**2023年IPV6改造项目的招标参数**

**第一部分 项目技术规范和服务要求**

## 主机漏洞扫描

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 期限及频率 | 1年4次 |
| 服务范围 | 浙江大学医学院附属儿童医院所有主机 |
| 服务内容 | 针对浙江大学医学院附属儿童医院的网站和业务系统，采用明鉴Web应用弱点扫描器、远程安全评估系统，通过定制的扫描规则，形成安全扫描策略，对指定网站和主机进行自动化安全扫描，发现系统主机层和应用层的安全漏洞，人工验证扫描结果并输出安全扫描报告及修复建议。发现系统应用代码和安全配置存在的安全隐患和缺陷。 |
| 输出物 | 《漏洞扫描报告》 |
| 工具要求 | 须提供专业的漏洞扫描系统。 |
| 漏洞扫描系统 | 1. 产品具备国家信息安全漏洞库《CNNVD兼容性资质证书》，提供有效证书的复印件。
2. 产品要求界面友好，并有详尽的技术支持文档，所有图形界面的文字要求为中文；
3. 支持分布式部署方式，上级管理设备能够方便查看下级设备的状态信息
4. 系统为B/S架构，并采用SSL加密通信方式，用户可以通过浏览器远程访问设备，方便用户操作，支持多用户同时登录操作；
5. ★支持用户自定义系统名称、版权信息和系统的Logo信息，而无需进行定制化，提供截图证明；
6. 厂商漏洞特征库大于200000条；提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与CVE、CNNVD、Bugtraq、CNCVE、CNVD等国际、国内漏洞库标准兼容；
7. 支持对各种网络主机、操作系统、网络设备（如交换机、路由器、防火墙等）、常用软件以及应用系统的识别和漏洞扫描；
8. 支持云平台的漏洞，覆盖OpenStack、KVM、VMware、Xen等主流的云计算平台，提供截图证明；
9. 支持扫描物联网设备的漏洞，至少支持国内主流摄像头品牌，包括海康威视、宇视、大华；打印机支持惠普、三星；路由器支持TP-Link、Netgear、D-Link等，提供截图证明；
10. 系统内置不同的策略模板如针对Linux操作系统、Windows操作系统、工控、大数据、虚拟化、数据库扫描模板，同时允许用户定制扫描策略模板；
11. 可以自定义扫描端口范围、端口扫描策略，提供功能截图；
12. ★具备弱口令扫描功能，支持弱口令扫描协议数量≥22种，包括FTP、SMB、RDP、SSH、TELNET、SMTP、IMAP、POP3、Oracle、MySQL、MSSQL、DB2、REDIS、MongoDB、Sybase、Rlogin、RTSP、SIP、Onvif、Weblogic、Tomcat、SNMP等协议进行弱口令扫描，允许用户自定义用户、密码字典，提供截图证明。
13. 支持发现非默认端口启动的服务，支持服务的协议及版本识别；
14. 同IP不同端口同漏洞的结果应明确给予端口标识；
15. 支持对误报的漏洞进行修正，避免将误报结果导出；
16. 支端口探测方式≥7种，如TCP ACK、TCP SYN、TCP Connect、TCP Null、TCP Xmas、TCP Window、TCP Fin等；
17. 支持将漏洞以紧急、高危、中危、低危、信息进行危害程度的分类，并且可根据用户需要自定义漏洞等级。
18. 支持自定义User-Agent、自定义请求头，自定义Cookies或录制获取、自定义LocalStorage、SessionStorage对Web应用进行扫描；
19. 支持多种网站认证方式：支持包括Basic、Digest、DigestIE、NTLM、GSS-Negotiate、Bearer在内的认证方式，支持HTTP和SOCKS代理，并支持各种代理的认证方式；
20. ★存在误报漏洞可通过产品在扫描结果处支持以及时通讯的方式第一时间反馈给厂商协助修改，提供截图证明；
21. 支持Oracle、MySQL、SQLServer、DB2、Informix、PostgreSQL、Sybase、达梦、人大金仓的授权数据库漏洞扫描；
22. 数据库扫描支持的检测类型大于10种，至少包括弱口令、执行权限过大、访问控制漏洞、提权漏洞、缓冲区溢出漏洞、缺省配置、访问权限绕过、PL-SQL注入、危险程序、安全信息查看等。
 |

