网络流量安全监测分析设备租赁服务
采购比选方案

一、比选人资质要求

*1、比选人应为在中华人民共和国境内依法成立，法律上和财务上独立的法人或依法登记注册的其他组织，具备有效的营业执照，并提供有效的营业执照副本复印件（加盖公章）；

2、提供法定代表人身份证复印件（加盖公章）；

3、本项目不接受联合体比选；

4、比选人不得存在下列情形之一：

（1）被责令停业的；

（2）被暂停或取消参选资格的；

（3）财产被接管或冻结的；

（4）在最近三年内有骗取中标或严重违约或服务质量出现重大问题的；

以上资质带“*”的条款为必须满足项

二、比选要求

（一）比选概况与范围

1、项目名称：网络流量安全监测分析设备租赁服务采购

2、项目范围：本项目主要是我公司租赁 1 台网络流量安全监测分析设备，设备主要功能是能够对流量进行全量还

原、存储与深度分析，及时发现攻击行为，获取攻击信息等。

2、租赁期限：自合同签订后设备调试完成之日起3年。

（二）租赁设备的功能要求

本次项目提供设备租赁服务需支持以下功能：

1、流量采集支持多种协议

网络协议：支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：http、dns、smtp、pop3、imap、webmail、DB2、Oracle、MySQL、sql server、Sybase、SMB、FTP、SNMP、telnet、nfs等；

文件协议：支持对流量中出现文件传输行为进行发现和还原，并记录文件MD5发送至分析设备，如可执行文件(EXE、DLL、OCX、SYS、COM、apk等)、压缩格式文件（RAR、ZIP、GZ、7Z等)、文档类型文件（word、excel、pdf、rtf、ppt等)；

自定义协议：支持自定义协议和端口，满足特殊场景下的流量抓取。

2、威胁检测能力

Web攻击检测：支持检测针对WEB应用的攻击，如SQL注入、XSS、系统配置等注入型攻击；

Webshell攻击检测：支持基于工具特征的WEBSHELL检测，能通过系统调用、系统配置、文件的操作来及时发现威胁；如：中国菜刀、小马上传工具、小马生成器等；

网络攻击检测：支持多种攻击检测，能更全面的从流量中发现威胁，如：协议异常、网络欺骗、黑市攻击、代码执行等。

3、策略配置要求

文件还原：支持对 HTTP、FTP_DATA、SMB、SMTP、POP3、WEBMAIL、IMAP、TFTP、QQ、NFS 等类型协议的流量进行文件还原；

语义分析：支持基于网络请求的语义分析检测，能够将网络请求拆分后从请求头、响应头、请求体、响应体四方面详细展示请求内容，并能提升对未知威胁检测能力；

旁路阻断：支持基于 IP 地址的旁路阻断，能够在实时镜像的流量中发现恶意 IP 并实现实时阻断；

自定义弱口令：支持自定义弱口令字典，支持 HTTP、HTTPS、Telnet、FTP、POP、SMTP、IMAP 等协议的自定义弱口令检测。

（三）比选文件要求

1、比选文件递交时间：自 2022 年 5 月 27 日至 2022 年 5 月 30 日止。

2、比选文件递交地点：河北省石家庄市新华区联盟路 699 号信投集团 2 层。

3、比选文件要求：比选文件需密封（加盖公章），一式三份。

4、比选要求：最高限价24万元，超过最高限价投标无效。

5、联系人及电话：王清 0311-86950230。

三、评分标准

本次项目的比选工作按以下标准进行评分。

评审内容	评审标准
参选报价（80分）	以所有有效报价的最低报价为评标基准价。有效报价最低者得满分，有效报价每高于评标基准价一个百分点的扣0.5分,扣完为止。
租赁设备的功能（10分）	1. 租赁设备的功能全部满足或优于本方案中比选要求中规定的所需支持的功能：得10.0分。 2. 租赁设备的功能仅部分满足本方案中比选要求中规定的所需支持的功能：得0分。
项目实施与培训（10分）	按照项目实施的时间、人员、培训安排的优劣进行分档打分，培训内容包括设备安装、使用等培训： 第一档，实施时间、人员和培训计划及培训内容方面安排合理可行，得7.1~10.0分； 第二档，实施时间、人员和培训计划及培训内容方面安排合理可行，但有不足之处，得4.1~7.0分； 第三档，实施时间、人员和培训计划及培训内容方面安排有缺陷，得0~4.0分。