

项目名称		网络安全设备购置	单价 (万元)	62	数量 (项)	1	预算总金额 (万元)	62
序号	需求名称	技术参数和需求内容						
技术要求								
(此项均为实质性响应条款, 不接受负偏离)	基本要求	本单位已经初步建设了终端安全管理系统, 保证了计算终端层面的基本安全, 但是在漏洞发现能力方面有所欠缺, 同时缺乏有效的防御手段, 为了提高本单位的网络安全能力, 本次购置漏洞扫描系统 1 套, 网络安全蜜罐系统 1 套, 要求国产自主品牌。						
	配置要求	1. 漏洞扫描系统 1 套 2. 网络安全蜜罐系统 1 套						
	其他符合性条款	投标人是产品制造商的需提供售后服务承诺函; 投标人非产品制造商的需提供制造商授权、制造商售后服务承诺函;						
1	技术力量	投标人应为本项目配备高水平售后服务团队, 其中: •1、项目经理应具备高级信息系统项目管理师; 2、团队其他成员应至少包含: 信息安全保障专家、中级以上的软件设计师、软件工程师、网络工程师等各 1 名。 3. 漏洞扫描系统应具有中国网络安全审查技术与认证中心颁发的《网络关键设备和网络安全专用产品安全认证》证书, 提供复印件盖原厂商公章 4. 漏洞扫描系统应具有国家信息安全漏洞库兼容性资质证书, 提供证书复印件盖原厂商公章 5. 漏洞扫描系统应具有国家信息安全漏洞库兼容性资质证书, 提供证书复印件盖原厂商公章 6. 蜜罐系统应具有国家信息安全漏洞库兼容性资质证书, 提供证书复印件盖原厂商公章 7. 蜜罐系统应具有中国网络安全审查技术与认证中心颁发的《IT 产品信息安全认证证书》, 提供证书复印件盖原厂商公章 •8. 产品厂商需具有 CNNVD 漏洞信息共享合作单位证书, 提供证书复印件盖原厂商公章 •9. 产品厂商需具备国家信息安全测评中心信息安全服务资质证书(安全工程类三级), 提供证书复印件盖原厂商公章。						

2	性能指标	
	漏洞扫描系统	
2.1		<p>*1. 标准机架式设备，双电源，内存：≥16G，磁盘：≥2T，网络接口：管理口≥1*千兆电口，业务口：≥6*千兆电口，≥1 个扩展槽位；USB 口≥2 个；</p> <p>*2. 默认自带无限制 IP 地址授权；支持≥10 个并发扫描任务。最大并发扫描主机数≥60；最大存储任务数≥8000；具备系统漏洞扫描、WEB 应用扫描、安全配置核查功能。</p>
2.2	漏洞管理和分析	<ul style="list-style-type: none"> 支持检测的漏洞数大于 230000 条，兼容 CVE、CNCVE、CNNVD、CNVD、Bugtraq 等主流标准。
2.3		支持针对弱口令扫描功能，包含不限于 MySQL、MongoDB、Redis、MSSQL、PostgreSQL、AMQP、SSH、SNMP、FTP、Telnet、Sybase、Oracle、RTSP、RDP、IMAP、POP3、SMTP、DB2、SMB、VNC、JBoss、WebLogic、Zabbix、phpMyAdmin 等协议。
2.4		产品支持对系统漏洞扫描、web 漏洞、配置合规进行检查和综合分析，可输出同时包含漏洞扫描和配置核查结果的报表。
2.5		提供高级漏洞模板过滤器，支持将符合筛选条件的漏洞自动加入到自定义漏洞模板中，及后续插件升级包中的漏洞也可以自动加入到模板中。
2.6		内置不同的漏洞模板针对 Unix、Windows 操作系统、网络设备和防火墙等模板，同时支持用户自定义扫描范围和扫描策略；支持自动模板匹配技术，请提供功能截图。
2.7		<ul style="list-style-type: none"> 同 IP 不同端口同漏洞的结果应明确给予端口标识扫描结果在产品界面中支持查看目标应用返回的软件版本，可以方便与漏洞描述对比进行漏洞验证。
2.8		支持扫描物联网设备的漏洞，至少支持国内主流摄像头品牌，包括海康威视、宇视、大华，路由器需支持扫描 TP-Link、Netgear、D-link 等。

