**附件：网络安全运维要求**

1. **项目概况**

安徽信息工程学院网络安全运维及等保测评项目旨在提升校园网络安全防御能力，确保网络信息系统稳定运行的项目。该项目的开展对于保障学院教学、科研和管理等业务的顺利进行至关重要。以下将详细解析该项目的概况：

1.项目背景与目标

提升网络安全防护能力：随着网络信息技术的快速发展，网络安全问题日益突出，学院需要加强网络安全防护措施。本次通过从检测类安全服务、运营保障类安全服务、合规保障类服务三个方面提供服务，以安全专家结合安全工具的形式，全面保障学校各类系统在常态化安全运营中的网络安全。

满足等级保护测评要求：依据国家网络安全等级保护制度的要求，学院需定期开展网络安全等级保护测评。

2.项目内容与范围

服务范围：24个站点域名的安全检测服务、20个系统的渗透测试服务及20个核心资产的7\*24小时远程安全运营服务安全运营服务

防护内容：漏洞扫描、渗透测试、攻防演练、云安全防护服务、安全加固服务、重要时期安全保障服务及远程安全运营服务。

等级保护测评：对学院网络系统进行全面安全评估，确保符合国家规定的等级保护要求。

安徽信息工程学院网络安全运维及等保测评项目是一个全面保障学院网络安全的重要项目。消除校内基础业务系统网站的安全风险，提升校园整体网络的安全性，尽量避免重大安全事件的发生。保障我校网络及系统实现安全、可靠、有序、高效的运行，为我校各项业务稳定、安全运行提供必要的支持；

**二、主要标的**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务名称 | 服务期限 | 服务说明 |
| 1 | 检测类安全服务 | 1年 | 提供4次漏洞扫描服务、20个系统的渗透测试服务、1次攻防演练服务、24个站点域名的云安全防护服务、4次现场加固服务 |
| 2 | 运营保障类服务 | 1年 | 日常安全提供包含20个核心资产的7\*24小时远程安全运营服务，针对两会、国庆、护网等，重要时期提供2名网络安全高级专家在线保障服务 |
| 3 | 合规保障类服务 | 1年 | 3个信息系统，开展等级保护二级测评和安全整改工作 |

**三、技术要求**

**3.1服务需求**

本次网络安全运营服务需满足运营服务过程中数据的量化、可视化等要求，以安全专家结合安全工具的形式，全面保障我校各类系统在常态化安全运营中的网络安全。要求运维服务内容包含：检测类安全服务、运营保障类服务及合规保障类服务等内容，具体要求有：

### 3.1.1检测类安全服务

#### 1、漏洞扫描服务

**服务内容：**

漏洞扫描服务主要针对安徽信息工程学院系统层、网络层、数据库层、应用层进行安全评估，包括但不限于：操作系统、中间件、数据库、网络设备、虚拟化平台，即对安徽信息工程学院应用系统的运行环境进行安全评估。扫描设备检测规则库及知识库应涵盖CVE、CNCVE、CNVD、CNNVD等标准。扫描完成后并人工验证所发现的操作系统漏洞、数据库漏洞、弱口令、信息泄露及配置不当等脆弱性问题。提出准确有效的扫描报告，并针对漏洞扫描中出现的问题，提供解决方案，协助安徽信息工程学院进行解决。

* 系统漏洞扫描

系统扫描主要用于分析和指出有关网络的安全漏洞及被测系统的薄弱环节，给出详细的检测报告，并针对检测到的网络安全隐患给出相应的修补措施和安全建议。是提高内部网络安全防护性能和抗破坏能力，检测评估已运行网络的安全性能，为网络系统管理员提供实时安全建议等的主流功能。

* WEB漏洞扫描

Web扫描全面支持OWASP\_TOP10检测，可以帮助用户充分了解Web应用存在的安全隐患，建立安全可靠的Web应用服务，改善并提升应用系统抗各类Web应用攻击的能力（如：注入攻击、跨站脚本、文件包含、反序列化漏洞、代码执行、目录遍历、弱口令、信息泄漏、表单绕过等），协助用户满足等级保护、PCI、内控审计等规范要求。

