综合日志审计平台招标公告

安信农业保险股份有限公司（以下简称“征集人”）现邀请合格的供应商（以下简称“应征人”）就征集人所需项目进行项目征集，征集人偿付能力符合监管规定,具体可上征集人官网查询[www.aaic.com.cn](http://www.aaic.com.cn)，征集人将择优选定中选人，欢迎符合条件的应征人前来参与方案比选，现将有关事项公告如下。

1. 征集项目内容
2. 设备数量

综合日志审计平台1套

1. 设备要求

设备及设备附属配件均为原厂提供。

1. 应征人必须具备的条件：
2. 应征人须为原厂商或授权代理商，所投产品品牌为国内外知名品牌，所投服务器产品性能可靠，不少于三年市场应用案例。
3. 应征人必须具有独立法人资格，具有独立承担民事责任的能力，具备相应的经营范围且其注册资金或净资产（所有者权益）必须不小于 1000（含）万元人民币（或等值外币）。须提供有效《企业法人营业执照》副本复印件。
4. 应征人必须具有专业团队，具有较强的售前、售中和售后服务支持能力，提供7\*24报修服务电话及固定的客户服务经理，省会城市、一类城市、直辖市均需要有办事处及备件库。提供全国性服务网点的证明材料。提供人员素质和技术能力资质证明。
5. 投标人未被“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网”（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单;并提供截图证明；
6. 财务状况：投标人应具备良好的财务状况，具有足够的流动资金来承担招标范围各事项,提供近两年的财务状况报告复印件（至少包括资产负债表和利润表）。
7. 近六个月中任一月份的依法缴纳税收和社会保障资金的相关材料。
8. 法定代表人为同一个人的两个及两个以上法人，母公司与全资子公司/由其控股的子公司，不得同时参加本项目。
9. 法律、行政法规规定的其他条件。
10. 应证人需提供厂商对本项目的授权书。
11. 应征人所需提交材料
12. 有效《企业法人营业执照》副本复印件
13. 全国性服务网点的证明材料
14. 人员素质和技术能力资质证明
15. 企业征信证明
16. 近两年的财务状况报告复印件（至少包括资产负债表和利润表）
17. 近六个月中任一月份的依法缴纳税收和社会保障资金的相关材料
18. 以上所有资质证明都需加盖应征人公司公章
19. 售后服务要求
20. 应证人应为征集人提供及时周到的系统技术支持。
21. 应证人应确保为甲方提供7\*24小时技术支持服务，响应时间不应该超过1小时，现场响应支持不应超过4小时。
22. 应证人所提供设备保质期(维保)均为三年，集成商所提供的设备在保质期内因硬件、软件本身质量问题所造成的损坏或无法正常运行，由此产生的维修、更换硬件和软件故障排除等所需一切费用（包括工程师差旅费用等支出）由集成商负责。
23. 应证人应提供相应的备件支持，以便及时更换损坏硬件。
24. 应证人应在质保期后设备生命周期内有义务继续对系统设备提供维保服务，甲方将支付相应费用。
25. 针对以上要求，应证人可提供具体可行的有吸引力的合作方案。
26. 验收
27. 所有设备均需提供安装服务，所采购设备（包括软件）安装都必须由生产厂商授权集成商执行。
28. 安装前由征集人信息技术部协同征集人行政办公室对货物的品牌、数量、包装等方面进行实物验收。征集人提供的所有包装的货物均应完好无损。如遇交付前已拆封的货物，征集人有权拒绝或要求更换。应证人交货时，必需提供所有产品原厂或总代理出具的供货相关证明。
29. 应证人根据征集人技术要求在征集人信息技术部指导下进行设备安装、调试，并由征集人信息技术部进行使用性能方面的验收。
30. 报名方式

