# 国家税务总局萍乡市税务局关于“赣税安”平台网络安全探针的采购要求

# 第一部分 商务条款要求

## 1.1、供应商资格要求

符合《中华人民共和国政府采购法》第二十二条的规定，符合《关于规范政府采购供应商资格设定及资格审查的通知》第六条规定且已在本系统注册并通过资质初审的供应商。

## 1.2、项目周期要求

因工作需要，需中标供应商在竞价结束5个工作日内完成产品安装调试。

### 1.3、项目实施要求

本项目须与国家税务总局江西省税务局“赣税安”网络安全管理平台级联对接，与本项目所涉及的软硬件集成连通，并完成软硬件部署及测试联调，达到稳定、流畅等项目预期需求和性能。

## 1.4、售后服务保证

1. 竞价结果出来之后，中标人须在合同签订前提供以下证明材料：

（1）针对本项目的原厂质保服务承诺书原件（加盖原厂商鲜章）；

（2）标注“★”项的技术要求和资质要求，中标人须提供设备原厂商出具的证明材料，如检测报告或截图等（加盖原厂商鲜章）。不能提供的，采购人有权不与中标人签订合同，取消中标人中标资格。

1. 招标人有权要求中标人在中标公示前对技术参数进行实际测试，如未通过实际测试而又在投标文件技术偏离表做无负偏离说明的，将取消其中标人资格。

# 产品技术参数要求

**注**：标“★”项为重要性指标，必须满足

|  |  |  |
| --- | --- | --- |
| 序号 | 设备名称 | 技术参数（基础参数）技术要求及指标 |
| 1 | 分布式性能采集探针 | 1、支持另外部署的分布式性能信息采集器，每个采集器都能对所辖片区资产的性能信息进行采集，并统一上报管理中心，实现集中化的性能与可用性监控；  ★2、性能采集器采用B/S架构设计，有独立的管理界面，通过浏览器可以登录到性能采集器上进行查看和配置，可以查看采集器上每个监控器的监控快照和性能指标数值；  3、性能采集器可以运行在Linux环境下；  ★4、性能采集器至少支持SNMP、TELNET、SSH、SSH2、ODBC、JMX、协议仿真等7种方式对IT资产进行性能与可用性信息的周期性采集；   1. 管理中心具备对多个性能信息采集器的集中管理功能。   ★6、设备相关信息日志可以与江西省税务局“赣税安”平台对接。 |
| 2 | 分布式事件采集探针 | 1、系统支持独立的日志采集器用于日志的采集、处理、范式化、日志源管理和传输等过程，进行分布式部署；  2、日志采集器采用B/S架构设计，有独立的管理界面，通过浏览器可以登录到日志采集器上进行查看和配置，能够对当前采集器进行配置，能够监视采集器所在服务器的运行状况、设置采集器的时钟同步服务器；  ★3、支持Lotus Domino、Check Point、VMWare的日志采集任务，支持定制任务进行日志数据采集扩展，包括文本格式、目录下文本和数据库格式日志采集，支持编辑正则表达式和SQL语句进行日志采集，支持设置自定义任务时间；  ★4、支持SNMP、Syslog、ODBC/JDBC、文件/文件夹、WMI、FTP、SFTP、SMB、NetBIOS、OPSEC等多种方式完成日志收集功能；  ★5、支持内置Cisco PIX和交换机的事件编码知识库；内置Windows、Linux、Solaris、AIX操作系统的事件ID知识库；内置Oracle、SQL Server、MySQL、Informix、DB2数据库的事件错误号；能够查看系统内置的事件库中事件类型名称及其描述信息；内置等级保护知识库；内置病毒爆发、网络攻击、网络拥堵、网络扫描、设备故障、系统瘫痪、信息泄密等案例库；  ★6、支持交互式事件分析模式，支持过滤条件和高级搜索模式方式查询，其中过滤条件查询可以对任意日志字段设置禁用、取反等操作；高级查询模式查询支持单一条件和组合条件复杂查询；  ★7、支持基于规则的关联分析引擎，能够提供逻辑关联、统计关联的关联分析能力；关联规则支持规则嵌套和引用，支持多规则联合；  ★8、设备相关信息日志可以与江西省税务局“赣税安”平台对接。 |
| 3 | 分布式基线核查采集探针 | 1、支持检查的内容包括但不限于账号、口令、授权、日志审计、不必要的服务、启动项、注册表、会话设置等配置。  2、支持在线和离线两种任务扫描方式。  3、支持AGENT、TELNET、SSH、SMB、RDP、WinRM协议的在线核查方式以及串口方式进行安全基线配置检查。  ★4、提供针对windows和linux系统类型不合规检查项的在线加固能力，可针对单一检查项加固，也可以批量加固不合规项。  ★5、支持配置变更监测，周期性监测系统的文件、目录、注册表、启动项、进程等配置信息及变更状态，支持检查项设置权重、规范来源及告警配置。  ★6、支持对无法立即得出是否合规的检查项，提供人工参与判定的机制，并把判断结果作为下次检查的标准。  ★7、支持配置变更检查，可以根据实际情况设置任意检查结果作为变更基线，支持与自身或者其他设备的同类型变更项进行对比，检查设备间核心配置项的异同之处。  ★8、设备相关信息日志可以与江西省税务局“赣税安”平台对接。 |
| 4 | 威胁检测探针 | 1、2U机架式设备，实际网络环境处理能力≥3G，每秒新建连接数≥4万，最大并发连接数≥300万，内存≥16G，硬盘≥2T，千兆电口≥8个（包含管理口），千兆光口≥4个，扩展槽≥2个，冗余电源；  2、支持导入HTTPS、POP3S、IMAPS、SMTPS、RDPS证书，对加密流量进行解密及还原：支持SSL3.0，TLS1.0/1.1/1.2  3、支持对常见的拒绝服务攻击（DDOS）的检测能力，针对TCP FLOOD、UDP FLOOD、ICMP FLOOD攻击行为进行检测，并支持通过控制界面配置攻击的检测时间和阈值条件；  ★4、基于网络全流量分析技术，对网络所有数据进行安全分析。通过对网络链路全流量采集、全数据分析，对网络异常行为有敏锐的感知能力，具备多维数据索引能力，能够对网络攻击进行定位与取证：  ★5、具备通过web页面导入pcap包离线回放检测能力，单个导入回放的数据包最大支持1G，支持批量导入或选择文件夹导入，支持选择回放流量业务口；  ★6、支持自定义规则，可结合用户业务进行深度检测，自定义内容包括源IP、源端口、目的IP、目的端口、协议、事件威胁等级、主机状态、事件类型、攻击阶段、攻击结果、攻击手段；支持关联规则分析，进行双向检测规则编写，兼容业界主流snort规则；  ★7、支持程序具备AI引擎自动对攻击进行威胁情报云查，页面自动呈现情报云查信息，查询结果至少包含：威胁等级、标签、威胁类型、IP地址、IP类型、活跃时间、发现时间、国家、地区、运营商、ASN号、ASO号、开放端口、恶意端口等；  ★8、设备相关信息日志可以与江西省税务局“赣税安”平台对接。 |

