**重庆西南铝医院**

**网络安全态势感知APT攻击预警平台邀标通知**

**项目名称: 网络安全态势感知APT攻击预警平台采购**

**项目联系人:王先生**

**项目联系电话:023-68823616**

**招标单位联系方式**

**招标单位:重庆西南铝医院**

**地址:重庆市九龙坡区西彭镇西华路15号**

**联系方式:023-65808299**

**纳税人识别号:125000007562427558**

**开户行:中国工商银行重庆西彭支行**

**账号:3100082209024901630**

# 一、项目的名称、数量、简要规格描述或项目基本概况介绍

(一)本项目名称网络安全态势感知攻击预警平台建设项目。预算金额为20万。

(二)本项目需要实现对我单位的内外网的安全攻击预警及追溯，能够及时发现攻击威胁和异常。全方位的提高我单位应对网络攻击和溯源的能力。

 （三）本项目由重庆西南铝医院提供资金。

 （四）本项目要求开工后20日内完成。

 (五) 本项目具体资料见附件

二、投标人的资格要求

投标人须满足下列要求：

1、具有独立承担民事责任的能力，资信良好，无不良行为记录；

2、具有履行合同所必需的设备和专业技术能力；

3、投标人需在重庆市设有正式服务机构并具有本地售后服务人员，需提供工商行政主管部门颁发的注册证明和近3个月的本地社保缴纳证明。（提供加盖投标人鲜章的复印件，原件备查）；

4、投标人具备中国信息安全测评中心颁发的《信息安全服务资质证书》。（提供加盖投标人鲜章的复印件，原件备查）；

5、法律、行政法规规定的其他条件；

6、本次邀标所有资格审查，技术参数符合性审查均为开标前置审查，审查符合后方可报名，缴纳保证金。

三、招标文件的发售时间及地点

2021年11月29日起免费到重庆西南铝医院信息科领取或索取电子版资料。

四、投标截止时间：2021年12月03日18时。

五、投标保证金

 本项目投标保证金4000元人民币。可以现金缴纳或打入医院指定账号。开标结束确定中标单位后，10个工作日内将未中标人保证金打入投标方开户银行账户。中标人投标保证金可直接转入履约保证金。

 缴纳投标保证金起止日期：2021年11月29日-2021年12月03日

六、开标时间：2021年12月 6日 下午15时。

七、开标地点：重庆西南铝医院。

八、其他补充事宜

(一)投标文件须全部盖章,并包括以下内容:

