一、项目采购需求

一、项目概述

按照网络安全等级保护建设要求，学院分别于2020年12月、2021年12月通过网络安全项目、网络安全（二期）项目，采购了防火墙、态势感知、上网行为管理等网络安全设备，并配置了线上安全托管服务来保障设备和策略的有效运行。2024年5月学院采购了线下安全专家服务项目(一年)，以实现安全问题处置闭环。现所有设备和服务均已到期，需采购本次网络安全运维服务，服务内容具体包含：

1.为防火墙、上网行为管理、态势感知等关键设备采购软件升级、特征库更新和规则库更新；

2.采购网络安全服务，包括线上安全托管服务、安全专家线下处置服务、网络安全应急演练、渗透测试、基线核查、威胁情报网关服务、网络安全教育培训等。

二、项目执行的相关标准

执行国家与地方相关法律法规及行业现行规范和标准，满足采购人的要求。

三、技术要求（功能和质量）

1、设备软件升级和特征库升级服务：

序号	设备名称/品牌/型号	服务名称	服务内容及要求	数量	单位
1	上网行为管理/深信服/AC-1000-B1400	URL&应用识别规则库升级	1.包含对各种 URL 类型精细化管控，所有 URL 类型都支持区分“网站浏览”、“文件上传”、“其他上传”、“HTTPS”等细分行为并分别做权限控制；支持加密的网页、论坛、BBS 上的发帖行为精细化管理：过滤同时匹配三个以上关键字过滤的网络发帖行为、允许用户浏览帖子但不准发帖功能； ▲2.定期更新规则库，支持不低于 9000 种应用规则数、支持不低于 6000 种的应用；支持根据标签选择应用，并支持给每个应用自定义标签；支持根据标签选择一类应用做控制；（需提供功能高清彩色截图，并加盖制造商公章）	3	年
2	上网行为管理/深信服/AC-1000-B2500	URL&应用识别规则库升级	1.包含对各种 URL 类型精细化管控，所有 URL 类型都支持区分“网站浏览”、“文件上传”、“其他上传”、“HTTPS”等细分行为并分别做权限控制；支持加密的网页、论坛、BBS 上的发帖行为精细化管理：过滤同时匹配三个以上关键字过滤的网络发帖行为、允许用户浏览帖子但不准发帖功能； ▲2.定期更新规则库，支持不低于 9000 种应用规则数、支持不低于 6000	3	年

			种的应用；支持根据标签选择应用，并支持给每个应用自定义标签；支持根据标签选择一类应用做控制；（需提供功能高清彩色截图，并加盖制造商公章）		
3	态势感知/深信服/SIP-1000-B400	特征库升级	1.态势感知规则库不低于33000种。 2.包含实体行为分析功能，通过对这些对象进行持续的行为分析和行为画像构建，识别服务器异常，包括DGA解析请求、外联C&C服务器、异常协议利用、下载可疑文件、异常横向访问等。 3.支持资产自动识别和资产扫描功能，支持自动入库、手动入库、设置扫描目标等功能，扫描类型可选择存活性（ARP/TCP/ICMP）、服务/端口（常用/全局）、操作系统、应用识别等。 ▲4.定期更新弱密码主动扫描能力，支持SMB、MySQL、Oracle、RDP、SSH、Redis、MongoDB、ElasticSearch、MSSQL等扫描协议，支持自定义扫描周期、发包频率、扫描时间段、扫描优先级、扫描对象等。弱密码检测规则支持高度自定义，包括规则名称、生效域名、规则配置、账号白名单、密码白名单、弱密码内容导入文件，其中规则配置至少支持密码长度、字符种类、字典序、密码与账号相同、web空密码等。	3	年

