**桌面终端安全管理项目需求**

**一、基本介绍**

目前医院信息化建设程度很高，但网络与信息安全风险问题也随之而来。专用网络和终端的安全性也面临着勒索病毒等最新型病毒的威胁，一旦出现黑客攻击、数据窃取等事件，将有可能造成治安管理失控、敏感信息泄漏等后果，严重危害社会稳定。本院意识到内网安全建设存在薄弱点，需要看清内网安全状况并溯源问题，而且要发现问题后，保障本院网络安全处于全天候安全健康稳定状态。

针对以上所述亟待解决的问题，从终端设备病毒防护、漏洞检测、攻击事件闭环等方面综合考虑，急需医院网络前端接入安全防护的整体解决方案。

**二、项目需求**

总体实现：通过在内网终端上部署终端检测与响应系统，除了具有杀毒功能以外，还具有微隔离和补丁功能，可以及时阻止问题机器发包并封锁端口，防止病毒在内网中蔓延扩散。

基于以上安全建设现状及实际需求，本院将围绕终端资产安全生命周期，通过预防、防御、检测、响应赋予终端更为细致的隔离策略、更为精准的查杀能力、更为持续的检测能力、更为快速的处置能力。在应对高级威胁的同时，快速处置终端安全问题，构建轻量级、智能化、响应快的终端安全系统。

**三、功能模块**

**3.1终端资产的全面管理**

全网终端资产的全面盘点，包含业务服务器的终端和用户 PC 的终端。盘点每台终端设备的名称、IP 地址、MAC 地址、所属组织、责任人、资产编号、资产位置等。每一台的终端上的资产信息清晰，每一个安全事件责任到人，使得安全管理能落实到位。

**3.2勒索病毒的实时防御**

勒索病毒通过加密文件的方式，要求中招者支持一定数额的赎金。这种攻击方式越来越流行，每天都有客户反馈中招。 EDR 能够非常精准的识别不同的勒索软件家族，并通过专业分析识别出种种勒索病毒感染行为和加密特征，对最新的勒索软件进行有效的查杀，防止用户感染最新的勒索软件。

**3.3入侵攻击的主动检测**

终端主机被入侵攻击，导致感染勒索病毒或者挖矿病毒，其中大部分攻击是通过暴力破解的弱口令攻击产生的。的 EDR 主动检测暴力破解行为，并对发现攻击行为的 IP 进行封堵响应。针对 Web 安全攻击行为，则主动检测 Web 后门的文件。针对僵尸网络的攻击，则根据僵尸网络的活跃行为，快速定位僵尸网络文件，并进行一键查杀。

**3.4热点事件的快速响应**

安全云脑通过全球的大数据安全分析，提供热点事件的 IOC 情报，推送情报数据给 EDR 产品。EDR 产品能根据 IOC 情报数据快速的全网威胁定位分析，及时发现和响应最新的热点事件，并且根据历史行为数据进行溯源分析，避免组织受到安全事件的通报。

**3.5 访问关系的策略控制**

当前各种感染性病毒大部分都是通过网络进行传播，从而导致大范围内的终端中招，影响范围较广。EDR的微隔离支持网络访问关系策略的配置，可以实现业务域之间或者终端之间的网络隔离，从源头上杜绝病毒的传播，减少用户的损失，进一步保证终端的安全。

