2025年网络安全服务项目招标项目需求

说明：

1、投标人须对同一采购项目为单位的服务进行整体响应，任何只对其中一部分内容进行的响应都被视为无效投标。

2、招标项目需求中打“★”号条款为实质性条款，投标人如有任何一条负偏离则导致投标无效。

3、招标项目需求中打“▲”号条款为重要技术条款，负偏离不作为无效投标条款。

一、项目背景

为落实深圳市党委（党组）网络安全工作责任制考核、市委网信办网络数据安全专项检查等工作要求，排查深圳市人力资源和社会保障局信息系统风险隐患，封堵深圳市人力资源和社会保障局信息系统安全漏洞，加强构建与深圳市人力资源和社会保障局数字人社建设相适应的网络安全体系，保障业务系统安全稳定运行，筑牢安全防线，特公开招标“深圳市人力资源和社会保障局2025年网络安全服务”项目。

二、具体技术要求

（一、）服务内容及要求

1、漏洞扫描

（1）服务期内，每月对采购人指定的网站、信息系统、服务器、数据库、网络设备、安全设备、终端等进行漏洞扫描，全方位检测采购人网络、信息系统及WEB应用潜在的各类脆弱性风险隐患，生成漏洞扫描报告。根据扫描结果制定安全修复加固方案，协助采购人修复漏洞，复核确认漏洞修复情况。

（2）在采购人新业务系统上线前，使用扫描工具对采购人的网络环境、主机环境、安全设备配置、应用程序等多个层面进行安全评估和安全检测，全面发现系统潜在的安全防护弱点，协助采购人修复加固，保障系统上线后安全稳定运行。

（3）对服务期内发现的安全漏洞类型、频率、修复方案进行总结，形成总结报告作为信息系统开发运维参考材料。

2、渗透测试

服务期内，每季度组织一次模拟黑客入侵的人工渗透测试服务，对采购人统一建设、维护的网站和信息系统进行渗透测试，如遇重大安全保障防护期，需提前对相关系统进行渗透

测试。渗透测试需结合白盒测试、外网测试等多种模式，利用主流的攻击技术，对采购人指定的信息系统进行非破坏性质的渗透测试。具体要求如下：

（1）详细分析渗透测试所带来的次生风险，主动规避渗透测试中的次生风险，确保不因渗透测试带来新的业务连续性风险问题。

（2）进行渗透测试时，协助采购人做好应急预案和演练，一旦发生安全事件尽快按照应急预案恢复业务应用。

（3）完成渗透测试后，需出具全面的渗透测试报告，明确风险漏洞等级并提供有效可行的解决建议。

（4）在各系统完成整改后，对相应的漏洞进行回归测试并提供复测报告。

（5）汇总分析渗透测试、回归测试报告，总结采购人各系统在渗透测试中发现的主要问题、风险等级、整改建议等，形成渗透测试总结报告。

（6）每季度发现不少于 10 个中高风险系统漏洞（漏洞级别参照<GB/T30279-2020 信息安全技术 网络安全漏洞分类分级指南>），并提供渗透测试报告。

（7）可按照采购人实际需要委派渗透测试工程师，如为更全面发现信息系统风险隐患，采购人可要求多次渗透测试委派非同一组织或同一团队人员；为更深入发现某系统风险隐患，采购人可要求针对特定系统多次渗透测试指派相同人员。

★（8）为保障服务质量，投标方需提供一套渗透测试工具，用于系统渗透测试。

3、代码审计

（1）服务期内，按采购人需求对相关信息系统进行代码审计，出具审计报告及修复建议，并协助采购人完成漏洞修复整改工作。采购人通常会在系统第一次上线、系统存在较大代码变动、重点防护期等情况发生时提交代码审计需求。