## 网站云防护

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 期限及频率 | 全年7\*24小时 |
| 服务范围 | 2个一级域名及不超过20个二级域名 |
| 整体要求 | ★支持集群化和高可用部署架构，全国范围至少具备90个云防护节点。提供服务平台界面截图 |
| 支持通过一体化平台提供云防护和云监测服务，以便在用户需要时将防护站点加入监测系统进行安全自检 |
| 支持为每个用户单独创建平台登录账号，用于查看网站的安全防护状况。 |
| 服务方式 | 系统基于云化SaaS架构，无需消耗虚拟机资源或本地物理资源，通过云端服务平台完成站点管理，为用户提供云防护服务。 |
| IPV6转换 | ★针对浙江大学医学院附属儿童医院2个一级域名及不超过20个二级域名，提供IPv6转换服务用户IPv4网站的访问转换服务，无需改动用户网络结构即可实现外部IPv6地址正常访问用户网站。 |
| IPV6带宽资源 | ★针对浙江大学医学院附属儿童医院10个网站系统（二级域名）提供带宽扩展包用于扩展云防护服务的实时带宽峰值（70M）。 |
| 安全概览 | 支持通过统一界面展示网站访问次数、拦截攻击次数、网站出入总流量、疑似攻击元IP数量，并以时间维度展示攻击与访问趋势图。提供服务平台界面截图 |
| 站点管理 | 支持通过服务平台以手工导入和批量导入的方式完成防护站点的添加申请，支持添加HTTP和HTTPS类型的站点，并支持自主上传网站公钥或和私钥。提供服务平台界面截图 |
| 支持HTTP强制跳转HTTPS，当用户访问HTTP端口（如80）时，支持强制将访问牵引至HTTPS端口（如443） |
| 访问控制 | ★支持区域访问控制，限制国外用户或者国内以市为最低行政单位的区域进行访问控制。提供服务平台界面截图 |
| 防护能力 | 支持检查提交的报文是否符合HTTP协议框架，如异常的请求方法、特殊字符、重点字段的缺失、超长报文造成的溢出攻击以及对高危文件的访问等；提供服务平台界面截图 |
| 支持对HTTP协议合法性进行验证，提供HTTP协议防护功能，支持对HTTP协议的URI、HOST、UA、Cookie、Referer、Content、Accept、Range、其他头部和参数在内的元素、参数进行检测与处理。且支持非法编码和解码的灵活控制与处理。 |
| 支持针对主流Web服务器及插件的已知漏洞防护。Web服务器应覆盖主流服务器：apache、tomcat、lightpd、NGINX、IIS等。 |
| 支持对用户上传的文件后缀名和文件内容进行全方面检查，杜绝Webshell的上传和访问；（提供服务平台界面截图并加盖公章） |
| ★支持流量监测的功能，基于用户的访问记录，实时检查被访问页面的安全状况，能够发现更深层次的暗链、Webshell等安全事件。提供服务平台界面截图 |
