**数字风险威胁检测与演练服务采购需求**

1. **项目背景**

根据《互联网政务应用安全管理规定》《上海市电子政务外网管理办法》等工作要求，应当依照有关法律、行政法规的规定以及国家标准的强制要求，采取技术措施和其他必要措施，保障互联网政务应用安全稳定运行和数据安全。行政服务中心（大数据中心）作为临港新片区管委会直属副处级事业单位，具有推进数字化项目建设管理及信息系统的技术支持与统筹运维，落实网络安全管理、政务云资源使用管理和政务网建设管理等职责。为深入挖掘互联网层面的风险隐患，及时发现数据泄露、网站异常等问题，强化外部视角下的网络安全问题发现与处置，同时充分验证基础安全运营服务成效，进一步促进安全防护能力的提升，亟需通过专业化技术手段提升资产风险动态识别能力与主动防御水平，以满足法定合规义务并筑牢安全基础。

本项目通过系统化实施数字风险威胁检测服务与非破坏性渗透测试服务，构建与高价值资产风险等级相匹配的防护体系：

* 实现互联网侧风险的主动探测与防御能力补充强化；
* 验证现有防护机制有效性并驱动策略动态调优；
* 输出防护体系演进路径的决策支撑依据；

**二、工作目标：**

通过常态化实施数字风险威胁检测服务与非破坏性渗透测试服务，重点开展互联网信息资产风险精准识别、系统漏洞深度挖掘及安全事件应急响应，实现临港新片区大数据中心资产暴露面有效收敛、漏洞全生命周期闭环管理以及数据泄露与网络攻击事件的高效处置，全面强化数字化转型的主动防御能力。

**三、服务需求**

**1、数字风险威胁检测服务**

**（1）自动化资产探查服务：**

①实施全面互联网资产（包括主机资产、网站资产、小程序、公众号、app等）自动化探测，覆盖第三方组件指纹识别、版本及关联依赖分析，通过协议解析与Web指纹识别技术构建资产画像，确保资产信息完整性与精准性。

②基于自动化资产探查发现的主机资产、网站资产等资产信息，人工核实资产真实性，并根据自动化测绘结果实时更新测绘策略、目标和范围。

③通过海量资产特征分析、建模，找出海量资产、网页、结构维度具有相似度的仿冒资产；

④识别互联网暴露面资产，基于攻击路径图谱分析高危节点（如高危服务、未授权API、敏感端口等），定位暴露面风险并驱动收敛。

⑤建立动态化互联网资产台账管理机制，定期执行端口探活与协议解析，同步资产状态变更（增/删/改），关联证书信息及备案数据，保障信息时效性。

⑥针对已识别资产进行安全基线监测和预警，监测网站暴露面安全基线，发现证书失效、使用高危组件、私自映射未经申报的系统等不符合暴露面安全基线的问题及时通知用户处置。

⑦服务期限内输出不少于20份的互联网资产画像报告（含资产趋势、主机攻击面、网站攻击面、风险概述与处置建议等内容）。

⑧本次服务投入的数据资产监测与管控平台需具备计算机软件著作权登记证书且与系统名称保持一致。

**（2）资产风险全生命周期管理**

**1）资产风险发现服务**：

①执行互联网侧漏洞深度发掘，支持且不限于SQL注入、XXE、XSS、任意文件上传、任意文件下载、任意文件操作、信息泄露、弱口令、本地文件包含、目录遍历、命令执行、错误配置、权限维持、WEB应用目录中存在敏感文件等漏洞发掘。

②实施互联网侧弱密码策略审计，支持MYSQL、SSH、RDP、SMB等协议爆破检测，支持web表单爆破监测，内置行业弱口令字典与自定义字典功能。

③实施互联网侧未授权访问监测，支持Redis、MongoDB、JBOSS、Elasticsearch、Docker等常见组件未授权监测。

④执行多维度安全攻击模拟，验证现有防御体系的实际有效性及安全设备的自身安全性。识别安全防护体系中的技术漏洞、配置缺陷、策略短板及流程弱点等防御盲点。

⑤基于资产风险发现的结果，进行漏洞利用链分析及攻击路径模拟技术支撑，动态优化风险扫描重点与数据监控机制，优化风险发现机制。

⑥生成可验证的安全缺陷清单，标注漏洞修复优先级（高危/中危/低危）。

⑦及时报告高风险问题，服务期限内输出不少于12份的风险监测报告（含风险情况和安全建议）。

**2）资产风险管理服务**：

①实施漏洞全生命周期管理，建立“探测→分析→修复→验证”闭环处置流程，对漏洞修复进度追踪。

②综合漏洞可利用性、业务影响面、威胁情报活跃度等指标，建立漏洞修复优先级评估模型，对需紧急修复得高危风险及时下发风险告知单并协助进行修复。

③基于风险评估动态优化防护策略，如协助关闭非必要端口、隔离仿冒资产、更新WAF规则，确保风险处置与业务连续性匹配。

④安全专家全程介入项目，动态审核测试方案风险并提供整改加固实施建议，

整合威胁情报制定风险缓解措施，并验证措施有效性。

⑤服务期限内，结合风险监测报告，输出不少于12份的风险评估报告（含风险分析、风险处置和后续建议）。

⑥本次服务投入的数据资产风险评估系统需具备计算机软件著作权登记证书且与系统名称保持一致。

**（3）数字资产风险保护服务：**

①利用外部资产发现服务，基于单位名称、域名信息、特有业务名称、邮箱后缀、代码常用变量名等关键词对网盘、文库、代码仓库、暗网论坛等渠道进行数据泄露排查服务，及时发现泄露数据。

