## 附件：铜仁幼儿师范高等专科学校网络安全服务采购项目清单

## 一、等保测评服务清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务项目** | **服务内容** | **服务要求** | **数量** |
|  | 二级测评 | 教务系统 | 1、安全测评服务人员和要求：开展等保测评工作，需明确一名具有信息安全等级测评师中级资格证书或以上的人员作为整个项目实施的项目经理，负责整个项目的协调、沟通、时间安排、进度督促、测评安排等工作。明确参与该项目现场测评并提供服务的人员具备安全等级测评师初级及以上资格，并按规定签订安全保密相关的协议或责任书，协助学校对信息系统进行定级确认、填写备案相关资料；2、网络安全等级保护测评，按照等保2.0标准，测评范围包括物理环境、主机、网络、业务、应用系统、安全管理制度和人员等。包含初次测评和验收测评，提供整改建议书和测评报告。3、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、安全运维管理十个方面，对被测评对象进行综合测评。4、二级等保测评指标68项，135个测评项。（仅安全通用标准，根据系统部署方式进行测评指标选择）5、提交资料：定级备案相关资料、问题清单、测评报告 |  |
| 学工系统 |
| 网络管理 |
|  | 安全建设整改服务 | 漏洞验证修复 | 1. 利用合法合规的安全扫描工具对现有网络系统服务器、网络设备、数据库、应用软件进行漏洞探测，对扫描结果进行人工验证，评估安全漏洞的危害程度及被威胁利用难易程度，根据情况进行验证修复，服务成果文档包含但不限于《验证修复报告》；
2. 针对评估结果并根据现状情况开展安全配置优化，进行风险规避；针对需要整改的漏洞协助相关系统业务人员开展整改。
 | 2次/2年 |
|  | 终端防御检测与响应平台 | 性能参数：最大支持管控终端安全管理系统软件客户端数量：纯内网场景或者2000点以上。安全策略模板一体化设置，全网资产盘点与风险可视，自动化日志可视化报表一键导出，管理账号分权分域，总分平台级联控制；管理平台需搭配客户端软件一齐使用，服务期内免费升级，含：终端安全管理系统软件V3.0（产品控制中心）(\*1套)；端点安全软件V3.0（服务器全量版）(\*10套)；软件升级（服务器端）；软件升级（PC端）。 | 1套 |
|  | 安全服务互联网出口加固服务 | 服务组件性能参数：网络层吞吐量：4G，应用层吞吐量：2G，防病毒吞吐量：600M，IPS吞吐量：600M，全威胁吞吐量：450M，并发连接数：200万，HTTP新建连接数：6万，SSL VPN推荐用户数：20，SSL VPN最大用户数：60，SSL VPN最大理论加密流量：160M，IPSec VPN 最大接入数：300，IPSec VPN吞吐量：270M。服务组件参数：规格：1U，内存大小：4G，硬盘容量：64G SSD，电源：单电源，接口：8千兆电口+2千兆光口SFP。含：防火墙软件基础级(\*1套)；防火墙软件增强级模块(\*1套)；云智订阅软件（AF8.0.7及以上版本适用）(\*1套)；产品质保(\*2年)；软件升级(\*2年)；硬件设备全部由中标商提供。 | 2年 |

## 二、网络信息化安全服务清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务项目** | **服务内容** | **服务要求** | **数量** |
|  | 网络信息化服务 | 应急演练服务 | 红方检测服务 | 通过专业渗透工程师组成红方【红队检测】，针对目标系统、软件、硬件和设备同时执行的多混合、基于对抗性的模拟攻击，以此来发现系统、技术和基础架构中存在的隐患。用尽可能接近真实环境攻击的方法来模拟黑客APT攻击，发现可能被黑客利用的安全漏洞，以此对目标网络安全状况进行评估，并出具成果报告：《铜仁幼儿师范高等专科学校渗透评估报告》、《铜仁幼儿师范高等专科学校渗透评估复测报告》。其中红方【红队检测】应具备信息安全风险评估服务能力，获得CCRC信息安全风险评估认证证书、工程师具备国家注册渗透测试专家认证、国家注册渗透测试工程师认证。 | 2次/2年 |
