附件1

**中国高校产学研创新基金-AI+网络安全治理技术专项**

**申请指南说明**

根据 《关于申报2025年中国高校产学研创新基金的通知》（教科发中心函〔2025〕3号)的相关要求，教育部高等学校科学研究发展中心与赛尔新技术（北京）有限公司、奇安信科技集团股份有限公司联合设立“中国高校产学研创新基金-AI+网络安全治理技术专项”，支持高校在新工科中的网络空间安全、大数据、云计算、人工智能等技术方向的开展相关科研、行业应用及创新研究。

**一、课题说明**

1.“AI+网络安全治理技术专项”旨在支持高校在网络空间安全、大数据、云计算、人工智能等技术方向的开展相关科研、行业应用及创新研究。以科技变革促进教育变革，创新人才培养机制，推动社会发展。

2.“AI+网络安全治理技术专项”的申请截止时间为2025年12月15日。计划执行时间为2026年4月1日～2027年3月31日，可根据课题复杂程度适度延长执行周期，最长不超过两年。

3.“AI+网络安全治理技术专项”为每个立项课题提供总经费10万元至50万元的课题研究经费及科研软硬件平台支持，其中课题研究经费5万元至25万元。

4.“AI+网络安全治理技术专项”基金课题的选题方向见表一，申请院校可从表一中选择一个课题方向进行申报。基金课题提供的相关技术、应用和软硬件平台见表二。

**表一 “AI+网络安全治理技术专项”选题列表**

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |  |  |
| --- | --- | --- |
| **课题方向编号** | **课题方向** | **课题研究内容** |
| A01 | 基于知识图谱与人工智能融合的辅助教学技术研究 | 针对“以学生为中心”的工程教育理念，用技术重构教育的“生产力”，推动教育从“经验驱动”向“数据驱动”、从“标准化”向“个性化”的范式转变，实现教育质量的整体提升与社会价值的最大化。研究围绕知识图谱与人工智能技术融合进行赋能教学展开，基于利用虚拟化技术进行仿真实践和演练的教学系统。  所需研究的技术包括但不限于：构建多模态知识点智能提取框架，基于NLP技术实现文本的实体识别、语义摘要生成，结合CV技术视频、图片进行文本提取，形成结构化知识图谱库；研发网络拓扑动态建模方法，通过图神经网络将物理网络架构抽象为语义图谱；开发基于图谱的问答AI助教系统，融合知识检索与自然语言生成技术，实现专业问题解答与学习路径推荐。 |
| A02 | 数据安全技术教材体系构建与实践研究 | 为应对数据安全领域人才培养的迫切需求，解决当前教材知识滞后、实践脱节等问题，聚焦数据安全全生命周期，关注数据安全领域的通用防护技术、核心技术与工程实践，以数据库防火墙、数据库审计、数据脱敏等关键技术切入，深度融合零信任架构、隐私计算等前沿技术，结合数据安全典型案例，构建“理论+案例+实践”三位一体的创新教材体系。以构建科学高效的数据安全技术教育体系为核心目标，通过系统性研究数据安全技术教育的理论框架、实践模式及创新路径，深入剖析行业需求与教学现状的矛盾点。  研究内容包括但不限于：数据库安全防护技术中的访问控制、SQL注入防御；数据脱敏方法与实践，涵盖数据使用过程中的静态脱敏、动态脱敏的技术原理和实现；操作系统安全的安全加固、身份认证、访问控制等；日志审计技术中的日志采集标准化、实时监控分析、异常行为溯源及合规审计等；容灾备份关键技术，涉及数据库备份、系统备份、增量/全量备份策略等内容；数据安全应急响应实践，涉及数据泄露、数据篡改、数据破坏等内容，数据安全保障体系架构和应对数据安全事件的能力。以此构建出一套包含课程体系设计、教学方法创新、实践平台搭建、师资能力提升在内的教育优化模型。 |
| A03 | 攻防靶场自动化渗透智能体应用研究 | 在靶场环境中，自动化渗透智能体不仅能够覆盖更广泛的攻击面，提升渗透测试的深度与广度，还能在演练过程中不断学习和优化攻击策略，实现对防御体系的持续压力测试与能力验证。相比传统人工渗透方式，智能体具备更高的效率、可重复性与自适应性，可广泛应用于网络靶场中的红队对抗、防御验证、靶机评估等场景，为构建智能化攻防对抗体系提供坚实支撑。基于网络安全攻防演练靶场系统，研究包括但不限于：基于MCP的传统自动化渗透工具的智能化编排技术；基于大语言模型的多阶段攻击链构建技术；基于大语言模型的攻击面测绘技术；利用AI自动化渗透智能体的蓝军能力评估技术；基于AI智能体的安全防御验证技术等。 |