			（需提供功能高清彩色截图，并加盖制造商公章）		
4	探针/深信服/STA-100-B 2600	特征库升级	1.探针规则库不低于 33000 种。 ▲2.定期更新检测能力，包括不限于命令注入检测、PHP 代码检测、XSS 攻击检测、Webshell 上传检测、SQL 注入检测、XXE 攻击检测、JAVA 代码检测、SQL 非注入型检测、MYSQL 解析增强、php 反序列化检测等，针对命令注入检测、SQL 注入检测等类型支持自定义高检出、低误报模式。（需提供功能高清彩色截图，并加盖制造商公章）。 3.支持多种类型弱口令策略可选；支持自定义 FTP 弱口令检测，规则设置如空口令、用户名和密码相同、长度、弱口令列表等；支持口令暴力破解检测不同类型（FTP/WEB 登录）的爆破次数。 ▲4.定期更新敏感信息检测功能，内置身份证、MD5、手机号码、银行卡号、邮箱等敏感信息，可自定义敏感信息检测策略选择组合的敏感信息，可基于 IP 统计和连接统计等方式进行命中次数统计（需提供功能高清彩色截图，并加盖制造商公章）。 ▲5.定期更新漏洞攻击检测能力，包括不限于 Database 漏洞攻击、DNS	3	年

			漏洞攻击、FTP 漏洞攻击、Mail 漏洞攻击、Media 漏洞攻击、Network Device、Shellcode 漏洞攻击、System 漏洞攻击、Telnet 漏洞攻击、Tftp 漏洞攻击、Web 漏洞攻击、IPS 云防护等服务漏洞攻击检测（需提供功能高清彩色截图，并加盖制造商公章）。		
5	零信任/深信服/aTrust-1000-B1080M	软件升级	设备的新软件版本上市后及时升级到最新稳定版本，保证设备稳定运行。（提供相关承诺函并加盖投标单位公章，格式自拟）	3	年
		移动端应用自动封装服务	1.提供移动端应用封装能力，支持和本地的移动端对接，收缩内网业务系统的暴露面，不低于 1200 个移动端并发授权。 2.无需进行代码开发，只需将原包应用上传到封装平台，系统会自动将 sdk 包打包进本地移动端应用中，实现认证后才能访问移动端内网应用的功能。不借助第三方 APP，师生无感知的实现业务访问。		
6	防火墙/深信服/AF-2000-B2300	特征库升级	1.定期更新包括不低于 4500 项 WEB 应用防护识别库、不低 17000 项 IPS 特征库、不低于 128 万种僵尸网络防护库、不低于 1500 种漏洞分析识别库和不低于 9000 种 URL&应用识别库，保持设备具备检测防御最新威胁的	3	年

			能力。 ▲2.定期更新漏洞检测规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。（需提供功能高清彩色截图，并加盖制造商公章） 3.定期更新僵尸主机检测模块，可识别主机的异常外联行为，最新的僵尸网络特征库不低于 128 万种。		
		软件升级	1.设备的新软件版本上市后及时升级到最新稳定版本，保证设备稳定运行。（提供相关承诺函并加盖投标单位公章，格式自拟）	3	年
7	防火墙/深信服/AF-2000-B2180	特征库升级	1.定期更新包括不低于 4500 项 WEB 应用防护识别库、不低 17000 项 IPS 特征库、不低于 128 万种僵尸网络防护库、不低于 1500 种漏洞分析识别库和不低于 9000 种 URL&应用识别库，保持设备具备检测防御最新威胁的能力。 ▲2.定期更新漏洞检测规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。（需提供功能高清彩色截图，并加盖制造	3	年

			商公章） 3.定期更新僵尸主机检测模块，可识别主机的异常外联行为，最新的僵尸网络特征库不低于128万种。		
		软件升级	设备的新软件版本上市后及时升级到最新稳定版本，保证设备稳定运行。（提供相关承诺函并加盖投标单位公章，格式自拟）	3	年
8	数据库审计DAS-1000-A620	软件升级	设备的新软件版本上市后及时升级到最新稳定版本，保证设备稳定运行。（提供相关承诺函并加盖投标单位公章，格式自拟）	3	年

