上海港湾学校终端检测响应平台

技术要求

## 项目概述

上海港湾学校部分教师电脑没有安装杀毒软件，学校每年都有因为电脑中毒出现的各种断网，数据丢失的情况，需要采购终端检测响应平台和终端防病毒许可200点，为全校所有的教师电脑提供杀毒防护的功能，服务期3年。

## 技术要求

|  |  |
| --- | --- |
| 产品形态 | 产品纯软件交付，包含管理控制中心软件及终端客户端软件 |
| 终端许可数量 | 200点 |
| 服务年限 | 3年 |
| 管理控制中心要求 | 单一管理控制中心可统一管理分别部署在Windows PC，Win服务器以及Linux服务器的客户端软件  |
| 多维度威胁展示 | 支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、WebShell后门数量、高危漏洞及其各自影响的终端数量 |
| 资产管理 | 支持全网视角的终端资产统一清点，清点信息包括操作系统、应用软件、监听端口和主机账户，其中操作系统、应用软件和监听端口支持从资产和终端两个视角进行统计和展示 |
| 支持资产登记功能，支持录入本终端所属责任人、责任人联系方式、邮箱、资产编号、资产位置信息，并可设置哪些为必填项，以便于进行终端资产管理 |
| 支持对单个终端运行状态的监控，包括但不限于进程、服务、网络连接、计划任务和开放共享信息 |
| 支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑root权限账号、长期未使用账号、半夜登录、多IP登录进行账号分类查看，支持统计最近一年未修改密码的账户 |
| 升级管理 | 支持客户端的错峰升级或灰度升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或I/O风暴 |
| 威胁检测 | 具备基于人工智能的检测引擎，支持无特征检测技术，有效应对恶意代码及其变种  |
| 终端自保护 | 支持客户端防卸载，客户端卸载需要输入密码才能卸载，避免非管理员卸载终端，造成终端安全真空 |
| 勒索病毒专防 | 基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御,支持监控诱饵文件，诱饵文件可被实时监控，当勒索病毒对该文件进行修改或加密操作时进行拦截, 支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具 |
| 挖矿病毒巡检 | 提供挖矿病毒巡检工具，支持通过内存、进程和启动项来检索病毒相关信息 |
| 暴力破解检测 | 统计单个攻击源及分布式攻击源的暴力破解检测，支持按照RDP、SMB和SSH类型进行封堵并自定义爆破阈值，可对封停时间进行自设置  |
| 威胁同步处置 | 构建全网文件信誉库，当一台终端发现某一病毒文件，全网可进行感知并进行针对性查杀，支持处置病毒时选择是否在其它终端上同步处置  |
| 漏洞修复及补丁管理 | 支持对终端的漏洞情况进行扫描，并查看漏洞具体情况及KB号，并显示具体修复情况  |
| 产品资质要求 | 提供公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》网络版防病毒产品（一级品）资质证书 |
| 提供终端安全产品获得的赛可达实验室“东方之星”证书 |
| 提供中华人民共和国国家版权局颁发的《计算机软件著作权登记证书》，且该证书仅针对终端安全软件的平台软件 |
| ★兼容性要求 | 能够与学校现有的深信服安全态势感知设备、深信服应用防火墙设备、深信服上午行为管理联动响应，提供联动响应相关产品截图证明**（必须提供，未提供废标处理）** |

## 公司资质要求

* 在中国境内注册的合格法人机构，并具有相应的经营范围
* 符合《中华人民共和国政府采购法》第二十二条规定的供应商；
* 在上海市有固定的服务点。
* ★提供制造厂商针对本项目的授权书和售后服务承诺书**（必须提供，未提供废标处理）**

## 投标文件组成

* 报价单（附件二）
* 营业执照、税务登记证、组织机构代码证或“三证合一”的营业执照
* 招标要求的其他材料