云原生安全与CSA人才培养

汇报人：李岩（北京老李）

目录

CONTENTS

- 云原生时代与人才发展
  Cloud native and talent training
- 组织级云原生安全成熟度
  Cloud-native security maturity at the organization level
- CSA云原生安全人才培养
  CSA cloud-native security related work
- CSA 数字安全人才体系2.0
  CSA Digital Security Talent System 2.0

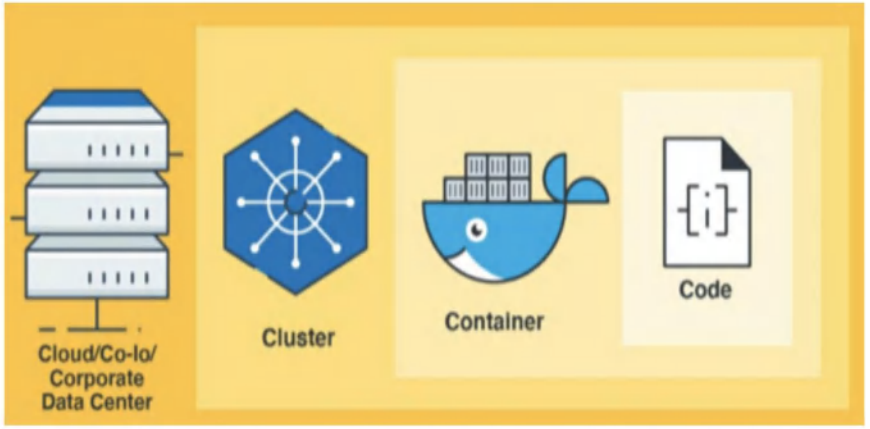
1 云原生时代与人才发展

Cloud native and talent training

云原生时代IT安全人才的需求与发展

“π”型人结合了广度和多种深度专长

云原生安全的**4C:**云安全、集群安全、容器安全、开发安全



云原生时代需要的IT安全人才是具备云原生技术栈知识、安全加固和渗透防护能力、开发运营一体化DevSecOps思维以及持续学习和自我提升能力的人才。

- 了解微服务架构和分布式环境，具备对云原生领域相关开源、主流安全厂商的产品功能和特性做对比、测试的能力
- 因此IT安全人才需要具备开发运营一体化DevSecOps的思维，能够与开发团队紧密合作，确保安全策略与业务需求同步更新。
- 能够对照业界最佳实践对容器和K8S环境进行安全加固及渗透工作，确保云原生环境的安全性。

云原生时代安全组织的角色与人才要求

角色定义	简述
安全冠军	帮助产品团队和开发人员采用与组织一致的安全计划，通常是已经从事软件或基础设施的开发人员或管理人员。持续评审其产品团队内针对威胁、漏洞和风险的安全状况。它可以作为混合角色共享。
安全领航者	领导策略来沟通关键的计划和成功案例，并评估安全工具和方法在整个组织、各个团队和业务领域中的采用影响。将安全计划与业务价值和战略目标保持一致。将实现安全和业务目标的高级数字战略与低级开发人员目标连接起来。协助管理和修复对应用程序造成的安全风险、漏洞和威胁。
解决方案架构师	开发解决方案架构和相关系统组件以满足用户需求。设计系统和系统间的接口，并确定目标环境的影响，包括但不限于安全状况。
安全构架师	与业务部门合作，讨论如何设计应用程序和使用基础设施服务（包括云），以安全的方式达成于业务目标。制定方法、框架和模式，并帮助开发人员遵循安全开发最佳实践。识别未来安全方法以演进现有的实践，应对行业、监管和技术变革，并确定DevSecOps的战略和运营适应性（例如，控制措施的左移或右移）。与开发人员一起和高级业务利益相关者合作，为部署流水线和仓库的安全方式、方法和使用自动化工具提供建议和评估。