★（2）为保障服务质量，投标方需在采购人机房部署一套源代码安全缺陷分析工具，免费使用一年，用于信息系统代码审计。

4、安全监测预警

服务期内，提供 7×24 小时对威胁事件的实时监测、快速分析研判、主动的处置闭环管理，以提升威胁响应效率降低安全风险。具体要求如下：

（1）威胁预警。对紧急漏洞、安全事件进行预警与响应，含漏洞/安全事件的预警、攻击日志确认、日志回溯，针对受影响情况提供处置建议并跟踪闭环。

（2）威胁监测。使用流量探针采集采购人的出入口网络流量及内部信息系统间的水平

交互网络流量，通过威胁检测与分析工具，对登录行为、服务器危险行为、可疑 DNS 解析行为、威胁告警等进行大数据分析，快速发现威胁事件。基于威胁情报进行威胁检测，及时有效地发现 APT 事件、僵尸网络、勒索软件、流氓推广、窃密木马、网络蠕虫、远控木马、黑市工具、其他恶意软件等威胁事件。

（3）威胁分析。配置一名全职驻场专家对所有网络安全设备采集的数据进行安全日志分析与安全事件发现，及时感知用户网络系统中的安全事件并提出解决方案，输出告警深度分析、爆破行为分析、恶意邮件行为分析、数据库行为分析、WEB 攻击分析等安全日志分析报告。

（4）威胁处置。对发现的威胁事件，根据采购人业务实际情况提供有效的处置建议，采用一键封堵、策略调优、人工封禁等措施抑制或消除事件影响。

（5）策略优化。持续优化监测平台、设备的安全策略，提高检测的覆盖度、准确度，提高分析效率。实时监控采购人信息系统安全防护边界的安全设备，定期评估并优化安全设备的准入策略。

★（6）为保障服务质量，投标人需在采购人机房部署一套具有公安部销售许可证的威胁检测与分析系统，对采购人网络进行全流量监控，免费使用一年。（需提供公安部销售许可证证书或者提供具备资格的机构安全认证合格或安全检测符合要求的相关证明材料，其中具备资格的机构是指列入《承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录》的机构）。

5、网站实时监控

对采购人指定网站提供 7×24 小时安全事件监测发现与预警通告服务。定期出具网站安全综合评估报告，提供专业可行的修复建议，协助采购人进行安全整改，并复核确认整改情况。具体要求如下：

（1）网站可用性监控

域名劫持监控：动态解析域名所对应的 IP 地址，一旦发现所解析出来的 IP 地址与预先设定的值不相符则发出告警。

网站可用性监控：实时监控 HTTP/HTTPS 网站域名可访问情况发现问题实时预警，所监控的异常类型包括 DNS 解析异常、协议错误、URL 不合法、无路由器跳转到主机、socket 连接请求被拒绝等 12 种类型。

全网性能分析：通过多点探头，对网站的 DNS 解析、建立链接、服务器计算、内容下载等性能指标进行分析。

全网可用性监控：通过在不同地区、不同运营商（电信、联通、移动）的网络中部署监控探头，来发现不同网络出口的访问状况，如DNS解析地域差异、多链路出口差异等问题，发现问题实时预警。

监控频率：不超过10分钟间隔。

预警方式：能够通过短信、邮件、电话等方式预警。

（2）网站安全性监控

网页挂马监控：利用丰富的挂马特征库对网页中存在的木马、病毒、恶意脚本等恶意代码进行定性分析和预警。

网站资源监控：利用搜索引擎技术，通过所配置的频率对网页进行循环扫描，将网站页面抓取到监控系统进行增量式存储，对网站静态页面（html、htm等）、脚本（包括css、javascript、vbscript等）、图片、可执行文件（如EXE文件、activeX控件等）及网站其他资源进行统计分析。监控范围包括网站内部资源（本域名下的资源）和网站外部资源（非本域名下的外链）。

监控频率：不超过60分钟间隔。

预警方式：能够通过短信、邮件、电话等方式预警。

6、信息安全风险评估

（1）风险识别。对采购人信息资产进行梳理，并参考相关标准对资产进行分类，识别重要信息资产，形成资产清单。对已识别重要资产，分析资产的保密性、完整性和可用性等安全属性的等级要求，并根据分析结果综合评定进行赋值。对已识别资产进行脆弱性识别、威胁识别、现有安全措施分析，了解已识别资产的脆弱性、潜在安全风险及已采取安全措施的有效性。

