## 附件

## 网络安全 服务内容及要求

**1、网络安全等级保护测评服务**

**服务要求：**合同期内，根据学校要求，对学校7个业务系统进行等级保护测评（二级）。

**待测评系统：**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **系统名称** | **系统开发厂商** | **备注** |
| **1** | 学校网站 | 学校自主开发 | 含官网及所有二级网站 |
| **2** | 智慧校园平台 | 江苏金智 | 含三大平台 |
| **3** | 教务系统 | 杭州正方 |  |
| **4** | 财务系统 | 天大天财 |  |
| **5** | OA系统 | 深圳蓝凌 |  |
| **6** | 学工系统 | 江苏金智 |  |
| **7** | 图书管理系统 | 北京金盘 |  |

**服务内容：**

测评工作阶段、流程、内容、及成果交付严格遵循《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019)和《信息安全技术网络安全等级保护测评过程指南》（GB/T 28449-2018）文件，根据系统等级开展相应级别的单项测评和整体测评。

按照《信息安全技术 网络安全等级保护实施指南》（GB∕T 25058-2019），从每个信息系统的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等10个层面进行测评，依据信息系统的业务应用和内外部环境，深入调研分析各信息系统资产状况和重要性程度，以及面临网络安全的威胁。

工作过程文件及项目交付成果（包括但不限于）：《网络安全等级保护测评报告》。

**交付期限：**

为本项目提供等级保护测评的服务商应有项目交付实力，在合同之日起算，30个工作日内出具《网络安全等级保护测评报告》。

**2、渗透测试服务**

**服务要求：**合同期内，根据校方需求，1年内针对一个系统提供至少一次针对关键系统的渗透测试服务。

**服务内容：**针对校方重要核心应用系统，重点发现技术或业务逻辑层面的漏洞。从技术、管理、业务逻辑的角度来发现漏洞，充分挖掘信息系统漏洞情况，从根源上解决存在的漏洞或问题，减少安全事件的发生。

结合校方实际情况，在授权的时间期限内进行渗透测试，对学校Web站点进行最大限度地挖掘SQL盲注、代码注入、struts2、越权、逻辑错误、存储型跨站脚本、中间件、弱口令等使用扫描工具无法排查或挖掘的安全漏洞，并提交漏洞风险报告和相关处置建议。

**交付物：渗透测试报告。**

**注：为保障渗透测试服务效果，切实的为学校查出问题，渗透测试服务须为学校发现不低于10个相关安全漏洞，少发现一个扣除项目合同额的1%，最高扣除10%。**

**3、资产梳理服务**

**服务要求：**合同期内，根据校方要求，不定期提供资产梳理服务。

**服务内容：**在服务过程中，对学校的资产进行梳理，建立有效安全资产管理，并且以资产为安全管理对象进行有效的安全运维工作，能够展示资产梳理后的详细信息。资产梳理服务主要包括：

1. 网站资产梳理服务

对学校网站进行梳理服务，探测互联网上暴露的资产，形成明确的资产清单，发现未知资产，并发现直接对外开放的危险连接方式。

1. 服务器资产梳理服务

对学校服务器进行梳理服务，包括操作系统版本、端口开放情况、协议情况、服务版本、应用程序版本等，实现对服务器的运维管理。

1. 终端资产梳理服务

对学校终端PC资产进行梳理服务，支持对跨网段的IP或多个网段对进行MAC地址探测识别，支持识别MAC地址的设备类型包含:“Windows、Linux、国产操作系统、交换机\路由器、安全设备、打印机、物理网设备、教学设备等”，包括操作系统版本、端口开放情况、协议情况、服务版本、应用程序版本等。