| ★支持提供攻击防护安全策略，支持对命令注入（包括SQL注入、SQL盲注、代码注入等）、跨站脚本、SSI指令、路径穿越、远程文件包含、WebShell防护。提供服务平台界面截图 |
| 支持提供信息泄露防护安全策略，包括目录信息泄露、服务器信息泄露、数据库信息泄露、源代码泄露等。 |
| 密码强度检测 | 支持对用户登录账户密码进行密码强度检测，支持进行弱口令登录拦截、密码爆破防护、账号爆破防护，并定义请求频率阈值，支持在用户界面展示账户安全状况。 |
| 一键关停 | 支持一键关停功能，当网站出现紧急安全事件时，可通过浏览器一键完成关停，防止产生恶劣影响。 |
| 永久在线 | 支持永久在线功能，当网站因为服务器故障、线路故障、电源等问题出现无法连接时，可显示云防护节点中的缓存页面。当在敏感期或特殊时期时，用户网站主动关闭期间可显示缓存页面，增强网站安全性。 |
| 微信自服务 | ★支持通过微信公众号查看网站整体防护态势，包含受攻击域名排行、攻击类型排行、攻击IP排行、攻击区域分布等状态信息。提供服务平台界面截图 |
| ★支持通过微信公众号完成防护配置，包括一键关停、防护模式切换等功能。提供服务平台界面截图 |
| 日志管理 | 支持访问和攻击日志查询与导出功能，可根据域名、URL、客户端IP、返回码、访问区域、访问时间段进行查询，查询后的日志数据支持下载到本地。 |
| 支持访问与攻击原始日志离线下载功能，可按天进行下载。原始日志包含访问IP、访问时间、URL、返回码、访问域名等信息. 攻击日志至少保存6个月，满足《网络安全法》要求。 |
| 防护报表 | 支持查看安全防护报告，包含攻击次数、攻击者区域统计、攻击者IP统计、攻击类型分布等报告。提供报告截图 |
| 支持查看网站访问报告，包含CDN加速流量、服务质量综合评价和关键指标信息、异常响应分析、访问区域统计、访问源IP统计、访问页面排行、访问终端、响应码分布等统计报告。提供报告截图 |
| 支持单个网站生成报表，也支持网站群生成一个汇总报表，支持日报、月报 ，并支持html、word格式导出。  |
| 告警管理 | 支持根据不同告警级别发送邮件、短信、微信公众号等多种告警方式。提供服务平台界面截图 |
| 可视化大屏 | 支持可视化分析大屏，展示访问与攻击流量趋势、受攻击网站排行、攻击源IP排行、攻击类型排行等信息。 |
| 支持单个网站可视化分析，包括防扫描告警、总体访问/攻击趋势、攻击源实时分析、IP追踪、访问量排行、防御能力分析等数据展示与挖掘。 |
| ★支持与威胁情报联动，在可视化大屏界面对发现的恶意IP进行下钻分析，获取IP地理位置、置信度、威胁等级、情报源、历史解析域名等信息。提供服务平台界面截图 |
| 输出物 | 《网站安全防护报告》 |

