



Cloud Security Alliance Greater China Region

中立权威的
国际非营
利性组织

CSA GCR
CLOUD SECURITY ALLIANCE GREATER CHINA REGION
云安全联盟大中华区

保障数字安全
拓展数字国际合作
促进数字繁荣

Ensure digital security
expand international digital cooperation
and promote digital prosperity



云安全联盟大中华区秘书处
官网: <https://c-csa.cn> 电话: 0755-86548359

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学大厦1号楼905



The logo for CSAGOR features the letters 'C', 'S', 'A', 'G', 'O', and 'R' in a bold, dark blue font. The 'C' and 'O' are stylized, each containing a red and orange circular graphic element. The background of the logo area is white, with a dark blue vertical bar on the left and a grey horizontal bar at the top. Below the logo, there is a blurred image of a modern building with large windows.

CSAGOR



李雨航 (Yale Li)
CSA大中华区主席

乌克兰国家工程院外籍院士,曾任华为首席网络安全专家兼国际CSO、微软全球首席安全架构师兼中国CISO,拥有建立标杆企业网信安全战略的丰富经验,并出版了《网络服务安全与监控》、《云计算360度》、《大数据革命-理论,模式与技术》等十余部著作,是国际网络安全领袖奖、联合国全球科技创新进步奖获等奖项的获得者。



Jim Reavis (吉瑞威)
CSA创始人兼首席执行官

云安全联盟(CSA)的联合创始人兼首席执行官,他在信息安全领域耕耘多年,不仅是企业家、作家、演说家,更是技术专家与商业战略家。Jim专注于信息安全,拥有对市场发展与未来趋势的深刻理解和创新观点,于2016年登入“信息系统安全协会”(ISSA)名人堂,并被SearchCloudComputing.com.评为“十大云计算领袖”之一。

无中立,不权威 Non-neutral, Non-authoritative——Jim Reavis
人类信任,世界安全 Trustable Human, Secure World——李雨航

CONTENTS

| | | |
|-----------|---|----|
| 01 | About Us 关于我们 | 01 |
| 02 | Our works 我们的工作 | 03 |
| 03 | Research 研究 | 04 |
| 04 | Certificates & Training 认证与培训 | 05 |
| 05 | Certificates & Assessment 评估与认证 | 18 |
| 06 | Events & Cooperation 活动与合作 | 25 |
| 07 | Memberhips 会员 | 33 |
| 08 | Awards & Recognition 奖项与认可 | 36 |
| 09 | Appendix 附录 | 39 |

云安全联盟

Cloud Security Alliance, CSA

是中立、权威的全球性非营利产业组织，于2009年正式成立，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，推动数字安全产业全面发展。



云安全联盟大中华区

Cloud Security Alliance
Greater China Region, CSA GCR

作为CSA全球四大区之一，2016年在香港独立注册，于2021年在中国登记注册，是数字安全领域首家在中国境内注册备案的国际NGO，旨在立足中国，连接全球，推动大中华区数字安全技术标准与产业的发展及国际合作。

欧非区 24+

英国、比利时、卢森堡、丹麦、埃及、法国、德国、爱尔兰、以色列、意大利、荷兰、挪威、波兰、葡萄牙、俄罗斯、西班牙、瑞典、瑞士、土耳其、阿拉伯联合酋长国.....

大中华区 8+

北京、杭州、上海、深圳、西安、大连、香港、澳门



CSA全球布局

CSA在全球设立四大区，包括美洲区、欧非区、亚太区和大中华区，100多支分会覆盖50多个国家，1500+会员企业，8000+研究专家，130000+社区专业人员。



50+
Countries



100+
Chapters



60000+
Research Experts



1500+
Corporate Members



130000+
Community Professionals

美洲区 48+

加拿大、智利、阿根廷、墨西哥、巴拿马、秘鲁、玻利维亚、温哥华、俄亥俄州东北部、匹兹堡、旧金山、硅谷、波士顿、巴西、哥伦比亚、芝加哥.....

亚太区 19+

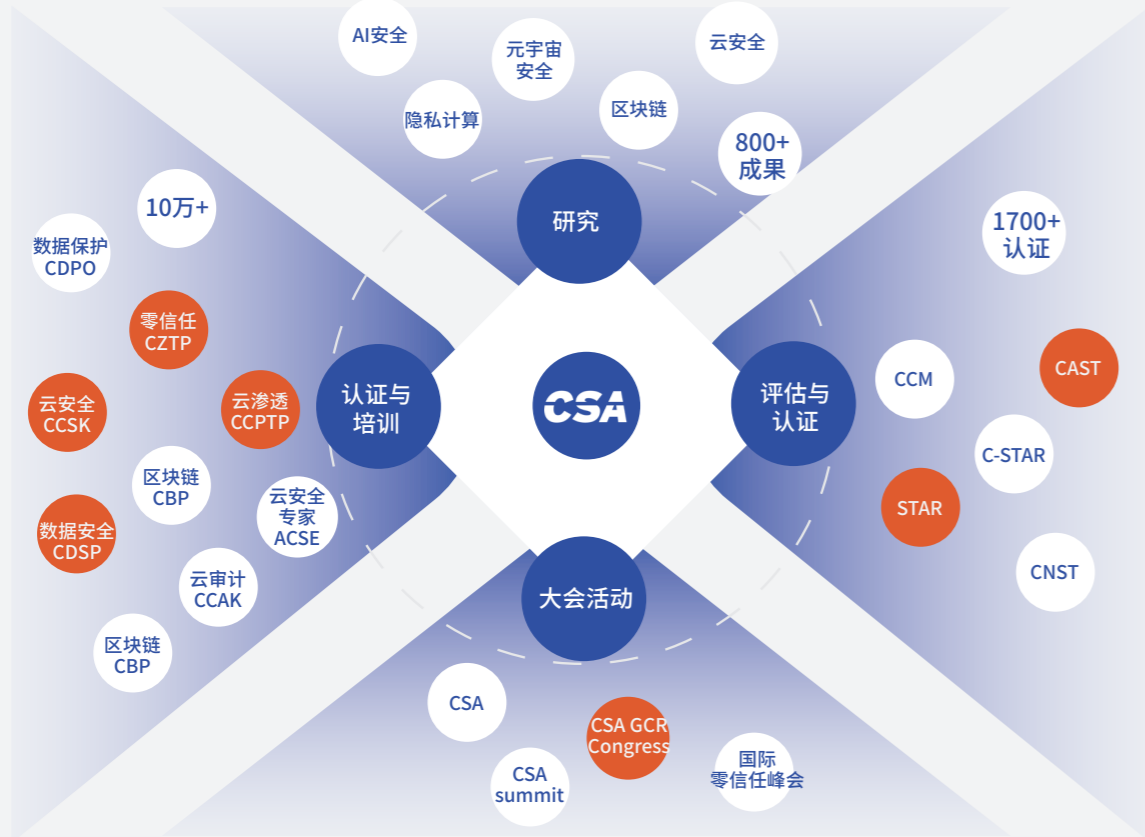
澳大利亚、日本、韩国、马来西亚、孟买、尼泊尔、泰国、菲律宾、沙特、越南、新加坡、孟加拉国.....

