**货物分项报价表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 货物名称 | 规格 | 数量 | 原产地和制造商名称 | 单价 | 合价 |
| 1 | 信息安全风险预警系统（检察院专版） | 科来网络回溯分析设备RAS400（检察院专版） | 1 | 原产地：成都制造商名称：成都科来软件有限公司 | 217500 | 217500 |
| 2 | 防木马病毒预警系统 | KILL僵尸木马预警系统KSG-T500 | 1 | 原产地：北京制造商名称： 北京冠群金辰软件有限公司 | 128300 | 128300 |
| 投标总价（元） | 大写：叁拾肆万伍仟捌佰圆整 小写： 345800.00 |

**技术规格和商务条款偏差表**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 产品名称 | 技术参数及要求 | 响应或偏差情况说明 |
| 招标文件要求 | 投标文件 |
| 1 | 信息安全风险预警系统（检察院专版） | 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个千兆电口；管理端口：2个千兆电口；4、保证与省检察院的信息安全风险预警平台互连互通。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ip地址，并分别统计上行和下行流量。5、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。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300Mbps线速保存能力，数据包处理性能不低于100,000pps。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。数据检索分析要求：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。6、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。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。数据分析要求：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。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。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、提供对相关协议的即时通的通讯记录功能。协议识别和解析要求：提供对常见互联网协议的协议识别功能，至少能对300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 QueryDSR, 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300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。 | 总体要求：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。界面支持全中文界面和资料文档，提供全中文的分析界面，提供全中文的文档资料。支持中英文双语协议解码功能。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个千兆电口；管理端口：2个千兆电口；保证与省检察院的信息安全风险预警平台互连互通。系统部署：分布式部署，能够部署在远程网络中进行长期实时分析，通过专用的控制台软件通过网络进行远程分析。能支持流量镜像、分路器等方式部署。在采用镜像方式进行部署时，能够通过设定本地网络，区分ip地址，并分别统计上行和下行流量支持多任务分析，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：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。集中用户管理，添加，配置用户权限，实现用户的权限管理。集中的监测数据呈现，图形化警报数据呈现，警报日志呈现。数据捕获保存：能够实时捕获并保存网络中的通讯数据包。网络中的通讯数据包能够长期保存，设备的存储容量2Tbytes。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。数据包保存的性能能够实现300Mbps线速保存能力，数据包处理性能100,000pps。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1个月。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1个月。数据检索分析要求：能够方便的检索捕获的任意时间范围的网络通讯数据。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。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。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。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。流量监测报警功能：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。能够对网络中关键主机的流量参数进行监测和报警。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。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。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。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。数据分析要求能够对检索到的网络通讯数据包进行深入分析提供物理端点和IP端点以及IP会话分析视图提供针对IP端点的入出流量，bps、pps、总流量、总数据包数分析。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。