漏洞扫面系统和安全运维服务招标公告

安信农业保险股份有限公司（以下简称“征集人”）现邀请合格的供应商（以下简称“应征人”）就征集人所需项目进行项目征集，征集人将择优选定中选人，欢迎符合条件的应征人前来参与方案比选，现将有关事项公告如下。

1. 征集项目内容
2. 设备数量

漏洞扫面系统1台，安全运维服务

1. 设备要求

设备及设备附属配件均为原厂提供。

1. 应征人必须具备的条件：
2. 应征人须为原厂商或授权代理商，所投产品品牌为国内外知名品牌，所投服务器产品性能可靠，不少于三年市场应用案例。
3. 应征人必须具有独立法人资格，具有独立承担民事责任的能力，具备相应的经营范围且其注册资金或净资产（所有者权益）必须不小于 1000（含）万元人民币（或等值外币）。
4. 应征人必须具有专业团队，具有较强的售前、售中和售后服务支持能力，提供7\*24报修服务电话及固定的客户服务经理，省会城市、一类城市、直辖市均需要有办事处及备件库。提供全国性服务网点的证明材料。
5. 应证人在最近三年内未因自身任何违约、违法行为及违反商业道德的行为而导致取消参选资格、合同解除或败诉。
6. 法定代表人为同一个人的两个及两个以上法人，母公司与全资子公司/由其控股的子公司，不得同时参加本项目。
7. 法律、行政法规规定的其他条件。
8. 应证人需提供厂商对本项目的授权书。
9. 售后服务要求
10. 应证人应为征集人提供及时周到的系统技术支持。
11. 应证人应确保为甲方提供7\*24小时技术支持服务，响应时间不应该超过1小时，现场响应支持不应超过4小时。
12. 应证人所提供设备保质期均为三年（具有特殊要求的除外），集成商所提供的设备在保质期内因硬件、软件本身质量问题所造成的损坏或无法正常运行，由此产生的维修、更换硬件和软件故障排除等所需一切费用（包括工程师差旅费用等支出）由集成商负责。
13. 应证人应提供相应的备件支持，以便及时更换损坏硬件。
14. 应证人应在质保期后设备生命周期内有义务继续对系统设备提供维保服务，甲方将支付相应费用。
15. 针对以上要求，应证人可提供具体可行的有吸引力的合作方案。
16. 验收
17. 所有设备均需提供安装服务，所采购设备（包括软件）安装都必须由生产厂商授权集成商执行。
18. 安装前由征集人信息技术部协同征集人行政办公室对货物的品牌、数量、包装等方面进行实物验收。征集人提供的所有包装的货物均应完好无损。如遇交付前已拆封的货物，征集人有权拒绝或要求更换。应证人交货时，必需提供所有产品原厂或总代理出具的供货相关证明。
19. 应证人根据征集人技术要求在征集人信息技术部指导下进行设备安装、调试，并由征集人信息技术部进行使用性能方面的验收。
20. 报名方式

