国家税务总局青岛市税务局
2024年度重大时期网络安全保障服务项目
（技术支持服务类）

合　同

合同编号：HYHAQDFGS2024-0099

甲　　方：国家税务总局青岛市税务局

乙　　方：上海斗象信息科技有限公司

根据《中华人民共和国政府采购法》《中华人民共和国民法典》等有关法律法规规定，国家税务总局青岛市税务局(以下简称：“甲方”)通过公开招标采购确定 上海斗象信息科技有限公司 (以下简称：“乙方”)为国家税务总局青岛市税务局2024年度重大时期网络安全保障服务项目的供应商。甲乙双方同意签署《国家税务总局青岛市税务局2024年度重大时期网络安全保障服务项目》(合同编号：_HYHAQDFGS2024-0099，以下简称：“合同”)。

1. 合同文件

下列文件是构成本合同不可分割的部分：

(1)合同条款；

(2)报价表；

(3)政府采购招标文件

(4)投标(响应)文件技术部分；

2. 采购内容及数量

服务名称	数量	单位	具体服务承诺(包含但不限于服务内容、范围和基本要求)
国家税务总局青岛市税务局2024年度重大时期网络安全保障服务项目	1	年	详见《一、合同条款》的《3.服务》内容

3. 合同金额

本合同金额为人民币柒拾捌万贰仟元整(￥782000.00 元)。本合同项下所有服务的人工费、交通费、管理费、税费及其他不可预见的全部费用均已包含于合同价中，除本合同另有约定外，甲方不再向乙方另行支付其他任何费用。

4. 付款方式

支付方式：银行转账

第一次支付：合同履行满5个月且满30个重保服务天数，甲方根据乙方实际履约情况验收合格后，支付合同金额的40%；

第二次支付：本合同服务期满且验收合格后，支付剩余金额。

甲方向乙方支付每笔费用之前，乙方需向甲方提交付款申请及合格发票等资料。乙方不能按照甲方要求提供上述发票等资料或提供的资料不适用、不合格的，甲方有权延付相应款项且不承担任何违约责任直至乙方提供合格付款资料。乙方不得以甲方逾期付款为由停止工作或拒绝、拖延本合同项下的任何义务。

5. 合同签订地

青岛市市南区延安三路 236 号。

6. 验收方式

6.1. 乙方在服务期间，应按甲方要求提供服务过程文档，并作为项目验收重要依据。

6.2. 乙方在服务期间，甲方定期对乙方服务质量进行评价，评价情况作为项目验收重要依据。

6.3. 合同期满 10 个工作日内，甲方根据乙方服务整体情况进行评价，做出整体验收结论，并形成验收报告，并由甲乙双方共同签章确认。

7. 合同有效期

本合同有效期为自合同生效之日起一年。

8. 合同生效

本合同一式 陆 份，甲方 肆 份，乙方 贰 份，经甲乙双方法定代表人或被授权代表签字（签章）并加盖单位公章后生效。

甲方：国家税务总局青岛市税务局

签字（或印章）：

盖章：

日期：2024年12月5日

乙方：上海斗象信息科技有限公司

签字（或印章）：

盖章：

日期：2024年12月5日

一、合同条款

合同条款前附表

序号	内容
1	合同名称：国家税务总局青岛市税务局 2024 年度重大时期网络安全保障服务项目 合同编号：HYHAQDFGS2024-0099
2	甲方名称：国家税务总局青岛市税务局
	甲方地址：青岛市市南区延安三路 236 号
	甲方联系人：赵长利 电话：0532-83931411
3	乙方名称：上海斗象信息科技有限公司
	乙方地址：中国(上海)自由贸易试验区张衡路 200 号 1 幢 1 层
	乙方联系
	乙方开户 账号：
4	合同金额：本合同金额为人民币 柒拾捌万贰仟元整(￥782000.00 元)。本合同金额为固定金额，除本合同另有约定外，甲方不再向乙方另行支付其他任何费用。
5	服务时间、地点：自本合同生效之日起一年。 青岛市市南区延安三路 236 号。
6	服务履行期：自 2024 年 12 月 26 日起一年。 如遇重大政策调整或不可抗力因素，可根据实际情况调整服务期限，甲方不承担任何责任。
7	验收方式及标准： 验收主要内容： 1、重保服务日报； 2、威胁情况分析报告； 3、现场服务和远程服务工单、服务确认单； 4、阶段性小结； 5、讲解记录； 6、服务总结报告及项目验收报告； 7、供应链安全管理相关资料； 8、甲方要求的其他与项目相关的资料和文档。
8	付款方式：银行转账 第一次支付：合同履行满 5 个月且满 30 个重保服务天数，甲方根据乙方实际履约情况验收合格后，支付合同金额的 40%；

	第二次支付：本合同服务期满且验收合格后，支付剩余金额。 甲方向乙方支付每笔费用之前，乙方需向甲方提交付款申请及合格发票等资料。乙方不能按照甲方要求提供上述发票等资料或提供的资料不适用、不合格的，甲方有权延付相应款项且不承担任何违约责任直至乙方提供合格付款资料。乙方不得以甲方逾期付款为由停止工作或拒绝、拖延本合同项下的任何义务。
9	履约保证金及其返还：不要求提供。
10	服务质量问题赔偿费约定：详见合同条款 8.违约责任
11	合同履行期限：自合同生效之日起至合同全部权利义务履行完毕之日止。
12	合同纠纷的解决方式： 首先通过双方协商解决，协商解决不成，则通过以下途径之一解决纠纷(请在方框内画“√”选择)： □提请青岛仲裁委员会仲裁。 ☑向甲方所在地人民法院提起诉讼