**四、技术参数**

|  |  |
| --- | --- |
| **技术指标** | **具体参数** |
| **产品形态** | 产品可以纯软件交付，包含管理控制中心软件及终端客户端软件，其中管理控制中心可云化部署； |
| 本次配置≥800套PC版终端检测响应软件授权 |
| **管理控制中心要求** | 要求环境：CPU≥4核，内存≥8G，硬盘≥1TB； |
| 单一管理控制中心可统一管理分别部署在WindowsPC、Windows服务器、Linux服务器以及国产化服务器的客户端软件 |
| **Windows PC 客户端支持** | Windows XP/Windows Vista/Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11 |
| **国产化终端管控** | 支持管控国产化操作系统终端，下发基本策略，配置病毒查杀、实时防护、桌面管控等策略，处理国产化终端发生的威胁事件。 |
| **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、高级威胁、暴力破解、僵尸网络、WebShell后门、高危漏洞及其各自影响的终端数量 |
| ★支持跳转链接至云端威胁情报中心，针对已发生的威胁提供详细的分析结果，包含威胁分析、网络行为、静态分析、分析环境和影响分析。（需提供产品截图证明 ） |
| **资产管理** | 支持全网视角的终端资产统一清点，便于帮助用户快速发现风险面。清点信息包括操作系统、应用软件、监听端口和终端账户，其中操作系统和监听端口支持从资产和终端两个视角进行统计和展示。 |
| 支持收集并展示单个终端的软件信息，包括软件名称、软件类型、软件版本、所属厂商、软件安装路径以及安装时间 |
| ★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、夜间登录、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（需提供产品截图证明 ） |
| **系统维护** | 支持对在线终端下发实时通知消息 |
| ★支持客户端的错峰升级，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（需提供产品截图证明 ） |
| **威胁防御** | ★通过智能识别终端环境情况（低配硬件、老旧设备、桌面虚拟化等）和当前终端资源占用，在闲时实时监控和病毒扫描场景，都可智能调整终端检测响应软件的资源占用（CPU、IO等），为业务让出资源，不卡业务，对业务零摩擦。（需提供产品截图证明 ） |
| 具备基于本地缓存信誉检测与全网信誉检测，构建全网信誉库的检测引擎，做到内网一台威胁，全网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有效提升查杀效率，减少终端资源开销 |
| 支持对zip， rar， jar， cab， 7z等常见压缩文件的扫描检测，支持压缩文件层级进行策略配置，最大可配置检查10层压缩文件 |
| 具备针对最新未知的文件，使用IOC特征（文件hash、dns、url、ip等）的技术，进行云端查询。云端的安全中心，使用大数据分析平台，基于多维威胁情报、云端沙箱技术、多引擎扩展的检测技术等，秒级响应未知文件的检测结果，构架公有云云查体系 |
| ★支持一键云鉴定服务，提供云端专家+沙箱+多引擎鉴定能力，结合云端威胁情报对已告警的威胁文件再次进行综合研判并给出100%黑白结果，用户可自助对管理平台告警的威胁快速判断是否误报和了解威胁详情。（需提供产品截图证明 ） |
| ★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（需提供产品截图证明 ） |
| 支持对Windows停更的系统提供专项防护，包括0day漏洞防护、文件防护、暴破入侵防护、系统脆弱点识别和风险端口封堵等多项核心功能； |
| **补丁管理** | 支持对Windows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 |
| ★支持流行Windows高危漏洞的轻补丁免疫防御，支持Windows补丁批量一键修复（需提供产品截图证明 ） |
| **轻桌管** | 支持应用管控功能，内置常用的系统应用，包括IM、下载工具、代理工具、办公软件等。并且支持新增自定义识别应用。帮助客户限制盗版、恶意软件使用，加强客户正版软件配置规范建设，事前拦截终端进程运行，事中可结束终端应用的运行，事后可审计进程管控日志。 |
| 支持屏幕水印功能，提供一种溯源追溯手段，敏感信息泄露后可以通过水印信息快速做到溯源。 |
| **产品及厂商资质** | 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》 |
| 厂商需是国家信息安全漏洞库CNNVD一级技术支撑单位； |
| 提供终端检测响应软件所使用检测引擎入围VirusTotal平台的资质证明 |

**五、功能简介**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能简介** | **功能描述** |
| **1** | 人工智能检测 | 通过高维度特征查杀文件检测率达到99.7，多类分类检测率达到90.3% |
| **2** | 网端联动闭环 | 网络端设备发现终端威胁，自动化告知EDR检测平台对终端进行处置。 |
| **3** | 终端肃杀 | 一台发现威胁，全网威胁感知，并且在网络中所有终端中查杀相同病毒文件，做到终端肃杀，片甲不留。 |
| **4** | 勒索诱饵 | 通过在系统关键目录及随机目录放置诱饵文件，当诱饵文件被加密时立马启动应急机制，阻止加密进程，查杀病毒安源文件。 |
| **5** | 端点安全的立体可视和发现 | 通过EDR控制中心对全网终端进行多维度高效管理，使全网终端风险可视，终端流量关系可视，终端资产可控，资产责任人可追 |
| **6** | 云端行为监控沙箱 | 基于用户态和内核态行为监控技术以及异常行为识别引擎，可提供文件动态鉴定、流量IoC提取、恶意行为记录能力。 |
| **7** | 多维度漏斗型检测框架 | 通过多维度漏斗型检测框架有效提升检测效率，轻量化终端资源消耗，通过包括人工智能检测引擎，安全云脑检测引擎等多维度引擎对全文件进行有效查杀。 |
| **8** | 终端闭环 | 根据Gartner四阶段模型，定义了在预防、组织、检测、响应各阶段共12个关键功能来有效保护终端安全 |
| **9** | 微隔离 | 利用应用角色之间的主机流量访问控制的技术，提供对业务安全域之间、业务安全域内不同应用角色之间、业务安全域内相同应用角色之间的访问控制策略配置，提供简单可视化的安全访问策略配置，提高了安全管理的效率。 |
| **10** | 动态安全边界 | 创新微隔离技术架构于主机防火墙之上，致力解决病毒东西向、横向移动和内网扩散和处置问题，提出了一种基于安全域应用角色之间的流量访问控制的系统解决方方案，提供全面基于主机应用角色之间的访问控制，做到可视化的安全访问策略配置，简单高效地对应用服务之间访问进行隔离技术实现。 |

**六、项目预算**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **单位（套）** | **单价**  **（万元）** | **总价**  **（万元）** |
| 1 | 内网终端检测与响应系统 | 1 | 25 | 25 |
| 合计 |  | | |  |