**重庆医科大学附属儿童医院**

**网络安全等级保护、数据分类分级及风险管理建设项目概况及要求**

# ****一、项目概况****

为全面落实《网络安全法》《数据安全法》及等级保护2.0要求，提升网络安全防护能力和数据安全管理水平，构建全方位、多层次的安全防护体系，通过等级保护建设、数据分类分级管理、数据安全管控平台和攻防能力建设等关键措施，建立更加完善的安全防护机制。项目建设主要包括三个主要内容：

一是网络安全等级保护建设，将升级部署符合等保2.0标准的下一代防火墙、入侵防御检测系统等专业设备，重点强化网络边界防护和访问控制能力；

二是数据分类分级及风险管理平台建设，通过建立完善的数据资产目录和分类分级标准，实现对各类数据的精准识别和动态管控，通过数据安全态势感知平台建设，整合多源安全数据，运用智能分析技术，构建实时监测、精准预警的主动防御体系；

三是攻防演练平台及装备，通过专业网络安全攻防实训平台和实战演练，持续检验和提升安全防护能力。

# ****二、项目要求****

## 项目清单

| **项目类别** | **设备名称** | **描述** | | **数量** | **单位** |
| --- | --- | --- | --- | --- | --- |
| 网络安全等级保护建设 | 防火墙1 | 边界防火墙 | | 1 | 台 |
| 防火墙2 | 管理区、银医专网防火墙 | | 3 | 台 |
| 应用防火墙 | 应用系统边界防火墙 | | 2 | 台 |
| 入侵防御检测 | 应用系统防御检测 | | 2 | 台 |
| 漏洞扫描 | 服务器操作系统、基线安全检查 | | 1 | 台 |
| 运维审计 | 运维堡垒机及运维操作记录、审计 | | 1 | 台 |
| 网络安全态势感知 | 网络入侵、行为分析、溯源分析 | | 1 | 套 |
| 数据分类分级及风险管理平台建设 | 数据分类分级系统 | 各类数据分类分级 | | 1 | 套 |
| API应用安全审计系统 | 检测API数据安全风险 | | 1 | 套 |
| 数据安全管理平台 | 综合数据安全态势情况 | | 1 | 套 |
| 攻防演练实训平台及装备 | 攻防演练实训平台 | | 网络安全技能学习、演练平台 | 1 | 套 |
| 平台辅助装备 | | 网络安全演练个人装备 | 5 | 台 |