1. 定义

本合同下列术语应解释为：

1.1. “甲方”是指招标人。

1.2. “乙方”是指中标/成交供应商。

1.3. “合同”系指甲乙双方签署的、合同中载明的甲乙双方所达成的协议，包括所有的附件、附录和上述文件所提到的构成合同的所有文件。

1.4. “服务”是指乙方按照招标(采购)、投标(响应)文件要求，向招标人提供的技术支持服务。

1.5. “项目现场”是指甲方指定的最终服务地点。

1.6. “天”除非特别指出，“天”均为自然天。

2. 服务标准

2.1. 乙方为甲方交付的服务应符合招标(采购)文件所述的内容，如果没有提及适用标准，则应符合相应的国家标准。这些标准必须是有关机构发布的最新版本的标准。

2.2. 除非技术要求中另有规定，计量单位均采用中华人民共和国法定计量单位。

3. 服务

乙方应按照合同的规定，提供符合甲方要求的服务。

3.1. 服务要求

3.1.1. 本项目要求服务期限为一年。

3.1.2. 服务期内根据甲方需求提供重大时期不低于70天且每天不少于4人团队(轮流，非同时）的7*24小时网络安全值守服务。为应对常态化开展攻防演练的发展趋势，参照总局重保人员安排，根据甲方工作需要，另提供临时性非工作日或夜间的值守服务。

投入本项目的值守人员应至少满足以下要求：

具有网络安全行业3年以上工作经验，本科及以上网络安全或相关专业，具备CISP或同等水平及以上的安全类认证证书；

具备网络安全测试、安全事件分析等能力，能够自主完成基础的安全事件分析处置工作。能熟练对安全平台告警日志进行分析，对存在的安全风险和隐患及时分析，根据事件的紧急程度及应用系统业务特点给出风险防范建议；

具体服务人员为乙方投标文件所投人员，所有服务人员在合同签订后6个月内不允许更换，6个月后确因特殊原因需要更换的应提出书面申请并经甲方同意后方可更换。

所有安全服务工具在合同约定之日起14日内完成部署、对接测试工作，且所有安全服务工具部署后，在未得到甲方授权的情况下禁止变更或撤除，服务期内禁止以任何形式将服务工具带回，服务期结束后如需带回，须经甲乙双方确认并对存储介质进行不可逆清理。

3.1.3. 在合同服务期内，若出现特殊情况，工程师及安全专家须在2小时内到场，及时消除安全事件不良后果，并在24小时内解决安全事件。处理事件并提交书面的安全事件调查分析报告（包括事故原因、过程描述、入侵来源、证据报告、解决方案、安全建议、处理结果等）。

3.2. 项目范围要求

3.2.1. 重大活动安全保障服务对象范围主要针对甲方各类网络资产，包括主机、网络、应用等，具体范围由甲方根据工作实际指定。

3.2.2. 重大活动时期主要包括但不限于重大节庆、重大会议等重要时期，具体由甲方根据保障工作需要进行指定。

3.3. 服务内容指标

乙方须组建专业服务团队，为甲方提供重大活动安全保障服务，主要服务内容包括：

- 攻击面梳理及安全性自查；
- 持续性威胁监控及分析；
- 持续性威胁防御与应急处置；
- 全面的攻击链梳理；
- 安全防御体系确认与加固；
- 动态防御技术补充；
- 攻击情况实时分析及检测；
- 安全事件应急。

服务期内，所需的各类服务支撑工具由乙方负责提供，产生的费用均包含在项目中。

（一）攻击面梳理及安全性自查

1、资产梳理和收敛

对甲方互联网系统进行广泛信息收集，发现防护措施薄弱点进行漏洞利用，识别出具有脆弱性的系统。全面梳理排查青岛税务全系统内（含区市局及派出机构）互联网出口及

互联网资产，识别对外暴露的服务应用系统，对资产收敛提供技术指导。

在服务期内，服务团队应以网络空间测绘技术为依托，构建云端扫描工具，以分布式资产监测节点对在互联网侧暴露的资产进行 7×24 小时持续探测。资产探测的内容至少包括：IP、域名、端口、操作系统指纹、中间件指纹、应用指纹、数据库指纹、服务协议、设备指纹等。

2、外部安全检查

2.1 渗透测试

由服务团队使用安全工具并结合专家经验，在测试矩阵的指导下，使用各种攻击技术对业务系统进行非破坏性质的模拟攻击和深入的安全测试，以发现信息系统代码层和功能逻辑方面的脆弱性。

2.2 Web 脆弱性扫描

服务团队须通过部署云端监测工具，对所有互联网开放业务定期进行脆弱性扫描，检查互联网业务系统是否存在 Web 程序安全漏洞，并标明漏洞类型和存在漏洞的网页链接，按照需求提供检查报告，并提出专家级漏洞修复建议。

