关于福建建筑学校网络安全设备采购项目比选采购通知

第一部分 比选采购通知

福建建筑学校对福建建筑学校网络安全设备采购项目进行比选，现欢迎符合要求的报价单位前来提交密封比选文件。

一.福建建筑学校网络安全设备采购项目概况：详见第二部分《技术服务要求》。

二.项目内容：

品目号	采购标的	数量	预算
1-1	运维安全管理系统	1（项）	29.4 万元
1-2	入侵防御	1（项）	
1-3	日志审计	1（项）	

三.报名时间及地址

1、报名时间：2020 年 11 月 19 日上午 9:00 至 2020 年 11 月 19 日上午 11:00。

2、报名地址：福建建筑学校校保安室（仓山区中店 43 号）。

3、报名应递交密封的投标材料并加盖公章：

（1）法定代表人授权委托书原件（法人本人报名不需要提供）；

（2）工商营业执照复印件（三证合一）；

（3）被授权人身份证原件和复印件；

（4）投标人承诺所投的具体产品均可直接在福建省政府采购网网上超市查询并购买，提供承诺函；

4、投标截止时间： 2020 年 11 月 19 日上午 11:00 点。投标人

应在此之前将密封的投标文件递交到校保安室，逾期递交的或不符合规定的投标文件将被拒绝接受。

四.报价文件递交

（1）时间：2020 年 11 月 19 日上午 9:00 至 2020 年 11 月 19 日上午 11:00。

（2）地点：报价方必须在上述时间段内将报价文件密封递交至福建建筑学校，逾期送达的报价文件将不予接受。

（3）递交联系人及电话：郑老师 13459114667

福建建筑学校

2020 年 11 月 13 日

第二部分 技术服务要求

一、项目概况

1.1 本项目名：福建建筑学校网络安全设备采购项目 。

1.2 报价方务必仔细阅读比选文件中所规定的，其中包括技术规格在内的所有细则。

二、技术和服务要求（以“★”标示的内容为不允许负偏离的实质性要求）

1-1 入侵防御

1、网络接口≥10 个千兆电口，网络层吞吐量≥4 Gbps，IPS 吞吐量≥1.5 Gbps，并发连接数（TCP）≥180 万，新建连接数≥4 万，单电源；

2、支持路由部署、透明网桥部署、旁路部署、虚拟网线以及混合部署等多种方式；

3、支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路；

4、★支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制，支持基于时间、地域、认证用户、子接口和 VLAN 等因素实现对象的流量控制；（需提供相关功能截图证明）

5、★支持采用无特征 AI 检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，给出基于 AI 技术的病毒检测报告；（需提供相关功能截图证明）

6、设备具备独立的入侵防护漏洞规则特征库，特征总数在 7000 条以上；

7、支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能；

8、★支持同访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间；（需提供相关功能截图证明）

9、★支持细致的服务器敏感数据识别，识别维度包含服务器 IP、业务重要性、识别方式、开放的服务与端口、敏感数据页面数以及更新时间等，并且可以进行详细的页面 URL 以及页面信息举证；（需提供相关功能截图证明）

10、★可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则；（需提供相关功能截图证明）

11、支持连接会话展示，可针对具体的 IP 地址进行会话详情查询，支持封锁异常会话信息，并支持设置监听具体 IP 的会话记录；

12、★支持木马远控类、恶意链接类、移动安全类、异常流量类僵尸网络行为的检测；（需提供相关功能截图证明）

13、★支持蜜罐功能，即恶意域名重定向至蜜罐 IP 地址，监听对蜜罐地址的访问，用于 DNS 代理服务器场景下定位内网感染僵尸网络病毒的真实主机 IP 地址；（需提供相关功能截图证明）

14、★支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析,展示和外部命令控制服务器的交互行为和其他可疑行为；（需提供相关功能截图证明）

