**参数需求表**

|  |  |
| --- | --- |
| 推荐品牌 | 深信服、绿盟、安恒 |
| **名称** | **参数需求**  注：1.“★”系指实质性要求条款； 2.允许功能相同但叫法不同 |
| 综合日志审计 | 1.工作模式：（1）能够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；（2）审计工作不影响被审计对象的性能、稳定性或日常管理流程；（3）审计结果存储于独立存储空间；（4）自身用户管理与设备或主机的管理、使用、权限无关联；（5）提供全中文WEB管理界面，无需安装任意客户端软件或插件；  2.硬件规格：（1）标准式机架设备，双电源，可用物理磁盘空间≥4\*4TB；★（2）日志存储量≥180天；（3）支持RAID架构以保证数据可靠性；（4）支持后期扩展外部网络存储(IP SAN、NAS、DAS、磁盘阵列等)；  3.处理性能：（1）提供≥200个日志源授权；（2）日志采集能力≥9000条/秒；  4.网络接口：（1）审计主机提供≥4个千兆电口；（2）支持IPv6网络协议；  5.日志收集：（1）提供Syslog、SNMP Trap、OPSec、FTP协议日志收集功能；（2）提供使用代理(Agent)方式提取日志并收集功能；（3）提供针对主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等的日志收集功能，其设备厂家包括但不限于：Cisco(思科)，Juniper，联想网御/网御神州，F5，华为，H3C，微软，绿盟，飞塔(fortinet)，Foundry，天融信，启明星辰，天网，趋势，东软，Nokia，CheckPoint，Hillstone(山石)，安恒，珠海伟思，BEA，中国电信，安氏，帕拉迪，apc，arbor，clam，戴尔（dell），digium，东方电子，EMC，中国电力科学研究院，Eudora，google，冠群金辰，linksys，Mcafee，netapp，NAS（美国国家安全局），永达，sonicwall，vigor，天存，西岭，Symantec（赛门铁克），Hardened-PHP，foundertech(方正)，三零盛安，allot，蓝盾，IBM，金诺网安，网威，nortel(北电)，citrix(思杰)，watchguard，中兴，阿帕奇，WINDOWS系统日志，Linux/UNIX syslog、IIS、Apache等；（4）提供常见的虚拟机环境日志收集功能，包括Xen、VMWare、Hyper-V等；  ★6.日志分析：（1）可以以日志等级进行过滤；（2）可以通过自定义配置将用户不关心的日志过滤掉；（3）能够对收集到的重复的日志进行自动的聚合归并，减少日志量；（4）可由用户定义和修改的日志的聚合归并逻辑规则;（5）能够将收集到的日志转发，当原始日志设备无法设置多个日志服务器时，可以通过本系统的日志转发功能将日志转发到其他日志存储设备；（6）能够对收集到的日志进行解析（标准化、归一化），解析规则可以根据客户要求定制扩展；（7）可对日志进行细粒度解析，解析后的日志根据具体日志包含但不限于：日期、发生时间、接收时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议、地理信息等；（8）提供基于内存的实时关联分析，跨设备的多事件关联分析；（9）提供自定义条件都事件进行聚合功能；（10）进行关联分析的规则可定制。关联分析功能：系统须具备一个安全知识库和包含资产信息的弱点库，当接收到指定资产并且匹配到弱点库中指定漏洞的攻击时，须触发与安全知识库、弱点库的关联，新增新的事件，并且提高威胁等级；  7.日志备份：（1）可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；（2）能够将日志备份自动传送到远程服务器；  8.