CSA cloud security alliance®

CSA GCR GREATER CHINA REGION cloud security alliance®

CAISP™

Certified Artificial Intelligence Security Professional

人工智能安全认证专家课程介绍

CAISP™
Certified Artificial Intelligence Security Professional

课程介绍

COURSE INTRODUCTION

随着人工智能及大模型深入各行各业，人工智能及人工智能安全越来越受到重视，在此背景下,CSA大中华区推出人工智能安全认证专家（CAISP）认证培训课程，人工智能安全认证专家（CAISP）旨在为从事AI(含AI安全)的研究、管理、运营、开发以及网络安全等从业人员提供一套全面覆盖AI安全领域、跨领域综合能力培养、实践导向与案例分析、结合全球视野与法规治理的AI安全课程。

课程专注于理解人工智能安全的治理与管理环境，学习AI安全的术语与安全目标、针对于算法、模型以及数据安全和隐私进行学习，全面提升对AI安全风险的识别、评估与测评等实战化能力；课程还涵盖了AI安全的国内与国外的法律法规框架，并通过实际案例，探讨如何在组织中实施AI安全；此外，学员还将具体学习如何应对AI安全的风险与挑战，包括应对数据投毒、对抗性攻击和供应链威胁等多种安全挑战。

课程要点

LEARNING OBJECTIVES

- 全面覆盖AI安全领域，从基础知识到高级技能；
- 结合技术、法律、伦理和管理，提升AI安全综合治理能力；
- 通过实际案例和实践指导，提升解决AI安全实际问题的能力；
- 结合全球AI安全标准和法规，培养国际视野，确保企业合规性。

学习对象

LEARNING SUBJECT

- AI行业相关人员：AI工程师与开发者、AI安全工程师、AI应用的终端用户
- 安全相关人员：安全研究员、合规与风险管理科技工作者、网络安全从业者;
- 其他：政策制定者和监管机构人员、数字化转型工作人员、理工类师生

CAISP™
Certified Artificial Intelligence Security Professional

课程大纲

CURRICULUM

模块1-AI安全概述篇

- AI与AI安全基本概念
- AI与安全衍生
- 技术发展脉络

模块2-技术基础篇

- 常见AI算法与模型介绍
- AI模型与算法安全性分析
- 数据隐私保护与安全措施

模块3-安全风险篇

- 大模型安全风险概述
- 典型攻击与应对策略：提示攻击、对抗攻击、梯度泄露攻击、推理攻击、模型萃取攻击、供应链攻击、应对策略
- 防御机制解析

模块4-政策与治理篇

- 国内外AI安全法律法规、标准规范分析
- AI安全治理框架

模块5-全生命周期管理篇

- DevSecOps与AI
- AI安全需求分析与设计
- 安全的AI系统开发指南与实践
- AI安全测评框架应用
- AI渗透测试技术与方法
- AI安全运营保障体系建设

