**许昌市检察院安全风险预警平台项目**

**采购需求**

## 一、投标人资格条件

（一）符合《中华人民共和国政府采购法》第22条的规定。

（二）本次招标不接受联合体投标。

（三）根据《关于在政府采购活动中查询及使用信用记录有关问题的通知》 (财库[2016]125 号)的规定，对列入失信被执行人、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及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，拒绝参与本项目政府采购活动。

## 二、技术要求

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **一、网络回溯分析设备招标参数（设备数量：1台）** | | | | | |
| **序号** | **设备名称** | | **技术指标及规格参数** | | |
| 1 | 网络回溯分析设备 | | **总体要求：**  1、★总体功能  能够分布式部署在关键的网络节点，长期实时分析并捕获流量，同时对捕获到的网络通讯数据包进行长期存储，从而提供对任何时间点的通讯数据进行回溯分析的能力。  2、界面要求  支持全中文界面和资料文档，要求提供全中文的分析界面，要求提供全中文的文档资料。  支持中英文双语协议解码功能。  3、 产品架构  标准机架式独立硬件设备，存储容量2TB；采集端口： 2或4个千兆电口；管理端口：2个千兆电口；支持RAID1存储，可热插拔。  4、★必须满足省、市、县互联互通，将市县级采集数据反馈到上级平台，实现市级、省级集中管理。 | | |
| **系统部署**  1、★分布式部署，要求能够部署在远程网络中进行长期实时分析，通过专用的  2、★控制台软件通过网络进行远程分析。  3、要求能支持流量镜像、分路器等方式部署。  4、★在采用镜像方式进行部署时，能够通过设定本地网络，区分内部和外部IP地址，并分别统计上行和下行流量。  5、能够实现链路聚合功能，能将多网卡的流量聚合捕获分析。  6、支持多任务分析，能够针对某网络接口支持多个捕获和分析任务同时进行分析。 | | |
| **集中管理系统**  1、基于Web的集中管理，能够集中管理所有分布式网络流量监测分析系统，收集监测结果数据。  2、集中用户管理，添加，配置用户权限，实现用户的权限管理。  3、集中的监测数据呈现，图形化警报数据呈现，警报日志呈现。 | | |
| **应用定义**  1、能够灵活的自定义应用，针对自定义的应用进行流量监测分析。  2、可根据TCP/UDP端口或端口范围、端口组自定义应用。  3、可根据IP地址、地址组、地址范围自定义应用。  4、可根据IP地址+端口自定义应用。  5、可根据网段、网段组自定义应用。 | | |
| **数据捕获保存**  1、能够实时捕获并保存网络中的通讯数据包。  2、网络中的通讯数据包能够长期保存，设备的存储容量不低于2Tbytes。  3、数据包以专用格式存储，只能采用专用的控制台软件读取和导出，不能用其他工具读取并导出。  4、数据包保存的性能要求能够实现800Mbps线速保存能力，数据包处理性能不低于200,000pps  5、能实时长期保存网络中的所有的网络总体流量统计数据包括比特率（上下行）、数据包率（上下行）、网络中TCP SYN数量、TCP SYN ACK数量、TCP SYN RST数量，总体流量统计数据要求能保存至少1个月。  6、能实时分析并长期保存网络中的所有数据流统计数据，包括详细的IP会话流、TCP会话流、UDP会话流数据，数据精度到秒级，数据流统计数据要求能保存至少1个月。  7、捕获数据包时能够根据条件过滤捕获，包括根据IP地址、地址段、通讯协议、TCP/UDP端口等条件过滤捕获。 | | |
| **数据检索分析要求**  1、能够方便的检索捕获的任意时间范围的网络通讯数据。  2、能够检索捕获的流量的趋势，包括总体流量的趋势，可区分网络的上行流量和下行流量；数据包趋势，可区分网络的上行数据包和下行数据包；TCP参数趋势，包括TCP同步数据包个数、TCP同步确认数据包个数、TCP同步重置数据包个数；利用率趋势，可区分网络的上行利用率和下行利用率。  3、能够检索指定时间范围的所有应用的通讯流量信息，包括接收发送流量，接收发送数据包等，用户可以根据自己的需求进行应用定义，定义条件包括IP地址、TCP/UDP端口、IP地址组和地址段、端口组或范围，以及多种条件的组合。  