采购清单及要求

1 采购清单

序号	项目	用途	数量
1	日志审计	实现网络设备、安全设备、主机操作系统、中间件、数据库、应用系统在内的设备及系统的全面日志审计、分析；≥40 个资产授权。	1 套
2	主机防护	对虚拟化主机进行统一的安全管理，进行防病毒，防暴力破解安全防护；≥30 个资产授权。	1 套
3	等保测评	由第三方具备信息系统等级保护测评资质的机构对网站系统进行等保测评，并出具测评报告。	1 次
4	安全服务	安全设备巡检，安全配置核查，病毒跟踪，故障诊断解决处理，安全预警；应急处置，信息安全培训，安全咨询服务，安全检查等。对照等保第二级要求进行整改。	1 年

备注：通过整改测评使网站信息系统符合信息系统安全等级保护第二级要求。

2 参数要求

清单及技术参数要求完全满足招标文件要求，标注★的实际响应参数不允许负偏离。

（1）日志审计

功能组件	功能描述
资产管理	具备资产录入、修改、删除、查询等操作和批量导入导出；
	资产属性中可标记所属安全域、业务域信息；
	★支持以资产维度看当前资产下所有的告警和日志及部分报表展示；（投标时提供产品截图及原厂盖章）
	支持按照资产的重要程度自定义权重及密级；
日志采集解析	支持对各类网络设备（路由器、交换机、VPN、负载均衡等）、安全设备（防火墙、IDS、IPS、防 DDOS 攻击、Web 应用防火墙等）、主机操作系统（Windows、Linux 等）、各种数据库（Oracle、Sqlserver、Mysql）、各种应用系统（Email、Web、FTP 等），终端管理系统告警日志，网络综合审计系统告警日志，上网行为审计系统日志，以及用户自己的业务系统的日志、事件、告警等安全信息进行全面的审计；
	支持 syslog、sftp、jdbc 等标准日志接口；
	支持 agent 本地采集；
	支持代理服务器采集，通过代理服务器过来的日志能准确匹配实际的类型；
	★主动采集日志，支持特定时间采集，防止业务繁忙影响系统性能；（投标时提供产品截图及原厂盖章）
	支持文件夹采集，支持文件通配符过滤采集；
	支持内置过滤，归并策略，对数据进行自动过滤和归并处理；
	采用非关系型数据库存储；支持海量数据存储；
	能够对原始日志全量采集和全量存储,能够按照自定义格式对原始日志进行准确解析；
	★日志采集解析至少包括直接信息解析和补全解析，直接信息包括日志中涵盖的信息，比如 IP，端口等，补全信息至少包括资产名称、所属人员、组织、网络区域、业务区域、厂家、操作系统名称、系统类型等（投标时提供产品截图

	及原厂盖章）
	★日志解析支持自定义解析，自定义解析支持灵活的语法，至少包括字符串函数，字符串函数支持级联语法、条件函数、引用函数等；（投标时提供产品截图及原厂盖章）
	支持自定义日志解析规则的导出；
数据分析	支持数据字典模型；
	数据支持多线程时时关联分析，不是定时统计分析；
	支持内置关联分析策略，可以设定告警策略的参数；
	支持自定义告警规则添加，告警规则模型至少包括单条告警，事件数量告警，多维度关联告警，基线对比告警等规则模型；提供基于图形化方式的规则编辑器；告警规则可导入导出，规则可实时启用和停用。
	支持杀伤链模型；
	★支持 linux 主机文件操作监控，时时发现违规行为；（投标时提供产品截图及原厂盖章）
	★支持 linux 主机用户操作行为监控；（投标时提供产品截图及原厂盖章）
系统查询	支持全文检索查询；
	支持关键字词检索查询，包括日志检索、事件检索、告警检索、高级检索及文件检索；
	支持内置常用查询模板，方便用户操作；
	支持查询模版创建、修改、删除功能；
	★支持系统对单个或者多个参数进行直观的查询功能，方便用户操作；（投标时提供产品截图及原厂盖章）
	支持查询日志导出功能；
	★支持内置 ip 知识库的能力，在鼠标放到 ip 字段上，可以显示 ip 归属地，归属地支持内网场景；（投标时提供产品截图及原厂盖章）
	支持高级检索以多条件组合查询方式；
	支持内置知识库的查询，以及自定义知识库内容；
	支持统计字段、查询结果显示字段、查询条件中搜索日期的配置。
报表展示	内置丰富的报表，包括主机数据库安全网络设备等；
	★支持灵活的自定义报表，可以手工添加报表（天、周、月）；（投标时提供产品截图及原厂盖章）
	★支持数据报表导出，可以导出 word、excel、pdf、html、图片；（投标时提供产品截图及原厂盖章）
	★支持自定义图表的能力，图表至少包括折线图，面积图，堆叠折线图，柱状图，堆叠柱状图，左右柱状图，环形图，嵌套饼图，数字块，关系图，面积地图，攻击地图，热力地图，地图要有全球地图，中国地图，省市地图；（投标时提供产品截图及原厂盖章）
	★支持自定义表格能力，至少包括查询列表，统计列表等；（投标时提供产品截图及原厂盖章）
	支持定制可视化大屏，仪表盘项可以灵活配置，可以通过导入升级仪表盘；
告警展示及处理	可以根据告警生成工单；
	支持工单的增删改查；
	支持工单确认，完成工单闭环处理；

