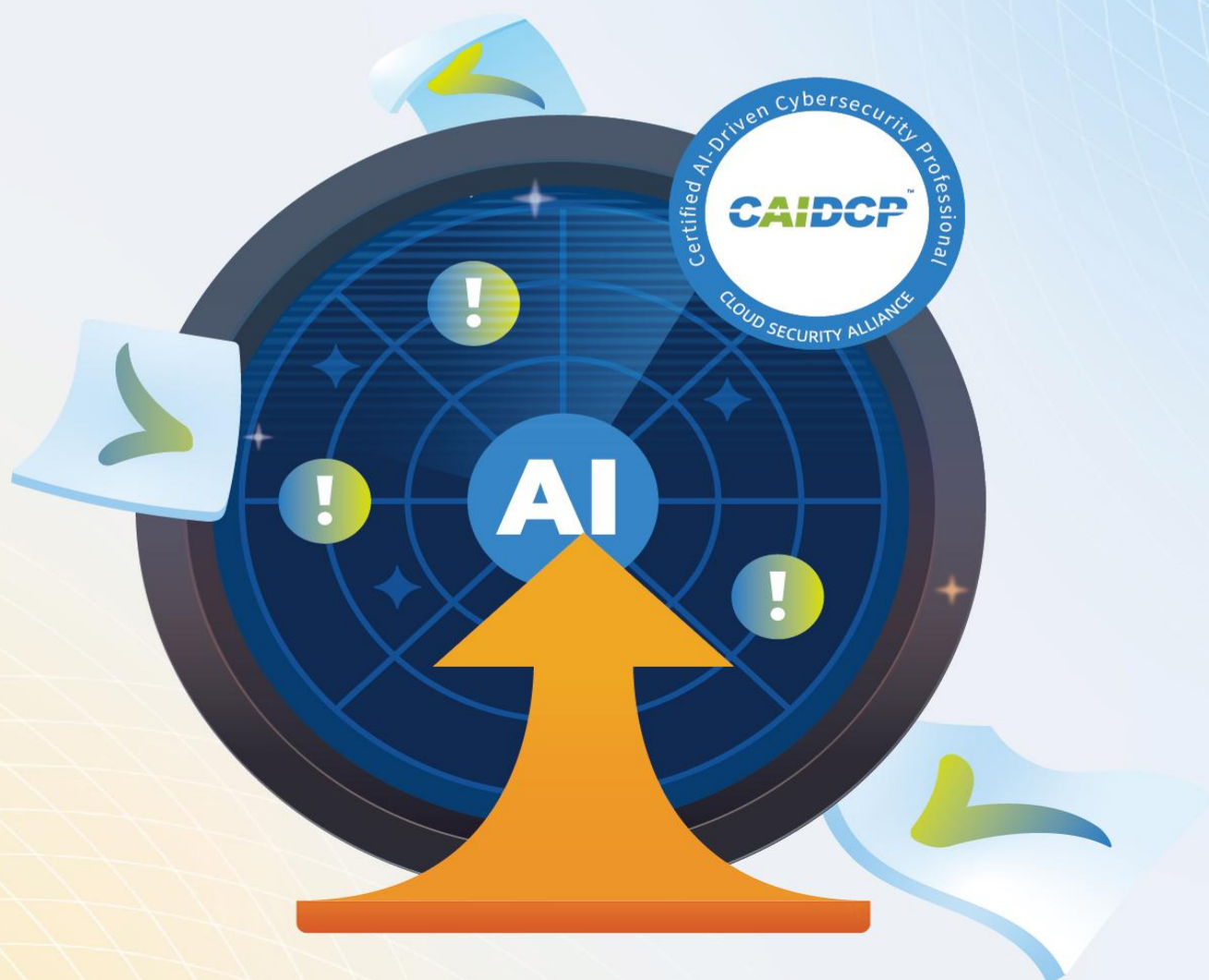


AI驱动安全专家认证

Certified AI-Driven Cybersecurity Professional

课程介绍



认证机构



国际云安全联盟

Cloud Security Alliance (CSA)