* 数据库漏洞扫描

数据库授权扫描可帮助用户充分了解数据库存在的安全隐患，通过定期数据库系统安全自我检测与评估，提升各类数据库的抗风险能力。同时可以协助用户完成数据库建设成效评估，协助数据库安全事故的分析调查与追踪。

**响应时间：**

运维服务开始后，每季度提供1次漏洞扫描服务，并出具《安徽信息工程学院漏洞扫描报告》等材料。

#### 2、渗透测试服务

**服务内容：**

1. 实施方案制定、用户书面同意

渗透测试首先必须将实施方法、实施时间、实施人员，实施工具等具体的实施方案提交给用户，并得到用户的相应书面委托和授权。应该做到用户对渗透测试所有细节和风险的知晓、所有过程都在用户的控制下进行。

1. 信息收集分析

信息收集是每一步渗透攻击的前提，通过信息收集可以有针对性地制定模拟攻击测试计划，提高模拟攻击的成功率，同时可以有效降低攻击测试对系统正常运行造成的不利影响。通过对网站注册信息、共享资源、系统版本信息、已知漏洞及弱口令等信息的收集，发现可利用的安全漏洞，为进一步对目标信息系统进行渗透入侵提供基础。

1. 内部计划制定、二次确认

安全专家根据用户委托范围和时间，并结合前一步初步的信息收集得到的设备存活情况、网络拓扑情况以及扫描得到的服务开放情况、漏洞情况制定内部的详细实施计划。具体包括每个地址下一步可能采用的测试手段，详细时间安排。并将以下一步工作的计划和时间安排与用户进行确认。

1. 取得权限、提升权限

通过初步的信息收集分析，存在两种可能性，一种是目标系统存在重大的安全弱点，测试可以直接控制目标系统；另一种是目标系统没有远程重大的安全弱点，但是可以获得普通用户权限，这时可以通过该普通用户权限进一步收集目标系统信息。接下来尽最大努力取得超级用户权限、收集目标主机资料信息，寻求本地权限提升的机会。这样不停的进行信息收集分析、权限提升的结果形成了整个的渗透测试过程。

1. 生成报告

提供渗透测试报告。渗透测试报告详细说明渗透测试过程中的得到的数据和信息、并且详细的纪录整个渗透测试的全部操作。

1. 复测阶段

在经过第一次渗透测试报告提交和沟通后，等待用户针对渗透测试发现的问题整改或加固。经整改或加固后，测试人员进行回归测试，即二次复测。复测结束后提交给用户复测报告和对复测结果进行沟通。

1. 成果汇报

根据一次渗透测试和二次复测结果，整理渗透测试服务输出成果，最后汇报项目领导。

**服务工具：**

★为保证本项目的交付质量，可携带先进的渗透测试工具箱进行服务支撑。渗透工具箱应集成多款渗透测试专用武器，具备内网探测、dnslog/httplog检测、杀软进程高亮、WinRAR漏洞利用生成器、通用密码、图标替换、编码工具、反弹shell、开源漏扫软件报告处理、命令编码、ICP备案查询、木马捆绑器、shellcode混淆等功能。（提供功能证明截图）

**响应时间：**

运维服务开始后，每季度提供5个应用系统的渗透测试服务并出具《安徽信息工程学院渗透测试报告》，1年内共提供20个系统的渗透测试服务，所需渗透的应用系统需得到学校的认可。

#### 3、攻防演练

**服务内容：**

攻防演练是要求模拟黑客攻击系统或应用，发现漏洞并修复，帮助学校深入了解：黑客是如何进行攻击的、漏洞的成因、黑客利用方法，提升用户安全人员技术水平，从而进行针对性的防御。开展攻防演练，可以帮助教育行业单位检验本单位及下属学校、行业单位等的防守能力，在规定时间范围内进行攻击。

