目 录

一、 合同内容 2
二、 合同价格 2
三、 合同款项支付 2
四、 服务条件 3
五、 技术服务 3
六、 违约责任 3
七、 验收 3
八、 其他事项 3
九、附件一：合同服务清单 5
十、附件二：保密协议 17
十一、附件三：渗透测试授权委托书 19

陕西省教育考试院（以下简称甲方）2026年信息安全监测服务项目采购，由陕西开源招标有限公司组织采购，选定杭州安恒信息技术股份有限公司（以下简称乙方）为该项目成交供应商。依据《中华人民共和国民法典》和《中华人民共和国政府采购法》，经甲、乙双方协商，按下述条款和条件签署本合同。

一、合同内容

为保障甲方关键网络及信息系统安全、稳定、连续运行，持续迭代完善网络安全综合防护体系，建立常态化、规范化网络安全服务保障运行机制，甲方拟委托具备对应网络安全资质、专业技术服务能力的乙方承接2026年信息安全监测服务项目专项工作。

乙方应按照本合同及磋商文件约定，向甲方提供IT资产管理服务、资产暴露面检测服务、AI交互式渗透测试服务、综合漏洞评估服务、主机安全加固服务、安全托管运营服务、AI代码审计服务、驻场运维服务（网络安全）、重要时期安全保障服务、应急响应服务、应急演练服务、安全培训服务、安全咨询规划服务、AI数据分类分级服务、数据库审计租赁服务、安全设备租赁服务（专网）、“三高一弱”专项检查服务、API与应用梳理服务、压力测试服务、安全策略运营服务、脆弱性闭环服务等全部服务内容。

详细服务内容请见附件一：合同服务清单

二、合同价格

本合同总价款为人民币陆拾玖万壹仟元整（¥691,000.00）（含税），对应增值税税率为6%，乙方应按该税率开具合法有效增值税发票。

说明：

（一）合同总价包含完成本项目的所有费用。

（二）合同总价一次包死，不受市场价格变化影响，并作为结算的唯一依据。

三、合同款项支付

（一）结算单位：甲方结算，乙方须在甲方付款前提供全额发票。

（二）付款方式：

（1）合同生效后30日内，甲方向乙方支付合同总金额的40.00%，即人民

币大写：贰拾柒万陆仟肆佰元整（¥276,400.00）。

（2）服务期结束并验收合格后30日内，甲方向乙方支付合同总金额的60.00%，即人民币大写：肆拾壹万肆仟陆佰元整（¥414,600.00）。

四、服务条件

（一）项目实施地点：甲方指定地点。

（二）服务期限：即2026年12月11日至2027年12月10日。

五、技术服务

（一）技术资料：按项目详细实施内容要求交付相关技术资料，见附件一。

（二）人员培训：免费为使用单位培训操作人员，使其能达到操作要求。

（三）服务承诺：乙方承诺严格按照磋商文件及响应文件要求实施服务，详见响应文件项目服务承诺函。

六、违约责任

（一）按照《中华人民共和国民法典》中的相关条款执行。

（二）未按合同要求提供产品，或设备质量不能满足技术要求，甲方有权终止合同，甚至对乙方违约行为进行追究。

（三）如有纠纷，双方应友好协商解决；协商不成时可向甲方所在地人民法院提起诉讼。诉讼费用（诉讼费、鉴定费、律师费、差旅费）由败诉方承担。

七、验收

项目达到使用条件时，由甲方负责组织验收，或者邀请有关专家、质检机构、采购代理机构共同进行验收。验收合格须交接项目实施的全部资料，并填写政府采购项目验收报告单。验收须以合同、磋商文件、响应文件、澄清内容以及国家相应的标准、规范等为依据。

八、其他事项

（一）陕西省教育考试院在合同的履行期间以及履行期后，可以随时检查项目的执行情况，对采购标准、采购内容进行调查核实，并对发现的问题进行处理。

（二）本合同一式六份，甲方陕西省教育考试院四份，乙方杭州安恒信息技

术股份有限公司一份，采购代理机构一份，甲乙双方签字盖章后生效。

（三）磋商文件、响应文件也是合同的组成部分，合同中未约定的以磋商文件、响应文件为准。

（四）本合同所有附件均为本合同不可分割的一部分，其内容与本合同正文具有同等约束力。

合同签订地点：陕西省西安市

合同签订时间：2026 年　月　　日

甲　　方： 单位名称：陕西省教育考试院 地址：陕西省西安市含光北路 40 号 法人代表： 联系电话： 开 户 行： 账　号：	**乙　　方：** 单位名称： 杭州安恒信息技术股份有限公司 地址：浙江省杭州市滨江区西兴街道 联慧街 188 号 法人代表：张小孟 联系电话：0571-28860999 开户行： 杭州银行股份有限公司科技支行 账号：77818100000385