围绕云计算及下一代数字技术安全产业发展需求,CSA通过标准指南引领、持续的研究报告、人才培养、安全评估及会议活动等方式,以提高企业及人员的安全水平和能力,并为其达到同等水平提供认证保障。

面向云计算与下一代数字技术安全的全面研究,保证研究的敏捷性、专业性、完整性。共有 83+工作组,6万多名专家,13万多名社区人员参与CSA的研究工作。

联盟宗旨

- 推动业界对云安全与数字安全的前沿研究;
- 推广正确使用云安全及数字安全的解决方案,和开展教育计划;
- 帮助个人、企业用户和供应商达到要求的安全认识水平与能力,并提供安全认证证书。



CSA数字安全人才认证与培训体系，课程的设计遵从系统性、专业性、实践性，与国际知识体系保持一致。



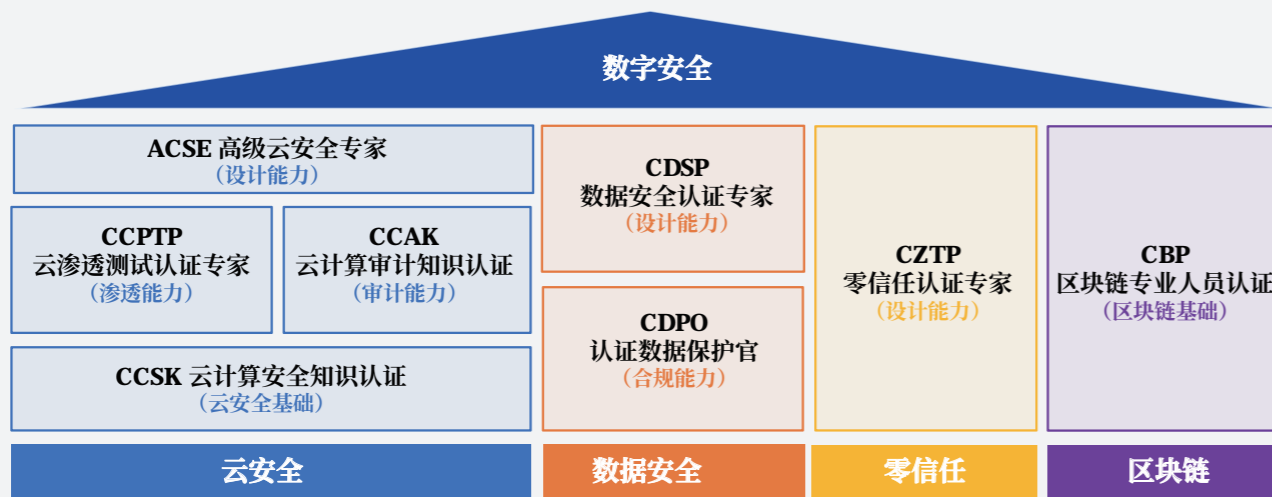
系统性



专业性



实践性



CSA数字安全人才认证与培训体系

云安全知识认证

CCSK, Certificate of Cloud Security Knowledge

首个面向个人用户的全球安全认证，被誉为“云计算之母”。

CSA为了让业界人员更好掌握云计算安全知识，基于《云安全指南》、《云控制矩阵》等知识内容，于2011年发布了云安全知识认证CCSK。通过CCSK课程学习，学员能对云安全架构、威胁、治理、合规性、运营、加密和虚拟化和最佳实践有一个全面的了解和广泛的认知。



课程大纲

CURRICULUM

01| 云架构

云计算简介
云架构简介
云的基本特征
云服务模型
云部署模型

02| 云基础设施安全

云计算基础设施安全
保护虚拟网络
保护计算工作负载
管理平面安全
业务连续性/灾难性恢复

03| 管理云安全和风险

风险与治理
法律
合规与审计

04| 云数据安全

云数据存储
保护云中的数据
其他数据安全选项
数据安全生命周期

05| 保护云应用程序、用户和相关技术

应用安全
身份和访问管理
相关技术介绍

06| 云安全操作

选择云提供商
安全即服务
事件响应

培训课时与费用：2天，共16小时；培训费为4500元/人。

考试题型及时间：60道选择题，限时90分钟；获得80%及以上的成绩视为考试通过。

考试认证费：2480元/人。



云渗透测试认证专家

CCPTP, Certified Cloud Penetration Test Professional

全球首个专注于云环境渗透测试能力的认证课程

CCPTP旨在提供针对云计算渗透测试所需的专业实操技能, 弥补云渗透测试认知的差距和技能人才培养的空白, 提升专业人员能力及提供认证证书, 为云计算产业发展提供渗透人才队伍保障。认证课程包含了云渗透测试知识体系、测试流程、实践技术、法律法规、渗透测试人员道德规范、渗透测试方法论 以及实操技术等内容。



课程大纲

CURRICULUM

01| 云计算概念和体系架构

云计算基本定义
云计算参考架构
共享职责模型
CSA共享职责评估

02| 云计算整体安全

云安全模型
云安全范围与职责
云计算架构参与者
云安全与 DevOps
云渗透测试技术

03| 渗透测试安全意识培训

定义及法律规范解读
渗透测试通用框架流程
渗透测试服务条款制定
渗透测试范围确定
云上渗透测试边界

04| 云计算攻击路径

传统攻防 vs 云攻防
云计算攻击路径全景
云纵向攻击路径
云横向扩展攻击路径
常见攻击路径与场景

05| 云上资产发现与信息收集

云基础架构组件介绍
云上大规模侦查技术
针对云计算架构中
不同参与角色的安全性测试

06| 云租户业务层渗透测试

云租户web应用攻击面概览
云计算安全威胁Top11测试方式
传统漏洞云危害升级

07| 云管理层渗透测试

云管理层攻击面概览
云控制台管理渗透测试技术
身份与访问管理渗透测试技术
应用程序编程接口渗透测试技术
云数据加密和解密攻防技术
云上监控、日志审计与防御绕过技术

08| 云服务层渗透测试

云服务模型攻击面
IaaS渗透测试技术
PaaS渗透测试技术
SaaS渗透测试技术
云原生应用程序漏洞
云服务滥用技术

09| 虚拟化与容器渗透测试

硬件虚拟化攻击概述
容器攻击面概览
容器攻击流程概览
容器逃逸技术

10| 云基础设施层渗透测试

云基础设施攻击面、路径与核心目标概述
云计算网络下的渗透测试技巧
多租户环境下网络渗透技术
混合云及其他渗透测试方法

培训课时与费用: 5天, 共30小时; 培训费为8800元/人。

考试题型及时间: (理论考试) 80道选择题, 限时120分钟; (实操考试) 4道操作题, 限时120分钟。

理论考试获得80%及以上&实操考试获得75%及以上视为考试通过。

考试认证费: 4000元/人。



云审计知识认证

CCAK, Certificate of Cloud Auditing Knowledge

全球首个专注云审计的中立的技术认证, 以专业的技能和证书, 提升审计人员的职业形象

CCAK是CSA与ISACA强强联手共同开发的认证, 为从业人员提供亟需的云审计知识、培训和证书, 应对云审计的独特挑战, 确保对机密性、完整性和可访问性进行正确的控制, 并降低审计管理和违规的风险及成本。



课程大纲 CURRICULUM

- 01| 云治理**
 - 治理概述
 - 云保障
 - 云治理框架
 - 云风险管理
 - 云治理工具
- 02| 针对使用CCM的云的威胁分析方法**
 - 定义和意图
 - 攻击细节和影响
 - 减轻控制和衡量标准
 - 案例
- 03| CCM : 审计控制、持续鉴证和合规**
 - CCM审计范围界定指南
 - CCM风险评估指南
 - CCM审计工作手册
 - CCM的一个审计示例
- 04| 云合规计划**
 - 设计云合规性计划
 - 制定云合规性计划
 - 法律和监管要求
 - 标准和安全框架
 - 确定控制措施和衡量有效性
 - CSA证书、认证和验证
- 05| 评估云合规计划**
 - 评估方法
 - 治理视角
 - 法律、监管和标准视角
 - 风险视角
 - 服务变更影响
 - 需要持续保证/持续合规
- 06| 持续保证与合规**
 - DevOps 和 DevSecOps
 - 审核 CI/CD 管道
 - DevSecOps 自动化和成熟度
- 07| CCM和CAIQ宗旨、目标和结构**
 - 云控制矩阵(CCM)
 - 共识评估调查问卷(CAIQ)
 - 与标准的关系:映射和差距分析
 - 从CCM V3.01进化到CCM V4
- 08| 云审计**
 - 审计特征、标准和原则
 - 云计算审核标准
 - 审核内部部署环境vs 云环境
 - 评估云服务和云交付模式方面的差异
 - 云审计构建、规划和执行
- 09| STAR 计划**
 - 安全和隐私标准
 - 开放式认证框架
 - STAR 注册
 - STAR 1级、STAR 2级、STAR 3级