有意者请于2019年9月23日之前将标书及相关材料送至以下地址：上海市静安区共和新路3651号 顾晓磊收

商务联系人：顾晓磊

联系方式：021-66988356 guxl@aaic.com.cn

技术联系人：卫金凯

联系方式：021-66988391 weijk@aaic.com.cn

1. 投诉邮箱：kehufuwu@aaic.com.cn
2. 设备技术指标

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 品牌要求 | * 产品获得公安部计算机信息系统安全产品销售许可证以及公安部信息安全产品检测中心出具产品检验报告。所提供的产品检验报告须符合《信息安全技术日志分析产品检验规范》，并提供完整的检测报告复印件；
* 产品获得国家保密科技测评中心检测并获得涉密信息系统产品检测证书，需符合《涉及国家秘密的信息系统安全监控与审计产品技术要求》，并提供完整的检测报告复印件；
* 产品获得中国信息安全认证中心颁发的《IT产品信息安全认证证书》，需符合ISCCC-TR-056-2016《日志采集与分析产品安全技术要求》，并提供完整的检测报告复印件；
* 产品取得软件著作权登记证书；
* 原厂商为《国家网络与信息安全信息通报中心》技术支撑单位；
* 原厂商具有《中国信息安全认证中心》颁发的信息安全应急处理服务资质（一级）；
* 原厂商获得国家级《计算机网络应急技术处理协调中心》颁发的国家级网络安全应急响应单位；
* 原厂商具有信息安全服务资质证书（安全工程类三级）；
* 原厂商为《中国信息安全测评中心》中国国家信息安全漏洞库共享平台（CNNVD）一级技术支撑单位；
* 原厂商通过 ISO27001信息安全体系国际认证；
* 原厂商通过ISO9001 2008质量管理体系认证；
* 原厂商应具有CMMI5等级资质证书；
* 原厂商具有云计算安全联盟成员（CSA）证书。
 |
| 工作模式 | * 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；
* 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；
* 审计结果存储于独立存储空间；
* 自身用户管理与设备或主机的管理、使用、权限无关联；
* 提供全中文WEB管理界面，无需安装任意客户端软件或插件
 |
| 硬件规格 | 4个工作口，2个管理口，1个console口内存：8GB，磁盘：1T\*1双电源★ 产品CF卡化（提供第三方检测报告）可扩展项：磁盘可扩展至4T网口可扩展至10个（可扩展模块：4电、4光） |
| 处理性能 | * 支持审计100个日志源；
* 平均处理能力（每秒日志解析能力EPS）：4000EPS；
* 峰值处理能力（每秒日志解析能力EPS）：5000EPS。
 |
| 功能扩展 | * ★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。
 |
| 日志收集 | * 支持Syslog、SNMP Trap、OPSec、FTP协议日志收集；
* 支持使用代理(Agent)方式提取日志并收集；
* 支持目前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；
* 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；
* ★支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等。
 |
| 日志分析 | * 可以以日志等级进行过滤；
* 应该可以通过自定义配置将用户不关心的日志过滤掉；
* 支持对收集到的重复的日志进行自动的聚合归并，减少日志量；
* 支持可由用户定义和修改的日志的聚合归并逻辑规则；
* 支持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；
* 支持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；
* 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（公网情况）；
* ★支持基于内存的实时关联分析，跨设备的多事件关联分析；
* ★支持自定义条件的事件进行聚合；
* 具备安全评估模型，评估模型基于设备故障、认证登陆、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。（提供截图并加盖公司公章）
* 内置非法访问、可疑入侵、病毒爆发、设备异常、弱点针对等5大类50子类的安全分析场景（提供截图并加盖公司公章）
* ★进行关联分析的规则可定制；
* ★支持根据资产价值、资产漏洞、针对漏洞的威胁事件三者进行威胁的自动关联分析（三维关联），所有的三维关联算法和准则以CVE、Bugtraq、OWASP公开协议和标准为为基础。（提供第三方检测报告）
 |
| 日志备份 | * 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；
* ★支持日志备份自动传送到远程服务器。
 |
| 日志查询 | * 支持B/S模式管理，支持SSL加密模式访问；
* 支持按日期、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；
* 支持用任意关键字对所有事件进行高性能全文检索；
* 支持可指定多个查询条件进行组合查询；
* 支持将查询的条件存储为查询模版，方便再次使用；
* ★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。
 |
| 应用性能监控（APM） | * 支持如下应用的性能监控（Windows、Linux、Aix、FeeBSD、HP-UX/Tru64、Max OS、Sun Solaris）、数据库（mysql、oracle）、应用服务器（weblogic、tomcat）、web服务器（apache）；
* 支持应用性能历史详情回溯查看；
* 支持如下性能监控参数
* 支持监控Windows操作系统如下参数：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；
* 支持监控Linux操作系统如下参数：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
* 支持监控Mysql如下参数：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；
* 支持监控Oracle如下参数：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；
* 支持监控Apache如下参数：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
* 支持监控应用服务器（tomcat、weblogic）如下参数：活动线程数、堆内存（已用）、守护线程数。
 |
| 脆弱性管理 | * 支持从IBM Rational AppScan导入资产弱点漏洞信息；
* 支持从安恒明鉴Web应用监测工具导入网站弱点漏洞信息；
* 支持从安恒明鉴数据库弱点扫描器导入数据库弱点漏洞信息；
* 支持从NetSparker Web应用扫描器导入网站弱点漏洞信息；
* 支持从Nessus网络扫描器导入网络弱点漏洞信息；
* 支持从OpenVAS扫描器导入弱点漏洞信息；
* 内置73000+条CVE漏洞数据知识库；
* 内置数十项符合OWASP的Web漏洞数据知识库。
 |
| 地理安全系统 | * 内置GeoSec地理安全子系统，内置世界以及中国安全GIS地图；
* 支持用地理地图展示来源威胁的趋势；
* 支持用地理地图展示目的威胁的趋势；
* 支持在地理地图上标注威胁事件的发生分布；
* 内置IP地址到经纬度的转换库；
* 支持以地理信息类进行统计的数据报表；
* 支持切换Google地图（需要连通互联网）。
 |
| 告警功能 | * 可预设置安全告警策略；
* 支持数据阀值设置，超过阀值将产生告警；
* 可以通过邮件、短信和屏幕显示进行告警；
* 支持自动防止报警信息在短时间内大量发送(告警抑制)；
* 具备报警合并和在一个时间段内抑制报警次数的能力。
 |
| 综合查询及报表管理 | * 内置合规性报表1000+种；
* ★内置SOX、ISO27001、WEB安全等解决方案包；
* ★内置完善的等级保护合规报表；
* 内置综合性自动化审计报告；
* 支持用户自定义报表；
* 自定义的报表支持多个统计维度的数据集合；
* 支持报表导出为PDF和Word格式文件。
 |
| 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；
* 系统自带自身管理日志；
* ★注册用户资产时，提供自动发现识别能力；
* ★提供一键式故障排除功能；
* 提供自助式的升级接口，支持对产品升级、规则升级。
 |
| 部署方式 | * ★支持分布式部署；
* ★支持集中式管理和升级模式；
* 支持分级管理模式；
* 采用B/S架构操作方式，无需客户端安装；
* 支持监控设备自身CPU、内存、磁盘等工作运行状况。
 |
| 售后服务支持 | * 提供3年免费升级维护；
* 提供安装调试后1天本地操作培训；
* 提供24小时支持热线；
* 本地应急响应时间<=2小时。
 |