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。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。安全分析要求：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。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。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。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。应用日志: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。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。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。提供对相关协议的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，能对300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 QueryDSR, 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,2、提供对网络协议的解码分析能力，3、提供300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。 | 响应招标文件 |
| 2 | 防木马病毒预警系统 | 网络接口：6×10/100/1000电口，2个USB外置接口，1个Console接口。性能要求：网络吞吐量≥1Gbps，病毒检测吞度量≥300Mbps，并发连接≥80万；接入方式：旁路接入模式，即插即用，适应各种复杂的网络环境，用户不需修改原有网络结构和配置，支持多路监听部署模式。液晶屏显示：可通过外置液晶屏显示系统CPU/内存使用率，查询设备管理IP。协议支持：支持非端口定义的协议识别，通讯服务端无论采用什么端口，都能正确识别HTTP/FTP/SMTP/POP3/IMAP/ SMB 等多种应用层协议，可根据需求选择所需监控的应用层协议。全面支持IPV4和IPV6网络环境。病毒过滤:精确识别邮件病毒、文件传输病毒、网页病毒等。蠕虫过滤:采用入侵防御（IPS）技术、IP/端口/数据包封锁技术，优化了蠕虫识别机制，不仅可监测已知蠕虫，还可以在未知蠕虫爆发时进行预警。木马通讯监控:可监控多数常见的木马通讯，内置数千种木马通讯协议识别特征，并且通过识别库不断再升级，可以识别新型木马，包括手机木马。僵尸网络监控:基于行为分析感知僵尸主机，通过多维度的数据分析和智能关联技术,实现对僵尸网络威胁的发现,便于用户提早发现网络中潜在的威胁风险。安全漏洞攻击监控:内置千余种漏洞攻击规则，可实时监控针对系统级发起的漏洞攻击。口令探测监控:可对常用的网络服务如：SMTP/POP3/IMAP/FTP/HTTP/SMB等进行口令探测的活动均可被监测。端口汇聚:支持最大四端口汇聚，支持主备、轮寻、802.3ad、自适应的汇聚模式。特征库升级:特征库每天至少更新一次，可根据需求灵活定义更新时间。通讯加密:提供Https、SSH等加密方式进行配置管理。管理IP:可以设置管理员IP地址，增加管理的安全性;权限划分:管理员按读配置和修改配置进行权限划为不同管理权限，例如配置管理、查看状态、系统维护等.管理界面提供对产品硬件本身CPU、内存、磁盘、网卡等运行状态的数据查询，提供CPU/内存/交换区负载曲线、网络流量曲线、过滤统计柱状图的查询。日志分析:通过管理界面，能够提供不同形式的日志展现及分析内容，包括类型统计、IP统计、趋势分析和明细查询等。部署模式:能实现与省、市、县互联互通，统一升级统一管理，同时省院平台能够对探针设备的数据进行采集分析等功能.拥有自主可控的防病毒引擎，资质要求：拥有自主可控的防病毒引擎，提供国家版权局颁发的防病毒软件著作权证书。 | 网络接口：6×10/100/1000电口，2个USB外置接口，1个Console接口。性能要求：网络吞吐量：1Gbps，病毒检测吞度量：300Mbps，并发连接：80万；接入方式：旁路接入模式，即插即用，适应各种复杂的网络环境，用户不需修改原有网络结构和配置，支持多路监听部署模式。液晶屏显示：可通过外置液晶屏显示系统CPU/内存使用率，查询设备管理IP。协议支持：支持非端口定义的协议识别，通讯服务端无论采用什么端口，都能正确识别HTTP/FTP/SMTP/POP3/IMAP/ SMB 等多种应用层协议，可根据需求选择所需监控的应用层协议。全面支持IPV4和IPV6网络环境。病毒过滤:精确识别邮件病毒、文件传输病毒、网页病毒等。蠕虫过滤:采用入侵防御（IPS）技术、IP/端口/数据包封锁技术，优化了蠕虫识别机制，不仅可监测已知蠕虫，还可以在未知蠕虫爆发时进行预警。木马通讯监控:可监控多数常见的木马通讯，内置数千种木马通讯协议识别特征，并且通过识别库不断再升级，可以识别新型木马，包括手机木马。僵尸网络监控:基于行为分析感知僵尸主机，通过多维度的数据分析和智能关联技术,实现对僵尸网络威胁的发现,便于用户提早发现网络中潜在的威胁风险。安全漏洞攻击监控:内置千余种漏洞攻击规则，可实时监控针对系统级发起的漏洞攻击。口令探测监控:可对常用的网络服务如：SMTP/POP3/IMAP/FTP/HTTP/SMB等进行口令探测的活动均可被监测。端口汇聚:支持最大四端口汇聚，支持主备、轮寻、802.3ad、自适应的汇聚模式。特征库升级:特征库每天更新一次，可根据需求灵活定义更新时间。通讯加密:提供Https、SSH等加密方式进行配置管理。管理IP:可以设置管理员IP地址，增加管理的安全性;权限划分:管理员按读配置和修改配置进行权限划为不同管理权限，例如配置管理、查看状态、系统维护等.管理界面提供对产品硬件本身CPU、内存、磁盘、网卡等运行状态的数据查询，提供CPU/内存/交换区负载曲线、网络流量曲线、过滤统计柱状图的查询。日志分析:通过管理界面，能够提供不同形式的日志展现及分析内容，包括类型统计、IP统计、趋势分析和明细查询等。部署模式:能实现与省、市、县互联互通，统一升级统一管理，同时省院平台能够对探针设备的数据进行采集分析等功能.拥有自主可控的防病毒引擎，资质要求：拥有自主可控的防病毒引擎，提供国家版权局颁发的防病毒软件著作权证书（见后文）。 | 响应招标文件 |