| A04 | 可观测的网络安全靶场构建技术研究 | 在复杂多变的网络空间安全形势下，构建具备可观测能力的网络安全靶场已成为推动实战化攻防演训、支撑新型安全技术验证与人才培养的重要基础设施。聚焦于构建具备高可观测性的网络安全靶场，基于网络安全攻防演练靶场系统，涵盖数据采集、传输存储、分析可视化等关键技术，旨在攻克数据处理性能瓶颈、多源数据融合等难题。期望通过深入研究，实现靶场安全态势实时感知、故障快速排查、攻防技术有效评估，为网络安全研究与实践提供坚实技术支撑。研究的内容包括但不限于：基于eBPF的全链路主机与容器事件采集；基于ebpf的rookit检测技术；海量观测数据的清洗、处理与建模；基于规则的威胁事件分析以及基于大语言模型的威胁事件分析与建模等。 |
| A05 | 靶场攻防演练场景体系研究 | 网络靶场作为网络安全防御能力提升的关键载体，其攻防演练场景的优化设计至关重要。本研究聚焦于当前靶场攻防演练场景真实性不足、复杂性欠缺、扩展性受限等问题，旨在构建一套创新型演练场景体系。  研究基于网络安全攻防演练靶场系统大规模网络节点的模拟仿真、攻击流量仿真、安全事件仿真、数据采集等能力，通过多源数据融合技术，采集真实网络环境中的流量、日志、漏洞等数据，运用大数据分析与机器学习算法，深度挖掘数据特征，构建高度逼真的网络环境模型，从网络拓扑动态变化到用户行为模拟，全方位还原真实场景。在攻防场景设计上，打造多层次、多维度的对抗体系，涵盖网络层、系统层、应用层等多类型攻击，以及信息收集到权限维持的全攻击阶段，结合多样化防御策略，满足不同层次的演练需求。同时，开发动态自适应技术，实时监测演练过程，依据参与者行为和系统状态智能调整场景参数，增强演练挑战性。推动网络安全人才培养与技术研究的发展，助力提升我国网络空间安全防御水平。研究场景包括但不限于关键信息基础设施防护、风险评估、安全运维、安全加固、应急响应、渗透测试、实战攻防演习、智能制造场景下的工控安全、智能电网工控安全、人工智能安全评测及网络安全热点安全事件等。 |
| A06 | 隐私计算驱动的数据安全体系研究 | 针对数据流通场景合规要求严、共享成本高等难题，研发以同态加密为主、可信执行环境为辅的隐私计算架构，基于多方安全计算与联邦学习的协同计算模型，通过密码学与AI技术的深度融合实现数据“可用不可见”，促进数据要素安全流通。  主要研究内容包括但不限于：  （1）密码算法：实现同态加密方案；  （2）联邦学习框架选型：对联邦学习框架进行横向评测，从通信效率、模型收敛速度、支持算法类型等维度形成技术选型报告；  （3）跨平台安全协议设计：集成Intel SGX与ARM TrustZone硬件方案，开发异构环境下的统一密钥管理模块。 |
| A07 | 云原生环境内生安全体系研究 | 针对云基础设施攻击面广、配置复杂度高、漏洞修复周期长等挑战，研发以零信任架构为主、运行时防护为辅的安全防护体系，基于策略即代码与eBPF技术的主动防御模型，通过基础设施的深度可见性实现威胁自愈，降低云环境安全运维成本。  主要研究内容包括但不限于：  （1）运行时防护技术选型：从系统性能损耗、事件捕获粒度、规则更新效率等维度完成技术路线决策；  （2）自动化响应体系设计：开发策略引擎与Istio服务网格的深度集成方案；  （3）攻击面管理：构建云资产自动化发现系统，集成漏洞扫描能力，实现新部署资源的安全基线检测。 |
| A08 | 物联网边缘设备接入安全体系研究 | 在物联网（IoT）领域，特别是涉及关键基础设施和环境监测（如地震预警、气象观测、能源管网监控、电力设施监测等）的场景中，广泛部署着大量专业化的数据采集终端。边缘设备的安全接入成为物联网体系的核心风险点。传统物联网设备普遍存在安全防护能力薄弱、改造复杂度高、异构环境适配性差等问题，易因密码体系漏洞、物理入侵或传输链路风险导致数据泄露、设备劫持等安全事件。  针对物联网边缘设备接入场景，研究安全接入密码技术，通过低侵入式改造架构与多维度防护机制，解决设备身份认证、传输链路安全、物理环境威胁等关键问题，构建适应多样化部署环境的边缘安全防护体系。  主要研究内容包括但不限于：  （1）透明安全加固技术：无缝适配主流物联网协议与安全通信协议，应用无感知的透明传输加密，不改变原有网络的任何结构和配置，实现对存量设备进行非侵入式安全改造，降低传统系统升级门槛；  （2）密码安全增强技术：集成国密算法（SM2/SM3/SM4）与动态密钥协商机制，实现设备身份认证、数据加密传输的全链路密码防护，抵御中间人攻击、固件篡改等风险；  （3）自动探测接入安全风险：通过网络流量分析，探测潜在安全风险，例如明文数据传输、弱密码算法等。 |
