政府采购合同

项目名称：山东省烟台市本级烟台市交通运输局
交通信息系统安全运营服务采购

项目编号：SDGP370600000202402000755

甲　方：烟台市交通运输局

乙　方：山东华安赛服智能科技有限公司

签署日期：2024年9月29日

（烟台市交通运输局）（山东省烟台市本级烟台市交通运输局交通信息系统安全运营服务采购）由（山东信一项目管理有限公司）以 SDGP370600000202402000755 号磋商文件在国内以 竞争性磋商（采购方式）方式进行采购。经磋商小组确定 山东华安赛服智能科技有限公司（乙方）为成交单位。甲乙双方同意按照下面的条款和条件签署本合同。

一、协议文件

下列文件构成本协议的组成部分，应该认为是一个整体，彼此相互解释，相互补充。

1. 磋商文件

2. 响应文件

3. 乙方在磋商时的书面承诺

4. 成交通知书

5. 协议补充条款或说明

6. 附件

7. 本合同（包括合同附件、补充协议）

二、协议范围和条件

本协议的范围和条件与第一条协议文件中的规定相一致。

三、服务内容要求：详见附件

四、合同金额：

本合同总金额：￥ 297600.00 元

（大写）： 贰拾玖万柒仟陆佰 元整。

该价格为包括完成本项目服务工作期间所需的所有费用除此之外甲方不予支付其他任何费用。乙方因收取合同金额而应承担的各项税费由其自行承担。

五、运营服务期： 自合同签订之日起1年 。

六、付款方式： 合同签订生效具备实施条件后 5 个工作日内凭成交单位提供的发票等有效凭证支付合同价款 30%的预付款，待运营服务期结束并验收合格后凭验收单、发票等有效凭证一次性无息付清剩余70%合同价款。 乙方知悉甲方使用财政资金拨款，如因甲方未收到财政资金而预期向乙方付款的，甲方对此不承担任何违约责任。

七、服务质量与验收

1、乙方必须按照甲方的委托事项进行服务。

2、服务程序、服务方法、服务内容及技术要求，乙方必须严格按照烟台市相关规定及甲方要求的工作标准执行，保证服务结论报告真实、可靠。

八、项目管理

乙方:指定商希超（联系电话：18953522876）全权负责该项目的商务和技术。每一项目实施必须指定相关负责人并由其全程管理。

九、违约责任

1、乙方未按委托书约定的时间、内容及要求完成服务项目，甲方有权单方终止本合同，乙方按照本合同总金额的30%向甲方支付违约金，乙方承担甲方为主张权利支出的诉讼费、保全担保费、律师费、评估鉴定费等所有费用。甲方有权另行委托其它服务机构，由此所产生的费用（包括但不限于评估费等）由乙方承担。但由于甲方未履行其应承担的义务而造成的，乙方不承担违约责任。

2、因乙方过失、舞弊行为而导致评估结果不真实、不准确的，乙方承担同第九条第一款的违约责任。但因甲方提供的资料不真实、不齐全而造成的，乙方不承担责任。

3、乙方给甲方造成的实际损失高于违约金的，对高出违约金的部分乙方应予以赔偿。

4、乙方迟延履行协议、不完全履行协议，除承担同第九条第一款的违约外，乙方仍应实际履行协议；不履行或履行协议不符合约定，甲方均有权解除协议，并就乙方违约给甲方造成的损失向乙方索赔。

5、其它未尽事宜，以《中华人民共和国民法典》和其它有关法律、法规规定为准，无相关规定的，双方协商解决。

十、合同的生效

本合同经甲乙双方授权代表签署并加盖公章或合同章后生效。

十一、不可抗力

甲、乙方中任何一方，因不可抗力不能及时或完全履行合同的，应及时通知对方，并在5 天内提供相应证明。未履行完合同部分是否继续履行、如何履行等问题，可由双方协商解决，但确定为不可抗力原因造成的损失，免予承担责任。

