2024年-2025年度
网络安全技术支持服务合同

甲　　方：中共宝鸡市委网络安全和信息化委员会办公室

乙　　方：杭州安恒信息技术股份有限公司

签订日期：2024 年 9 月 20 日

合同编号：

甲方：中共宝鸡市委网络安全和信息化委员会办公室	乙方：杭州安恒信息技术股份有限公司
法定代表人：冯军平	法定代表人：张小孟
授权代理人：袁阳	授权代理人：赵晶晶
电子邮箱：/	电子邮箱：aria.zhao@dbappsecurity.com.cn
财务联系人：王斌	财务联系人：张越芳 0571-88380999-1387
税号：11610300MB2990335R	税号：913301086623011957
文书送达地址及电话：陕西省宝鸡市金台区行政西路行政中心6号楼A座7楼	文书送达地址及电话：杭州市滨江区联慧街188号安恒大厦 0571-28860999
开户行及账号：中国建设银行宝鸡政府广场支行 61050162910108000059	开户行及账号：招商银行杭州钱塘支行 571905187410303

甲乙双方经过友好协商，就甲方向乙方购买安全服务有关事宜，达成如下条款：

一．名称、数量、价款

1.1 具体的网络安全服务明细及报价详见以下表格　人民币/元

服务名称	服务项目	服务报价	小计
互联网资产探查	通过资产探查，协助梳理市域互联网范围内当前存活的站点、应用平台、数据服务等，为安全管理、数据治理、资产纳管提供基础信息。年互联网资产探查量不少于 1000 个。	40000/年	40000/年
网络安全日常监测	包括信息资产安全预警、漏洞扫描、态势分析、专项整治、技术支撑等，根据资产探查情况，常态化监测资产不少于 500 个。	30000/年	30000/年
渗透测试	对日常监测资产开展渗透测试，出具测试报告，年渗透目标不少于 50 个。	79000/年	79000/年
网络安全检查现场技术支撑	一年两次。包含网络安全和数据安全相关软硬件的部署和防护现状、安全组织管理、安全运维能力、应急保障等情况进行调研和检查。	40000/年	40000/年
网络安全突发事件应急技术支撑	通过远程和现场支持的形式协助中共宝鸡市委网信办对遇到的突发性安全事件进行紧急分析和处理。	19000/年	19000/年
服务期限：一年（2024 年 9 月 20 起至 2025 年 9 月 20 止）			
含税合同总价（人民币大写）：贰拾万零捌仟元整（小写：208000.00）			

详细服务内容安排见附件一技术服务规范书。

二．支付

2.1 本合同总价为人民币贰拾万零捌仟元整（小写：208000.00）。

2.2 合同生效之日起 15 日内，甲方向乙方支付合同总价的 60%，计人民币壹拾贰万肆仟捌佰元整（小写 124800.00 元）。

2.3 余款的支付：服务协议结束后 15 个工作日内，甲方按照协议完成情况向乙方支付剩余 40%，计人民币捌万叁仟贰佰元整（小写 83200.00 元）。

2.4 在甲方支付合同款的同时，乙方向甲方开具相应金额的增值税发票，甲方开票信息如下：

单 位 名称：宝鸡市市级国库集中支付往来资金账户

开户行名称：中国银行宝鸡高新广场支行

开户行账号：102831264647522001

三．项目的进度

3.1 乙方受甲方委托，在合同期限内，按照甲方要求完成约定的网络安全技术服务，甲方提供必要配合。

3.2 乙方负责在服务期限内向甲方提供安全服务报告。甲方在收到乙方安全服务报告后 5 个工作日内确认并签署服务确认单。如甲方逾期未签署的，视为确认通过。

四．保密条款

4.1 本合同中所指的保密信息包括了任何一方在方案决定前期以及实施过程中向对方提供的任何技术上、商业上或贸易上的具有经济价值的以书面、口头或任何其他方式提供给对方的所有非公开资料。

4.2 双方同意，在任何时候，不论是合同有效期内还是合同终止以后，对另一方提供的技术文件以及事务、业务或操作方法（下称秘密信息）实行严格保密。泄露方应就一切有意、无意泄露对方秘密信息的行为向对方承担赔偿责任。赔偿金包括一切直接、间接损失及由此而支出的费用。

4.3 一方保证，其依本合同所知悉的秘密信息只用于本合同的目的，不用于其他任何目的或向任何第三方（包括单位、个人，也包括甲、乙方的关联企业如子公司、参股公司、母公司等）披露。一方承认并同意，对方是秘密信息的独家拥有者，将不直接、间接侵犯或损害对方对秘密信息的所有权。

4.4 一方应只在下述情况下，方可使用秘密信息：

4.4.1 出于履行本合同的需要。

4.4.2 不论如何，秘密信息均不得以任何方式用于对对方不利、有损或相竞争的目的。秘密信息未经对方事先书面同意，不得被复制、全部或部分与其他信息相编纂、透露给第三方。

