

第四届网络空间安全(天津)论坛圆满闭幕

集结全球智慧 共探AI时代网络治理新路径

昨日,为期3天的第四届网络空间安全(天津)论坛在天津滨海新区圆满闭幕。近800位国内外嘉宾齐聚一堂,围绕“共建网络安全 共治网络空间”主题,参与“一主五分一会一赛”系列主题活动,持续深化网络空间国际对话与合作,共商网络空间前沿发展、共享网络安全创新成果,推动国家战略与地方实践深度融合,实现全球智慧与中国方案同频共振。

本届论坛将AI安全作为核心主线贯穿全环节,围绕技术创新、产业融合、治理升级等核心命题开展高端对话,精准回应智能时代网络安全治理课题。论坛期间,与会嘉宾从不同维度剖析现实风险,提供治理方案。

本届论坛聚焦产业一线痛点与技术前沿赛道,分领域开展精准化、实战化研讨,推动治理共识转化为行业实践,全面覆盖网络安全重点产业与关键应用场景。

同期举办的第七届天津国际反病毒大会以“重构安全防护新范式”为主题,邀请俄罗斯、美国、韩国等多国顶尖安全企业与国内行业骨干力量,围绕智能体时代新型病毒重定义、后量子时代文件安全、海量流量分析等前沿课题开展技术交流,推动全球反病毒领域协同共治、联动发展。

第四届“天网杯”网络安全大赛设置信创关键产品漏洞挖掘、人工智能安全、智能网联汽车安全三大核心赛道,通过高强度、实战化技术对抗深挖前沿安全漏洞,持续完善“以赛育才、以赛促研、以赛助产”的产学研融合模式,一批优秀的网络安全人才脱颖而出,为产业高质量发展注入新生动力。

论坛期间,《网络空间安全态势分析报告(2026)》《移动互联网应用安全统计分析报告(2026)》《暗网监测年度报告(2025)》《大模型与智能体安全综合测评报告》四大权威报告集中发布,系统梳理年度网络空间安全态势、行业风险特征与技术演进趋势,为监管部门科学决策提供数据支撑。论坛同步推出计算机病毒发展史线上展,以数字化形式全景呈现反病毒技术演进历程,打造行业历史积淀与科普传播新阵地;面向全球公开征集演讲议题,拓宽国际交流合作渠道。

昨日,中国—上海合作组织口岸经济合作中心(以下简称上合口岸经济合作中心)在天津正式揭牌成立。此举标志着天津服务上合组织国家的开放载体全面升级,正式构建起“两平台、两中心”的全新格局,将为区域互联互通和口岸经济高质量发展注入强劲新动能。

据介绍,此次在天津国际贸易与航运服务中心正式揭牌启用的上合口岸经济合作中心,作为天津深化高水平对外开放、推进上合务实合作的全新核心载体,在功能定位与核心任务上,重点聚焦三大领域精准发力。持续推动口



“AI+信创”安全发展主题论坛

“AI+信创”安全发展主题论坛锚定AI与信创深度融合、内生安全等核心议题展开探讨,推动安全能力与信创芯片、操作系统、全场景应用深度融合,助力信创产业从“可用”向“安全可信、高效好用”系统性升级。

昨日,亚信安全高级副总裁吴湘宇在论坛上指出,伴随智能体在信创场景规模化落地,安全范式要由被动抵御攻击,升级为对智能体主体的全生命周期信任治理。他认为,应建设统一的智能体安全治理平面,围绕身份、行为、审计维度,达成智能体身份可信、行为可控、责任可追溯的治理目标。

天融信科技集团助理总裁张博认为,信创已经从替代阶段迈向技术创新阶段,应该构建国产化智算基础设施,实现大模型全链路内生安全防护,同时利用AI智慧引擎、多安全智能体,升级威胁检测、研判处置,赋能信创安全运营智能化转型。

数智城市安全与治理主题论坛

数智城市安全与治理主题论坛聚焦城市全域数字化转型中的大数据、物联网、人工智能、区块链等前沿数智技术应用带来的安全问题和智慧城市安全治理面临的风险挑战,搭建“政策—技术—产业—应用”四位一体的交流平台,推动构建安全可控的智慧城市安全模式,凝聚以数智安全赋能推动城市治理体系和治理能力现代化的广泛共识。

中国星网数字科技有限公司人工

智能首席专家曹辉指出,可信数据空间作为国家重点推动的新型数据流通基础设施,坚持制度、技术、运营三位一体,依托隐私计算、区块链等技术,实现数据“可用不可见、可控可计量”,是破解数据信任与流通难题、赋能城市治理现代化的关键路径。他强调,可信数据空间能够在保障数据安全的前提下充分释放数据要素价值,为智慧城市全域监测、风险预警、统筹调度提供坚实支撑。

360数字安全集团副总裁余凯则认为,以智能体安全扩展防护边界,管住智能体的决策、执行与外部依赖,让AI既成为防御生产力,又在安全、可信、可控的边界内规模化落地。

新型威胁与攻防对抗主题论坛

新型威胁与攻防对抗主题论坛研判AI赋能下的网络威胁演化趋势,围绕APT防御体系、代码安全评估、AI威胁狩猎等实战方向开展深度技术交锋,为关键信息基础设施防护提供技术支撑。