培训课时与费用:2天,共16小时;培训费4500元/人。
 考试题型及时间:76道选择题,限时120分钟。获得70%及以上的成绩视为考试通过。
 考试认证费:3380元/人。



高级云安全专家

ACSE, Advanced Cloud Security Expert

集云安全、云原生、与相关新兴技术安全于一体的高级云安全专家认证

ACSE旨在培养数字化时代云原生环境及DevSecOps环境的安全专家,解决如何做好新一代云原生安全及DevSecOps安全的问题。通过课程学习掌握最新的云原生的安全防护管理体系与专家级的评估方法、业内先进的DevSecOps安全的实现模型与技术,以及云运维与事件响应与云安全合规与审计的最新方法。



课程大纲

CURRICULUM

- 01| 云计算及云原生概论**
 - 云计算概述
 - 云原生技术
 - 云原生风险评估
- 02| 云计算风险管理**
 - 基本概念
 - 云计算顶级威胁总览
 - 云计算顶级威胁分析
 - 云计算风险评估
- 03| 云主机安全**
 - 云主机资产现况与威胁总览
 - 云工作负载保护平台(CWPP)介绍
 - 云主机安全防护体系
 - 云主机安全在攻防实战中的价值
 - 主机安全三级要求测评
- 04| 云网络与多云安全**
 - 云网络安全概念和挑战
 - 云网络安全解决方案
 - 多云网络安全解决方案
 - 云网络安全能力满足度评估
 - 云网络安全新技术
- 05| 微服务安全**
 - 微服务基本概念
 - 微服务安全挑战
 - 设计可信的微服务安全
 - 微服务安全评估
 - 举例: Spring Cloud
 - 微服务的安全
- 06| 容器安全**
 - 容器安全关键概念及原则
 - 容器安全风险及应对策略
 - 容器安全保护实践
 - 容器安全成熟度分析
- 07| DevSecOps安全**
 - 基本概念
 - 六大支柱
 - 交付流水线
 - 工具链
 - 成熟度与评估

08| 无服务器计算 Serverless安全

- 基本概念
- 治理与安全模型
- 无服务器典型威胁
- 十二个最关键的风险
- 安全设计、控制以及最佳实践
- 评估无服务器及安全工具

09| 云应用安全

- 云应用安全概述
- 云应用测试安全
- 云应用防护安全
- 云应用身份安全
- 云应用接口安全

10| 云数据安全

- 云数据安全相关风险
- 云数据安全相关法规与标准
- 云数据安全基本概念
- 云数据安全整体保护框架
- 云数据安全防护设计思路
- 云数据安全具体保护技术
- 云数据安全防护措施评估
- 云数据安全改进建议

11| 云原生安全架构设计与安全上云建议

- 云原生安全架构设计
- 云原生安全新型风险
- 云原生安全架构设计
- 安全上云技术建议
- 安全上云技术评估

12| 云安全运维与事件响应

- 云安全运维概述
- 云安全运维工具
- 云事件响应框架
- SOAR平台

13| 云安全合规治理与审计

- 云安全合规治理框架
- 共享职责与云控制矩阵
- 云安全审计

14| 新兴技术在云场景下的安全挑战

- 大数据安全
- 物联网安全
- 移动安全
- 人工智能安全
- 区块链安全

ACSE课程将于2023第四季度正式推出, 考试及费用相关情况后续公布。



零信任认证专家

CZTP, Certified Zero Trust Professional

全球首个提供零信任系统知识及提升实践能力的安全认证

CZTP涵盖最新的零信任架构技术与实践知识, 旨在为网络信息安全从业者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, 传播与践行零信任理念, 为企业守护核心数字资产。



课程大纲

CURRICULUM

01| 零信任的演进

- 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

02| 零信任架构

- 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

03| 身份管理与访问控制 (IAM) 技术详解

- 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

04| 软件定义边界 (SDP) 技术详解

- SDP的技术演进
- SDP的基本架构及核心技术
- SDP的部署方式及其代表的场景
- SDP的功能和应用场景
- SDP与传统产品关系

05| 微隔离 (MSG) 技术详解

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

06| 零信任安全的应用场景及案例分析

- 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

07| 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

08| 零信任行业实践案例分享

- BeyondCorp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

09| 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

培训课时与费用: 2天, 共16小时; 培训费5000元/人。

考试题型及时间: 60道选择题, 限时90分钟; 获得80%及以上的成绩视为考试通过。

考试认证费: 2480元/人。



数据安全认证专家

CDSP, Certified Data Security Professional

贯彻国内外法律法规,培养数据安全技术与合规方面专业人才

CDSP针对云数据安全、ICT数据安全和新兴热点业务的数据安全展开,并结合各类新兴技术的不同场景,给出数据安全架构、安全设计、隐私保护的一般原则和业界最佳实践,旨在确保信息安全、数据安全、云计算、隐私保护的从业人员对数据安全威胁和数据安全框架和最佳实践有系统性地认知并掌握基本技能。



课程大纲

CURRICULUM

01| 数据安全导论

数据安全的纲领
数据分类的原则与实施
数据安全体系

02| 数据安全风险挑战与应对

数据安全的风险和
数据安全应对机制

03| 数据安全架构与设计

数据安全架构的设计、实施和案例
数据安全治理框架和架构模型
访问控制关键技术
数据安全业务场景

04| 数据安全的基石:
密码学与加密

各类密码学技术
密钥管理体系和安全协议
量子时代的密码学与密钥管理
密码学技术实践

05| 隐私保护与
数据安全合规

隐私的概念及监管
隐私保护原则和技术
海外垂直行业数据与隐私合规需求
中国数据安全与隐私保护监管的演进

06| 新兴技术的
数据安全挑战

AI与数据安全
以区块链为代表的新兴应用
物联网数据安全
5G与数据安全
隐私保护技术

07| 金融行业案例分享

培训课时与费用:2天,共16小时;培训费5000元/人。

考试题型及时间:60道选择题,限时90分钟;获得70%及以上的成绩视为考试通过。

考试认证费:2480元/人。



认证数据保护官

CDPO, Certified Data Protection Officer

专注中国特色的个人信息保护实操培训

CDPO聚焦数据法律法规剖析、隐私保护合规体系建设以及梳理并理解数据治理和信息安全的基本概念,打造综合性的专注中国特色的个人信息保护实操培训课程体系。CDPO旨在促进数字化领域从业人员对中国法律、法规的理解及隐私保护意识,主动跟踪合规要求变化,梳理内部的合规差距,真正能设计和落实具体的合规管理和技术措施进而规避合规风险,充分应用到工作中。



课程大纲

CURRICULUM

01| 数据保护的社会和法律背景

数字经济和个人信息保护
个人信息保护的治理和管理
什么是数据保护管理系统
如何开发数据保护管理系统
个人信息保护政策
个人信息保护中的人员的角色和职责
数据保护官的作用
DPO的工作范围和职责

02| 数据安全风险挑战与应对

谁有资格成为DPO
中国的DPO设置的考量
个人信息保护需要建立的流程及其内容要点
什么是Privacy by Design
DPIA的中国落地 - 个人信息安全影响评估PISIA
PISIA模板和内部采纳流程
如何维护个人信息保护体系
个人信息保护体系建设路线图

03| 数据安全架构与设计

04| 企业个人信息保护体系建设从模型到实施

05| 企业个人信息跨境数据传输合规建设

跨境数据传输的国际限制
中国跨境数据传输的相关法律法规
企业内部个人信息数据跨境要点和合规流程

07| 企业隐私保护主要管理制度示例介绍

| | |
|-------------|-------------|
| 企业隐私保护政策 | 数据处理活动记录 |
| 企业隐私保护声明的开发 | 数据流梳理 |
| 数据主体权利响应 | 数据资产清单 |
| 直接营销 | 数据生命周期 |
| 数据保护影响评估 | 数据归档及销毁 |
| 数据跨境转移 | 数据泄露事件响应及管理 |