扫描出的脆弱性问题须输入至金四安全管理平台漏洞处置流程，并跟踪完成闭环管理。

3、内部安全检查

在进行资产探测的同时建立资产台账，对资产定期进行组件级脆弱性探测，主要包括：

3.1 内网漏洞扫描

对内网关键应用进行漏洞扫描并对扫描结果进行人工分析，提交经过人工处理的漏洞扫描报告。漏洞探测内容应至少包括：操作系统漏洞、中间件漏洞、常用软件漏洞、应用程序漏洞、网络设备漏洞、数据库漏洞等。重大活动安全保障期间，服务团队须自行配备专用漏洞扫描工具，以支撑内网漏洞扫描服务工作，甲方不承担专用漏洞扫描工具所产生的费用。服务期结束后，乙方须彻底清除扫描工具中的数据。

3.2 服务器安全检查

服务团队应根据甲方使用系统情况，定制服务器安全检查工具，并提供检查手册，检查内容应包含网络连接检查、进程检查、异常文件检查、隐藏账号检查、克隆账号检查、异常账号检查、服务端口检查、系统日志检查、启动项检查等对服务器安全状况进行全面评估。

3.3 安全防护策略调优

对重点应用系统、主机、路由等相关核心资产提供立体防护措施，对已部署防御性安全设备（包括 IPS、WAF、FW）策略进行验证测试，并对防护策略进行调优，根据每个应用系统特点定制安全防御策略。

检查出的漏洞等问题须输入至金四安全管理平台漏洞处置流程，并跟踪完成闭环管理。

3.3.1 互联网边界策略

根据提供安全监测和防护策略信息，梳理互联网边界防火墙、VPN、堡垒机、WAF 等安全设备的策略配置，检查项包括策略控制粒度、特征库升级、帐号口令、日志记录等，检验策略是否遵循“最小原则”，关闭不必要的服务和端口。

3.3.2 安全域边界策略

根据提供安全监测和防护策略信息，梳理安全域边界防火墙、VPN、堡垒机、WAF 等安全设备的策略配置，检查项包括策略控制粒度、特征库升级、帐号口令、日志记录等，检验策略是否遵循“最小原则”，关闭不必要的服务和端口。

4、制定安全整改方案并实施

根据脆弱性检查和渗透测试结果，针对其中较严重的安全隐患，结合重保目标，制定有针对性的安全整改方案，以消除或减少脆弱性，降低安全风险，安全整改方案主要包括以下内容：

4.1 安全加固：对要重点保障的业务系统相关的网络设备、安全设备、操作系统、数据库以及中间件等对象的安全策略进行调整，针对不同加固对象设计不同的加固策略和方法，提高被加固对象自身的安全防护能力；

4.2 安全集成：对于部分安全问题采用部署安全产品的方式进行解决，针对技术措施、产品选型和部署进行详细设计。

5、制定应急预案

结合甲方信息安全应急响应要求，制定应急预案，建立应急响应组织以及预防、预警机制，针对信息系统特点和可能的突发性安全事件制定规范的应急处理流程。

6、安全知识讲解

定制讲解内容，提供相关教材，提高相关人员的安全意识，帮助人员熟悉相应信息安全管理机制、应急保障工作流程、网络安全防护技术等。

重保前的安全检查及整改不限于上述要求，如有需要乙方应积极采取必要措施进行安全加固。

（二）持续威胁监控及分析

1、持续威胁监测

1.1 内部持续威胁监测

乙方实时分析全网安全设备的告警日志，对常见网络威胁和未知威胁进行全面检测与分析，关联流量审计日志进行攻击行为识别。要求持续威胁监测范围覆盖互联网接入域、互联网核心、专网核心；安全监测技术应覆盖网络层、主机层、应用层等多种途径；安全监测应识别信息收集、权限获取、远程控制、数据盗取、系统破坏、木马/病毒/僵尸网络等攻击行为。

1.2 外部持续脆弱性监测

服务团队须通过部署云端监测工具，在重大活动期间对所有互联网开放业务进行 7×24 小时脆弱性扫描与监测。监测内容包括且不限于漏洞、挂马、暗链、敏感字、页面篡改等。

1.3 蜜罐或蜜网组建与维护

服务团队应根据防护需要及甲方要求，适时部署蜜罐或蜜网以应对外部威胁。

1.4 自动化导流溯源

乙方通过现有安全设施构建自动化导流溯源机制，优化现有安全措施，通过安全机制，将实际的攻击流量主动分流到水坑系统中，实现攻击溯源。

威胁监测不限于上述要求，如有需要乙方应积极配合甲方开展相应监测。

2、事件排查与溯源分析

服务团队须及时对监测到的安全事件进行深入排查分析，重保期间现场每日白天不少于 2 名安全分析师进行告警分析，每日不少于 1 名安全专家对当日触发的事件进行深入分析工作。

具体服务内容应至少包含：

2.1 厘清安全事件损害范围：分析师对安全事件进行排查，梳理安全事件的损害范围，并将受影响资产在重保支撑系统中进行标记；

2.2 判断安全防御措施有效性：分析师对安全事件进行分析排查，判断安全事件攻击路径中安全防御技术措施的有效性，并将确认结果录入至重保支撑系统中；

2.3 由服务团队提供快速抑制攻击的措施，并将抑制方法形成处置手册。

2.4 对攻击行为进行攻击溯源，找到真实攻击者，编制完整的事件报告。

（三）持续威胁防御

服务团队应积极采取各类必要工具及手段应对外部威胁，包括但不限于上述工具及手段，确保甲方各类系统不被攻破，数据不被泄露。

（四）分析与总结

在重保服务期间，乙方应根据监测及防御处置情况，每日提交分析报告，报告内容包含但不限于每日整体安全状况、事件详细信息、事件处置建议、后续改进建议等；对每次重保服务结束后，乙方应对相关工作进行总结分析，分析其取得的经验和存在的不足，形成总结报告，报告应包含但不限于事前的检测、监测、应对情况，存在的安全问题，进一步提高安全防护的意见建议等。

