**采购需求**

**一、项目背景：**

随着新技术的持续涌现与应用领域的不断拓展，高校网络安全领域正面临着日益复杂且多变的挑战。特别是人工智能、大数据、云计算等前沿技术的广泛应用，在为高校网络注入新的发展活力的同时，也引入了新的安全威胁，显著扩大了潜在的攻击面。自2021年底以来，我校积极应对这一形势，引入了全驻场形式的网络安全服务项目，该项目全面覆盖了我校网络安全监测、检测评估、信息系统安全升级与优化、网络安全教育培训、专项安全检查、事件应急处置以及安全运维等关键环节，显著增强了我校的网络安全防护屏障。为了进一步巩固和提升网络安全防护能力，今年我校计划引入半驻场人员服务模式与安全专家团队的强力支撑，以期在网络安全防护领域实现更为坚实和高效的保障。

**二、项目组团队及过程控制要求：**

**1.团队要求**

为了保证服务质量，项目组成员不少于6人（含项目经理1人，网络安全技术服务人员1人，须支持7\*24远程技术应急服务），在项目服务过程中，未经采购人批准，不得随意更换项目组成员（工程师），如果采购人认为项目组成员（工程师）不具备本项目所需的技术能力，采购人有权随时要求投标人进行更换；

**投标人投标时需提供项目组成员名单及技术分工配置单及投标人为其缴纳的近三个月以来任意一个月的社保证明材料（未提供按不实质性响应处理）。**

**2.项目过程控制要求**

项目前期：制定全面、具体的服务方案。

项目进行：阶段性服务工作完成后需要输出相应的报表、报告等材料。

项目结束：编制总结报告，纸质文档交接，电子文档集中销毁。

**三、项目主要内容：**

服务内容包括（不限于）：资产梳理、安全设备巡检、漏洞扫描、新系统上线检测、渗透测试、安全预警、重要时期保障、应急响应、应急演练、安全培训、网络安全宣传周宣传教育、安全咨询与策略优化、安全威胁专项检查、网络技术运维保障等相关工作，主要内容如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **服务名称** | **详细内容** | **服务要求** |
| 1 | 资产梳理、设备巡检 | 　　每月定期针对校方的网络安全设备执行全面巡检。配合完成所有的安全资产（包括服务器内新增设备）建档立册，对其品牌、型号、部署位置、实现功能、在保状态、授权情况等做出详细梳理。巡检完成后，依据设备运行的实际情况以及发现的问题，进行系统梳理与整合，并编制出详尽的报告。 | **服务周期：**每月定期；**交付物**：月度巡检报告。 |
| 2 | 漏洞扫描 | 　　1.针对校方指定网站和信息系统进行全方位多维度自动化的漏洞扫描，通过漏洞扫描工具结合人工确认的方式从内网和外网两个角度发现安全风险、漏洞和威胁。　　2.给出全面的安全评估报告，对可能存在的误报进行验证，详细说明存在的安全风险，对确认存在的安全风险提供对应的修复建议，并协助校方进行风险修复。一周内提供安全评估报告，紧急情况需3天内提供报告。报告包含原因分析、解决方案以及校方要求的其他内容。 | **服务范围：**服务期内学校提供的所有网站、业务系统（含复测)；**服务频率:每季度****交付物:**漏洞扫描报告和修复工作。 |
| 3 | 新系统上线检测 | 3.系统上线前安全检测服务主要是针对校方新上线的系统进行安全检测，确保系统在没有中危及以上安全隐患，才允许上线正式运行。系统上线前安全检测方式主要包括：漏洞扫描（内外网结合）、渗透测试。出具详细的安全评估报告，并配合对新系统相关的安全整改与复核。 | **服务频率：**根据学校要求响应；**交付物：**安全评估报告、安全整改与复核。 |
| 4 | 渗透测试 | 　　1.以模拟黑客入侵的方式对目标系统进行模拟入侵测试，最大限度挖掘注入漏洞、越权访问漏洞、业务逻辑漏洞、Web框架漏洞、文件上传漏洞、弱密码、关联性漏洞等安全风险，一周内提供渗透测试报告，紧急情况需3天内提供渗透测试报告。　　2.渗透测试报告包含原因分析、解决方案以及校方要求的其他内容，协助校方进行漏洞、安全隐患等修复工作后进行复测。 | **服务范围:**学校提供的业务系统（不低于20个业务系统，不区分内外网，含复测，提供测试报告并协助做好整改工作)；**服务频率:**一年不少于4次（不含复测）；**交付物:**测试报告和整改工作。 |
| ★5 | 现场保障 | 　　1.在服务中将会对安全设备进行维护和配置，并最大化利用设备完成安全工作，并根据实际风险情况输出安全代维报告。工作内容包括但不限于：态势感知：挖矿、后门、黑IP、异常流量等处置。WAF：攻击IP封禁，异常行为溯源；防火墙：对外开放端口限制；虚拟化杀毒：周常扫描处置。2.在服务期中向学校提供风险预警服务，在服务中会对于最新漏洞的情况生成告警信息提供给学校，并协助老师关联校内资产完成风险排查。3.协助老师完成联系厂商，漏洞分析等常规事务，并提供巡检报告。4.重要时期现场保障巡检服务，配合学校完进行特殊时刻的安全保障，为校方提供专项网络及信息安全保障服务，具体根据学校的要求执行。  | **服务频率：**一周三次（8：00-17：30）；**交付物：**安全保障应急响应预案、安全保障工作日志、安全保障工作总结。 |
