**2024年安全设备升级项目**

**采购需求**

**一、项目预算金额：226万元。**

**二、不面向中小企业，行业标准为软件和信息技术服务业。**

|  |
| --- |
|  **三、采购需求** |
| 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 | Web漏洞感知系统 | 2台 | 1. ★硬件配置：机架式设备≤2U，冗余电源，CPU核数≥8核；内存容量≥64G；硬盘容量≥20TB ；管理口≥1个；千兆电口≥4个；万兆光口≥2个（含万兆多模光模块）；
2. 性能要求：处理能力≥2Gbps ；监控并发连接数≥200万；IP碎片包重组能力≥20M；支持保存1-6个月的Web双向数据包，同时能够保存请求包和响应包。检测规则数量不少于200种。
3. 部署要求：支持旁路部署模式；系统管理可支持IPv4，可扩展IPv6协议;
4. 数据采集探测能力：
5. 支持ASCII、UNICODE等编码解码，将复杂编码后的数据还原为最基本的数据格式进行检测，以便有效防止黑客利用大小写变换、ASCII编码、UNICODE编码、注释、混淆等方式绕过检测引擎。
6. 支持分析基于TCP、UDP、ICMP、ARP、RIP、RPC、HTTP、FTP、TFTP、IMAP、SNMP、TELNET、DNS、SMTP、POP3、NETBIOS、NFS等协议的事件。
7. 支持监视端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击、网络蠕虫攻击、文件脆弱性攻击、浏览器脆弱性攻击、应用层安全漏洞攻击等攻击行为。
8. 威胁检测能力：
9. 具备对OWASP Top10的Web应用攻击检测能力，具备Web漏洞感知和Web入侵分析两种功能，能够识别包括：SQL注入、XSS跨站攻击、OS命令注入、WEB文件泄露、目录遍历、命令执行、文件包含、web后门、暴力破解等攻击。
10. 支持http会话双向数据流的追踪和检测分析，如服务器返回的网页中包含特定敏感关键字、泄密数据库信息时报警。
11. 支持http、mysql、ssh、smb、ftp、远程桌面等协议的双向分析。可在同一个规则内关联分析一个TCP会话的双向报文，当请求包含有指定攻击报文，返回包含有受影响的报文时，才发出报警。在同一条报警日志中要求同时展示双向报文，同时针对每条单独的告警下载PCAP报文。（投标文件中提供相应功能截图证明）
12. 数据防泄漏：支持检测服务器泄漏大型数据文件事件,如服务器返回超过20兆的数据文件。
13. DNS检测能力：域名解析：支持对访问的所有域名进行解析和分析（包含正常的访问记录），并记录的字段包括：会话时间、来源IP、域名IP、DNS服务器IP、DNS返回记录、查询域名、协议、长度、数据源、信息摘要等。（投标文件中提供相应功能截图证明）
14. 风险告警能力：
15. 支持提供充足证明此次告警的信息，报警内容包含完整的双向数据包，包括HTTP报文头部、URL、POST数据包，以及服务器返回的内容，同时针对每条单独的告警下载PCAP报文。
16. ★支持以网页快照形式展示服务器返回的内容。（投标文件中提供相应功能截图证明）
17. ★支持在告警中展示数据包交互的文件，如:PDF、word、excel、exe等文件（非展示文件存放的路径）。（投标文件中提供相应功能截图证明）
18. 告警管理与回溯分析能力：
19. ★支持通过时间、IP、Url、Post数据包、状态码、检索关键字等内容进行回溯分析，支持在回溯分析时去除含特定关键字的相关日志记录，支持复现整个攻击事件全部HTTP报文的关联分析。
20. 支持通过时间、IP、关键字、get参数、目的主机、日志类型、状态码等多个关键字及正则表达式的模式进行全文检索和回溯分析。
21. 支持存储全量的Web应用交互双向数据包，包含正常交互的http日志数据包，且有单独页面展示，http日志数据包需包括HTTP报文头部、URL、POST数据包，以及服务器返回的内容，且可存储1-6个月的全量应用日志。（投标文件中提供相应功能截图证明）
22. 资产管理能力：
23. 支持扩展资产识别，能够识别资产的http、https、ftp、smtp、dhcp、rdp、ssh等协议。
24. 支持扩展外联告警识别，能监测非法外联（如服务器设备中了木马）、异常通信，并发出报警。
25. 支持扩展以图表的形式，展示B段、C段、应用、域名、ip、端口的分布情况。
26. 协同联动能力：支持能够和一种或多种防火墙联动，阻断指定url的访问。
27. ★UEBA行为分析功能要求：支持用户和实体行为分析(user and entity behavior analytics,UEBA），可自动关联分析多个会话、日志、行为；可自定义关联分析策略；关联时长不少于10分钟。（投标文件中提供相应功能截图证明）
28. ★旁路阻断能力：支持扩展旁路阻断模块。设备旁路部署时，可阻断攻击请求。（投标文件中提供相应功能截图证明）
29. ★漏洞检测能力：支持扩展漏洞检测模块，可自主扫描操作系统及网站漏洞。包括缓冲区溢出、SQL注入、跨站脚本漏洞（XSS）、信息泄漏等常见的Web应用漏洞。
30. 自定义检测规则能力：
31. 支持以多个关键字及正则表达式的方式制定请求包检测规则：可同时按域名主机关键字、URL关键字、文件名关键字、请求报文、等多维度以多个关键字及正则表达式的方式制定检测规则。
32. 支持以多个关键字及正则表达式的方式制定返回包检测规则：可同时按域名主机关键字、URL关键字、文件名关键字、返回报文、返回页面MD5等多维度以多个关键字及正则表达式的方式制定检测规则。（投标文件中提供相应功能截图证明）
