提供定期的勒索病毒入侵风险专项排查，投标方应按照勒索预防Checklist开展勒索风险评估，勒索预防Checklist应当包含勒索高危利用漏洞、端口、安全策略、攻击行为、勒索残留隐患几个纬度。 |
| 投标方定期按照勒索预防Checklist开展勒索风险评估后应当每季度一次向招标方提供《勒索病毒风险排查报告》，包括中应包含全面的勒索风险分析和隐患加固处置的情况，并且投标方有义务按招标方要求进行远程或现场的成果汇报。 |
| 勒索风险排查工具 | 服务平台应支持面向招标方按照勒索预防Checklist的一键风险排查，支持纬度至少包含弱密码扫描、勒索高危利用漏洞扫描、高危利用端口扫描、勒索风险策略检查、勒索行为监测，并且投标方可按照招标方要求设置定时勒索风险排查任务。 |
| 保险金额 | 在服务期间内，当服务资产遭受勒索时，针对最终用户为消除勒索事件影响或减少勒索事件损失所支出的赎金费用，视情况予以赔偿，累计赔偿限额不超过100W，具体赔偿条件、赔偿范围及资产对象以双方正式签署的协议为准 |

**8、高级安全与应急服务**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 内网安全评估服务 | 通过安全扫描、渗透测试等方式全方位检测网络中存在的脆弱性，发现信息系统存在的安全漏洞、安全配置问题、应用系统安全漏洞，检查系统存在的弱口令等等，形成整体安全风险报告，并对安全隐患提出合理的加固建议。 |
| 内网安全加固服务 | 依据安全检查和评估的各项报告，针对信息系统的网络设备存在的重要安全隐患给出相应的安全加固建议。协助我院通过补丁更新、修补漏洞、安全配置增强、系统架构和安全策略调整等措施进行安全加固，帮助提升系统的安全性和抗攻击能力。 |
| 网络安全培训服务 | 根据医院需要协助医院信息中心开展全院的网络安全培训和考试服务。 |
| 应急演练服务和应急响应服务 | 选取内网一个核心业务系统，提供全方位的应急演练场景模拟策划、方案编制和组织实施。并在当安全威胁事件发生后迅速采取的措施和行动，最快速恢复系统的保密性、完整性和可用性。 |