| 蓝队应急服务 | 通过资深的网络安全技术人员组成蓝方（应急方），提供应急支撑服务（第三方应急支撑服务）。在应急演练过程中，对学校提供重要时期安全保障服务。在重要时期为关键信息系统提供：组织架构设计、积极防御、实时检测、响应处置、攻击预测等安全服务，以提高学校的网络安全保障能力，保障应急演练活动的顺利进行，并出具成果报告：《铜仁幼儿师范高等专科学校应急支撑报告》，对红方渗透发现的漏洞和弱点进行修复，出具相应的整改报告包含但不限于整改方式与结果。蓝方【应急方】应具备信息安全应急处理服务能力，获得CCRC信息安全应急处理认证证书，工程师具备国家注册渗透测试专家认证、国家注册渗透测试工程师认证。 | 2次/2年 |
|  | 渗透测试服务 | 渗透测试：模拟黑客的真实攻击方法对系统和网络进行非破坏性质的攻击性测试。对重要的业务系统，进行模拟黑客的安全渗透测试，对系统中存在的安全漏洞进行准确查找，同时利用渗透性技术检测，发现应用系统未知的漏洞和安全隐患（包含但不限于：弱口令、本地权限提升、远程溢出、数据库查询等），并出具渗透测试报告及修复整改建议。同时在学校方修复漏洞后，对漏洞修复情况进行回归性测试。相对其他服务而言，渗透测试是一种对测试人员技术能力要求较高的纯技术服务，要求渗透测试人员有丰富的渗透经验及新颖的渗透思路。服务商安全团队有国家注册渗透测试专家，国家注册渗透测试工程师，高级网络安全管理师，拥有CISP、CCSC相应持证人员。服务过高校、医疗、政府、企业、能源等多个行业，有相当丰富的渗透测试经验，能从专业的角度执行标准化的测试工作，对渗透测试报告进行专业的解读，并提供相应的修复建议，协助学校有效提升网络安全能力。 | 4次/2年 |
|  | 安全巡检 |  每月一次。 对学校所有网络信息资产进行例行的安全检查，发现问题及时协调修复，并且出具相应《巡检报告》。要求运维服务商应具备信息系统建设和服务能力认证、ITSS运行维护认证。 | 24次/2年 |
|  | 基线及漏扫服务 | 基线及漏扫：利用合法合规的安全扫描工具对现有网络系统的服务器、网络设备、数据库、应用软件进行漏洞探测，对扫描结果进行人工验证，评估安全漏洞的危害程度及被威胁利用难易程度。服务成果文档包含但不限于《漏洞扫描报告》、《基线扫描报告》；服务商应具备信息安全风险评估服务能力，获得CCRC信息安全风险评估认证证书，服务工程师具备国家注册渗透测试专家认证、国家注册渗透测试工程师认证。 | 8次/2年 |
|  | 网络安全培训培训服务 | 安全意识培训 | 1. 提供一次网络安全意识培训工作，网络安全建设咨询不限次数。
2. 针对全校人员网络与信息安全现场或线上培训。安全意识培训内容包含法律法规要求、安全意识与安全管理、日常网络安全意识、本省实际同行业案例等内容并和学校沟通后出具相应的培训方案。
3. 培训方式：线上或线下，根据校方情况，灵活安排，线下培训场地由校方提供。
 | 2次/年 |
| 网络安全CISP培训 | 1. 在服务期内为学校从事网络安全相关工作的2名教职工提供网络安全CISP专业认证培训及考试认证服务。
2. 培训周期：15个工作日，全天；
3. 培训方式：线上或线下；
4. 考试方式：线下考试。
 | 2人 |