06| 第三方供应商管理和数据安全风险

变化环境中的第三方安全合规
第三方安全风险评估
第三方合规方案的设计
第三方合规的审查和跟踪

课程大纲

CURRICULUM

01| 区块链背景

区块链市场现状
区块链相关标准发展
区块链发展趋势
区块链相关岗位

02| 区块链基本概念

区块链定义与特点
区块链分类与价值
区块链应用领域
区块链问题与挑战

03| 分布式核心问题

区块链存储
共识机制
智能合约
非对称加密和授权

04| 区块链与密码学

密码学
非对称加密与解密
哈希算法
共识机制与算法

05| 比特币与以太坊

如何定义主流加密货币
主流加密货币简介
稳定币
比特币应用举例

06| 区块链与开发

| | |
|-----------|-----------------------|
| 采用的开发语言 | GO语言及区块链 |
| 语言特点及应用场景 | Flow Cadence智能合约语言的介绍 |
| GO语言及特性 | |

07| 区块链与安全

区块链整体框架与安全
智能合约与安全
DAPP与安全
数字货币相关安全

08| 区块链行业应用

| | |
|----------|-------------|
| 数字身份安全 | Fabric跨行业应用 |
| 保障物联网安全 | 区块链+电子商务 |
| 区块链与数据安全 | 区块链供应链金融 |
| | 去中心化交易所 |

09| 区块链的生态及未来

培养区块链思维
区块链政策剖析
应用趋势及未来介绍

培训标准课时:2天,共16小时;培训费用5000元/人。

考试题型及时间:理论考试(占80%)—60道选择题,限时90分钟。实操测试(占20%)——学生通过培训后,由培训机构组织线上合规评估的实操测试。总分达到70%及以上通过考试。

考试认证费:2480元/人。



CBP区块链专业人员认证

CBP, Certified Blockchain Professional

涵盖最新的区块链原理与实践知识

CBP旨在为IT从业者在数字化时代下提供全面的区块链原理、安全思维及应用区块链技术解决网络信息安全的问题。通过本课程学习,学生掌握区块链中涉及的密码技术、分布式一致性等基础知识,理解和掌握区块链、密码技术、共识机制、激励机制、智能合约、P2P网络等的基本原理和实际应用,进一步能准确分析各行业存在的去中心化信任、公开透明、不可篡改、不可伪造以及跟踪溯源等安全问题,设计和使用区块链技术解决各行业应用问题。



培训标准课时:2天,共16小时;培训费4500元/人。

考试题型及时间:60道选择题,限时90分钟;获得80%及以上的成绩视为考试通过。

考试认证费:2480元/人。



CSA 云安全联盟丛书

丛书的编写将坚持理论与实践并重的原则,既保证理论知识的准确严谨,又注重实践方案的价值落地。丛书内容将涵盖云安全、大数据安全、物联网安全、零信任安全、5G安全、人工智能安全和区块链安全等新兴技术领域安全。本丛书既可用于CSA认证课程学习教材、高等院校和社会教育所用教材或教学参考书,也可以作为产业界的专业安全读物。



授权培训机构

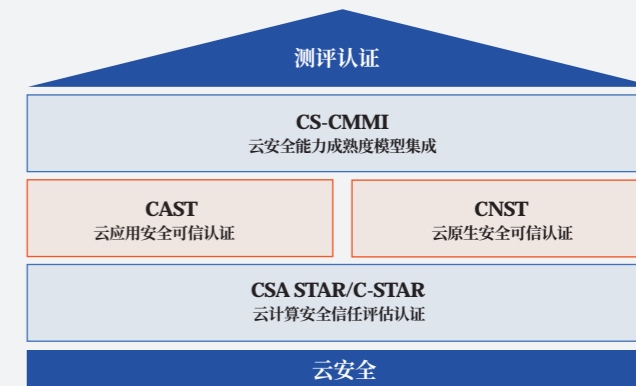


CSA倡导使用最佳实践为云计算提供安全保障,提供企业用户和云服务供应商必要的安全需求和评估认证。

CSA云安全领域的标准被世界各国认可,被誉为云计算安全的全球性通用标准。

面向企业服务管理体系,CSA推出云安全信任评估认证STAR和云安全能力成熟度模型集成CS-CMMI;

面向云安全产品,CSA推出云应用安全可信认证CAST和云原生安全可信认证CNST。



企业获得C-STAR、CS-CMMI、CAST、CNST等认证,标志着企业的安全运营管理和产品能力获得国际权威认可,持续为用户提共安全可信的云服务。目前,全球已通过认证的企业单位达1700多家,包括:微软、华为、腾讯、亚马逊、深信服、阿里云、中国电信、腾讯云、金山云、中兴、中国平安、北森、天融信等。



云安全评估认证

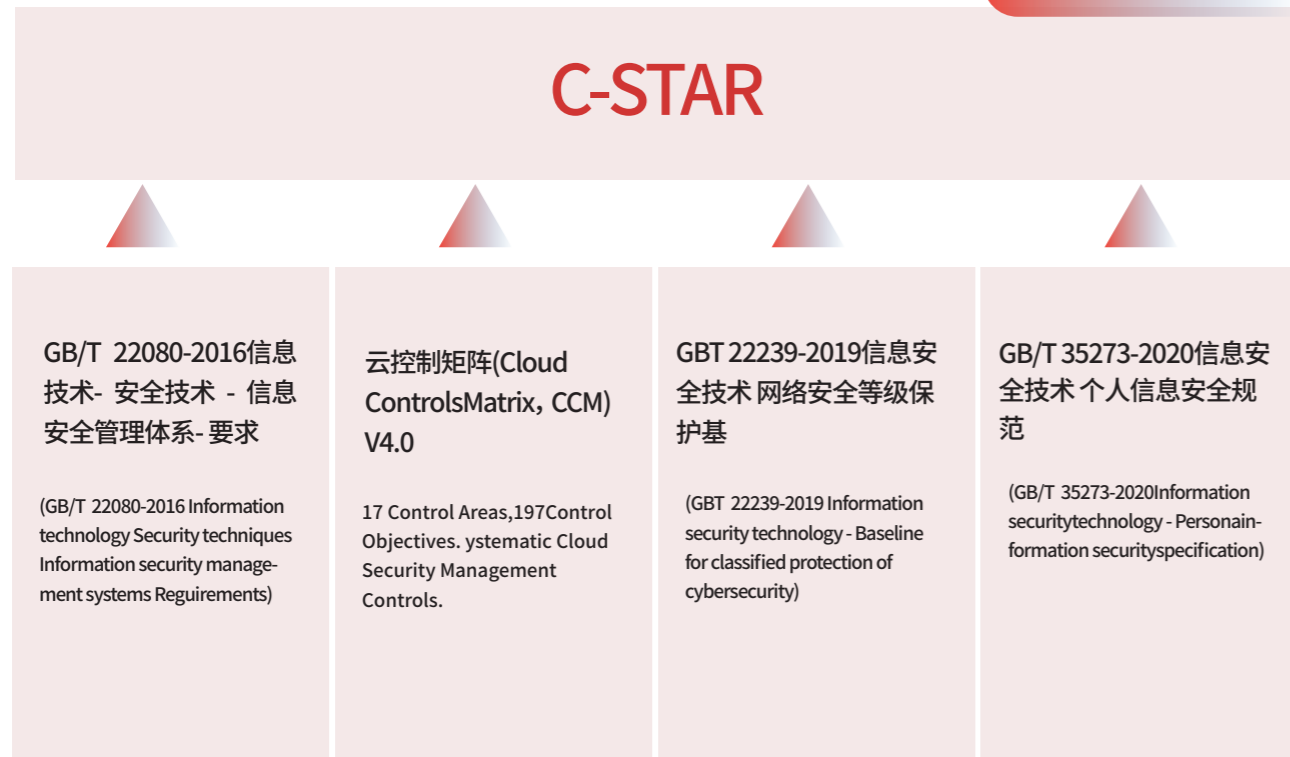
C-STAR (Cloud Security Trust, Assurance and Risk)