3.4. 服务方式要求

重大活动期间，服务团队须提供 7×24 小时现场轮流值守，不少于 4 人的值守团队，每日白天不少于 3 人，夜间不少于 1 人。为确保服务质量，值守服务人员值守前应熟练掌握甲方网络架构及网络安全设备，至少 2 人为甲方主要网络安全设备的原厂服务工程师，甲方所使用主要网络安全设备有启明星辰防火墙、深信服 WAF、瑞数动态 WAF、网域星云 IPS、天融信态势感知系统、长亭主机防护系统、360 终端安全管理系统等。具体服务人员应为乙方投标文件所投人员。

乙方在接到甲方重保活动通知后，服务团队应在 2 日内到达甲方指定地点开展工作。

发生安全事件时，现场值守人员应立即上报，并果断采取防御处置措施，重大安全事件须 30 分钟内进行现场实质性响应。

在服务期内，乙方应按照招标文件的要求，部署必要的服务支撑工具，因服务支撑工具产生的费用均包含在本项目中，甲方不另行支付。

合同签订后 7 个工作日内，完成重保服务准备工作。如迟延，乙方应承担违约责任。

（一）事件遏制与响应

1、服务团队须利用重保服务支撑工具及甲方网络环境中已具备的安全设备设施及平台针对安全威胁开展遏制工作，对攻击进行抑制、清除等快速处置操作。

2、服务团队团队须依循溯源分析结论协助业务负责人对攻击路径上的漏洞进行处置修复。

（二）持续威胁防御

1、服务团队需要结合防火墙、入侵防御系统、入侵检测系统、WEB 应用防火墙等设备进行日志审计分析，检查策略是否有效、配置是否安全，在得到授权时对相应设备的安全

防护策略进行调整。通过对事件的分析、处置、响应过程进行复盘，提取持续性威胁防御配置，发起安全策略配置变更流程，并持续监测配置变更有效性。

2、重保期间对甲方互联网区域提供同类型的安全设备（包括 IPS、WAF、防火墙）的备机。

3、服务团队应获取最新网络安全态势及预警情报，并根据最新态势和情报对相应设备快速推送适应性策略配置。

3.5. 服务流程要求

重大活动安全保障服务期间，乙方应提供完善的、可行的、闭环工作流程。

1、提供资产管理流程，资产收敛后通过重保支撑系统建立资产清单。

2、提供脆弱性管理流程，将渗透测试结果、服务器安全检查结果、漏洞扫描与重保支撑平台对接，实现从漏洞提报（导入）到处置、复测的闭环处理流程。应将脆弱性管理与资产管理相关联。

3、提供安全事件分析与处置流程，所有分析过程应通过重保支撑系统编写分析记录。应配置有效的告警确认机制，通过相应支撑系统进行任务分派，确保每条告警正常处置。

4、在进行威胁事件监测服务时，安全分析师依照分析流程开展安全分析工作，并对每个流程环节进行质量监控。要求能够根据不同的威胁事件类型进行针对性设计，细化威胁事件检测的确认过程及分析要点，将检测确认步骤拆分成固定任务，有效完成威胁事件的检测及确认工作。

5、提供重保值守报告流程，重保值守期间应通过日结方式汇总每日攻击态势形成防守日报，值守结束后应编写重保值守期间值守报告。报告内容应包含每日攻击形态、发现脆弱性、高风险事件处置报告。

3.6. 重保服务工具要求

重大活动安全保障期间，乙方应按照本项目服务要求提供的服务支撑工具。除符合服务要求外，其中部分工具要求如下：

（一）防火墙联动脚本

为更迅速响应特殊时期高风险 IP 地址的封禁，乙方应对甲方边界防火墙提供 IP 地址自动封禁脚本，脚本应能够与重保支撑平台形成联动，对识别的攻击行为采取主动封禁。

（二）动态 WAF

提供一套动态 WAF，按照重保实际需求及甲方要求进行安装部署，安装部署的动态 WAF

应不影响甲方业务正常使用与运转，同时能够满足保护 Web 应用安全的防护作用，乙方应负责协调原厂技术工程师进行现场调试，动态 WAF 应能够具备基于用户流量特征的分析能力，通过机器学习，对各类请求进行学习，生成基于用户流量的特征模型，依据特征模型进行判断，阻断不符合业务特征的流量访问，有效防范非正常访问，具备主备切换功能。

