附件1

报价单

报价方（盖章）：

日期：

联系人：

联系方式：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 名称 | 内容 | 维保费用（元/年） |
| 1 | 信息系统安全评估优化服务 | 网络架构安全评估、系统漏洞和配置扫描检查、安全加固等，详见附件2 |  |
| 2 | 支撑、保障服务 | 漏洞扫描和安全配置核查服务，安全巡检服务，安全日志采集、分析服务，详见附件2 |  |
| 合计： | |  |  |
| 备注：  项目服务内容以附件2为依据，报价方可提供补充服务内容并作为附件提交。 | | | |

附件2

项目服务内容

（一）服务规范

安全服务供应商所提供的所有服务应符合技术标准的要求如下：

1、符合有关标准(如ISO、IEEE、ITU-T、ETSI、IETF、OMA、3GPP等)的，安全服务供应商应在投标书中具体说明，并附上相应的详细技术资料。

2、若安全服务供应商的服务包含自己的专用标准，应在投标书中具体说明，并附上相应的详细技术资料。

3、遵循《信息安全技术 信息安全评估规范》（GB/T20984-2007），《信息安全技术信息系统安全等级保护基本要求》（GB/T22239-2008），《中华人民共和国计算机信息系统安全保护条列》。

4、安全服务还应依据自然资源部海岛研究中心（以下称甲方）已经发布的各类配置规范进行。

（二）服务原则

1、安全服务应严格遵守保密原则，对服务的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害甲方网络的行为，否则甲方有权追究安全服务供应商的责任。

2、服务方案的设计与实施应依据国内或国际的相关标准进行；

3、服务用的工具、方法和过程要在双方认可的范围之内，服务的进度要跟上进度表的安排，保证需求方对于服务工作的可控性；

4、服务的范围和内容应当整体全面，包括安全涉及的各个层面，避免由于遗漏造成未来的安全隐患。且服务中的过程和文档，具有严格的规范性，可以便于项目的跟踪和控制

5、服务工作应尽可能小的影响系统和网络的正常运行，不能对现网的运行和业务的正常提供产生显著影响（包括系统性能明显下降、网络拥塞、服务中断，如无法避免出现这些情况应在服务方案中详细描述）；

（三）服务内容

安全服务供应商应对自然资源部海岛研究中心信息系统所涉及的所有应用业务系统、网站系统、网上服务等系统。

1、信息系统安全评估优化服务

(1)在服务期内安全服务供应商为甲方提供业务系统评估优化服务，主要包括：网络架构安全评估、系统漏洞和配置扫描检查、安全加固等。该服务需严格参照下列标准进行：

* GB/T20984-2007信息安全技术 信息安全风险评估规范
* GB/T22239-2008信息安全技术信息系统安全等级保护基本要求
* GB/T22239-2008信息安全技术信息系统安全等级保护基本要求
* GB/T 20270-2006 信息安全技术网络基础安全技术要求
* GB/T 20271-2006 信息安全技术信息系统通用安全技术要求
* GB/T 20272-2006 信息安全技术操作系统安全技术要求
* GB/T 20273-2006 信息安全技术数据库管理系统安全技术要求
* GB/T 20228-2007 信息安全技术服务器安全技术要求
* GB/T 21050-2007 信息安全技术网络交换机安全技术要求
* GB/T 18018-2007 信息安全技术路由器安全技术要求
* GB/T 20988-2007信息系统灾难恢复规范

(2)安全服务供应商应依据相关规范对项目范围内所涉及的所有防火墙、路由器、交换机、服务器等设备的安全配置的合理性进行检查。并根据合理的业务数据流和运维管理数据流提出安全设备部署位置建议，实施策略优化调整或提出优化建议。

(3)安全服务供应商应对每次评估的结果进行综合分析，形成评估报告。要求提供的报告列表如下，但不限于以下内容：

**评估阶段最终报告，内容应当包括：**

* 漏洞评估，要求包括但不限于以下方面的漏洞分析：网络结构、网络设备、安全设备、主机设备。
* 风险评估，说明风险计算方法，要求包括但不限于以下方面的风险分析：网络结构、网络服务、网络设备、设备配置、主机系统、安全策略。
* 应对风险的结果进行统计分析，形成风险分布统计报表、风险严重程度统计报表；并在安全服务方案中提供图样示例。