| A09 | 内部威胁安全防护技术研究 | 内部威胁是当下数据泄露最主要的原因。《全球内部威胁成本报告》显示，2024年较过去两年相比，内部威胁事件的总数增加了44%。56%事件的发生根本原因是内部人员的疏忽，这其中用权限账号盗窃近两年安全事件的18%。由此可见，特权访问管理不当已经成为内部威胁带来的数据泄露的最主要原因。  主要研究内容包括但不限于：  （1）研究实现特权账号的全生命周期管理，实现特权账号的最小化权限策略，并持续监控与治理特权账号威胁，进行特权行为审计与威胁分析；  （2）研究基于国密算法的密码保险箱的特权账号存储技术；  （3）基于安全统一网关的特权会话管控技术和非侵入式的大数据分析应用内嵌特权账号管理技术；  （4）研制出可信的特权安全访问系统，帮助企业系统化的落地并实现各种业务场景下特权访问的统一管理、规范使用与全局监控。 |
| A10 | 基于动态分析与机器学习的API接口业务逻辑漏洞检测技术研究 | 随着微服务架构和云计算的普及，API已成为现代软件系统的核心组件，然而，API接口的复杂性和开放性也使其成为攻击者的主要目标，尤其是业务逻辑漏洞检测也成为重点难点问题。因此，开发一种针对API接口业务逻辑漏洞的智能检测技术，具有重要的理论价值和实际意义。  本项目主要研究内容包括不限于以下：  (1)研究API接口业务逻辑漏洞的常见类型及其特征，构建检测所需指标识别引擎，针对特征编写检测规则和异常行为模型；  (2)研究API接口调用行为的动态捕获机制，实时监控请求与响应数据，开发数据接口异常调用/访问行为的检测方法；  （3）研究基于访问实体、访问时间、访问资产、传输数据属性等多维度因素，设计分析规则，针对越权访问、数据篡改、逻辑绕过等安全事件，形成检测模型或规则不少于10种； |
| A11 | 特权会话访问控制策略及审计关键技术研究 | 堡垒机提供的脚本运维功能目前仅能通过人工审核的方式来确保脚本运维安全，难以有效识别shell和python脚本的执行意图，并检测出其中的安全风险，可能导致拦截失效的问题。同时，运维过程中执行的命令通常采用字符串正则匹配的方式进行分析，容易绕过，风险告警准确率低。  本项目主要研究内容包括不限于以下：  （1）研究基于AI的运维指令、脚本检测和拦截技术。运维分为命令运维与脚本运维。当用户在一个运维会话中执行命令或使用脚本运维时，需要基于AI技术对用户输入的命令进行风险分析，识别出其执行意图以及可能存在的风险，并生成相应告警；  （2）研究基于AI的运维会话风险告警技术。基于AI技术对用户的历史运维会话数据进行分析，精准识别其中可能存在风险的历史会话，并生成告警。运维数据主要包括用户使用堡垒机期间执行过的命令，上传过的脚本。生成的告警应能对应到具体用户、受影响的资产、操作时间。 |
| A12 | 大模型运行态数据泄露防护及关键技术研究 | 随着大模型应用的爆发式普及，随之带来的安全风险也愈发严重，安全风险范围包扩：大模型基础设施安全，环境及供应链安全，运行时的数据安全、内容安全、大模型攻击注入等各类风险。大模型应用对应的攻击手法较传统应用也有极大的区别，当前的传统检测手段和防护措施，也无法应对大模型环境下的检测要求。  本项目主要研究内容包括不限于以下：  （1）本研究主要聚焦在大模型运行态风险检测及发现；  （2）关注AI Agent场景及RAG应用场景下的数据泄露风险研究；  （3）针对数据泄露的方法，检测及防护手段及进行深入研究及分析。 |
| A13 | AI安全漏洞检测关键技术研究 | AI技术加快演进，但由算法黑盒、不可解释性等内生问题导致的AI安全漏洞使得AI系统容易受到对抗样本攻击，影响运行安全。我国高度重视AI安全问题，先后出台多个人工智能安全治理文件；产业界也急需适用于各类人工智能应用的成熟安全产品。故此，研究AI安全检测技术以提前发现模型安全漏洞、科学评估安全威胁和运行风险，有助于大大提升AI系统的运行鲁棒性和面向安全威胁的应对能力。  本项目主要研究内容包括不限于以下：  （1）AI对抗攻击漏洞检测设计报告，包含高迁移性对抗攻击技术，可攻击人脸识别、交通标志识别等场景的AI视觉目标模型；  （2）AI模型安全缺陷分析报告，包含误分类性、感知隐蔽性和扰动鲁棒性等项评估指标；  （3）AI安全漏洞检测平台，支持人脸识别、交通标志识别等应用场景，支持6个针对AI视觉应用场景模型的漏洞检测。 |