日志查询：（1）提供B/S模式管理，支持SSL加密模式访问；（2）能够按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询；（3）能够用任意关键字对所有事件进行高性能全文检索；（4）可指定多个查询条件进行组合查询；（5）能够将查询的条件存储为查询模版，方便再次使用；（6）具有极高的日志高查询性能，支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果；  9.应用性能监控：（1）通过在目标主机上安装agent程序，能够监控目标主机的CPU利用率、内存使用率、磁盘使用情况、流量等信息，并能设置报警阈值；（2）提供如下应用的性能监控功能：操作系统（Windows、Linux、Aix、FeeBSD、HP-UX/Tru64、Max OS、Sun Solaris等）、数据库（mysql、oracle等）、应用服务器（weblogic、tomcat等）、web服务器（apache等）；（3）提供应用性能历史详情回溯查看功能；（4）提供如下性能监控参数：<1>提供监控Windows操作系统参数：cpu使用率、内存使用率、磁盘使用率、网络发送流量、网络接收流量、网络发送接收总流量、交换区使用率、磁盘总使用率、进程数、线程数等；<2>提供监控Linux操作系统参数：一分钟系统负载、5分钟系统负载、15分钟系统负载、cpu使用率、内存使用率、磁盘使用率、网络发送流量、网络接收流量、网络发送接收总流量、交换区使用率、磁盘总使用率、进程数、线程数等；<3>提供监控Mysql数据库参数：查询缓存命中率、键缓存命中率、立即获得锁数、连接数、线程数、每秒SQL查询数、每秒发送字节、每秒接收字节等；<4>提供监控Oracle数据库参数：库缓存命中率、内存排序比率、词典缓存命中率、SGA数据缓存命中率、重做日志缓存命中率等；<5>提供监控Apache参数：总访问数、写日志次数、每秒发送字节数、长连接数、关闭连接数、空闲活动数、查询DNS数、正在发送数、请求完成数、负载、等待连接数、总数据量、读操作数、工作线程数、空闲线程数、CPU占用率等；<6>提供监控应用服务器（tomcat、weblogic）参数：活动线程数、堆内存（已用）、守护线程数等；  10.脆弱性管理：（1）弱点管理：提供导入主流扫描器的扫描报告，可进行统一检索，并支持计算威胁等级；（2）内置≥73000条CVE漏洞数据知识库；（3）内置充足的符合OWASP的Web漏洞数据知识库；  11.告警功能：（1）可预设置安全告警策略；（2）提供数据阀值设置功能，超过阀值将产生告警;（3）可以通过邮件、短信和屏幕显示进行告警；（4）提供自动防止报警信息在短时间内大量发送功能(告警抑制)；（5）具备报警合并和在一个时间段内抑制报警次数的能力；  ★12.综合查询及报表管理：（1）内置合规性报表≥1000种；（2）内置SOX、ISO27001、WEB安全等解决方案包；（3）内置完善的等级保护合规报表；（4）内置综合性自动化审计报告；（5）提供用户自定义报表功能；（6）自定义的报表支持多个统计维度的数据集合；（7）数据报表支持数据趋势预测功能，根据历史规律数据对未来数据的发展趋势进行预测  报表支持详单数据钻取；（8）提供报表导出为PDF和Word等格式文件功能；  13.用户管理：（1）系统自带自身管理日志；（2）提供一键式故障排除功能；（3）提供自助式的升级接口，支持对产品升级、规则升级；  14.部署方式：（1）支持分布式部署；（2）支持集中式管理和升级模式；（3）支持分级管理模式；（5）采用B/S架构操作方式，无需客户端安装；（6）能够监控设备自身CPU、内存、磁盘等工作运行状况；  ★15.产品资质：具备公安部颁发的《计算机信息系统安全专用产品销售许可证》,提供证书复印件 |