2、安全服务：

服务类别	服务名称	服务内容	数量	单位
线上安全托管服务	线上安全运营服务	管控的资产数量≥40. 1.资产管理服务：对用户资产进行全面发现和深度识别，并在后续服务过程中触发资产变更等相关服务流程，确保资产信息的准确性和全面性；结合安全工具发现的资产信息，首次进行服务范围内资产的全面梳理（梳理的信息包含支撑业务系统运转的操作系统、数据库、中间件、应用系统的版本、类型、IP地址、应用开放协议和端口等）。资产指纹信息梳理，梳理信息化资产详情（含操作系统、中间件、数据库、应用框架，开发语言等指纹信息）并将梳理的信息录入系统。 ▲2.漏洞管理：前期每月或根据客户需求对服务的资产、应用系统开展漏洞扫描工作（包括漏洞	3	年

		扫描及复检，发现系统环境潜在风险隐患），并提供专业安全测评报告，报告需提供客观的漏洞修复优先级指导，不能以漏洞危害等级作为唯一的修复优先级排序依据。排序依据包含但不限于资产重要性、漏洞等级以及威胁情报（漏洞被利用的可能性）三个维度（提供漏洞优先级排序截图，展示优先级排序情况）。中期持续对资产漏洞、弱密码以及攻击事件负责，结合线下服务对未覆盖完全的资产进行防护，进行相应漏洞补丁等操作； 3.为用户提供服务监控门户，在门户中可查看业务安全状态，处置中的失陷事件以及针对这些事件的处置进度，处置责任人、联系方式等信息，方便用户实时了解服务效果； ▲4.实时监测网络安全状态，对攻击事件自动化生成工单，及时进行分析与预警。攻击事件包含境内外黑客攻击事件、暴力破解攻击事件、持续攻击事件（提供安全事件（如暴力破解）的工单截图，需展示当前安全事件的处置状态）。工单需详细记录威胁事件的分析过程，便于工单流转和过程回溯。当处置完威胁事件后，将对应的威胁事件进行关闭，完成整个威胁闭环过程。工单支持展示出当前需要用户审批的工单及其具体情况，使得用户能完成与服务人员的协同处置，共同确保安全威胁和事件得到准确处置。 5.根据安全事件分析的结果以及处置方式，根据用户授权情况按需对安全组件上的安全策略进行优化调整工作。		

		6.威胁监测与主动响应服务：结合最新威胁情报，及时对流行威胁进行评估、风险通告预警。提供威胁情报预警实际案例。线上安全专家需排查是否对用户资产造成威胁，及时通知用户并协助修复或调整安全策略。 7.每周检查全网设备异常日志，并做好工单记录。 8.每周进行备份数据完整性检查，模拟各份数据恢复，检查其可用性。 9.支持面向用户的安全报告与交付物管理，可生成、导出、下载各类安全报告，包括但不限于风险评估报告、安全服务运营报告、安全能力差距分析报告、未公开威胁报告、事件分析与处置报告、应急响应报告等，使得用户能直观查看服务成果和使用效果。 10.提供 7*24*365 的应急响应服务，出现安全攻击事件，第一时间处理。 11.提供节假日、特殊时期网络安全重点保障服务。在国家或省市等重要特殊时期提供人工线上安全服务值守，包括态势感知等安全流量设备日志分析与研判，保障学院重要特殊时期的网络安全。		
	结合处置服务	1.漏洞扫描：使用漏洞扫描工具的漏洞扫描功能，按照学院实际需求，快速从内网和外网两个角度来查找网络结构、网络设备、服务器主机、数据和用户账号/口令等(需线下进行）。按照学院实际需求，提供对应线下资产数的漏洞扫描服务。同时通过安全托管服务实现前期对服务的资产进行扫描，中期持续对资产漏洞、弱密码以及攻击事件负责，结合线下服务对未覆盖完全的资产		