**9、扩展检测与响应服务**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 产品形态 | 平台SAAS化形态，无需要在数据中心进行任何下载和安装，通过账号密码在云端获取服务。 |
| 快捷入口 | 支持快捷入口配置，对关心的模块可标星置顶。实现自定义入口设定。 |
| 监控大屏 | 支持不同安全视角展示4个独立的大屏展示功能 ，包括全网安全能力监控大屏、安全运维大屏、告警态势大屏、资产态势大屏等，支持配置大屏统计周期。 |
| 全网安全能力监控大屏支持展示网端数据源展示，并支持跳转相关日志检索页面。可直观展示日志到告警，告警到事件的消减比例。 |
| 可视化中心 | 支持自定义可视化组件，包括柱形图、水平条形图、趋势图、饼图、表格、指标、Markdown形式。 |
| 支持自定义仪表盘，可圈定资产范围，内置安全告警视图、资产视图、脆弱性风险视图、风险资产视图等模板，展示图表样例包括条形图、水平条形图、趋势图、饼图、表格、指标、Markdown等，可编辑背景及标题样式，可全局预览。 |
| 支持自定义报告生成，包括时间、报告组件、可视化模块、图标设置及文字编辑，可上传自定义页眉和自动化目录生成，支持预览和导出。 |
| 云端威胁狩猎XTH | 支持云端专家提供轻量安全服务，进行持续的威胁狩猎，发现潜在威胁；在有攻击事件生成后，进行二次确认，通过Threat Hunting标签进行辨别，对热门威胁进行响应； |
| 安全事件 | 支持对事件等级、事件来源、事件定性、威胁标签、数据源、处置状态等进行快速筛选，并提供简易模式和专家模式两种调查方式，简易模式可基于字段名称进行选取组合统一检索、专家模式采用SPL语句检索。支持保存检索条件。 |
| 支持通过安全事件详情查看攻击故事线。安全事件按照攻击入口和进程树的视角进行安全分析。可详细点开进程链中任意进程查看进程详情，包括基础信息、威胁告警、网络连接行为、文件行为、域名访问行为、模块加载行为，并且自带解码工具。 |
| 支持对安全事件推送处置和响应建议，响应建议包括原理介绍、危害影响、处置建议。通过建议描述、业务影响标签和安全效果标签清晰明确指导下一步响应动作，可一键封禁IP、隔离主机等。支持在线实时聊天框或离线留言咨询攻防专家，获取云端专家支持。 |
| 支持一键遏制功能，可联动网端防护设备使用端网能力一键处置关键实体，实现外部威胁不入内网，关键数据不出内网，保证内网安全。 |
| 风险主机分析 | 支持风险资产总览，对包括影响资产、风险等级、威胁标签、资产类型、事件数、漏洞/弱密码攻击面情况、最近检测时间等进行展示。可自定义编辑风险资产统计图。可通过风险等级、标签、重要级别、资产类型、数据源对资产进行筛选。可导出风险资产列表。 |
| 告警智能定性 | 支持告警智能定性分析，通过分析告警的上下文关联、时序关系、历史告警发生的频率规律性，结合威胁情报与安全专家经验对当前的安全告警进行目的性确认、从而确认安全告警的优先级顺序，帮助安全人员高效的完成攻击告警的运营工作。 |
| 资产详情 | 支持展示资产基础信息、关联IP、操作系统、设备信息、地理位置、资产责任人。 |
| 资产清点 | 支持通过开放端口、应用软件、数据库、web服务、web框架、web应用、web站点、账号信息、运行进程、运行服务、启动项、计划任务、注册表维度进行资产清点。清点可展示相关资产列表及资产责任人、数据源。 |
| 资产体检 | 根据资产的维度呈现安全事件、安全告警、攻击面风险等多角度呈现问题，结合ATT&CK矩阵更好发现风险资产已知威胁和潜在风险。 |
| 封禁地址 | 支持配置规则可按IP/域名/url联动防火墙设备进行封堵，封禁时长可按天/时/分细粒度进行设置。可对封禁对象进行删除、解封、再次封禁等操作 |
| 阻断进程记录 | 支持阻断进程记录的展示，包括匹配条件、参数、所属资产、关联告警、关联事件等。并支持检索。 |
| 拦截域名 | 支持拦截域名功能，联动EDR/CWPP进行拦截域名，在拦截域名界面可查看拦截域名信息，并且支持取消拦截。 |
| 微信推送 | 支持绑定微信公众号，自定义推送内容包括安全事件和热点漏洞事件，有效延缓威胁扩散。 |
| 自定义告警规则 | 支持自定义告警规则，基础信息包括规则名称、确定性级别、告警级别、适用系统、ATT&CK、规则描述等。规则定义支持进程创建、文件创建、域名访问、网络连接等。 |
| 支持新增规则，删除、启用、禁用、编辑已生成的规则。并可以通过生效状态、规则类型、确定性级别、告警级别、名称/规则ID等快速检索自定义的规则。 |
| 角色管理 | 支持角色创建和角色分配，内置包括安全管理员、超级管理员、审计管理员、系统管理员角色，可新建角色及配置相关编辑和查看权限。可对账号和角色进行关联，一个账号可以关联多种权限。 |
| 二次鉴权 | 针对外部威胁防止规模化的数据丢失、泄露、设备被控制，支持账号二次鉴权、设备管理二次鉴权、弱密码二次鉴权 |
| 全局智能调查 | 支持智能调查功能，通过对威胁情报以及威胁实体IP、域名、MD5的检索，自动进行统计分析，提供全局威胁狩猎，进行快速调查溯源。 |

**10、下一代防火墙**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 性能要求 | 网络层吞吐量≥15Gbps，应用层吞吐量≥8Gbps，并发连接数≥200万，HTTP新建连接数≥9万。 |
| 硬件配置 | 内存≥8G，硬盘≥128 G SSD，接口≥8个千兆电口+2万兆光口。 |
| 基础网络特性 | 支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。 |
| 支持链路连通性检查功能，支持基于3种以上协议对链路连通性进行探测，探测协议至少包括DNS解析、ARP探测、PING和BFD等方式。 |
| 产品支持IPSec VPN智能选路功能，根据线路质量和应用实现自动链路切换。 |
| 支持NAT44、NAT64、NAT66地址转换方式，支持IPv4/IPv6双栈工作模式，以适应IPv6发展趋势。 |
| 访问控制 | 支持不少于9000种应用的识别和控制，对包括游戏、购物、图书百科、工作招聘、P2P、社交网络、旅游出行、金融交易等类型应用进行检测与控制 |
| 支持基于地区维度设置流控策略，实现多区域流量批量快速管控功能 |
| 安全防护 | 产品支持勒索病毒检测与防御功能，针对勒索病毒攻击设置专项安全策略 |
| 产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过128万种，可识别主机的异常外联行为 |
| 支持用户账号安全保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生 |
| 支持CC攻击防护功能 |
| 产品支持管控非法、违规网站的访问行为，具备海量的URL分类库。 |
| 入侵防御 | 产品内置不低于10000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则。 |
| 支持僵尸主机检测功能，产品内置僵尸网络特征库超过130万种，可识别主机的异常外联行为。 |
| 联动能力 | 产品支持主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危IP |
| 策略管理 | 产品支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议。 |
| 产品支持策略生命周期管理功能，记录安全策略变更时间、变更账号、变更类型等内容，提升日常安全策略运维管理效率。 |
| 产品支持管理员双因子认证，可以通过用户密码和Key等不同方式登陆产品管理界面 |

