**一、项目概述**

通过购买第三方安全服务，为采购方信息系统提供网络安全专项服务、应用安全服务、资产发现与管理、安全评估与检查等服务，实现基础安全防护能力、日常网络安全保障、威胁感知与预防、风险事件预警复核及处置、应急事件分析溯源、重大活动保障等能力建设，保障我厅信息系统安全平稳运行，无重大网络安全事件发生，信息系统安全维护项目服务期为1年。

1. **服务范围**

本次项目的服务范围包括：西安市政府网站集约化站群平台、西安市人民政府门户网站、西安市政府综合办公平台、西安市人民政府邮箱系统等相关信息系统。

**三、服务依据**

本次安全服务工作主要依据以下法律法规和标准：

《中华人民共和国网络安全法》

《中华人民共和国数据安全法》

《中华人民共和国个人信息保护法》

《网络数据安全管理条例》

《互联网政务应用安全管理规定》

《信息安全技术个人信息安全规范》（GB/T35273-2017）

《网络安全等级保护管理办法》（公通字[2007]43号）

《网络安全技术信息系统安全等级保护测评要求》（GB/T28448-2019）

《网络安全技术信息系统安全等级保护基本要求》（GB/T22239-2019）

《信息安全技术 政府门户网站系统安全技术指南》（GB/T 31506-2015）

《信息安全技术 政府部门信息技术服务外包信息安全管理标准规范》（GB/T 32926-2016）

《信息安全技术 政务网站系统安全指南》（GB/T 31506-2022）

《信息安全技术 信息安全风险管理实施指南》（GB/T 24364-2023）

**四、服务内容**

本次项目包括以下16项服务内容：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务大类 | 服务名称 | 数量 | 单位 |
| 1 | 网络安全专项服务 | 安全及保密保障服务 | ≥3 | 人 |
| 2 | SSL证书服务 | 1 | 套 |
| 3 | 专项培训服务 | 1 | 次 |
| 4 | 安全培训服务 | ≥4 | 次 |
| 5 | 重保服务 | ≥7 | 次 |
| 6 | 应急响应及演练服务 | ≥1 | 项 |
| 7 | 应用安全服务 | 网站安全监测服务 | 1 | 项 |
| 8 | 网站云防护服务 | 1 | 项 |
| 9 | 主机动态威胁监测服务 | 1 | 项 |
| 10 | 网页防篡改服务 | 1 | 套 |
| 11 | 资产发现与管理 | 政务网资产梳理服务 | 1 | 项 |
| 12 | 互联网暴漏面排查服务 | ≥2 | 次 |
| 13 | 系统基线核查服务 | ≥4 | 次 |
| 14 | 安全评估与检查 | 渗透测试服务 | ≥8 | 次 |
| 15 | 开源组件排查服务 | ≥4 | 次 |
| 16 | 漏洞扫描服务 | ≥16 | 次 |

**（一）专项安全服务**

本项服务包括6项工作，具体包括：安全及保密保障服务、SSL证书服务、专项培训服务、安全培训服务、重大活动保障服务、应急响应及演练服务。

**1.1安全及保密保障服务**

**基本要求**

服务商提供不少于3名现场驻场保障服务，为办公厅提供常态化计算机安全巡检及保密检查服务，保证计算机的稳定运行。需根据现场业务情况，开展日常运维驻场工作。在运维期内完成办公厅办公区域内的计算机及外设的软硬件和网络维护，具体内容包括：计算机及外设（台式机、笔记本电脑、扫描仪、集线器、刻录机、打印机和移动硬盘等）的硬件故障诊断、安装、扩展等；操作系统、防病毒软件及各类应用软件的安装升级及调试、各类驱动程序的安装及调试；计算机网络故障维护；维护故障时数据的导出及备份等。协助完成办公厅计算机终端及网络等安全保密检查工作；协助安全保密软件管理；完成办公厅安全保密检查其他相关工作；

**服务内容要求**

计算机设备及外设的维护：及时处理计算机设备及外设的各种故障，每季度对计算机设备及外设进行巡检和维护，按照采购人要求进行硬件设备普查工作，并负责与采购人的资产管理系统进行衔接。