国际云安全联盟（CSA）创立于2009年，作为世界领先的独立、权威国际产业组织，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识和全面发展，在全球范围内与其他国际组织机构、政府、高校、企业开展深入而广泛的合作中，以其中立性、敏捷性和专业性被各界认可，是云计算领域的“ISO”、“ITU”国际标准组织。

云安全联盟大中华区（CSA GCR）作为CSA全球四大区之一（其它大区为美洲区、亚太区、欧非区），是在中国工信部、公安部、网信办支持下首家注册备案的国际非营利组织。

CSA GCR立足于中国，作为国际桥梁联接世界，致力于构建国际数字安全的生态体系。

CSA组织行业协会、政府、企业及其从业者和个人成员的专业知识，提供特定于云安全和下一代数字技术安全的研究、教育、认证、活动。通过CSA平台，使CSA成员及社区所有成员各方可以共同工作，相互受益。



4大区运营实体



1000+企业会员



100+分支机构



60+研究工作组



10万+个人会员



6000+研究专家

CSA正式成立，发布了全球首个全面的云安全最佳实践《云计算关键领域安全指南》

2009

发布云安全领域黄金标准云控制矩阵CCM，推出云计算安全知识认证CCSK

2010

欧盟、美国云计算战略在CSA峰会上发布

2011

推出全球权威云安全评估认证CSA STAR

2013

在中国推出CSA的C-STAR认证

2015

发布云安全系统认证专家CCSSP

2017

推出CSA GDPR首席认证审计师课程，受欧盟国家认可

2019

发布零信任认证专家CZTP，推出针对企业的GDPR合规自检和第三方认证

2020

发布数据安全认证专家CDSP，以及区块链专业人员认证CBP

2021

发布认证数据保护官CDPO，云应用安全可信认证CAST和云原生安全可信认证CNST

2022

发布云渗透测试认证专家CCPTP，并推出零信任认证专家CZTP2.0

2023

发布数据安全认证专家CDSP2.0，人工智能安全认证专家CAISP

2024

发布AI安全驱动专家认证CAIDCP

2025

AI 安全行动

集结全球权威专家，开发 AI 安全指南工具，助力组织合规部署 AI 方案，并通过敏捷计划及全球资源推进最佳实践与工具推广。



全球标准制定者：定义AI安全基准

首创AI安全测试框架：2024年联合蚂蚁集团、微软、谷歌等编写AI STR系列标准，在27届联合国科技大会上发布，为AI开发提供安全“标尺”。

- 《生成式AI应用安全测试标准》
- 《大模型供应链安全要求》
- 《大语言模型安全测试方法》



国际人才认证：培养AI安全实践人才



CAISP认证（AI安全专家）

识别AI风险，提高AI安全建设能力（攻防/合规/审计）。



CAIDCP认证（AI驱动安全专家）

助力安全人员掌握 AI 驱动技术（开发/测试/运营），以及助力IT人员应用AI技术增强网安技能。

顶尖智库与全球协作

CSA汇聚了谷歌、微软、亚马逊、阿里、腾讯、Anthropic、OpenAI 等科技巨头，以及 政府机构、学术界和1500余名行业专家，组成全球规模最大的AI安全协作网络。



(部分合作伙伴)



课程介绍

COURSE INTRODUCTION

人工智能（AI）作为第四次工业革命的核心引擎，正深刻重塑全球产业格局。在此进程中，掌握 AI 底层逻辑与应用方法论，已成为顺应技术浪潮、构建未来核心竞争力的战略路径。

AI 驱动安全专家认证课程（CAIDCP） 立足 AI 与网络安全的交叉创新领域，致力于系统培养 “AI 技术 + 网络安全” 的复合型专业人才。课程全面覆盖 AI 驱动网络安全系统的全生命周期实践，通过理论与实战结合的系统化训练体系，深度传授新一代智能防御体系的方法论与实践经验。

