

## 采购内容及要求

服务类型	名称	服务描述	单位	数量
网络安全 应急演练	演练方案编制	提供关键信息基础设施网络安全事件应急演练 1 次。编制网络安全应急演练方案，演练方案要通过模拟真实事件及应急处置过程、全方位多角度模拟突发网络安全重大事件的应对全流程，检验关键信息基础设施运营者、网络安全应急技术服务队伍等多方协调联动工作机制，切实落实网络安全责任制，加强信息报告和共享，全面提升网络安全保障应急能力。	项	1
	演练靶机搭建 服务	1、进行靶机的搭建和调试，准备攻击机器人和攻击工具，在演练服务器上部署两台虚拟机，进行模拟攻击。 2、服务商需负责整个应急演练场地平台搭建，包括但不限于会场布置、桌椅、台签摆放等会场布置相关工作。 3、服务商需负责应急演练场地的设备上架、网络布线、弱电部署等相关工作。 服务商负责应急演练相关的设备部署、调试、优化、测试等相关工作。		

	应急演练复盘	通过应急演练，发现应急预案中存在的问题，在突发事件发生前暴露预案的缺点，验证预案在应对网络安全突发事件所具备的适应性、有效性、完善性等，系统地检验应急工作机制是否完善，找出预案需要进一步完善和修正的地方。对演练结果进行全面复盘，总结应急预案以及防护手段，并编写：《网络安全应急演练总结报告》。		
关键信息基础设施网络安全检查 技术支撑服务	服务内容	对全市关键信息基础设施、重要业务系统、核心网络系统安全运行管理情况进行安全检测及技术评估、按照相关要求对网络安全和技术措施进行检查，全面准确地指出存在的问题和漏洞，列出整改清单，形成完整的整改方案及意见。	月	6
	检查工具箱	服务商提供的检查工具箱需列装公安部检查工具目录（提供相关做证明文件），具备检查报表系统、现场处理、用户管理、系统自身管理；内置工具软件包含：网站安全检查、数据库安全扫描、Windows 主机安全配置检查、Linux 主机安全配置检查、网络设备安全配置检查、SQL 注入验证检查、网站恶意代码检查、主机病毒检查、主机木马检查、弱口令检查、系统漏洞检查等功能，提供相关功能的技术说明。		
网络安全培训服务	服务内容	服务商提供每年 2 次网络安全相关的培训服务，需负责整个培训会议的场地租赁及大屏搭建，包含会场布置、桌椅、台签摆放等会场布置相关工作。每次培训需邀请 2 名副教授以上的网络安全领域的相关专家教授，并承担培训老师的授课费，差旅费、住宿及餐费，同时承担场地费及参加培训人员住宿及餐费。（标准不低于《陕西省省直机关差旅费管理办法》）	项	1
网站云监测服务 及	网站云监测	提供网站云监测服务并提供以下内容：对 500 个站点提供监测服务漏洞扫描、违规内容监测、网页挂马监测、内容变更监测、黑链监测、网站可用性监测，并每月提供安全监测报告。	月	6

<b>网络安全威胁情报服务</b>	威胁情报	提供基于大流量监测，实现威胁情报与大数据分析能力服务。同时结合主动防御机制上报的恶意线索信息，实现对甲方指定区域内网络空间威胁的全天候监测，实时输出威胁事件记录与失陷主机信息，帮助用户及时发现区域关键威胁。		
<b>漏洞测试验证服务</b>	服务内容	提供远程漏洞扫描及高危漏洞人工验证，提供威胁情报检测引擎，主要用于感知分析全市在线和离线环境下基于威胁情报检测和发现，可检测威胁类型包括：APT 攻击、远控木马、蠕虫木马、僵尸网络、勒索软件、挖矿、黑客利用 EXP 等。提供漏洞数据服务。提供全市重点单位的相关漏洞：包括漏洞标题、漏洞所属单位名称、域名、URL、漏洞详情、漏洞等级、漏洞类型等。提供漏洞审核验证服务。	月	6
<b>资质要求</b>		<p>★1.具有《网络安全等级测评与检测评估机构服务认证证书》；</p> <p>★2.服务商应具有信息安全服务（安全工程）能力证明；</p> <p>★3.具有中国网络安全审查技术与认证中心颁发的二级信息安全风险评估资质；</p> <p>★4.具有中国网络安全审查技术与认证中心颁发的二级信息安全应急处理资质；</p> <p>注：“★”项参数不允许负偏离，否则视为无效响应。并提供相关证明材料。</p>		