采购项目技术、服务及其他商务要求

一、采购内容

序号	服务名称	单位	数量
1	基础网络安全支撑服务项目	项	1

二、项目基本情况

基础网络安全支撑服务项目依托第三方专业信息安全团队，为四川省大数据中心提供网络与信息安全服务。本项目主要服务内容包括安全检查、风险评估试点等。安全检查主要是对四川省大数据中心多个信息系统进行渗透测试、漏洞扫描和基线检查等，挖掘系统潜在隐患和漏洞，提供报告和整改措施；风险评估试点服务主要是对中心重要政务应用进行系统及数据安全风险评估，判定系统及数据资产的重要程度，分析系统及数据资产面临的安全威胁。

三、服务要求

安全检查类

1、应用系统渗透测试

针对四川省大数据中心信息系统（至少 18 个），服务期内至少 2 次，采用人工黑盒的方式对各信息系统进行模拟攻击测试，挖掘潜在隐患，找出系统弱点。

（1）按照 PTES(渗透测试执行标准)进行模拟黑客攻击。主要测试手段包括：信息收集、端口扫描、远程溢出、口令猜测、本地溢出、客户端攻击、中间人攻击、web 脚本渗透、B/S 或 C/S 应用程序测试等。

（2）渗透测试内容应包括：SQL 注入检测、XSS 跨站脚本检测、缓冲区溢出检测、上传漏洞检测、隐藏目录泄露检测、弱口令检测、数据库泄露检测等。

（3）渗透测试应建立完善的测试计划，使用符合法规要求的自动化测试工具，根据测试需求情况编写攻击插件，确保测试过程流畅、影响可控。

（4）服务期内，根据四川省大数据中心需求，在重要时间节点（重大活动、重要会议举办前等），开展不定期的应用系统渗透测试。

（5）渗透测试包含沟通准备、信息收集、脆弱性分析、渗透执行和报告五个执行阶段。沟通准备包括制定服务协议、客户授权、环境准备；信息收集阶段包括目标识别、信息收集；脆弱性分析阶段包括资产分析、威胁分析和漏洞挖掘；渗透执行包括攻击执行和测试后清，由点到面、由外向内完全模拟黑客入侵的方式，对中心信息系统纵深防御体系中所有脆弱性问题进行发现，再由面到点对发现的每个问题点进行分析与利用，最终明确验证整个安全防护体系中最关键的隐患点；报告阶段包括报告编写、成果汇报等，应记录渗透测试过程，输出《XXXX 系统渗透测试报告》《XXXX 系统渗透测试复测报告》等渗透测试报告。报告内容至少包含问题位置、成因及修复建议等信息。

2、漏洞扫描

针对四川省大数据中心信息系统（至少 18 个），服务期内至少 3 次，进行脆弱性漏洞扫描，以发现主机上不同应用对象（如操作系统和应用软件）的弱点和漏洞。

（1）对四川省大数据中心信息系统所属的主机进行扫描，扫描内容包括主机操作系统补丁更新情况、远程服务端口开放情况等。根据扫描结果及评估报告，指导系统管理员进行漏洞修复。

（2）开展系统弱口令专项测试检查。

（3）漏洞扫描服务应使用安全合规扫描专业工具，支持多种协议口令猜测，包括 SMB、Snmp、Telnet、Pop3、SSH、Ftp、RDP、DB2、MySQL、Oracle、PostgreSQL、HighGo、MongoDB、UXDB、STDB、kingbase、RTSP、ActiveMQ、WebLogic、WebCAM 等（提供服务工具功能截图）。

（4）漏洞库中的漏洞数量不少于 150000 个，且漏洞库兼容 CVE.CNNVD.CNCVE.CNVD.CVSS 等标准（提供服务工具功能截图）。

（5）漏洞扫描支持漏洞验证功能，扫描后能够对结果中的重要漏洞进行现场验证，展示漏洞利用过程和风险。

（6）漏洞扫描支持灵活的扫描任务制定功能，可设定检测开始时间、检测入口地址、网站 COOKIE、检测周期、任务模式、最大检测页面数、最大相似页

面数、检测深度、扫描线程数、漏洞类型设置等。

（7）服务期内，根据四川省大数据中心需求，在重要时间节点（重大活动、重要会议举办前等），开展不定期的漏洞扫描。

（8）服务期内，根据四川省大数据中心需求，对四川省大数据中心所属个人终端进行至少 1 次安全检查。

（9）每次扫描后提交《漏洞扫描报告》等。

3、基线检查

针对四川省大数据中心信息系统（至少 18 个），服务期内至少 2 次，开展远程/离线安全配置检查服务。

（1）基于安全基线标准，开展远程/离线安全配置检查服务，检查 Web 服务器、中间件等的配置情况等；对所发现的安全问题，提交安全加固建议方案并形成报告。

（2）基线检查服务应提供专业的工具进行基线配置核查，识别的内容应包括操作系统和中间件等的账号、口令、授权、日志安全要求、不必要的服务、启动项、注册表、会话设置等配置。其安全基线标准应是最新的。

