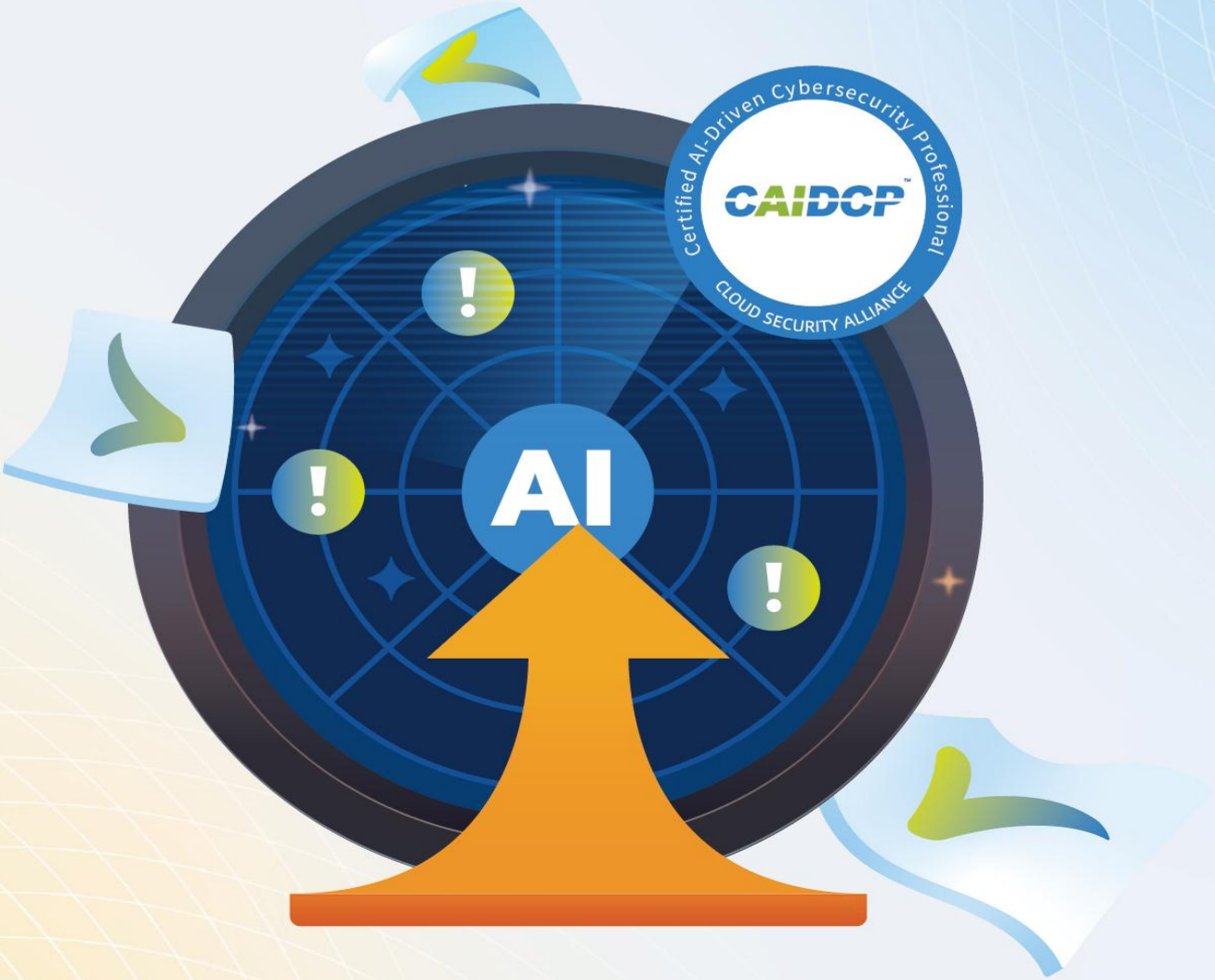
AI驱动安全专家认证

Certified AI-Driven Cybersecurity Professional

课程介绍



CSA cloud security alliance®

CSA GCR GREATER CHINA REGION cloud security alliance®

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

100+分支机构

10万+个人会员

1000+企业会员

60+研究工作组

6000+研究专家

2009 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》**

2010 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**

2011 欧盟、美国**云计算战略**在CSA峰会上发布

2013 推出全球权威云安全评估认证**CSA STAR**

2015 在中国推出**CSA**的 **C-STAR认证**

2017 发布云安全系统认证专家**CCSSP**

2019 推出CSA **GDPR首席认证审计师**课程，受欧盟国家认可

2020 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

2021 发布数据安全认证专家**CDSP**，以及区块链专业人员认证**CBP**