2.9		支持断点续扫，可对已完成的扫描任务中没有被覆盖到的目标重新下发扫描任务，需提供功能截图。
2.10		支持授权管理，对已知用户名、密码的资产可预先进行配置存放至授权管理，再下发扫描任务时能对该部分资产的授权信息同步。
2.11		支持在线查看报告和离线导出报告，报告导出可将弱口令隐藏不以明文的形式展现至报告。
2.12	基线核查要求	<ul style="list-style-type: none"> •1. 产品提供系统安全配置核查功能，能够对主流操作系统、中间件、数据库、网络设备、虚拟化设备的安全配置项目进行检查 •2. 基线核查的标准支持公安部等级保护和工信部电信网及互联网安全防护基线配置要求
2.13	用户管理功能	<ul style="list-style-type: none"> •1. 提供三权分立的账户体系，支持上下级部门管理，非上下级的不同部门任务、资产隔离。 •2. 支持对用户有效期进行详细设置，可以设置不限制，也可以设置每天的哪个时段、每周的周几至周几、每月几号至几号才能正常使用。
	网络安全蜜罐系统	
2.14		<ul style="list-style-type: none"> *1. 软硬一体化标准机架式设备，CPU\geq10 核 20 线程*2 颗，内存\geq64G，硬盘容量\geq2T，标配网口：管理口\geq2*千兆电口，业务口\geq4*千兆电口，\geq4*千兆光口，\geq2*万兆 SFP 光口，扩展槽\geq3，1+1 冗余电源； *2. 单设备支持部署高交互蜜罐节点\geq64 个，单设备支持部署低交互蜜罐节点\geq160 个，单设备支持安装管理流量转发 Agent 节点\geq160 个。
2.15		<ul style="list-style-type: none"> • 支持 Windows、Linux 类操作系统蜜罐，提供不低于 8 种蜜罐，包括但不限于：Centos7、Suse12、Suse12sp2、Suse12sp3、Redha7、Windows7、Windows10、WindowsServer2008 等。
2.16	蜜罐类型	<ul style="list-style-type: none"> • 支持 Web 类蜜罐，提供不低于 29 种蜜罐，包括但不限于 Thinkphp6、Thinkphp5 漏洞、Jenkins、Zabbix、OA、Nginx、Discuz、DokuWiki、渗透、邮箱、Webmin、Struts2、JumpServer、SugarCRM、Joomla、Web 克隆、Web 自定义、VPN、Fastjson 漏洞、Sonarqube 漏洞、Shiro 漏洞、Discuz 漏洞、Struts2 漏洞、Httpd 漏洞、Gitlab 漏洞、Log4j2 漏洞、泛微 OA、致远 OA、MES 生产执行管理系统蜜罐等。