网络维护：负责维护市政府办公厅的局域网、机关办公区域内的内部网络（指办公室房间内部、楼层交换机到房间的桌面设备应用端电脑网络）。检查办公厅机关大楼网络健康状况，查找故障网线、调测不稳定端口，分析网络故障，及时发现和协助解决存在的问题。每月对网络进行巡检，调试优化网络配置。

设备故障处理：7\*24在线受理故障，提供电话、邮件技术支持，远程解决故障；工程师现场服务（工作日响应时间小于15分钟）；故障排除时间小于4小时（零部件所需的运输时间不计算在内）；建立故障处理小组，对紧急故障及时响应并处置。

协助完成办公厅各处室的办公计算机、移动存储介质、办公网络安全保密事项的日常检查和抽查；

完成采购人交办的其它事务性工作。

**文档输出要求：**

运维驻场服务需定期向采购方提供：

建立《计算机及相关外设台账》、《故障维护清单》；

完善《计算机数据安全及保密规定》

《安全检查月报》、《保密检查季报》。

**1.2 SSL证书服务**

**服务内容要求：**

提供一年期SSL证书服务（含SSL国际算法站点证书及国密SM2站点证书，均需为域名通配符证书）。

SSL国际站点证书至少需为class3级以上，加密强度不低于256位。

国密站点证书加密强度需不低于SM2 256位，且实现与SSL国际算法站点证书+国密站点证书双证书机制。

**文档输出要求：**

《证书服务方案》

**1.3专项培训服务**

**服务内容要求：**

提供1人次的线下专项培训服务。

培训内容不限于安全专业技术学习、攻防实操、红蓝对抗、应急处置等，服务商须与采购人沟通确定，承担培训人员的培训及考试费用。

**文档输出要求：**

《培训签到表》

《培训汇总材料》

**1.4安全培训服务**

**基本要求：**

服务商提供安全培训服务，为采购人信息化相关技术、管理、运维人员进行集中培训，通过培训使参训人员全面深度掌握国家网络安全相关的法律法规、制度、标准和相关行业要求，了解网络安全细分领域相关情况，掌握应急及安全防范技术措施等，服务期内提供至少4次业务培训服务。

**服务内容要求：**

在培训前需与采购人确认培训主题，定制符合采购人实际需求的培训课程，完成培训课程的相关讲义、课件、资料等准备，培训师资视采购人实际需求确定，包括但不限于服务商自身提供、聘请外部专家。

培训的课程内容包括但不限于安全意识、安全政策及法律法规、安全基础常识、安全风险应对、安全处置响应、安全运维、安全加固、安全产品使用等方面。

**文档输出要求：**

《培训签到表》，培训签到表应至少包括培训地点、时间、主题、参训人员名称、签字等。

《培训课件》

**1.5重大活动保障服务**

**基本要求：**

服务商提供重大活动保障服务，在重大活动期间（两会、春节、国庆、或采购人要求的特殊时期）开展7\*24小时安全保障工作，满足采购人在重要时期的安全保障要求，保障业务的正常稳定运行。服务期内按采购人要求时间节点提供重保支撑服务，保障次数不少于7次。

**服务内容要求：**

提供重保活动前风险自查工作，扫描发现潜在的安全风险威胁等，同时对自查出的风险问题进行跟进闭环。

重保活动期间7×24小时进行值守、实时监测、预警提醒、处置闭环，一旦发生安全事件或风险第一时间进行处置响应，并同步采购人相关接口人，对高危事件即时响应。除现场驻场、重保值守保障人员外，服务商应提供后端专家团队进行即时支持，快速支撑处置安全问题，阻止和降低重保期间发生的安全事件带来的严重性影响，及时消除安全隐患。

**文档输出要求：**

在重保活动结束后输出相应的《重要活动保障服务总结报告》，报告至少包含重保总体工作概况、重保值守情况总结、保障过程、保障风险总结等。

**1.6应急响应及演练服务**

**基本要求：**

服务商提供服务期1次以上的应急响应服务。应急范围包括但不限于挖矿、数据泄露、勒索病毒、系统失陷等。服务期提供不少于1次应急演练服务，根据采购人需求定制应急演练服务，通过演练检验各业务、应急流程环节的配合程度。通过演练落实应急处置工作责任制，明确应急处置责任人，提升安全防范意识和处理能力。

