入侵防御系统及主机安全软件项目

一、**基本要求**

1、名称：入侵防御系统及主机安全软件

2、数量：1套

3、货期：签订合同一个月内

**二、主要技术要求（达到或优于）**

**入侵防御系统**

|  |
| --- |
| **技术参数要求要求** |
| 1.▲配置标准国产化硬件平台，国产化操作系统,1U标准机架式上架设备，配置单电源，内存≥16G，32G+128G SSD硬盘存储,配置≥6个千兆电接口（接口支持bypass），≥2个千兆光接口，≥2个网络扩展插槽(可额外扩展千兆电口/光口、万兆光口)，≥2个USB口；提供三年入侵防御特征库、三年原厂标准硬件维保服务。 |
| 2.▲在开启入侵防御安全防护规则下，IPS吞吐率≥30G，最大并发连接数≥500万；每秒新建HTTP连接数≥5万。 |
| 3.支持网线模式部署和透明多口桥部署 |
| 4.支持端口聚合包括手动端口聚合模式和LACP聚合模式 |
| 5.▲支持内置专业的入侵防御特征库，覆盖勒索、挖矿、webshell、僵尸网络、木马后门、蠕虫、信息泄漏、权限绕过、未授权访问、文件上传、文件读取、文件下载、文件包含、SSRF、XXE、CSRF、反序列化、代码执行、命令执行、XSS攻击、SQL注入、DOS等攻击类型，入侵防御特征数量在14000条以上；提供带有CMA、ilac-MRA、CNAS标志的检测报告，报告中必须体现该条测试内容用于证明功能有效性； |
| 6.▲支持多种规则变更部署模式，至少包括自动防御模式、试运行模式和手动防御模式，提供带有CMA、ilac-MRA、CNAS标志的检测报告，报告中必须体现该条测试内容用于证明功能有效性； |
| 7.规则详情应至少包含影响系统、影响服务、影响应用、事件处理流程和判定，并支持攻击阶段、攻击结果、精确度、ATT&CK编号及概述措施 |
| 8.▲支持双向检测功能，根据双向流量检测攻击，输出检测结果包含正在利用、攻击成功，应支持HTTP请求/响应缓存（提供产品功能截图） |
| 9.支持代理环境部署，支持通过Tcp-Options和X-Forwarded-For提取源  |
| 10.支持规则响应动作应支持阻断、重置和通过和返回错误页面，返回错误页面应支持自定义重定向url和自定义页面 |
| 11.支持规则响应动作应支持标记设备信息，重置报文携带设备信息 |
| 12.▲支持SQL注入防护和XSS攻击防护，检测点至少支持URL、Cookie、Reference、Form、User-Agent、X-Forwarded-For，内置AI检测模型，利用机器学习技术对SQL注入报文进行分析，检测和识别SQL注入行为（提供产品功能截图） |
| 13.支持多种防web扫描能力，防止攻击者通过扫描发现Web网站中的缺陷从而发起精确攻击，至少包括如下能力：防爬虫、防止CGI和漏洞扫描等，并支持阻断扫描行为和并记录日志，系统支持设置至少4个级别的扫描容忍度/扫描敏感度，方便安全管理者采用不同安全级别的行为控制。 |
| 14.▲支持HTTP协议自适应解码、URL解码、UTF7解码、base64解码、XML解码、Unicode解码、十六进制转换、CHR解码、UTF-7解码，支持解析7层以上混合编解码能力，可实现对多层编码攻击的检测，支持格式文本解析JSON解析、html解析、multipart解析（提供产品功能截图） |
| 15.支持内置智能分析能力，具备阻断的活动专项分析和综合威胁告警分析，其中阻断的活动应包括阻断的威胁、阻断的文件和阻断的IP专项分析 |
| 16.▲支持策略调优，分析日志自动关联配置可一键修订规则动作和模板响应方式，具备详细的策略调优记录包含操作时间、操作模块、操作对象、动作、调优结果等，提供带有CMA、ilac-MRA、CNAS标志的检测报告，报告中必须体现该条测试内容用于证明功能有效性 |
| 17.支持告警标识，包含确认攻击、误报、忽略操作，具备详细的标识记录包含标识时间、状态等 |
| 18.支持告警处置，包含一键加白和临时封禁，并具备详细的处置记录包含处置时间、处置方式、处置动作等 |
| 19.支持攻击日志展示自动聚合，聚合条件包含源、目的IP+威胁名称、目的IP+威胁名称、威胁名称，系统应支持攻击源目地址归属地显示，日志信息应包含威胁级别、攻击阶段、攻击结果、标识状态、处置状态展示，应支持存储攻击日志网络负载，其中WEB攻击应支持存储HTTP头 |
| 20.▲支持设备监控指标，至少包含CPU利用率,内存利用率,硬盘利用率,CPU温度,主机温度,系统连接数,授权有效性,HA主备切换,磁盘利用率,电源温度,日志存储量,风扇转速,接口等。设备监控告警条件应支持持续时间、阈值配置、告警频率，告警方式支持邮件告警和推送到本地消息中心。设备巡检包括硬件巡检、运行状态巡检、安全配置巡检、升级版本巡检、网络巡检、日志巡检等，巡检报告支持邮件与飞书群通知（提供产品功能截图） |
| 21.支持安全状态展示不少于20种维度，至少包括攻击类型和阶段分布展示、攻击者区域展示、威胁级别趋势、弱口令账号TOP、弱口令协议分布、、弱口令风险源 TOP、暴力破解主机TOP、被暴破成功主机TOP、暴破源 TOP、攻击者区域分布、恶意文件传播通道、恶意文件威胁类型 TOP等，支持定义展示界面添加和删除控件 |
| 22.支持系统运行情况监控不少于10种维度，至少包括BYPASS状态、CPU内存使用率、硬件状态、关键服务状态、授权状态、接口信息、设备流量趋势、最近登录信息、公告板等 |
| 23.▲产品需符合GB 42250-2022《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准的强制性要求，提供有效证明材料。 |
| 24.产品需具备由中国信息安全测评中心颁发的《信息技术产品安全测评证书》，认证级别为EAL3+或更高级别；提供证书复印件 |
| 25.产品需具备《国家信息安全漏洞库兼容性资质证书》，提供证书复印件 |