九、附件一：合同服务清单

序号	服务名称	服务范围	数量
1	IT资产管理服务	1.对考试院所有业务资产包括物理主机、虚拟机、业务端口等，开展细致全面的资产梳理工作。基于考试院现有资产探测工具如态势感知平台、数据库审计设备、EDR终端防护系统及现有资产台账，开展全量业务资产梳理工作，形成准确、完整、可持续更新的资产台账，资产梳理频率服务期内每季度提供1次。 2.对考试院物理主机、虚拟机、服务器、PC终端、业务端口、Web业务系统、数据库实例、重点业务IP等资产进行识别、核查和分类管理。资产识别方式应包括但不限于流量被动识别、主动探测、数据库审计被动发现、EDR终端发现、人工核查和台账比对等方式，发现Web业务资产、数据库资产，以及终端及服务器资产，同时在现有识别成果基础上，进一步梳理内网存活IP、离线资产、开放端口、服务类型、资产指纹、责任人、所属区域、重要程度等信息，对核心业务系统、DNS服务器、数据库服务器、考试报名、成绩查询、志愿填报、缴费等关键业务相关资产进行重要性标识，形成重点资产标签，例如“DNS服务器－重要”“核心业务系统－重要”等，支撑后续安全监测、告警研判、漏洞整改、应急响应和重要时期安全保障工作。 3.乙方提供数据安全资产梳理服务，通过技术扫描与人工核查相结合的方式，全面发现、识别并梳理考试院信息系统中的各类数据资产，包括但不限于：各类库表数据资产、数据接口资产、业务应用数据、备份数据资产等，清晰反映资产的名称、类型及责任人等关键信息。 4.服务实施完成后，输出《资产统计清单》《数据安全资产清单》，资产清单包括资产名称、IP、用途、责任人等信息。清单包括资产名称、IP、用途、责任人等信息，协助考试院进行资产台账登记，并录入现网已有态势感知平台。	1项
2	资产暴露面检测服务	1.对考试院暴露在互联网上的资产进行测绘，包括但不限于域名、端口、IP等资产，对发现的高危风险资产进行关停或协助整改，减少资产在互联网上的暴露风险，降低被黑客攻破的可能。服务期内开展2次资产暴露面检测服务，每次提供25个互联网系统资产暴露面检测。 2.对考试院互联网资产（互联网域名、端口、IP等资产）开展暴露面检测，评估互联网资产的安全暴露风险，基于检测结果协助处置高危风险资产，减少互联网资产风险隐患。 3.乙方在确保不影响业务稳定性的情况下开展检测工作，对所	1项

		有互联网资产进行检测，提供所有互联网资产的测绘结果数据，人工对检测结果进行分析，针对高危资产提供安全建议。 4. 乙方完成检测服务工作后，输出《互联网暴露面检测报告》和《互联网资产清单》，暴露面检测报告包括检测到的高危资产列表及详情、安全建议等，互联网资产清单包括资产URL、IP地址、资产名称、开放端口、返回标题等信息。 5. 乙方提供资产暴露面检测工具，针对暴露资产的攻击面分析结果支持通过风险标签分类，风险类型包括高危端口开放、高危指纹、疑似敏感应用等。	
3	AI交互式渗透测试服务	1.乙方提供交互式的AI渗透测试服务，对考试院的重要业务进行测试，通过AI自动研判与任务规划，尽可能多地发现测试对象的各类安全风险、漏洞问题，并提供相应的修复建议，在整改修复后，完成复测。服务期内提供30个系统的测试服务。 2.乙方在得到考试院授权的前提下，通过AI渗透测试工具对存量重要系统、业务变更、新上线业务及重大业务前进行测试，基于AI大模型技术模拟真实的安全攻击，发现黑客入侵信息系统的潜在可能途径，挖掘测试目标存在的安全隐患、漏洞，查找系统存在的安全隐患点，并验证每个安全隐患点的可利用程度。根据测试结果输出渗透测试报告，对每个安全风险进行详细描述，并给出相关的安全建议。 3.乙方在修复安全风险问题后，完成风险复测验证，AI渗透测试支持POC包回放进行一键复测，并快速生成复测报告，确保渗透的安全风险问题完全修复，完成渗透测试工作后5个工作日内输出《渗透测试报告》。 4.乙方服务工具具备AI推理能力，对业务系统通过AI推理分析渗透测试步骤并拆解成多个任务。 5.乙方服务工具在测试任务过程中可以结合AI推理能力并融合MCP协议，支持通过MCP协议调用20多种渗透测试工具。	1项
4	综合漏洞评估服务	1. 乙方提供漏洞评估服务，对考试院的所有资产或用户指定资产开展漏洞扫描工作，并出具相应的扫描报告，对甲方有疑问的漏洞进行答疑解惑，并提供针对性的漏洞修复建议，对发现的高危漏洞风险进行闭环跟踪，在业务人员修复漏洞后进行漏洞复测，并留存相应的复测记录。 2. 乙方在服务期内完成12次全量资产的漏洞扫描工作，以及按考试院需求提供不限次、不定期针对指定资产、组件等提供专项漏洞扫描，每次扫描结束后输出相应的《漏洞扫描报告》，并记录复测结果。 3. 乙方服务工具具备主机扫描、网站扫描、数据库扫描、基线	1项

