**关于南京医科大学附属口腔医院全路径安全检测与响应平台项目征集潜在供应商的调研公告**

南京医科大学附属口腔医院拟对以下项目进行摸底、调研，公开征集潜在供应商。欢迎符合要求的供应商前来报名。

**一、项目概况**

**项目名称：全路径安全检测与响应平台**

**项目简介：**随着网络攻击手段的不断进化，单一的安全产品已经无法有效应对复杂的威胁。现代网络威胁通常具有高复杂性、多阶段性和隐蔽性，传统的安全信息和事件管理（SIEM）和孤立的安全产品（如防火墙、杀毒软件）在应对这些高级威胁时，且存在大量的安全事件和日志信息，需要有效的收集、分析和处理，显得力不从心。因此，通过本次项目搭建全路径安全检测与响应平台，通过快速响应和处理安全事件，自动化功能将大幅提高安全运营效率，减少人工干预，降低医院运营成本，同时提高医院安全事件处理的准确性和及时性。

**数量：**1套

不接受进口产品

**二、资质要求：**

1、响应供应商应具有独立法人资格，营业执照。

2、与本项目相关的特殊资质证照。

**提供有效的证书复印件加盖公章。**

**三、项目基本技术要求（见附件）：**

1、软件部分见附件；

2、请同时提供满足本项目实施要求所需硬件配置清单及技术要求。

**四、请仔细阅读本项目技术参数要求，并提供以下书面材料一式四份。**

1. 本公司满足本项目全部技术参数要求，无疑问。

或

本公司对本项目技术参数有正/负偏离，并附下表表述。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 指标 | 原技术指标 | 正/负偏离 | 原因 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

2、本公司对本项目技术参数有疑问，并附下表表述，标明原技术参数，建议修改内容并阐明原因。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 指标 | 原技术指标 | 建议修改 | 原因 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

1. 该项目人员配置（项目建设及服务团队）

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 姓名 | 所属工种 | 证书 |
| 1 |  |  |  |
| 2 |  |  |  |

1. 与本项目类似的成功案例（合同或中标通知书复印件）
2. 与本项目相关的公司资质证书专利等证明材料。
3. 描述质保期内及质保期后的服务方案。
4. 硬件产品须为合同签订时间一年内出厂，全新、未使用过的原装合格正品，不得使用已停产或拟停产产品，提供承诺书并加盖公章。
5. 请同时将所投调研产品的调研文件（包含详细参数）发至邮箱：[2066748093@qq.com](mailto:2066748093@qq.com)，调研文件名称设置：公司名称+项目名称。

**五、 价款的支付方式、时间及条件：**签订合同后，凭发票支付合同总价款的30%；乙方完成全部产品安装、调试，正常使用30日后，经甲方验收合格，签署《南京医科大学附属口腔医院验收报告》，凭发票支付合同总价的60%；留合同总价的10%作为本项目的尾款，自甲方支付至90%合同款12个月后，产品运行正常，售后服务良好，无质量、安全和服务问题，经甲方确认，支付合同尾款10%。

**六、报价一览表**

按照硬件、软件进行分项报价，硬件部分应按照设备组成分项报价，软件部分应按照功能模块分项报价。所有价格信息在报价一览表中详细列明，可另行加行。

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **项目名称** | | **南京医科大学附属口腔医院全路径安全检测与响应平台项目** | | | | | | |
| **软 件** | | | | | | | | |
| **序号** | **产品名称** | | **品牌规格型号** | **单位** | **数量** | | **单价（元）** | **总价（元）** |
| 1 |  | |  |  |  | |  |  |
| 2 |  | |  |  |  | |  |  |
|  |  | |  |  |  | |  |  |
| **硬 件** | | | | | | | | |
| **序号** | **产品名称** | | **品牌规格型号** | **单位** | **数量** | | **单价（元）** | **总价（元）** |
| 1 |  | |  |  |  | |  |  |
| 2 |  | |  |  |  | |  |  |
| **合计金额** | | **人民币（大写） 元**  **（¥ 元）** | | | | **软件：¥ 元** | | |
| **硬件：¥ 元** | | |
| **质保期** | | **硬件：** | | | | | | |
| **软件：** | | | | | | |
| **质保期后**  **维保费用** | | **硬件：** | | | | | | |
| **软件：** | | | | | | |
| **项目实施期** | |  | | | | | | |