分类要求	详细说明
语义引擎	具有独立防护能力的具有自主知识产权的智能分析检测引擎。
未知威胁防护	具备 0day 漏洞防护能力，检测攻击行为特征进行，实现告警和拦截。
协议识别解码	具备 http 协议深层解码能力，支持递归解码，解码方式包括：URL 解码、JSON 解码、Base64 解码、16 进制转换、斜杠反转义、XML 解析、PHP 反序列化解析、UTF-7 解码。
攻击检测	支持反序列化攻击检测，支持 PHP、JAVA 语言的反序列化攻击检测，能够识别相关程序语言的序列化流并进行分析、解码，进行告警和阻断。 支持 CSRF 和 SSRF 检测，通过分析 Payload 代码特征，告警并阻断相关请求。
	支持 SQL 注入攻击检测，通过解析 http 协议中 payload 内容，识别符合 sql 语句的词法、语法特征，评估威胁等级并阻断；支持 SQL 非注入型攻击检测，如完整 SQL 语句执行。 支持文件上传、文件包含攻击检测；支持代码注入、命令注入攻击检测，支持检测上传文件中是否包含 Java、Php 代码注入信息；支持服务器响应信息检测，防止响应错误信息包含服务器列目录、SQL 报错、服务器异常信息等；支持 CC 攻击防护，通过限制 IP 和 Session 实现对异常访问行为的限制，并内置 Session 系统。
BOT 防护	支持以站点为配置粒度的 BOT 防护功能，支持至少 2 种验证方式，并可以将常见搜索引擎一键置白，例如：百度、谷歌、必应、360 等搜索引擎设置。
WEBshell 检测	支持 WebShell 检测功能，通过检测上传文件的语法特征和分析访问行为，检测 Web 请求是否存在上传 WebShell 或调用 WebShell 的行为，实

	现告警和阻断。
机器人检测	支持机器人检测，能够识别扫描器检测、爬虫检测、非浏览器请求。
信息泄漏检测	支持信息泄漏检测，检测内容包括测试文件、备份文件、代码仓库和服务器敏感文件等。
系统管理	提供准确有效的攻击行为分级策略，包括低危、中危和高危，在拦截日志中明确体现；攻击检测日志支持自定义筛选器功能，支持配置高级筛选规则；可根据业务特点自定义相关属性通过 OR、AND 逻辑操作组合条件进行日志查询。 支持用户登录支持双因素认证，无需外接硬件设备 支持全功能接口 Open API，可实现全功能的远程调用；API 接口需具备高强度的安全认证机制，防止非法调用。支持 SNMP 网络管理；Syslog 日志外发； 支持系统配置备份与还原；支持 PCI-DSS 合规报告导出，根据国际安全标准从 web 应用安全角度检查防护配置情况，帮助提早识别和解决业务安全配置问题。 支持对于“高危操作”的操作限制和操作提醒，例如关闭入侵检测开关、恢复出厂设置等。

（三）高级威胁检测系统

提供高级威胁检测系统一套，能够具备深层攻击检测分析能力，依据特征模型进行判断安全风险，具体应支持以下检测能力。

威胁检测	支持对恶意软件利用、可疑行为、攻击利用、攻击探测、APT 攻击事件等常见攻击类型进行检测。
	支持自定义规则进行检测，支持自定义检测规则的协议类型包括：TCP、UDP、ICMP、HTTP、SMTP、IMAP、POP3、MySQL、MSSQL、Oracle、MODBUS 等。
	自定义规则维度包括：事件名称、事件别名、事件说明、协议类型、事件级别、事件类型、影响系统、影响设备、IP 是否反转、攻击阶段、攻击状态、pcap 是否存储、自定义规则是否启用。

	自定义阶段须对应 ATTCK 战术矩阵编号，可自定义攻击阶段至少包括：发现（T1124）、侦查（T1597）、防御绕过（T1140）、执行（T1203）、命令控制（T1090）、凭证获取（T1056）、横向移动（T1210）、命令控制（T1092）、持久化（T1554）。（提供截图）
	为应对复杂的安全分析场景，设备告警事件须按照 ATT&CK 战术矩阵进行数据映射，特征告警事件须映射到 ATT&CK 战术矩阵，并具备 ATT&CK 战术矩阵视图，以提供持续狩猎和研判攻击。（提供截图）
	具备全流量检测能力，告警事件须自动给出攻击结果判定，以减少分析噪音，攻击结果包括成功、失败、正在利用等，对于告警事件须提供原始数据报文以供研判分析。
	支持对后渗透平台 C2 回连检测，包括但不限于：CobaltStrike、MSF。
	支持对常见 webshell 管理工具进行检测，包括但不限于：菜刀、冰蝎 3.0、哥斯拉、蚁剑。
	支持邮件二维码检测和钓鱼邮件算法检测。
	支持对暴力破解行为进行检测，可自定义检测周期、检测频率，支持检测的协议类型包括但不限于：HTTP、HTTPS、FTP、SSH、SMTP、IMAP、RDP、MySQL、Oracle、MSSQL、POP3、Telnet 等。
	支持对协议元数据进行识别提取，支持提取元数据的协议类型包括但不限于：TCP、HTTP、DNS、ICMP、SMTP、POP3、FTP、SMB、IP、TLS、UDP、PPTP、L2TP、MySQL、Telnet、ARP、WebMail、MSSQL、Oracle、IPSecVPN、IMAP、IPV6、RADIUS。
	支持工控协议识别解析，支持识别的协议包括：MODBUS、S7COMM、BACNET、DNP3、ENIP、IEC104、GOOSE、MMS、SV、DCERPC、OPCUA、PROFINET、RSSP。
	支持对 DNS 恶意域名请求、DGA 域名、DNS 隧道进行检测。
	支持对协议元数据进行抽样采集，可自定义检测频率、检测周期、协议类型、检测配置是否开启。

	支持对 TLS 加密流量进行检测，可通过导入证书对 TLS 流量进行解密并自动进行检测，支持协议包括但不限于：HTTPS、SMTPS、POP3S、IMAPS 等。
	支持无证书情况下 JA3 指纹识别，支持以 syslog 和 kafka 外发 JA3 日志到第三方平台。

