网络安全项目采购需求

一、采购清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **数量** | **单位** |
| 1 | 网神SecVSS 3600 漏洞扫描系统 V3.0 | 1 | 台 |
| 2 | 天融信EDR | 1 | 套 |

二、拟申报采购方式

□公开招标 □邀请招标 □竞争性磋商 □竞争性谈判

□询价 □单一来源 ☑网上商城

三、其他

采购预算：590000元

质保期：5年；

供货期：合同签订后30日历天；

年 月 日

四、采购需求

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **数量** | **采购需求** |
| 1 | 网神SecVSS 3600 漏洞扫描系统 | 1台 | 1. 标准2U机架式，≥1TB硬盘，标准配置≥6个10/100/1000M自适应电口，2个SFP接口，有扩展槽，冗余电源；支持快速部署上线。  2. 扫描IP地址和扫描Web域名数量无限制，Web扫描任务并发数为15个域名，支持≥150个IP地址并行扫描，支持扫描A类、B类、C类。  ★3. 至少提供系统扫描、WEB扫描、数据库扫描、基线配置核查、弱口令扫描五大功能模块，含各类授权。  4. 支持Web漏洞扫描，检测基于OWASP Top10标准定义扫描规则；支持同时下发系统扫描、Web扫描、弱口令扫描任务，扫描目标可以是IP、域名、URL任一格式。  5. 具有Web登录扫描、SQL注入、XSS、网页木马、系统命令执行漏洞、信息泄露、资源位置预测漏洞、目录遍历漏洞、配置不当漏洞、弱密码、内容欺骗漏洞、外链、暗链、已知webshell、各类CGI漏洞等扫描，支持Cookie认证、Form认证、Basic认证、NTLM认证、Session认证、Digest认证、SSL，并支持Web登陆验证，确保Web登录成功。  6. 支持Web扫描会话录制，通过登录预录制方式扫描常规网页爬虫爬取不到的URL；支持HTTPS协议，对基于HTTPS协议的WEB应用进行自动安全评估。  7. 支持以树形结构展示网站目录结构，并在网站目录上关联显示相应漏洞，便于直观确定漏洞位置。  ★8. 支持自动探测指定网段中的Web站点，并可转为Web扫描任务。  9. 支持至少三种漏洞验证方式如浏览器验证、注入验证、通用验证。  10. 支持对常见设备、数据库、应用服务器的配置核查。支持主机设备操作系统包括Windows系列、Linux系列、HP-UX、AIX、Solaris、麒麟、凝思等；支持主流数据库包括Oracle、Mysql、SQL Server、Sybase、DB2、Informix、达梦、南大通用、人大金仓；支持主流网络设备包括思科、华为、H3C、力腾、锐捷、Juniper等品牌的交换机和路由器；支持主流防火墙包括思科、华为、Juniper/Netscreen、网神、天融信；支持主流中间件和应用包括Apache、Bind、Domino、IIS、Jboss、Nginx、Resin、Tomcat、TongWeb、Weblogic、Websphere；支持虚拟化配置核查，包括VMware、Xen、FusionCompute、Esxi；  11. 支持大数据组件框架漏洞检测，如zookeeper、ElasticSearch、ActiveMQ、Kibana、Hadoop等；支持扫描国产系统、数据库扫描；支持检测VMware、KVM、XEN在内的虚拟化漏洞扫描；支持扫描物联网设备，支持扫描Brickcom、大华、索尼、TP-LINK、宇视、AXIS、佳能、海康威视等国内外厂商的摄像头，支持扫描佳能、惠普等网络打印。  12. 支持常用的SSH、SMB、TELNET、RDP、POP、POP3、IMAP、FTP协议的登录弱口令扫描；支持批量导入登录信息、批量登录验证。  13. 