## 应急响应

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 期限及频率 | 1年2次 |
| 服务范围 | 所有应用系统安全事件 |
| 服务内容 | 服务期内，通过远程和现场支持的形式协助客户对遇到的突发性安全事件进行紧急分析和处理。 |
| 服务要求 | 当出现安全事件时，必须及时进行响应，具体要求包括：1、技术人员必须在2小时内到达现场；2、对入侵事件进行分析，查找原因；3、抑制入侵事件的进一步发展，将事故的损害降低到最小化；4、排除安全隐患，消除安全威胁，协助恢复系统正常运作；5、提交应急响应报告及系统安全改进方案。 |
| 输出物 | 《安全事件应急响应报告》 |
| 工具要求 | 须提供应急处置工具箱1、任务管理（1）支持新建应急处置任务，包括事件名称、事件等级、事件发生时间、事件发生单位关键信息记录.2、资产与数据管理（1）支持按资产上传专用数据采集工具所生成的采集数据包，并对上传数据进行分析；（2）支持添加多个处置对象资产，分别上传所采集的数据信息3、数据分析★（1）支持设置线索，发现关键可疑行为，包括IP线索、关键词线索、文件名线索、时间线索的设置，提供截图证明；（2）支持对所采集的系统配置数据、使用痕迹数据、运行状态数据、恶意代码情况、系统日志、中间件日志等进行数据分析；（3）支持按照策略进行自动分析，包括非授权时间登录、口令爆破、恶意启动项、DDOS、可疑账号、木马回连、webshell攻击、SQL注入、java反序列化攻击等主机安全事件、网站安全事件、病毒感染事件等高危、中危、低危、信息等级的安全事件进行分析，形成可疑行为事件。（4）支持手动分析，支持处置人员查看采集的数据信息，标记关键数据形成可疑行为事件；★（5）支持根据所提供的线索自动发现关键可疑行为并进行标记；提供证明截图（6）可疑行为信息应可疑行为名称、行为时间、行为描述、行为主机、危险等级等关键信息；（7）支持在处置过程中的发现，动态调整线索内容并进行重新分析。4、情况调查（1）支持安全事件基本情况调查，包括系统名称、备案等级、时间发生时间、调查处置时间的记录，支持处置过程人员记录，包括涉事单位人员、研发单位人员、运维单位人员、调查人员相关信息记录。（2）支持访谈笔录的管理并提供事件调查详表、事件调查简表、人员访谈记录等常用表单的模板下载，支持这些表单填写后的上传、下载与删除。（3）支持处置定性，对事件发生原因、现场调查情况、事件后果评估等定性信息记录。5、处置报告（1）支持生成应急处置报告，报告内容包括事件基本信息、后果评估等定性信息记录6、知识库要求（1）包括应急处置知识、应急处置案例、政策法规，提供证明截图★（2）支持根据关键字搜索相关知识内容；提供证明截图7、勒索病毒专项★（1）支持根据勒索文件后缀查找对应解密工具，提供解密工具的下载、使用介绍等；提供证明截图8、威胁情报★（1）支持提供IP、域名、文件等威胁情报查询，提供证明截图；（2）支持连接互联网情况下的在线情报查询；（3）支持与互联网断开情况下的离线情报查询；9、常用工具（1）支持windows数据采集工具的下载（2）支持windows恶意代码检测工具的下载，包括windows病毒木马检测工具、windows Webshell检测工具（3）支持Linux数据采集工具的下载（4）支持linux恶意代码检测工具的下载，包括linux病毒木马检测工具、linux检测工具★（5）支持Ubuntu、opensuse、Debian、centos的bin文件下载，提供截图证明；10、策略管理（1）支持策略的开启与关闭（2）支持新建策略与删除策略★（3）支持自定义设置策略规则、描述信息、处置建议等内容，提供截图证明；11、安全配置管理（1）配置管理应提供对平台参数进行配置:支持系统最大登录次数设置；支持锁定用户时间设置；12、用户管理（1）支持对用户账户进行管理、口令修改：支持对账户新增、修改、删除；支持创建审计员、操作员、管理员；13、日志管理（1）可查看操作日期、操作用户、操作事件等日志记录（2）提供日志筛选功能（3）提供日志导出备份恢复等功能14、访问控制（1）应依据安全策略严格控制用户文件，数据表等重要信息资源的操作（2）应确保不提供已注销用户的任何信息，包括鉴别信息等15、通信安全（1）应采取措施确保导入和导出数据的完整性 |

**第二部分 安全服务要求**

## 质量保证措施及服务承诺

1、中标人提供7\*24小时的技术支持（包括电话咨询与现场服务）。

2、中标人在接到电话后，必须在30分钟内响应，2个小时内必须到达用户现场，如无法到场，按合总同价的1％/次作为赔偿，扣除合同余款。

3、每次对系统进行扫描之前必须要先提供相应的技术方案与业主方技术人员充分沟通，以确保系统的安全运行。

4、进行任何测试，需要在业主方许可的时间、环境下由经验丰富的专业技术人员进行。

5、实施过程中应尽可能小的影响系统和网络的正常运行，做好备份和应急措施，不能对用户应用系统的正常运行产生影响，包括系统性能明显下降、网络拥塞、服务中断等，如无法避免出现这些情况应先停止项目实施，并向业主方书面详细描述。

6、中标人须对本次安全建设项目实施过程的数据和结果数据严格保密，未经业主方授权，任何机构和个人不得泄露给其它单位和个人，同时要求中标人在此次项目结束之后将所有和本项目有关的数据和文档移交业主方后全部销毁。

## 服务时间及考核

1、服务时间

服务时间为合同签订生效后，投标方人员到位正式开始服务后1年。

2、验收方式

考核至少满足：提供用户单位所列的安全服务，提交各类报告；响应甲方提出的应急服务请求，响应时间未超出规定期限。否则不具备考核条件，招标单位可单方中止服务合同。

**三、付款**

服务期结束，验收合格，凭有效票据付全款。