**业务系统信息安全优化方案和实施建议，并应注意以下几点：**

* 实施风险削减建议的优先度，便于甲方在评估后根据揭示出的安全风险建立实施风险管理的计划；
* 提请注意风险削减与实施费用的平衡控制，做到适度安全；
* 提出的具体整改措施、方案、建议等，应覆盖所有评估内容

**评估过程报告**

* 《XXX业务系统主机设备安全漏洞扫描报告》；
* 《XXX业务系统主机设备安全配置检查报告》；
* 《XXX业务系统主机设备安全加固方案》；

**安全优化过程报告**

* 《XXX业务系统主机设备安全漏洞扫描对比分析报告》；
* 《XXX业务系统主机设备安全配置对比分析报告》；

**项目管理报告**

* 《项目实施进展周报》

2、支撑、保障服务技术要求

（1）漏洞扫描和安全配置核查服务

安全服务供应商需提供自合同签订后1年期的漏洞扫描和安全配置核查服务，服务频度每半年一次，全年不低于2次。

**实施风险控制**

在进行漏洞扫描和安全配置核查前，安全服务供应商需进行小范围的模拟试验，检验漏洞扫描和安全配置核查的有效性和安全可靠性。

在漏洞扫描和安全配置核查过程中安全实施顾问会对操作的每一个步骤及系统状态进行详细记录，一旦发现异常立刻退回上一步。

在漏洞扫描和安全配置核查过程中，需要甲方相关人员全程跟进，对要检查的系统进行确认，对可能存在的风险由安全服务供应商及时提出，确认后再进行漏洞扫描和安全配置核查。

**漏洞扫描和配置核查服务框架**

漏洞扫描服务主要包括：

* 弱口令扫描，至少包含以下应用的弱口令：FTP、SNMP、Telnet、SSH、SYBASE、Oracle、MySQL、MSSQL等；
* 系统漏洞：Windows、AIX、HP-UX、等操作系统漏洞、系统后门；
* 网络设备漏洞：Cisco、华为、H3C、PIX firewall、等网络设备漏洞；
* 数据库及应用服务漏洞：MS SQL Server、MySQL、Oracle、Apache、IIS、Tomcat、WebLogic、等漏洞；
* 对互联网开放的系统是否开启telnet、ssh、远程桌面、pcanywhere等常用维护端口（23、22、3389、5631、5632等）但是没有严格限制访问原IP；
* Web应用漏洞：Web服务器是否存在测试页面、后台登录是否有限制、Web页面是否存在SQL注入、跨站等漏洞；

本项目中安全服务供应商使用的漏洞规则库应保持最新状态，每条漏洞具有CVE编码，并提供详细的漏洞描述和加固建议措施。

安全配置核查服务有：

根据专用安全配置规范，安全服务供应商将针对以下业务数据网络系统提供安全配置配置核查服务：

* 主机设备：Windows、AIX、HP-UX、Linux、Solaris、UNIX
* 网络设备：Cisco、华为、H3C、Juniper、PIX firewall、NetScreen Firewall
* 业务系统：MS SQL Server、MySQL、Oracle、Apache、IIS、Tomcat、WebLogic、Informix、BIND、Web、DNS

本项目中安全服务供应商使用的安全配置核查工具应支持的足够数量的检查模板，能够支持自定义安全配置核查的模板。

**输出成果**

每次漏洞扫描和安全配置核查检查完成后，安全服务供应商需向甲方提交不同业务系统的《漏扫扫描报告》、《漏扫扫描加固建议》、《安全配置核查报告》、以及建立各个业务系统每台服务器开放端口、服务的安全配置核查清单。

其中，《漏洞扫描报告》和《安全配置核查报告》应包括整体扫描任务和单个主机扫描任务的情况。安全服务供应商须分别提供漏洞扫描服务和安全配置核查服务的对比报告，能够直观展示多次服务任务中系统资产的风险变化情况。对比报告应支持HTML、WORD、PDF和EXCLE（XML）等格式。

