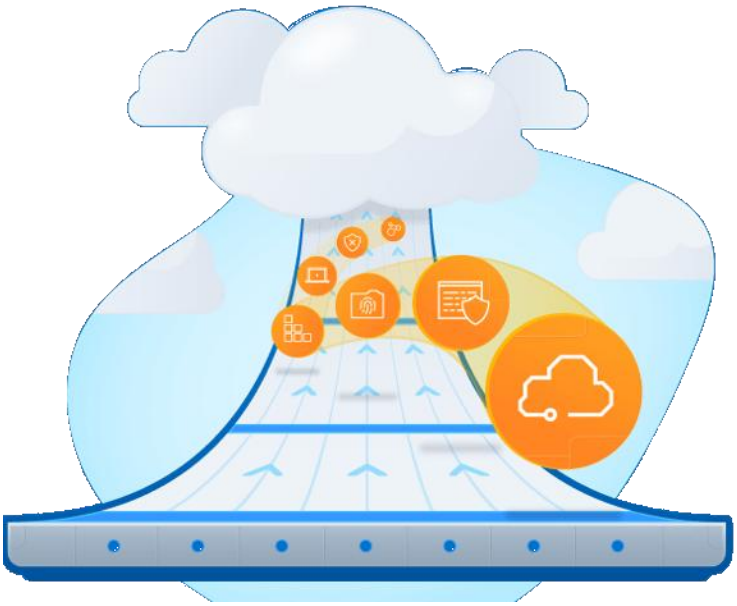
cloud security alliance

Certified Zero Trust Professional（CZTP）

零信任认证专家

面向新一代网络及新业务场景的新理念及信息安全知识体系，保障企业数字化转型、打造可持续数字化竞争力 。



https://c-csa.cn/training/course/

CZTP™
Certified
Zero Trust Professional

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 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**，以及推出针对云产品的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**

零信任认证专家

课程介绍

CZTP（Certified Zero Trust Professional）零信任认证专家由国际云安全联盟CSA于2020年发布，是零信任领域首个面向从业人员的安全认证，涵盖最新的国际零信任架构技术与系统的实践知识，旨在为网络信息安全从业人员在数字化时代下提供零信任全面的安全知识，培养零信任安全思维与实战能力，为企业守护核心数字资产。

2023年11月，CSA升级发布CZTP 2.0版本，CZTP 2.0知识面更加全面，完整涵盖了零信任的所有方面，从理论到实践，从入门到精通，从总结过去到未来展望；课程内容更偏实战，增加了不同行业的案例，强调零信任的落地实战经验。

CZTP持续保持课程国际领先性、知识系统完整性，培养具有数字安全战略思维，架构思维及零信任安全实战能力的产业级专业人才，为数字安全的创新、零信任产业发展，提供人才支撑保障。

认证价值

- **能力证明：**证明持证人员在零信任领域上的能力
- **就业机会增加：**安全职业生涯提供更多选择的可能
- **能力提升：**获得全球顶尖的系统的零信任知识，可以全面掌握全球先进的零信任理论知识，SDP、IAM、微隔离等核心的技术及部署实践知识
- **持续学习：**获取宝贵的职业提升资源，包括交流想法、工具和与同龄人建立联系，并且在国际社区中持续学习。

课程目标

- 了解零信任基本概念、发展趋势
- 熟练掌握IAM、SDP、MSG优劣势
- 学习零信任与新兴技术的应用融合与发展

CZTP®
Certified
Zero Trust Professional

课程大纲

模块1-为什么是零信任?

- 安全现状
- 零信任架构的发展历程
- 零信任的安全定义
- 基本原则与战略

模块2-零信任安全基本概念

- 架构概述
- 身份管理与访问控制技术
- 软件定义边界技术
- 微隔离技术
- 辨别零信任产品

模块3-IAM身份管理与访问控制

- IAM基本概念
- 身份管理
- 登录认证
- 访问控制
- 审计风控
- IAM发展趋势展望

模块4-SDP 软件定义边界

- SDP的技术演进
- SDP的基本架构与核心技术
- SDP的部署方式
- SDP主要功能和应用场景
- SDP替换VPN场景
- SDP与十二大安全威胁
- SDP与传统产品的关系