开展攻防演练，将从准备、实战、总结三个阶段进行：

1. 准备阶段

* 安全演练方案

组织召开安全演练工作动员会，落实工作组织机构，明确工作职责和任务，制定安全演练方案。

* 安全演练平台搭建

协助搭建安全演练监控指挥平台，保障演练过程中全程视频监控、全程录屏、全程审计。

* 安全演练规则宣贯

集中式演练规范规则的统一培训，说明攻击范围及攻击手法原则，严格禁止攻击团队违规操作，对因违规操作造成的后果予以追责，指挥部向被攻击方团队下发关于防守方法的规范，说明防守原则，遇到攻击时应正常应急处置，严禁进行断网等影响学校业务正常开展、过度防守的操作。

1. 实战阶段

* 信息收集

信息采集是所有实战攻击的第一步，也是最重要的一步。前期充足的资产收集工作会对后期实战攻击带来大量便利，甚至带来更多的突破口，降低实战攻击的难度。我们会从域名、IP、备案信息、业务、代码等层面收集资产信息，并从相关专业搜索引擎搜索敏感信息。

* 外网评估

从外网对目标进行外网攻击，评估目标互联网暴漏敏感信息情况。

从外网对目标单位开放在互联网上的网站或服务开展攻击，以获取核心数据、服务器权限或漫游进入内网为目的，从而暴露各教育单位对外网的防御薄弱点。

* 内网评估

在评估内网环节中，会对内网跳板机进行权限提升、权限维持、凭证窃取、网络拓扑分析、内网横向。

* 社会工程学

社会工程学是所有攻击中最有效的一种攻击方式，主要利用了人性的弱点来进行相关的攻击。社会工程学主要分为主动社会工程学与被动社会工程学的攻击。主动社会工程学主要集中在鱼叉攻击、水坑攻击、钓鱼邮件等交互式的攻击上，需要巧妙构造攻击场景才能成功。被动社会工程学主要集中在口令的猜解上，通过社工库发现相关用户的密码规则，收集生日、QQ号等信息进行排列组合，进而形成针对有效的社工字典进行口令猜解。

* 供应链

打击供应链已经成为目前主流的迂回攻击方式之一，测试过程中，寻找目标单位的木桶短板，通过打击供应链方式快速获得可以入侵用户系统的相关敏感信息。

* 0day

通常会使用通用组件、通用软件，如：操作系统、中间件、边界路由、防火墙、堡垒机、通用CMS等。安全演练时，会针对此类通用型组件，搜索其0day漏洞相关情报，并结合自由的相关0day储备，针对业务系统进行0day漏洞检测。

1. 总结阶段

* 安全演练总结

根据本次安全演练，对本次的攻击路径、漏洞详情以及溯源分析等内容。从攻击者、防守的思路分析总结。

进一步提升内部人员的技术水平，提高网络安全防护水平，提出增强防护建议并落实，建立和完善后续安全演练保障方案。

* 安全演练结果整改及复测

安全演练结束，下发安全演练的整改文件，协助完成整改及复测。

* 安全演练培训

通过本次安全演练总结，对本次攻击者攻击思路、攻击手段进行培训。防守队在本次防守的思路、攻击告警分析、应急处置等内容进行培训。

**运维响应时间：**

运维服务开始后，提供1次攻防演练服务，并出具《攻防演练总结报告》等材料。

#### 4、云安全防护服务

**服务范围：**

提供24个站点域名的云安全防护服务

**服务内容：**

1. 整体要求

通过统一云端平台提供网站防护服务能力，在需要时可以将防护站点纳入监测并作数据统一分析。系统基于云化SaaS架构，无需消耗虚拟机资源或本地物理资源，将CNAME别名指向云防护平台完成流量牵引。★能够对80和443端口以外的非标准端口提供防护，可配置非标准HTTP端口≥10000个，可配置非标准HTTPS端口≥5个。（提供可配置端口范围清单和功能证明截图）

