|  |  |  |
| --- | --- | --- |
| 产品及制造商能力 | 产品资质 | 1. 产品具备中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》； 2. 产品具备国家保密局涉密信息系统安全保密测评中心《涉密信息系统产品检测证书》； 3. 产品具有《军用信息安全产品认证证书》军B级； 4. 产品具有中国信息安全测评中心《信息技术产品安全测评证书》EAL3+级； 5. 产品具有《IPv6 Ready Logo Phase-2》认证证书 |
| 制造商资质 | 1. 具备《国家信息安全认证信息安全服务资质证书》（安全工程类二级）。 2. 具备《涉及国家秘密的计算机信息系统集成资质证书》（甲级） 3. 具备环境管理体系认证证书（ISO14001:2004） 4. 产品制造商是微软MAPP（Microsoft Active Protection Program）计划战略合作伙伴、云安全联盟全球企业会员，提供权威网站截图证明文件。 5. 具备自己发现主流操作系统或应用系统新漏洞的能力，并提供2010年以后至少2个以上厂商发现的新漏洞及国内外相关权威机构(如：国家漏洞库和CVE等)的证明 |

| **指标项** | **产品指标项** | **产品性能参数和要求** |
| --- | --- | --- |
| 总体  要求 | 产品形态 | 软件，采用64位 Linux操作系统部署。 |
| 运行环境 | 1）用户的浏览器客户端无需安装JRE或者JAVA Web Start即可访问管理中心；  2）集成数据库，数据库应可满足海量安全事件的存储与快速查询与检索，可支持分布式弹性扩展，提供数据冗余存储。 |
| 管理范围 | 涵盖网络设备、安全设备、主机、数据库、中间件以及各种应用系统 |
| 管理节点 | 250个 |
| 事件处理性能要求 | 管理中心的事件处理性能最大可达到平均每秒50000条事件  15亿条事件简单搜索完成用时2秒 |
| 监控性能要求 | 管理中心的并发监控任务个数可以达到1000个 |
| 功能  要求 | ★综合展示 | 1. 在综合展示界面中能够显示系统的基本管理信息，包括最近30分钟告警状态雷达图、最近1小时事件趋势图，最近24小时资产告警排行Top10等以及事件量曲线【提供截图】； |
| ★态势综合展示 | 1. 提供态势综合展示界面，能够对全网安全态势进行多维度的整体监视。 2. 支持安全态势细分呈现，包括但不限于全局安全态势地图、攻击威胁态势视图、安全隐患态势视图等。 |
| ★资产态势展现 | 1. 各资产类型的概要信息：可以监视每类资产类型中的几个主要统计指标，包括告警数量、产生的漏洞总数、配置弱点总数以及安全事件数。 2. 资产受危害概览：包括每个资产类型的高危告警影响度，高危漏洞影响程度，高危攻击影响度以及告警在各资产类型中的总覆盖率和随时间变化趋势。 3. 资产受攻击情况：包括各资产类型中受攻击的主要类型，安全日志的接入情况，攻击相关事件所利用资产端口的比例分布。   资产风险态势：包括各资产类型的风险等级，在风险态势矩阵上的风险值分布以及风险趋势。 |
| ★攻击威胁态势 | 1. 可综合各类安全威胁及攻击行为事件形成类型分布、资产对象遭受攻击分析、攻击地图、攻击发生趋势等的态势展现，通过动态攻击地图、趋势图等各类数据可视化形式辅助数据的直观展示； 2. 支持从内部、外部攻击源的角度对攻击事件进行分析统计，并呈现态势； 3. 支持攻击威胁KPI雷达图展示； 4. 支持攻击量与攻击对象的分析态势呈现； |
| ★威胁态势分析 | 1. 系统通过建立并针对一组关键指标体系（KPI）计算得到一个威胁指数，以此来表征一段时间内、某个网络区域的网络安全威胁状态及其发展趋势； 2. 系统能够描绘出态势成因雷达图和帕累托图，展示出每种态势成因在态势指数中所占的比重； 3. 系统能够分析并展示当前态势指数与上个周期的态势指数的环比变化情况【提供截图】； |
| 资产管理 | 1. 系统具有资产管理的功能，能够将被管理IT资产进行分组、分域的统一维护。 2. 系统提供基于资产的拓扑视图，可以显示资产之间的逻辑连接关系。【提供截图】； 3. 在资产拓扑上可查看每个资产节点的基本属性、事件信息、告警信息、漏洞信息等，并且支持向下钻取； |