**4、攻击面监测服务**

**服务要求：**合同期内，根据学校需求，每月提供一次攻击面监测服务。

**服务内容：**通过多外网云端扫描技术，探测互联网上潜在的未知资产，不必要开放的资产，并自动验证互联网资产是否存在可利用漏洞、弱口令，提供暴露面收敛等相关整改建议，监测数据通过本地服务平台统一展现和管理。包括但不限于：

互联网资产详情：从基本信息到应用组件、应用指纹、开放端口等

风险暴露面排查：远程访问端口、VPN入口、后台入口、弱口令、可入侵漏洞等

未知资产排查：那些被忽略的域名、IP、应用、信息通道等

生成暴露面监测报告：提供暴露面收敛整改建议，定期更新和审核

**5、主机漏洞监测服务**

**服务要求：**合同期内，根据采购人需求，每月提供一次主机漏洞监测服务。

**服务内容：**对主机进行常态化安全漏洞扫描，提供主机漏洞台账与报告，能够自动对漏洞状态进行处置，自动识别“新增、已修复、未修复”的漏洞，同时支持人工方式进行漏洞状态处置，以及编写漏洞备注。并根据漏洞风险等级、漏洞被利用可能性、漏洞加固或规避措施等内容，为采购人进行漏洞处置决策提供参考依据。

每次安全漏洞扫描完成后，提交完整的漏洞扫描分析报告，详细说明存在的安全风险，而且对系统以后整改的方向提供适当的解决方案；扫描报告包括综述、主机、漏洞、趋势等信息进行分类，综述中应对漏洞和风险分布进行定量统计分析并展示，主机中应提供漏洞分布、可入侵情况、风险值和风险等级信息。

**注：为保障漏洞监测服务效果，切实的为学校主机发现新漏洞，主机漏洞监测服务须与安全通告服务相结合，安全通告所体现新漏洞，须在每次漏洞扫描过程中进行发现，少发现一次扣除项目合同额的1%，最高扣除12%。**

**6、漏洞屏蔽服务**

**服务要求：**合同期内，根据采购人需求，对学院系统主机进行7\*24小时漏洞屏蔽服务。

**服务内容：**通过技术手段帮助学院屏蔽各类漏洞，使漏洞扫描器、恶意攻击源无法扫描到主机或web应用系统存在的漏洞，包括可利用漏洞、版本漏洞、web代码层面的漏洞。

**注：为保障漏洞屏蔽服务效果，切实的为学校主机屏蔽高危漏洞，保障学校在被上级单位安全检查时顺利通过，须在被上级单位扫描时不被发现无法修复的高危漏洞，漏洞屏蔽准确率需超过95%，当准确率低于90%时，每被上级单位发现一次将扣除应付服务费1000元（此项扣除最高不超过2万元）。当准确率低于80%时，将不予付款，并纳入学校安全服务黑名单，未来此类项目不予以合作。**

**7、WEB应用漏洞监测服务**

**服务要求：**合同期内，根据学校需求，每季度提供一次WEB应用漏洞监测服务。

**服务内容：**对网站或WEB应用系统进行常态化WEB漏洞扫描、检测，提供WEB资产漏洞报告，基于漏洞风险等级、漏洞被利用可能性、漏洞加固或规避措施等内容，为学校进行漏洞处置决策提供参考依据。

每次WEB应用漏洞扫描完成后，提交完整的WEB应用漏洞扫描分析报告，详细说明存在的安全风险，而且对系统以后整改的方向提供适当的解决方案。

**8、Webshell监测服务**

**服务要求：**合同期内，根据学校需求，每月提供一次Webshell监测服务。

**服务内容：**除了对网站或WEB应用系统进行WEB应用漏洞扫描外，还需针对此类服务器中产生的文件进行常态化的安全扫描、监测，发现网站或WEB应用系统存在的Webshell文件风险，提供完整的扫描报告以及相应的处置建议，及时解决服务器的存在后门的风险。

**9、弱口令监测服务**

**服务要求：**合同期内，根据学校需求，每月提供一次弱口令监测服务。

**服务内容：**对服务范围内主机中，包含redis、smb、rdp、telnet、ftp、ssh、pop3、smtp、mysql、imap、vnc、snmp、vmauthd、postgres、mssql、oracle、mongodb、onvif等多种服务协议进行常态化弱口令检测，支持用户针对指定的目标IP与应用，通过在web界面上手工输入“用户名、密码”，系统将返回口令登录后的校验结果，确认弱口令是否真实存在，并提供弱口令处置方案。

