中国医学科学院肿瘤医院

配置安全核查

技术需求

**信息中心/计算机室**

**2017年5月**

# 项目简介

根据信息安全等级保护工作要求，需要定期对系统进行配置核查工作。定期检查网络、主机系统、软件系统等配置是否正确、合理，是否存在风险项。管理员及时进行问题修复。

# 参数要求

需求数量：1台，具体参数要求如下：

| **序号** | **指标项** | **规格要求** |
| --- | --- | --- |
| 1 | **厂商**  **要求** | 产品源厂商应具备多年的安全配置研究经验和专业的攻防技术研究团队，具备独立配置信息采集和比对的能力。请提供安全基线检查工具支持设备检查列表及相关证明文件。 |
| 产品源厂商应了解各个行业安全配置检查安全功能和配置规范要求。 |
| 产品源厂商应具备完善的服务保障体系和遍及全国的技术支持队伍，提供统一的免费服务热线。 |
| 2 | **扫描**  **能力** | 安全基线检查脚本库与安全检查功能和配置规范要求兼容。  支持对安全对象的配置脆弱性进行全面检查，识别内容应包括操作系统和网络设备、数据库和中间件等的账号、口令、授权、日志安全要求、不必要的服务、启动项、注册表、会话设置等配置。  **支持TELNET、SSH、SMB、RDP、WinRM协议的安全基线配置检查方式。**  支持对主机设备的安全配置核查，包括：Windows、Linux、HP-UX、AIX、Solaris  支持对主流数据库的安全配置检查，包括：Oracle、Mysql、SQL Server、sybase、DB2、informix。  **支持对主流网络设备的安全配置核查，包括：cisco交换机、华为交换机、H3C交换机、力腾交换机 、锐捷交换机、cisco路由器、华为路由器、H3C路由器、juniper路由器**  支持对主流防火墙的安全配置核查，cisco防火墙 、华为防火墙、Fortigate、火墙、netscreen防火墙、启明星辰（网御powerV系列）防火墙、juniper防火墙、山石防火墙  **支持对主流中间件的安全配置核查，包括：Apache、Bind、Domino、IIS、Jboss、Nginx、Resin、Tomcat、TongWeb、Weblogic、Websphere**  安全配置核查时，程序占用的资源应尽量的少，扫描主机的CPU平均占用率小于10％，内存占用小于50M；被扫描主机的CPU占用率小于1％，内存占用小于3M；网络带宽的占用率均不大于2％（以百兆网络为基准）。  支持灵活的检查任务制定功能，可以设定手动、定时和离线任务的配置任务检查方式。  支持实时显示检查任务进度和检查任务状态。  支持检查策略的脚本导出，通过离线方式将脚本拷贝到目标设备上支持对于的脚本文件，将生产的结果导入到基线核查服务器完成离线方式的核查。  **在建立核查任务时支持从“资产库获取、IP段添加、Excel导入”方式添加核查设备。**  对于部分检查项无法立即得出是否合规的标准时，应提供人工参与判定的机制，并把判断结果作为下次检查的标准。  **提供任务的复制功能，在不影响原有任务的情况下，对复制的任务进行修改和裁剪**  提供对不合规核查项对外通过syslog方式发送功能，并具备发送按级别过滤功能 |
| 3 | **核查**  **方式** | **对于管理较好的不可达网络或者物理隔离网络，提供分布式采集器，可实现批量核查，批量上报，并根据实际情况实现在线及离线两种方式。**  **在线：从安全基线配置检查服务器获取批量任务，点击执行后讲结果批量上报**  **离线：从安全基线配置检查服务器获取批量任务，将获得的任务的移动设备接入不可达网络中自动执行批量检查任务，任务完成后将离线采集移动设备接回安全基线检查服务器将任务结果导入安全基线检查服务器完成离线批量核查。**   1. 离线核查支持：**提供所有设备按照策略及自定义策略的VBS离线脚本下载功能，在目标设备上执行完成后将结果导入基线系统。** 2. **网络设备支持：支持将离线命令在目标设备上运行后，通过提供执行命令集Session Log方式检查；**   **对于不希望提供管理员账号和密码的个人主机系统，支持提供代理检查的方式，代理检查结果自动上传到检查服务器，并支持代理设备中的中间件及数据库核查。**  **对扫描失败的设备和检查项有非常准确的失败信息反馈。** |