**二、申报条件和要求**

1. 团队成员在选定的研究课题方向有较好的技术储备，包括与申报课题研究内容相关的研究成果、教材、论文、专利、获奖等。

2. 团队组成合理，分工明确，数量不少于3人。原则上申请人需具备中级以上职称。

3. 优先支持已经设立网络空间安全、大数据、云计算、人工智能相关专业或者已经成立相关研究中心的院校。

4. 优先支持研究内容有创造性、前瞻性和实用性，有商业化前景的课题。

5. 优先支持有明确研究成果，成果有应用价值，可复制、可推广的课题。

6. 优先支持研究方向明确，研究内容详实，研究方案完整可行的课题。

7. 申请人应客观、真实地填写申请书，没有知识产权争议，遵守国家有关知识产权法规。在课题申请书中引用他人研究成果时，必须以脚注或其他方式注明出处，引用目的应是介绍、评论与自己的研究相关的成果或说明与自己的研究相关的技术问题。对于伪造、篡改科学数据，抄袭他人著作、论文或者剽窃他人科研成果等科研不端行为，一经查实，将取消申请资格。

8. 资助课题获得的知识产权由资助方和课题承担单位共同所有。

9. 课题组需具备可独立支配的课题研究基础软硬件条件。

**三、资源及服务**

针对入选合作院校，基金将提供完善的资源和服务体系，以保证院校顺利开展合作课题，并为院校在网络空间安全、大数据、云计算、人工智能方向的科研、教学和人才培养提供长期有效的支持。