1.投标函；

2.承诺书；

3.单位营业执照副本；

4.银行开户许可证复印件；

5.法定代表人身份证明；

6.投标人身份证复印件；

7.授权委托书(非法定代表人投标的)；

8.简化费用清单(见附件7)；

9.商务承诺(见附件8)。

本项目质保期按照国家标准与规范,并承担相应责任。

(二)提供投标文件的方式、地点

（1）书面提交:每个文件都盖章后装入大牛皮纸信。

封,密封后加盖公章,信封上留下联系人姓名及联系电话。

（2）接受投标地点：重庆西南铝医院

**网络安全态势感知APT预警攻击平台一套**

**技术要求：**

|  |  |  |
| --- | --- | --- |
| **规格性能** | 软硬一体化1U标准机架式设备，单电源，可用磁盘空间不小于2T， 6个以上10/100/1000M以太网端口。文件检测能力≥1万个/24小时。 | 推荐品牌：深信服、安恒、启明星辰、奇安信、H3C、华为 |
| **部署方式** | 支持旁路部署和分布式部署，旁路镜像模式部署不影响服务器处理性能和网络架构。 |  |
| **IPv6支持** | 支持IPv4和IPv6网络环境下的部署，可同时对IPv4和IPv6网络流量分析检测。 |  |
| **审计协议** | 支持解析HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、HTTPS、SMTPS、POP3S、IMAPS、RADIUS、KRB5、SNMP、NETFLOW V9等协议报文，并提供审计协议类型的端口号配置，可根据需要变更端口号。 |  |
| **检测风险类别** | 支持检测WEB攻击、恶意文件攻击、远程控制、WEB后门访问、行为分析、DGA域名请求、SMB远程溢出攻击、弱口令、拒绝服务攻击、隧道通信、暴力破解、挖矿、恶意工具利用、扫描行为、漏洞利用、邮件社工攻击、ARP欺骗、密码明文形式传输等行为。（提供web界面功能截图并加盖供应商公章） |  |
| **告警黑白名单过滤** | 支持文件白名单、发件人邮箱白名单、发件人域名白名单、黑域名白名单、黑IP白名单、域名白名单、客户端IP白名单、服务端IP白名单、WEB特征风险白名单、IDS规则白名单的配置。 |  |
| **弱口令风险检测** | 支持对HTTP、IMAP、SMTP、POP3、Redis、Telnet、FTP等协议的弱口令检测。 |  |
| **暴力破解检测** | 支持HTTP、SMB、SMTP、IMAP、POP3、FTP、TELNET、RADMIN、SSH、RDP、ORACLE、MSSQL、SYBASE、MYSQL、DB2、PGSQL、LDAP等协议的暴力破解，能识别出尝试登录次数、账户信息、爆破成功与否的攻击状态。 |  |
| **拒绝服务攻击检测** | 支持UDP FLOOD、DNS FLOOD、NTP FLOOD、Chargen FLOOD、SNMP FLOOD、SSDP FLOOD、 Memcached FLOOD、SYN FLOOD、RST FLOOD、FIN FLOOD、ACK FLOOD、HTTP FLOOD、ICMP FLOOD、SEANET\_FLOOD检测。 |  |
| **主机威胁分析** | 支持对内网主机进行主机威胁分析，详细展示具体的威胁等级、威胁次数、攻击开始时间、攻击结束时间、威胁性指数统计等；可按攻击链阶段（弱点探测、渗透入侵、获取权限、命令与控制、数据盗取）详细展示主机相关事件数量。（提供web界面功能截图并加盖供应商公章） |  |
| **威胁情报检索** | 支持对IP、域名、恶意文件SHA256进行威胁情报检索，或跳转第三方链接（Whois、VirusTotal）进行检索。 |  |
| **Web攻击检测** | 支持SQL注入、命令注入、跨站脚本、代码注入、WEB扫描或爬虫、网页篡改、服务错误攻击检测（提供web界面功能截图并加盖供应商公章） |  |
| **Mail攻击检测** | 支持解析webmail、SMTP、POP3、IMAP、SMTPS、POP3S、IMAPS（加密协议需要导入服务器私钥证书）类型报文。（提供web界面功能截图并加盖供应商公章） |  |
| **文件攻击检测** | 支持 HTTP、FTP、SMB、SMTP、POP3、IMAP、NFS、TFTP、HTTPS、SMTPS、POP3S、IMAPS等协议传输文件检测；支持doc, xls, ppt, swf, pdf, rar, zip, rar, exe, vbs, scr、ps1、elf等多种文件解析。 |  |
| **动态沙箱检测** | 支持动态执行可疑文件，分析代码的注册表、进程、网络、文件等行为，分析其安全风险；可展示具体文件的行为，包括所有的注册表行为、进程行为、互斥量、返回结果、返回值等信息。（提供web界面功能截图并加盖供应商公章） |  |
| **威胁情报** | 设备集成离线的高可用威胁情报库，支持离线环境下，根据威胁情报进行检测，增量威胁情报随策略升级包升级支持在告警详情页面直接查询与告警IP、域名相关的威胁情报，获取样本通信记录、情报画像等信息 |  |
| **一键登录排错** | 支持一键登录排错平台，对系统进行深度配置和排错，支持一键检测故障、配置核对、表分区检查、表检测、信息收集等功能。（提供web界面功能截图并加盖供应商公章） |  |
| **可视化展示** | 支持大屏展示网络攻击态势，包括攻击地图、紧急事件数/总数、恶意文件数/扫描总数、风险趋势（高、中、低风险）、流量分析（吞吐量、HTTP流量、DNS流量）、高危风险类别排名、攻击源区域排名、紧急事件/高危事件，并支持全球地图、中国地图切换展示。支持大屏展示风险较为严重的事件，并进行攻击溯源，包括攻击主机个数最多的情报事件TOP10、威胁情报告警类型分布、3D攻击关系图、包括攻击拓扑图、攻击者基本信息、被攻击者信息、攻击过程 |  |
| **告警与报表** | 支持kafka、短信、邮件、syslog、ftp、sftp、钉钉等数据外送方式（提供web界面功能截图并加盖供应商公章）支持在线预览报表，以及WORD、PDF、HTML等格式导出 |  |
| **资质要求** | 产品需具备公安部颁发的《计算机信息系统安全专用产品销售许可证（APT安全监测类产品）》 |  |