安全服务供应商须根据报告情况协助甲方完成安全加固，并对加固后的系统提供二次评估，验证发现的安全风险已经有效处理。

**相关工具**

漏洞扫描和配置核查服务过程中需要使用到大量的技术工具，列出部分重要工具包括如下：

表2.3 测试工具：远程安全评估系统

|  |  |
| --- | --- |
| 工具名称 | 远程安全评估系统 |
| 工具用途 | 安全漏洞扫描工具 |
| 性能参数 | 1、支持检测的漏洞数大于220000条，兼容CVE、CNCVE、CNNVD、CNVD、Bugtraq等主流标准，提供CVE Compatible证书和产品系统截图；  2、提供高级漏洞模板过滤器，支持将符合筛选条件的漏洞自动加入到自定义漏洞模板中，及后续插件升级包中的漏洞也可以自动加入到模板中；  3、支持扫描主流云主机机管理系统的安全漏洞，如：VMWareESX/ESXi、KVM、Xen，要求能够扫描大于5000条相关漏洞，提供功能截图和支持的漏洞列表；  4、支持对C/C++/Python/Java/Php/go等语言的代码解析，语言的词法、语法分析。内置缺陷模板和缺陷规则，并支持自定义，提供功能截图；  5、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，提供功能截图；  6、支持将按IP范围、起止时间、任务名称、任务状态、漏洞模板、用户等筛选扫描任务,并对筛选结果进行汇总,和生成在线及离线报表，提供功能截图；  7、支持风险告警和风险闭环处理，可在集中告警平台灵活配置告警内容、告警方式、告警资产范围等，支持邮件和页面告警，支持单个或批量修改风险状态，提供功能截图；  8、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，提供详细漏洞列表；  9、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；提供功能截图；  10、产品要求为国内开发，具备自主知识产权，并经过十五年以上应用检验，厂商应承诺产品的高度稳定性和可靠性；  11、产品厂商应具备独立的安全漏洞研究能力，独立发现并被CVE组织（世界漏洞编号官方组织）收录的安全漏洞超过30个，请提供CVE官方网站通过搜索单位名称所获得的CVE数量截图证明，同时提供这些安全漏洞的CVE编号、漏洞详细介绍及截图、网站链接； |

表2.4测试工具：安全配置核查系统

|  |  |
| --- | --- |
| 工具名称 | 安全配置核查系统 |
| 工具用途 | 安全配置检查工具 |
| 性能参数 | 1、支持虚拟化设备配置彻查，包括Hyper-V、VMWare ESXi、VMWare vCenter、XEN、XenServer配置核查；  2、系统默认支持工信部配置核查规范，依据工信部发布的《电信网和互联网安全防护基线配置要求及检测要求》（报批稿）进行配置核查；  3、支持本地检查，可以利用ActiveX控件对windows主机进行本地检查，仅需要IE访问配置核查设备即可SS进行本机配置核查；  4、支持时间段设置，只在指定时间段内执行任务，未完成任务在下一时间段自动继续执行；  5、可按IP范围、起止时间、任务名称、任务状态、配置模板、用户账号筛选任务并汇总，并在线查看风险详情和输出离线汇总报表；  6、支持风险告警和风险闭环处理，可在集中告警平台灵活配置告警内容、告警方式、告警资产范围等，支持邮件和页面告警，支持单个或批量修改风险状态；  7、支持报表自定义，可定制报表标题、封面logo、报表页眉和页脚、报表各章节显示内容； |

（2）安全巡检

安全巡检服务的内容包括安全设备巡检和安全日志分析两部分。

安全服务供应商需提供自合同签订后1年期的安全巡检服务，服务频度每半年一次，全年不低于2次。

**安全设备巡检**

检查机房环境及服务器、存储等外设的使用情况，检查主机操作系统及应用软件运行状况，检查安全产品及配套软件运行状况，检查日志服务器运行情况，更新事件库、漏洞库、病毒库等，并对各项配置加以优化。

**安全日志采集、分析服务**

安全服务供应商向甲方提供1年期每半年1次，全年不低于2次安全日志分析服务。主要针对业务支撑系统，服务内容包括：

* 梳理业务支撑系统现有安全设备日志平台可用性
* 搜集现有安全设备日志
* 分析日志，及时发现安全威胁和业务异常
* 具体要求：收集现有安全设备如IPS、WAF、审计等的日志信息。安全服务供应商对收集到的日志进行人工分析，提交《安全告警分析报告》及时发现安全威胁和业务异常，并向甲方相关人员汇报。