		进行防护，进行相应漏洞补丁等操作。使用系统漏洞扫描工具对需要线下进行的操作系统、中间件等进行漏洞、端口、弱口令扫描，扫描完成后由技术人员对漏洞进行确认测试，取得授权后，主动联系并协助开发人员整改。 2.应急响应：基于主动响应和被动响应流程，对页面篡改、通报、断网、webshell、黑链等各类严重安全事件进行紧急响应和处置的解决方案。出现安全攻击事件。提供 7*24*365 的应急响应服务，出现安全攻击事件，第一时间处理，若需线下处置，2 小时内进行线下处置响应。 3.需对线上发现的问题进行处置，包括但不仅限于内网脆弱性问题，病毒类事件，入侵行为、勒索、挖矿类事件等。针对分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，帮助用户快速恢复业务，消除或减轻影响。基于主动响应和被动响应流程，对页面篡改、通报、断网、webshell、黑链等各类严重安全事件进行紧急响应和处置。 4.提供节假日、特殊时期网络安全重点保障服务。在国家或省市等重要特殊时期提供线上专家值守，包括态势感知等安全流量设备日志分析与研判，保障学院重要特殊时期的网络安全。每月检查全网设备的特征库、病毒库版本发布情况，提供现网设备的免费特征库、病毒库的持续升级服务。 5.每月检查全网设备的软件版本升级发布情况，提供现网设备的免费软件版本升级服务。		

		6.协助学院进行主管单位网络安全检查工作，提供相应的检查前技术先检及资料准备等服务。 7.协助学院开展信息系统等级保护测评，开展相应的网络安全检查和整改工作，提供等级保护2.0测评差距报告上，有关于网络结构、网络设备配置、安全设备的整改优化工作。 8.提供其他网络安全相关的咨询和顾问工作，包含但不仅限于对网络安全相关的设备选型、系统建设方案提供咨询建议，提供校内新建、改扩建项目的安全技术服务咨询支撑服务等。 9.人工审核：通过人工的资料审阅、现场勘查、上机测试等方法，人为的对相关资料进行筛选核实与审批。		
专项安全服务	安全专家线下处置服务	1.每周至少1次，需高级安全服务工程师及以上人员，到现场综合运用丰富的技术经验及威胁情报知识库，借助态势感知平台设备对接能力及安全检测能力结合业务应用、实际情况，以及安全专家线下现场的自主发现，包括但不限于以下内容: 2.线下处置终端侧的安全告警，根据不同病毒类型，为学院提供相应网络安全处置专业工具，其中对于频繁告警问题进行深度研判处置闭环，协助学院做好防护措施。 3.线下处置服务器侧安全告警及分析告警数据，进行相应修复整改，并协助学院做好持续运维防护措施。 4.线下处置网络侧攻击告警并协助学院做好处置及策略预防。 5.线下协助学院各业务系统供应商做好漏洞管理，	3	年

		漏洞整改部分需系统供应商进行的，由学院授权并协调安全专家协助系统供应商进行整改。 6.协助学院梳理并完善网络安全相关管理制度。 7.确保学院无网络安全重大事故发生，及时处置线下突发安全事件。		
	网络安全应急演练	一、服务概述： 每年 1 次，根据相关国家标准或国际标准，按照应急演练实际情况结合学院的 IT 建设现状，修订对应的应急演练场景专项应急预案，以指导应急响应团队应对与处置安全事件；制定应急演练方案及脚本并协助开展应急演练，模拟安全事件发生及处置的全过程，提高应对安全事件的处置能力，预防和减少安全事件造成的危害和损失。 二、具体服务内容： 应急演练服务主要通过模拟各种突发事件场景进行，根据突发网络安全事件的性质，应急演练场景可分为：有害程序事件演练、网络攻击事件演练、信息破坏事件演练、设备设施故障演练；有害程序事件：内网传播型病毒应急演练、勒索病毒应急演练、挖矿病毒应急演练等；网络攻击事件：漏洞攻击应急演练、后门攻击应急演练等；信息破坏事件：网站篡改应急演练、网页挂马应急演练等；设备设施故障事件：网络设备故障应急演练、服务器故障应急演练等；多场景多样化：按照客户要求设计多场景的演练方案，综合检验突发事件时的应急处置能力及预案完善性。演练效果展示：通过态势感知平台（按需）直观展现内网主机状况，更好的展现演练效果。修订专项应急演练预案：应急演练结束后，按照应急演练实际情况并结合学院的 IT 建设	3	年

