深圳市前海蛇口自贸区医院

数据安全监测预警系统建设方案征集

## ****一、征集单位****

深圳市前海蛇口自贸区医院

### ****二、项目概况****

### ****（一）项目名称****

数据安全监测预警系统

### ****（二）项目地点****

深圳市前海蛇口自贸区医院

****（三）**项目内容**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **设备参数** | **数量** | **单位** | **备注** |
| 1 | 数据安全监测预警系统 | 1.支持API资产梳理；通过流量解析的方式自动梳理API列表、应用地址、API路径、请求类型、敏感数据类型、发现时间等，支持通过列表模式展示最近7天请求次数、最近7天访问IP数、最近一次访问时间、是否涉敏、接口状态等。2.支持敏感数据识别；通过对API接口返回内容为JSON、XML的数据进行敏感内容识别。内置敏感数据数据规则特征，特征包含姓名、手机号、身份证号、邮箱，银行卡号等；3.支持API脆弱性分析；通过自动识别接口的脆弱性，包括敏感接口未鉴权、敏感接口参数遍历、明文传输密码、登录弱密码等API存在的数据安全脆弱性。4.支持API风险发现；支持自动识别IP和账号维度的异常行为，例如账号账号多地访问、账号多IP访问等5.数据泄密溯源分析；支持导入、手动输入两种方式，对泄密数据样本进行溯源审计，分析可疑用户的泄密可疑度，以及可疑用户举证，举证信息包括数据访问匹配度可视化、可疑用户访问可疑数据的路径行为展示和访问详细日志等。6.风险报告导出；平台具备风险报告导出，能够根据系统分析结果产出报告。7.支持导入数据分类分级标准，如国家标准“GB/T39725-2020信息安全技术健康医疗数据安全指南”或院内自定义标准等；支持导出指定数据资产清单，需要包括动态指标：今日访问量、数据量与变化；支持关联数据分布应用及风险事件等；8.支持手动匹配数据库，基于数据源的连接和授权，获取其下库、表、字段的层级结构、元数据等信息；支持对采集到的表、字段信息进行删除、Excel导出等管理；支持统计各数据源、库、表、字段下静态数据量、涉敏数据量；9.数据资产总览要求：要求至少包括数据资产名称、数据分类、数据分级、数据类型、今日访问量、数据量与变化、分布应用、关联风险与变化等；10.敏感数据识别规则：支持多种医疗行业专属数据标签识别规则，包括但不限于个人身份信息数据：身份证、社保卡号；联系方式：手机号、邮箱等；支持自定义添加数据标签识别规则；11.API类型识别支持：支持识别HTTP和HTTPS业务中的API接口资产；支持识别RESTFul、SOAP、MQTT、Websocket、GraphQL、JSON-RPC、XML-RPC、Dubbo等API；12.支持手工添加API接口资产；支持导入和导出API资产台账；支持API属性的编辑与删除操作；支持屏蔽特定的API接口资产；查看屏蔽清单并进行屏蔽移除；支持API上下线管理、支持API自动或手动打标签、支持编辑和删除API；13.API资产详情包括：API请求样例、API响应样例；API调用分析，至少含：调用趋势、访问元IP归属地排行；敏感性分析，至少含：数据分类分级统计、数据标签排行；性能与稳定性分析，至少含：调用成功率趋势、吞吐率趋势；脆弱性分析，至少含：弱点等级分布、OWASP TOP10分布、处置状态分布、弱点触发趋势、弱点触发排行Top5；安全性分析，至少含：风险等级分布、风险类型分布、处置状态分布、风险触发趋势、风险触发排行Top5；14.API用户调用安全：支持自动识别和整理用户使用的源IP，形成用户源IP清单；支持根据用户源IP与关联账号风险行为进行用户源IP安全评分、评估用户IP风险等级；支持查看用户详情，对用户进行分析，包括关系图谱分析、行为分析、轨迹分析、风险分析等；15.文件识别：支持从流量中自动识别出文件资产，支持手动添加文件资产信息；至少能识别出文件名称、类型、MD5值等属性；支持对识别出来的文件基于内容进行分类分级及敏感数据标注；16.数据态势大屏功能：提供数据流动整体态势看板，含资产、用户、风险、治理等态势看板；直观展示访问趋势、敏感数据态势、风险趋势、风险态势等；直观展示风险主体TOP5、风险事件TOP5、实时安全告警事件等；大屏汇总转发机和管理机数据和流量，并支持国内国际两个视角绘制数据流转地图；17.支持基于机器学习、智能分词、相似度算法等对文件进行相似度分析和相关性分析；支持对文件资产从文件构成、文件相关性、文件热度、文件操作记录等维度进行分析与可视化呈现，构建文件基础画像。18.支持按单次、每天、每周、每月生成安全报告并发送医院指定邮箱，报告内容需包括资产统计分析、风险统计分析、安全等级评估标准等。19.系统采用数控分离架构设计，实现数据处理转发面与控制管理面的完全解耦，控制管理面负责策略配置、状态监控等功能，数据转发面负责数据包的接受、处理和转发，互不影响；转发机+管理机+功能插件模式：即转发机负责数据处理转发，管理机负责转发机的配置管理监控等，通过功能插件灵活满足多种业务需求；20.串接代理部署：支持串接部署在网络链路中，对用户进出业务系统的流量进行识别、分析、处置、治理等；旁路镜像部署：支持通过交换机镜像端口接收镜像数据实现流量的识别、分析、预警等；分级分布部署：支持向业务系统部署Agent，实现东西向流量的识别、分析、预警等；21.环境部署要求：纯软件交付，支持虚拟化、超融合、私有云、公有云等环境部署；支持部署于信创环境；产品须具备《网络安全专用产品安全检测证书》应用审计类证书；至少3年软件升级。 | 1 | 套 | 部署在1号楼应用区 |

****（四）**项目预算：300000元**

## ****三、参加报名的供应商应具备的条件****

1、具有独立履行民事责任的主体资格；

2、遵守国家法律法规，具有良好的信誉和诚实的商业道德；

3、具有履行合同的能力;

4、所供产品符合国家、行业标准；

5、符合国家相关法律法规和政策要求。

**本着“公平、公开、公正”的原则，欢迎国内厂商填写好《调研表》并与产品相关材料一起（全部资料装订成册，一式五份）送达（寄达）深圳市南山区南海大道1067号蛇口科技大厦主楼6楼北座科教信息部办公室，同时将扫描件发至Email：13923843010@139.com 。**

**调研表**

|  |  |
| --- | --- |
| 产品名称、品牌型号 |  详细方案、产品清单及参数可另附 |
| 厂家/代理商联系人和联系方式 |   |
| 国内销售案例（包括单位名称、联系人和联系电话。一般不少于3个） 请提供中标通知书或合同 |   |
| 主要技术指标 |   |
| 报价（全包价） |   |
| 售后服务及支持方案 |   |
| 驻场要求 |   |
| 后续运行维护及费用情况 |   |
| 服务器配置要求（如需要采购方提供必须填写） |  |

注：需提供公司营业执照复印件，所有材料要加盖公章。

**报名截止时间：2025年9月17日17点。项目专家论证会时间（需准备5分钟的PPT进行项目建设方案的介绍）另行通知。**

**报名联系人：刘曙恒  电话：13923843010**

**项目技术需求及沟通联系人：陈良森 电话：18033057806**