| **序号** | **总体建设** | **建设内容** | **主要功能参数** | **年限** |
| --- | --- | --- | --- | --- |
| 1 | 安全服务 | 渗透测试服务 | 模仿黑客的手法远程或本地对重要资产进行模拟攻击，渗透测试内容，应包括数据库系统、中间件、应用系统以及身份认证等安全机制，具体要求内容：根据网络脆弱性检测中发现的脆弱点，模拟黑客对系统中的终端、服务器进行现场滲透性验证、SQL 注入、XSS (跨站脚本)、CRLF 注入、代码执行、目录遍历、文件包含、输入验证、认证、逻辑错误、密码保护匿域猜测、字典攻击、特定的错误页面检测、脆弱权限的目录和危险的 HTTP 方法（如：PUT、DELETE)等。由安全专家进行深入的手工测试和分析，识别弱点扫描工具或者脆弱性扫描工具无法发现的问题。主要分析内容包括逻辑设计缺陷、上传绕过、输入输出校验绕过、数据篡改、功能绕过、异常错误、逻辑漏洞、越权等以及其他专项内容测试与分析，了解应用系统可能存在的潜在漏洞以及发生漏洞利用时可能造成的危害，渗透结束后生成相关报告并提供修复建议。漏洞扫描不限次数。  **交付物：《渗透测试报告》**  **服务频次：不低于20个系统** | 一年 |
| 风险评估服务 | 通过全局的脆弱性评估、威胁评估和风险评估，掌握通过信息摸排、基线核查等手段对信息系统安全风险状况，以更好地满足国家、行业要求，并与信息系统自身安全保护需求结合起来，针对信息系统进行一次完整的风险评估，明确风险实际状况，并提出风险处置建议和风险评估报告。  **交付物：《风险评估报告》**  **服务频次：不低于10个系统** |
| 应急响应服务 | 在出现重要安全事件时（如信息系统遭受攻击、网络病毒爆发等），派遣高级安服人员，通过远程和现场支持的形式协助采购人对遇到的突发性安全事件进行紧急分析和处理。主要工作内容包括：突发事件相关信息的收集、事件的分析、报告提交、问题解决建议等，协助用户解决突发安全事件，并提供应急响应报告。  **交付物：《应急响应技术服务单》，需客户签字**  **服务频次：4次** |
| 网站监测服务 | 通过对目标站点进行 7×24 小时不间断的页面爬取、分析、匹配，主动实时的发现网站的风险隐患，并及时采取修补措施，对采购人指定网站进行远程安全监测、安全检查、实时告警。网站安全监测服务主要包括以下几方面的内容：   * 远程网站漏洞扫描：通过远程网站漏洞扫描服务，由供应商提供的网络安全专家每月 1 次定期进行网站结构分析、漏洞分析，获知网站系统层和应用层的漏洞情况，以及对修补漏洞的安全建议。 * 远程网页木马监测：基于安全云平台，采用智能木马检测技术，高效、准确的识别网站页面中的恶意代码，使网站管理员能够第一时间得知网站的安全状态 * 网页敏感内容监测：实时监测网站是否出现一些敏感关键字，如果发现敏感内容，在第一时间通知采购人。采购人也可以自定义所关心的敏感关键字。 * 网站平稳度检测：对网站进行实时远程访问平稳度的动态监视，跟踪访问平稳度动态变化情况，并根据严重程度及时发出报警信号。 * 网页篡改监测：实时监测网站页面状况，如发现页面被篡改情况，第一时间通知采购人。   **交付物：《网站监测报告》-每周一次**  **服务频次： 不低于个站点** |
| 重保值守服务 | 根据学校实际业务场景和安全需求制定安全保障计划，协助学校圆满完成重大会议或信息安全保障任务。重要时期安全保障服务内容贯穿事前、事中和事后三个阶段，其中事前包括互联网暴露面扫描探测、漏洞扫描、渗透测试、安全基线检查、安全设备策略检查、综合安全能力评估、安全整改加固、应急预案编制、应急演练、安全培训、安全设备补充完善；事中包括现场安全值守、网站安全监测、定期安全巡检、安全事件分析、应急响应与处置；事后包括安全保障处置报告与建议。  **交付物：《现场重保值守签到表》，需客户签字**  **服务频次：50人/天** |  |
| 安全巡检服务 | * 以环境稳定性、安全性为目标针对主机、网络及安全设备进行深入、严谨的日常性安全检查，服务内容包括日志分析、策略优化和状态检查，并提供可视化报告和统计   **交付物：《安全巡检技术服务单》，需客户签字**  **服务频次：12次** |
| 驻场运维服务 | 提供网络安全服务工程师（CISP）一名，包括不限于网络安全应急事件处理，网络安全监控，网络安全培训，网络安全策略调整，网络安全资产管理，网络安全材料撰写等与网络安全相关服务事宜。根据安全值守的实际情况，将安全值守分为进场、驻场和离场三个过程，各个阶段的描述如下：   * 进场   进场阶段为熟悉相关环境，接口人员，为驻场做好响应的准备。   * 驻场   工作内容为监控、安全加固、应急响应等，凡是涉及到信息系统的运维安全的工作都是安全值守工程师的工作重点。   * 离场   安全值守任务后，需要交接相应的工作，按照保密协议和事先约定进行离场。  **交付物：《驻场运维服务单》，需客户签字**  **服务频次：每周1人/天** |  |