**主机安全软件订阅服务工具参数要求**

|  |
| --- |
| 技术要求 |
| 1.▲由服务商提供一套主机安全软件；服务期内需要满足医院服务器数量的并发授权数，服务器内服务商需保障软件安全特征库更新，攻防演练期间策略优化，溯源攻击队的服务器入侵行为 |
| 2.探针支持部署在 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 等国产化操作系统中部署。 |
| 3.探针支持在非 root 权限下运行和正常使用。 |
| 4.支持根据当前系统安全状态对主机及整个系统进行安全评分。 |
| 5.提供可视化大屏，对主机的安全状态进行实时监控。 |
| 6.支持自动清点和梳理主机信息，包含主机名称、主机IP地址、主机状态、操作系统、主机关联威胁事件、主机关联漏洞风险、最近一次发现时间等。可设置主机分组信息和备注信息，按照多维度进行主机信息筛选过滤。 |
| 7.支持清点主机上的进程信息，内容至少包括：进程名，父进程，PID，进程启动参数，进程状态，启动时间，工作目录，启动用户，可执行文件等。 |
| 8.支持自动清点和梳理主机端口和开放进程信息，包含主机名称、主机IP地址、协议、监听地址、端口对应的进程名、进程PID，可对端口进行多维度筛选过滤操作。 |
| 9.自动清点和梳理已经安装探针的主机应用信息，包含主机名称、主机IP地址、应用名称、版本号、路径信息、厂商、CPE信息、应用类型。可对应用进行多维度筛选过滤操作。 |
| 10.支持清点的软件应用类型包括 java 依赖、系统库、系统工具、编译器、解释器、web 服务、web 框架、数据库、消息队列、web 应用、操作系统内核、其他网络服务、第三方工具、虚拟化工具。 |
| 11.支持自动清点和梳理服务器上的系统用户信息，包含主机名称、主机IP地址、用户名称、用户说明、home目录。可对系统用户进行多维度筛选过滤操作。 |
| 12.支持自动清点和梳理主机上运行的web站点信息，包含主机名称、主机IP地址、服务类型、对应端口、端口协议类型、域名、web路径信息。服务类型包含Nginx、Apache、Tomcat，端口协议类型包含http和https 。可对web站点进行多维度筛选过滤操作。 |
| 13.支持清点操作系统启动项信息。 |
| 14.支持清点操作系统的内核模块，驱动等信息。 |
| 15.▲支持自定义资产业务组，对业务组进行多级树形管理。展示业务组名称、业务组下级分组数量、业务组资产数量、业务组风险事件总数信息，可添加、删除、修改业务组信息和调整隶属关系，支持按照多维度筛选过滤业务组信息。 |
| 16.支持检测当前网络中尚未安装探针的未知资产。 |
| 17.基于指纹识别和POC插件方式精准识别资产漏洞信息，兼容CNNVD、CVE、CPE、BID等国内国际规范。漏洞信息包含影响资产信息、漏洞级别、漏洞名称、漏洞类型、利用特征、CVSS分值、CVSS 向量信息、CVE 编号、CNNVD 编号、CNVD 编号、CWE 编号等信息。 |
| 18.▲提供全网漏洞情报。关联全网漏洞利用情报，提供全网漏洞信息搜索、查询、关联能力。展示漏洞信息包含漏洞级别、漏洞名称、利用特征、CVSS分值、CVE 编号、CNNVD 编号、CNVD 编号、CWE 编号、漏洞类型、CVSS 向量信息。提供漏洞情报详细信息的查看和多维度筛选过滤功能。 |