国家信息中心信息与网络安全部政务外网安全监测处副处长陈永刚提出,政务AI应用已步入全面普及阶段,智能体逃逸、提示注入等新型风险凸显,传统防护手段难以适配。亟须构建智能体时代政务安全监测预警体系,落地事前AI审计、事中意图感知、事后全链路溯源能力,建设行业统一人工智能监测预警平台,进一步筑牢“人工智能+政务”安全防线。

中关村国家实验室科研04部部长陈庶樵,在演讲中系统描述了大

模型与智能体驱动网络攻防范式的革新,从自动化信息收集、智能化漏洞挖掘,到精准化漏洞利用与高效打点渗透,分析AI在安全攻防中的实战效能,揭示了智能技术对攻击效率的颠覆性提升,也为构建主动式、自适应防御体系提供了关键思路。

绿盟科技伏羲实验室主任吴铁军表示,当前APT攻击正逐步瓦解传统四层防御,AI供应链植入、USB隔离网渗透、地理围栏规避检测、黑灰产借道隐匿痕迹等新型威胁高发,攻击隐蔽性与溯源难度大幅提升。他建议,前移安全关口,强化开发阶段供应链校验,升级隔离网USB管控,搭建多环境动态检测,构建全链路溯源体系,进一步筑牢安全防线。

智能体安全治理主题论坛

智能体安全治理主题论坛直面智能体记忆模块、自主执行、供应链等新型技术风险,从技术防护、合规治理、产业应用多维度展开探讨,推动构建算法、数据、模型、应用全生命周期安全生态。

天津大学网络安全学院执行院长吕勇强在演讲中指出,智能体认知形成机制正由模型参数主导,扩展至预置技能与长期记忆共同驱动。智能体认知安全应界定为对认知要素全生命周期的安全保障,需系统分析技能供应链风险与记忆投毒耦合形成的攻击链,构建涵盖来源认证、完整性校验、最小权限、执行隔离的防护体系。

国家超级计算天津中心首席科学家孟祥飞针对国产超算异构性强、可靠性不足及安全响应滞后等问题,提出多智能体自主协同运维架构,实现状态实时感知、异常事件识别与自适应响应,并通过红蓝对抗演练验证主动防御能力,为提升国产超算安全运维提供技术支撑。

论坛举办期间,国家计算机病毒应急处理中心联合天津大学、天津师范大学发布《大模型与智能体安全综合测评报告》,系统梳理大模型与智能体领域的安全风险态势,为行业测评、标准制定和安全加固提供了重要依据。

图片由市公安局提供

中国—上海合作组织口岸经济合作中心在津揭牌

昨日,中国—上海合作组织口岸经济合作中心(以下简称上合口岸经济合作中心)在天津正式揭牌成立。此举标志着天津服务上合组织国家的开放载体全面升级,正式构建起“两平台、两中心”的全新格局,将为区域互联互通和口岸经济高质量发展注入强劲新动能。

据介绍,此次在天津国际贸易与航运服务中心正式揭牌启用的上合口岸经济合作中心,作为天津深化高水平对外开放、推进上合务实合作的全新核心载体,在功能定位与核心任务上,重点聚焦三大领域精准发力。持续推动口

岸通关模式创新升级,建设海关总署“智慧海关建设与合作示范点”,积极探索技术性贸易措施协调对接与标准互通,不断提升跨境通关智能化、便利化水平。持续深化海事领域对外开放与便利化合作,创新开展离岸船舶登记特色业务,全面提升涉外海事政务服务质效,从严筑牢危险货物海上运输安全屏障,保障国际航运通道安全畅通。提升滨海新区港航产业集聚区发展能级,推动港航基础设施建设、先进运营管理技术对外输出,推动港航产业要素集聚提质。依托上合口岸经济合作中心平台作用,持续深化精准合作、畅通双向对

接渠道,持续织密对上合组织国家及共建“一带一路”国家口岸合作服务网络。

下一步,天津将紧扣天津港产城高质量融合发展主线,持续对标市场化、法治化、国际化建设标准,分阶段、分层次推进上合口岸经济合作中心各项重点任务落地落实。近期将充分发挥口岸对外开放前沿阵地优势,主动融入本市“十五五”高水平对外开放布局,依托天津国际贸易与航运服务中心实体载体,以上合口岸经济合作中心为抓手,持续深化与上合组织国家多领域务实合作,聚力吸引跨境企业集聚,推动双向合作项目落地见效。

中长期将坚持以天津口岸一域服务全国大局,持续深化与上合组织国家、共建“一带一路”国家口岸经济全方位、深层次务实合作,逐步构建协同高效、互利共生的国际口岸经济产业生态圈。统筹用好绿色产业、数字经济两大合作平台和职业教育、口岸经济两大合作中心的矩阵叠加优势,持续畅通产业对接、贸易互通、物流联通、人文交流合作渠道,落地实施一批重点示范合作项目,持续擦亮天津对上合组织国家对外开放的金字招牌,全力打造北方地区高水平对外开放新高地和国际互利合作新标杆。

记者 张艳