**10、配置核查服务**

**服务要求：**合同期内，根据学校需求，每月提供一次配置核查服务。

**服务内容：**配置核查是实现信息安全风险评估和风险管理的前提和基础，为了满足各业务系统的基本安全需求，需要充分参考国家及行业标准、规范以及成熟经验，建立并形成一个针对各业务系统的基线安全模型。

根据学校的实际情况，对学校管辖范围内网络设备、主机、操作系统、数据库、中间件、应用软件、新上线业务系统进行增量基线配置核查及是否满足最小化服务原则进行配置，并提供相对应报告和整改建议。

**11、网站监测服务**

**服务要求：**合同期内，根据学校需求，对学校网站进行7\*24小时监测。

**服务内容：**

网站漏洞监测：对学校域名范围内的Web站点进行扫描，排查WEB站点中的SQL、XSS、敏感信息泄露、文件包含、CSRF、目录遍历、XML注入、备份文件、弱口令等多种web代码层面的漏洞。

黑链/篡改事件监测：高频率监测站点是否存在被黑客植入黑链、篡改的事件，监测频率低至5分钟/次。

敏感词事件监测：自定义敏感词库，支持自定义监控周期，持续对学校网站进行全站页面爬取，发现敏感词字眼。

敏感文件泄露事件监测：对学校网站发布的文件中是否含有用户信息等敏感文件进行监测，包括excel、txt、pdf等类型的文件。

网马监测：通过对网页中的恶意脚本的链接进行分析，追查出网页木马传播的病毒、木马程序所在位置，对网络中的有害程序进行准确定位。

域名劫持事件监测：监测站点的DNS解析是否异常，监测频率低至5分钟/次。

可用性异常事件监测：模拟浏览器访问，监测站点的可用性情况，监测频率低至5分钟/次。

网站主机环境安全监测：在服务器部署主机安全监测软件，主动对网站篡改、webshell、后门以及挖矿等主机安全事件与行为进行7\*24实时监测，第一时间对攻击行为进行告警。

**12、安全事件监测服务**

**服务要求：**合同期内，根据学校需求，对学校事件通过流量监测、主机监测、全网蜜罐进行7\*24小时监测。

**服务内容：**

**流量入侵检测**

通过流量镜像对海量流量进行采集，对于捕获的流量进行存储、分析，结合内置多重检测引擎，自动对威胁源进行风险评级，精准识别攻击源头，发现不同场景下的已知威胁和未知威胁。

**全网威胁诱捕**

本次服务项目通过部署资产安全运维服务平台，在不改变单位的网络架构前提下（包括：不做镜像流量、不做牵引流量等），通过旁路部署，在“DMZ区”、“服务器区”、“终端区”分别生成仿真业务系统，与待监测的目标“IP、web”等资产网络可达，通过虚拟出来的蜜罐主机，在每个网段部署虚拟蜜罐，达到监测内网病毒威胁安全事件，并提前做安全预警。

**主机威胁监测**

在重要系统服务器部署主机安全监测软件，可主动监测恶意文件（webshell、病毒木马）、挖矿进程与病毒检测、网站篡改检测等，发现可疑的入侵事件，并实时将告警同步到资产安全运维平台服务平台，第一时间对攻击行为进行告警。

|  |  |  |
| --- | --- | --- |
| 序号 | 监控项 | 监控说明 |
| 1 | 恶意文件检测 | 支持检测“Webshell网马、病毒木马、攻击脚本、宏病毒文件等” |
| 2 | 挖矿进程与病毒检测 | 支持检测挖矿病毒，识别挖矿程序文件、挖矿进程名称、进程号、运行参数、CPU运行异常状态、网络连接状态、病毒程序打开的文件 |
| 3 | 网站篡改检测 | 可检测网站文件的篡改行为，包括：“创建、写入、修改权限、重命名、删除”等篡改行为 |