课程亮点

COURSE Highlights

- **理论与实践并重：**结合最新AI理论和工具在实际安全场景中的应用
- **全生命周期覆盖：**从需求→规划→设计→开发→测试→运营的完整流程
- **行业框架导向：**基于MITRE ATT&CK、OWASP、NIST CSF、STRIDE等权威框架
- **实操项目丰富：**涵盖安全设计、代码审计、威胁检测等多个实操项目，学员将亲自动手操作，运用 AI 工具和技术解决真实的安全问题。
- **前沿技术融合：**涵盖后量子密码、对抗攻击等新兴技术领域。

学习对象

LEARNING SUBJECT



安全从业与技术实践者

- 希望提升 AI 驱动安全领域专业技能，以提高工作效率与自动化水平、增强威胁应对能力，更好地应对复杂网络风险。

- 角色：SOC分析师/工程师、安全工程师、安全分析师、渗透测试工程师、威胁分析师、漏洞研究员、事件响应专员、安全架构师、安全顾问、安全运维、DevSecOps工程师、安全自动化工程师、安全研发工程师等安全相关人员；



安全战略与决策管理者

- 掌握先进 AI 安全技术与管理方法，洞悉 AI 对安全产品及防御模式的重塑，助力企业告别“大而全”的资源浪费，以精准有效的 AI 安全方案实现降本增效。

- 角色：CISO, CIO, CTO, IT总监/经理、安全总监/经理、安全合规负责人、风险管理总监/专员、产品总监/经理（安全产品）、业务线负责人/总监、采购经理（负责安全采购）、内部审计师（IT/安全方向）、外部审计顾问、合规官等；



能力拓展与职业转型者

- 希望将现有技能迁移至 AI 安全领域或奠定入行基础，以拓宽职业发展路径，把握 AI 与安全融合的新机遇。

- 角色：传统IT运维/开发/网络工程师、数据科学家、机器学习工程师、安全厂商的售前/售后/研发/产品/市场人员、应届毕业生、相关专业在校生、寻求跨领域发展的专业人士（如法律合规人员想懂技术基础）等。

课程目标

COURSE Objectives

知识目标

构建AI安全底层认知

掌握 AI 在网络安全中的应用场景、技术演进，明晰人才能力需求。

全流程安全知识覆盖

贯通 AI 驱动网络安全全生命周期方法论，掌握全流程技术逻辑与工具。

前沿技术与伦理认知

解析后量子密码对 AI 安全影响，理解 AI 伦理框架与合规治理要求。

技能目标

AI 驱动安全系统落地能力

完成 AI 驱动安全需求分析与设计，输出可落地方案，用 AI 工具解决实际问题。

全流程技术实操能力

掌握 AI 驱动安全编码规范，修复代码漏洞，借 AI 技术提测试攻防效率。

智能运营与决策能力

搭建 AI 安全运营体系，用 AI 优化应急响应，缩短响应时间、降误判率。
素养目标

素养目标

伦理与合规思维

树立 AI 安全伦理意识，建合规治理思维，应对监管挑战。

跨领域整合与前瞻视野

培养 “AI + 安全” 跨界能力，预判技术融合趋势，设计演进安全架构。

工程化与问题解决能力

构建工程化思维，以系统性方法解决复杂安全问题，强化攻防实战敏捷响应。

课程大纲

CURRICULUM

认知篇

模块1-AI驱动的安全体系

- AI安全在网络空间安全的现状
- AI安全如何满足网络空间安全需求
- AI驱动的安全体系分级实现
- AI驱动的安全体系在各领域应用
- AI安全对网络安全人才职责要求

实践篇·AI驱动
安全全生命周期

模块2-AI驱动的安全需求

- AI需求管理优势与价值
- AI驱动的需求管理框架
- AI驱动的需求管理要点
- AI驱动的需求挑战未来

模块3-AI驱动的安全规划

- AI安全规划目标与目的
- AI安全规划实施思路
- AI安全规划 建立AI管理体系
- AI安全规划 建立AI安全评估体系
- AI安全规划 建立AI安全技术体系
- AI安全规划 建立安全AI技术体系