## 网络安全等级保护建设要求

| **设备名称** | **描述** | **数量** | **单位** |
| --- | --- | --- | --- |
| 防火墙1 | 1.性能要求：防火墙吞吐量≥16Gbps，IPS吞吐量≥10Gbps，AV吞吐量≥6Gbps，最大并发连接数≥250万，每秒新建连接数≥13万，IPSec VPN吞吐量≥5Gbps。  2.配置要求：标准机架式1U设备，千兆电口≥8，千兆光口≥8，万兆光口≥2；配置ZTNA零信任并发用户数≥8个，IPSec VPN隧道≥6000；配置2个冗余交流电源，配置2块不少于960 GB硬盘（单块），配置6年IPS入侵防御/AV防病毒/URL过滤/C2僵尸网络防御/云沙箱特征库升级许可和原厂维保服务。  3.智能威胁防御：具有未知威胁检测能力，支持与云沙箱和本地沙箱联动，实现对APT攻击的防御功能。  4.策略管控：能够基于时间、用户/用户组/安全组、应用层协议、地理位置、IP地址、端口、域名组、URL分类、接入类型、终端类型、设备组、内容安全统一界面进行安全策略配置。  5.路由功能：支持静态路由、策略路由、RIP、OSPF、BGP、ISIS等路由协议。  6.IPv6: 支持IPv6协议栈、IPv6穿越技术、IPv6路由协议。  7.最近3年以来IDC市场排名前三。  8.不得与防火墙2、应用防火墙同一品牌。 | 1 | 台 |
| 防火墙2 | 1.性能要求：防火墙吞吐量2.5Gbps，最大并发连接数≥300万，每秒新建连接数≥8万；IPS吞吐量≥1.8Gbps，IPSec VPN吞吐量≥2.1Gbps，SSL VPN吞吐量≥300Mbps，IPSec VPN隧道数≥4000，SSL VPN并发在线用户数≥500。  2.配置要求：标准机架式1U设备，千兆光口≥8，千兆电口≥2，万兆光口≥2。配置SSL VPN授权≥100，虚拟防火墙数量≥100，配置不少于200GB固态硬盘，配置2个冗余交流电源，配置6年IPS入侵防御/AV防病毒/URL过滤功能授权和原厂维保服务。  3.支持静态路由、策略路由、RIP、OSPF、BGP、ISIS、SRv6等路由协议。支持NAT地址复用技术，可实现单个公网IP地址的无限制端口转换，可有效解决地址短缺问题。  4.支持URL识别能力和URL地址识别库，云端URL识别库≥1.2亿，可识别应用层协议数量≥6000种。  5.系统预定义IPS签名数量≥13000，CVE和CNNVD编号的签名条目数不得少于8000，支持用户自定义签名规则，支持正则表达式。  6.双机主备模式故障切换时间<1秒。  7.最近3年以来IDC市场排名前三。  8.不得与防火墙1、应用防火墙同一品牌。 | 3 | 台 |
| 应用防火墙 | 1.性能要求:防火墙吞吐量≥10G，应用层吞吐量≥4G。  2.配置要求：标准机架式2U设备，配置2个冗余交流电源，配置不少于960 GB硬盘（支持扩展至40T），具备液晶屏，支持接口聚合与接口联动，支持热备、集群及插件式部署。千兆电口≥8，千兆光口≥4，扩展槽位≥8。配置6年应用识别特征库、URL地址库、WEB防护特征库和原厂维保服务。  3.具备HSTS、IP信誉、HTTPS检测、语义引擎、智能补丁等功能。支持HTTPS国密算法。  4.支持XML防护、人机识别、动态混淆防护、API资产梳理、API攻击防护、OAS合规检测、ARP欺骗防护等功能。  5.除支持常见的串联、旁路、反向代理、镜像监听部署模式外，支持Nginx插件部署，插件及部署模式不会影响现有业务。  6.支持串联、反向代理和旁路部署时VRRP功能。  7.最近3年以来IDC市场排名前三。  8.不得与防火墙1、防火墙2同一品牌。 | 2 | 台 |
