项目咨询公告-智能威胁防御系统(硬件)

为完善项目建设方案，提高采购预算的准确度，特对以下项目开展公开咨询。本公告发布平台为湖南生物机电职业技术学院信息中心网站。

网址：https://ic.hnbemc.edu.cn/channel/1666/index.html

有效期为三个工作日。

一、项目名称：智能威胁防御系统(硬件)

二、功能需求：详见附件 1

三、咨询报价

1.供应商提交的咨询报价将作为学院制定项目建设方案的重要依据，在满足功能需求的前提下，学院优先参考性价比高的产品和方案。**无论基于何种情况，供应商参与的本次“咨询报价”与采购过程和结果无任何关联。**

2.本项目的咨询报价建议不超过【26】万元。

四、截止日期

公开咨询响应文件（格式见附件 2）请于【2024 年 7 月 2 日】16:00 前密封提交（文件袋封口帖密封条，加盖公章，注明项目名称、联系人及电话），逾期将被拒收。不接受快递和邮件方式提交。

提交地点：湖南生物机电职业技术学院博达楼 2005。

联系人/电话：曾伍 15874907732。

发布日期：【2024 年 6 月 27 日】

附件 1：采购需求

品名	技术参数	数量	备注
智能威胁防御系统（硬件）	见附件	1 台	

附件：技术参数要求

1.硬件规格

（1）本地环境部署，提供南北向流量解析，支持资产识别与管理、实时威胁检测、持续脆弱性检查、自动化和云端联动防御能力。

（2）最大支持 5G 吞吐能力，支持 2 个千兆电口，2 个万兆光口，内存 16G，标配外置交流电源适配器。

2.流量分析

可全面覆盖各类常见网络流量协议、应用协议，支持通过获取到的流量信息，基于数据包字段内需五元组信息、协议号、报文长度、包长度等解析，也可根据协议自身行为特征和行为轨迹进行协议解析。

3.资产识别

支持基于主/被动的方式识别出用户的局域网资产。

（1）资产主动扫描：利用智能威胁网关的资产梳理模块对用户局域网资产进行主动扫描，识别出资产信息。

（2）资产被动探测：基于南北向流量的解析能力，从流量中被动识别出用户局域网网络资产信息。

（3）资产主动录入：支持资产的主动录入，用户可在平台上手动添加单个资产信息或根据平台提供的资产模板填写资产信息。

4.资产梳理

（1）基于智能威胁网关识别出资产信息，依据资产的重要程度进行自动化分组（互联网暴露资产、内网业务资产及其他资产），同时进行资产的全面梳理，梳理的维度包括资产的 IP 地址及 MAC 地址、资产开放的端口及服务、资产运行的操作系统等，将资产信息形成资产列表。

（2）通过识别梳理内网站点信息，包括站点列表、站点标题、对应公网 IP 及端口、使用的第三方组件名称、业务系统名称、站点最新访问时间。

5.资产管理

支持对资产进行管理，包括资产标签、资产等级划分等，同时平台会根据资产的在线状况、端口开放详情及对外提供服务详情等维度实时更新资产列表，当资产发生变更时，由团队对变更信息进行确认与更新。

6.弱口令检测

提供弱口令扫描功能，支持对重要资产的不同协议弱口令的检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat 等，平台提供常见弱口令库，用户也可自定义导入弱口令信息。

7.高危服务检测

提供高危服务梳理功能，支持对常见高危端口及服务的被动检测，并统计暴露在互联网上的高危服务。

8.本地化漏扫

提供本地化漏扫功能，支持包含 SQL 注入、CSRF、CRLF 注入、命令注入、XML 实体注入、SSRF、XSS、文件上传、操作系统、系统服务及数据库服务等在内的主机服务及 WEB 应用漏洞的扫描发现。

9.风险优先级排序

提供客观的风险修复优先级指导，不能以脆弱性危害等级作为唯一的风险优先级排序依据，排序依据包括资产重要性、漏洞等级、弱口令、互联网暴露高危服务以及安全事件等级等多个维度。