模块5-MSG微隔离

- 微隔离基本概念介绍
- 微隔离的价值
- 微隔离的技术路线及趋势
- 微隔离的优势
- 微隔离如何实施及其业界最佳实践

模块6-零信任安全的应用场景及案例

- 企业内部的安全访问场景
- 企业与外部的协作场景
- 系统间的安全访问
- 物联网安全连接
- 安全与合规要求
- 敏感数据的零信任方案

模块7-零信任安全的战略规划与实施

- 零信任安全战略综述
- 确立零信任战略实施愿景
- 制定零信任战略行动计划
- 零信任战略实现—部署迁移
- 零信任实施问题及解决思路
- 规划与实践案例-谷歌BeyondCorp

模块8-SASE安全访问服务边缘

- SASE的基本概念
- SASE系统架构
- SASE核心特征
- SASE核心技术
- SASE现状与应用
- SASE技术总结

模块9-零信任行业评估标准及认证

- 零信任安全专家认证CZTP
- 零信任成熟度模型CZTM

模块10-零信任实践案例

- 政企行业实践案例
- 金融行业实践案例
- 运营商行业实践案例
- 制造行业实践案例
- 能源行业实践案例
- 医疗行业实践案例
- 互联网行业实践案例

模块11-零信任安全总结与展望

- 网络安全技术的演进历程
- 零信任安全理念以及技术
- 零信任架构的潜在威胁
- 网络安全技术未来的发展展望

CZTP®
Certified
Zero Trust Professional

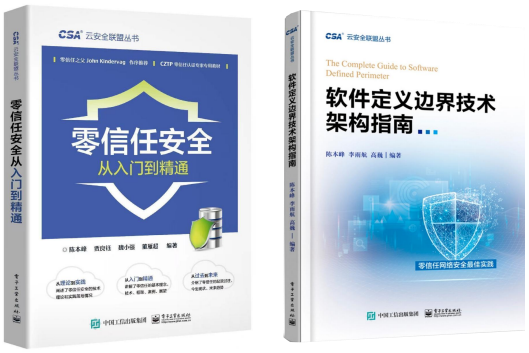
考试与认证培训

- **教学标准课时：**16小时
- **考试认证费用：**7480元/人（其中：培训费用5000元/人；考试认证费2480元/人）。
- **考试认证：**限时考试，题型为单选题和多选题，共60道题，须在90分钟内完成；获得80%以上的成绩通过考试。
- **考试入口：**https://exam.c-csa.cn 线上考试。

CZTP证书

学习材料

- CSA云安全联盟丛书《零信任安全-从入门到精通》（CZTP课程专用教材）
- CSA云安全联盟丛书《零信任网络安全-软件定义边界SDP技术架构指南》（汇编了CSA发布的：《SDP标准规范1.0》、《SDP架构指南》、《软件定义边界（SDP）和零信任》、《软件定义边界在IaaS中的应用》、《SDP实现等保2.0合规技术指南》，及NIST发布的《NIST零信任架构》）
- CSA大中华区整理《零信任落地案例集》(61个案例)
- CSA报告《实战零信任架构》



（可在京东上购买）

学习材料下载入口: https://c-csa.cn/research/results/i-1/

通过 CSA CZTP认证，学员可以获取如下收益：

1. 标志着你具有了零信任“永不信任”的安全思维，这是更前沿的网络安全尝试，将更能帮助你守护网络安全。
2. 获得全球顶尖的系统的零信任知识，可以全面掌握全球先进的零信任理论知识，SDP、IAM、微隔离等核心的技术及部署实践知识。
3. 庞大的雇主会员单位与行业专家资源庞大的全球 CSA 会员单位与行业专家人脉资源，为你安全职业生涯提供更多选择的可能。

CZTP®
Certified
Zero Trust Professional

什么是零信任?

零信任是一种安全理念，一种安全战略，强调“永不信任，始终验证”的安全思维；对于“零信任”来说网络安全无时限，危险来自每时每刻；网络安全无边界，威胁来自各个方面；网络安全不取决于位置/部门，无法决定可信度；所有人/物/端/网/信息/供应链均需认证授权（动态安全策略）。

零信任的安全架构“消除了可信网络的概念”，认为所有网络流量都是不可信的，所以必须验证和保护所有资源、限制并严格执行访问控制、检查和记录所有网络流量。

为什么零信任很重要?

