# 技术参数要求：

## 1、安全感知管理平台

| **技术指标** | **指标参数** |
| --- | --- |
| 硬件要求 | 规格不低于2U，内存≧3\*32GB DDR4 2933，系统盘≧1\*240GB SATA SSD，数据盘≧6\*4TB，标配盘位数≧8，电源需为白金，冗余电源，接口不少于4千兆电口和4个万兆光口； |
| 性能要求 | 带宽性能1Gbps时存储时长≧900天/1Gbps。 |
| 大屏可视 | ★支持安全态势的可视化呈现，以大屏的方式从全网安全态势感知大屏、分支安全态势、安全事件态势、通报/工单预警态势、全网攻击、资产态势、网络安全指挥调度安全态势、设备运行态势、外联风险态势大屏等提供不少于9块大屏展示界面，支持大屏轮播及大屏顺序设置和大屏名称等。**（需提供产品功能截图证明）** |
| 支持大屏展示业务脆弱性态势，包括漏洞风险态势、漏洞类型TOP5、高危漏洞TOP5、业务总览、脆弱性业务TOP5、实时脆弱性监测。 |
| ★支持对安全事件、外部攻击者等维度进行自定义设置实现实时告警展示，支持大屏轮播，可在一个屏幕上自动切换轮播不同的大屏，所有大屏可自定义播放顺序。**（需提供CMA或CNAS认证的第三方权威测评机构的检测报告扫描件作为证明材料）** |
| 重保中心 | ★支持自动化溯源，可自动化复现受害者从最开始的遭受攻击到权限维持各个阶段的黑客行为，包括攻击入口溯源。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的威胁影响面，同时基于列表模式展示攻击、违规访问、风险访问、可疑行为、正常访问等详细信息。支持攻击溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息。**（需提供产品功能截图证明）** |
| 资产管理 | 支持自动识别业务/服务器资产，可定义IP地址、所属分支、主机名、责任人、责任人邮箱、所属业务、操作系统、服务与端口；并支持基于流量自动识别操作系统、开放的服务与端口。 |
| 支持自动识别终端资产，可定义终端/IP组、主机名、用户名、用户邮箱。 |
| 支持通过主动发送微量包的扫描方式探测潜在的服务器（影子资产）以及学习服务器的基础信息，资产指纹信息包括资产类型、端口、操作系统、mac地址、主机名等。 |
| ★支持自定义分支管理权限，分支管理员具备独立的管理页面，只能管理和查看所属分支的业务和终端资产的安全信息且具备完整的功能展示。**（需提供CMA或CNAS认证的第三方权威测评机构的检测报告扫描件作为证明材料）** |
| ★支持跨三层取mac地址，识别资产mac地址，并能够解决不同资产IP冲突问题，以及DHCP场景IP变更的问题。**（需提供产品功能截图证明）** |
| 脆弱性管理 | 支持业务脆弱性风险分布展示，包括不同严重级别业务分布，漏洞类型分布，漏洞整体态势。 |
| 弱密码检测技术基于机器学习（无监督自我学习）提取登录成功的特征，通过机器学习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，包括响应体内容Json、响应体关键字Keyword、响应体MD5值、响应体长度Length、登录跳转路径Location，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、txt文件格式导入。 |
| 支持流量实时识别漏洞分析，漏洞分析类型包含配置错误漏洞、OpenSSH漏洞、OpenLDAP等操作系统、数据库、Web应用等 ，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。 |
| 威胁检测 | 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。 |
| 支持挖矿病毒告警检测，可以检测出挖矿病毒感染事件。 |
| ★平台内置挖矿安全知识库，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、ZombieBoy挖矿木马等提供详细的介绍和分析等信息。**（需提供产品功能截图证明）** |
| 支持安全检测日志、审计日志、第三方日志存储；日志类型包括漏洞利用攻击、网站攻击、僵尸网络、业务弱点、DOS攻击、邮件安全、文件安全、网络流量、DNS、HTTP、用户、数据库、文件审计、POP3、SMTP、IMAP、LDAP、FTP、Telnet。 |
| 处置中心 | 支持多维度模糊聚类算法将大量外部攻击日志聚合成少量攻击事件，聚合维度包括攻击IP、攻击地址、攻击目标和目标手法。 |
| 报表中心 | 可快速生成月度、季度、年度PPT报表，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等，帮助用户高效汇报，体现安全工作价值。 |
| 告警方式支持邮件告警、短信、微信告警方式。 |
| 设备管理 | 支持流量探针统一升级管理，支持监控流量探针与安全组件的运行状态，包含日志传输模式、日志传输量、最近同步信息。 |
| 支持管理员账号的新增、删除、启用、禁用，支持免登陆及单点登录设置，支持可信IP设置。支持角色的管理范围及页面权限的收敛设置。支持系统管理员、安全保密管理员和安全审计员三个管理员角色。 |
| ★安全白名单支持安全告警白名单和脆弱性检测白名单新增、启用、禁用、还支持设置生效设备和时间，并支持导入导出白名单等操作。安全白名单可多选或全选威胁类型。**（需提供产品功能截图证明）** |
| 资质要求 | ★为确保安全感知管理平台自身的安全性，要求所投产品的生产厂商具备软件安全开发服务资质，且符合中国网络安全审查技术与认证中心（CCRC)颁发的《信息安全服务规范》一级服务资质要求**（需提供相关证明材料）** |
| ★为了确保安全感知管理平台的安全能力，要求所投产品具备国家IT产品信息安全产品认证证书**（需提供相关证明材料）** |