2.17		<ul style="list-style-type: none"> 支持物联网类蜜罐，提供不低于 7 种蜜罐，包括但不限于 Dlink 摄像头、Dlink 路由器、Linksys 路由器、Asus 路由器、Trendnet 路由器、Netgear 路由器、OSPF 蜜罐等。
2.18	诱捕攻击分析	<ul style="list-style-type: none"> 支持基于攻击者聚合攻击事件，能够对攻击者打标签，且展示其基础信息、社交账号、硬件指纹、系统指纹、浏览器账号、攻击工具、反制监控、所有攻击事件等信息。
2.19		<ul style="list-style-type: none"> 支持查看攻击路径、下载爆破字典、下载流量 PCAP 包、下载攻击样本附件包、攻击视频回放、还原攻击日志、Url 地址下载等内容。
2.20		<ul style="list-style-type: none"> 支持 ATT&CK 框架，能对捕获到的攻击行为进行映射形成视图，直观展示攻击者意图及相关攻击行为的命中情况，可帮助用户进行安全能力评估。
2.21		<ul style="list-style-type: none"> 支持内置流量分析引擎，支持检测 WEB 攻击、恶意文件攻击、远程控制、WEB 后门访问、DGA 域名请求、SMB 远程溢出攻击、拒绝服务攻击、隧道通信、挖矿、恶意工具利用等行为。
2.22		<ul style="list-style-type: none"> 支持捕捉、下载可疑落盘文件，并通过在线和离线两种方式进行云端情报库/沙箱深度检测分析，获得 HTML 格式的分析报告。报告内容包括文件的基本信息、静态分析、软件环境、威胁情报、动态行为、可疑行为、进程行为、网络行为、文件行为、注册表行为、其他行为、内存字符串、截屏信息等。
2.23		<ul style="list-style-type: none"> 支持至少 16 种攻击工具识别，包括但不限于：Nessus、AWVS、RsaS、Sqlmap、X-Ray、Requests 爬虫、百度爬虫、360 爬虫、谷歌爬虫、必应爬虫、腾讯搜搜爬虫、雅虎爬虫、搜狗爬虫、字节头条爬虫、网易有道爬虫、Scrapy 爬虫等。
2.24	攻击溯源	支持态势大屏实时展示系统诱捕的攻击行为，包括但不限于：业务拓扑、杀伤链分析、访问蜜罐流量趋势、蜜罐统计、攻击源 TOP5、攻击事件分布、实时告警日志、攻击路径、溯源信息、联动情况等。
2.25		支持分析展示系统综合概况，包括但不限于攻击行为趋势、杀伤链分布、攻击行为服务占比、事件风险等级分布、爆破名、爆破密码、系统资源使用率等安全数据统计。

2.26	报告管理	支持生成、预览、导出欺骗诱捕系统攻击报告、高危攻击源分析报告、攻击者溯源分析报告、失陷主机分析报告和自定义报告等至少 5 种分析报告，导出格式为 PDF、HTML、WORD 等。
2.27	系统管理	<ul style="list-style-type: none"> 1. 支持添加真实网络的 IP 资源池，便于蜜罐可以自动获取 IP，快速部署。 2. 支持多因子认证，提供多种登录认证方式，包括但不限于验证码登录、认证证书登录、短信验证码登录等。
*商务要求(均为实质性响应条款，不接受负偏离)		
3	售后服务	<ul style="list-style-type: none"> 1. 软硬件设备待项目验收后免费维保≥ 3 年。 2. 服务期内出现紧急故障情况，公司应在收到服务请求后 30 分钟内响应，2 个小时内到现场，4 个小时内解决问题，4 小时内无法解决的硬件问题应及时提供相应的备用设备，提供 7\times24 小时热线电话支持服务，负责提供技术问题的解答和技术指导。 3. 每年不少于 4 次的巡检服务并提供巡检报告，提供维修及配件服务，提供软件免费升级和维护。 4. 无专用维修工具，可提供维护使用手册。 5. 厂家工程师上门培训不少于 3 次。 6. 合同签订后 3 个月内安装调试完毕，具备运行条件。
4	付款条件	物资到货项目实施完成且验收合格后支付 95 %，维保期满后支付 5 %
<p>说明：1. 加注“*”号的技术指标为关键指标，≥ 1 项未达到招标文件要求，即做废标处理</p> <p>2. 加注“•”号的技术指标为重要指标</p> <p>3. 加注“*”、“•”号的技术指标均需投标企业提供证明材料</p> <p>4. 供应商须提供相关技术指标证明材料予以佐证（证明材料不限于产品规格表、制造商官方网站发布的产品信息、说明书等或检测机构出具的检测报告等技术资料支持的、产品彩页、技术白皮书、厂家出具的技术证明文件、实物照片、软件功能截图等）。</p>		