**附件一：服务需求**

**安全运维管家服务技术需求**

上海海事大学临港校区网络与信息安全运维需要委托专业技术公司来完成。

**一、服务内容和范围**

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | 项目 | 数量 | 范围 |
| 1 | 安全运维规划服务 | \ | 优化学校的安全防护体系建设，通过对学校安全体系的评估，协助学校进行安全体系规划 |
| \ | 协助学校开展日常网络安全指导工作，制定学校网络安全工作计划 |
| 2 | 日常安全扫描检测服务 | 每季度一次 | 网络安全检测。通过对学校网络系统进行规范化的定期检查，通过检测工具进行网络安全评估检查，并经过人工核验，生成安全检测报告，提供过安全加固建议 |
| 每季度一次 | 服务器安全检测。针对我校中心机房内所有服务器，通过检测工具进行安全监测，并经过人工核验生成安全检测报告，提出安全加固建议 |
| 3 | 日常运维监控服务 | 每月一次 | 按月巡检相关安全设备上的日志，提供巡检报告，并根据情况协助跟进安全整改（监控对象：态势感知、防火墙、WAF、漏洞管理设备）， |
| 4 | 渗透测试服务 | 2个系统 | 针对应用系统，从攻击者的视角，模拟黑客所使用的攻击手段对目标系统进行模拟入侵，以充分挖掘和暴露系统的弱点，从而让管理人员了解其系统所面临的威胁 |
| 4 | 重点时期检测服务 | 按实际需要 | 在我校和上级部门要求的重点时期内，服务单位需对我校开放在互联网上的业务提供远程5\*8小时监测服务，一旦发现异常情况立即汇报给校方对应人员，并配合校方妥善处理。 |
| 5 | 协助服务 | 按实际需要 | 针对来自上级部门（教委、公安、文保等）要求需要报送涉及学校网络安全的相关材料，要求服务单位协助我校完成与报送材料安全有关的调查、收集、整理、报告等相关工作。针对外部安全单位提交的校内网站和系统的安全漏洞情况，进行跟进处理直至漏洞修复完成，并给出相关部门整改情况统计。 |
| 6 | 应急响应 | 按实际需要，不超过2次 | 服务针对我校已经发生的网络安全事件，提供应急响应服务。应急响应要求服务人员7×24小时在线，30分钟内应急响应，3小时内赶赴现场 |

**二、安全服务要求**

（一）中标的公司须在上海市区有固定的售后服务团队（公司注册地在上海或在上海有固定办公地点），具有成熟的服务质控体系；

（二）鉴于本次项目内容较多，为保障服务质量、服务效率，中标方须做好服务实施计划，计划内容须包括如下内容（包含但不仅限于）：

|  |  |
| --- | --- |
| 序号 | 人员及售后服务要求 |
| 1 | 项目经理（服务对接人）需具有10年以上安全相关项目经验，且同时具备**CISSP、CISA、PMP、ISO27001LA、RHCE、等保安全建设专业技术人员证书** |
| 2 | 项目团队人员具备信息安全资质**CISP、CISSP、CISAW、ISO27001LA、等保安全建设专业技术人员证书**等资格证书.  |
| 3 | 中标后，中标方的每次服务须由有资质的项目经理具体负责。保证项目人员未经甲方同意，不得调换或撤离，项目人员必须接受招标人的项目管理、保障服务交付时间及质量要求 |
| 4 | 中标后，中标方的服务人员须提供两个季度（包含）及以上的社保证明，且同甲方签订保密协议； |
| 5 | ▲1、0.5\*7\*24响应服务，6\*7\*24小时到达现场；2、每季度出安全分析报告；3、提供相关技术安全培训，提供培训视频和考核相关能力； |

▲为重要服务要求，如不能满足将会予以扣分。

**三、服务时间**

服务期为1年，服务期满后若甲方对中标单位提供的服务满意且服务价格保持不变，经双方商定后，可与中标单位续约一年服务合同，最多可续约两次。

**四、服务类型**

现场服务

**五、响应时间**

6小时之内到现场（或更短时间）

7x24小时电话技术支持

**六、付款方式**

合同生效后，10个工作日内，甲方向乙方支付合同额的100%款，乙方进入服务交付期，并制定服务实施方案，经甲方同意后，根据实施方案向甲方提供安全服务支持并生成实施报告，甲方将对全年的服务实施报告进行考核。考核不合格，乙方退还10%合同款项给甲方。

**七、服务考评办法**

 供应商须提供详细的文档，包括但不限于以下内容：

《漏扫报告》

《应急事件处理报告》

《设备巡检报告》

《安全咨询规划报告》

《全年服务总结报告》