|  | 安全托管服务 | 安全托管服务 | 1. 服务概述：安全运营服务以保障网络安全“持续有效”为目标，围绕资产、漏洞、威胁、事件四个要素，通过云端安全运营中心和安全专家团队有效协同的“人机共智”模式7\*24H持续性开展网络安全保障工作，与用户一同构建持续（7\*24小时）、主动、闭环的安全运营体系。

二、服务内容1、运营准备阶段1.1、上线前策略检查：上线前安全专家对安全组件上的安全策略进行统一检查，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果。1.2、资产管理资产收集与录入：安全专家对服务资产进行收集，并将资产信息录入到安全运营平台进行管理。资产指纹探测：持续服务过程中安全专家定期对资产进行指纹（操作系统、中间件、软件厂商等信息）探测，并对指纹信息进行确认与更新，确保安全运营中心中资产指纹信息的准确性和全面性。资产变更管理：持续服务过程中安全专家定期对资产进行存活性探测，当发现未存活资产或资产发生变更时，安全专家对变更信息进行确认与更新，确保安全运营中心中资产信息的准确性和全面性。1.3、安全现状评估与处置对服务资产内漏洞问题、策略配置隐患问题进行归纳汇总。针对发现的问题提供修复方案与协助处理2、持续有效运营2.1、脆弱性管理漏洞扫描与验证：每季度针对服务资产的系统漏洞和Web漏洞进行全量扫描，并针对发现的漏洞进行验证，验证漏洞在已有的安全体系发生风险及分析发生后可造成的危害。漏洞修复优先级排序与通告：基于漏洞扫描结果、资产重要性及漏洞的威胁情报，对漏洞进行重要性排序，确定修复的优先级；并将最终结果通告给用户。漏洞可落地修复方案：对漏洞进行分析并输出可落地的修复方案，通过工单系统跟踪修复情况。漏洞复测与状态追踪：对修复的漏洞进行复测，及时更新漏洞工单的漏洞修复状态。弱口令分析与管理：实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat等。针对不同行业提供行业密码字典，有针对性的进行内网弱口令检测，并将检测发现的问题通过工单系统跟踪修复状态。最新漏洞通告与排查：实时抓取互联网最新漏洞与详细资产信息进行匹配，对最新漏洞进行通告与排查。通告信息中包含最新漏洞信息、服务资产受影响情况。最新漏洞处置指导：一旦确认漏洞影响范围后，安全专家提供专业的处置建议，处置建议包含两部分，修复方案以及临时规避措施。最新漏洞复测与状态跟踪：由安全专家对该最新漏洞建立工单进行持续跟踪。2.2、威胁管理7\*24H威胁分析研判：基于云端安全能力平台，云端专家提供7\*24小时的威胁监测：依托于安全防护组件、检测响应组件和安全平台，将海量安全数据脱敏，包括漏洞信息、共享威胁情报、异常流量、攻击日志等数据，经由大数据处理平台结合人工智能和云端安全专家使用多种数据分析算法模型进行数据归因关联分析，实时监测网络安全状态，对安全告警和威胁进行分析研判，并生成工单；7\*24H威胁通告：安全专家将云端分析确认后的真实威胁、事件实时通过微信、邮件等方式向用户通告，并提供处置建议。威胁影响面分析：安全专家针对每一个真实的威胁和告警，进行深度分析验证，分析判断受影响范围以及是否攻击成功，将深度关联分析的结果通过服务群/邮件等方式告知用户。威胁协助处置：安全专家针对分析结果提供对应的处置或加固建议（如封锁攻击源、设置安全策略防护等措施），并协助用户闭环流行威胁通告与排查：结合威胁情报，安全专家排查是否对服务资产造成影响并通知用户，及时协助进行安全加固。策略检查：每季度安全专家对安全组件上的安全策略进行统一检查，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果。策略调优：每季度安全专家根据安全威胁/事件分析的结果以及处置方式，按需对安全组件上的安全策略进行调整工作。