《武汉科技大学网络安全建设项目》

需求及价格调查说明

学校拟建设《武汉科技大学网络安全建设项目》，现面向社会进行项目需求及价格调查，具体内容说明如下:

一、 项目名称及编号

- 项目名称：武汉科技大学网络安全建设项目
- 项目编号：2023-XXZX-01
- 项目地点：青山校区

二、 项目基本内容

随着我校信息化水平的发展，对网络信息安全的需求增加，拟采购数据中心防火墙 1 台、WEB 应用防火墙 1 台、日志审计 1 套、态势感知 1 台、漏洞扫描 1 台、网管软件 1 套、网络资产安全治理平台 1 台、数据中心安全软件 1 套。

三、 相关技术要求及现状说明

1. 数据中心防火墙

功能需求：用于学校数据中心出口，提供威胁检测、攻击防护、入侵防御、病毒防护以及僵尸网络防御等能力，实现针对数据中心网络 L2-L7 层的安全防

护。需支持与现有数据中心防火墙设备实现 HA，保障业务的高可用性。

主要参数：标准机架式硬件设备，支持 IPv4/IPv6 协议双栈，SFP 千兆光口≥8 个，万兆 SFP+接口≥6 个，≥2TB SATA SSD 硬盘；吞吐量≥20Gbps，最大并发连接数≥1000 万，每秒新建连接数≥31 万，ipsec 吞吐量≥12Gbps，IPS 吞吐量≥17.5Gbps，防病毒吞吐量≥9.4Gbps；提供原厂五年质保服务，日志必须支持本地保存 180 天以上。

2.WEB 应用防火墙

功能需求：用于数据中心 WEB 应用业务的安全防护，支持基于规则和语义分析的检测引擎，支持可配置的内置规则；支持非法文件上传防护，有效识别文件上传行为，并对上传行为的内容做安全检测；支持站点网页防篡改功能，至少可授权接入 80 个站点数进行防护；支持 HTTPS 国密算法和 SSL 证书卸载；支持旁路镜像、透明代理、透明桥、路由代理和反向代理部署。

主要参数：标准机架式硬件设备，交流冗余电源模块；≥1 个 RJ45 串口，≥2 个 USB 口，≥6 个千兆电口，≥4 个千兆光口插槽，≥2 个接口扩展槽，硬盘≥1TB，网络层吞吐量≥6Gbps，应用层吞吐≥

3Gbps，最大并发连接数≥200 万，事务处理能力≥60000TPS，支持 IPv4/IPv6 协议双栈，提供原厂五年质保服务，日志必须支持本地保存 180 天以上。

3. 日志审计

功能需求：全面收集学校 IT 系统中的安全设备、网络设备、数据库、服务器（含虚拟机）、应用系统等所产生的日志并进行存储、监控、审计、分析、报警、响应和报告。支持多种数据采集方式，能接入市场主流硬件品牌、操作系统和软件系统等的日志，可对重复日志自动聚合归并；包含常用的日志管理功能，具备日志转发、备份恢复、日志检索、事件告警、资产监控等功能，能为安全事件的事后分析、调查取证提供追踪溯源信息。

主要参数：支持 IPv4/IPv6 协议双栈；存储容量≥8TB，授权接入≥500 个日志源，可购买授权扩展，最大可扩展授权≥1000 个日志源，日志支持本地存储时间≥六个月。系统支持单节点部署、分布式多节点部署和分级部署模式。单台设备综合日志处理性能≥6 万 EPS，分布式≥10 万 EPS 以上。

4. 态势感知

功能需求：结合云端威胁情报，对全网流量进行多维度安全分析，精准威胁溯源取证，全网安全风险

呈现，使用户能够快速准确地掌握网络当前的安全态势，并进行联动响应闭环处置。产品具备可视化呈现、威胁情报、关联分析、威胁检测、攻击溯源等功能，对多种异构安全源数据采集、接入、分析，对不同场景下的威胁事件，编排的特定响应流程，实现自动/半自动闭环响应。具备与其他网络安全产品联动和一键下发控制命令功能，通过持续性的监控和分析，构建预测、发现、检测、持续响应的安全能力。