C-STAR 由云安全联盟大中华区和赛宝联合颁发的第三方认证,旨在协助云服务厂商展现其云服务安全水平及安全管理成熟度,增强云服务用户的安全信心,并用云计算信息安全管理最佳实践指导企业提升云服务信息安全水平。

■ 认证对象:采用云计算技术/提供云计算服务的企业,包括各类型的云服务商。

■ 认证依据:《CSA CCM 云安全控制矩阵》、GB/T22080-2016信息技术-安全技术-信息安全管理体系-要求、GB/T 22239-2019信息安全技术 网络安全等级保护基本要求、GB/T 35273-2020信息安全技术 个人信息安全规范。

C-STAR构成图



云应用安全可信认证

CAST (Cloud Application Security Trust)

CAST 由云安全联盟大中华区和公安部第三研究所联合颁发的第三方认证,旨在提升云应用类产品在生命周期各阶段的安全性、提升云应用类产品的整体安全能力,客观公正地对云应用进行安全和可信能力测评,更能确保其安全性和提升客户对应用安全的信任度。

■ 认证对象:云应用包括但不限于SaaS产品、所有在线订阅类服务、IaaS/PaaS云的应用部分。

■ 认证依据:CSA云安全联盟标准《CSA C001-2022:云应用安全技术规范》。

云应用安全框架





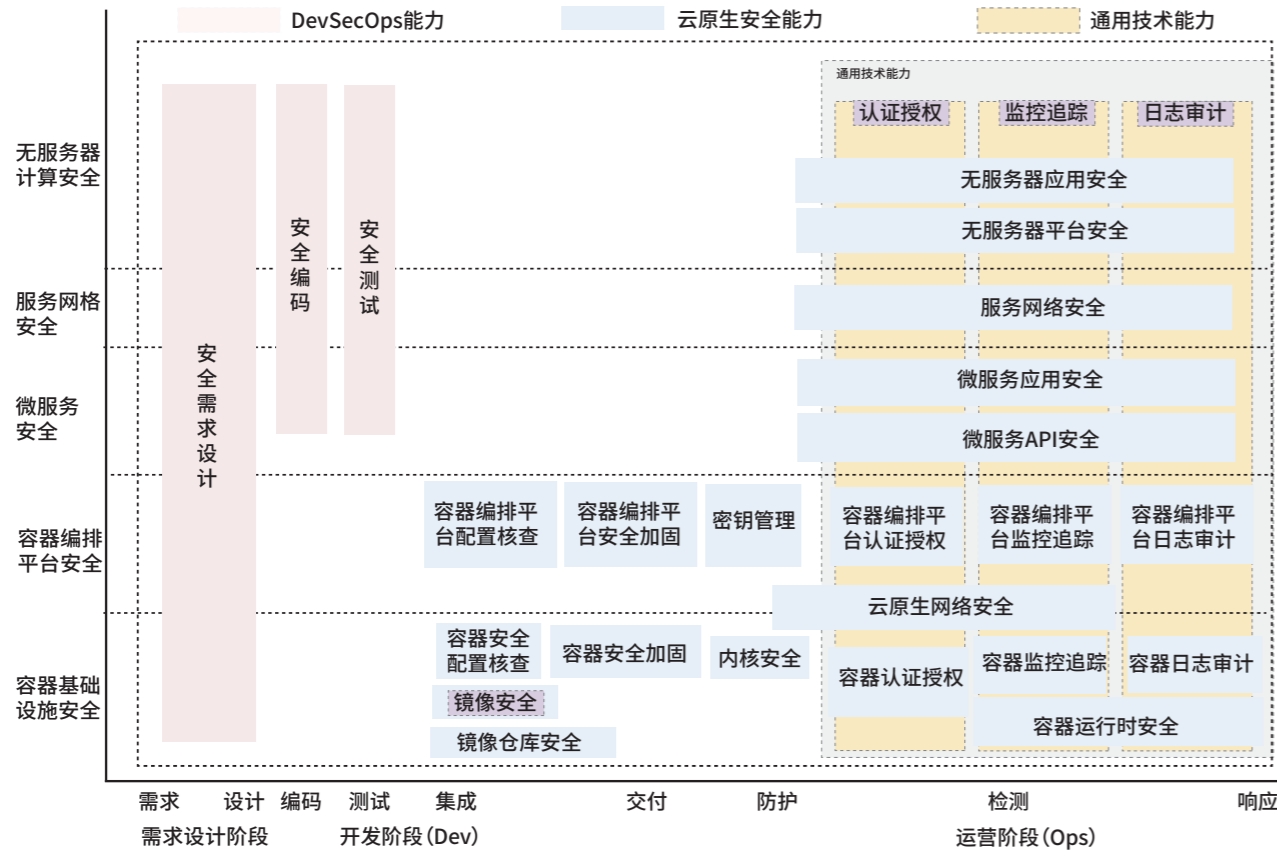
CNST 由云安全联盟大中华区和公安部第三研究所联合颁发的第三方认证,旨在提升云原生类产品技术,以及提升云原生类产品在生命周期各阶段的安全性和整体安全能力,指导云服务商和企业单位建设云原生安全体系。

■ 认证对象:云原生类产品厂商或甲方单位构建安全的云原生类产品。

■ 认证依据:CSA云安全联盟标准《CSA C002-2022:云原生安全技术规范》。

云原生安全可信认证

CNST (Cloud Native Security Trust)



云原生安全体系框架



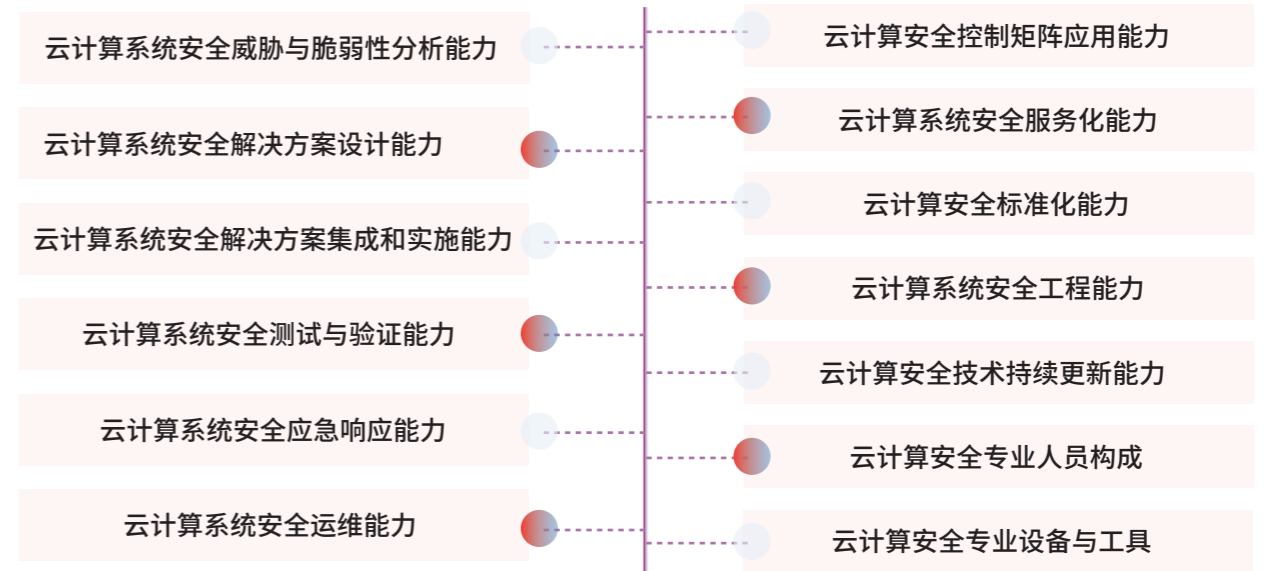
CS-CMMI由云安全联盟大中华区推出,旨在为云计算产品和解决方案提供商、云计算服务提供商、云安全技术服务组织等对象提供一个评估自身云安全能力的标准。CS-CMMI帮助他们评估其在不同方面的安全水平,以便他们能够更好地保护客户数据和隐私。