| 入侵防御检测 | 1.性能要求:防火墙吞吐量≥10G，应用层吞吐量≥4G。  2.配置要求：标准机架式2U设备，配置2个冗余交流电源，配置不少于960 GB硬盘（支持扩展至40T），具备液晶屏，支持接口聚合与接口联动，支持热备、集群及插件式部署。千兆电口≥8，千兆光口≥4，扩展槽位≥8。配置6年应用识别特征库、URL地址库、WEB防护特征库和原厂维保服务。  3.支持IPv6/IPv4双协议栈，能识别IPv4和IPv6流量。支持IPv6环境下攻击检测技术和基于IPv6地址格式的安全控制策略。配置6年应用识别特征库、URL地址库、WEB防护特征库和原厂维保服务。  4.支持如勒索、挖矿、SQL注入、XSS注入、webshell、命令代码执行、内存破坏、类型混淆、反序列化、信息泄露、目录遍历、文件操作漏洞、注入攻击、重定向漏洞、CSRF、僵木蠕、拒绝服务、弱口令、欺骗劫持、扫描类攻击等。  5.支持自定义报表模板，可设置报表封面、logo等信息；可选报表维度、可配置过滤条件、可设置执行周期、数据统计区间、并可配置报表格式和输出方式（如本地存储、邮件外发或FTP外发）、支持PDF、html、docx、xlsx等格式；支持设置手动报表、自动报表。  6.支持多种威胁情报场景，可针对不同场景的威胁攻击进行检测，包括APT检测/挖矿检测/勒索检测/反诈检测/失陷检测/暗网节点检测。  7.最近3年以来IDC市场排名前三。 | 2 | 台 |
| 漏洞扫描 | 1.配置要求：标准机架式2U设备，配置2个冗余交流电源，内存≥16G，配置不少于4T B硬盘，千兆电口≥6，万兆电口≥2。提供无限制扫描IP授权、无限制WEB漏洞扫描URL授权。配置6年特征库升级和原厂维保服务。  2.具备全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息，并可查看详情；支持快速进行漏洞验证，验证漏洞有效性。  3.具备从漏洞视角分类型呈现风险概览和详情信息功能，可一键加白名单，支持在线查看展示“系统漏洞”、“WEB漏洞”、“弱口令”和“基线风险”的名称、风险等级、漏洞数、最近发现时间，并可关联漏洞详情。漏洞详情可支持展示漏洞名称、CVSS漏洞评分、漏洞类型、发现时间、影响资产、漏洞描述、漏洞影响、修复建议、CVE编号、CNCVE、CNNVD编号和举证信息。  4.具备全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB漏洞扫描、基线配置核查功能，其中全面扫描支持系统漏洞扫描、WEB漏洞扫描、弱口令扫描同时执行，可同时输出包含系统漏洞扫描、WEB漏洞扫描、基线配置核查、弱口令扫描结果的报表。  5.具备紧急漏洞进行单独评估功能，实现紧急漏洞批量排查，包括Microsoft Windows RDP 远程代码执行漏洞（CVE-2019-0708）、OpenSSL Heartbleed 心脏滴血漏洞（CVE-2014-0160）、Windows SMB 远程代码执行漏洞（MS08-067）、Windows SMB 远程代码执行漏洞（MS17-010）等。  6.内置不同的系统漏洞模板，包括高可利用系统漏洞、原理检测系统漏洞、系统漏洞、数据库漏洞等类型，支持报表形式展示漏洞模板风险等级分布概览，支持报表形式展示漏洞模板详情，包括漏洞总数、漏洞名称、漏洞类型、风险等级等信息。  7.最近3年以来IDC市场排名前三。 | 1 | 台 |
