**调研要求**

## 一．项目背景

近年来，南京市第二医院深入开展网络安全建设，不断完善信息安全防护体系，为进一步保障南京市第二医院网络安全能力，医院计划采购终端安全DNS系统和相关的服务，完成终端实名登记、准入管理，实现恶意域名访问的有效过滤和阻止，降低恶意软件、病毒、钓鱼网站等网络威胁渗透进医院网络环境的风险。

## 二．产品服务清单及技术参数要求

## 2.1产品清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 标的名称 | 数量 | 单位 | 采购标的所属行业 |
| 1 | 终端安全DNS云监测服务 | 2 | 套 | 服务 |
| 2 | 终端实名登记和准入实施服务 | 1 | 项 | 服务 |

## 2.2技术参数要求

### 2.2.1终端安全DNS

|  |  |
| --- | --- |
| **功能指标** | **技术参数要求** |
| 部署模式 | 支持流量镜像、Syslog日志转发两种旁路接入模式，支持IPV4/IPV6接入网络。 |
| 支持递归-阻断模式，终端将DNS服务器指向DNS安全网关进行DNS解析，支持IPV4/IPV6接入网络。 |
| 支持代理软件本地化交付，可部署在用户自有的物理服务器、虚拟机等环境中。 |
| 智能解析 | ★支持智能联动“云端安全DNS”，基于运营商、所属地理区域等提供智能递归解析能力，支持联通/电信/移动/教育/BGP多线路接入 |
| 解析稳定性 | 支持HA主备机制，检测和解析进程分离机制，保障解析稳定性。 |
| 传输加密 | ▲支持本地和云端DoH、DoT加密域名解析服务，对解析流量加密处理。（提供功能截图加盖公章） |
| 威胁情报 | 威胁情报数量不少于1500万条，APT情报不少于4万条；情报包含丰富的上下文，至少包括：威胁家族、威胁类型、感染平台、攻击特点、处置建议、公开分析等。 |
| 威胁检测 | 支持识别的攻击类型应至少包含：后门、远控木马、DDOS、挖矿、银行木马、APT、DGA、黑客工具、勒索软件、数据窃取、蠕虫、钓鱼网站、黄赌毒等威胁。 |
| 威胁告警 | 支持根据威胁检测结果生成告警事件，告警信息应至少包括：攻击者域名/IP、被攻击单位、被攻击资产、所属区域、恶意家族、攻击特点、处置建议、公开分析等 |
| 失陷资产 | 支持从资产维度对告警进行统计分析，展示自定义时间段失陷资产趋势以及失陷资产详细信息，详细信息应至少包括：资产IP、恶意类型、感染时间、历史告警数、是否重点资产等。 |
| 恶意域名 | 支持从域名的维度对告警进行统计分析，展示自定义时间段恶意域名类型以及详情信息，详情信息应至少包括：域名、恶意类型、最新告警、去重资产数、首次出现时间、最近一次出现时间等。 |
| 告警合并 | ▲支持根据IoC、攻击家族等对告警进行合并，避免相同攻击重复告警。（提供功能截图加盖公章） |
| 告警事件分析 | 支持展示自定义时间段内资产IP请求域名次数TOP统计、恶意域名解析趋势、资产归属告警次数分布、威胁类型TOP5统计、恶意域名处理方式分布、资产IP请求域名次数TOP统计等。 |
| 解析日志分析 | 支持展示最近一个月的DNS解析日志，日志字段应至少包括：解析时间、资产IP、请求域名、请求类型、Rdate、处理方式等，并支持根据时间、资产IP、请求域名等进行查询分析。 |
| 策略设置 | ▲支持自定义阻断策略，可自定义策略生效范围（基于资产）、威胁类型、自定义黑名单域名等（提供功能截图加盖公章） |
| 黑名单 | 支持手动添加全局域名黑名单 |
| 白名单 | 支持手动添加全局域名白名单 |
| 内网域名 | 支持对内网域名的DNS请求转发，可添加、删除内网域名以及内网DNS服务器。 |
| 报表中心 | 支持定期报表、自定义生成报表，按照日、周、月或自定义时间导出报表。 |
| 资产管理 | 支持内网资产自动发现，可新增、删除、编辑资产、支持标记为重点资产 |
| 账号管理 | 支持账号的新增、删除、编辑，支持账号按照不同的权限分配账号角色。 |
| 系统监控 | 支持对平台涉及的硬件环境、数据库、关键进程、Kafka的状态监控。 |
| 系统日志 | 支持对用户关键操作进行日志记录、支持日志导出功能。 |
| 告警通知 | 支持通过SMTP服务器的配置，通过邮件将威胁告警状态通知用户。 |
| 安全设置 | 支持配置登录密码长度、密码强度、登录超时等。 |
| API接口 | 可提供API接口，将威胁告警、DNS解析数据、拦截日志同步至本地或第三方平台 |
| 产品资质 | ▲软件著作权、销售许可证 |
| 数量 | ★提供不少于1200个终端用户的用户许可 |
| 服务 | ★提供不少于一年的原厂技术支持及云端情报服务 |

### 2.2.1终端实名登记和准入实施服务

|  |  |
| --- | --- |
| **功能指标** | **技术参数要求** |
| 服务 | 根据采购人要求完成本部及公卫两院区的对办公外网进行入网登记、准入；以及对恶意域名进行拦截、代理工具进行封禁等服务； |

# 项目实施要求

1、供应商必须提供本次采购的产品的安装与调试服务，保证本次采购的设备能够接入采购人单位现有的终端网络实现无缝对接；

2、供应商必须提供本次采购的产品的集成服务，负责完成本次采购的产品与采购人现有的网络、终端、安全等设备的对接集成工作，并完成终端网络环境的实名认证和安全加固，在过程中需确保业务不中断；