广东省中医院API风险监测系统项目需求书

**一、项目内容**

1. **项目概述**

为响应和落实国家有关政策要求，从医院数据安全需求出发，为了不断推进完善医院数据安全体系化建设，拟开展“广东省中医院API风险监测系统项目”。

随着医院业务扩展，应用系统逐年增加，应用间、应用与数据库之间的API调用量随之增多，数据流转路径变得更为复杂，数据层面的安全措施存在明显短板。针对敏感数据泄露、API自身脆弱性、API相关攻击行为等几类典型的API风险，当前欠缺专业技术手段进行体系化的实时监测、审计、溯源，面对相关风险存在无法实时感知、难以确认风险影响面，应用和数据库与API之间关联关系不清晰的问题，这也导致针对现有的大量API资产无法实现有效管理，数据安全方面存在明显隐患。基于上述背景，采用专业的API风险监测系统成为筑牢医院数据安全防线的必然选择。

1. **功能需求**

1.系统应能够实现对应用、数据库和API的资产实现发现和纳管功能，其中可纳管应用数量不少于400个，数据库数量不少于400个，API数量不少于2000个。应用、数据库与API之间应能以直观形式建立关联关系，便于运维人员对监测到的API风险项做出判断。

2.系统应能够定期更新特征库、规则库，保证能够监测和识别到新发的API风险并予以告警；更新频率不少于每季度1次。

3.系统应支持对API风险进行分级分类，精准识别命令注入攻击、跨站脚本攻击、非工作时段访问、敏感数据泄露、撞库、暴力破解、使用异常参数访问接口等攻击行为，以及接口未授权访问、明文传输口令等API自身缺陷。

4.系统应具备对API资产进行全生命周期管理的能力，对API资产的活跃和失活状态予以标记，并能向运维人员呈现必要的提示。

5.系统应保留发生数据交互的原始报文，包括源和目标IP地址、应用完整路径、请求方法、传参和响应体，具体的涉敏内容等。具备对通过API传输数据和文件留下完整记录的能力，以便对可能存在的敏感数据和文件泄露风险进行评估、审计和溯源。

6.系统应支持自定义规则，在默认规则库的基础上定制与业务特性有更强关联度的个性化API风险监测规则。

7.系统应支持自定义数据特征，对未包含在默认敏感数据类型库当中的重要数据定制规则以进行识别和监测。

8.系统应具备向其他安全设备或安全系统外发Syslog日志的能力。

9.系统应具备合理的白名单配置规则，以便对必要且符合正常业务逻辑的数据流转进行加白。

10.系统应支持API画像或类似功能，能够通过接口业务情况、接口访问情况、数据暴露情况和风险情况等多维度信息对接口的访问及其风险进行画像分析，包括数据流转趋势、数据暴露分布、访问分布和风险分布等详情。

11.系统应支持部署在VMware等主流虚拟化平台，且支持国产化平台部署。

12.推荐项：对API风险项进行验证、复核的能力。

**二、基本要求**

1.采购内容：API风险监测系统两套。本项目标的为纯软件，不含硬件设备。

2.应标产品应具有在二级以上医疗卫生机构或金融行业、运营商用户等实施案例，并能予以详细说明。

3.应标产品应满足等保合规要求。

4.应标产品应包含不少于三年的软件维保服务，以及不少于三年的特征库、规则库升级服务。

5.本项目为一个整体，投标人须对全部内容进行投标，不得分拆。

6.本项目不接受联合体投标。