（2）风险分析。建立风险分析模型，对已识别资产的威胁、脆弱性及安全措施进行分析，确定风险等级，并出具风险评估报告，报告应包括但不限于评估过程、评估方法、评估结果、处置建议等内容。

（3）风险处置。根据风险评估报告及采购人实际情况，协助采购人对采购人不可接受风险进行修复。

7、互联网攻击面管理

以攻击者视角监控采购人、相关直属单位及其供应链暴露在互联网侧的泛资产及其关联的外部攻击点，主动映射攻击面，分析并预测易被攻击者利用的安全风险，及时进行风险预警，协助采购人完成风险处置闭环。具体要求如下：

（1）资产梳理。通过采购人提供的相关信息对采购人互联网信息资产进行核查和识别，提供资产清单，同时标记和确认未知资产、告警和提醒、资产变化监测。

（2）资产暴露面风险探测。定期对端口服务风险、主域名风险、IP 风险、移动端资产风险等资产暴漏面风险进行探测并人工验证后，告知并协助采购人及时处置风险。

（3）社工风险探测。通过扫描论坛、黑市交易平台和非法数据交换区域等，快速识别出是否存在个人信息的非法流通和交易行为，对个人信息泄露进行探测和防范。一旦发现风险，立即向采购人发送警报和通知，同时提供详细报告，包括泄露来源、泄露的个人信息类型以及相关建议，帮助采购人迅速应对和解决问题。

（4）编制服务报告。根据资产梳理及风险探测情况，汇总相关数据，形成包含全部资产和风险数据的服务报告，并提供风险处置建议，帮助采购人全面了解、处置资产风险。

8、实战攻防诱捕

基于网络欺骗和主动防御理论，组建具有迷惑、诱捕、监控能力的“欺骗防御体系”，加强安全防御措施的主动性，为采购人提供准确的攻击者情报与反制溯源能力。当攻击者绕过或突破防御措施时，对攻击行为进行捕获和分析，了解攻击者使用的攻击与方法，推测攻击意图和动机，让采购人清晰地了解所面对的安全威胁。具体要求如下：

（1）伪装诱捕。根据采购人需求，在安全检查或重保期间，通过操作系统类蜜罐、Web 类蜜罐、数据库类蜜罐、物联网类蜜罐、中间件类蜜罐、系统服务类蜜罐、综合型服务蜜罐以及 5G 网元仿真等进行伪装诱捕。通过在线制作反制型蜜饵，对反制对象进行命令控制、上传下载文件、截屏、录像、敏感信息收集等操作。

（2）威胁分析溯源。分析针对采购人蜜罐/蜜饵的所有攻击行为，包括扫描、探测、入侵尝试等，分析攻击者相关信息，了解攻击者意图，识别攻击者使用的攻击方法和工具，明确相关攻击行为的命中情况等。

（3）安全加固。针对攻击行为及攻击手段，为采购人制定针对性的防御措施，协助采购人消除盲点，发现更多潜在漏洞，查漏补缺，进一步加固相关信息系统。

9、协助自查及直属单位、指定行业单位开展安全检查服务

（1）按采购人年度网络安全自查及直属单位检查工作要求，协助制定网络安全检查指标、检查方案。

（2）协助采购人根据市党政机关网络安全联合检查和绩效考核工作要求，按需开展网络安全自查迎检工作，严格按照检查内容和评分指标进行自查自纠，防止在检查和考核中失

分被相关监管单位通报。

（3）协助采购人对相关直属单位进行网络安全检查，根据检查情况编制检查报告，明确检查发现问题及整改措施，指导相关单位按要求整改，并对整改结果进行复核。

（4）根据业务需要，协助采购人对指定的相关行业单位进行网络安全检查，根据检查情况编制检查报告，明确检查发现问题及整改措施，指导相关行业单位按要求整改，并对整改结果进行复核。

