**软件运维项目要求**

**一、报价供应商资格条件：**

符合《中华人民共和国政府采购法》第二十二条资格条件：

1.具有独立承担民事责任的能力；

2.具有良好的商业信誉和健全的财务会计制度；

3.具有履行合同所必需的设备和专业技术能力；

4.有依法缴纳税收和社会保障资金的良好记录；

5.参加政府采购活动前3年内，在经营活动中没有重大违法记录；

6.法律、行政法规规定的其他条件。

7.本项目不接受联合体投标。

上述资格条件提供相关证明材料。

**二、采购要求**

1.具有国家或有关政府部门颁发的具有相关经营范围的营业执照。

2.维护期内供应商须7\*24小时电话响应，4小时内到达现场并协助采购方将问题处理完毕，所提供服务3年质保。

3.为避免低价低质恶性竞争，需实事求是报价，如有违反市场价格规律恶意以低价谋取中标后，不能按照招标人实际需求提供合格服务或设备设施的，一律按无效标处理并上报财政部门予以相应处罚。

**三、详细参数**

# **（一）产品基本要求：**

1.提供资产清点、风险评估、合规基线、微隔离、入侵检测、防病毒、威胁猎杀、威胁溯源等安全服务，服务期三年。

2.操作系统适配要求需支持以下环境：

（1）Linux操作系统：CentOS7、CentOS8、Ubuntu16、Ubuntu17、Ubuntu18、Ubuntu19、Ubuntu20、Redhat7、Suse15、Suse12、麒麟Kylin V10、openEuler21、openEuler22等；

（2）Window操作系统：Windows7 x64、Windows10 x64、Windows Server 2008 r2、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019、Windows Server 2022等；

# **（二）**功能指标项要求：

1.安全态势展示：支持图形化综合展示全局态势，查看主机和容器资产的整体安全状态，包括：资产、风险、威胁、告警、安全事件、被攻击资产等数据汇总统计，以及趋势图、top分析、分布分析等信息。（投标时提供产品功能证明截图并加盖公章）

2.资产清点功能：支持自动对主机和主机内容器资产进行资产清点，包括账户、进程、端口、软件应用、数据库、web应用、web站点、安装包、计划任务、启动项、容器所属镜像、容器运行状态、命名空间、POD、所属节点等信息，另外支持主动发现目标网络内未知主机。支持通过Agent自动识别、手动录入、批量导入三种方式管理相关业务资产，包括主机资产、安全设备、网络设备等资产，可设置相关资产等级、资产编号、负责人、负责人部门、负责人电话、负责人邮箱、机房位置等。（投标时提供产品功能证明截图并加盖公章）

3.容器资产识别：支持容器、集群、镜像、POD、服务、Namespace等容器类资产的快速清点。自动获取所有与容器相关信息，如：容器的运行状态、连接情况、关联镜像等，可为用户提供容器内资产分层、分类的集中可视化，帮助用户从整体安全角度细粒度观察容器类资产运行状况。（投标时提供产品功能证明截图并加盖公章）

4.资产安全评估：通过对目标主机资产进行安全评估，从主机信息异常变更风险、漏洞风险、弱密码风险、安全基线风险、恶意代码风险、威胁入侵风险、网络微隔离风险等方面进行安全评分，根据安全评分判定安全等级，安全等级包括严重0~20分、高危21~40分、中危41~60分、低危61~80分、安全81~100分。（投标时提供产品功能证明截图并加盖公章）

5.未知资产探测功能：支持通过主机客户端扫描探测网内其他未安装客户端的主机资产，支持创建多个主机发现任务，并进行管理，提供ARP、PING、NMAP三种方式探测未知主机，支持自定义扫描网段，以及选择获取操作信息，如主机IP、操作系统等信息。

6.漏洞检测：支持对主流操作系统、中间件、数据库、容器进行漏洞检测，版本比对和POC脚本验证两种漏洞检测方式支持按需选择。支持自定义漏洞扫描，支持针对指定漏洞、指定主机、指定业务组进行漏洞扫描。漏洞详细信息包括：漏洞等级，漏洞名称、漏洞说明、漏洞类型、影响应用、漏洞exp链接、修复建议、CVE编号、CVSS评分与详情、风险特征、CNNVD 编号等信息。（投标时提供产品功能证明截图并加盖公章）

7.虚拟补丁：实时监控并主动防御利用已知漏洞的恶意攻击，可以在不干扰现有系统正常运行的情况下，为系统提供即时的安全防护。

8.支持按照国际CIS检测标准（Level1、Level2）和国内等级保护检测标准（等保二级、三级）对操作系统、应用中间件、数据库进行基线检测，内容至少应包含检查项，检查结果，通过率、修复方法等。（投标时提供产品功能证明截图并加盖公章）

9.威胁防护：支持对主机和容器进行持续威胁监测和分析，可实时发现反弹shell、本地提权、异常登录、非法外连、webshell、暴力破解、文件恶意篡改、容器逃逸等攻击行为，并提供告警和处置能力。（投标时提供产品功能证明截图并加盖公章）

10.行为自学习：支持基于主机、容器、应用的行为学习能力，形成主机、容器、应用的行为基线，并可以根据学习的行为基线对主机、容器、或应用进行行为监控或阻止。

11.具备自主可控的病毒查杀引擎，支持对主机内部存在的恶意代码、病毒、木马、勒索程序、挖矿、webshll、宏病毒、黑客工具等恶意程序进行实时查杀，对于可疑、未知的样本支持沙箱动态检测并提供预警。（提供厂商病毒查杀引擎软件著作证明）

12.★勒索防护：通过恶意代码扫描过滤、诱饵文件监测、勒索行为特征监测、文档/图片/数据文件专项保护等多种方式，建立勒索病毒静/动态特征检测与防御能力。（投标时提供产品功能证明截图并加盖公章）

13.应用安全：通过规则特征过滤HTTP请求里的攻击Payload，以及监控函数调用上下文信息，可实时感知并拦截网络漏洞利用攻击，包括命令执行类攻击检测、任意文件删除类攻击保护、反序列化攻击检测、目录遍历检测、危险DNS解析识别、任意文件上传保护、JNDI注入攻击检测、文件链接写后门防护、异常库加载检测、内存马检测、OGNL 代码执行检测、文件重命名保护、HTTP 响应采样检测、SQL 注入检测、跨站脚本攻击(XSS)、SSRF 请求伪造检测等网络攻击行为。（投标时提供产品功能证明截图并加盖公章）

14.★威胁溯源：通过自主算法将具有关联的多条告警生成一条入侵事件，按照时间顺序还原攻击过程，并以图形化的方式呈现攻击者入侵链路全景图，帮助安全人员识别攻击者使用的技战术以及触发的检测点。（投标时提供产品功能证明截图并加盖公章）

15.★微隔离功能：支持对主机、容器、应用按照IP、端口、协议、应用、工作负载标签等字段进行网络访问控制策略配置。支持微隔离模块与入侵检测、风险发现模块联动，当发现某主机发现高危漏洞或入侵行为时，可自动强制隔离该主机，避免攻击横向移动。（投标时提供产品功能证明截图并加盖公章）

16.安全报告导出：支持指定主机或全部主机按照时间段导出安全分析报告，包括资产统计、风险统计、安全基线统计、威胁事件统计、网络异常流量统计、整体安全分析等。

# **（三）**资质要求：

1.产品应具备网络关键设备和网络安全专用产品安全认证证书

2.产品应具备计算机软件著作权登记证书

3.产品应具备IT产品信息安全认证证书

1. **报价单**