品目 1-2 运维安全管理系统

1、软硬一体化机架式设备，至少提供 6 个电口，可管理资源数≥50 个，支持 licence 扩容

2、支持 windows 系统、linux/unix 系统、网络设备，支持 KVM、Vmware、数据库、http/https 等类型

3、★支持 Windows AD 域账号与堡垒主机账号周期比对，自动或手动删除或锁定失效的域账号（提供截图）

4、同时支持本地口令认证、LDAP 认证、AD 认证、短信认证、Radius、usbkey、动态口令认证

5、★支持定期变更目标设备真实口令，支持自定义口令变更周期和口令强度。口令变更方式至少支持手动指定固定口令、通过密码表生成口令、依照设备挂载的口令策略生成随机口令、依照密码策略生成同一口令等方式（提供截图）

6、支持访问控制，支持用户访问时间策略、资源访问时间策略、用户 IP 地址策略

7、★能够对访问进行审批，支持自定义多级审批流程，可设置一级或多级审批人，每级审批流程可以指定通过投票数（提供截图），用户访问关键设备需相关审批人逐级审批通过才允许访问

8、支持基于单条操作命令或命令组设置行为规则，当运维人员输入违规命令时（包括通过 table 键、上下键、复制等方式）自动进行告警或阻断

9、支持云端快速部署，实现远程运维管理的规范化；可按照运维人员数量，调整云端服务器配置，即可实现性能优化。

10、支持紧急运维流程，当运维人员需对目标设备进行紧急运维时，可通过紧急运维流程直接访问目标设备，同时记录为紧急运维工单，便于相关审批人事后对该流程进行确认以及审计员事后查看

11、支持自定义报表，可记录审计报表模板，可生成图形报表，并提供 EXCAL、CSV、WORD、PDF、HTML 等格式导出

12、★具有日志防溢出功能，当磁盘空间达到阈值时，可设置停止记录审计日志或日志回滚（提供截图）

13、全面支持 Windows、linux、国产麒麟系统、Android、IOS、Mac OS 等客户端。

14、★需支持 HA，配置信息实时同步，配置过程在 web 界面完成（提供截图）

15、支持对常见设备运维操作进行记录（至少包括 windows 主机、linux/unix 主机、网络设备等），审计信息至少包括以下内容：用户账户、起止时间、登陆 IP、设备 IP、设备名称、设备类型、访问账号、访问协议等信息

16、★为了方便维护和配置，应支持手动和自动定期备份配置信息，支持配置信息本地备份及异地 FTP 备份（提供截图）

17、支持 NTP 系统时间同步配置，保证审计日志拥有可靠的时间戳，支持告警对外转发，转发方式支持 syslog、SNMP 等方式

18、★支持运维审计自查询功能，用户可查看自身的运维审计历史（提供截图）

品目 1-3 日志审计

1、1U 标准机架设备，6 个 1000M 电口，1 个扩展槽，2 个 USB 口，1 个 COM 口；1T 硬盘；性能参数：日志处理能力≥3000 EPS；日志容量：6 亿条；支持资源数：60 个。

2、基于大数据分析构架，具备高效性、实时性、灵活性和扩展性；通过 web 方式对本系统实现管理，支持 SSL 加密模式传输。

3、支持市面主流安全设备、网络设备、中间件、服务器、数据库、操作系统等设备对象的日志数据采集；支持主动、被动相结合的数据采集方式，支持日志转发；支持 Syslog、SNMP、JDBC、WMI、FTP、文件等进行数据采集；支持通过 Agent 采集日志数据；

4、★采集 Agent 至少支持采集日志监控、文件监控、主机网络流量监控数据，支持在 Agent 上控制采集时间、过滤级别（提供界面截图）；

5、★支持采集网络流量，解析协议不少于 ICMP、AMQP、Cassandra、DNS、HTTP、Memcache、MySQL、PgSQL、TNS、Redis、Thrift、MongoDB、NFS、TDS、Sybase、Drda、Dameng、POP、SMTP；（提供界面截图）；

6、支持日志数据采集实时展示；支持实时显示日志采集速度，无需人工统计；

7、★支持日志的数据的冷热模式切换，即基于时间索引的及时关闭和开启索引；（提供界面截图）；

8、★系统内置不少于 50 种常见安全事件关联分析规则；提供可视化关联分析规则编辑视图，可根据实际业务编辑关联分析规则（提供界面截图）。

9、支持自动生成主机访问关系图谱。关系图谱支持无限级延伸，支持点击业务主机节点自动绘制访问关系；支持关系图谱搜索、过滤，支持自定义关系节点图标、支持基于节点下钻查看日志信息、查看和拓展该点关系图等。