■ 认证对象:云计算产品和解决方案提供商、计算服务提供商、安全技术服务组织。

■ 认证依据:《CSA CCM 云安全控制矩阵》、CSA云安全联盟标准《CSA 0001-2016 云安全技术要求》、ISO/IEC 21827:2002《信息技术 系统安全工程 能力成熟度模型》。

云安全能力成熟度模型集成

CS-CMMI (Cloud Security Capability Maturity Model Integration)



云安全能力成熟度模型集成框架

测评机构(部分)



获证单位(部分)

1700+企业通过认证



评估认证咨询



活动与合作

组织国际大会、技术峰会、研讨会,为企业提供发展风向标指引,促进国际间、企业间创新与交流

云安全联盟大中华区大会 (CSA GCR Congress)

已成功举办五届，旨在整合“政产学研用金介”等各界资源，搭建国内外专家学术与产业合作交流平台，给会员们和业界带来更多价值。



云起龙骧, 安全共商



云涌起, 安共商



云安盛筵, 智观己亥



数字经济大发展,
云安精英再出发



数字合作创新,
安全赋能基建



数字信任, 共同安全

北京 1st, 2016

安徽宿州 2nd, 2017

广东深圳 3rd, 2018

广东深圳 4th, 2019

上海 5th, 2020

上海 6th, 2021-2023



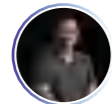
毛作奎
中央网信办网络安全
协调局副局长



Roman Sheredin
俄罗斯通信总局副局长



张亚勤
中国工程院外籍院
士, 前百度总裁



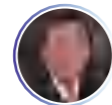
李欲晓
中国网络空间安全
协会秘书长



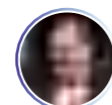
杨义先
北京邮电大学教授



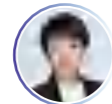
陈志宽
美国新思科技联合
CEO兼总裁



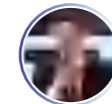
柴洪峰
中国工程院院士



Tony Scott
美国联邦原CIO/
微软原CIO



尹丽波
工信部国家工业信息安
全发展研究中心主任



高林
中央网信办网络安
全协调局副局长



Mikhail Konarovskiy
俄罗斯上海合作组
织秘书处大使



郝叶力
国家创新与发展战略
研究会副会长、少将



方滨兴
中国工程院院士



陈钟
北京大学教授



季统凯
中科院云计算
中心主任



颜亮
浪潮云副总裁



William (Bill) M Genovese
华为副总裁/国际
著名金融安全专家



邓小四
江南天安CEO



陈智敏
中国友谊促进会理事长、
公安部原副部长



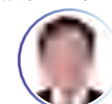
邬江兴
中国工程院院士



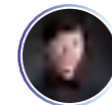
贾焰
国防科技大学 教授



高文
中国工程院院士, 鹏
城实验室主任



陆军
中国工程院院士



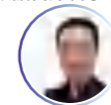
李雪莹
天融信CEO



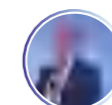
彼特·梅杰
联合国科学和技术促
进发展委员会主席



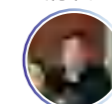
容淳铭
挪威工程院院士、欧盟
大数据首席科学家



金波
公安三所所长助理、信
息网络安全首席科学家



亚历山·大朱可夫
俄罗斯国家信息安
全论坛秘书长



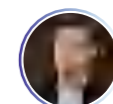
何小龙
国家工业信息安全
发展研究中心副主任



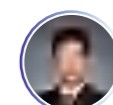
季昕华
UCloud创始人
兼CEO



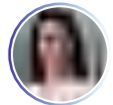
彼特·梅杰
联合国科学和技术促
进发展委员会主席



李伟
俄罗斯工程院外籍院士



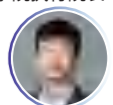
王安宇
OPPO终端总经理



Jeannette Wing(周以真)
美国哥伦比亚大学常务副校
长、美国艺术与科学院院士



陈宇翱
中国科学技术大学物
理学院执行院长



李滨
腾讯云安全总经理

CSA SUMMIT 云安全联盟峰会

云安全领域峰会的风向标,已连续举办14年,2011年2月,白宫在首届CSA Summit上发布了美国联邦云战略(Federal Cloud Strategy),提出了“云优先”(Cloud First)的政策原则。



CSA Summit每年在多个国家和地区举办,如:中国-北京、美国-旧金山、华盛顿、纽约、波士顿、德国-法兰克福、柏林、慕尼黑、新加坡、英国-伦敦、俄罗斯-曼彻斯特、日本-东京、大阪等。

历届演讲嘉宾

1. 白宫国家安全副顾问Anne Neuberger
2. 美国国土安全部(DHS)网络安全与基础设施安全局(CISA)副局长Nitin Natarajan
3. 欧盟网络与信息安全局(ENISA)执行主任Juhan Lepassaar
4. 新加坡信息通信发展管理局(IMDA)首席执行官Tan Kiat How



5. 微软云安全副总裁Ann Johnson
6. IBM云安全副总裁Sridhar Muppidi
7. 亚马逊(AWS)首席信息安全官Stephen Schmidt
8. RSA首席执行官Rohit Ghai

国际零信任峰会

已成功举办三届,对推动零信任的落地起到极大的推动及引领作用,已成为国际上零信任的风向标会议。



倡议
线上直播

1st, 2020
十年磨一剑,零信任出鞘

这是全球首个以零信任为主题的峰会,倡导零信任理念的普及



落地
山东青岛

2nd, 2021
数字时代,零信任剑行天下

增强企业落地零信任的信心,促进零信任在疫情时代的发展



验证
浙江湖州

3rd, 2022
因为看见,所以信任

站在解决用户现实安全问题的角度,验证零信任的实力,坚定用户对零信任的选择。

攻防挑战赛

在第三届零信任峰会期间,CSA大中华区举办首届零信任攻防挑战赛。这是在全球范围内首次集合多家零信任商用产品进行攻防对抗,这种结合实际场景的公开比赛,既是直接为市场验证零信任,也是助推零信任的技术创新,这是数字安全领域的一项重要里程碑事件。



CSA 研讨会

围绕热点话题，组织联盟成员单位及专家，通过线上或线下分享的方式，至今已举办超过30期。
云安全、零信任、元宇宙安全、区块链、SASE、数据安全、物联网、隐私保护、XDR.....



合作案例

(一) 联合国科学与技术发展促进委员会

云安全联盟大中华区是联合国科学与技术促进发展委员会的合作伙伴，并作为数字安全领域唯一的国际组织参与到联合国《全球数字契约》项目中，其提出的数字可信与安全被联合国采用纳入契约草案中，在数字安全领域国际平台发声，输出中国声音，中国方案。



“联合国秘书长古特雷斯在第五届云安全联盟大中华区大会上发表讲话”

“联合国科技委主席彼特·梅杰分别在第五届云安全联盟大中华区大会和第三届国际零信任峰会上发表讲话。”



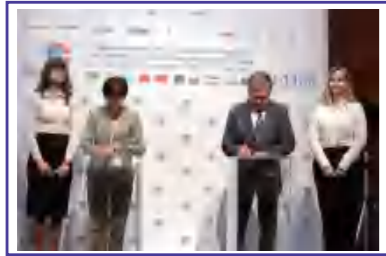
“云安全联盟大中华区主席李雨航出席参加联合国活动”



“彼特·梅杰主席表示“云安全联盟大中华区大会是非常重要的活动，它为数字化合作的落地做出了贡献”。”

(二) 俄罗斯国际信息安全论坛 InfoForum

2018年, CSA GCR与InfoForum签订战略合作协议, 双方合作在“金砖国家和上合组织成员国参与的国家信息技术论坛”上连续举办4届中俄数字论坛, 加强全球在数字安全领域的国际联动, 搭建国际交流与合作平台。