主要参数：支持 IPv4/IPv6 协议双栈；标准机架设备，含滑轨；CPU≥2 颗 12 核 主频 2.2 GHZ；内存≥128G（总容量）DDR4；总容量≥32T；电源：冗余双电源；网口≥4*GE 管理电口、≥2*SPF+插槽。配置吞吐量不低于 10G 的 1 个和 1G 的 2 个的风险感知探针。

5. 漏洞扫描

功能需求：针对学校的信息系统（包括操作系统、WEB、数据库和应用系统等）进行漏洞扫描，同时支持 Web 和主机服务扫描，及时发现安全漏洞，扫描结果（资产、漏洞）能够实现联动；针对 0day 漏洞，可生成特定扫描策略，快速定位并进行风险监测；支持资产信息批量导入。

主要参数：支持 IPv4/IPv6 协议双栈；标准机架设备，标配 4 个千兆电口业务，1 个 RJ45 串口,2 个 GE 管理口，1 个网卡接口扩展槽位,可购买千兆或万兆链路扩展板卡进行接口扩展，≥1T 硬盘；单节点性能：主机扫描单节点最大并发端口数≥200，Web 扫描最大并发连接数≥1000。

6. 网管软件

功能需求：对校园网上所有链路、网络设备、主机等的运行状况和流量进行监测和远程管理，发现问题及时报警，监测记录至少保存六个月。

主要参数：

- 支持多种 IT 资源的管理，实现对交换机、路由器、防火墙、WLAN、服务器、存储、PON、 应用、虚拟机、业务、UPS、空调等对象的监控；
- 提供有线网络设备监控授权≥100 个，服务器管理授权≥50 个；
- 提供统一集中展示网络拓扑、业务拓扑及各类 IT 资源的关键指标数据；
- 提供灵活自定义告警策略，可通过邮件、短信、微信，语音将告警及时发送给指定接收人；

- 支持与业务相关的资源以业务拓扑方式直观呈现，清晰展现各层 IT 资源的结构脉络；
- 支持 IPv4/IPv6 协议双栈。

7. 网络资产安全治理平台

功能需求：对全网网络资产进行全生命周期管理，包括统一备案、上线安全检查、资产安全监控等，支持 Web/IP 资产自动获取，并对自学习资产进行自动分类，包括 web 资产、交换路由设备、IoT 设备资产、数据库资产、邮件服务资产、其他资产；具备指纹学习、资产管理、备案管理、脆弱性监测、威胁情报分析、一键阻断和报表管理等功能。

主要参数：标准机架设备，双电源，≥1T 硬盘，千兆电口≥2 个，万兆光口≥2 个，支持网络接口扩展，IP 资产管理授权≥500 个、WEB 资产≥500 个，处理能力≥5G；支持 IPv4/IPv6 协议双栈。

8. 数据中心安全软件

功能描述：解决数据中心机房内部安全威胁，对物理服务器、虚拟服务器的风险暴露面梳理、防爆破、漏洞扫描、弱口令治理、等保合规检查及修复建议、异常行为分析、防勒索/挖矿、微隔离、Webshell 防护、网页/文件/系统防篡改等安全防护，构筑服务器外防输入、内防扩散的安全屏障。

主要参数：支持 IPv4/IPv6 协议双栈，使用授权≥300 个，支持 windows/linux/国产主流操作系统。

四、 调查内容

1. 项目技术方案；

2. 项目设备清单及价格（含设备名称、数量、规格型号、参数、分项价格等，还应包括配件、线路辅材、实施和 5 年维保服务）。

五、 调查提交方式及其它

1. 请将调查内容形成《武汉科技大学网络安全项目建设方案及预算》），纸质版请加盖公章并邮寄或送至以下地址：武汉科技大学青山校区主楼 707 办公室 ，电子版请提交至邮箱 its@wust.edu.cn；

2. 联系人：邹老师，联系电话：15697180808，027-68862223；

3. 截止日期：2023 年 3 月 3 日 18 时前；

4. 提交调查文件即表示承诺不得以任何方式将本项目进行转包或分包；理解最低价格不是学校制定项目技术方案和预算的唯一条件。

武汉科技大学网络信息中心

2023 年 2 月 24 日