# 项目概述

## 项目背景

根据《网络安全法》、《国家税务总局关于强化税务系统网络安全的意见》（税总发〔2019〕123号）和《国家税务总局网络安全和信息化领导小组办公室关于全面推进网络安全态势感知平台应用的通知》（税总信息办便函〔2022〕30号）的要求，我局需进一步提升网络安全和数据安全防护能力，健全完善网络安全和数据安全综合防控体系，开展日志服务器升级、态势感知平台升级和网络安全准入系统升级等工作。

## **项目内容**

（一）日志服务器升级

根据《网络安全法》和《国家税务总局网络安全和信息化领导小组办公室关于落实网络日志留存工作的通知》（税总信息办便函〔2018〕72号）的要求，网络运营者应采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于6个月。为有效开展日志采集分析工作，实现对网络日志的收集、保存和分析，有必要升级完善日志分析平台。

（二）态势感知平台升级

根据《国家税务总局网络安全和信息化领导小组办公室关于全面推进网络安全态势感知平台应用的通知》（税总信息办便函〔2022〕30号）的要求，各省税务局要积极探索创新态势感知平台“小而美”的功能应用场景。因此，有必要升级态势感知平台，深化扩展态势感知平台的数据安全检测、分析和排查等功能。

（三）网络安全准入系统升级

根据2022年税务总局数据安全专项核查工作的要求，各省税务局必须实现Windows终端和国产化终端的网络准入进行控制。因此，有必要升级网络安全准入系统，确保准入系统符合税务总局数据安全相关要求。

# **投标/响应要求**

投标/响应要求主要包括供应商资质要求、投标/响应产品资质要求、投标/响应文件技术部分的响应内容要求等。

1.供应商资质要求包括供应商必备的资质及优选资质、是否允许联合体投标等。拟采用单一来源方式采购的项目，需列明单一来源的供应商及单一来源理由。

2.投标/响应产品资质要求包括投标/响应产品必备资质及优选资质（安全产品的销售许可证、原厂售后服务承诺函等）。

3.投标/响应文件技术部分响应内容要求一般包括对产品指标的响应要求和对服务的响应要求。

产品指标响应要求需列明产品指标的种类（必备指标、重要指标、一般指标等）、标识（一般★号指标为必备指标、▲为重要指标、无标识的为一般指标）和响应要求。

服务的响应要求指供应商依据业务技术需求需响应的服务方案及内容，一般包括项目需求理解、集成服务方案、技术支持服务方案、售后和质量保障方案、实施方案、验收方案、知识转移方案等，并列明供应商需响应各个方案的具体内容。