模块4-AI驱动的安全设计 模块5-AI驱动的安全开发 模块6-AI驱动的安全编码 模块7-AI驱动的安全测试

- AI驱动的安全范围设计
- AI驱动的安全整体设计原则
- AI基础设施层安全设计
- AI数据与模型层设计
- AI应用层安全设计
- 迈向AI驱动安全新范式
- 传统安全开发与TDD
- AI驱动的安全开发
- 安全编码的引言
- AI在软件编码的变革
- AI辅助生代码的风险
- 安全编码规范实例
- 传统安全测试
- AI辅助安全测试
- AI驱动安全测试

模块8-AI驱动的安全运营 模块9-AI在威胁检测中的应用 模块10-AI在应急响应中的应用 模块11-知识库与智能检索

- 现状分析与传统挑战
- AI赋能安全运营
- 智能运营系统的落地实践
- 传统威胁检测的局限性
- 机器学习威胁检测方法
- 深度学习模型实践
- AI威胁检测面临的挑战与未来方向
- 网络安全应急响应概述
- 传统应急响应的挑战
- AI在应急响应各阶段的应用
- 核心AI技术在应急响应中的实践
- AI辅助应急响应面临的挑战
- 安全运营的知识挑战与机遇
- 智能知识库的构建：基石与架构
- 智能检索的核心技术：智慧之源
- 智能检索在安全运营中的应用实践

模块12-AI+安全的高级应用

- 新范式：工程化构建安全可控的AI智能体
- 新动能：从人工渗透到自主的攻击模拟
- 新中枢：迈向自主运营的SOC与主动防御
- 动手实验：构建安全事件时间线自动梳理与可视化工具

模块13-AI伦理与合规

- AI伦理基础与伦理框架
- AI伦理矛盾与伦理挑战
- AI伦理协作与分层治理
- AI伦理未来与突破方向

模块14-AI驱动的未来与展望

- 未来发展趋势综述
- 自动化安全与AI系统自愈
- Cyber技术与AI发展
- AI安全与量子计算

课程价值——一个人：抢占 AI 安全黄金赛道，解锁职业新高度

Course Value - Enterprise

技能壁垒构建：从“传统安全”到“AI 安全专家”的质变

- **复合知识体系**：掌握 AI 技术在安全全流程核心原理与方法，构建“AI + 安全”跨域知识框架。
- **全周期工程实践**：通过真实项目实操，深度参与 AI 驱动网络安全全生命周期。
- **权威认证背书**：完成考核获 CAIDCP 认证，掌握 AI 在网络安全中的实践能力，竞争力远超传统从业者。

职业路径拓宽：多维度岗位机会与薪资跃升

- **适配高价值方向**：覆盖 SOC 分析等前沿岗位技术，支持向技术管理岗转型。
- **增强行业竞争力**：聚焦 AI 安全稀缺性，一线 AI 安全工程师年薪 30 - 80 万，提升职业适配性。
- **转型跳板**：为传统 IT / 安全从业者等提供系统化转型知识，抓住“AI + 安全”行业机遇。

持续学习：关注前瞻技术与伦理思维

- **技术前瞻性**：学习自动化安全与 AI 系统自愈；Cyber 技术与 AI 发展；AI 安全与量子计算等前沿技术能力，适配未来技术演进节奏，保持能力先进性。
- **伦理合规素养**：掌握 AI 在伦理协同，分层治理和工具落地的多维度能力，实现 AI “可控、可审、可信”的伦理价值平衡。

课程价值——企业：AI 驱动安全新基建 “降本增效 + 风险可控”

Course Value - Individual

战略价值：构建智能时代的核心安全竞争力

- **抢占 AI 安全市场增长红利**：企业快速切入数字经济 “新蓝海”，形成差异化竞争优势。
- **支撑智能化转型的安全底座**：企业AI业务变革，认证人才能为这些创新提供可信、安全的技术支撑。
- **提升安全战略的前瞻性与系统性**：获得专业训练的员工能够从全生命周期、系统思维、AI伦理等角度参与战略安全决策，帮助企业规避未来风险。