# 第三部分 重要说明

3.1、投标供应商必须满足该技术指标要求，如被证明不满足要求或者无证据其满足，将视为不符合本项目要求，属未进行实质响应，采购人可拒绝签订合同，并有权按照无效标处理；

3.2、采购人在竞价结束后或签订合同前有权要求供应商提供商务条款与产品技术参数条款中所述的证明文件，如供应商不提供或无法证明其满足的，采购人有权废除供应商中标资格或终止合同，并追究供应商相关责任。

3.3、付款方式：根据项目验收情况，双方协商。

3.4、推荐品牌：启明星辰、网御星云，新华三（H3C）。

3.5、竞价单位提交在线竞价文件时需提供采购方带鲜章的《实施现场调研函》电子扫描件,文件内容参考如下模板：

实施现场调研函

致：国家税务总局萍乡市税务局

我司有意参与贵单位组织的国家税务总局萍乡市税务局“赣税安”平台对接设备采购项目的在线竞价工作，兹委派我司项目负责人 （身份证号： ），按竞价文件规定要求于 2024年 月 日到国家税务局萍乡市税务局现场勘察。请予以证明。

感谢！

竞价单位：

日 期：

为保障实施工作的快速开展要求，竞价单位需对项目现场进行实地调研。现竞价单位已进行实地调研，获得该项目实施交付所需要相关信息和资料。

1.经现场调研，该投标单位对该项目现场现状已充分了解。

2.该竞价单位若中标，不对场地现状提供异议，不以实施环境缺失、条件不充分等因素为由拒绝签署项目合同书或履行所约定的各项义务。

特此证明！

竞价单位： 采购单位：国家税务总局萍乡市税务局

日 期： 年 月 日 日 期： 年 月 日

注：本文件一式三份，采购单位留存两份，竞价单位留存一份，提交在线竞价文件时竞价单位需提供采购方带鲜章的本文件电子扫描件，中标后签订合同时本文件作为附件装订。