		配置、事件内容、协同扫描、弱口令扫描、存活主机探测、大数据漏洞扫描、物联网漏洞扫描、信创漏洞扫描、无感扫描等任务类型。 4.乙方服务工具模拟勒索攻击路径，评测考试院网络环境对勒索风险的防护能力，提供babuk、BlackBasta、BlackCat、conti、crylock、mallox等流行勒索家族攻击检测，涵盖ATT&CK中初始化访问、执行、持久化、权限提升、防御规避、信息搜集、发现、横向移动、命令控制等方向技术。	
5	主机安全加固服务	1.乙方提供主机病毒查杀、网马查杀、补丁管理、微隔离、主动防御功能，包括已知和未知类型勒索病毒检测查杀，挖矿防御查杀，高级威胁防御，渗透攻击防护，系统登录防护，防暴力破解，进程防御，WEB应用防护，文件访问监控等功能。提供200台服务器（包括虚拟主机）、200个PC终端的防护能力。 2.乙方提供未知勒索病毒的诱饵防护引擎，通过自动生成的高仿真文件诱捕未知勒索病毒的攻击，并进行实时阻断。 3.乙方服务工具通过实时监控能力，可以发现各主机进程内存中是否被注入后门，包括内存马风险说明、内存马类名、内存马路径、堆栈轨迹、攻击技战术、处理建议，可以有效检测无文件攻击的事件。 4.乙方每季度输出《主机安全防护服务报告》，在服务期内提供4份，并对当季度的安全防护服务情况进行汇总分析。 5.乙方服务工具具备暴力破解防护功能，支持开启AI值守监测模式，持续学习业务特征，识别行为偏差及非法登录特征，阻断爆破行为。	1项
6	安全托管运营服务	1.乙方提供全年7×24小时安全托管运营服务，基于现场已有的态势感知平台对考试院相关安全风险、威胁等进行远程实时监测和安全运营，服务内容包括：威胁监测与分析、威胁处置、应急响应、安全有效性调优、安全汇报等，安全运营重要资产数100个。 2.乙方面向考试院的云网基础设施、业务系统提供远程安全监测分析能力，对发现的安全风险进行专业人工分析、验证后，在考试院指定的内部工作群发布安全风险提醒，由安全驻场人员辅助进行风险处置，对每个风险需完成风险提醒、处置、反馈、验证归档的闭环管理，在处置完成后，进行风险复测验证，确保风险修复闭环，对因客观原因无法处置的，应尽可能采取措施降低风险，并进行记录归档。 3.服务人员每月输出《安全托管运营服务报告》，服务期内提供12份，并对当月的安全运营分析情况进行汇总分析。 4.乙方服务期间每发生一次安全事件，经确认属于服务未通知或不到位的，扣除本项服务费用的5%。	1项

		5.乙方提供的服务工具具备AI数字专家，能够辅助运营人员对安全事件进行分析，分析环节包括数据基本信息查询、事件顶级标准查询、客户运营备注获取、攻击者分析、资产历史事件查询、受害者分析、事件综合研判等。	
7	AI代码审计服务	1.乙方提供AI代码审计服务，对重要业务的程序源代码逐条进行检查、分析，发现其中的错误信息、安全隐患和规范性缺陷问题，以及由这些问题引发的安全漏洞，提供代码优化建议。服务期内提供1次代码审计服务，审计工作量100万行代码。 2.乙方提供基于AI的审计需求理解能力，通过自然语言描述审计目标与范围，能够自动解析代码压缩包，识别项目语言类型、代码结构及相关特征信息，并结合审计场景智能推荐或自动生成审计策略。 3.审计服务能够从可靠性、可维护性、覆盖率、重复度、大小、复杂度、问题、安全等方面量化源代码的详细质量情况，评估源代码的质量情况。 4.乙方完成审计工作后10个工作日内输出《代码审计报告》，审计报告包括文件数量、代码数量、开发语言、缺陷类型、缺陷风险级别、缺陷数量等信息。 5.乙方服务工具提供对源代码AI漏洞降噪和AI研判能力，研判白盒漏洞是否为误报，结合历史漏洞数据特征、上下文环境信息，对每个漏洞自动生成置信度评分、成因分析、修复方案等。	1项
8	驻场运维服务（网络安全）	1.服务期内为考试院提供全年1人5×8小时驻场安全运维保障服务。网络安全驻场技术人员负责现场既有安全设备、业务系统、安全平台及本项目配套服务工具的全生命周期日常运维管理，包括但不限于设备启停、参数配置、日常操作、故障排查与应急处置等核心工作，确保各类安全基础设施及相关系统稳定、合规、高效运行；同时承担现场安全态势分析、安全事件响应、应急处置及其他协作等专项工作。 2.网络安全驻场技术人员协助考试院处理各类现场网络安全相关事务性工作，在重大活动网络安全保障、攻防演练等关键节点，全程现场配合开展业务系统安全防护部署、实时监测、异常处置等工作，保障核心业务系统在关键时期的网络安全。 3.网络安全驻场技术人员负责对考试院现场既有安全设备、业务系统、安全平台及本项目服务工具实施规范化管理与常态化维护，严格按照运维标准，每月完成全量定期巡检，及时发现并闭环处理设备运行异常、配置偏差等问题；每周完成安全特征库版本更新升级，确保安全防护能力同步提升，并结合考试院实际网络安全需求，动态调整、优化安全策略，提升防护精准度与有效性。	1项