1. 网站安全自检自查

对网站web漏洞、暗链、黑页、挂马、挖矿、webshell、网站可用性、敏感词汇等进行实时监测并预警。★支持监测访问流量，发现被访问网页是否存在深层暗链、Webshell等安全风险。（提供功能证明截图）同时对网站中的脆弱性定期进行检测，通过WEB应用漏洞扫描引擎定期对安徽信息工程学院站点域名进行网站漏洞检测，发现网站潜在的安全风险，同时针对发现的脆弱性进行验证，持续追踪监测，提供漏洞的新增、遗留与修复情况，对发现的漏洞提供虚拟补丁功能，在出现漏洞时通过虚拟补丁快速修补能力，为人工修复争取时间，保障能够及时修复，收敛网站安全风险。

1. 网站互联网业务实时防护

对网站的安全防护需要关注应用层与网络层的恶意攻击，对SQL注入、跨站脚本、恶意扫描、CC攻击等恶意攻击行为进行防护拦截。通过互联网业务实时防护，保障网站不出现暗链、黑页等情况，网站内容不被恶意篡改，网站业务不受CC攻击等网络层攻击而导致网站停摆，从防护层面上实现安徽信息工程学院网站互联网业务的整体安全。

1. 网站突发安全事件处理

当网站日常防护过程中突发安全事件时，7\*24小时值守的专家可通过云监测及时将安全事件通知管理人员，协同网站管理员进行应急处置。在面对严重安全事故时，通过微信公众号对网站进行一键关停，关停后访问网站的流量将被牵引至云端的镜像站，待应急处置完成后再重新开启网站，在保障攻击者无法实施下一步的攻击行为的同时不影响网站正常信息展示，最大程度减小事件带来的影响。

1. 网站业务高可用保障

为保障网站日常运行持续安全，方案提供实时数据监测，以多链路多点监测形式，进行域名解析可用性、网站服务可用性、以及网站内容可用性监测。网站可用性监测能够使学校实时了解网站可用性状态，包括域名、网站服务以及网站内容安全。同时，对于业务日常运行中因出口带宽阻塞而无法满足对外业务持续可用的情况，提供有效的DDoS攻击防护手段，进一步保障网站及各类业务系统的持续可用。

#### 5、安全加固服务

**服务范围：**

对漏洞扫描及日常巡检时发现的漏洞进行修复、配置隐患进行优化的过程。加固内容包括但不限于系统补丁、防火墙、防病毒、危险服务、共享、自动播放、密码安全等及所有服务器 。

1. 操作系统加固内容

可进行安全加固的操作系统包括Windows、Linux。操作系统的加固内容如下表所示，详细的加固列表可参见的操作系统安全加固规范。

|  |  |  |
| --- | --- | --- |
| 序号 | 加固大项 | 加固小项 |
| 1 | 账号管理和认证授权 | 账号、口令、授权、关机设置 |
| 2 | 协议安全配置 | IP协议安全、防火墙、SYN攻击防护 |
| 3 | 服务和共享配置 | 系统服务、默认共享、共享权限 |
| 4 | 日志安全配置 | 日志审核策略、日志文件设置 |
| 5 | 其它安全配置 | 空闲超时设置、自动播放、启动项、数据执行保护 |

1. 数据库安全加固

可进行安全加固的数据库系统包括Oracle、SQL Server、DB2。数据库的加固内容如下表所示，详细的加固列表可参见的数据库安全加固规范。

|  |  |  |
| --- | --- | --- |
| 序号 | 加固大项 | 加固小项 |
| 1 | 账号管理和认证授权 | 账号、口令 |
| 2 | 通信协议安全 | 网络数据传输安全、信任IP设置 |
| 3 | 日志安全配置 | 数据库审核策略、数据库日志文件设置 |
| 4 | 其它安全配置 | 连接超时设置、监听器密码 |

1. 中间件安全加固

可进行安全加固的中间件系统包括Tomcat、Apache、WebLogic、WebSphere。中间件系统的加固内容如下表所示，详细的加固列表可参见的中间件安全加固规范。

|  |  |  |
| --- | --- | --- |
| 序号 | 加固大项 | 加固小项 |
| 1 | 账号管理和认证授权 | 账号、口令 |
| 2 | 通信协议安全 | 启用https传输、更改tomcat默认端口 |
| 3 | 日志安全配置 | 日志记录设置 |
| 4 | 其它安全配置 | 登录超时、错误重定向、禁止显示文件 |

