采购需求

（一）采购标的

1.采购标的内容：六安市生态环境局现有部分网络安全设备存在服务到期、设备老化，网络安全专业技术力量不足，存在一定的网络安全风险。为有效提升我单位整体网络安全防护能力，需对现有部分网络安全设备进行续保升级，引入网络安全运维托管服务，将现有网络边界安全设备、态势感知平台、威胁检测探针等设备和安全托管服务相结合，联动分析实现安全事件的预警监测，同时搭配7*24 持续安全监测及研判机制，实现网络安全事件的分析定位和精准溯源，实现单位网络安全管理可查、可控。

2.采购标的所属行业：软件和信息技术服务业。

（二）商务要求

1.交付时间和地点。

交付的时间：签订合同后，原则上 60 日历天完成设备供货，验收通过后提供 1 年服务（以验收通过日期起算）。

交付地点：六安市长安南路 207 号六安市生态环境局。

2. 付款条件

合同签订后预付款为合同金额的 60%；剩余款支付方式：运维服务期满并考核合格后一次性结清尾款。

（三）技术要求

本次项目采购内容及技术要求如下：

采购清单

序号	服务内容	技术参数及要求	数量
1	日志审计设备	1、标准 2U 机架式设备，主机审计许可证书数量≥50，最大可扩展审计主机许可数≥150，数据盘≥4T*2（raid1），平均每秒处理日志数（eps）性能≥2500。内存≥16G，网络接口≥6 千兆电口+2 万兆光口 SFP+（满配光模块），含 3 年产品质保及软件升级服	1 台

		务。 2、支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于 800 种日志对象的日志数据采集。 3、支持自动解析主流网络设备、安全设备和中间件的日志数据，标准化自动识别系统类型至少达到 200 种。 4、支持通过正则、分隔符、json、xml 的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射，以满足除内置解析规则之外未被覆盖的日志类型的解析。**（投标文件中提供产品功能截图等相关证明材料）** 5、支持自动识别采集设备、支持设备异常告警、设备异常告警发送邮件或第三方接口。 6、支持 POC 测试工具一键生成数据,验证日志数据采集是否成功，避免设备部署后采集失效但不被发现等风险。**（投标文件中提供产品功能截图等相关证明材料）** 7、支持日志检索数据的投屏。支持日志查询结果的统计与导出，支持历史备份文件导入查询。 8、支持告警事件归并、告警确认和告警归档，支持基于频率、频次、时间的设定条件。 9、支持设置日志存储策略，包括设置日志存储周期（天）、存储空间容量使用阈值等。 10、支持对单个/多个日志源批量转发，支持定时转发，可通过 syslog 和 kafka 方式转发到第三方平台，同时支持转发已解析日志和原始日志的两种日志。**（投标文件中提供产品功能截图等相关证明材料）** 11、支持资产全生命周期管理，资产入库审核、资产离线风险识别、资产退库、资产数据更新，责任人管理机制等，支持自定义资产标签、属性。	
2	安全运营平台服务	1.支持实时监测网络安全状态，对攻击事件自动化生成工单，及时进行分析与预警；攻击事件包含境外黑客攻击事件、暴力破解攻击事件、持续攻击事件。 2.暴露面梳理：投标人应具备互联网暴露面梳理的服务工具，该工具应当支持全资产和精确资产两种模式暴露资产收集模式，收集到的暴露面信息至少包括域名、域名标题、	1 年

		IP 地址、开放端口、资产指纹、网站截图、移动端暴露面，并且能采集对应暴露资产的访问截图向招标人举证，及对应暴露资产存在的漏洞**(投标文件中提供服务工具具备以上暴露面梳理能力的证明截图等相关材料)。** 3.脆弱性管理：针对服务范围内资产扫描到的高危可利用漏洞，投标人应当为招标人做好每一个高危可利用漏洞的防护工作，包括但不限于为招标人提供漏洞修复方案和安全设备防护策略，以及帮助招标人配置防护规则，保证招标人不因此出现重大事件和损失。 4.威胁管理：投标人应当具备云端检测和分析平台，通过采集招标人安全设备和工具的安全告警和安全日志，结合大数据分析、人工智能等技术手段，为招标人提供 7*24 小时持续不间断的安全威胁分析鉴定，同时在用户界面进行展示。 5.安全运营服务承诺 SLA：从安全日志产生到事件通告给采购人的时间方面，按照国家标准对安全事件的分类分级指南，重大安全事件通告时间小于 30 分钟，一般事件的通告时间少于 1 小时。运营服务对于重大安全事件的遏制影响和处置完成时间小于 1 小时，对于一般事件的遏制影响和处置完成时间小于 4 小时。安全事件经过服务人员的确认后，各类安全事件的判断准确率不低于 99%。安全事件的闭环处置比例达到 100%。**（投标文件中需提供投标人盖章的承诺函，承诺函格式自拟）。** 6.服务质量监控：投标人需为招标人提供的服务成果展示门户（或用户 Portal）应具备服务质量可视化展示，投标人能通过可视化的数据，清晰的了解安全专家的服务水平，至少包括脆弱性闭环率、脆弱性平均响应时长、脆弱性平均闭环时长、威胁闭环率、威胁平均响应时长、威胁平均闭环时长、事件闭环率、事件平均闭环时长，以验证投标人所承诺的服务指标（或称为服务 SLA）**(投标文件中提供服务成果展示门户中服务质量监控相关的功能截图证明等相关材料)。** 7.投标人需提供客观的修复优先级指导，不能以脆弱性危害等级作为唯一的修复优先	