		2. 乙方协助考试院组建专项应急响应小组，明确小组人员职责、分工及联络方式，协助建立健全应急上报流程、分级响应机制及多方联络机制，规范应急事件处置流程，确保突发安全事件发生时，能够快速启动对应等级应急流程，及时联络相关责任人员、协同推进处置工作，保障应急响应高效有序。 3. 乙方在接到应急需求通知后，承诺 1 小时内抵达考试院指定现场开展应急响应工作，服务内容包括快速控制事件范围，全面开展事件取证，事件处置消除隐患，攻击溯源定位攻击来源、攻击路径及攻击手段等，协助考试院完成核心业务、关键数据的恢复工作，保障业务快速回归正常运转。 4. 应急响应处置工作完成后，开展事件回溯复盘工作，全面调查事件发生的根本原因，结合应急处置全过程的台账、数据及痕迹信息，对安全事件的发生原因、传播路径、影响范围及处置效果进行专业、全面的分析，精准完成攻击溯源追踪，梳理事件处置过程中的不足，提出针对性的优化建议及防范措施，避免同类安全事件再次发生。 5. 应急响应服务完成后，在 3 个工作日内，结合应急处置过程、调查分析结果及优化建议，编制并提交《应急响应报告》，报告内容完整、详实，涵盖事件概况、处置过程、原因分析、溯源结果、恢复情况及后续防范措施等核心内容，为考试院后续安全管理工作提供参考依据。	
11	应急演练服务	1. 乙方服务团队结合考试院业务特性，提供定制化应急演练服务，聚焦业务突发情况处置，提升技术人员、管理人员及相关岗位人员的协同配合能力、应急响应速度和突发安全事件处置水平，服务期内提供 1 次应急演练服务。 2. 乙方联合考试院相关负责人，成立应急演练专项工作小组，明确小组架构及各成员职责；结合考试院实际业务系统，模拟各类高频、高风险业务突发安全事件场景，包括但不限于系统宕机、数据泄露、网络中断、异常访问攻击、考试流程异常等，确保演练场景的真实性和针对性。 3. 应急演练工作包括制定演练计划、演练方案设计、演练动员与培训、应急演练实施、应急演练评估与总结等。 4. 开展实战化演练，强化各岗位人员在事件识别、信息上报、协同处置、流程衔接等环节的操作规范性，确保相关人员熟练掌握应急处置流程、职责分工及操作要点，提升应急处置实战能力。 5. 在演练服务开始前，乙方结合考试院需求及实际场景，编制并提交《应急演练实施方案》，明确演练目标、演练环境、资源配置、参与人员、演练流程、场景细节、动作规范及注意事项，经考	1 项

		4. 乙方服务人员定期推送漏洞威胁情报及针对性防护建议，结合网络安全态势变化，及时提供精准化威胁情报预警服务；针对业务系统安全加固工作，同步配合业务应用部门开展安全加固技术指导、漏洞复测等工作，确保加固效果达标，降低安全风险。 5. 服务人员严格按照项目管理规范及进度要求，完成各类服务文档的整理、审核、归档工作，确保文档的完整性、规范性与可追溯性，支撑项目全流程管控；完成考试院交办的其他各类网络安全相关事务性、辅助性工作，主动配合考试院落实各项网络安全管理要求。 6. 驻场运维服务成果需满足规范化、可追溯要求，包括《运维巡检报告》《项目驻场周报/月报》《安全情报资讯》《故障处置报告》《安全策略调整记录》等相关成果资料。	
9	重要时期安全保障服务	1. 乙方组建5人的专项重保团队，团队成员具备丰富的重大活动安全保障经验，熟悉教育考试系统架构及安全防护要点。重保范围覆盖两会、春节、国庆等重大节假日及各类招生考试、资格考试等关键时期，服务期时长为五周。 2. 在重保活动启动前，开展全面的安全风险摸排工作，对考试院网络设备、服务器、业务系统、数据库等核心资产进行全面梳理，精准识别潜在安全风险、漏洞及威胁隐患，建立完整的风险排查台账，明确风险等级、影响范围及整改建议；对摸排出的所有风险问题实行闭环管理，全程跟进整改进度，确保整改到位、隐患清零。 3. 在重保期间实行7×24小时全天候值守，专项重保团队现场驻场值守，开展实时安全监测、风险分析研判、应急处置等工作。依托安全监测工具与人工巡查相结合的方式，实时监测网络流量、系统运行状态及安全告警信息，及时发现异常情况并快速分析研判，最大限度降低事件影响。同时，乙方组建专业后端技术支撑团队，为现场值守人员提供全方位技术支持，协助处置复杂安全风险、疑难技术问题，保障考试院网络与业务系统持续稳定运行。 4. 在重保活动结束后7个工作日内，乙方编制并提交《重要活动保障服务总结报告》，报告内容详实、数据准确、重点突出，全面涵盖重保值守情况、风险排查及整改闭环情况、安全事件处置详情、保障工作成效、存在的问题及优化建议等内容，为考试院后续安全防护工作提供参考依据。	1项
10	应急响应服务	1. 乙方在服务期内提供不限次数的应急响应服务，对已发生的重大网络安全、数据安全等突发安全事件，全面开展事中处置、事后溯源复盘及加固优化工作，涵盖事件取证、原因分析、攻击溯源、系统恢复、安全加固等核心环节，降低事件对考试院业务正常开展的影响。	1项