1. 网络设备安全加固

可进行安全加固的网络设备包括主流厂商的路由器、交换机。网络设备的加固内容如下表所示，详细的加固列表可参见的网络设备安全加固规范。

|  |  |  |
| --- | --- | --- |
| 序号 | 加固大项 | 加固小项 |
| 1 | 账号管理和认证授权 | 账号管理、登录安全要求、认证授权 |
| 2 | 通信协议安全 | SNMP协议安全、路由协议安全、IP协议安全 |
| 3 | 日志安全配置 | 日志记录设置 |
| 4 | 其它安全配置 | 关闭不必要的服务、端口 |

1. 安全设备安全加固

可进行安全加固的安全设备是主流厂商的防火墙。安全设备的加固内容如下表所示，具体的加固列表可参见的安全设备安全加固规范。

|  |  |  |
| --- | --- | --- |
| 序号 | 加固大项 | 加固小项 |
| 1 | 账号管理和认证授权 | 账号、口令、授权 |
| 2 | 访问控制安全 | 安全策略、远程管理 |
| 3 | 日志安全配置 | 启用本地日志、启用远程日志 |
| 4 | 增强安全要求 | 限定管理IP、更改默认Banner、设备自身安全设置 |

**响应时间：**

服务开始后，每季度提供1次安全加固，1年共提供4次现场的安全加固服务，对现有的安全设备进行评估，在得到学校授权和允许的情况下进行安全加固服务。

### 3.1.2运营保障类服务

#### 1、重要时期安全保障服务

**服务范围：**

1. 资产梳理

对服务范围内信息系统的物理资产、系统资产、数据资产以及网络结构等进行深入了解并分析，并输出《重要时期保障业务系统和资产列表》。

1. 脆弱性检查

根据《重要时期保障业务系统和资产列表》，对用户信息系统相关的网络结构、设备配置和主机配置等进行检查。涉及网络结构、安全设备、服务器、应用系统脆弱性检查。

1. 安全架构梳理与差距分析

网络架构分析是通过对用户评估范围内信息系统的网络拓扑及网络层面细节架构的评估。

1. 制定安全整改方案

根据脆弱性检查和渗透测试结果，针对其中较严重的安全隐患，结合重大活动的信息安全保障目标，为用户制定有针对性的安全整改方案，以消除或减少脆弱性，降低安全风险。

1. 制定应急预案

应急预案是针对可能发生的安全事件，为应急准备、事件报告、事件处理、灾难恢复的各个方面，预先制定的科学有效的行动规范和工作流程。在发生信息安全事件时，能够及时开展有序和有效的应急响应工作。

1. 组织应急演练

协助用户制定应急预案演练工作方案，并模拟在学校网络及重要设备出现故障等紧急情况下，依据前期制定的应急预案进行处理，其中包括事件的发现、上报、处理等环节。通过演练，使相关方熟悉应急处理流程，提高对安全事件的响应能力；同时验证预案的正确性和适用性，进行总结分析，并根据需要对应急预案进行修订。

1. 专题安全培训

针对用户在重大活动期间的信息安全组织结构、岗位职责、安全事件发现和上报机制以及处理流程等内容，为用户提供符合客户特点的安全培训内容。

1. 现场安全值守

通过现场值守人员对网络、主机、应用、数据库及其他设备运行状况进行监测，随时监控系统“健康”状态，如果发现问题及时与用户进行沟通，并提出解决方案，得到用户确认后对出现的问题进行解决，做到及时、准确保证无差错。

1. 定期安全巡检

根据用户在重大活动需要重点保护的资产规模及其面临的风险程度，安全专家定期前往用户现场进行安全巡检，及时发现信息系统中存在的安全隐患并进行改进。

1. 快速应急响应

在用户出现紧急情况、发生安全事件时，安全专家及时到达现场，进行有效的应急处理，最大限度地减少损失和降低影响。

1. 威胁情报赋能

重保期间云端威胁情报中心对全球重要产品、软件、系统的安全威胁资讯实时跟踪，收集、验证、转化为最新安全威胁情报，赋能给用户部署的安全设备，帮助用户掌握最新安全态势与热点技术，提前布置针对性措施。