4.5 一方除经按本合同许可外，不得传播、透露秘密信息的全部或部分。秘密信息可向本方的代表和需获悉秘密信息以辅助本方履行其义务的员工披露。一方保证，在上述本方代表和员工知悉秘密信息之前，向其提示秘密信息的机密性与专有性，并保证上述代表与员工同意接受本合同条款的约束。根据此项保证，一方将向对方赔偿因上述代表、员工违约披露、使用秘密信息造成的一切直接、间接损失、费用（包括律师费）与其他支出。

4.6 如果一方由于法律要求被迫公开对方的保密信息，则应该及时通知对方，使得对方能与作出法定强制行为的机构进行协商处理。

4.7 本条款约定的双方的义务不因本合同的终止而终止。本条款的效力于全部秘密信息的秘密性全部丧失时终止。

4.8 如无乙方预先书面同意，甲方不得向任何第三方转让乙方提供的技术文件的使用权。

4.9 任何一方违反保密义务泄露对方保密信息的，应赔偿对方损失，损失难以计算的按本合同总金额的10%进行赔偿。

五．知识产权

5.1 除非另有约定，任何一方均不因本合同的生效取得另一方在合同签署前已拥有的版权、专利、商业秘密、商标或任何其他知识产权。已存在的版权及其他知识产权应属拥有该等权利的一方所有。

六．不可抗力

6.1 合同生效后，任何一方由于火灾、台风、水灾、地震、战争等不可抗力事件而影响本合同履行时，则延长履行合同的期限，这一期限应相当于事件所影响的时间，并可根据情况部分或全部免予承担违约责任。不可抗力事件发生

后，双方应尽可能减少损失，如一方未能履行此义务，则对因此扩大的损失承担责任。

6.2 受不可抗力影响方应尽快将所发生的情况以邮件通知对方。

6.3 当不可抗力事件停止或消除后，受影响的一方应尽快以电传或电报方式通知另一方。如不可抗力的影响连续二十天以上时，双方应通过友好协商并尽快达成合同，解决本合同的履行问题。

七．违约责任

7.1 因乙方工作不力，未按照约定完成资产探查、渗透测试、日常监测、技术支撑、应急响应等服务，或在服务质量和数量上与约定存在差异，则甲方有权扣除部分费用，具体金额由甲乙双方协商确定。

7.2 除不可抗力因素或合同另有约定外任何一方不得解除合同，否则需向守约方支付本合同金额 10%的违约金。

7.3 因违约行为致守约方的实际损失超出违约方按照本合同约定应支付的违约金时，守约方有权就超出部分向违约方索赔。

八.争议解决

8.1 双方应尽最大努力友好协商解决与合同或与合同执行有关所产生的任何争议。如果未能友好解决，双方可向甲方所在地有管辖权的人民法院提起诉讼。诉讼费、律师费、担保费、保全费、调查费、公告费、鉴定费、差旅费、执行费等守约方因维权产生的费用均由违约方承担。

九．合同的生效、解除和终止

9.1 本合同签订后，自 2024 年 9 月 20 日起生效，服务期限一年。

9.2 如果发生以下情况，可以视为本合同达到解除条件或终止：

9.2.1 乙方进入解体或倒闭阶段；

9.2.2 乙方被判为破产或其它原因致使资不抵债；

9.2.3 乙方提供的服务出现严重失误，其服务不能达到甲方要求；

9.2.4 双方共同同意提前解除合同；

9.2.5 按法院的裁决，合同解除或终止。

十. 附件

10.1 本合同附件 1《技术服务规范书》附件 2《渗透测试授权委托书》，为合同不可或缺部分，与合同正文具有同等法律效力。

十一. 其它

11.1 本合同采用纸质件签署，纸质盖章件壹式肆份，甲乙双方各执贰份，具有同等法律效力。

11.2 所需的通知或双方其它形式的往来通讯应采用书面/电子送达形式，以下情形下视为已送达：

（1）本人亲自送达且有书面收据；

（2）邮寄、挂号邮寄至本合同首部载明的送达地址，排除不可抗力的情况，无论收件方是否有签收，自该等文件投邮之日起的第五日视为送达之日；

（3）文件发送至本合同或电子合同签约平台上记载的电子邮箱。

（以下无正文）

甲方：中共宝鸡市委网络安全和信息化委员会办公室

负责人：

日 期：2024.9.20

乙方：杭州安恒信息技术股份有限公司

负责人：

日 期：2024.9.20

附件一

技术服务规范书

网络安全技术服务工作主要包含五个方面，分别为互联网资产探查、网络安全日常监测、渗透测试、网络安全检查技术支撑和应急支撑响应五大类技术支撑。

一、互联网资产探查

互联网资产探查：通过资产探查，协助梳理市域互联网范围内当前存活的站点、应用平台、数据服务等，为安全管理、数据治理、资产纳管提供基础信息，年互联网资产探查量不少于1000个。