# **项目需求**

|  |  |  |  |
| --- | --- | --- | --- |
| **一、项目要求及技术需求** | | | |
| **序号** | **产品名称或标的名称** | **数量及单位** | **项目要求及技术需求** |
| 1 | 日志管理与分析平台 | 1套 | 1、★平台配备不少于2台硬件服务器，每台服务器配置不低于：cpu：24核48线程；内存：256G；磁盘：系统盘480G\*2RAID1(企业级SSD)、数据盘8T\*5 RAID5，网口：4千兆电口+2万兆光口。  2、★平台日志源授权不少于700点；  3、平台能独立完成审计日志采集，不依赖于设备或系统自身的日志系统；日志审计工作不影响被审计对象的性能、稳定性或日常管理流程。  4、▲平台支持集群部署，支持计算和存储服务的横向动态扩容，不影响日志管理平台的正常业务运行；（投标文件中提供相关截图证明）。  5、平台综合日志处理速度≥50000EPS（投标文件中提供第三方权威检测报告）。  6、平台可通过Syslog协议进行日志收集，要求能够保证现有防火墙日志、NAT日志、会话日志、威胁日志等信息保存时间超过180天，同时能对接现网其他安全设备日志信息。  7、平台支持日志等级进行过滤；支持对收集到的重复的日志进行自动的聚合归并，减少日志量，支持由用户定义和修改的日志的聚合归并逻辑规则；  8、平台支持通过Syslog、SNMPTrap、HTTP、JDBC、WMI、FTP、SFTP等协议开展日志收集；支持使用代理(Agent)方式提取日志并收集，agent采集代理支持统一批量下发安装、卸载。  9、▲平台具备日志自定义查询条件功能，日志解析字段不少于300个，解析规则可以根据客户要求定制扩展。实现可指定多个查询条件进行组合查询，内置5000+解析规则，支持对收集的5000+设备类型日志进行解析（标准化、归一化）（投标文件中提供相关截图证明）。  10、平台日志查询支持可视化展示，支持对查询结果任意字段进行点击即可统计分析，同时生成可视化统计分析图表，至少包括柱状图、饼图、折线图、散点图、表格等形式，检索百亿条日志查询，响应时间小于1秒；（投标文件中提供相关截图证明）  11、平台支持对设备的可用性状态监控，包括CPU、内存、硬盘（包括NFS存储），支持各类型日志、各设备日志接收趋势统计，支持对设备磁盘可用存储空间监控。  12、平台根据三权分立的原则和要求进行职、权分离，系统自带自身管理日志；支持用户隔离，不同的用户管理不同的日志资产，满足资产管理、日志数据、审计报表、仪表盘，告警的隔离。  13、▲平台支持集群节点的在线运维，在线节点性能监控，在线配置更新和组件间的健康检查以及灾难自动恢复；数据存储支持动态扩容、冗余、高可用，支持数据的多分片和多副本配置。（投标文件中提供相关截图证明）。  14、★产品具备公安部颁发的产品销售许可证，具备网络关键设备和网络安全专用产品安全认证； |
| 2 | 智能内网威胁感知平台 | 1套 | 1、平台能够对接入的业务系统支持展示风险员工、风险设备、风险业务系统、风险账号、风险IP、告警事件数据的统计及TOP5统计，支持展示与昨日对比的风险趋势，展示风险员工和风险设备等级评分。  2.平台支持对接入系统按照杀伤链阶段（网络攻击生命周期）进行告警分析，支持不少于7个杀伤链阶段，包括但不限于侦查跟踪、武器构建、载荷投递等，并可进行详细信息的下钻，支持告警事件类型TOP5统计。（投标文件中提供产品功能截图）  3、平台支持对接入系统的告警进行多维统计分析及3D展示，包括但不限于风险员工、风险设备、风险业务系统、风险账号、风险IP等。支持对系统的告警进行TOP5分析展示，包括但不限于员工风险评分、设备风险评分、告警事件类型、告警事件次数、高危业务系统、高危账号、高危IP等。  4、★平台支持对接入系统使用的用户行为进行分析，支持对风险员工的行为进行用户画像分析，包括但不限于常用资源（常用账号、常用设备、常用IP）、邮件往来、内部资源使用等。支持对风险员工的网络活动进行统计监测，常访问的域名、应用协议使用、常访问业务系统、常访问安全域、常访问URL类型、常访问数据库、常访问设备IP/端口。支持对风险员工的通联关系进行分析，支持以可视化关系图表方式进行展示。  5、平台支持对接入设备行为进行分析，以多维度对设备进行画像分析，包括常用资源（常被访问端口、常用浏览器、常用账号、部署业务系统、常被使用员工、常使用IP）、日常活跃情况（协议组、HTTP）、30天流量分布、主动外联行为（访问内外IP、访问业务系统、访问数据库、访问安全域）、被动外联行为（内外源IP、内外访问端口、外网源IP）。