

我司因网络安全建设需要，对网络安全运维服务项目进行公开询价，欢迎有意向的供应商参与，现将有关事项公告如下：

一、项目概况与询价范围

- 1、询价人：山西天地煤机装备有限公司
- 2、服务地点：山西省太原市小店区科荟路1号/山西省太原市小店区电子街1号
- 3、服务期：由报价单位根据询价约定耗材及服务费用（服务开始时间为：服务签订后开始计算）。
- 4、技术要求：与询价人的技术联系人沟通
- 5、询价内容

序号	服务项目	服务类别	服务内容	次数	单价	报价
1	安全监测、事件上报专项	MSS托管式安全运营	<p>1.为20个核心业务资产提供全年的7*24小时安全托管运营服务；</p> <p>2.资产管理服务：基于态势感知或终端安全发现的资产，结合用户提供的资产台账，为资产的重要性进行分级打标；</p> <p>3.互联网暴露面检测服务1年2次：运营专家在用户提供的根域名、IP等信息的基础上，对用户在互联网上暴露的IP资产、域名、资产指纹等信息进行搜集，并在人工检查整理后输出报告。</p> <p>4.互联网漏洞扫描与管理服务1年4次：运营专家通过互联网扫描引擎对服务范围内互联网资产进行漏洞扫描并完成验证，持续跟踪修复情况。用户可在租户界面看到相关进展，实现漏洞全生命周期管理。</p> <p>5.服务范围内资产威胁监测与分析服务1年：运营专家通过云端安全托管运营平台对服务内资产提供7*24小时威胁监测，分析各项安全隐患，包括漏洞利用、弱密码、挖矿、Webshell写入、异常登录、木马回连等安全风险，并通过企业微信、服务号等方式告知用户。</p> <p>6.服务范围内资产安全事件处置服务1年：针对服务范围内资产，运营专家发现安全事件后，在获取用户授权后开展安全处置工作，通过运营服务平台联动对同厂商网络防火墙、EDR实现查杀、封锁联动处置工作。</p> <p>7.服务范围内资产应急响应服务1年：针对服务范围内资产，对发生的勒索病毒、黑客入侵成功事件、数据篡改等高危害安全事件，运营专家通过远程支持的形式协助用户对遇到的突发性安全事件进行紧急分析和协助处置。</p> <p>8.服务组件策略定期升级服务1年4次：在服务组件维保期内，运营专家每季度对同厂商运营组件（如：态势感知、终端安全）上的安全策略进行统一更新，确保运营组件上的安全策略、规则库版本、设备版本处于阶段性最优水平。</p> <p>9.情报订阅服务：服务期间提供《全球重要漏洞预警报告（触发）》、《网络安全月刊》、《网络安全攻防周刊》</p> <p>10.阶段汇报服务1年2次：每半年度安全运营经理现场进行阶段汇报，确认是否调整服务资产，沟通后续运营重点工作。</p> <p>11.服务交付物：《互联网暴露面检测报告》、《漏洞扫描报告》、《应急响应报告》、《漏洞预警报告》、《网络安全月刊》、《攻防资讯报告》、《季度汇报PPT》、《年度汇报PPT》。</p>	全年		
2		新建项目上线前策略检查	<p>1.上线前对服务器、中间件等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。本服务不纳入重保专项服务。</p> <p>2.服务交付物：《系统上线安全配置检测报告》</p>	1次		
3		漏洞风险扫描	<p>1.定期对资产对漏洞扫描，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，并按照甲方要求，协助完成补丁更新及漏洞修复，内容包含应用资产、服务器资产、数据库资产、网络设备资产等。本服务不纳入重保专项服务。</p> <p>2.服务交付物：《漏洞扫描报告》、《漏洞整改报告》。</p>	1次		
	安全	互联	1.梳理互联网暴露面，针对公网上资产、边缘资产进行排查，协助甲方完成加固处			