## 2、潜伏威胁探针1型

| **技术指标** | **指标参数** |
| --- | --- |
| 参数要求 | 设备需为万兆级平台，规格不低于2U，网络层吞吐≧3Gbps，内存大小≧8G，硬盘容量≧480G SSD，电源需为冗余电源，接口不少于6千兆电口、4千兆光口和2万兆光口SFP+； |
| 部署模式 | 旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响。 |
| 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。 |
| 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；具备多种的入侵攻击模式或恶意UR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。 |
| 网站攻击检测 | ★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整站系统漏洞网站攻击检测。**（需提供产品功能截图证明）** |
| 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、Scan漏洞攻击、System漏洞攻击、Telnet漏洞攻击、Tftp漏洞攻击、Web漏洞攻击的检测。**（需提供产品功能截图证明）** |
| 支持Application漏洞攻击、File漏洞攻击、Scan漏洞攻击、Shellcode漏洞攻击、System漏洞利用攻击、Web Activex客户端漏洞攻击检测。 |
| 支持FTP、IMAP、MS Sql、Mysql、Oracle、POP3、RDP、SMTP、SSH、Telnet、VNC协议暴力破解检测。 |
| 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。**（需提供产品功能截图证明）** |
| 支持ICMP、UDP、SYN、DNS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通信僵尸网络行为检测。 |
| 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，命名方式可多样化，但需要能适应不同应用场景需求。**（需提供产品功能截图证明）** |
| 支持传输协议审计日志，包括https协议日志、http协议审计日志、DNS协议审计日志、邮件协议审计日志、SMB协议审计日志、AD域协议审计日志、WEB登录审计日志、FTP协议审计日志、Telnet协议审计日志、ICMP协议审计日志、LLMNR协议审计日志。 |
| 抓包分析 | ★支持流量抓包分析，基于五元组灵活抓取数据包，可定义配置源IP、源端口、目的IP和目的端口、传输层协议以及标签类型（vlan、vxlan、mpls）选择添加抓包任务，接口额外提供标签选项，帮助安全工程师高效分析威胁。**（需提供产品功能截图证明）** |
| 管理功能 | 支持设备内置简单命令行管理窗口，便于基础运维调试；  可实时监控设备的CPU、内存、存储空间使用情况；  能够监控监听接口的实时流量情况。 |
| 资质要求 | ★为保障潜伏威胁探针产品自身的安全能力，要求所投产品的生产厂商是国家信息安全漏洞共享平台CNVD技术组和用户组成员。**（需提供相关证明材料）** |