		现状修订对应演练场景的专项应急预案。		
	渗透测试	一、服务概述： 每年 1 次，每次 4 人/天，高级服务工程师在获得授权的情况下，线下以主流渗透工具结合自有的工具模拟黑客攻击为主要手段，发现常见的高中危漏洞为主要目标，将发现的安全漏洞进行整理，给出详细说明，并针对每一安全漏洞提供相应的解决方法，并结合客户修复情况，协助客户针对修复后的漏洞进行复测验证。 二、渗透测试具体服务内容： a.前期交互阶段 与用户进行沟通、确定渗透测试的时间、范围、深度、测试方式（黑盒 OR 白盒、现场 OR 远程）等问题，并拿到用户签署的渗透测试授权函； b.情报搜集阶段 服务团队在拿到用户授权后开始情报搜集工作，搜集阶段是对目标用户的系统进行一系列踩点工作，包括：基础资产收集、互联网信息泄露搜集、指纹识别、业务系统功能收集、接口信息收集等。 c.威胁建模阶段 在搜集到充分的情报信息之后，服务工程师对获取的信息进行威胁建模与攻击规划，从大量的信息情报中理清思路，确定出最可行的攻击通道。 d.漏洞分析阶段 漏洞分析阶段是对威胁建模阶段的初步实践，本阶段需要针对威胁建模阶段总结的测试方法进行一一验证，通过测试总结出可行的测试方法，排除不可行的测试方法。	3	年

		e.渗透攻击阶段 本阶段是对用户的业务系统进行攻击性测试的阶段，漏洞分析阶段总结出的可行的漏洞利用方法，本阶段可以直接拿来利用，并以此为基础扩大渗透战果。 f.报告输出阶段 渗透测试工作全部完成后输出报告，报告中阐明客户系统中存在的安全隐患以及专业的漏洞风险处置建议。 g.汇报阶段 本阶段由安全服务团队向用户汇报本次渗透测试的成果，并现场对用户提出的疑问进行现场答疑。 三、补充说明 当学院有攻防演练需求时，可以提供攻防演练人员技术服务支持。实际演练，以保障学校隐私数据为前提，和学校沟通由组织攻防两端针对业务系统、主机、网络设备、内网环境安全以及数据等采取必要的攻击行为，以提权、控制业务、获取数据为目的，检验参演单位的人机结合、协同处置等网络安全方面的综合防护能力。		
	基线核查	一、服务概述： 每年 2 次，对重要服务器、操作系统、网络设备、安全设备、中间件、数据库等基于信息安全风险的角度进行配置核查，检测网络设备的安全策略弱点和部分主机的安全配置错误等安全隐患。提出整改建议，指导运维人员优化配置策略，从而达到相应的安全防护要求。 二、具体服务内容： a.主机操作系统检查内容	3	年

		主机操作系统安全配置检查包含但不限于以下内容：帐号和口令管理、异常启动项、认证和授权策略、访问控制、通信协议、日志审核策略、文件系统权限、防 ddos 攻击、剩余信息保护、其它安全配置。 b.数据库检查内容 数据库安全配置检查包含但不限于以下内容：帐号和口令管理认证、认证和授权策略、访问控制、通讯协议、日志审核功能、其他安全配置。 c.中间件检查内容 中间件及常见网络服务安全配置检查包含但不限于以下内容：帐号和口令管理认证、授权策略、通讯协议、日志审核功能、其他安全配置。 d.网络设备及安全设备检查内容 网络及安全设备安全配置检查包含但不限于以下内容：OS 安全、异常启动项、帐号和口令管理、认证和授权策略、网络与服务、访问控制策略、通讯协议、路由协议、日志审核策略、加密管理、设备其他安全配置。		
	威胁情报网关服务	一、具体服务内容： 1.威胁情报联动能力:通过云端主动探测+挖矿、黑客工具等协议特征库，实现第一次未知通信即可检测出未知威胁的失陷主机，并拦截通信流量，避免被占用资源，5min 内全网同步，保护业务资产安全。 2.威胁情报主动探测:主动向目的 IP+端口发送多种挖矿、黑客工具协议相关请求包，若服务器对任意请求包有相应返回，则认为该目的 IP+端口开启挖矿、恶意通信服务，同时形成挖矿、黑客	3	年