1. 重保复盘总结

在重保时期保障结束后，将整合服务过程中的现场保障数据、云端防护数据、安全事件数据等，结合用户实际需求，梳理出工作过程亮点及重大成就，并输出总结报告。同时，根据重保期间的防护数据和安全事件处理等内容，对防护体系、处理流程和应急预案进行优化。

**响应时间：**

★运维服务开始后，针对两会、国庆、护网等重要时期提供网络安全高级专家现场保障服务，服务期间保障服务专家人数不少于 2 人，利用人工结合工具等方式对指定的单位信息系统、网站、服务器等资产进行实时监测，及时处理发现的系统安全事件。同时对安全威胁及事件进行取证溯源，并对内部安全设备策略进行配置优化，帮助用户建立完善的网络安全保障机制，并出具《安徽信息工程学院重要时期保障总结报告》，提供服务承诺函。

#### 2、远程安全运营服务

**服务范围：**

提供包含20个核心资产的7\*24小时远程安全运营服务，服务期间应按照要求提供《互联网暴露面检测报告》、《漏洞扫描报告》、《应急响应报告》、《漏洞预警报告》、《网络安全月刊》、《网络安全攻防周刊》、《半年度汇报PPT》、《年度汇报PPT》。

**服务内容：**

1. 资产发现与管理服务：

通过多种扫描器对学校网络中的业务进行全方位探测和识别的方式，发现如指纹、服务、端口、设备类型、CMS、应用等多种信息，并将其汇总成资产表格。协助学校完成资产管理制度的建设，协助在日常运维的过程中完成资产的新增、变更、下线等工作，并在此过程中明确资产的主要负责人。同时定期对资产进行扫描探测，检验是否有遗漏资产情况。

1. 互联网暴露面检测服务

从攻击者视角自动对学校资产周期性监控并对互联网资产暴露面的边界进行梳理，检测内容包括但不限于子域名、ip/ip段、服务、红队高关注的应用指纹以发现和清点学校未知的面向外部的资产和系统，并对搜集后的资产进行评估和分析资产属性确定资产是否存在风险。

1. 漏洞扫描与管理

★为了深入分析和理解漏洞影响和利用方式，服务专家通过互联网扫描引擎对服务范围内互联网资产进行漏洞扫描后，用户可在平台用户端界面看到漏洞详细信息，如风险等级、影响资产、涉事URL、处置状态、确认时间等。漏洞工单信息应包括漏洞的CVE编号、CVND编号、原始URL、测试URL、漏洞POC等信息、支持查看漏洞的POC和相关数据包并自动化生成针对漏洞的修复建议。（提供平台用户端界面截图证明）

1. 威胁检测与响应服务

建立威胁7\*24小时的持续监测机制，对学校内部安全设备的安全日志、流量进行关联分析，云端安全专家主动识别网络和主机中的安全威胁如邮件反诈检测等，并通过企业微信、钉钉等方式告知用户。在学校授权前提下，云端安全专家可根据学校操作规范进行安全威胁处置工作。安全事件处置的过程中，云端专家协助完成安全事件通报至对应的责任人，持续主动/协助完成事件处置，并在平台完成处置记录。★为满足日益复杂的安全趋势所带来的安全监测需求应支持为用户定义个性化策略，策略编排应支持分析组件和标准动作，至少包括过滤条件、AI研判、重复过滤、升级工单、联动处置等内容。（提供平台用户端界面截图证明）

1. 威胁情报服务

对重要产品、软件、系统的安全漏洞安全更新进行实时跟踪，提供漏洞简介、影响范围、安全建议等预警。同时对近期发生的重要安全事件进行分析，协助学校排查当前网络环境中是否有受影响的资产，同时协助学校开启相关防护策略，并持续跟踪威胁最新进展。