10.风险管理

针对风险状况，可对风险进行统一管理，查看网络环境中存在的高危端口、弱口令、漏洞及安全事件状况，及各类风险的等级分布及排名情况，也可通过风险资产 IP、风险等级进行检索，快速掌握具体资产风险情况。

11.业务系统梳理

根据梳理出的资产信息分析出单位内部所使用的业务系统详情，梳理的维度包括业务系统关联的 IP 信息、关联站点信息、业务系统中存在的弱口令、高危服务、漏洞及提供的虚拟补丁数量。

12.多源情报防御

基于多源威胁情报平台、历年护网红队 IP、云端蜜罐诱捕的攻击者 IP 等多方面情报来源实时丰富平台的威胁情报库，拦截来自威胁域名/IP 发起的攻击行为，阻断局域资产的非法外联行为。

13.扫描行为阻断

支持对常见的网络扫描工具的特征行为防御，包括资产存活扫描行为、端口扫描行为、服务扫描行为、目录扫描行为、漏洞扫描行为等，短时间触发大量告警自动阻断。

支持对常见的密码口令流量和暴破行为进行判断与防御，例如针对 WEB 应用的接口登录 N 次行为、组件默认口令检测等，短时间触发告警自动阻断。

14.漏洞无效化

支持基于 Nday 漏洞及热点 1day 漏洞的漏洞利用特征行为进行检测，例如 CVE 漏洞、QwaspTop10 漏洞、重点国产化软件漏洞、护网热点漏洞、近期更新的热点漏洞等，发现漏洞利用行为自动进行阻断，实现漏洞的无效化。

15.恶意工具及文件防御

提供漏洞利用或黑客工具执行恶意操作行为进行检测及防御，包括工具特征行为检测（红队常用工具，扫描类工具等）和远程恶意命令检测，发现攻击行为自动进行阻断。

支持针对恶意文件的检测能力，还原上传文件，同时对常见隧道攻击特征进行检测，发现恶意文件及时进行阻断。

16.超基线行为封禁

支持服务器基线学习能力，学习服务器社交行为，管控服务器超基线风险动作，建立服务器访问白名单，发现超基线行为自动进行封禁，由安全专家分析，判断该行为是正常访问行为还是恶意行为，并添加黑/白名单。

17.安全事件分析

检测发现的可疑攻击行为形成原始安全日志通过平台的关联分析规则对原始安全日志进行归并后，形成安全告警信息，基于告警信息分析研判出真实的安全事件。

18.安全策略下发

支持对处置后的安全事件编写安全防护策略发给智能威胁防御网关，提升用户的安全防御策略。

19.工单管理

（1）支持通过统一的界面查看工单服务情况，包括正在进行、已完成以及待评价的工单情况，并自主创建工单。

（2）可以针对已完成的工单详情进行查看，支持通过评星、文字描述等方式对该工单的处理情况进行评价。

20.威胁诱捕能力

可通过对各类应用系统仿真，对网络环境中存在的各类攻击者进行发现、诱捕，当检测到恶意攻击行为、爆破行为时进行及时告警，告警内容需包括攻击源、风险等级等相关纬度

21.攻击者画像测绘

支持展示捕获到的攻击者画像，画像信息需聚合攻击手段、攻击路径、攻击端口、受影响业务系统信息等维度，并对攻击活动分布进行统计

22.售后服务

（1）整机及硬件免费质保期三年。

（2）软件和产品特征库升级免费授权三年。

附件 2：公开咨询响应文件（模板）

湖南生物机电职业技术学院

信息化建设项目公开咨询响应文件

项目名称：

供应商名称：

联系人：

联系电话：

承诺：本公司已知晓本次公开咨询的目的和有关事项，完全明白本公司提交的咨询响应文件仅供学院在制定项目建设方案和采购预算时参考，无论基于何种情况均与项目采购过程和结果无任何关联。

供应商公章：

提交日期：202　年　月　日

一、项目建设方案及报价（逐页加盖公章，格式可自拟）

序号	品名	品牌型号	技术参数是否符合采购需求	数量	单位	单价(元)	金额(元)
1							
2							
3							
合计（元）							

二、供应商营业执照（加盖公章）

三、方案优势阐述（加盖公章，没有的可不提供）