		工具协议等规则下发。 3.百亿级规则库赋能防火墙：联动云端的百亿级威胁情报（防火墙自身本地规则库大概只有百万级），实时拦截非法的外联访问行为和恶意病毒，通过云端情报带来更强的杀毒能力，支持文件MD5的云端检测功能，每五分钟下发全球最新病毒情报，全面识别已知和未知变种病毒（勒索、变种病毒检出率90%以上）性能消耗小，高检出低误报。		
	网络安全教育培训	一、具体服务内容： 每年不少于1次，对贵州电子科技职业学院的师生开展网络信息安全意识教育与培训，内容包括：信息安全基础、最新网络安全及趋势、密码安全、上网安全防护、正确使用软件、邮件安全、手机安全、工作环境安全等。	3	年

四、商务要求

（一）交付时间：自合同签订起，15个工作日内开始提供服务，服务期3年。

（二）交付地点：采购人指定地点。

（三）付款条件（进度和方式）：

运维服务费用每年支付1次，合同期届满前一个月内，采购人对供应商进行考核且达标后15个工作日内向中标供应商支付年度服务费用。

（四）售后服务：

提供7×24小时、周一至周日全天电话支持服务，

若遇紧急问题需现场支持，2 小时电话响应，4 小时内赶到现场。

（五）保险：按照国家相关法律法规执行。

（六）投标有效期：90 天

（七）其他：

1.专业技术服务：中标供应商需要根据业务规则制定培训方案，包含但不仅限于关键用户应用培训、系统管理员培训、软件安装配置培训等，每年不少于 1 次。

2.供应商中标后在领取成交通知书时须提供 2 份纸质响应文件，纸质响应文件须与上传到贵阳市公共资源交易中心的电子响应文件内容完全一致。

二、供应商资格条件

符合政府采购法第二十二条规定，提供政府采购法实施条例第十七条规定资料。

1.具有独立承担民事责任的能力：提供法人或者其他组织的营业执照等证明文件或自然人的身份证明；

2.具有良好的商业信誉和健全的财务会计制度：提供2023年度或2024年度经合法有效的第三方会计师事务机构审计的完整财务报告；新成立未满1年的公司需提供基本开户银行出具的资信证明。部分其他组织和自然人，没有经审计的财务报告，可以提供银行2025年出具的（有效期内）的资信证明。(复印件或扫描件加盖供应商公章)

3.具有履行合同所必需的设备和专业技术能力：投标供应商自行书面承诺具备履行合同所必需的设备和专业技术能力；(提供承诺函)

4.具有依法缴纳税收和社会保障资金的良好记录：提供2025年至投标截止时间前任意1个月依法缴纳税收和社会保障资金的有效证明材料（依法免征、免缴、缓交的须提供相应证明材料）；(复印件或扫描件加盖供应商公章)

5.参加本次政府采购活动前三年内，在经营活动中没有重大违法记录：提供参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明；

6.法律、行政法规规定的其他条件：

（1）供应商须承诺在“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）等渠道未被列入失信被执行人名单、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单中。