10、重要时期安全保障服务

在服务期内的重大保障时期，加强驻场和人力保障，确保业务系统安全运行，避免敏感事件或影响业务的安全事件发生。重大保障时期包括两会、国庆等重点时期，深蓝、粤盾、粤网安、攻防演练期等国家、广东省或深圳市要求的特殊防护期，重大保障工作包括但不限于以下内容：

（1）根据重保时期的工作要求或安全主管单位的具体要求，协助制定重保时期网络安全工作方案。

（2）重保期间，充分利用采购人现有安全设备，协助开展攻击行为检测与分析，快速响应及处置，抑制攻击事件，顺利完成重保。

（3）重保期间，按需提供 7*24 小时安全服务工程师驻场及远程安全技术专家服务，随时按要求进行驻场防守和应急处置，配合做好重保、攻防演练期间的网络安全防护工作。

（4）完成重保工作后，分析总结经验教训，输出重保时期安全防护总结报告。

11、应急体系建设与演练服务

协助采购人完善应急体系，针对突发的网络安全事件提供 7×24 小时应急响应服务，具体要求如下：

（1）协助采购人修订应急预案；

（2）按照深圳市常态化攻防演练活动的标准要求及采购人网络安全实战攻防演练服务需求，至少组织 1 次针对采购人基础网络及信息系统的网络安全应急演练活动，尤其针对“钓鱼邮件”、“跨网攻击”、“数据泄露”、“网页篡改”等风险，设计演练方式，发现安全隐患点，提高应急处置能力，协助完善防护措施。同时需记录应急演练过程，并制定应急演练报告。

（3）建立 7×24 小时服务响应热线，按照采购人网络安全应急需求，不限次的及时提供安全应急支援服务。发生网络安全事件时，投标人技术人员必须在 2 小时内到达采购人现场，在 4 小时内发现原因尽快解决，或在 4 小时内提供临时解决方案并协助实施，对事件过

程进行回溯分析，对数据固证，做好应急响应和处置服务。

12、其他安全服务

（1）人员驻场服务

提供 2 人全职驻场服务，服务内容包括：

1）协助配置安全设备的安全策略，保障安全设备正常运行，及时发现异常情况；

2）协助配置安全设备告警规则，对监测到的安全事件按照级别和类型产生不同的告警及时通知相关工作人员处置；

3）利用工具，结合资产信息等实际情况，协助采购人对安全设备日志进行审计分析，挖掘出潜在的网络攻击、运行故障等信息；

4）根据安全监控告警，及时判断问题，定位故障，进行处理，必要时，协调更多资源支持，确保按照安全服务要求及时处理安全故障，保障系统正常运行；

5）每月按采购人需求协助编制监测和处置月报；

6）其他网络安全日常工作。

（2）安全制度及培训

1）服务期内，协助采购人至少开展 1 次针对全体工作人员的网络安全培训、开展 4 次针对采购人及其供应商专业技术人员的网络安全专题培训，合理设计培训课程，制订培训计划，准备培训材料，协调培训专家，做好培训，同时记录培训过程；

