|  |  |
| --- | --- |
| **功能项** | **技术要求** |
| 产品架构与要求 | 支持对物理服务器、虚拟机、云服务器等及多种混合环境实施集中管理和监控，支持B/S模式部署 |
| ★采购300个主机授权许可 |
| ★采购的功能模块至少包含资产梳理、入侵检测、风险评估、账号风险扫描、漏洞扫描、安全基线、防病毒、Webshell、微隔离、勒索场景化防护、微蜜罐、系统加固、性能监控、主机IPS（虚拟补丁）等至少14个能力（提供截图） |
| 支持Windows服务器操作系统、Linux、统信、麒麟操作系统 |
| 资产梳理 | 提供服务器资产的自定义采集能力。支持自动采集和任务采集两种资产收集方式，自动采集支持设置不同类型资产以小时/天/周/月的不同频率采集，任务采集支持选择不同类型资产、采集频率和服务器范围。 |
| ★提供账号、端口、计划任务的新增、修改、删除等变更行为的监控能力。支持展示上述资产变更的变更类型、变更内容、变更详情，支持设置资产变更监控频率。（提供截图） |
| ★提供Windows、Linux服务器统一的资产展示能力。支持跨系统、跨资产类型、跨主机进行快捷搜索。对搜索匹配到的资产关键字进行高亮标记，统计搜索到的资产数量，并提供搜索高级查询语法规则和快捷保存搜索条件以方便搜索。（提供截图） |
| 入侵检测与风险评估 | 支持对攻击者发起的恶意扫描行为进行识别，可防护端口扫描和扫描器扫描行为，以攻击和受害两种视角展示扫描信息包括：发生时间、受害IP、攻击IP、攻击类型、扫描端口、扫描次数、在威胁情报中是否为黑IP等信息。 |
| 支持统计总风险及各类风险数量，展示影响服务器信息。通过各类图表展示安全评分趋势、风险项趋势、账户风险类型分布、口令风险应用排行、漏洞风险项数量、配置风险排行等相关统计信息，便于用户快速了解风险整体情况 |
| 支持对不同账号使用同一密码的口令复用行为进行检测，支持统计相同密码的账户数量、账户所在服务器、账户名称、账户状态等信息，并支持导出。 |
| 病毒查杀 | 支持勒索病毒实时防护，提供勒索诱饵防护、系统还原点和卷影保护、内核免疫等多种手段增强对勒索病毒的实时防护能力。 |
| 漏洞扫描 | 支持通过扫描任务方式检测服务器存在的漏洞。  1、支持检测的漏洞数量应不低于4000个。厂商应提供推荐扫描的漏洞项，形成模板供客户快速选择；同时支持按照漏洞名称、漏洞编号、漏洞等级、漏洞类型、系统类型、应用名称、检测原理、披露时间、存在EXP、本地提权、内核风险、修复影响、是否可防护等信息搜索或筛选特定漏洞进行扫描。2、支持查看扫描任务运行情况，展示扫描目标服务器当前的扫描状态。针对服务器扫描失败的情况，需给出扫描失败原因。  3、支持将扫描任务结果进行报表导出，至少应支持Word和HTML两种格式。 |
| 支持对Windows服务器漏洞进行补丁修复安装。  1、支持展示漏洞关联对应的补丁信息，包括补丁编号、补丁大小、发布日期、补丁描述、是否重启系统等参考信息。  2、支持对漏洞操作进行实体补丁修复，修复前需二次校验密码和验证码，以避免误操作和恶意利用。  3、支持的补丁数量应不低于400个，并提供补丁信息的导出。  4、支持设置补丁修复的并发，避免大量服务器同时修复对计算、网络资源的瞬时开销过大。 |
| 安全基线 | 支持基线检查能力，支持灵活可自定义的基线规则。  1、支持等保二级、等保三级、CIS等合规性基线。  2、支持Tomcat、TongWeb、Weblogic、Resin、Nginx、Jetty、Jboss、IIS、Apache等Web应用中间件的基线。  3、支持AntDB、DB2、GaussDB、GreatDB、HBase、MySQL、MongDB、Oracle、Redis、PostgreSQL、SQL Server、人大金仓DB等数据库基线。  4、支持厂商最佳实践、推荐类基线。  5、支持自定义基线模板。 |
