越牛新闻平台网络安全服务

采购技术参数

一、 采购标的

序号	采购内容	数量	预算（元）	要求
1	越牛新闻平台网络安全服务	1 项	60000	详见参数

二、 越牛新闻平台网络安全服务采购参数

2.1 漏洞评估服务

序号	采购参数要求	备注
1	**服务描述：** 提供对各类系统的安全漏洞发现能力，客观分析安全风险等级，并根据检测结果和危害分析，适度修复安全漏洞和系统中的错误设置，在黑客攻击前开展防范措施，提高黑客的攻击成本，拉长黑客的攻击周期。	
2	**服务内容：** 1、安全漏洞检测：如操作系统、中间件、B/S 业务系统、数据库等漏洞。 2、业务逻辑漏洞检测：如后台登录处存在逻辑错误，登陆时没有错误次数限制用户登录，并且没有判断验证码过期，导致验证码可以重复使用，可被爆破用户名密码或撞库。 3、Webshell 检测：如网页后门程序、线程插入后门程序、扩展后门程序。 4、安全基线核查：如端口策略、账户策略、系统策略、应用策略以及中间件策略缺陷核查。 5、弱口令核查：密码字典爆破测试。 6、APP 客户端检测:对功能调用、系统组件、接口、漏洞等安全风险进行综合评估。	
3	**服务人数：**2 人	
4	**服务人员：**安全服务工程师	
5	**服务方式：**现场服务	
6	**服务范围：**越牛内网以及外网	
7	**服务频率：**4 次/年	
8	**服务输出：**《漏洞评估报告》	
9	**工具要求：**	

	支持检测的漏洞数大于 230000 条，兼容 CVE、CNNVD、CNVD、Bugtraq 等主流标准。 支持国产操作系统的漏洞扫描，包括麒麟（Kylin）、统信（UnionTechOS）、中兴新节点（NewStartCGSL）等。（提供截图并盖章） 支持操作系统、网络设备、数据库、中间件等漏洞扫描。（提供截图并盖章） 支持采用 SMB、RDP、Telnet、SSH 等协议对系统进行登录扫描。 ▲支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB 漏洞扫描、基线配置核查六种任务类型，其中全面扫描支持系统漏洞扫描、WEB 漏洞扫描、弱口令扫描同时执行。（提供截图并盖章） ▲提供检测结果综述分析，按照等保 2.0 的检测项要求，统计客户业务系统存在的不符合、部分符合、符合、待确认、不适用检测项，直观了解自身业务系统合规情况。（提供截图并盖章） ▲产品支持对系统漏洞、WEB 漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB 漏洞扫描、基线配置核查、弱口令扫描结果的报表。（提供截图并盖章）	

2.2 渗透测试服务

序号	采购参数要求	备注
1	**服务描述：** 站在黑客视角，实战化演练，采用无害攻击手段，模拟黑客真实的攻击行为，深度检验网络安全防线效果，为越牛新闻信息化安全建设方向提供有效依据。	
2	**服务内容：** 尝试验证每一个漏洞的真实威胁，同时查清漏洞的成因，做到自主可控可防，测试完成后，提出专业修复建议，协助解决安全问题。 渗透测试主要内容如下： ■ **Windows 系列操作系统渗透测试包括：** 1)端口扫描；2)NetBIOSnameservice 测试；3)RFC 漏洞攻击；4)SMB 漏洞攻击；5)WindowsDNS 测试；6)Snmp 漏洞测试；7)活动目录测试；8)SqlServer 弱口令测试；9)系统弱口令测试；10)终端服务弱口令测试；11)IIS 权限及溢出测试；12)Exchangeserver 漏洞测试；13)ftp 弱口令测试。 ■ ***nix 系列主机操作系统渗透** SOLARIS、AIX、LINUX、SCO、SGI 等操作系统渗透测试包括: 1)端口扫描；2)ssh 弱口令测试；3)telnet 弱口令测试；	

