需求参数公示

1.技术标准

（一）采购内容：拟采购新型计算环境安全训练靶场一套。

（二）具体技术指标要求：

本次采购要求如下：新型计算环境安全训练靶场采购分成包1和包2，其中包1为云原生安全训练，如表1所示，包2为边缘计算安全训练，如表2所示。本项目包1、包2可以兼投兼中。

表1 云原生安全训练采购要求

序号	需求名称	技术参数	数量
1	功能参数	1、总体要求 1）需满足采购单位集成规范要求； 2）★提供云原生环境构建所需的镜像资源； 3）★提供云原生训练案例和对应训练内容，训练内容包含具有云原生特色的安全能力训练，覆盖：信息收集和网络探测、初始访问、执行、权限提升、横向移动、容器逃逸、集群控制等阶段以及对应检测和防护技术； 4）★提供云原生训练案例对应的训练指导书、工具、训练环境等资源。 2、★提供信息收集和网络探测的安全能力训练。包含：对通过端口扫描、暴力破解试图获取容器内的敏感数据或对其他容器攻击行为的检测。 3、★提供初始访问权限的安全能力训练。包含：对通过暴力破解、web渗透等攻击手段获得云原生环境的初始访问权限行为的检测。	1套

		4、★提供容器内执行命令的安全能力训练。包含：对容器内执行敏感命令、容器内执行恶意脚本、篡改容器内可执行文件、反弹 shell、容器内操作敏感文件等攻击；对相应攻击行为的检测。 5、★提供容器逃逸的安全能力训练。包含：对容器逃逸、容器提权、启动特权容器、容器启动挂载敏感目录等行为的检测。 6、★提供横向移动的安全能力训练。包含：对在云原生环境中横向移动并获取更高级别的权限行为的检测。 7、★提供权限提升的安全能力训练。包含：对从普通用户升级为管理员权限、获取整体集群的访问权限行为的检测。 8、★提供集群控制的安全能力训练。包含：对获取整个 K8s 集群的控制权并对云原生环境进行控制或破坏，如修改配置、窃取敏感数据、拒绝服务攻击等行为的检测；对容器内搜索私钥行为、集群角色拥有 Pod-Exec 权限、Kubernetes-Roles 异常访问、Kubernetes-ClusterRoles 异常访问等行为的检测。 9、★提供容器防护能力训练。包含：容器内进程阻断、容器内文件防篡改、IP 一键封堵等。 10、★云原生安全训练应用场景包含基于云原生的电子政务系统、社交媒体网站等应用场景或其他类似云原生应用场景，训练内容包括针对相应云原生场景的攻击的检测、防护步骤。	
2	技术指标	1）★案例覆盖的获取初始访问权限及其检测技能分别不少于 2 项； 2）★案例覆盖的获取容器内部执行命令及其检测技能分别不少于 2 项； 3）★案例覆盖的容器逃逸及其检测技能分别不少于 2 项： 4）案例覆盖的云原生环境内横向移动及其检测技能分别不少于 3 项：	1 套

		5）案例覆盖的云原生环境内权限提升及其检测技能分别不少于 3 项； 6）案例覆盖的集群控制及其检测技能分别不少于 3 项； 7）案例覆盖的容器安全防护技能不少于 5 项。	

表 2 边缘计算安全训练采购要求

序号	需求名称	技术参数	数量
1	功能参数	1）需满足采购单位集成规范要求； 2）★提供车联网与模拟自动驾驶车辆系统构建所需的镜像资源； 3）★提供车联网相关安全训练场景； 4）★训练场景具备边缘计算模型和云边端网络架构设计。	1 套
2	技术指标	1）★车联网训练环境支持不少于 4 种主流工业协议设备，包括但不限于控制器局域网（CAN）、具有灵活速率的控制器局域网（CAN-FD）、车载以太网、消息队列遥测传输协议（MQTT）； 2）★车联网训练环境包含不少于 10 类虚拟设备，至少包括车机、远程/车载通信模块（T-BOX））、域控制器等； 3）★车联网训练环境提供不少于 3 种仿真内容，包括但不限于车辆 CAN 总线协议仿真、车载系统内核仿真、车载系统应用的仿真等； 4）提供训练案例数量不少于 20 个，至少包括：分布式计算集群攻击防护、激光雷达（LiDAR）传感器攻击防护、车联网远程控制业务攻击防护、汽车固件破解攻击防护、假冒 ECU 的攻击防护、自动驾驶攻击防护等； 5）★车联网训练环境车机系统支持预埋不少于 3 类智能汽车相关漏洞（包括但不限于 APP、固件、系统、服务等），每一类至少包含 2 种，并提供对应漏洞扫描工具或检测脚本； 6）★提供至少 3 种面向车联网远程控制业务攻击防护的	1 套

