广州番禺职业技术学院

网络空间安全产业学院设备采购

（项目编号：**ZYGA232311608**）

合 同 书

甲方（采购人）：广州番禺职业技术学院

乙方（供应商）：联奕科技股份有限公司

签 约 地 点：广州市番禺区

甲　　方：广州番禺职业技术学院
项目联系人：王伟
电　　话：13672444481
地　　址：广东省广州市番禺区沙湾街市良路 1342 号

乙　　方：联奕科技股份有限公司
项目联系人：缪雪姣
电　　话：020-37621045
地　　址：广州市天河区科韵路 16 号自编 1 栋 501

根据 广州番禺职业技术学院网络空间安全产业学院采购项目（二次）（项目编号： ZYGA232311608）的采购结果，按照《中华人民共和国政府采购法》、《中华人民共和国民法典》的规定，经双方协商，本着平等互利和诚实信用的原则，一致同意签订本合同如下。

一、　货物内容

序号	产品名称	规格型号	品牌	产地	制造商名称	单价	数量	总价
1	威胁监测与分析引擎	TY-TSS10000-A57-WS-JYSX	奇安信	北京	奇安信科技集团股份有限公司	97000	1	97000
2	课程资源包	定制	优速致网	南京	南京优速网络科技有限公司	50000	1	50000
合计：人民币大写壹拾肆万柒仟圆整								147000

二、合同金额

合同金额为人民币（大写）：人民币大写壹拾肆万柒仟圆整（￥147000.00）。合同总额包括乙方设计、安装、随机零配件、标配工具、运输保险、调试、培训、

质保期服务、各项税费及合同实施过程中不可预见费用等。甲方不再支付其他任何费用。

三、设备要求

1. 货物为原制造商制造的全新产品，整机无污染，无侵权行为、表面无划损、无任何缺陷隐患，在中国境内可依常规安全合法使用。

2. 交付验收标准依次序对照适用标准为：①符合中华人民共和国国家安全质量标准、环保标准或行业标准；②符合采购文件和响应承诺中甲方认可的合理最佳配置、参数及各项要求；③货物来源国官方标准。

3. 货物为原厂商未启封全新包装，具出厂合格证，序列号、包装箱号与出厂批号一致，并可追索查阅。

4 乙方应将关键主机设备的用户手册、保修手册、有关单证资料及配备件、随机工具等交付给甲方，使用操作及安全须知等重要资料应附有中文说明。

四、交货期、交货方式及交货地点

1. 交货期：合同签订后 30 天内完成设备供货、安装、调试及验收。

2. 交货方式：汽车运输。

3. 交货地点：广州番禺职业技术学院（信息工程学院内）

五、付款方式

1. 签署合同生效且财政资金到位后5个工作日内，甲方支付合同总价的60%；即：人民币（大写）捌万捌仟贰佰元整（￥88200 元）。

2. 货物全部到场齐全，经甲方现场清点确认并签署到货单，货物及系统软件安装调试完毕、试运行期满，且项目通过校内验收后甲方支付给乙方合同总价的40%，即：人民币（大写）伍万捌仟捌佰元整（￥58800 元）。

3. 以上款项在乙方提交付款申请(首期款无须申请)及相应 发票并由甲方审核确认后启动办理支付程序，甲方向财政主管部门完成支付材料提交即视为完成支付手续，具体款项支付时间视资金到位情况而定。

4. 乙方帐户信息

开户名称：联奕科技股份有限公司

银行帐号：44050147051309001101

开 户 行：中国建设银行股份有限公司广州天河工业园支行

六、质保期及售后服务要求

1. 本合同的质量保证期（简称“质保期”）。质保期自甲方在完成校内验收之日起计算，威胁监测与分析引擎，提供一年威胁情报与检测引擎规则升级授权，

一年产品硬件标准维保服务。课程资源包，整体质保一年，在质保期内对平台软件进行免费升级、提供技术指导、功能优化与支持服务，服务方式包含网络支持、电话支持及现场服务。质保期内，如设备或零部件因非人为因素出现故障而造成短期停用时，则质保期和免费维修期相应顺延。如停用时间累计超过60天则质保期重新计算。