| ★6 | 应急响应 | 1.当校方网络与信息系统发生紧急安全事件时，迅速组织应急安全专家小组提供远程及现场支持，最快速处置事件，并采取有效措施，遏制事件蔓延并降低安全威胁事件带来的严重影响。2.安全服务人员根据事件类别，通过远程和现场支持的方式协助校方对遇到的突发性安全事件进行紧急分析和处理。3.应急响应服务应至少包括现场取证备查、事件分析、分析报告提交、问题解决建议等，保证重要系统能及时恢复上线。**4.应急安全专家小组远程响应时间不超过1小时，应急安全专家小组12小时内到达现场。** | **服务频率：**根据学校要求响应。**交付物：**网络安全事件应急响应报告、处置建议、协助进行安全事件处置 |
| 7 | 应急演练 | 1.通过应急演练服务，建立健全网络与信息安全运行应急工作机制，检验网络与信息安全综合应急预案的有效性，验证相关组织和人员应对网络和信息安全突发事件的组织指挥能力和应急处置能力。同时，通过演练，不断提高各部门开展应急工作的水平和效率，发现不足，进一步完善应急预案。2.根据实际业务环境，提供专项预案，准备演练场景，以模拟攻防演练的方式检验应急预案和应急流程是否完善，提高应急处理能力。 | **服务频率：**不少于2次；**交付物：**应急演练预案（周期性完善）、应急演练方案、应急演练汇报、更新的应急预案。 |
| 8 | 安全培训 |  根据校方的网络安全培训要求，提供网络安全培训课程，培训形式由校方指定，培训内容包含但不限于网络安全意识培训、网络安全管理培训、网络安全技能培训网络安全等级保护标准培训、商用密码应用安全性评估培训。 | **服务频率：**面向校内专业人员2次技术培训，面向师生2次知识讲座；**交付物：**技术培训、网络安全知识讲座、培训及相关文稿。 |
| 9 | 网络安全宣传周宣传教育 |  根据国家网络安全宣传周的要求，协助校方开展网络安全宣传周各种形式的宣传并提供相关物料支持，对师生开展网络安全教育活动。 | **服务频率：**不少于1年1次；**交付物：**网络安全宣传方案、组织过程、活动文稿等相关材料。 |
| 10 | 安全预警 | 　　1.密切关注零日漏洞、业界新发现的高危安全漏洞，针对高危安全漏洞及时预警，预警包括对安全漏洞的描述、影响范围、修复建议等内容。　　2.网信办、公安机关等相关的行业安全事件分析、安全规范解读、安全检查范围方法预警、通告。　　3.预警范围包含但不限于：应用安全漏洞通告、重大安全事件通告、采购方自身安全漏洞通告；通报时间7\*24小时，实时通报；通报后根据实际情况提供远程或现场技术支持。 | **服务频率：**根据学校要求响应；**交付物：**安全漏洞详情、修复建议、协助完成修复；安全预警通告及后续技术支持工作。 |
| 11 | 安全咨询与策略优化 | 提供网络安全咨询服务，解答我校在网络安全建设、运维过程中的安全问题。同时，全面了解学校网络安全建设现状，参照国家及教育行业相关标准，协助我校制定网络安全建设方案和规划。根据等级保护要求和上级主管部门要求，协助学校制定、优化数据中心安全策略、互联网出口安全策略等;协助制定学校网络安全相关标准、制度，提供专业化安全建议。 | **服务频率：**根据学校要求响应；**交付物：**各类网络安全文件、制度、规范等，策略优化报告。 |
| 12 | 安全威胁专项检查 | 根据上级主管部门及学校要求，开展如弱口令等各类网络安全专项检查，进行安全威胁检查，出具检查报告并协助做好相关威胁、漏洞等修复工作 | **服务频率：**根据学校要求响应；**交付物：**检查报告和修复工作。 |
| ▲13 | 网站安全监测 | 对互联网测站点进行实时监测，“篡改、黑链、敏感文件、敏感词、网马监测、可用性、域名劫持”等维度开展实时7\*24小时监测，并通过邮件等告警形式提供网站风险预警服务。 | **服务频率：**根据学校要求响应；**交付物：**监测报告。 |
| 14 | 服务器运维 | 协助校方针对业务服务无法访问或访问存在问题，定位服务程序/软件/硬件问题并联系相应的人员解决具体问题。 | **服务频率：**根据学校要求响应。 |
| ★15 | 安全通告 | 结合网络安全主管机构下发的安全整改通知、日常安全漏洞检测情况及行业安全趋势情况定期形成网络安全报告，并及时汇报给学校。配合处理上级通告，通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务。结合现有安全防御体系，指导安全加固、提供整改建议、防止再次出现。对修复的漏洞开展复测，对潜在风险问题进行处置，包含内网脆弱性问题。 | **服务频率：**根据学校要求响应；**交付物：**网络安全报告。 |
| **注：1.以上服务项及服务频率、交付物仅为本项目最低实施标准，必须全部满足。否则按无效投标处理；****2.带“★”条款为实质性条款，投标人必须按照采购文件的要求做出实质性响应。** |