		试院确认后启动演练。 6. 乙方在演练服务结束后，2个工作日内输出《应急演练总结报告》，全面梳理演练开展情况、各环节处置成效，重点分析演练过程中暴露出的流程漏洞、人员操作不足、资源配置短板等问题，同步提出可落地、可执行的优化改进建议，协助考试院完善应急预案、优化应急处置流程。	
12	安全培训服务	1. 提供安全培训服务，为考试院信息化相关技术、管理、运维人员进行集中培训，通过培训使参训人员全面深度掌握国家网络安全相关的法律法规、制度、标准和相关行业要求，了解网络安全细分领域相关情况，掌握应急及安全防范技术措施等。服务期内提供2次培训服务，由外部高级工程师/教授级别以上的安全专家提供培训。 2. 乙方定制贴合考试院工作实际、针对性强的专属培训课程，完成培训讲义、PPT课件、案例素材、实操手册等相关资料的编制与审核，培训师资可根据考试院实际需求及培训主题进行匹配确认，确保师资专业方向与培训内容高度契合。 3. 乙方提供的培训服务，可选的课程内容包括但不限于安全意识、安全政策及法律法规、安全基础常识、安全风险应对、安全处置响应、安全运维、安全加固、安全产品使用、认证培训等方面。 4. 乙方提供网络安全相关认证培训服务，提供5人的认证培训服务，认证类型包括：注册信息安全专业人员认证（CISP）、网络安全能力认证（CCSC）、信息安全保障人员认证（CISAW）、首席数据官认证（CCRC-CDO）、人工智能安全官（CCRC-AISO）等，考试院业务人员可根据业务需求选择培训方向。 5. 乙方在培训完成后输出培训相关归档资料，输出《培训签到表》《培训质量反馈表》，同时根据需求提供培训照片、培训视频、学员考核成绩等资料。	1项
13	安全咨询规划服务	1. 乙方结合考试院实际工作场景，提供数据安全咨询服务、网络安全咨询服务、安全运营咨询等服务，提供相关安全管理制度、标准规范的撰写等服务，服务期内为考试院提供不限次数的专业安全咨询规划服务。 2. 对考试院安全管理现状进行全面、深入的调研排查与细致分析，通过对考试院当前安全管理痛点、难点及实际需求分析，结合长远安全发展规划，构建贴合实际、覆盖全面的安全制度标准体系，制度体系需涵盖网络安全运维管理、安全运行实时监测、日志集中分析与安全审计、安全风险监测与预警响应等核心领域，为考试院安全管理工作提供规范指引。 3. 对考试院日常安全管理工作中遇到的各类实际问题，结合当	1项

		前网络安全发展趋势、国家及行业相关法律法规、标准规范要求，从安全技术应用、安全管理流程、风险防控措施等多维度，为考试院提供不限次数、专业精准的安全分析、技术指导及咨询建议。 4.结合考试院实际业务需求进行网络与信息安全蓝图设计，包括管理体系框架设计，运营体系框架设计、技术体系框架设计，网络与信息安全差距分析及提升举措等内容。 5.乙方服务输出物，结合咨询过程及制度优化成果，输出相应的《咨询建议》《设计方案》等文档，同步输出修订完善后、可直接落地执行的《安全管理制度规范》汇编。	
14	AI数据分类分级服务	1.乙方服务期内提供AI分类分级工具，基于行业分类分级标准、框架和AI大模型，对考试院指定的数据资源进行调研、梳理、分类分级和安全评估，提升考试院数据分级管理能力，保障数据安全，严格防范数据泄露、篡改、丢失等安全风险。服务期内完成1个指定数据资产的AI分类分级工作，完成3W数据字段的分类分级工作，提供数据分类分级所需的系统软件，分类分级处理性能100字段/秒。 2.服务工具具备大模型能力，提升分类识别率与准确率，支持以自然语言方式输入专家经验，以对大模型的识别效果进行调优，并支持对专家经验效果进行验证。 3.分类分级工具具备有监督学习模型的训练，模型算法包括传统集成学习、快速神经网络、深度神经网络、AI大模型等类型。 4.乙方服务完成后输出《考试院数据资源清单》《考试院分类分级结果报告》。 5.服务工具提供AI大模型，自动生成数据分类分级框架，支持对行业、最大类别层级、最高级别、提示词、数据源进行配置。同时支持在生成分类分级框架后对部分节点进行自动化优化，包括：生成类别、生成级别、生成示例、拆分类别。	1项
15	数据库审计设备租赁服务	1.乙方提供数据库审计硬件设备租赁服务，对考试院现网数据库进行审计，针对采集发现的数据访问行为、数据风险行为等提供安全预警。所提供的数据库安全审计分析设备符合采集区域的数据流量需求，支持70个数据库实例审计，可审计数据库流量1Gbps，双向审计数据库流量300Mbps，数据存储空间2TB。 2.服务工具支持云环境、物理网络环境下的数据库流量检测能力，支持主流关系型、非关系型、国产、大数据等数据库的审计，支持本地数据库工具登录数据库场景下的数据操作行为审计。 3.服务工具支持审计记录中敏感数据的脱敏处理，提供敏感数据脱敏规则，并支持脱敏规则自定义；安全审计规则提供SQL注入、账号安全、数据泄漏和违规操作等。	1项

		4.服务工具支持基于日期、时间、报文、审计ID、会话ID、SQL模板ID、资产、数据库账号、客户端IP、服务端IP、客户端端口、服务端端口、客户端MAC、服务端MAC、数据库名/实例名、数据库对象（库、表、字段等）、客户端工具、主机名、操作系统用户名、影响行数、执行时长、执行结果描述、返回结果集、关联IP、关联账号、操作类型、数据库类型、执行状态等条件的审计查询。 5.乙方服务期内每季度输出《数据库安全审计分析服务报告》，服务期内提供4份，并对当季度的数据访问和数据库风险情况进行汇总分析。 6.服务工具支持在审计日志中一键添加过滤规则，支持在告警规则中一键添加信任规则或规则白名单。	
16	安全设备租赁 服务（专网）	1.乙方提供专网安全设备租赁服务，面向考试院专网提供符合要求的运维安全审计设备租赁服务、日志审计设备租赁服务、入侵监测设备租赁服务等，提供1年期设备租赁服务。 2.提供的运维安全审计设备在服务期内可运维资产数100个；日志审计设备在服务期内可采集日志源资产80个，日志采集能力5000EPS；入侵监测设备可采集应用层流量能力1Gbps。 3.提供的运维安全审计具备身份认证、账户管理、控制权限、运维审计等功能，支持多种字符终端协议、文件传输协议、图形终端协议、远程应用协议的安全监控与历史查询，提供专网运维安全管理能力，方便事前管控、事中监控和事后溯源。 4.提供的服务工具具备对重要命令进行审核，运维人员执行命令后，等到管理员审批通过后才可执行成功；支持动态对象授权，提供基于属性策略的动态授权能力；支持主机命令控制，数据库命令控制；支持对运维操作会话的在线监控、实时阻断。 5.提供的日志审计工具，日志转发与存储支持数字签名与加密，数字签名支持SM3和SHA256，加密模式支持AES和SM4，日志接收支持解密，支持SSL加密模式访问。 6.提供的日志审计工具，提供5000多个解析规则，可以对多源异构的设备类型日志进行解析（标准化、归一化），解析维度多达200多种，解析规则可以根据考试院要求定制扩展；对日志样例可进行划词辅助解析，一键生成正则表达式；支持基于跨设备的多事件关联分析，支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件。 7.提供的日志审计服务工具具备安全评估模型，评估模型基于设备故障、认证登录、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数，安全评估模型可以显示总体评分、历史评	1项