十二、争议的解决方式

（1）在解释或者执行本合同的过程中出现疑问或发生争议时，双方应通过协商方式解决。

（2）经协商不能解决的争议，可向芝罘区人民法院提起诉讼。

（3）除有争议部分外，本合同其他部分仍应按合同条款继续履行。

十三、本合同未尽事宜，由双方协商后可签订补充协议，所签订的补充协议与本合同具有同等的法律效力。

十四、本协议一式五份，甲、乙双方各两份，山东信一项目管理有限公司一份。

甲　方：

名称：（盖章）烟台市交通运输局

法定代表人（签字）：

授权代表（签字）：

开户银行：

银行账号：

签订日期：2024.9.29

乙 方：

名称：（盖章）山东华安赛服智能科技有限公司

法定代表人（签字）：

授权代表（签字）：高东超

开户银行：中国工商银行股份有限公司烟台莱山支行

银行账号：1606022119200364766

签订日期：2024.9.29

附件：

序号	服务项目	服务内容	单位	数量	单价	总价	备注
1	资产识别与梳理服务	1、我司所投深信服资产识别与梳理服务支持资产发现与识别，在烟台市交通运输局授权和监督下，借助安全工具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，确保安全运营中心中资产信息的准确性和全面性。 2、我司所投深信服资产识别与梳理服务支持资产信息梳理与管理，支持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；应用系统管理方式、资产的重要性以及网络拓扑），并将信息录入到安全运营平台中进行管理；当资产发生变更时，安全专家对变更信息进行确认与更新。	宗	1	12896	12896	
2	整网风险评估服务	1、我司所投深信服整网风险评估服务支持策略检查，安全组件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。 2、我司所投深信服整网风险评估服务支持脆弱性评估：（1）系统与Web漏洞扫描：对操作系统、数据库、常见应用/协议、Web通用漏洞与常规漏洞进行漏洞扫描。（2）弱口令扫描：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。暴露面梳理安全专家使用扫描组	宗	1	14880	14880	

		件对资产开展暴露面探测，以梳理资产面向互联网的开放情况，快速发现违规暴露在互联网中的资产及存在的风险并进行处置，实现对暴露面资产可管可控，降低暴露面资产的风险。 3、我司所投深信服整网风险评估服务支持失陷类事件评估： （1）勒索病毒事件分析：安服专家分析判断主机是否感染了勒索病毒；是否已感染勒索病毒文件；根据已发生的漏洞攻击行为分析判断否存在勒索病毒攻击等。 （2）挖矿病毒事件分析：安服专家分析是否感染了挖矿病毒/木马；是否处于挖矿状态；根据已发生的漏洞攻击行为分析判断是否存在以植入挖矿木马为目的的漏洞攻击等。 （3）蠕虫病毒事件：安服专家确认文件是否被感染，定位失陷的代码并进行修复。 （4）失陷主机分析：安全专家对失陷主机进行分析研判（如恶意程序及后门脚本类事件），并给出处置及加固建议。 （5）潜伏威胁分析：安全专家分析内网主机的非法外联威胁行为，判断是否存在潜伏威胁，并给出处置及加固建议。含：对外攻击、APTC&C通道、隐藏外联通道等外联威胁行为。 4、我司所投深信服整网风险评估服务支持攻击行为评估，支持针对漏洞利用攻击行为、Webshell上传行为、Web系统目录遍历攻击行为、SQL注入攻击行为、信息泄露攻击行为、口令暴力破解攻击行为、僵尸网络攻击行为、系统命令注入攻击行为及僵尸网络攻击行为进行分析评估，判断攻击行为是否成功以及业务风险点。					

3	安全体系建设差距分析服务	1、我司所投深信服安全体系建设差距分析服务支持对信息系统的安全现状进行安全体系建设差距测评，分析信息系统保护现状和信息安全等级保护基本要求之间的差距，为通过信息系统等级保护奠定基础。 2、我司所投深信服安全体系建设差距分析服务支持综合重要信息系统的特点，明确安全需求，协助梳理正式的现有安全体系建设文件，设计符合相应等级要求的信息系统安全技术建设整改方案，配合烟台市交通运输局下发各个二级单位，协助进行信息安全体系建设技术整改。 3、我司所投深信服安全体系建设差距分析服务支持分区分域管理，对交通运输局现有网环境进行区域划分，明确信任区与非信任区，将无线网络纳入网络安全管理范畴。	宗	1	9920	9920	
4	漏洞管理服务	1、我司所投深信服漏洞管理服务支持漏洞管理，支持漏洞扫描与验证，针对服务范围内的资产的系统漏洞和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的风险及分析发生后可造成的危害。 2、我司所投深信服漏洞管理服务支持漏洞优先级排序：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。排序依据包含资产重要性、漏洞等级以及威胁情报三个维度。 3、我司所投深信服漏洞管理服务支持漏洞验证，提供漏洞验证服务，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的风险及分析发生后可造成的危害。针对已	宗	1	19840	19840	