| 19.支持扫描主机上文件权限被恶意篡改的风险。 |
| 20.支持扫描主机上存在的恶意账户。 |
| 21.支持扫描主机上的应用服务存在不安全的配置行为。 |
| 22.支持扫描主机操作系统存在不安全的配置行为。 |
| 23.支持检测 Linux 与 Windows 系统弱口令。24.支持检测 MySQL、PostgreSQL、Redis、Oracle等数据库弱口令。25.支持检测 Tomcat、Jenkins、WebLogic、SVN中间件弱口令。26.支持检测 FTP、Rsync 、OpenLdap网络服务弱口令。27.支持用户自定义用户名和密码字典。 |
| 28.支持根据用户自定义策略对系统关键文件或目录进行监控，并对修改文件的事件进行告警。 |
| 29.▲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。 |
| 30.提供全网补丁情报，支持检测主机未打的安全补丁。 |
| 31.支持对操作系统、应用程序的等级保护、CIS合规基线和重保基线的快速核查与结果报告导出。支持用户自定义合规基线核查项管理与策略管理，能按照企业自身行业属性自定义基线。支持提供合规基线核查项的快速自定义和高级自定义。 |
| 32.支持实时发现服务器上的网页后门文件，展示webshell文件影响的资产信息、资产所在业务组信息、webshell文件路径、影响域名、发现时间、事件状态、事件处理记录以及webshell文件详情信息，给出详细的webshell事件描述和解决方案。支持检测的文件类型包含且不限于 PHP、java、asp、aspx、jsp 、jspx 、class 、war，可查看文件详情信息和下载样本文件进行分析。 |
| 33.支持检测内存型无文件 WebShell。 |
| 34.▲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。 |
| 35.支持实时检测服务器上的反弹shell行为，展示反弹shell事件影响的资产信息、资产所在业务组信息、远程地址和端口信息、发现时间、事件状态、事件处理记录以及进程pid、进程命令、进程路径、进程启动时间等进程详细信息，给出详细的反弹shell事件描述和解决方案。 |
| 36.支持实时监控用户进程行为，识别异常进程事件。检测类型包含存在恶意关键字的进程、外连恶意端口进程、sshd 后门等。 展示异常进程影响的资产信息、资产所在业务组信息、发现时间、事件状态、事件处理记录以及进程pid、进程命令、进程启动时间等进程详细信息。 |
| 37.支持通过自定义或者自学习的方式对主机上的命令操作事件进行白名单设置，并对白名单外的命令操作进行告警上报。 |
| 38.支持检测系统存在的恶意文件，支持检测的恶意文件类型包括但不限于：病毒、木马、蠕虫、钓鱼程序、黑客工具、漏洞利用代码、恶意宏文档等。给出详细的恶意文件事件描述和解决方案，可查看恶意文件类型、文件MD5、文件路径、文件大小等详情信息和下载样本文件进行分析。 |
| 39.支持实时发现暴力破解行为，可检测高频暴破、低频暴破、账号暴破、口令暴破、多源暴破等多种暴力破解行为。展示暴力破解影响的资产信息、资产所在业务组信息、发起攻击的源IP地址、服务类型、发起攻击时间、发现时间、事件状态、事件处理记录等信息。 |
| 40.▲支持部署轻量级蜜罐，对内网存在的扫描行为进行检测，发现黑客扫描行为实时告警，支持自定义配置。 |