| webshell | 支持Webshell的实时监测，支持批量开启关闭实时监测。 |
| 支持对内存型Webshell的实时检测。  - 支持展示内存马的发现时间、风险等级、事件描述、处理意见、来源、分类、类型、类名、父类名、实现的接口、所属类加载器、文件MD5、进程名、进程PID、进程路径、进程所属用户、进程启动时间、端口、命令行  - 支持下载内存马的原class文件，支持下载反编译后的java文件。  - 支持对内存马进行加白，支持对已加白的内存马白名单进行编辑、删除、导出等操作。  - 支持记录管理内存马的操作历史。 |
| 账号风险 | 所投产品应支持对不同账号使用同一密码的口令复用行为进行检测，支持统计相同密码的账户数量、账户所在服务器、账户名称、账户状态等信息，并支持导出。 |
| 入侵检测 | 1、支持对攻击者发起的恶意扫描行为进行识别，可防护端口扫描和扫描器扫描行为，以攻击和受害两种视角展示扫描信息包括：发生时间、受害IP、攻击IP、攻击类型、扫描端口、扫描次数、在威胁情报中是否为黑IP等信息。  2、支持根据单个IP请求时间范围和扫描端口数量设置对发起扫描的IP锁定时间。  3、支持使用者根据判断手动对发起扫描行为的IP地址进行黑名单/白名单操作。 |
| ★文件分发 | 支持批量向服务器传输文件并具备一定的自动执行的能力。可通过此功能将需要执行的脚本或补丁快速传输到指定服务器，节省运维成本。 |
| 1、支持定义下发文件的存储位置。  2、支持在下发文件存在相同名称时可选择是否覆盖或增加文件后缀方式区分文件。  3、支持当文件所推送的目录不存在时可选择自动创建目录或不推送文件。  4、支持对文件推送时间设定，可选择立即推送文件或延迟推送。  5、支持设置文件推送到服务器后是否需要运行。  6、支持限制客户端下载文件时的下载速度，避免占用过大带宽 （提供上述功能截图） |
| 在管理中心上传的文件超过90天上且未被任务引用的文件可自动清理，避免占用管理中心过多空间。  文件使用空间超过管理中心存储空间的90%时进行告警提示，避免导致管理中心异常。  管理中心支持记录下发文件的信息，包括：文件名、文件MD5、文件大小、文件状态、上传人、上传时间、最近推送时间等信息。 |
| 支持管理中心上传即将要下发的文件时通过OTP动态口令验证下发者身份是否合法。 |
| 微隔离 | 微隔离能力应模块化集成在主机安全中，无需部署微隔离控制台、微隔离插件等额外组件，降低部署及运维成本。 |
| ★支持梳理展示访问端口的目标IP地址、IP归属、威胁情报匹配、首次时间和最近时间，并支持导出。（提供功能截图） |
| ★支持梳理展示进程外连的外连IP地址、外连域名、外连端口、IP归属、威胁情报匹配、首次时间和最近时间，并支持导出。（提供功能截图） |
| 性能监控 | 支持业务优先设置、支持Agent自动降级、自动停用、自动重启、性能限制等操作 |
| 主机IPS | 支持主机IPS（入侵防御）能力。 |
| 支持IPS特征库的升级。 |
| 具备强大的威胁情报生产能力，提供不少于10份公开发布的APT报告作为证明，提供报告链接、名称与封面 |
| 系统加固 | ★支持监控文件和文件夹，并可设置可信进程和可信路径允许操作。（提供功能截图） |
| 控制文件和文件夹的权限包括：读取、写入、链接、创建、执行、删除、重命名等，同时可提供监控和防护两种模式。 |