	4)Ftp 弱口令测试；5)Samba 弱口令测试；6)RPc 枚举和漏洞测试；7)NFS 漏洞测试；8)Snmp 漏洞测试；9)DNS 漏洞测试；10)rlogin,rsh 漏洞测试。 ■ **数据库系统的测试** 对 MS-SQL、ORACLE、MYSQL、DB2 等数据库应用系统渗透测试： 1)默认账号及弱口令攻击；2)存储过程漏洞攻击；3)数据库运行权限探测；4)提权漏洞攻击；5)低版本溢出漏洞攻击。 ■ **WEB 应用系统渗透** 对渗透目标提供的各种应用，如 JSP、PHP 等组成的 WEB 应用渗透测试： 1）检查应用系统架构、防止用户绕过系统直接修改数据库；2）检查身份认证模块，防止非法用户绕过身份认证；3）检查数据库接口模块，防止用户获取系统权限；4）检查文件接口模块，防止用户获取系统文件；5）检查其他安全威胁。 ■ **网络设备渗透** 对防火墙、入侵检测系统、网络设备进行渗透测试： 1)tftp 获取配置攻击；2)管理界面默认账号密码；3)snmp 读写权限攻击；4)telnet,ssh 默认账号弱口令攻击；5)低版本溢出漏洞攻击。 ■ **口令猜解** 口令猜测也是一种出现概率很高的风险，几乎不需要任何攻击工具，利用一个简单的暴力攻击程序和一个比较完善的字典，就可以猜测口令。 对一个系统账号的猜测通常包括两个方面：首先是对用户名的猜测，其次是对密码的猜测。 ■ **其他方面渗透** 除了上述的测试手段外，还会在渗透测试过程中使用的技术： 1)社会工程学；2)客户端攻击；3)拒绝服务攻击；4)中间人攻击。	
3	**服务人数：**2 人	
4	**服务方式：**现场或远程服务	
5	**服务范围：**越牛内外网重要业务系统	
6	**服务频率：**4 次/年	
7	**服务输出：**《渗透测试报告》	

2.3 应急演练服务

序号	采购参数要求	备注

1	**服务描述：** 应急演练服务/攻防演练围绕网络安全攻击场景，结合市局风险控制策略，制定或完善风险控制应急预案体系；以应急预案为基础，制定应急演练服务/攻防演练方案，通过应急预案和演练方案的培训，使管理人员明确其在演练过程中的职责范围、报告与指挥关系，明确应急处置的操作规范和操作程序。在演练的实施过程中，提供模拟网络攻击，协助工控环境单位、实施应急响应工作，包括预警与评估、应急响应预案启动和应急处置工作。在应急演练服务/攻防演练结束后，对演练过程进行分析和回顾，协助撰写应急演练情况总结报告，并开展应急演练工作的审核，以确定改进目标和改进的具体工作内容。演练总结报告、演练审核结果作为策划阶段各项工作的改进要素，持续完善应急体系。	
2	**服务内容：** 1.演练准备工作阶段：确定演练攻击与防守的目标系统、场景和方式等，建立专项工作组织架构，编写初步演练脚本。 2.演练环境搭建阶段：基于演练场景进行环境搭建，初步形成应急演练的演示环境，进一步确定演练环境、系统、攻击展现方法和防守展现方法，根据演练地点位置，搭建、测试与调试演练系统环境。 3.演练剧本编写阶段：按照演练场景编写具体的工作操作指导手册，形成演练脚本，指导工作开展。 4.演练彩排工作阶段：通过多次应急演练排练，在过程中及时发现问题，并进行完善，确保正式演练的顺利开展。 5.正式演练大会阶段：通过正式应急演练，来表现和传达日常应急响应工作要点，提高应急响应工作效率。	
3	**服务人数：**2-3 人	
4	**服务方式：**现场服务	
5	**服务频率：**1 次	
6	**服务输出：**《应急演练报告》	

2.4 安全巡检服务

序号	采购参数要求	备注
1	**服务描述：** 通过人工现场巡查方式对全网重要信息系统（业务系统、安全系统、网络系统）的运行状态、安全策略以及日志等风险进行识别、分析和定位，提出可行性修复建议，协助现场处置。	
2	**服务内容：** 基础检查	

	1、各系统运行状态检查。 2、物理环境风险检查。 3、版本、特征库及策略更新。 专业检查 1、安全事件分析与处置。 2、业务系统后门检测。 3、弱口令核查，复用口令核查。	
3	**服务人数：**1 人	
4	**服务方式：**现场	
5	**服务对象：**越牛安全设备巡检排查	
6	**服务频率：**4 次/年	
7	**服务输出：**《安全巡检报告》	

2.5 安全意识培训服务

序号	采购参数要求	备注
1	**服务描述：** 安全讲师为越牛职工进行网络安全意识培训，通过课堂演示、案例剖析等多个维度的授课方式，将安全意识有效地传递下去，不断规范其日常工作、生活操作行为，实现信息安全"人防"保障业务高效稳定运行。	
2	**服务人数：**1 人	
3	**服务方式：**现场	
4	**服务对象：**越牛职工	
5	**服务频率：**1 次/年	
6	**时间要求：**培训时长约 45 分钟	
7	**服务输出：**《安全意识培训定制 PPT》	

2.6 应急响应服务

序号	采购参数要求	备注
1	**服务描述：** 在发生确切的网络安全事件时，应急响应实施人员将及时采取行动，限制事件扩散和影响的范围，检查所有受影响的系统，在准确判断安全事件原因的基础上，提出基于安全事件解决方案，追查事件来源，协助后续处置。	

