景德镇学院关于“挖矿”病毒处置安全加固系统建设项目询价公告

我校需建设一套“挖矿”病毒处置安全加固系统，现就“公开、公平、公正”的原则进行询价，以更科学合理地确定项目预算，欢迎具备条件的供应商参与报价。

一、项目名称：景德镇学院“挖矿”病毒处置安全加固系统建设项目

二、项目总体需求：

（一）在各终端（主机）上安装专业杀毒软件

1、主机安全基线核查

通过对主机进行安全基线核查，可判断在身份策略，访问控制策略，安全审计策略，剩余信息保护策略，入侵防范，恶意代码防范六个方面的基线策略是否合乎要求。同时，EDR 提供 RDP 二次登录验证功能，即使黑客利用弱密码登录系统，也无法进行控制。

2、多维度的智能检测技术

基于 AI 技术的查杀引擎，利用深度学习的技术，通过对海量样本数据的学习，提炼出来的高维特征，具备有很强的泛化能力，从而可以应对更多的未知威胁。

构建了一个多维度、轻量级的漏斗型检测框架，包含文件信誉检测引擎、基因特征检测引擎、AI 技术的 SAVE 引擎、行为引擎、云查引擎等。通过层层过滤，检测更准确、更高效，资源占用消耗更低。

3、创新微隔离技术

在东西向访问关系控制上，优先对所有的服务器进行业务安全域的逻辑划域隔离，并对业务区域内的服务器提供的服务进行应用角色划分，对不同应用角色之间服务访问进行访问控制配置，减少了对物理、虚拟的服务器被攻击的机会，集中统一管理服务器的访问控制策略。并且基于安装轻量级主机 Agent 软件的访问控制，不受虚拟化平台的影响，不受物理机器和虚拟机器的影响。另一方面，微隔离功能的应用，可在发生病毒感染情况下，将威胁放置在可控范围内，从而有效提升安全防护水平。

（二）安全态势感知平台持续检测

1、识别原理

安全感知平台对相关虚拟货币的挖矿协议进行识别，并收集了绝大部分的矿池服务器 IP 以及相关挖矿域名，通过结合社区威胁情报，可以有效地对主机挖矿行为进行识别。

安全感知平台在威胁等级上将其标记为中等级威胁，在失陷确定性等级上将其标记

为已失陷。

2、日志分析

在非工作/上课时间，主机对境外 IP 有较多访问记录，针对可疑的行为可以和主机使用者确认之后，判断是人为还是挖矿程序行为

3、对流量进行分析

能够针对挖矿时候的流量进行抓包，然后对关键信息进行抓包分析，可以看到挖矿程序进行登陆或认证等行为。

（三）安全运营服务

需构建安全运营团队。通过线上收集 7*24h 来自终端、防火墙、杀毒软件、态势感知平台、潜伏威胁探针等设备来源的日志及流量进行分析研判，能做到当出现安全事件时，可以在第一时间发现并协助用户进行应急处置；线下设有安服专家线下协助处置安全威胁事件。

特别说明：具体建设方案请务必事先进行详细咨询，并向现教中心索取。

三、报价说明：

1、报价包含本项目所需的任何费用，如在后期的招标过程中中标，其**中标价不得高于此次报价**。

2、本次报价方案是我校制定采购方案的参考依据，具体采购实施需通过后续招标完成；

3、不保证以最低价作为我校制定采购方案的依据，综合考量性价比、服务等因素；

4、以厂商签字盖章的纸质报价为准；

5、厂商应保证提供的所有材料的真实性；

6、询价论证会仅作为制定采购方案的依据；

7、询价论证会后学校保留索取与本项目相关文件的权力。

四、供应商应提交以下资料：

1、提交有效的三证合一营业执照副本复印件；

2、法定代表人授权书、法人身份证及被授权人身份证复印件；

3、具有履行本次项目合同所必需的设备和专业技术能力的承诺书；

4、关于本项目的报价（以其他高校相同或相近案例合同作为报价的支撑材料）。

5、承诺以不高于此次报价参加我校本项目后续采购招标的承诺函。

五、报价文件的密封和标记及其他应注意事项

1、密封和标记：

（1）供应商应将报价函及相关资料装订成册并装入袋内加以密封，并在封签处加盖公章；

（2）装报价文件的信袋上应写明：项目名称、报价单位名称、地址、注明报价截止时间以前不得开封；

（3）封条格式：

项目名称： 景德镇学院“挖矿”病毒处置安全加固系统建设项目 供应商名称（加盖公章）： 联系人： 联系号码： 地址： 报价截止时间以前不得开封

2、供应商提供的技术指标要求需响应或超过项目功能及需求，如确有差异，在报价文件中使用明显的标记加以强调。

六、报价方式

自发布之日起至 2022 年 3 月 23 日 17：30 前。根据当前疫情防控形势，对外地供应商只接收邮寄材料。本地供应商可邮寄或直接提交至景德镇学院现代教育技术中心。地址：景德镇市浮梁县浮梁大道 3 号，邮编 333400，逾期不再受理。

报价文件接收人：朱老师 18370894201

项目咨询：程老师 13707982592

七、以上公告内容如有变动，将在学校官网上另行通知。

现代教育技术中心

2022 年 3 月 17 日