33. 研判助手：针对每条单独的告警，可自动关联该IP在48小时内的异常请求详情，同时关联该IP触发攻击的类型、该IP触发的攻击的次数、其他IP触发该攻击类型的次数、其他IP访问该URL次数等协助用户研判此次攻击的危害，并可标记为高危、中危、低危和忽略，提供忽略加白功能等。（投标文件中提供相应功能截图证明）
 |
| 2 | API安全审计系统 | 1台 | 1. 硬件配置：2U机架式设备；1+1冗余电源；内存≥32\*2GB，硬盘≥16TB（4T\*4）； ≥2个千兆电口管理口；≥2个千兆电口；≥2个万兆光口（含万兆多模光模块）；整机数据吞吐量≥ 5 Gbps，提供三年维保授权。
2. ★系统内置的脆弱性策略匹配规则达1500条左右可对常用应用漏洞进行监测。其中接口未鉴权支持100条匹配规则，可覆盖Apache Spark、OpenAPI、Weblogic等常用组件未授权漏洞监测。命令执行漏洞支持近1000条匹配规则。（投标文件中提供相应功能截图证明）
3. 系统具有丰富的风险详情，包含：风险基本信息、历史记录、API影响面评估、可被利用方式、修复建议等。其中API影响面评估可从去重数据量、API访问量、暴露数据标签、访问域等维度进行综合分析，与同类风险API进行对比，形成影响面评估结果，区分API治理重点。
4. 支持以IP、账号、IP+API、账号+API、数据维度进行行为风险配置。支持通过多种指标自定义新增风险策略，例如：访问次数、访问时间、访问敏感数据等、上传下载文件、访问账号等。
5. 支持以数据为维度进行风险监测，以数据为线索关联分析相关API、相关应用、相关主体等内容，可适用于洞察二次封装风险、核心数据防泄漏场景。（投标文件中提供相应功能截图证明）
6. 支持对少量多次的点滴泄漏数据行为构建风险行为画像，对数据的路径流转进行可视化拓扑分析。
7. 支持丰富的敏感数据识别技术：包括正则表达式、关键字典等先进技术自定义创建识别规则。
8. 内置100+敏感数据标签，包括身份证号、手机号、银行卡号、姓名、地址、邮箱等个人敏感数据标签。（投标文件中提供相应功能截图证明）
9. ★可识别文件中的敏感数据，可识别文件种类总计100+类。例如 OFFICE办公文档((DOC/DOCX、 XLS/XLSX、PPT/PPTX）、 WPS、PDF、OFD、纯文本、标记文本、图片内容、设计文档等。（投标文件中提供相应功能截图证明）
10. 支持HTML、PDF、png、word多种格式的报表订阅，可定期通过邮件发送最新的报告。
11. 支持通过界面自定义新增脆弱性漏洞，可细粒度配置到请求头字段、API类型、请求方法、响应状态、返回字段等，支持对以上维度正则匹配、敏感数据类型识别或敏感数据量数量识别等方式进行配置。
12. 支持监测API的生命周期变化，并可通过可视化方式修改生命周期的打标周期。
13. 支持根据策略自动识别划分静态资源页面和数据共享API，支持可视化多指标组合配置划分规则，配置指标维度包括：URL、请求用户代理、请求方法、响应内容类型、请求头、响应头。
14. 支持以IP、账号、IP+API、账号+API、数据维度进行行为风险配置。支持通过多种指标组合自定义配置新增风险策略，例如：请求数据标签、返回数据标签、下载文件、上传文件、访问频次、登录账号数、账号密码去重数、手机号验证码去重数、操作时间等。支持以滑动窗口计数方式匹配监测规则。
15. 支持留存全量的API操作日志，最高可审计的单日志大小为 16MB，支持配置日志留存时间，默认日志完整保存 180天以上。
16. 支持根据内置脆弱性风险策略自动从流量中识别监测接口中存在脆弱性，并留存 API 脆弱性证据样例，并给出对应的修复建议。
 |
| **二、商务条款** |
| ★合同履行期限 | 合同签订后30天内交货；设备到货验收后60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 | 广西南宁市。 |
| ★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2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，并提供中标产品原厂商对此项目的售后服务承诺函。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60%；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 | 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在项目采购需求中，中标人必须严格按照税务系统供应链安全管理的各项规定要求开展运维服务，包括但不限于：（1）中标人销售的产品具备销售许可证、满足国家认可的网络安全规范和认证要求；（2）中标人销售产品满足业务持续稳定运行时限需求的使用授权；（3）中标人采用安全可控的方式、渠道，交付产品或开展服务等；（4）中标人必须明确产品安全性，如不可利用产品的便利条件非法获取用户数据、控制和操纵用户系统和设备，不得在未授权情况下对产品进行升级或更新换代等；（5）中标人必须明确安全责任和义务，如供应商对软硬件产品和服务的设计、研发、生产、交付等关键环节加强安全管理；（6）中标人必须按照国家法律法规开展的安全审查、安全评估、渗透测试等；（7）中标人必须设置声明条款，说明采购第三方产品、开源限制性、知识产权等情况。★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。 |