**相关工具**

表2.5测试工具：日志审计系统

|  |  |
| --- | --- |
| 工具名称 | 日志审计系统 |
| 工具用途 | 日志采集、分析工具 |
| 性能参数 | 1. 系统应基于大数据平台架构，具备海量数据收集与快速检索能力系统应基于B/S架构，支持SSL加密模式访问，可通过web方式直接对系统进行管理。 2. 系统应支持内置采集器，不依赖其他设备即可进行日志采集。支持外置采集器，外置采集器数据应提供加密压缩传输，以确保数据安全以及传输效率。须提供界面截图。 3. 系统应支持NAT环境下的Agent部署模式，支持单机部署，集群部署，分布式部署，须提供界面截图。 4. 系统应能实现海量日志数据的采集并保存原始日志数据，能够对异构日志格式进行统一化处理并保存统一化处理后的日志数据。 5. 系统支持的数据采集范围包括但不限于网络安全设备、交换设备、路由设备、操作系统、应用系统等。 6. 系统支持的数据采集方式包括但不限于SYSLOG、RSYSLOG、SNMP Trap、FTP、ODBC、JDBC、Net flow、WMI、二进制数据、专用Agent等方式采集日志 7. 系统支持采集的设备厂家包括但不限于：NSFOCUS(绿盟科技)、Venustech(启明星辰)、Topsec(天融信)、DBAPPSecurit(安恒)、SANGFOR(深信服)、Hillstone(山石网科)、东软、瑞星、金山、网康、360网神、Dptech(迪普)、艾科网信、Imperva、Juniper(瞻博网络)、F5、Symantec(赛门铁克)、Deep Security(趋势科技)、MaAfee(迈克菲)、Fortinet(飞塔)、Windows、Linux/Unix、Cisco(思科)、HUAWEI(华为)、H3C(华三)、中兴、Apache、nginx 、IIS、WebLogic、Vmware、Kvm、Xen、OpenStack、Hyper-V、华为FusionSphere、Oracle、MySQL、PostgreSQL、SQL Server、Bind等 8. 系统应支持界面配置即可完成未识别日志接入，无需编写xml。支持范式化日志多级提取。支持正则、KV、格式串等多种灵活的提取方式。支持自动生成正则以高效的辅助提取，须提供界面截图。 9. 系统应能够实现范式化日志的枚举值管理，实现对范式化日志字段的灵活翻译。系统应支持日志源监控能力，包括采集器维度及资产维度的监控，资产维度支持展示资产详细信息，须提供界面截图。 10. 系统应提供日志转发功能，应支持日志转发多个目标地址，可实现原始日志、范式化日志的转发，且不丢失原始日志源IP信息，须提供界面截图。 11. 系统应支持资产属性配置，支持资产标签，且至少6种标签以上，根据标签可快速查询资产。系统应支持资产以拓扑图形式展示，鼠标移动至资产图标可展示对应的资产信息，须提供界面截图。 |

**服务范围包括：**

* 安全漏洞检查，提供加固建议。
* 安全配置合规检查。
* 应用系统配置安全检查。

**具体要求如下：**

安全服务供应商应首先提供业务系统安全检查流程、方法。

每次服务完成后，提供安全漏洞、安全配置、web应用漏洞以及互联网渗透的报告，提出安全加固建议。

5、服务实施要求

1. 安全服务供应商应详细描述安全服务过程中人员的组成及各自职责的划分。
2. 安全服务供应商应配置有经验的安全服务人员进行本项目的服务工作，未经与招标方协商确认安全服务供应商不允许随意更换安全服务人员，安全服务供应商应确保选派高级咨询人员参与整个项目，确保项目的进度和质量。
3. 本项目实施过程中所使用到的各种工具软件由安全服务供应商推荐，经甲方确认后由安全服务供应商提供并在安全服务中使用。
4. 安全服务工具软件运行可能需要的硬件平台（如笔记本电脑、PC、工作站等）和操作系统软件等由安全服务供应商推荐，经甲方确认后由安全服务供应商提供并在评估中使用。
5. 安全服务需要的运行环境（如场地、网络环境等）由甲方提供，安全服务供应商应详细描述甲方的运行环境的具体要求。
6. 安全服务应实施风险控制：
   * 在进行漏洞扫描和安全配置核查前，安全服务供应商需进行小范围的模拟试验，检验漏洞扫描和安全配置核查的有效性和安全可靠性。
   * 在漏洞扫描和安全配置核查过程中安全服务供应商应对操作的每一个步骤及系统状态进行详细记录，一旦发现异常立刻退回上一步。
   * 在漏洞扫描和安全配置核查过程中，由甲方相关人员全程跟进，对要检查的系统进行确认，对可能存在的风险由安全服务供应商工程人员及时提出，确认后再进行漏洞扫描和安全配置核查。
7. 计划实施任务表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 任务名称 | 计划开始时间 | 计划完成时间 | 服务输出 |
| 1 |  |  |  | - |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |