**附件1**

**招标内容及要求**

**1.安全运维服务**

**1.1服务范围要求**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **所属业务系统** | **域名或IP地址** | **服务器/虚拟机数量** | **等保定级** | **备注** |
| 1 | 福建省产品质量检验研究院门户网站 | 中文版门户网站：www.fcii.net 英文版门户网站：en.fcii.net | 1 | 二级 |  |

注：应用系统服务范围包括其支撑的网络设备、安全设备、服务器。

**1.2服务期限要求**

服务期限为自合同签订之日起1年。

服务项目预算：不高于9.9万元。

项目付款方式：签订合同后付合同金额的40%，完成第一季度和第二季度报告后支付合同金额的30%，服务完成最终报告后支付合同金额的30%。（发票应开具增值税专用发票）

**1.3服务内容要求**

**1.3.1网络与信息系统安全检测服务**

提供每季度1次派遣安全服务工程师到现场进行网络与信息系统安全检测，此项服务包括网络安全检测、主机安全检测、个人终端安全检测、系统安全检测、补丁升级、数据库维护服务。所有检测项目在检测后提供详细的检测评估报告,包括电子档材料。

|  |  |  |
| --- | --- | --- |
| **服务项目** | **服务内容** | **服务提供方式** |
| 安全检测 | 网络安全检测 | 梳理网络拓扑与设备清单。主要检查网络拓扑设计的合理性，是否符合相关规定要求以及设备清单等信息资料是否准确完整等。 | 每季度一次上门检测，全年4次，提供检测报告。 |
| 检测网络设备运行状况。主要检查交换机、路由器等网络设备是否运行良好，同时对网络设备的日志进行分析。 |
| 检测安全防护措施运行状况。主要检查防火墙、入侵防御、数据库审计、堡垒机、负载均衡等产品的运行情况，确保上述产品正常运行，防护规则更新及时，防护策略有效配置，防火墙访问控制策略优化，堡垒机账号使用情况检查，对安全产品日志进行分析，并协助处置。 |
| 主机安全检测 | 检测主机性能状况。主要检查主机运行的服务是否遵循最小化原则，关闭不必要的服务，降低业务风险。 |
| 检测补丁更新状况。主要检查操作系统补丁是否及时更新，是否存在安全漏洞等。 |
| 检测防病毒系统运行状况。主要检查主机是否安装防病毒系统，病毒库是否为及时更新升级，是否定期查杀病毒等。 |
| 检测主机授权管理和访问控制状况。主要检查主机是否制定详细的授权管理和访问控制策略，限制不必要权限。 |
| 检测主机身份鉴别状况。主要检查主机是否合理配置口令的复杂度及锁定策略等，是否存在多余默认账号和弱口令，能否有效降低被暴力破解的可能性。 |
| 扫描主机漏洞状况。通过专业工具扫描检查服务器主机、操作系统等是否存在安全漏洞和危险应用。 |
| 个人终端检测 | 终端系统安全风险扫描。通过专业工具扫描个人终端是否存在安全漏洞以、危险应用以及不必要的服务。 |
| 终端弱口令风险扫描。主要检查个人终端是否存在操作系统弱口令账号和应用程序弱口令账号。 |
| 终端恶意代码扫描。通过专业工具扫描个人终端是否存在恶意软件、恶意代码。 |
| 终端系统配置核查。主要检查个人终端是否按照标准配置安全策略、是否开启系统自动更新、是否关闭默认共享等。 |
| 系统安全检测 | 安全检测 | 检测包含不少于5个信息系统缺陷及风险，包括源代码危险函数使用、系统中身份认证安全、会话管理安全、上传下载、信息泄漏、数据验证等方面，评估系统在信息泄漏、数据破坏、身份仿冒等方面的安全风险。 | 每季度一次上门检测，全年4次，提供评估报告。 |
| 漏洞扫描 | 通过漏洞扫描的方式检查不少于5个指定的信息系统，是否存在安全漏洞和危险应用，包括sql注入、xss注入、恶意文件上传、命令执行等。 |
| 漏洞修复 | 对Linux系统扫描出的漏洞进行[定期打补丁修复](https://www.cnblogs.com/yxnchinahlj/p/9012529.html)。 |
| 补丁升级 | 补丁升级 | 提供2台服务器的补丁升级 | 每季度一次，一年4次 |
| 数据库维护服务 | 数据库优化 | 外部性能调整（系统级）、数据库调整(实例级)、应用层调优(sql级)。 | 每季度一次，一年4次 |
| 巡检服务 | 检查数据库及应用系统的配置健康情况、检查数据库及应用系统的性能健康情况、检查数据库及应用系统备份的完整性、检查数据库。 |

**1.3.2网站安全监控服务**

提供全年通过专业的网站安全监控平台对网站进行以下服务：

1. **网站可用性监控服务：**

全年每隔5分钟一次对网站首页进行轮询探测，网站访问不到则通过邮件或短信等方式进行告警，确保网站的可用性、安全性实时掌控。

1. **域名劫持监控服务：**

全年每隔5分钟一次对网站首页进行域名劫持探测，一旦发现域名被劫持则通过邮件或短信等方式进行告警。

1. **网页挂马监控服务：**

每周一次采用远程监控方式对网站页面进行网页挂马分析，一旦识别到网页挂马行为，则进行邮件或短信进行告警。

1. **网站暗链监控服务：**

每周一次采用远程监控方式对网站页面进行暗链分析，一旦识别到网页存在暗链行为，则进行邮件或短信进行告警。

1. **敏感内容监控服务：**

每周一次对关键网页的敏感内容进行监控，识别网站存在政治、低俗等敏感内容情况，并进行邮件或短信进行告警。

1. **网站监控人工告警服务：**

针对网站监控平台发现的问题，监控平台发送告警信息到监控值班人员的手机，由值班人员进行人工验证，确认为安全事件后，进行人工电话告警。

1. **网站安全监控报告：**

安全服务提供商定期汇总安全监控情况，并提交详细的监控报告。

**1.3.3应急保障及技术支持服务**

提供全年应急保障及技术支持，当发生安全事件时，可根据用户需求，安排安全工程师上门响应，工作时间1小时内响应，4小时内到达发生现场（市内）。提供信息安全技术支撑，协助用户快速定位问题，减轻或消除事件影响，同时协助进行事件取证并提供后续的防控建议和措施。

**1.3.4应急演练服务**

提供每年1次应急演练服务。服务主要包括以下内容：

**1) 网络与信息安全应急预案服务**

定制5个预案场景的《安全应急预案》。

**2) 网络与信息安全应急演练服务**

针对1个预案场景进行应急演练，并提交《安全应急演练报告》。

**1.3.5安全培训服务**

每年提供1次派遣资深的安全服务工程师到现场进行安全培训服务。培训服务内容可根据客户要求进行定制，主要分为以下两类：

A、安全意识培训：结合近期的网络安全热点事件、安全漏洞、安全技术，讲解日常工作中需要注意的安全问题和应对方法，帮助学员理解信息安全基本概念，树立信息安全意识，掌握日常安全防范意识。

B、安全技能培训：讲解日常安全保障工作中使用的安全技术、安全工具等，帮助学员了解安全的安全攻击手段及原理，并能够有一定的应对能力。

**1.3.6安全预警通告服务**

**1) 安全资讯通告**

提供每月一次电子邮件发送安全咨询，及时推送最新的信息安全相关资讯，如安全事件、安全技术、政策法规等，帮助用户及时掌握最新的信息安全态势，有效提升信息安全的意识和能力。