4、能够检索指定时间范围的所有IP主机的通讯流量信息，包括接收发送流量，接收发送数据包，比特率，数据包率，tcp连接请求数量，tcp同步响应数量，tcp同步重置数量，数据包的发收比等流量参数，并能够根据参数的大小进行排序。  5、能够显示Internet IP的区域归属，包括IP地址所属的国家和地区，可以根据国家和地区进行IP地址检索分析。  6、能够检索指定时间范围的所有IP主机间的通讯流量信息，包括接收发送流量，接收发送数据包等。  7、能够检索指定时间范围的所有TCP会话和UDP会话的通讯流量信息，包括接收发送流量，接收发送数据包等。  8、能够针对应用进行进一步的数据挖掘，分析某个应用中IP主机流量、IP会话、TCP会话和UDP会话详细列表。  9、能够针对IP主机进行进一步数据挖掘分析，分析某个IP主机的应用、IP会话、TCP会话和UDP会话。 | | |
| **流量监测报警功能**  1、能够对网络中的总体流量异常进行监控和报警。可根据链路的上下行bps、pps、上下行pps、利用率、上下行利用率、每秒tcp syn个数、每秒tcp syn ack个数设定阀值产生警报。警报的触发时间间隔可以为1秒，5秒，15秒，60秒。  2、能够对网络中关键主机的流量参数进行监测和报警。  3、警报流量参数：能够针对关键主机或全局主机的每秒字节数、收发每秒字节数、数据包数、收发每秒数据包数、平均包长、收发平均包长、数据包发收比、每秒发送tcp syn包数、每秒接收tcp syn包数、每秒发送tcp syn ack包数、每秒接收tcp syn ack数据包数等参数设定阀值，产生警报。  警报条件：能设定>=条件、<条件，多种参数条件的与或关系时间警报。  4、能够对网络中关键应用的流量参数进行监测和报警。  警报流量参数：能够针对关键应用或全局应用的每秒字节数、每秒数据包数、平均包长等参数设定阀值，产生警报。  5、警报条件：能设定>=条件、<条件，多种参数条件的与或关系时间警报。  触发时间间隔：1秒，5秒，15秒，60秒。  6、能够对可疑域名解析行为进行监测产生警报，可以定义域名列表、域名地址列表进行监测，发现可疑的域名解析，产生警报。  7、能够对电子邮件内容进行监测，定义敏感字参数，监测邮件内容中是否包含敏感信息。  8、能够对HTTP内容进行监测，定义敏感字参数，监测HTTP内容中的敏感信息。  9、能够对TCP/UDP数据流进行监测，通过定义特征值，监测异常的TCP/UDP通讯并产生警报，特征值可以包括十六进制和ASCII的特征定义。可定义多种特征的与或关系来监测异常数据流。  10、能够通过邮件和Syslog将报警信息发给指定接收者。 | | |
| **数据分析要求**  1、能够对检索到的网络通讯数据包进行深入分析。  2、提供物理端点和IP端点以及IP会话分析视图。  3、提供针对IP端点的入出流量，bps、pps、总流量、总数据包数分析。  4、提供针对IP端点的IP会话数量、TCP连接数量的统计分析，并可以按大小顺序进行排序。  5、提供针对IP端点的tcp同步包发送/接收数量、同步确认包发送/接收数量、TCP重置包发送/接收数量的统计，并可以按大小顺序进行排序。  6、提供针对IP端点的数据包发送/接收比的统计分析，提供针对IP端点的字节数发送/接收比的统计分析。  7、提供自动的IP端点分组功能，能将不同网段的IP端点按网段自动分组，同时能按Internet IP的地域归属进行自动分组，如美国、日本等。 | | |
| **TCP/UDP会话分析**  1、提供所有的tcp/udp会话列表，提供针对每个会话的数据包、字节数等统计参数。  2、提供针对TCP/UDP会话的流重组功能，将会话中的数据流重组显示。  3、能够对TCP会话中的详细应用数据传输过程进行深入分析，能够区分每一个应用交易处理请求和响应，对传输过程中的重传、重复的确认进行统计，对应用交易处理间隔响应进行分析。  4、提供针对TCP会话的时序图分析功能，能够图形化的显示TCP会话中的数据交互传输过程，能够图形化显示数据传输中的时间间隔。 | | |
| **安全分析要求**  1、提供ARP攻击分析视图，通过流量特征主动过滤疑似感染ARP病毒的主机列表，并在单独的分析视图中展现。  2、提供蠕虫病毒主机分析视图，自动判断存在感染蠕虫病毒的主机的网络行为特征并在单独的分析视图中展现。  3、支持自动判断存在DOS攻击或被攻击现象的主机的网络行为特征并在单独的分析视图中展现。  4、支持自动判断存在TCP端口扫描的主机的网络行为特征并在单独的分析视图中展现。  5、支持自动判断存在可疑的HTTP、POP3、SMTP会话的主机的网络行为特征并在单独的分析视图中展现。 | | |