4	运维专项	网暴露面	置。 <u>本服务不纳入重保专项服务。</u> <u>2.服务交付物：《互联网暴露面检测报告》、《互联网暴露面整改报告》。</u>	1次		
5		安全配置检查	1.定期对资产对应用资产、服务器资产、数据库资产、网络设备资产等的安全配置进行检查，并按照甲方要求，协助完成安全配置的加固。 <u>本服务不纳入重保专项服务。</u> <u>2.服务交付物：《安全配置检测报告》、《安全配置整改报告》。</u>	1次		
6		弱口令专项	1.信息化资产及信息化系统不同应用弱口令猜解检测，如：SAP、OA、SRM、WMS、CRM、QMS、售后服务系统、SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat等业务系统。针对不同行业提供行业密码字典，有针对性的进行内网弱口令检测。 <u>本服务不纳入重保专项服务。</u> <u>2.服务交付物：《弱口令专项检测报告》。</u>	1次		
7	应急响应服务专项	安全事件响应	1.提供7x24小时的原厂应急技术支持服务，并明确联系人和联系方式； 2.遇到突发的安全问题如：大规模病毒爆发、网络入侵事件、拒绝服务攻击、主机或网络异常事件、网络攻击事件、挂马事件、网页篡改事件、网络钓鱼事件、信息泄露事件、APT事件等，无法及时对该事件进行处理或解决时，在收到客户的应急响应服务请求的告警信息后，技术专家2小时内赶到现场，协助系统管理人员查明安全事件原因，确定安全事件的威胁和破坏的严重程度，解决出现问题。 <u>3.服务交付物：《应急处置报告》。</u>	1次		
8	应急演练专项	安全场景应急演练	1.协助客户完成应急演练工作，协助制定或完善相应应急演练预案或应急规范，并根据实际环境，提供专项预案，准备演练场景，以模拟演练的方式检验应急预案和应急流程是否完善，提高应急处理能力。 <u>2.服务交付物：《应急演练预案》、《应急规范》、《应急演练总结报告》。</u>	1次		
9	重要时期保障服务专项	重保服务	1.在重大节假日、重大活动期间，以及其他专项工作期间，制定专项保障服务措施及方案，对业务应用系统运行状况进行实时监控，对网络安全进行全面保障。并制定出符合实际情况的专项保障服务方案，方案包括渗透测试、安全配置加固、安全监测、应急响应等四项服务，按方案进行实施安全保障工作，输出安全保障报告。提供远程支持和现场支持两种方式，提供原厂线上7*24小时应急响应服务，按照甲方要求响应现场服务。 <u>2.服务交付物：《资产梳理报告》、《专项漏洞检查与修复》、《漏洞扫描报告》、《协助加固报告》、《安全防护日报》、《安全值守日报》、《应急响应报告》、《安全事件处置报告》、《重保服务总结报告》、《复盘培训》。</u> <u>3.重保服务专项付款条件：重保期间内，依据攻防演练的评判标准，按照沦陷资产条数，每条沦陷资产扣除重保专项服务资金的5%。</u>	15人天		
10	安全意识培训专项	安全意识培训	1.提供信息安全意识培训，安全意识培训旨在提升企业内部员工安全认知，让员工认识到信息安全意识不足对组织可能造成的危害，传导应正确恪守的行为方式；通过全员安全意识的理论培训和案例分析以及关键行为上的最佳实践指导，让信息安全“人防”保障有效支撑业务高效稳定运行。培训内容包括普通员工的上网安全、邮件安全、通信安全等常见的安全意识内容。 <u>2.服务交付物：《网络安全培训PPT》。</u>	1次		

表中按次数计费项目单独根据实际发生次数计费，未发生不计费。

6、报价截至时间：2023年7月3日至2023年7月8日

二、供应商资格要求

本次询价实行资格预审，供应商应满足下列资格条件：

1、必须是中华人民共和国境内注册的具有独立法人资格的企业，本次招标内容必须在其经营范围内并具备国家、行业要求的相关资质；

2、负责人、主要股东为同一人或者存在控股、管理关系的不同单位不得参与本次投标；

3、具有良好的商业信誉，被列入失信企业“黑名单”或者发生过严重违约行为的企业不得参与本次投标；

4、近三年内在经营活动中没有重大违法记录；

5、本项目不接受联合体投标。

三、联系方式

询价人：山西天地煤机装备有限公司

地址：山西省太原市小店区科荟路1号

经办人：邢志伟 联系电话：0351-7685077

技术联系人：冯杰 联系电话：18835112912