**投标须知**

一、投标人须知

（一）投标人资质要求

 投标人须满足下列要求：

1、具有独立承担民事责任的能力，资信良好，无不良行为记录；

2、具有履行合同所必需的设备和专业技术能力；

3、投标人需在重庆市设有正式服务机构并具有本地售后服务人员，需提供工商行政主管部门颁发的注册证明和近3个月的本地社保缴纳证明；（提供加盖投标人鲜章的复印件，原件备查）

4、投标人具备中国信息安全测评中心颁发的《信息安全服务资质证书》；（提供加盖投标人鲜章的复印件，原件备查）

5、法律、行政法规规定的其他条件；

6、本次邀标所有资格审查，技术参数符合性审查均为开标前置审查，审查符合后方可报名，缴纳保证金。

(二)投标文件须全部盖章,并包括以下内容:

1.投标函；

2.承诺书；

3.单位营业执照副本；

4.银行开户许可证复印件；

5.法定代表人身份证明；

6.投标人身份证复印件；

7.授权委托书(非法定代表人投标的)；

8.商务承诺(见附件)。

本项目质保期按照国家标准与规范,并承担相应责任。

(三)提供投标文件的方式、地点和起止日期

（1）书面提交:每个文件都盖章后装入大牛皮纸信。

封,密封后加盖公章,信封上留下联系人姓名及联系电话。

（2）医院通知开标现场提交标书。

### 二、招标项目的基本情况

(一)本项目名称网络安全态势感知攻击预警平台建设项目。预算金额为20万。

(二)本项目需要实现对我单位的内外网的安全攻击预警及追溯，能够及时发现攻击威胁和异常。全方位的提高我单位应对网络攻击和溯源的能力。

 （三）本项目由重庆西南铝医院提供资金。

 （四）本项目要求开工后20日内完成。

 (五) 本项目具体资料见附件

### 三、交货或项目实施地点:重庆西南铝医院。

### 四、交货或项目实施时间:发送中标通知后20个工作日内。

### 五、评标的方法标准

综合排序评分法,得分最高的推荐作为第一中标单位,得分次高的,推荐作为第二中标单位。

### 六、日程安排

(一)开标时间:2021年12月 06 日

地点：重庆西南铝医院门诊409会议室

(二)发放中标通知书

### 七、主要合同条款

（一）项目地点:重庆西南铝医院。

(二)质量保证及售后服务

本项目网络安全产品质量保证期为2年。

(三)标的物价款结算及付款方式

签订合同后预付设备定金40%（需开具40%发票），设备到达医院并调试完成合格后付款50%（需开具60%发票）。质保期结束后付款10%。

（四）本邀标公告由医院负责解释。

附件1、投标承诺书

**投标承诺书**

国药重庆西南铝医院：

我方已仔细研究 邀标文书的全部内容,经自行踏勘现场和研究竞标文件的内容、工程建设标准,并通过你方下属项目部等相关部门,充分了解了该工程的实际施工组织情况及参建各方的情况。我方完全理解招标文书的意思并全部接受其中的所有条件,愿意按招标文件要求,并按贵方要求组织提供材料。

2、一旦我方中标,我方保证在招标文书规定的时间内完成投标文件的全部要求

(1)我方承诺在收到中标通知后,在规定的期限内与你方签订合同

(2)我方承诺在合同约定的期限内保质保量组织供应材料并施

3.我方在此声明,所递交的投标文件及有关资料內容完整、真实和准确

XXX公司

年 月 日

## 附件2、法人代表授权委托书

**法人代表授权委托书**

国药重庆西南铝医院：

我方特授权\_\_\_\_\_\_\_\_\_\_ (身份证号码)\_\_\_\_\_\_\_\_\_\_\_\_\_为我公司全权代表,以我公司名义全权办理与医院有关的一切事宜,我公司对被授权人签署的所有文件和提供的相关资料承担全部责任。

法定代表人

被授权人签字:

XXX公司

年 月 日

## 附件3、商务承诺（包括但不限于）：

1、质保期；

2、售后服务能力情况；

3、履约能力证明文件；

4、售后服务承诺（格式自定）。