有意者请于2019年9月13日之前将标书及相关材料送至以下地址：上海市静安区共和新路3651号 顾晓磊收

联系人：顾晓磊

联系方式：021-66988356 guxl@aaic.com.cn

1. 举报邮箱：[kehufuwu@aaic.com.cn](mailto:kehufuwu@aaic.com.cn)
2. 招标参数要求
3. 漏洞扫面系统

|  |  |
| --- | --- |
| 基本需求 | 产品要求为国内开发，具备自主知识产权，并经过十年以上应用检验，厂商应承诺产品的高度稳定性和可靠性。 |
| 产品应该是被广泛应用的成熟产品，在国内市场具有较高的市场份额，国内市场占有率近五年排名在不低于前三名。须提供知名第三方机构（如IDC）出具的市场占有率有效证明材料。 |
| 投标设备应支持热插拔的冗余双电源，避免电源硬件故障时设备宕机，提高设备可用性。 |
| 产品需为2U机架式设备，含1个RJ45串口，至少7个电口（包括1个管理口，6个扫描口），1个接口扩展槽位（支持4电、4光、8电、8光）。 |
| 产品应支持多路扫描功能，可以同时对多个隔离网络进行脆弱性检测。 |
| 产品需采用B/S设计架构，系统配置文件和扫描结果文件需加密保存在本地，并采用SSL加密通信方式，无须安装客户端，用户可通过浏览器远程方便的对产品进行管理。 |
| 支持将按IP范围、起止时间、任务名称、任务状态、漏洞模板、用户等对扫描任务进行筛选和结果汇总，并生成报表，请提供功能截图。 |
| 厂商资质 | 厂商应具备足够的信息安全服务技术实力及安全服务保障能力，获得中国信息安全测评中心颁发的信息安全服务安全开发类一级资质证书，提供证书复印件证明 |
| 厂商应具备足够的信息安全服务技术实力及安全服务保障能力，获得中国信息安全测评中心颁发的信息安全服务安全工程类三级资质证书，提供证书复印件证明 |
| 厂商应具备足够的安全运维服务保障能力，获得中国网络安全审查技术与认证中心颁发的信息系统安全运维（一级）服务资质，提供证书复印件证明 |
| 厂商应具备足够的安全应急响应能力，获得CNVD网络安全应急服务支撑单位（国家级）证书，提供证书复印件证明 |
| 厂商为微软MAPP成员，并有48小时内发布产品版本响应微软紧急安全公告能力。请提供微软证明。 |
| 厂商应具备十年以上漏洞研究经验和独立漏洞发掘能力，自主发现且公开详情的CVE漏洞数量不少于90个，且获得漏洞厂商安全公告致谢不少于60次，请提供漏洞列表和致谢截图证明。 |
| 请提供与漏洞扫描相关的公开专利，要求数量不少于5个，请提供证明 |
| 厂商应具备完善的服务保障体系，拥有总部、分公司、办事处三级技术支持平台，提供统一的免费服务热线，为客户提供高效及时的支持服务 |
| 产品资质 | 公安部颁发的《计算机信息系统安全专用产品销售许可证(增强级)》， |
| 国家版权局颁发的《计算机软件著作权登记证书》， |
| 网络关键设备和网络安全专用产品安全认证证书 |
| 中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书(EAL3+级)》， |
| IPv6 Ready证书 |
| 产品功能 | 单机扫描速度不低于600ip/h。（不同型号详情见规格功能表） |
| 允许最大并发扫描≥90个IP地址，允许最大并发任务≥15个任务，支持无限IP授权扫描。（不同型号详情见规格功能表） |
| 支持检测的漏洞数大于40000条，其中含CVE编号的系统漏洞不少于30000条，兼容CVE、CNCVE、CNNVD、CNVD、Bugtraq等主流标准，并提供CVE Compatible证书。 |
| 产品支持对系统漏洞扫描、web应用和网站漏洞、配置合规、弱口令进行检查和综合分析，并进行统一授权管理，请提供证明。 |
| 针对每一个漏洞显示漏洞详细信息，包括但不限于漏洞名称、漏洞描述、解决方案、补丁下载链接、危险分值、CVSS评分、发现日期、CVE编号、CNVD编号、CNNVD编号等。 |
| 支持扫描国产操作系统、应用及软件的安全漏洞，如红旗、麒麟、起点操作系统漏洞扫描，请提供功能截图和支持的漏洞列表。 |
| 支持针对大数据组件框架的漏洞检测，如Elasticsearch、Splunk、Hdoop、ZooKeeper 等漏洞扫描，请提供功能截图和支持的漏洞列表。 |
| 支持扫描主流虚拟机管理系统的安全漏洞，如VMWare、Hyper-V、VirtualBox、KVM等漏洞扫描，要求大于300条，请提供功能截图和支持的漏洞列表。 |
| 支持专门针对DNS服务的安全漏洞检测，包括DNS投毒等漏洞检测能力；支持“幽灵木马”检测；请提供功能截图和支持的漏洞列表。 |
| 支持专门针对已有攻击利用代码的漏洞检测，检测用户资产是否存在可利用的漏洞，请提供功能截图和支持的漏洞列表。 |
| 支持Oracle、MySQL、MS SQL、DB2、Sybase数据库漏洞检查，要求大于1400条，请提供功能截图和支持的漏洞列表。 |
| 支持弱口令检测功能，包括但不限于RDP、SMB、TELNET、FTP、SSH、POP3、TOMCAT、SQL SERVER、MYSQL、ORACLE、SYBASE、DB2、SNMP协议。 |