**单位名称（公章）：**

**法定代表人（授权代表）签名：**

**联系电话（手机）：**

**年 月 日**

**七、项目调研会议安排：**

时间：2024年7月2日(星期二 )下午14:30

**（请各供应商委派商务及技术人员参会，PPT产品介绍时间不超过10分钟）**

地 点：江苏省口腔医院新综合楼十三楼1301会议室

使用部门：信息中心 陈主任 联系方式：69593126

采购中心：李老师 联系方式：69593206

**注： 1. 提供虚假文件一经查实将终止其参与资格。**

**2. 资料一式四份，加盖单位公章并装订成册，概不退还。**

**3. 其中《报价一览表》除在调研文件中体现外，另需单独封装一份。**

**附件1：南京医科大学附属口腔医院科全路径安全检测与响应平台项目要求**

## 1、硬件要求

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 参数 |
| 1 | 硬件性能参数 | ***提供≥3台标准机架式服务器，单台配置：CPU≥2.4GHz 16核32线程,内存：≥128GB DDR4 3200及以上，系统盘：≥1块240GB SSD，数据盘：≥12块4TB硬盘，冗余电源，2U机箱；接口：≥4千兆电口+≥2万兆光口。性能参数：日志量/天：≥2亿；提供≥3年原厂质保服务。（需提供服务承诺函）*** |