		训练案例，包括对智能网联汽车 T-BOX 的攻击防护、通过 TSP 云平台身份仿冒控制消息伪造防护、对车联网边缘节点中的加密库 OpenSSL 的攻击防护； 7）★提供至少 2 种针对加密的汽车固件破解防护的训练案例。固件类型包括但不限于车机、T-BOX； 8）★提供至少 1 种面向车联网分布式计算集群攻击防护的训练案例，包括但不限于对车联网分布式边缘计算设备的攻击防护； 9）★提供至少 2 种面向车联网 CAN 总线的 DoS 攻击防护的训练案例，至少包括 CAN 总线优先级攻击防护、CAN 总线泛洪攻击防护； 10）★提供至少 1 种基于车联网假冒 ECU 攻击防护的训练案例，至少包括通过冒充车载 ECU 边缘结点，无需授权即可接入车载 CAN 总线，最终接管车辆的防护； 11）提供至少 1 种面向自动驾驶汽车轨道行驶攻击防护的训练案例，至少包括对正常行驶在轨道上的自动驾驶汽车的视觉感知模块添加强扰动，迫使汽车偏离轨道行驶的防护； 12）提供至少 3 种覆盖“车路云一体化”业务场景攻击防护的训练案例，包括仿冒路侧单元（RSU）与车辆进行交互发送伪造消息、通过云端 TSP 平台身份仿冒伪造控制消息、非法篡改 RSU/OBU 认证证书制造设备异常的防护； 13）提供至少 2 种 LiDAR 传感器攻击防护的训练案例，包括 LiDAR 传感器目标检测模型点扰动攻击防护、鸟瞰视角（BEV）和体素 LiDAR 传感器时延攻击防护。	

2、商务要求

★（一）交付（服务）时间、地点和方式

1.交付（服务）时间：合同生效后，包 1 云原生安全训练子系统中标供应商在 30 日内完成阶段性试用版本的安装及调试，在 90 日内完成安装

及调试；包 2 边缘计算安全训练子系统中标供应商在 30 日内完成阶段性试用版本的安装及调试，在 90 日内完成安装及调试。

2.交付（服务）地点：湖南长沙采购单位指定地点。

3.交付（服务）方式：现场交付。中标供应商提供设备的各项技术性能指标必须达到合同和技术文件规定的要求。

（二）售后服务

1.中标供应商负责对采购单位使用、维护人员进行软件的安装、调试、使用和运维培训。至少免费培训四名操作维护人员；具体培训计划（时间、地点、人数、内容）由中标供应商提供，其费用应包括在投标价格内。

2.产品维保期为自验收合格之日起不少于五年，维保期内中标供应商提供免费的维护服务、系统升级服务、上门服务，提供 7*24 小时电话、线上技术支持。质保期满后，终身免费技术支持维护，软件使用寿命期内，软件修复只计成本价。

3.中标供应商应有常用配件库和快速服务保障能力。

4.出现产品、使用问题采购单位提出后，中标供应商在 30 分钟内运维人员远程故障响应，24 小时内提供解决方案，48 小时内提供相关的维修、升级等解决问题的服务。维保内如系统故障导致系统停用时间超过 7 天，维保期按照故障时间顺延，期间产生的损失由中标供应商承担。

5.定期提供例行检查和维修服务。

★（三）知识产权和保密要求

对采购单位提供的人员、地址、采购情况等信息要保守秘密，不得向外界透露。中标通知书发出后，采购单位将与中标供应商签订保密协议。

基于项目合同履行形成的知识产权和其他权益,其权属归采购单位所有，法律另有规定的除外。

采购单位、中标供应商在采购和履行合同过程中所获悉的对方信息，如采购单位提供的人员、地址、采购情况等属于保密的内容，采购单位、中标供应商双方均有保密义务。

中标供应商应保证采购单位在使用该货物或其任何一部分时,不受第三方侵权指控。同时，中标供应商不得向第三方泄露需求单位的技术文件等资料。

★（四）付款及结算方式

合同签订后，采购单位在 30 个工作日内向中标供应商支付 30%合同款。货物交付并验收合格后，中标供应商提供全额发票，采购单位在 30 个工作日内向中标供应商支付 65%合同款,剩余 5%合同款为质量保证金，维保期满且无质量问题,采购单位在接到中标供应商的质量保证金返还申请后 30 日内无息全额支付。