2022 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**

2023 发布云渗透测试认证专家**CCPTP**，并推出零信任认证专家**CZTP2.0**

2024 发布数据安全认证专家**CDSP2.0**，人工智能安全认证专家 **CAISP**

2025 发布AI安全驱动专家认证**CAIDCP**

CSA GCR 云安全联盟大中华区

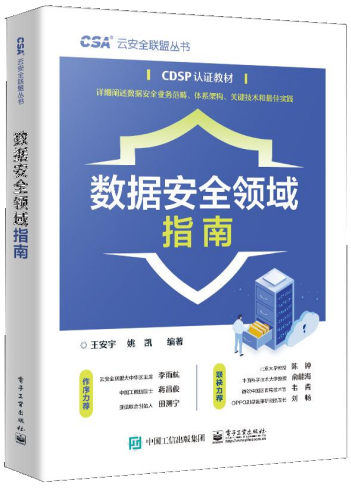
CSA GCR cloud security GREATER CHINA REGION alliance®

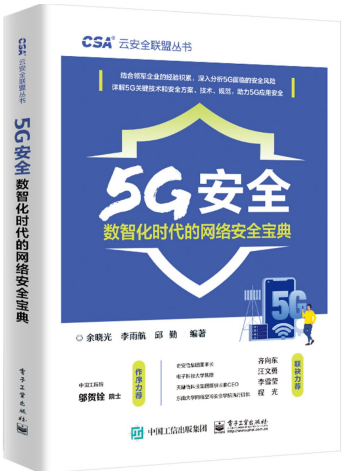
CSA数字安全人才认证与培训体系：

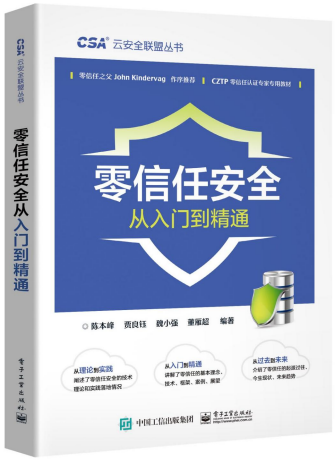
CSA 安全人才认证

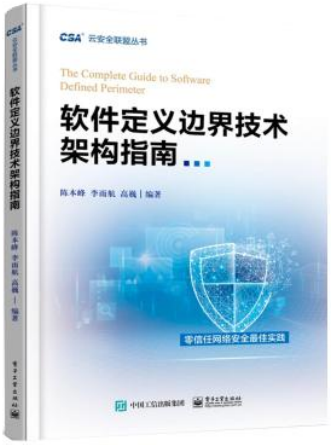
云计算安全		企业网络安全		数据安全防护		安全+AI	
CCSK 云计算安全知识认证 （通识理论）	CCPTP 云渗透测试专家 （渗透测试） CCAK 云计算审计知识认证 （审计能力）	CCZT 零信任能力证书 （通识能力）	CZTP 零信任认证专家 （设计能力）	CDSP 数据安全认证专家 （安全建设）	CDPO 认证数据保护官 （合规能力）	CAIDCP AI驱动安全专家认证 （应用能力）	CAISP AI安全认证专家 （设计能力）