| 41，▲支持联动第三方动态蜜罐或高交互蜜罐，构建全局蜜网，有效诱捕黑客攻击行为，并由高交互蜜罐实现溯源反制。 |
| 支持检测本地提权行为。 |
| 42.▲支持检测系统请求非法 DNS 或非法 IP 地址的行为。 |
| 43.实时监控主机上发生的异常登录事件，检测的异常登录事件类型包括异常时间登录、异常IP登录、异常登陆地点、异常用户名登录四种，支持用户自定义配置登录时间、登录IP、登陆地点、登录用户名黑白名单。支持展示异常登录事件影响的资产信息、异常登录IP、登陆地点、登录时间、登录用户名、发现时间、事件状态、事件处理记录等信息，同时给出详细的异常登录事件描述和解决方案。 |
| 44.支持对暴力破解行为依据事件不同严重程度进行自动或手动阻断，并能自定义阻断时间。 |
| 45.支持对异常登录行为依据事件不同严重程度进行自动阻断，并能自定义阻断时间。 |
| 46.支持对反弹Shell行为依据事件不同严重程度进行自动或手动阻断，并能自定义阻断时间。 |
| 47.支持对 WebShell 文件实施手动隔离或自动隔离。 |
| 48.支持对病毒文件实施手动隔离或自动隔离，支持多引擎技术识别并查杀最新病毒，包含多种防护等级。 |
| 49.▲支持用户自定义网络层防护规则，限制出入流量。限制协议包含 TCP、UDP、ICMP 等。 |
| 50.▲支持记录所有用户在主机上执行的命令历史。 |
| 51.支持基于 RBAC 的用户管理防止，允许对系统用户的集中管理操作，满足多角色多权限的管理模型。 |
| 52.▲支持基于 Oauth、TOTP 等方式的第三方登录行为。 |
| 53.▲支持对产品关键行为进行除密码以外的多因子认证。 |
| 54.可生成全站攻击趋势、攻击类型分布、资产分布、漏洞风险分布、入侵威胁分布等图表，支持自定义报告模版，具备报告生成、查看、导出等功能。 |
| 55.记录系统自身日志信息，方便进行运维管理。 |
| 56.支持以 Syslog 的方式采集系统基础日志。 |
| 57.可通过 API 使用管理平台的所有功能。 |
| 58.▲提供 SaaS 化的升级中心，支持用户在线升级产品内容。 |
| 59.▲支持通过邮件、syslog、钉钉、企业微信四种方式发送风险事件告警，可设置告警阈值，自定义选择告警内容。 |
| 60.查看已经部署代理的主机状态与探针状态，包含探针状态、探针版本，CPU，内存，运行时长，最近发现时间等。 |
| 61.支持一条命令快速安装代理。 |
| 62.支持通过离线升级包的方式进行管理系统和代理的更新。 |
| 63.所有模块均提供可配置参数，允许用户自定义规则。支持为不同的探针下发不同的策略。 |
| 64.默认情况下探针运行时 CPU 占用不超过 10%，内存占用不超过 200MB |
| 65.▲支持设定探针 CPU 与内存资源使用配额。 |
| 66.▲产品具备主机型入侵检测产品（增强级）销售许可证 |
| 67.产品具备主机型入侵检测产品CCRC证书 |
| 68.产品具备国家信息安全漏洞库兼容性资质证书 |
| 69.产品具备中标麒麟兼容性认证、银河麒麟兼容性认证、鲲鹏云兼容性认证、统信兼容性认证、海光兼容性认证、泰山服务器兼容性认证、鲲鹏920兼容性认证证书、中科方德兼容性认证、飞腾兼容性认证 |
| 70.产品具备IPV6兼容性认证 |

