## 网络安全等级保护测评整改项目采购清单与技术要求

## 1.采购需求清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **产品名称** | **数量** | **品牌** |
| 1 | 综合日志审计分析系统 | 1台 | **奇安信、安恒** |
| 2 | 安全加固与服务 | 1项 |  |

# 2.技术要求

## 2.1综合日志审计分析系统技术要求

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 硬件规格 | **标准2U硬件设备，≥1个console口，≥1个千兆管理电口，≥1个HA口，≥4个千兆审计电口，≥4个千兆审计光口，硬盘≥12T，支持raid5，内存≥16G，双电源。** |
| 性能指标 | **日志处理能力≥9000EPS（峰值：12000EPS），资产授权≥200个，支持最大扩展至450个，日志保存时间6个月以上。** |
| 工作模式 | 支持独立完成审计日志采集，不依赖于设备或系统自身的日志系统。  提供全中文WEB管理界面，无需安装任意客户端软件或插件。 |
| 日志收集 | 支持Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP协议日志收集；支持阿里云SLS日志的采集。  可通过接收协议限制日志接收速率，包括Http接收、syslog接收、SNMPtrap接收、TCP接收、WMI接收、aliyun接收。（提供功能截图）  支持使用代理(Agent)方式提取日志并收集，安装包支持界面下载，且安装支持可视化向导。  支持对Agent进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发。  支持对重点日志源的个性化管理和日志源分组管理。 |
| 日志分析 | 支持对收集到的重复日志进行自动聚合归并，减少日志量。  支持内置≥5000条解析规则，支持对收集的≥5000种设备类型日志进行解析（标准化、归一化），解析维度200个以上，解析规则可以根据要求实现定制扩展。  具备安全评估模型，评估模型基于设备故障、认证登录、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件。  内置设备异常、漏洞利用、横向渗透、权限提升、命令执行、可疑行为6大类50个以上子类的安全分析场景。  三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件。 |
| 日志备份 | 支持设置日志存储备份策略，包括系统日志保存期（天）、磁盘使用率百分比等策略。  支持日志备份自动传送到远程服务器，支持从远程仓库恢复数据。 |
| 应用性能监控APM | 支持监控设备自身CPU、内存、磁盘等工作运行状况。  通过在目标主机上安装Agent程序，支持监测目标主机的CPU利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息。 |
| 告警功能 | 支持磁盘空间阈值告警，当磁盘使用率达到设定的阈值时可产生并外发告警；资产性能监控异常告警，对于监控的资产系统资源进行监测当指定指标使用率达到设定的阈值时可产生并外发告警；资产状态监控，当资产处于不活跃状态时可产生并外发告警；远程仓库状态监测可告警，当远程仓库可用性检测失败或备份包自动上传失败时可产生并外发告警。 |
| 资产管理 | 资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息。 |
| 功能扩展 | 支持采用解决方案包上传对产品进行功能扩展，无需要代码开发。 |
| 用户管理 | 根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容；日志员只负责完成对系统本身的用户操作日志管理。 |
| 产品资质 | 产品具备软件著作权登记证书。  产品获得公安部计算机信息系统安全产品销售许可证。  产品获得中国网络安全审查技术与认证中心颁发的《中国国家信息安全产品认证证书》（增强级）。 |
| 应急响应服务 | 支持发生信息安全事件时，由安全专家现场和后台技术专家及时采取行动限制事件扩散和影响的范围，限制潜在的损失与破坏服务基础上，检查所有受影响的系统，在准确判断安全事件原因的基础上，提出基于安全事件整体安全解决方案，排除系统安全风险并协助追查事件来源、提出解决方案、协助后续处置。  输出:包括但不仅限于《网络安全事件应急响应报告》。 |
| 巡检服务 | 提供原厂安装实施，在保修期内提供每季度巡检一次的服务,共计12次巡检服务； |
| 联动预警服务 | 支持与湖南省教育厅监管平台对接，满足联动预警需求 |
| 售后服务 | 提供不少于三年免费原厂售后服务、升级维护和永久使用授权，供应商提供承诺函。 |