**13、安全加固服务**

**服务要求：**合同期内，根据学校需求，提供不少于二次安全加固服务。

**服务内容：**对网络环境中资产已存在的安全风险、漏洞、不合规配置项等内容，进行安全加固、安全处置的措施，减少因资产的安全风险被黑客利用导致安全事件的发生。

基于常态化的监测结果以及漏洞信息情况，协助学校针对网络设备、安全设备、服务器操作系统等进行安全整改措施。

**14、应急响应服务**

**服务要求：**合同期内，根据采购人需求，提供不超过二次应急响应服务。

**服务内容：**提供7\*24小时全天候、2小时到达现场，每次提供相应的响应报告，找出根源并提供可行解决方案。

安全事件应急处理流程应包含三个阶段，包括事件初期、应急响应实施及输出报告与汇报：

事件初期：在实施应急响应工作前，客户经理或项目经理收到学校申请应急响应支持，由客户经理或项目经理协调内部技术支持人员和采购人第一时间取得联系，了解事件发生情况。技术人员判断事件类型，是否需要启用应急响应服务。

应急响应实施：在判断事件类型可能为安全事件，启用应急响应后，技术人员通过现场或非现场等方式进行信息收集工作，详细了解掌握事件发生的始终、现状、可能的影响，对事件进行详细分析，提供事件处理建议，并协助采购人解决事件。

输出报告与汇报：待事件处理结束后，技术人员整理事件分析、事件处理的过程记录和相关资料，撰写应急响应服务记录报告，提交给采购人。对于大型、复杂的应急响应过程还需进行整体的事件处理汇报工作。

安全事件应急处理过程中，关联失陷主机发现过程，并结合实现主机分析报告进行处置汇报。

**15、安全运维服务**

**服务要求：**合同期内，根据学校需求，安排一名技术人员提供每周一次安全运维服务。

**服务内容：**服务提供商拟派的运维服务人员需具有五年及以上网络安全工作经验，并同时具备注册渗透测试工程师（CISP-PTE）、信息安全保障专业级人员（CISAW）、注册信息安全专业人员（CISE）证书、国家中级信息安全工程师、并加盖服务提供商公章，运维人员进场服务时学校对运维服务人员身份信息、证书信息进行核对。提供拟派运维人员的上述相关证书扫描件加盖供应商公章及近三个月任意一个月的社保缴纳证明。运维技术人员依据学校实际情况，在工作时间驻守学校中心机房并开展日常安全工作（包括：设备状态检查、安全巡检、安全事件分析等），当发生突发事件时，运维技术人员及时采取必要措施，排查、分析问题并提供解决方案，事后进行分析总结提供相应防范措施。帮助学校梳理安全问题、规范运维流程、健全安全制度，最终为学校构建一个完善的安全运维管理体系。

**16、重保值守服务**

**服务要求：**合同期内，根据学校需求，1年内提供一次重保值守服务。

**服务内容：**我们的重要时期安全保障服务主要针对重要IT系统资产、包括主机、网络、应用等系统运行维护场景。针对互联网IT服务业务、IT资产为服务对象。

在重要活动开始至结束期间，服务提供商需派遣经验丰富的安全专家至现场进行安全值守支持。

现场安全值守工作主要包括如下方面工作：

1. 安全设备日常监控

安全设备健康情况实时监控，包含：CPU使用率、内存占用率、接口流量、接口工作状态、硬盘使用情况等设备健康相关的基本参数监控。

安全设备告警事件实时监控，包含：拒绝服务攻击，网络病毒爆发，漏洞远程利用、恶意代码传递等高危事件告警信息。

1. 安全事件协助处理

当安全设备产生高危事件报警时，我们安全专家将积极协助相关人员对报警事件进行确定、排查、分析和处理。

1. 日志分析

注：为了做好重保值守服务，服务供应商需提供一套满足重保值守服务工作的工具供采购人使用，为了防止数据泄露，要求服务工具须本地部署。

服务工具要求：2U机架式设备，支持4个接口板卡扩展插槽，默认配置6个千兆电口，2T硬盘存储空间，64G内存，冗余电源，包含了漏洞扫描、管理、屏蔽，资产探测及管理，网站监测，蜜罐、流量监测等功能，持续监测资产变化情况，提供主机和网站资产的自动发现和资产管理功能授权许可。

