海南热带海洋学院

全天候安全监测服务项目采购公告

经研究，我校对全天候安全监测服务项目进行公开竞价采购，竞价活动由网络与教育技术中心进行组织。具体竞价内容及要求如下:

一、项目名称

全天候安全监测服务项目

二、项目预算

人民币：壹拾贰万元整（最高限价 12 万）

三、竞价内容

服务名称	服务内容描述
全天候安全监测服务	**（一）安全托管服务:** 1、服务资产（IP）数量≥20 个，围绕资产、脆弱性、威胁、事件四个要素为用户提供 7*24H 的安全托管服务，扩展持续有效的安全运营能力，保障可承诺的风险管控效果; 2、配置一名经验丰富的安全专家作为专属服务经理，并且实时响应投标方咨询的网络安全相关问题; 3、应使用安全工具对服务资产开展互联网暴露面探测，以梳理资产面向互联网的开放情况，快速发现违规暴露在互联网中的资产及存在的风险并进行处置; 4、具备云端检测和分析平台，通过采集招标方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，为招标方提供 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、安全专家每月对招标方的安全设备的防护策略进行检查，确保安全设备上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果。投标方云端服务平台应当具备丰富的策略检查工具; 6、云端服务平台应当支持对接招标方本次采购的主要服务工具，边界安全防护服务组件、终端安全系统服务组件，支持实时接收安全组件检测到的安全事件信息、安全日志数据提供 7*24 小时的服务; 7、提供安全托管服务相关信息的详细展示和呈现，分别为安全运营概览、事件&威胁概况、服务承诺协议 SLA、勒索风险概况、设备安全策略检查、行业情报，并支持全屏投放展示。 **（二）边界安全防护服务：**

	1、提供边界安全防护服务组件，性能指标：网络层吞吐量≥4Gbps，应用层吞吐量≥2Gbps，并发连接数≥200 万，每秒新建连接数≥4.5 万； 2、服务组件支持链路连通性检查功能，支持基于 3 种以上协议对链路连通性进行探测，探测协议至少包括 DNS 解析、ARP 探测、PING 和 BFD 等方式； 3、服务组件支持多对一、一对多和一对一等多种地址转换方式； 4、服务组件支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护； 5、服务组件支持云端未知威胁主动探测技术，实现 5min 内未知威胁情报全网设备下发，能够对 15 层以上的压缩病毒文件进行检测和拦截； 6、服务组件支持与终端杀毒软件联动管理，支持检测到某主机有僵木蠕毒的 C2 通信时，手动或自动化将恶意域名信息下发到终端安全软件做 C2 通信的封锁遏制，下发一键隔离指令，对终端恶意文件进行隔离。 **（三）终端安全系统服务：** 1、提供终端安全系统服务组件，纯软件交付，包含管理控制中心软件及终端客户端软件； 2、单一管理控制中心可统一管理分别部署在 WindowsPC、Windows 服务器、Linux 服务器以及国产化服务器的客户端软件； 3、提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果； 4、支持客户端的错峰升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或 I/O 风暴； 5、支持安全策略一体化配置，通过单一策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、文件实时监控的参数配置、WebShell 检测和威胁处置方式、暴力破解的威胁处置方式和 Windows 白名单信任目录； 6、为了建设立体安全防护，支持与本次防火墙进行安全联动，管理员可以在防火墙管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息； **（四）服务承诺：** 1、分析研判通知时效 MTTA：从安全日志上传分析研判到通告给招标方的时间方面，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 60 分钟； 2、安全事件经过投标方服务人员的确认后，通告给招标方的各类安全事件的准确率不低于 99%（即误报不能超过 1%）； 3、服务范围内的所有安全事件的闭环处置比例达到 100%。 **（五）授权服务限期：**一年。

四、竞价方法

海南热带海洋学院网络与教育技术中心将通过公开竞价的方式，

参加竞价的单位按竞价内容及要求进行报名，并由网络与教育技术中心召开竞价会议，对参与竞价活动单位提交的报价及相关材料进行审查，满足使用单位需求，按照“价格优先”的原则，在规定服务时间内以最低报价承担该项目的服务工作。

五、资格要求

1.满足《中华人民共和国政府采购法》第二十二条规定。

2.满足竞价供应商未被列入“信用中国”网站（www.creditchina.gov.cn）失信被执行人名单和没有列入中国政府采购网（www.ccgp.gov.cn）政府采购严重违法失信行为记录名单;

3.在中华人民共和国注册，具有独立承担民事责任的能力：① 供应商若为企业法人：提供有效的“统一社会信用代码营业执照”；未换证的提供有效的“营业执照、税务登 记证、组织机构代码证”；②若为事业法人：提供“统一社会信用代码法人登记证书”；未换证的提交“事业 法人登记证书、组织机构代码证”；③若为其他组织：提供“对应主管部门颁发的准许执业证明文件或营业执照”。

4.投标单位必须保证提供产品售后服务，投标单位投标时必须提供售后服务机构或厂家、地址、电话、联系人等资料。

5.参加投标的单位需提供法人营业执照的复印件（复印件须加盖本单位公章）备案。

6.为保证项目质量和售后服务保障的及时有效响应，要求参与本项目响应的供应商应满足如下要求：开展本项目售后服务期间，对于采购人的紧急应急响应服务请求需在6小时内到达招标人现场。