**服务内容要求：**

应协助采购人成立专项应急响应小组，协助建立健全应急上报及联络机制，发布应急联络人表单，确保在应急事件发生时，能及时启动应急流程并及时联系到相关人员。在完成应急响应工作后，服务商应协助采购方进行事件回溯，基于应急的全过程，对事件的原因、过程、处理结果等进行总结，对暴露出的安全缺陷问题进行加固整改、优化提升，避免再次发生类似问题事件。

应协助采购人完成应急演练工作，设立应急演练工作小组，并设置不同角色负责不同职责，拉通所有相关人员，包括但不限于安全团队、业务系统运维和管理人员、采购人相关人员，搭建模拟仿真业务环境，模拟各种业务突发安全事件场景，严格按照应急预案设定的应急事件的响应流程，进行分析研判、溯源分析、应急处置、隐患消除、处置恢复等，确保各角色、各流程环节熟悉应急流程，并在演练完成后输出演练总结报告，对演练暴露出的问题进行优化提升。

**文档输出要求：**

《应急响应报告》

《应急演练实施方案》

《应急演练总结报告》

**（二）应用安全服务**

本项服务包括4项工作，具体包括：网站云监测服务、网站云防护服务、主机动态监测服务、网页防篡改服务。

**2.1网站云监测服务**

**基本要求：**

服务商针对采购人所有互联网系统提供网站云监测服务，包括Web漏洞监测、挂马/暗链/篡改监测、敏感内容监测、网站IPv4/IPv6可用性监测等，服务期内提供采购人所有互联网站点的7\*24小时实时监测，并定期提供监测报告。

**服务内容要求：**

对采购人管理的互联网站点提供安全监测服务，包括对网站挂马监测、暗链监测、篡改监测、可用性监测、漏洞监测、敏感内容监测等。

统一管理：需提供统一管理页面，通过Web、手机端在线查看网站监测情况，可通过可视化大屏单站点概览查看网站安全监测概况，可通过多种维度统计和展示安全监测趋势及概况，可查询监测结果详情，包括但不限于漏洞风险详情、取证截图。

挂马、暗链、篡改监测：对网站进行页面资源与指纹信息的分析，通过监测技术对各类网站安全事件进行全面分析感知，包括篡改、暗链、黑页、挂马等。

可用性监测：服务商以多运营商多区域多链路多点监测形式，发现在不同区域内采购人互联网业务站点的多线路访问可用性情况。对监测站点的域名解析可用性、网站服务可用性、IPv6访问可用性监测等进行监测，并在发生问题后自动进行可用性告警。

漏洞监测：对目标站点进行全面的互联网漏洞扫描，实时发现系统存在的各类安全隐患，支持所有常见的Web应用漏洞，支持OWASP TOP10等主流安全漏洞监测。

敏感内容监测：可识别身份证信息泄露、敏感词汇内容等。

人工验证：服务商应对挂马监测、暗链监测、篡改监测、漏洞监测、敏感内容监测等监测结果提供24小时人工验证工作，在发现问题的第一时间上传风险验证截图，标记验证状态，并在人工验证确定为风险后立即对采购人进行预警。

实时提醒：要求服务商在发现安全风险后，可实时通过邮件、短信等方式对采购人进行安全提醒。

**文档输出要求：**

每月输出每个站点的《安全监测报告》，服务期内不少于12份，报告至少包括站点漏洞风险分析、站点安全事件分析、站点可用性监测结果等。

**2.2网站云防护服务**

**基本要求：**

服务商针对采购人所有互联网系统提供云端安全防护服务，提供多维网络攻击防护能力，应对当前复杂的网络安全形势，保障采购人网站的安全稳定运行，服务期内提供采购人互联网站点的7\*24小时实时防护，并定期提供防护报告。

**服务内容要求：**

对采购人管理的互联网站点提供云防护服务，包括Web应用安全防护、Webshell攻击防护、CC攻击防护、扫描防护、区域访问控制、网站一键关停、网站应急展示等能力。

统一管理：需提供统一管理页面，可通过可视化大屏单站点概览查看网站的安全防护状况，可在Web、手机端查看和调整每个站点的防护策略，查看站点访问状态、访问量、攻击量等，可回溯查询历史防护日志记录。

Web应用安全防护：覆盖OWASP TOP10漏洞进行防护，对注入攻击、跨站脚本攻击、网站组件漏洞攻击、HTTP异常请求、信息泄露等常见Web攻击行为和风险进行防护。

