如有建议或意见，请以书面形式并加盖公章、注明联系人、联系方式，于2025 年08月22日 17:00 之前送至我单位，逾期不受理（如邮寄，2025年08月22日 17:00 之后到达本公司的邮件将不再受理）。

采购需求

一、采购预算

本项目不接受超过65.292万元人民币（采购项目预算金额）的投标报价。采购人不再支付报价以外的任何费用。

二、项目概括

1、采购人：徐州市医疗保障局

2、项目名称：徐州市医疗保障局医保网络安全服务项目

3、项目地点：江苏省徐州市

4、质量要求：合格

三、服务清单及技术要求：

服务清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务名称 | 服务范围 | 服务频率 | 服务年限 |
| 1 | 一体化MDR安全运营服务 | 全网 | 7\*24h\*365天 | 2年 |
| 2 | 基线检查服务 | 服务器系统 | 4次/年 | 2年 |
| 3 | 漏洞扫描服务 | 服务器、网络设备、安全设备、终端等 | 1年 | 2年 |
| 4 | 渗透测试服务 | 10个应用系统 | 1年 | 2年 |
| 5 | 新系统上线检查服务 | 新上线系统 | 4次/年 | 2年 |
| 6 | 应急响应服务 | 全网 | 全年 | 2年 |
| 7 | 宣传教育培训服务 | 医保信息部门 | 2次/年 | 2年 |
| 8 | 重大时期保障服务 | 全网 | 重大活动时期 | 2年 |
| 9 | 现有安全运维工具升级 | 全网 | 1年 | 2年 |

服务技术要求

1、★MDR安全运营服务

围绕资产、威胁、事件等为业务系统提供7\*24小时威胁监测与分析服务，云端安全运营团队对威胁事件持续监测，实时事件分析及研判，并将确认的攻陷/重点攻击事件等及时通知，提供事件处置建议，协助事件闭环管理，建立7\*24h、持续主动、有效闭环的安全运营体系。

1.支持僵木蠕类威胁事件的监测、研判、处置，如勒索病毒、挖矿病毒等多种类型的僵木蠕类事件监测与响应。

2.日常情况下，每周针对攻击检测规则及能力进行升级更新。紧急高危事件情况下，1小时内提供自定义检测规则，24小时内进行工具规则更新

3.支持恶意软件类（挖矿软件、勒索软件等）威胁事件监测、研判、处置，如恶意程序通信类事件的监测与响应。

4.▲支持webshell类威胁监测、研判、处置。如冰蝎、哥斯拉等大量webshell样本的连接、上传,加密webshell检测等监测与响应，同时为了能够更好针对web类攻击形成阻断，需要本次服务的云端平台能够和现有网站防火墙形成联动机制，云端平台能够下发针对风险IP阻断指令给网站防火墙（提供所投安全服务厂商承诺函加盖原厂公章）。

5.▲支持针对攻防演练实战中常见高危漏洞的真实攻击类威胁事件监测、研判、处置。如组件RCE、OA系统RCE等常见攻防演练高危漏洞威胁监测与响应。

6.支持对客户发现、威胁监测以及狩猎场景发现的安全事件，按需进行应急响应。云端安全专家7\*24进行威胁事件的应急响应，对勒索病毒类、挖矿木马类、僵尸网络类、其他恶意程序通信类、漏洞利用成功类等失陷事件提供应急响应服务，协助完成恶意程序、后门、权限维持收到清理，并提供后续建议。

7.▲服务交付中需应用厂商自有安全大模型及多个其他模型，如deepseek等，辅助威胁分析交叉验证，同时可支持大模型研判结果的反馈及校验，确保分析模型持续学习，以提升分析能力，确保对安全事件检出的效果（提供功能截图）

8.大模型支持对海量告警降噪，并可提供事件优先级判定分数，帮助分析人员尽快确定事件处置优先级别，提升分析效率。

9.展示客户威胁态势，包括：威胁风险情况（事件、失陷主机等）、被攻击IP及恶意攻击IPTOP5；威胁事件的闭环情况、事件状态情况；威胁事件列表及威胁事件的所处状态情况；威胁事件趋势及事件闭环趋势等。