（投标文件中提供产品功能截图）  6、平台支持对接入的业务系统进行风险分析，支持对高风险业务系统进行监测；支持展示全部业务系统的告警次数、组织机构、业务系统名称、告警事件涉及的风险标签。支持展示业务系统风险详情，展示内容包括但不限于业务系统档案基本信息、近10日风险分布趋势图、告警事件、通联关系等；支持以时间轴的形式展示告警事件；支持可拖拽关联关系图。  7、★平台支持多维度的对内网实体（用户相关的应用和终端等）外联分析，包括外联会话流量占比、外联行为地理分布、外网行为关系展示、外联行为列表、资产外联次数排名、外联目标排名、外联行为趋势、访问时间段分布等。支持基于世界热力地图进行外联行为地理分布，支持分析时间范围设定。  8、★平台支持多维度的对内网实体（用户相关的应用和终端等）外联心跳行为分析，包括资产外联列表、外联目标列表、心跳类型占比、心跳时间分布、应用协议心跳、传输协议心跳、心跳事件列表等。支持基于时间序列散点图进行心跳时间分布展示，支持通过散点面积大小展示心跳行为数量多少，支持分析时间范围设定。  9、平台支持对行为审计数据进行可视化场景分析，包括网络活动情况、内网资源访问情况、热门资源访问情况，网络活动情况包括总会话数、总协议种类、源IP数、目的IP数、访问域名数，内网资源访问情况包括域名数、数据库数、URL数、文件数及变化趋势图，热门资源访问情况包括域名、URL、文件、数据库、IP等。  10、平台支持高级模式数据检索，可通过SPL语法输入检索条件，包括但不限于：全文检索、结构化检索、组合过滤、排序子句、限定查询范围、限定查询字段等。支持检索条件保存为策略，可查看检索策略列表，可将检索策略添加到检索条件进行数据检索。  11、平台支持事件时间变化趋势图表化展示，支持图表下钻展示更细粒度时间数据，其它图表数据将联动刷新，支持返回上级时间粒度展示。  12、平台支持对接入设备下发联动策略，支持按条件查询联动策略；支持联动策略列表展示，展示字段包括策略名称、描述、联动设备名称、类型、厂商、软件版本、策略状态、执行状态；支持对策略进行添加、启停、编辑、删除等操作；  13、★平台支持按分析引擎类型及专题场景对智能分析模型进行总体概览，分析引擎类型包括关联分析、行为分析、深度分析，专题场景包括外联分析、IP活跃分析、横向移动、DNS异常、异常时间活跃、零信任，专题场景包括至少20种二级场景，包括但不限于恶意外联、频繁变更、异常请求、静默行为等。支持专题分析和模型列表的信息下钻。支持模型的启用和停用。  14、平台支持基于算子拖拽式自定义添加关联分析模型，支持至少4大类15种算子，包括但不限于事件选择、事件筛选、事件关联、事件统计；支持对模型进行基础设置、安全事件设置、告警事件设置，基础设置包括启用状态、模型专题、分类、ATT&CK、描述，安全事件设置包括事件名称、类型、主体、风险评分、事件标签、描述、处置建议，告警事件设置包括威胁分数、归并字段、告警限制，模型响应设置包括生成情报、生成知识、删除知识、触发剧本。支持模型测试。  15、平台支持基于行为基线检测原理自定义添加行为分析模型，支持行为定义，包括但不限于行为数据来源筛选、行为主体选择、行为客体选择、度量字段及算法设置，度量周期设置；支持多种个体比较检测算法设置，包括集合偏离行为检测算法、阈值行为检测算法。支持对模型进行基础设置、安全事件设置、告警事件设置，基础设置包括启用状态、模型专题、分类、ATT&CK、描述，安全事件设置包括事件名称、类型、主体、风险评分、事件标签、描述、处置建议，告警事件设置包括生成状态、生成情报、生成知识、删除知识，支持模型测试。  16、★平台支持至少内置10种深度分析模型，包括但不限于恶意参数识别、基于图算法的孤立页面检测、钓鱼邮件识别等，支持查看模型的基础设置、安全事件设置、告警事件设置，基础设置包括启用状态、ATT&CK，安全事件设置包括主体、风险评分、事件标签、描述，告警事件设置包括生成状态、生成情报、生成知识、删除知识，支持模型测试（删除）。支持对模型原理进行说明。  17、平台支持自定义解析模板，支持按照标准和高级两种模式进行模板配置；支持基于关键字特征和正则表达式进行特征匹配；支持至少10种字段提取规则，包括但不限于字符串分割、KV提取；支持选择标准字段进行泛化操作；至少预置5种富化规则，包括但不限于DHCP映射、杀伤链事件定位库；支持通过与或逻辑进行字段过滤  18、平台支持对使用系统用户的行为审计，包括最近登录用户、最近登录用户次数排名、最常用使用功能菜单占比的数据统计；支持对用户行为查询及列表展示，查询字段包括用户名、业务模块、客户端IP、操作结果、时间，支持对审计列表的导出和存储周期设置。 |