Webshell攻击防护：针对webshell上传攻击进行实时检测和分析，对恶意文件进行实时有效阻断。

CC攻击防护：针对CC攻击，根据访问频率、访问集中度、访问行为等进行过滤和防护。

扫描防护：对针对网站的扫描攻击行为进行防护和阻断，防止网站信息被攻击者扫描获取，并对高频攻击地址进行拉黑。

区域访问控制：可设置仅指定区域可访问业务系统，限定高危区域访问，降低被攻击风险。

网站一键关停：当网站出现紧急安全事件时，可实现一键秒级站点关停，并弹出友好维护界面，防止网站安全事件产生的不良影响扩大。

网站应急展示：可记录和缓存网站内容，在站点出现安全事件或故障时，可紧急展示缓存的站点内容，确保网站正常展示。

**文档输出要求：**

每月输出每个站点的《安全防护报告》，服务期内不少于12份，报告至少包括站点风险概况、攻击威胁详情分析、风险详情分析、攻击源地址分析、攻击源区域分析等。

**2.3主机动态监测服务**

**基本要求：**

服务商提供主机动态监测服务，服务工具的性能和数量须满足客户实际业务需求，覆盖不少于200个云主机的监测能力，针对当前所有资产的Web攻击、恶意病毒样本、勒索病毒爆发、挖矿行为、内部主机受控、暴力破解、隐蔽信道数据传输、弱口令攻击等进行安全监测，提升业务的安全监测预警能力。

**服务内容要求：**

对采购人管理的所有业务提供威胁监测服务，包括安全威胁监测、政务邮件安全检测、业务附件威胁检测、深度威胁检测、攻击溯源、业务资产管理、场景分析、可视化等能力。

安全威胁监测：支持国产化云环境下的威胁检测能力，能够实时发现Web攻击、恶意文件攻击、可疑流量、后门访问、挖矿行为、扫描行为、暴力破解、漏洞攻击、邮件社工类攻击等常见攻击行为，可实现对高危风险攻击行为的实时监测和预警，支持智能语义分析能力。能够基于攻击者维度、受害者维度等进行多维视角的聚合分析，自动识别出攻击者的攻击总次数以及攻击行为是否成功。能够基于威胁情报技术，进行威胁情报分析，并进行聚类展示，包括挖矿、隧道通信、远控等分类进行展示。

政务邮件安全检测：支持对邮件社工攻击的检测，可检测类型包括但不限于邮件头欺骗、发件人欺骗、钓鱼邮件、恶意链接邮件等；支持对邮件附件、二维码等内容进行检测，识别潜在的内容安全风险。

业务附件威胁分析：支持对业务站点上传或传输的文件附件进行威胁分析，检测是否为病毒或黑客上传的文件。

深度威胁检测：支持对哥斯拉、冰蝎4.0等高级威胁的深度威胁检测能力，支持对加密流量进行检测，可查看加密流量详情，并支持通过技术手段对TLS1.3、DH密钥算法加密的流量进行检测。

攻击溯源：支持对攻击者进行深度溯源，可一键溯源查看攻击全过程，展示攻击路径、攻击过程等。

业务资产管理：支持实时基于业务云主机资产监控状态，展示资产健康度、资产类型分布、资产重要性分布等，并支持对云主机资产详情进行查看和配置。

场景分析：提供安全场景化展示，包括对勒索病毒、弱口令、挖矿等常见安全场景的专项展示，可统计展示风险IP、风险详情；支持提供AI安全助手，实现在线安全知识检索、智能问答、安全威胁详情分析等。

可视化：提供云主机安全态势的可视化呈现，包括但不限于攻击来源地图、风险趋势、风险攻击类别等内容，可点击查看风险详情。

**文档输出要求：**

每月输出《威胁监测服务报告》，服务期内不少于12份，针对当月的威胁监测服务情况进行汇总分析，至少包括威胁监测总览概述、监测情况、高危事件情况等。

**2.4网页防篡改服务**

**基本要求：**

服务商应提供网站安全保障服务，提升网站的防篡改及篡改恢复能力，降低网站被篡改的风险，具备网站篡改发现和阻断能力，保障网站安全。服务期内提供采购人互联网站点的安全保障服务。