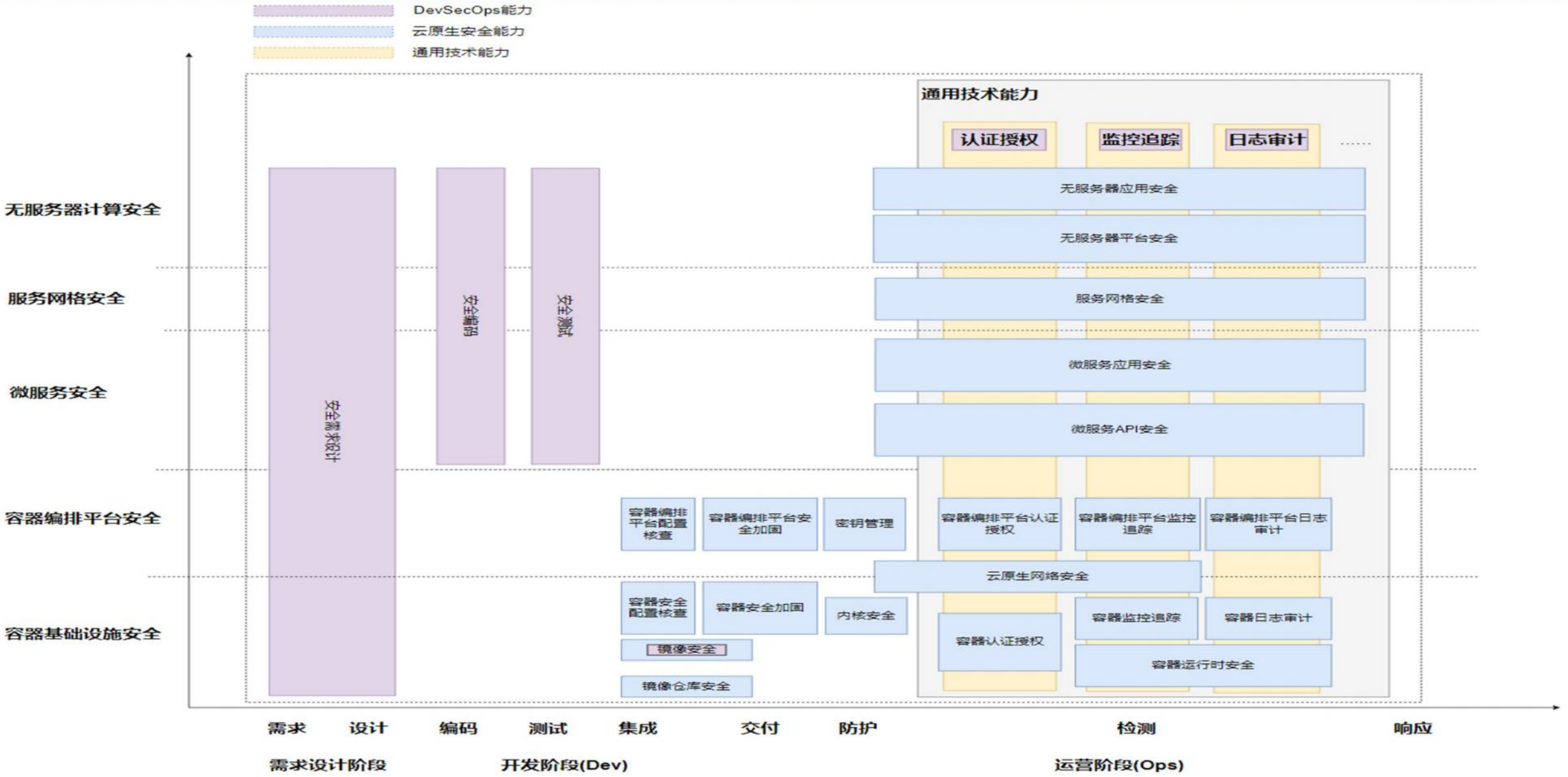
云原生时代安全组织的角色与人才要求

角色定义	简述
应用程序安全工程师	识别应用程序代码中的潜在缺陷，并通过修复安全问题来缓解漏洞。应用安全编码和测试标准，并记录安全编码指南。将安全测试工具（如静态和动态应用程序测试工具）集成进源代码仓库和持续集成和交付的流水线中。对应用程序代码应用安全控制（如加密、标识和身份验证），以减少攻击面并最大程度地降低被利用风险。
软件开发人员	与架构师一起识别、设计和编写代码实现软件特性。他们将帮助测试、维护和更新产品，以确保所有安全、性能和功能问题得到解决。安全角色和成果使开发人员能够根据软件工程方法论、工具、实践以及安全代码指南安全地编写代码。
云开发者运营工程师	配置和运营云基础设施，包括服务器、存储和网络。使用持续集成和部署方法自动配置云基础设施和应用程序
集成工程师	有助于确保安全活动应用于集成的软件包和集成的应用程序特性。引入影响整个应用程序的整体应用程序安全控制和过程-利用工具在运行时进行完整性校验并扫描应用程序。
性能测试人员	负责编写和执行负载和压力测试基础设施、平台和应用程序的测试计划。
安全测试人员	解决软件测试阶段的安全问题，包括风险接受、安全验收标准和安全测试方法。定期执行手动渗透测试，以暴露应用程序和基础设施的弱点，并确认安全强制执行功能的正确实施。根据测试输出提出修复建议。
安全运营工程师	提供有关云、基础设施和平台服务的安全状况的建议。在基础设施和平台上应用系统加固实践，并确保强大的安全机制。执行漏洞扫描和修复，以减少基础设施上的攻击面。