②针对账号口令、源码信息、文档信息、人员信息进行监控，第一时间发现泄露情况并上报，减少数据泄露带来的负面影响。

③提供国内数据泄露情报分析，需重点关注合作方或供应商的数据泄露情报，分析泄露数据与本单位的关联性。

③服务期限内，若发现针对采购人目标系统的数据泄露事件或者威胁情报，需及时输出风险告知，输出不少于4份数据泄露监测报告（含数据泄露详情、近期国内数据泄露情报）。

④本次服务投入的数据异常监测行为系统需具备计算机软件著作权登记证书且与系统名称保持一致。

**2、非破坏性渗透测试服务**

提供3次的非破坏性渗透测试服务，服务形式为以下两种，具体实施以实际采用的形式为准，同时需包含技术支撑服务。

1）1次临港新片区非破坏性渗透测试：为采购人指定的被测单位（可包括但不限于临港新片区管委会，具体参与单位名单由采购人提供）开展非破坏性渗透测试。主要工作内容为：

（1）活动前进行技术培训、提供前期漏洞检查。

（2）活动阶段提供测试服务。

（3）活动结束后指导修复漏洞、清除痕迹、复测修复情况、防御加固建议、开展总结培训。

2）2次临港新片区管委会非破坏性渗透测试：为临港新片区管委会开展非破坏性渗透测试。提供测试阶段的攻击服务和测试后的指导修复漏洞、清除痕迹、复测修复情况、防御加固建议等服务。

**四、服务要求**

1. 服务各环节严格遵循既定流程与标准，确保资产采集准确、风险识别全面、活动有序开展。定期开展服务质量评估，持续优化流程。
2. 投入服务的工具须具备国家版权局软件著作权登记证书，功能适配且稳定，确保服务合法、有效开展。按要求及时输出各类报告，内容详实且含可行建议。发现高风险问题1小时内多渠道通报，2小时内提交初步分析报告。
3. 建立7×24小时应急响应机制，组建专业团队。发现数据泄露、系统攻击等紧急情况，30分钟内响应，2小时内启动处置（远程服务2小时内提供方案），问题解决后24小时内提交完整应急报告。
4. 非破坏性渗透测试严格遵循授权范围，禁止对未授权目标操作，测试过程实时监控，避免影响正常业务。测试后协同完成漏洞修复、痕迹清除、复测及加固建议工作，组织总结培训提升防御能力。

五、保密承诺

成交供应商需承诺严格保守与本项目有关的技术秘密和商业秘密，任何涉及采购人及使用单位的信息，包括但不限于数据、特有的功能需求等，未得到采购人及使用单位的书面同意，不得对任何第三方展示、举例乃至销售，否则成交供应商将承担由此产生的一切后果。

成交供应商不以实施项目为名，侵害本项目各参与单位的技术、商业秘密或者知识产权。

本采购需求书仅作为成交供应商投报依据，未经采购方书面许可，不可转发第三方或随意传播。

六、人员要求

为确保本项目的交付质量保障，要求供应商负责本项目的人员团队，至少提供8人，配置如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 角色 | 主要职责 | 人数 | 资质要求 |
| 1 | 项目经理 | 统筹协调全流程安全服务实施，通过客户对接与资源调配保障项目按期交付且风险可控。 | 1人 | 1. 本科及以上学历； 2. 计算机相关专业高级专业技术资格 |
| 2 | 安全技术工程师 | 实施全域资产探查与风险闭环管理，通过动态台账维护及漏洞生命周期追踪驱动暴露面收敛。 | 1人 | 计算机信息安全工程师专业证书 |
| 3 | 数据安全工程师​ | 监控内外部数据泄露情报，通过暗网监控和搜索引擎情报聚合识别数据泄露风险并及时预警。 | 2人 | CISAW证书 |
| 4 | 安全产品工程师 | 执行多维度攻击模拟验证，通过防御失效路径分析及策略动态调优提升安全设备检测率。 | 1人 | CISAW证书 |
| 5 | 渗透测试工程师 | 开展非破坏性渗透测试，通过漏洞挖掘发现高风险漏洞并输出可验证的漏洞利用链报告。 | 3人 | CISP证书 |

供应商应保证项目人员的稳定，未经采购人允许不得私自进行人员更换。如遇不可抗力（如：员工离职）的情况应当进行人员更换，则要求提前30日通知采购人知晓，并得到采购人的同意，后方可入场。

供应商在项目过程中进行人员更换时，需开具相关说明（如：人员更换申请说明等）并加盖公章。

供应商在项目实施过程中，由于人员流失、人员素质不高等导致项目质量问题的，采购人有权推迟项目验收或终止项目，损失由供应商无偿补足，并由供应商承担全部责任。