| 3 | 终端安全准入系统 | 1套 | 1、★硬件配备不少于2台设备，每台设备配置：标准机架式设备≥2U、板载≥6个千兆电口、USB口≥2个、配置一个RJ45串口、配置≥4TB硬盘，支持网卡扩展插槽。  2、★系统使用专用安全操作系统，支持管理windows以及信创用户终端的安全准入。支持不小于1600个终端准入认证接入。  3、系统支持对全网终端或指定范围终端进行准入管理,系统支持对客户端准入进行认证授权，支持对客户端的合规性、完整性进行安全检查。  4、▲系统支持硬件服务器部署形态，集成网关准入、802.1x准入、Portal准入、DHCP准入等管理模块。系统部署方式支持网桥方式、旁路镜像、策略路由部署等方式，支持NAT形式的地址转换环境。  5、系统支持实现终端安全准入系统由现有终端安全管理系统中心统一纳管，通过终端安全管理系统中心实现对终端安全准入系统策略配置及策略下发等功能。  6、系统支持手动和自动两种入网审批方式，审批通过的才能入网。支持审计所有入网审批操作记录。  7、系统支持根据终端的MAC地址设置准入例外，例外列表中的设备无需进行认证也可以顺利通过访问网络。  8、系统支持内置用户系统认证入网用户身份，支持口令、UKEY至少两种认证方式。  9、系统支持通过第三方认证源认证入网用户身份，至少支持AD域、Ldap认证。支持将AD域或LDAP的组结构和用户信息导入到系统用户列表。  10、系统支持是否开启身份认证，关闭身份认证，终端只需安装客户端，不需要用户输入口令即可入网。（投标文件中提供产品功能截图）  11、▲系统支持身份认证通过与失败后的处理方式，认证通过后的处理方式，至少包括自动发起入网申请、放行。  12、★系统支持通过设备MAC、认证用户、用户组、入网交换设备IP及端口、入网无线设备IP及SSID、是否安装客户端等条件组合，生成终端及用户的入网绑定规则，符合规则才能入网。  13、系统支持通过数据包的IPID、客户端在线、UDP探测、小路由方式判断终端合法性。（投标文件中提供产品功能截图）  14、系统支持对未安装客户端的终端支持页面重定向，重定向页面可自定义配置页面展示内容和布局。  15、系统支持配置例外终端，对于例外列表中的计算机或特殊网络设备，即使未安装客户端也可以顺利通过准入。其中，移动终端支持通过识别数据包的关键字进行例外，可下线不活跃的移动终端。  16、★系统支持无客户端准入管理，支持管理员为用户分配用户名（账号）和密码（口令），以及账号的有效时长，实现终端用户的临时入网，支持设置重新认证时长。  17、★系统支持编辑临时用户《入网协议》。可以在入网终端上提交入网申请，由管理员审批通过后才可以入网。申请单内容支持自定义，管理员可根据本单位实际业务情况修改申请单采集内容。  18、系统支持无客户端准入管理，支持管理为用户分配用户名（账号）和密码（口令），以及账号的有效时长，实现终端用户的临时入网，支持设置登出时长。  19、系统支持DHCP模式下动态分配IP，可设置访客IP网段和工作IP网段，支持配置最长租期。其中，未安装客户端的终端可获得临时访客IP，已安装客户端的终端自动获得正常工作网段IP。  20、系统支持设置保留IP与MAC地址绑定，当绑定的终端上线时，确保保留IP地址分配给此终端。  21、系统支持查看IP地址资源分配情况，包括地址池的大小、使用率、已安装客户端的统计。（投标文件中提供产品功能截图）  22、系统支持审计IP地址的分配及释放情况，并显示关联的终端。  23、系统支持开启或关闭802.1x准入认证，支持radius服务器认证配置，应同时支持有线、无线连接入网终端的准入认证；管理员可以查看Radius服务器基础信息和活动情况。  24、▲系统支持正式用户、临时用户、访客用户三种身份角色列表。正式用户主要用于有客户端的终端进行身份认证，正式用户列表具备用户组和用户的建立、修改、删除、导入，用户支持移动组；可以对用户进行启用和停用，支持有效期设置；支持为每个用户签发证书、下载证书用于用户制作UKEY身份认证。支持定义用户角色，用户密码复杂度配置。临时用户、访客用户主要用于无客户端的终端，通过WEB页面进行身份认证，通过管理员审批才能入网。临时用户列表支持对用户组和用户的建立、修改、删除、导入，用户支持移动组；可以对用户进行启用和停用，支持有效期设置；支持定义用户角色。 |

