# 第一部分 投标邀请函

* 1. 项目内容及要求：（采购项目技术规格、参数及要求，需要落实的采购政策）

|  |  |  |
| --- | --- | --- |
| **项目名称** | **采购内容** | **数量** |
| 广东南方新媒体股份有限公司2023年主机安全防护系统扩容项目 | 主机安全防护系统 | 422套 |

# 第二部分 招标需求部分

**一、项目概述**

随着《网络安全法》、《数据安全法》及《关键信息基础设施安全保护条例》等法律法规的相继出台，网络安全被提升到了战略高度，重要性不言而喻。因此，公司各业务运营平台，特别是业务平台侧急需在技术手段上加以升级，以应对网络空间安全严峻挑战，保障信息基础设施安全稳定运行。

**二、招标产品清单**

|  |  |  |
| --- | --- | --- |
| **产品名称** | **指标** | **数量** |
| 主机安全防护系统 | 含系统软件，3年威胁情报更新授权与规则升级，3年维保升级服务。 | 422套 |

1. **技术参数**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **招标要求** |
| 1 | 操作系统兼容性客户端 | Windows Server 2003 sp2/R2 x86/x64  Windows Server 2008 sp1及以上/R2 x86/x64  Windows Server 2012~2019 sp1及以上/R2 x86/x64  CentOs 5.0及以上 x86/x64  RHEL 5.5及以上 x86/x64  Ubuntu 14.04及以上 x86/x64  SUSE 11及以上版本 x86/x64  Kylin Linux 4.18.0-147  Deepin-4.19.0-arm64-server\_1707/1813 |
| 2 | 产品安全机制 | 支持自我防护技术，即使客户端被意外关闭，防护依然有效（提供产品界面截图并加盖原厂公章）。 |
| 3 | 资产管理 | 支持全量资产的关键字及语法搜索，支持检索的语法包括但不限于：服务器资产类、进程资产类、账号资产类、软件应用类、web资产类、web服务类、web框架、数据库类、端口资产类、网络连接类、启动服务类、安装包类、计划任务类、环境变量类、内核类、类库资产类、注册表类、证书资产类进行检索（提供产品界面截图并加盖原厂公章）。 |
| 4 | 关键字语法搜索支持至少5个搜索历史的保存，并支持将检索条件保存为快捷搜索项（至少保存20个以上）。 |
| 5 | 支持统一入口查看Windows/Linux系统资产，不应将Windows、Linux系统资产分菜单展示。 |
| 6 | 支持以列表的形式，统一列出Windows/Linux服务器基础信息，并在列表中对服务器的关键软硬件进行统计，包括但不限于：CPU数、CPU核数、分区数、账户数、软件应用数、web站点数、web服务数、web框架数、数据库数、端口数、网络连接数、启动服务数、安装包数、计划任务数、环境变量数、内核模块数、证书数、注册表数、类库数等（提供产品界面截图并加盖原厂公章）。 |
| 7 | 进程资产 | 支持以列表的形式，统一列出Windows/Linux服务器进程资产，并可查看进程的软件包名、运行时间、同步时间、启动参数等信息（提供产品界面截图并加盖原厂公章）。 |
| 8 | 行为管理 | 学习每台服务器的网络外连行为、命令执行行为、文件创建行为，并形成图形化的时间轴行为基线，对于偏离行为以外的动作进行告警。 |
| 9 | 网络连接 | 支持以列表的形式，统一列出Windows/Linux服务器的进程连接资产，并可查看进程名称、协议、IP地址、源端口、目标端口、目标IP、连接状态、同步时间等信息。 |
| 10 | 启动服务 | 支持以列表的形式，统一列出Windows/Linux服务器的启动服务或启动项，并可查看服务名/启动项名、启动状态、服务描述、脚本路径、启动类型、文件公司名、文件MD5等信息（提供产品界面截图并加盖原厂公章）。 |
| 11 | 主机发现 | 可通过自动、手动的任务设置，对局域网内服务器的服务器进行扫描（支持ARP、Ping、Nmap扫描方式，并支持离线分析），并自动获取服务器相关信息，包括MAC地址、设备类型、未知主机IP、操作系统、发现方式、首次发现时间等信息（提供产品界面截图并加盖原厂公章）。 |
| 12 | 微隔离 | 支持服务器防火墙功能，可对服务器定制访问策略，包括允许本地IP/端口访问指定IP/端口、禁止本地IP/端口访问指定IP/端口，并可设置访问放心，并支持TCP、UDP、ICMP等协议。并根据设置的规则进行访问告警（提供产品界面截图并加盖原厂公章）。 |
| 13 | 支持设置端口的暴露控制规则，包括但不限于：禁止/允许外网暴露、禁止/允许内网暴露等策略，并支持例外端口的添加。 |