（五）实施人员要求

本项目包 1 和包 2 至少分别投入项目负责人 1 名，运维人员 1 名，开发项目团队人员 5 名（不含项目负责人以及运维人员），在投标文件中提供上述人员名单。

（六）验收方式

1.在完成全部采购及服务内容后，中标供应商应对交付物进行全面自检，符合交付条件后，由中标供应商向采购单位提出验收申请，采购单位按照合同、招标文件及中标供应商投标文件要求以及学校验收相关规定组

织专家对本项目进行验收。具体组织程序、验收标准和方法，按采购单位规定程序执行，中标供应商配合。

2. 采购单位在验收中，如果发现有与合同规定不符的，应在十个工作日内向中标供应商提出书面异议，不签发验收单。

3.中标供应商在接到采购单位书面异议后，应在十天内予以纠正，并承担由此发生的一切费用和损失。再次验收所产生的费用由中标供应商承担。如果再次验收仍不合格，采购单位有权取消或解除采购合同，由此造成的损失，由中标供应商承担。

4.采购单位在中标供应商按合同规定交货和/或安装、调试后，无正当理由而拖延接收、验收或拒绝接收、验收的，应承担因此给中标供应商造成的直接损失。

5.采购单位对货物进行检查验收合格后，应当收取发票并在《交货验收单》上签署验收意见及加盖单位印章。

（七）生产及安装调试等要求

1.中标供应商负责所有软件的供货与安装、调试，解决系统联调中相关技术问题。

2.该采购项目中标供应商应配合靶场管理平台的中标供应商，完成相关的集成工作。

（八）报价要求

1.报价方式：本项目采用合同总价方式，报价总价一次性包干，包含供应、运输、安装调试、技术培训、售后服务、备品备件和伴随服务等价格，价格不因实施期间市场变化及政策调整因素而变化。

2.报价币种：人民币（含税）。

（九）原型系统演示

★1.投标供应商须现场对原型软件运行演示，未提供演示的为无效投标（演示功能满足情况不作为无效投标的依据。）

2.演示时间不得超过 15 分钟。系统演示如需特殊设备（载体）的由投标供应商自备。

3.具体演示要求详见“技术评审标准表 原型系统演示”。现场演示其他要求：非授权代表演示的，演示时须单独提供授权书。

3、资质要求

（一）具有企（事）业法人资格（有行业特殊情况的银行、保险、电力、电信等法人分支机构，会计师、律师等非法人组织，行业协会等社会团体法人除外）；

（二）国有企业；事业单位；军队单位；成立三年以上的非外资（含港澳台）独资或控股企业，国内市场无类似或可替代产品的企业除外。

（三）具有良好的商业信誉和健全的财务会计制度；

（四）具有履行合同所必需的设施设备、专业技术能力、质量保证体系和固定的生产经营、服务场地；

（五）有依法缴纳税收和社会保障资金的良好记录；

（六）参加军队采购活动前 3 年内，在经营活动中没有受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款（200 万元以上）等重大违法记录；

（七）未被中国政府采购网（www.ccgp.gov.cn）列入政府采购严重违法失信行为记录名单，未在军队采购网（www.plap.mil.cn）军队采购暂停名单处罚范围内或军队采购失信名单禁入处罚期和处罚范围内，以及未被“信用中国”（www.creditchina.gov.cn）列入严重失信主体名单或国家企业信用信息公示系统（www.gsxt.gov.cn）列入严重违法失信名单（处罚期内）。

（八）投标企业应当具备服务履约的能力。

（九）单位负责人为同一人或存在直接控股或管理关系的不同供应商，不得同时参加同一包的采购活动。生产场经营地址或注册登记地址为同一地址的不同生产型企业，股东和管理人员（法定代表人、董事或监事）之间存在近亲属或相互占股等关联关系的不同非国有销售型企业，也不得同时参加同一包的采购活动。近亲属指夫妻、直系血亲、三代以内旁系血亲或近姻亲关系。

（十）法律、行政法规规定的其他条件。

（十一）本项目特定资格：无。