| 支持设置可信进程和可信注册表项/值允许操作。 |
| 控制文件和文件夹的权限包括：读取、写入、创建、删除、重命名等，同时可提供监控和防护两种模式。 |
| ★通过对Linux和Windows操作系统深度解析提供对操作系统加固能力，具体防护项覆盖系统关键文件、系统重要服务、系统网络访问方面，且加固条数不少于60项。 （提供功能截图） |
| 支持设置可信进程和可信文件允许操作，同时可提供监控和防护两种模式。（提供功能截图） |
| 应用防护 | ★支持学习每台服务器的网络外连行为、命令执行行为、文件创建行为，并形成图形化的时间轴行为基线，对于偏离行为以外的动作进行告警。（提供功能截图） |
| 支持支持对一台或一组服务器进行白名单学习策略，并可设置学习时长，学习后可形成应用列表及HASH值，对偏离学习列表以外的应用进行告警和拦截。 |
| RASP高级防护 | 一体化RASP、不需要再单独部署RASP控制台 |
| 支持 web入侵防护、Web服务器溢出攻击防护、文件名解析漏洞防护、禁止浏览畸形文件、自动屏蔽扫描器、X-Forwarded-For防护、禁止下载特定类型文件 、网站浏览实时防护 、 请求类型控制 、 HTTP请求头防护功能，同时针对高危web应用漏洞提供虚拟补丁能力，在不打实体补丁情况下可防止漏洞被利用。 （提供功能截图） |
| 支持禁止下载特定类型文件可限制文件类型不少于1000种，同时支持自定义文件类型。 |
| 支持分析URL请求，仅允许指定IP访问特定URL地址 ，以解决服务器访问恶意网站 |
| 提供服务器后台URL资产采集能力。通过手动添加或文件导入的方式设置URL关键字，从流量中匹配学习服务器上存在的后台URL资产，并支持导出。 |
| ★支持借助主机RASP插件、主机WAF插件增强Webshell的实时监测能力，支持额外获取Webshell植入时的HTTP信息，包括方法、user-agent、url、域名等信息。（提供截图） |
| 勒索场景化防护 | 支持对勒索事件全杀伤链的防护能力，通过产品帮助建设服务器勒索能力，可从勒索事件链条的三个阶段解决勒索攻击问题（尝试入侵、发起攻击、网内传播）。  可结合勒索事件攻击链条依次进行告警查看和安全加固配置  Step01：限制端口连接范围收敛服务器外网暴露面  Step02：多项风险点排查，提升服务器整体安全性防患于未然  Step03：勒索病毒实时查杀，防止恶意程序落地  Step04：勒索病毒专项防护，提供勒索诱饵防护、系统还原点保护、卷影保护能力  Step05：系统关键目录加固防护（操作系统加固、用户目录保护、敏感配置文件保护、WEB目录保护）  Step06：勒索病毒应急处置（全局文件黑名单、勒索病毒查杀、一键隔离） （提供上述功能截图） |
| 支持针对勒索攻击事件可独立展示告警和防护配置，同时产品预置Linux和Windows系统勒索防护配置模版，可一键下发防护策略 |
| 提供国家级第三方机构对产品防勒索能力的检验证明/证书 |
| 运维管理 | ★具备对日志的高性能处理能力，投标时提供信息产业信息安全测评中心、公安部计算机信息系统安全产品质量监督检验中心或国家知识产权局第三方权威机构出具的检测报告或证明文件复印件（检测报告或证明文件中须具有 “高性能”以及“Syslog日志处理”等关键字样来明确体现支持该技术） |
| 资质要求 | 软件开发商要求为“信息安全等级保护关键技术国家工程实验室”参建单位 |
| ★其他要求 | 一年软件升级、一年库升级服务，投标时提供原厂商出具的售后服务承诺函 |

备注：打★为关键指标，必须满足