		经验证的漏洞，自动生成漏洞工单，安全专家跟进漏洞状态，各个处理进度透明，方便招标方清晰了解当前漏洞的处置状态，将漏洞处理工作可视化。 4、我司所投深信服漏洞管理服务支持针对存在的漏洞提供修复建议，能够提供精准、易懂、可落地的漏洞修复方案。 5、我司所投深信服漏洞管理服务支持提供漏洞复测措施，及时检验漏洞真实修复情况。复测措施可按需针对指定漏洞，指定资产等小范围进行，降低漏洞复测时的潜在影响范围。 6、我司所投深信服漏洞管理服务支持对发现的漏洞建立状态追踪机制，自动化持续跟踪漏洞情况，清晰直观地展示漏洞的修复情况，可以有效地追踪资产漏洞生命周期，清楚地掌握资产的脆弱性状况，实现漏洞全生命周期的可视、可控和可管。 7、我司所投深信服漏洞管理服务支持最新漏洞预警与排查，支持针对已经梳理录入安全运营平台的信息化资产，需实时抓取互联网最新漏洞与详细资产信息进行匹配，对最新漏洞进行预警与排查。预警信息中包含最新漏洞信息、影响资产范围。 8、我司所投深信服漏洞管理服务支持最新漏洞处置指导，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，补丁方案以及临时规避措施。 9、我司所投深信服漏洞管理服务支持最新漏洞复测与状态跟踪，由我方对该最新漏洞建立状态追踪机制；跟踪修复状态，遗留情况。					

		10、我司所投深信服漏洞管理服务支持漏洞报告下发，协助科教科整理完善漏洞报告，定时下发至二级单位督促整改。					
5	威胁管理服务	1、我司所投深信服威胁管理服务7*24H威胁鉴定与通告： （1）7*24H威胁鉴定：安全专家依托于安全能力平台的大数据分析和威胁检测能力实时监测用户网络安全状态，对平台监测到的安全威胁进行分析鉴定，识别到真正的安全事件。 （2）7*24H专家通告：服务专家对分析鉴定后的各类威胁告警、安全事件生成服务工单，并及时向用户通告。 2、我司所投深信服威胁管理服务支持威胁分析与处置： （1）威胁分析：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。 （2）威胁处置：安全专家提供对应的处置和加固建议（如封锁攻击源、设置安全策略防护等措施），并借助客户已有的安全组件帮助用户闭环威胁 3、我司所投深信服威胁管理服务支持威胁情报管理： （1）精准威胁情报推送：实时抓取互联网最新威胁情报与详细资产信息进行匹配，对最新威胁情报进行通告与排查。 （2）支持受影响资产排查与加固：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。	宗	1	19840	19840	

		4、我司所投深信服威胁管理服务，安全专家可针对内/外网或特定业务系统及特定漏洞，基于客户业务定制检测逻辑，尽可能快地发现漏洞或攻击痕迹，发现潜在的安全隐患和已失陷的主机/被钓鱼成功的员工/账密信息泄露等，最大限度地降低攻击者造成的危害，评估造成的损失等内容，最终帮助客户验证风险并推动发现的问题和隐患进行闭环处理。 5、我司所投深信服威胁管理服务支持安全策略检查，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。 6、我司所投深信服威胁管理服务支持安全策略调优，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。					
6	事件管理服务	1、我司所投深信服事件管理服务支持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。 2、我司所投深信服事件管理服务支持安全事件处置与闭环：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，闭环事件工单。 3、我司所投深信服事件管理服务提供重大事件应急响应：	宗	1	19840	19840	

		（1）事件影响抑制：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。 （2）入侵威胁清除：排查攻击路径、恶意文件、清除。 （3）入侵原因分析：还原攻击路径，分析入侵事件原因，提供安全事件溯源结果。 （4）加固建议指导：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。					
7	7*24H 团队对接服务	1、我司所投深信服7*24H团队对接服务为交通运输局配置一名经验丰富的安全专家作为专属服务经理。 2、我司所投深信服7*24H团队对接服务提供实时专家咨询，安全专家对交通运输局咨询或上报的安全问题进行及时响应并给出建议，如主机加固建议咨询、安全事件处置建议咨询等。 3、我司所投深信服7*24H团队对接服务支持节假日值守，安全值守专家进行7*24小时安全监测，对发生的安全事件进行及时响应并在节假日期间每日进行值守总结，在服务群发送值守总结快报。	宗	1	19840	19840	
8	安全培训服务	1、我司所投深信服安全培训服务支持安全意识培训，为增强交通运输局员工的安全意识、提升全员的网络及信息安全知识，通过当前典型的安全事件导入，定期开展信息安	宗	1	12896	12896	