模块6-标准与评估篇

- AI安全框架
- AI成熟度模型应用与评估
- AI安全标准与测评认证实践

模块7-特别篇ChatGPT的安全影响

- 恶意行为者利用LLM的安全分析
- 防御者如何将LLM应用于网络安全
- 恶意提示词攻击的防范措施
- 企业安全使用ChatGPT的最佳实践

模块8-实践案例篇

- 现实世界中的AI安全问题深度分析
- 解决方案制定与应对策略
- 关键领域的AI安全最佳实践案例
- 行业大模型应用及安全实践案例

模块9-伦理与未来发展篇

- AI伦理道德挑战与分析
- 典型场景下的AI伦理道德风险
- 未来发展趋势

CAISP™
Certified Artificial Intelligence Security Professional

培养关键能力

DEVELOPING CORE COMPETENCIES

- **核心知识与技能构建：**培养学员在AI安全领域的扎实基础，确保其能有效应对现代数字化安全挑战。掌握识别并防御各类安全威胁，特别是应对对抗性攻击的能力。

- **AI算法与模型安全精通：**深入理解AI常用算法和模型及其安全性，强化防范对抗性攻击的技巧，实施有效防御措施，确保数据安全免受泄露。

- **大模型安全风险管理：**掌握大型AI模型的安全漏洞识别、应对策略与管理，提升对各类攻击的防御能力以及系统性评估AI安全威胁能力。

- **AI安全法规与安全治理：**全面掌握国内外AI安全相关的政策法规与标准规范及AI安全治理体系，掌握AI安全治理的方法论、整体体系架构及各模块能力，全面提升学员对AI安全治理的能力。

- **DevSecOps与AI集成安全：**融合DevSecOps原则于AI开发流程，熟练运用DevSecOps框架于AI项目中，提升开发环境中的安全实践水平，确保AI应用的安全集成与维护。

