**服务器安全增强系统管理平台**

**一、技术需求**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **技术指标** | **数量** | **单位** | **备注** |
|  | 核心管理控制 分析平台 | 1、支持对实体服务器、虚拟机、VPS和云服务器等及多种混合环境实施集中管理和监控，同时支持OpenStack等云操作平台，Xen、Hyper-V、Vmware、KVM等虚拟化架构。▲2、操作系统兼容性：支持windows/linux主流操作系统，包括但不限于以下的操作系统：Windows Server 2003 SP2（x86/x64）、Windows Server 2008（x86/x64）、Windows Server 2012、Windows Server 2016、Windows Server 2019；RedHat 4.3~RedHat 5.11（x86/x64）、RedHat 6.0~RedHat 6.7（x86/x64）、RedHat 7.0~RedHat 7.2 RedHat8.0 ；CentOS 4.3~CentOS 5.11（x86/x64）、CentOS 6.0~CentOS 6.10（x86/x64）、CentOS 7.0~CentOS 7.6、Centos8.0；Ubuntu10.0以上；Suse 10~Suse 10 sp3、Suse 11~Suse 11 sp3、Suse 12；中标麒麟 ；红旗Redflag3~4。3、web中间件支持：支持主流web中间件，包括但不限于以下的web中间件：IIS 6/IIS 7/IIS 7.5/IIS 8；Apache 2.0/Apache 2.2/Apache 2.4（x86、x64）； Nginx 1.0.\*、Nginx 1.2.\*、Nginx 1.4.\*、Nginx 1.6.\*~1.17.\*； Kangle；Tomcat、Weblogic、WebSphere、TongWeb、Jboss、Glassfish、Jetty等。4、支持全类型网络流量检测，包括但不限于以下语言：Asp,.net,php,java。5、支持可视化虚拟安全域功能，将服务器隔离在受限环境，有效抵御提权等高级攻击方式，形成检测、响应、拦截、溯源为一体的未知威胁响应能力。▲6、通过在业务服务器上部署探针（包括内核探针和应用探针）持续对业务服务器上的流量和行为进行监控，并支持与核心管理控制分析平台的联动，完成资产识别、风险识别、威胁感知、安全防御、攻击事件判定及回溯等功能（提供功能截图证明）。7、采用PC控制端与web浏览器管理方式，实时展示探针安全状况、回溯事件以及下发安全策略，对安全事件进行邮件告警，方便用户查看资产以及探针安全状态。8、支持驱动级防护技术，即使探针被意外关闭，防护依然有效。9、核心管理控制分析平台支持系统防护、网络攻击防护功能，服务器探支持反逆向、反调试、自保护功能，对服务器端探针的数据收集、挖掘分析、风险扫描等全部从内部架构完成，通信采用安全加密机制，提供更高的私密性和安全性。10、程序对WEB系统造成的延迟低于2%。程序占用的CPU、内存资源低于10%，系统具有自动降级机制，可设置自杀阈值。▲11、生产厂商具备由中国信息安全测评中心颁发的：国家信息安全测评信息安全服务资质证书（云计算安全类）（提供证书复印件）。▲12、生产厂商具备由国家工业和信息化部认证颁发的ITSS认证证书，服务类型为SaaS服务，能力等级为二级及以上（一级最高）（提供证书复印件）。▲13、支持与现网部署的终端安全管理系统联动，将发现的恶意代码程序 、病毒进行实时同步，并进行查杀和阻断（提供功能截图证明）。 | 1 | 套 |  |
|  | 服务器监测与防护探针 | 1、探针功能须包括内核探针和应用探针，实现系统权限及应用的控制与隔离，并持续对业务服务器上的流量和行为进行监控有效抵御恶意程序执行，提权等已知未知APT攻击，实现提供整体的安全加固。▲2、支持服务器内核加固技术，加强操作系统自身对抗恶意代码和黑客攻击的能力，抵御非法提权、非法创建可执行文件等黑客行为，有效降低无补丁可打、无法打补丁带来的的安全风险，实现 Windows操作系统权限控制：将非管理员组账户添加到管理员组；在系统目录下对可执行类型文件进行读写操作；添加启动项；加载没有数字签名的驱动；Linux操作系统权限控制：修改账户信息；修改系统配置文件；添加系统自启动项；在系统目录下创建及修改可执行文件；修改系统日志（提供功能截图证明）。3、支持通过读取路径、进程名、配置文件、执行命令等方式来获得相应的资产指纹，进行细粒度资产收集，可以获取服务器配置信息、应用、端口、进程、账户、计划任务等服务器关键资产。