2 组织级云原生安全成熟度

Cloud-native security maturity at the organization level

CSA 组织级云原生安全成熟度



组织级云原生安全成熟度


CSA GCR C002—2022

CSA 云安全联盟标准

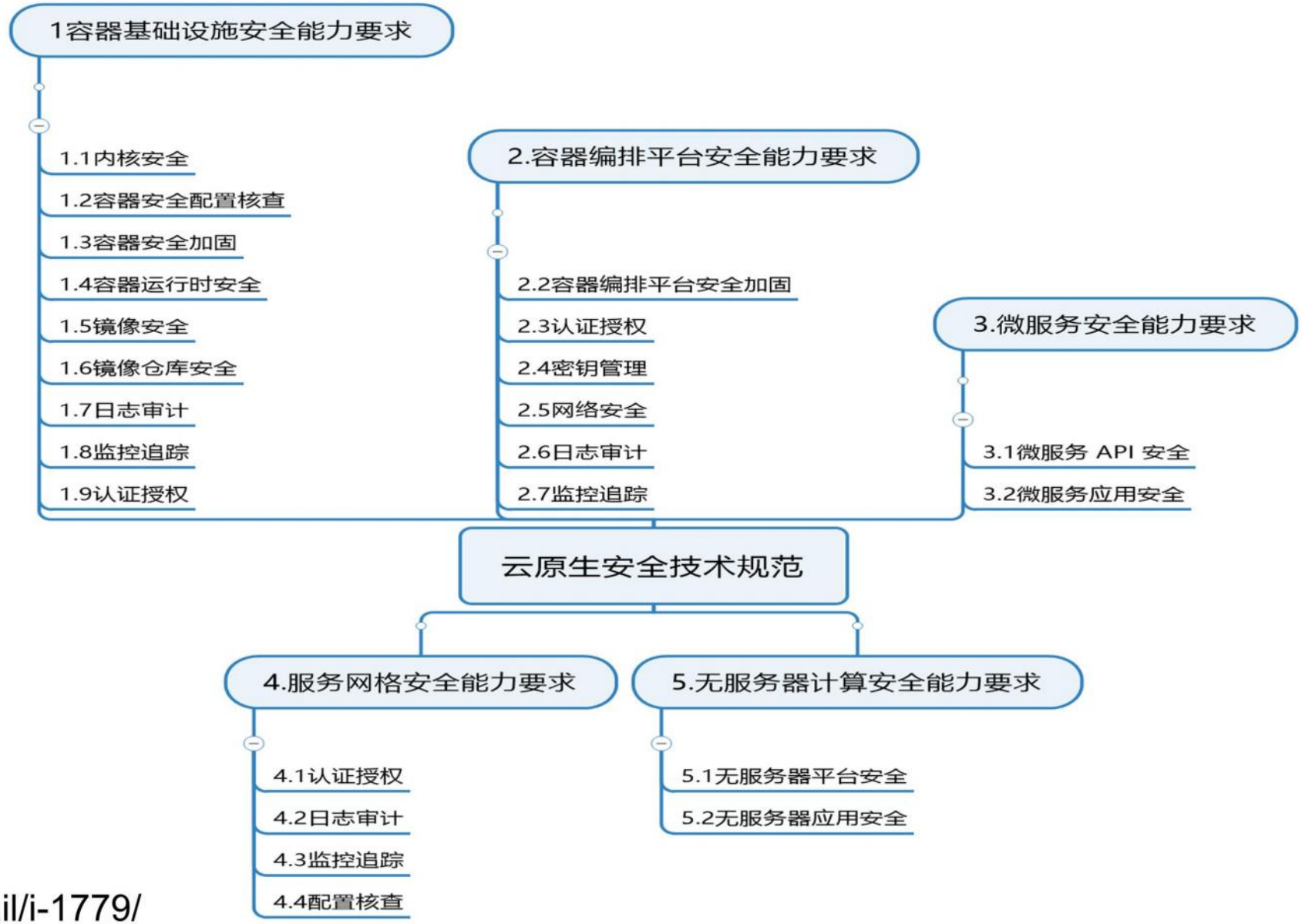
CSA GCR C002—2022