2.乙方售后人员需持有相应的培训证书。设有专业的售后服务中心，同时能够提供常用耗材及配件的及时供应。维修工程师需持有相应产品维修授权证书。

3.任何时候，乙方均不能免除因设备本身的缺陷所应负的责任，乙方有义务对所提供的货物实行终生维护和对设备进行定期的检测和维修；

4.质保期内乙方提供上门免费服务，

第一等级:不影响系统正常运行的一般性故障，乙方将通过市内公共电话网，进行远程维护，或者在二十四小时内上门维护排除故障；

第二等级:系统个别服务不正常，但不影响整个系统运行，乙方将在四小时内响应派遣工程师进行现场维护；

第三等级:系统严重故障，部分服务不正常，但系统仍可运行，乙方将在二小时内响派遣工程师进行现场维护；

第四等级:网终系统或主机系统严重故障，系统瘫痪，乙方将立刻专人应答，现场解决问题。质保期后，乙方须提供终生技术支持保障服务。

七、安装与调试

乙方将设备、系统安装并调试至正常运行的最佳状态。

八、验收

1.验收标准：按照甲方相关标准规定进行验收。所有货物需为原制造商制造的全新产品，整体无污染、无侵权行为、表面无划损、无任何缺陷隐患，在中国境内可依常规安全合法使用，同时符合本合同约定的质量要求。

2.验收程序：

验收程序，校内验收：乙方完成设备安装调试后，由甲方统一发起验收。

1）货物若有国家标准按照国家标准验收，若无国家标准按行业标准验收，为原制造商制造的全新产品，整机无污染，无侵权行为、表面无划损、无任何缺陷隐患，在中国境内可依常规安全合法使用。

2）货物为原厂商未启封全新包装，具出厂合格证，序列号、包装箱号与出厂批号一致，并可追索查阅。所有随设备的附件必须齐全。

3）乙方应将关键主机设备的用户手册、保修手册、有关单证资料及配备件、

随机工具等交付给采购人，使用操作及安全须知等重要资料应附有中文说明。

4）甲方组成验收小组按国家有关规定、规范进行验收，必要时邀请相关的专业人员或机构参与验收。因货物质量问题发生争议时，由本地质量技术监督部门鉴定。货物符合质量技术标准的，鉴定费由甲方承担；否则鉴定费由乙方承担。

九、违约责任与赔偿损失

1. 乙方交付的货物、工程/提供的服务不符合本合同规定的，甲方有权拒收，并且乙方须向甲方支付本合同总价 5%的违约金。

2. 乙方未能按本合同规定的交货时间交付货物的/提供服务，从逾期之日起每日按本合同总价 3‰的数额向甲方支付违约金，违约金累计总额不超过合同总价的 5%；逾期半个月以上的，甲方有权终止合同，由此造成的甲方经济损失由乙方承担。

3. 甲方无正当理由拒收货物/接受服务，到期拒付货物/服务款项的，甲方向乙方偿付本合同总的 5%的违约金。甲方人逾期付款，则每日按本合同总价的 3‰向乙方偿付违约金，违约金累计总额不超过欠款总价的 5%。

4. 其它违约责任按《中华人民共和国民法典》处理。

十、争议的解决

合同执行过程中发生的任何争议，如双方不能通过友好协商解决，向甲方所在地的人民法院提起诉讼。

十一、不可抗力

任何一方由于不可抗力原因不能履行合同时，应在不可抗力事件发生后 1 日内向对方通报，以减轻可能给对方造成的损失，在取得有关机构的不可抗力证明或双方谅解确认后，允许延期履行或变更合同，并根据情况可部分或全部免于承担违约责任。