## 2.2安全加固服务技术要求

|  |  |  |
| --- | --- | --- |
| **服务内容** | **指标项** | **指标参数** |
| 安全加固服务 | 安全加固 | 针对网络环境、服务器操作系统、数据库、应用中间件、应用系统等软件系统，通过打补丁、强化帐号安全、加固服务、修改安全配置、优化访问控制策略、增加安全机制等方法，堵塞漏洞及“后门”，合理进行安全性加强，提高其健壮性和安全性。  服务范围：**包含11个应用系统及其涉及的网络环境、服务器操作系统、数据库、应用中间件、应用系统等，等保测评报告中涉及的所有高危和中危漏洞（数量200多个）。**  服务效果：**满足等保2.0测评要求，确保通过等保测评**。  服务内容：   1. **调查与评估**   对信息系统资产进行调研，明确系统所涉及资产；  双方进行讨论，确认加固实施范围；   1. **安全评估**   对加固范围内的设施实施安全评估，以明确可以实施的加固措施；评估维度如下：  网络设备安全加固：包括禁用不必要的网络服务、修改不安全的配置、利用最小特权原则严格对设备的访问控制、及时对系统进行软件升级、提供符合IPP要求的物理保护环境等。对网络设备进行检测评估，提出可行性的加固方案。  操作系统安全加固：包括检查系统补丁、停止不必要的服务、修改不合适的权限、修改安全策略、检查账户与口令安全、开启审核策略、关闭不必要的端口等。  应用系统（WEB系统、数据库）安全加固：包括对要使用的操作数据库软件（程序）进行必要的安全审核，比如对ASP、PHP等脚本，这是很多基于数据库的WEB应用常出现的安全隐患，对于脚本主要是一个过滤问题，需要过滤一些类似,‘;@/等字符，防止破坏者构造恶意的SQL语句。安装最新的补丁，使用安全的密码、账号策略，加强日志的记录审核，修改默认端口，使用加密协议，加固TCP/IP端口，对网络连接进行IP限制等。  根据明确的加固措施制定安全加固方案。   1. **安全加固**   与我校对安全加固方案讨论，确定最终加固对象和措施；  安全加固实施。  输出:包括但不仅限于《安全加固报告》 |
| 资产探测 | 针对暴露在互联网上的所有域名或IP地址的资产、域名，采用基于网络扫描、搜索引擎、互联网基础数据引擎等方法进行主动探测，提供互联网资产的详细基础数据列表。通过本地/云端资产探测工具对单位的IP段、域名、单位名称等多种条件进行全网探测。  输出:包括但不仅限于《资产探测报告》 |
| 漏洞扫描 | 使用业界认可的安全扫描工具对现网的所有资产包括主机、数据库、中间、网络安全设备、Web应用进行漏洞扫描风险评估，发现漏洞并给出相关漏洞信息，并为漏洞提供相关解决方案。  输出:包括但不仅限于《漏洞风险评估报告》 |
| 基线检查 | 使用业界认可的安全基线核查工具对现网的所有资产包括主机、数据库、中间件、应用系统、网络安全设备进行全面的安全配置核查和分析，发现基线安全风险，并为风险提供相关解决方案。  输出:包括但不仅限于《基线检查检测报告》。 |
| 态势感知 | 提供网络安全态势感知、资产梳理、威胁监测、监测预警、追踪溯源服务，从宏观层面展示我校网络安全态势，为安全运维人员提供包括外部攻击态势、横向威胁感知、资产失陷态势、Web业务系统态势、数据中心态势、AI异常分析、攻击者溯源态势、重保等信息；通过关联分析多维大数据，实现发现现网系统中存在的安全事件、安全风险点，进行实时安全威胁预警。 |
| 应急响应 | 支持发生信息安全事件时，由安全专家现场和后台技术专家及时采取行动限制事件扩散和影响的范围，限制潜在的损失与破坏服务基础上，检查所有受影响的系统，在准确判断安全事件原因的基础上，提出基于安全事件整体安全解决方案，排除系统安全风险并协助追查事件来源、提出解决方案、协助后续处置。  输出:包括但不仅限于《网络安全事件应急响应报告》。 |
| 巡检服务 | 定期针对安全设备物理状态、安全配置、设备运行状态进行检查。  提供原厂每季度一次的巡检服务,3年共计12次巡检服务. |
| 其它要求 | 要求原厂工程师服务，不少于2人\*30天的实施服务。 |