3.7. 服务团队

乙方应根据项目投标文件约定人员提供服务，项目经理负责与甲方进行项目对接，安全专家负责分析研判重大问题并提供咨询服务，安全服务人员负责在重大时期的网络安全值守服务。未经甲方同意，乙方不得随意更换服务团队人员，确需更换的应由乙方向甲方提出书面申请，并提供更换人员的资质证明文件，最终经甲方同意后进行更换。

3.8. 其他约定

1. 乙方在本项目实施过程中发生违反网络安全规定行为，造成数据失窃或丢失，敏感信息泄露，主要业务系统瘫痪等不良后果的，自甲方或甲方主管机关做出认定之日起三年内，税务系统各单位可以拒绝乙方参加税务系统政府采购活动。

2. 乙方及乙方的工作人员不可披露甲方信息，不得另行开发合同业务需求范围内，供纳税人、缴费人使用的软件，对违反合约的，纳入失信名单。

3. 乙方应建立防止违法违规聘用离职税务人员风险控制制度，若出现，甲方将和乙方解除合同，乙方支付甲方的违约金；自甲方或甲方主管机关做出认定之日起三年内，税务系统各单位可以拒绝乙方参加税务系统政府采购活动。

4. 乙方不得以获取不正当利益为目的，采取馈赠礼品礼金、邀请娱乐旅游服务、提供便利条件等非正当手段交往相关税务人员及亲属。

5. 乙方须严格按照国家税务总局青岛市税务局相关要求落实供应链安全管理各项规定，包括按照国家相关法律法规开展的安全审查、安全评估、渗透测试等，落实情况作为项目验收的检查内容。

6. 乙方供应清单内的产品需具备销售许可并满足国家认可的网络安全规范和认证要求；乙方需签订《税务信息化供应链安全承诺书》；乙方需配合采购人落实供应链安全管理的要求，落实情况将作为项目验收的检查内容。如合同期间乙方因违反采购人供应链安全管理要求造成采购人被总局通报批评或绩效考核扣分的，采购人有权根据事件程度，按次扣

除合同金额的 5%-20%。

7. 因国家政策重大调整、系统重大变更或不可抗力等因素，采购人有权根据实际情况调整服务期限及相关合同内容，并按照调整后的实际工作量结算费用，中标人应积极配合，采购人不承担任何责任。

8. 乙方及服务人员应严格遵守甲方的信息安全保密制度和日常办公规定。乙方派驻招标方的人员必须与甲方签订保密协议。项目人员若违反保密协议造成损失，相关责任乙方承担。对于违反网络安全规定行为造成不良后果的，3 年内限制参加税务系统政府采购活动；

9. 服务人员严禁擅自操作所负责系统以外的设备，遵守内外网计算机严格隔离规定，严禁出现内网计算机违规外联情况，出现责任事故甲方有权追究投标方的责任。

10. 乙方所提供的工作人员的工作成果归甲方所有，乙方在未征得投标方书面同意的前提下，不得将技术资料泄露给其他人员及单位。如违反上述协议内容，甲方将保留追究投标方法律责任的权利。

3.9. 项目验收

项目验收主要内容：

1、重保服务日报；

2、威胁情况分析报告；

3、现场服务和远程服务工单、服务确认单；

4、阶段性小结；

5、讲解记录；

6、服务总结报告及项目验收报告；

7、供应链安全管理相关资料；

8、甲方要求的其他与项目相关的资料和文档。

4. 知识产权

4.1. 乙方应保证所提供的服务免受第三方提出侵犯其知识产权(专利权、商标权、版权等)的起诉。因侵害他人知识产权而产生的法律责任，全部由乙方承担。

4.2. 甲方委托乙方开发的产品，甲方享有知识产权，未经甲方许可不得转让任何第三人。

5. 保密条款

5.1. 甲乙双方应对在本合同签订或履行过程中所接触的对方信息，包括但不限于知识产权、技术资料、技术诀窍、内部管理及其他相关信息，负有保密义务。

5.2. 乙方及服务人员应严格遵守甲方的信息安全保密制度和日常办公规定，乙方在使用甲方为乙方及其工作人员提供的数据、程序、用户名、口令、资料及甲方相关的业务和技术文档，包括税收政策、方案设计细节、程序文件、数据结构，以及相关业务系统的硬软件、文档、测试和测试产生的数据时，应遵循以下规定：

(1)应以审慎态度避免泄露、公开或传播甲方的信息；

(2)未经甲方书面许可，不得对有关信息进行修改、补充、复制；

(3)未经甲方书面许可，不得将信息以任何方式(如E—mail)携带出甲方场所；

(4)未经甲方书面许可，不得将信息透露给任何其他人；

(5)甲方以书面形式提出的其他保密措施。

5.3. 保密期限不受合同有效期的限制，在合同有效期结束后，信息接受方仍应承担保密义务，直至该等信息成为公开信息。

5.4. 甲乙双方如出现泄密行为，泄密方应承担相关的法律责任，包括但是不限于对由此给对方造成的经济损失进行赔偿。

5.5. 按照国家税务总局、青岛市税务局关于建立信息系统服务外包运维人员背景审查机制、以及关于加强税务信息化供应链安全管理工作的要求，乙方以及乙方项目组人员须签署网络安全承诺书、保密协议、信息系统服务外包运维人员基础信息备案表、信息系统服务外包运维人员清册、提供运维人员无犯罪记录证明等并加盖公章，同时指定一名网络安全负责人。项目人员若违反保密协议造成损失，相关责任由乙方承担。对于违反网络安全规定行为造成不良后果的乙方，3年内限制参加税务系统政府采购活动。