	支持以告警页面、邮件、SYSLOG、SNMP Trap、脚本执行、短信、告警铃等各种方式输出告警；
	实现多维度告警检索，可以根据告警信息生成自定义报表展示；
	★具备同类告警合并策略，减少告警数量；（投标时提供产品截图及原厂盖章）
	具备显示当前事件和自定义时间段内的告警事件、告警级别、告警数量；
	告警与日志关联：支持将告警与产生该告警的日志信息进行关联展示，便于进行告警的进一步分析，支持将告警信息进行导出（导出的内容至少包括告警内容、告警对应的规则等），导出的格式至少包含 excel；
	支持告警铃自定义以及是否关闭功能；
系统监控	支持以图表方式（饼图、柱图、曲线图）显示当日日志数据采集情况；
	支持以图表方式显示近期安全事件及告警日志数据分布情况；
	支持实时监控系统当前运行状态，包括系统 CPU、内存、硬盘状态；
	支持对存储空间实时监视，图形化显示最新存储空间使用情况；
	支持存储空间超过设定阀值则系统自动报警，提醒管理者备份原始数据；
系统管理	支持系统自身管理记录；
	支持三权分立，用户、角色、权限配置；
	支持自动备份归档方式；
	支持资产管理，即所有采集日志源管理维护；
	★支持日志的数据的冷热模式切换，即基于时间索引的及时关闭和开启索引；（投标时提供产品截图及原厂盖章）
	支持根据磁盘空间大小超过阀值自动清理历史日志的功能；
	支持 FTP 备份方式对数据进行远程备份；
	支持日志、告警和知识库字段别名的修改；
	支持配置日志存储期限；
	支持日志和告警导出加密设置；
资质要求	《计算机信息系统安全专用产品销售许可证》、《软件产品证书》、《计算机软件著作权登记证书》
系统升级	在系统维保期内，厂家提供对系统软件的免费升级服务，保证系统软件为最新版本；

（2）主机防护

模块	功能	要求
形态部署	管理架构要求	★采用 B/S 架构设计，管理控制中心高度集成化，无需额外安装或外接数据库即可实现日志存储和分析展示，无需额外安装或对接升级服务器即可实现文件、特征库的升级和分发
	管理控制中心要求	★提供已加固的操作系统作为管理控制中心寄宿环境，保证管理控制中心自身安全；支持从老旧控制中心平滑迁移至新控制中心 ★提供控制中心多升级负载均衡，保证控制中心在集中升级时不会出性能瓶颈
	客户端要求	采用轻量级 Agent 部署，无需依赖虚拟化平台 API 即可实现安全防护；客户端支持手动从控制中心获取安装，也可通过管理控制中心批量远程安装；客户端对 windows 类、linux 类；物理服务器、虚拟服务器、桌面云具备相同的防护和部署模式 ★产品支持对已防护的主机统计在线率，对虚拟机是否安装客户端统