| 数据库审计 | 1.硬件规格：（1）标准式机架设备，双电源；（2）可用物理磁盘空间≥2\*4TB，支持RAID架构以保证数据可靠性；（3）标配≥4个千兆电口；（4）支持IPv6网络协议；  2.处理性能：（1）数据吞吐量≥800Mbps；（2）业务流量吞吐≥4Gbps；（3）SQL审计抓包≥20000条SQL语句/s；（4）日志审计能力≥20亿条/天；（5）日志留存时长≥90天；（6）日志检索能力≥30000条/秒；  3.部署方式：（1）支持单机（采集器）、多机（管理器）部署，多机部署支持集中管理，可集中管理多台采集器审计的事件、分析，实现统一配置、统一报表、统一查询等；（2）支持数据库审计旁路镜像模式部署不影响数据库性能和网络架构；（3）数据库审计Agent抓包方式支持业务系统和数据库一体化部署的审计；  4.部署环境：支持虚拟化平台部署。（1）支持导入到主流虚拟化平台以模板的方式部署；（2）支持Sangfor-HCI (vma格式)、Kvm (qcow2格式)、Vmware (ova格式)等环境部署；  5.部署管理：（1）采用B/S管理方式，无需在被审计系统上安装任何代理；（2）无需单独的数据中心，一台设备完成所有工作；（3）提供图形用户界面，以简单、直观的方式完成策略配置、警报查询、攻击响应、集中管理等各种任务；  6.审计能力：（1）提供多种数据库类型的审计：包括Oracle数据库审计、SQL-Server数据库审计、DB2数据库审计、MySQL数据库审计、Informix数据库审计、达梦数据库审计、人大金仓数据库审计、postgresql数据库审计、sysbase数据库审计等；（2）能够同时审计多种数据库及跨多种数据库平台操作；（3）能够在windows平台上安装插件的方式审计，插件方式更快捷更稳定；（4）无需改变系统内核和驱动的原有工作方式来支撑审计，有效防止修改内核或驱动带来的系统崩溃隐患；（5）能够进行超长SQL语句解析、记录、账号、关联SQL操作语句绑定变量参数；（6）提供白名单审计，系统使用审计白名单将非关注的内容进行过滤，不进行记录，降低了存储空间和无用信息的堆砌。主要有：<1> SQL模版：源IP、业务系统、生效时间、SQL模版等；<2> URL地址：源IP、业务系统、生效时间、URL地址等；<3>数据库条件：源IP、业务系统、生效时间、客户端程序、数据库用户、数据库名、表名、操作类型等；（7）提供客户端程序、数据库用户、操作类型、数据库名表名、响应时间、返回行数、影响行数、响应内容等实现对敏感数据库操作的精细监控；（8）提供HTTP请求审计，可指定GET、POST、URL、响应码进行精细审计；（9）提供按时间段、源IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码等方式对数据库日志进行精细检索的功能；（10）提供按时间段、源IP、业务系统、搜索关键字等方式对WEB审计日志进行精细检索的功能；（11）提供按时间段、IP等方式对管理员操作日志进行检索的功能；（12）能够以PDF、Execl等形式导出日志；（13）深度解码数据库网络传输协议，完整记录用户数据库会话细节，包括发生时间、源IP、源端口、源MAC、目的IP、目的端口、数据库用户、数据库类型、操作类型、SQL语句、SQL模版、客户端程序名、响应码、影响行数、返回行数、SQL预计响应时间；（14）提供web审计日志的查询页面，支持通过日期、源IP、业务系统、以及指定url地址作为搜索关键字进行过滤查询，查询结果包括源区域、目的区域、操作对象、影响结果及其web三层关联信息等；（15）允许查看SQL语句会话日志、柱状图、会话视图等；  ★7.