		全宣传活动，宣传内容包括：网络及信息安全法律法规、员工安全意识、网络及信息安全制度等。 2、我司所投深信服安全培训服务提供专业网络安全技术能力提升培训，结合交通运输局现有网络安全现状与网络安全建设需求，提供两人的与网络安全相关的培训名额（包含全部学习、培训及考试费用）。 3、我司所投深信服安全培训服务为网络安全宣传周提供定制化的的4个宣传展架和100本手册。					
9	应急演练服务	1、我司所投深信服应急演练服务配合交通运输局完成年度安全应急演练，演练前提供专业的演练计划和场景方案，结束后完成应急演练的总结。 2、我司所投深信服应急演练服务支持协助交通运输局完善安全应急响应机制，向交通运输局提供规范的应急预案文本并指导交通局完善安全应急响应预案，并根据实际情况，提供安全应急事件演练方案。	宗	1	9920	9920	
10	新业务上线安全检查服务	我司所投深信服新业务上线安全检查服务针对新上线业务系统的安全检查项目，包含漏洞检查、应用系统配置核查、安全加固建议以及加固后复查、模拟业务流的渗透测试、WEB站点渗透和业务系统网络架构优化、审计等。包括代码安全检测服务。用合理化手段和工具，对目前已部署的全部应用系统进行代码安全检测，发现系统源代码存在的安全缺陷，并采用安全测试等技术手段进行漏洞验证。	宗	1	14880	14880	

11	办公区终端安全扫描服务	1、我司所投深信服办公区终端安全扫描服务专注于对市交通局办公区内的所有终端进行深度的安全漏洞扫描，利用专业的漏洞扫描工具和技术，识别潜在的安全风险。 2、我司所投深信服办公区终端安全扫描服务支持对扫描结果进行分析，特别关注那些被识别为重要或高风险的终端电脑，优先进行漏洞修复工作。 3、我司所投深信服办公区终端安全扫描服务为市交通局信息技术部门提供详细的漏洞修复指导，包括修复步骤、所需补丁或更新程序等。对于关键终端电脑，可提供现场技术支持，确保漏洞得到及时、有效的修复。 4、我司所投深信服办公区终端安全扫描服务支持溯源排查工作，如果局内存在被通报的存在失陷主机电脑，为确保系统安全、防止攻击进一步扩散，我方可以协助进行失陷主机电脑的全面溯源排查工作。	宗	1	9920	9920	
12	网络安全检查服务	我司所投深信服网络安全检查服务支持协助市交通局完成对局属各单位及重点交通企业的网络安全工作检查。根据年度重点网络安全工作任务安排，针对不同网络安全检查工作，形成《检查方案》，包括：任务目标、检查内容及方式、人员安排、时间安排等；根据不同的检查要求，整理对应的检查资料，最终形成完整的安全检查报告。	宗	1	9920	9920	
13	成果交付服务	我司支持以下服务交付物，交付物名称及报告频率如下： 交付物名称：《安全服务运营报告》，报告频率：每周一次 交付物名称：《首次威胁分析与处置报告》，报告频率：一次	宗	1	9920	9920	

		交付物名称：《事件分析与处置报告》，报告频率：按需触发，不限次数 交付物名称：《安全通告》，报告频率：按需触发，不限次数，每月汇总一次 交付物名称：《综合分析报告》，报告频率：每月一次 交付物名称：《季度汇报PPT》，报告频率：每季度一次 交付物名称：《年度汇报PPT》，报告频率：每年一次 交付物名称：《应急演练报告》，报告频率：每年一次交付物名称：《新业务上线安全检查报告》，报告频率：新业务数量 交付物名称：《办公网络安全扫描报告》，报告频率：每年两次 交付物名称：《检查方案》《检查报告》，报告频率：每年一次					
14	安全感知系统	我司提供1套深信服安全感知系统，定位为交通运输局的安全大脑，是一个检测、预警、响应处置的大数据安全分析平台。以全流量分析为核心，结合威胁情报、行为分析建模、UEBA、失陷主机检测、图关联分析、机器学习、大数据关联分析、可视化等技术，对全网流量实现全网业务可视化、威胁可视化、攻击与可疑流量可视化等，帮助交通运输局在高级威胁入侵之后，损失发生之前及时发现威胁。	宗	1	43648	43648	
15	流量采集系统	我司提供4套深信服流量采集系统，对各种攻击行为以及网络威胁进行高精度的检测，采用被动扫描和主动扫描两种方式帮助交通运输局进行资产识别和脆弱性识别，设计各种数据接口向安全感知系统提供检测数据和原始数据，一方面降低第三方平台	宗	1	69440	69440	

		的安全分析压力，另一方面又提供原始素材供其进行进一步安全分析。					
合计		大写：贰拾玖万柒仟陆佰元整　　小写：297600.00					