已出版









CSA大中华区在电子工业出版社开设“云安全联盟丛书”，**丛书方向覆盖云安全、数据安全、5G安全、零信任等前沿技术方向。**既可用于CSA认证课程和社会教育所用教学参考书，也可以作为产业界的专业安全读物。

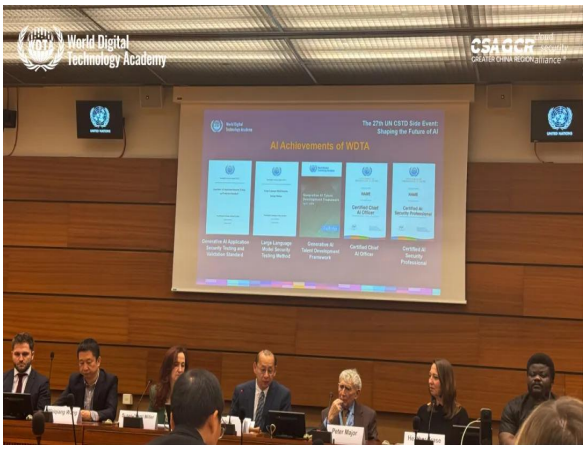
AI 安全行动

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)

CAIDCP™

Certified AI-Driven Cybersecurity Professional

“AI 驱动安全”是指利用人工智能(AI)技术，变革网络安全的策略、架构、实践等，实现网络安全管理全流程的自动化、智能化和动态自适应能力。在AI驱动安全的模式下，安全系统能够自主学习、分析和应对复杂的安全威胁，突破传统安全防护依赖人工的局限，构建起具备自主决策能力与持续进化属性的网络安全新范式 。人才掌握AI底层逻辑与应用方法论是顺应技术浪潮、构建未来生存力的核心路径。

课程介绍

COURSE INTRODUCTION

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

- **构建网络安全全局观**：突破单一技能训练，系统串联网络安全的业务需求、技术逻辑与管理机制，帮助学员建立体系化认知。
- **覆盖安全全生命周期**：课程完整覆盖从**需求→规划→设计→开发→测试→运营→审计**的全生命周期，帮助学员全面理解和掌握安全建设各阶段的关键要素与联动关系。
- **掌握新形态AI应用技能：**课程紧跟AI技术发展，深度解析如何在安全软件开发生命周期各环节中应用生成式AI与自动化技术，以提升效率与效果。
- **实战驱动的项目教学**：课程设置多个高度贴近真实业务场景的实操项目，学员将在导师指导下动手实践，应用AI工具解决实际安全问题，强化技能转化与实战经验积累。
- **解析前沿AI驱动案例**：邀请大型科技企业的资深专家，分享AI驱动网络安全的典型落地案例，帮助学员理解AI技术在不同行业、不同场景中的实战路径“学以致用”。

CAIDCP™

Certified AI-Driven Cybersecurity Professional

课程体系

COURSE FRAMEWORK

认知篇：以**AI驱动安全体系**为导入，说明“AI 驱动安全”的定义及演变并举例；

实践篇：开启AI驱动安全的全生命周期：以**AI驱动安全需求**为内核→**AI驱动安全规划**确定产品开发整体思路→**AI驱动安全设计**+**AI驱动安全开发**+**AI驱动安全测试**用AI来实现完整产品开发过程→产品投入使用，以**AI驱动安全运营**→审计人员以**AI驱动安全审计**更好的审查分析；