| 运维审计 | 1.配置要求：标准机架式2U设备，配置2个冗余交流电源；内存≥16GB千兆电口≥6，千兆光口≥4，配置不少于4TB硬盘，USB口≥2，RJ45串口≥1。配置资产授权数量≥500个，运维用户无限制。配置6年原厂维保服务。  2.支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等。  3.支持基于不同的用户设置不同的双因子认证模式，支持手机APP动态口令及微信小程序动态口令认证方式登录堡垒机，支持使用基于国密算法的动态令牌、国密USBkey对堡垒机的登录实行双因素认证。  4.支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin、X11；支持ssh、telnet、rlogin、rdp、vnc等协议的H5运维，无需本地运维客户端工具。支持DB2、oracle、mysql、sqlserver、PG、人大金仓、达梦数据库的协议运维代理，可实现自动登录，可直接调用本地windows系统的数据库客户端工具无需应用发布前置机。  5.具备工单管理能力，支持运维工单、密码工单、紧急运维工单、命令审批、运维复核、运维任务的审批规则配置。具备定期自动修改windows服务器、网络设备、linux/unix等目标设备密码的功能。  6.支持对审计录像、键盘记录、文件审计、字符输出审计、数据库双向审计等进行控制；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、拖拽查看功能。  7.最近3年以来IDC市场排名前三。 | 1 | 台 |
| 网络安全态势感知 | 1.分析平台\*1台。配置要求：标准机架式2U设备，配置2个冗余交流电源；内存≥128GB；千兆电口≥4，具备1个扩展板卡插槽；配置不少于960GB系统盘，数据盘≥8\*8TB SATA；日志接入能力：≥30000eps。含系统软件一套。配置6年威胁情报升级授权及原厂维保服务。  2.网络威胁流量监测探针\*2台。单台配置要求：标准机架式2U设备，配置2个冗余交流电源；千兆电口≥8，万兆光口≥4，具备1个扩展板卡插槽；配置不少于4TB硬盘；应用层吞吐量：≥5G。包含基础系统软件一套，包括网页漏洞利用检测、webshell上传检测、网络攻击检测、威胁情报检测功能，提供离线pcap包导入检测、基础旁路阻断和基础SSL解密功能。配置6年威胁情报升级授权与检测引擎规则升级授权及原厂维保服务。  3.产品支持对勒索告警进行专项分析，可识别勒索家族包括：Cerber、Tescrypt、Strictor、WannaCry等；威胁统计包括：活跃勒索家族（受害资产数）分布统计、勒索受害资产Top10、勒索告警趋势图；勒索告警信息包括：最近发生时间、资产IP、勒索家族、勒索阶段、告警次数、攻击结果、威胁级别、级联单位、资产分组、资产类型、告警来源、告警设备，以及对应的详细告警列表。  4.产品支持发现和还原流量中的文件传输行为，包括RAR、ZIP、GZ、7Z、tar等压缩格式文件，EXE、apk、DLL、COM、bin、OCX、SYS等可执行文件，pdf、rtf、ppt、txt、word、excel等文档类型文件，并记录文件MD5发送至分析设备。实现基于webshell函数的攻击检测，如文件包含漏洞、任意文件写入、任意目录读取、任意文件包含、preg\_replace代码执行等。  5.具备灵活开启机器学习模型能力，增强检测精度，模型至少包括：ICMP隧道检测、DNSTunnel检测、HTTP隧道检测、CS流量检测、MSF检测、挖矿流量检测、代理流量检测、暗网流量检测、弱口令检测、SSH爆破登录成功检测。  6.最近3年以来IDC市场排名前三。 | 1 | 套 |