随着数字化转型不断加速，尤其是云计算、物联网等新兴技术与创新业务不断打破企业原有安全边界，企业信息安全面临着前所未有的挑战：

1.访问者身份及接入终端的多样化、复杂化打破了网络的边界。

2.业务上云后各种数据的集中部署打破了数据的边界，同时放大了静态授权的管控风险，数据滥用风险变大。

3.资源从分散到云化集中管理，按需部署。

零信任是一种新颖的网络安全方法，它比传统解决方案更高的网络安全性。零信任方案在安全性和弹性方面的优势，更能适应未来网络环境企业的信息安全建设。采用零信任方案能更好管控风险，降低设备部署及漏洞管理成本，提升用户访问业务的速度与敏捷性，协助企业合规管理，并且能改善组织各部门间的合作与管理。

零信任是安全保障企业数字化转型、打造可持续数字化竞争力的一次最关键范式迁移。

学习对象

适用于云供应商、网络安全服务商、云服务用户、大中小型企业用户、信息化咨询服务、数字化转型服务提供商等组织的安全管理（信息部门主管或 IT 负责人、CIO、CTO、企业信息系统管理人员）、架构产品、技术开发（云计算、网络工程、安全）、咨询、运维服务等人员参与学习。

CZTP®
Certified
Zero Trust Professional

Q&A

企业为什么要实施零信任?

零信任架构更能适应未来的网络，实际的数据和负载无论在何时何地，以身份为核心的安全保障都无处不在，企业必须保持零信任网络架构才能保持竞争力。零信任对企业的优势：

- **有效控制云和容器环境**

实施零信任架构时，安全策略基于所识别的通信工作负载，并直接与工作负载相关联。因此，安全措施会尽可能贴近需要保护的资产，不受 IP 地址和协议等网络结构的影响。保护机制不仅能够适应试图传输的工作负载，而且环境变化后，依然能够保持一致。

- **降低数据泄露风险**

由于零信任基于最小特权原则，因此会假设每个实体（设备、用户和工作负载）都是敌对的。每个请求都要经过审查，个人和设备都需得到确认，权限都要得到评估，之后才能建立信任。此外，每当环境发生变化，比如用户的位置或所访问的数据，这种“信任”都会进行重复审查。

- **助力合规计划**

零信任分段可用于针对特定类别的敏感数据设立边界，这包括数据备份、PCI 数据和信用卡数据。采用细粒度限制有助于受监管的信息和不受监管的信息之间保持数据的清晰分离。对于在数据泄露事件中提供过度特权访问的扁平网络设计，零信任分段解决方案提供了更大的可见性和控制性。

- **降低业务和组织层面的风险**

在零信任模型中，所有应用程序和服务都被视为是有害的，除非它们的身份特征得到明确验证，否则无法通信。因此，零信任通过暴露网络上的所有内容以及这些资产的连接方式来降低风险。由于已建立了基准，零信任还会删除过度配置的软件和服务以及定期验证每个通信资产的凭据，以降低风险。

为什么要培养零信任人才?

作为安全用户：企业要采用零信任方案必须在企业内培养“永不信任”的安全思维,并了解组织安全文化和变革管理能力至关重要的。零信任ZT起初对管理员或开发人员来说
可能看起来很吓人，会被认为进一步限制了他们的访问权限和执行工作的能力。企业将需要支持和培养他们的人才，了解采用零信任ZT原则和技术的好处，这不仅有利于推动企业安全业务的部署，还能培养人才整体的网络安全管理观，帮助企业更好守护企业核心资产和作出创新。

