**采购内容及要求**

**一、项目概述**

（一）项目背景

2022年西安教育系统网络与信息安全评估保障项目，针对西安市教育局机关、直属学校、直属单位以及区县教育局的网络系统、系统规模庞大、管理分散、网络系统标准不一、教育局及直属学校/单位的网络安全状况无法及时获取等问题，建设了覆盖全市近3000所学校的用户管理系统、网络信息管理系统、网络安全管理系统、应急响应系统、学校信息系统，满足了全市教育局系统信息用户集中管理需求、网络安全持续检测需求；对26个西安市教育局及直属单位进行了正版化系统及办公软件的安装工作，实现了可安装正版化系统的办公电脑全正版化覆盖；对西安市教育局及直属单位的网络现状进行了网络情况摸查工作、对内部网络进行了漏洞扫描工作、对现有网页服务器进行漏洞扫描工作，根据以上收集情况向单位、院校给出改造意见及系统定级意见；向西安市教育局及直属单位提供信息化咨询服务。

为进一步加强西安市教育网络系统安全管理工作，提高信息化管理水平，西安市教育局计划2023年继续实施西安教育系统网络与信息安全评估保障项目，主要包含网络安全管理系统云资源服务、网络安全攻防实训服务、正版化软件服务、安全巡检服务4部分。

（二）项目概况

本项目包含网络安全管理系统云资源服务、网络安全攻防实训服务、正版化软件服务、安全巡检服务4部分，旨在全面提升西安市教育系统网络安全管理水平和办公信息化水平，更好的支撑西安市教育系统各项业务发展。

（三）项目目标

项目将严格落实《中华人民共和国网络安全法》、《关于推进教育新型基础设施建设构建高质量教育支撑体系的指导意见》等文件精神，持续做好网络安全管理系统的云平台服务；对接市教育大数据平台实现数据互通；实现西安市教育局及直属单位软件正版化，通过培训、实训、校园日等活动培养专业网络安全技术人才队伍。

**二、功能需求**

本项目包含网络安全管理系统云资源服务、网络安全攻防实训服务、正版化软件服务、安全巡检服务4部分。

采购清单如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **名称** | **功能模块** | **数量** |
| 1 | 网络安全管理系统服务 | 云端应用服务 | 1套 |
| 云端主机安全服务 |
| 云端应用安全服务 |
| 弹性IP服务 |
| 接口对接及数据整理服务 |
| 2 | 网络安全攻防实训服务 | 通过风险排查与加固、渗透性测试等方式提升现教中心整体安全防护能力 | 1项 |
| 3 | 正版化软件服务系统 | 为西安市教育局及直属26家单位已安装操作系统及办公软件的设备提供正版软件区域授权服务1年 | 1项 |
| 4 | 安全巡检服务 | 安全巡检服务 | 1项 |
| 巡检报告上载 |
| 巡检报告下载 |
| 第三方安全服务 |

1. **网络安全管理系统云资源服务**

对全市联网学校的网络安全提供云资源服务，对接市教育大数据平台，与市教育大数据平台实现数据互通。

具体参数如下：

|  |  |
| --- | --- |
| **名称** | **参数** |
| 云端应用服务 | 一年云端应用租赁服务，服务配置不低于：16核64G、1T硬盘 |
| 云端主机安全服务 | 入侵检测、漏洞风险预警，包括密码破解拦截、异常登陆提醒、木马文件查杀、高危漏洞检测等服务 |
| 云端应用安全服务 | 防范Web攻击、入侵、漏洞利用、挂马、篡改、域名劫持等网站及Web业务安全防护问题服务。 |
| 弹性IP服务 | 独立公网IP资源，包括公网IP地址与公网出口带宽不小于20M |
| 接口对接及数据整理服务 | 与市教育大数据平台对接及数据整理服务，保障两平台之间的数据格式一致及数据互通 |

1. **网络安全攻防实训服务**

为应对潜在的网络安全风险，检验全市教育系统安全保障能力、信息系统可靠性及网络安全防护体系健壮性，尽量消除安全风险隐患，确保全市教育系统圆满完成各项重点保障任务，通过风险排查与加固、渗透性测试等方式提升全市教育系统整体安全防护能力。网络安全攻防实训主要通过引入外部专业安全厂商服务，首先开展为期3天的真实环境攻防培训工作，其次面向西安市教育系统所有学生进行线上的知识普及和网络安全知识答题、面向全市教育系统安全管理人员进行专业的网络安全知识培训及答题活动。在前期培训及答题的基础上，进行网络安全主题绘画作品和节目征集活动，并对活动征集到的作品进行专家评审，挑选出200份获奖作品，进行主题校园日的展示及宣传活动。