**11、上网行为管理**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 硬件配置 | 规格2U，内存≥8 GB，硬盘≥128GB SSD+960GB SSD，冗余电源，接口≥6个千兆电口+2个万兆光口 |
| 性能指标 | 网络层吞吐量≥10Gbps，应用层吞吐量≥1.5Gbps，支持用户数≥6000，包转发率≥132Kpps，每秒新建连接数≥14000，最大并发连接数≥600000 |
| 基础功能 | 为适应ipv6的发展趋势，支持部署在IPv6环境中，设备接口及部署模式均支持ipv6配置，所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持IPv6 |
| 支持首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行 |
| 针对内网用户的Web访问质量进行检测，对整体网络提供清晰的整体网络质量评级，同时支持以列表形式展示访问质量差的用户名单，对单用户进行定向Web访问质量检测 |
| 支持针对特权用户配置免认证key和特权key，特权免key支持免审计和免控制 |
| 终端管理 | 支持图形化查看当前内网IP使用情况，帮助管理员减少人工维护IP表的工作量 |
| 支持对网络接入的终端进行可视化管理，支持查看终端类型分布，以及终端详细信息（IP、MAC、厂商、操作系统、开放端口等） |
| 行为管理 | 内置海量预分类的URL地址库，能够针对各种URL类型做识别和分类，同时所有URL类型都支持区分“网站浏览”、“文件上传”、“其他上传”、“HTTPS”等细分行为并分别做权限控制 |
| 设备内置应用识别规则库，支持超过9000条应用规则数、支持超过6000种以上的应用；支持根据标签选择应用，并支持给每个应用自定义标签；支持根据标签选择一类应用做控制 |
| 对SaaS应用有默认分类标签，帮助客户统一配置策略，支持超过200种主流网络会议/办公OA/教育学习应用 |
| 能够对teamview、QQ远程桌面等远程控制应用做细分控制，如：接受对方远程控制 |
| 支持对移动应用的细分权限控制，微信：微信网页版、微信传文件、微信朋友圈、微信游戏，QQ：QQ传文件、QQ视频语音等 |
| 支持代理控制，不允许使用外部HTTP代理，不允许使用外部Sock4/5代理以及不允许在HTTP，SSL一些的标准端口上使用其他协议 |
| 流量管理 | 支持基于用户组、位置、终端类型、URL类型配置流量管控策略 |
| 支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率，空闲值可自定义 |
| 支持通过抑制P2P的下行丢包，来减缓P2P的下行流量，从而解决网络出口在做流控后仍然压力较大的问题 |
| 支持把每一个外网IP作为通道内的用户，使得通道的用户间公平分配带宽，以及单用户最高带宽属性对外网IP有效 |
| 基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中 |

**三、服务要求**

1.工期：30天。

2.服务内容和要求：

（1）服务期：一年（从安全服务产品投放部署到位验收之日起计）。服务期满后，服务期间投放的相关安全设备必须承诺免费延用半年，以确保采购人安全服务交接期的基本网络安全和日常工作更好地延续。

投标人需指定一名主要联系人及两名替补联系人与采购人联系。一旦接到采购人请求电话，投标人的技术人员将在规定时间内通过远程解决或上门服务。若投标人指定工程师如果因特殊原因离职或更换电话，及时通知采购人，并指定合格的接替人员。

（2）投标人须有良好的售后服务能力，设有售后服务机构和设施，并配备受过专业培训的售后服务人员，能够保证售后的速度和质量，维修工程师为制造商或销售商在职人员。提供全年7天24小时服务（电话、远程或现场），响应时间：30分钟内电话响应，4小时内到达现场。

（3）驻点巡访：每周服务工程师需到客户巡更系统打卡，驻点一天，完成安全日志分析、设备运营情况、问题处置及其巡检报告；

每月需做好巡检以及巡更系统打卡；

每月销售管理负责人及其以上2个工程师需要召开月度会议，总结一月安全汇总工作；

重要时期驻点服务：重要时期如两会、亚运会等重大日期需要驻点现场。

（4）遇到安全事情处置（不限次数）：

对于关键性问题（影响采购人业务正常运作的故障）

响应时间：1～20分钟；

到场时间：工作时间半小时内到达现场；节假日以及休息时间1小时到达现场；

修复时间：3小时内修复。

对于一般问题（不影响采购人业务正常运作的故障）

响应时间：1～20分钟；

到场时间：1小时内到达现场；

修复时间：8小时内修复。

1. 培训：免费为采购人院内管理人员、技术人员、使用人员提供培训。投标人将详细的培训课程以及时间表交给采购人，最后以采购人认可为准。
2. **完成网络安全相关的全资产梳理工作。**
3. **制定完善的网络安全制度、网络安全闭环管理流程、月度网络安全评价体系。**
4. 其他要求：承诺确保采购人的网络安全达到《网络安全等级保护2.0》测评标准。

**四、付款方式**

1.服务期满半年且未发生重大安全问题支付合同金额的50%，服务期满且未发生重大安全问题并提交采购人验收签字确认的维护报告后支付剩余金额。

2.投标人须提供正式的税务发票并凭税务发票付款。

3.一年服务期满后，甲乙双方无异议可续签1~2年合同，续签期间服务费用及服务内容不变，合同每年一签。