10、支持以世界地图和中国地图显示 IP 连接信息，显示 IP 地址地理位置，直观发现敏感外联日志；

11、支持在告警信息页面，以环形图形式对告警类型进行统计；

12、支持根据时间范围、级别、规则类型、告警全文关键字等方式快速检索安全事件告警，检索结果支持 Excel 等格式导出。支持邮件、声音、syslog 等多种告警方式，支持在全局显示告警提醒；可以针对不同类型、不同种类以及不同安全级别的安全事件制定不同的告警方式。

13、提供符合等级保护、SOX、ISO27001、PCI 相关要求的报表数据，支持自定义报表；支持 PDF、Word、HTML 等方式导出报表。支持生成周期定时报表，可选统一报表不同生成时间预览和下载；

14、支持实时日志查看，默认提供近 15 分钟日志信息；支持搜索条件保存、读取和删除；

15、支持全文检索、短语检索、字段值精确查询、通配符检索、正则表达式检索高量显示。支持过滤条件不少于以下条件类型：设备 IP、来源 IP、目的 MAC、来源端口、目的端口、目的地址 IPV6、源 MAC、源地址 IPV6、操作用户、目的 IP、事件名称、域名、事件级别、应用名称、请求信息、服务名称、错误信息、响应信息、资源类型、错误码、接收字节、数据库表名、状态码、协议、发送字节、请求方式等。

16、★支持在资产列表页面，以环形图、饼状图形式对资产分组和类型进行统计，显示日志源资产的日志数量（提供界面截图）；

第三部分 报价文件格式

项目名称：福建建筑学校网络安全设备采购项目

报 价 文 件

报价单位:_____（盖单位公章）

日期：2020 年　月　日

一、报价函

致：福建建筑学校：

1．根据已收到的福建建筑学校网络安全设备采购项目询价文件，经研究，我方愿以　　（大写人民币　）的总价并按上述要求承包该项目服务工作。

2．我方已详细审查全部询价文件以及全部参考资料和有关附件。我方完全理解并同意放弃对这方面有不明及误解的权利。我方将接受并遵守询价文件所规定的各项条款。

3．除非另外达成协议并生效，你方的询价成功通知书和本报价文件将构成约束我们双方的合同组成部分。

报价方名称：　　金额单位：人民币元

货品名称	询价报价(单位元)	服务期限	备注
福建建筑学校网络安全设备采购项目			

报价单位：　（盖单位公章）

法定代表人：　　（签字或盖章）或其委托代理人：　　（签字）

二、分项报价表

报价方名称：　　金额单位：人民币元

品目号	采购标的	规格型号	来源地	单价（现场）	数量	总价（现场）	备注

报价单位：_____（盖单位公章）

日期：　　年　　月　　日

三、法定代表人身份证明书或授权委托书

（一） 法定代表人身份证明书

法定代表人身份证明书

单位名称：_____

地址：_____

姓名：____性别：_____年龄：_____职务：_____

系_____（单位名称）的法定代表人。

身份证号码：

特此证明

报价单位：_____（盖单位公章）

日期： 年 月 日

（二）授权委托书

本授权委托书声明：_____法定代表人现授权委托 _____为我单位的委托代理人，以 报价方 的名义参加 福建建筑学校（询价方） 的福建建筑学校网络安全设备采购项目 工程的询价活动。代理人在询价、开标、评标、合同谈判、签署合同过程中所签署的一切文件和处理与之有关的一切事务，我均予以承认。

代理人无转委权。特此委托。

代理人：_____性别：

身份证号：_____ 。

报价单位：（单位名称）

法定代表人：_____（签字或盖章）

被授权委托代理人：_____（签字）

日期：2020 年 月 日

四、资格证明材料

（一）营业执照（副本复印件）

报价方应提交营业执照（副本复印件）等资质文件，以上证件的复印件须加盖报价方单位公章。

（二）报价方需提供的资质证明文件

按询价文件要求报价方需提供资质证明文件，并加盖报价方单位公章。

五、技术偏离表