构建网络安全环境，组织进行为期2天与培训相关的网络安全实训演练，提升老师的实战能力、应急能力，应对网络安全事件的处理能力。

在一年的服务期内根据教育系统时间举办两次网络安全培训活动，让未参加到培训、实训的教职工人员可以参与并了解网络安全，深刻的认识到网络安全已经深入到我们生活中，也建立起一个基础的网络安全防范意识。

实训详细内容包括：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **队伍** | **工作内容** | **工作说明** |
| 1 | 攻击队 | 暴露面资产探测 | 攻击队从互联网侧对用户开展资产探测，不限以下手段：IP、端口、代码托管平台、邮箱、公众号等进行敏感信息获取利用，并输出《互联网暴露面资产报告》 |
| 2 | 攻击测试 | 攻击队从互联网侧对甲方开展攻击，演练目标为获取我方内网主机管理权限。攻击方可使用但不限于以下技术手段用来获取内外网系统、终端和设备的控制权限进而达成演练目标：系统信息泄露、系统安全配置不当、弱口令、SQL注入、跨站攻击、任意文件操作、恶意文件上传、缓冲区溢出、信息泄露等。 |
| 3 | 防守队 | 应用安全测试 | 根据提供的应用系统域名，提供模拟黑客的方式进行应用安全测试，发现互联网应用系统的脆弱性，并提供测试报告。 |
| 4 | 基线核查 | 根据提供的资产范围：如主机、中间件、网络设备、数据库进行基线核查，实现资产安全基本要求，并提供整改依据 |
| 5 | 漏洞扫描 | 根据提供的资产范围：如主机、中间件、网络设备、数据库进行漏洞扫描，识别资产自身漏洞情况，并提供整改依据 |
| 6 | 协助加固 | 根据识别的技术脆弱性，进行协助整改加固，并提供安全加固整改方案。 |
| 7 | 指导协防 | 服务商根据攻击的情况将提供1人，在现场提供指导，用户安全人员将参与进来防守工作，熟知防守流程与防守技术； |
| 8 | 实训总结 | 根据攻击与防守的结果进行总结分析，整理固化可行经验，优化防护缺失手段。 |

1. **正版化软件服务**

正版化软件服务系统主要是为西安市教育局及直属26家单位已安装操作系统及办公软件的设备提供正版软件区域授权服务，软件使用期为1年。

包括操作系统、办公软件，可根据需要选择。

|  |
| --- |
| **正版化软件服务清单** |
| 产品类型 | 产品名称 |
| 国产系统 | 1. ▲操作系统产品支持保障安全升级，可以进行系统升级内容追溯；
2. 操作系统产品具有应用商店，适配主流教育行业应用软件；
3. ▲为保障系统不被恶意软件破坏，保障系统安全，提供应用来源检查和应用执行控制功能，阻止未知软件、应用程序的非法安装和恶意执行；
4. 操作系统可以实现恢复出厂设置或者备份还原功能；
5. 操作系统产品同源异构方式支持龙芯、鲲鹏、兆芯、海光、飞腾、申威等国产主流芯片处理器，并在不同硬件平台上提供版本一致的内核、系统服务、开发和运行环境；
6. 操作系统产品具备中文运行环境，系统内置中文输入法，符合GB18030-2005标准。支持全拼、双拼、五笔等多种主流输入方案；
7. 操作系统产品支持不同CPU架构平台提供自主研发的统一桌面环境，保障用户体验的一致性；
8. 操作系统产品支持多种桌面应用：QQ、微信、自研邮件客户端、画图工具、截图工具、图片查看器、音频播放器、视频播放器、文件管理器、压缩工具、刻录软件、应用商店等；
9. 操作系统产品支持360安全浏览器、奇安信可信浏览器、红莲花安全浏览器、火狐浏览器、QQ浏览器等；
10. 操作系统产品提供分区管理、文件系统管理、系统监视器、备份还原、安全中心、系统更新等系统工具；
11. 操作系统产品支持2K及以上高分屏应用；
 |
|
| 办公软件 | 1. 安全可靠：符合 OFD 版式文档国家标准，符合电子公文应用领域的相关标准规范，通过OFD 标准符合性测试。
2. 文件操作：提供 OFD/PDF 版式文档打开、保存、另存功能，可将打开文档导出图片、PDF或 TXT 格式文档，导出为图片时自动分页保存。支持自动保存。