## 3、潜伏威胁探针2型

| **技术指标** | **指标参数** |
| --- | --- |
| 参数要求 | 设备需为千兆级平台，规格不低于1U，网络层吞吐≧1.5Gbps。内存大小≧8G，硬盘容量≧256GB SSD，电源需为单电源，接口不少于6千兆电口和2千兆光口SFP。 |
| 部署模式 | 旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响。 |
| 内网资产 | 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。 |
| 违规访问 | 1.检测内网主机的访问情况是否符合规定，需要人工事先进行梳理好访问关系再进行配置。策略从上到下进行匹配，可以通过右侧置顶功能对策略优先级进行调节。  2.支持IP，IP组，服务，端口，访问时间等定义访问策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单和黑名单方式 |
| WEB智能检测 | ★支持命令注入检测、PHP代码检测、XSS攻击检测、Webshell上传检测、SQL注入检测、XXE攻击检测、JAVA代码检测、SQL非注入型检测、MYSQL解析增强、php反序列化检测等，并可自定义配置不同模式。**（需提供产品功能截图证明）** |
| 弱口令检测 | 支持多种类型弱口令策略可选；支持自定义FTP弱口令检测、口令暴力破解检测不同格式和爆破次数，规则设置如空口令、用户名和密码相同、长度、弱口令列表等。 |
| 漏洞利用攻击检测 | ★支持FTP、IMAP、MS Sql、Mysql、Oracle、POP3、RDP、Sip 、Redis 、Ldap 、Nntp 、Openssl 、SMTP、SSH、Telnet、Tomcat、Sybase、Xmpp 、Zabbix 、Weblogic 、Wordpress 、VNC等70种协议暴力破解检测  **（需提供产品功能截图证明）** |
| 安全策略 | 支持检测出网络中的网络拓扑设备进行绘制，更多直观可视化查看网络整体情况。  支持通过白流量过滤的方式，过滤安全网站访问，提升性能。 |
| 旁路阻断 | ★支持基于IP和域名的旁路阻断，能够在实时镜像的流量中发现恶意IP并实现实时阻断，支持24小时/7天/30或者自定义时间在5分钟内阻断威胁。**（需提供产品功能截图证明）** |
| 高级检测 | 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 |
| 特征库 | ★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**（需提供产品功能截图证明）** |
| 抓包分析 | 支持流量抓包分析，基于五元组灵活抓取数据包，可定义配置源IP、源端口、目的IP和目的端口、传输层协议以及标签类型（vlan、vxlan、mpls）选择添加抓包任务，接口额外提供标签选项，帮助安全工程师高效分析威胁。 |
| 探针管理能力 | 支持设备内置简单命令行管理窗口，便于基础运维调试 |
| 资质要求 | ★为保障用户业务能够稳定连续运行，要求所投潜伏威胁探针产品的生产厂商应是国家互联网应急响应中心网络安全应急服务国家级支撑单位**（需提供相关证明材料）** |

# 技术能力及其他要求

1、所投产品包含三年硬件质保，三年特征库升级及软件升级。中标单位提供三年售后服务（提供7\*24小时技术服务热线，提供5\*8小时现场技术支持服务；提供以下故障保修服务：半小时内电话响应，1小时内到达现场，2个工作日内解决问题。）

2、在实施现场应对使用单位进行不少于8小时的专业技术培训；

3、为了保障用户权益，中标后提供原厂质保承诺函，并加盖厂商公章。

4、所投产品需完全满足上述技术参数要求。上述要求中涉及的证书复印件及其它证明材料，中标人须在竞价结束48小时内携带加盖厂商公章的书面材料至甲方现场，参加甲方组织的全面、严格的验收测试，验收测试不通过或资料不全、虚假应标、弄虚作假，将严格按照《税务采购网供应商管理办法》相关条款进行处理（作废标处理并列入黑名单）。

5、供货及实施要求：必须在合同生效之日起20工作日内完成全部软、硬件产品到货，并在到货之日起10日内完成设备的集成安装、调试工作。

6、备注：上表中标注“★”的参数为重要参数，不允许负偏离，发生负偏离将做废标处理并承担相应责任。