数据库安全：（1）内置充足的SQL安全规则，可以针对导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用grant、业务系统使用grant、客户端sp\_addrolemember 提权、web端sp\_addrolemember提权、查询内置敏感表、篡改内置敏感表等；（2）提供自定义数据库安全策略，可根据业务需要自定义各种场景的安全规则，对于违规的数据库访问可进行实时警告和阻断；（3）识别当前的SQL操作是否有暴库、撞库等严重性安全问题，如果命中了安全风险规则，那么可根据动作进行阻断、告警、记录等操作，可提示管理员作出相应的防御措施；（4）提供webshell日志查询功能，可查看webshell攻击的时间、源IP、业务系统、webshell名称、webshell所在目录；  8.统计分析：（1）提供以源IP、业务主机、操作类型、SQL模版、数据库用户为维度的数据库行为排行以及行为趋势分析的功能；（2）提供以新型SQL趋势统计、SQL响应性能分析；（3）提供执行SQL语句失败分析功能，包括登录失败排行，SQL语句失败排行；（4）提供吞吐量分析功能，包括SQL语句吞吐量排行、SQL语句吞吐量趋势、SQL操作类型吞吐量排行、SQL操作类型吞吐量趋势、数据库用户吞吐量排行、数据库用户吞吐量趋势、业务主机吞吐量排行、业务主机吞吐量趋势；（5）支持TB级日志秒级查询、支持指定源IP、时间日期、客户端程序、业务系统、数据库用户、操作类型等精细日志查询、支持操作类型精细化日志查询、支持风险级别排行统计查询、支持数据库条件的统计查询、支持统计趋势查询分析、支持风险级别查询分析、支持通过多SQL语句的统计查询、支持统计分析下钻、支持业务系统元素统计查询；（6）支持以时间、源IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码、策略、规则、风险级别、SQL模版为条件的数据库风险查询；（7）支持以风险级别、源IP、业务主机、数据库用户、风险类型为维度的数据库风险排行；  9.风险分析：（1）提供以风险级别、源IP、业务主机、数据库用户、风险类型为维度的数据库风险趋势功能；（2）提供查看最近的账号安全事件功能；（3）提供Syslog告警、SNMP trap告警、邮件告警，短信告警等告警方式；（4）旁路主动发rest包阻断技术，Netfilter框架技术可针对IP、端口、业务系统做精准阻断；  10.响应方式：提供系统异常、磁盘空间占用过高、采集器离线等告警方式；  11.系统管理：（1）提供日志备份和日志恢复功能；（2）提供系统日志查看，系统升级，重启操作，磁盘空间自动删除系统必备功能；（3）可以实时监控系统的CPU使用率，内存使用率和磁盘占用率，快速定位系统的负载压力和系统运行状况；（4）支持Syslog等方式向外发送审计日志；（5）支持SNMP方式，提供系统运行状态给第三方网管系统；  ★12.产品资质：具备公安部颁发的《计算机信息系统安全专用产品销售许可证》,提供证书复印件 |
| 堡垒机 | 1.硬件配置：（1）软硬件一体化产品，≤2U机架式设备；；（2）数据存储空间≥4T，支持RAID架构以保证数据可靠性；（3）配置≥6个千兆电口；  2.性能指标：（1）可管理资产数≥200个；（2）字符并发数≥1000个；（3）图形并发数≥500个；  3.支持IPv6网络协议；  4.部署方式：采用物理旁路模式部署，不影响网络结构  5.用户管理要求：（1）提供用户多角色划分功能，如系统管理员、资产管理员、普通用户、审计管理员等，对各类角色需要进行细粒度的权限管理；（2）提供用户的批量导入/导出功能，并支持按部门组织架构、按用户类型等分组方式；（3）提供用户安全策略功能，如密码锁定次数、密码有效期、密码复杂度、用户有效期、用户登录时间限制、用户登录IP范围等。  6.身份认证要求：（1）堡垒机须内嵌认证引擎，登录堡垒机的用户支持本地静态密码认证、短信认证、AD域认证、LDAP认证、RADIUS认证等认证方式；（2）支持基于用户或用户组设置不同的双因子认证模式，如网络组用户动态令牌、系统组用USBkey、外包人员用短信认证；（3）支持单个用户同时使用2种认证方式，如使用AD/LDAP的密码加动态口令的认证方式登录堡垒机、使用AD/LDAP的密码加短信口令的认证方式登录堡垒机；  7.