十二、税费

在中国境内、外发生的与本合同执行有关的一切税费均由乙方负担。

十三、其它

1. 本合同所有附件、采购文件、投标文件、中标通知书通知书均为合同的有效组成部分，与本合同具有同等法律效力。

2. 在执行本合同的过程中，所有经双方签署确认的文件（包括会议纪要、补充协议、往来信函）即成为本合同的有效组成部分。

3. 如一方地址、电话、传真号码有变更，应在变更当日内书面通知对方，否则，应承担相应责任。

4. 除甲方事先书面同意外，乙方不得部分或全部转让其应履行的合同项下的义务。

十四、合同生效

1. 本合同在甲乙双方法定代表人或其授权代表签字盖章后生效。

2. 合同一式 陆 份，甲方执肆份，乙方执贰份。

（以下无正文）

甲方（盖章）：广州番禺职业技术学院　乙方（盖章）：联奕科技股份有限公司

法定代表人/授权代表：

签订日期：2023 年 7 月 28 日　签订日期：2023 年 7 月 28 日

附件：货物技术参数（指标）要求

序号	设备名称	技术参数要求
1	威胁监测与分析引擎	引擎（2U 标准上架设备，含滑轨）一台。 4*GE 管理电口，3*USB3.0 接口，1*DB9 Console 接口，冗余电源，内存 128G，960G SSD + 8*4TB SATA 存储硬盘。 含系统软件一套。 含 12 个月产品标准维保服务，含一年威胁情报更新授权与规则升级。 威胁监测与分析引擎功能需满足以下要求： 1、支持对重保任务的增删改操作，任务分战前、战中、战后三个阶段，支持对任务记录的导出查看及多个任务并行等功能； 2、支持根据用户业务需要进行个性化监测工作台自定义，支持重点监测内容集中添加或单个页面随意添加，个人监测工作台模板导入导出等功能； 3、支持对全部数据来源的分享展示与汇总展示，支持告警页面自动刷新时间自定义配置；支持自定义告警高级检索场景；告警列表可以进行包括基本信息、规则信息、原始告警、攻击行为、资产详情、取证分析、ATT&CK 分析、攻击带外分析等内容的详情查看，以及基于告警列表可以对告警进行联动处置和添加白名单操作； 4、支持告警的深度行为分析，行为包括 DNS 解析行为、TCP/UDP 交互行为、WEB 访问行为、传输文件行为； 5、支持以攻击者的维度进行分析，对攻击者进行画像，画像内容包括地理位置信息、国家信息、所属组织、使用的攻击手段、攻击的所有资产； 6、支持从威胁情报、应用安全、系统安全和设备安全的业务场景维度对告警进行攻击带外分析 7、支持挖矿行为的分析，分析内容包括挖矿阶段、币种分布、挖矿告警趋势以及挖矿告警信息 8、支持与云端威胁情报中心联动，可对攻击 IP、C&C 域名和恶意样本 MD5 进行一键搜索，查看基本信息、相关样本、关联 URL、可视化分析、域名解析、注册信息、关联域名、数字证书等 9、支持基于威胁情报的威胁检测，检测类型包含 APT 事件、僵尸网络、勒索软件、流氓推广、窃密木马、网络蠕虫、远控木马、黑市工具、其他恶意软件，并可自定义威胁情报 10、支持对告警进行加白，加白参数包括：受害 IP（IP 段）、攻击 IP（IP 段）、威胁情报 IOC/规则 ID、威胁名称、XFF 代理、URI、域名、目的端口、源 IP（IP 段）、目的 IP（IP 段）、payload、referer； 11、支持可疑 DNS 解析：能够检测发现 DGA 域名与 DNS 隧道域名，支持根据时间范围、请求次数、DNS 域名总长度自定义 DNS 隧道检测规则