运营价值：提升团队效能与攻防能力

- **优化安全运营中心（SOC）的智能化水平**：认证人才可应用AI辅助事件检测、行为分析、自动响应等能力，推动安全运营向 “数据驱动+智能协同” 演进。
- **提升威胁预测与响应速度**：认证人才具备AI威胁建模、日志智能分析、对抗样本检测等技能，显著提升安全响应效率。
- **助力企业通过国际合规审查**：例如GDPR、ISO 42001等越来越关注AI治理，拥有专业认证人才是满足合规要求的有效加分项。

品牌价值：提升企业声誉与国际影响力

- **树立 “可信AI安全实践者” 的品牌形象**：在外部交流、客户审计、政府合作中，展示认证专家队伍，可增强客户信任与市场认可。
- **提升企业在产业链中的议价与主导权**：拥有AI安全专家代表企业具备前沿安全能力，在大型项目招投标、产业联盟中具备话语权。
- **推动企业进入国际化人才与技术生态**：认证往往与国际机构（如WDTA、CSA GCR）连接，企业可借此拓展全球资源网络与影响力。

培训与认证考试

TRAINING AND CERTIFICATE



CAIDCP证书

● **教学标准课时：**24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。

● **考试入口：**<https://exam.c-csa.cn> 线上考试。

课程专家组 (排名不分先后)