设备管理要求：（1）支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP；可通过应用发布的方式进行协议扩展，无需定制即可支持其他通用及专有的应用程序，如数据库运维客户端工具Oracle/MSSQL/MySQL/DB2等、远程管理工具VMware vSphere Client、AS400等；（2）HTTP、HTTPS协议的web系统，且可以直接代填账号和密码；  （3）提供对设备进行按设备类型分组、按部门分组功能，设备批量导入/导出功能；（4）提供设备帐户和密码的自动登录、手工登录、半自动登录模式；（5）提供自动收集设备IP、运维协议、账号密码、与用户的权限关系功能，甚至可自动完成授权；  8.自动改密要求：（1）提供定期自动修改windows服务器、网络设备、linux/unix等目标设备密码功能；（2）自动修改windows服务器密码无需在目标服务器上安装agent、开启telnet服务等；（3）提供完善的自动改密策略功能，包括改密前发送密码、改密后发送密码、密码文件加密、密码传输加密、密码强度控制、自动密码恢复等。发送方式包括邮件、FTP、SFTP等；  9.设备访问方式要求：（1）Web访问方式：至少支持使用IE、谷歌、火狐等主流浏览器打开堡垒机的Web页面直接调用mstsc、VNC、Xmanager、SecureCRT、Putty、winscp、flashFXP、FileZilla、SecureFX等运维客户端工具；（2）客户端访问方式：支持使用本地的mstsc/Xshell/SecureCRT/Putty等客户端工具登录堡垒机访问图形或字符设备，视图界面一致性、搜索能力；（2）能够使用本地的winscp/flashFXP/FileZilla/SecureFX等客户端工具登录堡垒机访问SFTP/FTP服务器；（3）提供批量登录字符设备功能：能自动生成SecurCRT/Xshell工具的批量登录文件，实现在工具中批量登录多台设备；  10.运维操作审计要求：（1）提供对运维操作会话的在线监控、实时阻断、日志回放、起止时间、来源用户、来源IP、目标设备、协议/应用类型、命令记录、操作内容（如对文件的上传、下载、删除、修改等操作等）等的详细行为日志功能：（2）提供保存SSH的sz/rz命令（zmodem）传输的原始文件，保存SFTP/FTP传输的原始文件，保存远程桌面之间上传或下载的原始文件，保存RDP磁盘映射传输的原始文件等的功能；（3）提供全局搜索审计日志功能，无需区分图形/字符/文件/应用类型，只需通过关键信息直接搜索定位；  11.安全策略要求：（1）提供通过基于时间、IP/IP段、用户/用户组、设备/设备组、设备账号、命令关键字、命令关键字正则表达式、危险级别、黑白名单等组合访问控制策略功能，授权用户可访问的目标设备；（2）提供支持对重要命令进行审核功能：运维人员执行命令后，须等到管理员审批通过后才可执行成功；（3）提供自动推送脚本任务功能，如可自动备份交换机/路由器的配置信息、可自动执行周期任务，并将结果以邮件/FTP/SFTP的方式发送给相关管理员；  12.报表统计要求：（1）内置丰富的报表统计模板，可点击柱状图、饼状图或曲线图进行数据钻取分析，且支持PDF、doc、html等格式导出；（2）内置根据运维人员和组生成各种维度的分析报表，维度包含总为运维次数、时长、活动时长、会话起止时间、会话大小、命令数、上传下载文件数，分别从全局及平均值、最大值、最小值、单次运维、单个会话等角度提供非常有价值有意义的报表；（3）提供一键导出符合等级保护、SOX法案要求的综合分析报告；  ★13.产品资质：具备公安部颁发的《计算机信息系统安全专用产品销售许可证》,提供证书复印件 |
| 质保期 | 提供≥5年的原厂质保服务，7\*24小时技术服务及设备维保服务 |