1.“AI+网络安全治理技术专项”为每个立项课题提供对应的研究经费及科研软硬件平台支持，为申报团队提供创新项目选题指导，并根据需求开展服务校方等工作。

2.基金课题发起单位将辅助、联合申报院校申报新的科研课题，提供项目咨询服务和技术支持，辅助科研成果的快速产品化及解决方案的包装。

**表二 提供给课题研究的资源说明**

|  |
| --- |
|  |

|  |  |  |
| --- | --- | --- |
| **平台编号** | **软硬件服务名称** | **详细介绍** |
| B01 | 业务仿真管理系统 | 1.支持自定义网络拓扑，拖拽虚拟设备、物理设备、漏洞靶标至画布区快速搭建业务拓扑，可配置拓扑中虚拟机的CPU、内存、网卡数量、网卡驱动、硬盘驱动等参数；  2.可将虚拟机和真实物理设备同时加入到同一个网络拓扑中进行实验；  3.数字路由器和数字交换机可通过页面简单配置即可完成网络调试；  4.支持设备连线、分组和取消分组展示、导出拓扑图功能，支持复制粘贴整个拓扑或单个虚拟机；  5.支持ISO镜像上传，支持创建KVM、容器两种类型的虚拟设备资源；  支持服务器IP、时间、SSH端口管控、XFF代理、访问IP白名单等页面配置维护；  6.支持多种IP地址管理及分配方式，可配置VNC、RDP、SSH几种连接访问模式，支持向虚拟机内粘贴文本和导入文件。 |
| B02 | 网络安全实践教学系统 | 1.支持实验进度保存功能，实验环境关闭时系统自动保留实验的操作进度，下次启动实验时可在上次实验进度基础上继续实验；  2.支持根据实验所需资源自动分配算力资源；  3.支持分步式实验手册设计，每一步可关联学习任务，并自动验证实验的完成条件，通过系统自动判定实验完成度实现闯关模式的实验形式；  4.支持在实训过程中自定义规划设计项目实验环境，如设计网络架构、划分网络区域、增加设备节点、更改设备连接线、搭建系统服务和配置网络策略。 |
| B03 | 网络安全攻防竞技系统 | 1.支持容器和KVM两种虚拟化技术，自定义上传环境镜像，支持预览启动查看赛题环境；  2.支持自定义检测规则设置，支持检测协议和检测脚本上传两种方式，根据需求可使用HTTP、TCP检测协议从服务端口、期望输出、URL等方面设置，也可以使用脚本方式；  3.支持动态flag，可根据需求使用关联路径、修改变量、命令执行、curl、脚本执行方式进行设置；  4.支持来源IP段输入验证、登录绑定，支持来源IP启用、不启用、批量清除IP等操作。 |
| B04 | 网络安全攻防演练靶场系统 | 1.支持场景拓扑搭建功能，拓扑搭建支持虚拟机间的链路设置，包括链路网卡、IP地址、子网掩码、网管地址、DNS、网速限制配置，支持QOS配置，可以设置丢包率及延迟时间进行设置，可设置数字VPN接入点进行演练过程中的外部用户接入；  2.支持回放位置、回放策略、回放速度的设置，可对流量的源IP地址、源端口、目的IP、目的端口进行更改配置用于重复回放配置，支持智能替换并可对流量回放速度进行自定义设置；  3.提供python在线编辑器及在线调试、流量回放在线编辑、MSF在线调试等功能；  4.支持数据采集功能，可以对仿真场景数据进行采集；  5.支持对演练事件的编排功能，通过设置事件发生轨道完成演练事件的自动化执行设置。 |
| B05 | 数据安全防护系统 | 1.实现外部攻击，漏洞攻击，SQL注入，内部窃取、越权操作、误操作，权限管控与审批等场景下的数据库综合防护；  2.可实现攻击型风险识别、防APT攻击、虚拟补丁、权限梳理、精准拦截、多维度分析、检索溯源等功能。可协助通过各种合规检测，能够实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行告警，对攻击行为进行阻断。  3.通过端口镜像或agent的方式采集所有数据库的访问流量，并基于SQL语法、语义的解析技术，记录下数据库的所有访问和操作行为，并进行风险行为告警，多重身份定位，事后溯源取证。  4.支持脱敏源和脱敏目标管理功能，具备敏感数据提供规则管理能力，能按照用户指定的部分敏感数据或预定义的敏感数据特征，在执行任务过程中，自动对抽取的数据进行识别并根据敏感数据发现规则确定敏感数据类型。可以根据各类数据应用场景如系统开发、功能测试、性能测试、数据分析等，制定不同的脱敏方案。 |
| B06 | 边界安全防护系统 | 1.含网页过滤、用户认证、应用控制、内容审计、带宽管理、行为监控分析、防私接等功能。提供基于时间、用户、应用的精细管理控制策略，提供外发信息监控审计功能、应用层的带宽管理功能，通过智能流量管理技术，有效限制P2P等应用的带宽，保证关键业务应用的带宽，避免网络拥塞和带宽资源浪费。  2.具有数据深度安全检测能力和攻击防御能力，可以识别7000+种以上的应用协议，且支持手动添加特定应用，支持深度内容检查技术，集成防火墙、VPN、应用与身份识别、防病毒、入侵防御、虚拟系统、行为管理、应用层内容安全防护、威胁情报等综合安全防御功能。  3.集成高性能病毒查杀、漏洞防护、主动防御引擎，深度融合威胁情报、大数据分析和安全可视化等创新技术，具有防病毒、漏洞管理、运维管控、基线合规检查、网络准入、终端审计、终端检测与响应（EDR）、终端数据防泄漏等安全功能。功能覆盖架构安全、被动防护、主动防御等各个安全能力阶段，深度集成了补丁管理、病毒查杀、终端管控、检测与响应、数据防泄漏等多项功能。 |