| 支持同时进行漏洞扫描和配置核查。 |
| 支持智能端口挖掘，可以智能发现非默认端口启动的服务，请提供功能截图。 |
| 具备快速应急漏洞响应能力，可在紧急漏洞爆发后第一时间提供检测插件。请提供功能截图和应急插件发布链接（数量不少于10个）。 |
| 内置20种以上漏洞策略模板，如Unix、Windows操作系统、网络设备和防火墙、数据库等扫描策略模板，同时支持用户自定义扫描策略模板；请提供功能截图 |
| 支持自定义漏洞策略模板，并支持自定义漏洞模板的导入和导出。 |
| 支持自动漏洞策略模板过滤器功能，升级包中符合定义条件的漏洞可自动添加到自定义漏洞模板中，无需每次手动添加。 |
| 支持自动模板匹配技术，可根据目标检测系统自动匹配相应模板，请提供功能截图。 |
| 支持立即执行、定时执行、周期执行扫描任务，自定义的周期时间可精确至每N月第N个星期几的几点，请提供功能截图。 |
| 支持自定义扫描任务策略，包括但不限于扫描IP范围、扫描端口、执行方式、登录检查、扫描深度、超时限制、扫描前提示被扫描主机等。 |
| 支持保存任务配置，并可复用，请提供功能截图。 |
| 支持实时显示扫描结果，包括扫描进度、主机存活数、预计扫描时间、扫描到的漏洞风险信息等，请提供功能截图。 |
| 支持断点续扫，以应对断电、突发网络状况和设备故障，能够对已经完成的扫描结果进行实时保存，可对已完成的扫描任务中没有被覆盖到的目标重新下发扫描任务，请提供功能截图。 |
| 弱口令检测允许外挂用户提供的用户名字典、密码字典和用户名密码组合字典，支持对外挂的用户名和密码自动组合，请提供功能截图。 |
| 支持漏洞登录检查和配置核查登录认证信息统一管理，无须每次下任务时单独配置，可自动填充，请提供功能截图。 |
| 产品应支持通过多种维度对漏洞进行检索，包括但不限于CVE ID、BUGTRAQ ID、CNCVE ID、CNVD ID、CNNVD ID、MS 编号、风险等级、漏洞名称、是否使用危险插件、漏洞发布日期等信息。 |
| 产品应支持任务查询，包括但不限于 |
| 产品应支持限制使用带宽 |
| 支持通过仪表盘直观展示资产风险值、主机风险等级分布、资产风险趋势、资产风险分布趋势等内容，并可查看详情，请提供功能截图。 |
| 支持风险告警和风险闭环处理，可配置告警内容、告警方式、告警资产范围等，支持邮件和页面告警，请提供功能截图。 |
| 产品支持对误报漏洞进行修正，并允许用户将修正结果体现在新生成的报表结果中。 |
| 提供通过资产树状结构对资产进行分级管理，可在资产树上直接指定主机开展扫描任务。请提供功能截图。 |
| 支持单个或批量配置漏洞风险状态，如确认、误报、忽略等。 |
| 支持自定义风险值计算标准配置，可对主机风险等级评定标准和网络风险等级评定标准进行自定义，请提供功能截图 |
| 可以通过多种维度搜索定位资产和查看资产风险，包括并不限于：节点或设备名称、资产IP范围、资产管理员、资产操作系统类型、资产风险等级、漏洞名称、开放的端口、资产banner信息等，请提供功能截图。 |
| 支持在线查看展示各部门节点和主机资产风险分布、漏洞分布、配置合规和脆弱账号风险详情，请提供功能截图。 |
| 支持与微软WSUS补丁系统的联动，能够在发给主机管理员的邮件中附带自动配置WSUS的注册表文件，方便进行自动化的补丁修补，请提供功能截图证明。 |
| 支持与堡垒机联动，自动获取目标设备账号密码信息，便于登录检查。 |
| 支持与防火墙设备进行联动，展示漏洞防护情况。请提供功能截图证明。 |
| 支持HTML、WORD、EXCEL、PDF、XML报表格式。 |
| 可输出同时包含漏洞扫描和配置核查结果的报表，请提供功能截图。 |
| 支持扫描任务完成后自动生成报表，并发送到指定邮箱或上传到FTP服务器，请提供功能截图。 |
| 内置针对不同角色的报表模板，请提供功能截图 |
| 支持报表模板自定义，可自定义报表标题、封面logo、报表页眉和页脚、报表各章节显示内容，请提供功能截图。 |
| 支持高级数据分析，可对同一IP的两次扫描结果进行风险对比分析，请提供功能截图。 |
| 支持将按IP范围、起止时间、任务名称、任务状态、漏洞模板、用户等对扫描任务进行筛选和结果汇总，并生成报表，请提供功能截图。 |
| 支持不同用户角色权限管理，区分系统管理员、普通用户、审计管理员等角色，不同管理员拥有不同的管理权限。请提供功能截图。 |
| 支持多用户分级权限管理，可为每个用户角色分配账号、任务权限分配、允许登录的IP范围和允许扫描的IP范围等, 请提供功能截图 |
| 提供日志审计功能，能够对登录日志、操作日志和异常报告进行记录和查询，请提供功能截图。 |
| 提供备份恢复机制，能够对系统创建还原点对系统进行备份和还原，请提供功能截图。 |
| 提供系统快照功能，当系统出现问题时，可以通过恢复快照，一次性将系统恢复到快照时的版本，并将用户数据一同恢复，请提供功能截图。 |
| 支持手动和自动升级，漏洞知识库至少每隔一周进行一次定期升级，请提供功能截图和升级站点链接 |
| 支持手动和自动系统时间同步 |
| 具备对外API接口，支持安全运营平台或其它安全产品通过该接口下发扫描任务以及获取检查结果。 |