2）协助采购人完善网络安全相关制度。

（二）项目服务内容中服务工具要求

序号	工具名称	工具要求
1	**渗透测试工具要求**	支持辅助快速创建钓鱼邮件、钓鱼文件、钓鱼网站，支持统计钓鱼邮件点击数、钓鱼网站访问数、客户端上线数；可以展示网站名称、网站链接、网站类型、创建日期、点击次数、上线次数、部署状态、操作信息。钓鱼文件支持 Word/Excel/可执行程序三种文件类型，支持 Windows、Linux 操作系统，x86、x64cpu 架构；钓鱼网站支持配置网站名称、网站路径、端口，部署位置可选本机、VPS，网站类型支持克隆站、模板站；（投标时提供工具的真实系统截图）
2	**渗透测试工具要求**	支持多种格式客户端生成，包括可执行文件格式如 exe、elf、powershell、dll 等，以及原始 Shellcode 的生成；提供权限清除接口，可一键清除获取到的权限；新增 Webshell 支持自定义代理设置，包含 http、https、socks4、socks5 协议，支持用户名+密码的方式进行认证。（投标时提供工具的真实系统截图）
3	**威胁监测及分析工具要求**	支持加密流量攻击检测，支持针对 SSL 加密协议的攻击检测。支持 JA3 指纹检测技术，支持多层 VLAN、VXLAN、MPLS、GRE 等网络流量的解析检测。云场景下，支持 GENEVE 协议双层隧道封装流量的解析检测。
4	**代码审计工具**	能够识别并支持 C/C++、Java/Jsp、JavaScript、Python 主流开发语言的代码扫描；支持 Go、PHP、C#、Objective-C、Swift、Kotlin 常见开发语言的代码扫描。支持直接对目标软件的源代码文件进行分析；支持对目标软件的源代码编译后的二进制或字节码文件进行分析。（提供第三方检测机构出具的具有 CMA 标识的检测报告证明）
5	**代码审计工具**	支持与主流 IDE 开发工具进行集成，包括：Jetbrains IDEs、Visual Studio Code、Eclipse 且在当前工具可对软件进行代码检测；支持与主流的代码仓库 Git、SVN 集成，可对代码仓库中的代码进行检测；支持与 CI/CD 工具 Jenkins 集成；支持主流的缺陷管理系统 Atlassian Jira、禅道集成，分析结果会同步到工具中；（提供第三方检测机构出具的具有 CMA 标识的检测报告证明）
6	**代码审计工**	支持与邮箱集成，对于检测的不符合项能够发送邮件通知；支持与

	具	LDAP 登录平台集成，使用 LDAP 登录方式登录；支持提供二次开发接口，提供接口规范文档，接口在授权情况下可被正常调用。（提供第三方检测机构出具的具有 CMA 标识的检测报告证明）

投标供应商严格核实所提交检测报告的真实性，除通过国家市场监督管理总局的全国认证认可信息公共服务平台核实报告编号、出具机构等基础信息外，还应尽可能通过检测报告出具机构的官网、邮箱、电话等可靠途径查询所提交检测报告具体内容的真实性（不可轻信检测报告上载明的网址、电话、二维码等），并留存核实过程证据备查，避免因未尽核实义务在投标文件中提交伪造、变造的虚假检测报告而被相关部门予以行政处罚.

（三）服务成果

序号	服务名称	服务成果
1	漏洞扫描	1、漏洞扫描报告≥12 份 2、漏洞扫描总结报告≥4 份
2	渗透测试	1、渗透测试报告≥4 份 2、渗透测试复测报告≥4 份
3	代码审计	按需提供系统代码审计报告
4	安全监测预警	1、按实际情况提供威胁预警信息 2、监测预警报告≥12 份，报告内容需包含监测到的威胁事件、告警深度分析、爆破行为分析、恶意邮件行为分析、数据库行为分析、WEB 攻击分析及具体处置措施、优化策略。
5	网站实时监测	1、按实际情况提供网站可用性、安全性预警 2、网站安全综合评估报告≥12 份
6	信息安全风险评估	1、网络安全风险评估实施方案 1 份 2、网络安全风险评估报告 1 份
7	互联网攻击面管理	1、互联网资产清单，根据探测情况更新 2、互联网资产风险报告≥2
8	实战攻防诱捕	攻防诱捕分析报告
9	协助自查及直属单位安全检查服务	1、按需提供网络安全检查指标清单； 2、按需提供检查方案 3、直属单位网络安全检查报告≥4 份
10	重要时期安全保障服务	1、按需提供重要时期安全保障服务工作方案 2、按需提供重要时期安全保障服务工作总结报告
11	应急体系建设与演练服务	1、按需提供应急预案 2、网络安全实战攻防演练活动方案≥1 3、应急演练报告≥1