## 数据分类分级及风险管理平台建设

| **项目** | **描述** | **数量** | **单位** |
| --- | --- | --- | --- |
| 数据分类分级系统 | 1.配置要求：标准机架式2U设备，配置2个冗余交流电源；处理性能≥100字段/秒。CPU：≥12核\*2颗，内存：≥128G，配置不少于32TB硬盘，万兆光口≥2，接口扩展插槽≥2。无数据库接入数量限制，配置6年原厂维保服务。  2.支持手动新增、批量导入两种方式添加数据源，并支持数据源信息的批量导出。支持通过指定IP段、端口方式，定时扫描当前网络环境下的数据库资产。  3.支持以库、表、列方式对于数据资产目录进行可视化展示，数据表资产信息包含但不限于：数据源、主机、库名、分类、分级、是否梳理、业务系统、部门、责任人、最后梳理时间、字段数等。可对于结构化分类分级任务进行相关配置，包括：数据源、抽样策略、执行逻辑、打标方式。  4.支持结构化分类分级任务流程化执行向导，包括：分类分级预测、人工校验打标、结果自动纠错等环节。支持对于非结构化文件进行分类分级，可支持的文件类型包括：doxc/doc/txt/pdf/dcm，且支持非结构化分类分级模版的维护。  5.能够通过AI大模型能力，帮助医院自动生成数据分类分级框架，并对分类分级结果进行自动化持续优化，包括：生成类别、生成级别、生成示例、拆分类别。能够通过调用AI大模型能力，帮助医院提升分类识别率与准确率，并给出大模型输出结果的“识别说明”，帮助人工更好地判断其结果是否准确。  6.系统能提供数据安全分类分级监管可视化大屏，包含数据源数、表数、列数、已梳理列数、数据分级/分类分布、数据源风险评分TOP、数据源弱密码风险数TOP等信息。  7.产品需通过由中国信息通信研究院检验的数据安全产品进阶能力测评；为保证产品稳定性。 | 1 | 套 |
| API应用安全审计系统 | 1.配置要求：标准机架式2U设备，配置2个冗余交流电源，吞吐量：≥5Gbps。CPU：≥20核40线程，内存：≥64G，配置不少于16TB硬盘，管理口≥1、千兆电口≥4、万兆光口≥2。配置6年风险特征库升级及原厂维保服务。  2.支持以agent和镜像流量混合模式采集流量，支持解析Restful、GraphQL、SOAP、JSON-RPC、XML-RPC、WebSocket协议的API流量。能自动识别流量中的应用系统，并对同应用进行合并，形成应用清单；  4.内置敏感数据标签，包括身份证号、手机号、银行卡号、姓名、地址、邮箱等个人敏感数据标签，能自动识别文件中包含的敏感数据标签。  5.内置脆弱性风险策略，至少包括：敏感接口未鉴权、认证令牌有效期过长、水平越权、脱敏策略不一致、任意文件读取、源代码泄漏、系统信息泄漏、敏感文件泄露等。  6.内置应用漏洞监测规则，覆盖Apache Spark、OpenAPI、Weblogic等常用组件未授权漏洞监测规则、敏感文件泄漏监测规则，命令执行漏洞监测规则等。  7.支持以IP、账号、IP+API、账号+API、数据维度进行行为风险配置，可根据风险日志自动绘制API风险链路关系。当监测到流量中有风险行为时能自动预警。  8.具备HTML、PDF、png、word多种格式的报表订阅功能，内置API数据安全运营、应用、文件、API、账号等专项分析报告。  9.支持通过开发接口或Kafka同步数据。能够对接AI大模型，授权AI自动纠偏API划分以及脆弱性风险告警的结果，支持立即执行存量API资源的划分、打标、聚合。  10.为保证产品的技术能力，产品需通过由中国信息通信研究院安全能力评估，获得API安全能力先进级产品认证。 | 1 | 套 |
| 数据安全管理平台 | 1配置要求：标准机架式2U设备，配置2个冗余交流电源，数据采集和处理性能≥50000EPS。CPU：≥24核\*2颗，内存：≥256G，配置不少于32TB硬盘，千兆电口≥4、万兆光口≥2。配置6年风险特征库升级及原厂维保服务。  2.综合安全态势支持展示数据安全防护情况，对数据安全告警进行分析，展示告警数量、告警类型分析、告警趋势分析、实时告警、数据接口安全风险、数据库安全风险。  3.对资产纳管情况进行统计，展示数据库、数据表、数据字段、业务应用、接口、账号数。敏感数据态势支持展示敏感数据在系统内的分布情况，清晰展现不同级别敏感表及敏感字段的数量、占比、数据库分布情况、敏感数据访问情况，以敏感数据为核心实时展现告警，支持告警详情下钻。  4.数据接口安全态势支持从接口的访问情况进行分析，展示接口的IP访问分布、接口访问TOP、接口访问趋势、敏感接口数量及占比、告警类型分布、高中低告警趋势、实时告警情况。  5.平台支持对分类分级、数据脱敏、数据安全网关、数据库审计、API应用安全审计、数据防泄漏等组件进行管理，支持组件单点登录。支持依据聚合规则定时聚合告警信息，有效降低告警数量。  6.支持告警的集中管理和智能分析，包括但不限于来源IP、目的IP、告警类型、事件名称、关联单位部门、告警等级等多维度分析字段，显著提升安全事件调查和分析的效率与精准度。  7.支持安全事件处置全流程管理，支持生成工单，实现事件从记录到处理的闭环管理。支持对特定数据内容进行追踪，包括但不限于搜索身份证内容、银行卡内容、手机号内容，系统将以数据内容为中心，将数据内容流经的数据源、应用系统、访问源进行追踪。支持用户角色的创建与管理。 | 1 | 套 |