| B07 | Web应用防护系统 | 1.可以有效地缓解网站及Web应用系统面临如0WASP TOP 10中定义的常见威胁；可以快速地应对恶意攻击者对Web业务带来的冲击。让网站免遭Web攻击侵扰并对网站代码进行合理加固。  2.可根据攻击特征进行的攻击检测技术，对于攻击特征进行有效分类和组织。支持检测恶意活动，包括恶意SSL证书、钓鱼攻击、非法获取权限等，支持检测漏洞后门类攻击，包括漏洞利用、后门攻击、文件包含、缓冲溢出、目录遍历等，支持检测僵木蠕类攻击，包括木马、蠕虫病毒、僵尸网络等。  3.支持针对指定IP段，同时一键下发系统扫描、Web扫描、弱口令扫描任务，其中Web扫描能够自动发现该网段内的在线网站并开展扫描；弱口令扫描能自动发现该网段IP开放服务并自动开展弱口令扫描。支持检测的系统漏洞数不少于17万个，覆盖CVE、CVSS、CNVD、CNNVD、CNCVE、Bugtraq多种漏洞标准。 |
| B08 | 人工智能评测系统 | 包含对人工智能模型的脆弱性、隐私性、公平性、可解释性评估，并提供多维度全方位的评估报告，支持在MindSpore、PaddlePaddle等不少于2种国产主流深度学习框架，Tensorflow、PyTorch等不少于2种国外主流深度学习框架上完成对图像感知、语音识别、自然语言理解、推理决策等不少于4类超过60种智能算法的训练、评估、分析等功能；支持多模态数据在不同模型上的评估，集成不少于60种针对不同模型架构的评估方法，包括模型中毒测试、数据与模型参数窃取测试等；集成50种以上恶意样本/模型检测方法。 |
| B09 | 人工智能评测数据集 | 1.包含图像、文本、音频、表格不同模态的20种数据集。  2.包含手写数字、猫狗分类、名人人脸识别、欧美人脸识别、行人检测、金融地产新闻、体育股票描述、语音情感分类、植物特征分析、低分辨率物体分类、欧洲交通标志识别、花朵分类、环境分类、航空遥感、场景识别、高分辨率物体分类、名人人脸分类、外卖评论分析、信用评估、车辆检测、语音分类等数据类型。 |
| B10 | 人工智能模型算法资源 | 1.包含图像、文本、音频、表格不同模态的20种模型算法源码；  2.包含LeNet、DenseNet121、VGG16、AlexNet、YOLOv5、TextCNN、BERT、MLP、LogisticRegression、InceptionV1、InceptionV2、ZFNet、InceptionV3、MobileNetV1、MobileNetV2、ResNet、EfficientNet、TextRNN、LSTM、SGDClassifier算法。 |
| B11 | 攻防算法资源 | 1.包含图像、文本、音频、表格不同模态的20种自然变换方法和20种对抗攻击方法的源码；  2.包含的自然变换方法有图像缩放、图像转置、图像旋转、镜像变换、局部扭曲、大小写替换、图像素描化、图像马赛克、内容遮挡、泊松噪声、伽马噪声、指数噪声、均匀噪声等；  3.包含的对抗攻击方法有快速梯度符号、投影梯度下降、边界攻击、牛顿梯度优化、深度欺骗、矩阵攻击、信号攻击、零阶梯度优化、弹性网络攻击、几何决策攻击、协作攻击、决策跳跃攻击、目标检测快速梯度下降等。 |
| B12 | 态势感知与安全运营平台 | 可对采集到的数据进行按照不同业务模型进行分类检测，平台引用机器学习、智能分诊、关联分析、异常行为以及情报分析能力，将多元异构信息有效转化为精准告警。  基于不同场景对平台产生的告警进行进一步分析，为分析师在研判溯源环节提供能力支撑，包含自动化调查、实体分析、场景分析、QAL分析等场景，实现攻击路径的完整呈现。  涵盖平台的资产、脆弱性、风险等运营管理能力以及其他辅助合规功能，实现对于资产风险的闭环和安全运营人员的日常工作提供辅助支撑。 |
| B13 | 网络流量传感器 | 将流量数据、威胁数据进行采集、还原、解密、外发，能够对威胁情报、恶意文件、漏洞、应用识别等多种数据进行检测，可对HTTPS流量进行SSL解密、检测和还原等。 |
| B14 | 国际科研学术资源加速服务系统 | 以硬件加速产品为载体，嵌入学校校园网络，支持旁路、串接、无线等接入模式。提供加速运维管理平台，实现域名、IP白名单控制、日志监控等功能。实现谷歌学术等国际科研学术资源访问。 |
| B15 | 教科网算力云服务 | 1.云服务器+权威解析+WEB站备案+网站迁移+网站建设。  2.共享型GPU算力服务器。  3.虚拟化云电脑、云电脑管理平台。  4.信创云邮箱。为高校提供信创/国产化邮箱解决方案。 |