2	**服务人数：**1-2 人	
3	**服务方式：**现场	
4	**服务对象：**所有网络安全事情，按需响应	
5	**服务频率：**全年	
6	**▲时间要求：**不限次数。30 分钟内抵达客户现场，2 小时内定位问题，4 小时内控制风险、事件。（提供响应证明材料，如营业执照并加盖供应商公章）	
7	**服务输出：**《应急响应处置报告》	

2.7 重要时期安全保障服务

序号	采购参数要求	备注
1	**服务描述：** 通过人工驻场的方式在重要时期为我单位提供威胁实时监控，日志分析、事件处理及加固等工作，实时处理信息系统中存在的安全问题，最大限度降低组织信息系统的安全风险。	
2	**服务内容：** 1、安全评估：通过安全扫描工具定期对信息系统进行漏洞扫描和配置检查；为越牛内部的相应迎检及对内/外检查工作提供技术支持。针对安全漏洞事件、安全检查事件、网络攻击事件、安全检查工作结果，收集加固方法及验证方法，协助相关供应商运维人员进行漏洞修复； 2、安全防护：持续关注网络、系统运行情况，一旦发生安全事件，及时分析安全系统及设备的事件日志，配合甲方进行事件的追踪定位。定期通过对项目范围内所有安全系统及设备的报警日志进行分析，梳理客户近一月的信息安全情势、安全状况，提出改进建议。 3、安全预警：及时准确的通报以国内外权威漏洞发布公开站点为主要数据源的安全漏洞信息（如 CVE、NVD、Bugtraq、CERT 等）；以“周”为单位，生成漏洞通报报告，漏洞信息包括 CVE 编号、Bugtraq 编号、漏洞名称、漏洞描述、漏洞类型、受影响的系统或软件、危险等级、发布时间、修复方式等。 4、安全响应：在发现或发生安全事件后配合相关汇报、跟踪、处置、总结汇报、记录工作。	
3	**服务方式：**现场服务、远程服务	
4	**服务人数：**1-2 人	
5	**服务次数：** 按需响应	

三、 商务要求

1、供应商须是具有本项目供货服务能力的独立法人资格的供应商。供应商一旦参与报价，即视为供应商已熟悉且愿意接受本采购文件的所有要求，且自愿承诺：若中标后违约，视作欺诈行为，自愿列入失信黑名单。

2、实施服务时必须保证业务的稳定性和完整性，否则，造成的一切损失由供应商承担后果。参加报价前，供应商可进行项目现场沟通，了解实际情况，并出具项目服务要求所需的相关证明（做成附件同报价文件一起上传）。供应商需严格按具体采购要求进行响应，如响应参数有误或者未按要求进行响应，视为无效报价。

3、▲供应商应严格按照标书和国家法律法规及有关行业标准提供服务，确保服务质量。**供应商需具有中国网络安全审查技术与认证中心颁发的信息安全“风险评估”服务资质；入选地市级及以上网信办和公安技术支撑单位的。**

4、采购人按常规检查与年终考核相结合，对服务质量进行检查和考核。检查：供应商按照采购文件中的服务要求及时向采购人提交各阶段交付成果，采购人根据供应商提交的交付成果进行常规检查，传达意见和建议， 促进此项工作良性的持续发展。合同期内，供应商若达不到合格服务标准，采购人对供应商提出限期整改，并有权要求承担相应违约金。考核：合同期内，供应商响应不及时的，每滞后 1 天，扣减服务费¥4000 元；有现场服务要求的，每缺 1 次(每 24 小时计 1 次)，扣减服务费¥4000； 若本次采购范围内的网络和信息安全出现重大安全事故， 被上级部门或区级网络和信息安全管理书面点名批评的，扣除年合同价的 20%并取消下一年度续签资格（以下二种情况除外：供应商确已尽到服务职责的，该事故确由第三方明显责任人直接导致的；确属其他不可抗力因素导致的）。

5、供应商应提供不限时间、不限数量的售后电话支持服务，在得到需求指令后 30 分钟内响应，通过电话给出解决方案，不能通过电话解决的，在 1 小时内到达现场，24 小时内排除故障，所产生的费用由供应商负责。供应商应指定专门的联络人，负责本项目的技术咨询、软硬件维护的接洽工作。合同期内，供应商不得单方面变更项目服务人员，因人员离职等原因确需变更项目服务人员的，应先行提交人员变更说明函，并附上变更工程师的相关资料并盖章确认，并提前做好工作交接，避免出现空档期。

6、保密原则：各供应商应对各相关信息严格保密，未经授权不得泄露给任何单位和个人，不得利用此信息进行任何侵害采购人的行为，否则采购人有权追究供应商的责任。

7、服务期限：从合同签订日开始的 1 年。

8、付款方式：服务合同签订后 20 个工作日内支付年合同金额的 50%；供应商按要求完成整体服务后，经采购人考核符合要求的，20 个工作日内支付余下合同金额的 50%。