| **应用日志**  1、提供对HTTP访问请求的日志记录功能，能记录所有的HTTP访问URL，并记录至日志文件中。  2、提供对DNS解析请求和响应的日志记录功能，能记录所有的DNS请求和响应日志，记录至日志文件。  3、提供对SMTP/POP3邮件发送接收的日志记录功能，能记录所有的邮件接收发送日志，并能还原保存相应的附件。  4、提供对MSN/Yahoo Messenger等即时通的通讯记录功能。 | | |
| **协议识别和解析要求**  1、提供对常见互联网协议的协议识别功能，至少能对350种以上的常见互联网协议进行识别。包括：  AARP, AARP Prbe, AARP Request, AARP Response, ACNET, AFP, AH, AIM, ARP, ARP Request, ARP Response, Auditd, BFTP, BGP, BOOTP, Biff, BitTorrent, CDC, CDP, CFS, CFTP, CGMP, CIFS, CMIP-Agent, CMIP-Man, COPS, CRIP, CRTP, CRUDP, CTF, Cisco-fna, Cisco-sys, Cisco-tna, Citrx ICA, DCCP, DCP, DDP,DECnet, DHCP, DIAG, DNS, DNS Error, DNS Query, DSR, Daytime, Discard, EGP, EIGRP, EIGRP Hello, EIGRP Query, EIGRP Reply, EIGRP Update, ESP, Echo, Emfis-cntl, Emfis-data, Ethernet - Other, Ethernet 802.2, Ethernet 802.3, Ethernet II, Ethernet SNAP, Ethernet SNAP - Other, eMule, FC, FCoE, FCP, FTP, FTP Ctrl, DTP Data, Finger, GDP, GGP, GRE, GTP, Gopher, H.225, H.323, HMP, HSRP, HTTP, HTTP Proxy, HTTPS, Http-mgmt, IBM-app, ICMP, ICMP DestUnreach, ICMP Echo Reply, ICMP Echo Req, ICMP Redirect, ICMP Time Ex, ICMPv6, ICP, IDFP, IDPR, IDRP, IGAP, IGMP, IGRP, IMAP, IAMP3, IAMP4, IMAP4/SSL, IP, IP - Other, IP Fragment, IPX, IPv6, IRC, IRC/SSL, IRTP, ISL, ISMP, ISO-IP, ISO-TP0, ISO-TP4, Kerberos, L2F, L2TP, LDAP, LDAPS, LPD, La-maint, Login, Loopback, MGCP, MPLS, MPLS Etype2, MPM, MPM-snd, MPP, MSN, MSP, MSRDP, MSSQL, Mcidas, Mit-ml-dev, Mnet-discovery, Mobile IP, Msg-auth, NAMP, NARP, NBDGM, NBIPX, NBNS, NBSSN, NCP, NETBLT, NFS, NLSP, NMSP, NNTP, NNTP/SSL, NPP, NSRMP, NTP, Nameserver, NetBEUI, NetBIOS,  提供对网络协议的解码分析能力，提供至少350种各种网络协议的解码分析能力。特别是如下协议的解码支持：MSN，QQ，Yahoo Messenger，BitTorrent，POP3，FTP，SMTP，HTTP，TELNET等。 | | |
| **二、综合监控分析中心招标参数(设备数量：1台)** | | | | | |
| **序号** | | **设备名称** | | **技术指标及规格参数** |
| 2 | | 综合监控分  析中心 | | **总体要求：**  1、界面要求  支持全中文界面和资料文档，要求提供全中文的分析界面，要求提供全中文的文档资料  2、产品结构  ★标准机架式独立硬件设备，存储容量8TB；管理端口：2个千兆电口；支持RAID5存储，可热插拔；  3、★必须满足省、市、县互联互通，将市县级采集数据反馈到上级平台，实现市级、省级集中管理。 |