# **其他要求**

|  |  |
| --- | --- |
| ★合同履行期限 | 合同签订后30天内交货；设备到货验收后30天内完成安装调试。技术支持、售后服务及质量保障期3年，从项目验收合格之日起计算。 |
| ★交货地点 | 广西区内采购人指定地点。 |
| ★报价要求 | 投标报价指货物、标准附件、备品备件、专用工具、运输、安装、调试、验收等各种费用和售后服务、税金及其它所有成本费用的总和。 |
| ★项目系统集成要求 | 1、 中标人须完成中标产品的安装调试、线缆部署等系统集成工作，本项目采购的设备的相应配件（譬如光纤线、电源线等）若与使用单位环境不符，中标人及中标品牌厂家需更换为符合环境的同等或更高级别配件；部署新增软硬件设备不得对现有系统造成影响，不得影响业务系统正常运行；  2、 中标人在实施前，须提供详细的安装实施方案给采购人审核，经采购人确认后，方可进行项目实施。中标供应商完成所供软硬件的安装部署还需根据采购人的要求按成以下集成工作：  （1）根据网络安全设备现有实际情况设置相关策略，完成新购设备的安装部署调试工作；  （2）对新购产品设备与现有网络安全相关软硬件设备环境进行集成联调及调优工作；须与采购人系统内网络安全相关软硬件设备的服务商等进行积极主动的合作，服从采购人的统一协调，完成项目的各个阶段；实施部署完成后提交采购人完整的配置文档。  （3）安装部署阶段,至少提供具备3年以上网络安全行业从业经历的3名服务工程师保障本项目的实施工作，其中一名工程师需是所供产品原厂工程师,一名工程师需获得CISP注册信息安全专业人员证书。 |
| 售后服务要求 | （1）安装实施服务：中标人必须按照本项目的要求，完成中标产品的安装部署实施工作。要求中标人确保中标产品能在采购人现有网络环境安全、可靠、稳定的运行，不影响现有业务系统的正常使用；实施过程中如中标产品可能会对现有业务系统有重大影响的，中标人应提前三天将涉及到这个环节的实施方案提交给采购人，经过采购人认可并商定实施时间后，方能按照商定的时间进行实施。  （2）质保期内技术支持服务：提供7\*24小时技术支持服务，电话服务请求的响应时间应少于1小时，在接到报故障后，应在2小时内派技术人员到现场，进行故障排查及修复工作。在质保期内由中标人提供中标产品的定期升级服务；对于软件版本的重大升级，需由原厂技术工程师亲自上门实施，确保中标产品的稳定运行；  （3）异常故障分析服务：采购人的网络环境发生调整导致中标产品不可用时，中标人要协调原厂技术工程师提供紧急现场服务，1小时内到达指定现场，分析故障原因并提出解决方案，故障处置过程复杂的，原厂技术工程师要提出临时解决方案，确保采购人网络的正常运行。  （5）培训服务：中标人负责对采购人指定的技术人员进行技术培训，培训内容包括产品操作、维护、简单维修和其他采购单位要求的内容，经培训应能进行日常运行维护工作。 |
| ★付款方式 | 签订合同之日起 15 个工作日内，采购人预付款合同总金额的50%；所有货物验收合格并交付正常使用后，采购人根据项目验收标准及本项目合同罚则条款进行考核，按考核结果对合同服务费进行核算后，15 个工作日内支付合同剩余款项。  采购人付款前，中标人应向采购人开具等额有效的增值税发票，采购人未收到发票的，有权不予支付相应款项直至中标人提供合格发票，并不承担延迟付款责任。 |