1. 应急响应服务

服务团队提供7\*24\*365的检测与实时响应；不同的安全专家根据不同的事件类型，协助学校第一时间进行解决，降低安全事件带来的影响。主要服务内容包括：突发事件信息收集、事件分析、分析报告提交、问题解决建议等在发生安全事件时协助业务恢复到正常服务状态，调查安全事件发生的原因，避免同类安全事件再次发生。

1. 复盘汇报服务

通过安全运营平台的数字化展示、安全大屏的展示、定期的网络安全工作汇报和常态化的安全运营报表，将网络安全工作变得可量化和可考核。每季度安排安全运营经理远程或现场进行阶段汇报，确认是否调整服务资产，沟通后续运营重点工作。

**服务工具：**

★提供流量探针作为远程安全运营服务的服务工具，流量探针应具备流量异常监控能力，支持对流量中的数据包、会话连接、重传包、网络报文等状态进行检测，可对业务网络流量传输异常告警；支持统计流量中的各类数据包进行统计，并通过图表形式展示，便于用户分析网络流量健康状态，支持的数据包类型不少于5种；（提供服务承诺函及第三方检测报告证明）流量探针基于大数据分析研判校园网络流量，发现高校整体安全威胁，通过采集流量信息进行安全分析，发现校园内安全威胁，将告警上报到安全运营服务平台，由安全运营服务平台生成服务工单，并触发后续安全服务流程。

### 3.1.3合规保障类服务

根据《网络安全法》及网络安全主管部门要求，对3个信息系统开展等级保护二级测评和安全整改工作。本次安全测评的范围主要包括基础支撑系统的物理环境、主机、网络、业务应用系统、安全管理制度和人员等等。安全测评通过静态评估、现场测试、综合评估等相关环节和阶段，从物理安全、网络安全、主机安全、应用安全、数据安全与备份恢复、安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理十个方面进行综合测评。

**四、服务输出标准**

**1、漏洞扫描服务：**

服务目标：通过对Web应用、数据库系统、弱口令、操作系统安全配置等进行漏洞扫描，了解现有信息系统的安全状况，识别信息系统的脆弱性、漏洞被利用的可能性、了解技术措施是否有效执行，并及时修补完善。

输出物：《安徽信息工程学院漏洞扫描报告》；

**2、渗透测试服务：**

服务目标：

1、全面漏洞检测：利用各类先进的渗透测试工具和技术，深入探测网络系统的各个层面，涵盖网络架构、应用程序、服务器配置等，确保不遗漏任何潜在的安全漏洞。精准定位SQL 注入、跨站脚本攻击（XSS）等 Web 应用漏洞及网络端口开放不当、弱密码等基础网络安全问题。

2、风险评估与分级：在发现漏洞后，依据漏洞的严重程度、被利用的可能性以及可能造成的影响，对安全风险进行科学合理的评估与分级。清晰区分出高、中、低不同等级的风险，直观展现网络安全隐患的优先级，提高安全问题处置效率。

3、提供可行修复建议：针对每一个被发现的安全漏洞和风险点，结合实际业务需求和网络架构特点，提供详细且具有可操作性的修复建议，包括技术层面的代码修改、配置优化，以及管理层面的安全策略调整、人员培训建议等。

输出物：《安徽信息工程学院渗透测试报告》

**3、攻防演练服务：**

服务目标：围绕学校目标展开全面深入的黑客攻击，检测学校网络安全纵深防护能力、评估应急响应手段是否有效，最后以测试结果为依据，对学校安全建设工作给出技术、管理上的优化调整建议。

输出物：《攻防演练总结报告》

**4、云安全防护服务**：

服务目标：1、网站安全自检自查，对网站web漏洞、暗链、黑页、挂马、挖矿、webshell、网站可用性、敏感词汇等进行实时监测并预警。定期对我校站点进行网站漏洞检测，发现网站潜在的安全风险，同时针对发现的脆弱性进行验证，持续追踪监测，提供漏洞的新增、遗留与修复情况，在出现漏洞时快速修补，收敛网站安全风险。