## 攻防演练实训平台及装备

| **项目** | **描述** | **数量** | **单位** |
| --- | --- | --- | --- |
| 攻防演练实训平台 | 1.具备基础课程学习功能，内容呈现应支持视频、图文等多种内容形式，并具备学习进度管理能力。具备实战课程学习功能，需提供实战课程的操作模拟环境搭建功能，课程内容需与实际安全场景结合设计。具备理论赛题练习功能，理论赛题适配单选、多选 、判断等题型，且实现答题过程中的即时反馈。具备CTF赛题练习功能，CTF 各类别（WEB/PWN 等）赛题的环境支撑功能，赛题解题思路的辅助呈现功能。  2.具备行业大赛真题使用功能，行业真题的内容分类与检索功能，真题与行业安全知识的匹配设计。具备夺旗赛组织功能，夺旗赛的规则配置（如 flag 设置、分值调整）功能，比赛过程的实时监控功能。具备运维赛组织功能，运维赛的场景模拟（如故障排查、配置优化）功能，比赛结果的自动评分功能。  3.具备后台学习统计功能，学习数据（如完成率、正确率）的统计维度设置功能，数据可视化呈现功能。具备后台工具库资源上传功能，工具资源的格式兼容（如压缩包、文档）功能，资源的分类标签管理功能。具备后台题库管理功能，理论 / CTF 题库的批量导入 / 导出功能，题目难度等级与知识点关联的标注功能。  4.具备课程学习与赛题练习结合功能，课程知识点与对应赛题的自动匹配功能，学习进度与练习权限的联动功能。具备实战课程与CTF 赛题关联功能，实战课程操作模块与 CTF 赛题考点的衔接设计，课程实操成果与赛题解题的辅助功能。  5.具备学习数据统计与学习课程匹配功能，基于学习统计数据对课程薄弱环节的定位功能，基于统计结果的课程内容推荐功能。具备工具库资源与实战课程适配功能，实战课程操作步骤与工具库资源的调用联动功能，工具使用说明与课程内容的整合设计。  6.学习统筹与资源协调的要求，完成院方学习需求对接，调整学习内容难度，确保契合实际需求。统筹管理学习资源与内容，确保教学资料的完整性与时效性。把控整体学习内容与时间安排，确保学习计划高效执行。  7.网络安全理论授课的要求，面向医院业务场景，内置 Web 漏洞原理、密码学基础、二进制漏洞利用逻辑、AI 安全威胁模型等核心知识；结合医疗数据泄露、加密传输、智能诊断系统失效等真实案例，剖析漏洞成因、攻击路径与防御思路，并演示对应工具的使用方法，为实训及竞赛奠定理论框架。  8.网络安全实训的要求，配置学习指导工作，统筹组织模拟竞赛，从 Web 漏洞挖掘与防御、密码学、逆向工程及 PWN 等多题型维度，系统评估实战能力与知识掌握程度。参与赛题设计，负责模拟竞赛全流程组织，并牵头开展赛后复盘分析，提炼问题、总结经验以优化竞赛与学习体系。  制定实操考试标准化流程，落地执行考试组织工作，同步完成学习成果评估，通过科学考评机制保障学习质量达标。基于表现与测试结果，制定个性化能力提升方案，聚焦实战技能强化与竞赛应对策略优化，助力突破能力短板。  9.学习闭环与后续支持的要求，归集学习档案，编制总结报告，形成完整的学习记录。跟踪学员后续学习需求，提供持续技术支持，实现学习闭环管理。  10.技术人员现场支持的要求， 需配备三名技术人员现场支撑，支撑人员须有国家级护网经验。技术支撑团队需参与过省级及以上攻防比赛，且获得过比赛二等奖及以上奖项。  11.提供6年原厂商维保。 | 1 | 套 |
| 平台辅助装备 | 笔记本电脑配置应高于或者等于如下：  搭载Intel 12代酷睿i5-12500H处理器（主频2.5GHz，睿频4.9GHz），内存16G、硬盘（SSD1T），配备RTX3060/3070显卡 | 5 | 台 |

# 三、报价要求

**注意事项：按附件1（市场调查表）进行填报，如漏项、增项、修改项则无效，报价时需有单价、总价、合计，并盖公章。**

1、本项目为交钥匙工程，供应商需综合评估所有风险。报价应包含有可能涉及的所有费用。

2、人民币报价，报价包括但不限于人工费、培训费、劳务费、保险费、税费、安装调试费等维保单位提供维保服务而产生的所有费用。

3、上述清单，提供6年原厂商维保。

**4、请提供所有调查产品的价格支撑材料，近12个月内的合同复印件（关键页），模糊不清晰的无效。**

附件1.市场调查表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 网络安全等级保护、数据分类分级及风险管理建设市场调查表 | | | | | | | |
| 序号 | 名称 | 品牌、规格型号 | 制造商 | 原产地 | 数量 | 单价 | 合计 |
| 网络安全等级保护建设 | | | | | | | |
| 1 | 防火墙1 |  |  |  | 1 |  |  |
| 2 | 防火墙2 |  |  |  | 3 |  |  |
| 3 | 应用防火墙 |  |  |  | 2 |  |  |
| 4 | 入侵防御检测 |  |  |  | 2 |  |  |
| 5 | 漏洞扫描 |  |  |  | 1 |  |  |
| 6 | 运维审计 |  |  |  | 1 |  |  |
| 7 | 网络安全态势感知 |  |  |  | 1 |  |  |
| 数据分类分级及风险管理平台建设 | | | | | | | |
| 1 | 数据分类分级系统 |  |  |  | 1 |  |  |
| 2 | API应用安全审计系统 |  |  |  | 1 |  |  |
| 3 | 数据安全管理平台 |  |  |  | 1 |  |  |
| 攻防演练实训平台及装备 | | | | | | | |
| 1 | 攻防演练实训平台 |  |  |  | 1 |  |  |
| 2 | 平台辅助装备 |  |  |  | 5 |  |  |
| 总计 | | （小写） 元 | | （大写）： 元整 | | | |
| 供应商名称（盖章）： | | | | | | | |