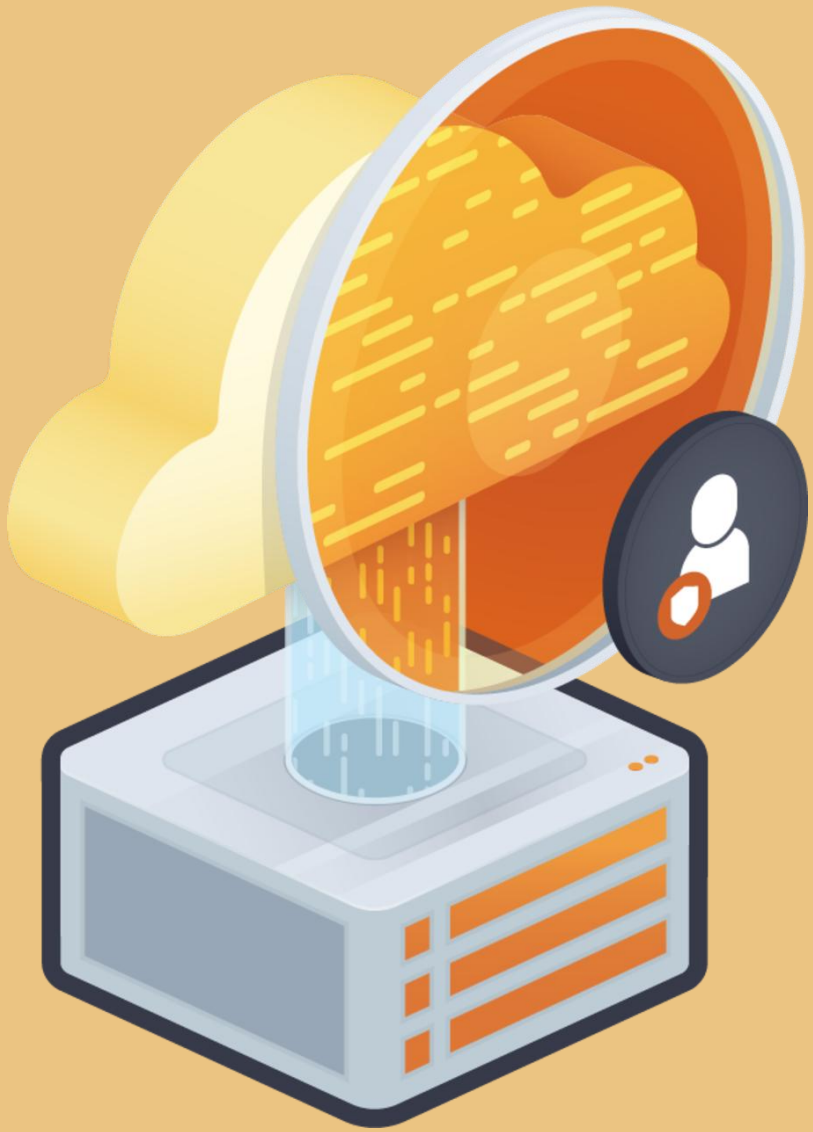
作为信息安全服务提供商：作为零信任解决方案的提供者，管理者、开发人员、实施交付人员、业务人员等都有具备系统的零信任知识，不仅能帮助促进企业人才跨技术之间的创新，在产品及服务方面进行更好的优化，还能促进企业内部提高在各项业务间、各岗位人员间沟通的效率，同时，更是能体现企业在零信任领域上下一致整体的专业水平，获得客户信任。

哪些机构的员工获得了CZTP的认证?

中国移动、中国电信、联通、阳光保险、中通快递、汽车之家、工商银行、汇丰银行、恒丰银行、盛宝银行、顺丰科技、欧莱雅、江西银行、蒙牛集团、伊利集团、五矿资本、联想、湖南公安、中兴、龙湖集团、海尔集团、金蝶、百度网盘、华为、腾讯、奇安信、绿盟、完美世界、微软、竹云、云深互联、联软、天风证券、陕西省人民医院、启明星辰、牧原股份、海通物流、新华三等500多家单位员工参与零信任学习及获得证书。

他们所从事的岗位包括：

CEO、CTO、CSO 、技术总监、安全专家、隐私安全负责人、信息安全总经理、信息部主任、行业解决方案总经理、安全架构师、产品交付专家、产品经理、安全主管、售前产品经理、网络安全工程师、大客户服务经理、安全服务工程师等。



官网：https://c-csa.cn
邮箱：info@c-csa.cn
电话：19925407556