▲4、支持弱口令检测，基于密码长度、复杂度、常见字典等检测系统及应用弱口令，并支持用户自定义规则，包括但不限于：系统弱口令、应用弱口令（oracle、mysql、sqlserver、PostgreSQL、tomcat、weblogi）；同时具备防暴力破解技术，能有效防御针对RDP、SSH、FTP服务的暴力破解，适用于FTP等其他类型的服务器（提供功能截图证明）。▲5、支持针对服务器和网站的目录及文件进行全面巡检扫描，对服务器和网站存在的安全隐患进行检查并修复。“服务器安全”主要针对计划任务、账户（登录账户、克隆账户、隐藏账户）及各功能开启状态进行检查和修复；“网站安全”主要针对网页木马、网站挂马和暗链进行检查和清除（提供功能截图证明）。▲6、支持登录防护”功能，针对Windows及Linux操作系统的远程登录进行限制及防护，用户可对“用户名”、“IP地址范围”、“时间范围”进行具体设置，并通过选择“允许登录”、“禁止登录”等相应的处理方式进行防护（提供功能截图证明）。▲7、具备“网站漏洞防护”功能，包括：SQL注入防护、XSS防护、漏洞利用攻击防护可根据不同检测对象（URL、Cookie、Post）进行具体防护规则的配置（开启与关闭）；禁止下载特定类型文件，可自定义设置禁止下载的特定文件类型；网站浏览实时防护可自定义设置网页木马的文件类型，将对设置列表中的网页类型进行基于行为的木马实时检测；HTTP请求头防护可自定义设置防护规则，自定义选择HTTP头标识进行防护（提供功能截图证明）；支持未知上传漏洞防护，对网站中存在的文件上传漏洞页面进行防护，上传危险页面或程序能自动拦截（提供功能截图证明）。8、支持虚拟化安全域技术，将应用进程隔离在虚拟化安全域内，限制应用进程权限，防止黑客利用应用程序漏洞提权、创建可执行文件等非法操作；支持WEB进程权限防护：限制WEB服务器进程权限，例如禁止执行cmd.exe等，数据库进程防护：MySQL 、SQL server 进程防护。▲9、支持基于服务器分布式防火墙技术，可以跨虚拟架构、跨网段定义服务器访问控制策略，防止攻击者入侵内部业务网络后的东西向移动（提供功能截图证明）；可基于网卡驱动，不依赖iptable等系统防火墙，可以基于角色、标签定义主机、主机应用间的细粒度访问控制策略（提供功能截图证明）。10、支持监控业务环境中服务器间访问关系（数据流）并将其可视化；支持业务资产可视化；业务资产间访问关系可视化；流量信息可视化；访问端口可视化以及访问数量可视化。11、支持微隔离技术，限制主机非法外连访问控制，可基于IP、IP段、网址定义进网及出网访问规则。12、支持文件防篡改功能，当选择被防护的网站目录后，其目录下的所有文件及子目录所有文件将禁止被篡改。可对网站目录下的文件进行防篡改设置，包括禁止被创建、删除、修改等，也可对其中的防篡改目录及文件进行“放行”操作，允许某些目录及文件被创建、删除、修改等。▲13、支持驱动级网页防篡改功能，可以保护整个目录、网页或文件不被恶意修改或者变更，支持监控与防护两种模式（提供功能截图证明）。▲14、支持在内核及应用层探针中设置监控点，将本地无法判断的异常webshell，上传至云中心沙盒，通过脚本虚拟机的无签名检测技术，有效发现加密、变形webshell（提供功能截图证明）。▲15、支持防护日志功能提供对防护过程中所产生的各类日志的查询，包括：网站防护日志、系统防护日志、登录日志、巡检日志及监控日志。日志包含具体时间、日志类别及描述等信息，用户可将日志导出，以便保存、查阅（提供功能截图证明）。16、实现智能化监控及预警，补充传统安全系统，解决高级持续性安全威胁问题。实现服务器统一安全运维管控，降低业务安全风险面，提升操作系统安全性。17、可基于内核探针、应用探针多维度收集黑客入侵轨迹，图形化IOC提供攻击者IP、攻击目标、操作手段、落地文件等信息。18、支持可提供服务器核心资源（CPU、内存、磁盘、网络IO）及web中间件实时性能监控（PV、并发连接数、进出网流量等），可设置报警阈值，实时掌控服务器状态。19、支持聚合多维度威胁情报，并于本地的流量检测引擎、漏扫引擎结合，包括但不限于： IP信誉库、MD5、漏洞等。20、可防止利用漏扫等端口扫描工具获取服务器敏感信息一键禁止端口扫描工具非法探测，可自定义检测规则。21、支持效防御SQL注入、命令执行、文件上传、任意文件读写、反序列化、Struts2 0day利用等基于传统签名方式无法防护的未知安全威胁，支持asp .net php java四种语言。▲22、生产厂商采用语境关联分析引擎软件技术实现准确的转发控制及威胁识别，取得该项技术的软件著作权（提供软件著作权证书复印件）。▲23、支持与现网部署的终端安全系统实现安全功能联动，探针与终端安全系统客户端实现威胁情报共享和同步，进行溯源结果比对，提升服务器防护为止威胁的能力（提供功能截图证明）。▲24、支持与现网部署的防火墙进行安全功能联动，发现威胁事件后支持对攻击IP、恶意域名和受害资产的流量进行阻断，将策略下发给防火墙，由防火墙执行阻断（提供功能截图证明）。 | 25 | 套 |  |