服务工具授权许可：

1）提供无授权限制的主机资产发现功能授权许可；

2）提供无授权限制的网站资产发现功能授权许可；

3）提供无授权限制的网站风险与威胁监测功能授权许可；

4）提供无授权限制的主机漏洞扫描和漏洞管理功能授权许可；

5）提供无授权限制的内网病毒诱捕功能授权许可；

6）提供1000个主机主动监测及漏洞屏蔽功能授权许可；

7）提供出口10G流量带宽监测功能授权许可；

8）提供无授权限制互联网攻击预警诱捕授权许可。

提供上述功能授权的承诺函证明并加盖响应供应商公章

**17、安全迎检服务**

**服务要求：**合同期内，根据学校需求，不定期提供安全迎检服务。

**服务内容：**在网信、公安等监管部门到现场进行网络安全检查前，协助学校按照监管单位的检查要求，对网络进行系统的自查工作，并提前准备相应的佐证材料，同时，在监管部门到现场进行网络安全检查时，协助学校进行相关检查工作。

**18、风险评估服务**

**服务要求：**合同期内，根据学校需求，1年内针对一个业务提供一次风险评估服务。

**服务内容：**风险评估主要分为准备、识别、分析、处置四个阶段，评估过程要能够严格按照《GBT 20984-2022 信息安全技术 信息安全风险评估规范》进行，**具备信息安全风险评估资质二级及以上资质的第三方进行评估，提供中国网络安全审查技术与认证中心颁发信息安全风险评估资质的证书的扫描件或复印件并加盖响应供应商公章，未提供或部分提供视为无效响应。**

准备阶段：安全评估公司工程师和专家和学校相关人员进行讨论确定项目组织结构及人员分工，然后双方确定项目目标、范围、项目交付文件、项目实施方案、工作方式、评估成果提交形式等内容，同时学院准备项目实施组的实施环境，项目实施团队进场，签署保密协议；召开项目启动会，项目正式启动。

识别阶段：实施组对被评估信息系统的关键资产进行识别，并合理分类，识别被评估信息系统的关键资产所面临的威胁源，从技术、管理两方面对被评估信息系统的脆弱性进行识别，并合理分类，识别被评估信息系统已采取的安全措施，并根据资产在遭受泄密、中断、损害等破坏时所遭受的影响，对资产的价值进行赋值。

分析阶段：在识别出信息资产后，需要对资产进行梳理分类并进行风险分析。将资产按硬件、软件、数据、人员和服务分为5类进行整理，按其资产价值识别出各资产类中的关键资产，从而明确信息安全保护的重点，合理分配各种资源进行安全保护工作。同时进行资产量化分析，其过程也就是对资产进行影响性分析的过程。关键资产在遭受泄密、中断、损害等破坏时对系统所承载的业务系统所产生的影响，这一后果可能会危及信息系统并使其丧失机密性、完整性、可用性，最终还会造成其他破坏。最终生成资产评估报告。

最后是处置阶段：风险评估项目组将根据风险分析的结果，结合国家有关的法律、法规，总结出当前的安全需求，根据安全需求的轻重缓急以及相关标准和电子政务保障框架，对各种风险根据导致该风险的脆弱性制定风险处置计划，为今后的安全建设提供参考。风险处置计划中明确应采取的弥补弱点的安全措施、预期效果等。

在风险处置计划完成后，风险评估小组将总结以上所有报告即资产分析报告、威胁分析报告、脆弱性分析报告、综合风险分析报告等各项报告，并向领导小组汇报并提交，详细介绍被评估信息系统所面临的风险，清晰的表达所面临的威胁状况、威胁所利用的脆弱性、产生的影响等状况，并在描述安全风险之后表述出采取何种对策防范威胁、减少脆弱性，并将问题的轻重缓急描述清楚。

**19、安全通告服务**

**服务要求：**合同期内，根据学校需求，每月提供一次安全通告服务。

**服务内容：**定期提供最新安全漏洞、威胁（0day、系统漏洞、网络攻击）的解决办法、安全问题描述和相应的处理意见，及时提供符合学校实际需求的安全信息。

**20、安全管理制度服务**

服务要求：合同期内，根据学校需求，1年内提供一次安全管理制度服务。

服务内容：根据学校的实际情况，为了避免日常网络安全管理中所忽视的问题，而导致安全事件的发生，协助学校制定本单位的信息安全管理制度，并且在日常的网络安全建设、运维中，提供制度落实的相关建议。