		级排序依据；排序依据包含但不限于资产重要性、漏洞等级以及威胁情报（漏洞被利用的可能性）三个维度。 8.投标人需为招标人提供服务资产授权不少于 10 个，提供不少于 1 年的 7*24 小时线上安全守护，不论白天、黑夜、节假日投标人均该能实现 7*24H 在线服务；**（投标文件中需提供投标人盖章的承诺函，承诺函格式自拟）。** 9.单位现有的防火墙，杀毒软件态势感知能够与安全运营服务平台对接，实现安全日志分析并联动处置**（投标文件中需提供产品功能截图等相关证明材料）。** 9.服务交付物： 供《项目启动会 PPT》 《首次安全风险分析报告》 《漏洞举证报告》（按需） 《漏洞清单》（按需） 《应急响应报告》（按需） 《威胁情报》 《暴露面梳理清单》(按需) 《威胁狩猎报告》（按需） 《安全运营周报》 《安全运营月报》 《半年度总结汇报》 《年度总结汇报》	
3	硬件防火墙(办公网区域)维保服务	对我单位现有硬件防火墙设备（品牌型号：深信服 AF-1000-B1600）进行维保服务，包含原厂 1 年硬件产品质保、原厂 1 年规则库升级服务。**（投标文件中提供投标人盖章的维保服务承诺函，承诺函格式自拟）**	1 项
4	上网行为管理设备维保服务	对我单位现有上网行为管理设备（品牌型号：深信服 AC-1000-1750）进行维保服务，包含原厂 1 年硬件产品质保、原厂 1 年应用识别库升级服务。**（投标文件中提供投标人盖章的维保服务承诺函，承诺函格式自拟）**	1 项
5	硬件防火墙(业务网区域)维保服务	对单位现有硬件防火墙（品牌型号：深信服 AF-1000-B1310）进行维保服务，包含原厂 1 年硬件产品质保、原厂 1 年规则库升级服务。**（投标文件中提供投标人盖章的维保服务承诺函，承诺函格式自拟）**	1 项
6	局大楼楼宇无线网优化服务	对我单位现有大楼楼宇无线网进行认证策略和权限等配置调试优化服务。	1 项

7	终端防护软件升级改造服务	对我单位现有的终端防护软件进行平台扩容、授权和升级服务，实现一个平台管理全局办公电脑等网络终端设备，本次配置250点PC授权数量。	1年
8	安全培训服务与技术支撑	1.成交供应商在成交后服务期内，须提供 2次专业安全技术培训服务，培训形式为面授或线上培训；培训内容要求内容充实，理论与实践相结合；培训教材须提前一个月提供，培训教材需经过采购人审核后，方可开展安全培训工作。培训内容包括安全技术培训、安全意识培训、攻防技战法培训等。 2.成交供应商需在网络安全宣传周期间提供宣传品（不限于宣传册、海报、视频等物料)的支撑。	1项

注：1.所有参数必须完全响应，采购需求中要求提供相应证明材料的必须提供，否则按不实质性响应采购文件处理，作无效标处理。

2. 投标人不得对采购需求中的技术参数要求虚假响应,为了保证投标文件的真实有效性，采购人有权要求中标人标后提供相关证明原件或产品进行查验，如发现投标人存在虚假响应情况（包括但不限于虚假技术参数响应、虚假网站、虚假证书、虚假检测报告等)，采购人有权取消该投标人的中标资格，并提请政府采购监管部门将卖方列入不良行为记录名单，在一至三年内禁止参加政府采购活动

（四）服务要求

1.本次网络安全服务主要内容包括网络安全设备升级维保和及网络安全托管技术服务。包括但不限于安全检查、特征库和规则库升级检查、策略配置调优和变更、设备日志审计、设备故障厂商对接以及其他六安市生态环境局安排的临时事项等服务。

2.设备交付调试 。项目合同签订之日起60个日历天内，中标人须完成设备的交付和项目验收。经过项目验收的设备可以由采购人工作人员稳定使用。

3.对我单位现有网络设备调试整改优化单位网络,对办公室的网络进行线路梳理、优化调整。

4.有关质量要求。(1）中标人提供的所有货物必须是全新的、未使用过的货物，所涉及的技术、设计、设备、技术培训和技术服务应来自于货物的合格原产

地，货物及其有关服务必须符合国家有关设计和制造生产标准或行业标准。（2）中标人应保证，提供的货物（含软件）均为正版产品，采购人在中华人民共和国境内使用该货物或货物的任何部分时，免受第三方提出的侵犯其专利权、商标权、著作权或其他知识产权的起诉。

5.质保时限要求。中标人须提供自项目验收之日起 1 年的质保服务 （此部分费用包含在报价中）。

6.提供单位办公、网络等设备的运维服务和技术支持，出现问题需及时处理。

7.售后、运维服务要求。（1）在货物质保服务期内，中标人应始终通过现场服务、电话服务、远程服务等方式提供快速、高效的设备运维保障服务。（2）质保服务期内，中标人须提供所供软件系统的 BUG 修复、系统性能优化等服务。（3）中标人应及时对产品进行打补丁、固件升级等服务。（4）中标人在实施系统维护或修改设计后，应在 1 周内更新有关技术文档并提交采购人（5）技术支持方面，中标人须提供 7×24 小时的技术咨询服务。（6）故障响应方面，中标人须提供 7×24 小时的故障服务受理；对重大故障提供 7×24 小时的现场支援，一般故障提供 5×8 小时支援；原则上对影响应用系统正常运行的重大故障，要求 2 个工作日内提供维护服务（不可抗力原因除外）。

8、中标人需与采购人签订网络安全保密协议，落实网络安全及信息保密的各项规定。

9、运维工程师与采购人签订网络安全保密承诺书。运维工程师需严格遵循保密义务，凡涉及客户的机型配置、IP 地址、软件、终端设备等信息不得向第三方泄露，维护过程中如需涉及客户系统的数据信息，必须经采购人同意。