		4、应急响应和处置服务总结报告≥4 份
12	其他安全服务	1、安全服务月报≥12，安全季报 4 份 2、培训计划 3、培训材料≥5 4、培训过程记录材料≥5 5、供应链风险评估报告≥1

三、商务要求

（一）项目管理和实施要求

中标方须根据本项目服务要求，制定项目服务方案，按照系统的划分，确定项目人员组成、管理组织实施方案和质量保证方案。

1、项目人员要求

中标方必须根据本项目的特点和服务内容，组建一支技术经验丰富、人员相对稳定的项目团队为项目服务，并在投标文件中确定项目负责人、项目团队成员（包括技术支持工程师、安全服务专家）等主要技术人员，说明每个人的角色、职责。要求在项目服务过程中项目团队成员不少于 7 人，具体包括：1 名项目负责人、2 名技术支持工程师（提供现场服务，遇紧急任务时可临时加派人员）、1 名应急保障专家、1 名网络安全服务专家、1 名数据安全服务专家、1 名渗透测试服务专家。

项目执行过程中，采购方有权对项目组人员进行考核和评价，不符合条件人员，采购方有权要求中标方及时更换。

中标方可以根据实际需要但必须经过采购方同意方可对人员进行更换调整（原则上项目经理、系统架构师及核心系统分析人员不得更换），但须保证所更换人员的技术素质和工作能力不低于被替换人员，且更换比例不得超过 30%，否则，采购方有权提前终止合同。

2、组织实施要求

中标方的软件开发和实施过程要遵循统一过程标准，项目实施过程各阶段的工作安排、工作管理以及各阶段提交的工件和质量标准都要严格遵循统一过程标准要求。

3、质量管理要求

投标方须在投标文件中提出项目质量保证计划、项目实施中质量保障和质量控制方案。

在项目实施全过程中，采购方有对项目进度和质量进行监督控制的职责和权利，中标方应全面配合，确保人力、物力的定量投入。

在服务期内，投标方对于合同范围内的安全工作执行不力，导致采购人被市级网络安全监管机构通报批评或绩效扣分的，发生 1 次或绩效每扣 1 分扣除合同总金额的 10%；导致采购人被省级网络安全监管机构点名通报批评，发生 1 次扣除合同总金额的 20%；以上扣款累计相加，且总扣款不超过合同总金额的 50%。发生重大网络安全事件（含一级、二级、三级），且被国家、省、市相关网络安全监管机构约谈的，直接扣除合同剩余款

4、其他要求

在合同签订时，中标方须与采购方签订《保密协议》、《供应链安全管理协议》，且必须确保参与项目的工作人员不能有涉外人员。在项目实施过程中，中标方必须严格遵守采购方的相关管理制度及操作规范。

项目所有成果的版权、使用权归属深圳市人力资源和社会保障数据管理中心，中标方不得对任何第三方泄露。中标方不得以任何形式对外泄露，否则采购方将依法追究其法律责任。

（二）服务期限、地点及付款方式：

1、服务期限：服务期一年有效，具体时间根据合同约定。该项目为长期服务项目，合同期满可以续签，但合同履行期限最长不得超过三十六个月。如甲方对履约情况不满意，甲方不再续约。

2、服务地点：深圳市人力资源和社会保障数据管理中心

3、付款方式：

首期款：合同签订后，甲方支付首期款，付款金额为合同总金额的 50%。

二期款：服务满 6 个月且项目阶段验收合格后，甲方支付二期款，付款金额为合同总金额的 20%。

尾款：项目最终验收合格后，甲方支付尾款，付款金额为合同总金额的 30%。

（三）供应商审查相关要求：

拟成交中标供应商应提交承诺函，承诺与其他投标供应商之间不存在《深圳经济特区政府采购条例实施细则》第七十五条（二）款的情形，详见附件 2《特定关系承诺函》。