| 4 | **资产**  **管理** | **对核查对象集中管理，实现手工添加、Excel文档方式的导入及导出，资产移动，删除及修改功能，并可对选中资产的提供连通性测试，对测试不通过的资产提供可参考的信息**  提供按照资产组和资产类型两个管理维度，并可自定义资产组  **可通过选中资产立即下发核查任务**  **可通过选中资产查看该资产的核查历史，并能够选中两个任务进行对比分析，展示两次核查的对比信息，包括核查时间及核查结果** |
| 5 | **帐号获取与**  **传输安全** | 支持被核查设备帐号信息的多种获取方式：   1. 数据库获取：支持系统保存帐号信息，采用AES高级加密标准，密钥不少于128位。 2. **密码文件读取：系统提供密码文件模版下载功能，在建立核查任务时提供导入功能，系统读取设备信息后保存在内存中，在任务执行完毕后销毁，做到一次性使用**。 3. 接口获取：系统提供与第三方系统的接口，在登录设备时获取并一次性使用   4、管理中心与代理服务器之间保证数据传输安全，防止脚本被恶意篆改，传输采用ssl方式，认证请求使用RSA加密。 |
| 6 | **策略**  **管理** | 系统默认可检查的配置检查点应不小于 1500个。  支持安全基线检查项自定义功能，并支持自定义检查项导入导出功能  支持检查项按设备类型管理，并实现设备类型的自定义功能，支持新增类型绑定已有的检查项  支持检查项参数化功能。  支持策略的导入导出功能  支持安全基线检查点的权重设定功能。  支持内置已有的安全基线检查脚本库，并不少于1000个，并实现检查项与脚本一对多的引用关系  **支持核查脚本的自定义功能，并能按顺序清晰展示脚本使用的命令集合，例如：[netstat, echo]**  支持灵活的检查策略管理功能，实现跨设备类型的检查项组合并实现检查项的参数实例化，提供必要的核查项查询过滤功能，对于展示的核查项可点击查询详细的说明信息，并实现多维度的检查策略维护。 |
| 7 | **报告**  **功能** | 提供按任务导出报告功能，任务多次执行应导出多个报告  报表应包含检查项详述和加固建议方案。  应提供多维度报告统计功能，提供导出功能，格式支持Html、Excel、PDF、Word等主流格式。  提供任务的合并功能，合并后的任务可统一出具报告，并保留合并前的任务及报告  支持在线报告查看报告功能  支持任务的对比分析和趋势分析 |
| 8 | **用户和**  **权限**  **管理** | 支持三权分立。具备独立用户管理功能，能够分管理员、操作员、分析员、审计员等角色对用户进行管理，能够调整不同角色用户的系统使用权限。  能够对登录日志、操作日志进行记录和查询。 |
| 9 | **对外**  **接口** | 具备对外接口，支持任务下发接口，根据任务ID将扫描结果上报接口，进度查询接口，获取核查策略接口。  预定标准接口，可以实现与资源管理系统的数据获取接口，如从4A系统获取资产管理员账号和密码信息。 |
| 10 | **性能** | 单设备扫描 3IP/分钟  网络设备/中间件视网络状况在 1IP/2分钟内  支持资产并发，既同一时间至少支持对20个资产进行同时扫描  单个核查作业对于资产扫描的数量无限制  被扫描主机资源占用情况:cpu波动区间3%~5%，内存无明显变化 |
| 11 | **部署** | 软件支持64位的主流操作系统，Windows2003、Windows2008Redhat 5、6、Windows7、CentOS5、6操作系统，可部署于主流PC、笔记本电脑以及服务器之上。  支持MySql(MariaDB) 数据库  支持windows、Linux代理部署，实现对部署代理主机基线检查。  支持分布式采集器部署，实现对不可达网络的基线检查。  支持采集器可视化，并能监控采集器的性能信息  支持上下级级联和管理，并能监控下级节点的性能信息  支持对下级节点下发核查策略，指定上报时间、上报周期说明、达标说明。 |

# 服务

提供原厂五年免费服务，包括软件升级，硬件质保，现场技术支持服务，永久电话支持服务。