		12、支持疑似 DNS 服务器发现：能够根据响应 DNS 请求与发起 DNS 请求进行行为分类 13、支持反弹 shell 分析：能够展示受害 IP、攻击 IP、端口、受害地域/资产组、攻击地域/资产组、最近访问时间等详细信息 14、支持异常登录行为检测，检测内容包括：源 ip、账号、登录资产 IP、使用协议、登录结果等信息，且能进行异常时间配置 15、支持 ssh、telnet、ftp、smb 等常见协议特权账号登录行为分析，且能自定义特权账号 16、支持明文密码泄露行为检测，检测内容包含：登录账号 IP、账号、密码、使用协议 17、支持可疑爬虫或扫描分析，能自定义 web 访问频率，且能设置源 IP 白名单。 18、支持可疑来源访问行为分析，能展示来源、源 IP、资产 IP、资产组、源地域、目的端口、URI 等信息，且能自定义可疑来源 19、支持联动服务管理，支持 python 语言与 javascript 语言在 web 页面编辑联动服务 20、支持检索异常报文、域名解析、文件传输、FTP 控制通道、LDAP 行为、登录动作、邮件行为、MQ 流量、网络阻断、数据库操作、SSL 加密协商、TCP 流量、Telnet 行为、UDP 流量、WEB 访问等网络流量日志，并可基于时间、IP、端口、协议、上下行负载等多重字段组合进行日志检索 21、支持告警日志检索，可基于时间、告警类型、文件 MD5、文件名、文件传输方向、攻击方式、攻击结果、来源/目的所属国、IP 地址、上下行负载等多字段混合搜索 22、支持检索终端 IM 文件传输、邮件附件传输、DNS 访问、 进程、U 盘文件传输等动作的日志，可以及时发现终端上存在的异常现象，并可结合网络日志及告警日志深挖威胁的攻击全过程 23、支持大屏展示综合态势包括整体系统概况、威胁等级分布、告警趋势、不同维度的攻击数量统计、攻击阶段等。 24、支持与云端安全运营中心联动。设备能连接互联网时，安全专家在云端分析并撰写威胁分析报告下发到设备上共用户查阅；设备离线时，可将关键数据离线导出上传到云端安全运营中心，安全专家进行分析撰写威胁分析报告 25、支持对资产进行分组管理及对应内网网段的录入，系统自动根据用户录入的网段发现资产信息，同时支持根据分组过滤资产列表； 26、支持 AES256、SM4 数据传输加密，确保数据传输的安全性） 27、支持基于深度学习的自然语言处理（NLP）技术，提供文本对话交互功能，为用户提供告警威胁类的问答服务； 28、支持 10 种以上的高频告警智能研判场景（web 弱口令登录、明文口令传输、

		SMB 信息泄露、OpenVPN 通信、SQL 注入、漏洞扫描、敏感文件探测、系统默认共享连接行为、系统命令注入、log4j2 远程代码执行等），可根据不同场景查看不同告警研判分析结果； 29、支持多种攻击源 IP 的情报标签（恶意扫描、漏洞利用、后门植入、暴力破解、恶意程序、钓鱼欺骗、挖矿病毒、WEB 攻击、IDC 主机、代理主机、黑产团伙、雇佣黑客、白帽子等）、自定义 IP 标签显示； 30、支持实时显示攻击源 IP 的画像信息，包括 IP 访问行为、IP 告警信息、网络测绘信息、处置建议、威胁级别，情报标签、关注热度、首次发现时间、最近发现时间等 31、威胁情报维度分析包括：情报详情、影响资产列表、资产的行为（行为包含：DNS 解析、TCP 流量、UDP 流量、WEB 访问、文件传输） 32、支持链路劫持分析：能够展示被劫持对象、CDN 服务器、被劫持资源、文件 MD5、访问时间等详细信息 33、支持 DNS 重绑定分析：能够展示受害 IP、攻击 IP、域名、DNS 解析记录、访问时间等详细信息
2	课程资源包	1、支持一个模拟校园网络的场景，分为内部网络和外部网络两部分，内网和外网能够互联。 2、支持 NAT 配置与维护，使内部网络可以安全地访问外部网络。 3、支持 SSL VPN 配置与维护，使得管理员可以通过 VPN 连接到内部网络进行管理操作。 4、支持防火墙的配置与维护：配置内部访问外部的防火墙策略，使内部主机能安全访问外网；配置外部访问内部的防火墙策略，使特定网段才能访问内网。 5、支持校园网文件共享系统配置与维护：部署校园网文件共享 web 系统，在网内可以访问该系统。 6、支持内部渗透测试：包括令暴力破解模拟、SQL 注入模拟和木马攻击模拟。