| **警报统计**   1. 支持以列表和饼图的形式统计各类警报的数量和所占百分比。 2. 支持显示警报趋势图。 3. 支持根据链路组查看警报的区域分布情况。 4. 支持根据链路组进行警报挖掘。 5. 支持警报分类Top 10统计。 6. 支持警报IP Top 10统计。 |
| **警报查询**  1、支持警报查询，查询条件包括链路组、状态、等级、日期和关键字。  2、支持警报导出为XLS或CSV格式。  3、支持警报简报功能。  4、支持从警报呼出控制台功能。 |
| **链路/链路组流量监控**  1、支持查看单条链路和链路组的流量信息。  2、支持以柱状图的形式显示链路和链路组的流量信息。  3、流量相关的字段包括每秒总流量、每秒上下行总流量、峰值流量、谷值流量、每秒上行流量、每秒下行流量、每秒数据包、每秒上行数据包、每秒下行数据包、每秒上行TCP同步包、每秒下行TCP同步包、每秒TCP确认包、每秒上行TCP确认包、每秒下行TCP确认包、每秒TCP复位包、每秒上行TCP复位包、每秒下行TCP复位包、每秒流量利用率、每秒上行流量利用率、每秒下行流量利用率、每秒未处理警报数量。 |
| **链路流量监控**  1、★支持查看链路的流量趋势图，趋势图的数据类型包括流量、上行流量、下行流量、数据包、上行数据包和下行数据包。  2、支持查看应用的流量趋势图，可以选择系统应用和自定义应用。  3、支持查看链路的网络使用情况，包括流量、平均流量、利用率、数据包数、平均数据包数、TCP同步包数、TCP同步确认包数和TCP重置包数。  4、支持查看链路的网段流量统计信息，字段包括网段名称、字节数、数据包数、段内字节数、段内数据包数、TCP同步包、段内TCP同步包、TCP同步确认包、段内TCP同步确认包和段内TCP重置包。  5、支持查看链路的Top统计，包括Top网络应用、Top流量主机、Top数据包主机、Top发送同步包主机和Top同步包发收比主机。Top包括Top5、Top10和Top20。 |
| **链路流量分析**  1、支持查看链路的历史流量趋势图，趋势图数据类型包括流量、数据包、流量发收比和数据包发收比。  2、支持对主机进行分析，包括流量、数据包、流量发收比和TCP连接数。  3、支持对链路应用进行分析，包括流量和数据包。  4、支持对网络使用情况进行分析，包括总流量、平均流量、利用率、总数据包数、平均数据包数和总TCP同步包数。 |
| **服务器管理**  1、支持为前端服务器创建账户信息，包括账户名称和密码。  2、支持查看前端服务器的运行信息，包括服务器名、连接状态、更新时间、持续运行、CPU占用、可用内存、磁盘可用、登录密码、固件版本、登录次数（总计）、登录IP、登录时间、是否自动升级和创建时间。  3、支持查看前端服务器的链路信息，包括服务器名称、链路名称、链路创建时间、组名称、链路带宽和链路ID。  4、支持查看前端服务器链路的网卡信息，包括连接名称、MAC地址、IP地址和带宽。  5、支持查看前端服务器的交互日志，包括时间、交互事件和状态。 |
| **链路/链路组管理**  1、★支持查看所有链路的信息，包括服务器名称、链路名称、链路创建时间、组名称和状态。  2、支持删除链路。  3、支持添加、修改和删除链路组。  4、支持查看所有链路组信息，包括链路组名称和描述。 |
| **报表**  1、系统具有报表功能，支持日报表、周报表、月报表和年报表。  2、支持警报报表和流量报表。  3、支持报表调度计划，能够自动发送到指定电子邮件接收者。  4、支持报表日志查看，可以看到报表的生成记录，包括报表类型、调度类型、报表编号、时间、日志内容和收件邮箱。 |
| **用户权限管理**  1、支持添加、修改和删除用户。  2、支持为用户指定用户角色和设置其可见的链路组。  3、支持用户的快速查询。  4、支持添加、修改和删除用户角色，每种用户角色具有不同的权限。  5、可以设置权限的模块包括警报、流量监控、分析服务器列表、链路列表、链路组列表、报表、报表日志、用户列表、角色管理、审计日志、系统和服务。 |
| **审计日志**  1、提供系统的所有操作日志信息。  2、支持将日志导出为XLS和CSV两个格式。  3、支持按用户和时间查询日志信息。  4、日志信息中包括姓名、IP、时间、请求和响应。 |
| **系统配置**  1、支持进行SMTP服务器设置  2、支持进行数据保存周期的设置，可以分别设置审计日志和警报数据的保存天数。  3、支持设置警告包的签报数量，取值范围为100-50000。 |

