**数据安全与商用密码应用安全评估项目**

**用户需求书**

## 项目背景

在医院信息化建设过程中，与之关联的基础和关键业务，会衍生关键数据、隐私数据、机密数据等，传统的基础安全防护手段心有余而力不足，数据安全已然成为了数据交换和共享平台核心的关切点，目前院内只部署了简单的数据库防护系统，未形成数据安全防护体系。

2020年1月1日《中华人民共和国密码法》的正式施行，更是为密码产业的规模化发展提供了重大机遇，也为商用密码应用市场的发展提供了广阔舞台。同时，作为指导商用密码应用与安全性评估工作的基础性标准，《信息安全技术信息系统密码应用基本要求》（GB/T39786-2021）也已经于2021年10月1日正式实施，这对于规范和引导信息系统合规、正确、有效应用密码，切实开展密评建设工作具有重要意义。密评将以评促建、以评促改、以评促用的方式，逐步引导网络运营者的密码规范使用，最终确保商用密码在重要信息系统和关键信息基础设施中使用的正确、合规、有效。

## 项目建设清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **产品清单** | **详细技术要求** | **数量** |
| 1 | 数据库资产梳理 | （1）能够根据资产价值评估结果、资产脆弱性评估结果、资产威胁评估结果综合计算，评估出数据资产的综合分值  （2）支持数据库漏洞扫描、数据库配置缺陷扫描、数据库弱口令扫描等数据库风险检测。  （3）支持数据库资产的发现  支持发现网络中所有的数据库，包括数据库类型、版本、IP、端口等信息:包括常见的关系型数据库mysql、sqlserver、Oracle、sqlpostgre、mongDB，国产数据库人大金仓、达梦、神通等。  1.可自动和手动的进行资产的盘点，并生成盘点报告。  2.盘点内容包括自动发现资产、资产风险情况扫描、资产网络连通性扫描、资产保护情况扫描。  （4）三年原厂质保 | 1台 |
| 2 | 数据库动态脱敏 | （1）支持动态脱敏功能，  （2）性能指标：脱敏峰值处理能力：8万条SQL/秒 吞吐量支持，并发连接数≥2000；  （3）动态功能模块包括：监控墙、数据源配置、脱敏权限管理、脱敏任务配置管理、脱敏报告管理、日志管理、系统管理。  （4）内置30种敏感数据类型用于敏感数据的发现，可覆盖政府、金融、学校、企业等多个行业相关的敏感数据类型。  （5）不限制实例数，三年原厂质保 | 1套 |
| 3 | 互联网医院商用密码应用安全性评估服务 | (1)物理和环境:信息系统重要区域环境，密码安全防护措施评估。  (2)网络和通信:访问和操作政务系统，客户端和系统服务器之间的网络和通信密码防护措施评估。  (3)设备与计算、服务器、网络设备、安全设备的操作和管理的安全防护评估。  (4)应用和数据应用系统本身的用户登录、数据传输、数据加密等各个环节的密码应用措施评估。  (5)密钥管理、密钥体系、密钥功能、密钥管理等是否符合要求评估。  本次针对互联网医院系统开展商用密码应用安全性评估，提出整改要求，依据 GB/T39786-2021《信息系统密码应用基本要求》对信息系统的密码应用合规性、正确性与有效性进行评估，最终评出“符合”、“基本符合”与“不符合”的评估结论，并出具正式的《商用密码应用安全性评估报告》。报告需按照国家或省密码管理部门的统一要求出具，并需要通 过当地密码管理局备案 | 1项 |
| 4 | 国密堡垒机 | 1. 性能要求：字符并发连接≥1000个，图形并发连接≥300个，授权资产≥1000个。 2. 支持手机APP动态口令认证方式登录堡垒机，新用户首次登录后需强制绑定APP动态口令；支持AD、LDAP、RADIUS、吉大正元、北京CA、深圳CA认证系统联动登录堡垒机；支持多个AD域认证源；支持自动同步AD/LDAP用户。 3. 支持自动收集设备IP、运维协议、端口号、账号、密码、与用户的权限关系，可自动完成授权。 4. 支持B/S架构进行堡垒机运维管理，至少支持使用IE、谷歌、火狐、Microsoft Edge等浏览器打开堡垒机的Web页面直接调用mstsc、VNC、Xshell、SecureCRT、Putty、winscp、flashFXP、FileZilla、SecureFX等本地运维客户端工具。 5. 支持Windows/macOS操作系统下C/S架构的堡垒机专用客户端，可通过此专用客户端登录堡垒机，对堡垒机进行简单的管理及运维资产操作。 6. 客户端支持通过访问域名堡垒机，且客户端支持AD认证、第三方认证系统联动认证登陆。 7. 支持使用本地的SecurCRT/Xshell/OpenSSH工具通过SSH网关代理方式直接登录字符设备。   (8)支持对运维操作会话的在线监控、实时阻断；支持录像慢速/快速回放（、支持记录起止时间、来源用户、来源IP、目标设备、协议/应用类型、命令记录、操作内容（如对文件的上传、下载、删除、修改等操作等）的详细行为日志。  (9)支持运维用户查询用户本人的运维审计会话，减轻审计管理员的负担，并且帮助运维用户提高运维效率。  (10)支持输出堡垒机告警和自身状态信息；支持邮件/Syslog/钉钉告警方式输出告警日志，可配置日志重要程度；支持通过SNMP方式输出系统信息.  (11)支持采用国密加密算法进行核心敏感数据进行加密存储，且支持使用软件/硬件方式加密，以保证重要数据在系统内存储的机密性和完整性。  (12）三年原厂质保 | 1台 |
| 5 | 数据安全咨询服务 | 在服务期内，需结合医院实际情况，提供信息化规划指导、安全咨询、技术咨询等数据安全相关的服务。 | 1项 |
| 6 | 商用密码应用安全性评估咨询服务 | 1. 在测评期间，协助院方收集资料，配合整改，帮助医院顺利完成商用密码应用型评估。 2. 在服务期内，需结合医院实际情况，提供信息化规划指导、安全咨询、技术咨询等商用密码应用安全相关的服务。 | 1项 |
| 7 | 产品应急响应服务 | (1)在质保如遇到重大故障，维保人员承诺并可实现30分钟内响应，两小时内工程师到达现场提供现场技术服务。  (2)重大节假日以及特殊时期，为医院开通24小时服务，对服务需求随时响应。 | 1项 |