10.▲支持移动端APP形式实时事件的通知。（为了保证为用户提供软件安全可靠、软件供应商需要达到中国信息通信研究院颁发《软件供应链安全能力成熟度》二级及以上，提功证书复印件证明）

11.门户支持用户门户同一客户下的账号分权分域，主账号管理所有事件，多个子账号分管各自事件。

12.▲云端安全运营平台支持与现有的安全运营工具联动，云端平台能够下发针对风险IP阻断指令给运营工具，提示运营处置效率（提供厂商承诺函）

13.研判分析过程中，可提供详细的分析过程，如分析思路、分析方法等，确保事件分析结论正确有效。

2、★基线检查服务

通过安全配置核查产品或人工方式，对系统中网络设备、操作系统、数据库和应用服务器的配置进行安全检查，提供安全配置评估报告和改进建议。每年4次。

3、★漏洞扫描服务

通过自动化扫描工具，针对网络设备、操作系统、数据库、常见应用服务器以及WEB应用等资产，检查存在的安全漏洞，提供漏洞评估报告和修复建议。每年4次。

4、★渗透测试服务

通过人工黑盒的测试方式，按照采购人要求对网络、应用、数据、终端等系统进行渗透测试,以判断现有存量系统是否存在风险隐患，出具正式检测报告。每年4次。

5、★新系统上线检查服务

提供新上线业务提供上线前安全检查服务，提供专业的安全检查方案、输出评估结果、解决建议，配合应用相关开发和维护人员解决或规避安全风险，以确保新上线的应用程序的安全风险可以被接受，并对评审通过的解决方案实施结果进行复查，确保即将上线的系统安全性。每年4次。

6、★应急响应服务

根据事件类别，提供全年的应急响应服务，通过远程和现场支持的形式协助客户对遇到的突发性安全事件进行紧急分析和处理。主要工作内容包括：突发事件相关信息的收集、事件的分析、报告提交、问题解决建议等。紧急事件主要包括：勒索病毒、病毒和蠕虫事件、数据泄露、挖矿事件等。全年7\*24小时即时响应。

7、★宣传教育培训服务

对医保信息部门提供专业技术培训1年4次。

8、★重大时期保障服务

在重要时间节点期间提供不少于一人的安全人员驻场，保障系统持续、稳定的运行，对客户重要系统进行安全保障。每年不少于4次。

9、★现有安全运维工具升级

现有安全运维工具：

1.绿盟UTS综合威胁探针UTSNX3-HD4100；

2.华为镜像交换机S5735S-L24T4X；

升级内容：

1. 现有安全监测工具（探针）主要包含入侵检测、威胁情报等模块，本次需要增加恶意文件检测、web应用检测等能力。所有功能模块授权增加2年，设备原厂续保增加2年。

2.镜像交换机增加设备原厂续保2年。

**注：上述除原厂授权外，各供应商能证明其升级方案符合同等技术标准（如支持相同硬件架构、性能指标、安全认证），并获原厂授权的视为有效响应。**

四、项目实施要求：

1.所有网络安全调整加固均需采购人同意后，方可实施，同时，要做好纸质资料、电子文档留存工作。合同期结束，由本项目产生的资料中标人装订交于招标方，同时中标人不应留存本项目任何资料，包括纸质资料、电子文档等。

2.中标人对项目实施过程中接触到的技术和业务信息（包括网络拓扑、设备清单、技术方案、服务内容、实现方法、运作流程、技术指标、软件系统、数据库、运行环境、测试结果、使用手册、技术文档等）应主动采取加密措施进行保护，防止任何第三方知悉及使用，不得刺探或者以其他不正当手段获取与该项目无关的信息，造成采购人遭受经济损失或者严重后果的，中标人应当承担相应经济和法律责任。

3.本项目服务的业务专网为市级医保网络。

五、项目服务期：自合同签订生效之日起2年。

六、其他要求：见磋商文件第十章《拟签订的合同文本》。