7.本项目所需特殊行业资质或要求：无。

8.本项目专门面向小微企业采购。行业为：软件和信息技术服务业。

三、评审规则（评审方法、评审因素、价格权重等）

评审项目	评分标准	分值
报价分（满分 10 分）	投标报价得分＝（评标基准价/有效投标报价）×10 注： ①评标基准价指满足磋商文件要求且投标价格最低的最后报价，投标报价指满足磋商文件要求的各投标单位的最后投标报价。 ②本项目专门面向中小企业（含监狱企业、残疾人福利性单位）采购，供应商的投标报价不再进行价格扣除。 ③磋商小组认为供应商的报价明显低于其他通过资格审查供应商的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在磋商小组规定的合理时间内提供书面说明，必要时提交相关证明材料【成本价格分析及近一年内所投产品签订的合同（原件）】；供应商不能证明其报价合理性的，磋商小组有权将其作为无效投标处理。	10 分
主观分（满分 15 分）	**1、总体服务方案（10 分）：** 磋商小组根据投标供应商提出的项目整体服务方案进行综合评价，方案内容包括但不限于(1)服务内容；(2)服务保障措施；(3)故障响应时间；(4)故障处理措施；(5)服务质量保证措施等。 ①方案内容完整，针对性、可行性、合理性、可靠性、安全性强，满足采购人需求得 10 分； ②方案内容基本完整，针对性、可行性、合理性、可靠性、安全性一般，得 6 分； ③方案内容不够完整，针对性、可行性、合理性、可靠性、安全性差，得 3 分； ④未提供服务方案的，本项不得分。 **注：** **方案内容完整、合理、可行、针对性强指：** **a.提供的方案内容完整、不存在缺项、漏项，服务内容在客**	

	观上有先后顺序，不存在顺序错误的逻辑，不存在前后表述不一的矛盾； b.准确把握本项目采购需求中的重、难点，分析各类情况可能发生的不可预见的情形，并尽可能列明多种详细预案； c.基于本项目采购需求的内容，针对不同的需求，提供有利于实现本项目目标的解决方案。 方案内容完整、合理、可行、针对性一般指： a.提供的方案内容完整、不存在缺项、漏项，但服务内容在客观上存在顺序错误的逻辑，有前后表述不一的矛盾； b.未能把握本项目采购需求中的重、难点，分析可能发生的不可预见各类情况； c.针对不同的需求，提供的解决方案不利于本项目本项目目标的实现。 方案内容不完整、针对性差指： a.提供的方案内容不完整，与采购需求存在明显的缺项、漏项； b.未提供分析本项目可能发生的不可预见各类情况； c.针对不同的需求，未提供实现本项目目标的解决方案。	
	2、售后服务方案（5 分）： 磋商小组根据供应商提供的售后服务方案进行评审，方案内容包含但不限于（1）售后服务机构；（2）人员配置、人员培训计划；（3）响应时间；（4）质量保障措施；（5）应急预案保障措施等。 ①方案内容完整，针对性、可行性、合理性强，得 5 分； ②方案内容基本完整，针对性、可行性、合理性一般，得 3 分； ③方案内容不够完整，针对性、可行性、合理性差，得 1 分； ④未提供服务方案的，本项不得分。 注： 方案内容完整、合理、可行、针对性强指： a.提供的方案内容完整、不存在缺项、漏项，服务内容在客	5 分

	观上有先后顺序，不存在顺序错误的逻辑，不存在前后表述不一的矛盾； b.准确把握本项目采购需求中的重、难点，分析各类情况可能发生的不可预见的情形，并尽可能列明多种详细预案； c.基于本项目采购需求的内容，针对不同的需求，提供有利于实现本项目目标的解决方案。 方案内容完整、合理、可行、针对性一般指： a.提供的方案内容完整、不存在缺项、漏项，但服务内容在客观上存在顺序错误的逻辑，有前后表述不一的矛盾； b.未能把握本项目采购需求中的重、难点，分析可能发生的不可预见各类情况； c.针对不同的需求，提供的解决方案不利于本项目本项目目标的实现。 方案内容不完整、针对性差指： a.提供的方案内容不完整，与采购需求存在明显的缺项、漏项； b.未提供分析本项目可能发生的不可预见各类情况； c.针对不同的需求，未提供实现本项目目标的解决方案。	