未来篇：以**AI驱动安全伦理**为背景，还融合**AI驱动安全高级应用**的实操实验，并展望**AI驱动安全未来**的发展趋势；

CAIDCP™

Certified AI-Driven Cybersecurity Professional

课程大纲

COURSE CURRICULUM

模块1-AI驱动安全体系

了解“AI驱动安全”的定义，学习“AI辅助安全→AI赋能安全→AI驱动安全”的演变及各阶段特点。AI驱动安全在各领域的应用举例，明确AI安全对网安人能力要求。

模块2-AI驱动安全需求

理解“AI驱动安全需求”的价值与要点，学习框架与内容，掌握如何做好需求管理，展望AI驱动需求的挑战与未来。

模块3-AI驱动安全规划

了解“AI驱动安全规划”的目标与实施思路，学习利用AI驱动建立规划的管理体系、评估体系、技术体系等。

模块4-AI驱动安全设计

了解“AI驱动安全设计”的定义与要点，原则与组成部分，掌握不同层级内容如何用AI来驱动设计的能力。

模块5-AI驱动安全开发

对比传统安全开发与“AI驱动安全开发”，了解安全开发发展方向与趋势，学习AI驱动安全开发案例与工具，掌握AI驱动开发的能力。

模块6-AI驱动安全测试

对比分析传统安全测试与现阶段AI辅助安全测试的发展与变革，掌握AI驱动安全测试的能力，了解未来AI驱动安全测试的发展核心与挑战。

模块7-AI驱动安全运营

对比传统安全运营与先阶段AI辅助安全运营的变革分析，学习AI在威胁检测、应急响应等环节中的应用与实践。

模块8-AI驱动安全审计

明确“AI驱动安全审计”的定义与要点，学习AI驱动安全审计的步骤流程以及任务拆解。

模块9-AI驱动安全伦理

学习AI伦理基础与框架，了解AI伦理矛盾与挑战，协作，治理及未来发展。

模块10-AI驱动安全高级应用

学习并实操工程化安全可控的智能体，掌握渗透测试从传统到智能化转变并迈向主动运营的SOC与主动防御。

模块11-AI驱动安全未来

了解AI驱动安全的未来发展趋势，学习自动化安全与AI系统自愈。

CAIDCP™

Certified AI-Driven Cybersecurity Professional

学习对象

LEARNING SUBJECT

安全战略与决策管理者

- **希望掌握先进 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；

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;

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。

CAIDCP™

Certified AI-Driven Cybersecurity Professional

课程价值-个人

抢占 AI 安全黄金赛道，解锁职业新高度

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系统白愈；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。

CAIDCP™

Certified AI-Driven Cybersecurity Professional

课程价值-企业

AI 驱动安全新基建“降本增效 + 风险可控”

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。

CAIDCP™

Certified AI-Driven Cybersecurity Professional

培训与认证考试

TRAINING AND CERTIFICATE

CAIDCP证书样式

- **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。

CAIDCP™

Certified **AI-Driven Cybersecurity Professional**

课程研发专家组 (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

崔鉴

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

魏明业

中兴通讯产品安全高级工程师
中兴终端产品安全能力中心运营经理
资深产品安全、数据合规、AI安全讲师

王思远

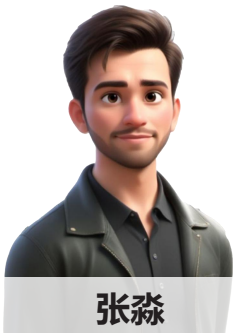
全球汽车零部件安全负责人
网信办+信通院双料安全专家
新能源车企安全体系奠基者
上海网安工匠得主、年度十佳CSO
多领域安全智库专家

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

CSA大中华区专家委员会专家
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

CAIDCP™
Certified AI-Driven Cybersecurity 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。		

CAIDCP™
Certified AI-Driven Cybersecurity 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。 详见下表：