**服务内容要求：**

对采购人管理的互联网站点提供网站安全保障服务，包括网站漏洞防护、访问控制、防篡改、后门查杀等能力。

网站漏洞防护：结合本地防护弥补云防护的不足，可针对注入攻击、跨站脚本攻击、漏洞攻击、CC攻击、扫描攻击等常见Web攻击行为和风险进行防护。

网站访问控制：针对不同站点的URL进行访问控制，实现对站点的URL级访问控制。

网站防篡改：有效防护网站目录文件不受篡改攻击，包括动态页面（脚本）、静态页面、音乐、图片、视频等，可基于网站目录、进程、IP等设置规则，防护内容包括网站文件内容、文件名、文件属性、文件路径等。

网站后门查杀：对网站目录文件进行全面检测，能够基于多种检测机制和算法，对网站后门进行查杀和隔离。

**文档输出要求：**

每月输出《防篡改服务报告》，服务期内不少于12份，针对当月的防篡改服务情况进行汇总分析，至少包括安全保障结果概述、防护情况、后门查杀情况、防篡改情况等。

**（三）资产发现与管理服务**

本项服务包括3项工作，具体包括：政务网资产梳理服务、互联网暴露面排查服务、系统基线核查服务。

**3.1政务网资产梳理服务**

**基本要求：**

服务商应对采购人所有业务资产包括虚拟机、端口等进行识别、分类和管理。包括收集资产信息、确定资产责任人、资产详细属性，将资产测绘结果与服务进行关联，确保资产的安全使用和管理。

**服务内容要求：**

结合已有台账和技术工具等资产数据来源，通过人工服务梳理采购人当前所有业务资产的分布数量以及部署位置，对资产进行梳理，形成全面的资产清单，完成资产台账的登记，作为安全管理的基础。

通过人工服务协助摸清家底，建立资产台账，包括资产属性、责任人、资产使用状态、部署位置等，协助采购方梳理资产管理制度和机制，关联“资产-责任人”，落实资产管理责任制，消除资产管理盲区。若在梳理完成后，资产有少量更新，需协助录入新增资产信息和数据。

**文档输出要求：**

完成资产管理服务后，输出《资产统计清单》，清单至少包括资产名称、IP、用途、责任人、部署位置等信息，协助采购人进行资产台账登记。

**3.2互联网暴露面排查服务**

**基本要求：**

服务商对采购人暴露在互联网上的系统应用相关的域名、端口、IP等进行梳理，并对存在暴露风险、高危风险的资产进行关停或整改，以减少信息系统在互联网上的暴露风险，降低被黑客攻破的可能，服务期内不少于2次服务。

**服务内容要求：**

针对采购人互联网资产（互联网域名、端口、IP等）开展暴露面检测，评估互联网资产的安全暴露风险，基于检测结果协助清除影子资产、无主资产、高危风险资产，减少资产风险隐患。

需在确保不影响业务稳定性的情况下开展检测工作，针对所有互联网资产进行检测，提供所有互联网资产的测绘结果数据，人工对检测结果进行分析，针对高危资产提供安全建议。

提供技术支撑工具，辅助完成暴露面检测，工具可针对IP地址、域名、DNS解析、端口服务等进行检测，对业务资产的域名备案、子域名、运营商、IP、端口、地理位置、返回标题、历史解析记录、Web框架等信息进行采集。

**文档输出要求：**

完成暴露面检测工作后，输出《互联网暴露面检测报告》和《互联网资产清单》，暴露面检测报告至少包括检测结果、检测资产情况、检测到的高危资产列表及详情、安全建议等内容，互联网资产清单至少包括资产URL、IP地址、资产名称、开放端口、web框架、返回标题等信息。

**3.3系统基线核查服务**

**基本要求：**

服务商对采购人指定信息系统提供基线核查服务，发现服务器、中间件、数据库系统、组件等风险，服务期内不少于4次服务。

**服务内容要求：**

针对采购人的应用系统，围绕基线核查的安全标准，从账号与认证安全、授权与访问控制、系统与服务安全、安全配置、其他关键配置等维度进行核查，将能够采集到的司机配置与预定义的、可定制的安全基线进行对比，结合自动化扫描结果，由安全专家进行结果分析，并给处加固建议。