六、竞价材料的递交时间、地点及要求

1.递交材料时间截止为：2026 年 9 月 22 日（星期二） 上午 11:30

2.地点：海南热带海洋学院 6 栋实验室楼 219 室

3.提供材料：营业执照、法人身份证、代理人身份证、无违法记录的证明或承诺函、报价一览表、承诺函等。（以上资料须提供复印件加盖公章）

4.逾期送达的竞价材料，不予受理。

七、联系方式

联系部门：网络与教育技术中心

联系电话：18289983690 李老师

海南热带海洋学院

2026 年 9 月 17 日

（一审：李亚男；二审：欧训勇；三审：陈作聪）

附件:

1.报价一览表

2.承诺函

附件一：报价一览表（参考模板）

序号	服务名称	描述	价格	备注
1	全天候安全监测服务	**（一）安全托管服务:** 1、服务资产（IP）数量≥20 个，围绕资产、脆弱性、威胁、事件四个要素为用户提供 7*24H 的安全托管服务，扩展持续有效的安全运营能力，保障可承诺的风险管控效果； 2、配置一名经验丰富的安全专家作为专属服务经理，并且实时响应投标方咨询的网络安全相关问题； 3、应使用安全工具对服务资产开展互联网暴露面探测，以梳理资产面向互联网的开放情况，快速发现违规暴露在互联网中的资产及存在的风险并进行处置； 4、具备云端检测和分析平台，通过采集招标方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，为招标方提供 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、安全专家每月对招标方的安全设备的防护策略进行检查，确保安全设备上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果。投标方云端服务平台应当具备丰富的策略检查工具； 6、云端服务平台应当支持对接招标方本次采购的主要服务工具，边界安全防护服务组件、终端安全系统服务组件，支持实时接收安全组件检测到的安全事件信息、安全日志数据提供 7*24 小时的服务； 7、提供安全托管服务相关信息的详细展示和呈现，分别为安全运营概览、事件&威胁概况、服务承诺协议 SLA、勒索风险概况、设备安全策略检查、行业情报，并支持全屏投放展示。 **（二）边界安全防护服务：** 1、提供边界安全防护服务组件，性能指标：网络层吞吐量≥4Gbps，应用层吞吐量≥2Gbps，并发连接数≥200 万，每秒新建连接数≥4.5 万； 2、服务组件支持链路连通性检查功能，支持基于 3 种以上协议对链路连通性进行探测，探测协议至少包括 DNS 解析、ARP 探测、PING 和 BFD 等方式； 3、服务组件支持多对一、一对多和一对一等多种地址转换方式； 4、服务组件支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护； 5、服务组件支持云端未知威胁主动探测技术，实现 5min 内未知威胁情报全网设备下发，能够对 15 层以上的压缩病毒文件进行检测和拦截； 6、服务组件支持与终端杀毒软件联动管理，支持检测到		

		某主机有僵木蠕毒的 C2 通信时，手动或自动化将恶意域名信息下发到终端安全软件做 C2 通信的封锁遏制，下发一键隔离指令，对终端恶意文件进行隔离。 **（三）终端安全系统服务：** 1、提供终端安全系统服务组件，纯软件交付，包含管理控制中心软件及终端客户端软件； 2、单一管理控制中心可统一管理分别部署在 WindowsPC、Windows 服务器、Linux 服务器以及国产化服务器的客户端软件； 3、提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果； 4、支持客户端的错峰升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或 I/O 风暴； 5、支持安全策略一体化配置，通过单一策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、文件实时监控的参数配置、WebShell 检测和威胁处置方式、暴力破解的威胁处置方式和 Windows 白名单信任目录； 6、为了建设立体安全防护，支持与本次防火墙进行安全联动，管理员可以在防火墙管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息； **（四）服务承诺：** 1、分析研判通知时效 MTTA：从安全日志上传分析研判到通告给招标方的时间方面，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 60 分钟； 2、安全事件经过投标方服务人员的确认后，通告给招标方的各类安全事件的准确率不低于 99%（即误报不能超过 1%）； 3、服务范围内的所有安全事件的闭环处置比例达到 100%。 **（五）授权服务限期：**一年。		
2	增值服务	投标人根据项目实际情况填写		
合计		小写：　　元　大写：人民币　　元整		
工期：				

报价人（公章）：

授权代表（签名）：

日期：

附件二：承诺函

承诺函

致：海南热带海洋学院

根据贵单位_____的公告要求，正式授权下述签字人_____（姓名和职务）代表报价人_____（报价单位名称），提交响应文件。

根据此函，我方承诺如下：

1、**我方接受竞价公告文件的所有的条款和规定**。

2、我方同意按照公告文件第五条“资格要求”的规定，本响应文件的有效期为从报价截止日期起计算的 45 天，在此期间，本响应文件将始终对我方具有约束力，并可随时被接受。

3、我方同意提供贵单位要求的有关本次报价的所有资料或证据，并保证资料、证据的真实有效性。

4、如果我方成交，我们将根据公告响应文件的规定严格履行自己的责任和义务。

特此承诺！

报价人名称：_____（公章）

地址：_____邮编：_____

电话：_____传真：_____

授权代表（受托人）：_____（签字或私章）_____ 职务：_____

日期：_____