6. 服务质量保证

6.1. 乙方应保证所提供的服务，符合合同规定的技术要求。如不符时，乙方应负全责并尽快处理解决，由此造成的损失和相关费用由乙方负责，甲方保留终止合同及索赔的权利。

6.2. 乙方应保证通过执行合同中全部方案后，可以取得本合同规定的结果，达到本合同规定的预期目标。对任何情况下出现问题的，应尽快提出解决方案。

6.3. 如果乙方提供的服务和解决方案不符合甲方要求，或在规定的时间内没有弥补缺陷，甲方有权采取一切必要的补救措施，由此产生的费用全部由乙方负责。

7. 服务时间、地点与验收

7.1. 服务地点：合同条款前附表指定地点。

7.2. 服务时间：合同条款前附表指定时间。

7.3. 甲方应在乙方完成相关服务工作后及时对服务质量、技术指标、服务成果进行验收，并出具验收意见书。

7.4. 验收意见书为乙方申请甲方付款时所必需的文件的组成部分。若验收意见为部分合格或不合格的，甲方有权拒绝付款。同时，乙方还应按甲方意见及时进行整改及承担违约责任。

8. 违约责任

8.1. 服务缺陷的补救措施和索赔

(1)在服务期间，如因乙方未尽到网络安全保障义务，造成甲方被上级部门通报相关问题，每次扣除合同金额的2%-5%；造成甲方各类系统、平台及网络安全设备等权限被控或在重大活动中造成甲方失分，甲方将根据事件的严重程度，每次扣除合同金额的5%—10%；造成甲方网络边界被突破，目标系统或服务器被控、数据泄露、页面篡改等问题，甲方将根据事件的严重程度，每次扣除合同金额的10%—20%；造成甲方被绩效考核扣分的，扣除合同金额的20%。

(2)累计扣除金额达到10%时，乙方应及时调整重保服务团队人员，提高保障能力和水平，尽力弥补过失，继续做好重保服务。累计扣除金额达到20%时，视为乙方不能满足招标要求，甲方有权终止合同，不再支付合同剩余金额。如因甲方原因导致的上述问题，乙方应积极配合甲方消除问题影响，并提供非乙方过失的证据。

(3)如果在甲方发出违约扣款通知后10日内乙方未作答复，上述通知应视为已被乙方接受。如果乙方未能在甲方发出通知后10日内或甲方同意延长的期限内，按照上述规定的任何一种方法采取补救措施，甲方有权从应付服务款中扣除相应的金额，如不足以弥补甲方损失的，甲方有权进一步要求乙方赔偿。

(4)如合同期间乙方因违反甲方供应链安全管理相关要求造成甲方严重损失的，甲方有权终止合同，并根据事件严重程度，按次扣除合同金额的2%-10%。

8.2. 迟延履约的违约责任

(1)乙方应按照本合同规定的时间、地点提供服务。

(2)在履行合同过程中，如果乙方遇到可能妨碍按时提供服务的情形时，应及时以书面形式将迟延的事实、可能迟延的期限和理由通知甲方。甲方在收到乙方通知后，应尽快对情况进行评价，并确定是否同意延期提供服务。

(3)除甲乙双方另有约定外，如果乙方没有按照合同规定的时间提供服务，且没有在甲方同意的延长的期限内进行补救时，甲方有权从服务款中扣除或要求乙方另行支付误期赔偿费而不影响合同项下的其他补救方法。赔偿费按每日加收合同金额的 0.5%计收，直至交货或提供服务为止。

(4)如果乙方延迟履约超过 30 日，甲方有权终止全部或部分合同，并依其认为适当的条件和方法购买与未履约类似的服务，乙方应负担购买类似服务所超出的费用。但是，乙方应继续执行合同中未终止的部分。

8.3. 未履行合同义务的违约责任

(1)守约方有权终止全部或部分合同，违约方应向守约方支付合同总额 20%违约金，并赔偿由此给守约方造成的全部损失。

8.4 其他违约责任

(1)乙方迟延履行本合同约定的各项义务或履行义务不符合合同约定或甲方要求的，甲方有权暂时不支付服务费，直至乙方履行合同义务符合约定为止。

(2)甲方因乙方违约选择终止或解除本合同，乙方除应退还已收取的费用外，还应当向甲方支付合同总额 20 %的违约金，并赔偿给甲方造成的损失（包括但不限于直接损失、间接损失、第三方索赔损失、律师费、诉讼费等）

(3)违约金不足以弥补守约方实际损失、可预见或者应当预见的损失，由违约方全额予以赔偿。本合同所称全部损失，包括但不限于：直接损失、预期利益、委托第三方完成的费用、第三方索赔损失及调查取证费、诉讼费、律师费等。

9. 不可抗力

9.1. 如果合同双方因不可抗力而导致合同实施延误或合同无法实施，不应该承担误期赔偿或不能履行合同义务的责任。

9.2. 本条所述的“不可抗力”系指那些双方不可预见、不可避免、不可克服的客观情况，但不包括双方的违约或疏忽。这些事件包括但不限于：战争、严重火灾、洪水、台风、地震等。