云原生安全技术规范

Cloud Native Security Technology Specification

2022-05-05 发布

云安全联盟大中华区　　发布



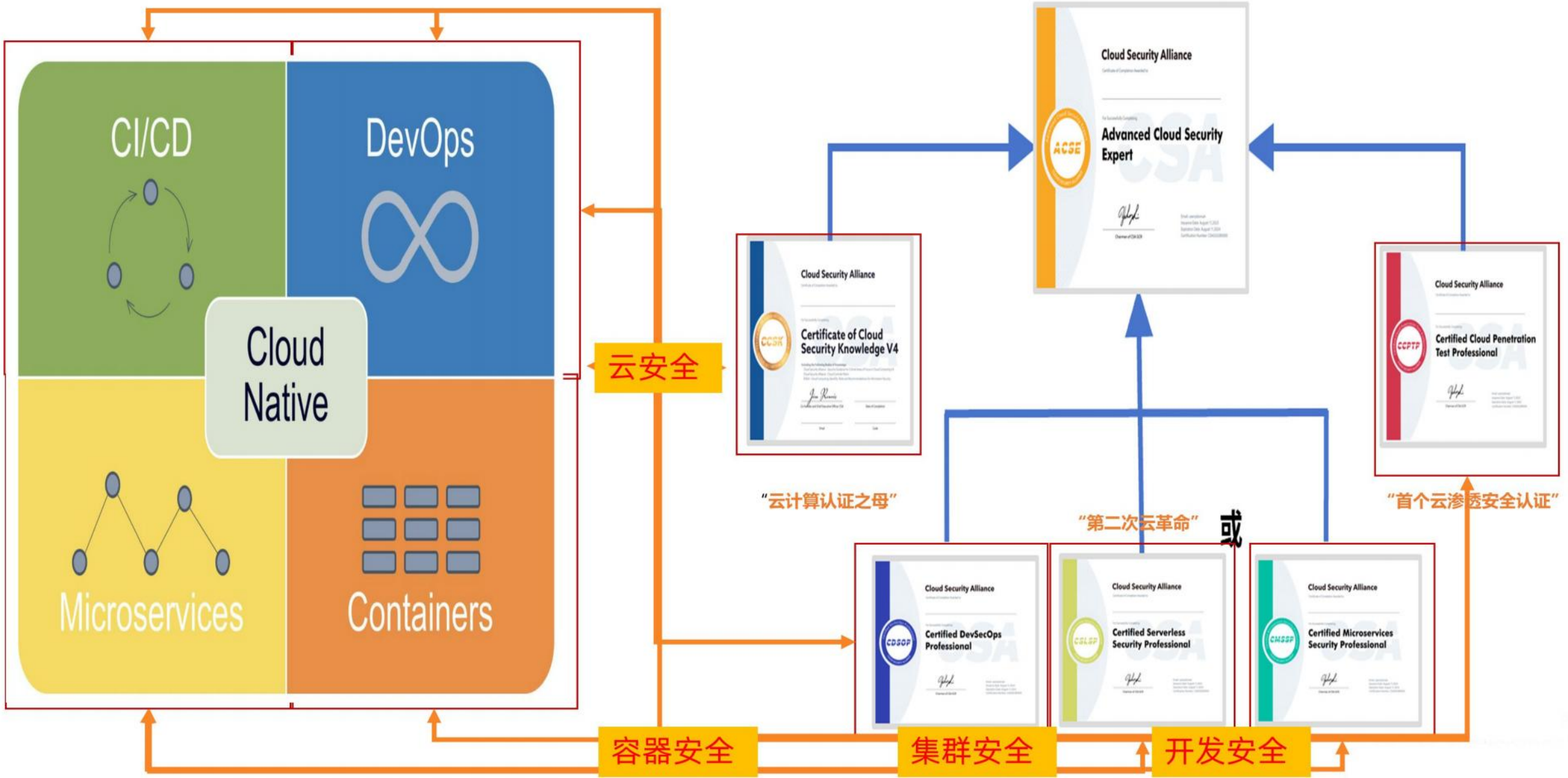
https://c-csa.cn/research/results-detail/i-1779/