		分趋势，安全评估模型各项指标可钻取具体的评分扣分事件。 8.提供的入侵检测工具，支持HTTPS、SMTPS、POP3S、IMAPS协议解析，无需提供私钥证书，通过在服务器部署Agent，以密钥截取及代理流量转发解析TLS1.3协议、DH密钥算法的加密流量；支持一键切换运营模式和专业模式，满足不同场景的研判需求，如日常安全监测预警和重保时期专项监测；场景分析提供攻击者视角分析、受害者视角分析、脆弱性分析、挖矿场景分析、勒索场景分析、主机威胁分析、失陷主机分析、情报事件分析、域名行为分析、钓鱼邮件分析、加密流量专项分析、加密隧道分析、文件威胁分析、沙箱报告分析、敏感信息分析和情报在线分析等；对产生的告警事件提供7*24小时在线分析研判服务。 9.提供的租赁设备具有AI引擎挖掘真实事件能力，具备99%高精度事件聚合能力，有助于提高考试院威胁事件处置效率。	
17	“三高一弱”专项检查服务	1.乙方针对考试院“三高一弱”规则和问题清单，开展常态化高危漏洞、高危端口、高危行为、弱口令风险隐患排查整治，内容包括但不限于：主机、web应用、中间件、应用组件、数据库、操作系统、网络及安全设备等各信息系统，并提供加固意见和修复建议，服务期内每季度提供1次“三高一弱”检查服务。 2.提供高危端口检查服务：对考试院网络内部开放端口情况进行检查，研判分析端口及承载的服务是否存在高危风险，识别脆弱性与威胁较高的接口及设备，并提供加固意见和修复建议，防范此类设备被恶意控制成为攻击载体引发安全风险事件。 3.提供高危行为检查服务：对考试院可能存在的违规接入与外联行为、高危攻击行为、高危（可疑）样本等进行检测，通过技术手段有效识别非授权设备接入、高危攻击风险行为等，并提供加固意见和修复建议，防范网络资源违规使用、遭受攻击或破坏、数据泄露及非法入侵等风险。 4.提供高危漏洞检查服务：对考试院业务系统、操作系统、数据库、中间件等支撑组件进行漏洞扫描和验证，识别当前存在的各种漏洞，对高危漏洞提供加固意见和修复建议，提升业务及支撑系统的安全性。 5.提供弱口令检查服务：检查考试院在应用用户登录、访问鉴权、系统后台、数据库、服务接口等方面存在的弱口令，大幅降低弱口令造成的安全风险。 6.服务实施完成后输出《“三高一弱”风险隐患排查报告》。	1项
18	API与应用梳理服务	1.乙方提供服务工具，通过服务工具识别梳理考试院API以及业务系统，检测API接口存在的脆弱性，对各种违规使用数据行为进行监控告警，防止发生敏感数据因API自身脆弱性造成的数据泄	1项

		漏事件发生，服务期内提供2次API与应用梳理服务，每次服务周期一个月。 2.提供的服务工具通过流量解析技术还原API操作日志，识别、提取API日志中的敏感数据和操作账号，关联账号身份和组织架构信息，追踪敏感数据的来源和去向，以及与敏感数据相关的用户和组织，识别潜在的安全威胁。 3.提供的服务工具基于已经还原的API日志进行分析和梳理，全面掌握API暴露面，实时监控API上线、活跃、失活等活动，助力考试院进行API资产管理和规划，及时发现API资产的利用率低下、已弃用API未及时下线、暴露面过大等风险问题，进一步优化API资产的管理和利用。 4.提供的服务工具提供API安全风险统计分析服务，持续、实时、全面地评估业务系统API是否存在脆弱性风险，覆盖OWASP API Security TOP 10问题，包括但不限于鉴权认证类风险、数据暴露风险、数据脱敏风险等，脆弱性风险策略包括：接口未鉴权、接口伪脱敏、敏感接口参数可遍历、源代码泄露等。 产品内置丰富的风险详情，包含：风险基本信息、历史记录、API影响面评估、可被利用方式、修复建议等。 5.提供的服务工具提供以IP、账号、IP+API、账号+API、数据等维度进行行为监测，实时预警短时间内大量获取敏感数据、访问频次异常、异常时间获取敏感数据、数据违规出境、违规跨域访问等异常调用API行为。针对高敏感API进行重点监测，自动绘制API风险链路关系，研判可疑的数据泄露路径。 6.乙方单次服务完成后，3个工作日内输出《应用综合分析报表》《API数据安全运营报表》《API资产综合分析报表》《API数据资产治理专项报表》以及特定场景下的安全评估报表等。 7.提供的服务工具对于数据维度的风险，提供丰富的审计详情信息和分析维度，可根据风险日志自动绘制API风险链路关系；当监测到流量中有风险行为时自动预警，历史风险日志自动合并，提高运营效率，同一主体触发相同的风险会自动累计风险触发次数和数据量。	
19	压力测试服务	1.乙方对考试院业务系统，包含但不限于Web端、移动端（APP/小程序）及后台接口层等提供1次压力测试服务。 2.提供峰值并发场景测试服务：能模拟高考报名截止前24小时（并发用户10万）、成绩查询首日（每秒查询请求9000次）的高负载场景压力测试。 3.提供数据量压力场景测试服务：能模拟考生数据量50万条、历史成绩数据200万条时的系统响应能力压力测试。	1项