**四、服务质量及要求：**

1.满足服务内容中相关要求。

2.投标人在项目服务前，须详细分析在本次项目服务过程中存在的可能影响现有系统安全性与稳定性的风险，并采取必要的风险控制措施。任何由投标人在项目服务工作中对采购人造成的负面影响，其后果都须由投标人承担。如给采购人造成任何经济损失，均由投标人承担赔偿责任，且采购人有权在未付款项中直接扣除。

3.投标人中标后需要对信息安全做出承诺，对涉及的安全服务操作中的风险有专业的规避和防范措施，并能够对可能发生的信息安全问题承担责任。中标投标人提供项目实施期间信息安全保障机制，提供信息安全保障方案，确保采购人信息安全。因投标人工作失责导致的网络安全责任，由投标人承担相关责任。如给采购人造成任何经济损失，均由投标人承担赔偿责任，且采购人有权在未付款项中直接扣除。

**4.项目实施前，签订保密协议；对项目实施中产生的数据和信息严格保密，未经授权不得泄露给任何单位和个人，否则招标人有权追究投标人的责任。如给采购人造成任何经济损失，均由投标人承担赔偿责任，且采购人有权在未付款项中直接扣除。**

**五、项目验收：**

1、网络安全技术服务人员的月报，项目阶段性工作的报告、报表，各类漏洞、安全事件处置的过程性文档，安全预警通告，培训资料，协助制定的各类制度、规范文件，及服务内容中所要求完成各类的预案、文稿等，要求内容记录完整、准确。

2、全年网络及信息系统安全运行是否正常、安全服务质量是否符合采购人要求，服务质量考核表得分情况。

**六、服务质量考核：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 考核 | 考核项目 | 分值 | 评价描述 | 评分 |
| 工作考核90分 | 任务完成效率 | 40 | 未充分规划、在规定时间内不能完成任务 | 每次扣5分 |
| 任务完成质量 | 50 | 出现质量异常（投诉、失误、返工） | 每次扣3分 |
| 出现严重质量异常（投诉、失误、返工） | 每次扣6分 |
| 出现因安全服务导致的宕机超过4小时 | 每次扣10分 |
| 响应需求被动，消极处理问题 | 每次扣5分 |
| 人员考核10分 | 服务质量 | 10 | 不注重沟通，遇到问题以强硬或回避的态度来应对 | 每次扣2分 |
| 服务态度差，甲方收到投诉 | 每次扣5分 |

 **考核说明：**

**1.考核初始赋值 100分。考核表格包括但不限于以上内容，在实际运作中不断完善。每个考核项目扣分项最多将该项分值扣至0分。**

**2.每季度考核分数在60到80分之间，将要求投标人对安全服务团队责任人进行谈话，并责令整改；每季度考核分数≦60分，投标人须更换安全服务实施人员，更换人员须符合安全服务人员要求；如无法更换符合要求的安全服务人员，采购人将终止合同，并拒付剩余合同款项。**