3 CSA云原生安全人才培养

CSA cloud-native security related work

ACSE-云安全全栈能力培养学习体系

ACSE-云安全全栈能力培养学习体系



ACSE中级课程-CCPTP云渗透测试（2023年已上线）

CSA研讨会

CSA CCPTP（Certified Cloud Penetration Test Professional）云渗透测试认证专家，认证与培训项目由国际云安全联盟中华区发布，是全球首个针对云环境渗透测试能力的认证课程，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。

课程时长：五天课程

CCPTP®
Certified
Cloud Penetration Test Professional
理论考试

CCPTP®
Certified
Cloud Penetration Test Professional
实操考试

CCPTP
云渗透测试认证专家
(Certified Cloud Penetration Test Professional)

1 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

2 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

3 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

4 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

5 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

6 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

7 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

8 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

9 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

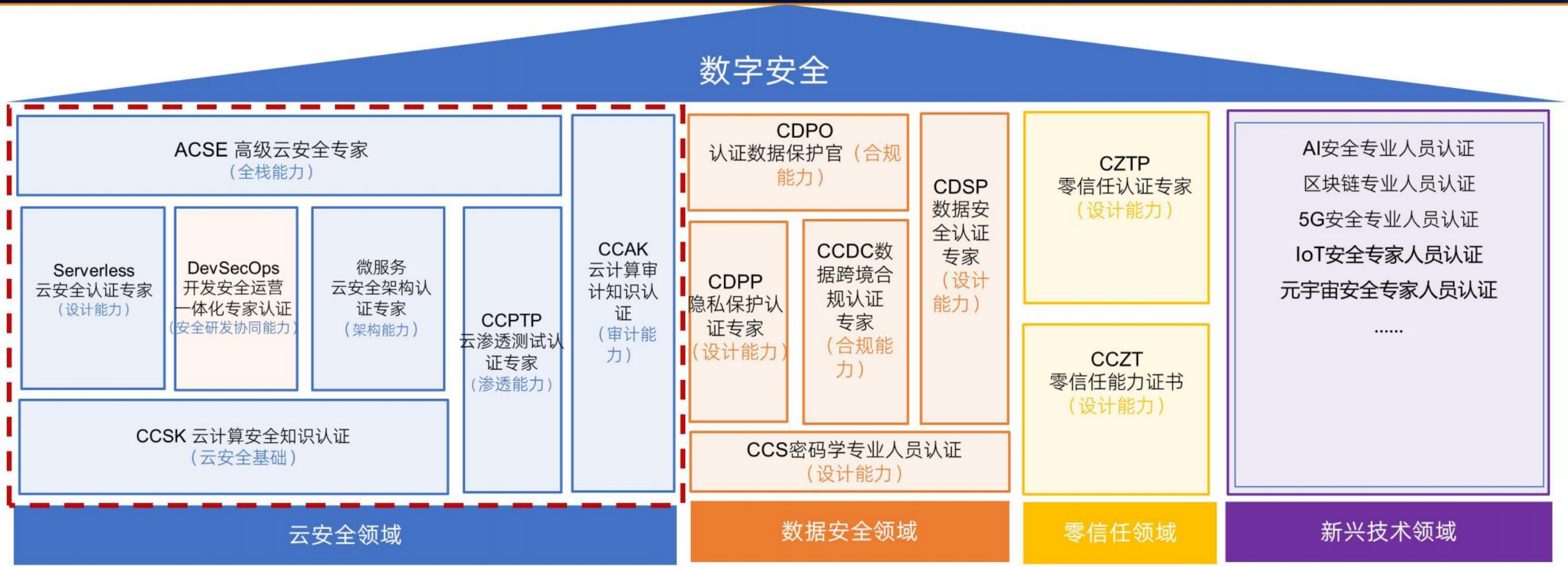
10 云基础设施层渗透测试
- 云基础设施攻击面、路径与核心目标概述
- 云计算网络下的渗透测试技巧
- 多租户环境下网络渗透技术
- 混合云及其他渗透测试方法

4 CSA 数字安全人才体系2.0

CSA Digital Security Talent System 2.0

CSA 数字安全人才体系2.0

CSA研讨会



专业方向能力提升，获得国际认证

数字安全人才基础课程

信息安全治理、数据安全导论、密码学、区块链、云安全、数据安全、零信任等理论基础

（零基础 IT人员/在校学生）

CSA GCR cloud security GREATER CHINA REGION alliance ®

TCCS

NSFOCUS 绿盟科技

安易科技 ANESEC TECHNOLOGY

THANKS