周口文理职业学院采购防翻墙安全检测系统项目采购内容、服务要求及参数

2U 标准机架设备，≥2*10 核 CPU，≥128GB 内存，≥240GB SSD，≥3*4TB 数据盘，≥4 个硬盘扩展槽位，硬件 RAID 卡，≥2 个千兆电口，≥2 个万兆光口，≥4 个接口扩展槽位，双冗余电源。处理流量≥2Gbps。

包含三年硬件维保，三年特征库升级服务。

横向威胁态势：监控内部资产之间的威胁态势，发现内部威胁源及影响的范围（需提供截图证明）

下一代入侵检测：内置 IDS 规则库和 Yara 规则库，IDS 规则库规模在 4 万以上，Yara 规则库规模在 8000 以上（需提供截图证明）；支持以下攻击检测：SQL 注入、XSS 注入、跨站请求伪造、webshell 上传、文件包含漏洞、远程代码执行漏洞、Web 溢出攻击、Web 目录遍历攻击、文件上传攻击、文件写入攻击、文件下载攻击、网络欺诈、Web 敏感文件访问、CVE 漏洞、微软漏洞、IE 漏洞利用、weblogic 漏洞利用、Struts 漏洞利用、Office 漏洞利用、Flash 漏洞利用、漏洞利用工具、信息泄露、Shellcode、后门程序、挖矿木马、间谍软件、银行木马、窃密木马、蠕虫病毒、恶意软件命令与控制、metasploit 工具利用、下载者木马、Powershell 工具利用、远控木马、流量劫持、CobalStrike 工具利用、移动恶意软件、恶意用户代理、ICMP Flood 攻击、DNS Flood 攻击、TCP Flood 攻击、UDP

Flood 攻击、HTTP Flood 攻击、拒绝服务攻击、恶意域名查询、异常证书访问、勒索软件、网络钓鱼、web 扫描、僵尸网络、远控工具识别、渗透工具识别、潜在恶意流量、潜在信息泄露、尝试获取用户权限、获取用户权限失败、成功获取用户权限、尝试获取管理员权限、管理员权限提权成功、RPC 查询解码、可疑文件名、可疑用户登录、特洛伊木马通信、混杂异常行为、混杂攻击模式、潜在隐私策略违反、尝试默认账号登录

隐蔽隧道检测：支持 DNS 隐蔽隧道通信检测：基于隧道工具的 DNS 隐蔽隧道；DNS 直连隧道；APT32 利用 DNS 隧道通信；基于 DNS 隐蔽隧道关联分析发现受控主机（需提供截图证明）；支持 ICMP 隐蔽隧道通信检测：利用 ICMP 隧道违规突破内网 web 访问；利用 ICMP 隧道传输数据；利用 ICMP 隧道进行远程控制（需提供截图证明）；支持 HTTP 隐蔽隧道通信检测：常用的 HTTP 隧道工具的识别（reDuh，CobaltStrike、Firepass、Tunna）；APT 利用 HTTP 隧道通信;（需提供截图证明）

加密流量检测：支持恶意加密流量检测：基于 JA3/JA3S/SSL 证书恶意指纹识别恶意加密流量检测，指纹规则库在 3000 条以上；利用机器学习方法检测恶意加密流量并与恶意指纹交叉验证（需提供截图证明）;

翻墙检测：支持 Shadowsocks 翻墙代理检测，基于机器学习方法检测 Shadowsocks 翻墙代理通信；支持 VPN 代理检测：基于机器学习方法检测 VPN 流量；基于流量特征方

法检测 VPN 流量。支持暗网（Tor）通信检测，基于机器学习方法检测暗网流量并与威胁情报、特征检测交叉验证;

智能模型检测：支持基于智能模型（人工智能模型）检测 DGA 域名；支持基于智能模型（人工智能模型）检测恶意代码加密外联通信流量；支持基于智能模型（人工智能模型）检测网络内暗网 Tor 流量；支持基于智能模型（人工智能模型）检测 DNS 隐秘隧道通信；支持基于智能模型（人工智能模型）检测 ICMP 隐秘隧道通信；支持基于智能模型（人工智能模型）检测 HTTP 隐秘隧道通信；支持基于智能模型（人工智能模型）检测 shadowsocks 代理流量；支持基于智能模型（人工智能模型）检测 VPN 加密流量；支持基于智能模型（人工智能模型）检测 Webshell;支持基于智能模型（人工智能模型）检测 SQL 注入；支持基于智能模型（人工智能模型）检测 XSS 注入；支持基于智能模型（人工智能模型）检测目录遍历攻击（需提供截图证明）

沙箱检测:支持沙箱行为签名检测，根据主机或网络行为判断其是否为恶意文件，支持显示沙箱内样本运行截图;支持多种沙箱运行模式，支持 windows、android 和 linux 类型沙箱，支持限制从流量中还原的可以进入沙箱的文件大小，内置沙箱数量不少于 10 个。;支持对沙箱内样本的流量进行检测、支持反虚拟机和反调试行为检

全流量协议元数据解析及存储:支持网络流量协议元数据提取、解析、存储和检索展示，支持的协议应包括 tcp、

icmp、dhcp、dns、ftp、http、krb、mysql、pop3、rdp、smb、smtp、imap、ssh、ssl、postgresql、oracle、mssql、IEC60870-5-104、IEC61850-MMS、IEC61850-GOOSE、IEC61850-SV、udp、ldap、nntp、telnet、rlogin、tacacs、cvs等。(需提供截图证明)

为保证交付质量，实施工程师需同时具备中国信息安全测评中心颁发的注册数据安全治理专业人员认证（CISP-DSG)、注册信息安全管理人员认证（CISP-CISO）和信息安全保障人员认证（CISAW）

为保证用户后续流量原数据能力扩展与定制开发，需提供产品流量分析模块源代码，厂家出具源代码承诺函并加盖公章。

产品具备网络安全专用产品安全检测证书，产品类型为防病毒网关 网络病毒监控系统。

产品需具备软件著作权。