**三、商务要求**

1、中标人必须按项目进度安排计划，派出适当的技术人员到安装现场负责免费安装和调试工作。在安装施工期间，严格遵守用户方的有关规定。

2、安装验收期间，在招标人所在地对招标人进行仪器操作、日常维护、所有检测指标的现场培训，2年内须提供不少于每年1次的上门免费培训服务。培训所需全部费用均已包含在投标报价中。

3、中标人应将关键主机设备的用户手册、保修手册、有关单证资料及配备件、随机工具等交付给采购人，使用操作及安全须知等重要资料应附有中文说明。

4、招标人按照采购合同规定的技术、服务、安全标准组织对中标人履约情况进行验收，并出具验收书。验收书应当包括每一项技术、服务、安全标准的履约情况。

5、交付验收标准依次序对照适用标准为：①符合中华人民共和国“国家安全质量标准、环保标准或行业标准；”②符合招标文件和响应承诺中招标人认可的合理最佳配置、参数及各项要求；③货物来源国官方标准。货物为原厂商未启封全新包装，具出厂合格证，序列号、包装箱号与出厂批号一致，并可追溯查阅。所有随设备的附件必须齐全。

6、中标人将货物的用户手册、保修手册、有关单证资料及备品备件、随机工具等交付给招标人，使用操作及安全须知等重要资料应附有中文说明。货物验收所发生的检验费用由中标人负担。

8、中标人负责设备的供货、安装调试、验收，经招标人验收合格方可。质量保证期不少于 2 年，自招标人和中标人代表在货物安装调试验收后的验收书上签字之日起计算。“技术要求”中另有要求的，以其中的要求为准。质保期内由原设备生产厂家授权的总代理或者原设备生产厂家对所供货物实行包修、包换、包退、包维护保养，质保期后设备维修配件更换只收取成本费用。须提供由原设备生产厂家授权的总代理或者原设备生产厂家针对本项目出具的售后服务承诺书。

9、对招标人的服务通知，中标人在接报后 24 小时内响应， 48 小时内到达现场， 72 小时内处理完毕。若在 72 小时内仍未能有效解决，则自取走故障件之日起，3个工作日内提供备品以保证业务正常开展，若无法按时修复或如期提供备品造成停机，则按1:7延长保修期(即停机1天，延长保修期7天，如停用时间累计超过60天则保修期重新计算。)，若完全不能修复则由中标人免费更换同款整机。