2.3、事件管理安全事件调查与分析：安全专家7\*24H在线服务，针对主机发生的安全事件开展调查分析和影响面分析，对发生的安全事件进行人工鉴定和举证分析。安全事件处置：对客户网络内服务资产爆发勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，利用一些工具和脚本对恶意文件、代码进行根除，帮助客户快速恢复业务，消除或减轻影响。安全事件跟踪闭环：对发生的安全事件进行分级分类，并通过事件工单跟踪处置的情况，保障安全事件闭环。重大事件应急响应：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。排查攻击路径、恶意文件等。还原攻击路径，分析入侵事件原因，提供安全事件溯源结果。结合现有安全防御体系，指导用户进行安全加固、提供整改建议、防止再次入侵。3、运营成果可视安全运营周报：安全专家每周对服务资产进行安全运营情况的分析总结并输出《安全运营周报》。安全运营月报：安全专家每月对服务资产及整体安全状况进行分析总结并输出《安全运营月报》。安全运营半年度汇报：安全专家每半年总结阶段性安全运营情况并输出《半年度总结报告》发送给用户，向用户进行远程总结汇报。安全运营年度汇报：安全专家总结年度安全运营情况并输出《年度总结报告》发送给用户，向用户进行总结汇报。用户Portal：可视化portal支持随时查看服务范围内业务资产安全状态。支持在线展示所有脆弱性、威胁、事件工单的处置进程和结果支持用户在线对服务SLA进行查阅和监督。4、人员配置供应商需具备信息安全风险评估认证以及信息安全应急处理认证，供应商获得CCRC信息安全风险评估认证证书安全服务团队不少于5人，至少包含一渗透测试专家，二名注册渗透测试工程师，二名注册信息安全工程师。三、服务交付物《项目启动会PPT》、《首次安全威胁分析报告》《漏洞举证报告》、《漏洞清单》、《应急响应报告》、《事件处置报告》、《威胁情报》、《安全运营周报》、《安全运营月报》、《半年度总结汇报》、《年度总结汇报》 | 2年 |
| 7 |  | 第三方应急支撑服务 | 1. 若遇省/市主管部门下达网络与信息安全自查整改通报，协助网络安全团队积极完成问题整改，形成问题回执函，并协助后期整改。国家级安全生产大型检查期间，派遣专职安全工程师指导。
2. 在突发/重大信息安全事件后对包括计算机运行在内的业务系统进行维持或恢复，提供7×24小时应急响应支持；接到应急响应需求后，30分钟以内，提供响应支撑，响应方式包括电话、邮件、微信、QQ、现场处置等。
3. 响应结束后提交详细《应急响应报告》，报告内容包含但不限于事件起因、分析过程、处理过程、处理方法、处理结果、整改建议等，并保持一个月的后期跟踪，因此服务商具应备信息安全风险评估服务能力，获得CCRC信息安全风险评估认证证书，服务工程师具备国家注册渗透测试专家认证、国家注册渗透测试工程师认证。
4. 针对主管部门要求学校对网络与信息安全状况开展自查工作时，协助学校完成网络安全自查报告。
5. 重保服务是在重要时期为关键信息系统提供：学校架构设计、积极防御、实时检测、响应处置、攻击预测等安全服务，以提高学校的网络安全保障能力，保障重大活动的顺利进行，成立重保领导小组，重保领导小组由学校分管网络安全领导及服务方重保负责人联合组成，主要负责安全保障工作中关键问题的决策，以及为重保工作的顺利开展协调充足的资源。重保领导小组下设学校重保工作小组和服务方重保工作小组，主要负责重保工作中的具体安保工作的执行以及双方在重保工作中的配合与沟通，因此服务商应具备信息系统建设和服务能力认证以及信息安全风险评估服务能力，获得CCRC信息安全风险评估认证证书，服务工程师具备国家注册渗透测试专家认证、国家注册渗透测试工程师认证。
6. 重要时期以贵州省教育厅文件及学校重保要求为准，累计时间不得少于2个月/年。
 | 2年 |