9.3. 在不可抗力事件发生后，当事方应及时将不可抗力情况通知合同对方，在不可

抗力事件结束后3日内以书面形式将不可抗力的情况和原因通知合同对方，并提供相应的证明文件。合同各方应尽可能继续履行合同义务，并积极寻求采取合理的措施履行不受不可抗力影响的其他事项。合同各方应通过友好协商在合理的时间内达成进一步履行的协议。

10. 合同纠纷的解决方式

10.1. 合同各方应通过友好协商，解决在执行合同过程中所发生的或与合同有关的一切争端。如协商30日内(根据实际情况设定)不能解决，可以按合同规定的方式提起仲裁或诉讼。

10.2. 仲裁裁决应为最终裁决，对双方均具有约束力。

10.3. 仲裁费除仲裁机关另有裁决外应由败诉方负担。

10.4. 诉讼应由甲方在地人民法院管辖。诉讼费除人民法院另有判决外应由败诉方负担。

10.5. 如仲裁或诉讼事项不影响合同其他部分的履行，则在仲裁或诉讼期间，除正在进行仲裁或诉讼的部分外，合同的其他部分应继续执行。

11. 合同修改或变更

11.1. 如无重大变故，甲乙双方不得擅自变更合同。

11.2. 如确需变更合同，甲乙双方应签署书面变更协议。变更协议为本合同不可分割的一部分。

11.3. 在不改变合同其他条款的前提下，甲方有权在合同价款10%的范围内追加与合同标的相同的货物或服务，并就此与乙方签订补充合同，乙方不得拒绝。

12. 合同中止

12.1. 合同在履行过程中，因采购计划调整，甲方可以要求中止履行，待计划确定后继续履行；合同履行过程中因供应商就采购过程或结果提起投诉的，甲方认为有必要或财政部责令中止的，应当中止合同的履行。

13. 违约终止合同

13.1. 若出现如下情况，在甲方对乙方违约行为而采取的任何补救措施不受影响的情况下，甲方可向乙方发出书面通知书，提出终止部分或全部合同。

13.1.1. 如果乙方未能在合同规定的期限或甲方同意延长的期限内提供服务；

13.1.2. 因乙方技术人员自身技术能力、经验不足等原因造成甲方硬件设备、应用

系统发生重大紧急故障或应用系统数据丢失，带来重大影响和损失的；

13.1.3. 乙方对甲方硬件设备、应用系统重大紧急故障没有及时响应，或不能在规定时间内解决处理故障，恢复系统正常运行的；

13.1.4. 不能满足本项目技术需求的管理要求和规范，且经多次整改无明显改进的；

13.1.5. 在合同规定的每个服务年度(12 个自然月)内，在运行维护支持服务过程中，出现 2 次经甲乙双方确认的违规操作的。

13.2. 如果甲方根据上述第 13.1 条的规定，终止了全部或部分合同，甲方可以适当的条件和方法购买乙方未能提供的服务，乙方应对甲方购买类似服务所超出的费用负责。同时，乙方应继续执行合同中未终止的部分。

14. 破产终止合同

14.1. 如果乙方破产或无清偿能力，甲方可在任何时候以书面形式通知乙方终止合同而不给乙方补偿。

14.2. 该终止协议将不损害或影响甲方已经采取或将要采取的任何行动或补救措施的权利。

15. 其他情况的终止合同

15.1. 若合同继续履行将给甲方造成重大损失的，甲方可以终止合同而不给予乙方任何补偿。

15.2. 乙方在执行合同的过程中发生重大事故，对履行合同有直接影响的，甲方可以终止合同而不给予乙方任何补偿。

15.3. 甲方因重大变故取消或部分取消原来的采购任务，导致合同全部或部分内容无须继续履行的，可以终止合同而不给予乙方任何补偿。

16. 合同转让和分包

16.1. 乙方不得以任何形式将合同转包，或部分或全部转让其应履行的合同义务。

16.2. 除经甲方事先书面同意外，乙方不得以任何形式将合同分包。

17. 适用法律

17.1. 本合同适用中华人民共和国现行法律、行政法规和规章，如合同条款与法律、行政法规和规章不一致的，按照法律、行政法规和规章修改本合同。

18. 合同语言

18.1. 本合同语言为中文。

18.2. 双方交换的与合同有关的信件和其他文件应用合同语言书写。

19. 合同生效

19.1. 本合同应在双方签字盖章后生效。

20. 合同效力

20.1. 除本合同和甲乙双方书面签署的补充协议外，其他任何形式的双方约定和往来函件均不具有合同效力，对本项目无约束。

21. 检查和审计

21.1. 在本合同的履行过程中，甲方有权对乙方的合同履约情况进行阶段性检查，并对乙方投标时提供的相关资料进行复核。

21.2. 在本合同的履行过程中，如果甲乙双方发生争议或者乙方没有按照合同约定履行义务，乙方应允许甲方检查乙方与实施本合同有关的账户和记录，并由甲方指定的审计人员对其进行审计。

22. 通知

双方均保证本合同所载的联系地址真实有效，保证对方或司法机关按该地址邮寄或送达的邮件或物品均能送达本方，若出现拒收、代收、退回等情况，均视为已送达本方。如因争议纠纷诉至法院的，双方确认以本合同所示地址为诉讼公文的有效送达地址。任何一方更改地址应在七日之内以书面形式通知对方，否则应自行承担通知不能的不利法律后果。