## 三、相关要求

1、货物技术要求中“网络回溯分析设备”、“综合监控分析中心”产品须保证满足省、市、县互联互通，将市县级采集数据反馈到上级平台，实现市级、省级集中管理，投标厂商需提供能够实现互联互通的有效证明材料。

2、投标人实施人员具有公安部颁发的信息安全等级保护安全建设专业技术人员证书；

3、投标人投标文件中须明确所投产品的厂家、产地、品牌、型号、详细参数，**否则为无效投标。**

4、投标人应就该项目完整投标，**否则为无效投标。**

5、随机资料及附件齐全。

6、设备必须符合国家质量检测标准和本招标文件规定标准的全新正品现货，随货物提供《产品合格证》及其它相关质量证明文件。

7、专利权：投标人应保证用户在使用该货物或其任何一部分时不受第三方提出侵犯其专利权、商标权和工业设计权等的起诉。

8、投标人须明确免费包修期，同时应提出故障响应时间，在免费包修期内，同一质量问题连续两次维修仍无法正常使用，投标人必须予以更换同品牌、同型号的全新产品，超过保修期发生故障，用户可自由选择维修单位，如委托给投标人，投标人不得借故推诿，并且维修费不能超过市场平均价格。

9、投标人须明确维修点地址、负责人、联系人和联系电话，维修点具备什么样的维修能力等详细资料。

10、本项目为交钥匙工程（包括设备、材料、元件等购置、安装调试、验收、与其它施工单位协作所产生的费用等），如有招标文件中没有明确，而本项目必须的各种材料、设备、施工器械均应包括在本项目中，采购人不再另行进行支付有关款项。