（3）基线配置核查提供由以下原因造成的扫描失败提示，包括用户密码错误、路由不同、协议端口未开启、远程连接数超限制等。（提供服务工具功能截图）。

（4）基线配置支持对多种操作系统、中间件、虚拟化系统及大数据、容器组件的检查。对应用系统（中间件）的核查，至少包括 Apache、Bind、Domino、IIS、Jboss、Nginx、Resin、Tomcat、TongWeb、Weblogic、Websphere、Tonglink、金蝶主流服务软件等。

（5）服务期内，根据四川省大数据中心需求，在重要时间节点（重大活动、重要会议举办前等），开展不定期的基线检查。

（6）检查结束后出具《基线核查报告》，提交《XXX IT 主流设备/系统/组件安全基线技术规范》《XX 信息系统配置核查安全加固方案》《XX 信息系统配置核查安全加固报告》《XX 信息系统配置核查报告》《XX 信息系统配置核查整改建议》等。

风险评估服务试点类

提供对中心重要政务应用（至少 3 个）的系统及数据安全风险评估服务，服务期内至少 1 次，判定系统及数据资产的重要程度，分析系统及数据资产面临的安全威胁，并计算风险值，为下一步数据分类分级防护提供技术支撑。

（1）按照《信息安全风险评估规范 GB/T20984》，提供科学规范的风险评估方案、工具及人力技术支持。确定资产风险等级，选择安全控制措施，制定风险处置计划，进行残余风险分析。

（2）风险评估实施方法应包括调查问卷、现场访谈、人工审计、工具检查等方式，从技术层面和管理层面进行评估。

（3）风险评估内容需包括数据资产评估、威胁评估、脆弱性评估、风险综合分析、风险处置计划等。

（4）数据资产识别。识别业务逻辑、业务功能、业务流程步骤等内容，调查信息系统收集、存储、使用了哪些业务数据，同时识别业务数据类型、数据所在位置、数据量、保存方式（信息系统、终端、文档服务器）等内容，并形成《数据资产清单》。

（5）数据重要程度分析。根据不同类别数据遭篡改、破坏、泄露或非法利用后，可能对党政机关、公共机构、其他机构、自然人等带来的潜在影响，对数据进行分级，并形成《数据分级建议方案》。

（6）数据威胁识别。能够识别数据生命周期各个阶段的威胁，包括数据采集威胁、数据传输威胁、数据存储威胁、数据共享和处理威胁、数据销毁威胁等。并提供防范相应威胁的建议，并形成《数据威胁及防护措施》。

（7）数据脆弱性识别。能够通过人工或工具对数据实体进行梳理，发现存在的敏感数据，并根据数据类别和级别确定数据实体的脆弱性，并形成《数据脆弱性分析报告》。

（8）系统脆弱性识别。能够通过人工或工具的方式对技术脆弱性进行识别，包括被评估范围的相应物理环境、网络结构、系统、应用系统等，能够从组织和流程管理角度对管理脆弱性进行识别，包括组织管理、流程管理等。应利用综合方法评估系统面临的网络安全风险，针对风险情况制定科学合理的整改方案，并形成《系统脆弱性分析报告》。

（9）评估后需出具《风险评估综合报告》《资产赋值列表》《威胁赋值列表》《脆弱性赋值列表》等。

四、实施要求

供应商应制定详细的服务实施方案，保证服务项目顺利实施。

1、供应商需提供素质高、专业性强、经验丰富、稳定的运维团队，7*24 小时及时响应；团队人员应包括包括 1 名以上项目经理、3 名以上专业技术人员，且人员需具备相应技术能力。在服务期内，供应商服务质量如达不到采购人要求，必须予以整改，并按规定予以处罚。一个月内整改不到位，采购人有权终止合同。服务期结束，采购人组织对供应商服务质量进行考核评估。

2、采购人邀请专家或委托第三方测评机构实施考核，综合考核因素包括：用户满意度、用户培训、服务能力、平台稳定性、故障处置分析能力、技术人员能力、应急响应能力、重大事故发生率、规范制度等。

3、成交供应商需按照采购人要求，与采购人以及相关运维人员等签订保密协议，确保数据安全。

4、供应商应提供与服务工具相关的所有技术文档和资料（含项目实施及验收报告等）。

5、成交供应商应保证所提供的服务或其任何一部分均不会侵犯第三方的专利权、商标权或著作权。如出现涉及此项目的知识产权纠纷问题，一律由成交供应商承担。

五、商务要求

（一）服务期限及地点

期限：服务时间从合同签订之日至 2022 年 12 月 31 日；

地点：采购人指定地点；

（二）付款方式

在项目开始实施后 10 个工作日之内支付项目服务费的 70%，项目服务期结

束前进行考核，考核合格后支付项目服务费的30%。

（三）其他要求

采购人根据国际国内形势，需要加强安全保障时，成交供应商应按采购方要求提供相应的安全服务。

（四）验收要求

按照《关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕 205号）号文件规定及磋商文件的规定进行验收。