采购项目询价清单

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 规格 | 数量 | 单位 | 单价 | 合计金额 |
| 1 | 安镜网络安全态势感知通报预警处置平台V2.0 | 1，支持含100点设备日志源接入授权，。  2. 要求支持与省厅及市 级安镜平台级联，能及时获取上级安镜平台派发任务及应急响应要求，并支持直接数据上报；  3. 支持syslog，sftp，jdbc标准日志接口和agent本地采集。  4. 要求与信息网“一机两用”系统进行对接，实现联动及获取现有保护，信任等设备信息。  5. 支持从多个安全设备、系统中采集日志并关联分析生成应用审计、数据库审计报告，报告支持模版设 计且内置至少3份审计报告模版，设备系统至少包括云桌面、堡垒机、桌管应用系统、数据库审计系统、上网行为管理、防火墙等。  6. 内置知识库系统，允许用户进行知识管理；用户可对所有的知识点进行基于关键字的全文检索。知识库可与采集日志关联查询，知识分类不少于5中，包括：案例库、漏洞库、事件库、文档库、字典库等  7. 内置工单系统，可自动将日志生成工单；允许用户将工单派发给指 定的处理人，工单处理人在接收到工单后可以记录工单的流转信息和状态信息。管理员可以查看所有的工单及其流转的全过程，能够对工单的数量、状态（处理情况）等进行统计分析。  8.产品需与违规外联检测系统无缝对接。 | 3 | 套 |  |  |
| 2 | 北信源防病毒系统V3.0 | 1、 系统支持控制中心支持多级级联部署，并支持病毒查杀日志上报和所有类型病毒库统一升级；并且具有良好的级联拓展能力，有良好的可扩展性和易用性，支持多级级联架构，支持大型网络跨地域、跨网段的部署和管理。  2、 系统支持展示客户端所有终端的操作日志，如：通过时间戳，终端名 称、操作类型（包含基础操作、文件监控、自保护、防护级别改变、白名单和隔离区、各类扫描操作等操作类型）、触发方式等信息，筛选完成后，可导出报表。  3、 设备信息支持上报至业务系统综合安全管控平台，实现数据统一汇总展示、分析、关联发现潜在风险  4.系统支持文件通过添加MD5、拓展名、路径方式的加白，可进行批量导入导出以及对不同分组设置不同白名单。  5.具备边界防护能力，对网页访问、浏览器下载、U盘拷贝等系统入口实时监控，拦截危险文件的落地  6.要求与信息网“一机两用”系统进行对接，实现联动及获取现有保护，信任等设备信息。  7.产品需与违规外联检测系统无缝对接。 | 1 | 套 |  |  |
| 3 | 内网安全管理系统V6.8 | 1，具备统一防火墙功能，可根据IP地址或域名、协议、端口控制终端网络访问权限；支持对于数据流向的控制，可以对出站和入站分别进行允许和拒绝链接；可以实现针对域名和IP地址的禁止通讯，支持超级端口和超级IP，可以不受黑名单中的管控。  2、支持进程黑白红名单控制；支持进程监控，可从黑白红名单库中选择进程或者手动添加；支持进程执行询问功能，用户可选择是否运行进程，并能对违规行为处理选择进行断开网络、告警提示、或不处理等操作；支持服务黑白红名单控制；支持服务监控，可从黑白红名单库选择服务名 称或手动添加，并能对违规进行为处理选择进行断开网络、告警提示、关机或不处理等操作  3、支持根据进程名 称、进程路径、源文件名 称、文件版本、产品名 称、公司名 称、数字签名、MD5对进程组合识别，确保软件运行控制准确有效  4、支持进行客户端防病毒软件检查，能够识别市场多种常见杀毒软件，监控防病毒软件在客户端的安装情况，对没有安装杀毒软件的计算机进行处理，如告警、断网，关机  5、支持主动防护，对系统关键点、注册表、驱动加载、程序防注入及进程等敏感系统位置的实时监控，拦截来自危险文件的风险攻击，支持主防锁定，防止终端用户手动修改配置从而降低终端安全防护系数；同时也支持对下载、U盘及上网的实时保护  6、设备信息支持上报至业务综合安全管理系统，实现数据统一汇总展示、分析、关联发现潜在风险  7、支持文件监控功能，在平衡系统性能和安全的关系时，可选择强效模式、高、中、低等监控类型；  8.要求与信息网“一机两用”系统进行对接，实现获取公安现有保护，信任等设备信息，及写入保护设备，避免跨部门间访问被阻断。  9.支持与上级政法委终端安全管控系统对接，实现级联管控 | 2 | 套 |  |  |

**合计金额：**

**报价单位（盖章）：**

**联系人：**

**日 期：**