## 2、软件要求

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 参数 |
| 1 | 软件要求 | ★支持将接入的第三方设备进行数据质量效果评级，应至少支持以下三级： 一级安全效果： 日志解析：设备上报日志触发规则后能够生成安全日志，触发一次规则生成一条安全日志； 二级安全效果： 告警聚合：将多条同类安全日志聚合生成告警； 告警融合：将不同来源设备上报的日志融合生成告警，比如天眼与SIP日志融合； 业务误报：能检测到告警是由正常业务访问行为触发，非攻击行为； 三级安全效果： 攻击成功：能够检测出告警的攻击结果为攻击成功； 威胁定性：能够对告警的攻击行为进行定性，比如是否业务行为、病毒行为、定向攻击行为、扫描行为等； 人为攻击：能够检测到告警定性为定向攻击，人为针对性攻击行为； 网端关联告警：网和端设备检测的告警能够关联成一条告警； 网端关联事件：网和端设备检测的事件能够关联成一条事件； 攻击链还原：能够将事件还原攻击过程并形成攻击链； 支持将第三方设备产生的每个级别的数据（日志，告警，事件）进行统计，直观的看出每个设备的数据使用情况； （需提供产品功能截图，并加盖原厂公章） |
| 2 | 全网安全能力监控大屏可展示全网日志、安全告警、安全事件的数量，以及全网日志到告警的削减比例和全网告警到事件的削减比例，并显示自有设备和第三方设备接入的情况，引擎告警和加白的数量，安全事件生成的方式分布以及多源检出、独报的占比等。此外，还支持展示数据采集到数据治理再到数据分析的关键阶段与技术。 |
| 3 | 支持威胁复测，平台支持对来自第三方网络和终端组件的安全告警和审计日志进行二次检测，从而发现组件中误报、漏报，并给出更新后的检测结果。 |
| 4 | 支持告警智能定性分析，可以将告警诊断定性为定向攻击、攻防演练、内部测试、监管通报、病毒、扫描器攻击、脆弱性风险、业务不规范与其他威胁等。 |
| 5 | 支持智能调查功能，通过对威胁情报以及威胁实体IP、域名、MD5的检索，自动进行统计分析，提供全局威胁狩猎，进行快速调查溯源。 |
| 6 | ★多源告警融合： 1、多源告警消减与融合能力，具备对告警进行 payload相似度、单个攻击源对多个目标发起的相似攻击、多个攻击源对单个目标发起的相似攻击等维度的深度聚合归并能力。 2、针对于同一个攻击行为，不同安全设备产生的多条安全告警可以关联融合成同一条告警,点击告警可查看到多条三方子告警 3、将同一个安全事件的不同阶段分散到端和网的告警聚合到同一条事件内，融合后的安全告警举证页面、可以展示不同数据来源的举证字段内容（需提供产品功能截图，并加盖原厂公章） |
| 7 | ★支持攻击链、入口点、父子进程、影响面的还原，可支持进程树纵向拓展至10个及以上层级，横向拓展至15个及以上层级，以对风险资产的复杂威胁提供更全面细颗粒度的展现视角。（需提供产品功能截图，并加盖原厂公章） |
| 8 | 针对终端遥测数据缺失、端点覆盖率不全的场景下，基于网端遥测数据采用图神经网络等AI算法实现故事线自动仿真模拟诊断，最大限度辅助诊断终端遥测数据缺失情境下的威胁风险，在无终端情况下提供近似有终端的安全效果。 |
| 9 | 支持对接入的资产数据进行未知资产分析，可以通过设置规则让需要管理的资产自动入库到资产台账中，支持根据资产的agent安装状态、资产数据源、资产组进行规则配置 |
| 10 | 支持通过开放端口、应用软件、数据库、web服务、web框架、web应用、web站点、账号信息、运行进程、运行服务、启动项、计划任务、注册表维度进行资产清点。清点可展示相关资产列表，包含IP地址、资产责任人、数据源、互联网暴露情况、关键进程等维度。 |
| 11 | 支持针对风险应用查看是否有资产安装该应用，并查看该资产上风险应用的数量及风险应用的介绍。 |
| 12 | 支持智能响应安全事件和安全告警中的关键威胁，针对于高置信度的重复或低危威胁实体可实现全自动化遏制闭环，可支持页面展示事件自动遏制率，可查看智能对抗记录及自定义对抗规则。 |
| 13 | 安全事件响应处置支持对遏制威胁的实体对象自动提取，包括自动化提取安全事件中需要响应处置的“IP、域名、主机、进程、文件”五类实体，查看实体详情列表。针对IP实体支持导出、复制IP、封禁地址、再次封禁、解除封禁、查看情报等操作，针对域名支持处置域名、复制域名、查看情报、导出等操作，针对主机实体支持隔离主机、导出等操作，针对文件实体支持处置文件、导出、查看请报等操作，针对进程实体支持阻断进程、导出、查看请报等操作，针对域名实体支持处置和复制域名、导出、再次处置、解除处置、查看请报等操作。 |
| 14 | ★支持隔离主机的管理，可联动医院现有AES（版本：3.8.6 ）进行隔离主机，展示隔离主机的详细信息，包括主机IP、关联告警、关联事件、处置人、处置时间、处置状态和联动设备等，可对已隔离的主机进行解除隔离。（需提供AES和投标软件平台配置功能截图，并加盖原厂公章） |
| 15 | ★支持封禁地址管理，配置规则可按IP/域名/URL联动医院现有互联网防火墙（型号：AF-2000-FH2350A，版本：8.0.75）设备进行封堵，封禁时长可按天/时/分细粒度进行设置。可对封禁对象进行接除封禁和再次封禁等操作。（需提供AF和投标软件平台配置功能截图，并加盖原厂公章） |
| 16 | 支持最新热点威胁趋势，对热点威胁进行时间轴展示，可展现漏洞名称、风险等级、CVE编号、可检测情况，影响资产、威胁标签、爆发时间。 |
| 17 | 支持平台操作记录，记录包括操作时间、用户名、IP地址、操作类型、操作对象、执行结果、操作描述，同时可基于时间、用户名、IP地址、操作对象、操作类型、执行结果等查找操作日志。 |
| 18 | ★提供对接安全运营服务，实现云端专家针对本院≥30个资产进行7\*24小时托管服务： 1、可在平台界面查看在线安全服务状态、处置阶段与详情，可查看工单跟踪ID、响应时长、当前处理人、闭环时长等信息。 2、支持针对服务平台生成的工单，招标方可按需催单，服务平台采用邮件等方式通知安全专家，督促投标方第一时间处理。 （需提供原厂服务承诺函） |

**附件2：调研文件模板**

**调 研 文 件**

**（正本/副本）**

**项目名称：南京医科大学附属口腔医院全路径安全检测与响应平台项目**

**供应商全称：**

**授权代表：**

**联系电话：**

**日期：**

**目 录**

**…**