| 14 | 支持对服务器的进程外连控制进行规则设置，包括但不限于：禁止/允许进程外连外网、禁止/允许进程外连内网，并支持进程白名单和例外进程的设置（提供产品界面截图并加盖原厂公章）。 |
| 15 | 风险发现 | 支持对服务器中复用的相同密码进行检测，可识别出某个密码被哪些服务器、哪个账户、哪个应用、哪个版本进行了复用（提供产品界面截图并加盖原厂公章）。 |
| 16 | 可对服务器杀毒引擎进行综合的设置，支持本地查杀、控制中心查杀的设置与切换，并可对某台服务器的查杀规则进行详细设置。 |
| 17 | 软件漏洞检测 | 可对扫描出的软件漏洞进行标记修复、加白、应用虚拟补丁等操作，并支持漏洞复扫（提供产品界面截图并加盖原厂公章）。 |
| 18 | 威胁监测 | 支持在事件列表的详情中，查看事件的基础信息、检测说明、动态攻击路径信息、资产等信息，并可在详情中以前后翻页的形式连续查看事件。 |
| 19 | 恶意扫描 | 以攻击者视角、受害者视角展示恶意扫描的事件，包括：服务器名称、负责人、所属部门、操作地址、最近发生时间、受害IP、攻击IP等信息，并可将事件加入黑名单或白名单，还可对受害的IP进行防端口扫描、屏蔽扫描器等设置。 |
| 20 | 异常登录 | 支持以违规登录视角对异常登录行为进行监控及告警，并可查看违规登录的账号、来源IP、登录区域、服务器IP、操作系统等信息，并可进行登陆规则策略的设置和告警设置（提供产品界面截图并加盖原厂公章）。 |
| 21 | 支持以可疑登录的视角对可疑登录行为进行监控，包括登录IP、发现时间等信息，并可创建可疑登录的监控规则和例外规则。 |
| 22 | webshell | 支持以多种检测方式（RASP、实时监控、本地扫描、特征规则、沙箱运行、动态脚本沙箱）检测webshell攻击（提供产品界面截图并加盖原厂公章）。 |
| 23 | 支持对内存堆栈调用行为特征的分析，可有效检测冰蝎等常见工具的内存WebShell攻击，可对内存攻击行为告警及处置（提供产品界面截图并加盖原厂公章） |
| 24 | 支持速度优先、性能优先两种模式检测Webshell，可在高速扫描（高性能）/低速扫（低功耗）描之间进行选择，满足多种服务器扫描场景。 |
| 25 | 本地提权 | 支持对提权行为的事件进行监控及检测，并对提权事件进行进程阻断、加白等处置方式； |
| 26 | 支持查看提权的详情，并以图形化的形式展示提权进程树信息，用于本地提权的溯源（提供产品界面截图并加盖原厂公章）。 |
| 27 | 无文件攻击 | 支持实时监控服务器上发生的无文件攻击（漏洞型攻击、灰色工具型攻击、潜伏型攻击）事件，并对无文件攻击事件进行加白、标记处置等操作（提供产品界面截图并加盖原厂公章）。 |
| 28 | OOB带外攻击 | 支持OOB带外攻击检测，并支持黑域名的添加与同步。 |
| 29 | RCE利用 | 基于行为分析，检测对外服务的远程命令执行漏洞利用行为，实现实时告警和追溯（提供产品界面截图并加盖原厂公章）。 |
| 30 | 后门检测 | 对操作系统、文件、软件中存在的后门进行检测，包括：发现时间、后门名称、后门类型、风险等级、服务器名称、服务器IP、操作系统等，并可进行隔离、删除、加白、下载等操作，并提供后门的详情信息 |
| 31 | 应用运行时防护 | 支持RASP（应用运行时自防护），可通过将脚本解析器语言注入到ASP、PHP、Java语言中，并细粒度的监控应用脚本行为及函数调用上下文信息，对上下文信息进行分析判断，及时发现恶意代码和漏洞利用行为（提供产品界面截图并加盖原厂公章）。 |
| 32 | 支持通过插件的方式，工作于IIS、Apache、Nginx等web中间件内部，通过判断流量特征和WAF规则引擎，对访问流量进行监控或防护，阻断SQL注入、XSS、漏洞利用等Web攻击（提供产品界面截图并加盖原厂公章）。 |
| 33 | 分析中心 | 记录当前所有服务器产生的事件日志，并支持全量日志的关键字及语法搜索，支持检索的语法包括但不限于：服务器相关参数、访问主体相关参数、网络相关参数、操作相关参数、客体相关参数、登陆日志相关参数等进行检索，并支持返回上次筛选的关键词（至少可返回不少于5个）（提供产品界面截图并加盖原厂公章）。 |
| 34 | 安全防护 | 可对系统防护（包括但不限于：文件监控与防护、操作系统加固、入侵检测）、应用防护（包括但不限于：高级防护、应用漏洞防护、URL控制）、网络防护（防端口扫描、微蜜罐）进行统一的设置及模板管理，并对各类防护策略以模板形式下发。 |
| 35 | 安全运维 | 显示当前所有服务器的环境现状，包括内存使用率、硬盘空间、操作系统、agent利用率等等信息，并提供报警和导出功能 |
| 36 | 子账号管理 | 提供子账号的管理，支持账号名称、账号角色、上级账户关联、归属人、手机号、邮箱、备注设置，并支持服务器的绑定； |
| 37 | 产品服务 | 原厂三年软件维保升级服务，提供原厂出具的项目授权函及售后服务承诺函。 |