1. 安全运维服务

|  |  |
| --- | --- |
| 厂商资质 | 1、具备中国信息安全测评中心颁发的信息安全服务安全工程资质（提供有效期内证明） |
| 2、其他安全资质至少5种（提供有效期内证明） |
| 3、其他安全资质至少10种（提供有效期内证明） |
| 与国内或国际漏洞组织有合作协议---如CVE、CNNVD、CNVD等（提供证明） |
| 近三年内有3家以上大型保险单位或国有、股份制银行等金融单位的安全服务的实施案例。 （提供证明） |
| 可提供在我司或者太保集团提供服务实施案例证明。（提供证明） |
| 1、近一年具备我司或者太保集团安全服务项目经验 |
| 2、近三年具备我司或者太保集团安全服务项目经验 |
| 3、近五年具备我司或者太保集团安全服务项目经验 |
| 人员资质 | 项目人员需80%以上具有本科学历 |
| 项目经理满足8年以上信息安全服务工作经验，具备CISSP、CISA、CISP、PMP资质等至少1项安全资质，并提供证书复印件。 |
| 项目人员或支持人员持有CISSP、CISA、CISP等安全资质证书（提供证明） |
| 安全驻场服务 | 提供每周一次的安全驻场服务，服务内容包括不限于以下内容： |
| 1、安信农保安全设备的巡检服务，监控安全设备的运行状态，以及系统规则库更新情况，发现问题及时提供完善建议； |
| 2、安信农保安全设备的日志分析，输出安全建议和优化方法。设备包含不限于ips、waf、漏扫等； |
| 3、安信农保的资产的漏洞扫描、应用资产扫描，及时发现漏洞，整合扫描报告的修复建议，形成一份可落实的修复方案； |
| 4、安信农保应用系统的渗透测试，及时发现应用系统漏洞并给具体加固建议； |
| 5、安信农保linux系统和Windows系统补丁更新方案撰写，提供详细的补丁升级建议； |
| 6、安信农保互联网资产口令检查，及时发现资产弱口令情况，提出整改清单； |
| 7、安信农保互联网资产梳理，暴露资产自查，全面发现公司的互联网资产暴露面，做到资产暴露面最小化控制； |
| 8、安信农保信息安全类方案协同编写，例如信息安全应急预案、安全建设方案等 |
| 培训服务 | 每季度提供一次4小时安全相关培训（培训内容由安信农保决定并提前1周通知） |
| 安全事件应急、重大保障服务 | 内外网信息安全事件现场分析处理高级技术支持。针对银保监会，补天，漏洞盒子等安全检测平台通报的应用安全问题提供专家验证服务。（说明方案） |
| 针对我司安发现的实际的或可疑的信息安全攻击事件，进行相关应急响应。国定假日、重大安全保障期间、监管机构安全检查抽查期间、重大安全事件期间提供远程和现场的技术支持。（说明方案） |
| 安全漏洞预警 | 对典型高危安全漏洞事件所曝露的问题，在外网进行漏洞排查。（提供技术支持方案说明） |
| 及时告知业界暴露的高危安全漏洞，如2014年OPENSSL心脏出血，Linux破壳漏洞等。包括具体漏洞漏洞验证方法（POC），漏洞利用方法（EXP），及漏洞利用条件，后果等。（提供技术支持方案说明） |