**文档输出要求：**

《系统基线核查报告》

**（四）安全评估与检查服务**

本项服务包括3项工作，具体包括：渗透测试服务、开源组件排查服务、漏洞扫描服务。

**4.1渗透测试服务**

**基本要求：**

服务商以模仿黑客的方式，借助工具，以人工为主，对采购方指定的测试对象业务进行测试，围绕指定测试业务，基于常见的渗透路径、测试方法，尽可能多的发现测试对象的各类安全风险、漏洞问题，并提供相应的修复建议、完成后续复测。通过渗透测试服务为安全加固、风险管理等工作提供依据，服务期内提供不少于8次服务。

**服务内容要求：**

在得到采购人授权的前提下，服务商通过采用辅助工具和适当的人工测试手段，对待测业务系统进行深层次的渗透测试，通过模拟黑客使用的工具、分析方法对信息系统进行安全测试，发现测试目标存在的安全隐患、漏洞，结合人工测试和分析，识别扫描工具无法发现的问题，从技术层面定性的分析业务系统的安全性，查找系统存在的安全隐患点，并通过有效的验证每个安全隐患点的可利用程度。并根据测试结果输出渗透测试报告，针对每种发现的脆弱性风险进行详细描述，内容包括测试过程、使用的技术手段以及风险成果，并给出相关的安全建议。

渗透测试内容包括但不限于：信息收集类、配置管理类（HTTP方法测试、应用中间件测试、信息泄露、异常错误等）、认证类（用户枚举、密码猜解、密码重置、密码策略测试等）、会话类（cookie测试、session会话测试等）、授权类（越权访问、路径遍历、任意文件下载、逻辑缺陷测试等）、数据验证类（SQL注入、跨站脚本、代码注入、URL跳转、文件上传测试等、输入输出校验绕过、数据篡改）、系统应用漏洞等。

在业务方修复安全风险问题后，完成复测验证，确保渗透的安全风险问题完全修复。对因客观原因暂时无法修复的问题，给出安全建议，协助进行风险规避或降低，并记录。

**文档输出要求：**

完成渗透测试工作后输出《渗透测试报告》，至少包含测试结论、测试情况、测试过程、测试内容、测试结果详情、安全加固建议等内容。

**4.2开源组件排查服务**

**基本要求：**

对采购人业务的软件成分进行安全评估，发现软件成分中的已知漏洞、代码许可证信息等，对组件成分及漏洞进行梳理和分析，服务期内提供不少于4次服务，提供组件漏洞优化更新建议。以服务提升业务软件的自身安全，降低业务系统的潜在安全风险，提升系统的自身安全性。

**服务内容要求：**

对重要业务系统的软件成分进行评估和扫描识别，收集待测系统相关的所有源代码、服务器应用系统信息，采用工具扫描和人工分析确认相结合的方式，对被测系统所使用的开源软件代码、组件等进行分析，识别内容包括但不限于软件成本名称、版本、已知漏洞等级、许可协议、漏洞利用难度等方面，并对软件依赖关系进行分析。

通过评估服务发现软件组件成分存在的已知安全漏洞，兼容CNVD、CNNVD、Github等漏洞情报信息，覆盖常见的组件漏洞类型，包括但不限于代码注入、信息泄露、授权问题、命令注入、访问控制问题、缓冲区错误、跨站脚本、跨站请求伪造、路径遍历、输入验证错误、配置错误等类型，同时对业务软件所使用的开源软件许可证进行分析，关联分析许可协议风险和许可依赖，出具代码组件成分评估报告，提供修复建议协助业务人员修复安全问题，在业务方修复安全风险问题后，完成复测验证，确保评估出的已知安全风险问题完全修复。对因客观原因暂时无法修复的问题，给出安全建议，协助进行风险规避或降低，并记录。

**文档输出要求：**

《代码组件成分评估报告》

**4.3漏洞扫描服务**

**基本要求：**

服务商利用成熟的商业工具，对采购人业务应用系统进行操作系统、中间件、数据库、应用层面开展扫描，不少于16次，针对采集到的漏洞、脆弱性风险进行分析、验证、安全提醒、线上流转、跟踪复测的全流程闭环管理，确保漏洞风险的闭环。对大数据服务中心发现的漏洞进行统计，建立漏洞台账，跟踪应用系统完成闭环处置。