1、互联网暴露面资产管理：根据提供的已知IP地址规划使用信息，通过整理完善相关记录表格并下发资产调研统计表，梳理出已知资产的归属单位、责任人、业务系统等管理信息属性，协助甲方完善互联网暴露面资产信息。

2、互联网暴露面资产发现和识别：梳理映射在互联网的IP、端口服务信息，确认其开放的资产和服务信息，补全已知业务用途及管理归属信息；根据已知的开放互联网IP地址或IP网段，对存活IP及开放的端口服务进行探测，人工核验后输出开放的IP、端口、服务列表。

二、网络安全日常监测：

网络安全日常监测：包括信息资产安全预警、漏洞扫描、态势分析、专项整治、技术支撑、整改核查等，常态化监测资产不少于500个。

1、安全预警：根据资产探查的结果，掌握资产服务、框架、中间件类型，爆发高危漏洞之后，在第一时间内向客户发布高危漏洞预警，向客户通告漏洞的危害程度、影响范围、检测方法及相关解决方案。

2、漏洞扫描：对重点互联网资产开展24小时漏洞扫描，检查否存在WEB程序安全漏洞，标明漏洞类型，提出解决方案，一周两次以网络安全漏洞整改通知的方式报甲方。

3、态势分析：每季度分析全市网络安全态势，形成季度网络安全态势分析报告，上一季度结束5日内报甲方。每年6月、12月对半年网络安全形势进行研判，出具研判报告。

4、专项整治：协助甲方开展专项整治活动，形成相关报告。

三、渗透测试

渗透测试：对日常监测资产开展渗透测试，出具测试报告，年渗透测试目标

不少于50个，成功渗透目标不少于20个。

技术手段包括但不限于SQL注入，XSS跨站脚本，网页挂马，缓冲区溢出，文件上传漏洞，源代码泄露，目录浏览、遍历漏洞，数据库泄露，弱口令，越权访问，会话验证绕过，管理地址泄露，舆论信息检测、中间件漏洞等。

渗透工作开始前应得到甲方授权后方可执行。在渗透测试过程中，尽量避免影响正常业务运行，在渗透测试前征求用户意见，并采取时间策略、测试策略、备份策略、应急策略、沟通策略等多条策略尽量规避渗透测试带来的风险。

渗透测试人员模拟黑客入侵攻击，对系统可能出现的不稳定现象提出相应对策，确保服务器和网络设备在进行渗透测试的过程中保持在可信状态。

四、网络安全检查技术支撑

网络安全检查技术支撑：乙方对甲方开展的网络安全检查工作提供现场技术支持服务，一年两次。服务内容可根据实际情况调整确定。检查内容主要包括：

1.合规检查：对网络安全和网络数据安全日常组织管理情况、相关软硬件的部署和防护现状，等级保护落实情况、安全运维能力情况、风险评估开展情况、应急保障处置情况、信息资产梳理、新技术新应用(APP、云计算、物联网、区块链等)等进行调研和检查。

2.技术检查：主要通过渗透测试、恶意代码检测及安全漏洞扫描实施检查，检查关键信息基础设施的信息系统基本情况、网络安全技术防护加固情况，是否存在安全隐患。

3.个人信息保护及重要数据保护检查：协助甲方检查有关单位在数据采集、传输、存储、交换等环节的工作是否按照有关法律法规开展，是否安全可靠。

4.工业控制系统安全检查：协助甲方检查有关单位重要信息资产的网络架构及边界安全防护情况、信息传送安全防护情况、工控系统情况摸底、安全操作规程建立等情况。

5.户外大屏安全检查：协助甲方对机关单位、市政设施的户外LED屏、广告屏等进行检查，是否存在违规联网等安全隐患。

6.其他检查：以辖区实际情况为准，进行检查内容的调整。

五、应急支撑响应

应急支撑响应：当发生网络安全事件时，乙方须协助甲方提供市辖区内各类网络安全事件的现场应急响应和技术支撑，并按时出具详细完整的检查报告。

附件二

渗透测试授权委托书

授 权 方：中共宝鸡市委网络安全和信息化委员会办公室

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（详情查看《安全测试对象表》），并保证相关测试范围均为具有管辖权，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．乙方有义务为相关测试信息、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．乙方不应除本协议规定的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不定)；

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、安全测试对象表

注：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。

序号	测试对象	服务器IP地址	备注

四、安全测试环境

安全测试环境	
测试时间：	2024年09月20日至2025年09月20日
测试地点：	杭州安恒信息技术股份有限公司

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：袁阳

甲方联系方式：19591210868

盖章：

2024 年 09 月 20 日

乙方代表：文振乾

乙方联系方式：15091675837

盖章：

2024 年 09 月 20 日