支持扫描物联网设备，支持扫描Brickcom、大华、索尼、TP-LINK、宇视、AXIS、佳能、海康威视等国内外厂商的摄像头，支持对工控专用设备的扫描。  14. 支持检测的漏洞数大于60000条以上，涵盖漏洞标准包含CVE、CVSS、CNVD、CNNVD、CNCVE、Bugtraq6种，CVSS覆盖CVSS2和CVSS3版本。  15. 支持导出报表，或扫描任务结束后自动发送报表到指定邮箱，报表包含5种常见格式：Excel、Word、HTML、PDF、XML；导出同时包含系统扫描、Web扫描、安全基线、弱口令扫描结果的报表，可以统一分析网站漏洞、网站所在主机漏洞以及主机弱口令。  16.支持缺省内置标准基线核查模板，包括：等保三级检测要求、工信部配置规范、中国电信安全配置规范、中国移动安全配置规范；  17.支持资产历史扫描结果变化趋势展示，并可对比任意两次扫描结果，查看新增漏洞和减少漏洞。  18.支持扫描任务完成后发送告警，告警方式包含邮件告警、短信告警、SNMPtrap告警、SYSLOG告警、FTP告警。  19.支持漏洞库的自动在线升级，升级授权5年。 |
| 2 | 天融信EDR | 1套 | 1.系统具备全中文界面，B/S架构。管理员只需通过浏览器登录控制中心，即可对系统进行管理，能够对客户端进行统一管理，统一下达指令。服务器端可采用Docker部署方式，能够快速恢复，横向扩展，可移植性强，windows和Linux管理端统共用一个。  2.病毒查杀支持多引擎的协同工作，对病毒、木马、恶意软件、引导区病毒、BIOS病毒等进行查杀，提供主动防御系统防护等功能。  3.本次至少提供WindowsServer授权≥200个，LinuxServer授权≥100个，支持各版本32位及64位，Windows PC授权≥300个，可支持国产化服务器操作系统。  4.客户端支持操作系统: Windows XP\_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10等操作系统，同时支持多种Linux操作系统以及中标麒麟、银河麒麟等国产操作系统；操作系统包含32位及64位；具有服务器等同的杀毒能力；安装后占用系统资源少，内存占用10M左右，软件无广告、无推送信息。  5.支持病毒木马威胁的快速扫描、全盘扫描、强力扫描、文件专杀、隔离区恢复、系统修复、插件管理；  6.具备虚拟补丁功能，针对网络数据流的深层分析，检测入站流量并保护应用程序免受攻击。  7. 对勒索病毒提供专有的防护功能；  8.支持内容拦截主动防御，文件系统实时防护，支持多种压缩格式，能够监控间谍文件，拦截局域网病毒，宏病毒免疫，DLL劫持免疫，支持开机延迟加载，实时监控级别设置高中低三种配置，监控文件类型包含所有文件或者程序及文档；杀毒程序进行动态自行调整，对CPU资源占用低。  9.要求对流行病毒的检测能力必须超过98%的检出率，超过98%的清除率，小于0.1%的误报率。  10.具备基于虚拟沙盒的高效的本地反病毒引擎，客户端具备本地查杀缓存。  11.支持对webshell后门进行扫描检测 , webshell后门库数量大于100000。  12.支持对移动存储设备采用标签式注册管理，定义禁用、启用只读、启用（只读\_运行）和启用读写、启用（读写\_运行）等操作，按照文件类型审计在移动存储介质上文件操作记录。  13.客户端安装具备本地安装，WEB安装，域推送安装等方式。  14.控制中心具备实时显示客户端的状态及终端基本信息，包括客户端连接状态、服务状态；控制中心具备全网/以分组、标签为单位/指定某些客户端定制操作，即时/定时实现客户端三种病毒查杀模式；支持对客户端上报的安全日志进行审计、告警；  15.具备客户端主动升级及平台即时/定时推送升级；具备全网/以分组、标签为单位/指定某些客户端定制不同版本升级包，实现差异管理、灰度升级。  16.产品具备公安部《信息技术产品安全测评证书》、《计算机信息系统安全专用产品销售许可证》  17.杀毒平台和病毒库升级授权5年。 |