客观分（满分 75 分）	**1、服务能力（7 分）：** ①投标供应商具有有效期内的 ISO9001 质量管理体系认证证书且证书通过中国合格评定国家认可委员会（CNAS），得 1 分。 ②投标供应商具有有效期内的 ISO27001 信息安全管理体系认证证书且证书通过中国合格评定国家认可委员会(CNAS)认证，得 1 分。 ③投标供应商具有有效期内的 ISO20000 信息技术服务管理体系认证证书且证书通过中国合格评定国家认可委员会（CNAS）认证，得 2 分。 ④投标供应商具备中国网络安全审查技术与认证中心颁发的 CCRC 信息安全服务资质认证证书（信息安全风险评估、信息系统安全运维、信息安全应急处理），每提供一个得 1 分，共 3 分。 **注：提供证书复印件加盖投标单位公章，不提供不得分。**	7 分
	2、类似业绩（6 分）： 提供的2022年1月至今在国内所完成网络安全服务类的类似业绩合同，每提供 1 份的得 2 分，满分 6 分。 注：①合同日期以合同签订时间为准； ②须提供采购合同关键页（封面页、内容页、签字盖章页）复印件并加盖投标供应商公章。不提供或未按要求提供的均不得分。	6 分
	3、人员具备资质及能力：（21 分） ①针对本项目拟派 1 名团队负责人具有有效期内的项目管理专业人员能力（CSPM）或系统规划与管理师(高级)证书、注册信息安全高级管理人员证书（CISP-CISO）、注册数据安全治理专业人员证书（CISP-DSG）、IT 服务项目经理证书（ITSS）、数据安全官证书；提供证书复印件加盖投标单位公章，每提供一个证书得 1.5 分，最高得 7.5 分。 ②针对本项目拟派 1 名技术负责人具有有效期内的项目管理专业人员能力证书（CSPM）或信息系统项目管理师(高级)	21 分

	证书、注册信息安全管理人员证书（CISP）、信息安全保障人员证书（CCRC-CISAW）、IT 服务项目经理证书（ITSS）；提供证书复印件加盖投标单位公章，每提供一个证书得 1.5 分，最高得 6 分； ③拟派本项目的线上技术人员具有注册信息安全管理人员证书（CISP）、信息安全保障人员证书（CCRC-CISAW）；提供证书复印件加盖投标单位公章，每提供一个证书得 1.5 分，最高得 3 分；（人员及证书均不重复计分，多提供不算分） ④拟派本项目的线下技术人员具有深信服安全服务工程师（T2）认证证书、深信服安全资深工程师证书、注册信息安全管理人员证书（CISP）；提供证书复印件加盖投标单位公章，每提供一个证书得 1.5 分，最高得 4.5 分；（人员及证书均不重复计分，多提供不算分） 注：拟派的团队负责人、技术负责人、线上技术人员、线下技术人员不可为同一人，以上人员需提供 2025 年 1 月至今任意 3 个月的投标供应商为其缴纳的社保证明，并提供证书复印件加盖投标单位公章，未提供不得分。	
	4、技术参数响应（36 分）： 供应商完全满足采购文件“第二章　第一节采购清单及技术参数”得 36 分，非“▲”项每存在 1 项不满足的扣 2 分，带“▲”项每存在 1 项不满足的扣 4 分，扣完为止。（注：以技术部分响应表为评审标准，注明提供截图证明或需要材料证明而未提供的，视为负偏离；如一项参数含多项指标，该参数中只要有一项指标不满足，也视为负偏离。）	36 分
	5、原厂商授权书及售后服务承诺（5 分）： 本项目是针对学院现有网络安全设备软件和规则特征库升级服务，为保障学院现有网络安全设备稳定运行和网络安全防护策略的实时性和有效性，以及减少因设备操作不熟悉、策略配置错误，导致学院网络中断和业务系统无法访问等故障的发生，要求供应商提供网络安全设备原厂商出具的授权书	5 分

	和售后服务承诺函加盖厂商公章，未提供或提供不全不得分。	