		计整体部署率，提供截图证明
	虚拟化平台支持	★产品应至少支持 VMware 、Ctrix、Microsoft、Huawei、H3C、浪潮等国内外主流虚拟化厂商平台，并能够采用一个管理控制中心进行统一管理，提供截图证明
	操作系统支持	产品应至少支持 Windows 7/8/10 等云桌面常见操作系统类型,Windows Server2003/2008/2012/2016 等虚拟化环境常见基于 Windows NT 的服务器操作系统； 产品应至少支持 SuSE、Red Hat、Ubuntu、Debian、CentOS、Asianux、NeoKylinLinux 等虚拟化环境常见基于 Linux 内核的操作系统
安全能力指标	文件防护要求	产品除支持一般性病毒木马查杀外，还应支持例如：宏病毒、敲诈勒索软件、注册表病毒、间谍软件、僵尸远程软件等特定恶意文件的查杀；除落地在本地文件系统中的文件外，对网络映射驱动器、移动存储路径、共享目录、局域网路径等扩展路径也能够进行扫描查杀 ★产品提供不少于 3 种病毒查杀引擎，可根据不同虚拟化环境和查杀要求灵活开启与关闭；同时产品应支持利用 CPU 虚拟化技术提升系统的安全防护能力，提供截图证明 提供主动防御保护，智能监控系统文件操作行为，利用文件审计关联技术，实时对病毒木马及恶意相关文件进行拦截和防护，特别是针对近期流行的敲诈者木马能够进行有效拦截 产品应提供对不同压缩包类型文件的监控防护，压缩包监控防护层级不小于 10 层，压缩包格式支持不少于 30 种，支持略过特定大小和特定层数的压缩包文件，并可以自定义添加或删除压缩包格式类型 产品应支持对病毒文件进行手动加白置黑操作，对目录、文件、扩展名进行信任操作，以提升查杀效率和降低误杀率 产品应支持对病毒扫描查杀进行资源占用限制和任务并发控制，防止引发启动风暴、扫描风暴，修改资源利用方式无需重启
	防护要求	★产品应支持防暴力破解，可对来自网络的暴力破解行为进行拦截，支持配置时间、破解次数等阈值，并提供暴力破解 IP 或 IP 段的黑白名单设置，提供截图证明 ★针对近期爆发流行的永恒之蓝攻击，能够进行有效防护，提供截图证明
其它管理要求	自动化运维	产品应支持自动化安全运维：支持自定义安全策略的定时、指定范围执行；支持对策略、主机组织结构、日志的手动或自动备份 支持手动或自定同步虚拟化平台组织结构 ★支持手动、自动升级系统文件、引擎版本、特征库信息，能够基于分组、时间设定灰度升级策略，提供截图证明 支持基于时间动态进行调整带宽和网络并发连接，减少控制中心升级对业务网络产生的影响 支持文件分发功能，可利用管理平台统一分发升级文件。
	Syslog 支持	支持 syslog 协议，将安全日志发送到第三方 syslog 服务器
	离线升级	提供在线或者离线升级方式，隔离网情况下能够采用离线工具进行更新
	LDAP 支持	支持 LDAP，将 LDAP 组织结构导入到本地用于本地系统管理
	展示与告警	支持动态展示安全事件并能够进行邮件告警
	多账号	支持不同账号设定不同的组织结构权限和策略使用权限
	报表订阅	支持报表订阅，能够对报表时间、内容定制、订阅信息等进行自定义

（3）安全服务

服务名称	主要内容	服务频率
等保测评	由第三方测评机构进行 1 个二级系统等保测评，并出测评报告；	1 次
安全设备巡检	对网络安全设备进行定期巡检，对全网进行风险探知扫描，识别和统计信息系统资产，并在之后对结果及相关参数进行详细记录。在发现隐患或故障后，在最短时间之内进行故障分析与排除，保证安全设备的正常运行。	每月 1 次
安全配置核查	对学校的重要资产进行抽样核查，并协助整改。	每季度 1 次
病毒跟踪	对内网恶意代码感染、传播情况进行跟踪和态势分析，分析病毒来源、种类、影响程度，提供防控措施，协助安全产品厂家解决问题。	即时
故障诊断解决处理	在安全设备发生突发故障或紧急事件时，运用专业故障处理流程，同时联系第三方技术支持人员迅速对故障进行定位、检测、排除，并记录故障相关细节，在故障排除之后加强对此类故障的预防措施并进行日后的统计分析，防止类似故障的再次发生。	即时
安全预警	对最新发布的安全漏洞及时发布重要的安全通告，包括硬件厂商、操作系统及中间件、官方及非官方主流安全组织或平台的安全通告等。	即时
应急处置	进行日常网络安全应急处理，在攻击演练、重大节日、敏感时期及必要时间段安全值守，针对发现的攻击事件，利用现有防御措施第一时间阻断并进行应急响应；分析攻击源 IP、攻击路径、攻击目标等并进行攻击行为取证。	即时
信息安全培训	协助学校进行信息安全专业技术培训。	每季度 1 次
安全咨询服务	对学校安全管理体系包括安全管理制度、安全管理机构、安全人员管理、系统建设管理与系统运维管理等相关方面进行问题梳理，完善安全管理体系。	即时
安全检查	定期协助学校网络信息安全管理部门进行网络安全检查工作。	即时
协助工作	协助客户进行等保测评及整改	即时