		4.提供混合业务场景压力测试服务：能同时模拟报名、审核、缴费、查询等多业务并发操作压力测试（业务比例按考试院历史数据配置）。 5.服务期内提供相关详细测试方案、详细测试用例（覆盖关键、复杂业务场景，避免简单页面压测）、压力测试报告（含测试数据、性能瓶颈分析、优化建议等）。 6.服务商具备有效的CMA和CNAS资质，具有中国网络安全审查认证和市场监管大数据中心（CCRC）颁发的《信息安全风险评估》服务资质。	
20	安全策略运营服务	1.乙方提供对平台及安全设备的策略运营服务，包含不同时期（日常、重保等）安全管理、数据汇总分析、用户需求等的策略确认、调整优化，对主机策略检查、调优，视情况调整监测细粒度、强度等策略；对平台视情况调整分析强度、颗粒度、预警等级、覆盖对象等。根据服务成果，整合现有数据，对主机与平台进行优化，与运营服务内容、成果深度融合。 2.服务期内建立策略调整动态台账，服务实施完成后最终形成一份统一、准确的《安全策略报告》，包含策略运营概述、策略分析情况、策略优化设计、优化结果等。	1项
21	脆弱性闭环服务	1.乙方对考试院相关安全设备及服务资产的脆弱性进行按需采集，并提供专业的管理分析服务。采集范围依据脆弱性的分类主要包括应用脆弱性、系统脆弱性、配置脆弱性、物理脆弱性、管理脆弱性等。脆弱性的采集主要可以通过漏洞扫描、三高一弱检查、调研访谈、监测发现等方式进行，可基于其他服务结果评估后得出。 2.服务内容包括但不限于：和考试院进行沟通确认，明确监测的资产范围，采集考试院专项分析需求后，服务人员进场开展监测工作，利用现有平台及工具对网内的脆弱性风险进行实时监测；实时对监测到的脆弱性风险进行验证，对确定的安全风险录入脆弱性风险记录单，经审核同意后提醒进行处置；对处置完成的脆弱性风险进行二次验证，确保风险完成修复，完成风险闭环，按照要求定期完成报告汇总。 3.服务期内建立《脆弱性风险记录清单》，包含风险资产名称、风险资产IP、风险时间、风险资产归属、风险等级、风险类型、风险处置状态、风险闭环状态等内容，后续内容可根据考试院要求进行调整。 4.服务实施完成后最终形成《脆弱性采集及闭环管理服务漏洞总结报告》，包含全年统计的脆弱性风险分布、数量统计、风险处置比例、风险资产TOP等内容全年服务汇总报告，年终对全年的脆弱性风险监测处置情况统计汇总后输出报告。	1项

十、附件二：保密协议

保密协议

甲方：陕西省教育考试院

乙方：杭州安恒信息技术股份有限公司

为了保护甲乙双方在 2026 年信息安全监测服务项目中涉及的专有信息不受侵害，经友好协商，甲乙双方在提供相关资料时，均应遵守《中华人民共和国保守国家秘密法》及以下条款的规定开展工作：

第一条：保密信息

本协议中所指的保密信息包括任何一方在项目实施时向另一方提供的任何技术上、商业上或贸易上具有经济价值的、以书面、口头或任何其他方式提供给另一方的所有非公开资料。

第二条：保密处理方法

在本项目执行过程中，任何一方在未获另一方书面同意的条件下，不得将从任何一方获得的保密信息泄露给第三方。任何一方不得将保密信息用于与本项目无关的任何方面。获得信息的任何一方只能在一定范围之内仅向有必要知道保密信息的本方雇员透露，并且仅透露相关的必要的内容。

第三条：被迫公开

如果一方由于法律要求被迫公开保密信息，则应及时通知另一方，使另一方能与作出法定强制行为的机构进行协商处理。

第四条：协商内容

除法律要求或得到另一方书面许可外，任何一方的讨论或谈判均应在双方之间进行，任何一方不得向任何个人或团体透露双方讨论、协商的任何内容，以及条件和条款中涉及保密要求的内容。