| 售后服务要求 | 1.售后服务必须包含软件更新服务、产品保修服务、远程支持服务等相关原厂服务，设备出现质量问题，中标方须负责三包（包修、包退、包换）。每台设备上均应订铭牌（内容包括制造单位、设备名称、型号规格、出厂日期等）；  2．质保期内，设备在使用阶段如发现质量问题或故障，中标方收到采购方使用部门的通知后，须在10分钟内响应，3小时之内到达现场，24小时内解决故障。如在24小时之内仍不能排除故障且需中断业务进行维修的，中标方须在5个工作日内提供相应的设备，以保障采购方业务的正常进行，直至设备维修完成并重新投入使用。故障排除后中标方应出具书面故障诊断报告备案。若20个工作日内中标方无法完成该设备的维修并投入使用，则必须提供与原设备同档次及同等配置或以上的设备投入使用；  3.中标方须提出具体的维护、服务以及今后技术支持的措施计划；  4.质保期内，全部设备每年提供两次巡检，并对整套系统进行运行情况检测，同时提交巡检报告及意见给采购方；  5.质保期内，若中标方如未按上述要求进行响应的，则记为一次事故。每记一次事故，采购方有权扣除质保金总额的百分之十。若累计事故达到5次，则视中标方违约，不退还质保金，同时中标方必须继续履行合同义务，若不履行则采购方有权解除合同，并上报市采购中心将其列入黑名单，并保留进一步索赔的权利；  6.质保期内，除人为损坏和不可抗力外，期间所产生的任何维护或维修及更换零配件、维修人员差旅等各项费用均由中标方承担。若因采购方保管及使用不当造成的质量问题，中标方亦应负责修理，费用承担按三包规定执行或双方专门约定执行。 |
| 其它要求 | 1.中标后签订合同前，中标方必须提供原厂质保函，并交纳合同总金额10%作为履约保证金。  2.自合同签订之日起，中标方必须在20个工作日内完成交货。自交货之日起，中标方必须在15个工作日内按照采购方需求完成设备安装调试，并能上线正常运行使用且各项功能均能满足采购方需求，按照采购方需求提供服务。若非采购方因素造成中标方逾期未完成交货或设备安装调试的，则中标方应按每日（自逾期之日算起）向采购方支付合同总价款的百分之一元作为违约金。若逾期10日还未完成的，则视中标方不能履约，采购方有权解除合同，不退还履约保证金，同时中标方必须支付合同价款的10%用以赔偿采购方的损失。  3.设备安装调试所需的零备件必须由中标方提供。  4.中标方所提供的货物必须是合同约定的厂家生产、全新未使用过的（包括零部件、备件等），并完全符合原厂质量检测标准（以说明书、合格证为准）和国家质量检测标准以及合同规定的性能和功能要求。  5.自设备安装调试完成之日起，试运行3个月。在试运行期间，若因设备本身质量问题引发的故障，则中标方必须在12小时内排除。故障排除后，试运行时间延长10日。若因设备本身质量问题再一次发生故障，则采购方有权解除合同，不退还履约保证金，同时中标方必须支付合同价款的10%用以赔偿采购方的损失。  6.若试运行期满后，设备的各项功能全面且无任何故障发生，且中标方已完成对采购方相关人员关于设备的使用、管理操作等培训工作，使采购方人员掌握所需技能，可组织项目验收。  7.对技术复杂的货物，采购方可请国家认可的专业检测机构参与验收，并由其出具质量检测报告，检测费用由中标方承担。  8.若验收不合格，则采购方有权解除合同，不退还履约保证金，中标方必须支付合同价款的10%用以赔偿采购方的损失。  9.若系统验收合格后，采购方将在15个工作日内支付总额的100%，履约保证金自动转为质保金。质保期期满后，采购方退还质保金（不计利息）。  11.未经过采购方的书面同意，中标方不得转让其应履行的合同项下的义务，不得将部分合同项下的义务分包给其他单位完成。  12.中标方工作人员须遵守采购方现场及国家相关安全管理规定，其一切安全（含人身安全）由中标方负责，采购方不负任何责任。如因中标方自身原因发生的事故，所产生的损失及费用由中标方自行承担。 |