（3)▲多文档支持：可打开 SFD、SEP、GW、GW2、GD、PS、S2/S72/S92、CEB、流式、图片等格式文档直接阅览。（4)打印操作，提供打印预览、打印功能，支持套红打印、装订成册打印，可设置打印属性。（5)阅读操作：提供翻页、页面跳转、缩放、页面自适应等阅读功能，提供缩略图、大纲、语义、书签、附件等阅读导览功能。（6)▲内容操作：支持选择与复制功能，可将复制内容的字体、段落格式、行间距等属性带入文档中。1. 电子签章：支持签章、骑缝章、署名章、预盖章、文字定位盖章、批量盖章等盖章功能，支持国密时间戳的自动加盖功能。支持符合标准的签章互认，可脱离第三方签章库直接验证签章。
2. 图文注释：提供箭头、直线、圆形等图形注释功能，提供高亮、下划线、删除线、波浪线等文本注释功能。
3. 注释增强：提供注释导入导出功能，以实现相似注释的快速录入；提供文本框注释功能，可设置文本框的外观属性，可为文本框注释内容添加数字签名。
4. 图文水印：提供图文水印功能，可设置水印的字体、字号、角度等属性；提供动态水印功能，可将当前用户、时间等信息作为水印内容叠加到文档中。

（11)▲版式修订：提供版式修订功能，包括删除、插入、替换、移动、修改、增加间距、缩小间距、前移、后移、切换字体、校对等，满足 OFD 版式公文校对需求。1. 手写签批：支持手写签批，实现铅笔、签字笔（粗、细）、软笔签批用笔选择，支持压感笔锋功能，支持跨页签批，提供橡皮檫功能。

（13)▲页面处理：支持拆分 OFD；提供插入、删除、替换、提取、交换、移动、裁剪/裁切等页面处理功能。（14)▲安全性：提供保存、另存、打印、复制、截屏等禁用控制功能，支持国密 https 打开远程文件，可为文档添加阅读有效期和操作权限，提供加密保护功能。（15) 兼容性：兼容信创领域操作系统、电子印章、流式等基础应用软件，支持 B/S 和 C/S集成模式，具有完善的二次开发接口。 |
|

1. **安全巡检服务**

按照《网络安全法》相关规定和要求，定期对全市教育系统的重要信息系统进行安全检查和风险评估，及时发现安全隐患。将巡检计划、技术人员安排以及各单位对接人员信息发布于网络安全管理平台，严格按照巡检计划进行定期网络安全巡检。安全巡检模块主要包括安全巡检服务、巡检报告上载、巡检报告下载、第三方安全服务。

1）安全巡检与评估服务具体内容包括：

A、巡检对象确定：西安市教育局及直属单位的每月巡检工作。

B、安全关键点分析：对影响系统、业务安全性的关键要素进行分析，确定安全状态监控的对象，这些对象可能包括防火墙、入侵检测、防病毒、核心路由器、核心交换机、主要通信线路、关键服务器或客户端等系统范围内的对象（对服务器挖矿软件进行针对性检测）；也可能包括安全标准和法律法规等外部对象。

C、形成巡检对象列表：根据确定的巡检对象，分析巡检的必要性和可行性，形成监控对象列表。

D、巡检对象状态信息收集

巡检工具：根据巡检对象的特点、巡检管理的具体要求、巡检工具的功能、性能特点等，选择合适的巡检工具。建立完善的运维巡检体系。

状态信息收集：整理备案巡检对象的各类状态信息，包括各个教育单位网络系统的漏洞扫描、网络流量、日志信息、安全报警、性能状况、外部环境的安全标准和变更信息。

E、巡检状态分析和报告

状态分析：对安全状态信息进行分析，及时发现险情、隐患或安全事件，并记录这些安全事件，分析其发展趋势。

形成安全状态分析报告：根据安全状态分析和影响分析的结果，形成安全状态分析《巡检报告》交付与现教中心，根据巡检结果可以通知各个教育单位的安全事件管理员或启动应急预案。

2）巡检及评估事项

A、在一年期的服务周期内，首次会对西安市教育局及直属单位、5个区县教育局，进行网络安全漏扫及WEB漏洞扫描，并根据漏洞扫描结果进行网络安全评测，加固工程师根据评测结果进行网络加固并最终生成网络安全评估报告（每单位一份）。

B、在一年期的服务周期内每季度对西安市教育局及直属单位和5个区县教育局进行网络安全巡检工作，根据巡检结果进行相应的风险评估及加固工作并在每个季度生产季度巡检报告交付现教中心。

3）第三方安全咨询服务，可以为西安市教育局及直属26家单位提供专业、可靠的网络安全咨询服务。

第三方安全咨询服务资质要求：

A、国家信息安全测评信息安全服务资质证书

B、网络安全等级保护测评机构证书