《日志收集与分析系统》要求明细

一、产品质量要求

1.中标供应商交付货物时须提供制造厂商正规渠道货物来源证明，以保证货物质量，否则，追究相应损失责任。

2.中标供应商提供的设备必须是相应设备合法生产厂家的合格产品，必须符合国家检测标准以及出厂标准，必须是全新软件，采购单位凭检验合格证验货，拒收验收不合格产品，一切损失概由供应商负责。

3.质保期(验收合格后开始计算):软件保修:不得小于12个月，质保期内，提供运维服务和软件版本及固件免费升级服务。

二、售后服务要求

在质保服务期内，中标供应商须提供24小时服务热线电话和紧急联系人，采购人有任何疑惑或问题，可用电话或其他形式通知，在5分钟内给予响应，在10 分钟内到达现场，30 分钟内排除故障。

三、安装要求:

软件安装调试由中标供应商负责，安装调试过程中需要的所有配件由中标供应商负责，中标供应商应严格按照采购人的施工要求进行，同时，采购人有权派出技术人员参加，中标供应商有义务对其进行指导。

四、付款方式

安装调试完成并最终验收合格后，支付80%，维保期结束后支付20%。

五、技术要求

1. 包含资产管理、日志采集、日志归一化、日志存储、日志查询、实时分析、关联分析、关联告警、统计报表功能，配置≥50个日志源授权节点。

2.支持通过 syslog、SNMP Trap、JDBC、文件\文件夹读取、Kafka等多种方式完成各种日志的收集功能;

3.支持资产管理，可显示资产IP地址地理信息并进行管理，支持单个IP、IP段设置行政区及经纬度，支持地图显示;

4.支持自动识别收集的日志并自动选择范化策略，也可由人工设置设备的范化策略。针对匹配的多条范化策略，系统支持用户手工设置策略匹配优先级;

5.支持日志交互式分析，点击事件任意属性字段，可以该字段为条件对事件进行统计分析，并展示Top 20排序，排序支持正序和倒序，并可对统计内容进行点击;

6.支持提供安全运维报告，帮助运维人员快速生成日常日志分析和运维报告;

7.支持对关联规则进行监控，了解该规则命中历史情况;

8.支持采用语境关联分析引擎技术对异常行为进行分析识别，以保证日志分析能力及效率；

9.支持任意品牌安全产品、网络产品、应用系统等的日志收集归纳到达公安部等四部委关于等保2.0中日志收集的相关要求。