CSA大中华区与俄罗斯国际信息安全论坛InfoForum签约



李雨航院士在大会开幕式上发布主旨演讲



InfoForum组织俄罗斯政企代表到深圳参加CSA GCR大会

“InfoForum Ugra”卓越贡献奖



授予世界上在网络与信息安全领域为人类建立信任做出杰出贡献的国际领袖, CSA GCR推荐中国专家获此荣誉。

该奖项获得者包括



方滨兴

中国工程院院士



李雨航

云安全联盟大中华区主席、乌克兰国家工程院外籍院士



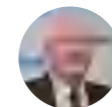
陈智敏

中国友谊促进会理事/公安部原副部长



邬江兴

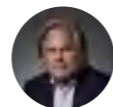
中国工程院院士



Andrey Krutskikh
俄罗斯国际合作与信息安全总统特使



Panglima Mohd Azumi Bin
前马来西亚国家网络安全委员会主席



Evgeny Kaspersky
卡巴斯实验室董事长&CEO

MORE 更多交流与合作



会见联合国副秘书长阿曼迪普·吉尔



与联合国科技委员会主席彼得·梅杰交流



与国际ITU秘书长赵厚麟交流



会见印尼总统特使卢胡特, 提供安全战略咨询



受马来西亚科技部部长邀请, CSA GCR为马来西亚内阁授课



与图灵奖获得者迪菲教授(左一)、诺贝尔奖获得者萨金特教授(右一)交流



授书: 全国政协社会和法制委员会副主任、公安部原副部长陈智敏



授书: 腾讯CEO马化腾



授予CSA大中华区顾问证书: 奇安信集团董事长齐向东



颁发CSA全球会员单位证书: 信通院院长余晓晖



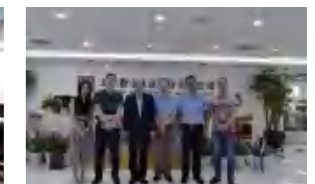
颁发CSA大中华区理事单位证书: 北森云CEO纪伟国



走访华为



走访腾讯



走访数字证

EXPERTS AND SCHOLARS

专家学者

CSA大中华区专家1000多名,包括院士教授学者、政府及研究机构专家、产业界创新创业者等安全专家,他们在专业方向输出经验,通过参与联盟的技术创新、产业研究、论坛会议等方式为行业贡献,部分专家如下



Peter Major
联合国科技委主席



陈智敏
中国友谊促进会理事长
/公安部原副部长



倪光南
中国工程院院士



邬江兴
中国工程院院士



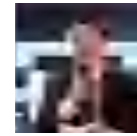
石文昌
中国人民大学教授



陈焱
浙江大学教授、
IEEE Fellow



杨学山
工信部原副部长



高林
中央网信办网络安全
协调局副局长



柴洪峰
中国工程院院士



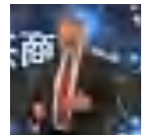
杨恩辉
加拿大皇家及工
程院两院院士



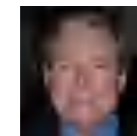
张亚勤
原百度总裁



周鸿祎
360 董事长



Tony Scott
原美国联邦CIO



Bob Flores
软件定义边界之父



李颀
日本工程院外籍院士



李挥
俄罗斯自然科学院院士



齐向东
奇安信董事长



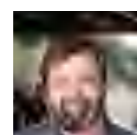
范渊
安恒信息董事长



Ernest yaly
俄罗斯国家杜马安全和
反腐败委员会执行主席



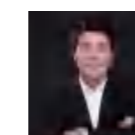
尹立波
国家工业信息安全
发展研究中心主任



John Kindervag
零信任之父
/CSA安全顾问



陈钟
北京大学教授



宁宇鹏
中宇万通董事长



陈本峰
云深互联 CEO

CORPORATE MEMBERS

企业会员

目前CSA企业会员已有1500+家,覆盖数据安全、零信任、隐私计算、云安全、人工智能等各个技术领域,企业类型包括世界500强科技公司、多数网络安全上市公司或独角兽公司、云服务商、云或安全用户、以及初创企业等。

CSA全球高级执行会员(部分)



CSA 全球会员(部分)



CSA大中华区理事单位(部分)



CSA大中华区会员单位(部分)



JOIN US
加入我们

成为CSA企业会员或专家会员，共同致力于云安全与下一代数字技术安全的全面发展。



更多联系：
CSA大中华区常务副秘书长 许女士 18218024060 melanxu@c-csa.cn
CSA大中华区办公室主任 叶女士 19925407556 candyye@c-csa.cn

一年一度,对联盟的优秀成员单位、优秀解决方案、优秀产品、优秀个人等进行荣誉表彰。

企业奖项

- 安全磐石奖**
表彰该解决方案综合性强,在方案思路和技术应用方面具备创新亮点,能够有效解决企业或用户在新型网络环境中的网络安全问题,可以为业内提供良好的参考价值及引领作用。
- 安全金盾奖**
表彰该单位的安全产品或安全服务具备核心竞争力,能够解决当前行业领域亟需解决的主要问题,在相关领域占据重要的市场份额,该单位的产品方案或安全服务被众多单位采用,且具备一定创新性,并得到业界认可,是相关安全领域的佼佼者。
- 安全创新奖**
表彰该单位在网络安全及各项新兴技术领域方向有创新的安全产品、新颖的解决方案,解决了行业当前关键的疑难问题,其关键技术指标达到国内外领先水平,为网络安全行业的发展提供新的思想和技术创新,能够实现产业化发展落地。
- 安全革新奖**
表彰该单位积极创新,勇于接纳网络安全新技术和新范式,自我革新,提升网络安全能力,整体建设处于行业领先地位,在业界有良好的声誉和影响力,是同领域其他企业网络安全建设的风向标。
- 育人奖**
鼓励企业重视网络安全人才培养,为员工提供学习安全技术和实践的机会,积极鼓励员工参与社会职业证书的学习,不断提高职业技能,倡导终身学习的理念。



优秀个人/项目奖项



主席特别奖

授予年度内为网络信息安全行业及联盟作出巨大贡献,同时提升了联盟在相关领域的影响力,为联盟认可度高及联盟主席特别颁发的个人荣誉奖。



领军人奖

授予年度内主导研究工作项目中体现了较强的专业水平和领导力个人,为联盟研究工作作出突出贡献。



研究贡献奖

授予年度内参与联盟多项研究工作项目,有较强的专业水平,并为联盟研究工作作出突出贡献。



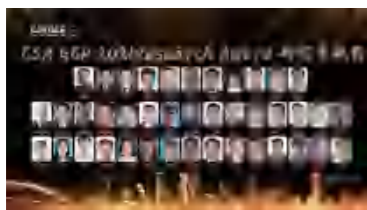
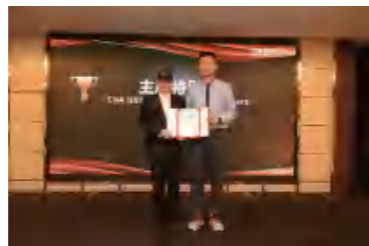
优秀项目奖