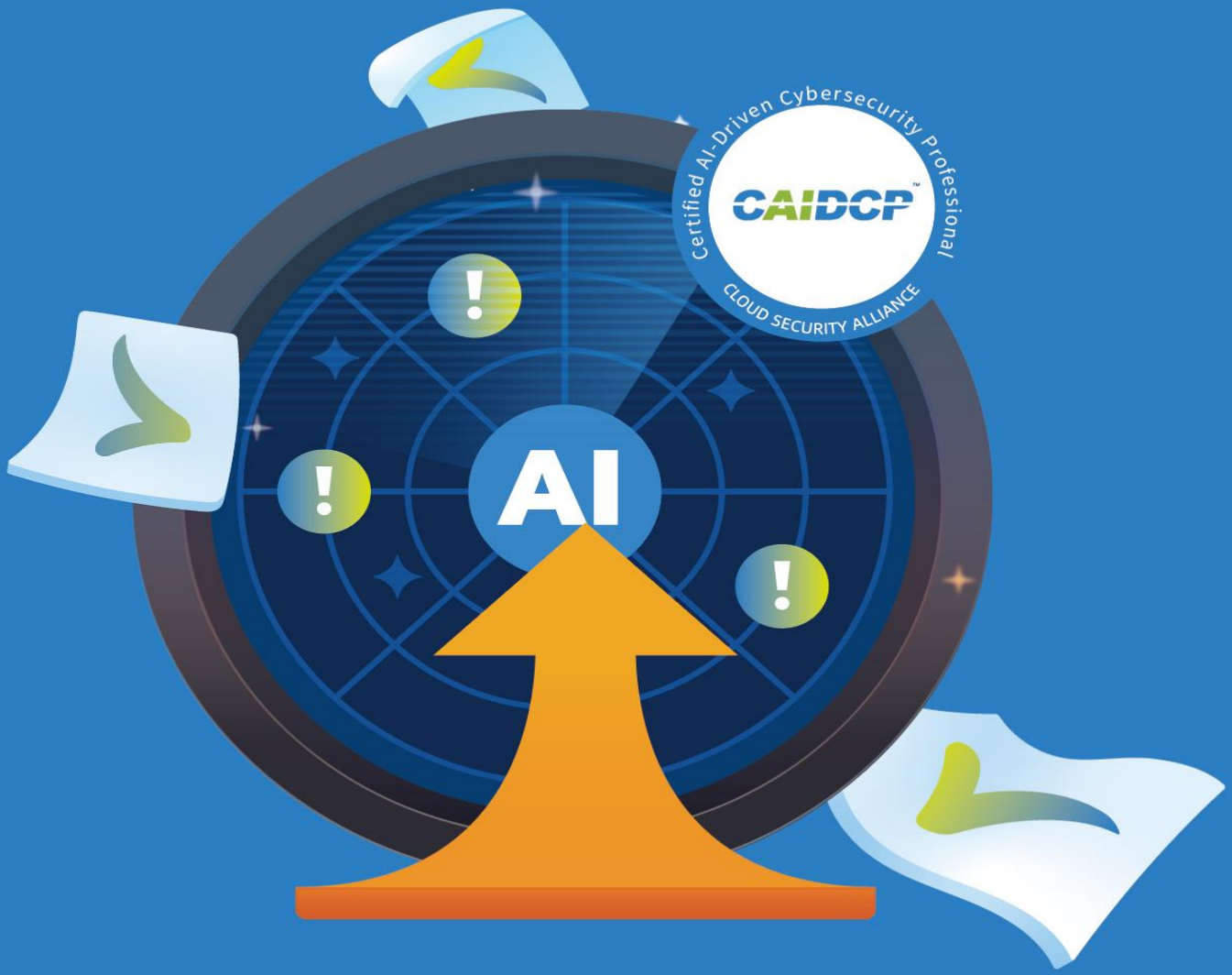
	证书维持费用原价/项	最高抵扣金额/项	备注
当学员持有1-2项CSA认证证书	2000元	1000元	每个证书最高可抵扣100个CPE（等同1000元），所以证书维持费用最低至1000元。
当学员持有3项及以上CSA认证证书	2000元	1500元	每个证书最高可抵扣150个CPE（等同1500元），所以证书维持费用最低至500元。
说明： （1）在证书有效期内，CSA持证学员参加活动获得的CPE积分，可同时累积至1项或多项当前有 效期的证书上。 （2）如参加的CPE活动不在某个证书有效期内，则不适用于该证书累积CPE积分。			

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