- **全生命周期AI安全管理：**掌握AI应用从需求设计到测试部署的全周期安全管理，设计安全的AI系统，执行渗透测试，强化企业AI安全实施能力。

- **大语言模型安全实践：**安全实施和管理大语言模型，专攻大语言模型（LLM）的安全应用，识别并抵御未来安全威胁，提升防御恶意利用的能力，增强风险应对策略。

- **AI安全成熟度提升：**运用AI安全成熟度模型，掌握评估与提升AI安全成熟度的方法，依据测评结果实施改进策略，全面评估并优化系统安全性能。

- **ChatGPT安全最佳实践：**掌握ChatGPT安全使用策略，在企业中安全高效地利用ChatGPT，制定并执行安全操作规范，确保技术应用的合规与安全。

- **政策法规与伦理道德：**熟悉相关政策法规，识别伦理风险，应用有效的治理机制。增强对国内外AI安全政策、法规及伦理道德的理解，促进负责任的AI发展。

对个人的价值

PERSONAL VALUE

- **专业能力提升：**学员将获得AI安全领域的深厚知识基础，有效提升识别和防御各类安全威胁的能力，尤其是对抗性攻击，增强个人在职场的竞争力。

- **技术与实战结合：**通过实际案例和实践指导，提升解决实际问题的能力，将理论知识转化为实际操作技能，促进个人技术成长与实操经验积累。

- **国际视野拓展：**结合全球AI安全标准和法规的学习，帮助个人形成国际化的视角，提升在跨国企业或国际合作项目中的适应性和价值。

- **法律法规精通：**熟悉国内外政策法规，增强伦理道德意识，为个人职业生涯树立合规操作的基石，降低法律风险。

- **职业发展加速：**获得CAISP认证，证明个人在AI安全领域的专业地位，有利于职业晋升、薪资增长以及更广泛的职业选择。

- **安全思维培养：**从设计到运营的全周期安全管理能力，使得个人能够在任何涉及AI安全的项目中发挥关键作用，成为企业不可或缺的安全专家。

对企业的价值

VALUE TO THE ORGANIZATION

风险防控强化：企业员工掌握大模型安全风险管理，有效识别并应对各类安全漏洞和攻击，减少安全事件的发生，保护企业资产和客户数据安全。

合规性保障：员工熟悉国内外AI安全政策和伦理道德，帮助企业建立合规的安全管理体系，避免法律风险，提升企业形象和社会责任感。

成本效率优化：通过DevSecOps的集成，提高AI开发流程的安全性与效率，减少因安全问题导致的修复成本和时间延误。

创新能力提升：在大语言模型安全实践与ChatGPT安全最佳实践的指导下，企业能够安全高效地利用最新技术，推动产品和服务创新。

安全化构建：培养员工在全生命周期的AI安全管理意识，形成以安全为导向的企业文化，为企业的可持续发展打下坚实基础。

竞争力增强：拥有具备CAISP认证的专家团队，企业能够在激烈的市场竞争中展现更高的安全标准和专业实力，吸引更多合作伙伴和客户信任。

CAISP™
Certified Artificial Intelligence Security Professional

培训与认证考试

TRAINING AND CERTIFICATE

CAISP证书

- **教学标准课时：**3天课程，18-20课时。

  考生获得70%以上的成绩通过考试，考试通过后，系统生成考试证书

- **培训及考试认证费用：** 6980元/人

  （其中：培训费4500元/人；考试认证费2480元/人）

考试说明

EXAMINATION INSTRUCTIONS

- **考试认证：**限时考试，题型为单选题和多选题，共60道题，必须在90分钟内完成。
- **考试入口：**https://exam.c-csa.cn 线上考试。

CAISP™
Certified Artificial Intelligence Security Professional

关于CSA大中华区CPE

CONTINUING PROFESSIONAL EDUCATION

CPE（Continuing Professional Education）是CSA对持证人员参加数字领域的持续教育、培训、研讨会等活动提供的积分奖励，CSA持证人员可用CPE积分抵扣CSA证书维持费用。鼓励每位持证人员将个人职业发展与持续学习相结合，以确保在其专业领域内始终保持最新的知识和技能，适应不断变化的行业要求和创新趋势。

CPE积分活动有哪些?

类别	具体项目	CPE分值/项
职业教育与发展	通过CSA认证考试	30
	通过其他安全认证考试	10
	参加行业竞赛，并获得奖项	10
	参加行业竞赛	5
	获得发明专利/发表国际学术论文	10
	获得软件著作权、实用新型等知识产权	5
	参与行业大会、研讨会、公开课、讲座	5
专业贡献	出版书籍 （担任书籍封面作者）	30
	出版书籍（参与书籍编写）	10
	参编专业报告（包括但不限于参与标准、报告等）	20
	授课/公开演讲	20
	翻译白皮书/外文文章	5
	发表文章（包括但不限于在公众号、网站、报纸等公开渠道）	5
志愿服务贡献	担任CSA大中华区志愿者	10
	参加其他公益组织、非盈利组织的志愿者活动	5
备注：以上项目应当属于数字技术与数字安全领域相关活动。		

CAISP™
Certified Artificial Intelligence Security Professional

CPE如何抵扣证书维持费用?

- 每个CSA CPE可抵扣10元，根据学员持有的CSA认证证书数量，可抵扣最高1000元/项或1500元/项。

  请见下表：

	证书维持费用原价/项	最高抵扣金额/项	备注
当学员持有1-2项CSA认证证书	2000元	1000元	每个证书最高可抵扣100个CPE（等同1000元），所以证书维持费用最低至1000元。
当学员持有3项及以上CSA认证证书	2000元	1500元	每个证书最高可抵扣150个CPE（等同1500元），所以证书维持费用最低至500元。
说明： （1）在证书有效期内，CSA持证学员参加活动获得的CPE积分，可同时累积至1项或多项当前有效期的证书上。 （2）如参加的CPE活动不在某个证书有效期内，则不适用于该证书累积CPE积分。			

CPE适用于哪些CSA认证证书?

- CZTP 零信任认证专家
- CDSP 数据安全认证专家
- CBP 区块链专业人员认证
- CCPTP 云渗透测试认证专家
- CDPO 认证数据保护官
- CAISP 人工智能安全认证专家

如何申报CPE?

- 学员登录CSA大中华区认证与考试系统 （网址：https://exam.c-csa.cn），右上角点击“证书维持”，可以查看CPE积分活动、申报CPE、证书维持续费及下载新证书。

云安全联盟大中华区

官网：https://c-csa.cn

电话：0755-86548359

秘书处邮箱：info@c-csa.cn

地址：上海市浦东新区东育路255弄5号3FB30(前滩国际经济组织集聚区)/

广东省深圳市南山区粤海街道北京航空航天大厦1号楼905

扫码关注
获取更多信息