授予年度内优秀的原创成果,团队高效协作,输出的成果质量高,获得评审组及行业的认可。



服务英雄奖

授予为年度内不吝贡献个人时间,积极参与联盟各项工作的组织,共同为联盟会员、专家搭建良好分享平台,具有较强的学术活动组织能力,是联盟幕后工作的优秀志愿者。



附录 Appendix

CSA重要研究成果清单(部分)

| 领域 | 项目名称 |
|------|--|
| 数字安全 | 《数字安全框架》 《全球数字安全报告》(2022) |
| 云安全 | 《云控制矩阵CCM》(标准) 《云应用安全技术规范》(标准) 《云原生安全技术规范》(标准) 《云计算的11类顶级威胁》(2022) 《云计算关键领域安全指南》 《云渗透测试指南》 《企业架构参考指南》 《微服务架构模式》 《2022 SaaS安全调查报告》 《云事件响应(CIR)框架》 《如何设计安全的无服务器架构》 《保护云中医疗健康数据隐私》 《云安全现状、挑战和安全事件》 《云安全风险、合规性和配置不当报告》 《面向云客户的SaaS治理最佳实践》 《实现安全应用容器架构的最佳实践》 |
| 数据安全 | 《企业网络安全合规白皮书》 《洞察2022 - 云上数据安全性与重要事项》 《企业数据安全风险管理指南》 《个人信息保护法》个人数据合规行为准则 |

| | |
|------|--|
| 区块链 | 《共识算法与共识安全》 《加密资产交易所安全指南》 《区块链在医疗健康中的使用》 《区块链的十大攻击、漏洞及弱点》 《Hyperledger Fabric2.0 架构安全报告》 《区块链数据层安全与隐私保护设计指南》 |
| 零信任 | 《软件定义边界(SDP)标准规范1.0》(标准) 《软件定义边界(SDP)标准规范2.0》(标准) 《实战零信任架构》 《SDP抗DDos攻击》 《2021中国零信任全景图》分析报告 《基于SDP与DNS融合的零信任安全增强策略模型》 《CISO研究报告:零信任的部署现状及未来展望》 |
| 物联网 | 《物联网安全规范》(标准) 《物联网安全控制框架》(第二版) 《物联网安全控制框架指南》(第二版) |
| 隐私保护 | 《隐私科技白皮书》 基于《个人信息保护法》的企业个人信息保护合规风险控制验证框架1.0 《基于NIST网络安全框架的勒索软件风险管理内部报告》 |

扫码关注, 回复关键词“研究报告”获取报告完整版



CSA大中华区研究工作组

CSA大中华区研究工作组12个,围绕云安全、物联网安全、数据安全、零信任、隐私科技等方向输出了100多项行业指南,中国注册专家1000多人,包括院士、教授、事业单位专家、科研人员、企业技术高层、安全专家等领域从业10年以上专家。

数据安全工作组

2019年成立,旨在形成数据安全合规指南、基础体系、总体框架,储备数据安全和隐私保护关键技术。工作组专家来自国家信息中心、北京邮电大学、华为、腾讯、OPPO、阿里云、奇安信、顺丰、金山云、IBM等单位。



● 王安宇
OPPO终端安全领域总经理



● 高巍
咨询顾问深耕德系车企15年

物联网安全工作组

2018年成立,旨在推动物联网安全技术的进步,物联网安全标准体系的建立,以及先进适用技术成果和产品的推广应用。工作组成员来自华为、国家互联网应急中心、中国信通院、中国电信、中国银联、中国移动、中国联通、海康威视、奇安信等单位。

● 余晓光
华为高级安全专家
IoT安全实验室负责人



零信任工作组

2019年成立软件定义边界(SDP)工作组,2020年升级为零信任工作组。旨在促进零信任理念及相关技术在中国的应用实践,让中国每一家企业了解零信任安全,推广零信任理念及技术在中国企业的应用,促进中国的零信任安全市场的发展。工作组专家来自国家电网、腾讯、奇安信、深信服、云深互联、芯盾、持安科技等单位。



● 陈本峰
云深互创始人兼CEO

区块链安全工作组

2020年成立,旨在整合国内外的先进经验及实践,建立和发展区块链安全指南、最佳实践以及测试标准等。工作组专家来自中国电子学会、耶鲁大学、北京大学、北京理工大学、武汉大学、世界银行、知道创宇、赛博英杰、元界DNA、慢雾科技、安比实验室等单位。

● 黄连金
CSA大中华区研究院副院长
2021年中国“区块链”60人



隐私与个人信息保护法律工作组

2021年成立,重点研究数据安全与个人信息保护前沿法律和合规性问题,聚焦云、区块链、物联网、智慧城市等各种场景中数据安全、隐私与个人信息保护突出问题。工作组成员来自竹辉律师事务所、西北大学、360、中科曙光、上海网综所、上海CA、工商银行、埃森哲、恩智浦等单位。



● 原浩
江苏竹辉律师事务所合伙人



● 方婷
法学博士,西北大学法学院讲师

IAM工作组

2020年成立,基于实战经验和研究积累,致力于助推IAM技术在产业加速落地应用,为组织面临的身份安全挑战提供应对策略。工作组成员来自微软、华为、天融信、碧桂园、龙湖集团、德勤、竹云科技、星展银行、吉大正元、易安联、DXC、绵安科技等单位。

● 戴立伟
竹云科技副总裁



● 于继万
华为云服务安全专家



● 谢琴
天融信助理总裁



CSA大中华区研究工作组

多云安全工作组

2021年成立,致力于提供产业合作平台,凝聚行业共识,在解决企业多云环境下面临的安全问题,促进云安全生态的健康发展。工作组成员来自中国工商银行、360、深信服、启明星辰、顺丰科技、海尔集团、山石网科、赛宝认证中心、神州数码、新华三、东软集团等单位。

Team leader

● 魏小强

360集团云安全研究院副院长



隐私科技工作组

2021年成立,旨在促进国内隐私科技相关领域的专业交流,为行业提供隐私科技前沿技术及解决方案的风向标,为企业提供科技赋能隐私及个人信息保护的实践参考,培养隐私科技相关人才。工作组成员来自阿里云、安永、优衣库、平安科技、极氪汽车、E签宝、优刻得、OPPO、360数科、安恒信息等单位。



Team leader

● 高轶峰

安永网络安全及隐私保护咨询
大中华区合伙人



Team leader

● 徐震天

某跨国消费品公司北亚区
数据隐私官



全球 83+ 研究工作组

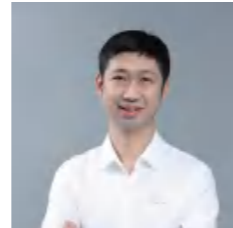
云原生安全工作组

2021年成立,旨在提升云原生类产品技术,针对云原生安全体系中涉及的每类技术制定相应标准,推动云原生安全技术在中国的应用发展,创造一个更安全更便利的网络环境。工作组成员来自绿盟科技、腾讯、公安三所、工商银行、深圳国家金融科技测评中心、浙江大华、浪潮云、中国电信研究院、中孚信息、亚信安全、北森等单位。

Team leader

● 刘文懋

绿盟科技首席创新官



Team leader

● 谢奕智

腾讯云主机安全
容器安全产品负责人



云应用安全工作组

2021年成立,旨在引领云应用安全(包括但不限于SaaS应用,PaaS和IaaS的应用程序部分,以及其他应用软件)标准的制定,输出云应用安全实践指南、云应用安全评估认证等的成果,助力云厂商提升云应用类产品在生命周期各阶段的安全性、提升云应用类产品的整体安全能力。工作组成员来自北森、公安三所、华为、江南天安、金山云、360、神州数码、中国电信研究院等单位。

Team leader

● 郭鹏程

云安全联盟大中华区助理院长
某SaaS独角兽首席信息安全官



Team leader

● 陈妍

公安部第三研究所检测中心云计算
与公安大数据测评实验室主任



SASE工作组

2021年成立,致力于推动SASE技术在中国的应用发展,创造一个更安全更便利的网络环境,推动用户间的经验分享与交流,推广国内先进落地经验。工作组成员来自深信服、中国电信、新华三、Fortinet、绿盟科技、白山云、启明星辰、缔盟云、奇安信、安恒信息、安全狗、万科等单位。



Team leader

● 林冠桦

深信服SaaS安全业务负责人



Team leader

● 何国锋

中国电信研究院安全技术
研究所所长

元宇宙技术安全工作组

2022年成立,旨在整合行业各方力量,推动元宇宙技术安全的专题研究,系统梳理元宇宙技术安全的产业需求、发展现状和未来趋势,引导产业形成元宇宙技术安全的落地方案和客户最佳实践。工作组成员来自北京大学、清华大学、武汉大学、中国人民大学、重庆邮电大学、华中科技大学、中国信通院、中国移动、腾讯、海尔集团、沃尔玛、观安信息、铭威信息、新奥集团等单位。

Team leader

● 陈钟

北京大学教授、元宇宙技术研究
所所长、区块链研究中心主任

