技术参数及规格要求

1. 标的物清单

序号	货物名称	数量	单位	预算金额	币种	简要技术要求
1	网络安全攻防演习服务	1	项	180，000.00	人民币	(1) 组建攻防队伍 (2) 提供完备攻防演习方案 (3) 外网风险排查与加固服务 (4)内网风险排查与加固服务 (5)重要系统检测服务 (6)防护评估和加固服务 (7)现场护网保障服务 (8)渗透测试服务 (9)演习总结报告 (10)成果交付

2. 详细技术参数及规格要求

标的物 A（表格式范本）

序号	参数及规格	详细要求
1	组建攻防队伍	组建 1 支安全检测团队，在演习最初阶段对学校现网整体网络安全风险进行排查并配合加固；协助学校招募组建不少于 4 支渗透测试队，在前期加固的基础上进行全方位攻击渗透。
2	提供完备攻防演习方案	建立攻防演习评价机制，可根据渗透攻击队成果进行公平合理的打分和排序。方案须体现对抗性、实战性和真实性，能够全方位营造常态下的高强度网络攻防环境。
3	外网风险排查与加固服务	安全检测团队须从外网盘查学校（校内外）网络信息资产，收集资产风险暴露情况（IP、开放端口等)、双非资产分布，整理交付网络信息资产风险暴露面、双非资产清单。发现外网暴露资产的高危漏洞、敏感信息泄露、高权限管理入口暴露等问题，并提交修复和加固建议。
4	内网风险排查与加固服务	安全检测团队须从内网全面盘查学校重要网络区域和关键业务部门涉及的网络信息资产，对系统和应用的重要漏洞、供应链漏洞、高危漏洞、ODAY 漏洞、账号弱口令等问题进行排查与验证，交付漏洞风险检测报告，含修复加固建议。
5	重要系统检测服务	安全检测团队对学校核心网络系统、重要业务服务系统进行渗透测试与白盒检测，交付检测报告、渗透测试报告与解决方案。
6	防护评估和加固服务	安全检测团队通过安全和有限的攻击渗透，检查网络安全相关设备工作情况，检验评估防守能力，提供加固建议和策略优化方案。
7	护网保障服务	安全检测团队提供 7*24 小时护网，随时参与攻击威胁发现、应急响应、处置恢复和防守技术支持，交付每日护网报告。
8	渗透测试服务	每支渗透测试队至少报备 2 名攻击成员，每日不少于 1 名成员进行渗透测试。每支渗透测试队在攻防演习结束后，按要求提交攻击成果。
9	演习总结	安全检测团队提供攻击画像、威胁溯源分析、攻防数据统计、经验总结，须交付防守总结分析报告。
10	成果交付	服务期间需现场提供安全运营平台一套，平台具备 IT 资产梳理、实战型漏洞扫描、弱密码检测、渗透测试、应急响应、安全通报、重要时期保障等功能，满足安全管理运营工作和实战攻防演习支撑需求，可对漏洞全生命周期进行管理。所有交付成果均通过安全运营平台来交付。