**四、课题申报说明**

1. 申请人须仔细阅读申请指南，按照指南详细填写申请书，填写不合要求的课题会按照格式不符合要求处理。

2. 请各课题申请人按要求填写申请书（申请书中手机和邮箱必须填写），加盖公章及签字后扫描上传至：https://cxjj.cutech.edu.cn；为方便评审，申请书扫描件请按以下命名规则命名：学校名称+申请人姓名。

3. 申请书书面材料一份，邮寄至：北京市海淀区中关村大街35号803室，教育部高等学校科学研究发展中心信息化研究发展处。

4. 申请截止时间为2025年12月15日。

5. 课题的执行时间为2026年4月1日～2027年3月31日，可根据课题复杂程度适度延长执行周期，最长不超过两年。

6. 每位申报人限报一项课题。

7. 课题选题列表上的选题方向都不限定课题数量，但是如果存在内容重复的相似课题，专家组将根据课题组技术积累、课题方案、课题支撑条件等要素择优选择资助课题。

8. 如果以联合课题组的形式申请课题，需要列明不同学校单位的课题任务。

9. 课题申请人无需向资助企业额外购买配套设备或软件。

**五、联系人及联系方式**

**教育部高等学校科学研究发展中心联系人：**

张 杰 电话：010-62514689

**赛尔新技术（北京）有限公司联系人：**

陈楚鹏 电话：18718743008

李晓霞 电话：18611627502

**奇安信科技集团有限公司联系人：**

杨 鑫 电话：18588723992

朱伶俐 电话：13601292437