**服务内容要求：**

提供漏洞扫描服务，同时针对采集的漏洞风险、基线安全风险、内容风险等，提供专项管理分析服务，对采集到的系统漏洞信息，通过人工分析、人工验证、漏洞POC测试等方式，验证该漏洞信息的真实性和准确性，并进一步获取详细的漏洞信息，以支撑进行后续漏洞提交。将已发现的漏洞通告到对应的资产负责人，并协助相关责任人进行脆弱性的修复，限定在一定时间范围内将问题处置完毕并提交审核。当相关资产负责人已完成脆弱性的修复工作后，通过人工漏洞复验方式，确认漏洞修复结果，同时将漏洞通告流程关闭并归档。

**文档输出要求：**

《漏洞扫描报告》

《漏洞采集及闭环管理记录》

《漏洞扫描年度分析报告》

**五、服务要求**

1.基于业务需求，保障网络稳定运行，需要具备业务流量可监测、回溯、审计，实现业务安全风险事件的快速发现、研判、预警和处置；实现所有业务资产、风险、漏洞的统一管理，达到业务风险可感知、可预警、可管控。

2.服务商应在合同签订后10个工作日内提交本项目服务计划，至少包括各项服务的分阶段工作内容、服务工作计划、预计开始与完成时间等，并报采购人确认，严格按计划节点执行，若未完成，需汇报说明未能按计划开展或完成工作的原因，并采取措施进行改进。

3.本次项目需要驻场服务人员不少于5人（其中安全及保密保障服务驻场服务人员不少于3人，安全专项服务驻场服务人员不少于2人），驻场完成终端、安全工具的日常维护、管理、操作、故障处理等，保障相关服务工具的安全稳定运行，开展漏洞扫描、基线核查、渗透测试等服务工作，同时完成现场监测、分析、响应、处置、协作等工作。需提供后端安全服务保障团队，负责安全评估自查服务、应急响应服务、重大活动保障等，根据采购人要求提供足够的后端支撑团队人员，不少于8人，并具备相应的专业服务能力，能够在5分钟内响应采购人需求，2小时内达到现场，最长48小时内解决问题。

4.服务商应按服务要求提供本项目服务所需的所有必备工具、零配件、辅料辅材等，工具符合采购人现场需求、符合国家和政府行业标准规范要求，且具备一定的技术先进性，至少应为行业市场的先进产品。

5.本次项目所提供的安全工具质量和功能稳定、可靠，不能影响采购人正常的业务运行，如若造成重大事故及问题，需根据造成的损失承担相应的责任。

6.原则上本项目所有服务人员在确定后不得更改，如在项目执行过程中发现服务团队不能胜任相关工作的，采购人有权要求更换，如服务商需主动调整服务团队成员，需向采购人提出申请并取得采购人同意后方可调整。

7.本项目中服务商因履行本项目而知悉的所有数据、信息和资料（包括但不限于账号信息、图表、文字、计算过程、任何形式的文件、访谈记录、现场实测数据、采购人相关工作程序等）以及因本项目而形成的数据、信息和任何形式的服务工作成果，均是采购人要求保密的信息。未经采购人书面同意，不得对外泄露，不得用于其他用途，否则需承担由此引起的法律责任和经济责任。服务商所有参与本项目工作的服务人员需签署个人保密承诺书。

8.项目服务期间应保障采购人现有应用系统的正常运行，未经采购人允许不得擅自改动业务系统配置、策略配置、系统参数、应用系统参数等。

**六、其他要求**

1.本次项目所涉及的各项服务需遵循国家相关规范要求，且符合采购人现场实际情况，服务工作需按照国家级行业相关的标准规范进行实施。

2.应采取各种控制手段保证项目实施的各项服务按与采购人约定的时间计划开展，服务质量严格遵守ISO9001质量管理体系，制定项目质量控制措施，保证在项目执行的各个阶段均得到有效控制，确保项目的交付质量满足采购人要求。

3.本次项目的所有交付服务成果文档需满足各项服务中的对应服务成果要求的时间节点和内容要求，需按采购人要求制定服务文档交付格式规范，包括但不限于文档命名标准、版本控制、文档格式要求等，确保交付的服务文档格式与内容符合采购人要求的标准格式。

4.本项目在签订合同后需与采购人签署《服务考核确认书》，约定所有服务内容的要求、完成指标要求、服务质量要求、交付要求等内容，验收前需通过采购人组织的服务考核，考核通过方可验收。