第五条：条款期限和终止

本协议中关于保密义务是永久性的，除非上述保密信息已成为公知信息。

第六条：更改

本协议在双方未书面签字的情况下不得修改或调整。本协议由双方共同执行，文件由双方共同制订，对双方均具有约束力。

第七条：违约识别与责任承担

任何一方泄露另一方保密信息，无论是故意或过失，均应承担赔偿责任。

任何一方泄密保密信息，导致被披露方遭受经济或商业损失，被披露方有权要求泄露方承担因披露秘密信息造成的一切直接、间接损失、费用（包括律师费）及其他支出。

任何一方不得因另一方的违约或侵权行为而泄露另一方的保密信息。

第八条：管辖

此协议的管辖和解释必须与中华人民共和国法律相一致。在此下面的任何争执、辩论、宣称或协议相关内容的解释、强制执行和适当性，如果在双方协议中无法得到解决，必须呈递被侵权方所在地法院提起诉讼。该法院或最高人民法院的最终裁定结果是不可变更的，对双方和全世界其他法院具有约束力。

甲方：陕西省教育考试院

签字：

盖章：

日期：_____年_____月_____日

乙方：杭州安恒信息技术股份有限公司

签字：

盖章：

日期：_____年_____月_____日

十一、附件三：渗透测试授权委托书

渗透测试授权委托书

授 权 方：陕西省教育考试院

被授权方：杭州安恒信息技术股份有限公司

一、授权相关说明

兹甲方与乙方协商，为确保与最终授权方需求中的安全测试工作能顺利进行，规避相关安全测试造成的安全风险，甲方对乙方进行以下使用授权：

1. 甲方向乙方提供需要安全测试必要的相关信息，并保证相关测试范围均具有管辖权。如果因给出范围非管辖范围导致的技术、民事、法律、行政、安全责任由甲方承担。

2. 乙方仅对甲方提供的安全测试对象清单进行安全测试，只做截图采证，不进行恶意数据篡改（甲方有特殊需求除外）；

3. 乙方有义务对相关测试信息、测试结果进行必要的保密，除非是为与甲方人员或授权代表商谈、讨论和协商之需，或在本协议签署后经甲方书面授权的任何目的。保密信息包括但不限于：测试所需信息、发现的安全问题、安全测试报告。

4. 乙方不应为除本协议规定目的以外的自身利益或任何其他方的利益而使用任何甲方的保密信息。

5. 测试过程会触发相关安全告警及日志记录，甲方需做好必要的分析及排除处理；如因此产生的不必要误解或法律责任，甲方有义务为乙方做免责辩护；

6. 监管单位对下属单位等开展测试工作，请做好事前告知。如因未事前告知所造成的服务不可用、系统故障、数据损失等，责任由授权的单位或授权人承担。

7. 为保障测试的效率和效果，建议对测试来源 IP 开放防火墙、Web 应用防火墙、IPS 等安全防护设备白名单，测试完成后请及时清除相关白名单；

8. 此授权经甲方盖章后生效。

二、测试相关说明

1. 乙方安全测试人员将采用业内统一的专业测试步骤，即信息收集（包括但不限于端口扫描、应用扫描、主机扫描）、人工测试及验证漏洞、获取权限、提升权限等步骤（具体步骤及方法视测试对象而定）。

2. 乙方将于甲方业务低峰期对测试对象使用乙方自主研发的明鉴系列扫描器及其他世界知名扫描器（明确使用了其他什么扫描器）进行复合扫描。扫描可能造成乙方提供的测试服务对象异常，如：网络卡顿、安全设备报警、服务器宕机（极少数发生）等状况。如测试对象具有特殊性、重要性，甲方应提供非生产环境测试对象。

3. 考虑到测试的非预期性，甲方有义务做好必要的安全备份和灾难恢复计划策略，甲方应明确提供测试范围及重要业务点（如有特殊情况请备注告知），甲方应做好必要的安全监测手段，发生问题时及时告知乙方，并进行必要的暂停测试处置；

4. 通过甲乙双方有效的事先沟通可避免发生如上意外情况，如实际情况中发生由于甲方提供测试对象及范围不明确、未明确告知测试对象重要性或特殊性、未第一时间通知乙方暂停测试、未进行必要的备份措施等导致的意外情况，乙方及乙方测试人员不负有任何责任。

三、安全测试对象

渗透测试对象由甲方根据自己的需求来择优选择，并提供给乙方准确的 IP 和域名等信息。

四、安全测试环境

安全测试环境	
测试时间：	年　月　日至　年　月　日
测试地点：	甲方指定地点

五、安全测试授权说明和注意事项

安全测试授权说明和注意事项
授权委托事项： 委托被授权方从互联网对授权方互联网 IP 资产进行渗透攻击测试，主要模拟黑客攻击的方式对授权方真实网络系统进行真实攻击。

渗透攻击方法：

被授权方测试方法遵循业界通用标准，包括但不限于：自动化扫描，口令穷举，身份验证突破，策略配置漏洞，Web应用漏洞利用，访问控制突破，系统用户提权，内外网混联检测，溢出漏洞攻击等。

渗透注意事项：

1. 攻击过程中攻击方要做到“点到为止”，不对目标系统做任何破坏性操作，如发现违规操作造成目标系统瘫痪、应用损坏、敏感数据泄露等网络安全事故，追究相关人员责任。

2. 禁止使用DDos攻击、带有感染功能的恶意木马，禁止插入垃圾评论、增加虚假文档、发布虚假指令等。

授权方声明：

授权方认可被授权方提供的渗透测试方法，知晓并接受渗透测试可能带来的后果（如系统负载上升，系统崩溃，数据库异常等），并提前做好必要的备份和风险应对措施准备。对因测试而导致的意外事件，双方将协商共同配合解决。

甲方代表：

甲方联系方式：

盖章：

年　　月　　日

乙方代表：张小宝

乙方联系方式：18096617208

盖章：

年　　月　　日