CURRICULUM



李岩

CSA大中华区专家委员会专家
CSA大中华区CAISP授权讲师
CSA大中华区CDSP授权讲师
CSA大中华区CCSK授权讲师



崔崑

微软全球技术专家工程师
清华工程物理本科+自动化系博士
物联网安全公司创始人&CSO
CSA全球报告核心主笔
CSA大中华区CAISP授权讲师



张镇

启明星辰网安学院院长
全国安全竞赛体系构建者
带队HW攻击方全国季军
清华出版网安专著主编
资深安全实战专家、讲师



刘广坤

北京天际友盟信息技术有限公司
CTO
某知名高校信息安全工程学院特聘
讲师
某知名民营大学校外导师
中国网络安全产业联盟(CCIA)专家



江泽鑫

珠江科技新星&华为难题揭榜奖
百项专利电力安全技术专家
清华硕士·工控网安专家
动车列控系统研发专家
电力网安标准制定者



潘万鹏

中兴通讯产品安全总监
保障中兴终端安全与隐私保护
web、移动、IOT三大安全领域
17+安全专利与认证专家
自主研发安全扫描工具



王思远

全球汽车零部件安全负责人
网信办+信通院双料安全专家
新能源车企安全体系奠基者
上海网安工匠得主、年度十佳CSO
多领域安全智库专家



贺志生

360资深安全专家
前中国电科某研究院常务副所长
高级工程师(网安领域)
北京网络空间安全协会学术理事
及高工团专家



温志宇

全国数安产教融合副秘书长
启明星辰教学中心负责人
北交大电子信息企业导师
全国网安攻防竞赛体系专家
安全人才培养高级专家



张淼

世界五百强网络安全总监
国际隐私保护协会院士
云安全联盟高级安全专家
曾荣获云安全联盟年度领军人奖



刘雨沆

达摩院AI训练师
M-Wiki创办者
某部委特聘讲师
两届全球红队通关者
AI安全多部指南作者

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。		

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。 详见下表：

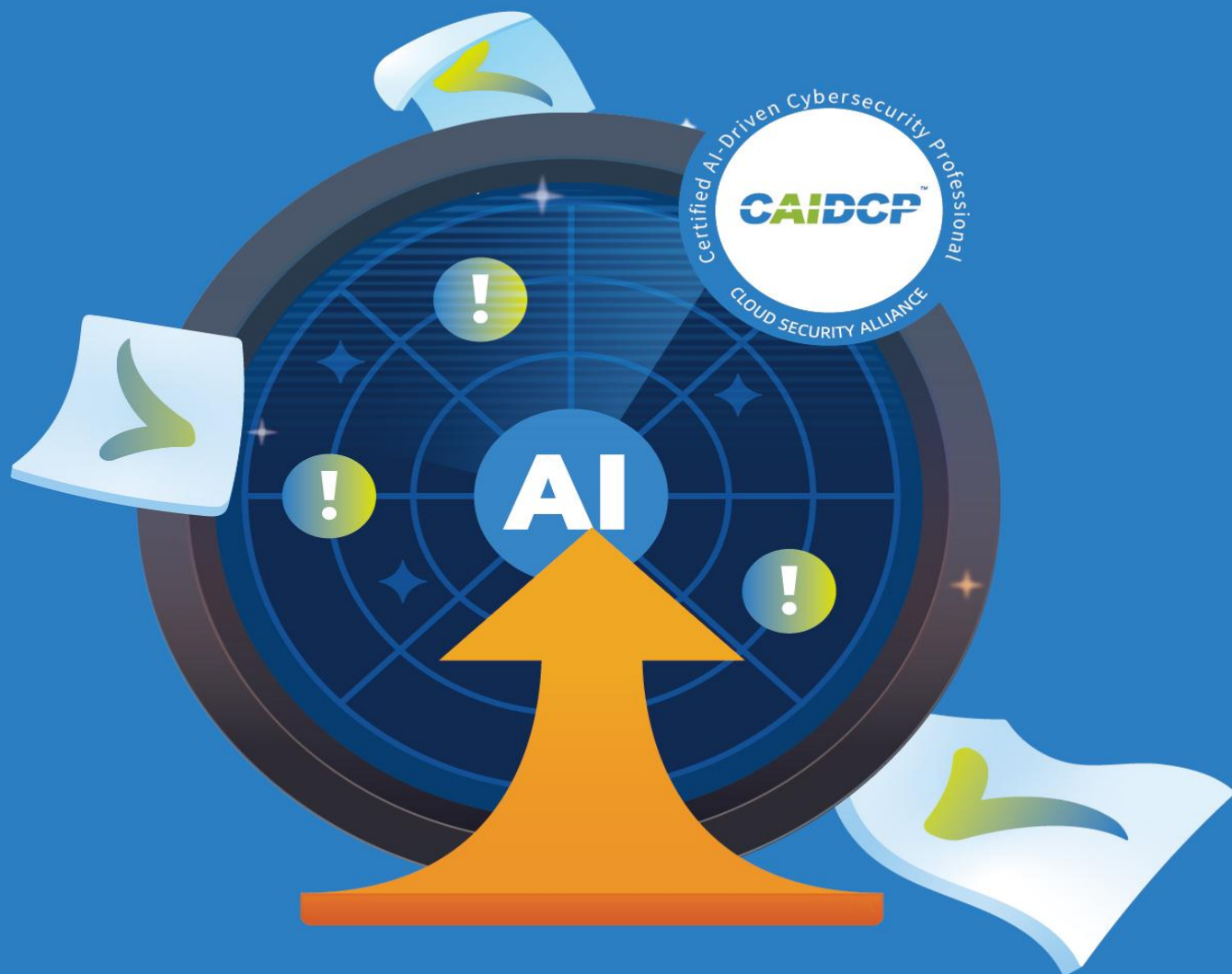
	证书维持费用 原价/项	最高抵扣金额/ 项	备注
当学员持有1-2项 CSA认证证书	2000元	1000元	每个证书最高可抵扣100个CPE（等同1000元），所以证书维持费用最低至1000元。
当学员持有3项及以上CSA认证证书	2000元	1500元	每个证书最高可抵扣150个CPE（等同1500元），所以证书维持费用最低至500元。
说明： （1）在证书有效期内，CSA持证学员参加活动获得的CPE积分，可同时累积至1项或多项当前有效期的证书上。 （2）如参加的CPE活动不在某个证书有效期内，则不适用于该证书累积CPE积分。			

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 AI安全认证专家
- CAIDCP AI 驱动安全专家认证

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深圳湾科技生态园9栋B4座603单元



扫码关注
获取更多课程信息