11、项目交货期为30天，交货地点为采购人指定地点。

12、投标人应制订切实可行的实施计划，并严格按照交货期进行交货。

13、投标人应提供人员培训方案，并组织实施，内容包括（但不限于）安装调试、使用和运行管理、问题检测与修复等。

14、投标人必须成立合理的组织机构，建立健全保障项目顺利实施的各项管理制度和质量保证体系，安排足够的高素质人才参加本项目的建设。

15、在项目机构中应明确各岗位的职责、任职资格，确保工程顺利实施。根据本项目的业务性质，配备具有同类系统建设经验的项目经理、技术总监等人员承担本项目工作。

16、付款方式**（不响应者为无效投标）**

经验收合格付合同总价款的95%，5%免费质保期满一次付清。

17、采购预算：93万元，**超出者为无效投标。**

## 四、评分标准

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 项目 | 标准 | 说明 |
| 一 | 信誉及认证 | 15分 | 投标人具有信用AAA等级证书的得2分。 |
| 投标人能提供ISO/IEC20000-1:2005服务管理体系认证及ISO/IEC27001信息安全管理认证体系证书的得4分，有其中一项得2分，没有不得分。须提供以上证书复印件并加盖投标人公章，否则不得分。 |
| 投标人能提供涉及国家秘密的计算机信息系统资质甲级证书（系统集成）资质的得4分，能提供乙级证书的得2分，没有不得分。  须提供以上证书复印件并加盖投标人公章，否则不得分。 |
| 投标人能提供信息安全服务资质证书（安全工程类一级）的得2分。  投标人具有公安部颁发的信息安全等级保护安全建设服务机构能力评估合格证书得3分，没有不得分。  须提供以上证书复印件并加盖投标人公章，否则不得分。 |
| 二 | 业绩 | 10分 | 投标人提供2015年以来，政府采购招标中，具有安全系统建设相关项目业绩，中标金额90-300万元（含90万元）的单个项目得1分；300万元（含300万元）以上的单个项目得2分。最高得分10分（同时提供中标通知书、与最终用户签订的合同及验收报告复印件，其中合同提供合同首页、盖章页、采购内容页、金额页复印件，并加盖投标人公章，否则不得分）。 |
| 三 | 实施及售后服务 | 20分 | 本项目实施人员具有信息安全等级保护安全建设专业技术人员证书的，每份得1分，最多得3分，投标文件中提供证书复印件并加盖投标人公章及人员对应社保缴纳证明否则不得分。 |
| 投标人注册地在省内（包括投标公司或其分公司），提供营业执照证明得2分；针对本项目服务团队不少于3人，安排1人为服务经理，服务经理具有ITSS信息技术服务标准认证、ITIL信息技术基础架构库认证、PMP项目管理专业人士资格认证、服务管理认证证书，每提供一项加1分，最多加4分，投标文件中提供证书复印件及人员对应社保缴纳证明并加盖投标人公章否则不得分。 |
| 为本次采购产品提供原厂三年售后服务，投标文件中提供产品原厂商加盖公章的售后服务文件得2分，不提供不得分。 |
| 本次采购“网络回溯分析设备”、“综合监控分析中心”产品须保证满足省、市、县互联互通，将市县级采集数据反馈到上级平台，实现市级、省级集中管理，投标文件中提供能够实现互联互通的有效证明材料得3分，否则不得分。 |
| 有人员技术培训计划的，根据计划的详细程度，评为：一般、良好、优秀，分别得分为1分、2分、3分。 |
| 有工程实施计划的，工期进度安排得当，项目实施保障可靠，根据计划的详细程度，评为：一般、良好、优秀，分别得分为1分、2分、3分。 |
| 四 | 产品符合度 | 15分 | 投标产品的技术参数完全满足招标文件要求的得15分；产品的技术参数每负偏差一项扣2分，带★号项每负偏差一项扣4分。 |
| 五 | 产品价格 | 40分 | 满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算：  投标报价得分=(评标基准价／投标报价)×40 |