**2）重大漏洞/事件预警通告**

提供重大漏洞/事件发生24小时内电话通知用户，并给出初步的防控建议。当互联网爆发严重安全漏洞或重大安全事件时，及时通知用户并给出初步的风险排查和防控建议，最大程度减轻或避免用户受到安全漏洞或安全事件的影响，提供详细的事件或者漏洞说明，内容包括问题复现方法、解决修复方案和修复验证方法。

|  |
| --- |
| **附件2 投标人报名表** |
| 投标项目名称（编号及合同包号） |  |
| 报名投标单位名称及盖章 |  |
| 报名投标单位联系人及联系电话 |  |
| 报名时间 |  |

**附件3评分标准和方法**

| **序号** | **评分界定** | **分值** | **得分** |
| --- | --- | --- | --- |
| 1. **技术因素（满分70分）**

**（投标人技术部分的实际得分少于35分的，属于无效投标）** |
| 1-1 | 根据投标人响应文件对招标文件要求中安全服务范围、安全服务时间、安全服务内容及要求的逐项响应承诺情况进行评分，完全满足招标文件要求的得40分，每负偏离1项扣1分，最低得0分。 | 40分 |  |
| 1-2 | 投标人在本次在安全服务中所采用的服务工具能够对WEB源代码进行扫描，检查代码中的网页木马，网页挂马以及网页暗链，并支持自定义规则。 | 5分 |  |
| 1-3 | 投标人在本次安全服务中的资产分析服务所采用的服务工具能够对网络空间资产进行探测，探测展示结果包含不限于：操作系统、Web容器、开发语言、安全防护、端口、协议等；并可以展示模糊查询对象的IP、信息系统的应用开发语言、中间件及操作系统类型等；具有统计分析功能，可以统计站点、端口及IP数量；并提供截图。 | 5分 |  |
| 1-4 | 投标人在本次安全服务中所采用的服务工具能够实现主机配置变更监控服务，实现主机安全配置核查和变更状态监控。当关键服务器的安全配置一旦发生变化，能实时监测配置变更情况进行告警，对于可能的安全入侵行为进行告警，并提供功能截图。 | 5分 |  |
| 1-5 | 投标人在本次安全服务中所采用的服务工具能够对目标信息系统进行等保综合合规评估管理，可展示系统定级备案总体趋势、定级状态分布情况、定级结果分布的相关报表图形、并且展示定级相关的责任人、负责定级系统数、未开始定级、已定级、已备案、定级结果的列表，并提供截图。并提供截图。服务工具应为国产，具有投标人或所投安全运维服务提供商自主知识产权，具备定制化开发能力。提供《等级保护综合管理系统》的国家著作权证书复印件（原件备查）。 | 5分 |  |
| 1-6 | 投标人在本次安全服务中所采用的服务工具有采用基于网络安全的大数据处理系统技术，能够有效提高数据库数据的计算处理能力，从而提高安全服务实施质量。提供该技术的相关证书证明材。 | 5分 |  |
| 1-7 | 投标人在本次安全服务中所采用的服务工具有采用防泄密的服务器网络安全装置技术，能够有效避免在服务过程中的数据资产泄密，提供数据监管过程的安全性及有效性，提供该技术的相关证书证明材料。 | 5分 |  |
| **2、商务因素（满分20分）** |  |
| 2-1 | 投标人具备省级或以上网络与信息安全信息通报中心支撑单位证书，具备市级或以上网信办技术支撑单位，设置有市级或以上专家工作站，需提供相关证明材料复印件。每提供1项证明材料得2分，满分10分。 | 10分 |  |
| 2-2 | 投标人具备[NISP](https://zhuanlan.zhihu.com/p/171753267)、CISP信息安全服务资质证书需提供相关证明材料复印件。每提供1项证明材料得2分，满分10分。（注：须提供近6个月内任意一个月社保缴纳证明材料复印件，项目经理与团队成员各项证书均不重复得分） | 10分 |  |
| **3、价格因素（满分10分）** |  |
| 3-1 | 价格分采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算：投标报价得分=（评标基准价／投标报价）×100。因落实政府采购政策需进行价格扣除的，以扣除后的价格计算评标基准价和投标报价。 | 10分 |  |
| **各有效投标人的综合得分＝技术因素＋商务因素＋价格因素** |  |