| 验收方式及标准 | （一）验收条件  本需求书中包含的设备按期完成安装、部署、配置，以及组织管理和项目文档满足本采购文件的规定要求。  （二）验收标准  以本需求书中相关内容及其要求为依据，作为项目验收标准。供应商是否按照本招标需求书中定义的各项要求开展各项设备安装部署工作，工作流程和结果是否符合采购人质量管理要求，是否在规定时间内提交相关工作文档。  （三）验收流程  符合项目验收条件后，供应商可提出项目验收书面申请。向采购人提交验收申请。向采购人整理提交项目相关管理、技术文档。  采购人对项目工作内容及文档进行验收，项目验收通过后，采购人出具项目验收报告。 |
| 安全保障和罚责要求 | ★1.信息安全保密要求  （1）中标人须严格遵守国家税务总局广西壮族自治区税务局的安全保密制度。  （2）中标人投入的项目人员须保证遵守国家有关版权和知识产权保护的政策、法律、法规和制度。  （3）中标人投入的项目人员应对本项目中接触到的国家税务总局广西壮族自治区税务局所有的知识产权、商业秘密、技术成果等信息负保密义务。未经国家税务总局广西壮族自治区税务局书面同意，不得向社会公众或第三方通过任何途径出示、泄露，不得许可使用，不得对上述信息进行复制、传播、销售；保证不向外泄漏任何相关数据，不向外泄漏任何保密的技术资料。如出现支持人员泄密事件，中标人应负有连带责任。  （4）中标人须与国家税务总局广西壮族自治区税务局签署合同项目实施期间的信息保密协议。  （5）中标人投入的项目人员须与国家税务总局广西壮族自治区税务局签署合同项目实施期间的信息保密承诺书。  ★2.供应链安全管理要求  (1)中标人应要求供应链厂商严格落实供应链安全管理各项规定，包括按照国家相关法律法规开展的安全审查、安全评估、渗透测试等，并将供应链厂商落实情况作为项目验收的检查内容。  (2)中标人应要求供应链厂商严格遵守采购合同、协议、承诺书等文件中的安全相关条款，对供应链厂商履行网络安全责任不到位、造成安全事件或产生不良影响的行为，采购人将视安全事件严重情况按合同金额的20%-30%的比例进行扣减。  ★3.网络安全和数据安全管理要求  中标人投入的项目人员在合同期间应严格按采购人的网络安全和数据安全相关规定开展工作，由于中标人投入的项目人员网络安全工作落实不到位引发安全事件的，采购人将视安全事件严重情况按合同金额的20%-30%的比例进行扣减。  安全事件具体内容主要包括(但不限于)以下内容：  （1）因补丁升级、漏洞修复、系统杀毒、数据备份、应用监控、网络监控等工作未落实到位，发生服务器被控制和应用系统被攻破的安全事件，被主管部门通报的。  （2）因违规进行税费数据查询、导出和拷出等操作造成敏感数据泄漏，以及发生非法窃取数据行为。  （3）因运维操作处置不当导致重要应用系统发生严重卡顿、停用的重大事件。  ★4.罚责条款  项目建设和运维过程中，因系统在对接、运行等服务中，导致其他系统受到影响的，由中标人负责组织相关服务厂商共同排查，明确问题根源、责任并报告采购人。中标人无法判定问题根源的，由中标人承担全部责任。采购人将根据问题的轻重、中标人责任的大小，扣除不高于合同款5%服务金额。 |
| 其他要求 | 1.中标人须在项目实施中负责解决全部技术问题。若投标文件中的设计或实施方案出现不合理或不完整的情况，中标人有责任和义务提出补充修改方案并征得采购人同意后付诸实施，所需费用由投标人承担，采购人不再支付任何费用。 |