| 拓扑管理 | 1. 系统能够描绘出网络拓扑图，展示IT资产之间的逻辑拓扑连接关系，并能够自动进行多种拓扑布局； 2. 网络拓扑图具备实时设备和链路运行监控功能，如果设备或者链路发生故障，能够自动的进行标记； |
| 日志采集 | 1. 无需另外安装软件组件，管理中心即可通过 SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFTP、NetBIOS、OPSEC等多种方式完成日志收集功能； 2. 可灵活定制不支持的数据源采集，而无须改动代码。 |
| 日志范式化 | 1. 具备日志范式化功能，实现对异构日志格式的统一化； 2. 范式化字段至少应包括事件接收时间、事件产生时间、用户名称、源地址、源端口、目的地址 、目的端口、设备地址、设备名称等； |
| 日志传输和存储转发 | 1. 日志可加密压缩传输，保证数据的完整性和机密性； 2. 日志可加密存储。支持大数据量存储； 3. 支持加密压缩方式转发，定时转发【提供截图】。 |
| 日志采集器 | 1. 系统提供独立的日志采集器用于日志的采集，日志采集器可分布式部署； 2. 具有独立的管理界面，能够监视采集器所在服务器的运行状况； 3. 审计中心可以集中对日志采集器进行统一管理，能够对日志的解析策略进行统一下发【提供截图】； 4. 日志采集器支持以SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、NetBIOS、OPSEC等多种方式完成日志收集； |
| 安全事件分析 | 1. 可自定义事件分析条件，并可保存为策略，以树形结构进行组织，形成一个分析策略树； 2. 可以显示一段时间的动态事件移动图，能够在图上显示每个时间切片的事件数量、等级，并能够在图上显示每秒事件数。 3. 可以多种形式展示动态事件移动图，包括折线图、柱状图、折柱混合图、等级堆积图等，并可进行选择切换【提供截图】； 4. 可以对事件依据其源目的IP和端口等各类字段信息进行深入的事件追踪调查，支持无限次数的追踪调查； |
| 关联分析 | 1. 系统具有基于规则的安全事件实时关联分析的能力，能够对不同的事件进行相关性分析，发掘潜在的信息； 2. 支持多事件关联，对不同来源的安全事件进行复杂的相关性分析【提供多事件关联分析规则的截图】 3. 能够对指定时间范围内的不同的历史日志进行相关性分析，发掘潜在的信息 |
| 集中设备运行监控 | 系统能够对各种不同厂商的安全设备、网络设备、主机的性能与可用性进行集中化实时监控 |
| 性能信息采集 | 1. 系统支持通过SNMP、TELNET、SSH、SSH2、ODBC、JMX、协议仿真等方式对IT资产进行性能与可用性信息的周期性采集； |
| 弱点管理 | 1. 系统具有弱点管理功能，能够导入资产的弱点信息，并计算资产/安全域/业务系统的脆弱性值。 2. 至少支持导入绿盟、启明星辰、榕基的漏扫结果； |
| 配置安全核查 | 1. 系统具有主动的配置安全核查功能，能够对核查对象的配置进行细粒度的安全符合性检查，并出具核查报告，报告中至少包含判定依据、检查点、标准值、实际值、原始结果、加固方案； 2. 提供Windows系列（Win2003、win2008、winXP、win7）安全配置核查项。 |
| 告警管理 | 1. 告警动作支持告警重定义、弹出提示框、播放警示音、发送邮件、发送SNMP Trap、发送短信、执行命令脚本、设备联动、发送Syslog、设置观察列表、引用通知等方式； |
| 报表管理 | 1. 系统内置了资产、事件、监控、风险等报表报告； 2. 支持按照天、月度、季度、年度等时间周期生成报表，，并支持邮件自动投递； 3. 支持报表报告的导出，导出的格式支持EXCEL、PDF、DOC、XML、HTML、RTF等，支持Office 2007格式； |
| 知识管理 | 1. 系统提供开放的知识管理功能，内置了大量的安全知识，同时也允许用户在系统使用过程中不断丰富和完善。 2. 系统预先建立的知识包括：案例库、漏洞库、事件分类库等； 3. 系统内置日志字典库，方便用户查询不同原始日志信息的错误ID号和详细描述信息 |