2、网站互联网业务实时防护，对网站的安全防护需要关注应用层与网络层的恶意攻击，对SQL注入、跨站脚本、恶意扫描、CC攻击等恶意攻击行为进行防护拦截。通过互联网业务实时防护，保障网站不出现暗链、黑页等情况，网站内容不被恶意篡改，网站业务不受CC攻击等网络层攻击而导致网站停摆。

2、网站突发安全事件处理，当网站日常防护过程中突发安全事件时，7\*24小时值守的安全服务人员将安全事件通知我校管理人员，协同网站管理员进行应急处置。在面对严重安全事故时，对网站进行一键关停，关停后访问网站的流量牵引至云端的镜像站，待应急处置完成后再重新开启网站，在保障攻击者无法实施下一步的攻击行为的同时不影响网站正常信息展示，最大程度减小事件带来的影响。

3、网站业务高可用保障，提供域名解析可用性、网站服务可用性、以及网站内容可用性监测。确保我校能够实时了解网站可用性状态，包括域名、网站服务以及网站内容安全。

输出物：网站安全事件实时告警（通过短信、邮件、手机微信等方式）

**5、安全加固服务：**

服务目标：1、为我校提供专业的信息资产安全配置建议，杜绝因配置不当导致存在的弱点，提升信息资产的安全性。

2、协助我校解决安全评估发现信息资产因配置不当存在的弱点，提高解决问题的效率。

3、提高信息资产防御外来入侵和蠕虫病毒袭击的能力，缩小影响范围，增强我校业务的连续性。

4、提高关键业务系统的可用性和可靠性，降低信息安全管理成本。

输出物：《安全加固方案》

**6、重要时期安全保障服务：**

服务目标：1、重保前期为学校提供安全自查、安全运维服务，提供信息安全防护及隐患检测能力；

1. 重保时期提供日志分析、安全值守、应急响应服务，保障网络和信息系统安全、可靠、稳定运行，最大限度地降低我校在重大会议及召开期间信息安全事故发生的可能性；
2. 重保后期复盘总结，梳理出工作过程亮点及重大成就，并输出总结报告。同时，根据重保期间的防护数据和安全事件处理等内容，对我校防护体系、处理流程和应急预案进行优化。

输出物：《安徽信息工程学院重要时期保障总结报告》、《应急响应处置报告》；

**7、远程安全运营服务：**

服务目标：1、协助学校梳理资产状况，结合学校组织和人员的梳理，将资产与人员关联起来，打通部门、人、资产、风险的关系。

1. 从攻击者视角自动对学校资产周期性监控并对互联网资产暴露面的边界进行梳理，实时感知网络资产的安全态势，协助学校将一些暴露的盲区资产进行精准管控，通过访问控制、关闭互联网访问、减少高危端口等手段，降低暴露面入侵风险。
2. 扫描学校网络中服务器、交换机、防火墙等，识别、分析系统中存在的资产漏洞，并将这些漏洞信息与业务资产信息通过漏洞管理平台进行统一关联、展示与追踪，使得管理人员可以有效地追踪业务资产漏洞全生命周期。
3. 对学校内部安全设备的安全日志、流量进行关联分析，云端安全专家主动识别网络和主机中的安全威胁，主动响应，协助学校闭环处置安全事件。云端建立威胁7\*24小时的持续监测机制，并提供安全威胁的修复协助与指导。
4. 帮助学校快速了解外部环境下最新的攻击行为和威胁信息，针对性地进行威胁防范。
5. 提供7\*24\*365的检测与实时响应，出现紧急安全状况时，值守人员会根据风险等级按照约定的流程进行快速响应、通报、处置，降低安全事件带来的影响。
6. 定期的网络安全工作汇报和常态化的安全运营报表，网络安全工作可量化和可考核。

输出物：《互联网暴露面检测报告》、《漏洞扫描报告》、《网络安全月刊》、《网络安全攻防周刊》、《半年度汇报PPT》、《年度汇报PPT》；

**8、等级保护测评服务：**

服务目标：对学院网络系统进行全面安全评估，确保符合国家规定的等级保护要求。

输出物：《等级保护测评报告》；